

# Analyzing Cobalt Strike PowerShell Payload

By AK1001

Published: 2024-09-25 · Archived: 2026-04-05 20:13:14 UTC



Since last year, cobalt strike payloads are everywhere. We saw hackers used Cobalt Strike in many attacks. Some serious cyber incident like SolarWinds supply chain attack [1]. In Proofpoint's new article, said that Cobalt Strike is the favorite tool from APT to crimeware [2]. Cobalt Strike is a penetration tool which developed by Strategic Cyber. It's a good framework for collaboration by Red team.

In these days, the executable and dll type of cobalt strike payload are most often used in attack. Other's payload type like macro or powershell sometimes were also be delivered by attackers. In this article, let's analysis the cobalt strike powershell payload.

## Sample

```
MD5: e0315aca119a9b3b7d89184ad2fa2603  
SHA-1: bfc928da46d2ae32e2c60373a5d968d2f15e497a  
SHA-256: 24b18a60020d05b32b13d2cf1e6d6b1ccda4f0af5fb5ec0da960746fde54b796
```

Press enter or click to view image in full size

28 / 58  
Community Score

24b18a60020d05b32b13d2cffe6d6b1ccda4f0af5fb5ec0da960746fde54b796  
ns.css  
274.43 KB Size  
2021-04-15 18:12:26 UTC  
2 months ago

checks-network-adapters detect-debug-environment direct-cpu-clock-access powershell runtime-modules

28 security vendors flagged this file as malicious

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	Generic.PwShell.Rozena.3.854753BA	ALYac	Generic.PwShell.Rozena.3.854753BA	
Arcabit	Generic.PwShell.Rozena.3.854753BA	Avast	PwrSh: Dropper-F [Trj]	
AVG	PwrSh: Dropper-F [Trj]	BitDefender	Generic.PwShell.Rozena.3.854753BA	
ClamAV	Win.Trojan.CobaltStrike-7917400-0	DrWeb	PowerShell.Inject.18	
Emsisoft	Generic.PwShell.Rozena.3.854753BA ...	eScan	Generic.PwShell.Rozena.3.854753BA	
ESET-NOD32	Win32/Rozena.ACE	FireEye	Generic.PwShell.Rozena.3.854753BA	
Fortinet	JS/Rozena.D/tr	GData	Generic.PwShell.Rozena.3.854753BA	
Ikarus	Trojan-Dropper.PowerShell.Cobacis	Kaspersky	HEUR:Trojan.Script.Generic	
MAX	Malware (ai Score=89)	McAfee	PS/Rozena.b	

### VirusTotal information

VirusTotal shows there are 28 AV vendors detect this malicious payload. 4 vendors detect it is cobalt strike related malware, and 8 vendors detect it as 「PwShell.Rozena」. That's interesting! After I searched what is Rozena, and I found an analysis report published in 2018 from GDATA [3]. Looks like the malware used some technique of command line to run powershell, performing fileless attacks.

## Analysis

Source: <https://ak100117.medium.com/analyzing-cobalt-strike-powershell-payload-64d55ed3521b>