ID: 639039
Sample Name:
20220531_180800.rtf
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 22:56:31
Date: 03/06/2022
Version: 35.0.0 Citrine

Table of Contents

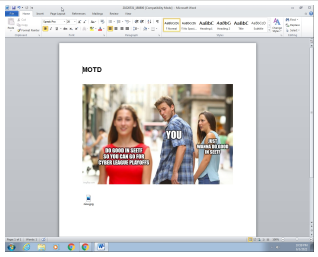
Windows Analysis Report

20220531_180800.rtf

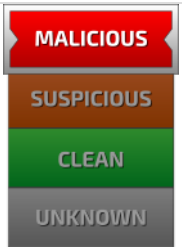
Overview

General Information

Sample Name:	20220531_180800.rtf
Analysis ID:	639039
MD5:	7b9c8e08371550..
SHA1:	ff8c9deb358b2d2..
SHA256:	b93326f795459d..
Infos:	



Detection



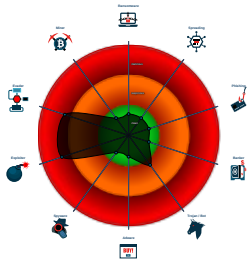
Follina CVE-2022-30190

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

Signatures

- Yara detected Microsoft Office Expl…
- Malicious sample detected (through…
- Contains an external reference to an…
- Detected suspicious Microsoft Offic…
- Obfuscated document found, RTF is…
- 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: 1424 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	Tobias Michalski, Christian Burkard, Wojciech Cie\305\233lak	• 0x39:$a1: <Relationships • 0x3b9:$a2: TargetMode="External" • 0x3b1:$x1: .html!
document.xml.rels	INDICATOR_OLE_RemoteTemplate	Detects XML relations where an OLE object is refrencing an external target in dropper OOXML documents	ditekSHen	• 0x375:$olerel: relationships/oleObject • 0x38e:$target1: Target="http • 0x3b9:$mode: TargetMode="External

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
sslproxydump.pcap	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x2e2d:$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\2B293583.htm	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x113c:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2B293583.htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\th1s[1].htm	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x113c:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\th1s[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\A0472FED.htm	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x113c:$re1: location.href = "ms-msdt:

Click to see the 1 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

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)

Data Obfuscation

Obfuscated document found, RTF is a DOCX

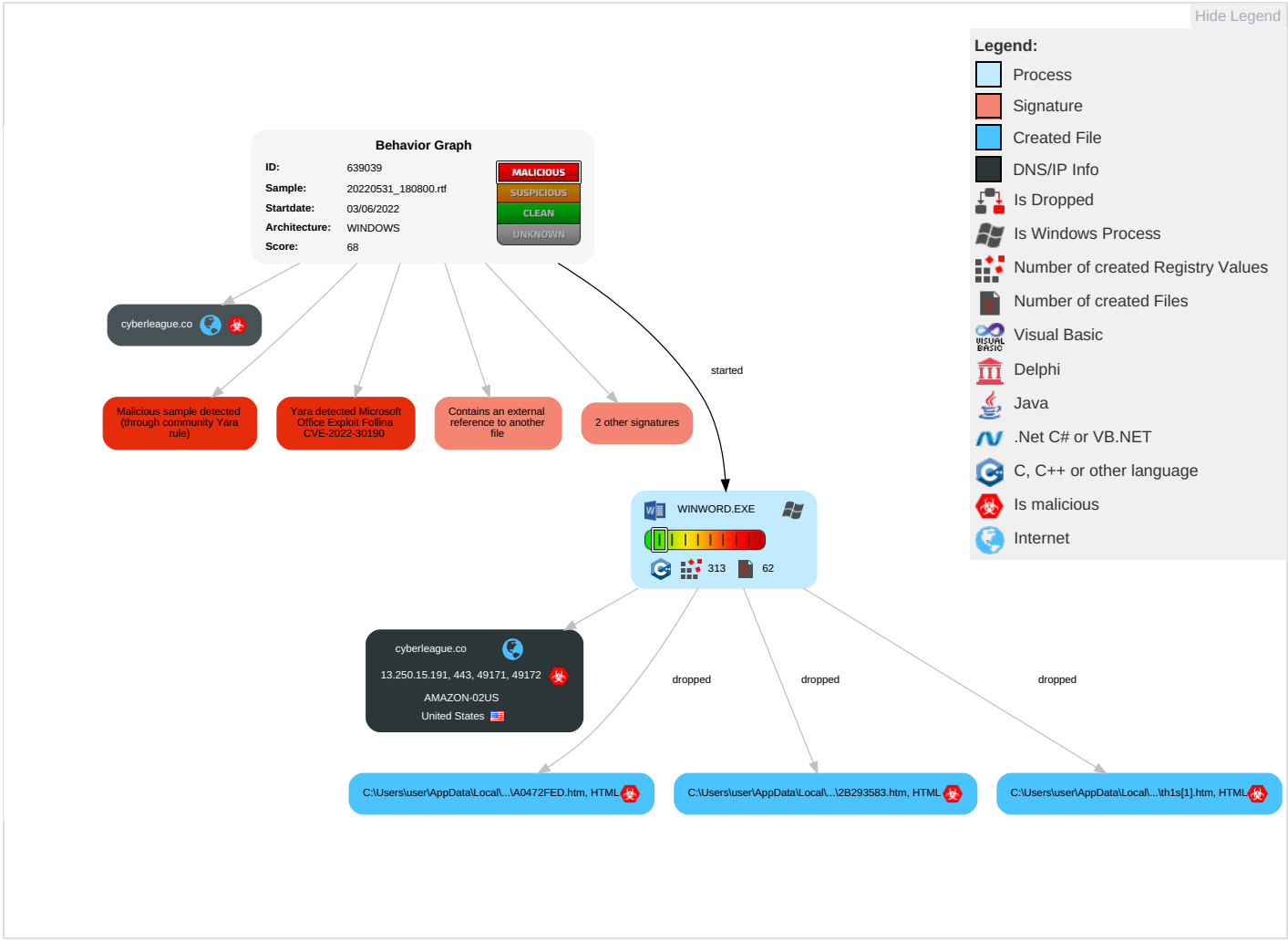
Persistence and Installation Behavior

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 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	1 Obfuscated Files or Information	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

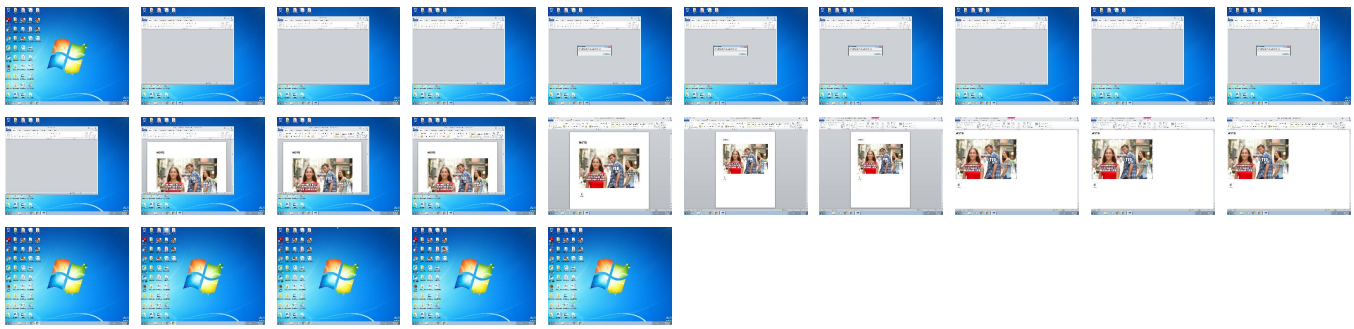
Behavior Graph

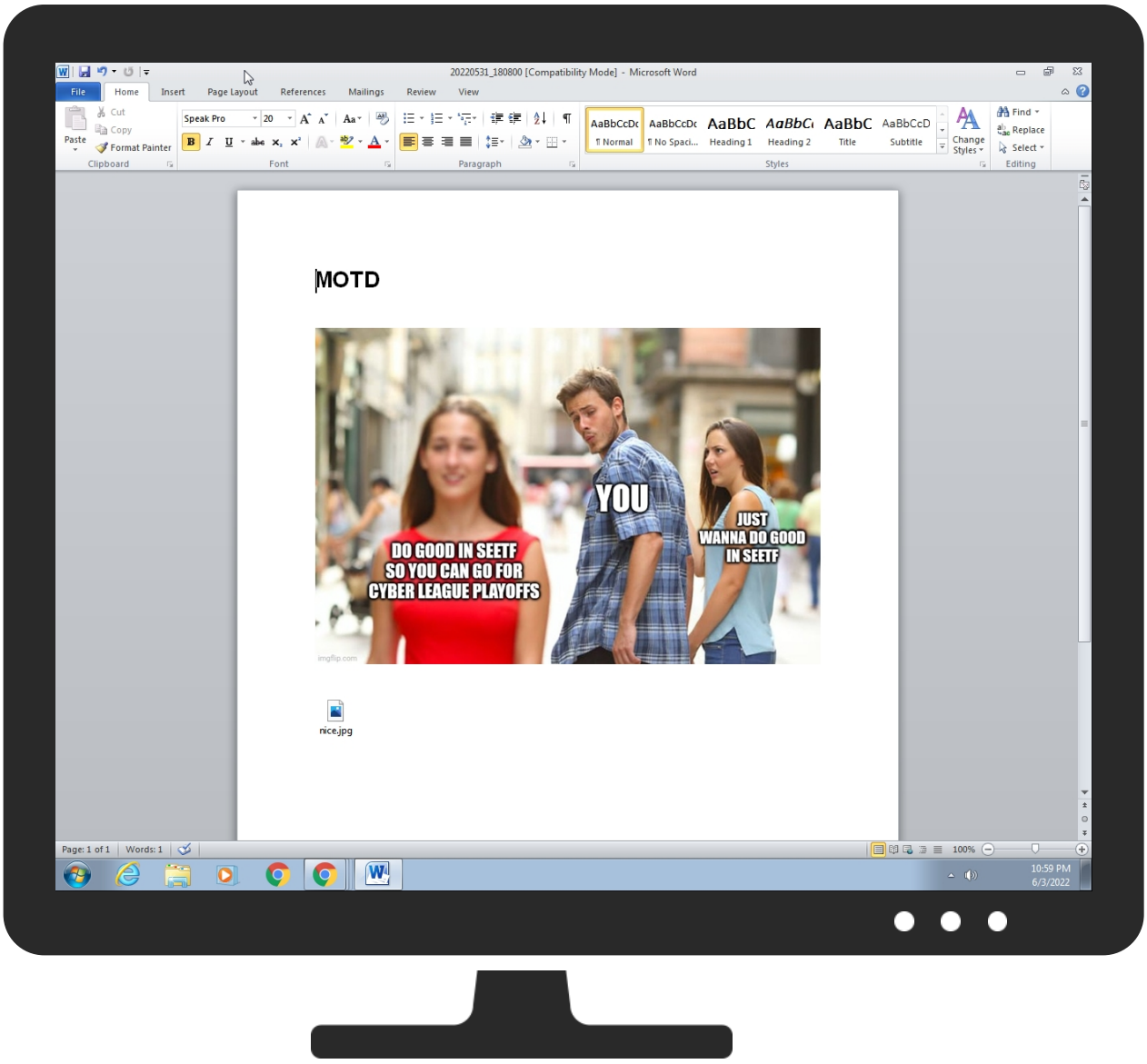


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cyberleague.co/th1s.htmlyX	0%	Avira URL Cloud	safe	
http://https://cyberleague.co/th1s.html	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cyberleague.co	13.250.15.191	true	true		unknown

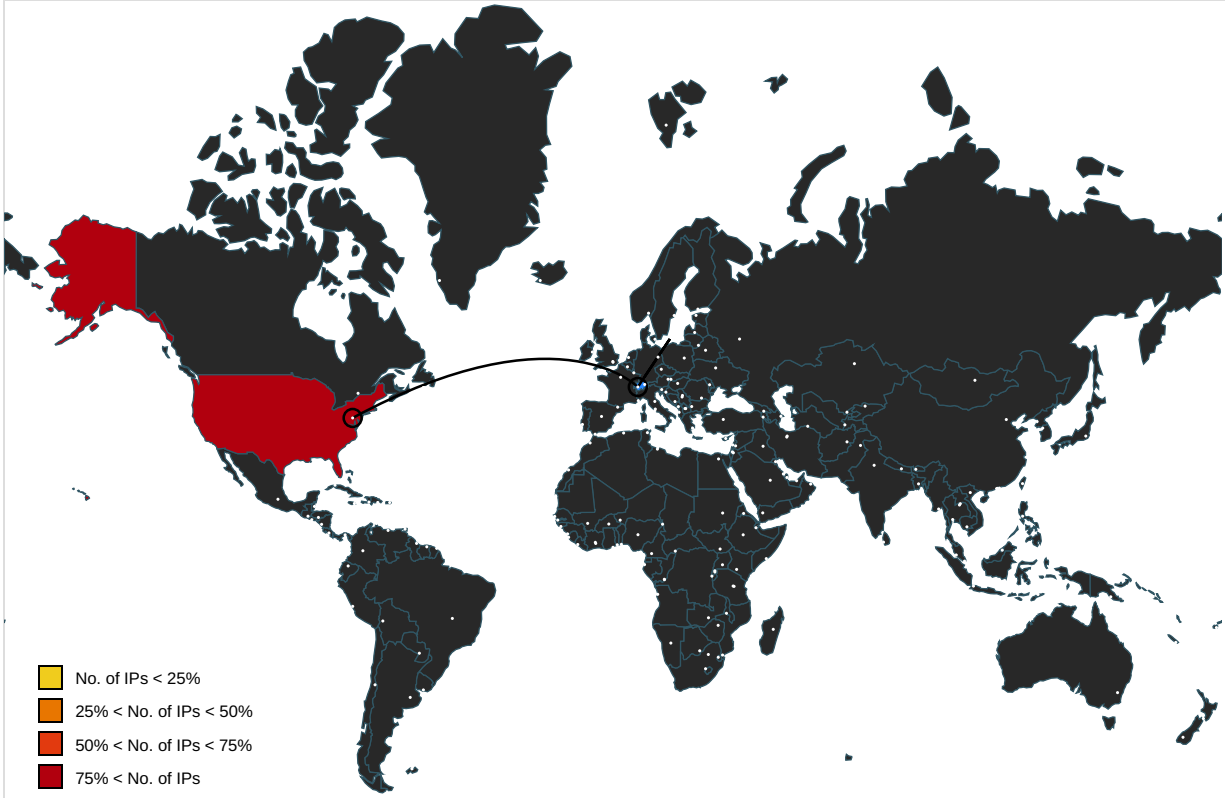
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cyberleague.co/th1s.html	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cyberleague.co/th1s.htmlyX	~WRF{529AA3F3-C7EA-493B-9EDD-4242ACBC44EE}.tmp.0.dr	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.250.15.191	cyberleague.co	United States		16509	AMAZON-02US	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	639039
Start date and time: 03/06/202222:56:31	2022-06-03 22:56:31 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	20220531_180800.rtf

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:	mal68.expl.evad.winRTF@1/20@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:	• Found application associated with file extension: .rtf • 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 NtCreateFile calls found.
- 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):	0.28805818698686764
Encrypted:	false
SSDEEP:	96:K80LHs15sXMfsKQYKg5EgkZ9SlxDZ9Slx1H:10ZQ5EgkgFgv
MD5:	0F53A328D727C7A8393CF8DB618D4D62
SHA1:	40630D0F9A6F68A29581FDA5E76576BF7AE71B7A
SHA-256:	A38F36CF8DA290265A3EBD5FFE647E624FC904C2B31B5D95A76A7DE879476C89
SHA-512:	31456776CEC78F653EEE9B95DC80322F4BD1183EE380F7766751ED271534AF4ECD987EBF91E5A61B17332D879AF642F01F0032E186B6FD02BA9656B38B2E43DE
Malicious:	false
Reputation:	low
Preview:	......M.eFy...zX1.U...E.....S,...X.F...Fa.q...../..R..G@..'..jS~.....%.k....I...-...Z.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-{D07E1317-E210-451E-906F-B47A5E9E2F72}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.6745994346547596
Encrypted:	false
SSDEEP:	96:KXpYCylKgE5XB6V+PAeAKoGR+EPRAriArrGRrDij8A7EAOiMrApMrA:94gEv9pIGNPR4i4UrDij8sEviMrmMr
MD5:	CE42E4E68F81AFD5140DEB010D3974D9
SHA1:	B28D3F230028716DE5868FCEB78FFD804CB64F20
SHA-256:	66046EDB9D30EE2110E19A0F6B13EB85BD3AD7C0E2F7A39DF5A243899C01B015
SHA-512:	562D29C5C5EADDDB09DA1CE689A793AE9177034D986291711AF6C51039EAE3C92B30626FE20645889C51D4FE8EFB73AF98163C0759BA5547E4AE31078252EBC 7
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z....H..N.].y....S,...X.F...Fa.q.....V.....J.tZ.Y*.$.....8...:..H.&I..F.d.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):	3.9333319485137532
Encrypted:	false
SSDEEP:	3:yVlgsRlz5nOlVilXKPIldOYRO+fzpWSR5l276:yPblz5nOlVilaIXOYRO+fzpWSt22
MD5:	DBA609DFDA4A5C85C8EE0FC4064E7EF1
SHA1:	5A08AFFB1250AEB5F1CABF76D4ACB41163B6EB21
SHA-256:	F63018A026B41D192965C2AF5B317D276F7A1752656DDC92553208C086C74918
SHA-512:	FB4531A2D4B2017E3F1C11584782A8F981C8C4858AAAFC8612275B5B707EFB6103CA48D63B73F13FCA5396BC4F419E69B4CC42E7478C5FBBF86C6B213D55FAE D
Malicious:	false

Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.D.0.7.E.1.3.1.7.-.E.2.1.0.-.4.5.1.E.-.9.0.6.F.-.B.4.7.A.5.E.9.E.2.F.7.2.}...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):	0.28681787155888283
Encrypted:	false
SSDEEP:	96:KoLGWkpIdVgNhBNHiN34xoByqVTh/JydVN0Quw+nYwVQXj7zVQuw+nYwVQXj7z6H:juAWZi/kqm8d78dv
MD5:	ABA9368EAF1B4D977D05230FA0AA98A3
SHA1:	30B33313B742BF2D6FF18C5F94A968BEA72AC1DF
SHA-256:	19E5D7038C725D60565FD1555F8327660BC49A35D2FBC98DDE8590919C9BCEB8
SHA-512:	F4C1954A2F70D90DAC1726915FC4D3AF07D6F8FF349ED7B6FF507DDDA1BEB26BFC47A473482D78CDBB0B9CD605E383EF7C918F1D094D2029420619247201D03
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.....F....Qk..S,...X.F...Fa.q.....L5G...L..tf).....F...H.4.....m.A.....E.....x...x...x...x..... ....zV..... ..@....p..G...s.q.Q9G..a`..qb.....p..G.....J..R.w.ps..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{2BA6A725-AC26-4BE3-96A9-7AB218EE9A3D}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.22146428280828123
Encrypted:	false
SSDEEP:	24:I3ev8LwnM0B34FlvHIJKqubKuXCZx6GSeWPOOVRb5XJr8IZxfpA5j36QIHu/w2fG:I3rUrB+vHyZMNdtfxxAUBiRiZ
MD5:	234B22C34D8E43311793320B0BA6E463
SHA1:	217801EE5CA96B065D4F1282983487272AB7D89A
SHA-256:	E59D9F9EBEDDF1697EC9B434F7D23C9EF4ACC4DB61E0B4942C28D2DADC0FDD87
SHA-512:	826B4DFF773E1F94E66847407EE1877E164C3C5C260CE5664B048B23F4C0190F91E5DEFBF7382138EDE9659434361790AC74B1C8D82A6556CC65B4674F07DFB4
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.8..U..F.....S,...X.F...Fa.q.....%....A9D..$.?.....z...FqF..^..\\.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):	3.9560520403188666
Encrypted:	false
SSDEEP:	3:yVlgsRlz1ylJ19X1vWSw/+9snKhmf276:yPblz125XdWSy+anKk22
MD5:	921A52A43CA18F34DA0D4E2EC1EB1864
SHA1:	386EAAD70D06862C0124558FB2D109A0048307D6
SHA-256:	4FEBAE4D1D78D716F73088AA1BE00524C09E132F293AE4F371C47CC29E38C51D
SHA-512:	1E7826AC83669F7411DA3E232695C8D85EEF466E8404893B5741C0A5E8D0D9C4CC26912E81F74A4DB9FAB01E2588A2BBB6D6414638D8DBE05543D81FF78FCC8C
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.2.B.A.6.A.7.2.5.-.A.C.2.6.-.4.B.E.3.-.9.6.A.9.-.7.A.B.2.1.8.E.E.9.A.3.D.}...F.S.D..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\th1s[1].htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	5092
Entropy (8bit):	1.5689266993578892
Encrypted:	false
SSDEEP:	12:hPlf7fguuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuyxH8d2GZfgGwf80K2GUJU6+LtSm:hP12dlRg7nfG/bLtF0ooS34BM3
MD5:	DA03F3022C8E3A07A6F196216B29135E
SHA1:	1F12DE0F50FF34CDB1C1BD99BCA553F7192FA416
SHA-256:	87E5A464DE2F85A500F1B8D1028F5742F0903D9C0C3387DC572AAC8CF9027BCC
SHA-512:	9E039948E2706E864656E1EE2D1CC659F60DC24A5964D220DA4409CCDC7815197F6E3636EC5CA43915BE70DA0A88888BE55B3EAA1F1AC828265D771145EF495E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\th1s[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\th1s[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://cyberleague.co/th1s.html
Preview:	<!DOCTYPE html>..<html>..<body>.. <script>.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. / /AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2B293583.htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	5092
Entropy (8bit):	1.5689266993578892
Encrypted:	false
SSDEEP:	12:hPlf7fguuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuyxH8d2GZfgGwf80K2GUJU6+LtSm:hP12dlRg7nfG/bLtF0ooS34BM3
MD5:	DA03F3022C8E3A07A6F196216B29135E
SHA1:	1F12DE0F50FF34CDB1C1BD99BCA553F7192FA416
SHA-256:	87E5A464DE2F85A500F1B8D1028F5742F0903D9C0C3387DC572AAC8CF9027BCC
SHA-512:	9E039948E2706E864656E1EE2D1CC659F60DC24A5964D220DA4409CCDC7815197F6E3636EC5CA43915BE70DA0A88888BE55B3EAA1F1AC828265D771145EF495E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2B293583.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\2B293583.htm, Author: Joe Security
Reputation:	low
Preview:	<!DOCTYPE html>..<html>..<body>.. <script>.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. / /AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\775ABF47.emf

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	4980
Entropy (8bit):	3.8087894377622136
Encrypted:	false

SSDEEP:	48:cqZDMN7gsdBgLfVTped//HksYHGui3DAjG6kpJoApdHk/O:cqi7lBSTped//qH3i3DAqXLE/O
MD5:	5B29927367C1C2BEBE25499E5602DE05
SHA1:	10EB42142920A3299851F183D624731B910C6FCE
SHA-256:	820E5CFE32DD64E31AEE40837BC3730B1B0F810787A7D3AAFC700191E6551C68
SHA-512:	CD1E48056BDCBDD8CE2C0B7C8E15CA645D26FF372CA68D20D6B3078580943D4D5FA68FEE84A0C1AAC86F275ACE0059A3F76C2AF402EEC918C6680549BAB2C 2EC
Malicious:	false
Reputation:	low
Preview:	....l............../.................. EMF....t......................p....... ...O...............5............................4...5...R...p.................................S.e.g.o.e. .U.I.. ....dv......%. ....r...............)............... ... .?..........?...............l...4........... ... ...(... ... .

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A0472FED.htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	5092
Entropy (8bit):	1.5689266993578892
Encrypted:	false
SSDEEP:	12:hPlf7fguuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuyxH8d2GZfgGwf80K2GUJU6+LtSm:hP12dlRg7nfG/bLtF0ooS34BM3
MD5:	DA03F3022C8E3A07A6F196216B29135E
SHA1:	1F12DE0F50FF34CDB1C1BD99BCA553F7192FA416
SHA-256:	87E5A464DE2F85A500F1B8D1028F5742F0903D9C0C3387DC572AAC8CF9027BCC
SHA-512:	9E039948E2706E864656E1EE2D1CC659F60DC24A5964D220DA4409CCDC7815197F6E3636EC5CA43915BE70DA0A88888BE55B3EAA1F1AC828265D771145EF495 E
Malicious:	**true**
Yara Hits:	• Rule: MAL_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A0472FED.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\A0472FED.htm, Author: Joe Security
Reputation:	low
Preview:	<!DOCTYPE html>..<html>..<body>.. <script>.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. / /AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.. //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D634E9A8.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	JPEG image data, Exif standard: [TIFF image data, big-endian, direntries=0], progressive, precision 8, 750x500, frames 3
Category:	dropped
Size (bytes):	91933
Entropy (8bit):	7.9892937833237845
Encrypted:	false
SSDEEP:	1536:7JCBhGCgBEFzvY1kH0R1ngxcrXo3N0rKL1nvFhbbrC3PJ4+6JaZB5:UBkCgBEZPml3rY3NBpvFRbAhOJi5
MD5:	A53C5995856D35B0097F80E38D258D33
SHA1:	31099B09DCCAC8C4A1BAA7E1F1B14E6C80FC516F
SHA-256:	E87E50F77EEC96A1F0E37FCA345001474B3A023EAABC8DBE6FB1989DCFCDA543
SHA-512:	92C0748B624D9C2C8941C7720EF34C7EF7793589C19517FA4AAAF40C5BE3DCDE3F7C601D1D2B142AED5EFA92E50E5B449B2A61AAB96D22FBBF2B2C9F0EEFA 1F6
Malicious:	false
Reputation:	low
Preview:	......Exif..MM.*............C..C..."..*.. ..4.`B.,}...3..x....:..wx.2...G.8...Z...;a..Tv..a..du"..`...Z...Y..1....s.i.c<.7....Dj...V..}y.r.:.....1z.D...sg.;.c..S`1..\9.u%...X..nDC.L.Z..-..D=..29......1:....DN..l+..P.m.U.LY=.c...-... .O....._w.Mj.v.A.;..v::.`l..C.......l.)....}q..D .h.h.9.U.[...(l.Da....^...c3~Y..c.#.7HC3{....PK.n.<"..L..S.^=..D..vL....<:.(....;..J..9...V...r.I........(/H...x..j]e...;.g.........t!.H.\b[.........{...bR...x.. Q.Q..}..eW.GD..........]M...Xk"#.G...x..t...mZ.-M...v)SJ.w.c...1.Jl.&2y..om.$..%..i:u1...1.{{....FIN...N8...=.)...8.7a!.lJ...h.U....6j.D~.....8._Hr.bY>M.a..z............m.+..wc."A.>..q.....? =..m.....n.CR\R.Vc.=..s...H.. ......+F..F.j.j..I.....9I.<.:{.#;...mc.gF5Ga.2gB..g..&..'...`..6..s...!..u

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{529AA3F3-C7EA-493B-9EDD-4242ACBC44EE}.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):	1.8698058088064178
Encrypted:	false
SSDEEP:	12:rl3bn+qFYsRY3ao92p0hCFySD5lzHSB2TTCt0aNB2TFn7iVjOFyS4CIFyS4FyS4U:rYdIp08B02UL2pigEiWBF4
MD5:	250374534DAFD474CE245E6A5281B3A9
SHA1:	8D3C4BD81822054D6811F54B16EE750903032071
SHA-256:	C142D359182AFDC3B726ADFD4E25161734D3D201027DD7B16C9632C05511D9F1
SHA-512:	E63C7F88A48269F2573FB300D1E2EDB88B2DEB97CE0A908C49579EDDD50F72BA3906DC1BB492BFF93B0B0C72CDE4D7A30BD60CCE1F4AB28CD920798D7E212 AFA
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{058B4FD5-0265-42FA-A9A3-3C51BC43AA1B}.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\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{3847A8D6-DBE6-42C6-982A-DFBC45D1EACD}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3186956359584476
Encrypted:	false
SSDEEP:	6:W4ofylIcElClbYS7plQalvbK/SterHr4PxZUttrasD3Salx3d4XsDialL1:9oal7MClc2HK/rLGZmra4zlb4XelJ
MD5:	969565D4524D45ACD7910BFECB14B97D
SHA1:	272B72B769BB8DB11CF5E3B9D13AE3512B71B890
SHA-256:	2380C8F197156562ED8C5024E8E7F361862FC307D5CF6B6F5EC417B8DA0093B4
SHA-512:	58C7DC7E487BE8135461A125061D10289F0D81E804EDC8B57CDC9CDD5157FEE9FF14EE104CE7450BFE3708EF0DC930EF30906F4B8570092AEE4A5F79FFEB76 BD
Malicious:	false
Preview:	..M.O.T.D.....L.I.N.K. .P.a.c.k.a.g.e. .".h.t.t.p.s.:.//./.c.y.b.e.r.l.e.a.g.u.e...c.o./.t.h.1.s...h.t.m.l.!.". .".". .\.b.... . ...

C:\Users\user\AppData\Local\Temp\{D8764150-CE0B-4AC6-837B-622F48A9918F}

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

Entropy (8bit):	0.0256287320096627
Encrypted:	false
SSDEEP:	6:I3DPcfObYvxggLRHF1NNSapRXv//4tfnRujlw//+GtluJ/eRuj:I3DPJbOr7PFHvYg3J/
MD5:	0F8D76FDBEDB717807CA629B7BFECABE
SHA1:	171373F8A5B5A47539DBD5CCE33C58CA2BD66EDD
SHA-256:	C1D337465844316985A4631572BEB8DE266EFBD2CD9A35AA991E24AFAB233FBF
SHA-512:	8473B7DC81543F660D7E1FD57CB9D215E62F8C4BDA3F1744DFA53C4AFDED4C9B1014F8E7AC298B33484103CCB3DB6077424D38018B106C33EB97EAE8E9FA16 5D
Malicious:	false
Preview:	......M.eFy...zX1.U...E.....S,...X.F...Fa.q.....`.C...H..A.....%.k....I..-...Z.....x...x...x...x..... ....zV..... ..@..... .....

C:\Users\user\AppData\Local\Temp\{E24AC2C6-D3C4-484F-AB4F-7956852A480A}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025609728427755104
Encrypted:	false
SSDEEP:	6:I3DPciIeBvxggLR21MtiX/t0tE3RXv//4tfnRujlw//+GtluJ/eRuj:I3DPrBPtivmtERvYg3J/
MD5:	560D6C31C54209C7E805EAC5ADA0DBB4
SHA1:	A4CAB559CB8FC78B59DE7F225BC5406257794615
SHA-256:	3B3232E7A76CD10AC33A42A30D2447BB78FA2AC693B94687A6F644BFB03D98E6
SHA-512:	0372D772A5DAE29AFEF459599119D6568BE5A2B690D9689F71B7FC84317503E3F4B4A3B785641683F754A3D22194020736D7B5AEA86F1819AD2235863AE8B5F8
Malicious:	false
Preview:	......M.eFy...z.....F....Qk..S,...X.F...Fa.q.....zKwG/K.9..`j.....F...H.4.....m.....x...x...x...x..... ....zV..... ..@..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\20220531_180800.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 15:45:51 2022, mtime=Tue Mar 8 15:45:51 2022, atime=Sat Jun 4 04:58:10 2022, length=199522, window=hide
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	4.495584157169374
Encrypted:	false
SSDEEP:	12:8epRgXg/XAlCPCHaXWBlXB/zxkpX+WZjewU0fWiLCicvbOd7MYDtZ3YilMMEpxRG:8En/XTm3xqbiwU0fpLJeqNDv3q/Y7h
MD5:	0D873EAEF2936CDC358A2B9E248B5432
SHA1:	78DAECA24D53D6739485EF2628959D3D7572CF86
SHA-256:	EDD37464C85F0C3932E9CE1741CA5B21BE7B65CD16165E93206F2C681E4119CB
SHA-512:	81D184F7B79B79BF0EDDEE9ECA67476981AA90AC1FFFBBAB5EB0428FD6411124FD6C2B65DCABD3B729E584CF9FDED99BFC64CCFDE1F1E9391548010815F23 56C
Malicious:	false
Preview:	L.....F.... ....X...3...X...3.....w..b.....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.....p.2.b....TF/ .202205~1.RTF..T.....hT..hT..*...r.....'.....2.0.2.2.0.5.3.1._.1.8.0.8.0.0...r.t.f.....}.....-...8...[.....?J.....C:\Users\..#.....\\405464 \Users.user\Desktop\20220531_180800.rtf.*.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.2.0.2.2.0.5.3.1._.1.8.0.8.0.0...r.t.f.....:.,.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.....405464.....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):	82
Entropy (8bit):	4.526832677737851
Encrypted:	false
SSDEEP:	3:bDuMJlHDISlmxWk1DISlv:bCBSjS1
MD5:	07CF9C274D2D15FCBB60B6FD51508E35
SHA1:	C35DD2A08AA5B765EDB55775B247CCE0C0090064

SHA-256:	07AB1BBAA3C36DDF78D815F20B1C37D36775AED93532D8BC8A3A200B92B6120F
SHA-512:	FEDAF1A0E92C4A3123F8916CB1F6AFFC708806AD9A825C070824CF27A11C52CE692AC579F955CA9503180229ECA49974D29643369C63DD77017732356E42B33F
Malicious:	false
Preview:	[folders]..Templates.LNK=0..20220531_180800.LNK=0..[misc]..20220531_180800.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:vrJlaCkWtVyEJbiJk/p2TKWWhMGHiV/ln:vdsCkWttViJkh2TKHM9V/l
MD5:	C5E24006AFAC8C2659023AD09A07EB0F
SHA1:	4B7B834BEDADFD0A2764743E021D40C55A51F284
SHA-256:	7C9E6D71E3F53D37A78CCE23FA21D259365A9571C6C3A01E8D216586177BA87E
SHA-512:	673649AF8318514414758F92756D408FB6F0CA4859CB2994A921E288126561A7B4EB3C7D824CC90352D939952EA167A473A4282838362B36E85B701A4B582396
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....16.....26.....@36.....36.....z.....p46.....x...

C:\Users\user\Desktop\~$220531_180800.rtf

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:vrJlaCkWtVyEJbiJk/p2TKWWhMGHiV/ln:vdsCkWttViJkh2TKHM9V/l
MD5:	C5E24006AFAC8C2659023AD09A07EB0F
SHA1:	4B7B834BEDADFD0A2764743E021D40C55A51F284
SHA-256:	7C9E6D71E3F53D37A78CCE23FA21D259365A9571C6C3A01E8D216586177BA87E
SHA-512:	673649AF8318514414758F92756D408FB6F0CA4859CB2994A921E288126561A7B4EB3C7D824CC90352D939952EA167A473A4282838362B36E85B701A4B582396
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....16.....26.....@36.....36.....z.....p46.....x...

Static File Info

General

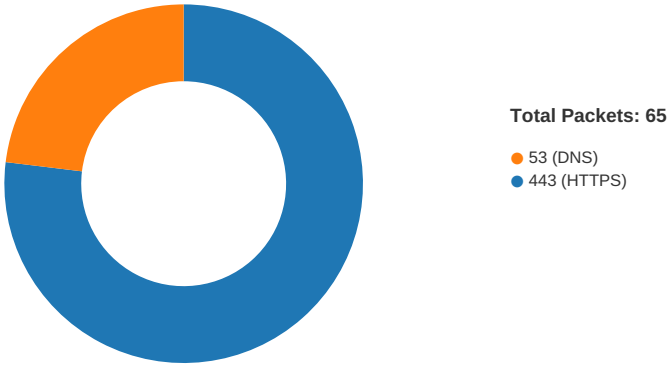
File type:	Microsoft OOXML
Entropy (8bit):	7.9948510704789975
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	20220531_180800.rtf
File size:	199522
MD5:	7b9c8e08371550238fbcd7cee1c8087d
SHA1:	ff8c9deb358b2d22aa086cf36406461e8e9978b2
SHA256:	b93326f795459d836c277730058e9923ab5f9bfbcef32e1c951e4a0d7538f9f5
SHA512:	962c4c0a48519ffa81a95771b25987cc6aeed4bb8737e1e5ab242233f849370d72675f08da3628270bad410659772f437209d7f02bed089b5a220f97314ec1f4
SSDEEP:	3072:LP/BkCPAXydgrYOUIr0XX95JQ7Anr5w2wJLWsk2n3rYxNYlT+MaJis19s9k:b/qXySM3XtQMnrq2Jon3MfYoL19s9k
TLSH:	7814131876E61EB9C60F3BB6B875A1076B9F0017EC14D2BF0C6065F98931964B670F8B
File Content Preview:	PK.....!....iw.....[Content_Types].xml.T.n.0..W.? _#p.CUU!9t96..~.1.q.M...}.HQ.....y..f.....F.d..I...\.2%.....D>0.3i4.d..L'.7.....}J.!.GJ=_.b>1.4".q..<..Z.?Y..n8.....:... ..3.l-C....M.Lh.=5u.UJ..Rp.....(.....BJb$....@h.>..H_.*....n.

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 3, 2022 22:57:19.943697929 CEST	49171	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:19.943775892 CEST	443	49171	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:19.943865061 CEST	49171	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:19.964051008 CEST	49171	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:19.964108944 CEST	443	49171	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:20.359473944 CEST	443	49171	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:20.359684944 CEST	49171	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:20.373123884 CEST	49171	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:20.373183012 CEST	443	49171	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:20.373627901 CEST	443	49171	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:20.373694897 CEST	49171	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:20.676564932 CEST	49171	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:20.720520973 CEST	443	49171	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:20.866599083 CEST	443	49171	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:20.866712093 CEST	49171	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:20.866750956 CEST	443	49171	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:20.866786957 CEST	443	49171	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:20.866797924 CEST	49171	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:20.866830111 CEST	49171	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:20.866849899 CEST	49171	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:20.866868019 CEST	443	49171	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:20.866874933 CEST	49171	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:20.866910934 CEST	49171	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:26.539957047 CEST	49172	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:26.540018082 CEST	443	49172	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:26.540102005 CEST	49172	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:26.540370941 CEST	49172	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:26.540399075 CEST	443	49172	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:26.960410118 CEST	443	49172	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:26.960488081 CEST	49172	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:26.967047930 CEST	49172	443	192.168.2.22	13.250.15.191

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 3, 2022 22:57:26.967062950 CEST	443	49172	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:26.967387915 CEST	443	49172	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:26.980971098 CEST	49172	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:27.024497986 CEST	443	49172	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:27.376456022 CEST	443	49172	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:27.376615047 CEST	443	49172	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:27.376735926 CEST	49172	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:27.376802921 CEST	49172	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:27.376820087 CEST	443	49172	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:31.790095091 CEST	49173	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:31.790122986 CEST	443	49173	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:31.790210962 CEST	49173	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:31.791918039 CEST	49173	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:31.791934967 CEST	443	49173	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:32.201199055 CEST	443	49173	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:32.202213049 CEST	49173	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:32.225771904 CEST	49173	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:32.225794077 CEST	443	49173	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:32.226578951 CEST	443	49173	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:32.272612095 CEST	49173	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:32.316492081 CEST	443	49173	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:32.602184057 CEST	443	49173	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:32.602251053 CEST	443	49173	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:32.602561951 CEST	49173	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:32.602585077 CEST	49173	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:32.602600098 CEST	443	49173	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:32.602688074 CEST	49173	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:32.602694988 CEST	443	49173	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:32.602695942 CEST	49173	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:32.602699041 CEST	443	49173	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:35.228313923 CEST	49174	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:35.228359938 CEST	443	49174	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:35.228441954 CEST	49174	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:35.228722095 CEST	49174	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:35.228737116 CEST	443	49174	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:35.606906891 CEST	443	49174	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:35.607220888 CEST	49174	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:35.621345997 CEST	49174	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:35.621412039 CEST	443	49174	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:35.622071028 CEST	443	49174	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:35.623574018 CEST	49174	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:35.668502092 CEST	443	49174	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:35.976391077 CEST	443	49174	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:35.976555109 CEST	443	49174	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:35.976737976 CEST	49174	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:35.983047962 CEST	49174	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:35.983087063 CEST	443	49174	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:37.074811935 CEST	49175	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:37.074841022 CEST	443	49175	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:37.074956894 CEST	49175	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:37.075555086 CEST	49175	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:37.075567007 CEST	443	49175	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:37.458427906 CEST	443	49175	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:37.458610058 CEST	49175	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:37.471674919 CEST	49175	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:37.471684933 CEST	443	49175	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:37.472399950 CEST	443	49175	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:37.474443913 CEST	49175	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:37.516489029 CEST	443	49175	13.250.15.191	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 3, 2022 22:57:37.833076000 CEST	443	49175	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:37.833199978 CEST	443	49175	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:37.833389997 CEST	49175	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:37.838345051 CEST	49175	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:37.838361979 CEST	443	49175	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:37.864737034 CEST	49176	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:37.864792109 CEST	443	49176	13.250.15.191	192.168.2.22
Jun 3, 2022 22:57:37.864876986 CEST	49176	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:37.866413116 CEST	49176	443	192.168.2.22	13.250.15.191
Jun 3, 2022 22:57:37.866449118 CEST	443	49176	13.250.15.191	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 3, 2022 22:57:19.871170998 CEST	55868	53	192.168.2.22	8.8.8.8
Jun 3, 2022 22:57:19.930835962 CEST	53	55868	8.8.8.8	192.168.2.22
Jun 3, 2022 22:57:26.314532042 CEST	49688	53	192.168.2.22	8.8.8.8
Jun 3, 2022 22:57:26.456120968 CEST	53	49688	8.8.8.8	192.168.2.22
Jun 3, 2022 22:57:26.459547043 CEST	58836	53	192.168.2.22	8.8.8.8
Jun 3, 2022 22:57:26.538995981 CEST	53	58836	8.8.8.8	192.168.2.22
Jun 3, 2022 22:57:31.445116997 CEST	50134	53	192.168.2.22	8.8.8.8
Jun 3, 2022 22:57:31.463130951 CEST	53	50134	8.8.8.8	192.168.2.22
Jun 3, 2022 22:57:31.464679003 CEST	55275	53	192.168.2.22	8.8.8.8
Jun 3, 2022 22:57:31.789314032 CEST	53	55275	8.8.8.8	192.168.2.22
Jun 3, 2022 22:57:35.143301010 CEST	59915	53	192.168.2.22	8.8.8.8
Jun 3, 2022 22:57:35.200170040 CEST	53	59915	8.8.8.8	192.168.2.22
Jun 3, 2022 22:57:35.210647106 CEST	54408	53	192.168.2.22	8.8.8.8
Jun 3, 2022 22:57:35.227852106 CEST	53	54408	8.8.8.8	192.168.2.22
Jun 3, 2022 22:57:36.922116995 CEST	50108	53	192.168.2.22	8.8.8.8
Jun 3, 2022 22:57:36.939106941 CEST	53	50108	8.8.8.8	192.168.2.22
Jun 3, 2022 22:57:36.942188978 CEST	54723	53	192.168.2.22	8.8.8.8
Jun 3, 2022 22:57:37.069972992 CEST	53	54723	8.8.8.8	192.168.2.22
Jun 3, 2022 22:57:40.868483067 CEST	58062	53	192.168.2.22	8.8.8.8
Jun 3, 2022 22:57:40.897502899 CEST	53	58062	8.8.8.8	192.168.2.22
Jun 3, 2022 22:57:40.899883986 CEST	56703	53	192.168.2.22	8.8.8.8
Jun 3, 2022 22:57:40.918878078 CEST	53	56703	8.8.8.8	192.168.2.22
Jun 3, 2022 22:57:42.643587112 CEST	59241	53	192.168.2.22	8.8.8.8
Jun 3, 2022 22:57:42.662676096 CEST	53	59241	8.8.8.8	192.168.2.22
Jun 3, 2022 22:57:42.665538073 CEST	55244	53	192.168.2.22	8.8.8.8
Jun 3, 2022 22:57:42.682970047 CEST	53	55244	8.8.8.8	192.168.2.22
Jun 3, 2022 22:57:44.315067053 CEST	53958	53	192.168.2.22	8.8.8.8
Jun 3, 2022 22:57:44.334134102 CEST	53	53958	8.8.8.8	192.168.2.22
Jun 3, 2022 22:57:44.336416960 CEST	56020	53	192.168.2.22	8.8.8.8
Jun 3, 2022 22:57:44.353132010 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
Jun 3, 2022 22:57:19.871170998 CEST	192.168.2.22	8.8.8.8	0xdcdd	Standard query (0)	cyberleague.co	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:26.314532042 CEST	192.168.2.22	8.8.8.8	0xd494	Standard query (0)	cyberleague.co	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:26.459547043 CEST	192.168.2.22	8.8.8.8	0x6c29	Standard query (0)	cyberleague.co	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:31.445116997 CEST	192.168.2.22	8.8.8.8	0xf2ca	Standard query (0)	cyberleague.co	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:31.464679003 CEST	192.168.2.22	8.8.8.8	0xdc64	Standard query (0)	cyberleague.co	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:35.143301010 CEST	192.168.2.22	8.8.8.8	0xbe50	Standard query (0)	cyberleague.co	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:35.210647106 CEST	192.168.2.22	8.8.8.8	0x646c	Standard query (0)	cyberleague.co	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 3, 2022 22:57:36.922116995 CEST	192.168.2.22	8.8.8.8	0x12f1	Standard query (0)	cyberleague.co	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:36.942188978 CEST	192.168.2.22	8.8.8.8	0xe6e0	Standard query (0)	cyberleague.co	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:40.868483067 CEST	192.168.2.22	8.8.8.8	0xbbd1	Standard query (0)	cyberleague.co	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:40.899883986 CEST	192.168.2.22	8.8.8.8	0x41b6	Standard query (0)	cyberleague.co	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:42.643587112 CEST	192.168.2.22	8.8.8.8	0x6703	Standard query (0)	cyberleague.co	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:42.665538073 CEST	192.168.2.22	8.8.8.8	0x7820	Standard query (0)	cyberleague.co	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:44.315067053 CEST	192.168.2.22	8.8.8.8	0x2c87	Standard query (0)	cyberleague.co	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:44.336416960 CEST	192.168.2.22	8.8.8.8	0x4c7a	Standard query (0)	cyberleague.co	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 3, 2022 22:57:19.930835962 CEST	8.8.8.8	192.168.2.22	0xdcdd	No error (0)	cyberleague.co		13.250.15.191	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:26.456120968 CEST	8.8.8.8	192.168.2.22	0xd494	No error (0)	cyberleague.co		13.250.15.191	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:26.538995981 CEST	8.8.8.8	192.168.2.22	0x6c29	No error (0)	cyberleague.co		13.250.15.191	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:31.463130951 CEST	8.8.8.8	192.168.2.22	0xf2ca	No error (0)	cyberleague.co		13.250.15.191	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:31.789314032 CEST	8.8.8.8	192.168.2.22	0xdc64	No error (0)	cyberleague.co		13.250.15.191	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:35.200170040 CEST	8.8.8.8	192.168.2.22	0xbe50	No error (0)	cyberleague.co		13.250.15.191	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:35.227852106 CEST	8.8.8.8	192.168.2.22	0x646c	No error (0)	cyberleague.co		13.250.15.191	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:36.939106941 CEST	8.8.8.8	192.168.2.22	0x12f1	No error (0)	cyberleague.co		13.250.15.191	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:37.069972992 CEST	8.8.8.8	192.168.2.22	0xe6e0	No error (0)	cyberleague.co		13.250.15.191	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:40.897502899 CEST	8.8.8.8	192.168.2.22	0xbbd1	No error (0)	cyberleague.co		13.250.15.191	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:40.918878078 CEST	8.8.8.8	192.168.2.22	0x41b6	No error (0)	cyberleague.co		13.250.15.191	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:42.662676096 CEST	8.8.8.8	192.168.2.22	0x6703	No error (0)	cyberleague.co		13.250.15.191	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:42.682970047 CEST	8.8.8.8	192.168.2.22	0x7820	No error (0)	cyberleague.co		13.250.15.191	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:44.334134102 CEST	8.8.8.8	192.168.2.22	0x2c87	No error (0)	cyberleague.co		13.250.15.191	A (IP address)	IN (0x0001)
Jun 3, 2022 22:57:44.353132010 CEST	8.8.8.8	192.168.2.22	0x4c7a	No error (0)	cyberleague.co		13.250.15.191	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- cyberleague.co

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	13.250.15.191	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-06-03 20:57:20 UTC	0	OUT	OPTIONS / HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: cyberleague.co Content-Length: 0 Connection: Keep-Alive
2022-06-03 20:57:20 UTC	0	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 20:57:20 GMT Content-Type: text/html Content-Length: 0 Connection: close Allow: GET,POST,OPTIONS,HEAD,TRACE

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49172	13.250.15.191	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 20:57:26 UTC	0	OUT	HEAD /th1s.html HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: cyberleague.co
2022-06-03 20:57:27 UTC	0	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 20:57:27 GMT Content-Type: text/html Content-Length: 5092 Connection: close Last-Modified: Wed, 01 Jun 2022 14:36:34 GMT ETag: "13e4-5e063d0e1ca1e" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.22	49181	13.250.15.191	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 20:57:44 UTC	9	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 63 79 62 65 72 6c 65 61 67 75 6 5 2e 63 6f 0d 0a 0d 0a Data Ascii: PROPFIND / HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0tr anslate: fContent-Length: 0Host: cyberleague.co
2022-06-03 20:57:45 UTC	9	IN	HTTP/1.1 405 Method Not Allowed Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 20:57:45 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 225 Connection: close Allow: GET,POST,OPTIONS,HEAD,TRACE
2022-06-03 20:57:45 UTC	9	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 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title ></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.22	49182	13.250.15.191	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-06-03 20:57:45 UTC	10	OUT	GET /th1s.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: cyberleague.co If-Modified-Since: Wed, 01 Jun 2022 14:36:34 GMT If-None-Match: "13e4-5e063d0e1ca1e" Connection: Keep-Alive
2022-06-03 20:57:45 UTC	10	IN	HTTP/1.1 304 Not Modified Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 20:57:45 GMT Connection: close Last-Modified: Wed, 01 Jun 2022 14:36:34 GMT ETag: "13e4-5e063d0e1ca1e" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.22	49183	13.250.15.191	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 20:57:46 UTC	10	OUT	HEAD /th1s.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: cyberleague.co Content-Length: 0 Connection: Keep-Alive
2022-06-03 20:57:46 UTC	10	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 20:57:46 GMT Content-Type: text/html Content-Length: 5092 Connection: close Last-Modified: Wed, 01 Jun 2022 14:36:34 GMT ETag: "13e4-5e063d0e1ca1e" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.22	49184	13.250.15.191	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 20:57:47 UTC	11	OUT	HEAD /th1s.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: cyberleague.co Content-Length: 0 Connection: Keep-Alive
2022-06-03 20:57:47 UTC	11	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 20:57:47 GMT Content-Type: text/html Content-Length: 5092 Connection: close Last-Modified: Wed, 01 Jun 2022 14:36:34 GMT ETag: "13e4-5e063d0e1ca1e" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49173	13.250.15.191	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 20:57:32 UTC	0	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: cyberleague.co

Timestamp	kBytes transferred	Direction	Data
2022-06-03 20:57:32 UTC	0	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 20:57:32 GMT Content-Type: text/html Content-Length: 0 Connection: close Allow: GET,POST,OPTIONS,HEAD,TRACE

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49174	13.250.15.191	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 20:57:35 UTC	0	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 63 79 62 65 72 6c 65 61 67 75 65 2e 63 6f 0d 0a 0d 0a Data Ascii: PROPFIND / HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: cyberleague.co
2022-06-03 20:57:35 UTC	1	IN	HTTP/1.1 405 Method Not Allowed Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 20:57:35 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 225 Connection: close Allow: GET,POST,OPTIONS,HEAD,TRACE
2022-06-03 20:57:35 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 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49175	13.250.15.191	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 20:57:37 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 63 79 62 65 72 6c 65 61 67 75 65 2e 63 6f 0d 0a 0d 0a Data Ascii: PROPFIND / HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: cyberleague.co
2022-06-03 20:57:37 UTC	1	IN	HTTP/1.1 405 Method Not Allowed Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 20:57:37 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 225 Connection: close Allow: GET,POST,OPTIONS,HEAD,TRACE
2022-06-03 20:57:37 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 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49176	13.250.15.191	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 20:57:38 UTC	2	OUT	GET /th1s.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: cyberleague.co Connection: Keep-Alive
2022-06-03 20:57:38 UTC	2	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 20:57:38 GMT Content-Type: text/html Content-Length: 5092 Connection: close Last-Modified: Wed, 01 Jun 2022 14:36:34 GMT ETag: "13e4-5e063d0e1ca1e" Accept-Ranges: bytes
2022-06-03 20:57:38 UTC	2	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 20 20 20 20 3c 73 63 72 69 70 74 3e 0d 0a 20 20 20 20 2f 2f 41 0d 0a 20 20 20 20 2f 2f 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 Data Ascii: <!DOCTYPE html><html><body> <script> //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAA //AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49177	13.250.15.191	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 20:57:39 UTC	7	OUT	HEAD /th1s.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: cyberleague.co Content-Length: 0 Connection: Keep-Alive
2022-06-03 20:57:39 UTC	7	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 20:57:39 GMT Content-Type: text/html Content-Length: 5092 Connection: close Last-Modified: Wed, 01 Jun 2022 14:36:34 GMT ETag: "13e4-5e063d0e1ca1e" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49178	13.250.15.191	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 20:57:40 UTC	8	OUT	HEAD /th1s.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: cyberleague.co Content-Length: 0 Connection: Keep-Alive
2022-06-03 20:57:40 UTC	8	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 20:57:40 GMT Content-Type: text/html Content-Length: 5092 Connection: close Last-Modified: Wed, 01 Jun 2022 14:36:34 GMT ETag: "13e4-5e063d0e1ca1e" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.22	49179	13.250.15.191	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 20:57:41 UTC	8	OUT	HEAD /th1s.html HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: cyberleague.co
2022-06-03 20:57:41 UTC	8	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 20:57:41 GMT Content-Type: text/html Content-Length: 5092 Connection: close Last-Modified: Wed, 01 Jun 2022 14:36:34 GMT ETag: "13e4-5e063d0e1ca1e" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.22	49180	13.250.15.191	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-03 20:57:43 UTC	8	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 63 79 62 65 72 6c 65 61 67 75 65 2e 63 6f 0d 0a 0d 0a Data Ascii: PROPFIND / HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: cyberleague.co
2022-06-03 20:57:43 UTC	9	IN	HTTP/1.1 405 Method Not Allowed Server: nginx/1.18.0 (Ubuntu) Date: Fri, 03 Jun 2022 20:57:43 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 225 Connection: close Allow: GET,POST,OPTIONS,HEAD,TRACE
2022-06-03 20:57:43 UTC	9	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 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. </body></html>

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: **1424**, Parent PID: **576**

General

Target ID:	0
Start time:	22:58:11
Start date:	03/06/2022
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:	0x13fb90000
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	6E282B14	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$220531_180800.rtf	success or wait	1	6E300648	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\Desktop\20220531_180800.rtf	1738	317	success or wait	1	6E300648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\775ABF47.emf	unknown	8192	success or wait	1	6E300648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\775ABF47.emf	unknown	8192	end of file	1	6E300648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\775ABF47.emf	unknown	8192	success or wait	1	6E300648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\775ABF47.emf	unknown	8192	end of file	1	6E300648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\775ABF47.emf	unknown	22	success or wait	1	6E300648	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E2DA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E2DA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E2DA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E300648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6E300648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6E300648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\74808	success or wait	1	6E300648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	6E300648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\74808	74808	binary	04 00 00 00 90 05 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	success or wait	1	6E300648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			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 85 7E 0D 38 D8 77 D8 01 08 48 07 00 08 48 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	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 FF FF FF FF				

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\74808	74808	binary	04 00 00 00 90 05 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 85 7E 0D 38 D8 77 D8 01 08 48 07 00 08 48 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	04 00 00 00 90 05 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 08 48 07 00 08 48 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	success or wait	1	6E300648	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 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 FF FF FF FF				

Disassembly

⊘ **No disassembly**