ID: 640940
Sample Name: doc782.docx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 19:43:37
Date: 07/06/2022
Version: 35.0.0 Citrine

Table of Contents

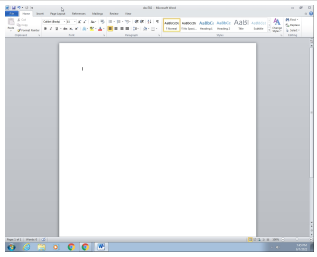
Windows Analysis Report

doc782.docx

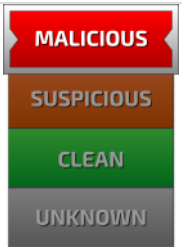
Overview

General Information

Sample Name:	doc782.docx
Analysis ID:	640940
MD5:	e7015438268464.
SHA1:	03ef0e06d678a0..
SHA256:	d20120cc046cef…
Infos:	



Detection



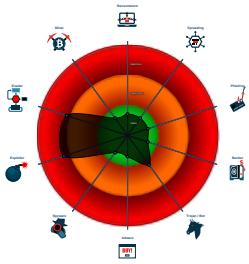
Follina CVE-2022-30190

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Microsoft Office Expl…
- Snort IDS alert for network traffic
- Contains an external reference to an…
- Yara signature match
- Potential document exploit detected…
- Uses a known web browser user age…
- Internet Provider seen in connection…
- Potential document exploit detected…
- Document misses a certain OLE str…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1168 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x2ca0:$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

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\123[1].RES	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x1447:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\123[1].RES	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FA120D60.RES	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x1447:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FA120D60.RES	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\CBBF3E02.RES	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	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

ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190) - Source IP: 185.234.247.119 - Destination IP: 192.168.2.22

Timestamp:	185.234.247.119192.168.2.2280491712036726 06/07/22-19:44:37.058628
SID:	2036726
Source Port:	80
Destination Port:	49171
Protocol:	TCP
Classtype:	Attempted User Privilege Gain

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Networking

Snort IDS alert for network traffic

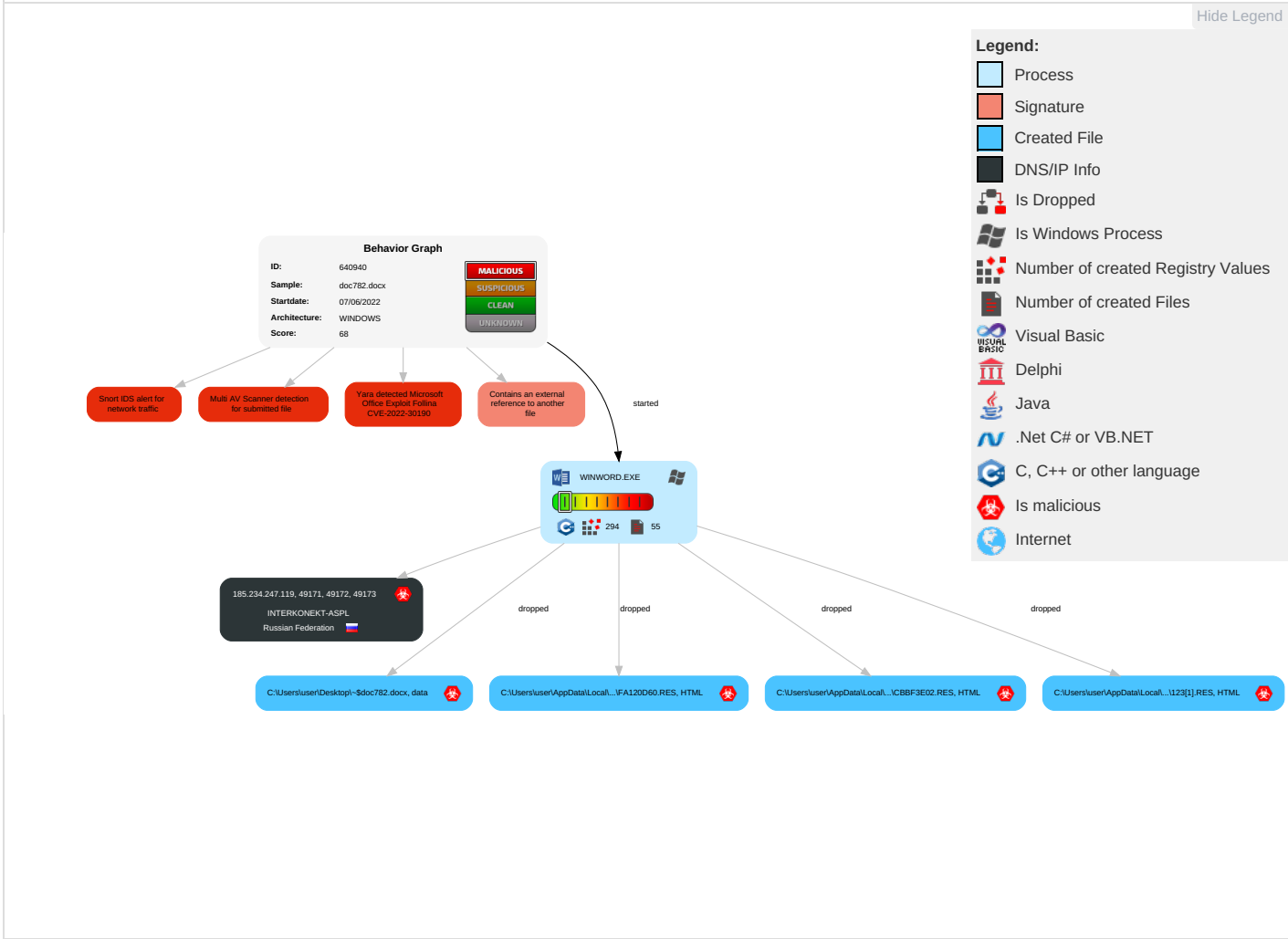
Persistence and Installation Behavior

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	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 Non-Application Layer Protocol	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 1 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	2 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

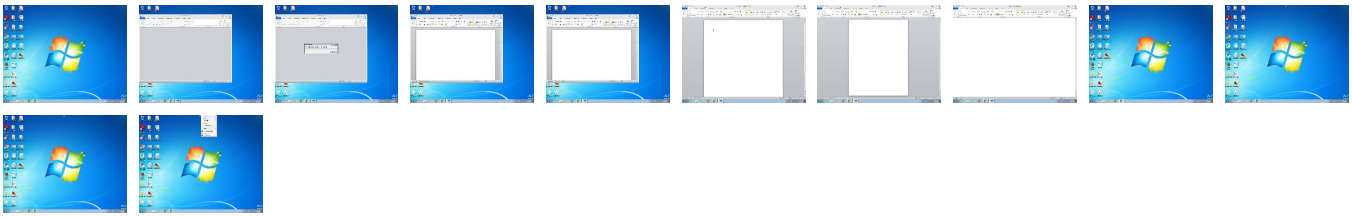
Behavior Graph

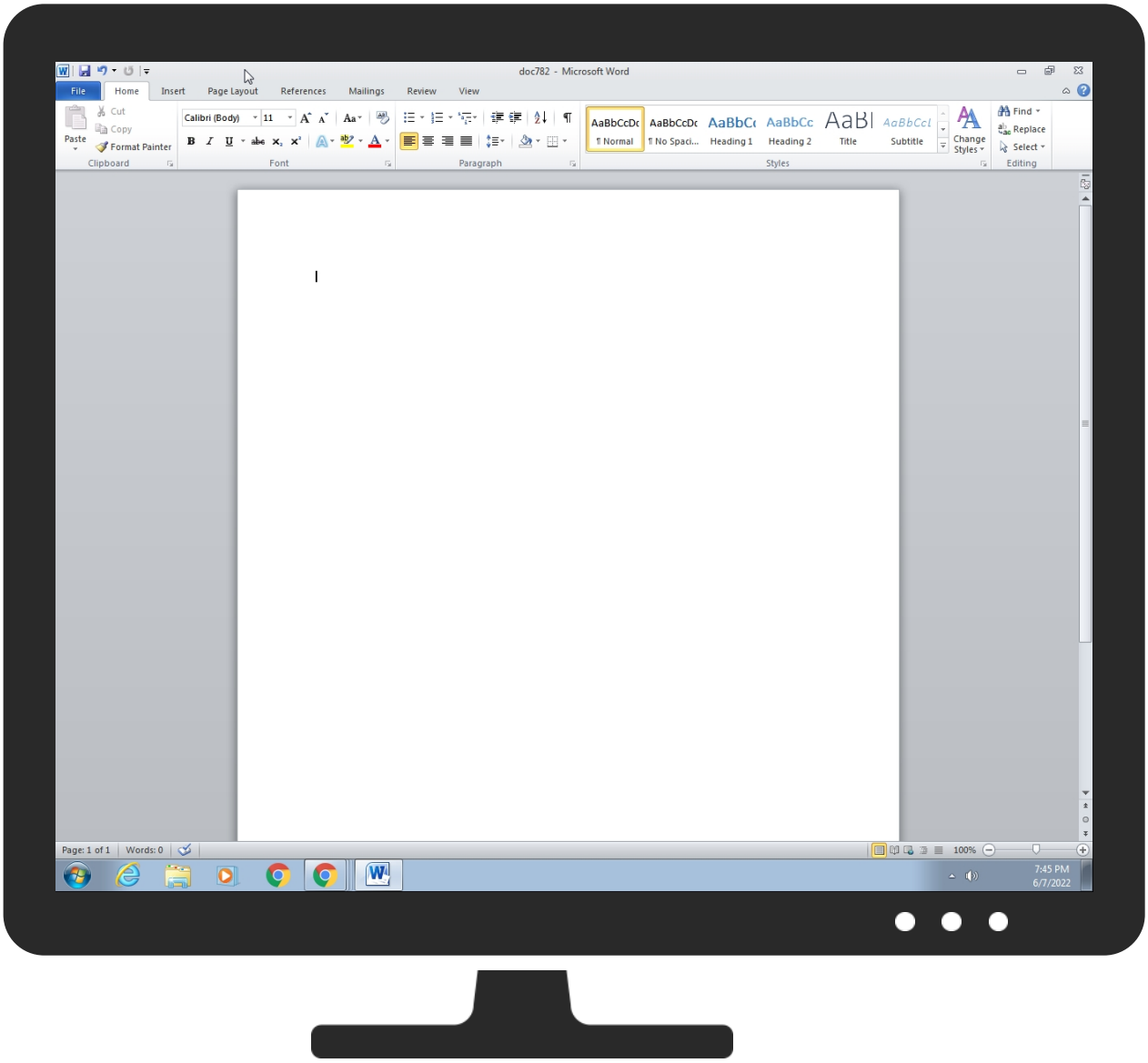


Screenshots

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
doc782.docx	27%	Virustotal		Browse
doc782.docx	17%	ReversingLabs	Document-Office.Exploit.CVE-2021-40444	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://185.234.247.119:80/123.RES	0%	Avira URL Cloud	safe	
http://185.234.247.119/123.RES	0%	Avira URL Cloud	safe	
http://185.2	0%	Avira URL Cloud	safe	
http://185.234.247.119/123.RESyX	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

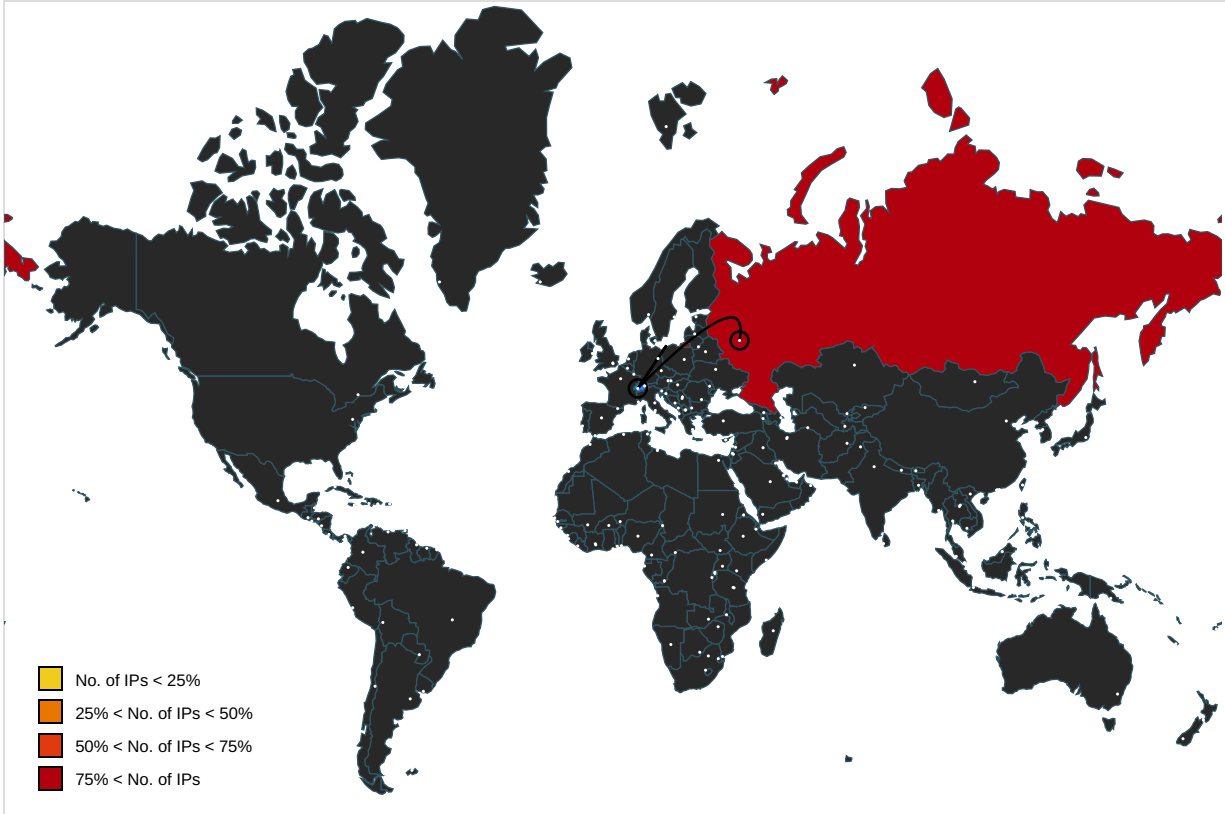
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.234.247.119/123.RES	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://185.234.247.119:80/123.RES	~WRF{AC1442A8-3209-457A-9C05-FC3521EE476C}.tmp.0.dr	false	• Avira URL Cloud: safe	unknown
http://185.2	~WRF{AC1442A8-3209-457A-9C05-FC3521EE476C}.tmp.0.dr	true	• Avira URL Cloud: safe	low
http://185.234.247.119/123.RESyX	~WRF{AC1442A8-3209-457A-9C05-FC3521EE476C}.tmp.0.dr	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs						
IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.234.247.119	unknown	Russian Federation		198004	INTERKONEKT-ASPL	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	640940
Start date and time: 07/06/202219:43:37	2022-06-07 19:43:37 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	doc782.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:	mal68.expl.evad.winDOCX@1/18@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
- Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.2872757882299728
Encrypted:	false
SSDEEP:	192:y1gV9sJSP4VfWbgIvNmujrzzZxpFcPX/QoZxpFcPX/QN:RRc16Xcf
MD5:	526A6E497879064B79111F0EB079DC69
SHA1:	A0C1A4BA670B7640F1373BE69695CBB8D29602EF
SHA-256:	BE1B8CE88A7FC126829F25E065A41BB623E975860C50196F9DEA860CA5683A48
SHA-512:	E7B903BAAA54CC700553DD777E855EEBC9D32C38A17FC9CDED800C74C63671EFEF1503DAD239CE059AD404FCEBE58FAD3FB5740B6A3078B21A553C1E1C02A2B0
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.Q..q.vG.Y.....S,...X.F...Fa.q...../kGO....p.?.....5.]?..L.....CX.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-{90C60528-C98F-4BCE-9AB0-F5E79340A27B}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.6736203037253643
Encrypted:	false
SSDEEP:	96:KTCyVFL4PGgYQIoGGXbMXGFIFiwLi9QtOwHtONXYhO4Y/:AbUPeQxGukLnhao
MD5:	121BD5A641D1017667991A6BED089C9D
SHA1:	C24150EEA5B9FAAF4EA85883F4A2010E848F1258
SHA-256:	8B2A4158CC6A2D08336F295074C4722095EFDE1513079CA76C7DCDDCD0CF40C6
SHA-512:	DF37BF55F2CA4ED734FC35B80BFF71D0D8910874E0D5A45A493310FF5A61A687418FFB87BD0EFE4139B30D9C70FB73B5C73D93E2F83673E1E30FE853763E05A4
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z...0...G._.....S,...X.F...Fa.q.....|....A.w[.....-.g.D.3.....S.....W.....x...x...x...x..*..... .....z V..... ..@....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):	3.9891611412909485
Encrypted:	false
SSDEEP:	3:yVlgsRlzLPlQ3IlFZYDn03cEVS5fIfRP+l1gYlRZ276:yPblzJQ3IlbYD03cxxlfwl1gYDZ22
MD5:	CCB1ED79CC6852066844CFAB96D39ED6
SHA1:	4D72D31AF6234AECC4EE48EFF6E3BEAE916EF0BD
SHA-256:	89EE3B6935806462AD3FD99A239D72CBCED744D8EF1506C3240FA0E916A8555B
SHA-512:	055E3D280BEBA5DD41D25A429DBA3D40FDA5AF560804FC7E5C397BA1D70291746D03D7176D96039151F5C995FF89FF7EA93024648F61AC15968F7F6E0ED31B6
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.9.0.C.6.0.5.2.8.-.C.9.8.F.-.4.B.C.E.-.9.A.B.0.-.F.5.E.7.9.3.4.0.A.2.7.B.}...F.S.D..

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.2885187828602524
Encrypted:	false
SSDEEP:	48:I3HCRBFG2NYJDWfDU/YCSY41oUi+ztEVXIeChj32glRrYOL0MNW9Rc5qpHWumB5w:KHCLFXO1amSBg8NyKINyK7H
MD5:	317DE8F3926F423F05DF5364DB71FEE7
SHA1:	DB169996DE45337D8A0C1A97B0EC5DAEA96D2A4C
SHA-256:	D6F1A882FCD48BF3D86FA004105B84A1BEC310411E6BAA7C444E63414F2308FA
SHA-512:	FCB7FA607792872C0848E5085E12F3C5690EC319EA3DBE1C5FDE6E19C67D0C7867DE70A57B68BDD0EEDD8B3579AF7C62166AEB68E88BC9B6BE374E532F3F9 27
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.o0.B..N.K....6NS,...X.F...Fa.q.....M)..N.. ...e.....qB..w..D.W.90....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-{4A9BEEDA-1620-41EC-85E7-8F2F9F4B21C8}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.22152754214705603
Encrypted:	false
SSDEEP:	24:I3Ca2rcLwnM0B34x6xPXFQfE+a3AmFHD0TXJFFmZ7fhmABvDzCARnZzqZzV6Egjt:I3Ca2AUrB1FJfT3Hja/C6SzsnIsnw
MD5:	9D421CB4E95C534AFA4DF087D46B16C6
SHA1:	A552DBB3209497D1246753410028BC8AA300BE05
SHA-256:	DD78DDB4B96B4CEAFDCB4FC5720419CAB5F873AC58E3CC4350F94C9B6B2E348E
SHA-512:	C3FF9888E2D64382B2FE5AB75DBD545B28B8CA0082ABF4FC0DC7480276544BBA3E21FF64625E9167FA844BA25024359205A87829A156D119C6D53D09F02F24FA
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z...v.JL..mc..'.S,...X.F...Fa.q.....(...`F.9.....kgt~.k.G.f.[.).fP>.....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):	3.9727198870722877
Encrypted:	false
SSDEEP:	3:yVlgsRlzCROa55VlJQwXuZ1jyjlRV8S27276:yPblzCR75B/E4ZIh22
MD5:	FF0683B5DA4293A1DE54EDCB8D4E8C1A
SHA1:	58322D98937093F90642D2220C7A4A1318A4629B
SHA-256:	30434BFC15C74DFA64C6C8DB56C4118A9D99D913B6578D04A1825DF5CF27B2DF
SHA-512:	2BD5A3A95B1F607F1065F74EB1FED9EBF3EA7B7C91388E15E090644E30D875E21AEF4ADE4F8122596AEE6CB9DAA490C7E1DB3C53E80BA92AD1100799AED988EA
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.4.A.9.B.E.E.D.A.-.1.6.2.0.-.4.1.E.C.-.8.5.E.7.-.8.F.2.F.9.F.4.B.2.1.C.8.}...F.S.D..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\123[1].RES

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):	6241
Entropy (8bit):	4.836014560592255
Encrypted:	false
SSDEEP:	192:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiSe+1hPw6utjdkGPgz47:wDwIwERY5V7VaGPgz47
MD5:	A32050027AEA96B3B70E1056490A98C9
SHA1:	EF28C67583C8C8048C0BAAEAD036680A60441213
SHA-256:	E3BA1C45F9DD1F432138654B5F19CF89C55E07219B88AA7628334D38BB036433
SHA-512:	1C2A1605B67FEB57F99DC4C7DAFFB16D1F3CC48D12CFC338C6D4FD84348DD6A872F6A0DAEDA70E96F49AD05B0F9690211F67346E3E4660CA2E79ED6F038A60C
Malicious:	**true**
Yara Hits:	• Rule: MAL_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\123[1].RES, 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\123[1].RES, Author: Joe Security
Reputation:	low
IE Cache URL:	http://185.234.247.119/123.RES
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\CBBF3E02.RES

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):	6241
Entropy (8bit):	4.836014560592255
Encrypted:	false
SSDEEP:	192:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiSe+1hPw6utjdkGPgz47:wDwIwERY5V7VaGPgz47
MD5:	A32050027AEA96B3B70E1056490A98C9
SHA1:	EF28C67583C8C8048C0BAAEAD036680A60441213
SHA-256:	E3BA1C45F9DD1F432138654B5F19CF89C55E07219B88AA7628334D38BB036433
SHA-512:	1C2A1605B67FEB57F99DC4C7DAFFB16D1F3CC48D12CFC338C6D4FD84348DD6A872F6A0DAEDA70E96F49AD05B0F9690211F67346E3E4660CA2E79ED6F038A60C
Malicious:	**true**
Yara Hits:	• Rule: MAL_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CBBF3E02.RES, 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\CBBF3E02.RES, 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\FA120D60.RES

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):	6241
Entropy (8bit):	4.836014560592255
Encrypted:	false
SSDEEP:	192:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiSe+1hPw6utjdkGPgz47:wDwIwERY5V7VaGPgz47
MD5:	A32050027AEA96B3B70E1056490A98C9
SHA1:	EF28C67583C8C8048C0BAAEAD036680A60441213
SHA-256:	E3BA1C45F9DD1F432138654B5F19CF89C55E07219B88AA7628334D38BB036433
SHA-512:	1C2A1605B67FEB57F99DC4C7DAFFB16D1F3CC48D12CFC338C6D4FD84348DD6A872F6A0DAEDA70E96F49AD05B0F9690211F67346E3E4660CA2E79ED6F038A60C
Malicious:	**true**
Yara Hits:	• Rule: MAL_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FA120D60.RES, 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\FA120D60.RES, Author: Joe Security
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.Word\~WRF{AC1442A8-3209-457A-9C05-FC3521EE476C}.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):	5632
Entropy (8bit):	2.2195179903071636
Encrypted:	false
SSDEEP:	12:rl3bn+kF/W/mYYaiT21U/hC9KSvuQWyRnNYnRn/5Co00RnNEKn7iv9KS4CI9KS4y:rdW/NK/5QV8nNoWisg6BAKoG8noxoWi
MD5:	3AB3539B70A9B80798F3669AC3483546
SHA1:	346E40AF0E4E582BD90E166E57A8B3A170AC4565
SHA-256:	5DBE81D54C8C3CF70075824A503914BC1C8240574AA22AB7C7B7BC63E1DDD654
SHA-512:	A407CB94888C76D85D50239C97A6CE89BBDB5EEC8FDB5792EEF8FFE56B6110BFF2E86AECC0B7B2C765AFC91BA3A30B3426659E705919BE960A4D37A5118FE40C
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{2921E275-B8BF-45B2-888A-BDBD2D0A4929}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false

Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{77318D9D-F0AF-4DD2-B489-88A56CEFB392}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	2130
Entropy (8bit):	1.1627960907898713
Encrypted:	false
SSDEEP:	6:/9IqgHu42sarhYkIuvgB4PxZUtr1il5lN24NLRnyOLfEznRnyOLflqDmPm1PcV5:mbb2sOhYk5vnZA5Rn/YnRn/dom5
MD5:	645EA66E0489C4D8B0D4877F7A930E07
SHA1:	2961C4A1FDD07A4A6EFA47655C6087EB011B079E
SHA-256:	ED0BFA2837448DD790D7C0450339FBAEF480535517847634136BF9F7F0B91468
SHA-512:	0D1E3C8280255B0F329931CE8CE1810DFE32F5DA29A2FD9FE90B907A2546699B955D50519CE310BD63B5D84F5873F5FB3CCB0467FB48E47ABEA16962DC6BAACE
Malicious:	false
Preview:	....S.H.A.P.E. .X. .\.*. .M.E.R.G.E.F.O.R.M.A.T... . ...0...2...6...D...F...D...F...J...N...P..... .....j....U....j....U...*....j....U

C:\Users\user\AppData\Local\Temp\{99E1AFB0-685D-4B38-97F2-71EBFEEE2F14}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025623734588153504
Encrypted:	false
SSDEEP:	6:I3DPc1V27HvxggLRvhGEAflWSks3RXv//4tfnRujlw//+GtluJ/eRuj:I3DPwuDhGEAfASk6vYg3J/
MD5:	B0EA46CCC2FA72CDEA1E8A970318C8C5
SHA1:	E8BB6DFCD4C726B015778B573CE00F8A98D190F7
SHA-256:	85EA4C6C1662274426EAFFE8C190A6F109D86DDF4021D8E4A9E3198F36A551A4
SHA-512:	62C38D380B430EDE994AA1561EE4CC07FD30D99D272A91D8F15B015CDA636C46605A83244CCDE01E87A132F325C7F9EB385AE7B2A9E981A845D8EB1F0B9449D8
Malicious:	false
Preview:	......M.eFy...z.o0.B..N.K....6NS,...X.F...Fa.q.....1...X.E..^...V.....qB..w..D.W.90.....x...x...x...x..... ....zV..... ..@..... .....

C:\Users\user\AppData\Local\Temp\{BC1313D8-3C5B-4901-A926-7D9B949D287F}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.0256237345881535
Encrypted:	false
SSDEEP:	6:I3DPcbYRvxggLRPqv5ibXbGRXv//4tfnRujlw//+GtluJ/eRuj:I3DPGYdjy5vYg3J/
MD5:	10E67C048099C90E1C0666278470E38A
SHA1:	D5A7F4B209F9732FB77E86F8A668E1512D66C2DB
SHA-256:	D8392841A423C66EA19FB60EA4E550FD547DE47B6A66521A05CB3FCFC5E83492
SHA-512:	BB2C07BF757A5CD6A874F60DD91605CC4C83918A43623466F649DD63BAE75340B2B203EFEBA155C96EEB0E22F4623A82E0D7C3382522046EC7F63302BCC8CA1
Malicious:	false
Preview:	......M.eFy...z.Q..q.vG.Y.....S,...X.F...Fa.q.....d.s.O.....Q.....5.]?..L.....CX.....x...x...x...x..... ....zV..... ..@..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\doc782.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 15:45:52 2022, mtime=Tue Mar 8 15:45:52 2022, atime=Wed Jun 8 01:45:12 2022, length=10144, window=hide
Category:	dropped
Size (bytes):	999
Entropy (8bit):	4.520744870739846
Encrypted:	false
SSDEEP:	12:8nlrgXg/XAlCPCHaXWBlXB/eLX+WqPW/xgitCicvbz6F42NDtZ3YilMMEpxRljK1:8f/XTm3MgPW/xftJekxDv3qa+Y7h
MD5:	04594E11A8EF65860D389E40AB032796
SHA1:	AA6792F586717AD57B20FD67B505E50D5AE0E5A3
SHA-256:	1BC5F3C148CE6BAFA95337883CC3B042968CD04F3BF61453FC99D46199056D8B
SHA-512:	049D931F8E51E9573F8B459018770975916EE6A87B1E9606BC89247CD8875C3FA9D77557D196DA4FE827AC8F3171DD6A37007FB2BABEB910FA872C01A4CDF0BA
Malicious:	false
Preview:	L.....F.... .....3.....3...LR..z...'.....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.....`.2..'...T.. .DOC782~1.DOC..D.....hT..hT..*...r....'.....d.o.c.7.8.2...d.o.c.x.....u.....-...8...[.....?J.....C:\Users\..#.....\\760639\Users.user\Desktop\doc782.docx."....\....\....\....\....\.D.e.s.k.t.o.p.\.d.o.c.7.8.2...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.....760639.....D_....3N...W...9...N..... .....[D_....3N...W...9...N..... .....[....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	64
Entropy (8bit):	4.601202445739505
Encrypted:	false
SSDEEP:	3:bDuMJlZIbFXCmxWKIbFXCv:bCSa6c
MD5:	538F5016C24249AC1799BBBB20B4BD97
SHA1:	1B0ECD98E7D3BFECA78B00528138FA8D84F35BED
SHA-256:	249CC3AF3819FB4142D7A65254BD454ACF580489E19A50D71007A7E998B4A70F
SHA-512:	E0E8040389BABFFD046E57AAD3ECFEE9A9171B4D00EC75EE3DF48710FC452C479692121776D17DCBCCC72E4A1CA0B6570484C007B282C9DBF05EDD34C9463EDA
Malicious:	false
Preview:	[folders]..Templates.LNK=0..doc782.LNK=0..[misc]..doc782.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\~$doc782.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:	**true**
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):	7.869060797789825
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:	doc782.docx
File size:	10144
MD5:	e7015438268464cedad98b1544d643ad
SHA1:	03ef0e06d678a07f0413d95f0deb8968190e4f6b
SHA256:	d20120cc046cef3c3f0292c6cbc406fcf2a714aa8e048c9188f1184e4bb16c93
SHA512:	d134d87c28acb758b897a287a9f6ce86776f384f43ee963f52b40e173b6bfcd9dc76e5f64b9a40b93d3bf2a5b988f842c27c90611a8b4408abd9e197191e4aad
SSDEEP:	192:s5VReDWRPj8Iugw1Blb8VPkf+CFk4v1Y2VveFLC9FJ9Q7dlpN2:snPj8I10lD9+2Vvx9qlpN2
TLSH:	A3228E3ADA5508B5CAD2A275E0AC0B2AD30C42BBB73BE9CB65C653E402C85DB0F5530C
File Content Preview:	PK.....k.T...L....'.....[Content_Types].xml...n.0.E....m.NR....,.X...~...`.I.....C .....I....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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
185.234.247.119192.168.2.2280491712036726 06/07/22-19:44:37.058628	TCP	2036726	ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190)	80	49171	185.234.247.119	192.168.2.22

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 7, 2022 19:44:27.159992933 CEST	49171	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:27.187441111 CEST	80	49171	185.234.247.119	192.168.2.22
Jun 7, 2022 19:44:27.187530041 CEST	49171	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:27.187803030 CEST	49171	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:27.215111017 CEST	80	49171	185.234.247.119	192.168.2.22
Jun 7, 2022 19:44:27.215137959 CEST	80	49171	185.234.247.119	192.168.2.22
Jun 7, 2022 19:44:27.215202093 CEST	49171	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:32.657025099 CEST	49172	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:32.684343100 CEST	80	49172	185.234.247.119	192.168.2.22
Jun 7, 2022 19:44:32.684530973 CEST	49172	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:32.684813023 CEST	49172	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:32.716893911 CEST	80	49172	185.234.247.119	192.168.2.22
Jun 7, 2022 19:44:32.718305111 CEST	80	49172	185.234.247.119	192.168.2.22
Jun 7, 2022 19:44:32.926908970 CEST	49172	80	192.168.2.22	185.234.247.119

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 7, 2022 19:44:36.916021109 CEST	49173	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:36.943603992 CEST	80	49173	185.234.247.119	192.168.2.22
Jun 7, 2022 19:44:36.943826914 CEST	49173	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:36.961354017 CEST	49173	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:36.991600990 CEST	80	49173	185.234.247.119	192.168.2.22
Jun 7, 2022 19:44:36.991637945 CEST	80	49173	185.234.247.119	192.168.2.22
Jun 7, 2022 19:44:37.030510902 CEST	49171	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:37.058628082 CEST	80	49171	185.234.247.119	192.168.2.22
Jun 7, 2022 19:44:37.058744907 CEST	80	49171	185.234.247.119	192.168.2.22
Jun 7, 2022 19:44:37.058758974 CEST	49171	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:37.058788061 CEST	49171	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:37.058864117 CEST	80	49171	185.234.247.119	192.168.2.22
Jun 7, 2022 19:44:37.058901072 CEST	49171	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:37.058957100 CEST	80	49171	185.234.247.119	192.168.2.22
Jun 7, 2022 19:44:37.058991909 CEST	49171	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:37.059087992 CEST	80	49171	185.234.247.119	192.168.2.22
Jun 7, 2022 19:44:37.059122086 CEST	49171	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:37.201658010 CEST	49173	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:37.435573101 CEST	49171	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:37.463280916 CEST	80	49171	185.234.247.119	192.168.2.22
Jun 7, 2022 19:44:37.463632107 CEST	49171	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:37.473567963 CEST	49171	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:37.501120090 CEST	80	49171	185.234.247.119	192.168.2.22
Jun 7, 2022 19:44:37.501225948 CEST	49171	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:37.536554098 CEST	49172	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:37.564064980 CEST	80	49172	185.234.247.119	192.168.2.22
Jun 7, 2022 19:44:37.579617977 CEST	49171	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:37.607300997 CEST	80	49171	185.234.247.119	192.168.2.22
Jun 7, 2022 19:44:37.607443094 CEST	49171	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:37.778932095 CEST	49172	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:37.834969997 CEST	49171	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:44:37.863265038 CEST	80	49171	185.234.247.119	192.168.2.22
Jun 7, 2022 19:44:37.863425970 CEST	49171	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:45:37.891575098 CEST	49172	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:45:40.323673010 CEST	49171	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:45:41.990484953 CEST	80	49173	185.234.247.119	192.168.2.22
Jun 7, 2022 19:45:41.990658045 CEST	49173	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:45:41.990782976 CEST	49173	80	192.168.2.22	185.234.247.119
Jun 7, 2022 19:45:42.018299103 CEST	80	49173	185.234.247.119	192.168.2.22

HTTP Request Dependency Graph

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	185.234.247.119	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 19:44:27.187803030 CEST	1	OUT	OPTIONS / HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: 185.234.247.119 Content-Length: 0 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 19:44:27.215137959 CEST	2	IN	HTTP/1.1 405 Not Allowed Server: nginx Date: Tue, 07 Jun 2022 17:44:27 GMT Content-Type: text/html Content-Length: 150 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> nginx </body></html>
Jun 7, 2022 19:44:37.030510902 CEST	4	OUT	GET /123.RES 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: 185.234.247.119 Connection: Keep-Alive
Jun 7, 2022 19:44:37.058628082 CEST	5	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:44:37 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 0d 0a 47 6f 6f 64 20 74 68 69 6e 67 20 77 65 20 64 69 73 61 62 6c 65 64 20 6d 61 63 72 6f 73 0d 0a 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 70 3e 0d 0a 4c 6f 72 65 6d 20 69 70 73 75 6d 20 64 6f 6c 6f 72 20 73 69 74 20 61 6d 65 74 2c 20 63 6f 6e 73 65 63 74 65 74 75 72 20 61 64 69 70 69 73 63 69 6e 67 20 65 6c 69 74 2e 20 51 75 69 73 71 75 65 20 70 65 6c 6c 65 6e 74 65 73 71 75 65 20 65 67 65 73 74 61 73 20 6e 75 6c 6c 61 20 69 6e 20 64 69 67 6e 69 73 73 69 6d 2e 20 4e 61 6d 20 69 64 20 6d 61 75 72 69 73 20 6c 6f 72 65 6d 2e 20 4e 75 6e 63 20 73 75 73 63 69 70 69 74 20 69 64 20 6d 61 67 6e 61 20 69 64 20 6d 6f 6c 69 73 2e 20 50 65 6c 6c 65 6e 74 65 73 71 75 65 20 73 75 73 63 69 70 69 74 20 6f 72 63 69 20 6e 65 71 75 65 2c 20 61 74 20 6f 72 6e 61 72 65 20 73 61 70 69 65 6e 20 62 69 62 65 6e 64 75 6d 20 65 75 2e 20 56 65 73 74 69 62 75 6c 75 6d 20 6d 61 6c 65 73 75 61 64 61 20 6e 65 63 20 73 65 6d 20 71 75 69 73 20 66 69 6e 69 62 75 73 2e 20 4e 61 6d 20 71 75 69 73 20 6c 69 67 75 6c 61 20 65 74 20 64 75 69 20 66 61 75 63 69 62 75 73 20 66 61 75 63 69 62 75 73 2e 20 49 6e 20 71 75 69 73 20 62 69 62 65 6e 64 75 6d 20 74 6f 72 74 6f 72 2e 0d 0a 0d 0a 43 75 72 61 62 69 74 75 72 20 72 75 74 72 75 6d 20 6c 65 6f 20 74 6f 72 74 6f 72 2c 20 76 65 6e 65 6e 61 74 69 73 20 66 65 72 6d 65 6e 74 75 6d 20 65 78 20 70 6f 72 74 74 69 74 6f 72 20 76 69 74 61 65 2e 20 50 72 6f 69 6e 20 65 75 20 69 6d 70 65 72 64 69 65 74 20 6c 6f 72 65 6d 2c 20 61 63 20 61 6c 69 71 75 65 74 20 72 69 73 75 73 2e 20 41 65 6e 65 61 6e 20 65 75 20 73 61 70 69 65 6e 20 70 68 61 72 65 74 72 61 2c 20 69 6d 70 65 72 64 69 65 74 20 69 70 73 75 6d 20 75 74 2c 20 73 65 6d 70 65 72 20 64 69 61 6d 2e 20 4e 75 6c 6c 61 20 66 61 63 69 6c 69 73 69 2e 20 53 65 64 20 65 75 69 73 6d 6f 64 20 74 6f 72 74 6f 72 20 74 6f 72 74 6f 72 2c 20 6e 6f 6e 20 65 6c 65 69 66 65 6e 64 20 6e 75 6e 63 20 66 65 72 6d 65 6e 74 75 6d 20 73 69 74 20 61 6d 65 74 2e 20 49 6e 74 65 67 65 72 20 6c 69 67 75 6c 61 20 6c 69 67 75 6c 61 2c 20 63 6f 6e 67 75 65 20 61 74 20 73 63 65 6c 65 72 69 73 71 75 65 20 73 69 74 20 61 6d 65 74 2c 20 70 6f 72 74 74 69 74 6f 72 20 71 75 69 73 20 66 65 6c 69 73 2e 20 4d 61 65 63 65 6e 61 73 20 6e 65 63 20 6a 75 73 74 6f 20 76 61 72 69 75 73 2c 20 73 65 6d 70 65 72 20 74 75 72 70 69 73 20 75 74 2c 20 67 72 61 76 69 64 61 20 6c 6f 72 65 6d 2e 20 50 72 6f 69 6e 20 61 72 63 75 20 6c 69 67 75 6c 61 2c 20 76 65 6e 65 6e 61 74 69 73 20 61 6c 69 71 75 61 6d 20 74 72 69 73 74 69 71 75 65 20 75 74 2c 20 70 72 65 74 69 75 6d 20 76 65 6c 69 74 2e 0d 0a 0d 0a 50 68 61 73 65 6c 6c 75 73 20 74 72 69 73 74 69 71 75 65 20 6f 72 63 69 20 65 6e 69 6d 2c 20 61 74 20 61 63 63 75 6d 73 61 6e 20 76 65 6c 69 74 20 69 6e 74 65 72 64 75 6d 20 65 74 2e 20 41 65 6e 65 61 6e 20 6e 65 63 20 74 72 69 73 74 69 71 75 65 20 61 6e 74 65 2c 20 64 69 67 6e 69 73 73 69 6d 20 63 6f 6e 76 61 6c 6c 69 73 20 6c 69 67 75 6c 61 2e 20 41 65 6e 65 61 6e 20 71 75 69 73 20 66 65 6c 69 73 20 64 6f 6c 6f 72 2e 20 49 6e 20 71 75 69 73 20 6c 65 63 74 75 73 20 6d 61 73 73 61 2e 20 50 65 6c 6c 65 6e 74 65 Data Ascii: <!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 l orem. 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 ante, dignissim convallis ligula. Aenean quis felis dolor. In quis lectus massa. Pellente
Jun 7, 2022 19:44:37.435573101 CEST	11	OUT	HEAD /123.RES HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: 185.234.247.119 Content-Length: 0 Connection: Keep-Alive
Jun 7, 2022 19:44:37.463280916 CEST	12	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:44:37 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes
Jun 7, 2022 19:44:37.473567963 CEST	12	OUT	OPTIONS / HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: 185.234.247.119 Content-Length: 0 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 19:44:37.501120090 CEST	12	IN	HTTP/1.1 405 Not Allowed Server: nginx Date: Tue, 07 Jun 2022 17:44:37 GMT Content-Type: text/html Content-Length: 150 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> nginx </body></html>
Jun 7, 2022 19:44:37.579617977 CEST	13	OUT	GET /123.RES 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: 185.234.247.119 If-Modified-Since: Fri, 03 Jun 2022 10:07:25 GMT If-None-Match: "6299dd5d-1861" Connection: Keep-Alive
Jun 7, 2022 19:44:37.607300997 CEST	13	IN	HTTP/1.1 304 Not Modified Server: nginx Date: Tue, 07 Jun 2022 17:44:37 GMT Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861"
Jun 7, 2022 19:44:37.834969997 CEST	14	OUT	HEAD /123.RES HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: 185.234.247.119 Content-Length: 0 Connection: Keep-Alive
Jun 7, 2022 19:44:37.863265038 CEST	14	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:44:37 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49172	185.234.247.119	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 19:44:32.684813023 CEST	3	OUT	HEAD /123.RES HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: 185.234.247.119
Jun 7, 2022 19:44:32.718305111 CEST	3	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:44:32 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes
Jun 7, 2022 19:44:37.536554098 CEST	12	OUT	HEAD /123.RES HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: 185.234.247.119
Jun 7, 2022 19:44:37.564064980 CEST	13	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:44:37 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49173	185.234.247.119	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 19:44:36.961354017 CEST	3	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: 185.234.247.119
Jun 7, 2022 19:44:36.991637945 CEST	4	IN	HTTP/1.1 405 Not Allowed Server: nginx Date: Tue, 07 Jun 2022 17:44:36 GMT Content-Type: text/html Content-Length: 150 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> nginx </body></html>

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 1168, Parent PID: 576

General

Target ID:	0
Start time:	19:45:12
Start date:	07/06/2022
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:	0x13f540000
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	6E262B14	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$doc782.docx	success or wait	1	6E2E0648	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	6E2BA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E2BA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E2BA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E2E0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6E2E0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6E2E0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\6FB5F	success or wait	1	6E2E0648	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\6FB5F	6FB5F	binary	04 00 00 00 90 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 9F 01 C3 DF E1 7A D8 01 5F FB 06 00 5F FB 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6E2E0648	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 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	1422327858	1422327859	success or wait	1	6E2E0648	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D3000000010000000F01FEC\Usage	ProductFiles	dword	1422327859	1422327860	success or wait	1	6E2E0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\6FB5F	6FB5F	binary	04 00 00 00 90 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	04 00 00 00 90 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	success or wait	1	6E2E0648	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			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 9F 01 C3 DF E1 7A D8 01 5F FB 06 00 5F FB 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 FF FF FF FF 00 00 00 00	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 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FB 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 FF FF FF FF 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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				

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 FF FF FF FF				

Disassembly

⊘ **No disassembly**