APT42: Crooked Charms, Cons, and Compromises

mandiant.com/resources/blog/apt42-charms-cons-compromises

Today, Mandiant is releasing a comprehensive report detailing APT42, an Iranian state-sponsored cyber espionage group tasked with conducting information collection and surveillance operations against individuals and organizations of strategic interest to the Iranian government. We estimate with moderate confidence that APT42 operates on behalf of the Islamic Revolutionary Guard Corps (IRGC)'s Intelligence Organization (IRGC-IO) based on targeting patterns that align with the organization's operational mandates and priorities.

The full published report covers APT42's recent and historical activity dating back to at least 2015, the group's tactics, techniques, and procedures, targeting patterns, and elucidates historical connections to APT35. APT42 partially coincides with public reporting on TA453 (Proofpoint), Yellow Garuda (PwC), ITG18 (IBM X-Force), Phosphorus (Microsoft), and Charming Kitten (ClearSky and CERTFA).

Read the APT42 report now, and check out our podcast for even more information on APT42.

APT42 Operations

APT42 uses highly targeted spear-phishing and social engineering techniques designed to build trust and rapport with their victims in order to access their personal or corporate email accounts or to install Android malware on their mobile devices. In addition, APT42 infrequently uses Windows malware to complement their credential harvesting and surveillance efforts.

APT42 operations broadly fall into three categories:

- **Credential harvesting:** APT42 frequently targets corporate and personal email accounts through highly targeted spear-phishing campaigns with enhanced emphasis on building trust and rapport with the target before attempting to steal their credentials. Mandiant also has indications that the group leverages credential harvesting to collect Multi-Factor Authentication (MFA) codes to bypass authentication methods and has used compromised credentials to pursue access to the networks, devices, and accounts of employers, colleagues, and relatives of the initial victim.

- **Surveillance operations:** As of at least late 2015, a subset of APT42's infrastructure served as command-and-control (C2) servers for Android mobile malware designed to track locations, monitor communications, and generally surveil the activities of individuals of interest to the Iranian government, including activists and dissidents inside Iran.
- **Malware deployment:** While APT42 primarily prefers credential harvesting over activity on disk, several custom backdoors and lightweight tools complement its arsenal. The group likely incorporates these tools into their operations when the objectives extend beyond credential harvesting.

Mandiant has observed over 30 confirmed targeted APT42 operations spanning these categories since early 2015. The total number of APT42 intrusion operations is almost certainly much higher based on the group's high operational tempo, visibility gaps caused in part by the group's targeting of personal email accounts and domestically focused efforts, and extensive open-source industry reporting on threat clusters likely associated with APT42.

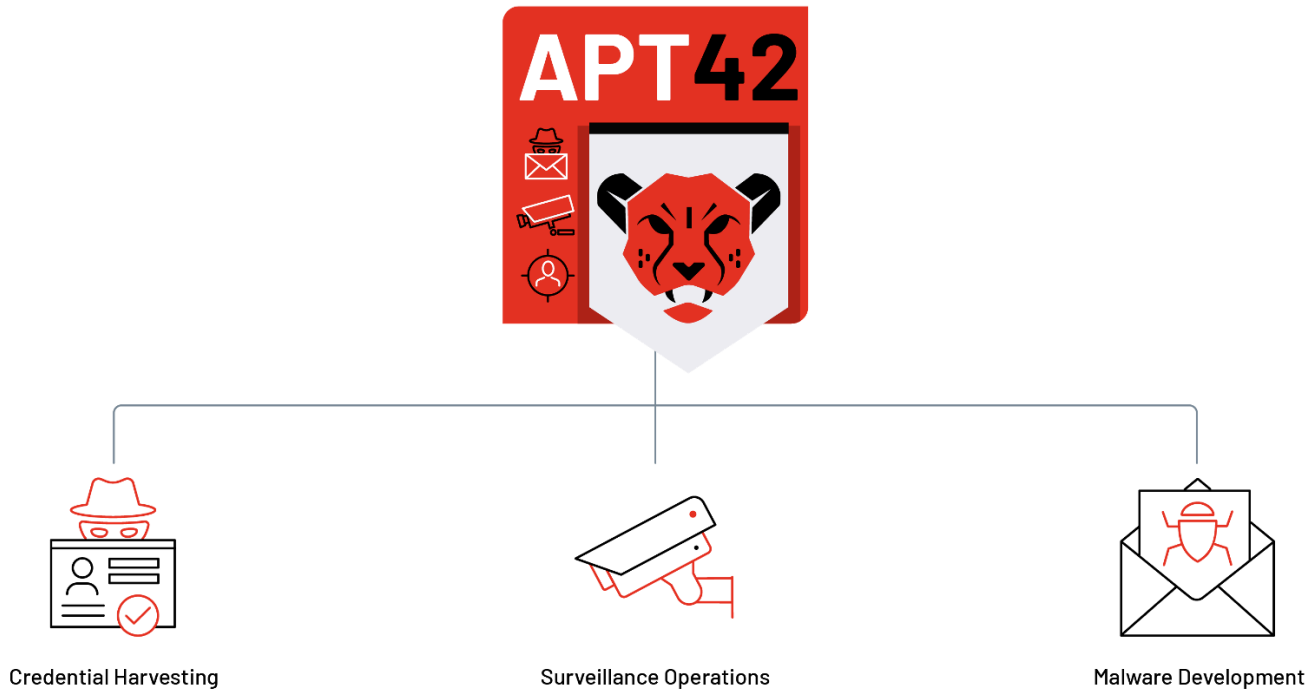

Figure 1: APT42 operations by category

APT42 Targeting Patterns

The targeting patterns for APT42 operations are similar to other Iranian cyber espionage actors, with a large segment of its activity focused on the Middle East region. However, unlike other suspected IRGC-affiliated cyber espionage groups that have focused on targeting the defense industrial base or conducting large-scale collection of personally identifiable information (PII), APT42 primarily targets organizations and individuals deemed opponents or enemies of the regime, specifically gaining access to their personal accounts

and mobile devices. The group has consistently targeted Western think tanks, researchers, journalists, current Western government officials, former Iranian government officials, and the Iranian diaspora abroad.

Some APT42 activity indicates the group alters its operational focus as Iran's priorities evolve, to include targeted operations against the pharmaceutical sector at the onset of the COVID-19 pandemic in March 2020 and pursuing domestic and foreign-based opposition groups prior to an Iranian presidential election. This indicates that APT42 is trusted by the Iranian government to quickly react to geopolitical changes by adjusting their flexible operations to targets of operational interest to Tehran.

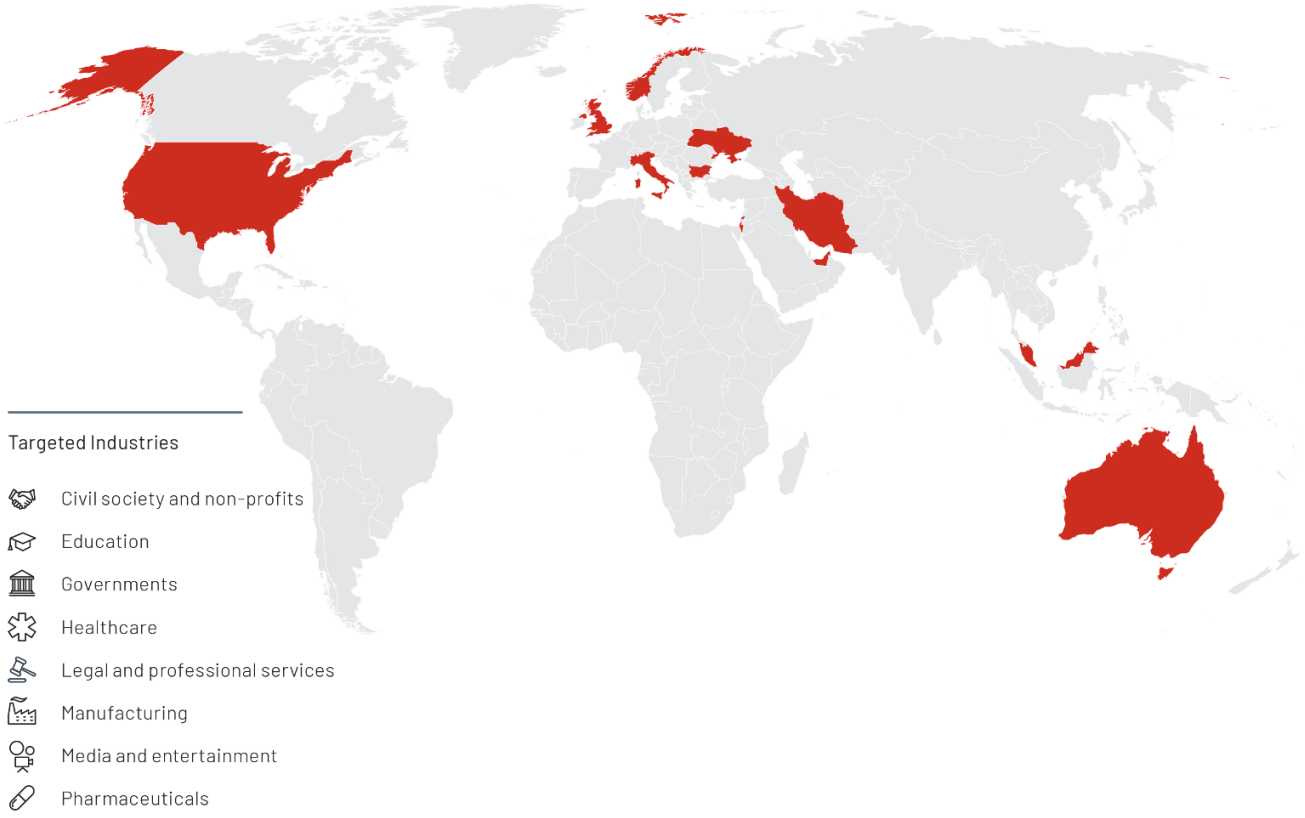

Figure 2: Countries and industries targeted directly by APT42

Potential Ties Between APT42 and Ransomware Activity

Mandiant further highlights open-source reporting from Microsoft claiming a connection between intrusion activity clusters that generally align with APT42 and UNC2448, an Iran-nexus threat actor known for widespread scanning for various vulnerabilities, the use of the Fast Reverse Proxy tool, and reported ransomware activity using BitLocker. Notably, Mandiant has not observed technical overlaps between APT42 and UNC2448.

In November 2021, Microsoft reported that “Phosphorus” had targeted Fortinet FortiOS SSL VPN and unpatched on-premises Exchange servers globally with the intent of deploying ransomware such as BitLocker on vulnerable networks, aligning with activity we track as UNC2448. Previous reporting on Phosphorus generally aligned with APT42’s credential harvesting and spear-phishing operations.

While Mandiant has not observed technical overlaps between APT42 and UNC2448, the latter may also have ties to the IRGC-IO. We assess with moderate confidence that UNC2448 and the Revengers Telegram persona are operated by at least two Iranian front companies, Najee Technology and Afkar System, based on open-source information and operational security lapses by the threat actors. Public leaking campaigns from the Lab Dookhtegan Telegram account further allege these companies are responsible for threat activity aligned with UNC2448 and operate on behalf of the IRGC-IO.

- Mandiant identified links between UNC2448, the Revengers persona, an individual named Ahmad Khatibi, and a likely Iranian front company named Afkar System.
- The Revengers persona had offered data and access to primarily Israeli companies for sale on its Telegram channel between February and September 2021.
- Additionally, infrastructure overlaps likely caused by human error indicate that UNC2448 has connections to a second front company, Najee Technology.
- Public posts by the Lab Dookhtegan Telegram channel in July 2022 claim Afkar System and Najee Technology are front companies conducting cyber operations on behalf of the IRGC’s Intelligence Organization.

Looking Ahead

APT42 activity poses a threat to foreign policy officials, commentators, and journalists, particularly those in the United States, the United Kingdom, and Israel, working on Iran-related projects. Additionally, the group’s surveillance activity highlights the real-world risk to individual targets of APT42 operations, which include Iranian dual-nationals, former government officials, and dissidents both inside Iran and those who previously left the country, often out of fear for their personal safety.

We do not anticipate significant changes to APT42’s operational tactics and mandate given the long history of activity and imperviousness to infrastructure take downs and a media spotlight on operational security failures. Nevertheless, the group has displayed its ability to rapidly alter its operational focus as Iran’s priorities change over time with evolving domestic and geopolitical conditions. We assess with high confidence that APT42 will continue to perform cyber espionage and surveillance operations aligned with evolving Iranian operational intelligence collection requirements.

Read the full APT42 report today and listen to *The Defender's Advantage Podcast* to learn more.