



**Prepared Statement of Kevin Mandia, CEO of FireEye, Inc.
before the United States Senate Select Committee on Intelligence**

March 30, 2017

Thank you, Mr. Chairman, Vice-Chairman Warner, and Members of the Senate Intelligence Committee, for the opportunity you have given me today to share our observations and our experiences regarding this important topic, as well as for your leadership on cybersecurity issues. As requested, I am going to discuss three topics here today: 1) the role of overt and covert cyber operations in support of Russian active measures, disinformation, and influence campaigns; 2) the cyber capabilities and techniques attributed to Russian state and non-state actors; and 3) recommendations to prevent and mitigate the threat posed by such cyber operations.

1. Background.

Before I turn to your specific questions, let me share some background on myself and my company to inform the context of my narrative. I have been working in cybersecurity for over two decades, since I was first stationed at the Pentagon at the outset of my career as a Computer Security Officer in 1993. During my time investigating computer intrusions while I was in the Air Force, I came to recognize that the biggest cyber threats to our infrastructure were intrusions from other countries, most notably Russia and China. I founded Mandiant in 2004 to create a company with that could effectively respond to these threats and innovate technologies to help detect and respond to advanced attacks. Fast forward a few years, Mandiant was bought by FireEye, and I became FireEye's CEO last June in 2016.

As I testify today, FireEye employees are on the front lines of the cyber battle, responding to active computer intrusions at dozens of the largest companies and organizations on a global scale, including incidents in cyber "hot zones" such as the Middle East and Southeast Asia. Over the last 13 years, we have responded to incidents at hundreds of companies around the world. During that time, we have investigated millions of systems, and we receive calls almost every single day from organizations that have suffered a cybersecurity breach.

In addition to the 300-plus security professionals responding to computer intrusions, FireEye has over 150 cyber-threat analysts on staff in 19 countries and speaking 32 different languages, to help us predict threats and better understand the adversary – often by considering the political and cultural environment of the threat actors. We have an enormous catalog of threat intelligence, and it continues to grow everyday coincident with the continually increasing attacks on organizations around the world.



The information I will share today, then, is derived from our experiences responding to computer security breaches, as well as intelligence derived from our experienced team of cyber threat analysts and collected from more than 5000 customers who use our products to detect intrusions into their networks and respond to these attacks.

2. 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 we released another report, this time regarding Russian cyber activities, entitled, "APT28: A Window into Russia's Cyber Espionage Operations?"² In that report, FireEye identified APT28 as a suspected Russian government-sponsored espionage actor, basing our conclusion on forensic details left in the malware employed since at least 2007. Since release of the initial report on APT28, we have continued to gather intelligence and collect data on the group's activities, and most recently, in January of this year, released "APT28: At the Center of the Storm"³ which provides additional detail on the continued evolution of Russian cyber operations.

As shown in our most recent report, an analysis of the activities of APT28 indicates the group's interest in foreign governments and militaries, particularly those of Europe, as well as regional security organizations. In addition, our research indicates that APT28 network activity has likely supported information operations designed to influence the domestic politics of foreign nations. We provide an extensive listing of targets including the World Anti-Doping Agency (WADA), the U.S. Democratic National Committee, Mr. John Podesta, the U.S. Democratic Congressional Campaign Committee (DCCC), as well as TV5Monde and the Ukrainian Central Election Commission (CEC).

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. We 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 for a long time included what the West terms 'information

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>.

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



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. I note that our 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. Cyber Capabilities and Techniques Attributed to Russian State and Non-State Actors

So how was this done, and why do we assess that the Russian government was likely behind this activity? *Let me first speak to the methodologies used.* During the course of our APT28 investigations, we analyzed over 550 customer malware variants, identified approximately 500 domains, over 70 lure documents and dozens of spear phishing emails to help us understand their tools, techniques, and procedures. We find that APT28 continues to evolve its toolkit and refine its tactics in an effort 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, we have also noted that APT28 is:

- 1 - 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.
- 2 - Increasing its reliance on public code depositories, such as Carberp, PowerShell Empire, P.A.S. webshell, Metasploit modules, and others in a likely effort to accelerate their development cycle and provide plausible deniability.
- 3 - Obtaining credentials through fabricated Google App authorization and OAuth access requests that allow the group to bypass two-factor authentication (2FA) and other security measures, and
- 4 - 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 we have witnessed an escalation of APT 28's overall activities and one notable change in its rules of engagement. Specifically, since 2014 we have 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 to create the perception of credibility.

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



Although we can link the collection activity to APT28, we have not been able to establish 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, we do see similar patterns in infrastructure procurement between APT28 and some personas to suggest they played at least some role. For example, we believe 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 prior to the first election-related leaks. These domains were registered using the service provider we have seen APT28 frequently use in the past to support cyber attacks. Thus, our 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.

I include the following timeline and analysis to illustrate the use of these techniques over the last few years.

In June of 2014, Ukrainian officials revealed the investigation into the compromise of the Ukrainian Central Election Commission (CEC) internal network identified custom malware traced to APT28. During the May 2014 Ukrainian presidential election, purported pro-Russian hacktivists "CyberBerkut" conducted a series of malicious activities against the CEC, including a system compromise, data destruction, a data leak, a distributed denial-of-service (DDoS) attack, and an attempted defacement of the CEC website with fake election results.

In February of 2015, FireEye identified APT28 (CORESHELL) traffic beaconing from TV5Monde's network, revealing APT28 had compromised TV5Monde's network. In April 2015, alleged pro-ISIS hacktivist group CyberCaliphate defaced TV5Monde's websites and social media profiles and forced the company's 11 broadcast channels offline. We identified overlaps between the domain registration details of CyberCaliphate's website and APT28 infrastructure.

In July of 2016, the U.S. Democratic Congressional Campaign Committee (DCCC) announced that it was investigating an ongoing "cybersecurity incident" that the FBI believed was linked to the compromise of the DNC. House Speaker Nancy Pelosi later confirmed that the DCCC had suffered a network compromise. Investigators indicated that the actors may have gained access to DCCC systems as early as March. In August, the Guccifer 2.0 persona contacted reporters covering the U.S. House of Representative races to announce newly leaked documents from the DCCC pertaining to Democratic candidates. From August to October, Guccifer 2.0 posted several additional installments of what appear to be internal DCCC documents on its WordPress site.



Between March and October of 2016, investigators found that John Podesta, Hillary Clinton's presidential campaign chairman, was one of thousands of individuals targeted in a mass phishing scheme using shortened URLs that security researchers attributed to APT28. Throughout October and into early November, WikiLeaks published 34 batches of email correspondence stolen from Mr. Podesta's personal email account. Correspondence of other individuals targeted in the same phishing campaign, including former Secretary of State Colin Powell and Clinton campaign staffer William Rinehart, were published on the "DC Leaks" website.

In April through September, 2016, the U.S. Democratic National Committee (DNC) suffered a network compromise and a subsequent investigation found evidence of two breaches, attributed to APT28 and APT29. FireEye analyzed the malware found on DNC networks and determined that it was consistent with our previous observations of APT28 tools. In June 2016, shortly after the DNC's public announcement about the breach, the Guccifer 2.0 persona claimed responsibility for the DNC breach and leaked documents taken from the organization's network. Guccifer 2.0 continued to leak DNC documents through September of 2016.

And finally, in September of 2016, WADA confirmed that APT28 had compromised its networks and accessed athlete medical data. On Sept. 12, 2016, the "Fancy 'Bears' Hack Team" persona claimed to have compromised WADA and released athletes' medical records as "proof of American athletes taking doping."

Let me now turn to explaining ***why we assess that the Russian government was likely behind this activity.***

In order to make such an assessment, we reviewed and compared intrusion methodologies and tools, malware or authored exploits and use of shared personnel. We also examined forensic details that were 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 that may have command and control IP addresses or domain names embedded.

Targeting was also critical to our assessment. Knowing the types of organizations, individuals, or data that a threat group targets provided us with insight into the group's motivations 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 into actual victim environments. We track all of the indicators and significant linkages associated with identified threat groups in a proprietary database that we have developed over many years comprised of millions of nodes and linkages between groups, and then analyze this information carefully in the context of the relevant political and cultural environment to develop our assessments.



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

There are alternative explanations for APT28's sponsorship, however in our view these only appear plausible for explaining one incident at a time, and are not credible in the context of the totality of APT28's operations. By combining an increasingly wide range of technical intelligence, hands-on remediation of compromised systems, and an understanding of Russia's geopolitical aims based on its own public statements, our confidence in assessing Russian government sponsorship or control of APT28 has only grown since release of our initial report in 2014.

Moreover, the activities of APT28 are not consistent with any basic criminal activities to which we have responded, nor are they consistent with those perpetrated by a lone actor. The size of the infrastructure, the targeted information, the amount of malware and the totality of the sophistication, suggests a long-term, well-resourced espionage campaign in which Russia is the benefactor.

In summary, while we do not have pictures of a building, names of individuals, or a government agency to name, our assessment is supported by evidence of long-standing, focused operations that indicates a Russian government sponsor and government capability.

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

Today, and into the foreseeable future, it is our 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, there currently exists a sizeable gap between what their safeguards can prevent and the ability of motivated attackers to circumvent those safeguards. Therefore, we will need to explore ways, both within and outside the cyber domain, to help deter these attacks.

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 we must consider effective deterrence and proportional response outside of the cyber domain as well.

While diplomacy is not often cited as a primary tool in this arena, evidence collected regarding Chinese activity appears to reinforce its potential effectiveness. We conducted a comprehensive study of 182 compromised U.S. targets by 72 Chinese cyber threat groups going back to 2013, and we saw a sharp decline in these operations after September 2015 – when President Obama and President Xi met and specifically agreed to curtail cyber operations for commercial benefit. To be sure, Chinese cyber operations for traditional espionage remain, and US companies are still targeted for the security, political, economic, and military intelligence that Beijing seeks. However, it appears that the agreement had an impact, demonstrating that diplomacy can also be a useful tool for reducing the cyber threat both countries face, coupled with the public-private sector collaboration. This experience leaves me optimistic that with the combined efforts of both governments and the private sector, diplomatic engagement with Russia and other nations to restrict harmful cyber activity would be enforceable.

In addition to Russia, North Korea and Iran have been tied to a series of escalating attacks that go back several years. We have been surprised by the audacity of the sponsoring nation and their willingness to surpass “redlines” that we previously believed were established. It is entirely reasonable to suspect that these nations are emboldened by each 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.

Again, we applaud the leadership shown by this Committee to bring important issues such as those discussed today to light, and we in the private sector look forward to continuing to work with you to disseminate and support industry best practices and encourage adoption of comprehensive and effective cybersecurity programs across government and industry. I look forward to answering your questions today.

* * *