Trend Micro Incorporated
Research Paper
2012

Spear-Phishing Email: Most Favored APT Attack Bait

TrendLabs℠ APT Research Team

Contents

Introduction

Advanced persistent threat (APT) campaigns comprise a growing part of the current threat landscape. Some APT campaigns remain active, in fact, even after drawing extensive media attention. Campaigns' routines may vary over time but their primary goal remains the same—to gain entry to a target organization's network and obtain confidential information.

Spear phishing continues to be a favored means by APT attackers to infiltrate target networks. In a typical spear-phishing attack, a specially crafted email is sent to specific individuals from a target organization. The recipients are convinced through clever and relevant social engineering tactics to either download a malicious file attachment or to click a link to a malware- or an exploit-laden site, starting a compromise.

While spear phishing may be a timeworn technique, it continues to be effective even in today's Web 2.0 landscape. In 2011, security firm RSA suffered a breach via a targeted attack. Analysis revealed that the compromise began with the opening of a spear-phishing email.[1] That same year, email service provider Epsilon also fell prey to a spear-phishing attack that caused the organization to lose an estimated US$4 billion.[2]

This research paper presents Trend Micro findings on APT-related spear phishing from February to September 2012. We analyzed APT-related spear-phishing emails collected throughout this period to understand and mitigate attacks. The information we gathered not only allowed us to obtain specific details on spear phishing but also on targeted attacks. We found, for instance, that 91% of targeted attacks involve spear-phishing emails, reinforcing the belief that spear phishing is a primary means by which APT attackers infiltrate target networks.

What Is Spear Phishing?

Spear phishing may be defined as "highly targeted phishing aimed at specific individuals or groups within an organization." Coined as a direct analogue to spearfishing, spear phishing makes the use of information about a target to make attacks more specific and "personal" to the target.[3] Spear-phishing emails, for instance, may refer to their targets by their specific name, rank, or position instead of using generic titles as in broader phishing campaigns.[4]

APT campaigns frequently make use of spear-phishing tactics because these are essential to get high-ranking targets to open phishing emails. These targets may either be sufficiently aware of security best practices to avoid ordinary phishing emails or may not have the time to read generic-sounding messages. Spear phishing significantly raises the chances that targets will read a message that will allow attackers to compromise their networks. In many cases, spear-phishing emails use attachments made to appear as legitimate documents because sharing via email is a common practice among large enterprises and government organizations—the usual targets of APT campaigns.

1 http://blogs.rsa.com/rivner/anatomy-of-an-attack/
2 http://www.informationweek.com/security/attacks/epsilon-fell-to-spear-phishing-attack/229401372 and http://www.net-security.org/secworld.php?id=10966
3 http://en.wikipedia.org/wiki/Spearfishing
4 http://about-threats.trendmicro.com/Glossary.aspx?index=P&language=au

Spear-Phishing Attack Ingredients

The Email

In a spear-phishing attack, a target recipient is lured to either download a seemingly harmless file attachment or to click a link to a malware- or an exploit-laden site. The file, often a vulnerability exploit, installs a malware in a compromised computer. The malware then accesses a malicious command-and-control (C&C) server to await instructions from a remote user. At the same time, it usually drops a decoy document that will open when the malware or exploit runs to hide malicious activity.

The Attachment

Spear-phishing emails can have attachments of varying file types. We found that the most commonly used and shared file types in organizations (e.g., .XLS, .PDF, .DOC, .DOCX, and .HWP) accounted for 70% of the total number of spear-phishing email attachments during our monitoring.

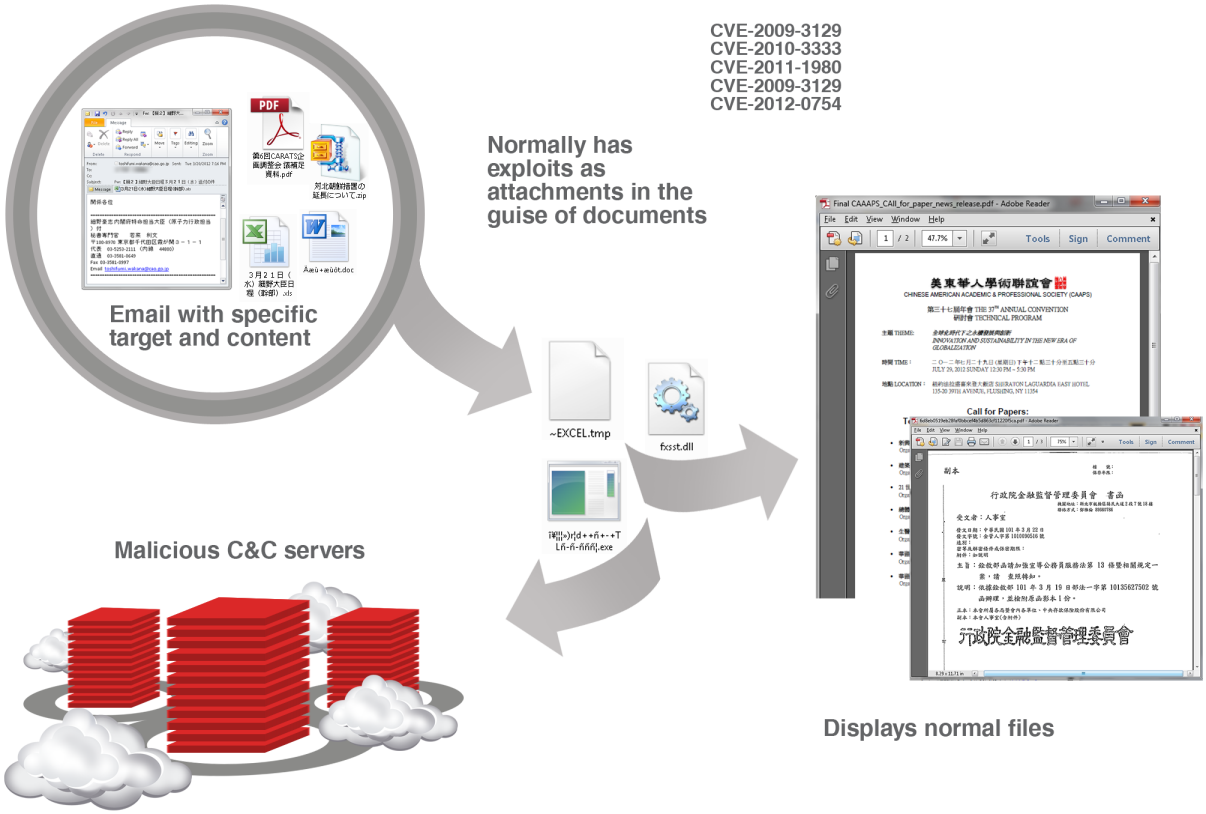

Figure 1: Infection chain that starts when a spear-phishing email is opened

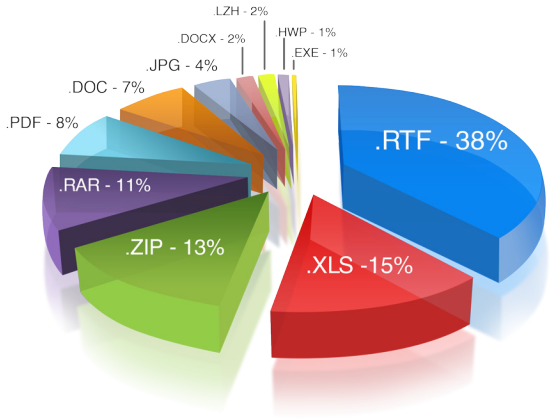

Figure 2: Top spear-phishing email attachment file types

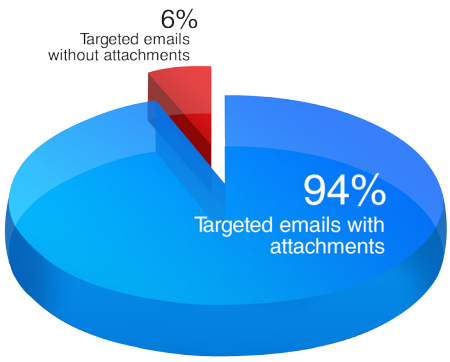

Figure 3: Ratio of targeted emails with attachments to those without attachments

Executable (.EXE) files were not commonly used as spear-phishing email attachments. This is likely due to the fact that emails with .EXE file attachments are usually detected and blocked by any security solution. This is also why .EXE files are usually compressed and archived before being sent. They instead came in the form of .LZH, .RAR, and .ZIP files. In some cases, compressed files were even password protected to further prevent their malicious content from being detected by security solutions. The passwords are indicated in the email body along with the social engineering bait.

When attached executable files are extracted, they generally look suspicious. That is why malicious executable files often come disguised as documents with fake icons, employ the right-to-left override (RLO) technique, and use file names appended with many spaces to hide the .EXE file name extension.[5]

The Usual Targets

Monitoring revealed that 94% of targeted emails use malicious file attachments while the rest use alternative methods like installing malware by luring victims to click malicious links and to download malicious files and using webmail exploits.[6]

People normally share files (e.g., reports, business documents, and resumes) in the corporate or government setting via email. This may be due to the fact that downloading off the Internet in such a setting is frowned upon. That is why a higher number of spear-phishing emails with attachments is sent to targets in the corporate or government sector.

Targeted emails without attachments are more often sent to noncorporate or nongovernmental organization (NGO) targets like activist groups and international organizations as their members typically reside in different countries. In such a case, a spear-phishing email that lures victims to click a link and to download a file from a remote site may not appear suspicious.

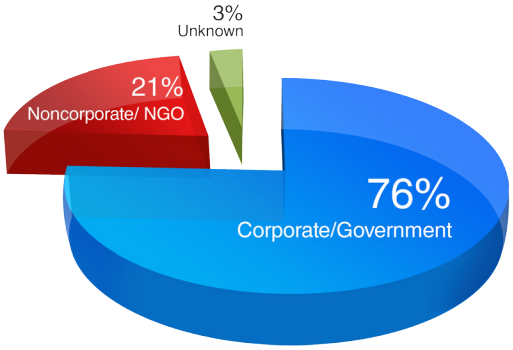

Figure 4: Ratio of APT corporate/government sector targets to noncorporate/NGO targets

5 http://krebsonsecurity.com/2011/09/right-to-left-override-aids-email-attacks/
6 http://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attacks-on-popular-web-mail-services-signal-future-attacks/

Most Targeted Industries

Throughout the eight months we have been monitoring APT-related spear-phishing attacks, the government sector and activist groups proved to be most targeted.

Apart from being a common cyber-espionage target, the government sector also topped the list of most targeted industries related to APTs. This may most probably be due to how accessible pertinent information about government agencies is on the Internet. Government agencies are likely to share contact information on their websites as they serve the public. Information on appointed members is also readily available to the public via government sites.

Activist groups often have social media pages apart from their own sites. These online pages usually contain points of contact along with member information to facilitate information exchange, to organize campaigns, or to recruit new members. In this case, information availability may make them easier targets.

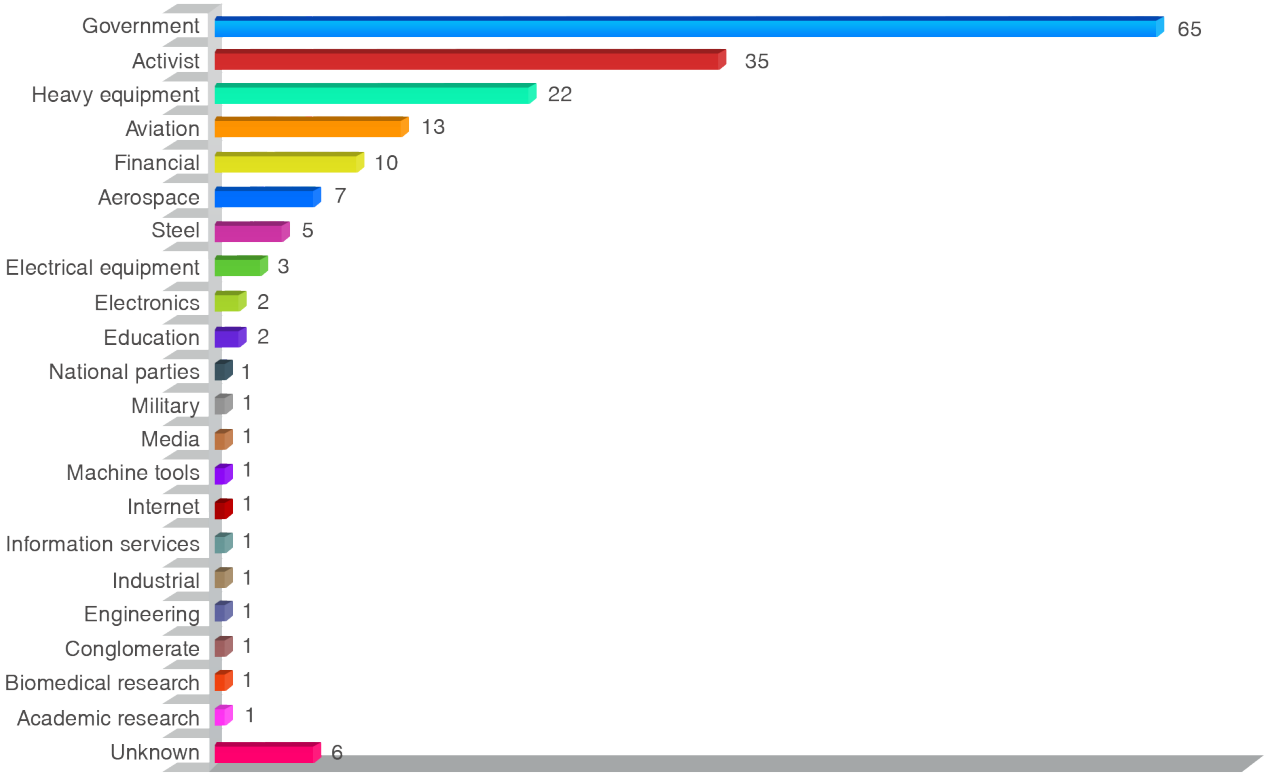

Figure 5: Most common industry targets of APT-related spear phishing

Most Targeted Regions

As part of protecting customers and their valuable data, Trend Micro consistently monitors and mitigates possible targeted attacks. The following figure shows the number of possible targeted attacks we have seen over the monitoring period, the majority of which were related to spear phishing.

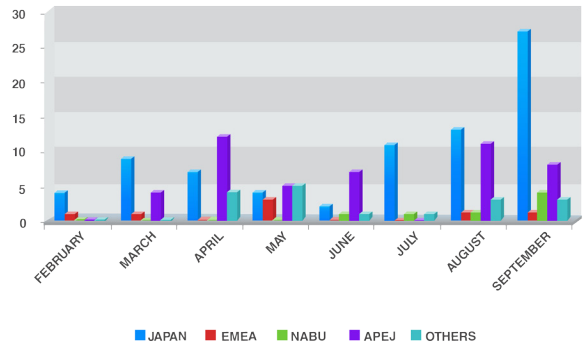

Figure 6: Most common regional targets of APT-related spear phishing

Spear Phishing for Reconnaissance

To increase the likelihood that a targeted attack would succeed, attackers first perform reconnaissance on their chosen targets. Reconnaissance is defined as "profiling a target in order to acquire information concerning its defensive posture and software deployment status and a contextual understanding of the roles and responsibilities key personnel play and relevant themes to employ in social engineering."[7] Reconnaissance can be further classified into two stages—pre- and post-infiltration reconnaissance.

Pre-infiltration reconnaissance is more generally associated with the human aspect. In this stage, attackers profile their human targets to gain initial entry to a target network. The delivery method, for instance, via a spear-phishing email often leveraging social engineering, is also determined. While human-related information like a target's name, job title, and email address may be bought from the underground market or be provided by the masterminds behind sanctioned attacks, the Internet is the most convenient source of such information. Social networking sites, corporate and academic publications, and organizations' sites allow miscreants to harvest relevant information on their targets for various social engineering schemes.

Pre-infiltration reconnaissance allows attackers to identify persons of interest in an organization. These people are usually in high positions in a targeted organization, individuals who may have copies of the documents or have access to the type of data attackers go after. Once identified, the attackers will obtain their email addresses for spear-phishing purposes.

Trend Micro research revealed that nearly half of the total number of spear-phishing recipient email addresses was just a Google search away.

7 http://www.trendmicro.co.uk/media/wp/apt-primer-whitepaper.pdf

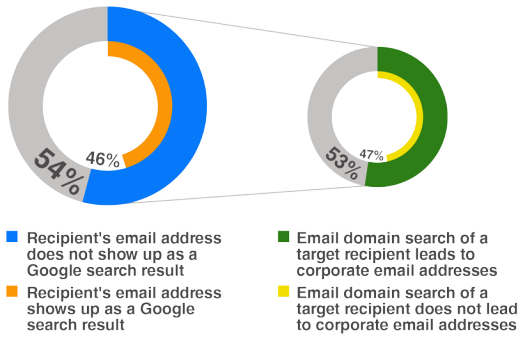

Figure 7: Ratio of spear-phishing recipient email addresses on the web to those that are not

More than half of the email addresses that did not appear in Google searches can be found by typing a target recipient's name with his/her company's email account domain name like recipient's_name@company_name.com. This means that three-fourths of the total number of spear-phishing-related email addresses we collected was easily obtainable from the web.

Post-infiltration reconnaissance, on the other hand, is conducted after a remote access Trojan (RAT) has successfully been installed in a victim's computer. In this stage, an attacker can use the RAT to profile the target network. Profiling includes knowing what OS and security software the victim's machine runs and obtaining access to local IP addresses, proxy servers, and other machines in the network. All of this information is used to maintain persistence, to perform lateral movement, and to exfiltrate data from the target network.

Conclusion

Spear phishing remains the most favored vector for instigating targeted attacks. Why? Because users continue to fall prey to spear-phishing emails, causing substantial damage to their respective organizations. Spear-phishing email attachments are difficult to spot from normal document attachments passed on from user to user each day in a corporate environment, increasing the likelihood of successful computer infection.

The availability of organizational information on the Internet allow attackers to gain relevant data on their chosen targets, making their APT campaigns more effective. Our findings highlight how spear phishing aids APT attacks because of the vast amount of information available at the touch of our fingertips. Organizations should strive to improve their existing defenses and take into careful consideration what types of and how much information they make available online.

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003
www.trendmicro.com

TREND MICRO™

Securing Your Journey to the Cloud