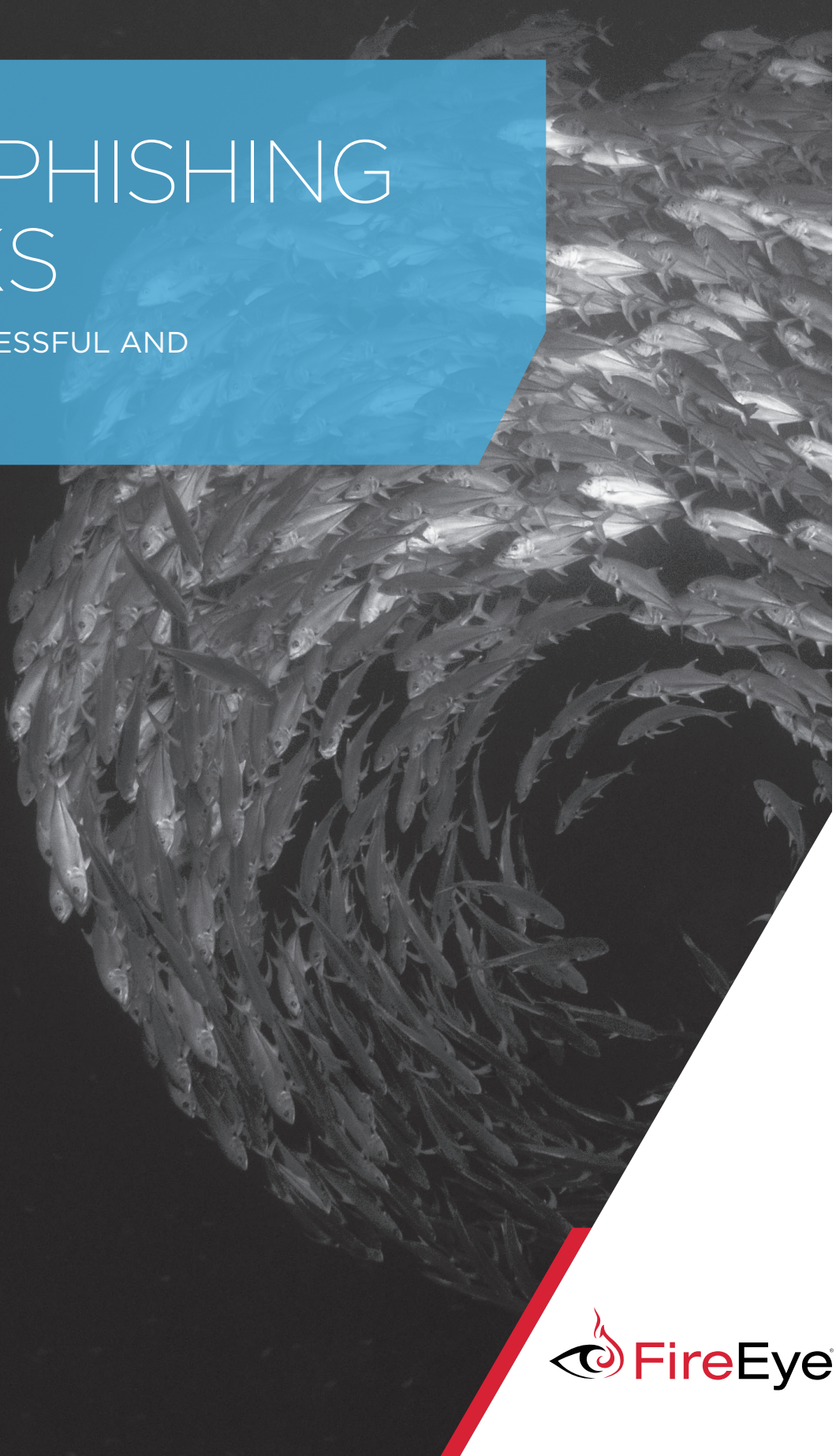
SPEAR-PHISHING ATTACKS

WHY THEY ARE SUCCESSFUL AND HOW TO STOP THEM



FireEye

WHITE PAPER

RECENTLY, THERE HAS BEEN A RAPID AND DRAMATIC SHIFT FROM BROAD SPAM ATTACKS TO TARGETED EMAIL-BASED-PHISHING CAMPAIGNS THAT ARE CAUSING SIGNIFICANT FINANCIAL, BRAND AND OPERATIONAL DAMAGE TO ORGANIZATIONS AROUND THE WORLD.

Some of the most notorious cyber crimes in recent history — such as the attacks on major banks, media companies and even security firms — started with just one person clicking on a spear-phishing email.

Spear phishing is on the rise because it works. Traditional security defenses simply do not detect and stop it. From a cyber criminal's point of view, spear phishing is the perfect vehicle for a broad array of damaging exploits. For example, threat actors are increasingly targeting executives and other high-level employees, tricking them into activating malware that gives criminals access into their companies' environments. This might be ransomware that encrypts company data, then extorts fees from the victim to remediate the situation. Other malware includes banking and point-of-sale reconnaissance Trojans that target businesses in the retail and hospitality industries. The targeted executives are usually key leaders with titles such as chief financial officer, head of finance, senior vice president and director. Spear phishing emails are created with enough detail to fool even experienced security professionals.

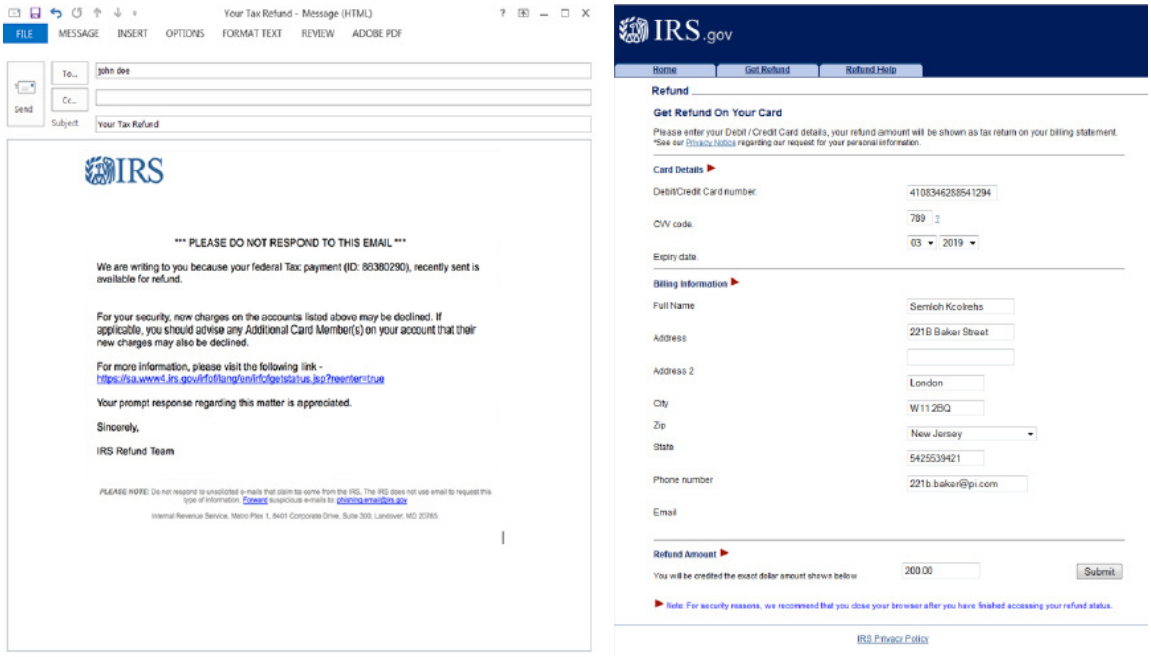
THE RISE OF SPEAR-PHISHING EMAIL ATTACKS

Phishing emails are exploratory attacks in which criminals attempt to obtain victims' sensitive data, such as personally identifiable information (PII) or network access credentials. These attacks open the door for further infiltration into any network the victim can access. 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 more targeted. Cyber criminals who use spear-phishing tactics segment their victims, personalize the emails, impersonate specific senders and use other techniques to bypass traditional email defenses. Their goal is to trick targets into clicking a link or opening an attachment. A phishing campaign may blanket an entire database of email addresses, but spear phishing targets specific individuals within specific organizations with a specific mission. By mining social networks for personal information about targets, an attacker can write emails that are extremely accurate and compelling. Once the target clicks on a link or opens an attachment, the attacker establishes a foothold in the network, enabling them to complete their illicit mission.

Spear phishing is the most prevalent delivery method for advanced persistent threat (APT) attacks. Today's cyber criminals and governments launch APT attacks with sophisticated malware and sustained, multi-vector and multi-stage campaigns to achieve a particular objective, gaining long-term access to an organization's sensitive networks, data and assets.

FIGURE 1: COMMON TACTICS USED IN SPEAR-PHISHING EMAILS.

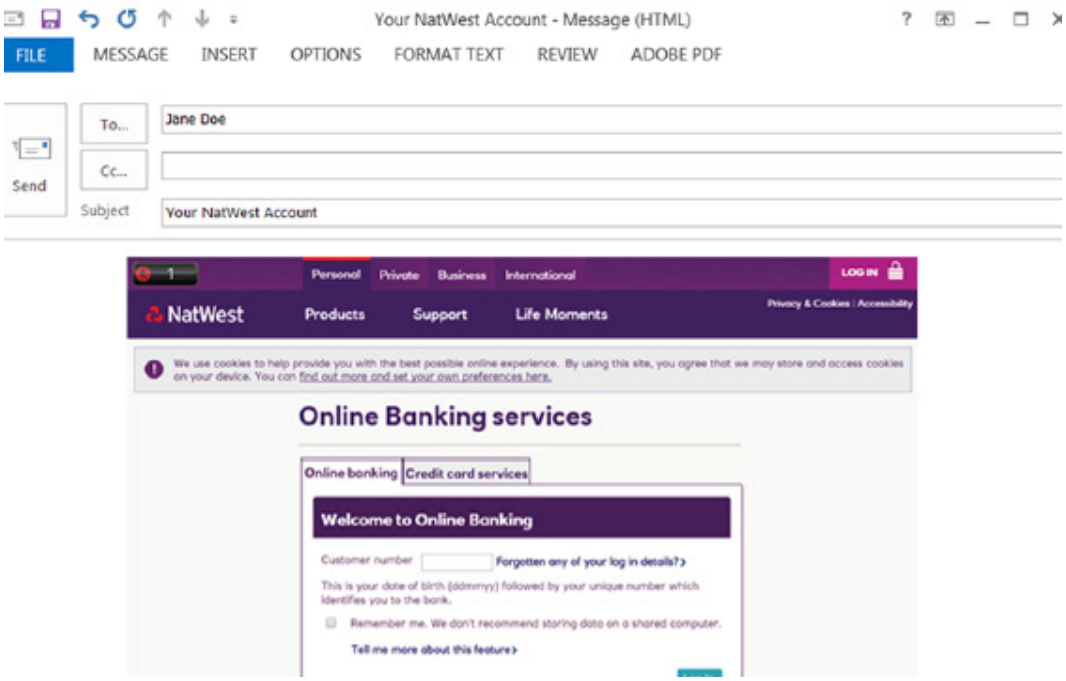


ON THE RISE BECAUSE IT WORKS

APT attacks that enter an organization via spear phishing represent a clear shift in strategy for cyber criminals. They no longer need mass spam campaigns. The return on an APT attack is much higher if criminals do their homework and target their victims with precision, expertly-crafted spear-phishing emails that can spoof senders and look completely legitimate (Fig.2).

84% of organizations said a spear-phishing attack successfully penetrated their organization in 2015. The average impact of a successful spear-phishing attack: $1.6 million. Victims saw their stock prices drop 15%.[1]

FIGURE 2: FALSIFIED WEB SITE THAT FOOLS USERS INTO REVEALING CREDENTIALS AND PII.



The average impact of a successful spear-phishing attack: $1.6 million.

[1] Vanson Bourne. "The Impact of Spear Phishing." 2016.

Spear phishing uses a blend of email spoofing, dynamic URLs and drive-by downloads to bypass traditional defenses.

SPEAR PHISHING EXAMPLES AND CHARACTERISTICS

A spear-phishing attack can display one or more of the following characteristics:

- **Blended or multi-vector threat.** Spear phishing uses a blend of email spoofing, dynamic URLs and drive-by downloads to bypass traditional defenses.
- **Use of zero-day vulnerabilities.** Advanced spear-phishing attacks leverage zero-day vulnerabilities in browsers, plug-ins and desktop applications to compromise systems.
- **Multi-stage 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.
- **Well-crafted email forgeries:** Spear-phishing email threats are usually targeted to individuals, so they don't bear much resemblance to the high-volume, broadcast spam that floods the Internet. This means traditional reputation and spam filters routinely miss these messages, rendering traditional email protections ineffective.

THIS TIME IT'S PERSONAL

Over the past year, Mandiant, a FireEye company, responded to several targeted attacks that resulted in the theft of PII by threat actors linked to China. The volume of PII stolen indicated that the objective was the mass collection of PII data, not that of specific individuals.

However, Mandiant had not previously observed a trend of indiscriminate theft of PII by China-based threat actors. Mandiant experts were aware of one-off instances of PII theft occurring as a byproduct of larger data-theft operations. For example, a cyber criminal might steal all data on a file server that happened to include PII, that was of no particular interest to the attacker.

This changed last year as Mandiant investigated several massive PII breaches that it believed were orchestrated by threat actors operating in China. These breaches spanned multiple sectors, including healthcare, travel, financial services and government. While Mandiant initially suspected the threat actors would target health records and credit card information, it found no evidence of that. Instead, Mandiant security professionals observed threat actors targeting and stealing information that could be used to verify identities such as Social Security numbers, mothers' maiden names, birthdates, employment history and challenge/response questions and answers.

REAL WORLD EXAMPLE

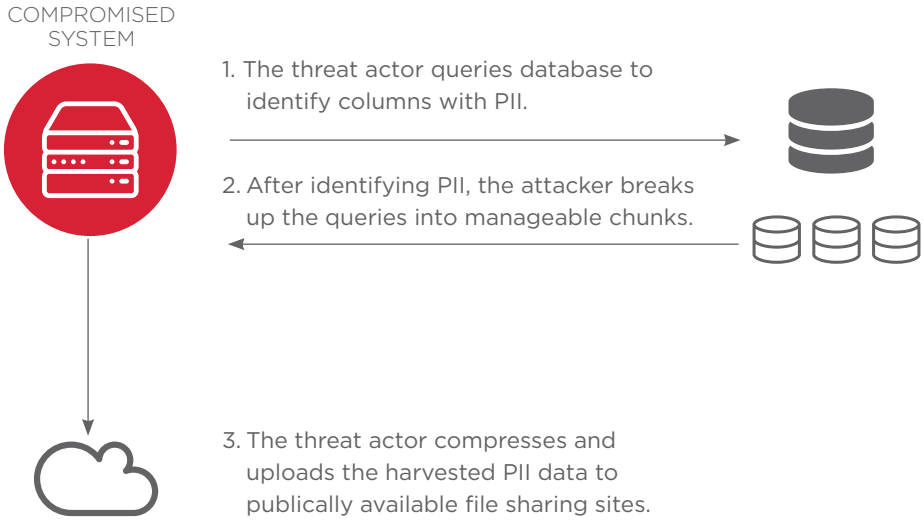
How a China-based attacker stole vast amount of PII

One attack began with threat actors successfully enticing an employee to click on a malicious link in a spear-phishing email. The link downloaded a backdoor, providing the attackers with access to the victim's environment. Once they obtained a foothold, the reconnaissance activity primarily centered on identifying databases with the greatest volume of PII.

The attackers gained access to the databases by leveraging the victim's Active Directory information to identify database administrators and their computers. They searched Active Directory group membership for the keyword "database." The threat actors moved laterally to those systems and harvested documentation to identify the names of databases, database servers and database credentials.

The attackers demonstrated a deep understanding of database systems from Microsoft, Teradata and Oracle, as well as the transaction gateways used to access these systems. With the database information in hand, the threat actors systematically tested authentication and inventoried databases. They then searched the database tables for column names that indicated storage of sensitive information, such as "Social Security numbers." Once the attackers found the information of interest, they extracted specific fields for every record in the targeted databases. The information included Social Security numbers, mothers' maiden names, and dates of birth. Due to the volume of information extracted, the threat actors:

1. Extracted information in chunks (100,000 to 1,000,000 records at a time).
2. Compressed the information into split archives.
3. Uploaded the compressed files containing PII to file sharing sites.



BETTER EMAIL SECURITY

Today, organizations need an innovative email security solution that automatically detects and blocks advanced targeted campaigns that involve spear phishing, the harvesting of credentials or the impersonation of legitimate senders. FireEye Email Security uniquely delivers an email security solution that is more effective than standard solutions, and which proactively protects organizations from email-based cyber crime.

Cohesive, integrated solution across threat vectors

To be effective at combatting today's cyber criminals, organizations need protection across multiple vectors. For example, email and network vectors are frequently used together in advanced attacks. By discovering a web-based attack in real time and tracing the attack to the initial phishing email that spawned the attack, businesses can determine if others within the organization have also been targeted. This kind of real-time defensive response is the most effective way to stop advanced targeted attacks. Organizations can further protect their corporate networks with systems that detect threats across many protocols and throughout the protocol stack, including the network layer, operating systems, applications, browsers and plug-ins.

Dynamic security that thwarts zero-day exploits

FireEye solutions 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 evade signature-based and reputation-based security. With this kind of exploit detection, FireEye can stop the advanced malware embedded in attachments as well as malware hosted on dynamic, fast-changing domains.

Defense against malicious code installs and block callbacks

In addition to detecting exploits, FireEye also identifies whether suspicious attachments and other objects are malicious. Any call-back communications are inspected for malicious activity. 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 are blocked to halt any transmissions of sensitive data. This prevents attackers from downloading more malware binary payloads and stops their lateral movement through the organization.

Timely, actionable threat intelligence and malware forensics

The information gathered from a thorough analysis of advanced malware can be used in the following ways.

- FireEye systems can fingerprint the malicious code to auto-generate protection data and identify compromised systems to prevent the infection from spreading.
- Forensics researchers can run files through automated offline tests to confirm and dissect malicious code.
- Experts and organizations can connect to unified intelligence systems to get critical analyses of current malware threats.

DETECT AND STOP SPEAR PHISHING

Targeted, multi-vector, multi-stage attacks have been extremely effective in penetrating today's networks despite a $20 billion annual investment in IT security. The majority of these attacks start with a malicious email. Specifically, socially engineered email, such as spear phishing, is the weapon of choice because it is effective. Criminals will continue to utilize it as long as organizations maintain status quo security that is unable to detect them. To stop advanced targeted attacks, organizations need comprehensive threat protection that safeguards multiple threat vectors and addresses every stage of an attack.

FireEye email security solutions offer flexible deployment options, supporting on-premise, cloud and hybrid environments. They deliver the comprehensive email protection necessary to stop advanced, targeted attacks, protecting your people, data and resources from compromise. FireEye Email Security is integrated with world-class threat intelligence — contextual intelligence gathered from millions of sensors and analytics from billions of events. This combination of capabilities makes FireEye Email Security the best way for organizations to effectively detect and stop damaging email-borne attacks.

To learn more about FireEye, visit:
www.FireEye.com/go/email

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

www.FireEye.com

FireEye