SENATE INTELLIGENCE COMMITTEE:

RUSSIA AND 2016 ELECTION

EXECUTIVE SUMMARY

On March 30, 2017, FireEye CEO Kevin Mandia testified before the Senate Intelligence Committee regarding Russian active measures behind the U.S. elections in the fall of 2016. Mr. Mandia was requested to testify because of his decades-long experience working in cybersecurity. This includes his service in the U.S. Air Force and the Pentagon; his role as the founder of Mandiant, a leader in responding to computer intrusions and cyber threats; and most recently his work as CEO of FireEye, which has done extensive tracking of Russian cyber activity. As the FireEye CEO, Mr. Mandia represents a team of employees on the front lines of today's cyber battles. Below is a summary of the testimony provided by Mr. Mandia at the hearing.

FireEye Expertise

FireEye responds to active computer intrusions at companies and government organizations on a global scale, including incidents in cyber "hot zones" such as the Middle East and Southeast Asia. From its inception 13 years ago, FireEye has responded to hundreds of incidents around the world and the company continues to receive calls almost every day from organizations that have suffered cybersecurity breaches.

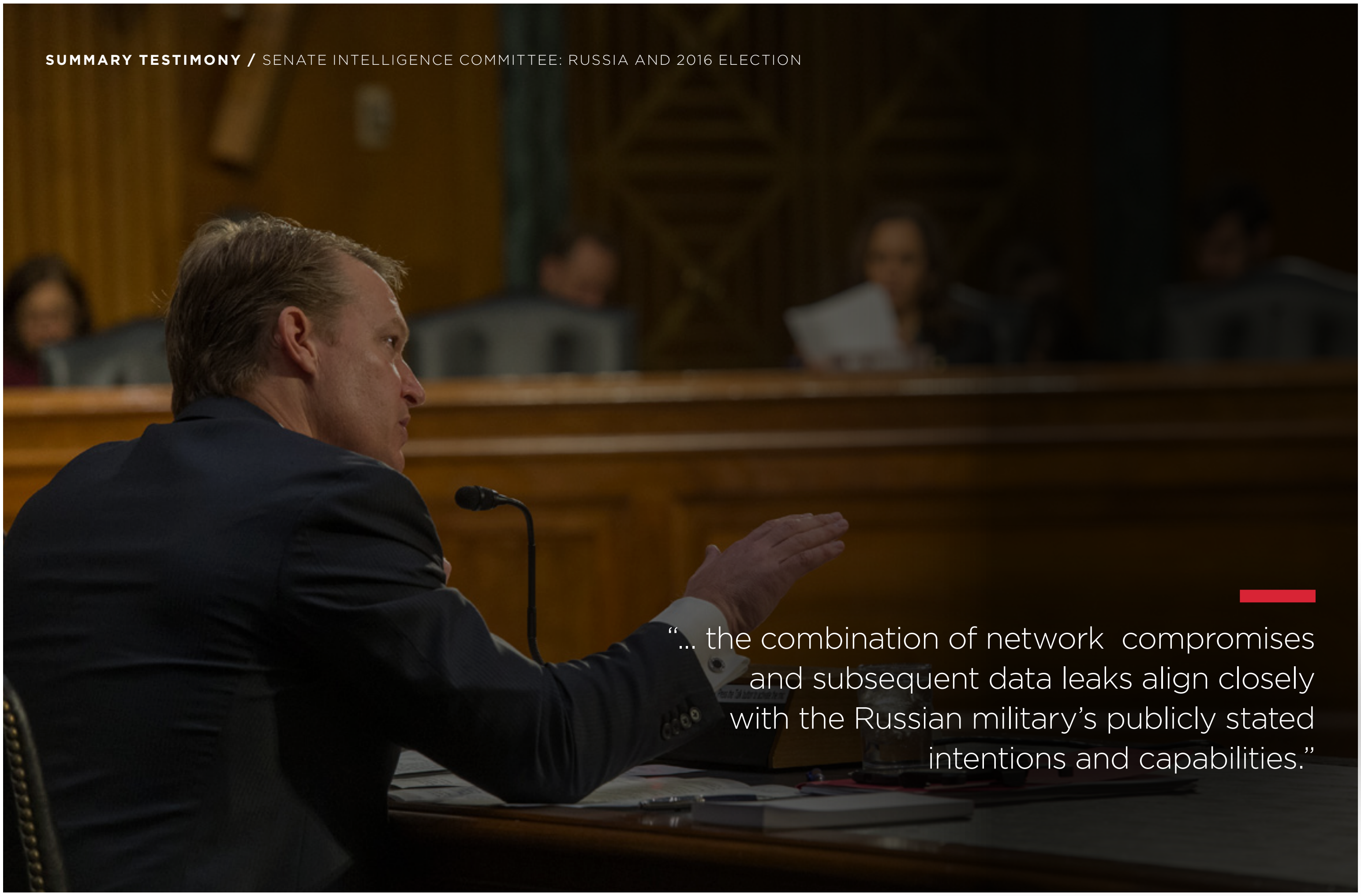
FireEye has amassed an enormous catalog of threat intelligence derived from its extensive experience responding to computer security breaches, insights derived from its cyber threat analysts and data collected from more than 5000 customers who use FireEye products to detect intrusions into their networks and respond to these attacks.

The Role of Overt and Covert Cyber Operations in Support of Russian Active Measures, Disinformation and Influence Campaigns

The role of nation-state actors in cyber attacks was perhaps most widely revealed in February 2013, when Mandiant released the report, "APT1: Exposing One of China's Cyber Espionage Units," which detailed a professional cyber espionage group based in China.[1] Several months later, in 2014, FireEye released another report focused on Russian cyber activities. In this report, "APT28: A Window into Russia's Cyber Espionage Operations,"[2] FireEye identified APT28 as a suspected Russian government-sponsored espionage actor, based on forensic details in the malware employed since at least 2007. Since its initial report on APT28, FireEye has continued to gather intelligence and collect data on the group's activities. In January of this year, FireEye released another report, "APT28: At the Center of the Storm,"[3] which provided additional detail on the continued evolution of Russian cyber operations.

[1] https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[2] https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf.



> "... the combination of network compromises and subsequent data leaks align closely with the Russian military's publicly stated intentions and capabilities."

As shown in this most recent report, an analysis of APT28 activities indicated the group's interest in regional security organizations and foreign governments and militaries, particularly those of Europe. FireEye research also indicated that APT28 network activity has likely supported information operations designed to influence the domestic politics of foreign nations. FireEye provided an extensive listing of targets, including the World Anti-Doping Agency, the U.S. Democratic National Committee, Mr. John Podesta, the U.S. Democratic Congressional Campaign Committee, TV5Monde and the Ukrainian Central Election Commission.

All of these breaches involved the theft of internal data — mostly emails — that was later strategically leaked through multiple forums and propagated in a manner almost certainly intended to advance particular Russian government goals. FireEye noted that the combination of network compromises and subsequent data leaks align closely with the Russian military's publicly stated intentions and capabilities. Russian strategic doctrine has long included what the West terms "information operations," which have been further developed, deployed and modernized. The recent activity in the United States is one of many instances of such operations conducted in support of Russian political objectives. It is important to note that FireEye's conclusions were consistent with the U.S. Office of the Director of National Intelligence report released on January 7, 2017, in which this activity is described as "an influence campaign."[4]

[3] https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf.

[4] https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf.

Cyber Capabilities and Techniques Attributed to Russian State and Non-State Actors

During FireEye's APT28 investigations, the company analyzed more than 550 customer malware variants, approximately 500 domains, over 70 lure documents and dozens of spear phishing emails to understand the threat actor's tools, techniques and procedures. FireEye found that APT28 continues to evolve its toolkit and refine its tactics to maintain its operational effectiveness in the face of heightened public exposure and scrutiny. In addition to the continued evolution of the group's first-stage tools, the company has also noted that APT28 is:

- Leveraging at least five zero-day vulnerabilities in Adobe Flash Player, Java and Windows in 2015 alone, including CVE-2015-1701, CVE-2015-2424, CVE-2015-2590, CVE-2015-3043, CVE-2016-7193 and CVE-2015-7645;
- Increasing its reliance on public code depositories, such as Carberp, PowerShell Empire, P.A.S. webshell, Metasploit modules and others, likely to accelerate their development cycle and provide plausible deniability;
- Obtaining credentials through fabricated Google App authorization and OAuth access requests that allow the group to bypass two-factor authentication and other security measures; and
- Moving laterally through a network relying only on legitimate tools that already exist within victims' systems, at times forgoing their traditional toolset for the duration of the compromise.

Over the past two years FireEye has witnessed an escalation of APT 28's overall activities, with one notable change in its rules of engagement. Since 2014, the company has seen APT28 in many instances compromise a victim organization, steal information and subsequently leak the stolen data into the public. Many of these leaks have been conducted through the use of "false hacktivist personas," including, among others, "CyberCaliphate," "Guccifer 2.0," "DC Leaks," "Anonymous Poland," and "Fancy Bears' Hack Team." These personas appropriated pre-existing hacktivist or political brands likely to obfuscate their true identity, provide plausible deniability and create credibility.

Although FireEye can link the collection activity to APT28, the company has not established whether the APT28 operators themselves directly control the false personas that then leak material or if that responsibility instead resides with a separate entity. However, similar patterns seen in infrastructure procurement between APT28 and some personas suggest they played at least some role. For example, it is believed that the actors behind the DCLeaks persona attempted to register the domain "electionleaks.com" one week prior to "DCLeaks.com" in April 2016 — approximately two months before the first election-related leaks. These domains were registered using the service provider that APT28 has frequently used to support cyber attacks. FireEye intelligence indicates that APT28 likely operated with the knowledge that the data they stole during cyber intrusions would leverage these domains for public exposure of the data.

Assessing Russian Government Involvement in this Activity

To make such an assessment, FireEye reviewed and compared intrusion methodologies, tools, malware and other evidence. FireEye also examined forensic details left behind, such as the specific IP addresses or email addresses from spear phishing attacks, file names, MD5 hashes, timestamps, custom functions, encryption algorithms or backdoors with embedded command and control IP addresses or domain names.

Targeting was also critical to the assessment. Knowing the types of organizations, individuals or data that a threat group targets provides insight into the group's motives and objectives. Gathering this type of data about a group typically requires visibility into the group's operational planning, their initial attacks or infection attempts or actual victim environments. FireEye tracks all of the indicators and significant linkages associated with identified threat groups in a proprietary database — composed of millions of nodes and linkages between groups — developed over many years. FireEye analyzes this information carefully in the context of the relevant political and cultural environment to develop its assessments.

Based on the extensive collected intelligence and analysis in this instance, FireEye determined that APT28's cyber operations are consistent with government sponsorship and control. Specifically, APT28 has relied on a steady supply of sophisticated tools only available to a nation-state or state-protected contractor. The group also pursued targets where Russian interests would be high. In addition, the level of activity it maintained over several years required significant financial and personnel resources — with no clear profit motive. Finally, APT28 closely integrated its cyber attacks into broader propaganda efforts of benefit to a nation-state actor.

There are alternative explanations for APT28's sponsorship, but these only appear to be a plausible explanation for one incident at a time and are not credible when considering the totality of APT28's operations. By combining increasingly wider ranging technical intelligence, hands-on remediation of compromised systems and Russia's apparent geopolitical aims based on its own public statements, our confidence that the Russian government sponsors or controls APT28 has grown since our initial 2014 report.

Moreover, APT28's activities are not consistent with any basic criminal activities to which FireEye has responded, nor are they consistent with a lone actor. The infrastructure size, the targeted information, the malware amount and the sophistication suggests a long-term, well-resourced espionage campaign that benefits Russia.

In summary, while FireEye does not have pictures of a building, names of individuals or a government agency to name, the evidence supports the company's assessment of a long-standing, focused operation that indicates a Russian government sponsor and government capability.

Recommendations to Prevent and Mitigate the Threat Posed by Such Cyber Operations

Today and into the foreseeable future, it is FireEye's view that the United States will face a motivated, technically sophisticated and well-resourced adversary intent on accessing our private data and potentially leaking it publicly. While many organizations are actively trying to counter these attacks, a sizeable gap exists between what their safeguards can prevent and the ability of motivated attackers to circumvent those safeguards — leaving an ongoing need to explore ways to help deter these attacks, both within and outside the cyber domain.

Of course, all enterprises — private sector or government — should work to accurately assess their own risk profiles and utilize updated technology and best practices to protect their networks and systems. However organizations cannot buy, hire or train their way to perfect security and effective deterrence and proportional response outside of the cyber domain must be considered.

While diplomacy is not often cited as a primary tool in this arena, evidence appears to reinforce its potential effectiveness. FireEye conducted a comprehensive study of 182 compromised U.S. targets by 72 Chinese cyber threat groups dating back to 2013. The company saw a sharp decline in these operations after September 2015, when President Obama and President Xi met and agreed to curtail cyber operations for commercial benefit. Certainly, Chinese cyber operations continue for traditional espionage and U.S. companies are still targeted for the security, political, economic and military intelligence that Beijing seeks. However, the agreement appears impactful, demonstrating that diplomacy can also be a useful tool for reducing the cyber threat both countries face, coupled with the public-private sector collaboration.

In addition to Russia, North Korea and Iran are tied to a series of escalating attacks dating back several years. FireEye has noted the audacity of the sponsoring nations and their willingness to surpass previously established "red lines." It is entirely reasonable to suspect each nation is emboldened by the other's behavior and it is important to note that any response to the Russian cyber activities discussed today will likely be assessed by other countries.

This represents select excerpts from Mr. Mandia's testimony. His full testimony can be viewed here in this **C-SPAN recording** of the Senate Intelligence Committee hearing.

For more information on FireEye, visit:
www.FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 5,600 customers across 67 countries, including more than 40 percent of the Forbes Global 2000.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye