FireEye Advanced Threat Report: 2013

FireEye Labs

February 2014

Contents

Executive Summary

This FireEye Advanced Threat Report (ATR) provides a high-level overview of computer network attacks discovered by FireEye in 2013. We believe the activities described in this report were designed to accomplish one or more of the following:

- Steal intellectual property
- Eavesdrop on sensitive government communications
- Undermine the overall security of national security-related sites

Advanced attacks described as advanced persistent threats (APTs) involve activity largely supported, directly or indirectly, by a nation-state.

The data contained in this report comes from the FireEye® Dynamic Threat Intelligence™ (DTI) cloud, which provides attack metrics shared by FireEye customers across the globe. It offers strong evidence that malware infections occur within enterprises at an alarming rate. It also shows that advanced attackers can penetrate legacy defenses such as firewalls and anti-virus (AV) defenses with ease.

During 2013, FireEye:

- Analyzed 39,504 unique cyber security incidents (more than 100 per day on average)
- Associated 4,192 of these attacks with APT actors (more than 11 per day on average)
- Discovered 17,995 unique malware infections due to APT activity (almost 50 per day on average)
- Logged over 22 million command-and-control (CnC) communications (more than one every 1.5 seconds on average)
- Found that the U.S., Canada, and Germany were targeted by the highest number of unique malware families

These attacks took many different forms, and arrived from nearly every country and territory in the world. In 2013, FireEye:

- Tracked 159 distinct APT-associated malware families
- Identified that some publicly available hacker tools, such Dark Comet, LV, Gh0stRAT, and Poison Ivy were also used by APTs
- Discovered CnC infrastructure in 206 countries and territories. That's up from FireEye's data of 184 in 2012 (81 percent of the United Nations)
- Found that the U.S., Germany, South Korea, China, Netherlands, United Kingdom, and Russia were home to the most CnC servers

Based on FireEye data, the ten countries that were most frequently targeted by APTs in 2013 were:

1. United States
2. South Korea
3. Canada
4. Japan
5. United Kingdom
6. Germany
7. Switzerland
8. Taiwan
9. Saudi Arabia
10. Israel

APTs target carefully selected, high-value data in every industry vertical:

- APTs targeted more than 20 vertical industry segments, from aerospace to wholesalers
- Education, finance, and high-tech were the most targeted verticals overall
- The U.S., South Korea, and Canada had the highest number of distinct industry verticals targeted

Based on our data, the following verticals were targeted by the highest number of unique malware families:

1. Government (Federal)
2. Services and consulting
3. Technology
4. Financial services
5. Telecommunications
6. Education
7. Aerospace and defense
8. Government (State and local)
9. Chemicals
10. Energy

FireEye security alerts are the result of multi-vector analysis. In 2013, the Web and email threat vectors were the most significant, as the following statistics reveal:

- FireEye analyzed five times more Web-derived alerts than email-derived alerts overall
- Country-by-country, FireEye saw three times more Web alerts than email alerts

Possible reasons for the gap between Web- and email-based attacks include increased awareness of spear phishing, increased use of social media, and users who are continuously connected to the Web.

Zero-day attacks are an important weapon in every APT arsenal, as the following statistics reveal:

- FireEye discovered eleven zero-day attacks in 2013
- In the first half of 2013, Java was the most common zero-day focus for attackers
- In the second half of 2013, FireEye observed a burst of Internet Explorer (IE) zero-days used in watering hole attacks
- Crimeware groups are now proficient in developing Java exploits
- APTs targeted U.S. government websites in “watering hole” attacks
- Attackers regularly find creative ways to “escape” malware sandboxes

In 2014, we predict that Java zero-day attacks may become less prevalent, but the list of browser-based vulnerabilities will grow.

About the Data in This Report

FireEye threat prevention platforms are normally placed behind traditional network defenses such as firewalls, next-generation firewalls, intrusion prevention systems (IPS), and anti-virus (AV) software. The FireEye appliances execute suspected malware in a virtual environment to observe and block malicious behavior. Most often, they analyze malicious activities that have succeeded in slipping past existing network defenses. Therefore they typically have extremely low false-positive alerts.

Nonetheless, this report describes only attacks that fell within the FireEye field of vision in 2013. In other words, this research data encompasses only those attacks that met two criteria:

1. They struck FireEye customers
2. Those FireEye customers agreed to share their attack metrics with FireEye.

Therefore, the data in this report does not represent all advanced, targeted attacks worldwide.

Furthermore, we took the precaution of filtering out any data that might skew our conclusions, such as test network traffic or apparent manual intelligence sharing among our customer base. We also realize that some techniques, tactics, and procedures (TTPs) are used by both cybercriminals and nation-state threat actors. APTs use multiple TTPs, and any given TTP can be used by multiple APTs. The complex dynamics associated with advanced computer network operations complicates cyber defense analysis. In order to mitigate possible confusion, FireEye employs conservative filters and manual crosschecks to reduce the likelihood of misidentifying attacks.

Introduction

In 2013, FireEye threat prevention platforms discovered millions of malicious incidents. From these, our researchers look for APT attacks, which we define as the use of distinct TTPs that appear to be employed directly or indirectly by a nation-state or professional criminal organization. The goals of such attacks range from short-term cyber espionage to long-term subversion of targeted networks.

In 2013, cyber attackers were active around the clock. Across our customer base, FireEye analyzed nearly 40,000 unique, advanced attacks—more than 100 per day on average. From these, we categorized over 4,000 unique attacks as APT-directed (more than 11 unique APT attacks per day on average). And we discovered nearly 18,000 unique malware infections due to APT activity (almost 50 per day on average).

These targeted attacks appear in many disguises, and can come from any point on the globe. In 2013, FireEye tracked 159 malware families associated with APT activity. And we discovered initial CnC infrastructure within 206 national top-level domains (TLDs) located in every region of the world.

Highest Number of Advanced Persistent Threat Attacks

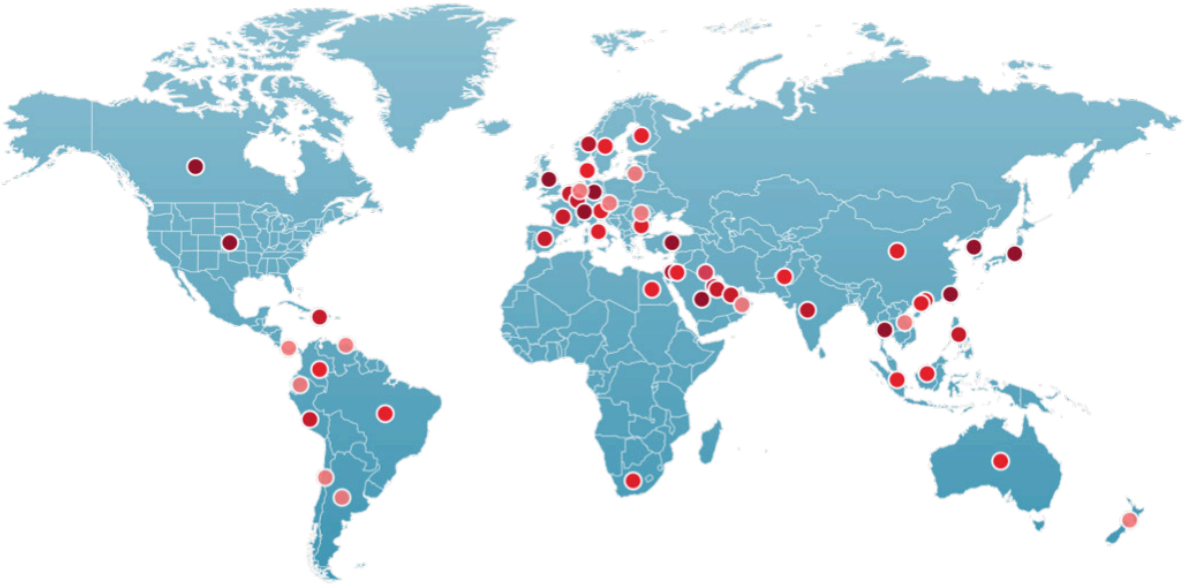


Figure 1: APT attacks by country

Over the course of 2013, APT actors targeted many nations around the world, seeking national security secrets, research and development data, and much more.

Figure 1 depicts the dispersed nature of APT targeting. The hue of each colored circle represents the volume of APT activity in that country.

Based on FireEye data from 2013, the top 10 countries targeted by APT actors are the following:

1. United States
2. South Korea
3. Canada
4. Japan
5. United Kingdom
6. Germany
7. Switzerland
8. Taiwan
9. Saudi Arabia
10. Israel

FireEye Security Alerts: 2013

FireEye alerts stem from many types of suspicious network events and security-related incidents. Based on our 2013 data, Figure 2 displays the relationship between two of the most common threat vectors: email and Web traffic.

Each circle represents a country, and its location in the graph represents the number of FireEye alerts generated from malicious email- and Web-based incidents.

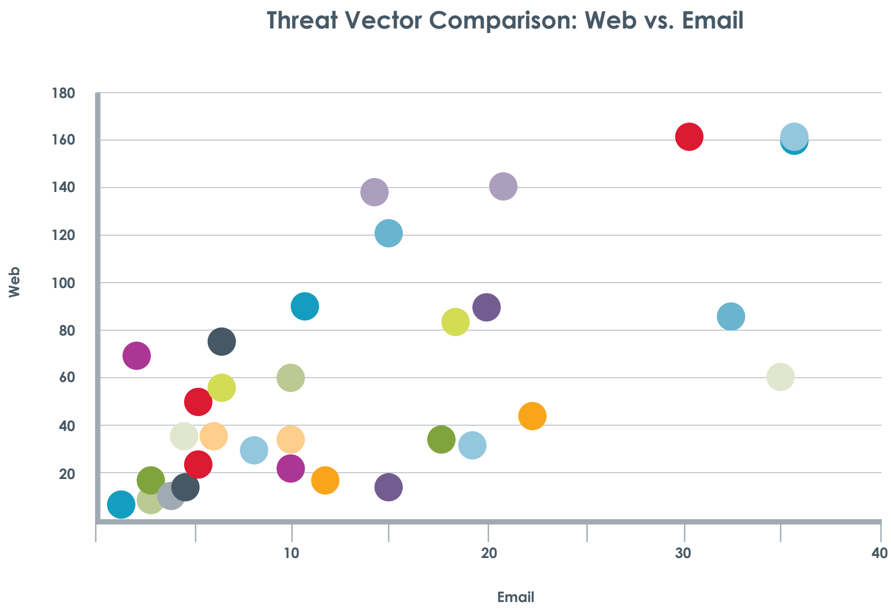


Figure 2: Threat vector comparison: Web vs. email

The graph excludes many outliers, showing only the lower left portion of a much larger data set for 2013. But the statistical relationship between email and Web alerts is clear. The overall number of network operations leveraging the Web vector was five times higher than those that leveraged the email vector. Country-by-country, the average number of Web-derived alerts was over three times higher than for email-derived alerts.

The takeaway for security administrators: in 2013, attackers were more likely to attempt to compromise a target network via malicious Web traffic than by sending malicious email traffic (although both methods were widely used). This gap may be due to an increased awareness of the threat posed by spear phishing, and a combination of increased social media communications and extremely complicated websites that are continuously connected to the Internet.

Highest Number of Unique APT Families, by Country

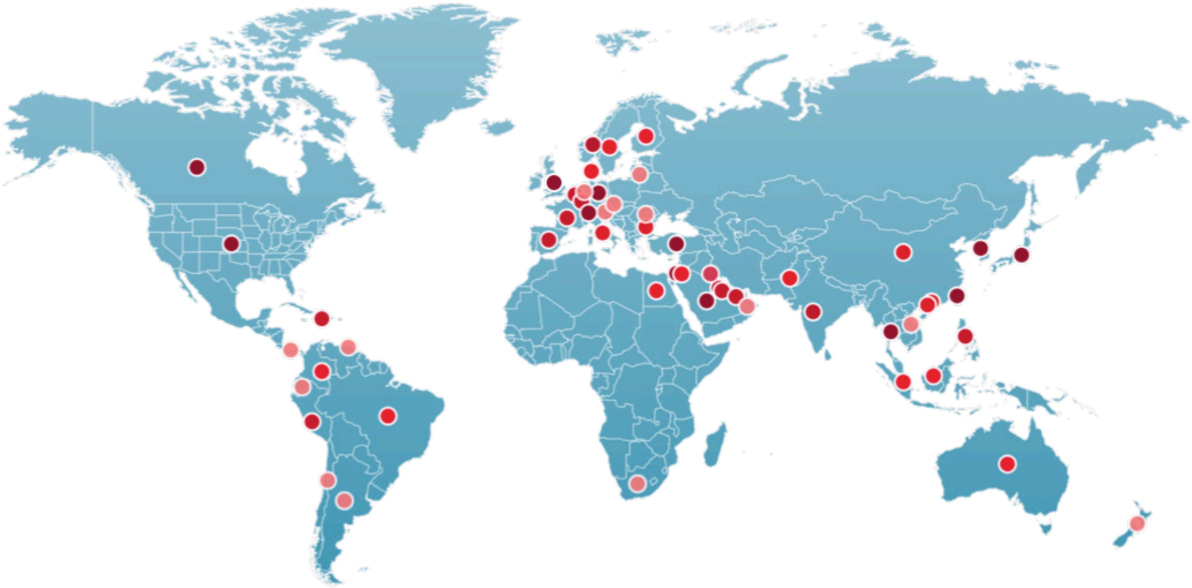


Figure 3: Unique APT families by country

Another important way to gauge the strategic nature of cyber security is to measure the number of unique APT families that target each country.

Weighing the variety of malware families provides a better sense of the complexity of the threat that each country faced in 2013. A higher number of APT malware families likely means a higher number and variety of adversaries—and a bigger challenge in defending against them.

Based on FireEye data in 2013, the United States is the world leader in this category—by far—with more than a hundred APT malware families detected. Canada, in second place, has 52—less than half the U.S. total.

Here are totals for the top 10 countries by malware family:

1. United States (125)
2. Canada (52)
3. Germany (45)
4. United Kingdom (43)
5. Japan (37)
6. Taiwan (35)
7. South Korea (34)
8. Israel (31)
9. Switzerland (22)
10. Turkey (21)

Common Malware Families: a Closer Look

Let’s take a closer look at three of the most common malicious software tools that FireEye tracked in 2013: Dark Comet, LV, and Gh0stRAT. These are publicly available remote administration tools, or RATs. They are often delivered to their targets as a key component of coordinated attacks that may use previously unknown (zero-day) software flaws or clever social engineering—or both.

RATs posses a devastating combination of power and simplicity. These malicious programs have been designed from the ground up to allow attackers to accomplish anything they wish on a target computer. That includes anything from data theft to data modification to a denial-of-service attack.

And these RATs typically require little technical savvy to use. They have simple graphical user interfaces (GUI) that allow attackers to simply point and click their way through a victim’s network. Common features include key logging, screen capture, video capture, file transfers, system administration, password theft, and traffic relay.

The majority of attacks that used Dark Comet, LV, or Gh0stRAT in 2013 involved non-APT actors. But APTs also employ these public RATs for two reasons:

1. They are effective
2. They may help APTs to fly under the radar of many cyber defenders, who may not realize that APTs use publicly available software for advanced, targeted computer network operations.

Dark Comet

FireEye has tracked the use of Dark Comet in targeted cyber operations since 2012. This malware leverages both email and Web traffic as attack vectors.

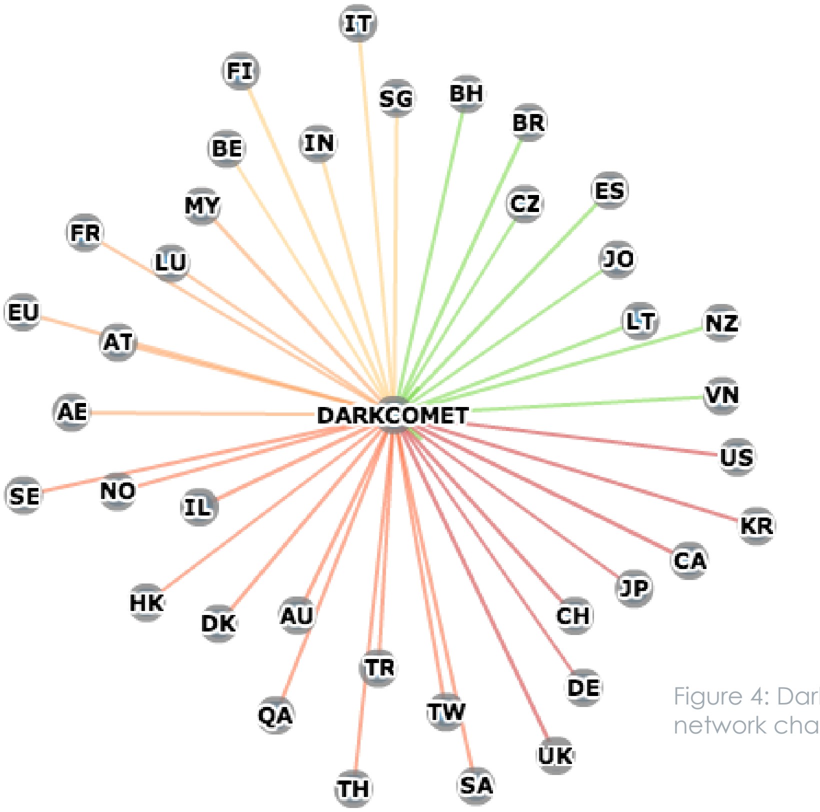


Figure 4: Dark Comet network chart

Figure 4 shows the countries in which FireEye most frequently found Dark Comet in 2013, ranked clockwise. (The colors represent various thresholds of activity). The most common targets were the U.S., South Korea, Canada, Japan, Switzerland, Germany, and the United Kingdom.

Figure 5 shows the most common vertical targets of Dark Comet operations in 2013. The top three verticals were financial services, energy/utilities, and education.

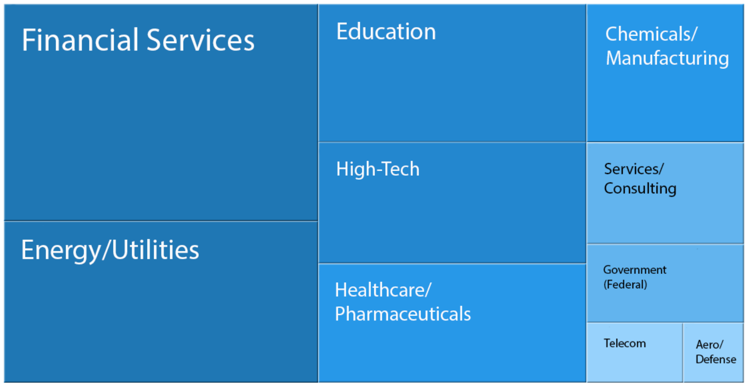


Figure 5: Dark Comet vertical targets

LV

FireEye has tracked the use of LV in targeted cyber operations since 2012. This malware leverages both email and Web traffic as attack vectors.

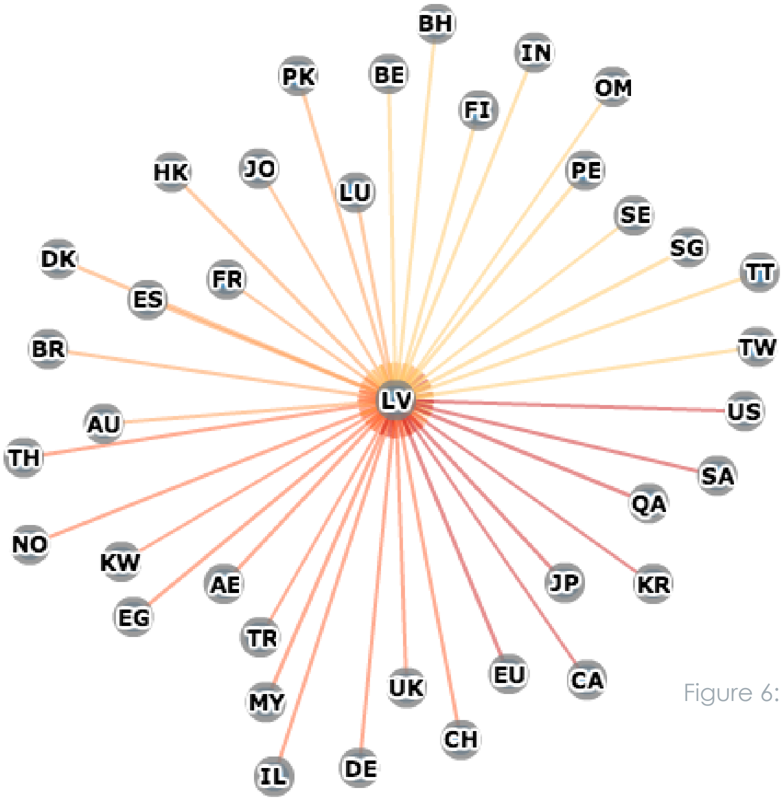


Figure 6: LV network chart

Figure 6 shows the countries in which FireEye most frequently found LV in 2013, ranked clockwise. (The colors represent various thresholds of activity). The most common targets were the U.S., Saudi Arabia, Qatar, South Korea, Japan, Canada, the European Union, Switzerland, and the United Kingdom.

Figure 7 shows the most common vertical targets of LV operations in 2013. The top four verticals were education, high-tech, government, and financial services.

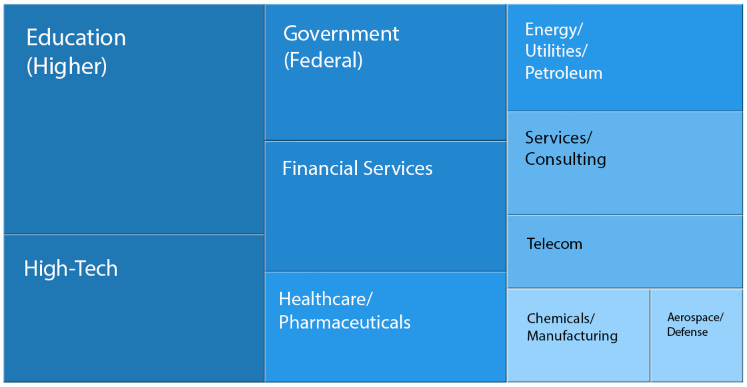


Figure 7: LV vertical targets

Gh0stRAT

FireEye has tracked the use of Gh0stRAT in targeted cyber operations since 2012. This malware leverages both email and Web traffic as attack vectors.

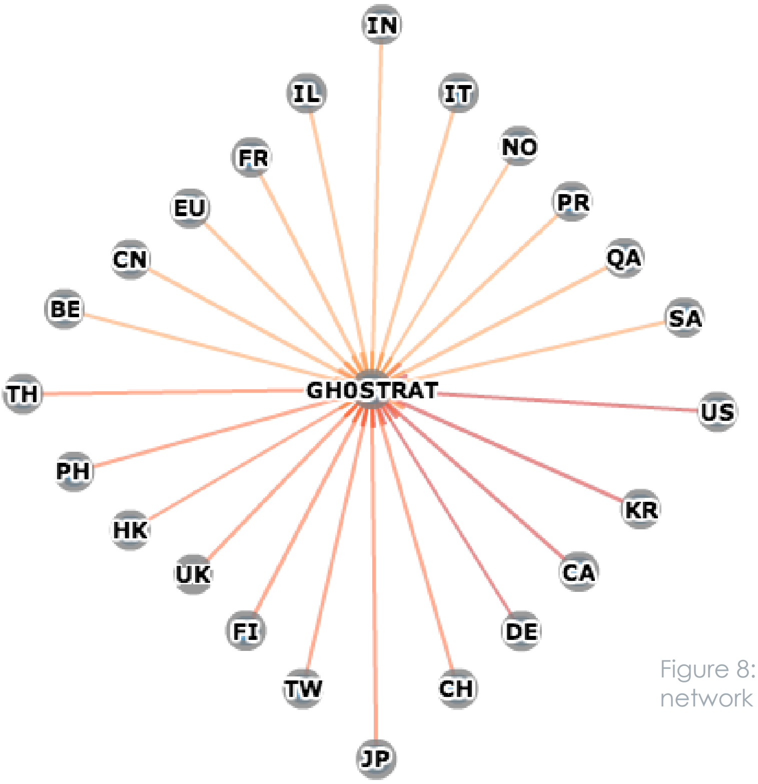


Figure 8: Gh0stRAT network chart

Figure 8 shows the countries in which FireEye most frequently found Gh0stRAT in 2013, ranked clockwise. (The colors represent various thresholds of activity). The most common targets were the U.S., South Korea, Canada, Germany, Switzerland, and Japan.

Figure 9 shows the most common vertical targets of Gh0stRAT operations in 2013. The top three verticals were high-tech, education, and financial services.

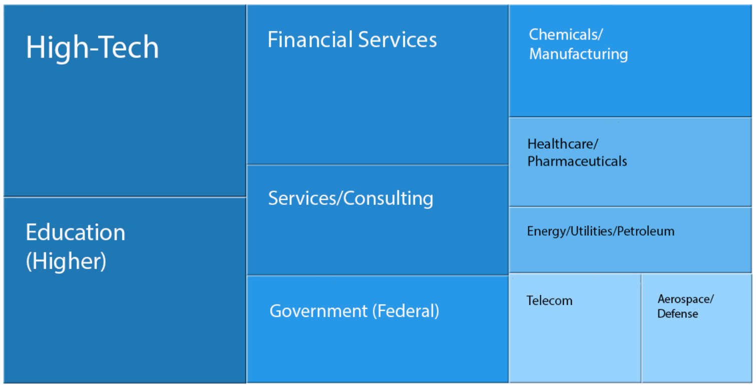


Figure 9: Gh0stRAT vertical targets

Malware Case Study: Poison Ivy

Since 2008, the publicly available Poison Ivy (PIVY) RAT (www.poisonivy-rat.com) has played a key role in some of the world's most damaging cyber attacks. These attacks include the compromise of RSA's SecureID authentication technology, the "Nitro" attacks against strategic political targets, and a "watering hole" trap targeting visitors to a U.S. government website.

System administrators should know that APTs are not above using free software such as PIVY to conduct targeted network operations. As described in a 2013 FireEye report, at least three threat actors based in China currently use PIVY: "admin@338", "th3bug", and "menuPass".

Although RATs have a well-earned reputation for being "script kiddy" tools, they nonetheless provide APT actors with a wide range of attractive features. And while PIVY is already eight years old, its maturity likely stands in its favor — just like hacking tools Nmap, Nessus, and John the Ripper.

APTs come with an additional bonus: PIVY is so widely used that any single attack may get lost in the noise. Or network defenders dismiss the discovery of PIVY as common cybercrime rather than a targeted APT attack.

To distinguish between crimeware and APT variants of PIVY, FireEye released a comprehensive set of tools in 2013 called "Calamine" to help network defenders cope with this challenge.

Calamine comprises two distinct open source tools: a PIVY configuration decoder and a PIVY communications decryptor. The information provided by Calamine to security analysts can be used to identify APT attackers, and even to reveal their targets and motives.

One distinguishing characteristic of RATs (in contrast to, say, many criminal botnets) is that they require communication between the target and a real human attacker. This means that RAT activity is more targeted and personal—and therefore more identifiable.

The use of commodity RATs such PIVY in APT attacks is unlikely to change in the near future. But an increased awareness of this and similar tools (combined with the use of innovative software such as Calamine) could complicate and disrupt their plans, forcing them to retool and change tactics. As such, APTs may be forced to adopt less widely used—and perhaps more uniquely identifiable—TTPs in the future.

Top Ten Vertical Targets: Worldwide

Based on the highest number of targeted operations discovered by FireEye threat prevention platforms in 2013, the top ten industry vertical targets are listed below. Each of these verticals possesses substantial intellectual property value, and often plays an important role in national security affairs.

1. **Education:** universities are home to cutting-edge research and emerging technology patents; unfortunately, their networks are large and porous.
2. **Financial Services:** most financial transactions today are conducted via the Internet, whether between people, businesses, or governments.
3. **High-Tech:** some hardware and software are used by millions of people; they can offer attackers an exponential return on investment.
4. **Government:** these bodies organize nations, determine policy, enforce law, and manage national security affairs.
5. **Services/Consulting**: large companies often have long supply chains and large contractor bases; at the political level, this includes think tanks.
6. **Energy/Utilities:** in physics, energy is required for any kind of "work," including starting engines, turning on city lights, or launching a missile.
7. **Chemicals/Manufacturing:** chemistry is the study of matter, and bridges all of the natural sciences, including their relationship to energy.
8. **Telecom (Internet, Phone & Cable):** this category encompasses all long-distance communications, by electrical signals or electromagnetic waves.
9. **Healthcare/Pharmaceuticals:** this category encompasses the development of medications and the provision of medical care.
10. **Aerospace/Defense/Airlines:** this category includes the development of spacecraft with myriad commercial and military applications.

Highest Number of Malware Families per Vertical

To get a better sense of the complexity of targeted operations against industry verticals, it is important to examine how many unique APT families typically target each vertical.

This number is a strong indicator of the number and variety of unique adversaries that target each vertical, and it helps to measure how difficult it will be to successfully defend any given infrastructure.

The table below displays the top ten most targeted verticals, based on the number of unique, APT-associated malware families that FireEye discovered in 2013.

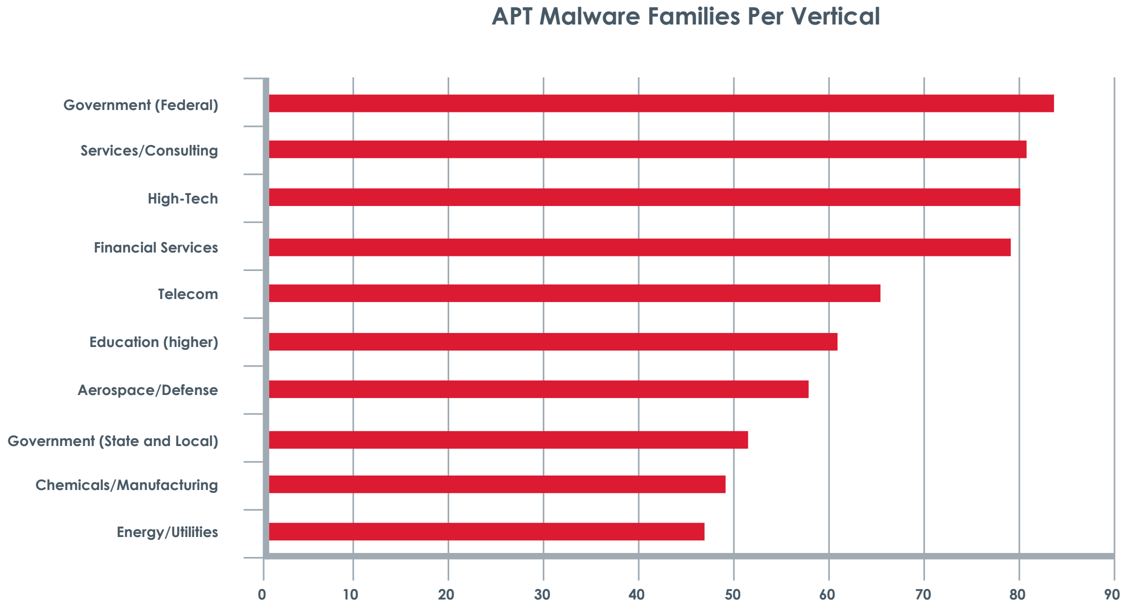


Figure 10: APT malware families per vertical

FireEye found that Government (Federal) was the most targeted vertical in the world in 2013, with 84 of the 159 malware families documented by FireEye.

Services/Consulting, High-Tech, and Financial Services were also heavily targeted; each had roughly half of the overall number of malware families present on their computer networks.

Highest Number of Targeted Verticals, by Country:

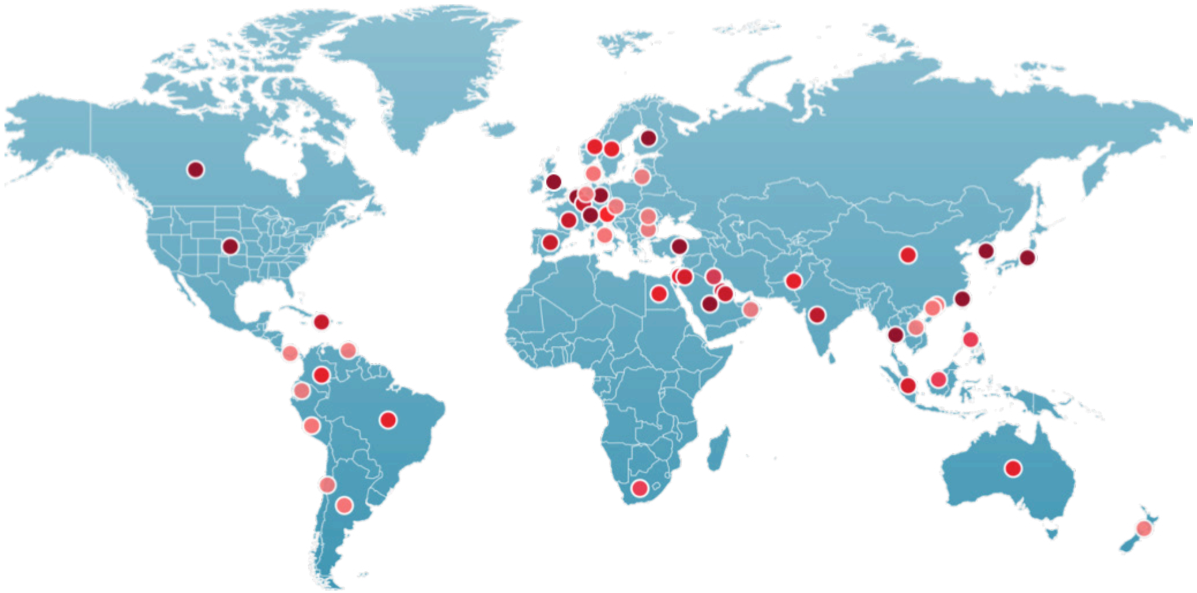


Figure 11: Targeted verticals by country

Within each country, it is also possible to demonstrate the breadth of interest in that country, from the point of view of attackers, simply by counting the number of distinct industry verticals that were targeted over the course of 2013.

Compiled from FireEye's data, the list below shows the countries that suffered the widest range of targeted computer network operations against their verticals last year.

1. United States (20)
2. South Korea (16)
3. Canada (13)
4. France (12)
5. Thailand (12)
6. United Kingdom (12)
7. Japan (11)
8. Turkey (11)
9. Germany (9)
10. Saudi Arabia (9)

The United States was the clear winner. FireEye documented attacks against 21 verticals in 2013, so the U.S. scored a near-perfect record!

Initial CNC Infrastructure: World Map

In today's cyber security environment, advanced network operations can come from any point on the globe. In 2013, FireEye discovered initial CnC infrastructure located within the Internet Protocol (IP) space of 206 distinct country code TLDs.

In 2013, FireEye analyzed 767,318 unique CnC communications, or more than one per minute; and 22,509,176 total CnC communications, or more than one every 1.5 seconds on average.

The world map below, which shows where initial CnC infrastructure has been discovered by FireEye in 2013, clearly demonstrates that CnC infrastructure is pervasive across the world.

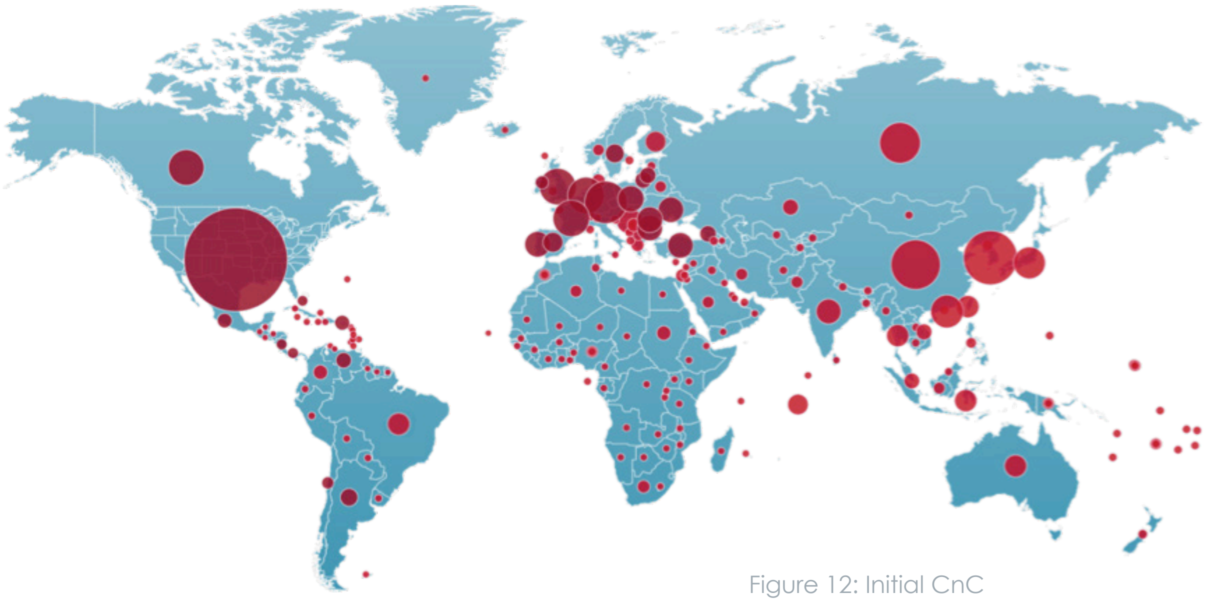


Figure 12: Initial CnC infrastructure: world map

Based on the data collected for 2013, the following are the top ten countries that were home to CnC infrastructure in 2013:

1. United States (24.1%)
2. Germany (5.6%)
3. South Korea (5.6%)
4. China (4.2%)
5. Netherlands (3.7%)
6. United Kingdom (3.5%)
7. Russia (3.2%)
8. Canada (2.9%)
9. France (2.7%)
10. Hong Kong (1.9%)

Although the United States had nearly one quarter of the world's initial CnC infrastructure in 2013, the largest international clusters of malicious servers were based in Europe and Asia.

Initial CNC Infrastructure: Country Breakdown

The pie chart below shows a breakdown of the world's initial CnC infrastructure by country, as seen by FireEye in 2013. It was not possible to show all 206 country code TLDs, but the primary countries are displayed, including the top ten: the U.S., Germany, South Korea, China, the Netherlands, the United Kingdom, Russia, Canada, France, and Hong Kong.

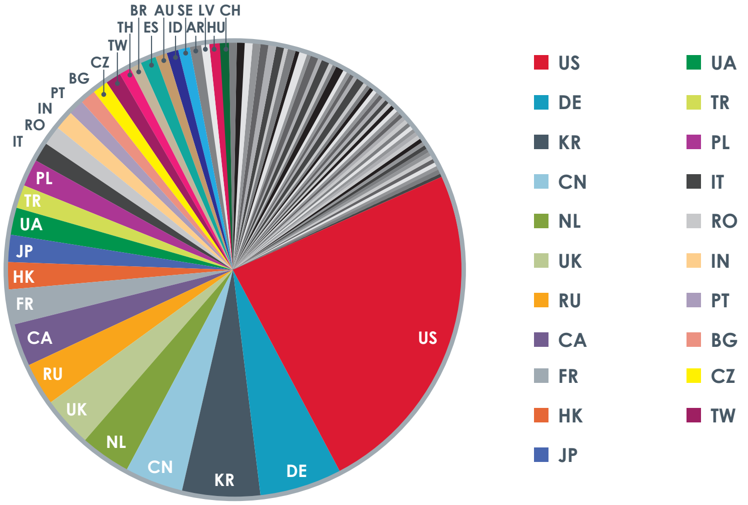


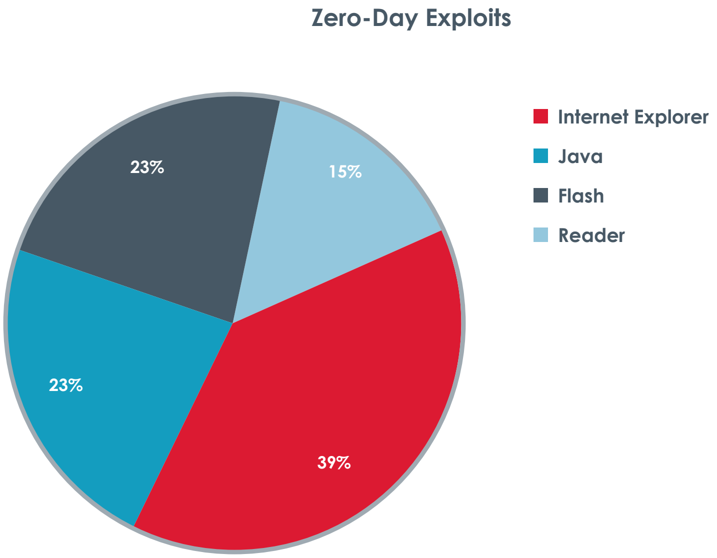
Figure 13: Initial CnC infrastructure: country breakdown

Note: It is important to remember that advanced attackers typically leverage multiple layers of infrastructure as a means of operational obfuscation (hence our use of the qualifying word "initial"). Just because malware communicates with a server in a particular country does not necessarily mean that the threat actor is based in that country. Attackers often route or proxy their traffic through multiple, intermediate servers, in order to make attribution more difficult for network defenders.

Attack Analysis: Zero-days

FireEye discovered eleven zero-day attacks in 2013, more than any other security company. This section highlights the most common software targets for zero-day attacks in 2013.

The figure below displays the most prominent zero-day exploitation campaigns that FireEye researchers followed last year.



Java Attacks

FireEye observed that, during the first half of 2013, Java was the most common focus for attackers in developing zero-day attacks. One of the primary reasons is that exploit development against Java is much easier than for most other software. Operating system attack mitigation, designed to prevent the execution of arbitrary code, is often ineffective in preventing Java exploits, because the attacker merely has to corrupt a "pointer" to the Java Security Manager.

Unfortunately, Java has historically received less attention from security researchers, but the recent surge in publicized Java vulnerabilities may help to improve security for the platform in the future. What was once limited to a subset of APT actors has now become mainstream for many crimeware groups. Java exploit development has become that easy.

Browser Attacks

During the second half of 2013, FireEye researchers observed a burst of Internet Explorer (IE) zero-days used in "watering hole" attacks, in which an attacker compromises a key website that is frequented by specific interest groups—who are in fact the ultimate target (and victim if their browsers are vulnerable to the exploit). We believe these attacks were serious enough to make Internet Explorer the single most dangerous zero-day attack vector in 2013.

The majority of these attacks targeted older versions of IE, such as 7.0 and 8.0. The reason for this could be due to the security enhancements in newer versions of Windows and Internet Explorer. Nonetheless, we also saw a higher number of zero-days that targeted more recent versions of IE, as well as the employment of new techniques to bypass Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP), which include leveraging Use After Free (UAF) and information leakage vulnerabilities. Unfortunately, this means that even newer versions of IE are likely not safe from attack, and that traditional security protections such as ASLR/DEP are also vulnerable.

Application Sandbox Escapes

Some applications use sandboxing techniques to separate potentially vulnerable code from privileged system access. In the event of an attack, any malicious code runs with reduced privileges, and the attacker would have to launch a separate attack to gain full access.

Two recent attack campaigns—one targeting Adobe Flash (CVE-2013-0643/0648),[1,2] and the other Adobe Reader (CVE-2013-0640/0641),[3,4] —exploited critical sandbox vulnerabilities. A third campaign used a Windows XP Kernel vulnerability to escape the Adobe Reader sandbox (CVE-2013-3346/5065).[5,6] A fourth campaign (CVE-2013-0633/0634),[7,8] embedded Flash exploits in Microsoft Office files to bypass sandboxes altogether, but its scope was therefore limited to users running Office 2008.

This highlights two important aspects of bypassing a sandbox. First, sandboxes make an attacker's job more difficult (and therefore more expensive) by requiring at least two exploits – one to obtain code execution, and another to bypass the sandbox. Second, even given these increased challenges, it is clear that attackers still find a sufficient return on investment to devote the time, energy, and resources required to bypass sandboxes altogether.

Targeting, Obfuscation, and Evasion

Some recent zero-day campaigns have presented vexing challenges to cyber defense researchers. They focused less on obfuscation, and more on regional/occupational targeting, reinfection prevention, and partitioned exploit files. For example, some attackers sent Microsoft Word documents that, instead of containing embedded images directly, referenced malicious .PNG files on remote servers. These files would exploit CVE-2013-1331[9]—a recently discovered Microsoft Office PNG-parsing vulnerability that may have been exploited by attackers since 2009. The critical problem for security researchers was that, even when in possession of the infected Word documents, they could not reverse engineer the exploit unless the attacker's server was still online and hosting the .PNG file.

[1] CVE-2013-0643, Common Vulnerabilities and Exposures (CVE), MITRE Corporation, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0643

[2] CVE-2013-0643, Common Vulnerabilities and Exposures (CVE), MITRE Corporation, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0648

[3] CVE-2013-0643, Common Vulnerabilities and Exposures (CVE), MITRE Corporation, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0640

[4] CVE-2013-0643, Common Vulnerabilities and Exposures (CVE), MITRE Corporation, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0641

[5] CVE-2013-0643, Common Vulnerabilities and Exposures (CVE), MITRE Corporation, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3346

[6] CVE-2013-0643, Common Vulnerabilities and Exposures (CVE), MITRE Corporation, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5065

[7] CVE-2013-0643, Common Vulnerabilities and Exposures (CVE), MITRE Corporation, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0633

[8] CVE-2013-0643, Common Vulnerabilities and Exposures (CVE), MITRE Corporation, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0634

[9] CVE-2013-1331, Common Vulnerabilities and Exposures (CVE), MITRE Corporation, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1331.

Similarly, attackers targeted CVE-2013-3163 (a Microsoft Internet Explorer (IE) 8 through 10 vulnerability that allows arbitrary code execution or a denial of service through memory corruption, via a crafted website),[10] sending the exploit in two parts. First, a Flash file was used to manipulate the target computer's memory heap, locate the Windows "`ntdll`" file's memory address, and build a return-oriented programming (ROP) attack. Second, JavaScript was used to trigger the CVE-2013-3163 vulnerability. Although it is possible that this attack was designed to work in two stages for reasons of mere functionality, it is also true that security researchers, if they are only in possession of the tainted Flash file, cannot fully reverse engineer the exploit.

Two attacks employed the watering hole technique[, in which the attacker compromises a website that is frequented by specific interest groups—who are in fact the ultimate target. In the first instance, attackers leveraged CVE-2013-1347, or IE 8's inability to properly handle objects in memory, allowing arbitrary code execution through the access of an object that was not properly allocated, or that had even been deleted.[11] The second attack used CVE-2013-3918,[12] which is a weakness in the InformationCardSignInHelper ActiveX control, in order to obtain code control, and CVE-2014-0266,[13] in order to leak information about DLLs running on the system. Once the exploits were hosted on the compromised websites, any website visitor using a vulnerable browser would be affected.

In an effort to remain stealthy, many of these recent attacks have used browser cookies or Flash storage to prevent reinfection. For security researchers, this means that one cannot run a captured exploit twice on the same test machine, or the exploit will detect this and abort, serving a blank page instead, or redirect the test browser to an innocuous website. This technique is trivial to circumvent for reverse engineering purposes, but it may have general operational value in helping an attack to stay below the detection radar of many users.

[10] CVE-2013-3163, Common Vulnerabilities and Exposures (CVE), MITRE Corporation, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3163.

[11] "IE Zero Day is Used in DoL Watering Hole Attack," Yichong Lin, May 3, 2013, FireEye Labs http://www.fireeye.com/blog/technical/cyber-exploits/2013/05/ie-zero-day-is-used-in-dol-watering-hole-attack.html.

[12] CVE-2013-1347, Common Vulnerabilities and Exposures (CVE), MITRE Corporation, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1347.

[13] CVE-2013-1331, Common Vulnerabilities and Exposures (CVE), MITRE Corporation, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3918.

Predictions

In the dynamic and quickly evolving landscape of cyber security, it is difficult to predict the future. However, here are two trends worth watching.

- Java zero-days may be less prevalent. Despite the comparative ease of Java exploit development, the frequent release of new Java zero-days stopped after February 2013, and it is unclear why. It may be in part due to the security warning pop-ups in Java 1.7, or to the increased attention of white hat security researchers. It is also possible that a sufficient demographic uses vulnerable versions of Java—such that exploit authors have little incentive to continue finding more bugs.
- In 2014, browser-based vulnerabilities may be more common. Attackers are becoming increasingly comfortable with bypassing ASLR in browsers, and, in contrast to Java and classic input-parsing vulnerabilities, the discovery of browser-based zero-days has not slowed.

About FireEye

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 1,500 customers across more than 40 countries, including over 100 of the Fortune 500.