IBM Security

The perils of phishing

How cybercriminals are targeting your weakest link

IBM X-Force® Research
Managed Security Services Report

IBM

Click here to start ▶

Contents

Executive overview

Email isn't a novelty any more. It ties us to our family, our friends and our work. It helps us track our schedules and keep our appointments. It lets us send each other pictures, videos and documents almost instantly, far faster than postal mail ever could. No wonder this hugely popular worldwide communications tool is now a prime target for cybercriminals and state-sponsored hackers. You and your employees are now the focus of many adversaries with a single objective: penetrating your network and stealing or manipulating financial and confidential data, personal and sensitive information, and intellectual capital.

This paper examines how criminals use emails specifically designed to gain access to your personal information as well as your company's network and details how they entice employees to fall victim to phishing.

History of phishing

The first recorded use of the word "phishing" was found in the AOL hacking tool AOHELL, which contained a function that allowed the attackers to glean user account passwords and financial information. AOHELL was designed specifically to allow attackers to pose as AOL representatives. The "phishers" would send a private message to users of AIM (AOL Instant messenger), asking them to reveal their passwords in order to "verify" their accounts. If the unwary user complied, the phisher could then use their AIM account for frauds or spamming.

Email has become a prime target for cybercriminals and state-sponsored hackers who want to penetrate your network and steal or manipulate your data.

Contents

Once they were able to capture credit card information, phishers realized that attacks against online payment systems might be feasible. That was indeed the case. The first known successful attack was in June 2001 against a digital gold currency operated by Gold and Silver Reserve. Retail banks suffered their first attack two years later (detailed by Kris Sangani in *The Banker*), and by 2004, phishers were enjoying waves of success against both banks and their customer bases. All kinds of new, ever-more-sophisticated varieties of phishing have been developed since then. The concept has proven effective.

Who are the attackers?

Because spear phishing campaigns—targeted attacks on specific organizations or individuals—are proving very effective (see Figure 1), many "threat actor" groups use this tactic alone. Here are a few groups that have been identified by CrowdStrike.

About this report

This report was created by the IBM Managed Security Services Threat Research group, a team of experienced and skilled security analysts working diligently to keep IBM clients informed and prepared for the latest cybersecurity threats. This research team analyzes security data from many internal and external sources including event data, activity, and trends sourced from tens of thousands of endpoints managed and monitored by IBM for Managed Security Services accounts around the globe.

Contents

Gothic Panda

This group has been targeting high-profile organizations within the government research and development sector since 2007. Their attacks include links to sites hosting exploits for Microsoft Internet Explorer, which usually results in Microsoft issuing out-of-band patches.

Temper Panda

First seen in June 2012, this group has been using extensive spear phishing attacks against U.S. government targets to deliver malicious attachments containing the Trojan Poison Ivy malware and the Java remote access tool (JRAT).

Extreme Jackal

Targeting Israeli law enforcement, this group sends spear phishing emails with an attachment containing a variant of Xtreme Rat, a remote access tool. The actors are individuals from Middle Eastern countries known to have hacktivist motivations.

Pirate Panda

First seen in April 2013 and active against victims in Japan, this group sends spear phishing emails containing an attachment with remote access tool characteristics. This allows it to upload/download files, have full file system access and execute remote shell commands. The attachment targets a known buffer overflow vulnerability in the ListView/TreeView ActiveX controls in the MSCOMCTL.OCX library.

Wolf Spider

Possibly to gain a trading advantage in financial markets, this cybercrime adversary group, first identified in July 2014, uses targeted intrusion tactics to gain access to sensitive information. It doesn't use malware but makes heavy use of social engineering to gain access to corporate email accounts. It then sends spear phishing emails containing Microsoft Office documents that require the intended target to enable macros. Once enabled, the documents display an email login interface which harvests victims' credentials and relays them back to the adversary. The actor uses this access to compromised accounts to perpetuate the attack by using the accounts to send seemingly legitimate emails to others within the organization and also to related entities such as consultants and legal counsel.

Contents

Toxic Panda

This actor has been found to use spear phishing emails with malicious Rich Text File (RTF) file attachments containing a ".doc" extension that exploits a Microsoft Windows Common Controls vulnerability (CVE-2012-0158). The exploit targets only Chinese language builds of pre-Vista versions of Windows and is designed to fail on all other systems. Upon successful exploitation, shellcode in the malicious document is used to drop and execute a WinRAR self-extracting archive (SFX), which in turn drops other malware components that allow a remote server to control the infected computer.

Magic Kitten

CrowdStrike Intelligence locates this adversary in Iran and traces its earliest activity back to November 2008. The group maintains a low profile and its activity does not appear to be widely tracked. It utilizes a highly modular remote access tool consisting of multiple independent components. The preferred delivery vector appears to be spear phishing emails with malicious attachments containing a dropper that places the base module of the remote access tool on the victim's system to establish a foothold in the victim's network. From there, the group can download follow-on modules with a number of functionalities: victim system enumeration, keylogging, data alteration, arbitrary file execution, remote shell, screenshot, voice recordings, web browser and email application credential collection, and file exfiltration. Magic Kitten targeting appears to be focused primarily on interests in the political sphere, most likely political opposition groups within Iran.

Toxic Panda targets only Chinese language builds of pre-Vista Windows installations and is designed to fail on all other systems.

Contents

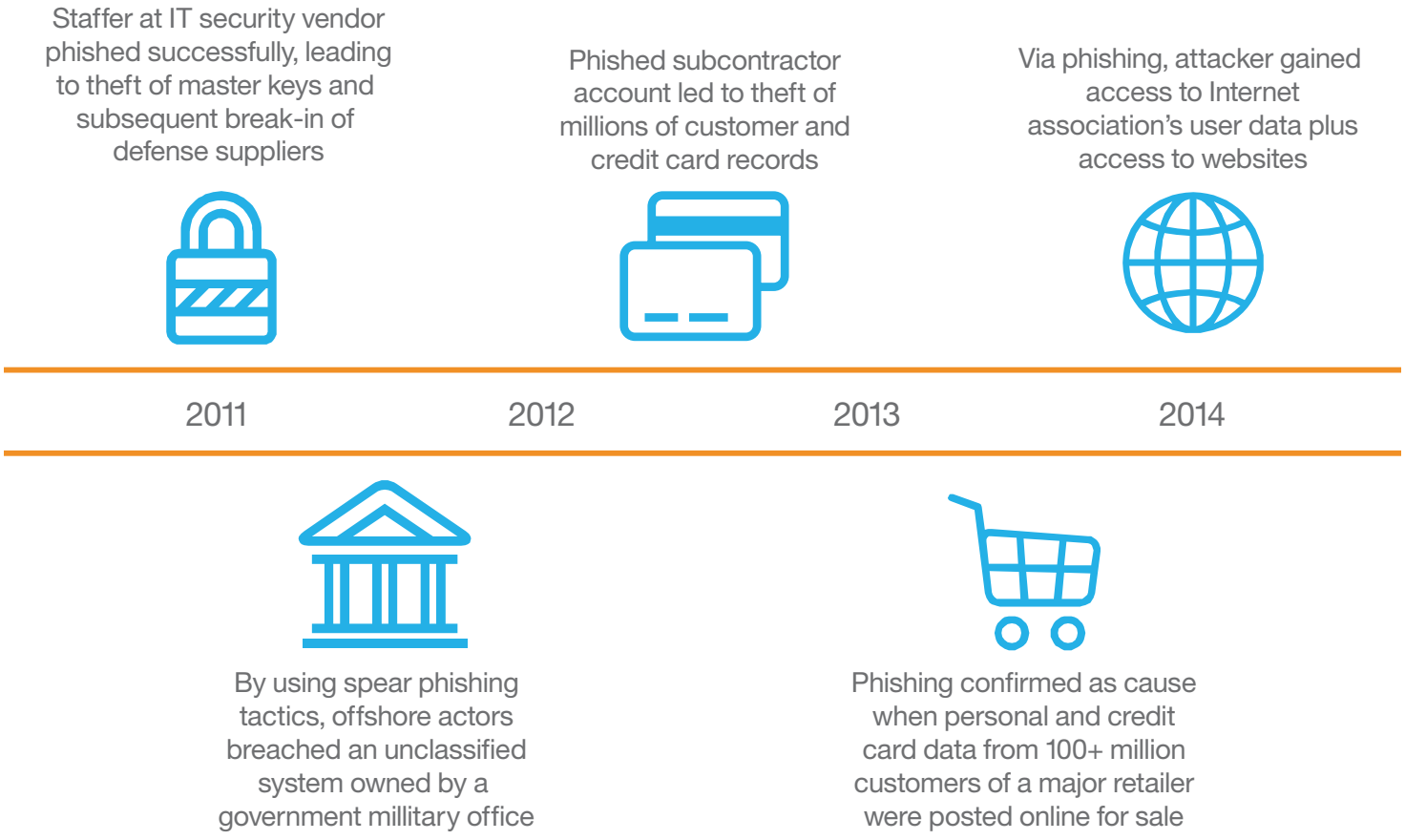

Figure 1. ***Notable phishing attacks.*** Phishing is a popular form of security attack because it is effective.

Contents

Types of phishing

Basic phishing

Basic phishing is a general method of using email to acquire personal information, financial data, usernames and passwords by pretending to be from a trustworthy source. These attacks, regarded as "incidental contact," are generally exploratory and aimed at a broad audience. Using a combination of social engineering and technical deceit, criminals try to persuade a potential victim to open embedded links or file attachments within the emails. The attacks are usually distributed in mass numbers and sent out like spam.

Spear phishing

Spear phishing, which consists of phishing aimed in a targeted attack at specific individuals or companies, uses tactics such as sender impersonation and mail filter and antivirus evasion techniques. Attackers may gather personal information about their target to increase their probability of success. Spear phishing emails can contain links to drive-by downloads, weaponized document attachments such as Word, PowerPoint or Excel, and websites frequented by a particular organization, industry or other group (known as a "watering hole" attack strategy). Spear phishing also leverages advanced personal threat vectors very successfully. According to Microsoft, the technique accounts for 91 percent of all advanced personal threat attacks on the Internet today. This method of phishing also leverages advanced persistent threat (APT) vectors.

Clone phishing

This is a type of phishing attack in which a legitimate, previously delivered email containing an attachment or link has its content and recipient addresses taken and used to create an almost identical or cloned email. The attachment or link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender. It may claim to be a resend of the original or an update to it. By exploiting the social trust individual users might assume when they have received the legitimate original email, this technique can then be used to pivot indirectly from an already infected machine to gain a foothold on another.

Contents

Whaling

Whaling is a method of phishing directed specifically at senior executives and other high-profile targets within businesses. It's also used against celebrities and politicians.

Vishing

Cybercriminals aren't limited to email. In telephone phishing, or vishing, they solicit their victims' personal information via unsolicited calls, most often using VoIP (Voice over IP) technology to spoof the source of the call. They pretend to be your utility company with ways to lower your bill, or a vehicle warranty company helpfully reminding you your warranty is about to expire and offering help renewing it. Vishing uses fake caller ID data to make it look as if the calls are coming from a trusted organization.

Smishing

This tactic is primarily used on cell phones and uses text messages that include URLs or phone numbers. The phone number often has an automated voice response system and, just like phishing, usually asks for your immediate attention.

Vishing uses fake caller ID data to make it look as if VoIP phone calls are coming from a trusted organization.

Contents

Methods used in phishing

Link manipulation

Most phishing methods use a form of technical deception in order to make a link in an email, and the spoofed website to which it actually points, appear to belong to a trusted organization. Simply inserting a trusted domain name between the <A> tags of the HTML code forces the visible link to look like a reliable destination, when in reality it leads to the phishing host. Many web browsers and email clients will reveal the real destination by hovering over the visible link in the email.

Filter evasion

Phishers have started using images instead of text to make it harder for anti-phishing filters to detect text commonly used in phishing emails. However, this has led to the evolution of more sophisticated anti-phishing filters that can recover hidden text in images. These filters use optical character recognition (OCR) to scan the image and filter it.

Some anti-phishing filters have even used intelligent word recognition (IWR) to supplement OCR. These filters can detect cursive, hand-written, distorted or rotated text, including upside-down text as well as text on colored backgrounds.

Website forgery

Once a victim visits the phishing website, the deception isn't over. Some phishing scams use JavaScript commands to change the appearance of their address bar by placing a picture of a legitimate URL over it or by closing the original bar and opening up a new one with the legitimate URL. An attacker can even use flaws in a trusted website's own scripts against the victim. These attacks, known as cross-site scripting, are particularly problematic because they direct users to sign in at their bank's or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack, making it very difficult to spot without specialist knowledge.

Contents

A Universal Man-in-the-Middle (MITM) Phishing Kit, discovered in 2007, provides a simple-to-use interface that allows a phisher to convincingly reproduce websites and capture login details entered at the fake site. To avoid anti-phishing techniques that scan websites for phishing-related text, phishers have begun to use Flash-based websites using a technique known as phlashing. These look much like the real websites, but hide the phishing text in a multimedia object.

Covert redirect

Normal phishing attempts can be easy to spot because the malicious page's URL will usually be off by a couple of letters from that of the real site. With covert redirect, however, an attacker can use the real website itself by corrupting it with a malicious login popup dialogue box, making this a perfect phishing method. Once the user logs in, the attacker can capture personal data, which in the case of social media sites could include an email address, birth date, contacts and work history—or, if the attacker is granted greater privileges, yet more sensitive information such as the target's mailbox, friends list and online presence. The attacker might even be able to operate and control the user's account.

Evil Twins

The Evil Twins phishing technique is particularly hard to detect. A phisher creates a fake wireless network that looks similar to a legitimate public network found in places like airports, hotels or coffee shops. Whenever someone logs on to the bogus network, fraudsters try to capture their passwords or credit card information.

Normal phishing attempts can be easy to spot. But covert redirect lets an attacker use the actual website, making it an ideal phishing method.

Contents

Recommendations and mitigation techniques

An organization's email system can be fortified by physical defensive mechanisms, but defense against phishing by cybercriminal organizations really begins with the user. And there, education is the key.

Education

When educating employees about phishing and how to avoid becoming a victim, use a variety of approaches—video, webinars, in-person instruction—and require training at intervals to make the risk clear. Openly communicate with your employees about any newsworthy data breaches involving phishing and emphasize that "this could happen to us." Also, consider adopting an employee testing program that encourages behavior modification.

Your education should include these main points:

- Most companies, banks and agencies never request personal information via email. Don't fall prey to this most common type of phishing.
- If you suspect an email might be a spear phishing campaign within your company, report it.
- Immediately suspect emails with generic greetings like "Dear Customer" or spelling and grammatical errors.
- Don't trust email attachments, even if they come from a trusted source. Unless you're expecting an email with a document attached, call the sender and confirm they sent it. Their computer might have been compromised and is sending emails without their knowledge, or their email address could have been spoofed.
- Never reveal personal or financial information in response to an email request, no matter who appears to have sent it.

Physical remedies

Security measures you can take to protect your systems and your employees include:

- **Inbound email sandboxing.** Deploy a solution that checks the safety of a link embedded in an email.

Contents

- **Real-time analysis and inspection of your web traffic.** Stop malicious URLs at your gateway, before they even get to your users' corporate inboxes. Even if your corporate email has inbound email sandboxing, a user might click on a malicious link through a personal email account like Gmail, in which case your corporate email spear phishing protection won't see the traffic. The web security gateway needs to be intelligent enough to analyze content in real time while being highly effective at stopping malware.
- **Virtual private networks (VPNs) for employees.** With many employees working from remote locations, the potential for them to use public networks in airports, restaurants or coffee houses is significant. Requiring VPN connections to encrypt the data connection back to the employer's network adds a layer of security to prevent cybercriminals from retrieving company data they can use in spear phishing attacks.

IDPS signatures and SIEM rules

Due primarily to the wide diversity of phishing attack types, IDS/IPS (intrusion detection system/intrusion prevention system) signatures and SIEM (security information and event management) rules do not exist. Because attackers will attempt to attach files that contain Trojan and malware characteristics, an anti-virus solution would be a more effective deterrent.

Protect your enterprise while reducing cost and complexity

From infrastructure, data and application protection to cloud and managed security services, IBM Security Services has the expertise to help safeguard your company's critical assets. We protect some of the most sophisticated networks in the world and employ some of the best minds in the business.

IBM offers services to help you optimize your security program, stop advanced threats, protect data and safeguard cloud or mobile. IBM Security Essentials and Maturity Consulting from IBM can help you address the challenges of phishing attacks by analyzing your security capabilities, documenting gaps in security controls across your organization and recommending short- and long-term improvements to reduce risks.

Contents

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 20 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

For more information

To learn more about the IBM Security portfolio, please contact your IBM representative or IBM Business Partner, or visit:
ibm.com/security

For more information on IBM Security Services, visit:
ibm.com/services/security

Follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

References

Spear Phishing
http://www.sans.edu/research/security-laboratory/article/spear-phish

History of Phishing
http://www.phishing.org/history-of-phishing

Phishing Defense
http://www.csoonline.com/article/2132618/social-engineering/11-tips-to-stop-spear-phishing.html

CrowdStrike Intelligence
http://www.crowdstrike.com

Contents

About the author

David McMillen, Senior Threat Researcher, IBM Managed Security Services, brings more than 25 years of network security knowledge to IBM. David began his career at IBM over 15 years ago as a member of the core team that created the IBM Emergency Response Service, which eventually grew and evolved into IBM Internet Security Systems.

As an industry-recognized security expert and thought leader, David has a rich background in IT security. He thrives on identifying threats and developing methods of solving complex problems. His specialties are intrusion detection and prevention, ethical hacking, forensics, and analysis of malware and advanced threats. As a member of the IBM Managed Security Services Threat Research Team, David takes the intelligence he has gathered and quickly produces tangible remedies that can be implemented within a customer's network on IBM's own proprietary threat detection engines.

David became interested in security in the 1980s, when he owned and operated one of the first companies to offer penetration and vulnerability testing. As the Internet's footprint grew, it became clear to him that there was a new challenge on the horizon: protecting data. David next worked with IBM Business Partner WheelGroup (later acquired by Cisco), where he helped develop the NetRanger IDS intrusion detection system and NetSonar, a vulnerability scanner. David also assisted with the development of the very first IBM intrusion detection system, BillyGoat. David has subsequently developed several other security-based methods and systems that have been patented by IBM.

Contributors

Michelle Alvarez, Threat Researcher/Editor

Nick Bradley, Practice Lead, Threat Research Group

Contents

IBM Security

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
December 2015

IBM

SEL03033-USEN-01