STATEMENT OF DR. PHYLLIS SCHNECK, VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, GLOBAL PUBLIC SECTOR

McAFEE, INC.

BEFORE:

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON FOREIGN RELATIONS

SUBCOMMITTEE ON ASIA AND THE PACIFIC

"ASIA: THE CYBER SECURITY BATTLEGROUND"

JULY 23, 2013

Good morning, Chairman Chabot, Ranking Member Faleomavaega, and other members of the subcommittee. I am Phyllis Schneck, Vice President and Chief Technology Officer, Global Public Sector for McAfee, Inc., a subsidiary of Intel Corporation. We appreciate the subcommittee's interest in cyber security threats and solutions as they affect Asia and the Pacific.

My testimony will focus on the following areas:

- The threat landscape in Asia Pacific
- Attacks against South Korea, as demonstrated by Operation Troy
- Recommended security solutions

I'm going to focus on something a little different, and that is the threats *to* the region rather than the threats *from* the region.

First I would like to provide some background on my experience and on McAfee.

I have dedicated my entire professional career to the security and infrastructure protection community. My technical background is in high performance computing and cryptography. In addition to my role with McAfee, I serve as Chairman of the Board of Directors of the National Cyber Forensics and Training Alliance (NCFTA), a partnership between government, law enforcement, and the private sector for information analytics that has been used to prosecute over 400 cyber criminals worldwide.

Earlier, I worked as Vice President of Threat Intelligence at McAfee and was responsible for the design and application of McAfee's™ Internet reputation intelligence. I am the Vice Chair of the Information Security and Privacy Advisory Board (ISPAB) and have

also served as a commissioner and working group co-chair on the public-private partnership for the Center for Strategic and International Studies (CSIS) Commission to Advise the 44th President on Cyber Security.

Additionally, I served for eight years as chairman of the National Board of Directors of the FBI's InfraGard™ program and as founding president of InfraGard Atlanta, growing the InfraGard program from 2000 to over 33,000 members nationwide. Prior to joining McAfee, I was Vice President of Research Integration at Secure Computing. I hold a Ph.D. in Computer Science from Georgia Tech, where I pioneered the field of information security and security-based high-performance computing.

McAfee's Role in Cyber Security

McAfee protects businesses, consumers and the public sector from cyber-attacks, viruses, and a wide range of online security threats. Headquartered in Santa Clara, California, and Plano, Texas, McAfee is the world's largest dedicated security technology company and is a proven force in combatting the world's toughest security challenges. McAfee is a wholly owned subsidiary of Intel Corporation.

McAfee delivers proactive and proven solutions, services, and global threat intelligence that help secure systems and networks around the world, allowing users to safely connect to the Internet and browse and shop the web more securely. Fueled by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security.

To help organizations take full advantage of their security infrastructure, McAfee launched the Security Innovation Alliance, which allows organizations to benefit from the most innovative security technologies from thousands of developers, who can now snap into our extensible management platform. Today, more than 160 technology partners—large and small businesses all committed to continuous innovation in security—have joined the alliance, with more to be announced soon.

Threat Landscape for Asia and The Pacific

The APAC region consists of over half of the world's population and is made up of a diverse group of countries with different levels of technological expertise and capacity. Capacity building is of utmost importance for all regional organizations in order to maintain a safe and prosperous cyber industry. Businesses relying on the Internet or IT industries are responsible for much of the region's recent prosperity and are critical for the continuing growth and development of APAC populations. Gaps in expertise, however, expose vulnerabilities in the cyber infrastructure of the region. In other words, if a hacker can target the weakest link in the APAC cyber infrastructure, one attack can

potentially cause damage throughout the region and to global supply chains. Thus, capacity building, information sharing and cyber security are critically important to APAC nations. This is particularly relevant as it pertains to certain extremist sectors of the population of Southeast Asian nations, who may potentially exploit weaknesses in the region's security infrastructure to meet their economic/political/ideological ends.

I want to focus in on South Korea, which has recently experienced attacks on several of its official websites, including that of its president and its ruling conservative party. Earlier, experts at McAfee investigated the Dark Seoul attacks in March that affected the country's financial and media sectors. This operation, led by McAfee researchers Ryan Sherstobitoff and Jim Walter, is known as Operation Troy.

Operation Troy

When reports of the Dark Seoul attack on South Korean financial services and media firms emerged in the wake of the attack on March 20, 2013, most of the focus was on the Master Boot Record (MBR) wipe functionality, or the ability to destroy the MBR, which is necessary for a computer to "boot" or start up, as it finds the correct location on the disk for boot instructions. In Dark Seoul, PCs infected by the attack had all of the data on their hard drives erased. McAfee Labs, however, has discovered that the Dark Seoul attack includes a broad range of technology and tactics beyond the MBR functionality. Our analysis has revealed a covert espionage campaign. Typically this sort of advanced persistent threat (APT) campaign has targeted a number of sectors in various countries, but Operation Troy, as these attacks are now called, targets solely South Korea.

The forensic data indicates that Dark Seoul is actually just the latest attack to emerge from a malware development project that has been named Operation Troy. The name "Troy" actually comes from repeated citations of the ancient city found in the compile path strings of the malware. The primary suspect group in these attacks is the New Romanic Cyber Army Team that makes significant use of Roman terms in their code. The McAfee Labs investigation into the Dark Seoul incident uncovered a long term domestic spying operation operating against South Korean targets all based on the same code base.

Software developers (both legitimate and criminal) tend to leave fingerprints and sometimes even footprints in their code that forensic researchers can use to identify where and when the code was developed. It's rare that a researcher can trace a product back to an individual developer (unless they're unusually careless). But, frequently these artifacts can be used to determine the original source and development legacy of a new "product." Sometimes, as in the case of the New Romanic Cyber Army Team or the Poetry Group, the developers insert such fingerprints on purpose to establish "ownership" of a new threat. McAfee Labs uses sophisticated code analysis and forensic techniques to identify the sources of new threats, as such analysis frequently sheds light on how to best mitigate an attack or predicts how the threat might evolve in the future.

Operation Troy History

The history of Operation Troy extends back to 2010 with the appearance of the "NSTAR Trojan," the first piece of malware in Operation Troy, and one designed to gain privileged system access by disguising its true intent. Since the appearance of NSTAR, seven known variants, or new pieces of malware based on the original NSTAR, have been identified. Despite the rather rapid release cycle, the core functionality of Operation Troy really has not evolved all that much, and the main differences between NSTAR and several of its future variants had more to do with programming technique than functionality.

The first real functional improvements were seen in early 2013, when a variant called Concealment Troy changed the Command & Control architecture and did a better job of concealing its presence from standard security techniques. The variant Dark Seoul added the functionality that disrupted financial services and media companies in South Korea and was also the first variant used to conduct international espionage. All previous versions were simple domestic cybercrime/cyber espionage weapons.

Linking malware to its developers isn't always an easy task, as most attackers are careful enough to ensure they can't be traced. This is especially important in cases such as cyber espionage, in which the intent is to remain invisible. Yet in our analysis we observed a number of unique attributes in the components involved in these attacks; these markers allowed us to link specific samples to a specific group.

While two groups have taken credit for these attacks, we can tell that the variants that destroyed the systems link to the New Romanic Cyber Army Team.

Fingerprints

As interesting as the legacy of Operation Troy is, what's more enlightening are the fingerprints and footprints that allow McAfee Labs to trace its legacy. In the "fingerprint" category is what developers term the compile path – which is simply the path through the developer's computer file directory to the location at which the source code is stored.

By analyzing attributes such as the compile path, Labs researchers were able to, among other things, confirm that the attackers have been operating for over three years against South Korean targets.

Footprints

In the footprint category McAfee Labs documented the most significant functional change that occurred as the 2013 release of the Concealment Troy. Historically, the Operation Troy Command & Control (C&C) process involved routing of operating commands through concealed Internet Relay Chat (IRC) servers. The first three Troy variants were managed through a Korean manufacturing website in which the attackers installed an IRC server.

From the attacker's perspective there are two issues with this approach. The first is that if the operator of the infected server discovered the rogue IRC process, they would remove it and the attacker would lose control of the Troy infected client devices. The second is that the Troy developers actually hard coded the name of the IRC server into each Troy variant. This means that they had to first find a vulnerable server, install an IRC server, and then recompile the Troy source into a new variant controlled by that specific server. For this reason nearly all Troy variants needed to be controlled by a separate C&C server.

The Concealment Troy variant was the first to break this dependency on finding an IRC Command & Control server. Concealment Troy presumably gets its operating instructions from a more sophisticated (and likely more distributed) botnet that is also under the control of the Troy syndicate.

What Operation Troy Reveals

This investigation into the cyber-attacks on March 20th, 2013 revealed ongoing covert intelligence gathering operations. McAfee Labs concludes that the attacks on March 20th, 2013 were not an isolated event strictly tied to the destruction of systems, but rather the latest in a series of attacks dating to 2010. These operations remained hidden for years and evaded the technical defenses that the targeted organizations had in place. Much of the malware from a technical standpoint is rather old, with the exception of Concealment Troy, which was released early 2013.

McAfee Labs can connect the Dark Seoul and other government attacks to a secret, long-term campaign that reveals the true intention of the Dark Seoul adversaries: attempting to spy on and disrupt South Korea's military and government activities. The Troy-era malware is based on the same source code used to create these specialized variants and shares many commonalities that are found consistently throughout the families. The attackers have attempted since 2009 to install the capability to destroy their targets using an MBR wiper component, as seen in the Dark Seoul incident. From our analysis we have established that Operation Troy had a focus from the beginning to gather intelligence on South Korean military targets. We have also linked other high-profile public campaigns conducted over the years against South Korea to Operation Troy, suggesting that a single group is responsible.

What's The Solution?

What could have prevented Operation Troy and other attacks against South Korea? It's difficult to say for certain, of course, but at McAfee we believe in a connected, adaptable, open and dynamic security platform to guide security decisions made by machines and people. We emphasize the importance of every network component being both a producer and consumer of intelligence. This intelligence can then be shared within the network and externally (as policy allows) to enable an adaptive, learning ecosystem that gets smarter as it protects.

This ecosystem concept is well described in the white paper from the National Protection and Programs Directorate within the U.S. Department of Homeland Security. Done correctly, networks can detect behaviors over time and begin to recognize, almost biologically, threats before those threats can overtake network functionality. Maturity models have shown that for any size organization, a wise design up-front leads to increasing security and decreasing cost over time. This ecosystem model would work well for any sector of a nation's economy.

A key technology that informs this ecosystem is Global Threat Intelligence (GTI), which feeds each security component, enabling it to have continual situational awareness. GTI serves as a cyber immune system, protecting against attacks by electronically detecting and correlating, at machine speed, cyber behavioral data from worldwide sources that is identified as harmful. In milliseconds GTI can assess changes, assign risk levels, and distribute protection recommendations to every product in the ecosystem.

Another key technology, application whitelisting, turns the old signature-based approach on its head. Rather than having to list every known piece of harmful code – a process where you're always behind the curve – whitelisting allows only code that is known to be good into the ecosystem.

At McAfee we call this ecosystem approach Security Connected: an integrated platform of intelligent products that leverage threat intelligence. McAfee provides every necessary component of the ecosystem. However, Security Connected is also an open platform, allowing products from a host of vendor partners from our Security Innovation Alliance (SIA) to participate just as fully. Currently SIA is 160 partners strong and growing.

This ecosystem approach can be applied at every level of the computing continuum – from the application layer down to the silicon in the chip. This is what McAfee and parent Intel developed together – the technology known as "DeepSafe" (and the product is DeepDefender). When DeepSafe is loaded on a machine it loads below the operating system level, which is significant because malware often installs itself in the kernel of an operating system. With DeepSafe the security sits below that, right on the hardware, protecting the entire ecosystem.

McAfee is also working beyond our own borders on the ecosystem concepts. We're helping to lead the creation of global protocols to transport cyber event indicators at machine speed to and from all components of the network, enabling the best intelligence from all sources to be used throughout the greater Internet architecture. These initiatives can enable any entity, any product, any company and any government – small or large -- to become part of a greater ecosystem in which the detection of a threat on the Internet is used as protection going forward – at the speed of light. This is the kind of agility our adversaries cannot achieve.

Thank you for requesting McAfee's views on these important issues. I am happy to answer any questions.