Targeted Phishing

Email is the medium most organizations have come to rely on for communication. Unfortunately, most incoming email is unwanted—or even malicious. Today's modern spam-blocking appliances have little problem sorting the vast majority of unsophisticated spam campaigns, leaving end-user in boxes filled with only legitimate email. That's in spite of the fact that more than 87 percent of incoming mail consists of spam or abusive messages, according to the Messaging Anti-Abuse Working Group (MAAWG).

To get around advanced antispam technology, online criminals are becoming more dangerous and sophisticated. In addition to enticing a spam recipient to buy a dubious product, more lucrative phishing attacks seek to glean users' personal information, such as names and addresses, and even login information for their banks. Although the number of such phishing emails being sent is still relatively low, it is increasing, and the danger for intended victims is high. As Internet users become more adept at detecting clumsy attempts to phish personal information, spammers are selectively phishing smaller and smaller demographics with content that appeals specifically to each group. This form of highly targeted, socially engineered email is called targeted phishing, or "spear phishing, and can fool even the savviest of Internet users.

Trends and Solutions

Since the late 1990s, phishing emails (messages designed to fool the recipient into revealing personal information, such as login names and passwords) have been flooding email inboxes. The phishers—the online criminals who create emails that mimic messages from well-known online services or legitimate companies—typically send out millions of emails at a time, in hopes of stealing the online banking or other login names and passwords of even just a few recipients.

The trend continues today, but phishers have improved their game. Emails are media rich with the correct business logos, have proper spelling and grammar, and often use URLs leading to websites that mimic the institution targeted.

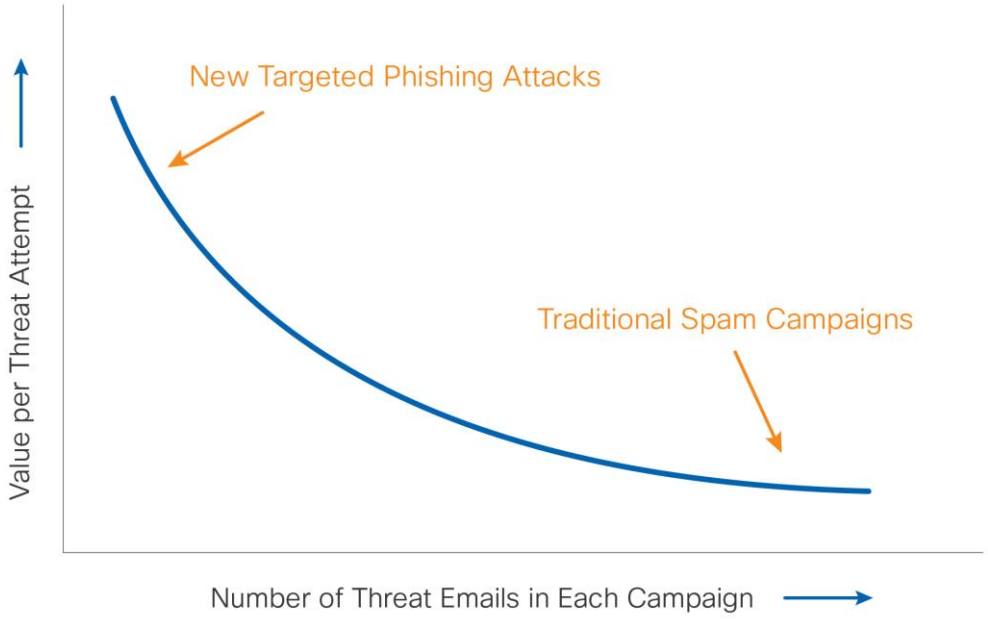
The Growth and Payoff of Targeted Phishing

A growing percentage of email-borne attacks are targeted phishing attacks, where a specific organization, or group of individuals, is singled out. The targets receive cleverly crafted phishing messages that are designed to solicit a deeper level of personal data, such as login and password information that can grant access to corporate networks or databases filled with sensitive information. In addition to soliciting login information, targeted phishing emails can also deliver malware: for instance, keystroke-logging programs to track everything the victim types.

Targeted phishing costs online criminals more time and money than traditional phishing campaigns. The scammers need to rent or steal lists of valid email addresses for a target organization, or group, and then create plausible emails that are likely to lure their recipients into supplying personal data. However, when targeted phishing succeeds, it has the potential for a bigger payoff, making the investment worthwhile.

Currently, targeted phishing messages represent about 1 percent of all phishing campaigns. However, because targeted phishing is often aimed at just a few well-placed individuals in an organization, it can potentially do a great deal of damage, from financial, data security, and customer relations standpoints. Additionally, the personalized approach of targeted phishing makes it more difficult to segregate these emails with standard antiphishing technologies, leaving organizations vulnerable.

Figure 1. Traditional spam campaigns are sent in high volumes with low expected click-through and sales conversion rates. New targeted attacks are more dangerous in nature and are relying on low volume to get through traditional spam filters.



Why Targeted Phishing Works

Techniques for getting victims to click through to websites (where they either unwittingly submit sensitive information to scammers or download malware on their computers) are becoming increasingly sophisticated. Most spam now includes URLs directing recipients to malicious websites. These days, the fraudulent websites that victims are directed to often look and feel extremely similar to legitimate sites.

According to a University of California Berkeley study, even long-time, frequent Internet users are sometimes fooled by malicious websites. To avoid being taken in by phishing websites, users have to use a strategy of consistently checking the content's apparent level of legitimacy, the address bar and its security settings, the padlock images in the browser frame, and the security certificate of any website they were directed to.

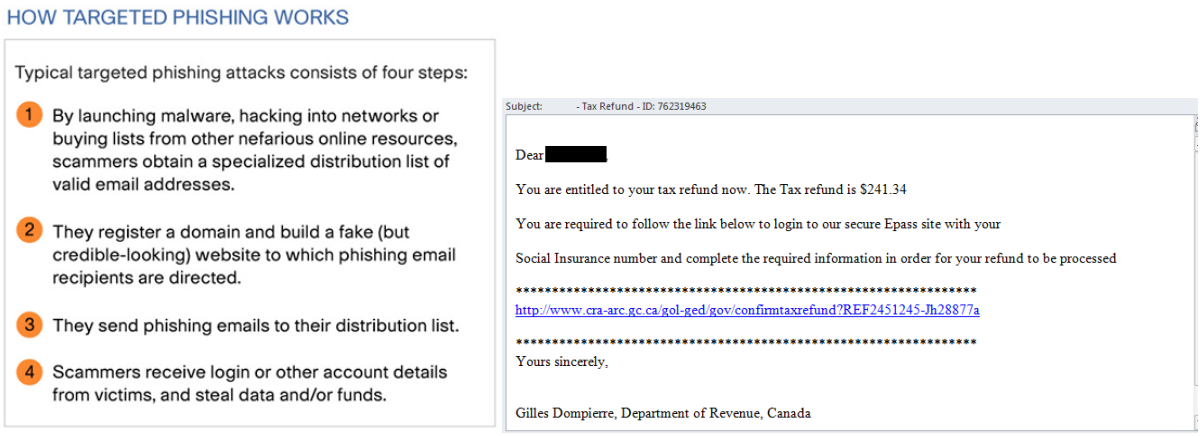
Phishing emails aimed at broad distribution lists today depend on social engineering techniques, such as content that demands an action from the recipient and referrals to legitimate-looking websites (such as fraudulent online banking sites). But these types of emails rarely use any personal data in the message.

Meanwhile, senders of targeted phishing emails take social engineering to a new level by researching their targets. By addressing recipients by name, sending the message directly to their email addresses, and making the content relevant to them, scammers make malicious email and the fake websites to which the victim is directed more credible.

In the following example shown in Figure 2, business executives received a phishing email purporting to be from the Canadian Department of Revenue, which claimed that citizens must log in to Epass and complete a form for their refunds to be processed.

A URL in the email launched an executable file for a Trojan that can steal all interactive data sent from the recipient's email browser and access data on the fake form before it was SSL-encrypted. Another targeted phishing email claimed electronically transmitted payments had not been received and instructed the recipient to resend payments to a specific banking account.

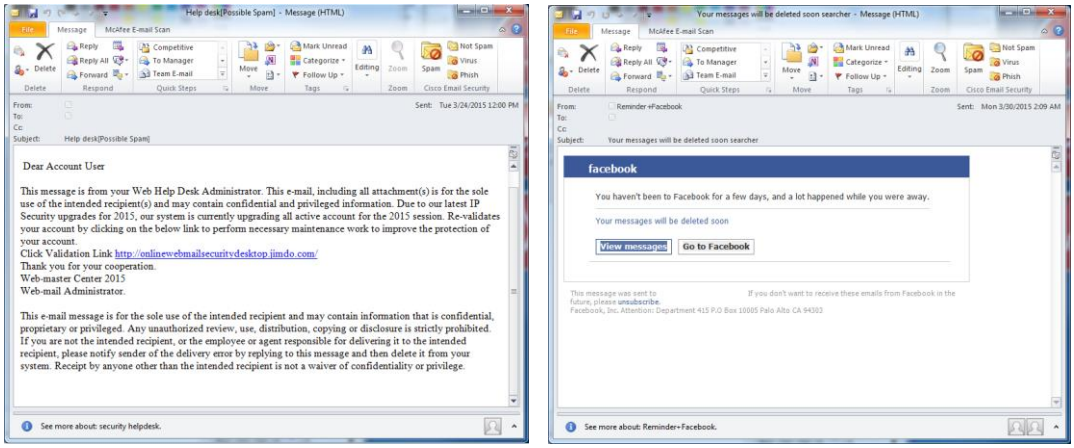
Figure 2. Targeted phishing attacks require criminals to efficiently build appropriate resources and trick victims into revealing valuable private information.



Social Engineering for Success

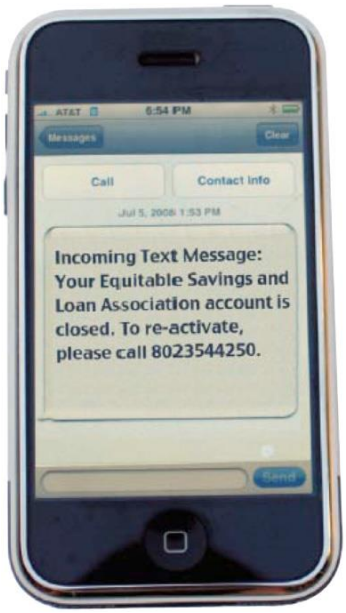
Targeted phishing attacks are not aimed at business executives only. Many recent campaigns involved emails, supposedly from Apple or Facebook to their customers, asking customers to review their accounts or log in to their accounts to read special messages, as shown in Figure 3. Other targeted attacks, seemingly from university IT departments, directed email users to reply with their webmail credentials to retain their university email account or take advantage of a security upgrade. These compromised accounts are then often used to send large-scale spam campaigns.

Figure 3. Examples of targeted phishing messages, purportedly from Facebook and university IT departments, designed to harvest account and email credentials.



Scammers sending out targeted phishing campaigns continue to refine their tactics for luring victims to fraudulent or compromised websites. Online criminals have even been known to send text messages to mobile phones (Figure 4). One such attack that targeted mobile numbers in the same area as a local bank informed customers that their accounts had been closed due to suspicious activity. The message then directed them to call a phone number to reactivate the account. The call-in number was set up by the scammers to collect account numbers and login credentials.

Figure 4. Criminals have also set up automated systems to collect banking login information from unsuspecting customers.



No matter how targeted phishing attacks are perpetrated, their goal is to glean personal data that allows online criminals to steal money or information. In 2015, senders of a successful targeted phishing campaign came close to scamming one of the sites for one of the most powerful government executive branches in the world, the United States White House, to divulge classified information.

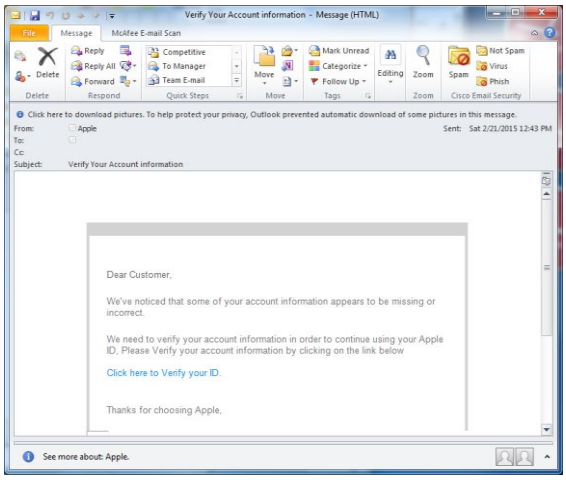
In the case of the White House, online scammers fraudulently obtained email account information from the U.S. Department of State (DOS), America's equivalent of a foreign ministry. The criminals (masquerading as employees of the DOS) then sent emails to individual White House employees indicating that they should click links that would ultimately compromise their system.

Fortunately, the attackers were only able to get access to its unclassified system where things, such as the U.S. President's schedule, reside. The White House security strategy is to separate information into two separate systems, classified and unclassified. This strategy suggests a pragmatic approach to data security, which is to assume that any information accessed by users will eventually be compromised.

Other recent phishing campaigns also demonstrate the threats associated with these messages and the fact that criminals are seeking to steal more than just banking information. One campaign involved emails sent to 80 million current and former customers of Anthem Blue Cross and Blue Shield, a major healthcare provider. These emails pretended to represent Anthem and told customers that their information was hacked. The phony email then offered a link to get free credit monitoring. Anthem had to physically mail all 80 million customers, warning them about the phishing email. Another campaign asked Apple iTunes customers (Figure 5) to confirm their accounts.

When they did so, not only was their iTunes account information stolen by the scammers, but also the victims' faced fraudulent charges on their accounts.

Figure 5. Messages that appear to be related to their iTunes accounts trick victims into providing login information.



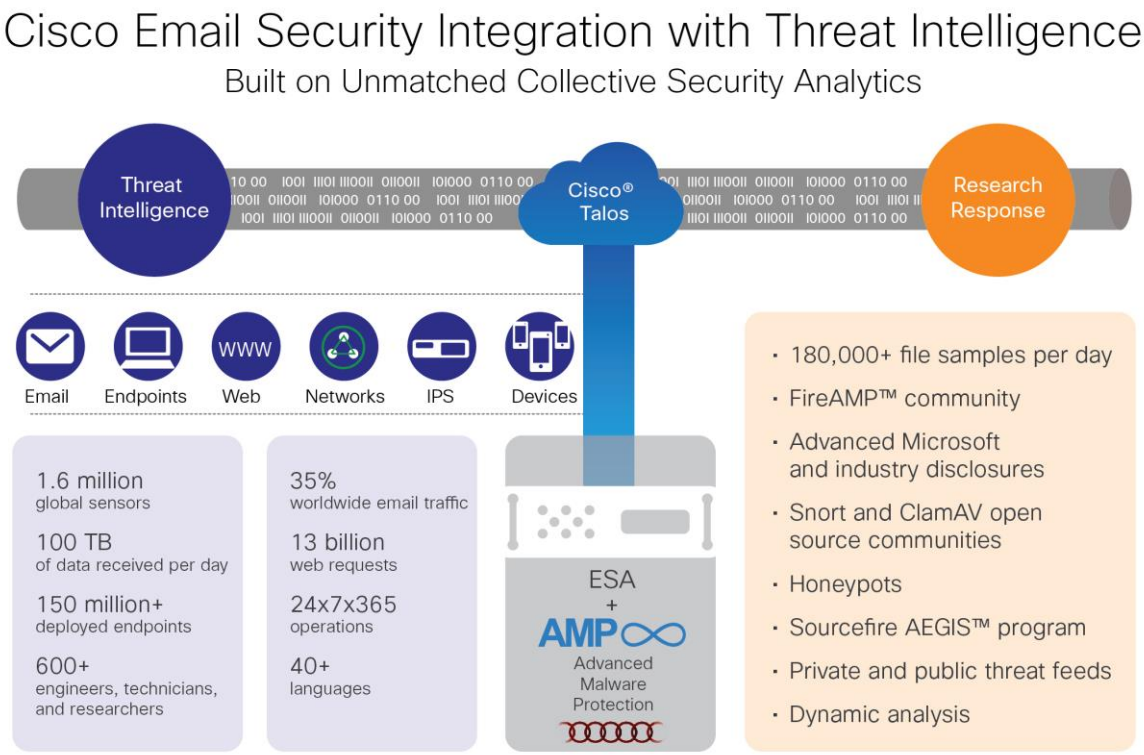
Even when recipients aren't fooled into responding to phishing emails, targeted phishing attacks adversely affect companies and their relationships with their customers. According to Forrester Research, executives who receive targeted phishing messages are losing confidence in email. In its Phishing Concerns Impact Consumer Online Financial Behavior report, Forrester notes that 26 percent of U.S. consumers will not use online financial products, and 20 percent of consumers won't open emails from their financial provider or enroll in online banking or bill payment, all because they fear falling victim to a phishing attack.

How Cisco Thwarts Targeted Phishing

Cisco provides a sophisticated array of ever-expanding technologies to ensure that end users don't have to make decisions about whether the email they are viewing is an illicit bid for account information. With Cisco® solutions, customers can safely use email and the web, and they are protected from new types of attacks such as targeted phishing. Cisco enables a multilayered approach that involves monitoring worldwide email and web traffic, and using sophisticated web reputation filters and advanced email authentication technologies.

SenderBase: Cisco SenderBase® Network constantly monitors 35 percent of worldwide email and web traffic. SenderBase tracks approximately 200 parameters, such as email sending and website traffic volume, complaint levels, spam-trap accounts, Domain Name System (DNS) resolution, country of origin, and blacklist presence. The system then uses the data collected to create a reputation score to indicate the threat level for every email message coming in to an organization, as well as the URLs contained in each email. Because 90 percent of malicious emails contain URLs, the SenderBase unique capability of monitoring both web and email traffic is a key component in Cisco's ability to effectively identify and block targeted phishing attacks.

Figure 6. Cisco product portfolio and security intelligence covers more than just email. By covering email and web security, firewalls, intrusion prevention system (IPS), endpoints, and more, you get the intelligence and insight into threats needed to deliver security effectively.



Cisco Web Reputation Filters: Cisco Web Reputation Filters assign web reputation scores to URLs in all emails, based on each URL's likelihood to host malicious content. Based on these reputation scores, Cisco email and web security appliances then allow, flag, or block emails from certain senders and traffic with certain websites.

Reputation scores are based on SenderBase data and additional analysis of hard-to-spoof IP address data, such as how long a domain name has been registered, in which country the site is hosted, whether a domain purporting to be hosted by a Fortune 500 company is in fact hosted by that company, and/or how frequently that changes.

Cisco Anti-Spam: The Cisco Anti-Spam engine makes use of the reputation components of URLs when making decisions on handling messages. URLs with poor reputations raise the scoring of messages on the threshold of spam verdicts, causing them to be tagged as spam or suspect spam.

Cisco Outbreak Filters: These filters use targeted rules, URL reputation, and analytics to identify approximately 20 different types of threats including phishes, robbed abroad, money mule, 419, and more. Outbreak Filters give administrators the option to prewrite warnings to messages and to rewrite suspicious URLs before delivery for click-time analysis in the cloud, stopping phishing sites and new, unknown threats, such as infected file downloads or drive-by malware sites.

Cisco AMP (Advanced Malware Protection): Cisco AMP provides a mixture of file reputation, sandboxing, and retrospection to stop malware and protect your users from malicious email attachments. Cisco AMP does more than protect your organization at the time of the file crossing the ESA. File retrospection provides updated information if the file's disposition changes after it has arrived in your organization. This unique feature provides protection against malicious files that try to hide their true intentions from sandboxing.

SPF, DKIM, and DMARC email verification: Advanced email authentication techniques enable the matching of purported and actual sender identities. Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) are two popular, complementary email authentication methods that can detect fraudulent emails and Domain-Based Message Authentication, Reporting, and Conformance (DMARC) provides additional logic to tie them together. These authentication technologies are currently gaining broader acceptance among industry groups, email providers, and enterprises, and their wider use enhances their efficacy in combating phishing email.

SPF is a form of sender path authentication that helps recipients identify the authorized mail servers for a particular domain and validate that emails they received did, in fact, originate from these authorized sources. Mail senders (such as ISPs and corporations) that use this technology publish SPF records that specify which hosts are permitted to use their names. SPF-compliant mail receivers use the published SPF records to test the authorization of the sending mail transfer agent's identity during an email transaction.	**DKIM** is a cryptographically based authentication method that helps verify and determine the authorization of email from a given domain. DKIM provides a cryptographic signature (or key) of multiple email header fields and the body of a message. In its DNS record, a web domain protected by DKIM publishes the public key (or domain key) that corresponds to its self-generated private signing key. Email recipients can use that key to verify that the message header and body match the identity of the sending domain, helping them determine whether the email is likely to be a phishing or other malicious message.
DMARC is a policy distribution mechanism that allows email senders to specify policies and preferences for message validation, disposition, and reporting. Recipients of messages from DMARC-enabled senders can use this information to improve mail handling. Recipients using DMARC can use this information to make decisions on incoming emails ranging from no acting on email, quarantining, or altering the message before delivery to rejecting the email.	

DMARC, SPF, and DKIM can be very effective at detecting targeted phishing messages, but they have limitations. According to the Authentication and Online Trust Alliance (AOTA), about half of all legitimate email worldwide is currently authenticated. This level of adoption means that high-profile executives, who receive extremely high levels of spam and phishing emails, can benefit from additional email filtering and blocking tools based on email authentication failures.

HTML sanitization: HTML sanitization (also known as HTML-Convert) offers additional protection for emails that meet predetermined criteria, such as when SPF and DKIM are not able to authenticate a message. When HTML sanitization is enabled, URLs are made nonclickable and converted to plain text, exposing hidden, potentially malicious content to the recipient. This does add some burden for recipients when they wish to visit legitimate URLs cited in messages, because they have to copy and paste the plain-text links into their browsers to visit the websites. But for those individuals targeted by scammers, it offers an excellent layer of additional protection because it enables them see which website they are attempting to visit.

The Cisco S-Series Web Security Appliance: For organizations looking for in-depth defense against targeted phishing and other malware attacks, the Cisco S-Series Web Security Appliance provides an integrated, layered, and easy-to-manage platform for web security. It addresses the entire spectrum of web traffic, protecting against both known and unknown sites through the use of powerful reputation filters and antimalware defense technologies.

Cisco Cloud Web Security: Cloud Web Security provides similar in-depth defense against targeted phishing and other malware attacks as the S-Series Web Security Appliance, but it allows organizations to gain cloud efficiencies and protect highly mobile knowledge workers from web threats across any location inside or outside an organization.

Summary

A new threat in phishing is becoming a dangerous problem: targeted phishing. These messages use advanced social engineering techniques, such as addressing recipients by name (and identifying their companies), to convince carefully selected victims to unwittingly pass sensitive data or money to online criminals.

As targeted phishing emails take more resources to set up, they currently are only a small portion of phishing email worldwide. However, their payoffs can be enormous, which means their numbers will undoubtedly increase.

To help organizations avoid falling victim to targeted phishing campaigns and other malicious attacks, Cisco offers a layered, integrated approach for email and web security, combining Internet traffic monitoring, reputation filters, URL-enabled antispam services, Cisco Outbreak Filters and Advanced Malware Protection, URL filtering, and authentication technologies.

Contact

Cisco sales representatives, channel partners, and support engineers are ready to help you evaluate how Cisco content security products can make your email infrastructure secure, reliable, and easier to manage. If you believe that your organization can benefit from industry-leading Cisco products, call 800-428-9596 or visit us on the web at http://www.cisco.com/go/emailsecurity.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-701843-01 05/15