APT41: A Dual Espionage and Cyber Crime Operation

fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html

Today, FireEye Intelligence is releasing a comprehensive report detailing APT41, a prolific Chinese cyber threat group that carries out state-sponsored espionage activity in parallel with financially motivated operations. APT41 is unique among tracked China-based actors in that it leverages non-public malware typically reserved for espionage campaigns in what appears to be activity for personal gain. Explicit financially-motivated targeting is unusual among Chinese state-sponsored threat groups, and evidence suggests APT41 has conducted simultaneous cyber crime and cyber espionage operations from 2014 onward.

The full published report covers historical and ongoing activity attributed to APT41, the evolution of the group's tactics, techniques, and procedures (TTPs), information on the individual actors, an overview of their malware toolset, and how these identifiers overlap with other known Chinese espionage operators. APT41 partially coincides with public reporting on groups including BARIUM (Microsoft) and Winnti (Kaspersky, ESET, Clearsky).

Who Does APT41 Target?

Like other Chinese espionage operators, APT41 espionage targeting has generally aligned with China's Five-Year economic development plans. The group has established and maintained strategic access to organizations in the healthcare, high-tech, and telecommunications sectors. APT41 operations against higher education, travel services, and news/media firms provide some indication that the group also tracks individuals and conducts surveillance. For example, the group has repeatedly targeted call record information at telecom companies. In another instance, APT41 targeted a hotel's reservation systems ahead of Chinese officials staying there, suggesting the group was tasked to reconnoiter the facility for security reasons.

The group's financially motivated activity has primarily focused on the video game industry, where APT41 has manipulated virtual currencies and even attempted to deploy ransomware. The group is adept at moving laterally within targeted networks, including pivoting between Windows and Linux systems, until it can access game production environments. From there, the group steals source code as well as digital certificates which are then used to sign malware. More importantly, APT41 is known to use its access to production environments to inject malicious code into legitimate files which are later distributed to victim organizations. These supply chain compromise tactics have also been characteristic of APT41's best known and most recent espionage campaigns.

Interestingly, despite the significant effort required to execute supply chain compromises and the large number of affected organizations, APT41 limits the deployment of follow-on malware to specific victim systems by matching against individual system identifiers. These multi-stage operations restrict malware delivery only to intended victims and significantly obfuscate the intended targets. In contrast, a typical spear-phishing campaign's desired targeting can be discerned based on recipients' email addresses.

A breakdown of industries directly targeted by APT41 over time can be found in Figure 1.

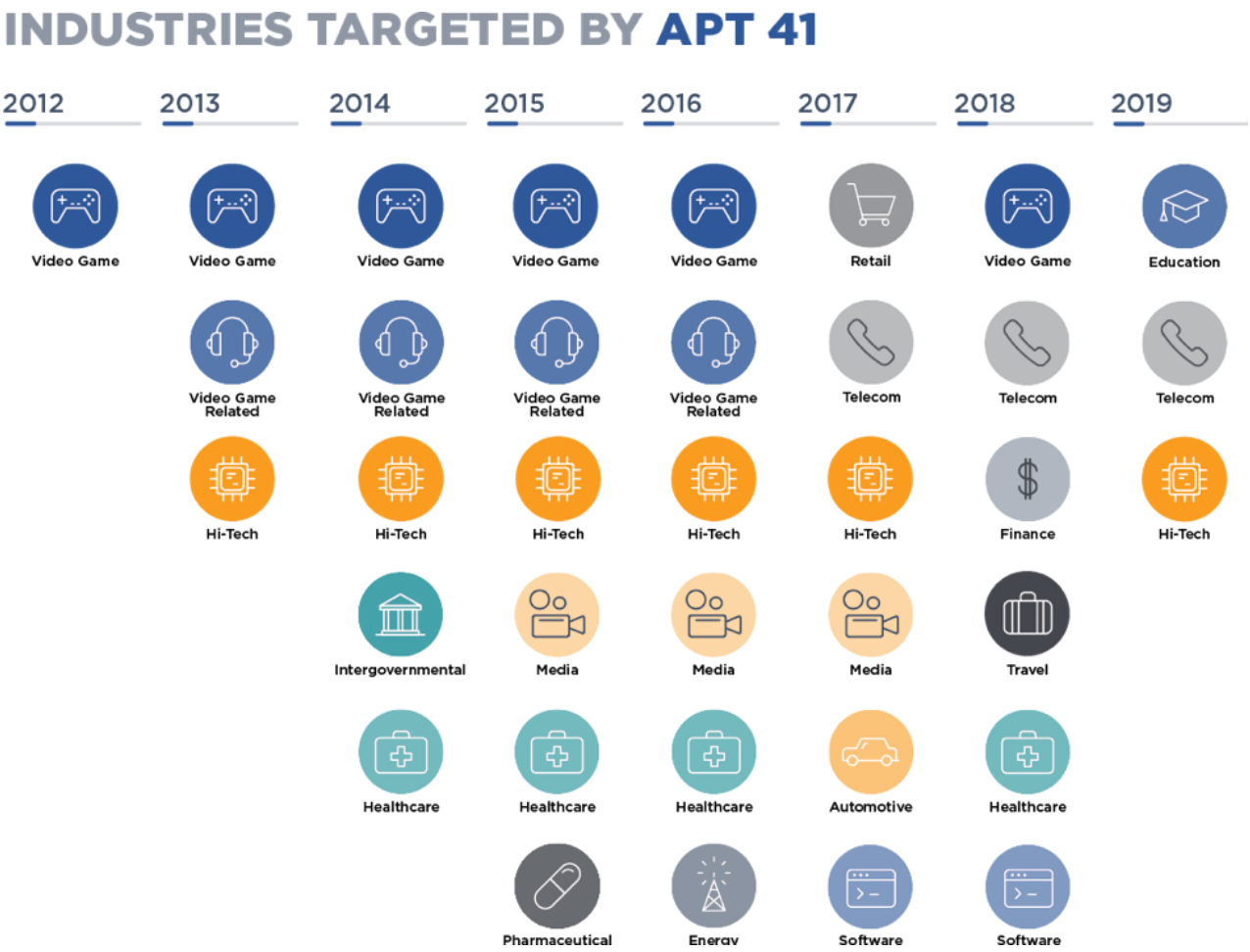

Figure 1: Timeline of industries directly targeted by APT41

Probable Chinese Espionage Contractors

Two identified personas using the monikers “Zhang Xuguang” and “Wolfzhi” linked to APT41 operations have also been identified in Chinese-language forums. These individuals advertised their skills and services and indicated that they could be hired. Zhang listed his online hours as 4:00pm to 6:00am, similar to APT41 operational times against online gaming targets and suggesting that he is moonlighting. Mapping the group’s activities since 2012 (Figure 2) also provides some indication that APT41 primarily conducts financially motivated operations outside of their normal day jobs.

Attribution to these individuals is backed by identified persona information, their previous work and apparent expertise in programming skills, and their targeting of Chinese market-specific online games. The latter is especially notable because APT41 has repeatedly returned to targeting the video game industry and we believe these activities were formative in the group’s later espionage operations.

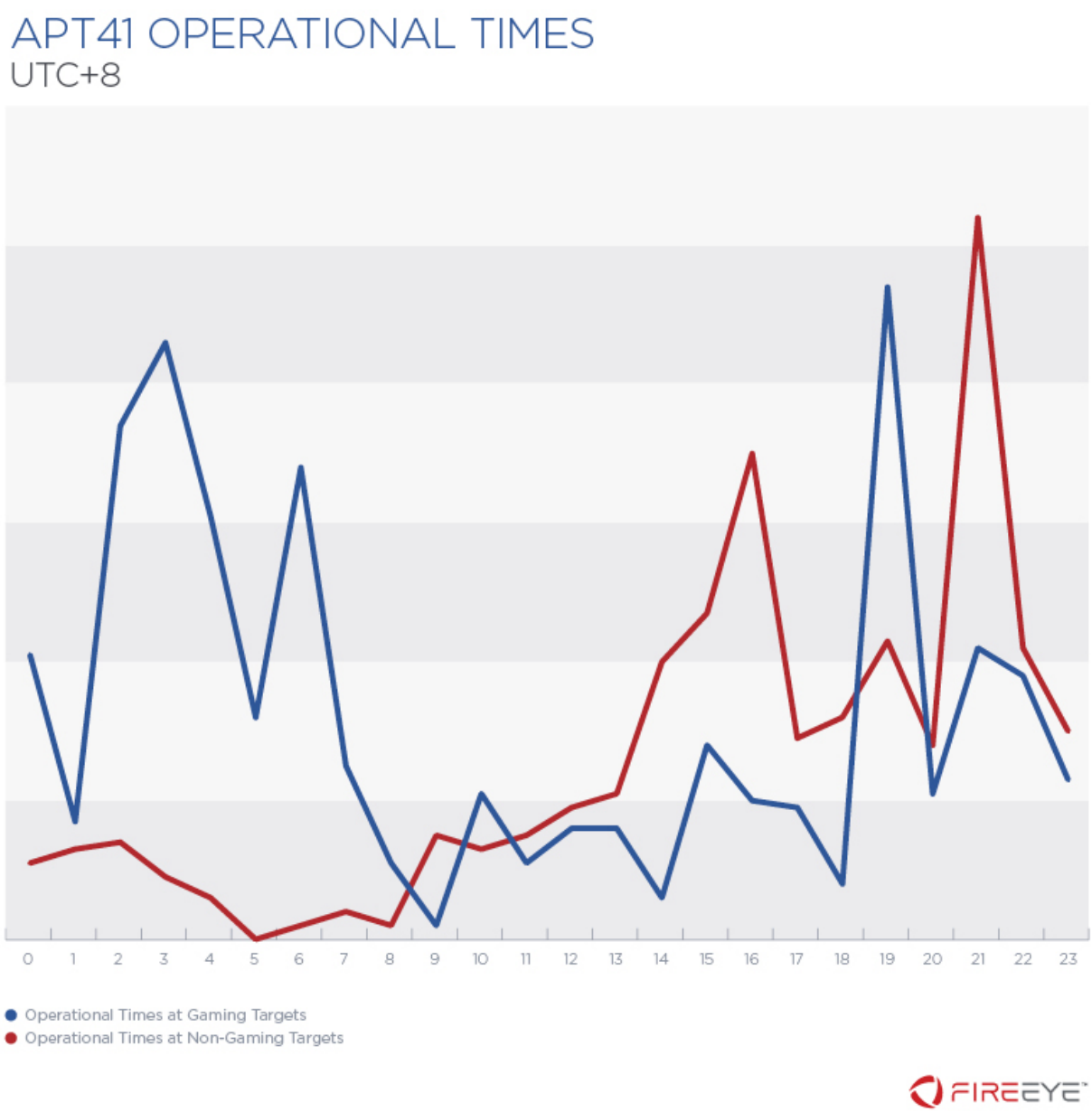

Figure 2: Operational activity for gaming versus non-gaming-related targeting based on observed operations since 2012

The Right Tool for the Job

APT41 leverages an arsenal of over 46 different malware families and tools to accomplish their missions, including publicly available utilities, malware shared with other Chinese espionage operations, and tools unique to the group. The group often relies on spear-phishing emails with attachments such as compiled HTML (.chm) files to initially compromise their victims. Once in a victim organization, APT41 can leverage more sophisticated TTPs and deploy additional malware. For example, in a campaign running almost a year, APT41 compromised hundreds of systems and used close to 150 unique pieces of malware including backdoors, credential stealers, keyloggers, and rootkits.

APT41 has also deployed rootkits and Master Boot Record (MBR) bootkits on a limited basis to hide their malware and maintain persistence on select victim systems. The use of bootkits in particular adds an extra layer of stealth because the code is executed prior to the operating system initializing. The limited use of these tools by APT41 suggests the group reserves more advanced TTPs and malware only for high-value targets.

Fast and Relentless

APT41 quickly identifies and compromises intermediary systems that provide access to otherwise segmented parts of an organization's network. In one case, the group compromised hundreds of systems across multiple network segments and several geographic regions in as little as two weeks.

The group is also highly agile and persistent, responding quickly to changes in victim environments and incident responder activity. Hours after a victimized organization made changes to thwart APT41, for example, the group compiled a new version of a backdoor using a freshly registered command-and-control domain and compromised several systems across multiple geographic regions. In a different instance, APT41 sent spear-phishing emails to multiple HR employees three days after an intrusion had been remediated and systems were brought back online. Within hours of a user opening a malicious attachment sent by APT41, the group had regained a foothold within the organization's servers across multiple geographic regions.

Looking Ahead

APT41 is a creative, skilled, and well-resourced adversary, as highlighted by the operation's distinct use of supply chain compromises to target select individuals, consistent signing of malware using compromised digital certificates, and deployment of bootkits (which is rare among Chinese APT groups).

Like other Chinese espionage operators, APT41 appears to have moved toward strategic intelligence collection and establishing access and away from direct intellectual property theft since 2015. This shift, however, has not affected the group's consistent interest in targeting the video game industry for financially motivated reasons. The group's capabilities and targeting have both broadened over time, signaling the potential for additional supply chain compromises affecting a variety of victims in additional verticals.

APT41's links to both underground marketplaces and state-sponsored activity may indicate the group enjoys protections that enables it to conduct its own for-profit activities, or authorities are willing to overlook them. It is also possible that APT41 has simply evaded scrutiny from Chinese authorities. Regardless, these operations underscore a blurred line between state power and crime that lies at the heart of threat ecosystems and is exemplified by APT41.