FireEye Intel Center
FireEye, Inc. · Security. Reimagined.
1440 McCarthy Blvd · Milpitas, CA 95035

High Tech Threat Trends (Q2 2015)

Date: July 7th, 2015 **Tags:** high tech

High Tech Threat Trends (Q2 2015)

Threat Trends #1: The TRANSPORTER APT Macro (Linked & Attached)

Threat Trends #2: Threat Actors Continue to Leverage Third Party Organizations to Facilitate Intrusion Operations (Linked & Attached)

Threat Horizon: High-Tech Strategic Risk Outlook

FireEye has observed a range of APT groups, including those based in China, Russia, and Iran, target the high-tech sector. This sector is unique for its rapid growth and innovation and introduction of disruptive, even revolutionary technologies. As consumers are empowered to rapidly switch between products and platforms, this further creates incentives for companies to minimize costs and undercut their competitors. These conditions create a strong inducement towards copycatting and IP theft, particularly through cyber espionage.

With China in particular, the high-tech sector is clearly a priority for the Chinese leadership and for China-based APT groups. Beijing's current response to economic pressures and prioritization of innovation will likely continue to drive the procurement, mimicry, and cooption of innovative foreign technologies and products, including through commercial cyber espionage. There are often not sufficient incentives for true innovation, as the payoffs for marginal improvements or 'cloning' Western companies and products remain quite high, while Chinese direct investments abroad allow for "innovation by acquisition." For instance, looking to the three dominant Chinese technology companies: Alibaba is known as China's eBay; Baidu as China's Google; and Sina Weibo as China's Twitter. Chinese tech start-ups have reproduced U.S. tech companies for a domestic Chinese market, including Facebook (Renren), Uber (Didi Dache) and Tumblr (Diandian). Although such mimicry hardly constitutes commercial cyber espionage, there have been

FireEye
COPYRIGHT 2015 FIREEYE

cases when incremental innovation has been facilitated by the activities of APT threat groups.

We expect the following factors to influence threat actors' targeting in the high–tech sector in the next quarter and beyond:

Companies who manufacturer products and services related to surveillance and big data are at increased risk for targeting. Due to the Chinese leadership's rising concerns over maintaining social stability and combatting domestic terrorism, surveillance is a priority. Indeed, spending on domestic security has exceeded the declared defense budget for years. Big data is starting to be used as a tool of surveillance and even to redefine citizenship; the Chinese government plans to establish by 2020 an Orwellian "social credit system" that rates citizens based on their criminal record, financial decisions, and social media behavior.[1]

Other technological developments such as the rise of robotics, artificial intelligence, and the Internet of Things will drive targeting. China has set the goal of leading the world in the Internet of Things[2] earmarking $800 million for investment in the Internet of Things by 2015. "Internet of Things" state-owned enterprise zones have been established nationwide.[3] Chinese companies are investing extensively in advancing artificial intelligence. The CEO of Baidu has called for the development of a national artificial intelligence program to be known as "China Brain" and sought government and military funding.[4]

Although cloud computing in China currently accounts for only 2% of the global market, this is expected to be an area of rapid growth in the years to come, and competition is intensifying. As leading U.S. technology giants seeking to gain a share of the cloud-computing market in China face an environment increasingly suspicious of foreign companies, China's local underdogs, such as Alibaba, have received substantial support from the government and have ambitions of becoming global players in the industry.[5]

High-Tech: Advanced Actor Targeting

The High Tech and Information Technology (IT) sector sees frequent activity from a range of threat actors given the competitive and prominent position organizations in this industry hold in the modern economy. These threats include:

- Advanced persistent threat (APT) groups are motivated to target this industry to conduct economic and scientific espionage. APT actors may steal data and intellectual property to support domestic development, economic efforts, reduce research and development costs, and give domestic

COPYRIGHT 2015 FIREEYE

companies a competitive edge. Organizations that provide services to governments or armed forces are high-priority targets for APT actors, and FireEye frequently observes APT actors steal documents related to this research.
- Financially motivated threat actors target this industry to steal account and financial data (e.g. credentials, payment information) or personal identifiable information that they can sell for profit.
- Threat actors with disruptive motivations, to include hacktivists, may target organizations in this industry that provide Internet services. These threat actors will likely be motivated to disrupt operations to gain publicity for their cause.

For the January-March 2015 timeframe, based on FireEye® Dynamic Threat Intelligence™ (DTI) cloud data, FireEye has assigned a Cybercon™ level of 3 to High Tech, which is considered Moderate.

High Tech Q2 2015 Trend Intelligence (Attached)

- Daily Detection Levels, April - June 2015
- APT Malware Detections by Industry
- Top Non-APT Malware Detections
- APT Detections

Download the Full Q2 Trends Report: HIGH TECH

1 FlorCruz, Michelle. "China To Use Big Data To Rate Citizens In New 'Social Credit System.'" *International Business Times*. April 28, 2015. <http://www.ibtimes.com/china-use-big-data-rate-citizens-new-social-credit-system-1898711>

2 Voigt, Kevin. "China looks to lead the Internet of Things." *CNN*. December 3, 2012. <http://www.cnn.com/2012/11/28/business/china-internet-of-things/>

3 Ibid.

4 Zhang Rui. Baidu CEO proposes national AI project. China.org.cn. March 12, 2015. <http://www.china.org.cn/china/NPC_CPPCC_2015/2015-03/12/content_35030729.htm>

5]Carsten, Paul. "Still an underdog, but China government deals help Alibaba's cloud ambitions." *Reuters*. June 18, 2015. <http://www.reuters.com/article/2015/06/19/us-alibaba-cloud-idUSKBN0OY2TC20150619>

FireEye
COPYRIGHT 2015 FIREEYE

This FireEye Intelligence product contains valuable intellectual property of FireEye and its licensors. Accordingly, use of this content is limited to internal reference, and this FireEye Intelligence product constitutes confidential information of FireEye, subject to your non-disclosure obligations. You may not permit any third party to access this content without express written permission from FireEye. *By clicking OK, you acknowledge your understanding that FireEye Intelligence products contain valuable intellectual property, constitute confidential information of FireEye, and are for internal use only.

Confidential : For Internal Customer Use Only. © 2014 FireEye Corporation. All Rights Reserved.