FireEye™

The Advanced Cyber Attack Landscape

Contents

Executive Summary

Recent reports have pinpointed China as a key driver behind cyber attacks designed to steal intellectual property and other sensitive information. But advanced cyber attacks are not confined to just one nation. Rather, cyber attacks are a widespread global activity. During the course of 2012, FireEye® monitored more than 12 million malware communications seeking instructions—or callbacks—across hundreds of thousands of infected enterprise hosts, capturing details of advanced attacks as well as more generic varieties. Callback activity reveals a great deal about an attacker's intentions, interests, and geographic location. Based on end-user data, FireEye found:

1. **Malware has become a multinational activity**. Over the past year, callbacks were sent to command and control (CnC) servers in 184 countries—a 42 percent increase when compared to 130 countries in 2010.

2. **Two key regions stand out as hotspots driving advanced cyber attacks: Asia and Eastern Europe**. Looking at the average callbacks per company by country the Asian nations of China, South Korea, India, Japan, and Hong Kong accounted for 24 percent. Not far behind, the Eastern European countries of Russia, Poland, Romania, Ukraine, Kazhakstan, and Latvia comprised 22 percent. (North America represented 44 percent but as we point out in Finding #6, this is due to CnC servers residing in the United States to help attackers with evasion.)

3. **The majority of Advanced Persistent Threat (APT) callback activities are associated with APT tools that are made in China or that originated from Chinese hacker groups**. By mapping the DNA of known APT malware families against callbacks, FireEye discovered that the majority of APT callback activities—89 percent—are associated with APT tools (mostly a tool named Gh0st RAT) that are made in China or that originated from Chinese hacker groups.

4. **Attackers are increasingly sending initial callbacks to servers within the same nation in which the target resides**. This approach not only improves evasion for the cybercriminals but it also gives organizations a strong indicator of which countries are most interesting to attackers.

5. **Technology organizations are experiencing the highest rate of APT callback activity**. With a high volume of intellectual property, technology firms are natural targets for attackers and are experiencing heavy APT malware activity.

6. **For APT attacks, CnC servers were hosted in the United States 66 percent of the time, a strong indicator that the U.S. is still the top target country for attacks**. As previously mentioned, attackers increasingly put CnC servers in the target country to help avoid detection. With such a high proportion of CnC servers, the U.S. is subject to the highest rate of malware attacks. This is most likely due to a very high concentration of intellectual property and digitized data that resides in the U.S.

7. **Techniques for disguising callback communications are evolving**. To evade detection, CnC servers are leveraging social networking sites like Facebook and Twitter for communicating with infected machines. Also, to mask exfiltrated content, attackers embed information inside common files such as JPGs to give network scanning tools the impression of normal traffic.

8. **Attack patterns vary substantially globally**:

    a. **South Korean firms experience the highest level of callback communications per organization**. Due to a robust internet infrastructure, South Korea has emerged as a fertile location for cybercriminals to host their CnC infrastructure. For example, FireEye found that callbacks from technology firms are most likely to go to South Korea.

    b. **In Japan, 87 percent of callbacks originated and stayed in country**. This may indicate the high value of Japanese intellectual property.

    c. **Exit rates for Canada and the U.K. were the highest at 99 and 90 percent respectively.** High exit rates indicate attackers are unconcerned about detection. In Canada and the U.K., attackers appear to be unconcerned about detection and pursue low-hanging fruit opportunistically.

This FireEye report draws on data from hundreds of thousands of hosts and millions of callback communications to provide a broader context of the global threat landscape.

Introduction

When seeking to root out corruption, journalists and detectives are taught to follow the money. When seeking to understand and combat today's new breed of cyber attacks, security teams are well advised to follow the callbacks—the traffic that flows from compromised devices to CnC servers. Drawing on end-user data gathered by the FireEye Malware Protection System™ (MPS), this report provides an in-depth look at the callback activity associated with this new breed of cyber attacks, including sophisticated malware and APTs that are evading traditional defenses and compromising organizations. This report provides new, unprecedented intelligence on the types and locations of organizations being targeted, as well as the locations of the CnC servers used in these attacks.

Today's organizations are constantly being victimized and besieged by sophisticated cyber attacks—including zero-day exploits and APTs—and traditional IT security defenses are providing little protection. The cybercriminals and nation-states behind these attacks are utilizing targeted approaches and advanced malware over the Web and email to routinely bypass traditional signature-based perimeter and endpoint security defenses, compromise enterprise networks, and exfiltrate sensitive and classified data.

This new breed of cyber attacks typically includes several distinct yet coordinated stages. They include system infection, malware download, callbacks, data exfiltration, and lateral movement. Within these stages, callbacks represent a critical juncture, one in which compromised machines establish communication with an external CnC server. Once this communication is established, cybercriminals can achieve a host of malicious objectives, including modifying malware to evade detection, exfiltrating data, and expanding an attack within a victim organization.

Given the pivotal role these callbacks play within the new breed of cyber attacks being waged today, it is important for security practitioners and researchers to understand them. This callback activity provides vital insights into the nature of today's attacks, offering details about the family of malicious software employed, the countries and industries of the companies being targeted, and the location of the CnC servers orchestrating these attacks.

The Data Source for this Report

FireEye is in a unique position to illuminate the callback activity associated with today's new breed of attacks. The FireEye MPS is deployed with firewalls, next-generation firewalls, intrusion prevention systems (IPS) and other security gateways, and represents an additional line of defense. The FireEye platform is designed to detect and thwart advanced attacks—after they've bypassed the traditional signature-based security defenses that enterprises have in place.

Thousands of FireEye appliances have been deployed around the globe. These appliances automatically gather threat intelligence associated with today's new breed of cyber attacks. This data can then be anonymized, aggregated, analyzed, and shared[1] via the FireEye Dynamic Threat Intelligence cloud. This report draws on an analysis of the callback data collected during the course of 2012. Over the year, callbacks were sent to 184 countries with more than 12 million events logged across hundreds of thousands of infected machines.

In conducting its research, FireEye calculated the number of events detected at each deployment, and then normalized the data based on per end-user metrics in order to make accurate comparisons of callback rates for various locations and industries. With this approach, FireEye has been able to gain vital insights into the locations of companies that are most frequently targeted. This data tells us that companies in specific countries are much more likely to be the target of frequent attacks than organizations in other locations.

Finding 1: Malware has become a multinational activity

During 2012 callbacks were sent to CnC servers in 184 countries—a 41 percent increase over the FireEye findings in 2010. In 2011, CnC servers were discovered in 150 countries, and in 2010, 130 countries. Cybercriminals and nation-states use these servers to orchestrate various types of malicious activities.

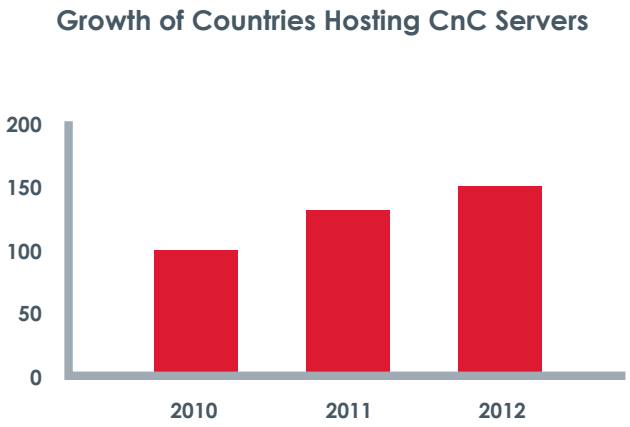

Figure 1: Total number of countries worldwide hosting CnC servers

1 FireEye intelligence is shared by end users in such industries as healthcare, financial services, technology, and manufacturing. Data from end users in government agencies is not shared, so is not included in these findings.

The distribution of countries involved is also changing. In 2011, the United States, Ukraine, and Russia were the top countries for hosting CnC servers. In 2012, the top 20 nations hosting CnC servers were:

1. U.S.
2. South Korea
3. China
4. Russia
5. Ukraine
6. Germany
7. Poland
8. Romania
9. India
10. Kazakhstan
11. Taiwan
12. U.K.
13. Canada
14. Netherlands
15. Japan
16. France
17. Turkey
18. Argentina
19. Brazil
20. Hong Kong

While Ukraine and Russia were in the top three countries to host CnC servers in 2011, they dropped to less than 5% in the 2012 findings.

Looking back we see explosive growth in the complexity of the malware problem, which created new challenges for the organizations that were relying solely on traditional security approaches to protect against malware. For example, this global evolving threat landscape poses significant challenges to organizations that are employing a traditional geographic location-based approach in which network administrators apply firewall rules to block suspicious activities going to countries like China or Russia. With hackers increasingly hosting their servers in less suspicious countries, these traditional defenses simply will not work anymore to protect against many sophisticated attacks. These trends make it clear that IT security governance models need to evolve.

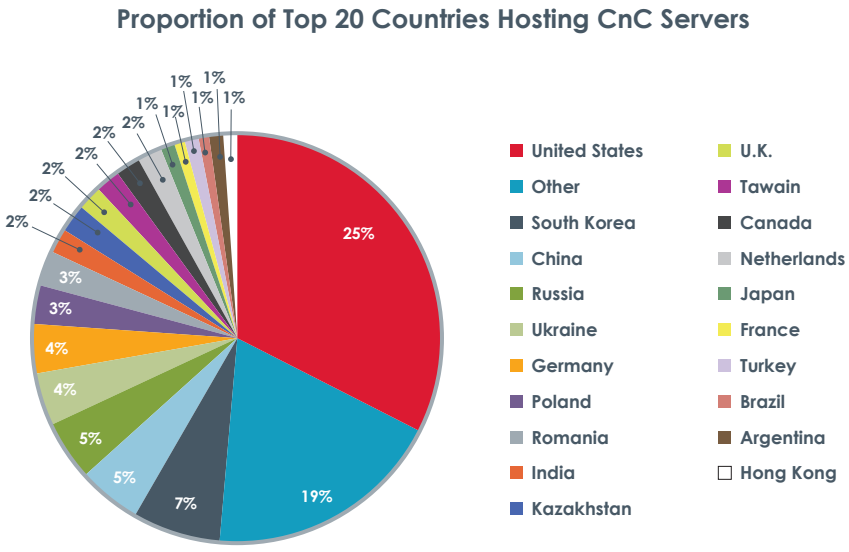

Figure 2: Top 20 countries hosting CnC servers

Global Distribution of CnC Servers

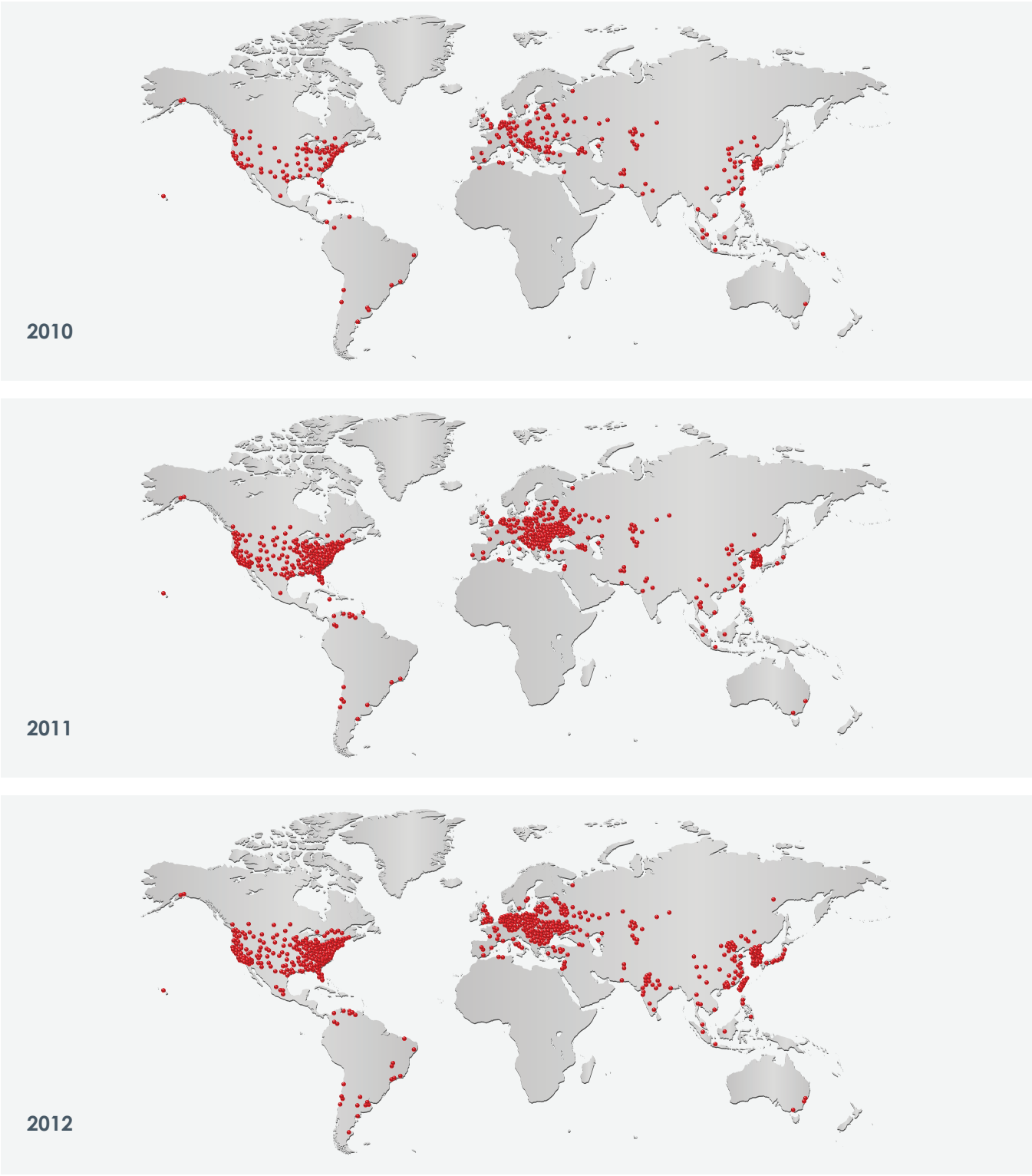

Figure 3: Heatmaps showing the distribution of CnC servers worldwide over time

Finding 2: Two key regions stand out as hotspots: Asia and Eastern Europe

Looking at the total callbacks per company across various regions, the Asian nations of China, South Korea, India, Japan, and Hong Kong accounted for 24 percent of the world's volume. Russia, Poland, Romania, Ukraine, Kazhakstan, and Latvia comprised 22 percent. North America represented 44 percent, but as pointed out in Finding #6, this is due to CnC servers residing in the United States to help attackers with evasion.

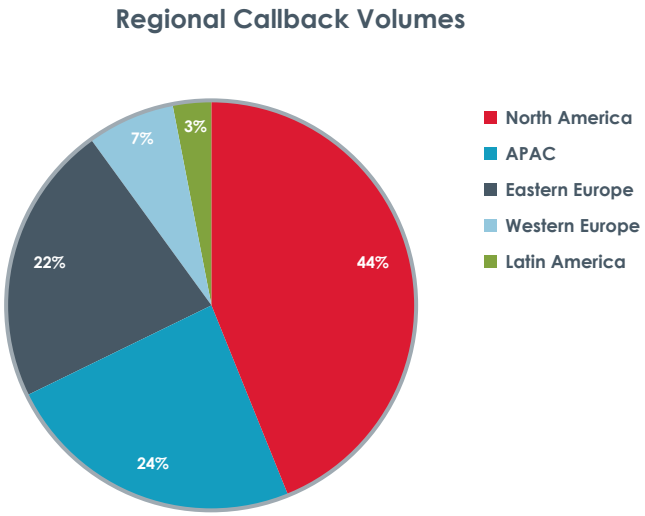

Figure 4: Average total callbacks per company summarized by region

Finding 3: The majority of APT callback activities are associated with APT tools that are made in China or that originated from Chinese hacker groups

By mapping the DNA of known APT malware families to APT-related callbacks, FireEye discovered that the majority of callback activities—89 percent—are associated with APT tools that are made in China or that originated from hacker groups based in China. However, only a relatively small percentage of callbacks associated with these tools are going directly to CnC servers based in China. The main tool, developed in China, is called Gh0st RAT.

In addition, FireEye discovered that the majority of the most popular non-APT callback activities in Japan and South Korea are also associated with APT tools that are made in China or that originated from Chinese hacker groups. And as previously referenced, only a small percentage of these callbacks are going to CnC servers based in China.

Finding 4: Attackers are increasingly sending initial callbacks to servers within the same nation in which the victim resides

Callback data makes it clear that APT attackers have become smarter about how they carry out their campaigns. To better evade detection hackers are increasingly placing CnC servers within the same nation as their targets. Cybercriminals often set up multiple network hops between their location and the CnC infrastructure. Thus, while a compromised system will communicate with a CnC server in one location, the cybercriminal may very well be in a different location.

In addition, in the past, CnC servers may have been hosted in locations far away from the target organization which would raise suspicions. This approach is increasingly uncommon. Attackers may go to significant lengths to try to make the attack and CnC traffic look as normal as possible. This is illustrated by the high percentage of callback traffic that originates and terminates within a country, such as Japan and South Korea, but that is based on malware developed by Chinese hacker groups.

We did find exceptions. In countries where defensive approaches lag, a large proportion of callbacks immediately exited the target nation (see Finding #8C).

Finding 5: Technology organizations are experiencing the highest rate of APT callback activity

While today's new breed of cyber attacks target many verticals, FireEye data reveals some industries are much more frequently attacked than others. In 2012, technology companies experienced the highest rate of callback activity associated with next-generation cyber attacks. Whether the objectives are theft of intellectual property, sabotage, or modification of source code that can support further criminal initiatives, it is clear that technology companies are prominent and consistent targets. The most interesting verticals for APT activity are:

- Technology
- Banking, Finance, and Insurance
- Manufacturing
- Healthcare
- Entertainment and Media
- Energy and Utilities
- Telecommunications
- Business services
- Retail
- Logistics and Transportation

In addition, while data from government agencies is not included in these statistics one only needs to read the headlines of industry publications to know that these organizations are also frequently being targeted.

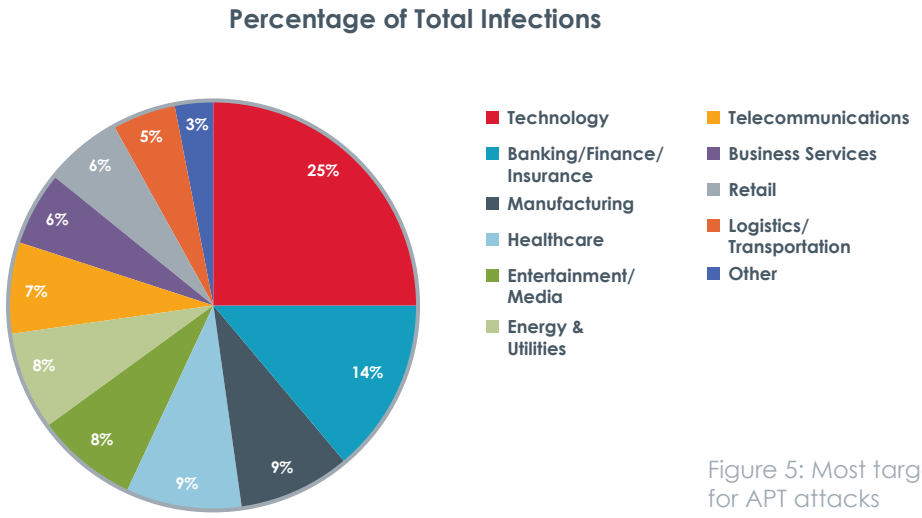

Figure 5: Most targeted industries for APT attacks

Finding 6: For APT attacks, CnC servers were hosted in the United States 66 percent of the time, a strong indicator that the U.S. is still the top target country for attacks

The 2012 data reveals that the United States hosts the most CnC servers that receive callbacks associated with RAT tools originating in China. Given that the majority of victims of these attacks are based in the U.S., it is clear that attackers are housing CnC servers in the same country as their targets in order to help avoid raising suspicions. FireEye found that 66 percent of CnC servers were hosted in the U.S. The U.S. is a prime target due to a high volume and concentration of intellectual property and digitized data.

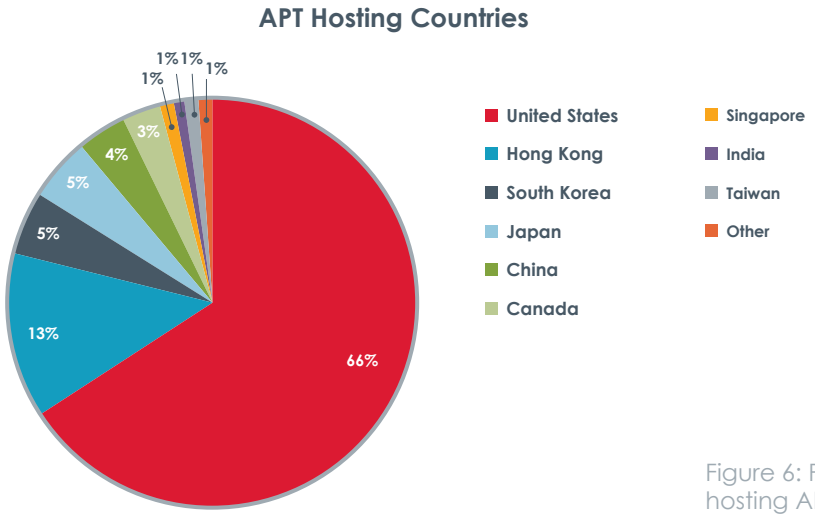

Figure 6: Percentage of countries hosting APT-focused CnCs

Finding 7: Techniques for disguising callback communications are evolving

Today, attackers spend significant effort innovating CnC communications methods.[2] Two recent advances highlight the variety of methods attackers deploy:

- **Use of social networks:** Attackers use social networks to easily and anonymously receive updates on exploits. Sites such as Facebook and Twitter are commonly used. However, in China local social networking sites are used. Baidu, a Chinese social network (see figure 7a), is used by attackers to get updates from malware.
- **Network Inspection Evasions:** In order to appear as normal network traffic and evade network deep packet inspection technologies, attackers now embed commands or stolen information within files that look standard, such as JPGs. Figure 7b is an example of an intercepted JPG file that contained attacker commands.

Figure 7a: screenshot of Baidu, a Chinese social network site

Figure 7b: JPG file that contained attacker commands

Finding 8: Attack patterns vary substantially globally

Finding 8A: South Korean firms are experiencing the highest event rate per organization

In 2012, companies in South Korea received the highest number of events per organization. In recent years, South Korea has emerged as a fertile location for cybercriminals to host their infrastructure and it seems these criminals are focused on targeting local organizations.

South Korea has a high concentration of manufacturing firms and other organizations with sensitive intellectual property. It appears cybercriminals that are looking to exploit this intellectual property have set up a significant CnC infrastructure within South Korea's borders.

2 For a deeper dive on this topic a recent FireEye blog gives more detail: http://blog.fireeye.com/research/2012/11/more-phish.html

Finding 8B: In Japan, 87 percent of callbacks originating in Japan stayed in country

Organizations across many countries are receiving significant volumes and rates of sophisticated cyber attack activity, but what distinguishes Japan is the percentage of callback traffic that originates and terminates within its borders. FireEye found that 87 percent of the callback traffic originating in Japan also terminated in the country, which is the highest percentage of intra-country callback traffic. South Korea had the second highest percentage of intra-country traffic, with 82 percent originating and terminating in the country. The United States was third on this list, with 47 percent of the callback traffic originating in the country also terminating there. A big part of these findings can be attributed to the fact that cybercriminals try to disguise their whereabouts by employing communications across multiple locations.

Like South Korea, Japan also has a high concentration of manufacturing firms and other organizations with sensitive intellectual property. This characteristic has likely drawn in attackers who host their CnC infrastructure within Japan's borders.

Finding 8C: Exit rates for Canada and the U.K. were the highest at 99 and 90 percent respectively

Depending on location, some companies see a big percentage of traffic remaining within the same country, while others see a big percentage of traffic leave the country. Organizations based in Canada fall very much into the latter category. Canadian companies encountered significant volumes of attack activity, and 99 percent of the callback traffic generated exited the country. In the U.K., 90 percent of callbacks stayed in country. Interestingly, companies in other countries, such as Turkey and Saudi Arabia, also saw 90 percent or more of callback traffic departing the country.

There are several factors that influence where CnC servers are located, and why traffic may be more likely to exit the country of the organization targeted. In some cases, attacks are less focused and stealthy, and the companies targeted are simply the low-hanging fruit for opportunistic cybercriminals—regardless of where the organization is located. In other cases, the location of CnC servers is driven by the relative ease or difficulty of setting up a nefarious CnC infrastructure. Finally, sometimes cybercriminals will set up CnC servers in specific regions in order to try and evade detection.

Finding 8D: Callbacks from technology firms are most likely heading to South Korea

Striking trends emerge when assessing the destinations of callbacks that originate in specific industries, which illustrate the high-level trends concerning the location and intent of the most active cybercriminals.

It is clear that a large percentage of cybercriminals targeting technology firms base their CnC servers in South Korea. In fact, three times more callback activity from technology firms is directed at South Korea than the United States, the second highest destination. However, much of this activity going to CnC servers located in South Korea is associated with tools developed in China.

For those targeting financial services, it is a two-country race, with the United States coming in number one and South Korea a very close second. In other industries, including manufacturing, healthcare, and energy and utilities, the United States is the destination of the vast majority of callbacks.

In a sense, South Korea is plagued by RATs. It is clear from the 2012 data that South Korea is one of the top callback destinations in the world and that some of the country's callback activities are associated with more targeted attacks that employ RATs. Most likely, one of the reasons is that South Korea has one of the best Internet infrastructures in Asia, making it a preferred locale for attackers looking to host their CnC servers.

By far, the most popular RAT sending callbacks to South Korea is known as Gh0st. Callbacks associated with Gh0st are not exclusive to South Korea, but for some reason this RAT is commonly used by attackers who set up their CnC servers in South Korea, which seems to indicate either a larger group or many groups have made this their tool of choice. Gh0st malware originated from a Chinese hacker group and has for a long time been a popular tool for hacker groups based in China.

Conclusion

Depending on your organization's industry and location, the scope, frequency, and nature of attacks your organization encounters can vary substantially. By assessing callback information, you can begin to take a more realistic look at the threats your organization will likely face, and the steps needed to guard against these attacks. To learn more be sure to explore the FireEye Advanced Cyber Attack Landscape [http://www.fireeye.com/cyber-attack-landscape/]. These interactive maps enable you to select specific views, including by country and industry, to see callback traffic details based on data collected by FireEye.

About FireEye

FireEye® has pioneered the next generation of threat protection to help organizations protect themselves from being compromised. Cyber attacks have become much more sophisticated and are now easily bypassing traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways, compromising the majority of enterprise networks. The FireEye platform supplements these legacy defenses with a new model of security to protect against the new breed of cyber attacks. The unique FireEye platform provides the industry's only cross-enterprise threat protection fabric to dynamically identify and block cyber attacks in real time. The core of the FireEye platform is a signature-less, virtualized detection engine and a cloud-based threat intelligence network, which help organizations protect their assets across all major threat vectors, including Web, email, mobile, and file-based cyber attacks. The FireEye platform is deployed in over 40 countries and more than 1,000 customers and partners, including over 25 percent of the Fortune 100.

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