Statement for the Record

Richard Bejtlich
Chief Security Officer
Mandiant Corporation

Before the

U.S. House of Representatives
Committee on Foreign Affairs
Subcommittee on Europe, Eurasia and Emerging Threats.

March 21, 2013

Since 2004, Mandiant has investigated computer security breaches at hundreds of organizations around the world. The majority of these security breaches are attributed to advanced threat actors referred to as the "Advanced Persistent Threat" (APT). We first published details about the APT in our January 2010 M-Trends report. As we stated in the report, our position was that "The Chinese government may authorize this activity, but there's no way to determine the extent of its involvement." Now, three years later, we have the evidence required to change our assessment. The details we have analyzed during hundreds of investigations convince us that the groups conducting these activities are based primarily in China and that the Chinese Government is aware of them.[1]

Mandiant continues to track dozens of APT groups around the world; however, this report is focused on the most prolific of these groups. We refer to this group as "APT1" and it is one of more than 20 APT groups with origins in China. APT1 is a single organization of operators that has conducted a cyber espionage campaign against a broad range of victims since at least 2006. From our observations, it is one of the most prolific cyber espionage groups in terms of the sheer quantity of information stolen. The scale and impact of APT1's operations compelled us to write this report.

The activity we have directly observed likely represents only a small fraction of the cyber espionage that APT1 has conducted. Though our visibility of APT1's activities is incomplete, we have analyzed the group's intrusions against nearly 150 victims over seven years. From our unique vantage point responding to victims, we tracked APT1 back to four large networks in Shanghai, two of which are allocated directly to the Pudong New Area. We uncovered a substantial amount of APT1's attack infrastructure, command and control, and modus operandi (tools, tactics, and procedures). In an effort to underscore there are actual individuals behind the keyboard, Mandiant is revealing three personas we have attributed to APT1. These operators, like soldiers, may merely be following orders given to them by others.

Our analysis has led us to conclude that APT1 is likely government-sponsored and one of the most persistent of China's cyber threat actors. We believe that APT1 is able to wage such a long-running and extensive cyber espionage campaign in large part because it receives direct government support. In seeking to identify the organization behind this activity, our research found that People's Liberation Army (PLA's) Unit 61398 is similar to APT1 in its mission, capabilities, and resources. PLA Unit 61398 is also located in precisely the same area from which APT1 activity appears to originate.

[1] Our conclusions are based exclusively on unclassified, open source information derived from Mandiant observations. None of the information in this report involves access to or confirmation by classified intelligence.

Key Findings

APT1 is believed to be the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department (总参三部二局), which is most commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398 (61398部队).

»» The nature of "Unit 61398's" work is considered by China to be a state secret; however, we believe it engages in harmful "Computer Network Operations."

»» Unit 61398 is partially situated on Datong Road (大同路) in Gaoqiaozhen (高桥镇), which is located in the Pudong New Area (浦东新区) of Shanghai (上海). The central building in this compound is a 130,663 square foot facility that is 12 stories high and was built in early 2007.

»» We estimate that Unit 61398 is staffed by hundreds, and perhaps thousands of people based on the size of Unit 61398's physical infrastructure.

»» China Telecom provided special fiber optic communications infrastructure for the unit in the name of national defense.

»» Unit 61398 requires its personnel to be trained in computer security and computer network operations and also requires its personnel to be proficient in the English language.

»» Mandiant has traced APT1's activity to four large networks in Shanghai, two of which serve the Pudong New Area where Unit 61398 is based.

APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously.[2]

»» Since 2006, Mandiant has observed APT1 compromise 141 companies spanning 20 major industries.

»» APT1 has a well-defined attack methodology, honed over years and designed to steal large volumes of valuable intellectual property.

»» Once APT1 has established access, they periodically revisit the victim's network over several months or years and steal broad categories of intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing

[2] We believe that the extensive activity we have directly observed represents only a small fraction of the cyber espionage that APT1 has conducted. Therefore, Mandiant is establishing the lower bounds of APT1activities in this report.

documents, partnership agreements, and emails and contact lists from victim organizations' leadership.

»» APT1 uses some tools and techniques that we have not yet observed being used by other groups including two utilities designed to steal email — GETMAIL and MAPIGET.

»» APT1 maintained access to victim networks for an average of 356 days.[3] The longest time period APT1 maintained access to a victim's network was 1,764 days, or four years and ten months.

»» Among other large-scale thefts of intellectual property, we have observed APT1 stealing 6.5 terabytes of compressed data from a single organization over a ten-month time period.

»» In the first month of 2011, APT1 successfully compromised at least 17 new victims operating in 10 different industries.

APT1 focuses on compromising organizations across a broad range of industries in English-speaking countries.

»» Of the 141 APT1 victims, 87% of them are headquartered in countries where English is the native language.

»» The industries APT1 targets match industries that China has identified as strategic to their growth, including four of the seven strategic emerging industries that China identified in its 12th Five Year Plan.

APT1 maintains an extensive infrastructure of computer systems around the world.

»» APT1 controls thousands of systems in support of their computer intrusion activities.

»» In the last two years we have observed APT1 establish a minimum of 937 Command and Control (C2) servers hosted on 849 distinct IP addresses in 13 countries. The majority of these 849 unique IP addresses were registered to organizations in China (709), followed by the U.S. (109).

»» In the last three years we have observed APT1 use fully qualified domain names (FQDNs) resolving to 988 unique IP addresses.

[3] This is based on 91 of the 141 victim organizations. In the remaining cases, APT1 activity is either ongoing or else we do not have visibility into the last known date of APT1 activity in the network.

»» Over a two-year period (January 2011 to January 2013) we confirmed 1,905 instances of APT1 actors logging into their attack infrastructure from 832 different IP addresses with Remote Desktop, a tool that provides a remote user with an interactive graphical interface to a system.

»» In the last several years we have confirmed 2,551 FQDNs attributed to APT1. In over 97% of the 1,905 times Mandiant observed APT1 intruders connecting to their attack infrastructure, APT1 used IP addresses registered in Shanghai and systems set to use the Simplified Chinese language.

»» In 1,849 of the 1,905 (97%) of the Remote Desktop sessions APT1 conducted under our observation, the APT1 operator's keyboard layout setting was "Chinese (Simplified) — US Keyboard". Microsoft's Remote Desktop client configures this setting automatically based on the selected language on the client system. Therefore, the APT1 attackers likely have their Microsoft® operating system configured to display Simplified Chinese fonts.

»» 817 of the 832 (98%) IP addresses logging into APT1 controlled systems using Remote Desktop resolved back to China.

»» We observed 767 separate instances in which APT1 intruders used the "HUC Packet Transmit Tool" or HTRAN to communicate between 614 distinct routable IP addresses and their victims' systems using their attack infrastructure. Of the 614 distinct IP addresses used for HTRAN communications:

- 614 of 614 (100%) were registered in China.
- 613 (99.8%) were registered to one of four Shanghai net blocks.

The size of APT1's infrastructure implies a large organization with at least dozens, but potentially hundreds of human operators.

»» We conservatively estimate that APT1's current attack infrastructure includes over 1,000 servers.

»» Given the volume, duration and type of attack activity we have observed, APT1 operators would need to be directly supported by linguists, open source researchers, malware authors, industry experts who translate task requests from requestors to the operators, and people who then transmit stolen information to the requestors.

»» APT1 would also need a sizable IT staff dedicated to acquiring and maintaining computer equipment, people who handle finances, facility management, and logistics (e.g., shipping).

In an effort to underscore that there are actual individuals behind the keyboard, Mandiant is revealing three personas that are associated with APT1 activity.

»» The first persona, “UglyGorilla”, has been active in computer network operations since October 2004. His activities include registering domains attributed to APT1 and authoring malware used in APT1 campaigns. “UglyGorilla” publicly expressed his interest in China’s “cyber troops” in January 2004.

»» The second persona, an actor we call “DOTA ”, has registered dozens of email accounts used to conduct social engineering and spear phishing attacks in support of APT1 campaigns. “DOTA” used a Shanghai phone number while registering these accounts.

»» We have observed both the “UglyGorilla” persona and the “DOTA ” persona using the same shared infrastructure, including FQDNs and IP ranges that we have attributed to APT1.

»» The third persona, who uses the nickname “SuperHard,” is the creator or a significant contributor to the AURIGA and BANGAT malware families which we have observed APT1 and other APT groups use. “SuperHard” discloses his location to be the Pudong New Area of Shanghai.

Mandiant is releasing more than 3,000 indicators to bolster defenses against APT1 operations.

»» Specifically, Mandiant is providing the following:

- –– Digital delivery of over 3,000 APT1 indicators, such as domain names, IP addresses, and MD5 hashes of malware.
- –– Sample Indicators of Compromise (IOCs) and detailed descriptions of over 40 families of malware in APT1’s arsenal of digital weapons.
- –– Thirteen (13) X.509 encryption certificates used by APT1.
- –– A compilation of videos showing actual attacker sessions and their intrusion activities.

»» While existing customers of Mandiant’s enterprise-level products, Mandiant Managed Defense and Mandiant Intelligent Response®, have had prior access to these APT1 Indicators, we are also making them available for use with Redline™, our free host-based investigative tool. Redline can be downloaded at www.mandiant.com/resources/download/redline.

The sheer scale and duration of sustained attacks against such a wide set of industries from a singularly identified group based in China leaves little doubt about the organization behind APT1. We believe the totality of the evidence we provide in this document bolsters the claim that APT1 is Unit 61398. However, we admit there is one other unlikely possibility:

> A secret, resourced organization full of mainland Chinese speakers with direct access to Shanghai-based telecommunications infrastructure is engaged in a multi-year, enterprise scale computer espionage campaign right outside of Unit 61398's gates, performing tasks similar to Unit 61398's known mission.

Why We Are Exposing APT1

The decision to publish a significant part of our intelligence about Unit 61398 was a painstaking one. What started as a "what if" discussion about our traditional nondisclosure policy quickly turned into the realization that the positive impact resulting from our decision to expose APT1 outweighed the risk to our ability to collect intelligence on this particular APT group. It is time to acknowledge the threat is originating in China, and we wanted to do our part to arm and prepare security professionals to combat that threat effectively. The issue of attribution has always been a missing link in publicly understanding the landscape of APT cyber espionage. Without establishing a solid connection to China, there will always be room for observers to dismiss APT actions as uncoordinated, solely criminal in nature, or peripheral to larger national security and global economic concerns. We hope that this report will lead to increased understanding and coordinated action in countering APT network breaches.

At the same time, there are downsides to publishing all of this information publicly. Many of the techniques and technologies described in this report are vastly more effective when attackers are not aware of them. Additionally, publishing certain kinds of indicators dramatically shortens their lifespan. When Unit 61398 changes their techniques after reading this report, they will undoubtedly force us to work harder to continue tracking them with such accuracy. It is our sincere hope, however, that this report can temporarily increase the costs of Unit 61398's operations and impede their progress in a meaningful way.

We are acutely aware of the risk this report poses for us. We expect reprisals from China as well as an onslaught of criticism.