

# Overview

FireEye Threat Intelligence assesses with high confidence that APT41 is a prolific cyber threat group that carries out Chinese state-sponsored espionage activity in addition to financially motivated activity potentially outside of state control. Activity traces back to 2012 when individual members of APT41 conducted primarily financially motivated operations focused on the video game industry before expanding into likely state-sponsored activity. This is remarkable because explicit financially motivated targeting is unusual among Chinese state-sponsored threat groups, and evidence suggests these two motivations were balanced concurrently from 2014 onward.

- APT41 is unique among tracked China-based actors in that it leverages non-public malware typically reserved for espionage operations in what appears to be activity that falls outside the scope of state-sponsored missions.
- Based on early observed activity, consistent behavior, and APT41's unusual focus on the video game industry, we believe the group's cyber crime activities are most likely motivated by personal financial gain or hobbyist interests.

This contrasts with the state-sponsored goals that likely drive the group's healthcare, high-tech, and politically related targeting.

- We believe that APT41 is highly sophisticated and innovative. Its history of financially motivated targeting of the video game industry has ultimately supported the group's state-sponsored activity.
- The group's distinct use of supply chain compromises to target select individuals, consistent use of compromised digital certificates, and deployment of bootkits (rare among APT operators), highlight a creative and well-resourced adversary.
- Some of the early operations driven by personal gain used techniques that would later be pivotal in executing supply chain compromises.
- Learning to access video game production environments enabled APT41 to develop the tactics, techniques, and procedures (TTPs) that were later leveraged against software companies to inject malicious code into software updates.

APT41 campaigns include most of the incidents previously attributed in FireEye Threat Intelligence reporting to GREF Team and a number of additional clusters that were previously unnamed.

# Targeting

Like other Chinese espionage operators, APT41 targets industries in a manner generally aligned with China's Five-Year economic development plans. However, some campaigns attributed to APT41 indicate that the group is also deployed to gather intelligence ahead of imminent events, such as mergers and acquisitions (M&A) and political events.

Directly targeted verticals include:















- Healthcare: including medical devices and diagnostics
- High-tech: including semiconductors, advanced computer hardware, battery technology, and electric vehicles
- Media: including news organizations
- Pharmaceuticals
- Retail
- Software companies: which were compromised in supply chain operations potentially affecting large numbers of victims
- Telecoms
- Travel services
- Education
- Video games: including development studios, distributors/publishers, and activities enabling supply chain compromises
- Virtual currencies: including in-game currencies, cryptocurrencies, and related services

APT41 has targeted organizations in 14 countries (and Hong Kong) over seven years, including: France, India, Italy, Japan, Myanmar, the Netherlands, Singapore, South Korea, South Africa, Switzerland, Thailand, Turkey, the United Kingdom, and the United States (Figure 1). APT41 espionage operations against entities in these countries follow targeting of verticals consistent with Chinese national policy priorities.

TARGETED IN 14 COUNTRIES



FIGURE 1. Countries and industries targeted directly by APT41.

Industries Targeted		
 Automotive	 Financial	 Pharmaceuticals
 Business Services	 Healthcare	 Retail
 Cryptocurrency	 High-Tech	 Telecommunications
 Education	 Intergovernmental	 Travel
 Energy	 Media and Entertainment	

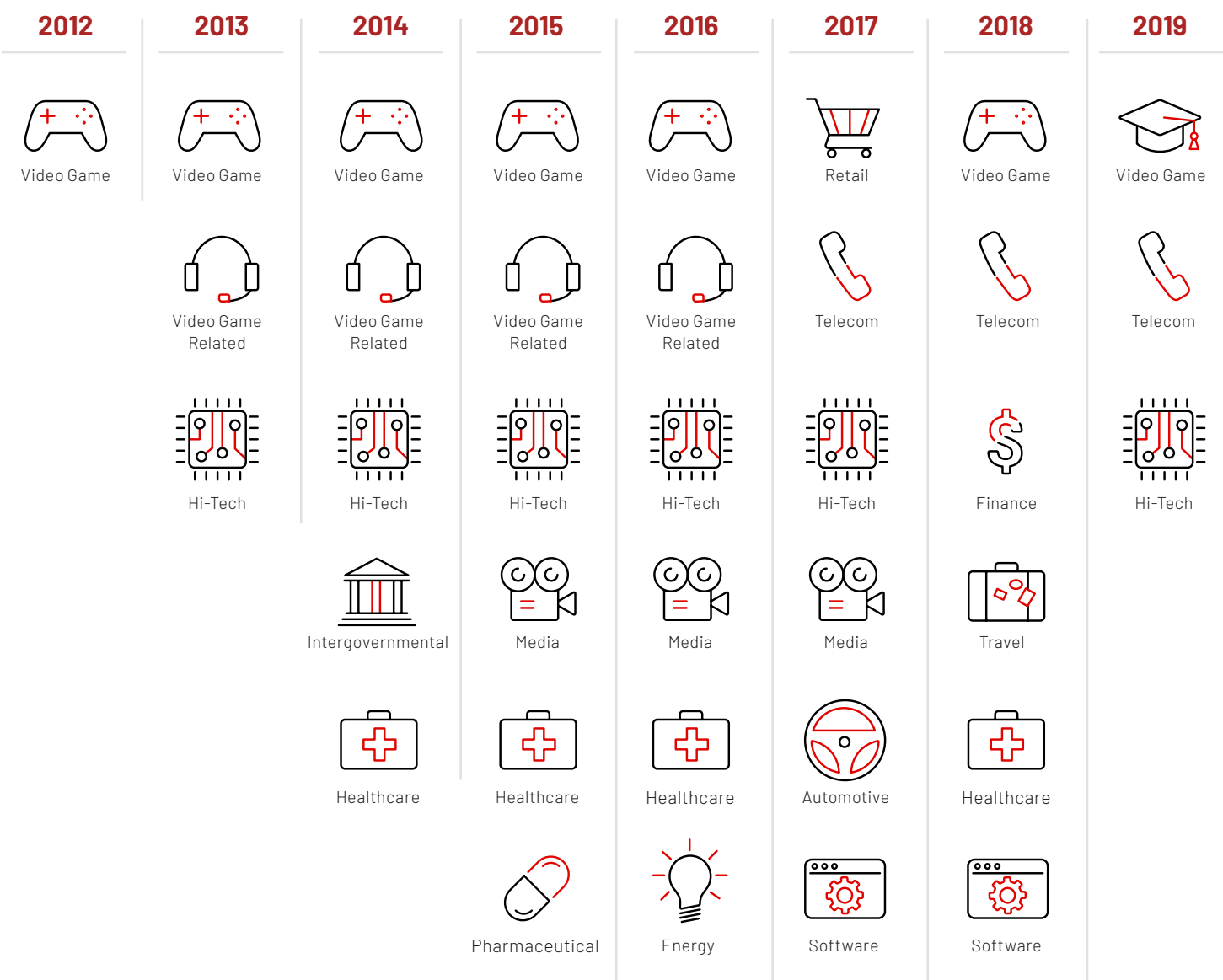
# Operations Over Time

The duality of APT41's state-sponsored activity and its own cyber crime operations is demonstrated in the group's simultaneous operations. Throughout the group's observable history, APT41 has consistently run its own financially motivated campaigns concurrently with espionage operations. In contrast, APT41 espionage targeting has changed significantly over time, suggesting shifts in assigned missions or new contracts to complete. A breakdown of industries targeted by APT41 over time can be found in Figure 2.

- We believe that like other Chinese espionage operators, APT41 has moved toward strategic intelligence collection and establishing access, but away from direct intellectual property theft. This shift, however, has not affected the group's consistent interest in targeting the video game industry for financially motivated reasons.
  - We have not observed evidence of IP theft since late 2015.
  - In 2014, APT41 was observed carrying out espionage campaigns concurrently with financially motivated intrusions, demonstrating that they could balance different objectives simultaneously.
- Espionage operations occurred while the group was still carrying out financially motivated campaigns, including longer-term intrusions, which typically extended for more than a year.
  - In one instance, APT41 was attempting to steal data from a healthcare target while also attempting to deploy ransomware at a video game studio.
- Compromising organizations in different sectors concurrently provides some indication that they are fulfilling specific assigned tasks.
  - Campaigns have expanded into additional industries including telecoms, the automotive sector, higher education, and travel services.
  - In 2015, we observed a time period in which eight organizations in six different industries were compromised simultaneously.
- Since 2017, APT41's activities have included a series of supply chain compromises. The operation injects malware into legitimate server software packages used by hundreds of companies worldwide but limits deployment of additional payloads to select targets.

FIGURE 2. Timeline of industries targeted by APT41.

INDUSTRIES TARGETED BY APT 41



# Cyber Espionage Activity

Observed APT41 targeting is consistent with China's national strategies to move production capabilities upmarket into research and development (R&D)-heavy fields. These initiatives were especially highlighted with "Made in China 2025," a plan announced in 2015 that aims to shift China's economy toward higher value products and services, including pharmaceuticals, semiconductors, and other high-tech industries.

- We assess that the targeting of high-tech firms that produce computer components aligns with Chinese interests in domestically developing high-end technologies as outlined in the **12th** (2011) and **13th** (2016) Five-Year plans, as well as the **Made in China 2025** (2015) initiative.
  - Since 2013, APT41 has targeted organizations involved in the research, development, and sale of computer components used for machine-learning, autonomous vehicles, medical imaging, and the consumer market. The group also targeted companies involved in producing motherboards, processors, and server solutions for enterprises.
  - In April 2013, the group targeted an enterprise cloud-computing provider. Developing domestic cloud-computing technologies was a goal in the 12th Five-Year Plan.
  - In a 2014 compromise, APT41 targeted a European conglomerate and specifically focused on systems physically located in China.
- The timing of multiple intrusions attributed to the group indicate a focused interest in strategic business decisions, including entry into the Chinese market, partnerships/M&A, and expansion into other regional markets.
  - In October 2017, an intrusion into a retailer targeted strategic investment plans at the same time as the firm was beginning to negotiate a partnership with a Chinese company (although this potential deal was not publicized).
  - In spring 2015, APT41 targeted information related to two entities undergoing a merger announced the previous year. This included data related to a senior executive, as well as payroll and communications integration issues.

- Since 2017, APT41 has consistently targeted telecommunications companies, possibly a crucial first step to establish a foothold in targeting a particular region.
  - Targeted telecom companies spanned several countries, and recently identified intrusions were concentrated in countries where we had not identified any prior APT41 activity.
  - APT41 has targeted large telecom companies and their subsidiaries in various locations, demonstrating consistent interest in obtaining access to these targets.
  - The group has also repeatedly targeted call record information at telecom companies, supporting indications of their wider intelligence collection efforts.

In addition to specifically targeting industries of strategic value, we suggest that APT41 is also given more tactical assignments, including reconnaissance and identifying dissidents.

- A hotel was targeted two weeks ahead of a diplomatic visit in which high-ranking Chinese officials stayed there. Personal data within the reservations system was directly accessed, suggesting the group was potentially tasked to reconnoiter the facility.
- We assess with moderate confidence that APT41 gathered intelligence on pro-democracy dissidents in Hong Kong based on the targets and timing of operations.