WRITTEN TESTIMONY OF

MANDIANT®

KEVIN MANDIA
CHIEF EXECUTIVE OFFICER
MANDIANT CORPORATION

BEFORE THE

SUBCOMMITTEE ON CRIME AND TERRORISM
JUDICIARY COMMITTEE
UNITED STATES SENATE

May 8, 2013

Introduction

Thank you Mr. Chairman, Ranking Member Graham, and Members of the Subcommittee, for this opportunity to share my observations and experience with you. As requested I am going to discuss three things: 1) the nature of the cyber threats facing American businesses; 2) the measures being taken by organizations to counter these threats; and 3) what law enforcement can do to help organizations protect themselves and their corporate secrets.

Today, and into the foreseeable future, American companies will face a motivated, technically sophisticated, and well-resourced adversary intent on depriving businesses of their wealth and intellectual property. While many organizations are actively trying to counter these threats, there currently exists a sizeable gap between what their safeguards can prevent and the ability of motivated attackers to circumvent those safeguards.

Narrowing this security gap is where law enforcement can best assist American businesses. The FBI and other agencies can provide an early warning system, informing businesses when they have been compromised by these motivated adversaries. Law enforcement and other agencies can also share actionable intelligence about cyber-threats that can help companies prevent or detect compromises on their own. While these actions cannot stop each and every cyber security breach, they are essential to suppressing the impact and consequences of the security breaches that will occur.

Background

Following several years as a Computer Security Specialist and an agent in the Air Force Office of Special Investigations, I founded Mandiant in 2004 to offer private sector companies the ability to respond effectively to emerging cyber threats. In addition to running Mandiant, I have had the honor of training FBI agents in cybersecurity investigations in an ongoing capacity for nearly 15 years. As I testify here today, Mandiant employees are on the front lines of the cyber battle, responding to active computer intrusions at dozens of the largest American companies and other organizations important to our nation, including attacks at the *New York Times* and the *Washington Post*.

Mandiant has responded to incidents at hundreds of companies. We have investigated millions of systems, and we receive calls almost every single day from companies that have suffered a cyber-security breach. These cyber intrusions continue to impact virtually every industry, including law firms, financial services, blue chip American manufacturers, retailers, the defense industrial base, telecommunications, space and satellite and imagery, cryptography and communications, government, mining, software and many others. I have witnessed the unique threats facing each of these sectors, and continue to help companies respond to these advanced cyber threats.

What are the Threats?

Cybersecurity professionals are aware that criminals and government operators are using the Internet to compromise American businesses. These intruders are able to steal both wealth and the means of generating wealth by exfiltrating the intellectual property and strategic business information that will drive commerce into the future. As General Keith Alexander noted last year, the loss of information and intellectual property through cybercrime and espionage constitutes the "greatest transfer of wealth in history."

In accessing these networks, our adversaries have the ability not to just steal our wealth, ideas and information, but they could also have a physical impact on our lives. Deleting valuable information, manipulating industrial control systems or introducing false data into a system could result in death or the destruction of property felt far beyond the loss of a bank account, patent application or corporate secrets.

Through my experience in combating cyber threats, I have seen firsthand the methods attackers use as they seek to undermine and exploit our nation's infrastructure. Simply put, these sophisticated threats have evolved faster than our ability or willingness to reliably safeguard our assets.

Most American organizations can secure their networks from "consumer-grade" threats by adhering to industry standards and best practices. From a technical perspective, these attacks are conducted using exploits and techniques that are relatively well known and preventable. These attacks are usually not advanced enough to exploit the gap in our security.

Today, I focus instead on the advanced threats that we are not preventing or detecting. It is reasonable to assume that, if an advanced attacker targets your company, a breach is inevitable. That surprises many people, but it is the undeniable truth, and a direct 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. Advanced threat actors have shifted the application of their sophisticated tools, tactics and procedures from U.S. government targets to corporate America. Many American companies, even if they are compliant with cyber-security regulations and best practices, are not prepared for these advanced threats.

An example of an advanced threat actor targeting American businesses is a group Mandiant refers to as APT1. Mandiant has identified APT1 as Unit 61398, or the 2nd Bureau of China's People's Liberation Army General Staff Department's 3rd Department. Unit 61398 has targeted thousands of English speaking businesses from various sectors of the economy around the world -- the majority right here in the United States.

The second reason attackers are able to successful exploit the security gap is that they are targeting people, not computer systems. While previous generations of attacks targeted technology and exploited vulnerabilities in software, attackers have now evolved to target human inadequacies and weaknesses. As Americans increasingly rely on the Internet, invest more in their online identities and continue to pour their personal details into online blogs and sites such as Facebook, Google+, LinkedIn and Twitter, attackers are able to target their attacks at individuals using the detailed, personal information they themselves make available. These personalized attacks are difficult to detect and prevent because they exploit two things that are difficult to secure: human vulnerabilities and human trust.

Mandiant documented this tactic in its recent report on APT1. In that report, Mandiant demonstrated that APT1's operatives were recruited for their proficiency in English in order to target English-speaking personnel at target companies. APT1 initiate attacks by researching specific individuals online in order to send a seemingly legitimate email, but the fake or spoofed email would contain malware embedded in attachment that appeared innocuous. When opened, the attachment launches the malware that creates a foothold for APT1 operatives to leverage access to the entire network.

Third, more attacks are coming from the "inside." Advanced attackers consistently leverage the pre-existing infrastructure of compromised networks in the United States to target and attack new companies. We frequently see attackers compromise smaller companies with fewer security resources, and then "upgrade" their access from those trusted, smaller companies to the main target. This is also a problem where large businesses "acquire" the infected networks through a corporate merger or acquisition of these smaller enterprises.

The fourth reason attacks continue to be successful involves the imbalanced nature of cyber-attacks and the number of defenders in the U.S. A single attacker can generate work for hundreds, if not thousands of defenders. Also, while a single attacker need only breach his target's defenses once to accomplish his goals, the victim company's entire cyber security staff must attempt to prevent 100% of the threats. 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 crimes, but provide resources and direction to the attackers. As long as state-sponsored criminals can infiltrate American networks and steal American intellectual property without risks or repercussions, these attacks will continue unabated. As if to prove that point, APT1 continues to operate even after being exposed in Mandiant's recent report.

Finally, one of the most valuable resources in detecting and responding to cyber-attacks – accurate and timely threat information – is often unavailable to many defenders. The U.S. needs an effective framework for sharing information among commercial entities, and between corporate America and the government. Too often attackers are finding success using resources and methods that are known by some, but have not been shared with potential victims because of a lack of authority and mechanisms to accomplish the communication.

What are Organizations Doing about the Threat?

As a result of the above six factors, corporate America continues to be routinely compromised by the advanced adversaries. Although it sounds dramatic, it is generally true that there are two sorts of businesses: those that know they have been compromised, and those that have been compromised but just do not know it yet.

Most of those organizations that are aware of the threats are taking the challenge seriously. They are buying technologies that are effective against the consumer-grade threats, especially if appropriately configured and operated by trained and conscientious professionals. The majority of the products available today, however, are less effective against the more sophisticated threats, and are significantly less effective if not operated by professionals trained to identify and appropriately scope the inevitable breaches.

Many organizations that do not yet understand the threat facing businesses today still attempt to implement some level of security through a compliance program. Though having compliance standards that align industry efforts provides important guidance, it often results in organizations concluding that compliance is "good enough," or that their efforts will eliminate the security gap. That is simply not the case.

Companies that are the most effective in dealing with advanced threat actors are those that employ appropriate technology correctly, and bolster that technology with skilled experts trained in identifying network compromises, tracking the adversary, and containing their activity.

What can the FBI do to Assist?

It is the law enforcement's job to protect Americans, be they individuals, businesses or government agencies. The FBI already conducts outreach to American companies who have been compromised by advanced threat groups. Indeed, about two-thirds of the breaches Mandiant responds to are first detected by a third party – usually the FBI or another law enforcement agency – not the victim companies. That means that a majority of the companies we assist had no idea they had been compromised until law enforcement or a business partner notified them.

The significance of that number cannot be overstated. With virtually every other crime, the victim is the first to know that they have been violated. Here, however, we have the government in the unique position of informing victims that they are, in fact, victims. Actionable information, if shared quickly and consistently, could be used to prevent or mitigate the impact of these breaches instead of merely notifying victims long after their intellectual property has been stolen.

Speed is critical to the effective mitigation of a compromise by an advanced threat actor. Once a foothold has been established, the infiltrator must conduct network reconnaissance in order to either upgrade his credentials or find data valuable enough to steal. This reconnaissance takes time, and, if appropriate action is taken during this time, the adversary can be thwarted with minimal impact to the victim. Increased speed of notification to victims provides them a chance at mitigation as opposed to just evaluating the impact of the compromise and the value lost to the adversary. Although we cannot eliminate every security breach, speed allows us to suppress the impact and consequences of the breach.

The FBI is uniquely positioned to be an early warning system for compromised organizations. Due to its tremendous top-down visibility into domestic networks, the FBI could increase the scale and speed at which it notifies victim companies. While speed of notification is critical, any additional actionable information shared with the victim makes containing the adversary faster and easier. A simple dossier including observed IP addresses and tactics used by the adversary allows the victim to quickly observe and orient on the malicious activity and appropriately contain the damage. Machine-readable intelligence, in a format such as Mandiant's OpenIOC, would be even more actionable.

The sharing of actionable threat information will narrow the security gap facing businesses today. Government, including law enforcement, and some companies have this actionable intelligence. We need to create a way in which they can share this information in a standard, codified, machine-readable way that does not betray or diminish the effectiveness of our national security or law enforcement missions, or significantly impact our privacy and civil rights. If we do it right, sharing threat information will promote an aggressive, dynamic “learning system” of cyber-security for the nation. Effective information sharing:

1 – Acts as an early warning system giving potential victims advance notice of significant threats;
2 – Promotes technologies that facilitate the effective use of threat information;
3 – Empowers the private sector to defend itself more effectively; and
4 – Significantly reduces the duration and impact of breaches, should they occur.

The private sector cannot do this alone. While many industry players have extremely capable security programs, the majority of threat information is currently in the hands of the government.

Conclusion

While private industry will not always win the battles being fought in cyberspace, we can drastically narrow the security gap by sharing actionable intelligence and enabling law enforcement to act as an early warning system. By establishing a system where law enforcement and the private sector share and proactively use accurate and timely threat information, America will build a dynamic cyber-defense system that grows smarter and more capable by the day.

Thank you very much, Mr. Chairman.