ARTICLE

Dropsuite

6 Critical Questions MSPs Should Ask About Spear Phishing Attacks

A spear phishing attack is one of the most effective phishing techniques. Businesses, especially MSPs, need to be extra vigilant about this kind of phishing – because when it succeeds, it can be devastating.

Spear phishers often target MSPs, since they often handle hundreds of clients at any given time. Get access to an MSP, and you get access to a whole cluster of victims. Surveys reflect MSP and IT staff spending hours responding to email-borne threats, cutting down productivity and efficiency.

The victims of spear phishing attacks are numerous – from tech giants to government agencies and authorities. Spear phishers have managed to infiltrate some of the most recognized brands throughout the years – Google, Facebook, Twitter, and more.

It can be very hard to distinguish a spear phishing email from a harmless email, but there are tell-tale signs that you can learn to spot. The most important thing is for businesses like MSPs to be vigilant and train their employees on the ways to spot a spear phishing attack. Some of the best techniques to mitigate the threat of spear phishing scams is to always think before clicking links; implement exercises and drills that simulate spear phishing attempts; and deploy a 'safety net' through backup and archiving solutions.

What Is a Spear Phishing Attack?

Spear phishing is a targeted phishing campaign or attack.

Both regular and spear phishing rely on impersonation and are often done to steal either money or sensitive information, but the main difference between phishing and spear phishing is that the former relies more on numbers and will send out numerous email blasts to see if anyone takes the bait, while the latter is more meticulous. Spear phishing is often:

1. **Low volume** – Targeting only a specific individual / particular group of people.
2. **Highly personalized** – Actors research their target for months on end to build a profile and craft a believable email
3. **Payload-less / zero-payload** – Not to be confused with zero-day attacks, in this situation, the hacker doesn't need a malicious payload (malware, ransomware, trojans, etc.) embedded in their email. All they need are carefully chosen words and cues to convince the victim to transfer money into a spoofed account owned by the bad actor or have them send sensitive files into a depository that the bad actor controls.

A 2022 report reveals that 79% of organizations experienced whaling and spear phishing attacks in 2021 – 20% higher than 2020. 37% of these organizations saw 11-50 attacks within the year.

Spear phishing attacks are potentially the deadliest and the most effective. They often target C-level executives or mid-level employees who have access to sensitive credentials, financial systems such as cash accounts or payroll systems, or other company financial software tools.

Attackers impersonate a senior executive at the company, either asking the employee to wire money, pay a fake vendor, or send employee or client information. Commonly, the requests from the cybercriminal will leverage urgency or even thinly veiled threats against the employee victim.

When a spear phishing attack succeeds, stolen usernames and passwords can be further used to compromise email systems or breach other software tools and financial systems.

Why Are MSPs Under Threat?

MSPs are like candy stores for bad actors. They have control of terabytes of data from tens, hundreds, maybe even thousands of customers. Successfully pulling off a spear phishing attack on an MSP can grant threat groups access to massive amounts of sensitive data, or allow them to steal thousands, even millions of dollars' worth of data.

IT and MSP staff members are constantly being inundated with phishing attacks, so it's easier for bad actors to slip through due to sheer volume.

In most organizations, employees are trained to forward suspected attacks to an email alias for analysis by professionals. In practice, these emails require tedious, one-by-one scrutiny and research, and it often takes a long time to even locate where the issue stemmed, much less solve it.

Avanan reports that, on average, each email forwarded to the Security Operations Center (SOC) takes 7.7 minutes for analysis and action. With the volume of email-borne attacks, the amount of time spent responding to these incidents can grow exponentially, especially if IT or MSP staff are overburdened. The company also found that 22.9% of SOC time is spent responding to email-borne threats.

In addition to investigation tasks, SOC staff will often have to perform additional prevention tasks such as updating block and allow lists, changing mail-flow rules, and fine-tuning sensitivity and confidence settings.

How Has Spear Phishing Evolved Throughout the Years?

To understand how spear phishing scams evolved into what they are now, let's travel back in time and look at how hackers evolved this modern thievery and espionage.

While the regular type of phishing itself has been around since the 90s, spear phishing and its targeted form of attack is more recent.

The first recognized cases of spear phishing occurred in 2010. Researchers noticed that mass phishing declined between 2010-2011, with spam messages going from 300 billion a day to 40 billion.

The reason was simple: by this time, hackers had discovered the benefits of fewer but more targeted emails:

- These had a 70% success rate, leagues higher than the 3% average of spam emails.
- These were proven to have 10x the ROI of regular phishing campaigns.

Between 2010 and 2011, these now-dubbed 'spear phishing campaigns' had grown by 300%. This new attack method made the news in 2011 when it was discovered that an attack was happening at RSA Security, the security division owned by Dell EMC, a multinational corporation selling data storage, information security, virtualization, analytics, and cloud computing solutions.

The attack was directed at only four people in the company. Another security company that investigated the incident discovered that one of the employees, under the behest of a convincingly legitimate email, downloaded a carefully crafted spreadsheet that served as a Trojan horse. This Trojan allowed the hackers access to the company's network by leveraging a zero-day flaw in Adobe Flash.

The result? Administration credentials and sensitive info from the company's Secure-ID customers like Northrop Grumman and Lockheed Martin were stolen.

What Are the Most Notable Spear Phishing Cases?

Here are some of the most notorious cases of spear phishing attacks that have occurred over the past decade:

2007-2013

- Various diplomatic, scientific, and government research departments had become spear phishing targets in a cyber-espionage-type incident that dated as far back as May 2007.
- Dubbed the 'Red October' campaign, hackers utilized the malware Rocra to steal various credentials, as well as intelligence and classified information. Victims were infected by a Trojan that came with the malware, sent through deceivingly convincing spear phishing emails.

2013-2015

- valdas Rimasauskas, a Lithuanian national, pled guilty to wire fraud from his orchestration of a business email compromise (BEC) scheme that targeted the employees of two US-based tech giants, Google and Facebook, to wire a total of over $100 million to bank accounts he controlled. He was sentenced to 30 years in prison in 2019.

2016

- valdas Rimasauskas, a Lithuanian national, pled guilty to wire fraud from his orchestration of a business email compromise (BEC) scheme that targeted the employees of two US-based tech giants, Google and Facebook, to wire a total of over $100 million to bank accounts he controlled. He was sentenced to 30 years in prison in 2019.

FACC, an aerospace parts producer from Austria, became the victim of a €42M spear-phishing attack. Hackers had posed as the company's CEO and sent a hoax email, asking an employee to transfer money to an account connected to a fake acquisition project. Because of this incident, the company's supervisory board decided to fire their CEO, citing that he had "severely violated his duties," which led to the incident. About a month later, the company fired their chief financial officer as well.

2020

Social media giant Twitter reported that their staff were spear-phished into giving up account credentials, allowing hackers to access celebrity accounts and steal about $100,000 worth of Bitcoin from their followers.

According to the company's own post:

> *"By obtaining employee credentials, they were able to target specific employees who had access to our account support tools. They then targeted **130 Twitter accounts – Tweeting from 45, accessing the DM inbox of 36, and downloading the Twitter Data of 7.**"*

2020

Microsoft discovered a large-scale spear phishing campaign conducted by NOBELIUM, the Russian advanced persistent threat (APT) group behind the SolarWinds Orion supply chain attack. The attackers gained access to the Constant Contact account of the US Agency for International Development (USAID) and delivered spear phishing messages under the guise of a USAID Special Alert. The messages claimed that former President Donald Trump "has published new documents on election fraud", and when the victims clicked on the link, the victims were directed to a site where a malicious ISO file – an exact copy of an entire optical disk such as a CD, DVD, or Blu-ray archived into a single file – was downloaded into their computer. Once deployed, the payloads allowed persistent access to the compromised systems.

Merseyrail, a UK rail network that handles train service for stations in England's Liverpool City Region, became a victim of an unusual cyberattack. The attackers stole data and infected systems with Lockbit ransomware, which caused a massive service outage. The actors also took control of the company's email system and – posing as Merseyrail's Director – emailed employees and journalists about what happened, going so far as to send screenshots of the data that was allegedly stolen from the company.

The Microsoft Threat Intelligence Center (MSTIC) discovered that Russian hacking group Gamaredon (aka ACTINIUM) had been sending spear-phishing emails against the Ukrainian government, NGOs, and other entities. MSTIC researchers said:

> *"**Since October 2021**, ACTINIUM has targeted or compromised accounts at organizations critical to emergency response and ensuring the security of Ukrainian territory, as well as organizations that would be involved in coordinating the distribution of international and humanitarian aid to Ukraine in a crisis."*

How Can We Identify Spear Phishing?

There are three main variants of targeted phishing campaigns:

1. Whaling: A spear phishing attack that is aimed at an especially valuable target such as a CEO, important political figure, or extremely high value security credentials.
2. Business Email Compromise: Similar to a whaling attack but aimed at a less high-profile victim. For example, sending emails to an accountant to try to convince them to transfer funds for a fake business transaction.
3. CEO Fraud: A BEC where fake CEO emails demand that finance transfer funds immediately to a fake account for a supposed merger or payment for a vendor.

A spear phishing attack's success hinges on three key things:

- The email must appear to come from a known and trusted individual.
- There is information within the message that supports its validity.
- The request, made by the individual, seems to have a logical basis (e.g. processing a payment for a vendor).

There are certain lines or qualities that are typical of a spear phishing attempt. Here are some of them:

A. "**...Too busy to talk**" – The person that sent the email will say they are either too busy to talk or stuck in a meeting and will sometimes add that they'll "only be available by email."

B. "**...Need money fast**" – The sender will request payments or wire transfers immediately – there is an urgency to the email.

C. “**Are you at your desk?**” or “**Got a moment?**” – This is typically followed by an urgent request for a wire transfer, file transfer, or a request to purchase gift cards.

D. Subtle errors in the email addresses – The attacker will register a similar domain name to the targeted organization but with an additional or wrong letter or number (e.g. sender@dropswite.com)

E. Gmail- or Hotmail-based addresses – Be wary of emails sent from Gmail, Hotmail or other free email domains, especially if your company is supposed to use a separate domain for your company emails.

F. Language and conversation cues that sound ‘off’ – If the words or language used in the email does not look like what the person used to write with, it could be a sign of a fraudulent email. (e.g. starting with “Hello, James” when they usually just say “James”)

G. Sender replies with a different email address – When reading the email, the sender address appears to be the expected company address; however, upon replying, a different email address shows up in the To: field.

How Can Businesses Defend Against Spear Phishing Attacks?

For MSPs and their customers, there is hope yet to prevent spear phishing attacks or, at the very least, make it more difficult for bad actors to execute an attack.

1. **Limit sharing information on social media and other websites**. In this day and age, oversharing and posting almost everything in social media is not advisable.
2. **Do not click on links in emails immediately**. Identify suspicious links first by hovering the cursor over the link. If the URL does not match the link’s anchor text and the email’s stated destination, you might be getting spear phished.
3. **For sensitive requests like wire transfers, ALWAYS try to contact the sender of the message**, preferably with a separate communications channel, and confirm the request.
4. **Use analytics software to assess the company’s inbound email history**, at least 12 months of it. Inspect email content, track suspicious email traffic to specific users or user areas, and assess user behavior. Such historical data can reveal security gaps and give insights on how to improve security.
5. **Train your employees and executives on identification and proper response against spear phishing attempts**. Security awareness training for employees and executives can help reduce the likelihood of a user falling for spear phishing scams. Make it part of the protocol to always report suspicious emails to the IT team.
6. **Perform exercises that simulate spear phishing attacks**. This way, employees can practice their threat detection skills in the normal course of a workday. Security teams can measure the effectiveness of training based on the results of these tests.
7. **If possible, have an outsourced, trusted security provider perform an outside audit**. This will also expose any holes in the business’ security and employee security behavior so that vulnerabilities can be remedied.
8. **Deploy and enable security software and solutions**, such as spam filters, antivirus software, and other advanced threat protection and security software. Keep them patched and up to date, as well.
9. **Enable an automated email backup and archiving system**. This will ensure that your emails remain secure from data loss due to accidental deletions, ransomware attacks, or spear phishing attempts. Your email archive can also serve as evidence, especially during a spear phishing attack investigation, which ensures a faster recovery and resolution.

MSPs need to think in terms of layers of defense to battle against a wide variety of cyber security challenges. With spear-phishing, protection starts with backing up your email and prevention starts with employee training and robust email security technologies and extends to additional levels of protection.

At Dropsuite, we arm MSPs with a cloud software platform to easily backup, recover and protect their important business information. We help form the first and last line of defense against hackers, phishers, and other cyber criminals.

CONTACT US

For more information, please contact us:
www.dropsuite.com | sales@dropsuite.com