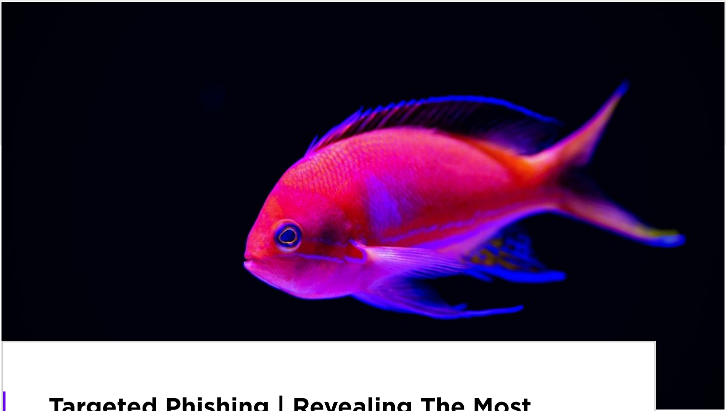
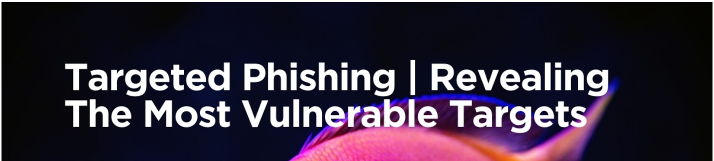


Targeted Phishing | Revealing The Most Vulnerable Targets

June 27, 2019
by SentinelOne

Phishing and spearphishing remain the two most widely used vectors for network security breaches, business email compromises and other enterprise security issues. With the number of reported email phishing attacks up for the third quarter in a row, the problem is only increasing as attackers from APTs to unsophisticated buyers of ransomware-as-a-service on the DarkNet understand that the weakest link in every security solution ever-devised is always the human element.

Understanding why phishing attacks work and which people and departments are most vulnerable is an important part of developing your security posture. In this post we'll take a tour of phishing techniques, vulnerable targets and organizational impacts to help you better prepare for the assault on your network, staff and business.



SentinelOne

What Are The Business Impacts of Phishing Attacks?

As the councils of Lake City and Riviera Beach recently found out, the impact of staff that fall for a phishing link can be immediate and costly. Lake City handed hackers $460,000 to regain control of their email and servers in the same week that Riviera Beach reportedly stumped up $600,000 to recover from a similar ransomware attack. It appears that in both cases the criminals used social engineering to convince employees to click an email link which then downloaded malware to the victim's device.

According to data collected by Proofpoint's State of the Phish 2019 report, over the last year, 65% of phishing attacks resulted in credential theft or a business email compromise, nearly 50% led to malware infections and almost a quarter to loss of business data.

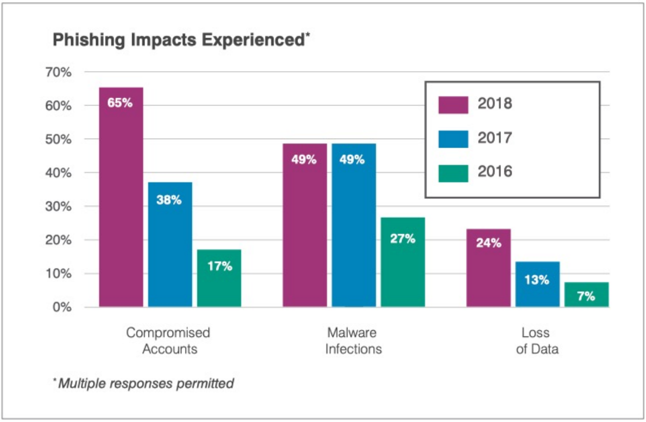


Image courtesy of Proofpoint

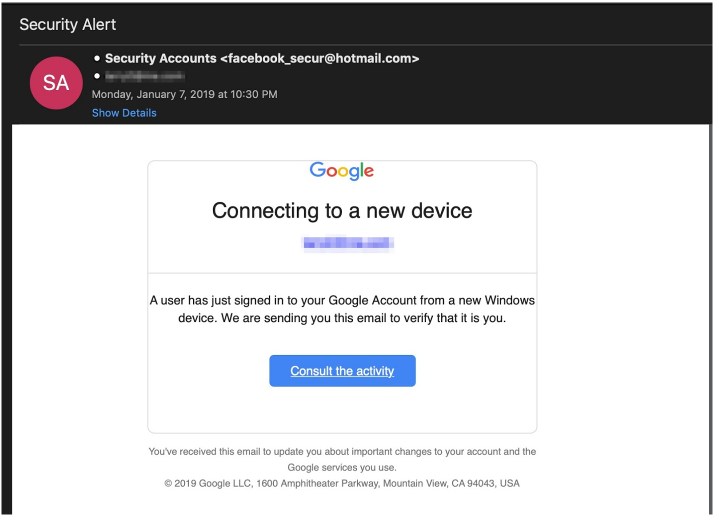
The impacts on a business after falling victim to an attack can be devastating. Aside from outright financial loss such as in a ransomware attack, there are other impacts to consider. For example, in the ransomware attacks on Atlanta, Baltimore, Greenville, Riviera Beach, Lake City and many others, there were huges losses in terms of productivity. Businesses may also likely suffer damage to their reputation if they do not report an attack but it later comes to light due to its affect on customers or services, or if they report it in a non-transparent way. The recent case of an attack on Coinbase is a good example of transparent reporting in which the business not only "saved face" but increased its reputation due to timely and responsible reporting.

In the case of a business email compromise, or so-called "man-in-the-email" attack, the organization may suffer both financial loss through fraudulent wire transfers or other transactions as well as data and IP loss through the transfer of confidential information to unauthorized parties.

There are also impacts on internal teams to consider. Being the victim of a successful phishing attack places extra burden on the organization’s IT and SOC teams and could also cause frustration among other employees impacted by the attack.

What Phishing Techniques Should I Look Out For?

The majority of phishing attacks occur through emails, and often purport to come from a legitimate organization and/or use the name of a person the recipient is familiar with such as this one:



Security Alert

SA

- **Security Accounts <facebook_secur@hotmail.com>**
- [redacted]

Monday, January 7, 2019 at 10:30 PM

Show Details

Google

Connecting to a new device

[redacted]

A user has just signed in to your Google Account from a new Windows device. We are sending you this email to verify that it is you.

Consult the activity

You've received this email to update you about important changes to your account and the Google services you use.

© 2019 Google LLC, 1600 Amphitheater Parkway, Mountain View, CA 94043, USA

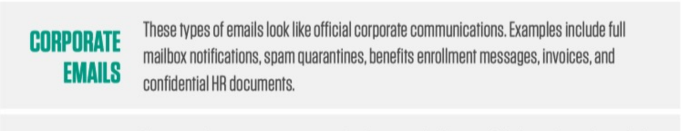
However, email is not the only means by which attackers attempt to social engineer targets. There’s also “smishing” – attempts to phish through SMS messages – and “vishing” – phone or voice message frauds that attempt to trick unsuspecting users.

Whether it’s by email, SMS, or voice, the name of the game is generally to manipulate vulnerable targets into one of three kinds of behavior: clicking a fraudulent link, opening a malicious attachment or entering data into a booby-trapped capture field, such as a fake login page on (what appears to be) a corporate website.

Cybercriminals continue to register around 20 fake domains for every single business targeted. The aim is to secure domain names that are close enough to the real one so that users could easily be fooled into navigating to the clone of a corporate website. When the real *mycompany.com* is cloned and registered as *mycornpany.com* or *mycompany.co*, it’s easy for unwary users to fall victim. On top of that, browser tricks that can mask or hide the real address of a site a user lands on are also known.

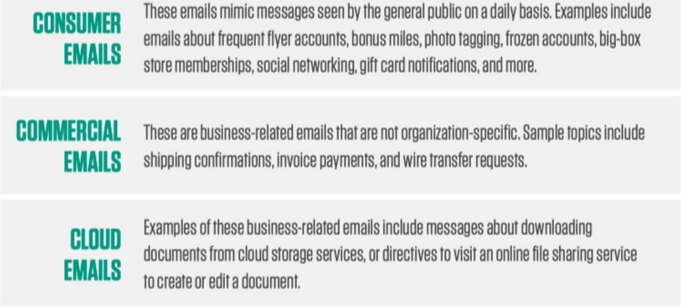
Macro and DDE malware hiding in attached documents have been well-documented, but continue to enjoy lasting success. On top of that, researchers have shown that it’s even possible for attackers to edit Youtube videos embedded in documents so that the video link redirects the unsuspecting user to a malicious site or delivers a malware payload.

In order to achieve their goals, cybercriminals are using a range of delivery techniques to scam business employees. These include targeted and generic business emails that request invoices to be paid, invite employees to sign-in to a cloud-base services in order to download or edit an online document, or threaten that an account or service will be suspended unless immediate action is taken.



CORPORATE EMAILS

These types of emails look like official corporate communications. Examples include full mailbox notifications, spam quarantines, benefits enrollment messages, invoices, and confidential HR documents.



CONSUMER EMAILS	These emails mimic messages seen by the general public on a daily basis. Examples include emails about frequent flyer accounts, bonus miles, photo tagging, frozen accounts, big-box store memberships, social networking, gift card notifications, and more.
COMMERCIAL EMAILS	These are business-related emails that are not organization-specific. Sample topics include shipping confirmations, invoice payments, and wire transfer requests.
CLOUD EMAILS	Examples of these business-related emails include messages about downloading documents from cloud storage services, or directives to visit an online file sharing service to create or edit a document.

Image courtesy of Proofpoint

Email subject lines to look out for include anything that might be "Urgent" or "Required", whether it's changing a password to paying a bill or cancelling a fake credit card charge.

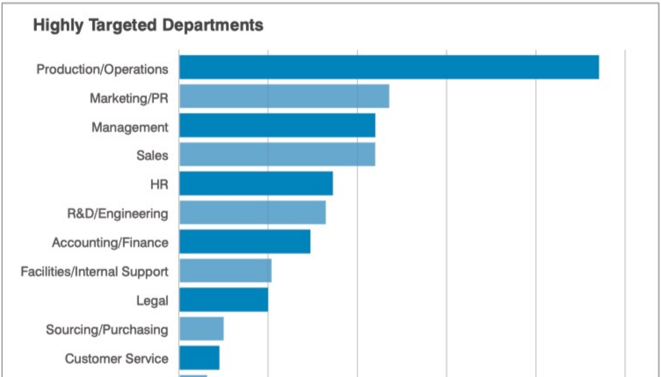
Who Is Being Targeted by Phishing Attacks?

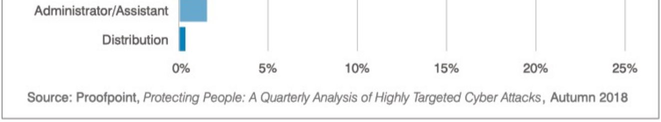
The short answer to that is: everybody! But in order to make better decisions about how to handle the threat and direct your phishing simulation and training activities, it's helpful to get into the sticky details. Who is the most vulnerable, and what kinds of attacks do they fall for?

Cybercriminals target specific job functions and departments in different industries, relevant to their goals. For example, ransomware attackers are more likely to focus on phishing campaigns that target HR inboxes as these commonly receive large amounts of legitimate attachments. For that reason, HR staff habitually open attachments in order to get their work done, so slipping in a malicious PDF or Word.doc obviously has greater chance of success there as opposed to an inbox that does not regularly receive attached documents.

On the other hand, a malicious link sent to Marketing staff who are used to following news and trends across social media may have greater chance of success than file attachments. Credential phishing attacks which convince senior staff to enter login details to a fake form or website are more likely to reap greater rewards if targeted towards VPs and Directors.

In Proofpoint's report, the most targeted departments were Production/Operations, seeing some nearly 25% of all attacks, with Marketing, Management and Sales departments receiving approximately the same volume, around 10-12%, of phishing email.





Source: Proofpoint, *Protecting People: A Quarterly Analysis of Highly Targeted Cyber Attacks*, Autumn 2018

Image courtesy of Proofpoint

What Can I Do To Protect Against Phishing Attacks?

Evidence suggests that active training such as running simulated phishing campaigns has a measurable impact on reducing the success rate of phishing attempts but training needs to be continuous. The phishing landscape does not stand still, and staff churn is likely to mean that there will always be a portion of your workforce that is not up to speed with the training programs that you have previously offered.

There are a number of resources you can use if you don't already have your own training programs in place, from the simple but useful tests like Jigsaw's Phishing Quiz to more convincing simulations provided by companies such as Proofpoint and KnowB4.

On top of training, be sure that you have good security solution like SentinelOne that can autonomously block code execution from phishing attacks – whether that is a malicious attachment or fileless malware executing in memory – and that can inspect encrypted traffic and enforce firewall control to block known phishing domains.

Conclusion

Understanding who, how and what is involved in phishing attacks is vital to an organization if it is to effectively manage the threat. Knowing which people and departments in your organization are most targeted, under what circumstances and with what techniques can help your infosec team to be able to better detect and respond to attacks.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- What Is Threat Hunting? (And Is It Really Necessary?)
- Our Take: SentinelOne's 2022 MITRE ATT&CK Evaluation Results
- Feature Spotlight | Combating Email Threats Through AI-Driven Defenses with Armorblox Integration
- Why Your Operating System Isn't Your Cybersecurity Friend
- SentinelOne's Cybersecurity Predictions 2022: What's Next?
- 12 Months of Fighting Cybercrime & Defending Enterprises | SentinelLabs 2021 Review

©2022 SentinelOne, All Rights Reserved.