Country Snapshot: Israel (Q1 2022)

Fusion (FS) | Strategic (ST)

April 12, 2022 01:20:49 PM, 22-00009569, Version: 1.0

Executive Summary

- This report provides a snapshot of tracked and targeted activity observed in Israel over the past two years. Tracked and targeted activity consists of incidents linked to tracked activity sets including targeted intrusions.
- This report is intended to provide quarterly semi-automated updates to augment the Profile for the specified country or region. For more details on threat activity affecting this region, please view the corresponding Profile.

Threat Detail

Threat Detail

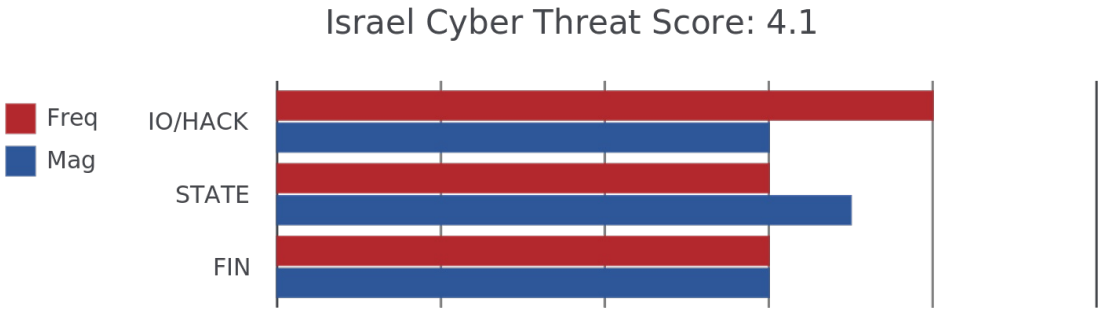
The Country Snapshot is a semi-automated quarterly report intended to provide updated information about tracked and targeted activity observed over the past two years (Q2 2020-Q1 2022) in Israel. For more details on threat activity affecting this region, please view the corresponding Profile.

Analyst Comment

Mandiant Threat Intelligence assesses with high confidence that state sponsored operations pose a moderate-frequency and moderate to high-intensity threat to organizations and individuals in Israel, with some incidents causing more serious impacts such as disruptive attacks. Iranian activity is observed most frequently. We believe information operations represent a growing and high-frequency and intensity threat to Israel, both from campaigns attempting to manipulate domestic opinion and internationally targeted campaigns attempting to foster anti-Israel sentiments. We assess with high confidence that financially motivated activity represents a moderate-frequency and intensity threat to Israel. Israel is a common target for hacktivist campaigns, particularly those with pro-Palestine, pro-Islam, and anti-Israel motivations, and such campaigns present a moderate-frequency but low-intensity threat. We expect hacktivist targeting of Israel to continue for the foreseeable future, particularly in response to triggering events, such as instances of conflict between Israeli forces and Palestinians.

Cyber Threat Score

Mandiant Threat Intelligence has developed industry- and geography-based cyber threat scores that provide a numerical shorthand to represent our best understanding of the aggregate cyber threat facing sectors, countries, and regions. We leverage Mandiant's unique visibility into the cyber threat landscape to evaluate the frequency and magnitude of cyber threat activity observed associated with four major actor or activity type categories: cyber espionage, financially motivated activity, information operations, and hacktivism. For a description of the methodology used to generate these scores and potential use cases, please see 20-00017245.



Targeted and Tracked Activity

Tracked and targeted activity includes targeted intrusions by tracked actors, including named state sponsored (APT) and financially motivated (FIN) actors. It also includes additional activity, such as operations linked to TEMP as well as unnamed activity sets that we monitor.

Target and Source Geography

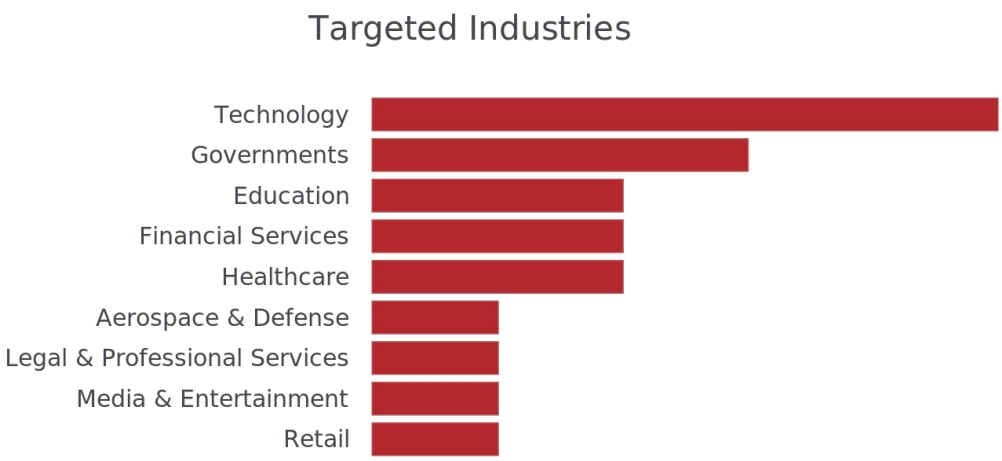
This map displays the suspected origins of threat actors observed active as well as locations of victims observed targeted over the past two years. This is not limited to suspected state sponsored actors but includes suspected locations of activity sets with various assessed motivations, for example, including financially motivated groups. In some cases, countries may be both a Target and a Source of threat activity, as reflected in the legend.

Target and Source Geography

Source	Target
Iran	Israel
Pakistan	

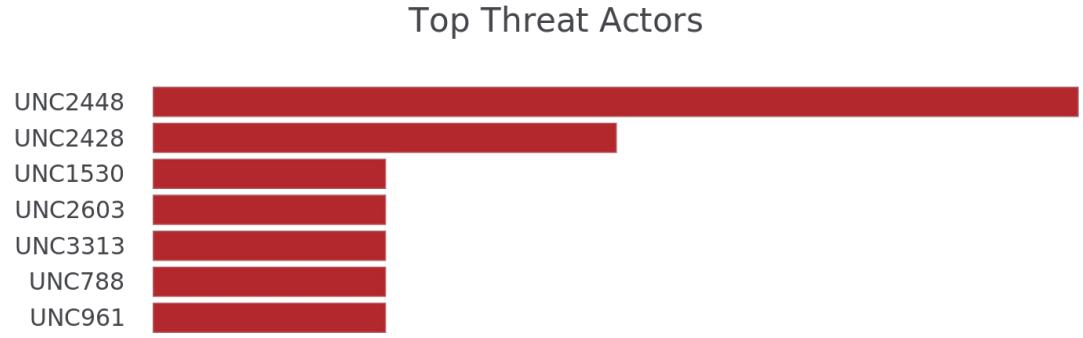
Top Targeted Industries

This shows the sectors most frequently impacted by tracked and targeted activity over the past two years. In cases where many industries were affected, results have been limited to those most frequently seen.



Top Actors

This shows the threat actors most frequently observed in tracked and targeted activity over the past two years. In cases where many actors were observed, results have been limited to those most frequently seen. In some cases, activity sets have been attributed to a named actor with low, medium, or high confidence, and these have been marked with appropriate confidence levels.



Top Malware Families

This shows the most frequently observed malware families in tracked and targeted activity over the past two years. In cases where many malware families were observed, results have been limited to the most frequently seen families.

Top Malware Families
ASYNCRAT
BLUEBEAM
CHILLSHELL
DOWNCOAT
GOPASSAGE
HOLEPUNCH
NIGHTCRYPT
REDBIN
REGEORG
SALTYBOAR

Top CVEs

This shows the most frequently observed CVEs in tracked and targeted activity over the past two years. In cases where many CVEs were observed, results have been limited to the most frequently seen families.

CVEs
CVE-2020-14750
CVE-2021-31207
CVE-2021-44228

Please rate this product by taking a short four question survey

First Version Publish Date

April 12, 2022 01:20:49 PM

Threat Intelligence Tags

Affected Industries

- Aerospace & Defense
- Education
- Financial Services
- Governments
- Healthcare
- High Tech/Software/Hardware/Services
- Legal & Professional Services
- Media & Entertainment
- Retail
- Technology

Source Geographies

- Iran
- Pakistan

Target Geographies

- Israel

Version Information

Version:1.0, April 12, 2022 01:20:49 PM

Common Vulnerabilities and Exposures

CVE ID:	CVE-2021-44228(CVE Description)Mandiant Vulnerability Analysis CVE-2020-14750(CVE Description)Mandiant Vulnerability Analysis CVE-2021-31207(CVE Description)Mandiant Vulnerability Analysis

MANDIANT ADVANTAGE

ilanaf@mail.gov.il