ORNA™

Cybersecurity Advisory

Dear ORNA Customer,

We are sending you this advisory to provide additional situational awareness about the ongoing Iranian cyber campaigns against organizations and individuals with ties to Israel or of relevant strategic value to the Iranian regime.

Why this matters

With the ongoing conflict in the Middle East, the Iranian regime and its supporters have been increasing their efforts in targeting Israeli and Jewish related organizations and individuals for intelligence gathering. This growing focus on cyber operations has increased the pressure on organizations to protect their data.

Overview

Several reports published by cybersecurity researchers have highlighted three distinct campaigns by Iranian threat actors against individuals and organizations with ties to Israel. These campaigns range from phishing attacks to collect individuals data to advanced intelligence gathering malware targeting organizations across the world.

Mandiant Report

The first report, published by Google's Mandiant team[1], highlights a social engineering campaign carried out by the Iranian State in conjunction with APT42, mainly targeting academics and media personalities.

The campaign involved creating fake recruitment websites and social media accounts to lure targets into submitting personal and professional details. This information likely aids Iranian intelligence in identifying and persecuting potential threats, including dissidents and activists. The operation, linked to Iran's IRGC and APT42, has been active since 2017, with similar tactics used in campaigns targeting Syria and Hezbollah.

This campaign highlights Iran's ever growing expertise of social engineering tactics and their indiscriminate use.

Microsoft Report

The second report, published by Microsoft[2], presents a new malware by the name of Tickler meant to quietly gather and exfiltrate intelligence data from compromised devices from companies across a wide range of sectors.

Between April and July 2024, cybersecurity experts observed the Iranian state-sponsored group Peach Sandstorm deploying a new custom multi-stage backdoor named Tickler. Targeting sectors like satellite, communications, oil and gas, and government in the U.S. and UAE, this backdoor represents an evolution in Peach Sandstorm's intelligence-gathering operations. In addition to cyber espionage, the group continued its password spray attacks and used LinkedIn for intelligence collection, indicating a persistent focus on sectors like education, defense, and satellite for infrastructure procurement and intelligence gathering.

This campaign likewise serves to demonstrate the technical ability of Iranian threat actors in developing novel tools.

CISA Joint Advisory

Lastly, the FBI and CISA published an advisory[3] warning about Iran-based cyber actors enabling ransomware attacks against U.S. organizations in sectors such as education, healthcare, and defense. These actors, linked to the Iranian government, exploit vulnerabilities left exposed on public facing assets and steal credentials in order to later facilitate ransomware deployments by groups like NoEscape and BlackCat.

The advisory provides detailed guidance on mitigations and indicators of compromise to help organizations defend against these persistent threats.

Recommendations

Recommendation #1: Follow the mitigation guides

ORNA **strongly recommends** that organizations follow the mitigation guides included within the Microsoft and CISA advisories.

Recommendation #2: Reduce exposure of vulnerable assets

ORNA **strongly recommends** that organizations regularly conduct internal audits and vulnerability assessments of their assets in order to discover potential avenues of compromise and then determine the best course of action to reduce the risk.

References

1. https://cloud.google.com/blog/topics/threat-intelligence/uncovering-iranian-counterintelligence-operation
2. https://www.microsoft.com/en-us/security/blog/2024/08/28/peach-sandstorm-deploys-new-custom-tickler-malware-in-long-running-intelligence-gathering-operations/
3. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a

If you have any additional questions, please reach out to your ORNA representative at sme@orna.app.
Sincerely,
ORNA Team