ID: 686188
Sample Name: 0mvOExDB0u
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:21:37
Date: 18/08/2022
Version: 35.0.0 Citrine

Table of Contents

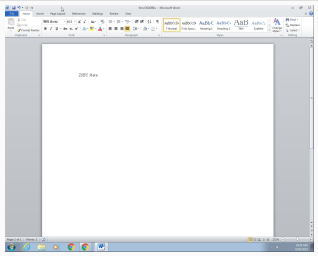
Windows Analysis Report

0mvOExDB0u

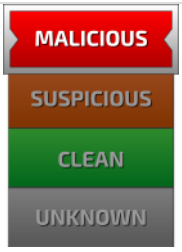
Overview

General Information

Sample Name:	0mvOExDB0u (renamed file extension from none to docx)
Analysis ID:	686188
MD5:	ba0bfeb5fe65522.
SHA1:	1f371d032ee40e..
SHA256:	a849eb6768d0d3.
Tags:	docx
Infos:	



Detection



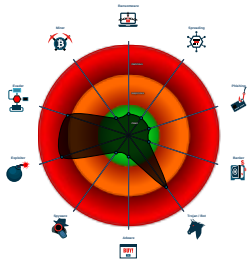
Follina CVE-2022-30190

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

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected Microsoft Office Expl…
- Antivirus detection for URL or domain
- Malicious sample detected (through…
- Antivirus detection for dropped file
- Contains an external reference to an…
- Uses dynamic DNS services
- Detected suspicious Microsoft Offic…
- Yara signature match
- Potential document exploit detected…
- Uses a known web browser user age…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2292 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	• 0x39:$a1: <Relationships • 0x3bd:$a2: TargetMode="External" • 0x3b5:$x1: .html!
document.xml.rels	INDICATOR_OLE_RemoteTemplate	Detects XML relations where an OLE object is refrencing an external target in dropper OOXML documents	ditekSHen	• 0x375:$olerel: relationships/oleObject • 0x38e:$target1: Target="http • 0x3bd:$mode: TargetMode="External

PCAP (Network Traffic)

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	• 0x4501:$a: PCWDiagnostic • 0x44f5:$sa3: ms-msdt • 0x4558:$sb3: IT_BrowseForFile=
sslproxydump.pcap	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x44e4:$re1: location.href = "ms-msdt:
sslproxydump.pcap	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BA0768EA.htm	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x2658:$a: PCWDiagnostic • 0x264c:$sa3: ms-msdt • 0x26af:$sb3: IT_BrowseForFile=
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BA0768EA.htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x263b:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BA0768EA.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\71E1C088.htm	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x2658:$a: PCWDiagnostic • 0x264c:$sa3: ms-msdt • 0x26af:$sb3: IT_BrowseForFile=
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\71E1C088.htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x263b:$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

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Antivirus detection for dropped file

Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Detected suspicious Microsoft Office reference URL

Networking

Uses dynamic DNS services

System Summary

Malicious sample detected (through community Yara rule)

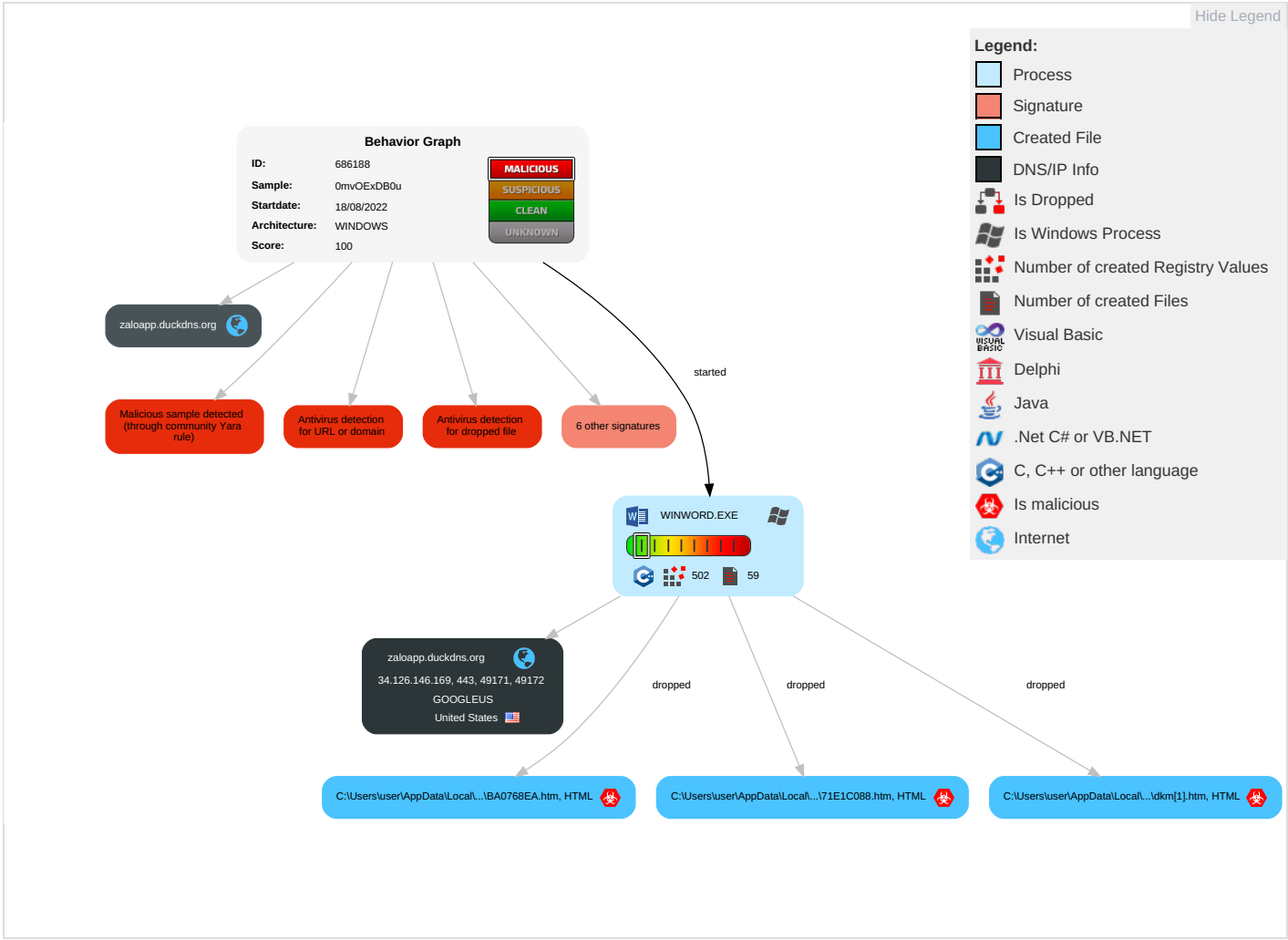
Persistence and Installation Behavior

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 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

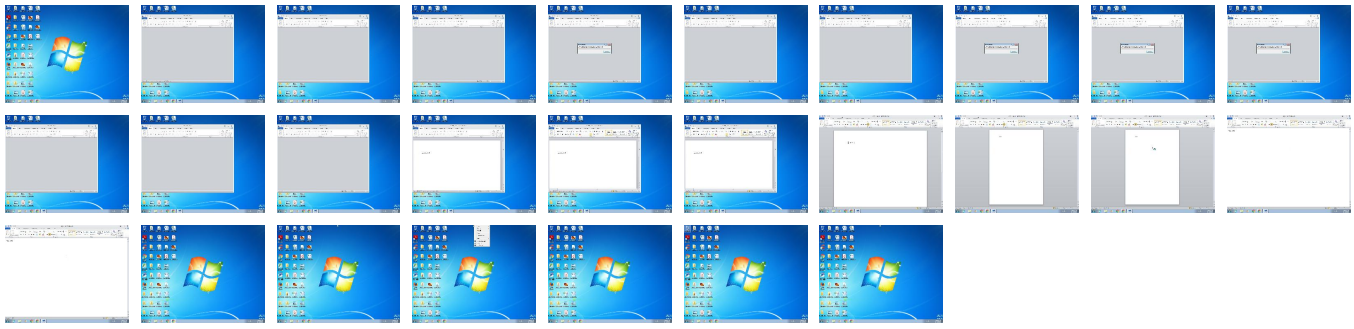
Behavior Graph

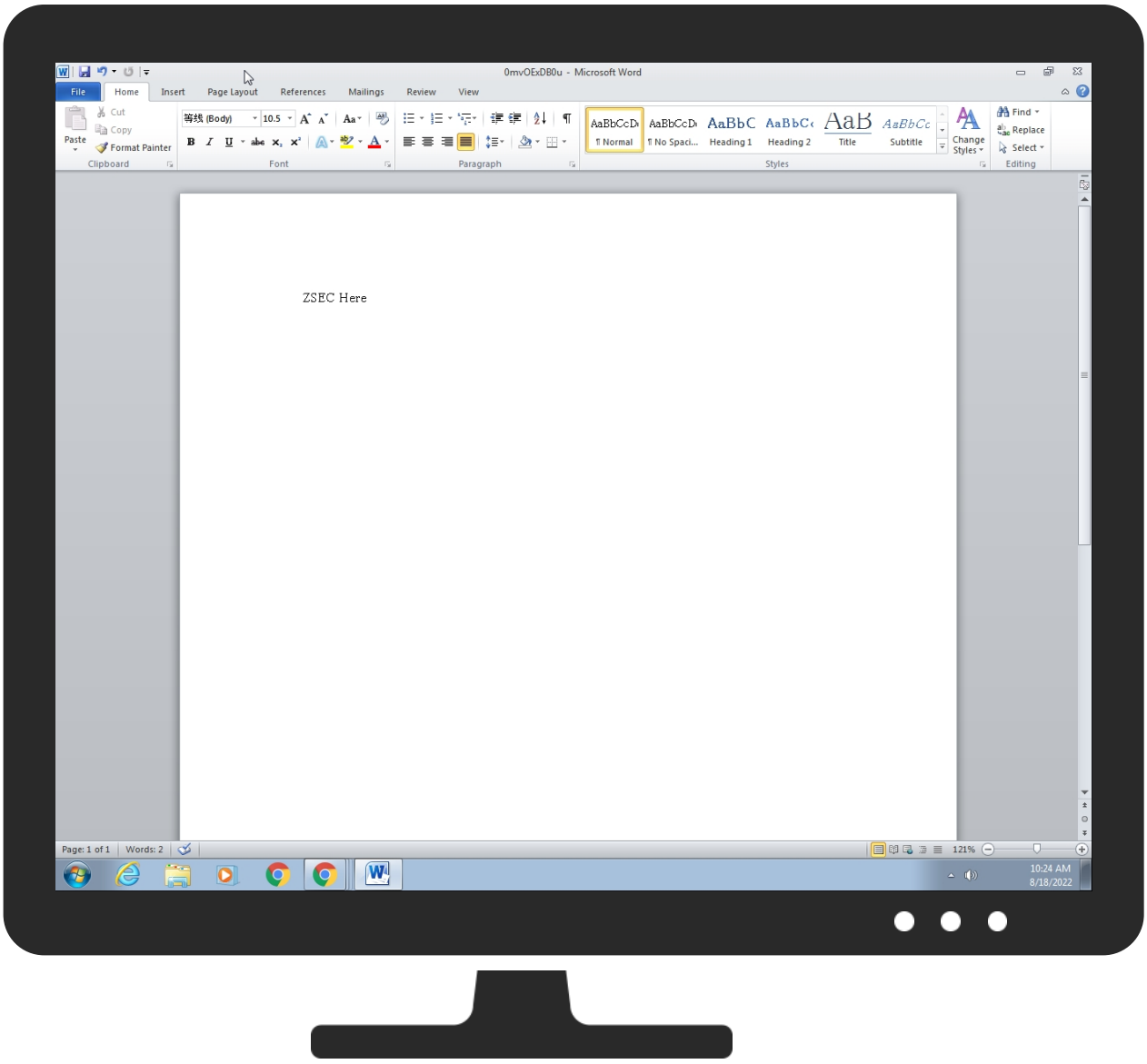


Screenshots

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
0mvOExDB0u.docx	47%	Virustotal		Browse
0mvOExDB0u.docx	29%	Metadefender		Browse
0mvOExDB0u.docx	59%	ReversingLabs	Document-Word.Trojan.Groooboor	
0mvOExDB0u.docx	100%	Avira	W97M/Dldr.Agent.G1	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BA0768EA.htm	100%	Avira	JS/CVE-2022-30190.G	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\dkm[1].htm	100%	Avira	JS/CVE-2022-30190.G	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\71E1C088.htm	100%	Avira	JS/CVE-2022-30190.G	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://zaloapp.duckdns.org/dkm.html	100%	Avira URL Cloud	malware	
http://https://zaloapp.duckdns.org/dkm.htmlyX	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
zaloapp.duckdns.org	34.126.146.169	true	false		unknown

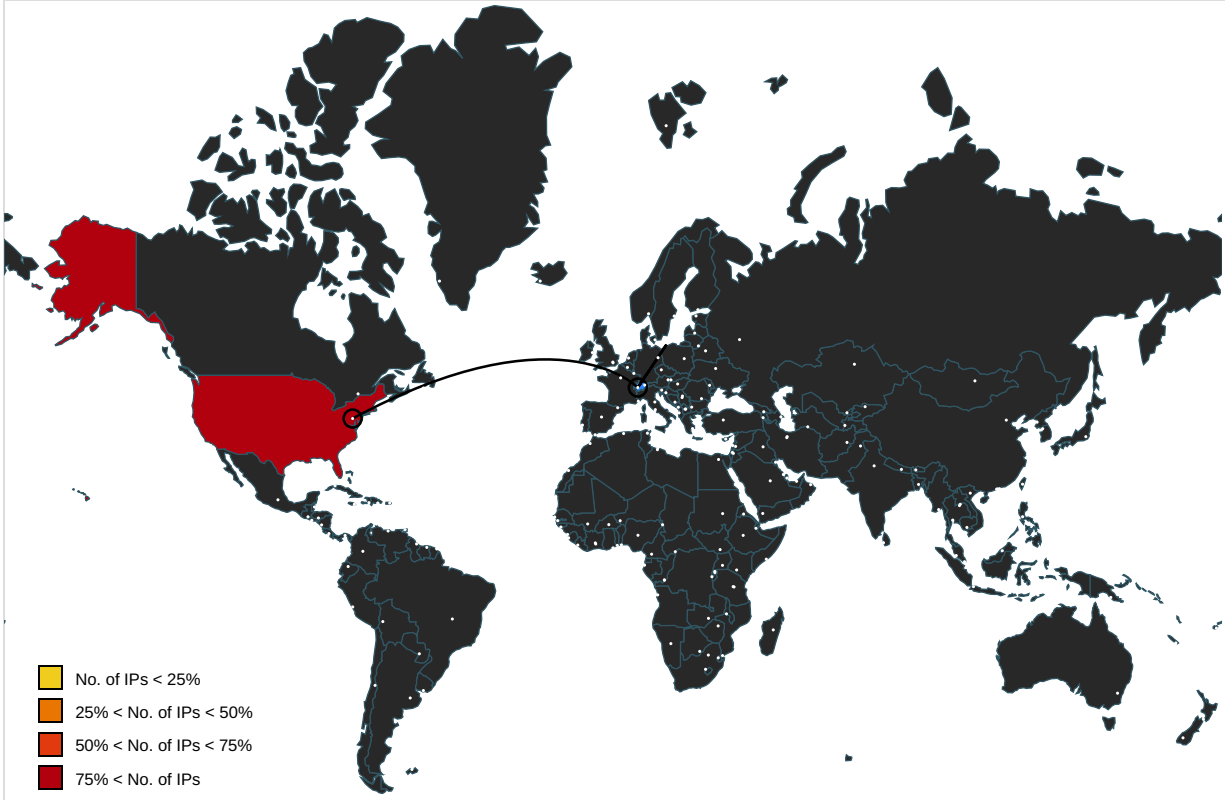
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://zaloapp.duckdns.org/dkm.html	false	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://zaloapp.duckdns.org/dkm.htmlyX	~WRF{54C3BB41-4824-4D76-9814-5AB27D135E39}.tmp.0.dr	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.126.146.169	zaloapp.duckdns.org	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	686188
Start date and time:	2022-08-18 10:21:37 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0mvOExDB0u (renamed file extension from none to docx)
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	10
Number of new started drivers analysed:	1
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winDOCX@1/19@15/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• 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.
- Report size getting too big, too many NtSetValueKey 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):	0.2853581143204819
Encrypted:	false
SSDEEP:	48:I3OeRBL7fCaX1yW7lCkH+ubmnsWr8O6HqGEGtH:KrLL8uQsO8DH7H
MD5:	B4EC9F550B9A27723E69F50CD728A1C3
SHA1:	D91C22484F51EC5FC78872A70BCB6385155EDAC7
SHA-256:	3B4196112446BA03696C1CB78B8DB2EBD4339365712938B47AE524E8D5BC92A1
SHA-512:	97AB4BBF2695F7D74C307C65C815898150A169BFF37842B37385194D712A281628C2AC4A457954AAA63B6C59A915967A85E023CFA2F00FD77EF121650053BB7F
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z8Z)-.c.C....>.S,...X.F...Fa.q.....w.]?..M....V^.....284..|.N..<.J,...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-{CC68C536-9CD4-4A67-8EC7-4282F7DE8CCB}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.6731627658053673
Encrypted:	false
SSDEEP:	96:KQBCyE1afuA2tW0K3JlqA/oGwofckwlvYTfQPSqpKCNGRsYi+ksYi+:fBE1aILK3yHGMYc
MD5:	DC3A133D8C9F7733D2F7C017149A71E9
SHA1:	2FC4E58E0CEF4234281962B3A15691F848E3E7B0
SHA-256:	8464C1FDEC7EC159B40629D5EE33F4A0CE1BD665E8B086EB61669610304DBBDD
SHA-512:	CF92EA1F9DDD8DFA30C2F7BE2F848B13BD72A18881333BAF87A430A50C0E93837CC1FAA0DE24033A2CD51167279F95A839C07E620E7881DC29A21EEA62EA5D 4C
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.....ByN.w?d..j.S,...X.F...Fa.q.....%.!n@.N....._.....22...vL...;...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):	3.9087992162143683
Encrypted:	false
SSDEEP:	3:yVlgsRlzfrSwWc17LWDyPgmIiXNiMUSmRZ276:yPblzfrSjc12D2INMKZ22
MD5:	69EAB43E70AC5A8DD1647EBCE3A05117
SHA1:	CD735629B8C99F5857D3BF2EEEFD239902B11C65
SHA-256:	E3CCCF8DDBC4968B975D8402A285A92B1C834A365EE7506F537FF72EC4AFDF7E
SHA-512:	0334D93ADD87F3CDFA29C7ED8A1A28B8B2F548217BB985E1B07F78EBB0F6C38435A6F61444C68F7EF1239B647DC99386AD586A373C127E748E2ADA345302BEE7
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.C.C.6.8.C.5.3.6.-.9.C.D.4.-.4.A.6.7.-.8.E.C.7.-.4.2.8.2.F.7.D.E.8.C.C.B.}...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):	0.28530361872249105
Encrypted:	false
SSDEEP:	48:I30jcpnRBuMMh2HhQ+/Xh/LtyHLc8fylYIN2ioEIrUj8j7E8j7UH:K0j+nLIh2HO2qeOINlg+H
MD5:	9EB88C7CC0659B145A02B67A553839F0
SHA1:	AFFAF04AC8D35EF1D7E067877AF80427BB9C38B3
SHA-256:	E442768F76531897C5AD2FF02566FD4D89E99B83488DFDA14FA092F6619533F9
SHA-512:	8D51595F54444FF14441090C0F32DF99421BDE5B4C78075F4B93D3FBF7054815161A221F48FE00710D8DAE798B6160162561B52670D457A0FBB0B224C0F9D447
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z..6..N.A...(.S,...X.F...Fa.q....._}...F.d....'.....{|.."M.[...ZO..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-{1B2D91C0-F32B-418D-958E-39DD37B1A090}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.22199601554512252
Encrypted:	false
SSDEEP:	48:I37ZUrBBA0dSa0LX2RXAn81RAgbwYLZiyifE5fES:K7ZC6MlXo6R
MD5:	46A9916CD1680C35383CC505149F2FBE
SHA1:	99438273FE2405D7A2A7FA3D633843C09156DE0F
SHA-256:	953FD74DDF202BE930B5D6E12374E40881F656A63C7FAFCD0DC3E8587FB473EA
SHA-512:	DF8F9A0FB1F0EFB5CE2E5B29F9D5ABBAED56835E854A875E62E2E645EFE9B6D4AF84ACF36BDCC7CEB6A9AAC1577D6FD7EDE19831F83E91D3EA233A801110F0E5
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z...+2SYL.....*.pS,...X.F...Fa.q.....].nr.E.q.....h.}..mf@...O.j.AP>.....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):	3.945130000864161
Encrypted:	false

SSDEEP:	3:yVlgsRlz8Nlhlc9Klj6lNG/lx9OlF0jl276:yPblzqw9KwlNQx08Z22
MD5:	DBF23C97AA8DAD1E2507C8A9950D0F4F
SHA1:	25239FB7E747517BEC244CEB79185EFDEB3D433C
SHA-256:	8094CA05E108A78D68916AD17D2EE6563EDF228C73040D365ED1CD230D837536
SHA-512:	B146BC6DCFE2968B46C7967785BB9D5F37B8159DF9306BEB1E5D703B1991E8618D9952FCF007A202ABDA13EC0F35FF86789DEC1ABCF78CB13F3B2C8EAE3B7 E5
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.1.B.2.D.9.1.C.0.-.F.3.2.B.-.4.1.8.D.-.9.5.8.E.-.3.9.D.D.3.7.B.1.A.0.9.0.}...F.S.D..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\dkm[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):	10046
Entropy (8bit):	0.39625399248312637
Encrypted:	false
SSDEEP:	6:qTIuJzhqIABckGX0ZifLSmmH8VztFCrOHfuG8+fg+OpyQzAw8Mhyu1JlYDXkZaXT:qTp4ckTcSxH8d2GZfgGw1sue4ZaoQL
MD5:	12DC70B699AD09EE089F094EABA151BE
SHA1:	77197B2B8C6BE62E565B3B4AA872CDCF4F34F68C
SHA-256:	1CB4E92945112FF717660F6E298ABFCF730D623144848403BDC876FED7EF030E
SHA-512:	E48B19AA1405A26F0C0B263FA3180438F4E2B52BC2C3EB7F8AEADF2D57EE85A8C80ACE7329F6F40B1B2000A003832D71D4D2587DC1D9EFFF129A17180D8D1F 31
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\dkm[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\dkm[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\dkm[1].htm, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
IE Cache URL:	http://https://zaloapp.duckdns.org/dkm.html
Preview:	<!doctype html>.<html lang="en">.<body>.<script>.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\71E1C088.htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	10046
Entropy (8bit):	0.39625399248312637
Encrypted:	false
SSDEEP:	6:qTIuJzhqIABckGX0ZifLSmmH8VztFCrOHfuG8+fg+OpyQzAw8Mhyu1JlYDXkZaXT:qTp4ckTcSxH8d2GZfgGw1sue4ZaoQL
MD5:	12DC70B699AD09EE089F094EABA151BE
SHA1:	77197B2B8C6BE62E565B3B4AA872CDCF4F34F68C
SHA-256:	1CB4E92945112FF717660F6E298ABFCF730D623144848403BDC876FED7EF030E
SHA-512:	E48B19AA1405A26F0C0B263FA3180438F4E2B52BC2C3EB7F8AEADF2D57EE85A8C80ACE7329F6F40B1B2000A003832D71D4D2587DC1D9EFFF129A17180D8D1F 31
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\71E1C088.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\71E1C088.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\71E1C088.htm, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100%

Reputation:	low
Preview:	<!doctype html>.<html lang="en">.<body>.<script>.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BA0768EA.htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	10046
Entropy (8bit):	0.39625399248312637
Encrypted:	false
SSDEEP:	6:qTIuJzhqIABckGX0ZifLSmmH8VztFCrOHfuG8+fg+OpyQzAw8Mhyu1JlYDXkZaXT:qTp4ckTcSxH8d2GZfgGw1sue4ZaoQL
MD5:	12DC70B699AD09EE089F094EABA151BE
SHA1:	77197B2B8C6BE62E565B3B4AA872CDCF4F34F68C
SHA-256:	1CB4E92945112FF717660F6E298ABFCF730D623144848403BDC876FED7EF030E
SHA-512:	E48B19AA1405A26F0C0B263FA3180438F4E2B52BC2C3EB7F8AEADF2D57EE85A8C80ACE7329F6F40B1B2000A003832D71D4D2587DC1D9EFFF129A17180D8D1F 31
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\BA0768EA.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\BA0768EA.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\BA0768EA.htm, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
Preview:	<!doctype html>.<html lang="en">.<body>.<script>.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{54C3BB41-4824-4D76-9814-5AB27D135E39}.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):	4096
Entropy (8bit):	1.9040508325537
Encrypted:	false
SSDEEP:	12:rl3bn+qFgsRYnhHao22p0hCaiDvChWWQtKh44kjC10SNBtKh44kFn7iVjuai4CIw:rgH/pp0Z7hWWQtKhrLtKh4iNO8Rs
MD5:	EE47AAD5E32A0B89C7A68F2D62FC4FE3
SHA1:	3A91BE006987E0E6CA2A06B3390EEDFA1FC92FCE
SHA-256:	8887507803A2E6E06733F15C39BC224D82CE9355DE19790BFC29C6C5363FFA71
SHA-512:	50CF40AAA68D1F77663E50E464FF11679DEA6D50AB9175E723C1D3E3E5508F29165E2E800BE4D1D79A56CFF3C011D930CC6918FE4C9DB8E6E3FDFD5D33C3D 91
Malicious:	false
Reputation:	low
Preview:	.........................>.. ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{99A334A3-9CCE-497E-9069-C0103D350D75}.tmp

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

Category:	dropped
Size (bytes):	1536
Entropy (8bit):	2.297626787151332
Encrypted:	false
SSDEEP:	12:YXHH3FlvtKh44gqI+zb1wuRjouQXemZFHXZ035ZEP:InHtKh5nuuqXfZRa3kP
MD5:	FAE056EB8034239A8BB76CF27BA316D2
SHA1:	33799DBEE29988E390F555AAAF29F3121547D4EC
SHA-256:	46A390F4B3A63A8D1324DF8FE943AC2DB2E81961A0888312EF7B7E6BB129792A
SHA-512:	353447AC2A51B8919CA1F3B468FDEEF5EADBE3FDFF771557D48B266C3DF70F5322084954565DC42EA59C0DAA24FFAAD147ED047287B9A5FE67D8938FA6CA80 25
Malicious:	false
Reputation:	low
Preview:	..... .!.".#.$.%.&.'.(.).*.+.,.-./.0.1.2.3.4.5.6.7.8.9.:.;.<.=.>.....L.I.N.K. .h.t.m.l.f.i.l.e. .".h.t.t.p.s.:././.z.a.l.o.a.p.p...d.u.c.k.d.n.s. ..o.r.g./.d.k.m...h.t.m.l.!.". .".". .\.p. .\.f. .0..... . ...Z.S.E.C. .H.e.r.e..... .....0...2...6...:...>..... ....gd.|q...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{F116EB59-8281-4971-8EDA-A57BD55E7891}.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
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\{6985C587-9066-4354-83B5-3F5856D587EC}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025663554541681895
Encrypted:	false
SSDEEP:	6:I3DPctHvxggLRViFz1qRXv//4tfnRujlw//+GtluJ/eRuj:I3DPCu6vYg3J/
MD5:	358C2EE90CF743E44AC340A608A0D639
SHA1:	DD52A1838416FBC90785D43C1690EF3E938C9C0E
SHA-256:	C0013D75C88E496EB9F2D2E518CA50B7DF71808A1983DBD9962FFCA2A986451C
SHA-512:	6A5B6D9FAB964544A94C71E2F1294627155F5C1C3B00051BA08B158A06F7C2C46F8E2E43B706C19611E0B059C6BAC770F40CB9C2C3C8B5631C9D8D893B38962
Malicious:	false
Preview:	......M.eFy...z8Z)-.c.C....>.S,...X.F...Fa.q.....B.....G...K.....284..|.N..<.J,.....x...x...x...x..... ....zV..... ..@..... .....

C:\Users\user\AppData\Local\Temp\{F4295DCF-A5E4-4365-A8E0-DC8DE21141CB}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025553961890493235

Encrypted:	false
SSDEEP:	6:I3DPcJB3N/NHvxggLRF31qFpB3RXv//4tfnRujlw//+GtluJ/eRuj:I3DPwZN/ZZmpBRvYg3J/
MD5:	757FB51249F13C7D7CF2E8A435D3A23D
SHA1:	D81504934D1D56BB4EA9E8668782EDD13B5AAABE
SHA-256:	9F6B8B9F1C3E178D35127C4C8AF75FE2D681ECF3940D6C0FB68E317AE1C76268
SHA-512:	0B9BBE263750C0E11C4BD9D431DBAD75A6C2E8FADBA481CD7521BFFCCADFC9FB37F779F3250873A86597EB19B9B89A39F3B1A60C9DF0EAA2BE5CBB05D79AB35C
Malicious:	false
Preview:	......M.eFy...z..6..N.A...(.S,...X.F...Fa.q.....2..,I....sK.m.....{|.."M.[...ZO.....x...x...x...x..... ....zV..... ..@..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\0mvOExDB0u.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=Thu Aug 18 16:23:00 2022, mtime=Thu Aug 18 16:23:00 2022, atime=Thu Aug 18 16:23:11 2022, length=13980, window=hide
Category:	dropped
Size (bytes):	1019
Entropy (8bit):	4.551296430094558
Encrypted:	false
SSDEEP:	12:8LR80gXg/XAlCPCHaXRBktB//GAEZX+W9DOjuicvbrqN64JNDtZ3YilMMEpxRljO:8Lek/XThO4ZeNeg9Dv3qmMu7D
MD5:	C65B2B7A9557CDC19D21E4D991F9812A
SHA1:	E559949AC9B95FF3B44D1B21A59B5A7168CB1509
SHA-256:	424FD3DE8D9C7BB5B820F7A1957D693EBB7CA87725631354305B7FBA96B5C138
SHA-512:	AFBB5F64F319ADBE9D9C3E571F7B4A519DB8276D4DBB0898D670A87C55625FCC2A1DE328C482D690B158EB7B500A3CAD6C987CA7CB690E5ED12D44BD89FF80E
Malicious:	false
Preview:	L.....F.... .....*'.....*'...6..0'....6.....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.....U...Desktop.d.....QK.X.U.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....h.2..6...U. .0MVOEX~1.DOC..L.....U..U.*...'.....0.m.v.O.E.x.D.B.0.u...d.o.c.x.....y.....-...8...[.....?J.....C:\Users\..#.....\\088753\Users.user\Desktop\0mvOExDB0u.docx.&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.0.m.v.O.E.x.D.B.0.u...d.o.c.x.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....088753.....D_....3N...W...9G..N..... .....[D_....3N...W...9G

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):	72
Entropy (8bit):	4.723328085908684
Encrypted:	false
SSDEEP:	3:bDuMJl4h6LBVomxWXmYh6LBVov:bCF6BV6N6BVy
MD5:	1E1C12B75E95D8C4BD23148E4A2288D8
SHA1:	278413E8CFC60AB4EE8CCE2DAA6D551CF001C78D
SHA-256:	BFBFB1A2D8168B3739C318EF769DE91B17CF827B2FF0AEF2B58013C0D17BDE94
SHA-512:	0C5AB8E903D669C242031CB30990997965F3FDD3E98CCC38A70FD765788EC91D77DB5470F6597655C14601D41061FB3FDFD0782977D6EB779E95CE0848C04DF
Malicious:	false
Preview:	[folders]..Templates.LNK=0..0mvOExDB0u.LNK=0..[misc]..0mvOExDB0u.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):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AEA

Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

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

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

C:\Users\user\Desktop\~$vOExDB0u.docx

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AEA
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

Static File Info

General

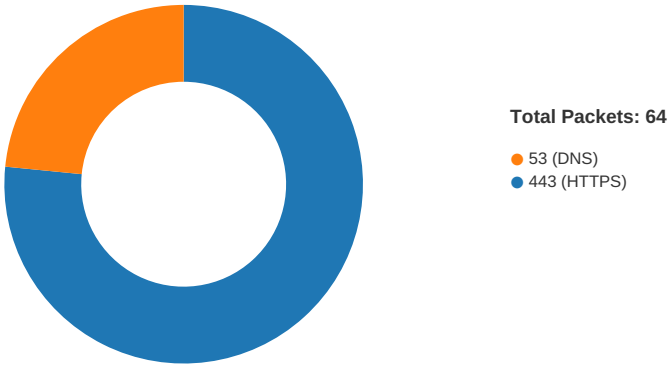
File type:	Microsoft OOXML
Entropy (8bit):	7.716105973707646
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	0mvOExDB0u.docx
File size:	13980
MD5:	ba0bfeb5fe6552217f5dd46eaf365db2
SHA1:	1f371d032ee40e1ff115f3d463246ab92b77e640
SHA256:	a849eb6768d0d38975faa5e2d0ad261e80468e3ec153e3511c41c86c7d58320b
SHA512:	96a241226deb38d1e0a87fe9dd3ffd26066af5c2fa0618011c1d8765451d84b3b3ce1cbb1480407330b17ab0c6536a2652d1b6ce79eedc0d21f7bd5f49506794
SSDEEP:	384:I9+EqKDGs8Pt5RqC+XahG/tL7EEig385jsU+9c3toPsh5tGQI581hgaQ:kUCah0tLRfc3WP++xB
TLSH:	8E526C70C618A11AF38F5538C119039AF2A6498753C23B397E592364FA5F3C3AB72745
File Content Preview:	PK.....!.J..qf...(.....[Content_Types].xmlUT....C...C..ux.....j.0.E.....6.J.(.....e.h...4NDeIH...w.;..4.M.1.3..3c..tW.d.!jgs6..,.+..v....sz....*a....!....j<. {...m.....s...J.3..R.p..H.a....b..f8...Y..)V.l2~.B..&O;.\..0.%.uc..3...R ....o)i

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 10:22:29.727519989 CEST	49171	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:29.727571964 CEST	443	49171	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:29.727643013 CEST	49171	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:29.739470959 CEST	49171	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:29.739531040 CEST	443	49171	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:30.381345987 CEST	443	49171	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:30.381658077 CEST	49171	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:30.396342993 CEST	49171	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:30.396378040 CEST	443	49171	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:30.397021055 CEST	443	49171	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:30.397164106 CEST	49171	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:30.678561926 CEST	49171	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:30.719372988 CEST	443	49171	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:30.985897064 CEST	443	49171	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:30.986017942 CEST	443	49171	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:30.986051083 CEST	49171	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:30.986083031 CEST	49171	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:30.986401081 CEST	49171	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:30.986413956 CEST	443	49171	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:37.106261969 CEST	49172	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:37.106331110 CEST	443	49172	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:37.106471062 CEST	49172	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:37.108634949 CEST	49172	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:37.108668089 CEST	443	49172	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:37.729034901 CEST	443	49172	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:37.729317904 CEST	49172	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:37.745069981 CEST	49172	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:37.745137930 CEST	443	49172	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:37.745790005 CEST	443	49172	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:37.776681900 CEST	49172	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:37.819430113 CEST	443	49172	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:38.339445114 CEST	443	49172	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:38.339561939 CEST	443	49172	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:38.339672089 CEST	49172	443	192.168.2.22	34.126.146.169

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 10:22:38.339729071 CEST	49172	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:38.339754105 CEST	443	49172	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:42.389955044 CEST	49173	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:42.389995098 CEST	443	49173	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:42.390104055 CEST	49173	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:42.393033981 CEST	49173	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:42.393057108 CEST	443	49173	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:43.015925884 CEST	443	49173	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:43.016022921 CEST	49173	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:43.022638083 CEST	49173	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:43.022651911 CEST	443	49173	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:43.023180008 CEST	443	49173	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:43.045002937 CEST	49173	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:43.087368011 CEST	443	49173	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:43.628778934 CEST	443	49173	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:43.628856897 CEST	443	49173	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:43.628931999 CEST	49173	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:43.635086060 CEST	49173	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:43.635117054 CEST	443	49173	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:43.635149956 CEST	49173	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:43.635157108 CEST	443	49173	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:44.919738054 CEST	49174	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:44.919780016 CEST	443	49174	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:44.919867992 CEST	49174	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:44.920417070 CEST	49174	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:44.920438051 CEST	443	49174	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:45.552894115 CEST	443	49174	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:45.553268909 CEST	49174	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:45.566783905 CEST	49174	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:45.566831112 CEST	443	49174	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:45.567609072 CEST	443	49174	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:45.569916010 CEST	49174	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:45.611463070 CEST	443	49174	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:46.175451040 CEST	443	49174	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:46.175620079 CEST	443	49174	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:46.175700903 CEST	49174	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:46.176309109 CEST	49174	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:46.176330090 CEST	443	49174	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:47.181730986 CEST	49175	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:47.181785107 CEST	443	49175	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:47.181859970 CEST	49175	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:47.182157993 CEST	49175	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:47.182188034 CEST	443	49175	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:47.808624029 CEST	443	49175	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:47.808806896 CEST	49175	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:47.822031021 CEST	49175	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:47.822077990 CEST	443	49175	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:47.822885990 CEST	443	49175	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:47.825006008 CEST	49175	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:47.871371984 CEST	443	49175	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:48.420911074 CEST	443	49175	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:48.421030045 CEST	443	49175	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:48.421329021 CEST	49175	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:48.421981096 CEST	49175	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:48.421994925 CEST	443	49175	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:48.463387012 CEST	49176	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:48.463448048 CEST	443	49176	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:48.463552952 CEST	49176	443	192.168.2.22	34.126.146.169

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 10:22:48.463743925 CEST	49176	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:48.463761091 CEST	443	49176	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:49.087546110 CEST	443	49176	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:49.087704897 CEST	49176	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:49.095005989 CEST	49176	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:49.095043898 CEST	443	49176	34.126.146.169	192.168.2.22
Aug 18, 2022 10:22:49.099301100 CEST	49176	443	192.168.2.22	34.126.146.169
Aug 18, 2022 10:22:49.099315882 CEST	443	49176	34.126.146.169	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 10:22:29.609472990 CEST	55868	53	192.168.2.22	8.8.8.8
Aug 18, 2022 10:22:29.717694998 CEST	53	55868	8.8.8.8	192.168.2.22
Aug 18, 2022 10:22:36.884685040 CEST	49688	53	192.168.2.22	8.8.8.8
Aug 18, 2022 10:22:36.993660927 CEST	53	49688	8.8.8.8	192.168.2.22
Aug 18, 2022 10:22:36.997009039 CEST	58836	53	192.168.2.22	8.8.8.8
Aug 18, 2022 10:22:37.105369091 CEST	53	58836	8.8.8.8	192.168.2.22
Aug 18, 2022 10:22:42.347714901 CEST	50134	53	192.168.2.22	8.8.8.8
Aug 18, 2022 10:22:42.366522074 CEST	53	50134	8.8.8.8	192.168.2.22
Aug 18, 2022 10:22:42.369672060 CEST	55275	53	192.168.2.22	8.8.8.8
Aug 18, 2022 10:22:42.388848066 CEST	53	55275	8.8.8.8	192.168.2.22
Aug 18, 2022 10:22:44.698024988 CEST	59915	53	192.168.2.22	8.8.8.8
Aug 18, 2022 10:22:44.807086945 CEST	53	59915	8.8.8.8	192.168.2.22
Aug 18, 2022 10:22:44.811660051 CEST	54408	53	192.168.2.22	8.8.8.8
Aug 18, 2022 10:22:44.918117046 CEST	53	54408	8.8.8.8	192.168.2.22
Aug 18, 2022 10:22:47.050482988 CEST	50108	53	192.168.2.22	8.8.8.8
Aug 18, 2022 10:22:47.067842960 CEST	53	50108	8.8.8.8	192.168.2.22
Aug 18, 2022 10:22:47.071903944 CEST	54723	53	192.168.2.22	8.8.8.8
Aug 18, 2022 10:22:47.180713892 CEST	53	54723	8.8.8.8	192.168.2.22
Aug 18, 2022 10:22:52.662750959 CEST	58062	53	192.168.2.22	8.8.8.8
Aug 18, 2022 10:22:52.769201040 CEST	53	58062	8.8.8.8	192.168.2.22
Aug 18, 2022 10:22:52.772412062 CEST	56703	53	192.168.2.22	8.8.8.8
Aug 18, 2022 10:22:52.791373014 CEST	53	56703	8.8.8.8	192.168.2.22
Aug 18, 2022 10:22:54.954214096 CEST	59241	53	192.168.2.22	8.8.8.8
Aug 18, 2022 10:22:54.973300934 CEST	53	59241	8.8.8.8	192.168.2.22
Aug 18, 2022 10:22:54.976391077 CEST	55244	53	192.168.2.22	8.8.8.8
Aug 18, 2022 10:22:54.993453026 CEST	53	55244	8.8.8.8	192.168.2.22
Aug 18, 2022 10:23:02.473371983 CEST	53958	53	192.168.2.22	8.8.8.8
Aug 18, 2022 10:23:02.503618002 CEST	53	53958	8.8.8.8	192.168.2.22
Aug 18, 2022 10:23:02.510858059 CEST	56020	53	192.168.2.22	8.8.8.8
Aug 18, 2022 10:23:02.527656078 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
Aug 18, 2022 10:22:29.609472990 CEST	192.168.2.22	8.8.8.8	0xe245	Standard query (0)	zaloapp.duckdns.org	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:36.884685040 CEST	192.168.2.22	8.8.8.8	0x52a8	Standard query (0)	zaloapp.duckdns.org	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:36.997009039 CEST	192.168.2.22	8.8.8.8	0xfc39	Standard query (0)	zaloapp.duckdns.org	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:42.347714901 CEST	192.168.2.22	8.8.8.8	0xf2ca	Standard query (0)	zaloapp.duckdns.org	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:42.369672060 CEST	192.168.2.22	8.8.8.8	0xdc64	Standard query (0)	zaloapp.duckdns.org	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:44.698024988 CEST	192.168.2.22	8.8.8.8	0x646c	Standard query (0)	zaloapp.duckdns.org	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:44.811660051 CEST	192.168.2.22	8.8.8.8	0x12f1	Standard query (0)	zaloapp.duckdns.org	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:47.050482988 CEST	192.168.2.22	8.8.8.8	0xe6e0	Standard query (0)	zaloapp.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 18, 2022 10:22:47.071903944 CEST	192.168.2.22	8.8.8.8	0x6703	Standard query (0)	zaloapp.duckdns.org	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:52.662750959 CEST	192.168.2.22	8.8.8.8	0xa1e7	Standard query (0)	zaloapp.duckdns.org	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:52.772412062 CEST	192.168.2.22	8.8.8.8	0x50dd	Standard query (0)	zaloapp.duckdns.org	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:54.954214096 CEST	192.168.2.22	8.8.8.8	0x7820	Standard query (0)	zaloapp.duckdns.org	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:54.976391077 CEST	192.168.2.22	8.8.8.8	0x2c87	Standard query (0)	zaloapp.duckdns.org	A (IP address)	IN (0x0001)
Aug 18, 2022 10:23:02.473371983 CEST	192.168.2.22	8.8.8.8	0x4c7a	Standard query (0)	zaloapp.duckdns.org	A (IP address)	IN (0x0001)
Aug 18, 2022 10:23:02.510858059 CEST	192.168.2.22	8.8.8.8	0x288a	Standard query (0)	zaloapp.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 18, 2022 10:22:29.717694998 CEST	8.8.8.8	192.168.2.22	0xe245	No error (0)	zaloapp.duckdns.org		34.126.146.169	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:36.993660927 CEST	8.8.8.8	192.168.2.22	0x52a8	No error (0)	zaloapp.duckdns.org		34.126.146.169	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:37.105369091 CEST	8.8.8.8	192.168.2.22	0xfc39	No error (0)	zaloapp.duckdns.org		34.126.146.169	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:42.366522074 CEST	8.8.8.8	192.168.2.22	0xf2ca	No error (0)	zaloapp.duckdns.org		34.126.146.169	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:42.388848066 CEST	8.8.8.8	192.168.2.22	0xdc64	No error (0)	zaloapp.duckdns.org		34.126.146.169	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:44.807086945 CEST	8.8.8.8	192.168.2.22	0x646c	No error (0)	zaloapp.duckdns.org		34.126.146.169	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:44.918117046 CEST	8.8.8.8	192.168.2.22	0x12f1	No error (0)	zaloapp.duckdns.org		34.126.146.169	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:47.067842960 CEST	8.8.8.8	192.168.2.22	0xe6e0	No error (0)	zaloapp.duckdns.org		34.126.146.169	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:47.180713892 CEST	8.8.8.8	192.168.2.22	0x6703	No error (0)	zaloapp.duckdns.org		34.126.146.169	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:52.769201040 CEST	8.8.8.8	192.168.2.22	0xa1e7	No error (0)	zaloapp.duckdns.org		34.126.146.169	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:52.791373014 CEST	8.8.8.8	192.168.2.22	0x50dd	No error (0)	zaloapp.duckdns.org		34.126.146.169	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:54.973300934 CEST	8.8.8.8	192.168.2.22	0x7820	No error (0)	zaloapp.duckdns.org		34.126.146.169	A (IP address)	IN (0x0001)
Aug 18, 2022 10:22:54.993453026 CEST	8.8.8.8	192.168.2.22	0x2c87	No error (0)	zaloapp.duckdns.org		34.126.146.169	A (IP address)	IN (0x0001)
Aug 18, 2022 10:23:02.503618002 CEST	8.8.8.8	192.168.2.22	0x4c7a	No error (0)	zaloapp.duckdns.org		34.126.146.169	A (IP address)	IN (0x0001)
Aug 18, 2022 10:23:02.527656078 CEST	8.8.8.8	192.168.2.22	0x288a	No error (0)	zaloapp.duckdns.org		34.126.146.169	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- zaloapp.duckdns.org

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	34.126.146.169	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 08:22:30 UTC	0	OUT	OPTIONS / HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: zaloapp.duckdns.org Content-Length: 0 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-08-18 08:22:30 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 18 Aug 2022 08:22:30 GMT Server: Apache/2.4.41 (Ubuntu) Allow: HEAD,GET,POST,OPTIONS Content-Length: 0 Connection: close Content-Type: text/html

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49172	34.126.146.169	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 08:22:37 UTC	0	OUT	HEAD /dkm.html HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: zaloapp.duckdns.org
2022-08-18 08:22:38 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 18 Aug 2022 08:22:38 GMT Server: Apache/2.4.41 (Ubuntu) Last-Modified: Thu, 02 Jun 2022 08:07:27 GMT ETag: "273e-5e0727f27f4ae" Accept-Ranges: bytes Content-Length: 10046 Vary: Accept-Encoding Connection: close Content-Type: text/html

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.22	49181	34.126.146.169	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 08:23:03 UTC	14	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 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 7a 61 6c 6f 61 70 70 2e 64 75 63 6b 64 6e 73 2e 6f 72 67 0d 0a 0d 0a Data Ascii: PROPFIND / HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0tr anslate: fContent-Length: 0Host: zaloapp.duckdns.org
2022-08-18 08:23:03 UTC	14	IN	HTTP/1.1 405 Method Not Allowed Date: Thu, 18 Aug 2022 08:23:03 GMT Server: Apache/2.4.41 (Ubuntu) Allow: HEAD,GET,POST,OPTIONS Content-Length: 311 Connection: close Content-Type: text/html; charset=iso-8859-1
2022-08-18 08:23:03 UTC	15	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 31 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title ></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.41 (Ubuntu) Server a

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.22	49182	34.126.146.169	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-08-18 08:23:04 UTC	15	OUT	GET /dkm.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: zaloapp.duckdns.org If-Modified-Since: Thu, 02 Jun 2022 08:07:27 GMT If-None-Match: "273e-5e0727f27f4ae" Connection: Keep-Alive
2022-08-18 08:23:05 UTC	15	IN	HTTP/1.1 304 Not Modified Date: Thu, 18 Aug 2022 08:23:04 GMT Server: Apache/2.4.41 (Ubuntu) Connection: close ETag: "273e-5e0727f27f4ae"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.22	49183	34.126.146.169	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 08:23:05 UTC	15	OUT	HEAD /dkm.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: zaloapp.duckdns.org Content-Length: 0 Connection: Keep-Alive
2022-08-18 08:23:06 UTC	16	IN	HTTP/1.1 200 OK Date: Thu, 18 Aug 2022 08:23:06 GMT Server: Apache/2.4.41 (Ubuntu) Last-Modified: Thu, 02 Jun 2022 08:07:27 GMT ETag: "273e-5e0727f27f4ae" Accept-Ranges: bytes Content-Length: 10046 Vary: Accept-Encoding Connection: close Content-Type: text/html

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.22	49184	34.126.146.169	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 08:23:07 UTC	16	OUT	HEAD /dkm.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: zaloapp.duckdns.org Content-Length: 0 Connection: Keep-Alive
2022-08-18 08:23:07 UTC	16	IN	HTTP/1.1 200 OK Date: Thu, 18 Aug 2022 08:23:07 GMT Server: Apache/2.4.41 (Ubuntu) Last-Modified: Thu, 02 Jun 2022 08:07:27 GMT ETag: "273e-5e0727f27f4ae" Accept-Ranges: bytes Content-Length: 10046 Vary: Accept-Encoding Connection: close Content-Type: text/html

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49173	34.126.146.169	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 08:22:43 UTC	0	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: zaloapp.duckdns.org

Timestamp	kBytes transferred	Direction	Data
2022-08-18 08:22:43 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 18 Aug 2022 08:22:43 GMT Server: Apache/2.4.41 (Ubuntu) Allow: HEAD,GET,POST,OPTIONS Content-Length: 0 Connection: close Content-Type: text/html

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49174	34.126.146.169	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 08:22:45 UTC	1	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 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 7a 61 6c 6f 61 70 70 2e 64 75 63 6b 64 6e 73 2e 6f 72 67 0d 0a 0d 0a Data Ascii: PROPFIND / HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: zaloapp.duckdns.org
2022-08-18 08:22:46 UTC	1	IN	HTTP/1.1 405 Method Not Allowed Date: Thu, 18 Aug 2022 08:22:45 GMT Server: Apache/2.4.41 (Ubuntu) Allow: HEAD,GET,POST,OPTIONS Content-Length: 311 Connection: close Content-Type: text/html; charset=iso-8859-1
2022-08-18 08:22:46 UTC	1	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 31 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.41 (Ubuntu) Server a

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49175	34.126.146.169	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 08:22:47 UTC	1	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 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 7a 61 6c 6f 61 70 70 2e 64 75 63 6b 64 6e 73 2e 6f 72 67 0d 0a 0d 0a Data Ascii: PROPFIND / HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: zaloapp.duckdns.org
2022-08-18 08:22:48 UTC	1	IN	HTTP/1.1 405 Method Not Allowed Date: Thu, 18 Aug 2022 08:22:48 GMT Server: Apache/2.4.41 (Ubuntu) Allow: HEAD,GET,POST,OPTIONS Content-Length: 311 Connection: close Content-Type: text/html; charset=iso-8859-1
2022-08-18 08:22:48 UTC	2	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 31 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.41 (Ubuntu) Server a

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49176	34.126.146.169	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 08:22:49 UTC	2	OUT	GET /dkm.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: zaloapp.duckdns.org Connection: Keep-Alive
2022-08-18 08:22:49 UTC	2	IN	HTTP/1.1 200 OK Date: Thu, 18 Aug 2022 08:22:49 GMT Server: Apache/2.4.41 (Ubuntu) Last-Modified: Thu, 02 Jun 2022 08:07:27 GMT ETag: "273e-5e0727f27f4ae" Accept-Ranges: bytes Content-Length: 10046 Vary: Accept-Encoding Connection: close Content-Type: text/html
2022-08-18 08:22:49 UTC	2	IN	Data Raw: 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 41 Data Ascii: <!doctype html><html lang="en"><body><script>//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49177	34.126.146.169	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 08:22:50 UTC	12	OUT	HEAD /dkm.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: zaloapp.duckdns.org Content-Length: 0 Connection: Keep-Alive
2022-08-18 08:22:51 UTC	12	IN	HTTP/1.1 200 OK Date: Thu, 18 Aug 2022 08:22:50 GMT Server: Apache/2.4.41 (Ubuntu) Last-Modified: Thu, 02 Jun 2022 08:07:27 GMT ETag: "273e-5e0727f27f4ae" Accept-Ranges: bytes Content-Length: 10046 Vary: Accept-Encoding Connection: close Content-Type: text/html

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49178	34.126.146.169	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 08:22:52 UTC	13	OUT	HEAD /dkm.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: zaloapp.duckdns.org Content-Length: 0 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-08-18 08:22:52 UTC	13	IN	HTTP/1.1 200 OK Date: Thu, 18 Aug 2022 08:22:52 GMT Server: Apache/2.4.41 (Ubuntu) Last-Modified: Thu, 02 Jun 2022 08:07:27 GMT ETag: "273e-5e0727f27f4ae" Accept-Ranges: bytes Content-Length: 10046 Vary: Accept-Encoding Connection: close Content-Type: text/html

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.22	49179	34.126.146.169	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 08:22:53 UTC	13	OUT	HEAD /dkm.html HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: zaloapp.duckdns.org
2022-08-18 08:22:54 UTC	13	IN	HTTP/1.1 200 OK Date: Thu, 18 Aug 2022 08:22:53 GMT Server: Apache/2.4.41 (Ubuntu) Last-Modified: Thu, 02 Jun 2022 08:07:27 GMT ETag: "273e-5e0727f27f4ae" Accept-Ranges: bytes Content-Length: 10046 Vary: Accept-Encoding Connection: close Content-Type: text/html

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.22	49180	34.126.146.169	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 08:22:55 UTC	14	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 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 7a 61 6c 6f 61 70 70 2e 64 75 63 6b 64 6e 73 2e 6f 72 67 0d 0a 0d 0a Data Ascii: PROPFIND / HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: zaloapp.duckdns.org
2022-08-18 08:22:56 UTC	14	IN	HTTP/1.1 405 Method Not Allowed Date: Thu, 18 Aug 2022 08:22:56 GMT Server: Apache/2.4.41 (Ubuntu) Allow: HEAD,GET,POST,OPTIONS Content-Length: 311 Connection: close Content-Type: text/html; charset=iso-8859-1
2022-08-18 08:22:56 UTC	14	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 31 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.41 (Ubuntu) Server a

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: **2292**, Parent PID: **576**

General

Target ID:	0
Start time:	10:23:11
Start date:	18/08/2022
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:	0x13f900000
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\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E202B14	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$vOExDB0u.docx	success or wait	1	6E280648	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\dkm[1].htm	unknown	1854	success or wait	1	7FEF0C43130	unknown
C:\Users\user\Desktop\0mvOExDB0u.docx	10759	313	success or wait	1	6E280648	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E25A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E25A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E25A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E280648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6E280648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6E280648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\77CBE	success or wait	1	6E280648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\77CBE	77CBE	binary	04 00 00 00 F4 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 74 30 77 5E 27 B3 D8 01 BE 7C 07 00 BE 7C 07 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6E280648	unknown

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

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Installer\UserData\S-1-5-18\Products\00004109D3000000010000 0000F01FEC\Usage	ProductFiles	dword	1427243058	1427243059	success or wait	1	6E280648	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Installer\UserData\S-1-5-18\Products\00004109D3000000010000 0000F01FEC\Usage	ProductFiles	dword	1427243059	1427243060	success or wait	1	6E280648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resili ency\DocumentRecovery\77CBE	77CBE	binary	04 00 00 00 F4 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 74 30 77 5E 27 B3 D8 01 BE 7C 07 00 BE 7C 07 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 F4 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 BE 7C 07 00 BE 7C 07 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6E280648	unknown

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

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

Disassembly

No disassembly