proofpoint™

Control tomorrow's email risks today

The New Phishing Threat: Phishing Attacks
A Proofpoint White Paper

Proofpoint, Inc. 892 Ross Drive Sunnyvale, CA 94089 P 408 517 4710 F 408 517 4711 info@proofpoint.com www.proofpoint.com

CONTENTS

INTRODUCTION

The Rustock botnet takedown in March 2011 resulted in an unprecedented and sustained drop of global spam volumes. Despite this drop, the threat of email borne attacks is greater than ever with malware volumes increasing drastically. Specifically, the email threat comes in the form of phishing and spear-phishing emails. Historically, phishing attacks targeted end-user with attackers going after credentials to financial accounts. But modern phishing attacks have evolved toward targeting sensitive corporate data as evidenced by the high profile data breaches referenced earlier. A clear driving force is the financial payoff of stolen data. Many of organizations have been targeted with advanced persistent threats and attackers have utilized phishing and spear-phishing emails as the entry vector into these targets because they are currently weakest link. Phishing and spear-phishing emails represent the greatest threat to all organizations today.

PHISHING ATTACKS

Phishing attacks leverage two elements to achieve their goals: social engineering and subterfuge.

- **Social Engineering:** Attackers will commonly use spoofed emails to lead recipients toward a call to action. Counterfeit websites may be designed to trick recipients into divulging information or worse, host drive-by downloads of malware. With the explosive usage of social networking sites, attackers have additional resources in which to concoct compelling and relevant phishing messages.
- **Subterfuge:** Subterfuge, or the act of deception to achieve a particular goal, is a core tactic in phishing. While traditional phishing attacks may utilize social engineering to get recipients to divulge account names and credentials directly, there has been a trend towards schemes that are used to install malware. Malware varies from phishing specific key-loggers that contain tracking components to monitor specific actions (such as website visits to financial institutions, retailers and other e-commerce merchants) or website redirection from legitimate to counterfeit sites. Even more malicious threats have surfaced with backdoors being exploited to search for and extract sensitive data.

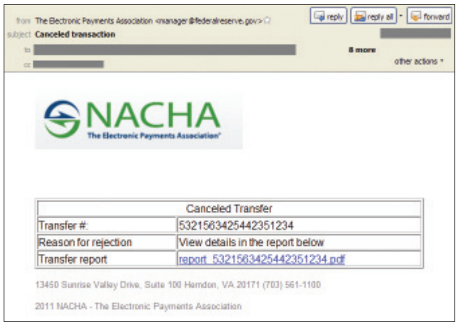
Together these elements emerge, masquerading as emails from government agencies, business partners, an internal IT department, or even company executives. To drive recipients to action, the messages may warn of an account suspension (financial services) or contain fake bills designed to encourage a user to perform further examination of fraudulent activity (PayPal).

If the recipient divulges passwords to other online accounts, such as PayPal, eBay, or a financial institution, more traditional cyber theft may occur with fraudulent transactions and purchases made.

If a recipient's system and/or email credentials are compromised, the accounts are often used to launch additional phishing attacks – typically with even higher conversion rates due to the use of a legitimate account and email system.

By far, the largest threat is the possibility that malware is delivered into the corporate environment. Once inside the network, it becomes significantly easier to propagate across the network by "shoulder-surfing" until access to a desired host is made and corporate and/or sensitive data acquired.

These last two scenarios are particularly dangerous to organizations because it is no longer just the end-user that becomes the victim of the phishing attack, but the enterprise is now truly at risk. An organization's reputation can be harmed if it suddenly finds itself as a source of spam and phishing attacks. As a consequence, valid business email may be undeliverable. In some cases, compromised machines have been used to launch attacks into trusted partner organizations, with the intent of stealing sensitive data.



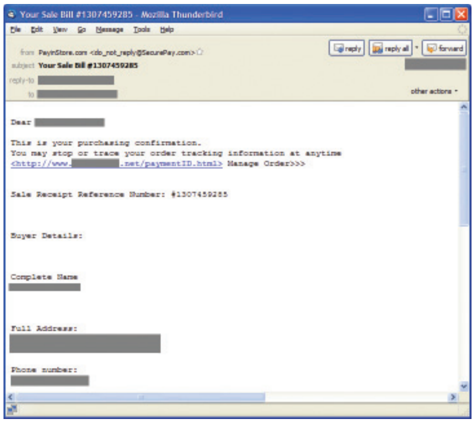
from The Electronic Payments Association <manager@federalreserve.gov>
subject **Canceled transaction** [redacted]
to [redacted] 8 more
cc [redacted]

Canceled Transfer	
Transfer #:	5321563425442351234
Reason for rejection	View details in the report below
Transfer report	report_5321563425442351234.pdf

13450 Sunrise Valley Drive, Suite 100 Herndon, VA 20171 (703) 561-1100

2011 NACHA - The Electronic Payments Association

Figure 1. The Electronic Payments Association (NACHA) has long been used by spammers in phish emails to elicit financial information from individuals. However, interesting new variants of these attacks were seen in June as well as an increase in volume. The variants included links to malware as opposed to the classic phishing request for information. As shown in this example, the link appears to be to a PDF report while in reality it was pointing to an executable hosted on a compromised web site.



Your Sale Bill #1307459285 - Mozilla Thunderbird
File Edit View Go Message Tools Help
reply
reply all
forward
other actions

from PayinStore.com <do_not_reply@SecurePay.com>
subject Your Sale Bill #1307459285
[redacted]
reply-to [redacted]
to [redacted]

```
Dear [redacted]

This is your purchasing confirmation.
You may stop or trace your order tracking information at anytime
<http://www.[redacted].net/paymentID.html> Manage Order>>>


Sale Receipt Reference Number: #1307459285



Buyer Details:



Complete Name
[redacted]



Full Address:
[redacted]

Phone number:
[redacted]
```

Figure 2. A highly varied attack used a purchase receipt as its phish attack vector. Highly varied attacks such as this one use many different subjects, URLs, etc. Most variations use some knowledge of the targeted victim and, even worse, contained a link pointed to a compromised website which led to a malware download.

Trends in Phishing Attacks

Sites hosting phishing attacks are longer-lived than before: ~30 hours in late 2009 to 58 hours in 1H 2010 and 73 in 2H 2010 – this corresponds to and supports the fact that there is an increase in use of legitimate/ compromised sites in which attacks are being launched. According to the Anti-Phishing Working Group's report in 2H 2010, "This data suggests that phishers are utilizing more targeted tactics in order to achieve a better ROI on their phishing campaigns."

Phishing Attacks Are Working

The seriousness of these threats may sound very theoretical, but the reality is that phishing attacks actually are achieving their malicious goals. With alarming regularity, organizations are in the news reporting devastating breaches resulting from phishing and spear-phishing attacks. Epsilon, RSA, the United States Department of Energy facilities at Oak Ridge National Labs and Pacific Northwest National Labs, and the International Monetary Fund, are just some of the organizations hit with email borne threats that led to data breaches.

Advanced Persistent Threats

Advanced Persistent Threats (APTs) have emerged as a new type of cyber-threat, where attackers are utilizing a broad spectrum of technologies and techniques. Rather than purely being opportunistic, these attacks are highly focused, hence the notion of "persistence". Though APTs may utilize a wide variety of entry vectors, recent APTs have successfully breached enterprises primarily via phishing messages. This is largely because of the relatively high success rates of phishing attacks versus other attack vectors.

Example Of A Phish Attack

1. Phishing emails sent – employees are not necessarily high profile or high value targets.
2. Email is crafted well enough that even if is caught by the email security solution, employees may be tricked to retrieving it from their quarantine.
3. The employee then clicks on the URL in the message, initiating a drive-by download of malware.
4. Malware may be designed such that the desktop machine will reach out to the command and control servers.
5. Malware begins to propagate across the network, seeking specific user accounts with relevant privileges (initial entry points/accounts may not have sufficient administrative rights).
6. Once sufficient privileges are reached and target systems are reached, data is acquired and staged for exfiltration.
7. Data is exfiltrated (extracted outside the organization), typically via encrypted files over available ports – FTP, HTTP, or SMTP.

COST AND DOWNFALL OF ATTACKS

The costs of dealing with an attack fall broadly into three categories:

1. Remediation Costs – if phishing attacks are successful, administrators will be burdened with identifying and cleaning compromised machines, which may extend beyond just the specific targeted recipient machines. On average, each phish incident costs $484 to remediate.
2. Financial Loss – if the phishing attacks succeed in stealing sensitive information, the financial ramifications are significant. While hard to quantify, organizations need to consider how they value their most critical information assets. RSA noted in the EMC Earnings Call (Q2 2011) that as a result of their data breach, $66M was spent to replace tokens, monitor customers, and handle the fallout from the breach.
3. Reputation Loss – the most difficult to quantify is the reputation loss associated with a significant data breach. Public examples include the Sony data breaches, estimated at more than $170M.

THE CHALLENGES OF PROTECTING AGAINST THE PHISHING THREAT

Phishing attacks are certainly not recent phenomena – so why have they been so successful, with numerous high profile data breaches reportedly initiated via phishing attacks and countless other unreported and/or still undetected cases? The answer lies in the target and intent of a specific phishing message.

Historically, phishing attacks were focused on the login credentials of end-users – with a focus on accounts such as online banking, PayPal, or eBay accounts. These types of attacks were typically broad-based, high volume attacks with very small open rates. Due to the high volume nature of the attack, many anti-spam solutions were quick to detect these messages in spam traps and suitably effective in filtering these messages. But even if the occasional phishing message was missed and passed to an end-user, the victims tended to be individuals and the damage limited to the specific account that the user provided credentials to.

The issue now is that many phishing attacks are highly targeted with low volumes of messages. In addition to the increased use of compromised accounts to launch attacks, this has resulted in the reducing the effectiveness of reputation services associated with traditional spam solutions to detect phishing messages. While the use of reputation services is still important in the overall strategy of dealing with external email threats, addressing targeted phishing attacks requires a filtering engine that is capable of deep content analysis without relying on reputation scores for efficacy.

In a further effort to bypass spam filters, phishing messages are increasingly crafted with sparse features and little or no malicious content. The call to action is nothing more than a simple URL. With such sparse content, traditional spam filters are not well equipped to determine if these messages are legitimate or malicious threats. What is required is deep content analysis of these messages, including analysis of the URL linked in the messages to determine the intent. Only then, can an accurate determination of the message be made.

PROOFPOINT THREAT PROTECTION

Proofpoint approaches threat protection with 3-Phased, full closed-loop approach.

- **Detect:** Sophisticated multi-layered detection
- **Manage:** Granular routing and policy management
- **Respond:** Tools to prevent data repatriation, real time message tracing and triage and enterprise-class support

Backed by the patented MLX Threat Classification Engine, emails are classified based on the level of threat to an organization and managed accordingly. Real-time message tracing provide the necessary tools to triage any attack and the solution is backed by an enterprise-class support organization focused on supporting the mission critical communications infrastructure.

Detect

Proofpoint Threat Protection starts with multi-layered detection. A dynamic email reputation service starts by dropping the vast majority of large volume spam by leveraging the industry's most powerful connection management service. Detailed analysis of the remaining messages is performed by the MLX Threat

Classification Engine. Powered by Proofpoint MLX machine learning technology, messages are evaluated for a number of elements, including:

- **Structural Elements –** Analysis of header, body, and attachments
- **Correlation Analysis –** Correlation of terms for contextual analysis
- **Masqueraded URLs –** "Liar Links" and hiding of destination URLs
- **Domain Permutations –** Tracking of permutated domains (e.g., http://www.numberonebank-customerservice.com, as a variation of the legitimate domain http://www.numberonebank.com by adding "-customerservice" to the URL)
- **URL Shorteners –** expanded to full URLs and analyzed for reputation

Zero-Hour Threat Detection provides the final layer of defense by identifying suspect messages during the early stages of low-volume attacks. Messages are held until additional data and information can be gathered to confirm the specific threat.

Proofpoint is committed to leveraging technology standards that can further alleviate phish attacks by identifying spoofed domains. Proofpoint supports both SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail).

Manage

Once the messages have been classified, Proofpoint manages against the varying degrees of threats by providing granular routing and control of messages. Phishing messages are dangerous because of their ability to trick users into believing they are valid, often urgent messages, as well as the malicious capabilities associated with a phishing attack. Proofpoint directs phishing and spear-phishing messages into distinct phishing quarantines that end-users cannot release. This prevents critical security decisions from being made by end-users.

Respond

A complete strategy to combating malicious threats and attacks such as phishing is a comprehensive plan and tools. This includes the ability to scan the outbound mail stream both for instances of data repatriation and exfiltration as well as ensuring that any compromised machines do not become launch pads for additional spam or phishing attacks targeting partner organizations.

If an organization is attacked, real-time message tracing with Proofpoint Smart Search provides the ability to search for messages based on dozens of attributes, such as subject, sender, recipient, and attachments, allowing administrators to quickly identify specific targets of phishing and spear-phishing attacks for immediate remediation. Furthermore, Proofpoint customers can leverage the world-class enterprise support organization that not only provides traditional product support, but also provides threat support when organizations are under attack.

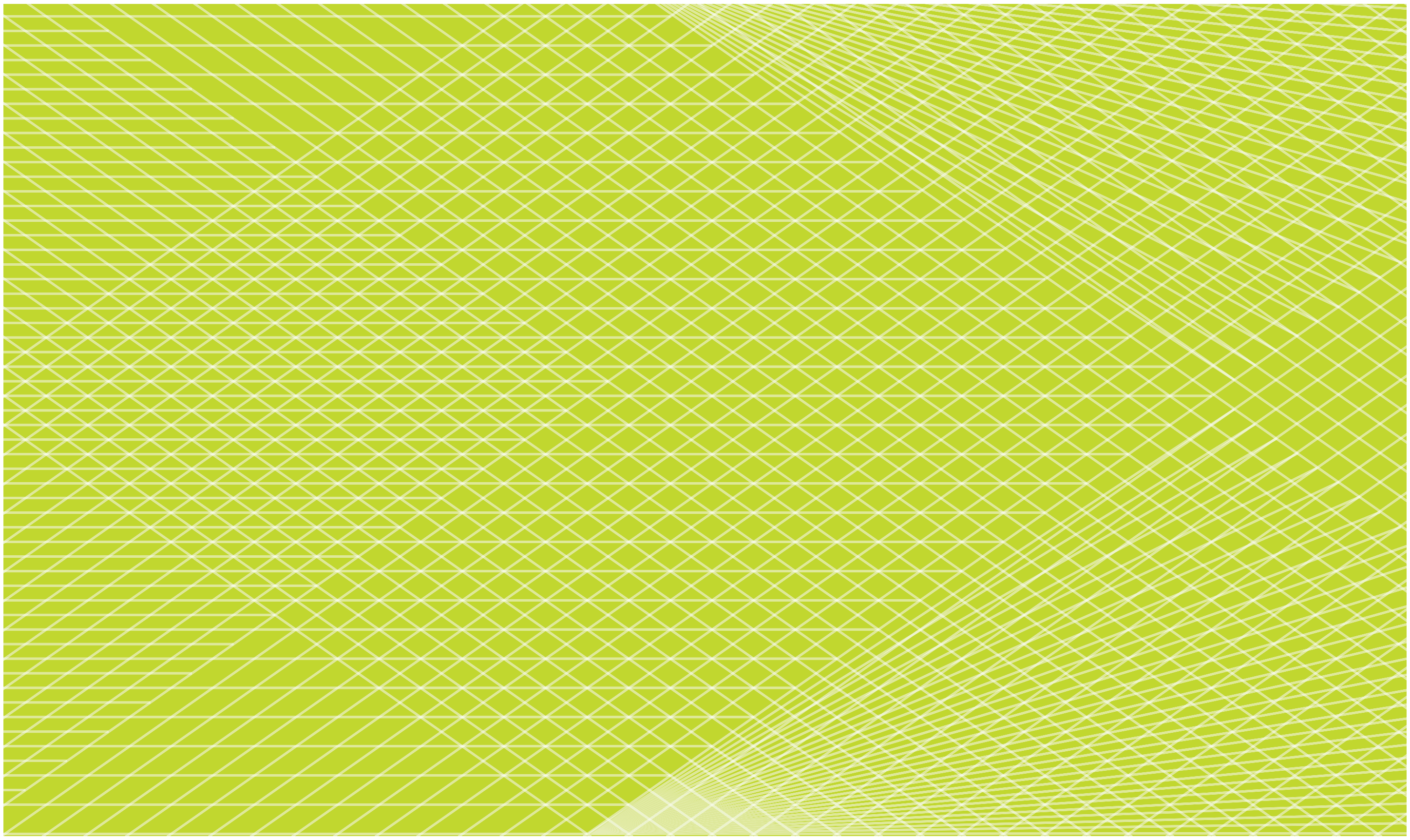
PROOFPOINT PHISH AUDIT

Proofpoint, in conjunction with the IT security team, can conduct an audit over a two-week period and deliver a complete audit report. This audit provides a mechanism to quantify the risk exposure your organization faces due to phishing as well as other types of malicious attacks, and includes factors such as remediation, financial, and reputation loss.

CONCLUSION

Addressing the modern day targeted phishing and spear-phishing attack requires a full-data protection approach that traditional email gateway solutions cannot address with antiquated technologies. A closed-loop approach of Detect, Manage, and Respond is necessary in order for organizations to be protected from the latest malicious threats. Proofpoint is dedicated to security and compliance for email and continues to invest and innovate to stay ahead of this evolving threat landscape.

To identify and assess your organization's current exposure, contact Proofpoint for a phishing audit. A full report of your number and types attacks at your organization can help you assess your organization's risk.



US Worldwide Headquarters
Proofpoint, Inc.
892 Ross Drive
Sunnyvale, CA 94089
United States
Tel +1 408 517 4710

US Federal Office
Proofpoint, Inc.
13800 Coppermine Road
Suite 203
Herndon, VA 20171
United States
Tel +1 703 885 6809

Asia Pacific
Proofpoint APAC
Suntec Tower 2,
9 Temasek Boulevard,
31F
Singapore 038989
Tel +65 6559 6128

EMEA
Proofpoint, Ltd.
200 Brook Drive
Green Park
Reading, UK
RG2 6UB
Tel +44 (0) 870 803 0704

Japan
Proofpoint Japan K.K.
BUREX Kojimachi
Kojimachi 3-5-2,
Chiyoda-ku
Tokyo, 102-0083
Japan
Tel +81 3 5210 3611

Canada
Proofpoint Canada
210 King Street East,
Suite 300
Toronto, Ontario,
M5A 1J7
Canada
Tel +1 647 436 1036

Mexico
Proofpoint Mexico
Salaverry 1199
Col. Zacatenco
CP 07360
México D.F.
Tel: +52 55 5905 5306

Proofpoint focuses exclusively on the art and science of cloud-based email security, eDiscovery and compliance solutions. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against spam and viruses, safeguard privacy, encrypt sensitive information, and archive messages for easier management and discovery. Proofpoint's enterprise email solutions mitigate the challenges and amplify the benefits of enterprise messaging.

Control tomorrow's email risks today

www.proofpoint.com