APT1 Three Months Later – Significantly Impacted, Though Active & Rebuilding

May 21, 2013 | by Dan McWhorter

On 18 February 2013, Mandiant released a report exposing one of China's cyber espionage units. The group, which Mandiant calls APT1, is one of the most prolific we track in terms of the sheer quantity of information it has stolen. The scale and impact of APT1's operations compelled us to write the report and release more than 3,000 Indicators to help organizations defend against APT1's tactics. The report linked APT1 to a unit within China's People's Liberation Army and received widespread attention from the media and from the U.S. government.

Three months later, Mandiant has observed a decrease in APT1's operations. However, we can confirm that APT1 continues cyber espionage operations against targeted computer networks. While Mandiant's APT1 report seems to have affected APT1 operations, APT1 is still active using a well-coordinated and well-defined attack methodology against a wide set of industries -- with a discernible post-report shift towards new tools and infrastructure.

Mandiant's report and the simultaneous release of 3,000+ indicators hindered APT1's operations by causing the group to retool and change some operational methodology. Since the report, APT1 has stopped using the vast majority of the infrastructure that was disclosed with the release of the indicators. However, APT1 maintained an extensive infrastructure of computer systems around the world, and it is highly likely that APT1 still maintains access to those systems or has utilized those systems to establish new attack infrastructure in the last three months.

One thing that has not changed is the activity level of many of the 20+ Advanced Persistent Threat (APT) groups of suspected Chinese origin that Mandiant tracks. These groups are still very active and Mandiant has observed no significant changes in their operations after the release of the APT1 report. These groups also conduct cyber espionage campaigns against a broad range of victims and, based on Mandiant's observations, they were not directly affected by the release of the Mandiant APT1 report.

The discovery and attribution of APT1 to China's 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department (Military Unit Cover Designator 61398) also elevated the public dialogue about cyber espionage and the theft of intellectual property to a level not seen before. President Obama's National Security Advisor, Thomas Donilon, said that cyber espionage has moved to the "forefront" of the US agenda in its relationship with China and called for the Chinese Government to stop the hacking and to join an international process for limiting economic espionage.

Congress is taking action as well. Earlier this month, Senators Levin, McCain, Coburn and Rockefeller introduced S. 884, the Deter Cyber Theft Act, which would require the Government to publish an annual report listing foreign countries that engage in economic espionage and block imports from those countries made with stolen technologies. This bill is designed to be that next step not only to "name and shame" the bad actors but also to punish them economically.

The subject of Chinese attacks, such as those conducted by APT1, seems poised to stay front and center on the diplomatic agenda where, according to the New York Times, it will be a "central issue in an upcoming visit to China by President Obama's national security adviser, Thomas Donilon."

This entry was posted on Tue May 21 17:10 EDT 2013 and filed under Mandiant, Indicator of Compromise, Apt1, Cyber Espionage, NYTimes, Dan McWhorter, and Advanced Persistent Threat.

Get information and insight on today's advanced threats from the leader in advanced threat prevention.

First Name

Last Name

Email Address

Company Name

☐ Threat Research Blog

☐ Products and Services Blog

☐ Executive Perspectives Blog

Company
About FireEye
Customer Stories
Careers
Partners
Investor Relations
Supplier Documents

News and Events
Newsroom
Press Releases
Webinars
Events
Awards and Honors
Email Preferences

Technical Support
Incident?
Report Security Issue
Contact Support
Customer Portal
Communities
Documentation Portal

FireEye Blogs
Threat Research
Products and Services
Executive Perspectives

Threat Map
View the Latest Threats

Contact Us
+1 877-347-3393

Stay Connected