Testimony of Jennifer Kolde
Technical Director, Threat Intelligence – FireEye, Inc.
Before the
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
Hearing on Emerging Cyber Threat to the United States
February 25, 2016

Mr. Chairman, Ranking Member Richmond, and members of the Subcommittee, thank you for the opportunity to contribute to today's hearing. I am the Lead Technical Director for Threat Intelligence at FireEye, a private company that provides software and services to detect and respond to digital intrusions. My testimony draws on our company's substantial experience remediating the most devastating breaches around the world by nation-state threat actors and cyber criminals and our advanced sensor network that protects our clients every day.

I have spent nearly twenty years in the information technology and information security fields, in roles from systems administration to network security to computer forensics and incident investigation. My experience includes five years as a computer scientist with the Federal Bureau of Investigation in support of cyber national security investigations. Following my government service, I joined Mandiant—later acquired by FireEye—to help protect the private sector.

FireEye learns about the threat landscape through a unique combination of sources and methods:

- Our security consulting practice,
- Our global network of more than ten million sensors, and
- A worldwide team of intelligence analysts.

Our consulting division, Mandiant, investigates and remediates the world's most devastating breaches; FireEye's endpoint and network sensors feed data to a repository of active cyber threat operations; and newly-acquired iSIGHT Partners offers unparalleled analytic insight. We use this robust set of data to correlate threat activity and characterize threat actors' capabilities and motivations. This combination of visibility and resources puts FireEye in a unique position to observe and analyze threat activity across a range of countries, industries, and customers, and to gain insight into adversarial operations during, after, and in some cases before an attack. I would like to describe the changing threat landscape as we see it.

Threat Actors

I have spent nearly ten years identifying and tracking sophisticated threat groups, both within the government and the private sector. During that time I have watched the number of adversaries increase and their methods change dramatically. FireEye now tracks approximately 500 threat groups, including 29 advanced persistent threat (APT)[1] groups that we strongly suspect are supported by governments. Other tracked groups include criminals operating for financial gain, as well as others where we currently have insufficient information to characterize their activity.

[1] Advanced Persistent Threat (APT) actors are assessed to take direction from a nation-state to steal information or conduct network attacks, tenaciously pursue their objectives, and are capable of using a range of tools and tactics.

This multitude of threat actors—suspected government actors and enterprise cyber criminals alike—continues to evolve more quickly than the ability of the private sector to safeguard assets, including financial data, personal health information, and intellectual property.

Governments

FireEye has regularly observed cyber threat activity from individuals we believe are sponsored by government agencies. While China has always been a prominent player in this area, in recent years we have seen additional threats from countries including Russia, Iran, North Korea, and Syria. This is likely due both to increased visibility into these threats, as well as an actual uptick in activity as nations attempt to increase and refine their capabilities in the cyber realm.

China

China-based groups have historically been the most prolific threat actors we observed in terms of the number of distinct threat groups and the number of victim organizations. The agreement reached in September between Chinese President Xi Jinping and President Barack Obama to restrict commercial cyber espionage has the potential to significantly realign the threat landscape. FireEye continues to monitor known and suspected activity from China-based groups, but we believe it is still too early to draw definitive conclusions about China's compliance or lack thereof with the agreement and how or whether China may change its operations. At a minimum, we assess that China will continue to engage in cyber espionage against the United States to obtain political and foreign policy information, to gain insight into the US activities of activists and religious and ethnic minorities advocating change in China, and possibly to acquire security-related information from private companies with a clear tie to national defense.

Russia

Russia has become increasingly aggressive over the past few years, both geopolitically and in cyber space. Russia has always held a reputation as a skilled and stealthy cyber opponent, but recently their activities have been more widely exposed and discussed, including by FireEye in our reporting on groups we call APT28 and APT29. Despite ongoing publicity surrounding their tools and operations, we have seen no significant drop in their activity. APT28 has used zero-day exploits and spear phishing to aggressively pursue military and political secrets in the United States, Europe, the Middle East, and the Asia-Pacific region. APT29, which we have observed through incident response engagements, proved to be a skilled and adaptable opponent. Many groups will go silent or abandon victim networks when discovered. However, in this case APT29 battled to retain control of the environment using speed and scale that would outmatch all but the most skilled and advanced network defenders.

Russia also appears to use its cyber skills in support of real-world military or information warfare operations. Examples include suspicions that Russian state-sponsored hackers were behind December 2015 power outages in the Ukraine, as well as a suspected "false flag" operation by APT28: while purportedly a pro-Jihadist activist group calling themselves the "CyberCaliphate" was responsible for an attack on French media outlet TV5Monde in April 2015, technical indicators suggest that APT28 was actually responsible.

Iran and North Korea

Iran and North Korea are more recent players on the stage, though what they currently lack in capability and sophistication they have been willing to make up for in brazenness. Both have demonstrated the intent and willingness to employ disruptive operations through denial of service or destructive malware—Iran purportedly overwriting data on thousands of computers at Saudi Aramco in 2012, and North Korea in a similar attack on Sony Pictures Entertainment in 2014.

To date, neither Iran nor North Korea has matched the scope of operations or level of sophistication seen by countries such as China or Russia. Iran is believed to have targeted US defense companies, politicians and policy makers, as well as political dissidents and reporters or members of the media. These types of attacks were documented in FireEye's report on "Operation Saffron Rose" and in the iSIGHT Partners—now part of FireEye—report on the "Newscaster" activity.

Both Iran and North Korea have been successful despite relative isolation from the global computer security community. Iranian attackers have custom tools including some made by domestic security companies, but they also use publicly available tools. Iranian threat groups frequently rely on spear phishing and social engineering techniques to trick victims into installing malware or providing usernames and passwords to fake login sites, as opposed to leveraging exploits to compromise computers.

Interestingly, as Iran and North Korea attempt to increase their capabilities in the cyber realm, they appear to be taking lessons not only in tools and techniques, but also in stealth and "false flag" operations. Iran has frequently leveraged social media, creating fake profiles used to connect with targets to learn about victims' movements, activities, and other connections. Several operations believed to have been carried out by North Korea were executed to appear to be the responsibility of hacktivists or patriotic hackers.

Cyber Criminals

Cyber crime continues to be a concern, impacting individual citizens through identity theft and corporations through large-scale financial fraud and associated costs, including network remediation and reissuance of payment cards. Theft of payment card data continues unabated, with merchants of all sizes affected. However, as the value of payment card and bank account data decreases in the criminal underground, cyber criminals are becoming more innovative in their methods to steal and monetize organizations' information. For example, FireEye identified criminal activity in 2014, carried out by a group we call FIN4, where that group stole insider information from pharmaceutical, healthcare, and consulting companies to gain a competitive advantage in capital markets in the U.S.

We are also seeing a rise in the use of ransomware—malware that encrypts the victim's data, requiring them to pay a ransom to the cyber criminal to "unlock" or decrypt their information. Criminals originally used ransomware targeted at individual computers to charge small unlocking fees, but we are now seeing criminals target organizations with more sizeable extortion demands to restore encrypted corporate data. These types of attacks could have significant impact if carried out against organizations that provide essential services or support critical infrastructure, including agencies and departments in the US government.

Beyond ransomware, criminals may take a cue from recent nation-state activity, and conduct extortion not merely by encrypting data, but by threatening to destroy computers or expose sensitive company data. The Sony Pictures incident, where both techniques were used, played out very publicly and very effectively for the attackers. Given law enforcement's limited ability to identify and prosecute perpetrators outside their borders or otherwise impose meaningful consequences, criminals may be emboldened to raise the stakes in exchange for a higher ransom.

Terrorists

To date, FireEye has observed very little cyber activity that we would directly attribute to terrorist groups. Most of the cyber activity from groups claiming affiliation with terrorist organizations, including groups claiming affiliation with the Islamic State, has been unsophisticated. Our company does not monitor terrorist social media use, but we assess these groups are using social networks to recruit individuals with advanced cyber skills. Other potential recruitment targets would include insiders who could facilitate cyber operations, based on the behavior of cybercrime groups who assemble their teams this way.

Terrorists are likely to continue using cyber operations to target and expose seemingly sensitive data, such as lists of government and military employees, most of which is gained through careful collection of publicly available information or by targeting personal accounts. We believe that most terrorist organizations currently do not have the capability to carry out sophisticated cyber attacks on their own, and would need to cultivate those capabilities through recruitment of highly skilled individuals, or through sufficient funds to purchase or hire such expertise. Current capabilities are likely limited to blunt attacks such as denial of service or destruction of data or resources, possibly carried out in concert with a kinetic attack.

Information Sharing

Information sharing is critical to the ability of the United States to successfully defend itself in cyber space. It will not, however, eliminate the risk of cyber attacks.

To defeat the most advanced threat groups, the private and public sector must share information not only about technical indicators—which are reactive—but about motivations, plans, and intentions that would enable forewarning. This information must be unclassified and shared in near-real time for network defenders to regain the upper hand against the best state-sponsored threat groups. Information sharing must be part of a comprehensive security strategy and combined with broader efforts to educate organizations about real risks, train security personnel to combat them effectively, and develop incentives so that the public and private sectors are motivated to invest in protecting data, assets, and critical infrastructure.

Reward Outweighs Risk

I have described how threat actors have increased in number and sophistication, and how groups of all types who once had only limited cyber capabilities have become more of a threat. This trend is due to multiple factors, including:

- The asymmetric advantage of cyber operations. Groups with otherwise limited military, political, or economic capabilities can leverage cyber operations to damage an opponent or deliver a political message, often with limited investment in resources and to disproportionate effect.
- The ongoing perception that threat groups can largely operate with impunity. The rewards to be had from conducting cyber operations greatly outweigh the risks, for state-sponsored, criminal, and terrorist hacking groups alike.

The perception of low risk and high reward for nation-state, criminal, and terrorist groups alike stems from a number of challenges related to the investigation, analysis, attribution, and prosecution of activity in the cyber realm:

- Forensic data can be volatile in the best of circumstances, and many groups take pains to limit or delete traces of their activity, further undermining investigators' ability to understand what occurred.
- Cyber crime and cyber operations are not limited by geographical boundaries, and groups may deliberately spread their activity across multiple countries to mislead and complicate investigation and prosecution.
- The ability to discern a threat group's true purpose and motivation becomes more difficult as nation-state and criminal actors adopt each other's tools and techniques. Groups may also attempt to actively misdirect investigators using "false flag" efforts.
- Attribution—the ability to link activity in the cyber realm to a real-world person or group—remains challenging, whether attempting to identify a criminal or a foreign government.

The challenges we face in the current threat landscape are many, but they are not insurmountable. Complex problems require multi-faceted solutions. I offer the following suggestions to facilitate these efforts:

- Continue to facilitate safe, trusted, and automated means for the public and private sector to share information about current and emerging threats. This sharing should encompass not merely indicators, but also contextual data about the nature, scope, and risk associated with those indicators. Context enables prioritization and decision making, allowing defenders to respond faster and more effectively.
- Recognize that the "fortress" approach of attempting to fully secure our networks and assets to prevent all possible attacks is infeasible. Organizations must secure their environments to the best of their ability, but understand that breaches can and will occur, and that they must have tools and resources in place to detect, respond to, and contain malicious activity across the entire attack lifecycle.
- Identify ways that organizations can "raise the bar" attackers must overcome to achieve their objectives. While the complexities of investigation and attribution

may make it difficult to impact threat actors in the wake of an attack, we can work together to make attacks more difficult and costly to carry out. This process may deter opportunistic attackers and slow down determined threats, giving defenders more time to detect and respond to attacks.

Mr. Chairman, Ranking Member Richmond, and members of the Subcommittee, I thank you for your attention and time today. I look forward to answering your questions.