ID: 686004
Sample Name: dl18aYTBo5
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 03:50:20
Date: 18/08/2022
Version: 35.0.0 Citrine

Table of Contents

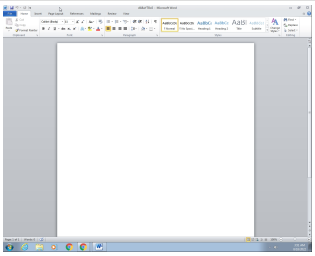
Windows Analysis Report

dl18aYTBo5

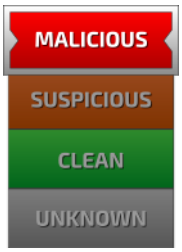
Overview

General Information

Sample Name:	dl18aYTBo5 (renamed file extension from none to docx)
Analysis ID:	686004
MD5:	b91615355a11f5..
SHA1:	7950b1730e05a2.
SHA256:	3fdd30eb0961c9..
Infos:	



Detection

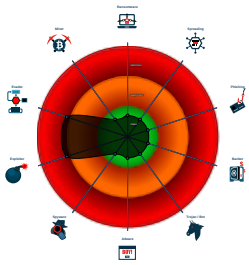


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Contains an external reference to an…
- Detected suspicious Microsoft Offic…
- Yara signature match
- Potential document exploit detected…
- Internet Provider seen in connection…
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…
- IP address seen in connection with …

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1216 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:$a1: <Relationships • 0x77c:$a2: TargetMode="External" • 0x774:$x1: .html!
document.xml.rels	INDICATOR_OLE_RemoteTemplate	Detects XML relations where an OLE object is refrencing an external target in dropper OOXML documents	ditekSHen	• 0x703:$olerel: relationships/oleObject • 0x71c:$target1: Target="http • 0x77c:$mode: TargetMode="External

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

Exploits

Detected suspicious Microsoft Office reference URL

System Summary

Malicious sample detected (through community Yara rule)

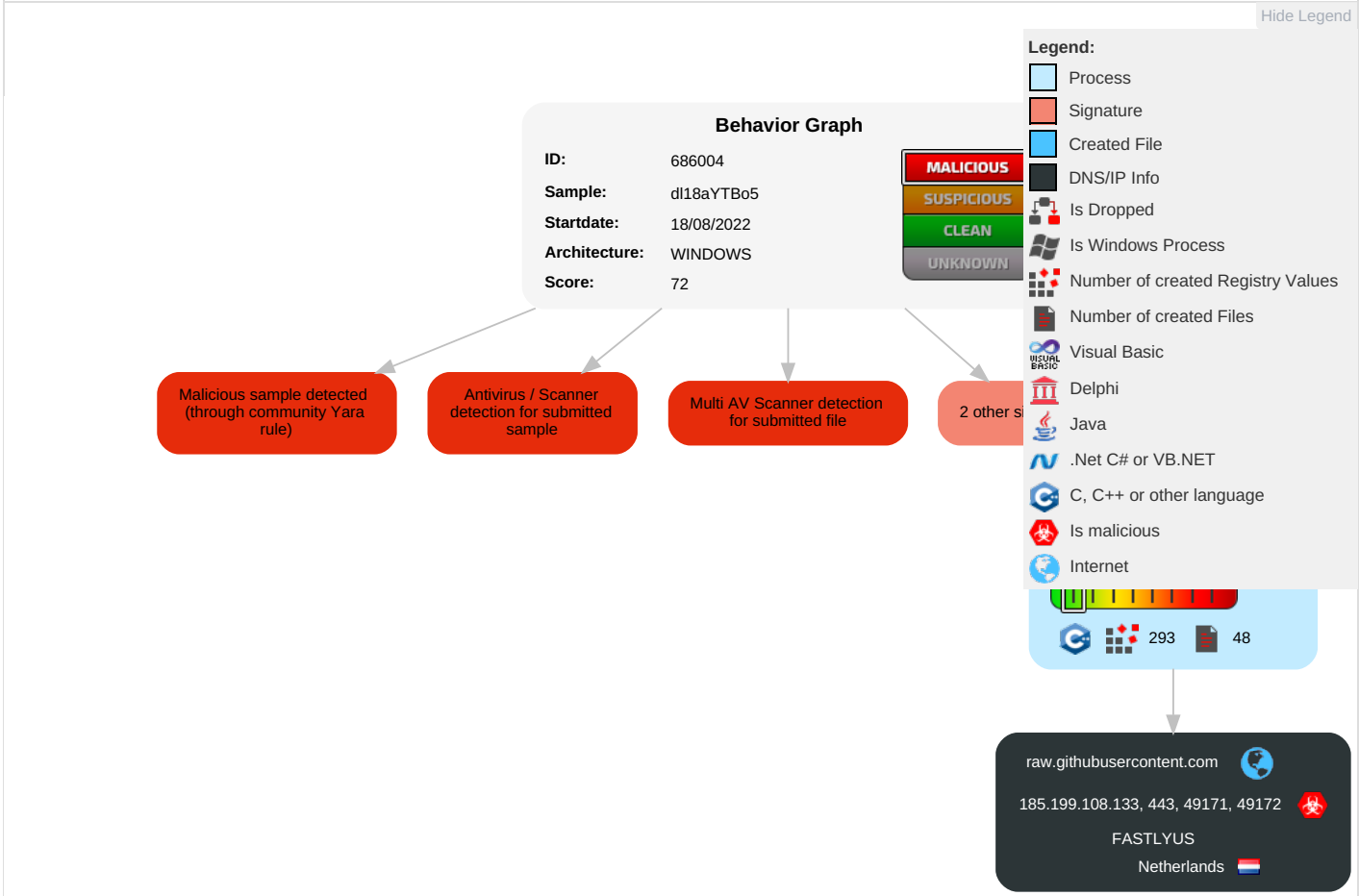
Persistence and Installation Behavior

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	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	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

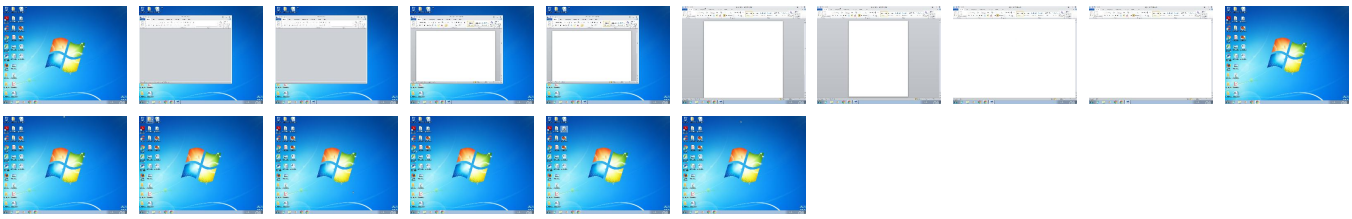
Behavior Graph

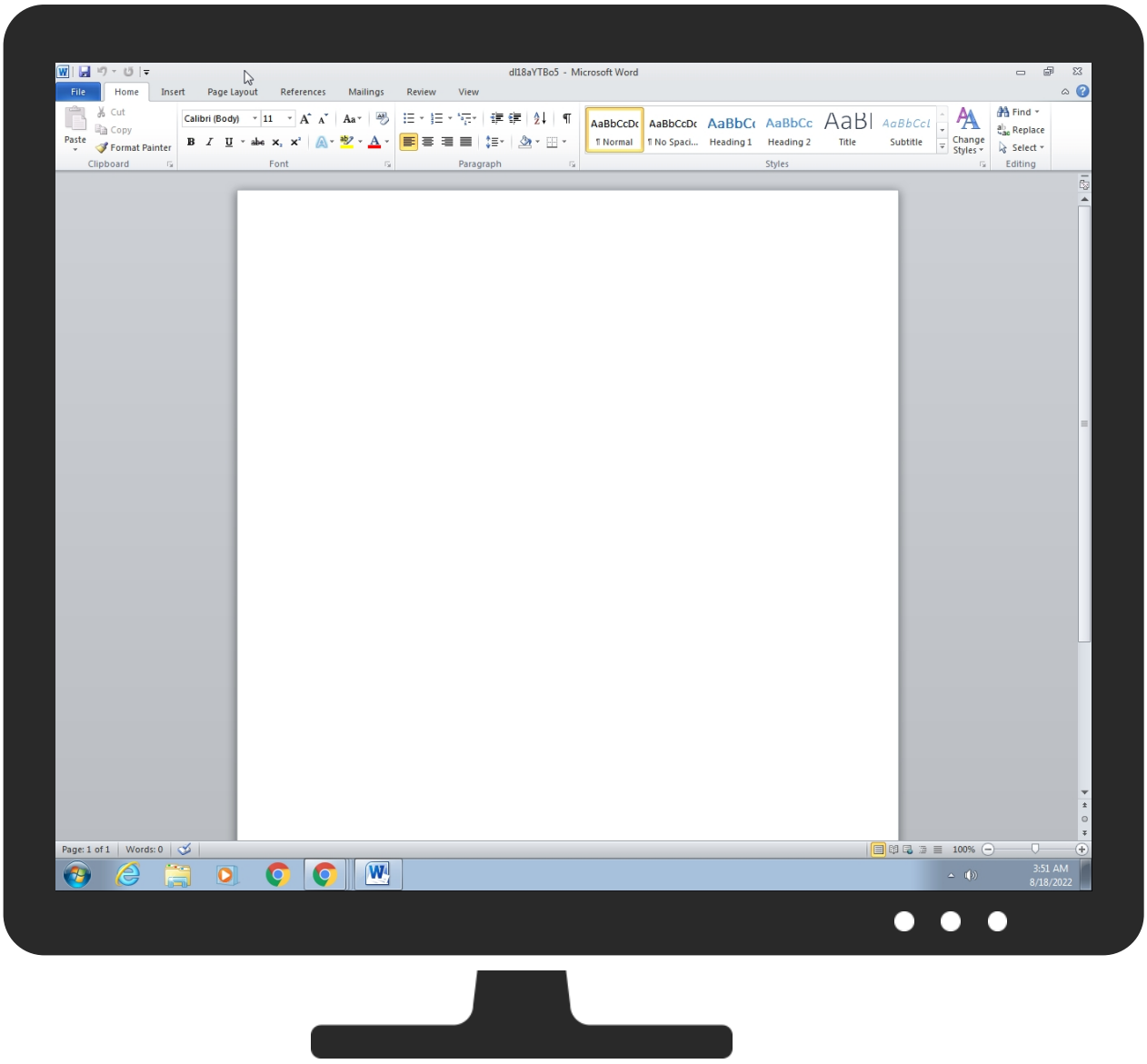


Screenshots

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
dl18aYTBo5.docx	20%	Metadefender		Browse
dl18aYTBo5.docx	28%	ReversingLabs	Document-Word.Exploit.Heuristic	
dl18aYTBo5.docx	100%	Avira	W97M/Dldr.Agent.G1	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://raw.githubusercontent.com/drgreenthumb93/CVE-2022-30190-follina/main/bad.html	0%	Avira URL Cloud	safe	

Domains and IPs

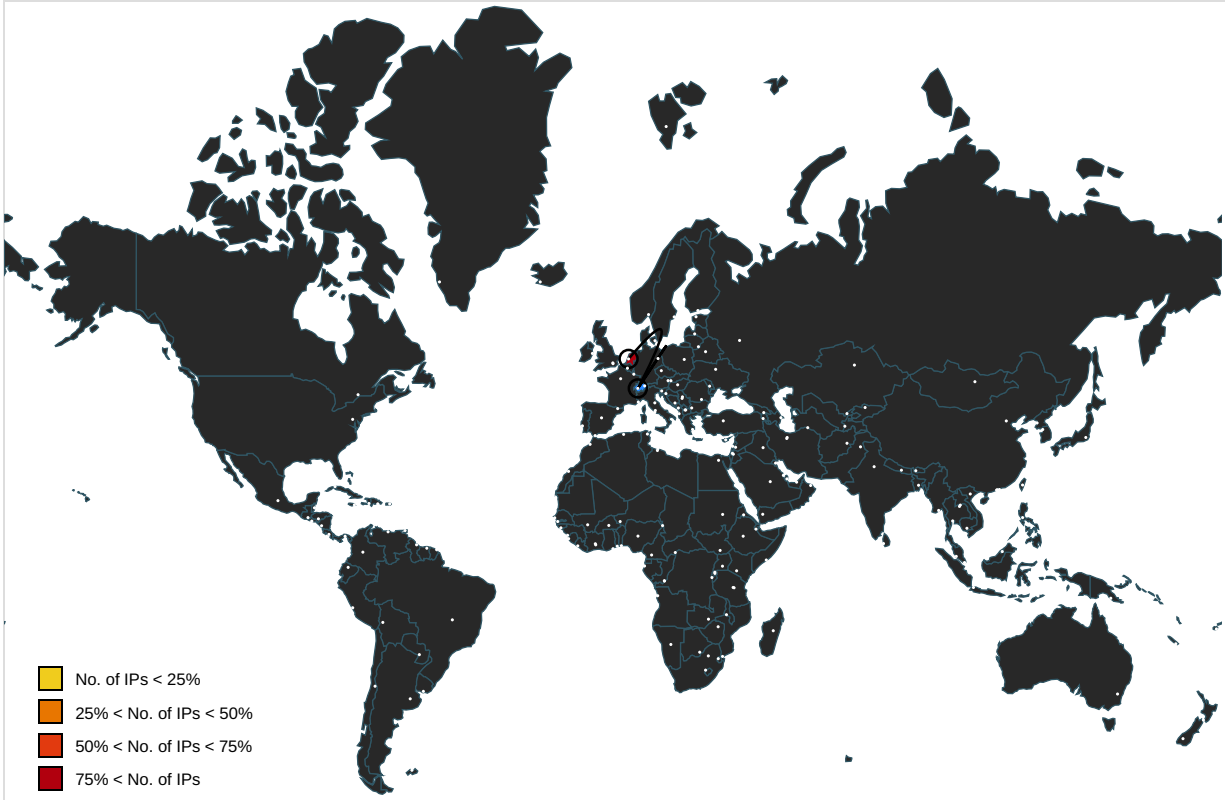
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
raw.githubusercontent.com	185.199.108.133	true	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://raw.githubusercontent.com/drgreenthumb93/CVE-2022-30190-follina/main/bad.html	~WRS{FEC6DCA0-7354-46DE-A8FC-629874E35853}.tmp.0.dr	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.199.108.133	raw.githubusercontent.com	Netherlands		54113	FASTLYUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	686004
Start date and time:	2022-08-18 03:50:20 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 4s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	dl18aYTBo5 (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:	4
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.expl.evad.winDOCX@1/15@1/1
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): dllhost.exe
- Report size getting too big, too many NtQueryAttributesFile calls found.
- VT rate limit hit for: dl18aYTBo5.docx

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):	0.2891798341270631
Encrypted:	false
SSDEEP:	96:Ku2LVP/Edg7qsruukLQEzyE5lAmIM6h5RK43fngxZJCa43fngxZJCIH:cCsrBoh3K5M
MD5:	AED282D47E74B35A963FA967845BEB55
SHA1:	95860C99A86CE925F3FF2847643FEB9D07601E09
SHA-256:	87636D9B14847B13BBCD785071FE01D09428F7E8ABA072BB06225830BCEFA3C4
SHA-512:	4D5ED432A1EED5639C341723B5418CA97343D75C21DC568D981ED5C7FAB0D0E8FB62C8A971B6F66620C5C41D8E5E564E418D14B4F4C835C389881ADEC8AF28 2
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z..PG..O.+...K}.S,...X.F...Fa.q.....\.k.gF.Q.%...q.....5..M....8....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-{DD8BC438-10B7-4304-B5F6-7629BCF1BBBD}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.671583368870765
Encrypted:	false
SSDEEP:	96:KTnCy+Gl917GyWhudBoG1mu/cN3NSOvFTyNnGv:mn+O9NK8mGfG9btUnGv
MD5:	26F11022DF18562138B60C6F037921A8
SHA1:	5B8B9FCD71EFBB596D32EAB2E5450B6A09F42A3E
SHA-256:	C7DE62732C7A4D01C61155AC93E2CDF8FF277BA66C5E997AFC68C4836B6C1876
SHA-512:	7D9185AD76AC4FCBB8A998149B0760529BF0E32C31D9E7D7D8776BC63A9BE92C81B4D326CE9858916F75F4D8550E3681009501B78EC4C77D84986D44CD2D6F9
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.....G...Q..0.S,...X.F...Fa.q.....y".c.J./.....5R.t..H..b..?.3.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):	3.9145450235130843
Encrypted:	false
SSDEEP:	3:yVlgsRlzV8LMFYEHpCRglQ7pYyUaO9H7mL7276:yPblzV8wFhYCQ7pYyUbFKf22
MD5:	7B90472AF641B5E703E37F1B849117D6
SHA1:	DBF52B00012494E56117FEF0F777FD7D0945C8EB
SHA-256:	7D461C93DFC0C71280E3F2B14C11345DE5BD87C7170C4A7F01F2155335D7543B
SHA-512:	81F7C12377FD567C6158D2E5FD5856AEE7754FA565CB320E9957F6D718642A19301F3D0AAD76CEA7A57E0D36FE0129E0CAC245D1A0412F7FC72FCA56DDB6E1 4
Malicious:	false
Reputation:	low

Preview:	..H..@....b..q....]F.S.D.-.{.D.D.8.B.C.4.3.8.-.1.0.B.7.-.4.3.0.4.-.B.5.F.6.-.7.6.2.9.B.C.F.1.B.B.B.D.}...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):	0.28761799644723346
Encrypted:	false
SSDEEP:	24:I3JuC4tB37/AtfJA2jeMFUWTk2n8YpS9ACOie6G9cPlSPl/KJGlFU8dyOJ2Xredk:I38RBzk29416Gus0o1yUErwo4VzKzVH
MD5:	0DDF9A2970B1B258F8A6DC09F10A59EB
SHA1:	1AC71AA6E71D102B35173A2C1861F4AD58DC521D
SHA-256:	9FFBE5DEB13327493B169738A498D95E872AD88E850FE8F54E182892E684D09E
SHA-512:	7C73E42854B8DDAD1978B82032AE12AC6B08D7DFC003067887F3D4D53B8EFD53633A518EEAF3568BE581E604CE1D69F8CA25BA25D8D4119886989F60BFA6A2A
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z...r8.JL..;a;...S,...X.F...Fa.q.....K]..Cy9B...#.{.....c....N.{..0...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-{4BE7BDD4-FFEC-446A-AFDD-8DCC2CB50000}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.22238376643707547
Encrypted:	false
SSDEEP:	24:I3L4MfPLwnM0B34P+ga0eQ/51AsnstTMERtr/XEJ4AyKyiJe/R/i5hm8MyYqMyY2:I3ZXUrBX0/A0YJy41hiS8eqe2
MD5:	46C2BB20992B8CE2496F7552C6C2B4E2
SHA1:	FC1D835CCA254539EB6DB0E3A86EA21DED1F1CB1
SHA-256:	EDDBA564DA065E559E253D85566ACEAD75B7B789DE900EAB15311CA8D3E52A08
SHA-512:	FAF1515F5AB321CDB368091B0015FC9B2F5CF38591919CCA61934CF82CEB8B8B201C38EF3D593B35A68D673EDBF885D037B92882BE4D44321346D2E1F2A5365B
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z....T^G..g..=.S,...X.F...Fa.q.....M....6.....%.(&...F.:...W.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):	3.861913444565715
Encrypted:	false
SSDEEP:	3:yVlgsRlzB6lSTzRWZ3IRSYmz8hPKQlPtEljl276:yPblzslST4Z4gRISQd6Z22
MD5:	198CFA2CB15C47E79B48D717F4D03634
SHA1:	1B74293BCEDC94E8965A4536DA7AD0C3AC309852
SHA-256:	9EEBDC29A70138CC5616F631F3141303C6DFBF34812D7805A0D573264D9ED6C0
SHA-512:	8A20F85B6732051D73C3EA662458BF9BBEFA7E057879CCAA0F8ABCC9CDB63E772EED623E919BD39A00AA963A03E49E522BF99FEADDE4B0D852BB893DBAA87F6E
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.4.B.E.7.B.D.D.4.-.F.F.E.C.-.4.4.6.A.-.A.F.D.D.-.8.D.C.C.2.C.B.5.0.0.0.0.}...F.S.D..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{24DDD834-E6C7-483D-822D-9FEFD1EF961E}.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):	2560
Entropy (8bit):	1.4190225457141796
Encrypted:	false
SSDEEP:	12:rl3lTpFQUhIc77k4c77k4CIc77k4c77k4CICICb77:rnxl77g77m77g77
MD5:	49805345EC222F9C40DE34EA93D3D9D4
SHA1:	43722C84F1BF1C76DA46EE10E388348CD90FC1CA
SHA-256:	2253D7B0AA718135507AE366237E893ADAD147B44C39B130007A9A3486FE2C14
SHA-512:	C402E7BE9E8A4C0610E6B59E9965E0CEAB7F5E815BDACB4807564211EC2DBABC63B553E857B80A07481AAF1A706F52BF4CF3F4FE0E8141F4A0BA146B57B1B87D
Malicious:	false
Reputation:	low
Preview:	.....................>...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{40655C52-0542-4D1D-95A6-44AB7A44DEAF}.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
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{FEC6DCA0-7354-46DE-A8FC-629874E35853}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.064573888851514
Encrypted:	false
SSDEEP:	6:olgI5lNcYTIee8c3XlimlcougZkl9AajJMdYB4PxZUtL2mN:4vTIx8c3Xlimlcb4WJcZk
MD5:	16983C4674C4429553475D2AE88B4044
SHA1:	749397398EF28AACA48E2F1295EFCDCF49C8804E
SHA-256:	2F1D2137E1F5F181D6295D7ADE057DDEB50F43FA5B5C99E8E9559E2AD8FA3B56
SHA-512:	6EDA1C367C1F28D4EDE0EBD9C675A4D1B0DC18AD3607398EBF6306FD2A45C47FC427E6E3F5FB7817E4387CCF40D118E5277B3CD85EA9F38510109C7C09B81EA
Malicious:	false
Reputation:	low
Preview:	..L.I.N.K. .h.t.m.l.f.i.l.e. .".h.t.t.p.s.:././.r.a.w...g.i.t.h.u.b.u.s.e.r.c.o.n.t.e.n.t...c.o.m./.d.r.g.r.e.e.n.t.h.u.m.b.9.3./.C.V.E.-.2.0.2.2.-.3.0.1.9.0.-.f.o.l.l.i.n.a./.m.a.i.n./.b.a.d...h.t.m.l.!.". .".". .\.p. .\.f. .0..... . ...j....U

C:\Users\user\AppData\Local\Temp\{1F19ED29-251F-4468-B6E5-D4261622E15F}	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025492164821171715
Encrypted:	false
SSDEEP:	6:I3DPcdH0FvxggLR2ajt/5SpRXv//4tfnRujlw//+GtluJ/eRuj:I3DPycVjmvYg3J/
MD5:	C321B22B28157B83D97EC320A2279932
SHA1:	0218F9A13568E812E90219318BB8869426985F95
SHA-256:	E6CC4B63B5471AA996CAEEFE102323A54DA38F5340FDC20E3B60B0D20F346350
SHA-512:	7880CF4C296FB1629BB668A196C4CB04AEDC9227FA446357FE4605CDBAD6853EE4F93700C91052C631A1800E5840950E98EA7B8DBF6785C2D74AFA3C7677F49
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z..PG..O.+...K}.S,...X.F...Fa.q.....m8T...$F.K..q6o.....5..M....8.....x...x...x...x..... .....zV..... ..@.....

C:\Users\user\AppData\Local\Temp\{8C1DA29E-F25D-4DB9-A9FE-FB8A44BD2C4F}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025708761401932248
Encrypted:	false
SSDEEP:	6:I3DPcM/UxFvxggLRpXKbswN6/3RXv//4tfnRujlw//+GtluJ/eRuj:I3DPcp4YwCvYg3J/
MD5:	732D631679C87125581E7C89CFF8C256
SHA1:	0EBF386158D24CEF051FA7E1A088C98B56795738
SHA-256:	50CD773653EA7A75E511AA6CB16273AB4D520D2FCA90F821002439FB4086C5CE
SHA-512:	22E4DEBEB39057FEAC8843A4B915D12F195ACE755A255A713A8D0039DE71661381968E7DE1F4CCF4E2DAA4FE5C87E743A97BE1DEF66A1E93D44B6EF523D3F9 F6
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z...r8.JL..;a;...S,...X.F...Fa.q.....~;..h}kC.V..:/%R.....c....N.{..0.....x...x...x...x..... .....zV..... ..@.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\dl18aYTBo5.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 09:50:59 2022, mtime=Thu Aug 18 09:50:59 2022, atime=Thu Aug 18 09:51:09 2022, length=10190, window=hide
Category:	dropped
Size (bytes):	1019
Entropy (8bit):	4.5484356470711464
Encrypted:	false
SSDEEP:	12:8h3580gXg/XAlCPCHaXRBktB/ZABpX+WyFzGjuicvbLKGM54J4NDtZ3YilMMEpxK:8h3mk/XThOcpQ56NevLMQIDv3q5u7D
MD5:	436843168046552772570 94B01BEEE4E
SHA1:	502183CF7142C836D557AFCC92A9E7A6604D68E8
SHA-256:	1D7F597BEA5ADAE9E47C8F3064B5EDA0FEFC1FDA0751D0198E7E060638AE6735
SHA-512:	21B45E003FFBB16ADD86B2A8269620BF9F74E930ABBFC99BDAE2EFB54DC2BE939ED61827AB36E0F1E64EC38E499BC3F94BC76319D48FB36D7C928561B63573 D2
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....".f...".f...>..l....'.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....hT....user.8.....QK.XhT..*...&=....U.....A.l.b.u.s.....z.1.....U`V..Desktop.d.....QK.X.U`V*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1. 7.6.9.....h.2..'...UeV .DL18AY~1.DOC..L.....U`V.U`V*.....d.l.1.8.a.Y.T.B.o.5...d.o.c.x.....y.....-...8...[.....?J.....C:\Users\..#.....\\445817\ Users.user\Desktop\dl18aYTBo5.docx.&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.l.1.8.a.Y.T.B.o.5...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.....445817.....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):	4.721620404569601
Encrypted:	false
SSDEEP:	3:bDuMJlZ0nLLUmxWK0nLLUv:bCS0L+LC
MD5:	78743467AD7B7A7C4AEA7B26F05F0159
SHA1:	1EE278AFB6EAE05D6BAD394AC28A4AC85E36A994
SHA-256:	ABD0F630011CFCF4BA855FFF7AF8C5644D09A8F1A424F1EC8D3C0186ECCB6582
SHA-512:	DBCB93CE9E7236A91C1BCDF35F7840ABE97FDD5B915E1698A703058F108986C7AC64C7E5276B5D237429F9B146A475BBC9C91C1442BEC56C80A0674AFA7EF4 48
Malicious:	false
Preview:	[folders]..Templates.LNK=0..dl18aYTBo5.LNK=0..[misc]..dl18aYTBo5.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\~$18aYTBo5.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 OOXML
Entropy (8bit):	7.869840361272895
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:	dl18aYTBo5.docx
File size:	10190
MD5:	b91615355a11f5bb8b7c381a8bc4485a
SHA1:	7950b1730e05a2dcdd19f1a98a697798a9edbf77
SHA256:	3fdd30eb0961c98259d58327745ec253588b1553d9822d613d45d076c4b07ec1

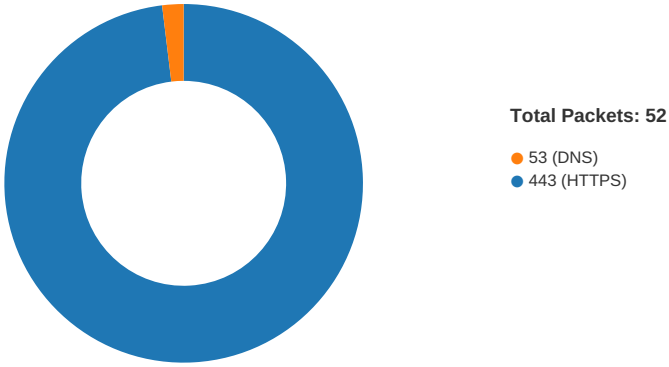
SHA512:	c8fbe110484db356ff4f67bcad94930b26fab9040a560a5a0d466d5766b2430b64585132048f787f0c7766b12e33ab765d415bd08a5fb7482a12d1da9160a00a
SSDEEP:	192:E5VR2DuRkZx41Jlb8VPkf+CFk4v1Y2VveFLC9Fi/CRQIZleDM:EHkZx0lD9+2Vv6aRdleDM
TLSH:	73229D3BEAA50DB4C6E69275E0AC1A25C35C06B7F33DF94A349423D812C85DD5BE530C
File Content Preview:	PK.....C.T...L....'.....[Content_Types].xml...n.0.E....m.NR....,.X...~...`.l.....C .....l....sg..'.m..kp^...Q4d...H..1.X...,. (.....x6..L.;.>.b.c.!...}.A!|d,h.....i.....K,....;....1.R.M'O..U....^WF.....Ub....6W.@.....(aM..r..3e....?J(#....7..S...p

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 03:51:10.470141888 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.470201969 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.470278025 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.484919071 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.484960079 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.535059929 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.535243034 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.551305056 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.551399946 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.551778078 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.551877975 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.826065063 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.852339029 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.852479935 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.852515936 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.852602005 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.852612972 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.852631092 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.852715969 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.852730989 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.852812052 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.852824926 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.852900982 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.852915049 CEST	443	49171	185.199.108.133	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 03:51:10.853101015 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.853199959 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.853224993 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.853241920 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.853260994 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.853307009 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.853318930 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.853382111 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.853393078 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.853451014 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.853463888 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.853545904 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.853558064 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.853617907 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.853631973 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.853689909 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.853702068 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.853780985 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.853796005 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.853857040 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.853871107 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.853933096 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.853950024 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.854020119 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.854032993 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.854093075 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.854106903 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.854167938 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.854178905 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.854254961 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.854268074 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.854326963 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.854343891 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.854352951 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.854372025 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.854377985 CEST	443	49171	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:10.854424953 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:10.854479074 CEST	49171	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:16.855664968 CEST	49172	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:16.855707884 CEST	443	49172	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:16.855793953 CEST	49172	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:16.856117010 CEST	49172	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:16.856132984 CEST	443	49172	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:16.893364906 CEST	443	49172	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:16.893438101 CEST	49172	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:16.904609919 CEST	49172	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:16.929476023 CEST	49172	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:16.929582119 CEST	443	49172	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:16.954840899 CEST	443	49172	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:16.954922915 CEST	49172	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:16.954951048 CEST	443	49172	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:16.955022097 CEST	49172	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:16.955034018 CEST	443	49172	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:16.955050945 CEST	443	49172	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:16.955094099 CEST	443	49172	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:16.955112934 CEST	49172	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:16.955132961 CEST	443	49172	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:16.955157995 CEST	49172	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:16.955171108 CEST	443	49172	185.199.108.133	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 03:51:16.955182076 CEST	49172	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:16.955188036 CEST	443	49172	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:16.955218077 CEST	49172	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:16.955234051 CEST	443	49172	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:16.955235958 CEST	49172	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:16.955246925 CEST	443	49172	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:16.955281019 CEST	49172	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:16.955291033 CEST	49172	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:16.955297947 CEST	443	49172	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:16.955310106 CEST	443	49172	185.199.108.133	192.168.2.22
Aug 18, 2022 03:51:16.955344915 CEST	49172	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:16.955380917 CEST	49172	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:16.955451965 CEST	49172	443	192.168.2.22	185.199.108.133
Aug 18, 2022 03:51:16.955471992 CEST	49172	443	192.168.2.22	185.199.108.133

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 03:51:10.438461065 CEST	55868	53	192.168.2.22	8.8.8.8
Aug 18, 2022 03:51:10.456965923 CEST	53	55868	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 03:51:10.438461065 CEST	192.168.2.22	8.8.8.8	0xca88	Standard query (0)	raw.github usercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 18, 2022 03:51:10.456965923 CEST	8.8.8.8	192.168.2.22	0xca88	No error (0)	raw.github usercontent.com		185.199.108.133	A (IP address)	IN (0x0001)
Aug 18, 2022 03:51:10.456965923 CEST	8.8.8.8	192.168.2.22	0xca88	No error (0)	raw.github usercontent.com		185.199.109.133	A (IP address)	IN (0x0001)
Aug 18, 2022 03:51:10.456965923 CEST	8.8.8.8	192.168.2.22	0xca88	No error (0)	raw.github usercontent.com		185.199.110.133	A (IP address)	IN (0x0001)
Aug 18, 2022 03:51:10.456965923 CEST	8.8.8.8	192.168.2.22	0xca88	No error (0)	raw.github usercontent.com		185.199.111.133	A (IP address)	IN (0x0001)

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	185.199.108.133	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:51:10 UTC	0	OUT	OPTIONS /drgreenthumb93/CVE-2022-30190-follina/main/ HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: raw.githubusercontent.com Content-Length: 0 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:51:10 UTC	0	IN	HTTP/1.1 403 Forbidden Connection: close Cache-Control: no-cache Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff X-Frame-Options: deny X-XSS-Protection: 0 Content-Security-Policy: default-src 'none'; style-src 'unsafe-inline' Accept-Ranges: bytes Date: Thu, 18 Aug 2022 01:51:10 GMT Via: 1.1 varnish X-Served-By: cache-mxp6935-MXP X-Cache: MISS X-Cache-Hits: 0 X-Timer: S1660787471.831212,VS0,VE9 Access-Control-Allow-Origin: * X-Fastly-Request-ID: 0038ae362210300c11e8b16daefe6a458ddf6fd4 Expires: Thu, 18 Aug 2022 01:56:10 GMT Vary: Authorization,Accept-Encoding transfer-encoding: chunked
2022-08-18 01:51:10 UTC	0	IN	Data Raw: 39 38 34 0d 0a Data Ascii: 984
2022-08-18 01:51:10 UTC	0	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 0d 0a 0d 0a 48 65 6c 6c 6f 20 66 75 74 75 72 65 20 47 69 74 48 75 62 62 65 72 21 20 49 20 62 65 74 20 79 6f 75 27 72 65 20 68 65 72 65 20 74 6f 20 72 65 6d 6f 76 65 20 74 68 6f 73 65 20 6e 61 73 74 79 20 69 6e 6c 69 6e 65 20 73 74 79 6c 65 73 2c 0d 0a 44 52 59 20 75 70 20 74 68 65 73 65 20 74 65 6d 70 6c 61 74 65 73 20 61 6e 64 20 6d 61 6b 65 20 27 65 6d 20 6e 69 63 65 20 61 6e 64 20 72 65 2d 75 73 61 62 6c 65 2c 20 72 69 67 68 74 3f 0d 0a 0d 0a 50 6c 65 61 73 65 2c 20 64 6f 6e 27 74 2e 20 68 74 74 70 73 3a 2f 2f 67 69 74 68 75 62 2e 63 6f 6d 2f 73 74 79 6c 65 67 75 69 64 65 2f 74 65 6d 70 6c 61 74 65 73 2f 32 2e 30 0d 0a 0d 0a 2d 2d 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 3c 68 65 61 64 3e 0d Data Ascii: <!DOCTYPE html>...Hello future GitHubber! I bet you're here to remove those nasty inline styles,DRY up these templates and make 'em nice and re-usable, right?Please, don't. https://github.com/styleguide/templates/2.0--><html> <head>
2022-08-18 01:51:10 UTC	2	IN	Data Raw: 20 20 20 20 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 20 32 29 2c 0d 0a 20 20 20 20 20 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 69 6e 2d 72 65 73 6f 6c 75 74 69 6f 6e 3a 20 31 39 32 64 70 69 29 2c 0d 0a 20 20 20 20 20 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 69 6e 2d 72 65 73 6f 6c 75 74 69 6f 6e 3a 20 32 64 70 70 78 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 2e 6c 6f 67 6f 2d 69 6d 67 2d 31 78 20 7b 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 6c 6f 67 6f 2d 69 6d 67 2d 32 78 20 7b 20 64 69 73 70 6c 61 79 3a 20 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 20 7d 0d 0a 20 20 Data Ascii: min-device-pixel-ratio: 2), only screen and (min-resolution: 192dpi), only screen and (min-resolution: 2dppx) { .logo-img-1x { display: none; } .logo-img-2x { display: inline-block; }
2022-08-18 01:51:10 UTC	3	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:51:10 UTC	3	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:51:10 UTC	3	IN	Data Raw: 6c 65 4a 62 55 35 6c 73 4f 46 52 76 45 35 46 75 4f 50 53 34 57 4c 53 74 37 2b 38 61 6a 76 58 63 4a 70 63 79 4e 76 68 7a 74 53 77 55 6b 54 47 67 5a 7a 39 75 44 53 78 52 6e 50 5a 77 73 6e 54 6b 71 79 37 6a 70 73 50 74 2f 41 78 79 76 6e 41 65 4a 4d 41 78 50 6e 4d 69 71 50 4a 59 49 79 7a 66 34 2f 4b 71 72 50 65 64 61 4b 35 62 49 73 51 77 66 54 6f 32 74 37 32 68 55 65 70 50 57 76 6e 36 6d 4f 38 56 6f 58 72 67 62 44 52 61 4a 58 6c 65 36 72 37 35 46 7a 5a 6d 37 53 32 54 6e 79 54 4e 55 58 76 35 65 69 44 41 41 36 6a 30 57 6d 4b 79 57 76 35 31 6c 69 52 41 41 43 6a 50 30 4f 5a 4e 56 75 77 61 34 4c 2b 75 51 41 63 77 2f 53 69 4e 47 48 35 37 6d 49 78 78 50 4b 6d 55 33 44 67 70 4c 32 73 58 33 72 75 74 63 33 2f 76 68 39 67 75 31 44 33 74 4e 45 41 74 76 4f 53 4b 56 41 6d Data Ascii: leJbU5lsOFRvE5FuOPS4WLSt7+8ajvXcJpcyNvhztSwUkTGgZz9uDSxRnPZwsnTkqy7jpsPt/Axyvn AeJMAxPnMiqPJYlyzf4/KqrPedaK5bIsQwfTo2t72hUepPWvn6mO8VoXrgbDRaJXle6r75FzZm7S2TnyTNUXv5eiDA A6j0WmKyWv51liRAACjP0OZNVuwa4L+uQAcw/SiNGH57mIxxPKmU3DgpL2sX3rutc3/vh9gu1D3tNEAtvOSKVAm
2022-08-18 01:51:10 UTC	4	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:51:10 UTC	4	IN	Data Raw: 61 62 34 0d 0a Data Ascii: ab4
2022-08-18 01:51:10 UTC	4	IN	Data Raw: 4f 4a 77 75 5a 67 39 62 31 6a 66 33 67 51 52 37 72 36 57 31 6b 54 53 63 51 70 46 6a 50 78 4b 4f 77 44 67 41 49 55 7a 79 7a 51 4f 51 52 59 4d 79 64 6b 7a 49 37 59 5a 62 69 64 44 6b 63 54 6b 55 4b 51 57 61 7a 4f 65 69 74 58 46 39 68 42 77 35 53 5a 63 69 5a 4f 69 39 54 36 47 6e 6b 4d 70 30 75 4b 79 6d 51 6b 44 48 48 41 78 7a 4d 4c 77 63 53 4d 2b 65 5a 4a 71 57 68 73 6b 68 4f 4d 69 76 44 44 73 63 49 43 35 6f 68 79 57 2b 78 31 6c 54 6d 35 36 2b 76 32 44 6b 47 47 6c 7a 39 46 53 45 6e 79 6e 52 64 67 50 4b 55 6c 65 7a 54 43 53 54 65 34 7a 47 6e 5a 66 73 56 74 6d 57 54 33 34 6b 6c 6a 41 6d 4a 67 41 62 42 53 45 75 59 79 51 49 6a 4c 6e 67 6e 6b 4c 42 55 67 6b 4a 46 59 36 50 64 62 67 63 4b 61 45 78 54 66 7a 34 38 46 6e 78 61 61 6e 78 38 66 47 70 36 68 6c 59 31 66 76 Data Ascii: OJwuZg9b1jf3gQR7r6W1kTScQpFjPxKOwDgAIUzyzQOQRYMydkzI7YZbidDkcTkUKQWazOeitXF9hB w5SZciZOi9T6GnkMp0uKymQkDHHAxzMLwcSM+eZJqWhskhOMivDDscIC5ohyW+x1ITm56+v2DkGGlz9FSEnynRdgPK UlezTCSTe4zGnZfsVtmWT34kljAmJgAbBSEuYyQIjLngnkLBUgkJFY6PdbgcKaExTfz48Fnxaanx8fGp6hlY1fv
2022-08-18 01:51:10 UTC	5	IN	Data Raw: 4c 51 41 67 44 51 31 6c 56 52 37 67 34 6f 63 43 4d 32 65 2b 37 31 46 64 32 4b 66 48 4a 42 34 32 73 76 46 77 7a 70 4b 67 41 7a 45 4e 56 6e 59 52 37 2f 64 62 68 7a 49 79 66 4e 64 61 7a 43 4b 42 30 52 70 37 38 35 4a 41 34 71 39 73 57 4c 39 2b 73 70 4b 69 35 65 68 66 76 52 62 30 63 46 76 72 4b 30 4a 34 75 2b 64 33 70 6d 56 47 52 6c 77 31 73 47 38 70 74 37 61 6b 75 70 67 30 4b 6b 45 5a 73 5a 2f 66 39 45 64 65 61 38 42 68 43 51 79 33 37 69 41 70 43 69 43 52 2f 33 4b 4d 56 31 49 5a 79 64 32 56 2b 73 6c 79 59 6e 34 45 61 30 48 56 35 4d 69 4e 77 61 7a 52 6c 67 53 55 6d 58 42 41 79 34 72 66 56 71 42 34 4c 2b 76 53 49 36 53 38 71 34 43 32 2f 77 61 68 42 4b 2f 4a 79 48 39 2b 2f 4a 62 77 6a 6d 68 55 68 63 34 68 4d 39 4b 54 6b 65 45 64 5a 6f 35 6a 36 70 6a 34 77 77 6b Data Ascii: LQAgDQ1lVR7g4ocCM2e+71Fd2KfHJB42svFwzpKgAzENVnYR7/dbhzIyfNdazCKB0Rp785JA4q9sWL 9+spKi5ehfvRb0cFvrK0J4u+d3pmVGRlw1sG8pt7akupg0KkEZsZ/f9Edea8BhCQy37iApCiCR/3KMV1IZyd2V+sly Yn4Ea0HV5MiNwazRlgSUmXBAy4rfVqB4L+vSI6S8q4C2/wahBK/JyH9+/JbwjmhUhc4hM9KTkeEdZo5j6pj4wwk
2022-08-18 01:51:10 UTC	7	IN	Data Raw: 0d 0a Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:51:10 UTC	7	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:51:10 UTC	7	IN	Data Raw: 50 36 30 55 2b 49 53 4f 45 67 41 65 41 31 49 38 68 71 75 73 68 76 54 4f 48 45 69 31 59 53 54 67 51 37 37 50 5a 49 34 71 4d 74 58 4f 31 4d 33 2f 36 31 4b 6c 69 4f 30 58 31 69 37 43 55 53 4c 56 6a 4b 32 73 76 61 34 38 51 6f 6a 72 45 6a 57 57 78 49 79 67 37 51 54 67 49 53 51 7a 74 52 6f 76 56 34 6e 43 49 4a 79 54 4a 6a 54 45 4a 4c 4a 39 49 69 62 4e 54 35 32 71 72 6a 4a 50 69 34 49 74 71 6f 66 51 6e 44 4f 73 7a 78 73 38 62 79 43 77 49 63 52 78 35 4a 62 61 53 49 67 6d 47 34 6d 46 50 59 69 53 30 42 6b 56 57 50 48 6e 72 42 4f 75 46 5a 42 36 45 70 4c 37 66 41 44 4b 57 63 78 49 68 76 61 6f 76 49 6f 61 41 78 38 48 44 41 38 4d 49 4a 42 61 52 62 42 57 66 4c 72 61 54 6e 54 52 65 31 48 53 63 66 78 6c 51 65 46 44 68 41 49 37 72 51 49 35 7a 38 77 41 4f 70 43 39 4f 48 48 Data Ascii: P60U+ISOEgAeA1I8hqushvTOHEi1YSTgQ77PZl4qMtXO1M3/61KliO0X1i7CUSLVjK2sva48QojrEj WWxIyg7QTgISQztRovV4nCIJyTJjTEJLJ9IibNT52qrjJPi4ItqofQnDOszxs8byCwIcRx5JbaSIgmG4mFPYiS0BkV WPHnrBOuFZB6EpL7fADKWcxIhvaovIoaAx8HDA8MIJBaRbBWfLraTnTRe1HScfxlQeFDhAl7rQI5z8wAOpC9OHH
2022-08-18 01:51:10 UTC	8	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:51:10 UTC	8	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:51:10 UTC	8	IN	Data Raw: 4f 52 4a 6e 48 6a 39 46 6b 57 49 44 71 52 71 50 42 42 69 45 64 48 4b 71 71 41 79 5a 50 6a 36 50 67 41 42 6b 66 64 61 52 74 79 63 53 48 38 78 67 41 43 4a 66 59 77 77 52 44 44 52 6f 5a 51 74 7a 6e 2f 2b 2b 66 7a 46 69 38 76 4b 68 4b 6c 4d 4a 49 31 4c 4e 4a 7a 49 4b 46 39 74 6c 55 45 46 55 76 66 4f 6d 71 4c 56 71 31 63 45 46 66 37 66 6a 42 30 51 45 30 39 53 6d 55 71 6b 70 41 42 49 43 6e 6f 4c 43 67 70 4f 35 51 55 56 4a 4d 53 4b 39 46 31 62 77 43 61 6b 74 58 35 47 6b 73 69 57 6f 36 74 30 33 55 41 67 57 6f 78 61 71 77 4b 5a 64 48 4b 58 67 4e 77 6e 6a 64 37 2b 53 38 38 77 49 79 49 71 6b 47 4a 78 58 31 78 73 38 43 69 47 78 6e 73 77 50 42 7a 76 76 6a 51 71 5a 57 55 62 4e 6d 79 6f 34 39 71 77 51 57 65 69 50 37 73 42 31 51 6e 48 45 6b 45 46 57 4b 70 72 6f 4f 6f 69 Data Ascii: ORJnHj9FkWIDqRqPBBiEdHKqqAyZPj6PgABkfdaRtycSH8xgACJfYwwRDDRoZQtzn/++fzFi8vKhKl MJI1LNJzIKF9tlUEFUvfOmqLVq1cEFf7fjB0QE09SmUqkpABICnoLCgpO5QUVJMSK9F1bwCaktX5GksiWo6t03UAgW oxaqwKZdHKXgNwnjd7+S88wIyIqkGJxX1xs8CiGxnswPBzvvjQqZWUbNmyo49qwQWeiP7sB1QnHEkEFWKproOoi
2022-08-18 01:51:10 UTC	9	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:51:10 UTC	9	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:51:10 UTC	9	IN	Data Raw: 54 54 4f 4a 38 59 56 6c 5a 4f 2b 2f 49 41 34 70 34 45 6e 76 44 4e 6c 5a 59 2f 55 45 4a 35 6b 48 79 70 45 34 52 45 4a 4e 36 7a 4a 69 4d 4e 63 51 6d 57 45 68 70 71 59 31 37 4c 54 4b 53 32 68 4a 6b 58 57 36 6d 31 69 51 50 50 34 6b 51 59 58 64 64 35 7a 6f 4d 4d 64 50 46 6a 55 30 36 44 7a 63 34 47 54 7a 77 43 45 43 71 39 6e 63 65 32 2b 51 50 76 55 68 41 71 71 4c 57 78 47 75 6b 62 47 2f 62 47 30 4d 75 5a 67 42 42 71 72 57 48 71 68 45 35 5a 4f 30 41 6b 54 45 65 53 4d 4b 67 52 46 4d 68 48 6c 39 2f 66 61 59 77 56 2f 56 64 47 38 72 47 5a 32 41 61 69 2f 4f 71 43 6e 4e 7a 38 52 52 38 46 73 53 66 46 55 59 42 72 56 68 52 59 33 55 6f 45 74 58 73 58 73 62 46 57 2b 2b 78 42 6d 4a 30 47 70 4d 43 50 50 75 31 67 49 6a 4e 56 74 72 56 61 30 4e 63 4a 2b 46 52 45 58 50 7a 77 6a Data Ascii: TTOJ8YVlZO+/IA4p4EnvDNlZY/UEJ5kHypE4REJN6zJiMNcQmWEhpqY17LTKS2hJkXW6m1iQPP4kQY Xdd5zoMMdPFjU06Dzc4GTzwCECq9nce2+QPvUhAqqLWxGukbG/bG0MuZgBBqrWHqhE5ZO0AkTEeSMKgR FMhHl9/faYwV/VdG8rGZ2Aai/OqCnNz8RR8FsSfFUYBrVhRY3UoEtXsXsbFW++xBmJ0GpMCPPu1gIjNVtrVa0NcJ+F REXPzwj
2022-08-18 01:51:10 UTC	11	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:51:10 UTC	11	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:51:10 UTC	11	IN	Data Raw: 2b 7a 45 6e 77 41 6b 6a 4d 69 62 71 4e 66 64 53 6d 68 52 62 79 53 4f 4b 46 76 52 65 65 51 69 62 38 72 6c 74 6c 4a 34 37 73 77 35 33 4d 36 63 51 6c 41 42 44 55 45 48 4f 41 51 52 76 6e 63 45 67 59 4e 5a 46 78 49 70 4e 63 42 54 76 69 56 4c 46 46 57 45 6e 66 69 54 71 46 43 65 63 69 41 30 69 35 64 41 2f 56 70 71 62 45 46 4d 64 73 41 36 6c 4f 70 6d 68 48 68 61 62 2b 66 74 52 6a 4c 58 6d 61 6b 45 59 49 4b 2b 43 57 5a 4b 43 41 68 61 68 6c 35 6d 32 59 53 69 52 46 62 49 68 34 48 49 68 46 42 65 67 73 63 53 51 49 36 74 6a 47 79 63 55 4a 4a 31 72 2b 32 6a 55 4d 2b 62 45 55 42 75 48 45 4c 53 51 2b 56 36 37 78 58 61 4a 70 54 4f 35 49 72 67 51 53 57 47 65 48 53 4f 61 73 52 7a 68 58 69 45 38 6a 31 61 51 49 42 5a 4b 49 6e 56 4c 4d 52 6a 56 57 68 68 71 56 51 63 59 43 4c 4d Data Ascii: +zEnwAkjMibqNfdSmhRbySOKFvReeQib8rltJ47sw53M6cQlABDUEHOAQRvncEgYNZFxIpNcBTviV LFFWEnfiTqFCeciA0i5dA/VpqbEFMdsA6lOpmhHhab+ftRjLXmakEYIK+CWZKCAhahl5m2YSiRFbIh4HIhFBegscSQ l6tjGycUJJ1r+2jUM+bEUBuHELSQ+V67xXaJpTO5IrgQSWGeHSOasRzhXiE8j1aQIBZKInVLMRjVWhhqVQcYCLM
2022-08-18 01:51:10 UTC	12	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:51:10 UTC	12	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a
2022-08-18 01:51:10 UTC	12	IN	Data Raw: 77 6c 4e 35 46 48 45 45 75 65 4f 43 52 49 53 44 5a 41 43 61 52 57 42 59 75 4e 4d 79 6c 62 69 6c 34 6b 46 5a 64 45 4e 6f 42 4b 50 42 66 45 44 63 53 6a 4a 30 51 6b 54 69 38 48 36 63 59 69 4e 48 39 42 5a 47 4e 52 49 52 63 56 6f 6d 74 74 37 79 38 76 4c 65 32 61 61 4f 58 65 5a 30 53 68 6f 31 68 73 33 77 47 51 6a 74 72 6b 62 33 59 79 73 57 54 58 76 46 64 6e 32 43 69 63 64 6d 45 4a 4e 6a 51 70 69 33 69 6e 6f 44 38 54 33 31 6b 4a 77 74 6c 43 49 69 38 32 53 4d 50 30 35 4a 68 64 46 67 66 52 73 74 58 4a 7a 41 35 46 58 54 66 6f 53 76 51 57 66 54 68 44 57 32 34 58 4b 68 37 73 49 6b 45 47 31 6b 71 73 72 41 64 46 77 79 74 65 58 6e 35 65 63 45 45 4f 77 79 65 45 4a 46 6b 49 6a 4b 6c 51 49 7a 30 56 33 49 47 48 55 53 6b 71 62 62 38 44 70 71 2f 61 50 32 69 39 32 75 56 6e 4c Data Ascii: wlN5FHEEueOCRISDZACaRWBYuNMylbil4kFZdENoBKPBfEDcSjJ0QkTi8H6cYiNH9BZGNRIRcVomtt 7y8vLe2aaOXeZ0Sho1hs3wGQjtrkb3YysWTXvFdn2CicdmEJNjQpi3inoD8T31kJwtlCli82SMP05JhdFgfRstXJzA 5FXTfoSvQWfThDW24XKh7sIkEG1kqsrAdFwyteXn5ecEEOwyeEJFkIjKlQIz0V3IGHUSkqbb8Dpq/aP2i92uVnL
2022-08-18 01:51:10 UTC	13	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:51:10 UTC	13	IN	Data Raw: 35 35 61 0d 0a Data Ascii: 55a

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:51:10 UTC	13	IN	Data Raw: 5a 33 49 65 6b 6d 52 64 61 45 4c 72 53 77 42 68 43 2b 49 52 45 58 31 4c 7a 2f 4b 51 76 4c 67 6b 72 4d 48 65 6b 34 4d 6a 64 65 4a 48 67 7a 58 44 52 34 34 34 48 4b 48 59 43 75 75 6d 75 65 58 61 30 41 45 6b 72 4f 4c 2b 50 31 44 6f 43 77 6c 4b 67 54 69 36 70 4b 6c 32 45 63 51 4d 54 4c 68 6c 35 66 58 72 61 43 35 4f 66 68 32 61 6a 56 4f 4f 52 44 52 6a 39 66 4f 44 56 58 4c 64 6c 74 70 65 55 6b 4a 70 6f 53 34 79 6c 64 54 6f 38 33 4e 33 2f 6d 49 49 77 33 72 6b 50 4a 71 38 51 51 33 32 6e 52 54 51 58 54 78 67 70 36 52 45 70 38 63 79 7a 6c 32 30 6f 36 49 48 67 31 45 62 67 47 51 74 74 75 76 39 77 7a 53 53 57 33 52 77 72 43 44 34 73 33 65 4e 54 42 34 63 4d 39 62 62 37 7a 39 39 68 2b 46 33 6e 37 37 6a 62 66 32 48 42 78 75 41 5a 63 42 47 63 61 69 45 42 54 48 38 34 67 71 Data Ascii: Z3IekmRdaELrSwBhC+IREX1Lz/KQvLgkrMHek4MjdeJHgzXDR444HKHYCuumueXa0AEkrOL+P1DoCw lKgTi6pKl2EcQMTLhl5fXraC5Ofh2ajVOORDRj9fODVXLdltpeUkJpoS4yldTo83N3/mIIw3rkPJq8QQ32nRTQXTxg p6REp8cyzl20o6lHg1EbgGQttuv9wzSSW3RwrCD4s3eNTB4cM9bb7z99h+F3n77jbf2HBxuAZcBGcaiEBTH84gq

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49172	185.199.108.133	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:51:16 UTC	15	OUT	OPTIONS /drgreenthumb93/CVE-2022-30190-follina/main/ HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: raw.githubusercontent.com Content-Length: 0 Connection: Keep-Alive
2022-08-18 01:51:16 UTC	15	IN	HTTP/1.1 403 Forbidden Connection: close Cache-Control: no-cache Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff X-Frame-Options: deny X-XSS-Protection: 0 Content-Security-Policy: default-src 'none'; style-src 'unsafe-inline' Accept-Ranges: bytes Date: Thu, 18 Aug 2022 01:51:16 GMT Via: 1.1 varnish X-Served-By: cache-mxp6942-MXP X-Cache: MISS X-Cache-Hits: 0 X-Timer: S1660787477.934296,VS0,VE9 Access-Control-Allow-Origin: * X-Fastly-Request-ID: 86ac34f2a7f5281d6f97d13ae2197222c90618af Expires: Thu, 18 Aug 2022 01:56:16 GMT Vary: Authorization,Accept-Encoding transfer-encoding: chunked
2022-08-18 01:51:16 UTC	16	IN	Data Raw: 34 32 61 0d 0a Data Ascii: 42a
2022-08-18 01:51:16 UTC	16	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 0d 0a 0d 0a 48 65 6c 6c 6f 20 66 75 74 75 72 65 20 47 69 74 48 75 62 62 65 72 21 20 49 20 62 65 74 20 79 6f 75 27 72 65 20 68 65 72 65 20 74 6f 20 72 65 6d 6f 76 65 20 74 68 6f 73 65 20 6e 61 73 74 79 20 69 6e 6c 69 6e 65 20 73 74 79 6c 65 73 2c 0d 0a 44 52 59 20 75 70 20 74 68 65 73 65 20 74 65 6d 70 6c 61 74 65 73 20 61 6e 64 20 6d 61 6b 65 20 27 65 6d 20 6e 69 63 65 20 61 6e 64 20 72 65 2d 75 73 61 62 6c 65 2c 20 72 69 67 68 74 3f 0d 0a 0d 0a 50 6c 65 61 73 65 2c 20 64 6f 6e 27 74 2e 20 68 74 74 70 73 3a 2f 2f 67 69 74 68 75 62 2e 63 6f 6d 2f 73 74 79 6c 65 67 75 69 64 65 2f 74 65 6d 70 6c 61 74 65 73 2f 32 2e 30 0d 0a 0d 0a 2d 2d 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 3c 68 65 61 64 3e 0d Data Ascii: <!DOCTYPE html>...Hello future GitHubber! I bet you're here to remove those nasty inline styles,DRY up these templates and make 'em nice and re-usable, right?Please, don't. https://github.com/styleguide/templates/2.0--><html> <head>
2022-08-18 01:51:16 UTC	17	IN	Data Raw: 0d 0a Data Ascii:
2022-08-18 01:51:16 UTC	17	IN	Data Raw: 32 30 31 63 0d 0a Data Ascii: 201c
2022-08-18 01:51:16 UTC	17	IN	Data Raw: 6f 67 6f 20 7b 20 64 69 73 70 6c 61 79 3a 20 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 20 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 33 35 70 78 3b 20 7d 0d 0a 20 20 20 20 20 20 2e 6c 6f 67 6f 2d 69 6d 67 2d 32 78 20 7b 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 20 7d 0d 0a 20 20 20 20 20 20 40 6d 65 64 69 61 0d 0a 20 20 20 20 20 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 20 32 29 2c 0d 0a 20 20 20 20 20 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 20 20 20 20 6d 69 6e 2d 6d 6f 7a 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 20 32 29 2c 0d 0a 20 20 20 20 20 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 20 20 20 20 20 2d 6f 2d 6d Data Ascii: ogo { display: inline-block; margin-top: 35px; } .logo-img-2x { display: none; } @media only screen and (-webkit-min-device-pixel-ratio: 2), only screen and (min--moz-device-pixel-ratio: 2), only screen and (-o-m
2022-08-18 01:51:16 UTC	18	IN	Data Raw: 4f 46 52 76 45 35 46 75 4f 50 53 34 57 4c 53 74 37 2b 38 61 6a 76 58 63 4a 70 63 79 4e 76 68 7a 74 53 77 55 6b 54 47 67 5a 7a 39 75 44 53 78 52 6e 50 5a 77 73 6e 54 6b 71 79 37 6a 70 73 50 74 2f 41 78 79 76 6e 41 65 4a 4d 41 78 50 6e 4d 69 71 50 4a 59 49 79 7a 66 34 2f 4b 71 72 50 65 64 61 4b 35 62 49 73 51 77 66 54 6f 32 74 37 32 68 55 65 70 50 57 76 6e 36 6d 4f 38 56 6f 58 72 67 62 44 52 61 4a 58 6c 65 36 72 37 35 46 7a 5a 6d 37 53 32 54 6e 79 54 4e 55 58 76 35 65 69 44 41 41 36 6a 30 57 6d 4b 79 57 76 35 31 6c 69 52 41 41 43 6a 50 30 4f 5a 4e 56 75 77 61 34 4c 2b 75 51 41 63 77 2f 53 69 4e 47 48 35 37 6d 49 78 78 50 4b 6d 55 33 44 67 70 4c 32 73 58 33 72 75 74 63 33 2f 76 68 39 67 75 31 44 33 74 4e 45 41 74 76 4f 53 4b 56 41 6d 78 66 61 67 52 6d 62 6e Data Ascii: OFRvE5FuOPS4WLSt7+8ajvXcJpcyNvhztSwUkTGgZz9uDSxRnPZwsnTkqy7jpsPt/AxyvnAeJMAxPn MiqPJYIyzf4/KqrPedaK5bIsQwfTo2t72hUepPWvn6mO8VoXrgbDRaJXle6r75FzZm7S2TnyTNUXv5eiDAA6j0WmKy Wv51liRAACjP0OZNVuwa4L+uQAcw/SiNGH57mIxxPKmU3DgpL2sX3rutc3/vh9gu1D3tNEAtvOSKVAmxfagRmbn

Timestamp	kBytes transferred	Direction	Data
2022-08-18 01:51:16 UTC	19	IN	Data Raw: 72 36 57 31 6b 54 53 63 51 70 46 6a 50 78 4b 4f 77 44 67 41 49 55 7a 79 7a 51 4f 51 52 59 4d 79 64 6b 7a 49 37 59 5a 62 69 64 44 6b 63 54 6b 55 4b 51 57 61 7a 4f 65 69 74 58 46 39 68 42 77 35 53 5a 63 69 5a 4f 69 39 54 36 47 6e 6b 4d 70 30 75 4b 79 6d 51 6b 44 48 48 41 78 7a 4d 4c 77 63 53 4d 2b 65 5a 4a 71 57 68 73 6b 68 4f 4d 69 76 44 44 73 63 49 43 35 6f 68 79 57 2b 78 31 6c 54 6d 35 36 2b 76 32 44 6b 47 47 6c 7a 39 46 53 45 6e 79 6e 52 64 67 50 4b 55 6c 65 7a 54 43 53 54 65 34 7a 47 6e 5a 66 73 56 74 6d 57 54 33 34 6b 6c 6a 41 6d 4a 67 41 62 42 53 45 75 59 79 51 49 6a 4c 6e 67 6e 6b 4c 42 55 67 6b 4a 46 59 36 50 64 62 67 63 4b 61 45 78 54 66 7a 34 38 46 6e 78 61 61 6e 78 38 66 47 70 36 68 6c 59 31 66 76 63 55 37 70 38 53 53 45 59 32 38 38 4e 41 6e 50 Data Ascii: r6W1kTScQpFjPxKOwDgAlUzyzQOQRYMydkzI7YZbidDkcTkUKQWazOeitXF9hBw5SZciZOi9T6GnkM p0uKymQkDHHAxzMLwcSM+eZJqWhskhOMivDDsclC5ohyW+x1lTm56+v2DkGGlz9FSEnynRdgPKUlezTCSTe4zGnZfs VtmWT34kljAmJgAbBSEuYyQljLngnkLBUgkJFY6PdbgcKaExTfz48Fnxaanx8fGp6hlY1fvcU7p8SSEY288NAnP
2022-08-18 01:51:16 UTC	21	IN	Data Raw: 4d 32 65 2b 37 31 46 64 32 4b 66 48 4a 42 34 32 73 76 46 77 7a 70 4b 67 41 7a 45 4e 56 6e 59 52 37 2f 64 62 68 7a 49 79 66 4e 64 61 7a 43 4b 42 30 52 70 37 38 35 4a 41 34 71 39 73 57 4c 39 2b 73 70 4b 69 35 65 68 66 76 52 62 30 63 46 76 72 4b 30 4a 34 75 2b 64 33 70 6d 56 47 52 6c 77 31 73 47 38 70 74 37 61 6b 75 70 67 30 4b 6b 45 5a 73 5a 2f 66 39 45 64 65 61 38 42 68 43 51 79 33 37 69 41 70 43 69 43 52 2f 33 4b 4d 56 31 49 5a 79 64 32 56 2b 73 6c 79 59 6e 34 45 61 30 48 56 35 4d 69 4e 77 61 7a 52 6c 67 53 55 6d 58 42 41 79 34 72 66 56 71 42 34 4c 2b 76 53 49 36 53 38 71 34 43 32 2f 77 61 68 42 4b 2f 4a 79 48 39 2b 2f 4a 62 77 6a 6d 68 55 68 63 34 68 4d 39 4b 54 6b 65 45 64 5a 6f 35 6a 36 70 6a 34 77 77 6b 33 34 71 4b 4a 42 70 48 52 61 55 5a 67 7a 2f 34 Data Ascii: M2e+71Fd2KfHJB42svFwzpKgAzENVnYR7/dbhzIyfNdazCKB0Rp785JA4q9sWL9+spKi5ehfvRb0cF vrK0J4u+d3pmVGRlw1sG8pt7akupg0KkEZsZ/f9Edea8BhCQy37iApCiCR/3KMV1IZyd2V+slyYn4Ea0HV5MiNwazR lgSUmXBAy4rfVqB4L+vSI6S8q4C2/wahBK/JyH9+/JbwjmhUhc4hM9KTkeEdZo5j6pj4wwk34qKJBpHRaUZgz/4
2022-08-18 01:51:16 UTC	22	IN	Data Raw: 51 37 37 50 5a 49 34 71 4d 74 58 4f 31 4d 33 2f 36 31 4b 6c 69 4f 30 58 31 69 37 43 55 53 4c 56 6a 4b 32 73 76 61 34 38 51 6f 6a 72 45 6a 57 57 78 49 79 67 37 51 54 67 49 53 51 7a 74 52 6f 76 56 34 6e 43 49 4a 79 54 4a 6a 54 45 4a 4c 4a 39 49 69 62 4e 54 35 32 71 72 6a 4a 50 69 34 49 74 71 6f 66 51 6e 44 4f 73 7a 78 73 38 62 79 43 77 49 63 52 78 35 4a 62 61 53 49 67 6d 47 34 6d 46 50 59 69 53 30 42 6b 56 57 50 48 6e 72 42 4f 75 46 5a 42 36 45 70 4c 37 66 41 44 4b 57 63 78 49 68 76 61 6f 76 49 6f 61 41 78 38 48 44 41 38 4d 49 4a 42 61 52 62 42 57 66 4c 72 61 54 6e 54 52 65 31 48 53 63 66 78 6c 51 65 46 44 68 41 49 37 72 51 49 35 7a 38 77 41 4f 70 43 39 4f 48 48 74 6d 72 53 6b 71 57 72 78 34 39 57 72 68 77 36 44 46 69 34 75 71 61 79 79 4d 44 67 61 67 59 42 Data Ascii: Q77PZI4qMtXO1M3/61KliO0X1i7CUSLVjK2sva48QojrEjWWxIyg7QTgISQztRovV4nCIJyTJjTEJLJ9IibNT52q rjJPi4ItqofQnDOszxs8byCwIcRx5JbaSIgmG4mFPYiS0BkVWPHnrBOuFZB6EpL7fADKWcxIhvaovIoaAx8HDA8MIJ BaRbBWfLraTnTRe1HScfxlQeFDhAI7rQI5z8wAOpC9OHHtmrSkqWrx49Wrhw6DFi4uqayyMDgagYB
2022-08-18 01:51:16 UTC	23	IN	Data Raw: 74 79 63 53 48 38 78 67 41 43 4a 66 59 77 77 52 44 44 52 6f 5a 51 74 7a 6e 2f 2b 2b 66 7a 46 69 38 76 4b 68 4b 6c 4d 4a 49 31 4c 4e 4a 7a 49 4b 46 39 74 6c 55 45 46 55 76 66 4f 6d 71 4c 56 71 31 63 45 46 66 37 66 6a 42 30 51 45 30 39 53 6d 55 71 6b 70 41 42 49 43 6e 6f 4c 43 67 70 4f 35 51 55 56 4a 4d 53 4b 39 46 31 62 77 43 61 6b 74 58 35 47 6b 73 69 57 6f 36 74 30 33 55 41 67 57 6f 78 61 71 77 4b 5a 64 48 4b 58 67 4e 77 6e 6a 64 37 2b 53 38 38 77 49 79 4 9 71 6b 47 4a 78 58 31 78 73 38 43 69 47 78 6e 73 77 50 42 7a 76 76 6a 51 71 5a 57 55 62 4e 6d 79 6f 34 39 71 77 51 57 65 69 50 37 73 42 31 51 6e 48 45 6b 45 46 57 4b 70 72 6f 4f 6f 69 6e 6a 61 76 50 6a 49 69 73 52 68 4d 64 4d 32 49 72 4f 50 38 54 43 58 53 62 4c 4e 31 6c 4b 4d 59 73 5a 58 4d 64 30 68 4f Data Ascii: tycSH8xgACJfYwwRDDRoZQtzn/++fzFi8vKhKlMJI1LNJzIKF9tlUEFUvfOmqLVq1cEFf7fjB0QE09SmUqkpABIC noLCgpO5QUVJMSK9F1bwCaktX5GksiWo6t03UAgWoxaqwKZdHKXgNwnjd7+S88wIyIqkGJxX1xs8CiGxnswPBzvvjQ qZWUbNmyo49qwQWeiP7sB1QnHEkEFWKproOoinjavPjlisRhMdM2IrOP8TCXSbLN1lKMYsZXMd0hO

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: **1216**, Parent PID: **576**

General

Target ID:	0
Start time:	03:51:10
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:	0x13f9f0000
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	6DFA2B14	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$18aYTBo5.docx	success or wait	1	6E020648	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6DFFA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6DFFA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6DFFA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E020648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6E020648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6E020648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\6EBC5	success or wait	1	6E020648	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\6EBC5	6EBC5	binary	04 00 00 00 C0 04 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 AF B8 65 85 F0 B2 D8 01 C5 EB 06 00 C5 EB 06 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	6E020648	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 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	6E020648	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	6E020648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\6EBC5	6EBC5	binary	04 00 00 00 C0 04 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 AF B8 65 85 F0 B2 D8 01 C5 EB 06 00 C5 EB 06 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	04 00 00 00 C0 04 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 C5 EB 06 00 C5 EB 06 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 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	success or wait	1	6E020648	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 FF FF FF FF				

Disassembly

No disassembly