Evolution of Spear Phishing

White Paper

Executive Summary

Phishing is a well-known security threat, but few people understand the difference between phishing and spear phishing. Spear phishing is the latest evolution in the phishing trend; it's highly targeted and rapidly becoming the most significant security threat today. According to the FBI, there were 40,000 reported spear phishing incidents between October 2013 and December 2016. Further, Business Email Compromise (BEC) attacks resulting from spear phishing have cost organizations $5 billion in reported losses. This white paper reviews the evolution of spear phishing, key targets, and best practices to prevent these pervasive attacks.

Organizations have lost $5B from spear phishing. This is a 2,730% increase from 2015 to 2016.

- FBI, 2017

History of Phishing

Phishing originated around 1995 when people were far less aware of the risks associated with doing business online. In those days, hackers were known as phreaks, which is why phishing ended up being spelled with a "ph" instead of an "f". The first phishers pretended to be AOL employees and sent messages to AOL users through the company's messenger and email services. These emails would ask AOL users to verify their billing information, allowing them to steal financial information. The practice eventually spread beyond AOL and into the wider internet. Today, phishers send out mass emails, typically containing a malicious link or attachment. Their aim is to trick people into providing their credentials or credit card information, which the criminals can then use for their own financial gain.

Spear Phishing Attacks are Personal

Many people think that spear phishing is just another term for phishing, but it's actually a very different type of attack. Whereas phishers send emails in bulk to large numbers of people, spear phishers do extensive research before starting their illegal campaigns. They send highly personalized messages to targeted people within an organization, often relying on impersonation techniques. For example, they may pretend to be the CEO, CFO, or another trusted executive. Because of the economics, spear phishers are willing to invest a significant amount of time and effort in targeting a particular person, engaging in conversation through multiple emails to build trust. The aim is to get the victim to do something that benefits the spear phisher, such as wire transfer funds into the criminal's account. Often the victim has no idea they have been tricked as they believe they have transferred funds to pay a legitimate bill—making it even harder to get back the lost funds.

Detail	Phishing	Spear Phishing
Contains link(s) to a malicious site	●	–
Sent to many people	●	–
Personalized	–	●
Primary goal	Steal credentials or credit card information	Wire transfer, SSNs, credentials

Everyone is a Target

Spear phishing attacks are personal, and everyone is a target. Traditionally, spear phishers have targeted people working in finance departments in large enterprises. These employees often have access to the financial accounts of the company, and therefore, the funds that the criminals are keen to obtain. However, as these professionals become wise to spear phishing tactics, the criminals are widening their reach to departments outside of finance.

Today, spear phishing attacks target anyone who has the authority to send payments via wire or credit card, or who might have access to sensitive information. While CFOs and finance department employees are still the primary targets of spear phishing, people working in human resources and legal departments are also popular targets. These employees typically have access to a lot of personal information, which criminals can use to commit identity theft. In recent years, engineers and IT workers have been targeted, as they have access to source codes and sensitive intellectual property. Some people working in these departments also have access to large budgets and have the authority to make wire transfers. Administrative assistants are another popular target, as they often provide a way to obtain personal information of senior executives.

Many business owners assume that their companies are too small to be of interest to cyber criminals, but this is a dangerous assumption to make. Spear phishers do not restrict their attacks to large enterprises and C-suite executives. Today, all organizations are at risk of spear phishing, particularly smaller organizations that might not have the technology or resources in place to prevent a large-scale attack.

Spear Phishing is Pervasive

According to the FBI, business email compromise (BEC) scams were responsible for $5 billion in cumulative reported losses through 2016. Further, the FBI also reports a 2,370% increase in the number of these BEC attacks from 2015 to 2016. This figure continues to increase as scammers find new ways to target and trick employees into transferring money or revealing sensitive information.

Traditional Email Security Solutions are not Enough

Spear phishing emails are highly personalized. They also happen in a much smaller volume than traditional spam or phishing, and typically they do not contain malicious attachments or links. Because of this, they very difficult to detect using existing email security solutions that rely on volume, rules, or heuristic-based detections. Instead, spear phishers engage in real human conversation with the victim. The messages are very compelling social engineering attacks that ultimately give instructions within the body of an otherwise clean email, making them virtually undetectable with traditional solutions.

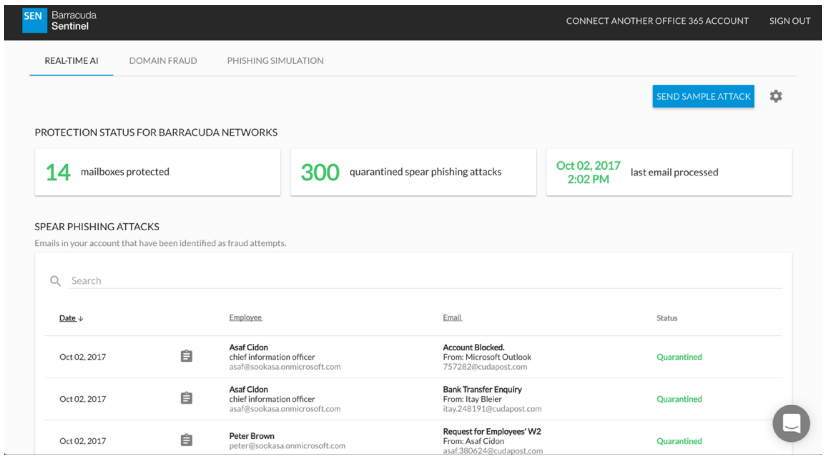
34% of organizations were hit with a phishing attack.

- Osterman Research, 2017

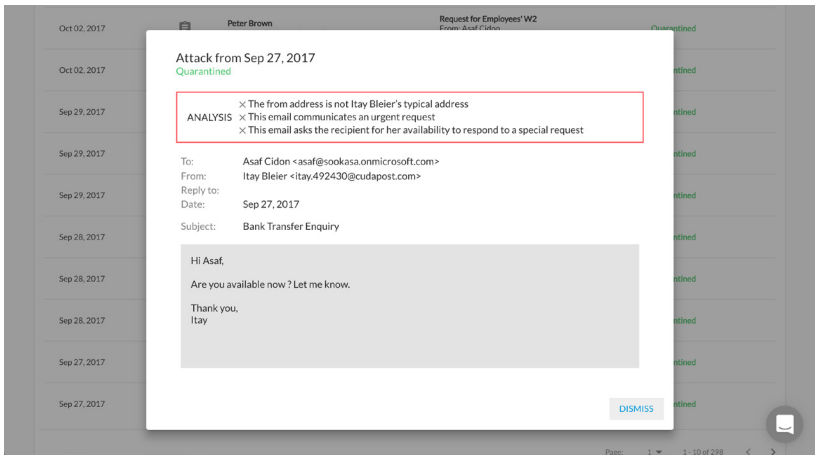
AI for Real-Time Spear Phishing and Cyber Fraud Defense

A comprehensive email security and management strategy is critical to keeping users, networks, and data safe from targeted spear phishing attacks. To combat these new targeted threats, it takes a new approach.

Barracuda Sentinel is a cloud service that uses artificial intelligence (AI) to stop spear phishing and cyber fraud in real time. The service combines three powerful layers into a comprehensive solution that prevents targeted attacks in real time. The first layer is an artificial intelligence engine that learns existing communications patterns to predict future attacks and identifies high-risk individuals inside an organization. The second layer provides domain fraud visibility and protection using DMARC authentication to prevent domain spoofing and brand hijacking. The third layer includes targeted fraud simulation training for high-risk individuals. Barracuda Sentinel integrates directly with Microsoft Office 365 via API, so there is no impact on network performance or user experience, and setup typically takes less than five minutes. Barracuda Sentinel works alongside any existing email security solution, including Barracuda Essentials, native Office 365, and others.



(Figure 1) Barracuda Sentinel Dashboard view



(Figure 2) Alert message indicating that the email contains a phishing attempt

Barracuda Essentials is one of the industry's leading solutions to protect against phishing and other email-borne attacks in Office 365. It addresses customers' security concerns with advanced features including attachment sandboxing, antivirus, anti-phishing, and typosquatting protection to secure against advanced threats. Data loss protection and email encryption keep sensitive information, such as credit cards and customer data, safe. Secure archiving and backup helps customers ensure regulatory compliance.

Barracuda Essentials and Barracuda Sentinel are also ideally suited for managed service providers (MSP), with their pure-cloud architecture, easy-to-use centralized management, and support for multi-tenancy.

About Barracuda Networks

Barracuda (NYSE: CUDA) simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications and data regardless of where they reside. These powerful, easy-to-use and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

Barracuda Networks Inc.
3175 S. Winchester Boulevard
Campbell, CA 95008
United States

t: 1-408-342-5400
1-888-268-4772 (US & Canada)
e: info@barracuda.com
w: barracuda.com