FireEye™

FireEye Advanced Threat Report – 2H 2012

Contents

Executive Summary

This report provides a detailed, current look at the nature of advanced threats targeting organizations today. Drawing on data gathered by FireEye® from several thousands of appliances at customer sites around the world, across 89 million events, this report provides an overview of the current threat landscape, evolving advanced persistent threat (APT) tactics, and the level of infiltration seen in organizations' networks today. Key findings include:

- **On average, a malware event occurs at a single organization once every three minutes.** Malware activity has become so pervasive and attacks so successful at penetrating legacy defenses—network firewalls, Intrusion Prevention Systems (IPS), and anti-virus (AV)—that once every three minutes organizations on average will experience a malicious email file attachment or Web link as well as malware communication—or callback—to a command and control (CnC) server. Across industries, the rate of malware activity varies, with technology experiencing the highest volume with about one event per minute.
- **Technology is the most targeted vertical.** Due to a high concentration of intellectual property, technology firms are hit with an intense barrage of malware campaigns, nearly double the next closest vertical.
- **Some industries are attacked cyclically, while some verticals experience erratic attacks.** Certain verticals, such as technology, experience fairly consistent attacks while others, such as healthcare, see much more volatility due to key events or attackers selectively focusing on specific verticals.
- **Attackers use common business terms used in the file names as spear phishing bait.** Spear phishing remains the most common method for initiating advanced malware campaigns. When sending spear phishing emails, attackers opt for file names with common business terms to lure unsuspecting users into opening the malware and initiating the attack. These terms fall into three general categories: shipping and delivery, finance, and general business. The top phrase in malware file names, for example, was "UPS".
- **ZIP files remain the preferred file of choice for malware delivery over email.** Malware is delivered in ZIP file format in 92 percent of attacks.
- **Malware writers have focused significant effort on evasion.** Several innovations designed to better evade detection have appeared. For example, instances of malware were uncovered that execute only when users move a mouse, a tactic which could dupe current sandbox detection systems since the malware doesn't generate any activity. In addition, malware writers have also incorporated virtual machine detection to bypass sandboxing.
- **Attackers are increasingly using dynamic link library (DLL) files to improve persistence.** By avoiding the more common .exe file type, attackers leverage DLL files to prolong infections.

This report provides a detailed look at trends taking place in specific industries, as well as a case study on an attack that was waged during the course of 2012.

Introduction and Methodology

The FireEye Advanced Threat Report for the second half of 2012 is based on research and trend analysis conducted by the FireEye Malware Intelligence Lab. Drawing on the data gathered from several thousand appliances at customer sites around the world, across 89 million malware events, this report provides an overview of the current threat landscape, evolving APT tactics, and the level of infiltration seen in organizations' networks today.

FireEye is in the unique position to illuminate this advanced targeted attack activity. There have been thousands of deployments around the world of the FireEye threat protection platform. These appliances automatically gather threat intelligence and send it to the FireEye Dynamic Threat Intelligence™ (DTI) cloud, which also includes new threat findings from the FireEye Malware Intelligence Lab. To report on this data, the FireEye Malware Intelligence Lab gathered industry-specific data and normalized it by customer to provide an accurate, consistent basis for comparing industry-specific trends and activities.

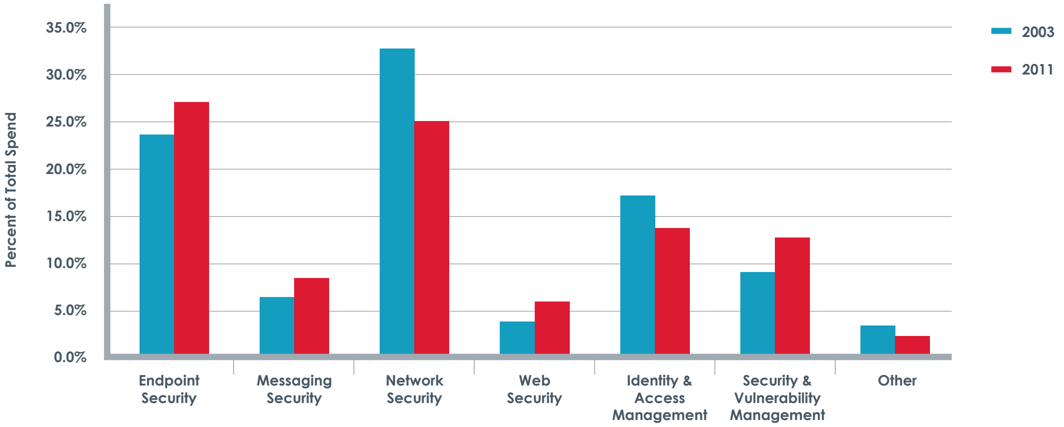
It is critical to note that the FireEye platform is deployed behind firewalls, next-generation firewalls, IPS, and other security gateways, and represents the last line of defense for organizations. Thus, the advanced activity being tracked and reported in this report represents the attacks that successfully evaded all of these initial defenses. Given this vantage point, FireEye is able to gain a highly informed perspective on the advanced threats that routinely bypass signature-, reputation-, and basic behavior-based technologies—the technologies that organizations spend $28 billion each year on, but that are failing to thwart today's advanced threats.

The report starts by providing some industry-level trends. The next few sections are organized around the process of infection following the anatomy of attacks from infection to payload to callbacks. Finally, the report offers a detailed look at one major malware campaign known as Operation Beebus.

IT security spending: a renewal market

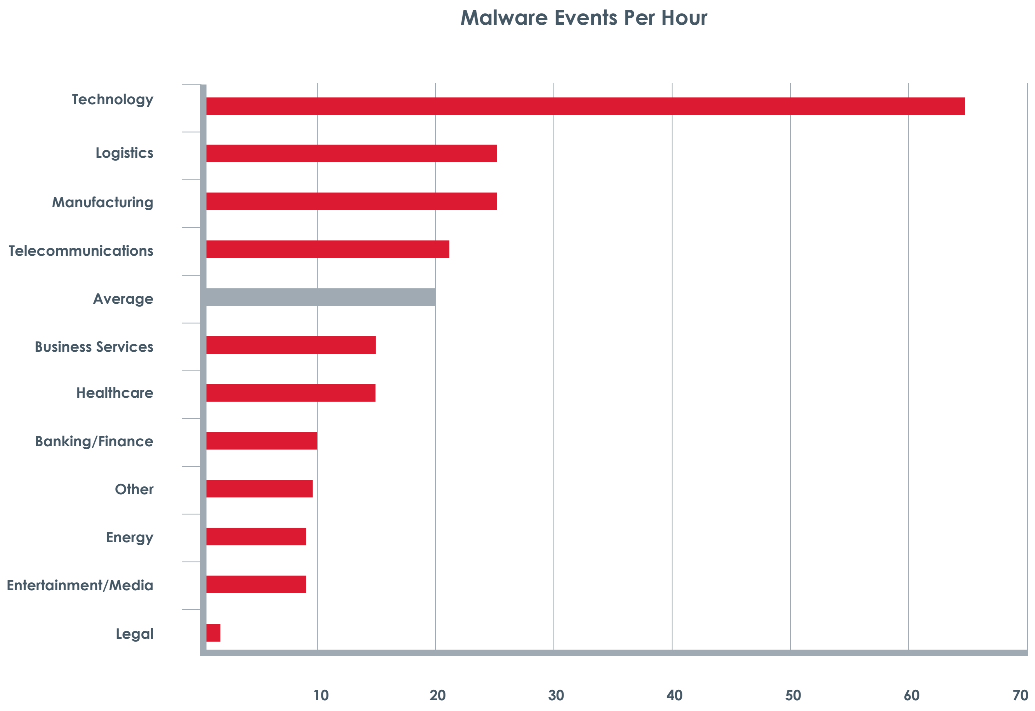
According to IDC, between 2003 and 2011, total IT security spend grew from $12 billion to $28 billion while the mix of security technologies purchased remained fairly consistent. In effect, organizations have been spending more without making any major changes to their security strategies. This stasis has helped malware writers move into the pole position in the cyber arms race.

IT Security Spend by Segment: 2003 and 2011



Finding 1: On average, malware events occur at a single organization once every three minutes

Across industries, organizations on average are experiencing malware-related activities once every three minutes. This activity can include the receipt of a malicious email, a user clicking a link on an infected website, or an infected machine making a callback to a command and control server.



This nearly continuous rate of attacks and activities is indicative of a fundamental reality: these attacks are working, yielding dividends. Through these mechanisms, attackers are circumventing traditional and next-generation firewalls, IPS, Web and email gateways, and other defenses—and they are then able to achieve their objectives, whether they are looking to make financial gains, steal intellectual property, or advance nation-state objectives.

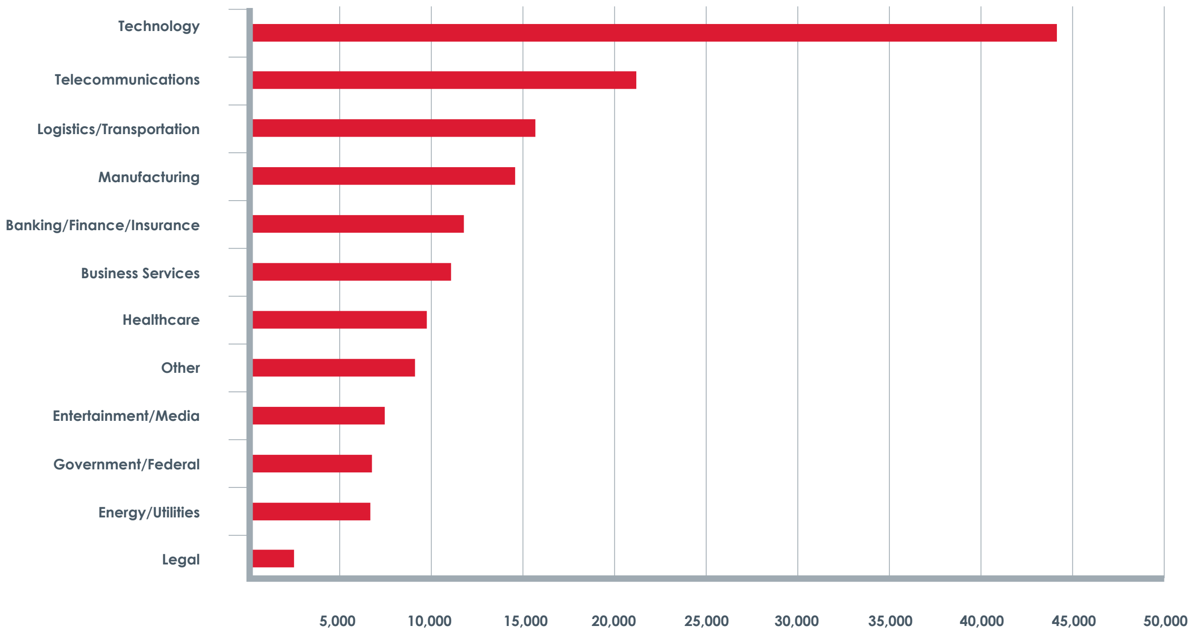
While virtually every company in every industry is being targeted by advanced attacks, there are some clear variances across industries. The goals of attackers, the tactics they use, and the frequency of attack can all vary substantially depending on the industry being examined. The following sections look at the similarities and differences that are seen in various industries.

Finding 2: Technology is the most targeted vertical

Due to a high concentration of intellectual property, technology firms are hit with an intense barrage of malware campaigns, nearly double compared to the next closest vertical.

The rate of malware activity being witnessed also provides useful insights into the threats facing various industries. The chart that follows offers a look at the rates of malware activity for companies in specific industries.

Industry Average Events Per Customer Second Half 2012



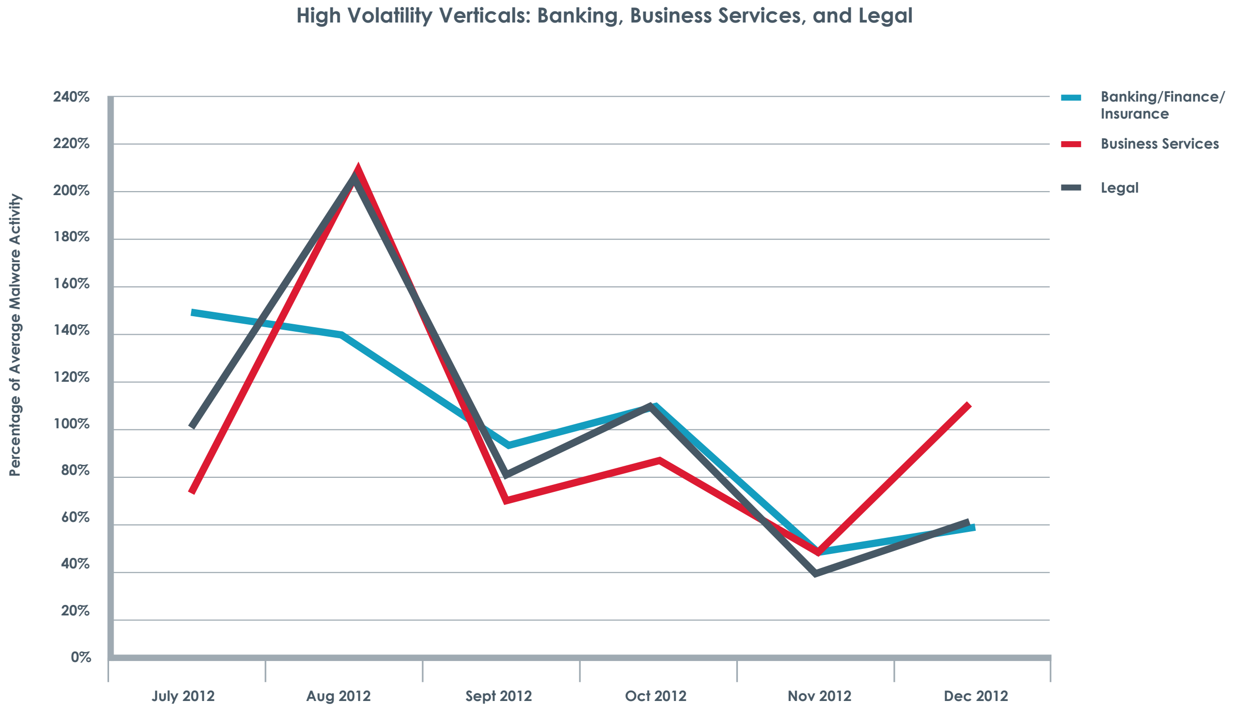
High technology firms lead all industries with malware activity, while telecommunications, logistics and transportation, manufacturing, and financial services round out the top five. The reasons organizations in these industries are being more highly targeted varies. Generally organizations in high technology, telecommunications, and manufacturing possess valuable intellectual property. In financial services the motive is clearly focused on fraud and theft.

Finding 3: Some industries are attacked cyclically, while some verticals experience erratic attacks

Certain verticals, such as technology, experience fairly consistent attacks while others, such as business services, see much more volatility. Generally all verticals experience a high volume of activity that is consistent year round. In this section we provide graphs and background on how the incidence of malware activities varies in each industry during the second half of 2012.

Finding 3A: High volatility verticals—banking, business services, and legal

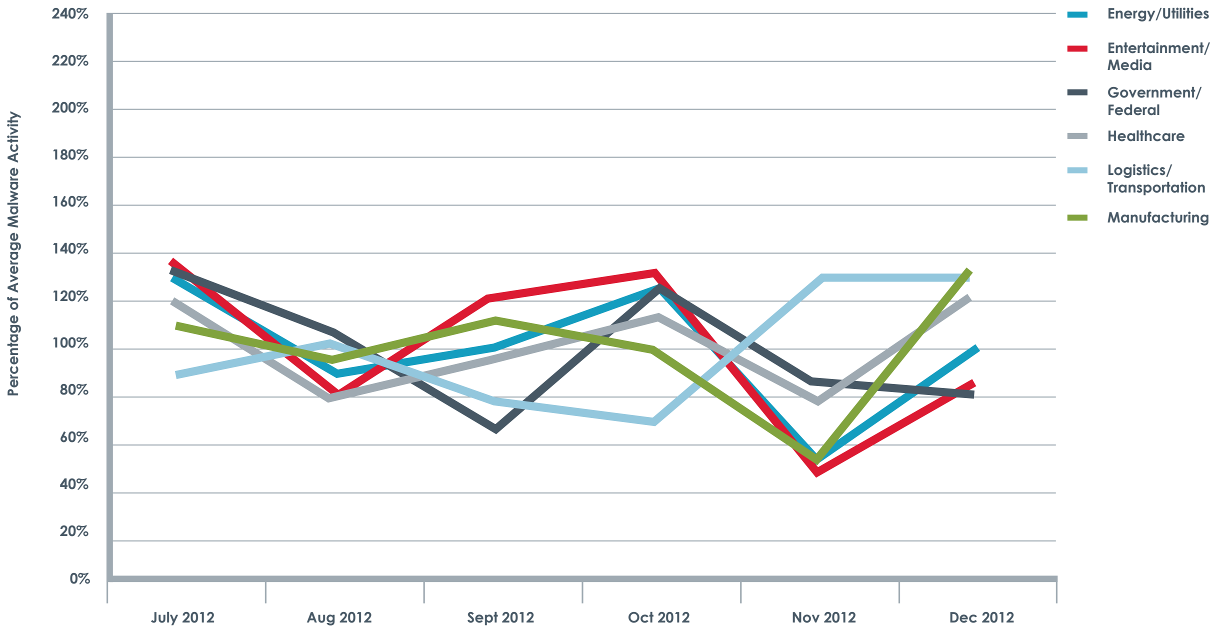
These verticals experienced between 200 to 300 percent above average, or 60 percent below average, malware activity over the course of 2H 2012.



Finding 3B: Medium volatility verticals—energy, entertainment/media, government, healthcare, logistics, and manufacturing

These verticals seem attractive to attackers only with some degree of variability. Typically, these verticals did not see malware activity spike above 140 percent of average. Such verticals underscore how attacks are difficult to predict. For instance, healthcare was recently listed as one of China's priorities in its 15-year science and technology development strategy for 2006 to 2020, which led to a surge in campaigns against healthcare firms.[1]

Medium Volatility Verticals: Energy, Entertainment/Media, Government, Healthcare, Logistics, and Manufacturing.

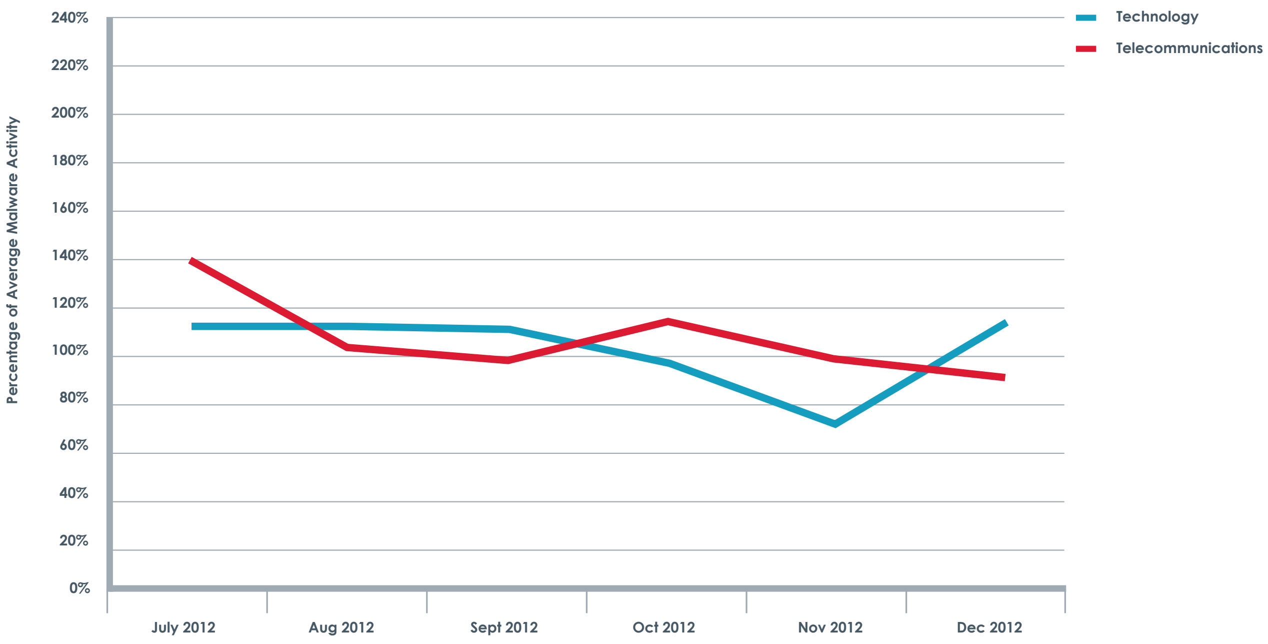


[1] http://www.darkreading.com/threat-intelligence/167901121/security/attacks-breaches/240150858/medical-industry-under-attack-by-chinese-hackers.html

Finding 3C: Low volatility verticals—technology and telecommunications

Both technology and telecommunications experienced malware activity that did not deviate more than 140 percent above average. This means attackers found these verticals an attractive target meriting consistent attention.

Low Volatility Verticals: Technology and Telecommunications



Finding 4: Attackers use common business terms used in the file names as spear phishing bait

Spear phishing remains the most common method for initiating advanced malware campaigns. When sending spear phishing emails, attackers opt for file names with common business terms to lure unsuspecting users into opening the malware and initiating the attack. These terms fall into three general categories: shipping and delivery, finance, and general business. The top phrase in malware file names, for example, was "UPS".

In examining the top 20 malicious email attachment names, the clear trend is for these file names to reference business-related topics. Rather than the types of broad spam that may be distributed to personal email accounts, it is clear that advanced attacks are targeting employees within specific organizations.

The list below provides a useful reference for IT security teams, helping them update email filtering rules. In addition, this information can be invaluable information to reference in employee education programs, giving employees clear examples of the potential damage of seemingly common, pertinent file names.

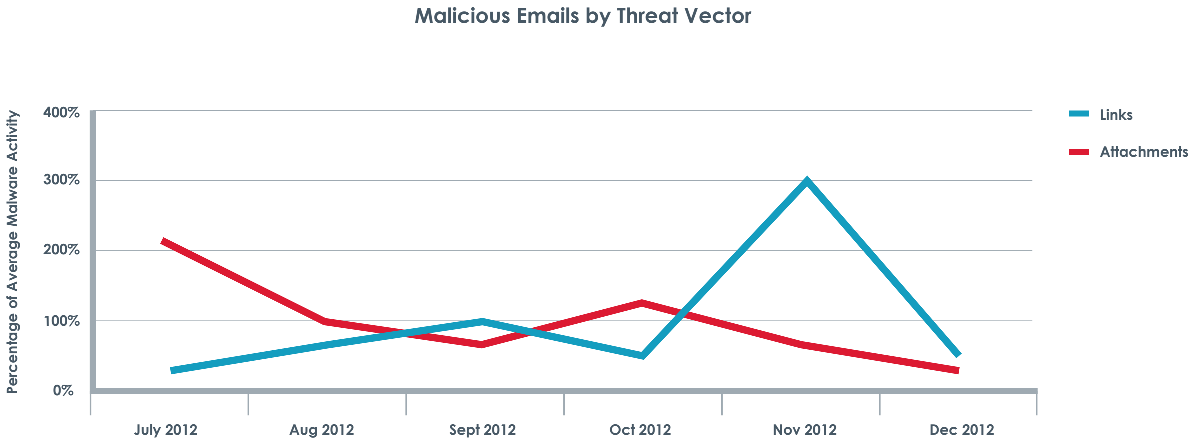
Rank	File Name	Percent of Email Attachments
1	Details.zip	6.9%
2	UPS_document.zip	4.0%
3	DCIM.zip	2.7%
4	HP_Document.zip	2.6%
5	Report.zip	1.9%
6	Scan.zip	1.8%
7	UPSDocument.zip	1.5%
8	Amazon_Report.zip	1.2%
9	postcard.zip	1.1%
10	UPSdocument.zip	0.8%
11	UK-Vodafone_MMS.zip	0.6%
12	HP_Scan.zip	0.5%
13	log_2012.zip	0.4%
14	SnowFairy.zip	0.3%
15	Changelog_10172012.zip	0.3%
16	Change_2012.zip	0.3%
17	Vodafone_MMS.zip	0.3%
18	Changelog_2012.zip	0.3%
19	changelog_2012.zip	0.3%
20	RoyalMailTrackingService.zip	0.3%
	Other	71.9%

The following is a list of the top terms that show up in malicious email attachment file names. Terms related to shipping are among the most common, with “UPS”, “fedex”, “myups”, and “tracking” being a few that are among the top ten most common. Other common categories include company names and finances. “dcim”, a default folder name for images, is also a common term. Attackers are also taking advantage of common office workflows. For example, a common method mimics how an office scanner emails scanned document by using words like “scan”, “hp”, and “Xerox”.

Rank	Word	Percent of Email Attachments
1	ups	17.0%
2	details	13.9%
3	documents	10.6%
4	fedex	7.4%
5	myups	7.1%
6	amazon	5.4%
7	tracking	5.1%
8	invoice	5.0%
9	report	4.7%
10	order	4.4%
11	notification	3.8%
12	scan	3.4%
13	08	3.2%
14	hp	3.1%
15	IRS	2.9%
16	booking	2.8%
17	xerox	2.7%
18	dcim	2.7%
19	2012	2.7%
20	label	2.3%

We also noticed some flux with respect to whether attackers use links or attachments. In the last six months of 2012, attackers used both links and attachments to infect targeted systems. While both approaches are always used, their usage fluctuates. The fluctuation is largely tied to:

- **Exploits that attackers have at hand:** If a zero-day exploit is discovered in Acrobat, for example, organizations will see a spike in malware distributed via PDFs. On the other hand, if a browser exploit is uncovered, more attacks will be waged.
- **Preference for specific targets:** sometimes fluctuations are determined by predilections of a specific attack group—such as the attacks on healthcare we describe earlier.



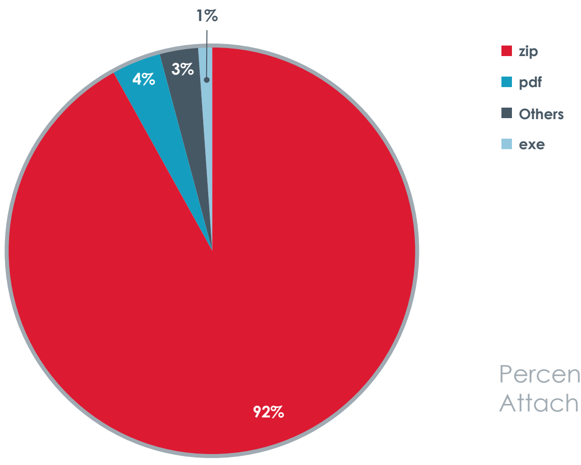
Comparison: Attachments vs. Links

Finding 5: ZIP files remain the preferred file for malware delivery by email

In evaluating email file attachment extensions, it quickly becomes obvious that .zip files are currently far and away the most common malware file type. Why? Currently, no organizations block these file extensions and attackers understand this. Further, attackers can hide their malicious payloads within .zip files so scanners do not detect them.

Given the high rate of .zip file use and its efficiency in evading traditional security mechanisms, organizations without effective tools to inspect and block these malicious attachments may need to consider taking the step of blocking all files with this extension which may hamper their business processes.

Top Malicious Email Attachment File Extensions

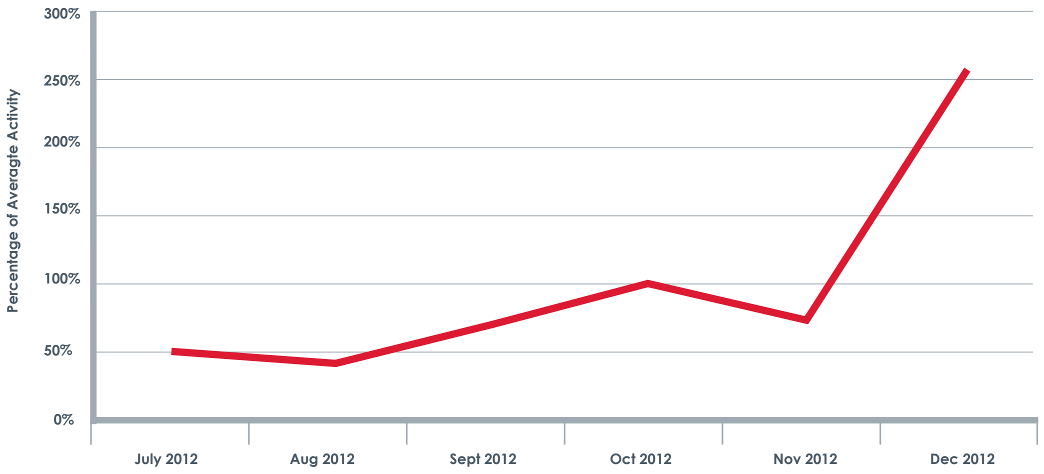


Percentage of Malicious Email Attachment Extensions

Web

For Web-based malware attacks there was a rise in infection rates. The increase was most likely due to the holiday season at the end of the year.

Infections Per Customer



Finding 6: Malware writers have focused significant effort on evasion

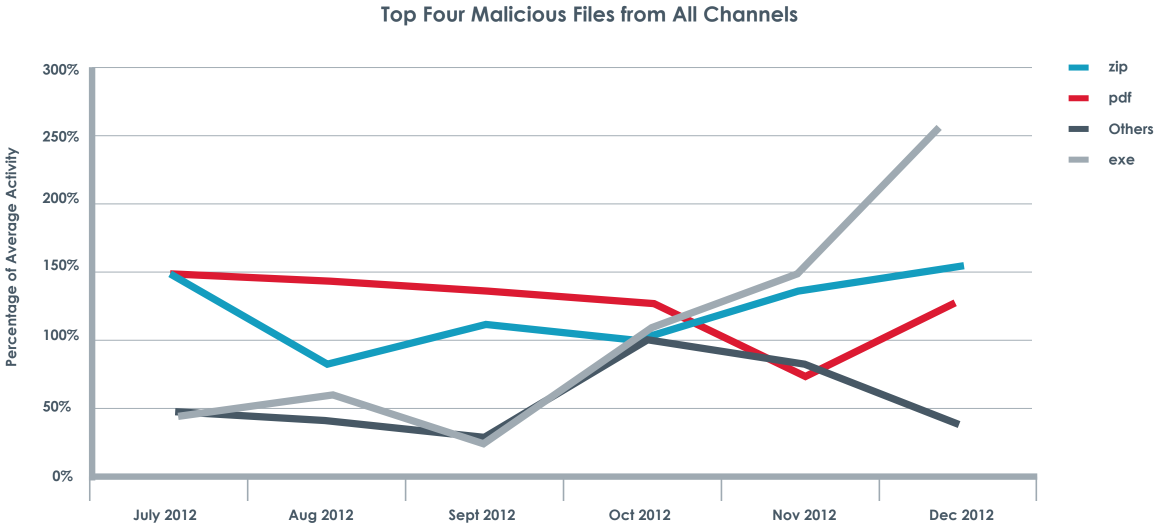
Several innovations designed to better evade detection have appeared. For example, instances of malware were uncovered that execute only when users move a mouse, a tactic which could dupe basic malware sandboxing systems since the malware seemingly fails to generate any activity.

1. **Hiding in the sandbox**. Analysis evasion is not new. For years malicious code has used various techniques to evade security systems. For example, malware would check for specific process names, DLLs, and drivers associated with specific security technologies. However, these techniques continue to grow more advanced. Recently, FireEye researchers have started seeing malware that tries to evade automated analysis that security programs run in so-called sandboxes. The malware is not initiated until a user employs a mouse command. Given that automated analysis systems do not employ mouse commands, these programs lie dormant and undetected when inspected in sandboxes. (More details on these evasion tactics are available at the following URL: http://www.fireeye.com/blog/technical/2012/12/dont-click-the-left-mouse-button-trojan-upclicker.html.)

2. **Digital certs not always trustworthy**. Over the last six months, FireEye researchers have been witnessing a rising trend in the amount of malware that is digitally signed. Many security technologies trust signed files and do not further scan them. By using certificates to sign their malware attackers can minimize the chances of detection. Malware is usually digitally signed with certificates that have been hijacked, stolen, or revoked, or that are otherwise invalid. (See the following URL to learn more about a piece of malware using a zero-day exploit that used an invalid certificate: http://www.fireeye.com/blog/technical/cyber-exploits/2013/02/lady-boyle-comes-to-town-with-a-new-exploit.html.)

Finding 7: Attackers are increasingly using DLL files to improve persistence

Traditional defense mechanisms, such as anti-virus, focus on finding .exe files. To bypass detection and prolong the infection attackers are dropping the use of .exe files and opting to use DLL. Technically DLLs work just like .exe files, that is they execute software but only when invoked. For example, a common DLL is invoked when an individual wishes to print a document, invoking a DLL file that executes software that runs the printer. By using DLLs, the malware can establish persistent control as every time a vital, commonly used application like Internet Explorer is used, the malicious payload is loaded automatically—without any user involvement or awareness. If the malware was dependent on user commands to execute a malicious payload chances are much more likely that users would get suspicious and not take the step necessary for the malware to operate.



APT case study: Operation Beebus

FireEye uncovered an APT campaign and this case study provides current insights into the group behind these attacks, the tactics employed, and how they have evaded organizations' defenses.

Who is targeted in this operation

The targets of Operation Beebus appear to be the top aerospace and defense contractors. FireEye has confirmed the attack on at least six major enterprises in the industry. Operation Beebus is an ongoing operation that is constantly evolving but has a single purpose: gather as much intelligence as possible about the top aerospace and defense organizations while attempting to evade detection.

How does that attack take place?

Initial infection

The new breed of APT attacks are not monolithic, rather they are blended relying on numerous infiltration techniques. The attackers leveraged well-known documents and white papers published by reputable companies as the attachments as part of the attack. The attackers took these normally safe documents and weaponized them. These documents were weaponized with a variation of three PDF exploits and two Word exploits.

Sample of attachment names:

sensorenvironments.doc

FY2013_Budget_Request.doc

RHT_SalaryGuide_2012.pdf

NationalHumanRightsActionPlanofChina(2012-2015).pdf

Boeing_Current_Market_Outlook_2011_to_2030.pdf

dodd-frank-conflict-minerals.doc

Global_A&D_outlook_2012.pdf

Understandyourbloodtestreport.pdf

SecurityPredictionsfor2012and2013.pdf

DeptofDefenseFY12ASTTRSolicitationTopicsofInteresttoBoeing.pdf

Conflict-Minerals-Overview-for-KPMG.doc

Persistence and evasion

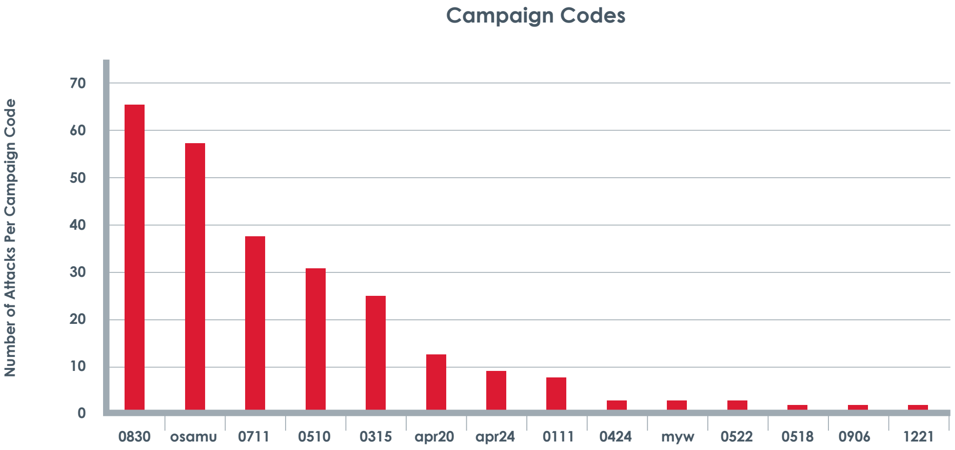
When a victim opens the weaponized files and they have a vulnerable version of the MS Word/Adobe PDF software, their machine is compromised. The exploit only lasts as long as the MS Word/Adobe PDF process is running, allowing attackers to quickly download or drop additional malware while they have control. In legacy attacks, which most traditional defenses look for, an attacker would use executable files (.exe) that launch upon startup. This legacy approach is not used in advanced attacks because it draws too much attention to itself.

Instead of dropping an .exe and launching it at startup Operation Beebus is much more evasive. Attackers drop a DLL named “ntshrui.dll” into the “C:\windows” directory. Attackers carefully selected this filename because it is a valid Windows DLL and resides in a different subdirectory under “C:\windows”. By placing their malicious file into a higher-level directory they take advantage of the “DLL Search Order Hijacking Vulnerability” in Windows. This vulnerability allows for their malicious DLL to be loaded by the critical Windows process “explorer.exe”. The “explorer.exe” process is loaded on login and will load the malicious DLL and persist the attacker’s control over the system.

Communication and tracking

Operation Beebus was intentionally designed to go undiscovered for as long as possible. To achieve this attackers were very careful as to how and where their malware communicated back to the CnC servers. First, they chose legitimate seeming domains like “bee.businessconsults.net” (from which the term Beebus is coined) to send communication. Next, they made sure their communication was not clear text or suspicious looking. They achieved this by encoding their data with a customized Base64 technique. This prevents most security solutions from inspecting the communication.

An essential part of Operation Beebus was tracking victims. Since this attack was carried out over a long time and is continually changing and evolving, the attackers need to track their progress and success. This operation deployed many campaigns carried out over many months, attacking several companies, targeting different roles in the companies, and using different file names in spear phishing. What tied all this information together was the campaign codes attackers encoded into their callback communication. This allowed the attackers to know which campaigns were successful and which were not. The actual campaign code was tied to the malicious DLL that would get dropped into the “C:\windows” directory. Most of the campaign codes the attackers selected correlated to the date of the campaign, i.e., 0111 meant January 11. Below is a graph showing the campaign codes used and the number of spear phishing attachments associated with the campaign code.



The group behind Operation Beebus

The size and technological sophistication of the organizations being targeted indicates that the groups behind Operation Beebus are well resourced and sophisticated. This is evidenced by the fact that the campaign has been linked to the "Comment Group", also referred to as Byzantine Candor by U.S. intelligence, which is a prolific hacking collective widely reported to be based in China.[2] While the motives are not understood at this point, all the facts would appear to indicate that Operation Beebus is a mission focused on collecting intelligence.

Summary

By understanding Beebus, security teams can understand the anatomy of an APT attack. Most importantly, Beebus identifies failure points in today's defense including network firewalls, IPS, and anti-virus. Today, sadly, the Beebus episode demonstrates how malware writers have the upper hand when it comes to cyber attacks.

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.

[2] http://www.businessweek.com/articles/2012-08-02/chinas-comment-group-hacks-europe-and-the-world