Industry Snapshot: Technology (Q1 2022)

Fusion (FS) | Strategic (ST)

April 12, 2022 05:41:18 PM, 22-00009753, Version: 1.0

Executive Summary

- This report provides a snapshot of tracked and targeted activity observed in the Technology sector over the past two years. Tracked and targeted activity consists of incidents linked to tracked activity sets including targeted intrusions.
- Also provided is information about high volume observations of malware families and CVEs in FireEye device detections in Technology in Q1 2022.
- This report is intended to provide quarterly semi-automated updates to augment the Profile for the specified industry. For more details on threat activity affecting this sector, please view the corresponding Profile.

Threat Detail

Threat Detail

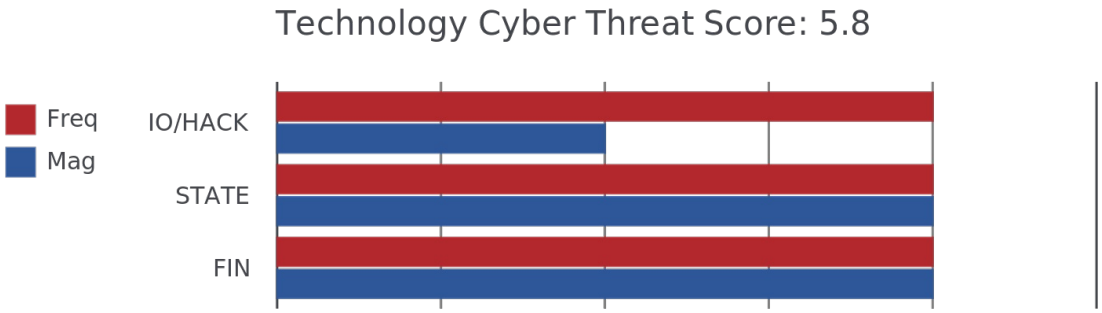
The Industry Snapshot is a semi-automated quarterly report intended to provide updated information about tracked and targeted activity observed over the past two years (Q2 2020-Q1 2022) in the Technology sector. Also included are high volume detections from Q1 2022. For more details on threat activity affecting this sector, please view the corresponding Profile.

Analyst Comment

Mandiant Threat Intelligence assesses with high confidence that cyber espionage poses a frequent and serious threat to the technology industry. This is very likely due primarily to the highly valuable proprietary information that these organizations often hold, which can often have military applications and/or provide domestic commerce with a competitive edge over international rivals. Additionally, many technology organizations can be used as a vector to compromise downstream targets via supply chain and third-party compromise. We believe that financially motivated threat actors pose a high frequency and severity threat to technology companies, with operations including ransomware, PII and financial data theft, and credential compromise. We assess with moderate confidence that information operations are a nearly continuous and moderate impact threat to social media platforms, primarily through reputational damage, credential theft, and platform abuse. These operations also likely pose an uncommon threat with negligible impact to other subsectors.

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.



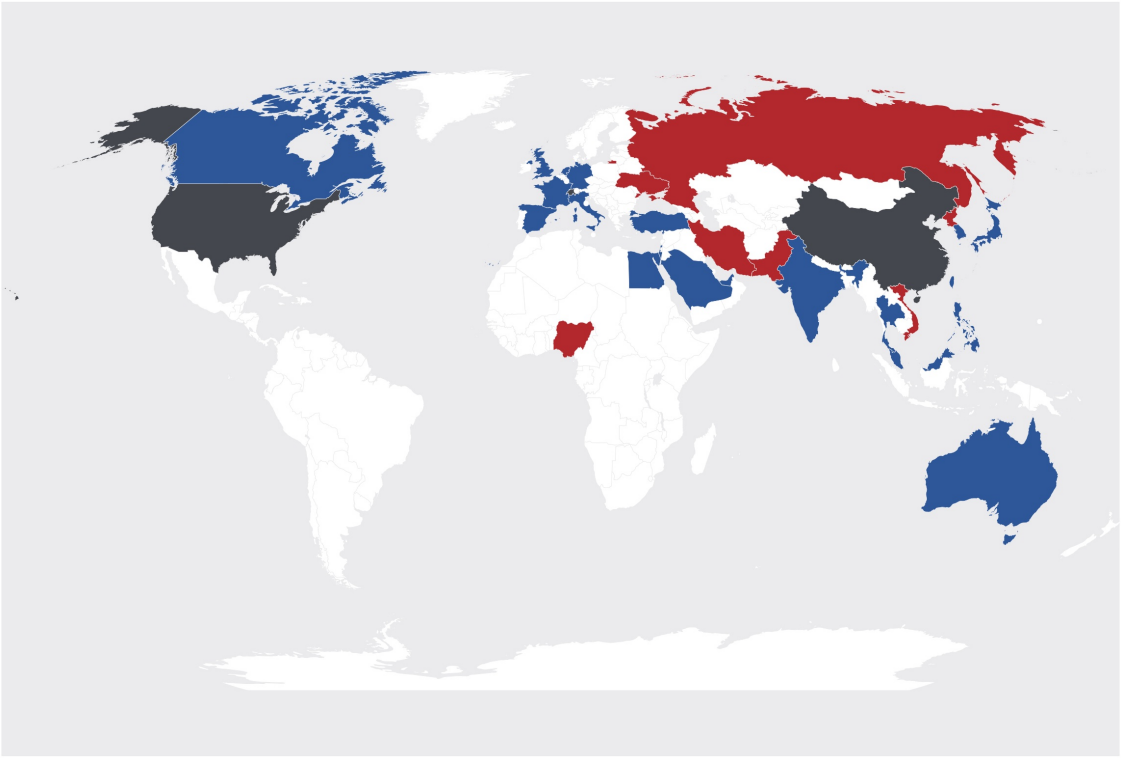
Targeted and Tracked Activity

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.

Source and Target 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, 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

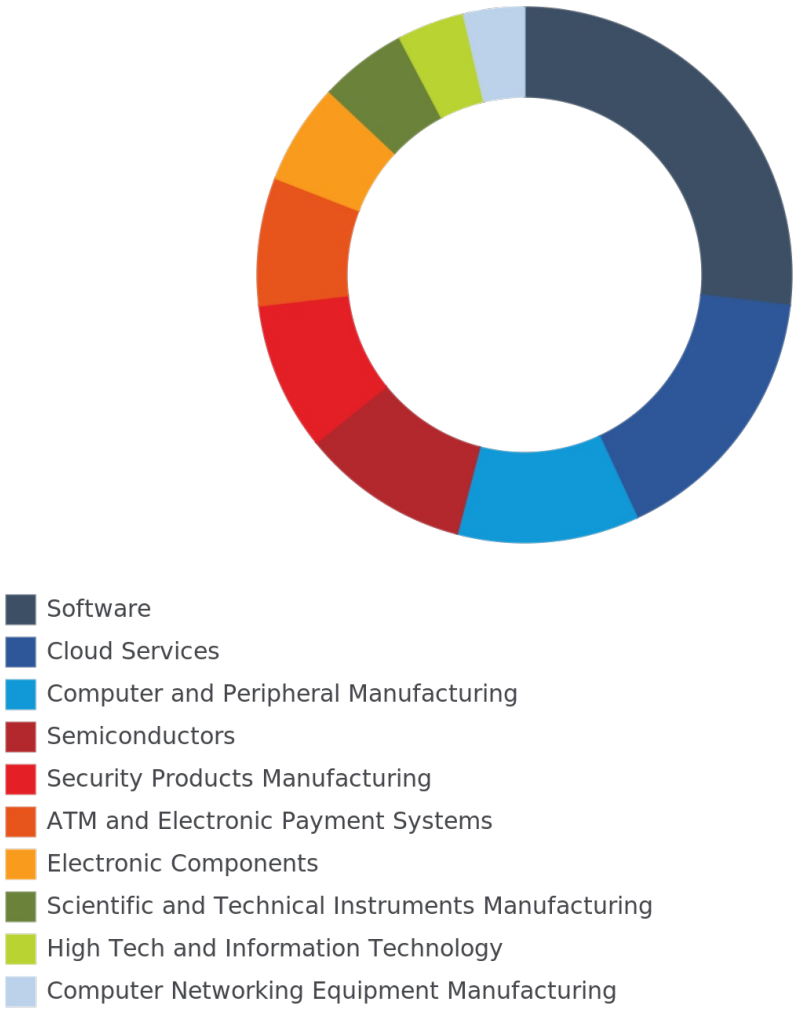


Source Geography Target Geography Source and Target

Source	Target
China	Australia
Iran	Canada
Nigeria	China
North Korea	Egypt
Pakistan	France
Russia	Germany
Switzerland	India
Ukraine	Israel
United States	Italy
Vietnam	Japan
	Malaysia
	Netherlands
	Philippines
	Saudi Arabia
	Singapore
	South Korea
	Spain
	Switzerland
	Taiwan
	Thailand
	Turkey
	United Arab Emirates
	United Kingdom
	United States

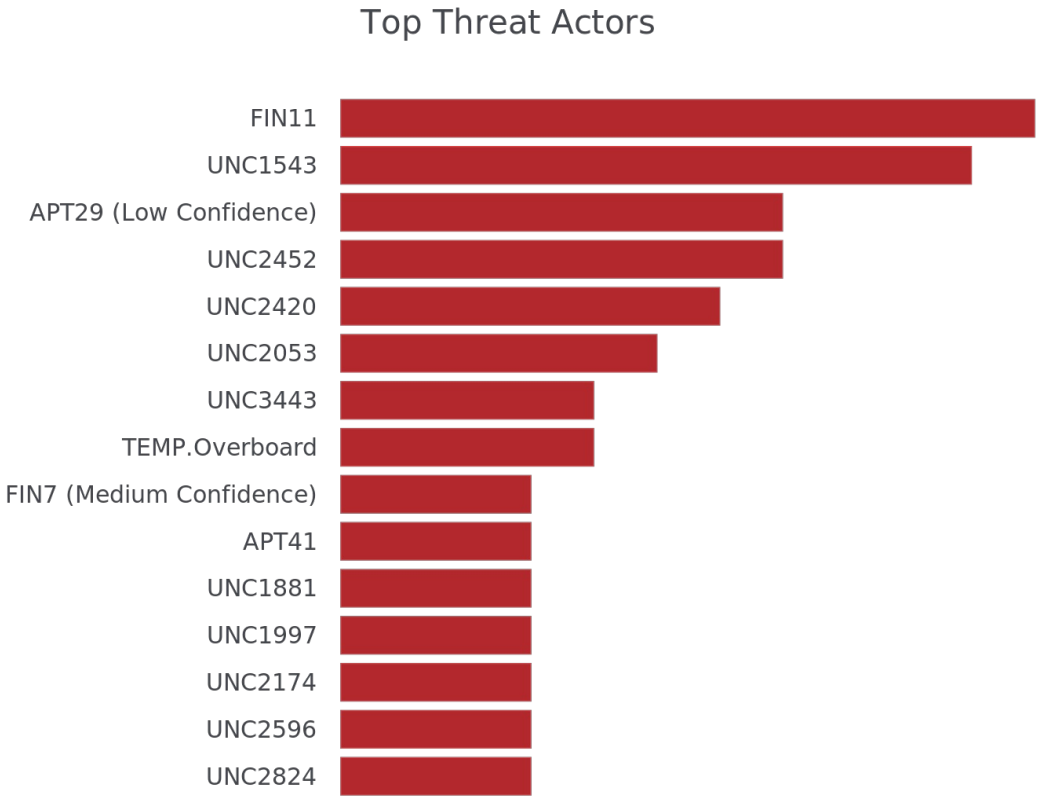
Targeted Subsectors

Targeted Subsectors



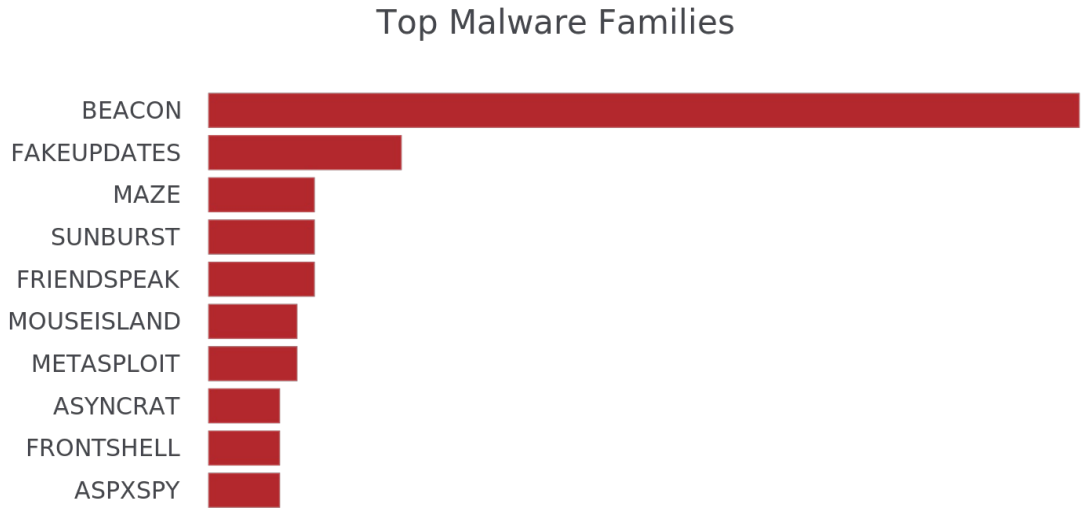
Top Threat Actors

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 activity sets have been marked with the appropriate confidence levels.



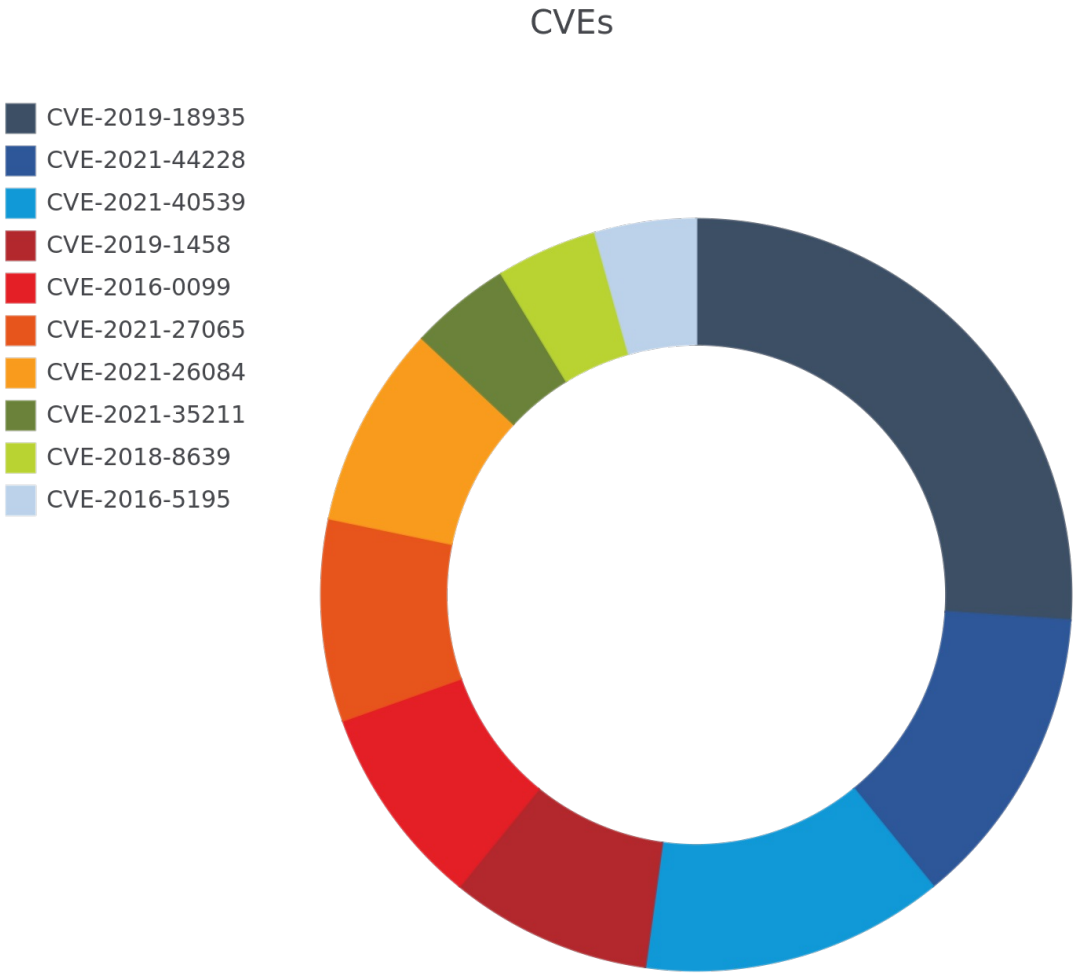
Top Malware Families

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 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.

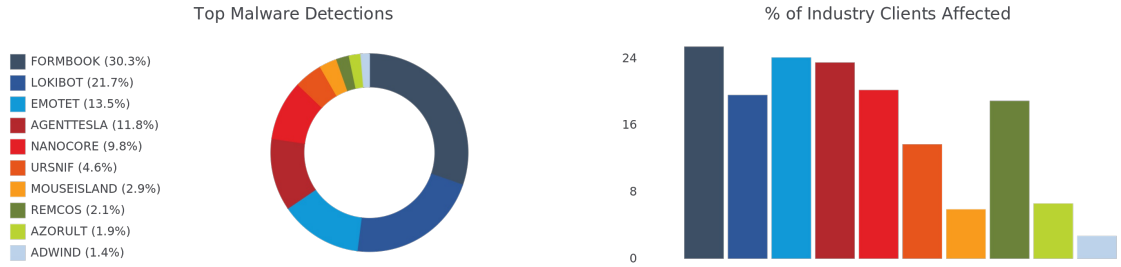


High Volume Trends

This section highlights high volume trends as observed in FireEye device detections. We suggest that this data may be broadly useful for keeping track of the widely distributed threat activity that is most prevalent in the Technology sector in Q1 2022. Due to structural differences in how detections data is collected and stored, in some cases industry categories do not match perfectly with the sector as addressed in the above sections. This data should still be useful for tracking high volume trends, as the data will reflect either a smaller or larger categorization that does overlap with the primary sector under consideration. We have included labels when appropriate to identify the differences.

Top Malware Detections

The following images represent the top malware detections in the high-tech sector in Q1 2022, factoring in both volume, the total number of detections for each malware family, and breadth, or, the percentage of sector customers impacted by the malware.



Top CVE Detections

The following images represent the top CVE detections in the high-tech sector in Q1 2022, factoring in both volume, the total number of detections for each CVE, and breadth, or, the percentage of sector clients impacted by the CVE.

Please rate this product by taking a short four question survey

First Version Publish Date

April 12, 2022 05:41:18 PM

Threat Intelligence Tags

Affected Industries

- High Tech/Software/Hardware/Services
- Technology

Source Geographies

- China
- Iran
- Nigeria
- North Korea
- Pakistan
- Russian Federation
- Switzerland
- Ukraine
- United States
- Vietnam

Target Geographies

- Australia
- Canada
- China
- Egypt
- France
- Germany
- India
- Israel
- Italy
- Japan
- Malaysia
- Netherlands
- Philippines
- Saudi Arabia
- Singapore
- South Korea
- Spain
- Switzerland
- Taiwan
- Thailand
- Turkey
- United Arab Emirates
- United Kingdom
- United States

Version Information

Version:1.0, April 12, 2022 05:41:18 PM

Common Vulnerabilities and Exposures

CVE ID:	cve-2012-1535(CVE Description)Mandiant Vulnerability Analysis cve-2017-0213(CVE Description)Mandiant Vulnerability Analysis CVE-2021-40539(CVE Description)Mandiant Vulnerability Analysis CVE-2016-5195(CVE Description)Mandiant Vulnerability Analysis CVE-2019-18935(CVE Description)Mandiant Vulnerability Analysis CVE-2019-1458(CVE Description)Mandiant Vulnerability Analysis cve-2017-11882(CVE Description)Mandiant Vulnerability Analysis cve-2012-0158(CVE Description)Mandiant Vulnerability Analysis cve-2010-3333(CVE Description)Mandiant Vulnerability Analysis CVE-2021-44228(CVE Description)Mandiant Vulnerability Analysis CVE-2016-0099(CVE Description)Mandiant Vulnerability Analysis CVE-2021-27065(CVE Description)Mandiant Vulnerability Analysis cve-2019-1458(CVE Description)Mandiant Vulnerability Analysis CVE-2021-26084(CVE Description)Mandiant Vulnerability Analysis cve-2020-1464(CVE Description)Mandiant Vulnerability Analysis CVE-2018-8639(CVE Description)Mandiant Vulnerability Analysis CVE-2021-35211(CVE Description)Mandiant Vulnerability Analysis

ilanaf@mail.gov.il