WHITEPAPER

Redmond MAGAZINE

EMAIL SECURITY: IT'S TIME TO SHUT THE FRONT DOOR

By Nick Cavalancia

mimecast®
unified email management

www.mimecast.com

As much as we work to secure our network with firewalls, patching, and vulnerability assessments, it's undeniable that there's one pathway into your network you're never truly going to block – email. It's a conduit for carrying some of the nastiest attacks onto your network, often acting as the very vehicle that gives initial access to some of your most sensitive systems and data. Email is somewhat unique in that it's the only medium whereby literally anyone in the entire world can walk right into your environment – if they have your email address, they can send you an email.

EMAIL: THE FRONT DOOR IS OPEN

Historically, email has been one of the easiest ways to introduce malicious code, as users are the one known vulnerability you can't patch. At a minimum, you're looking for the users themselves to act as a security guard when they are usually the least security-minded. Users receive countless emails daily and should a message appear to be legitimately related to their job, their mindset is focused on work, not security.

With such a minimal security stance, malicious attackers send in everything from emails with links to malware-laden websites, to malicious attachments, to seemingly benign Word documents. The intent is to gain a foothold within your organization (in the form of a compromised endpoint) serving as the base camp to continue their malicious actions – which usually include exfiltration of data, data destruction, or holding data for ransom.[1]

In recent months, the threat has evolved into something much worse to where email no longer is necessarily used as a delivery mechanism (as in the case of an email containing a malicious attachment). In most recent iterations of malicious email activity, email is only needed as a communications mechanism to deliver a message purporting to be from someone within the company (we'll talk more about that later) by someone with malicious intent.

And, given that email, by definition is a communications mechanism, should malicious actions only require delivery of a message without the need for opening an attachment or clicking a link, these new types of "malware-less" threats are even more dangerous.

Despite the varying and evolving methods of attack, IT is still charged with keeping these evils at bay. So how can you ensure you're protecting the "front door" to your network – all while the evils are constantly changing?

In this whitepaper, we'll take a look at the current state and evolution of email-based attacks, and look at methods of protecting your organization against this ever-changing threat.

THE CURRENT STATE OF EMAIL THREATS: IT'S WORSE THAN YOU THINK

Nearly every organization is under attack. Some are the opportunistic prey of a simple phishing email, while others are the specific target of an organized company whose interest is the business of inserting malware and stealing data. And if you think your company is exempt, think again.

In a recent Ponemon study of the state of endpoint security[1], a set of eye-opening numbers revealed the reality of attacks. When asked whether attacks of varying types had been experienced within the last 12 months, 55% had experienced a spear phishing attack – a value higher than the average of the previous four years. Other attack methods experienced over the previous 12 months included web-borne malware (80%), advanced persistent threats (65%), rootkits (65%), and spyware (35%). All of these other attack methods have one thing in common – the initial injection often (and in some cases solely) originates from phishing and spear-phishing attacks.

EVOLUTION OF THE BATTLE

It started with spam and viruses, and moved to phishing and spear-phishing. Spear-phishing emails containing links to malware-laden websites as a tactic has actually started to decline in favor of attacks that have attachments. Executables, PDFs, even script files – anything that can work to establish a connection to a malicious website and pull down a custom piece of malware. Spear phishing emails receive a 23% open rate, and an attachment click rate of 11%, generating a 90% chance of infection by sending just 10 spear-phishing emails[2]!

Macro-based attacks are making a comeback because attackers can socially-engineer the user (by pretending to be someone within the company or a vendor) to download the document and open it. In addition, macro-based attacks are difficult to detect because there are ways to obfuscate the code within a macro, making them a desirable method. But, as expected, attackers are beginning to move past the use of attachments, and looking at attacks that don't require a single click of a link or attachment.

SPEAR PHISHING EMAILS RECEIVE A **23% OPEN RATE**, AND AN ATTACHMENT **CLICK RATE OF 11%**, GENERATING A 90% CHANCE OF INFECTION!

GOING MALWARE-LESS WITH WHALING

Attackers desired to find a way to extract money from your organization in a way that doesn't require a link or attachment. And whaling was born. With whaling, attackers start by doing a lot of research on your company and employees, building out a reporting structure, listing its vendors, etc.

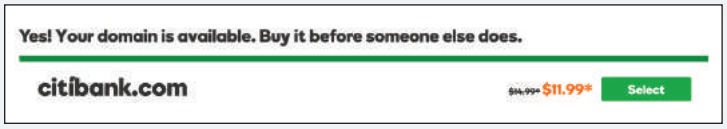
[1] Ponemon, State of the Endpoint Report (2015)
[2] Verizon, Data Breach Investigations Report (2015)

Helpful tools like LinkedIn, data.com, and other legitimate business services can be used to paint a very accurate picture of your company's internal structure. Attackers use this information to convince someone in the finance department to wire money to fraudulent accounts just by pretending to be the CEO or CFO.

Whaling emails are usually sent from seemingly-known individuals or entities using personal details to add credibility. (After all, figuring out that the CEO is in the Lesser Antilles on vacation is only a matter of monitoring their social media accounts, right?) Whaling emails use a domain that visually looks like the right domain, but is one that was only registered perhaps within the 48 hours prior to the whaling attack.

SPOTTING THE FAKE DOMAIN

One would think it's easy to spot a fake domain, after all something like "cit1bank.com" is pretty obvious, right? But, someone could use the citíbank.com domain when sending an email as the CEO to the CFO. Didn't notice the difference, did you? That second "i" in citibank is actually the letter "i" but with an acute accent instead of a dot. Technically, a different character, it makes obtaining a domain that looks very similar – so much that no one will notice – a pretty easy task.



Seems a bit implausible, doesn't it? You're probably thinking "Come on! Who falls for that?" But real companies just like yours fall victim. In 2015, Ubiquiti Networks disclosed a loss of nearly $47 million in a scam that involved whaling emails and fraudulent requests of the finance department.

ATTACKER ORGANIZATIONS PURCHASE EMAIL SECURITY VENDOR SOFTWARE – THE SAME ONE YOU'D BUY – AND REVERSE ENGINEER THEM TO FIGURE OUT WHAT CAN AND CAN'T BE DETECTED. IT'S SCARY STUFF THESE DAYS.

And, because the take can be this large, attackers have shifted from the shady-looking guy in the hoodie behind a single computer in a dark room, to a far more business-like approach. Actual companies exist today that offer Malware as a Service! Attacker organizations purchase email security vendor software – the same one you'd buy – and reverse engineer them to figure out what can and can't be detected. It's scary stuff these days.

So, how are you supposed to protect your organization against such intent and organized threats?

PROTECTING YOUR ORGANIZATION

Because of the evident ability for attackers to gain entrance and access to your network using an evolving set of methods, "shutting the front door"

Type of Attack	How they succeed	How a solution should protect against this attack
Malicious Links in email	These links point to websites that attempt to install malware via either tricking the user into downloading it, or by taking advantage of known browser vulnerabilities.	Every link in an email needs to be rewritten to point back to a secure gateway that first checks the link for malware before allowing the user to reach the intended destination. Some solutions claim methods of knowing which links are good or bad without URL rewriting. But, the most secure way is with a solution that assumes every link is "guilty until proven innocent."
Weaponized Attachments	Attachments can either be directly weaponized, such as with zero-day malware. Or the attachment can download malware as in the case of a macro inside a Word document the user has been social engineered to open.	Attachments need to be sandboxed, where the attachment is opened in a secure and closed environment, its running behavior observed, and a determination of whether or not it's safe is made. For example, if the attachment makes a call out to a suspicious website in some foreign country, it may be deemed unsafe and is not delivered to the user within the original email.
Malware-less	Also known as a business email compromise, or whaling attack, these attacks rely on nothing but social engineering; there's no link, no attachment, and nothing to download.	Because these emails try to appear to come from, say, the CEO, the right solution needs to be looking at a number of indicators within the message itself that include source domain names that look similar to yours, use of domains that were recently created, and use of specific combinations of words in the email itself, such as wire transfer, W-2s, IRS, etc. Adding all of these indicators together and it's possible for a solution to identify an email is suspicious.

involves a defense-in-depth strategy. Taking a coordinated, multi-layered approach to security, a defense-in-depth strategy involves the use of both technology and users to achieve the goal of stopping external attacks via email. Your layered defense should follow the path of an email that puts security solutions first in line to prevent an attack.

SECURITY THROUGH SOLUTIONS: YOUR FIRST LINE OF DEFENSE

Email-based threats are a constantly moving target. The sheer number of gambits played in an email – who it's from, what it's about, why the recipient needs to click a link or open an attachment, and what do those links and attachments represent to the recipient – it all adds up to more possibilities than any one user should need to be responsible for on their own.

The following table outlines the various attack methods discussed in this paper and the means of protecting the organization you should be looking for in a solution.

Given the constant evolution of the email-based attack, it still makes sense to include educating the user in your layered

approach as a last means of identifying an email of malicious intent.

USER EDUCATION: THE LAST LINE OF DEFENSE

Because attackers always rely on users being socially-engineered to open emails, click links, and run attachments, users need to be educated on the threats that exist, and the repercussions to the organization of a successful attack. Even the best email security solution may initially allow an email using the latest attack method to get through. So, users need to participate in the layered defense.

SHUTTING THE FRONT DOOR

Attackers are working tirelessly to come up with more effective ways to fool users (who are not coming to work every day thinking about and looking for suspicious emails) all in an effort to get your organization's most precious asset – its data. To properly close the security gap that exists within your email, you're going to need to implement a layered, defensive approach consisting of one or more continually-updated solutions that scrutinize messages for typical indicators of malicious intent. While user education is an important layer in your defense, keep in mind users are still going to click links, open attachments, and interact with senders that appear legitimate – making your reliance on the right technology the key to shutting the front door.

EVEN THE BEST EMAIL SECURITY SOLUTION MAY INITIALLY **ALLOW AN EMAIL** USING THE LATEST ATTACK METHOD **TO GET THROUGH.**

Now, remember, a user doesn't know what is and isn't a malicious email, and that definition is always changing anyway. So user education needs to focus on awareness that email attacks occur, and what users should do about it if they come across a suspicious email. Education needs to be engaging and relevant, so holding a quarterly update lunch-and-learn will likely be forgotten, and even bi-weekly emails from the security team with warnings will be overlooked. Focusing on creative ways such as a security awareness program with mugs, flyers, etc. over a period of time will help raise awareness and keep users a bit more vigilant.

Nick Cavalancia is founder & chief techvangelist at Techvangelism. Nick has 20 years of enterprise IT experience,
and is an accomplished consultant, speaker, trainer, writer, and columnist.
He has several certifications including MCSE, MCT, Master CNE and Master CNI. He has authored, co-authored and contributed to over a dozen books on Microsoft technologies.