WHITE PAPER

SPEAR PHISHING ATTACKS— WHY THEY ARE SUCCESSFUL AND HOW TO STOP THEM

Why Automated Analysis Tools are not Created Equal

SECURITY
REIMAGINED

CONTENTS

Executive Summary

There's been a rapid and dramatic shift from broad, scattershot attacks to advanced targeted attacks that have had serious consequences for victim organizations. Some of the most famous advanced targeted attacks, such as the attack on RSA, on HBGary Federal, and Operation Aurora all used spear phishing. The increased use of spear phishing is directly related to the fact that it works, as traditional security defenses simply do not stop these types of attacks. This paper provides a detailed look at how spear phishing is used within advanced targeted attacks. It will provide an overview of spear phishing, its characteristics, and a notable attack case study. Finally, the paper looks at the key capabilities organizations need in order to effectively combat these emerging and evolving threats.

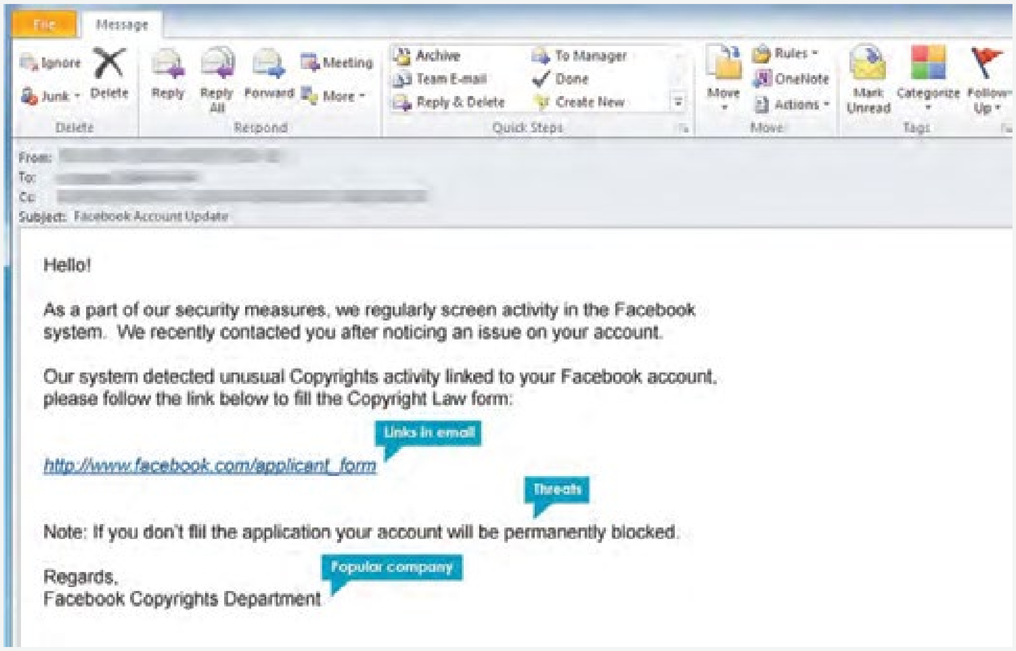
Introduction: The Rise of Spear Phishing Email Attacks

Generally speaking, 'phishing' emails are exploratory attacks in which criminals attempt to obtain victims' sensitive data, such as personally identifiable information and/or network access credentials. These attacks open the door for further infiltration into the network. Phishing typically involves both social engineering and technical trickery to deceive victims into opening attached files, clicking on embedded links, and revealing sensitive information.

'Spear phishing' is a more targeted version of phishing attacks that combines tactics such as victim segmentation, email personalization, sender impersonation, and other techniques to bypass email filters and trick targets into clicking a link or opening an attachment. Whereas a phishing attack may blanket an entire database of email addresses, spear phishing targets specific individuals within specific organi-zations. By mining social networks, for example, the personalization and impersonation used in the spear phishing emails can be extremely accurate and compelling. Once a link is clicked or attachment opened, the foothold in the network is established allowing spear phishers to move forward with the advanced targeted attack.

Spear phishing attacks need to be seen within the context of advanced targeted attacks, otherwise known as advanced persistent threat (APT) attacks. Today, sophisticated cybercriminals (and nation-states) conduct APT attacks through the use of advanced malware and sustained, multi-vector, multi-stage attacks to reach a particular objective. For most APT attacks, the objective is to gain long-term access to an organization's sensitive networks, data, and resources.

Figure 1:
Common tactics used in phishing emails



From: [redacted]
To: [redacted]
Cc: [redacted]
Subject: Facebook Account Update

Hello!

As a part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Our system detected unusual Copyrights activity linked to your Facebook account, please follow the link below to fill the Copyright Law form:

http://www.facebook.com/applicant_form

Note: If you don't fill the application your account will be permanently blocked.

Regards,
Facebook Copyrights Department

The Reason for the Growth in Spear Phishing: It Works

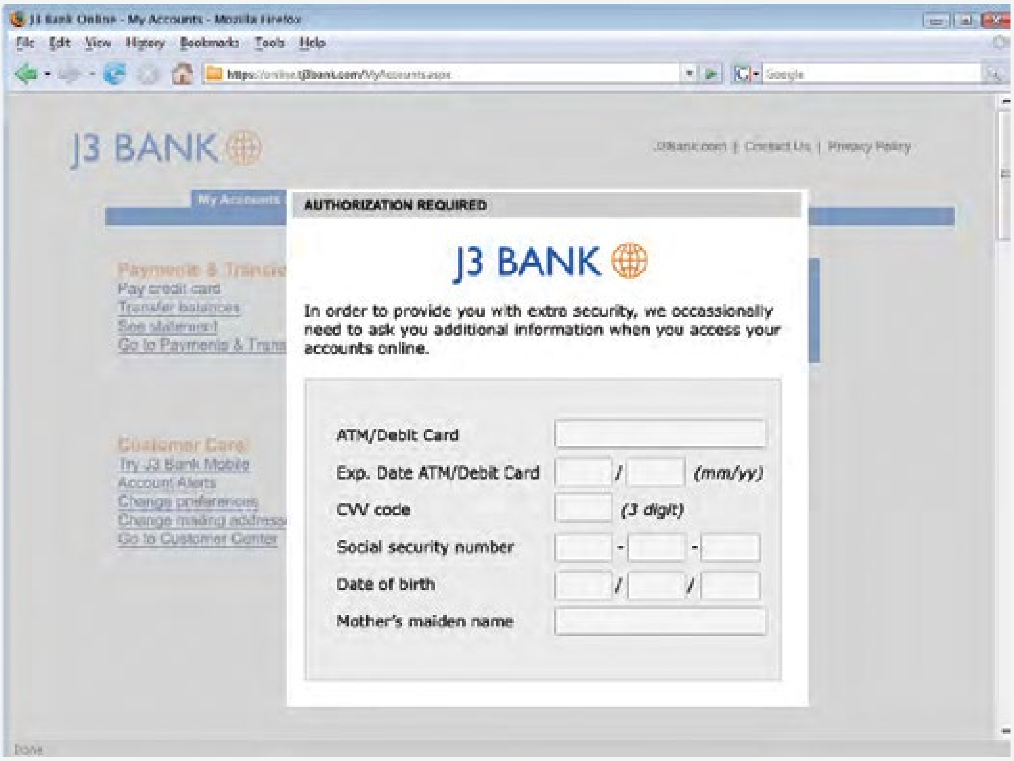
Advanced targeted attacks using spear phishing aren't an anomaly; they represent a clear shift in the approach of cybercriminals. Increasingly, criminals are moving from massive phishing attacks to spear phishing on a much smaller, more targeted scale because it has proven very effective.

A recent study[1] uncovered the following findings:

- Between 2010 and 2011, annual returns for mass email-based attacks fell from $1.1 billion to $500 million. During that same period, spam volume fell from 300 billion messages per day to 40 billion.

- In inline mode, you can quarantine spear-phishing emails, identify recipients, and block advanced attacks. These attacks often include malicious file types that exploit zero-day and other unpatched vulnerabilities.

- Spear phishing emails had an open rate of 70 percent, compared with an open rate of just three percent for mass spam emails. Further, 50 percent of recipients who open spear phishing emails also click on enclosed links, which is 10 times the rate for mass mailings.



AUTHORIZATION REQUIRED

J3 BANK

In order to provide you with extra security, we occassionally need to ask you additional information when you access your accounts online.

ATM/Debit Card

Exp. Date ATM/Debit Card / *(mm/yy)*

CVV code *(3 digit)*

Social security number - -

Date of birth / /

Mother's maiden name

Figure 2: Falsified Web site used to fool users into revealing credentials and personally identifiable information

[1] http://www.scmagazine.com/crooks-opt-for-spear-phishing-despite-higher-upfront-cost/article/206586/

- Compared to broad-based emails, spear phishing costs 20 times more per individual targeted. However, the average return from each spear phishing victim is 40 times more than that of phishing.
- A spear phishing campaign comprised of 1,000 messages is likely to generate 10 times the revenue of a phishing mailing targeting 1 million individuals.

Spear Phishing Examples and Characteristics

Following are some of the key characteristics of advanced targeted spear phishing attacks:

- **Blended/multi-vector threat.** Spear phishing uses a blend of email spoofing, zero-day application exploits, dynamic URLs, and drive-by downloads to bypass traditional defenses.
- **Leverages zero-day vulnerabilities.** Advanced spear phishing attacks leverage zero-day vulnerabilities in browsers, plug-ins, and desktop applications to compromise systems.
- **Multi-staged attack.** The initial exploit of systems is the first stage of an APT attack that involves further stages of malware outbound communications, binary downloads, and data exfiltration.
- **Lack characteristics of spam.** Spear phishing email threats are targeted, often on an individualized basis, so they don't bear a resemblance to the high-volume, broadcast nature of traditional spam. This means reputation filters are unlikely to flag these messages minimizing the likelihood of spam filters catching them.

RSA: A Case Study in Spear Phishing and an APT

The attacks targeting RSA, the security division of EMC Corp., in 2011 provide a very clear picture of the way spear phishing can set the stage for a devastating and incredibly far-reaching assault on a corporation — and its customers.

The assault began with spear phishing attacks that sent targeted users an email with a Microsoft Excel file attachment that leveraged a zero-day flaw in Adobe Flash. It is clear that not only was RSA the focus of the attack, but only four individuals within RSA were the recipients of the malicious emails. It took just one user to open the email and attachment, which downloaded a Trojan onto the user's PC.

This successful spear phishing attack was part of a much more complex advanced targeted attack. With this malware installed on the victim's PC, criminals were able to search the corporate network, harvest administrator credentials, and ultimately gain access to a server housing proprietary information on the SecurID two-factor authentication platform.

The attack didn't end there. In fact, all this was a precursor to the ultimate objective: Gaining entry to the networks of RSA's customers, focusing on those in the defense industrial base. With the stolen data, the criminals then targeted numerous high-profile SecurID customers, including defense contractors Lockheed Martin, L-3, and Northrop Grumman.

The takeaway for enterprises is that this example makes clear that even seemingly rudimentary attacks may be just the first in a series of advanced, coordinated, and devastating crimes. In addition, advanced targeted attacks against seemingly low level resources or employees without particularly sensitive roles or permissions can still open the door to vital information and huge consequences.

The Solution: Next Generation Threat Protection

Today, organizations need a new generation of security system, one that detects and blocks the advanced targeted attack techniques that include spear phishing. The following are more details on the FireEye solution to effectively stop advanced targeted attacks.

Offers a cohesive, integrated solution across threat vectors

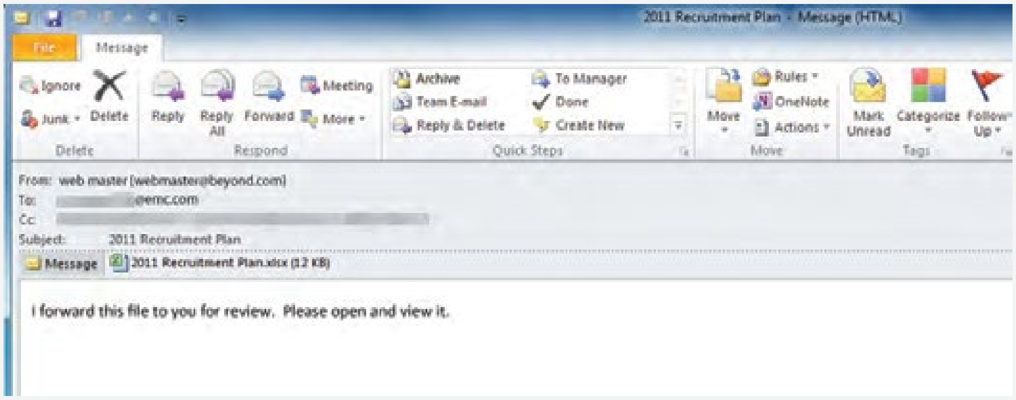
FireEye provides organizations integrated protection across Web and email attack vectors used in an advanced targeted attack. For example, stopping spear phishing requires capabilities for discovering a Web-based attack in real-time, tracing the attack to the initial phishing email that spawned the attack, and then doing the analysis required to determine if others within the organization have also been targeted. This kind of real-time cyber response is the only way to diffuse advanced targeted attacks.

Organizations are using FireEye solutions because they offer real-time analysis of URLs in emails, email attachments, and Web objects to accurately determine whether they're malicious or not. This is a critical requirement for guarding against spear phishing and other email-based attacks because zero-day tactics easily circumvent signature-based and reputation-based analysis. Further, to effectively defend corporate networks, organizations need systems that inspect across many protocols and throughout the protocol stack, including the network layer, operating systems, applications, browsers, and plug-ins like Flash.

Delivers signature-less, dynamic security that thwarts zero-day exploits

FireEye solutions provide dynamic, real-time exploit analysis of email attachments and URLs, rather than just comparing bits of code to signatures or relying on reputations. This signature-less analysis is critical to defending against advanced tactics because it all starts with zero-day exploits. With exploit detection, it is possible to stop the advanced malware embedded in attachments as well as malware hosted on dynamic, fast-changing domains.

Figure 3:
RSA spear phishing email used to launch targeted APT attack



From: web master [webmaster@beyond.com]
To: [redacted]@emc.com
Cc: [redacted]
Subject: 2011 Recruitment Plan
Message 2011 Recruitment Plan.xlsx (12 KB)

I forward this file to you for review. Please open and view it.

Guards against malicious code installs and block callbacks

In addition to exploit detection, FireEye also identifies whether suspicious attachments and other objects are malicious. Further, resulting callback communications are inspected to identify if they are malicious in nature. This includes monitoring outbound host communications over multiple protocols in real-time to determine if the communications indicate an infected system is on the network. Callbacks can be stopped based on the unique characteristics of the communication protocols employed, rather than just the destination IP or domain name.

Once malicious code and its communications are flagged, the ports, IP addresses, and protocols must be blocked in order to halt any transmissions of sensitive data. This prevents the further download of malware binary payloads and the lateral spread inside the organization.

Yields timely, actionable threat intelligence and malware forensics

Once advanced malware has been analyzed in detail, the information gathered needs to be fully leveraged. FireEye customers are able to use this information for a number of purposes:

- FireEye systems fingerprint the malicious code to auto-generate protection data and identify compromised systems to prevent the infection from spreading.
- Forensics researchers can run files individually through automated offline tests to confirm and dissect malicious code.
- Information can be shared through unified intelligence systems that keep other experts and organizations current.

Conclusion

Multi-vectored, multi-stage attacks have been extremely effective for penetrating today's networks despite $20 billion invested annually in IT security. As part of advanced targeted attacks, spear phishing is growing increasingly prevalent because it is so effective. Criminals will continue to leverage spear phishing so long as organizations maintain a status quo level of security that has proven no match for spear phishing. To thwart these advanced targeted attacks, organizations need next-generation threat protection that protects across multiple threat vectors and addresses every stage of an attack.

By integrating Web and email security, guarding against inbound malicious binaries and malware callbacks, and leveraging signature-less, dynamic code execution to detect zero-day exploits, FireEye offers the next-generation threat protection necessary to stop advanced targeted attacks. With FireEye, organizations have real-time, contextual views of both Web and email-based threats. A Web-based, zero-day attack can be detected in real-time and stopped. The attack is then traced back to the initial spear phishing email that spawned the attack to determine if others within the organization have also been targeted. This kind of context-aware security analysis is the only way to get timely, actionable information about advanced targeted attacks and how they can be stopped.

About FireEye, Inc.

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 2,700 customers across 67 countries, including over 157 of the Fortune 500.

For more information on advanced threat protection, visit: www.FireEye.com

FireEye