Cobalt Mirage Ransomware Group Steps Up Its Game in 2022

May 24, 2022

The Cobalt Mirage cybercriminal group has dealt some massive blows this year in the EU and the US, and its selection of targets is nothing short of odd compared to previous operations, researchers warn.

Table Of Contents

About Cobalt Mirage

The group mainly conducts cyber-espionage operations and ransomware attacks, and it picks its potential victims from the EU and the US. In a recent blog post, Secureworks researchers wrote about a series of cyberattacks carried out in 2022, including ransomware and data theft, linked to an Iranian group that they named Cobalt Mirage – other researchers refer to the group as APT35, Charming Kitten, Phosphorus, and TA453.

Targeting Government Institutions

Secureworks has attributed a notable cybersecurity incident that hit an undisclosed US local government institution in March 2022 to the group as the way the attack was conducted was very similar to previous attacks.

In their attacks, the threat actors usually go for exploiting the ProxyShell vulnerabilities to deploy FRPC (Fast Reverse Proxy client) to enable remote access to compromised systems and leveraging the weak infrastructure of the target.

Exactly how the group initially breached the targeted system remains unclear. However, Secureworks experts say the attackers likely exploited unpatched Log4j flaws, even if a patch was available at the time. Unfortunately, many organizations don't pay enough attention to patching and keeping their systems up to date and secure, leaving the door open for all kinds of cyberattacks.

As for the group's March attack, there's evidence that suggests the initial exploitation might have begun in January 2022.

Odd Selection of Victims

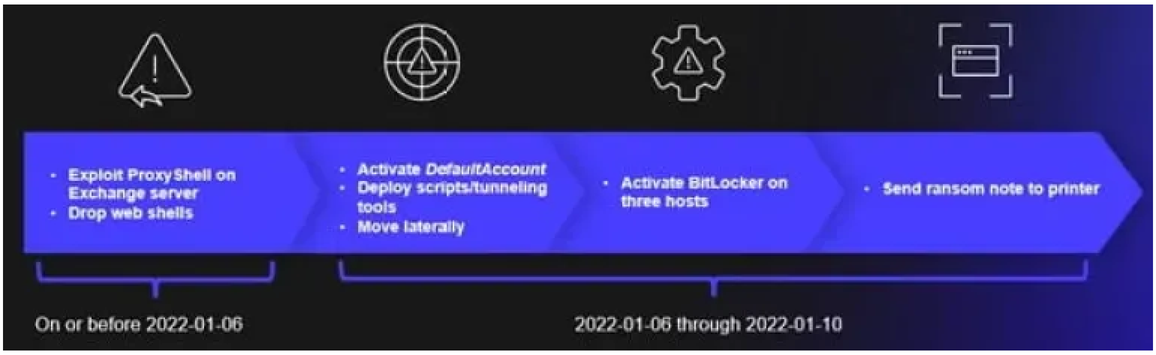
The intrusion took place over a four-day period in March, scanning the environment and stealing data. Secureworks noted that these malicious operations are odd, considering that, as with other attacks from the same period, the victims had no strategic or political value to Iran.

Soon after being discovered, the illicit activity was disrupted and no further attempts were observed. The hackers were most likely motivated by financial gain, but researchers have yet to discover in what way Cobalt Mirage would profit from these attacks.

"While the threat actors appear to have had a reasonable level of success gaining initial access to a wide range of targets, their ability to capitalize on that access for financial gain or intelligence collection appears limited," Secureworks Counter Threat Unit (CTU) researchers wrote in the post.

The group did not deploy ransomware in the March incident, but they did in another attack targeting a 'US philanthropic organization' in January 2022.

Secureworks noted that the initial infiltration and the remote access were achieved by exploiting ProxyShell and Microsoft Exchange vulnerabilities. The threat group then triggered a BitLocker ransomware attack.



Exploit ProxyShell on Exchange server
Drop web shells
Activate DefaultAccount
Deploy scripts/tunneling tools
Move laterally
Activate BitLocker on three hosts
Send ransom note to printer
On or before 2022-01-06
2022-01-06 through 2022-01-10

COBALT MIRAGE actions in January 2022 intrusion. Source: Secureworks

Sending the Ransom Note Straight to the Victim's Printer

The group made its presence known in the ransomware landscape in a rather unique way – they send the ransom note straight to a printer on the compromised system and print it on paper (while most ransomware operators send it to screens or servers). The note contains an email address and contact information.

"The threat actors completed the attack with an unusual tactic of sending a ransom note to a local printer. The note includes a contact email address and Telegram account to discuss decryption and recovery. This approach suggests a small operation that relies on manual processes to map victims to the encryption keys used to lock their data," the security researchers said.

Both incidents started off with the exploitation of unpatched vulnerabilities. Researchers recommend patching as soon as possible and keeping your systems updated, using MFA, and implementing security awareness training in your company.

Educate your employees on phishing and how to combat it with the help of one of our comprehensive Security Awareness Training plans.

Get your quote today.

Sources:

Secureworks *COBALT MIRAGE Conducts Ransomware Operations in U.S.*

ZDNet *These ransomware attackers sent their ransom note to the victim's printer*

Security Magazine *COBALT MIRAGE conducts ransomware operations in US*

Attribution: