Opsec Mistakes Reveal COBALT MIRAGE Threat Actors

secureworks.com/blog/opsec-mistakes-reveal-cobalt-mirage-threat-actors

Counter Threat Unit Research Team

Artifacts exposed personas and companies associated with the Iranian threat group.
Wednesday, September 14, 2022 *By: Counter Threat Unit Research Team*

Secureworks® Counter Threat Unit™ (CTU) analysis of a June 2022 ransomware incident revealed details about Iranian COBALT MIRAGE threat group operations. Despite CTU™ researchers publicly disclosing COBALT MIRAGE tactics, techniques, and procedures

(TTPs) in May 2022, the threat actors continue to demonstrate many of the same behaviors.

In this incident, COBALT MIRAGE exploited the ProxyShell vulnerabilities (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207). It is likely that the compromise was opportunistic rather than targeted. In keeping with their established intrusion pattern, the threat actors deployed multiple web shells and TunnelFish, a customized variant of Fast Reverse Proxy (FRPC). They then enabled the DefaultAccount with a password commonly used by COBALT MIRAGE (P@ssw0rd1234) and encrypted several servers using BitLocker.

The threat actors attempted to remove traces of their activities, deleting web shells, tools, and audit logs. However, several tools and artifacts were recoverable. The TunnelFish sample was configured to communicate with two command and control (C2) domains: gupdate . us and msupdate . top. While investigating these domains, CTU researchers discovered additional infrastructure linked to COBALT MIRAGE: mssync . one, upmirror . top, 104 . 168 . 117 . 149, 172 . 245 . 26 . 118, and 193 . 142 . 59 . 174. CTU researchers also discovered copies of a ransom note in the victim's environment that referenced a Telegram account (@BuySafety) and email address (buysafety @ onionmail . org) observed in prior intrusions.

COBALT MIRAGE usually leaves a ransom note in the form of a .txt text file. However, in this case the threat actors copied a PDF file containing the ransom text (Hi.pdf) into the victim's environment. Based on evidence from recovered log files, it appears multiple copies of the PDF file were created alongside multiple .txt files with the same content. While other copies of the PDF were deleted, a copy remained in the threat actor's staging directory. This oversight resulted in the disclosure of information that could reveal the identity of an individual engaged in COBALT MIRAGE activity. The metadata of the Hi.pdf ransom note indicates that the document was created on December 17, 2021 by "ahmad khatibi" in a UTC +3.30 time zone (see Figure 1). This time zone corresponds to Iran Standard Time (IRST). The timestamp appears to be authentic.

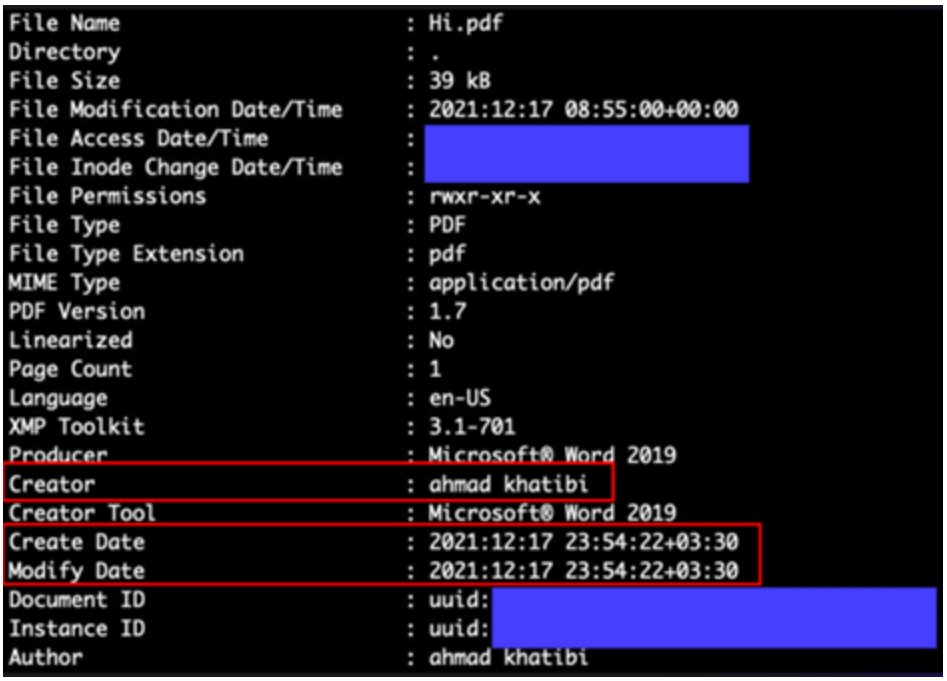

Figure 1. Metadata from Hi.pdf showing creator name and time zone. (Source: Secureworks)

A LinkedIn profile lists Ahmad Khatibi as the CEO of Afkar System Co., a company based in Iran. In June 2022, anti-Iranian regime whistleblower persona Lab_Dookhtegan posted a series of tweets about Ahmad Khatibi and Afkar System, stating they are operating on behalf of Intelligence Organization of Sepah (see Figure 2). Sepah is a reference to the Islamic Revolutionary Guard Corp (IRGC), and the Intelligence Organization (IRGC-IO) is a subordinate unit. The IRGC-IO is one of Iran's primary intelligence functions and reportedly operates a cyber division.

Figure 2. Lab_Dookhtegan tweet on June 23, 2022 referencing Ahmad Khatibi and Afkar System. (Source: Secureworks)

Lab_Dookhtegan's allegations appear to reinforce that the creator reference in the ransom note is legitimate and is not a false flag implicating an unrelated individual. Operational security failures revealing attribution is not uncommon with Iranian cyber operations. Past examples documented by CTU researchers include the identification of a developer linked to malicious Iranian activity, and Iranian malware developers infecting their own system and disclosing screenshots of their development environments on the internet.

Lab_Dookhtegan has been active on Twitter and Telegram since 2019. They have leaked verified source code and tools linked to several Iranian threat groups, including COBALT GYPSY and COBALT EDGEWATER. They have also leaked information about multiple individuals and companies that allegedly work for the IRGC and the Iranian Ministry of Intelligence and Security (MOIS).

In April 2022, Lab_Dookhtegan reported via their Telegram and Twitter channels that Iranian company Najee Technology and Secnerd also operate on behalf of the IRGC-IO (see Figure 3).

Figure 3. Tweet alleging connections among Najee Technology, Secnerd, and the IRGC. (Source: Secureworks)

The source of Lab_Dookhtegan's information is unknown, but CTU researchers independently identified links between known COBALT MIRAGE infrastructure and Najee Technology. DNS resolution data, WHOIS data, and website analysis reveal a series of connections between two COBALT MIRAGE domains (newdesk . top and symantecserver . co) and an IP address (185 . 208 . 77 . 164) hosting two Iranian (.ir) domains: secnerd . ir and najee . ir (see Figure 4). Najee . ir was an official website for Najee Technology but no longer hosts content promoting the company’s presence.

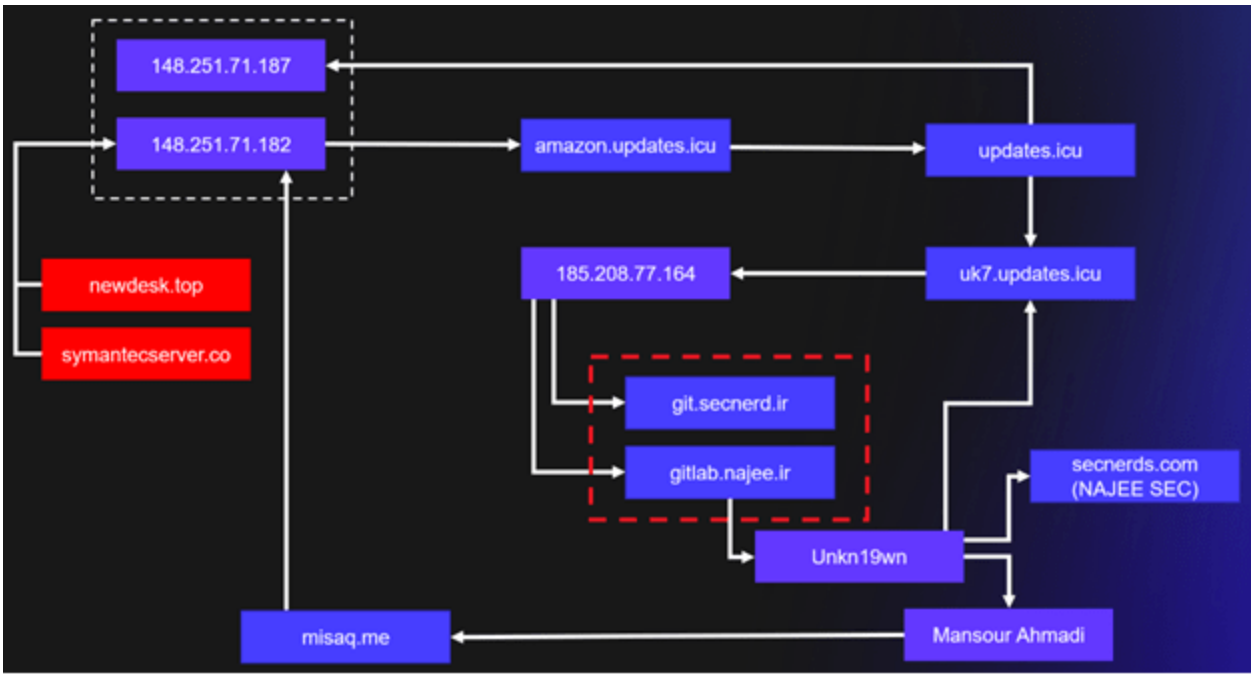

Figure 4. Connections between COBALT MIRAGE infrastructure and Najee Technology. (Source: Secureworks)

The uk7 . updates . icu domain hosts an instance of the GitLab code collaboration platform that reveals an account for a user named unkn19wn (see Figure 5). This detail links updates . icu to secnerd . ir and najee . ir.

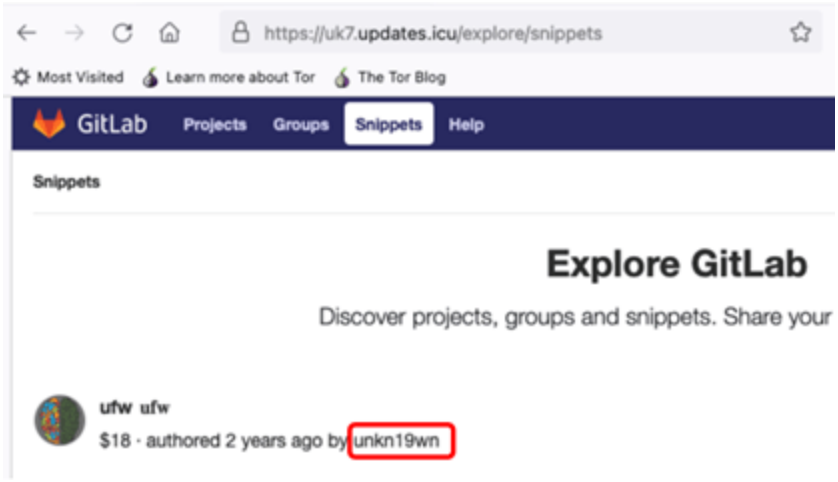

Figure 5. GitLab interface showing unkn19wn account. (Source: Secureworks)

This same alias appears in an email address (unkn19wn @ gmail . com) that was used to register najee . ir and secnerds . com. WHOIS records show the domain registrant as Mansour Ahmadi. Public records of Iranian companies list Mansour Ahmadi as the CEO of Najee Technology. Mansour Ahmadi also appears in the WHOIS registrant information for the domain misaq . me, which has resolved to COBALT MIRAGE IP address 148 . 251 . 71 . 182.

Content hosted on najee . ir in 2015 shows Mansour Ahmadi (also known as Unkn19wn) developing an interest in hacking and website defacement and expressing dislike for the U.S. and Israel. Secnerd . ir is offline as of this publication but previously hosted content related to cybersecurity and advertised for iOS and Android developers. It was cited in an incident involving the mass accumulation and accidental disclosure of Iranian citizens' social media data. It is likely that Mansour Ahmadi leads both Najee Technology and Secnerd and that these entities' connection to COBALT MIRAGE activity represent just a portion of their technology and cybersecurity-related projects.

It is likely that updates . icu, secnerd . ir and najee . ir are all operated by the same group of individuals and that those individuals support COBALT MIRAGE attacks. CTU analysis links Afkar System, Najee Technology, and Secnerd to COBALT MIRAGE but cannot verify reported links to the IRGC-IO. However, the pattern of private Iranian companies acting as fronts or providing support for Iranian intelligence operations is well established. In 2016, the U.S. Department of Justice indicted seven Iranians employees of ITSec Team and Mersad Company for supporting the government of Iran and the IRGC in attacking the U.S. financial sector in 2011 and 2012. In 2019, the U.S. Department of the Treasury sanctioned individuals linked to Net Peygard Samavat Company (later known as Emennet Pasargad) for working with the IRGC and MOIS. In 2020, the U.S. Department of the Treasury sanctioned Rana Intelligence Computing Company and some of its employees, describing it as a front company that conducts computer intrusions and malware campaigns on behalf of MOIS.

Figure 6 likely represents the working relationship between Najee Technology, Secnerd, Afkar System, and the IRGC-IO. The exact nature of these companies' involvement in COBALT MIRAGE activity remains unclear, although evidence indicates that at a minimum they provide network infrastructure and support the ransomware attacks. Third-party reporting on UNC2448 appears to describe COBALT MIRAGE activity and links the group to Najee Technology and Afkar System. Similar reporting on DEV-0270, another COBALT MIRAGE alias, attributes the group to a company that functions under two public aliases: Secnerd (secnerd . ir) and Lifeweb (lifeweb . ir). The DEV-0270 reporting states that these organizations are linked to Najee Technology.

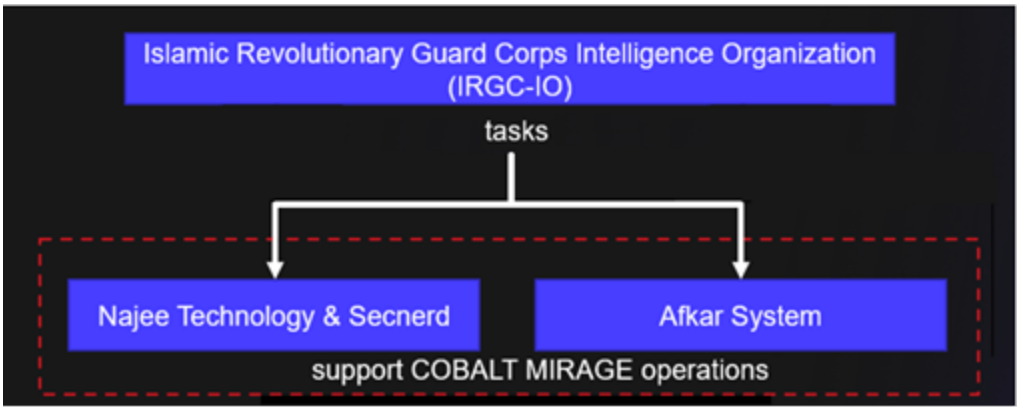

Figure 6. Potential relationships between Najee, Secnerd, Afkar System, and the IRGC-IO. (Source: Secureworks)

The model of Iranian government intelligence functions using contractors blurs the lines between the actions tasked by the government and the actions that the private company takes on its own initiative. While part of COBALT MIRAGE activity appears espionage-focused, a significant portion is focused on opportunistic revenue generation through its ransomware activities. While these companies may work with the IRGC-IO, the ransomware attacks could be another source of revenue that they can pursue without fear of prosecution by Iranian law enforcement. Other Iranian threat groups such as COBALT SAPLING (also known as Moses Staff) and COBALT SHADOW (also known as Agrius and BlackShadow) have made use of ransomware in their attacks. However, the primary intent of these attacks appeared to be disruption and harassment of the victim rather than revenue generation.

Although the ProxyShell vulnerabilities were disclosed in August 2021, COBALT MIRAGE continues to have success exploiting them to compromise organizations. CTU researchers advise organizations to routinely validate that all internet-facing systems are appropriately patched and take swift mitigating actions where gaps are found.

To mitigate exposure to this malware, CTU researchers recommend that organizations use available controls to review and restrict access using the indicators listed in Table 1. Note that IP addresses can be reallocated. The domains and IP address may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
gupdate.us	Domain name	TunnelFish C2 server used by COBALT MIRAGE
msupdate.top	Domain name	TunnelFish C2 server used by COBALT MIRAGE
193.142.59.174	IP address	Hosting TunnelFish domains used by COBALT MIRAGE

Indicator	Type	Context
172.245.26.118	IP address	Staging and distributing COBALT MIRAGE malware
mssync.one	Domain name	Suspected C2 server linked to COBALT MIRAGE
upmirror.top	Domain name	Suspected C2 server linked to COBALT MIRAGE
104.168.117.149	IP address	Hosting COBALT MIRAGE domains
69314c1969f28bfab34683769286326e25d9a0f07c4bad3443d08efe4f43e0a8	SHA256 hash	TunnelFish malware used by COBALT MIRAGE
f38f3a1cda90229434e8ab8c59342838106b9778	SHA1 hash	TunnelFish malware used by COBALT MIRAGE
00e4c488558492b80fd27d51b159a099	MD5 hash	TunnelFish malware used by COBALT MIRAGE

Table 1. Indicators for this threat.

Learn more about ransomware threats and how to protect your organization. If you need urgent assistance with an incident, contact the Secureworks Incident Response team.