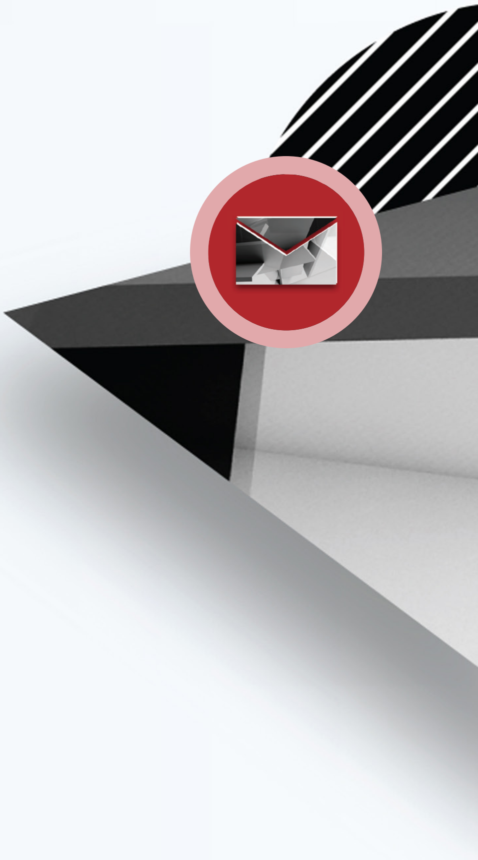
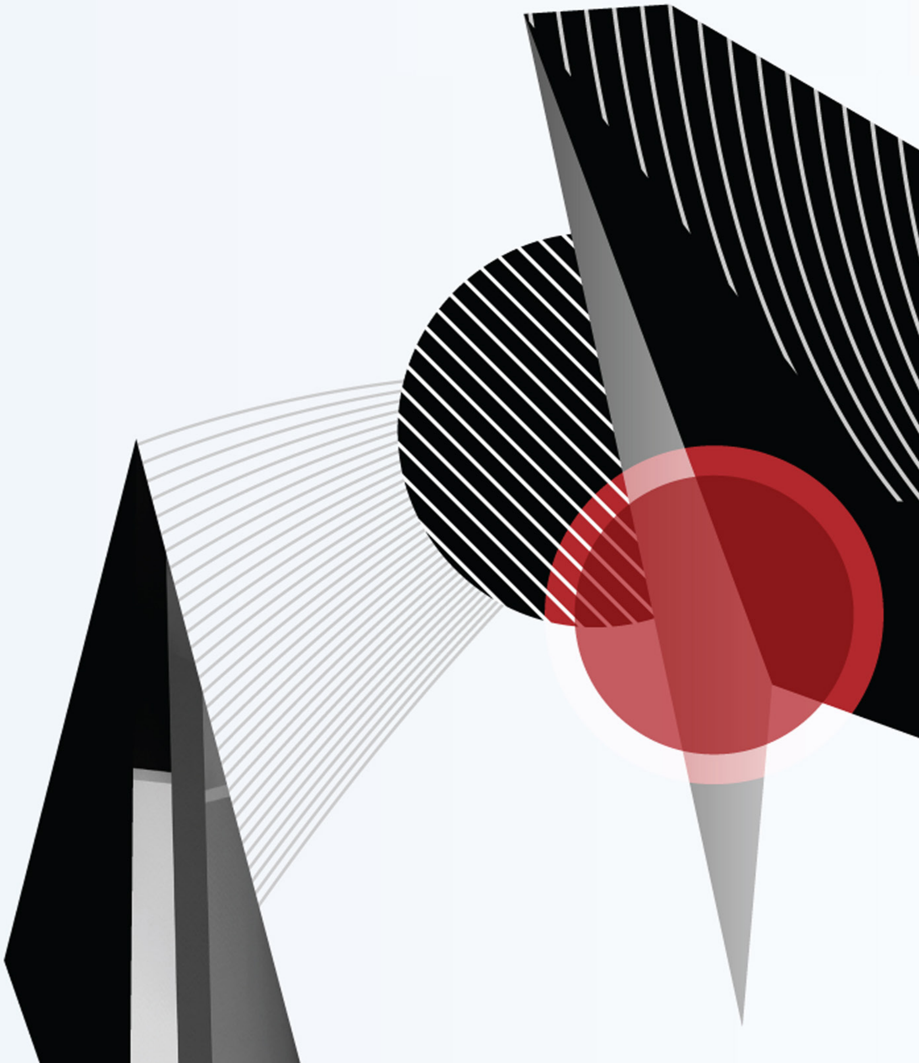
WHITE PAPER



FireEye

Spear-Phishing Attacks

Why they are successful and how to stop them



> "With FireEye Email Security in blocking mode we've seen the phishing and other malicious activity drop off enormously."
>
> — **Freud Alexandre,** Enterprise Architect and Security Manager, City of New Orleans

Spear phishing attacks target specific individuals within a specific organization for a specific purpose. The email threat landscape has dramatically shifted 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 — such as the attacks on major banks, media companies and even security firms — started with just one person clicking on a spear-phishing email.

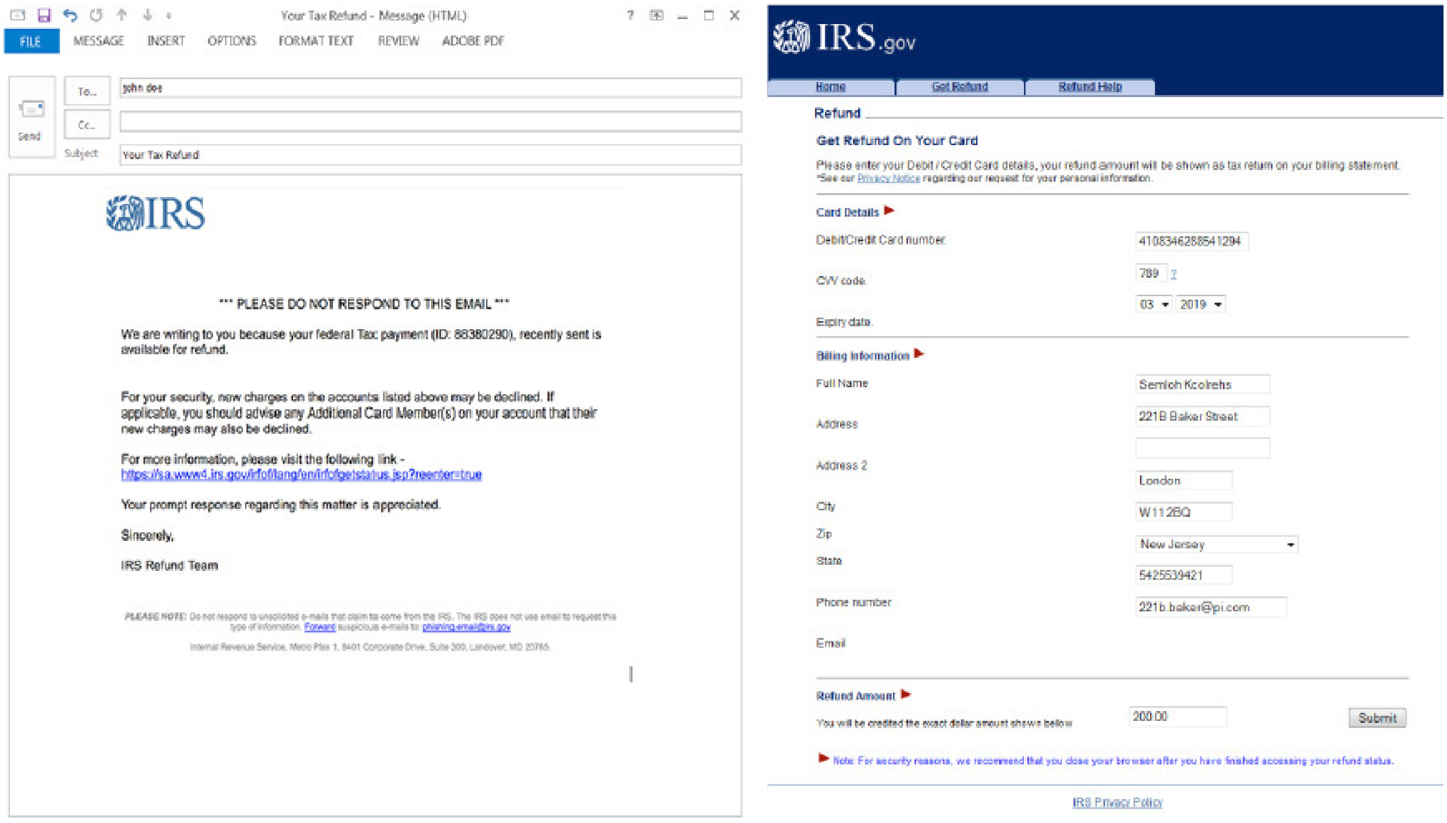
Spear phishing is a popular delivery method because it works. Traditional security defenses such as antivirus and anti-spam solutions as well as secure email gateways simply do not detect and stop it. From a cyber criminal's point of view, spear phishing is the perfect vehicle for a broad array of damaging exploits. For example, threat actors are increasingly targeting executives and employees with administrator rights, 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. Impersonation attacks, or whaling, happens when attackers impersonate executives and trick other employees into taking an action such as an unauthorized wire transfer. 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 and impersonate specific senders. Their goal is to trick targets into clicking a link, opening an attachment or taking an unauthorized action. 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 the dangerous cyber threats such as malware-laden attachments and URLs, credential phishing sites and impersonation attacks hidden among millions of messages. Today's sophisticated attackers launch malware and malware-less attacks as well as sustained, multi-vector and multi-stage campaigns to achieve a particular objective such as gaining long-term access to an organization's sensitive networks, data and assets.



To... john doe

Cc...

Subject Your Tax Refund

*** PLEASE DO NOT RESPOND TO THIS EMAIL ***

We are writing to you because your federal Tax payment (ID: 88380290), recently sent is available for refund.

For your security, new charges on the accounts listed above may be declined. If applicable, you should advise any Additional Card Member(s) on your account that their new charges may also be declined.

For more information, please visit the following link -
https://sa.www4.irs.gov/irfof/lang/en/irfofgetstatus.jsp?reenter=true

Your prompt response regarding this matter is appreciated.

Sincerely,

IRS Refund Team

PLEASE NOTE: Do not respond to unsolicited e-mails that claim to come from the IRS. The IRS does not use email to request this type of information. Forward suspicious e-mails to: phishing.email@irs.gov

Internal Revenue Service, Metro Plex 1, 8401 Corporate Drive, Suite 300, Landover, MD 20785.

Refund

Get Refund On Your Card

Please enter your Debit / Credit Card details, your refund amount will be shown as tax return on your billing statement.
*See our Privacy Notice regarding our request for your personal information.

Card Details

Debit/Credit Card number	4108346288541294
CVV code	789 ?
	03 ▾ 2019 ▾
Expiry date	

Billing Information

Full Name	Semloh Kcolrehs
Address	221B Baker Street
Address 2	
	London
City	W112BQ
Zip	
	New Jersey ▾
State	
	5425539421
Phone number	221b.baker@pi.com
Email	

Refund Amount

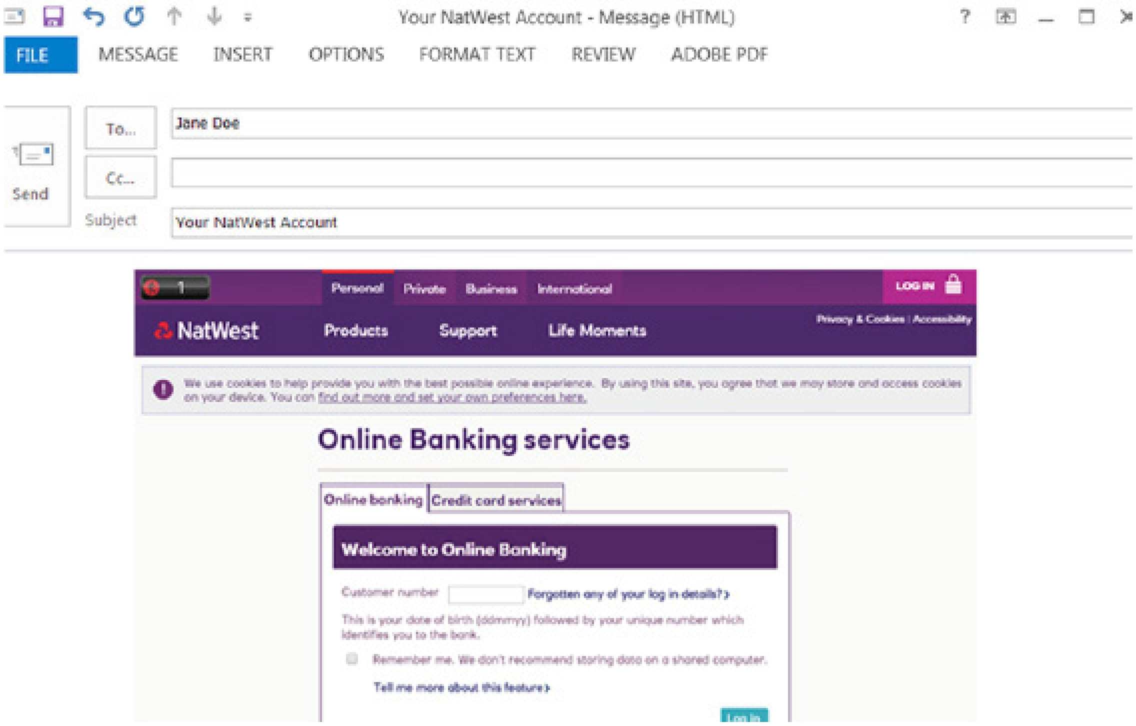
You will be credited the exact dollar amount shown below 200.00

Note: For security reasons, we recommend that you close your browser after you have finished accessing your refund status.

Figure 1. Common tactics used in spear-phishing emails.

Evolution and Impact

Sophisticated, targeted attacks that enter an organization via a spear-phishing email represent a clear shift in strategy for cyber criminals. Attackers no longer need mass spam campaigns. The return on a targeted attack is much higher if criminals do their homework and target their victims with precise, expertly-crafted spear-phishing emails that can spoof senders and look completely legitimate (Fig.2). Zero-day vulnerabilities and sophisticated malware now tend to be used sparingly and attackers are increasingly attempting to hide in plain sight. They rely on straightforward approaches such as spear-phishing emails.[1]



To... Jane Doe

Subject Your NatWest Account

We use cookies to help provide you with the best possible online experience. By using this site, you agree that we may store and access cookies on your device. You can find out more and set your own preferences here.

Online Banking services

Welcome to Online Banking

Customer number Forgotten any of your log in details? ›

This is your date of birth (ddmmyy) followed by your unique number which identifies you to the bank.

□ Remember me. We don't recommend storing data on a shared computer.

Tell me more about this feature ›

Figure 2. Falsified web site that fools users into revealing credentials and PII.

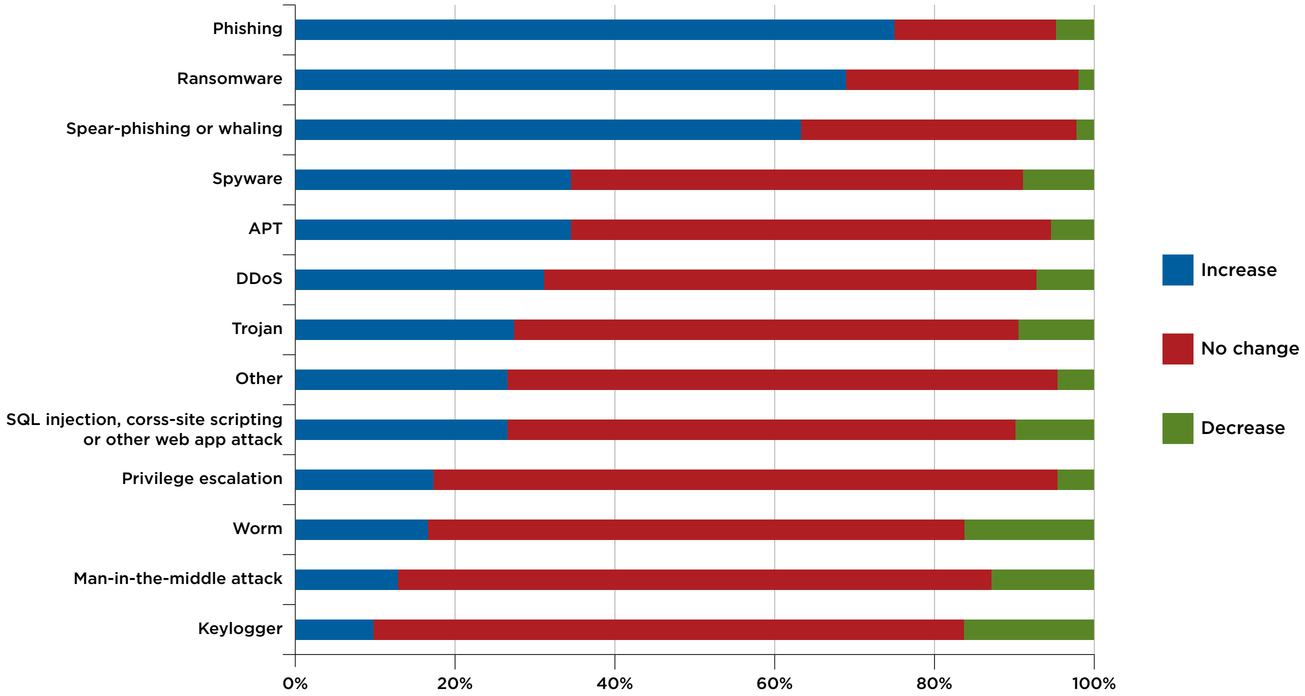
Phishing, followed by ransomware and spear phishing or whaling, are the fastest-growing types of cyber threats (Fig.3). Eighty percent of organizations reported having a phishing incident in the past 12 months, and 27% said those threats resulted in a significant impact. Spear phishing or whaling occurred in 58% of organizations, with 13% reporting a significant impact.[2] The average impact of a successful spear-phishing attack: $1.6 million.[3]

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

[1] Symantec (April 2017). Internet Security Threat Report.

[2] SANS (September 2016). Exploits at the Endpoint: SANS 2016 Threat Landscape Survey.

[3] Vanson Bourne (2016). Spear Phishing: The Secret Weapon Behind the Worst Cyber Attacks.



Source: SANS Analyst Program (September 2016). Exploits at the Endpoint: SANS 2016 Threat Landscape Survey.

Figure 3. Phishing, ransomware and spear phishing outpacing other attack types.

Not only are spear-phishing emails personalized and targeted, the malware delivered with each email is also unique. Legacy anti-spam and antivirus (ASAV) systems cannot catch unique malware because their signatures have not been seen before. Phishing campaigns are short lived, using databases with landing pages that stay live for just a few hours. Traditional ASAV solutions need to see an instance of a threat-laden message and update their data feeds to address the new threats. Phishing sites often go offline by the time traditional solutions update their data feeds.

Spear Phishing 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 spear-phishing email is the first stage of a blended attack that involves further stages of malware outbound communications, binary downloads and data exfiltration.
- Well-crafted email forgeries. Spear-phishing email threats usually target 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.

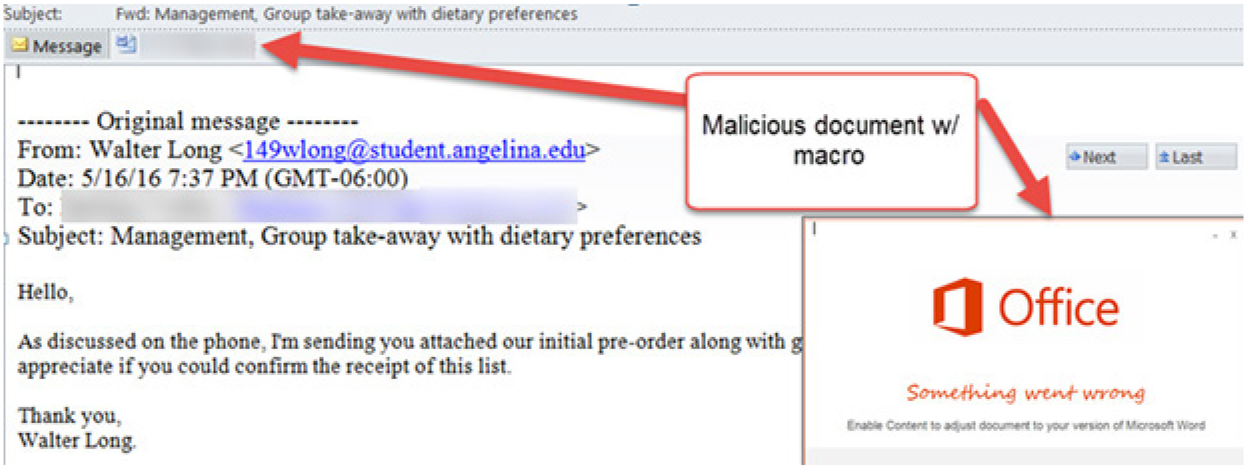
Spear phishing uses a blend of email spoofing, dynamic URLs and drive-by downloads to bypass traditional defenses.

Personalization

Instead of using generic themes or subjects for phishing emails such as “invoice” or “delivery confirmation,” which are still used in many attacks, sophisticated financial attackers tailor their phishing email to a specific client, location or employee.

Mandiant, a FireEye company, identified an unexpected trend in which attackers called victims on the telephone to help them enable macros in a phishing document, or tried to obtain a personal email address where the phishing document could be sent to avoid controls protecting corporate email. When a phishing email did not result in access to a target environment, these attackers sought to circumvent controls, even when it required a conversation.

Figure 4 is a sample email that was sent to our client after the attacker had spoken with an employee.



Subject: Fwd: Management, Group take-away with dietary preferences

[redacted]

-------- Original message --------
From: Walter Long <149wlong@student.angelina.edu>
Date: 5/16/16 7:37 PM (GMT-06:00)
To: [redacted] >
Subject: Management, Group take-away with dietary preferences

Hello,

As discussed on the phone, I'm sending you attached our initial pre-order along with g
appreciate if you could confirm the receipt of this list.

Thank you,
Walter Long.

Malicious document w/ macro

Something went wrong

Enable Content to adjust document to your version of Microsoft Word

Figure 4. Email sent after attacker called an employee on the telephone.

Real World Example

How a China-based attacker stole vast amounts of PII

One attack began when threat actors successfully enticed 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, the threat actors:

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

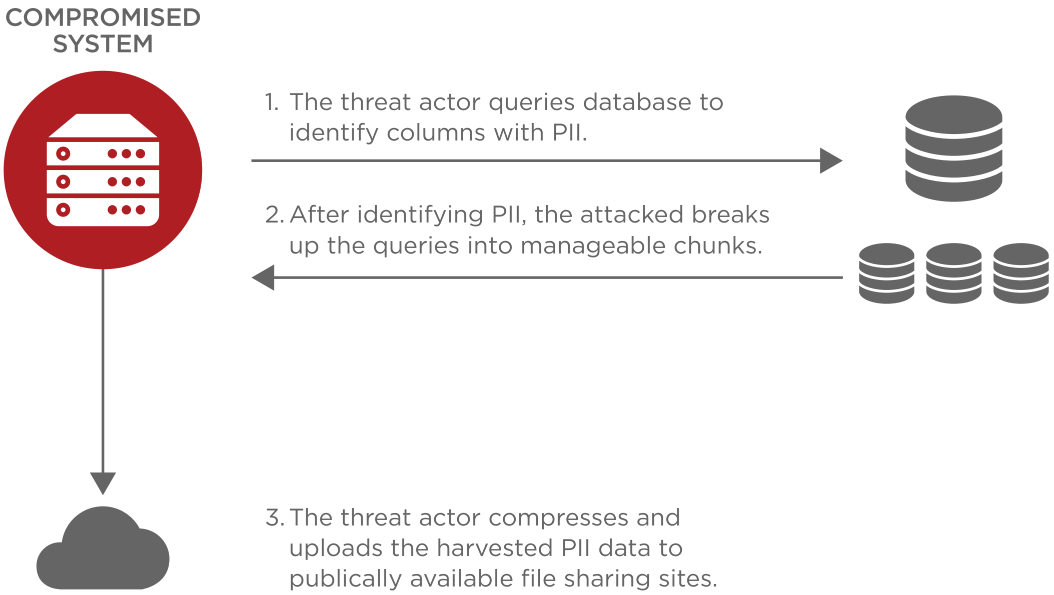

COMPROMISED SYSTEM
1. The threat actor queries database to identify columns with PII.
2. After identifying PII, the attacked breaks up the queries into manageable chunks.
3. The threat actor compresses and uploads the harvested PII data to publically available file sharing sites.

Figure 5. Exfiltration of PII data.

Better Email Security

Organizations need an innovative email security solution that automatically detects and blocks advanced targeted campaigns that involve spear phishing, ransomware, the harvesting of credentials or the impersonation of legitimate senders. FireEye Email Security uniquely delivers these capabilities to proactively protect 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, organizations can determine which individuals within the organization have 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 the most dangerous cyber threats

FireEye Email Security offers dynamic defense to detect attacks from the very first time they're seen and block the most dangerous cyber threats, including malware-laden attachments and URLs, credential phishing sites and impersonation attacks hidden among millions of messages. This is a critical requirement because spear phishing and other email-based attacks are always changing and easily evade signature-based and reputation-based security. With this kind of detection, FireEye technology can block the advanced malware embedded in attachments and hosted on dynamic, fast-changing domains and block malware-less impersonation attacks that get past other email security products.

Defense against malicious code installs and block callbacks

FireEye technology identifies whether suspicious attachments and URLs are malicious. Any callback 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

FireEye is on the front lines of cyber attacks every day, and real-time knowledge of the threat landscape ensures that FireEye Email Security directly addresses today's threat actors and the techniques they employ. The technology is informed by our unique intelligence network combining machine, adversary and victim intelligence that provides unparalleled visibility into emerging threats to accelerate response.

The information gathered from a thorough analysis of spam campaigns and advanced attacks can be used in the following ways.

- FireEye systems can fingerprint 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 email-borne threats.

Detect and block 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 or malware-less 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 spam campaigns and advanced, targeted attacks, organizations need comprehensive threat protection that safeguards multiple threat vectors and addresses every stage of an attack.

FireEye Email Security offers flexible deployment options with support for on-premises, cloud with an AVAS add on and hybrid environments. It delivers the comprehensive email protection necessary to stop spam campaigns and advanced, targeted attacks and protect 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**

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

© 2018 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. **WP.SPA.US-EN-032018**

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 5,300 customers across 67 countries, including more than 845 of the Forbes Global 2000.