Obfuscated Files or Information: Command Obfuscation, Sub-technique T1027.010 - Enterprise

Archived: 2026-04-05 12:39:11 UTC

G0073 APT19

APT19 used Base64 to obfuscate executed commands.[10]

G0050 APT32

APT32 has used the `Invoke-Obfuscation` framework to obfuscate their PowerShell.[11][12][13]

G0143 Aquatic Panda

Aquatic Panda has encoded PowerShell commands in Base64.[14]

S0373 Astaroth

Astaroth has obfuscated and randomized parts of the JScript code it is initiating.[15]

S0475 BackConfig

BackConfig has used compressed and decimal encoded VBS scripts.[16]

S1081 BADHATCH

BADHATCH malicious PowerShell commands can be encoded with base64.[17]

C0018 C0018

During C0018, the threat actors used Base64 to encode their PowerShell scripts.[18][19]

C0021 C0021

During C0021, the threat actors used encoded PowerShell commands.[20][21]

S0462 CARROTBAT

CARROTBAT has the ability to execute obfuscated commands on the infected host.[22]

G0114 Chimera

Chimera has encoded PowerShell commands.[23]

G0080 Cobalt Group

Cobalt Group obfuscated several scriptlets and code used on the victim's machine, including through use of XOR and RC4.[24][25]

S0126 ComRAT

ComRAT has used encryption and base64 to obfuscate its orchestrator code in the Registry. ComRAT has also used encoded PowerShell scripts.[26][27]

G1052 Contagious Interview

Contagious Interview has obfuscated JavaScript code using Base64 and variable substitutions.[28][29][30][31]

S0492 CookieMiner

CookieMiner has used base64 encoding to obfuscate scripts on the system.[32]

S0673 DarkWatchman

DarkWatchman has used Base64 to encode PowerShell commands.[33]

S0354 Denis

Denis has encoded its PowerShell commands in Base64.[13]

S0367 Emotet

Emotet has obfuscated macros within malicious documents to hide the URLs hosting the malware, CMD.exe arguments, and PowerShell scripts. [34][35][36][37]

S0363 Empire

Empire has the ability to obfuscate commands using `Invoke-Obfuscation`.[38]

G0037 FIN6

FIN6 has used encoded PowerShell commands.[39]

G0046 FIN7

FIN7 has used fragmented strings, environment variables, standard input (stdin), and native character-replacement functionalities to obfuscate commands.[6][40][41]

G0061 FIN8

FIN8 has used environment variables and standard input (stdin) to obfuscate command-line arguments. FIN8 also obfuscates malicious macros delivered as payloads.[6][42][43]

G0117 Fox Kitten

Fox Kitten has base64 encoded scripts to avoid detection.[44]

C0001 Frankenstein

During Frankenstein, the threat actors ran encoded commands from the command line.[45]

S0277 FruitFly

FruitFly executes and stores obfuscated Perl scripts.[46]

G0047 Gamaredon Group

Gamaredon Group has used obfuscated or encrypted scripts.[47][48][49][50]

G0115 GOLD SOUTHFIELD

GOLD SOUTHFIELD has executed base64 encoded PowerShell scripts on compromised hosts.[51]

G1001 HEXANE

HEXANE has used Base64-encoded scripts.[52]

S1022 IceApple

IceApple can use Base64 and "junk" JavaScript code to obfuscate information.[53]

G0094 Kimsuky

Kimsuky has encoded malicious PowerShell scripts using Base64.[54]

S0669 KOCTOPUS

KOCTOPUS has obfuscated scripts with the BatchEncryption tool.[55]

G0140 LazyScripter

LazyScripter has leveraged the BatchEncryption tool to perform advanced batch script obfuscation and encoding techniques.[55]

G0077 Leafminer

Leafminer obfuscated scripts that were used on victim machines.[56]

S0451 LoudMiner

LoudMiner has obfuscated various scripts.[57]

S0409 Machete

Machete has used pyobfuscate, zlib compression, and base64 encoding for obfuscation. Machete has also used some visual obfuscation techniques by naming variables as combinations of letters to hinder analysis.[58][59]

G0059 Magic Hound

Magic Hound has used base64-encoded commands.[60][61]

G1051 Medusa Group

Medusa Group has obfuscated PowerShell scripts with Base64 encoding.[62] Medusa Group has also obfuscated the code of dropped kernel drivers using a software known as Safengine Shielden which randomized the code through code mutations and then leveraged an embedded virtual machine interpreter to execute the code.[63]

G0069 MuddyWater

MuddyWater has used Daniel Bohannon’s Invoke-Obfuscation framework and obfuscated PowerShell scripts.[64] [12] The group has also used other obfuscation methods, including Base64 obfuscation of VBScripts and PowerShell commands.[64][65][66][67][68][69][70]

S0457 Netwalker

Netwalker's PowerShell script has been obfuscated with multiple layers including base64 and hexadecimal encoding and XOR-encryption, as well as obfuscated PowerShell functions and variables.[71][72]

C0012 Operation CuckooBees

During Operation CuckooBees, the threat actors executed an encoded VBScript file.[73]

C0014 Operation Wocao

During Operation Wocao, threat actors executed PowerShell commands which were encoded or compressed using Base64, zlib, and XOR.[74]

G0040 Patchwork

Patchwork has obfuscated a script with Crypto Obfuscator.[75]

G1040 Play

Play has used Base64-encoded PowerShell scripts for post exploit activities on compromised hosts.[76]

S0428 PoetRAT

PoetRAT has `pyminifier` to obfuscate scripts.[77]

S0685 PowerPunch

PowerPunch can use Base64-encoded scripts.[48]

S0194 PowerSploit

PowerSploit contains a collection of ScriptModification modules that compress and encode scripts and payloads. [78][79]

S0223 POWERSTATS

POWERSTATS uses character replacement, PowerShell environment variables, and XOR encoding to obfuscate code. POWERSTATS's backdoor code is a multi-layer obfuscated, encoded, and compressed blob. [65][80] POWERSTATS has used PowerShell code with custom string obfuscation [81]

S0650 QakBot

QakBot can use obfuscated and encoded scripts.[82][83]

S0269 QUADAGENT

QUADAGENT was likely obfuscated using `Invoke-Obfuscation`.[84][12]

S1240 RedLine Stealer

RedLine Stealer has obfuscated scripts within text files used in execution.[85]

S0270 RogueRobin

The PowerShell script with the RogueRobin payload was obfuscated using the COMPRESS technique in `Invoke-Obfuscation`.[86][12]

G0034 Sandworm Team

Sandworm Team has used ROT13 encoding, AES encryption and compression with the zlib library for their Python-based backdoor.[87]

S1085 Sardonic

Sardonic PowerShell scripts can be encrypted with RC4 and compressed using Gzip.[88]

C0058 SharePoint ToolShell Exploitation

During SharePoint ToolShell Exploitation, threat actors executed Base64-encoded PowerShell commands.[89][90][91][92][93]

S0450 SHARPSTATS

SHARPSTATS has used base64 encoding and XOR to obfuscate PowerShell scripts.[81]

S0589 Sibot

Sibot has obfuscated scripts used in execution.[94]

G0121 Sidewinder

Sidewinder has used base64 encoding for scripts.[95][96]

G0091 Silence

Silence has used environment variable string substitution for obfuscation.[97]

S0390 SQLRat

SQLRat has used a character insertion obfuscation technique, making the script appear to contain Chinese characters.[98]

G0092 TA505

TA505 has used base64 encoded PowerShell commands.[99][100]

G0127 TA551

TA551 has used obfuscated variable names in a JavaScript configuration file.[101]

G0010 Turla

Turla has used encryption (including salted 3DES via PowerSploit's `Out-EncryptedScript.ps1`), random variable names, and base64 encoding to obfuscate PowerShell commands and payloads.[102]

S0386 Ursnif

Ursnif droppers execute base64 encoded PowerShell commands.[103]

G0102 Wizard Spider

Wizard Spider used Base64 encoding to obfuscate an Empire service and PowerShell commands.[104][105]

S1248 XORIndex Loader

XORIndex Loader has obfuscated strings using ASCII buffers and TextDecoder.[106]

S0330 Zeus Panda

Zeus Panda obfuscates the macro commands in its initial payload.[107]
