U.S.-China Economic and Security Review Commission
Hearing on "Developments in China's Cyber and Nuclear Capabilities"
Submission by Nart Villeneuve
March 26, 2012

I would like to thank the members of the U.S.-China Economic and Security Review Commission for inviting me to participate in today's hearing on Developments in China's Cyber and Nuclear Capabilities. I spend my days investigating targeted malware attacks as a Senior Threat Researcher at Trend Micro Inc. While my statement today is drawn from my experience, particularly from an inside view into three cyber-espionage campaigns that I have helped uncover, GhostNet (which compromised diplomatic entities around the world), ShadowNet (which targeted the Indian government and military) and LURID (which targeted space-related agencies in the former Soviet Union), it is entirely my own opinion and does not necessarily reflect the views of my employer.

My testimony today focuses on malware-based espionage, or what some refer to as, or as a component of, Advanced Persistent Threat (APT) activity. This APT activity can be tracked over time and linked through specific indicators to threat actors operating in the Chinese language or using command and control infrastructure in China. However, I recommend caution when attempting to determine attribution based solely on technical indicators that are frequently spoofed and often misleading because there is no "smoking gun" in cyberspace.

While there have been a lot of accusations of "hype" surrounding APT, the problem is severely understated, not overstated. Instead of focusing on the effect of these attacks, most are concerned with the level of "sophistication" and debate whether these attacks are "advanced" or not. I would like to emphasize three key points:

- Targeted malware attacks are extremely successful. The scope of the problem is truly global, extending far beyond the US. It affects governments, militaries, defense industries, high tech companies, the energy and finance sectors, inter-governmental organizations, non-governmental organizations, media outlets, academic institutions, and activists around the world.
- Targeted malware attacks are not isolated incidents of "smash and grab" attacks. They are part of consistent *campaigns* aimed at establishing a persistent, covert presence in a target's network so that information can be extracted as needed.
- Targeted malware attacks are not well understood. However, careful monitoring can leverage mistakes made by the attackers that allow us to get a glimpse inside their operations. Moreover, these malware-based espionage campaigns can be tracked over time through a combination of technical and contextual indicators but this information is not often made public.

1. Targeted Malware Attacks

There has been dramatic increase in targeted malware attacks. Unlike the largely indiscriminate attacks that focus on stealing credit card and banking information associated with cybercrime,

these targeted attacks are noticeably different and are better characterized as malware-based espionage. These highly targeted attacks are computer intrusions staged by threat actors that aggressively pursue and compromise specific targets, often leveraging social engineering or the "art of manipulation", in order to maintain a persistent presence within the victim's network so that they can move laterally and extract sensitive information.

In a typical targeted attack, a target receives a message – such as an email or instant message – that is contextually relevant to the potential victim and encourages the target to click on a link or open a file. The links and files sent by the attacker contain malicious code that exploits vulnerabilities in popular software. The payload of these exploits is malware that is silently executed on the target's computer. This exploitation allows the attackers to take control of and obtain data from the compromised computer. The malware connects back to command and control servers under the attacker's control from which the attackers may then command the compromised computer to download additional malware and tools that allow them to move laterally throughout the target's network. These are not isolated incidents of "smash and grab" attacks but are part of consistent campaigns aimed at establishing a covert presence in a target's network so that information can be extracted as needed.

Targeting

While government and military networks have long been targets, these highly targeted attacks have spread to the defense industrial base and high tech companies, the energy and finance sectors, telecommunications companies as well as media outlets, civil society organizations and academic institutions. Often, these attacks target "communities of interest" that span the aforementioned categories. Compromised "soft" targets can then be used to launch attacks against hardened targets. These attacks are successful because they are designed to manipulate individuals into revealing sensitive information or executing malicious code. The delivery mechanism, usually an email, is often specifically addressed to the target and appears to have originated from someone within the target's organization or someone in target's social network. In extremely targeted cases, attackers may actually send email directly from a compromised, but real, email account of someone the target knows and trusts.

While some might believe that the threat actors behind targeted malware attacks have mythical capabilities, both in terms of their operational security and the exploits and malware tools used, they, in fact, often use older exploits and simple malware. They do not always use "zero day" vulnerabilities – exploits for vulnerabilities for which there is no patch available. The objective of these attacks is to obtain sensitive data; the malware used in the attacks is just an instrument. The discovery of GhostNet, for example, highlighted the fact that attackers do not need to be technically "sophisticated" or "advanced". With some functional but less-than-impressive code along with the publicly available gh0st RAT tool these attackers were able to compromise and maintain persistent control of embassies around the world. They can be successful without being "advanced" because of their exploitation of trust through social engineering as well as the learning gained from continual probes as well as both successful and unsuccessful attacks. This allows the attackers to select exploits based on what they know about the target's environment and they do leverage "zeroday" exploits when needed.

Campaigns

These targeted attacks are rarely isolated events; in fact, they are constant. It is more useful to think of them as *campaigns* – a series of failed and successful attempts to compromise a target over a period of time. In fact, the attackers themselves often keep track of the different attacks within a campaign in order to determine which individual attack compromised a specific victim. As the attackers learn more about their targets, from open source research as well previous attacks, the specificity of the attacks may sharply increase.

Once enough information is obtained from separate incidents *indicators* obtained from technical, operational and contextual artifacts can be assembled that allow attacks to be grouped in campaigns. This analysis is important because the information gleaned from any individual incident is usually partial because there are varying levels of visibility across the stages of an attack. For any one incident, we may have the attack vector, such as an email, or the malware payload of simply command and control server activity. Others, especially those involved with incident response, may have information on the attacker's lateral movement and data ex-filtration points. But the most revealing information usually comes from mis-configured command and control servers used by the attackers that reveal an inside look at their operations.

Operations

One of the most important and often overlooked element of malware-based espionage is reliance on human labor which stands in stark contrast to the largely automated botnets operated by cybercriminals. In addition to manual reconnaissance the attacker will craft individualized emails and package malware specifically for an individual or group of targets. In addition, they will adjust their tactics in reaction to the defenses of the victim. This customization and low distribution provides the attackers with a significant advantage over defenders that are largely relying on automated systems. However, this human element also, occasionally, exposes one of their weaknesses.

The attackers can and do make mistakes. Careful monitoring of their command and control infrastructure can reveal the inner workings of their operations. The data obtained from the attacker's infrastructure often reveals the length of the operation, the number of individual attacks, the identity of the victims, additional tools used by the attackers and sometimes even the data that has been ex-filtrated.

The data often reveals the breadth of the victims the attackers are targeting and it is almost always broader than the conventional wisdom based on analysis of individual or even small clusters of activity. While a campaign may maintain subsets of infrastructure for specific geographic regions we have found that campaigns often have a global, thematic focus. While there are often exceptions, the attackers often target "communities of interest" that stretch across geographic boundaries. We have found that campaigns that are well known in the U.S. aggressively targeting Asia (particularly Taiwan, Japan, South Korea and Vietnam) as well as Russia and Central Asian countries.

The information obtained from the attacker's command and control servers reveals that the average length of compromise is considerable. In the case of GhostNet, for example, we found that the average compromise was 145 days with many being compromised for over 400 days (the longest was 660 days). In other cases, such as LURID, we were able to discover the campaign

codes the attackers were using which revealed that they had conducted 301 attacks in a two month period (between June 9 2011 and August 3 2011).

The data may reveal the IP addresses from which the attackers are interacting with the command and control servers. In the past, as was the case in GhostNet, the attackers often hosted their infrastructure in China. We now see command and control servers hosted in a variety of countries, especially in the U.S. Furthermore, the attackers are often using tools such as "Htran" that allow them to "proxy" through an intermediary computer so that the attackers and the victims computers never directly connect to one another. These developments further obfuscate attribution.

2. Recommendations

Broaden the scope of stakeholders. While the US government, military, critical infrastructure and defense industrial base are well understood as targets and often share information amongst each other, the scope of the threat extends globally and government needs to engage additional stakeholders both inside and outside the US. Major malware-based espionage campaigns have been uncovered and disclosed by researchers and private companies who need clearer avenues of information exchange. In addition, the NGO community, particularly those involved in democracy promotion and Tibetan activism, are also being targeted by the same campaigns that threaten the national security of the US. While many of these threats are understood by a select few, the indicators that are so critical to defense are rarely shared outside trusted circles in order to avoid potentially tipping off the attackers who may subsequently adapt and change tactics. However, the scope of the problem is so severe that I recommend broadening stakeholder engagement with diverse communities in order to build a wider network of trust so that the threat intelligence that is so critical for an active defense can be shared.

Encourage responsible disclosures of compromise. No one wants to admit that their organization has been compromised. However, this obscures the true extent of the problem. It hides the constant attacks and successful penetrations by a discrete set of targeted malware campaigns affecting governments, businesses and civil society organizations around the world. When Google broke the disclosure barrier and revealed that they had been breached, in what is now known as "Aurora", it firmly placed the issue of targeted malware attacks in the public domain and made it clear that companies face the same attacks that had previously focused on government and military networks. Recently, the SEC has been encouraging companies to disclose cyber attacks because they recognize the effect of such attacks and their importance to investors. Ultimately, the public needs to understand the full scope of the APT problem.