Statement for the Record

Richard Bejtlich
Chief Security Officer
Mandiant Corporation

Before the

U.S. House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies

March 20, 2013

Thank you, Chairman Meehan, Ranking member Clarke and members of the subcommittee, for inviting me to discuss threats to our nation's computer networks. My name is Richard Bejtlich and I am the Chief Security Officer (CSO) at Mandiant. As CSO, part of my role is to understand the threats affecting Mandiant and our customers. I developed these skills as a military intelligence officer with the Air Force Computer Emergency Response Team and as director of the Computer Incident Response Team for General Electric, where I helped defend over 300,000 employees and more than half a million computers.

Mandiant protects the assets of the world's most respected organizations from digital intruders. In addition to responding to high-profile computer security incidents, such as the New York Times, we equip security organizations with the tools, intelligence and expertise required to find and stop attackers who would otherwise roam freely on their networks. We serve more than 30% of the Fortune 100. As I sit here Mandiant is responding to dozens of computer security incidents while our products protect hundreds more organizations from targeted attackers.

We have investigated millions of systems, and we receive calls almost every single day from companies that have suffered a cyber-security breach. These intrusions affect many industries, including law firms, financial services, manufacturers, retailers, the defense industrial base, telecommunications, space and satellite and imagery, cryptography and communications, government, mining, software and many others.

It is reasonable to assume that, if an advanced attacker targets a particular company, a breach is inevitable. That surprises many people, but it is the result of the gap between our ability to defend ourselves and our adversaries' ability to circumvent those defenses. There are at least six reasons why attackers continue to successfully exploit this gap in security:

First, the sophisticated, cutting-edge attacks that were previously reserved solely for government targets have spread to the private sector. Many American corporations, even if they are compliant with appropriate cyber-security regulations and best practices, are not prepared for these advanced threats.

Second, the attackers are targeting people, not computers. While previous generations of attacks targeted technology and exploited vulnerabilities in software, attackers now target human weaknesses. These attacks focus on individuals and leverage personal information the victim made public via social media. These personalized attacks can be difficult to detect and prevent because they exploit human vulnerabilities and trust.

Third, more attacks are coming from the "inside." It is common to see attackers compromise smaller companies with fewer security resources, and then "upgrade" their access from the trusted, smaller companies to the main target. This problem also occurs when large businesses "acquire" infected networks through a corporate merger or acquisition of a smaller company.

The fourth reason a security gap exists involves an imbalance between offense and defense. A single attacker can generate work for hundreds, if not thousands of defenders. A lone attacker need only breach his target's defenses once to accomplish his goals, but the victim must try to prevent 100% of the attacks. This imbalance is compounded by the critical shortage of skilled security professionals here in the U.S.

Fifth, many advanced attackers reside in nations that not only refuse to hold attackers accountable for their actions, but also provide resources and direction to the attackers. So long as state-sponsored criminals can infiltrate American networks and steal American intellectual property without risks or repercussions, these attacks will continue unabated.

Mandiant documented one example of this threat in our APT1 report, released on February 19, 2013. We identified the Chinese cyber espionage unit we call Advanced Persistent Threat 1. We assess APT1 to be Unit 61398, a military hacking unit inside the People's Liberation Army. Unit 61398 is one of approximately 20 groups targeting intellectual property from companies around the world that we assess as operating out of China. Unit 61398 is a single operation 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 sheer quantity of information stolen. While it seems clear that Unit 61398 is headquartered in Shanghai, it should be stated that Mandiant tracks dozens of APT groups and not all of them originate in China.

Finally, one of the most valuable resources in detecting and responding to cyber-attacks – accurate and timely threat intelligence – is often unavailable to many defenders. Even if defenders have threat intelligence, the means to share it are cumbersome and manual. The U.S. needs an effective framework for sharing information among commercial entities, and between corporate America and the government.

Because of these six factors, corporate America continues to be routinely compromised. However, there are steps we can take to significantly narrow the security gap and increase the costs and effort required to steal our intellectual capital.

First, the government should promote policies that encourage sharing threat intelligence between the private sector and government, and among private sector entities. Threat intelligence does not contain personal information of American citizens and privacy can be maintained while learning about threats. Intelligence should be published in an automated, machine-consumable, standardized manner. Current systems rely on exchanging emails with documents that people must read and transcribe. Mandiant's free OpenIOC standard is one example of a way to codify and exchange threat intelligence.

Second, the government should support and expand programs whereby law enforcement agencies notify private sector victims of compromise. Mandiant's recent 2013 M-Trends report shows that only a third of advanced intrusion victims discover breaches on their own. Two-thirds of the time, an external

entity, such as the FBI, tells the victim that a foreign entity has stolen their data. External notification is a powerful tool to counter cyber thieves.

Third, the government should encourage governments hosting or sponsoring the most egregious cyber spies to reduce their activity to internationally acceptable norms. All governments spy to some degree, but they should not target and overwhelm private sector companies, organizations, and individuals. Countering digital threats is challenging, but adopting these three recommendations will help reduce the security gap. I look forward to your questions.

Thank you, Mr. Chairman.