BitLyft
Cybersecurity

HIDDEN THREATS AND ATTACKERS

How to prepare your organization to reveal, respond, and remediate in today's threat landscape

TABLE OF CONTENT

Introduction 2
Browser Injections 3
Adware 6
Using TOR 9
DDOS Attacks 13
Phishing 16
Ransomware 19
Compromised Accounts 22
Education Tips 24
Cybersecurity Toolbox 29

INTRODUCTION

The Internet has been a boon for productivity. Businesses and organizations are able to collect, monitor, and manage previously unimaginable amounts of information on their operations, their customers, their suppliers, and their stakeholders. The result is organizations are better able to manage customer relationships better, increase sales, streamline operations, automate processes, and cut costs. But what's happening under the surface?

As more and more systems come online and organizations realize the benefits of automation and integration, while at the same time the complexity of the "black box" of technology gets bigger and harder to understand to keep safe. Often times we're only focused on the output of technology (reports, sales, projections, relationships, etc) rather than how to keep it all safe from attackers.

If the Internet has been a boon for productivity, the proliferation of RESTful APIs and system integrations has been a welcome cherry on top. Instead of having to find - or rely on - a single provider who can meet all of our organizational needs, we have the ability to pick and choose the tools that work best for us and our stakeholders.

Let's imagine, for example, you need a place to store a repository of documents for collaboration. In the past, Sharepoint might have been your only option. Now, you can use cloud services such as Box, Dropbox, Google Drive, Github, iCloud...and the list goes on. For collaboration, you can use these tools, plus Slack, Hipchat, Gmail, and Zoom. But with the increase in tools and connections, comes an increase in potential "attack vectors," opportunities for malicious attackers to find their way into your system and exploit vulnerabilities. By exploiting vulnerabilities in web browsers, on-and-off premise infrastructure, and user behavior, the productivity boon has simultaneously yielded a boon to criminals seeking to exploit information for personal, political, or financial gain.

In this guide, we explore some of those vulnerabilities so that you can peer into your organization's black box and determine how best to protect your information, your stakeholders, and your organization.

BROWSER INJECTIONS

We all use the Internet every day to work, connect with friends, or watch cat videos. It is perhaps our most common touch point to the rest of the world. Because most of us trust our technology, our browsers, and ourselves, we aren't as vigilant (or aware) as we could be to the hidden threats we're exposed to everyday.

DRIVE-BY-DOWNLOADS

A "Drive-by-Download" begins when a legitimate website is injected with malicious code (often via JavaScript) or a user is redirected to an infected web page. An attacker, unbeknownst to the user, invokes a client-side (e.g., browser) vulnerability and delivers a payload (e.g., malware) to the user's machine.

This malware can be used for a variety of things from simply messing with the user's preferences to "watching" for credit card information to steal data - or worse. Oftentimes these vulnerabilities exist because users - either those hosting legitimate websites or those consuming the information - don't keep their software up to date.

For example, Wordpress has had a history of security vulnerabilities with different versions of the software. A website with outdated software may be the perfect target for drive-by- download attacks. Similarly if a user doesn't keep their browser up to date, they may be increasing their risk of exposure. For example, Chrome, IE, and Firefox had 1004 potential vulnerabilities in 2016 that may have exposed an unwitting user.

DELIVERY MECHANISM

Users can be exposed to “drive-by-downloads” in a variety of ways:

- Visiting an infected webpage
- Opening an infected email attachment
- Clicking an infected link

In many cases, attackers may try to make the email, link, or popup look legitimate: “Your computer has been infected, click “ok” to clean your system.” Trusting users then click the link or popup, inviting the malware to be installed on their computer, where it searches other applications it uses - or encounters online - for vulnerabilities. If that computer is connected to a network, malware can start to migrate through the network seeking out vulnerabilities on other machines (or the network proper).

WHAT ATTACKERS DO

Once an attacker has installed the relevant malware on a system, there are a lot of things they can do to harm. Here’s what happens when this exploit occurs:

- The user is exposed to a drive-by-download, often in seemingly innocuous ways.
- The payload (e.g., malware) is download to their machine
- The malware crawls the machine looking for outdated plugins, software, or extensions that it can use to take over the system. Or it just “watches” to find a bigger payoff opportunity like obtaining password or financial information
- The malware realizes the machine is networked to other machines and repeats the above on other machines.

A WORD ABOUT KEYLOGGING

One of the most common use cases for drive-by-download events is the use of keylogging for capturing data. In many cases, the malware is looking for input forms in a browser to know what to record or capture.

As a user fills out the form online, sensitive data is recorded and sent back to the attacker's server, often leaving little or no trace to the user. This kind of attack can be used not only to steal credit card information, but also FTP/SSH credentials or system login credentials. This could result in ransomware attack, where important information is locked down and ransomed until the ransom is paid - or worse.

HOW TO PREVENT THIS THREAT

The best way to prevent this threat is to make sure that all the software your organization uses stays updated and patched. As an IT professional, you probably do that with your core systems. But what about your company website? Or the browsers your employees are users? Do you have control over what extensions or plugins they're downloading and using? You want to make sure that you do.

Unfortunately, so much of prevention in this space relies on users being vigilant which, very often, they aren't. That's why a good user education and accountability program is absolutely necessary (more on that, later). The next best thing is to make sure that you've got great logging in place and a vigilant security operations team watching watching the system.

Drive-by-Download attacks can leave clues, such as aberrant behavior caused by bots running their software, that a good SIEM will catch and a good security team will recognize. That way, they can make adjustments while it's merely a security event and before it becomes an all-out security incident.

ADWARE

The Internet is awash with advertising. Companies like Google & Facebook earn billions of dollars a year serving ads. Blogging moms, news websites, YouTubers, and so many more are serving you ads every day. And all those ads pose a potential threat to users and, by extension, your organization.

WHAT IS ADWARE

At its most basic level, adware is just software that generates revenue for a developer by generating online advertisements. For example, Gmail is supported by adware. While you check your email, ads are served that Google thinks is relevant to you. So far, so good. The problem occurs when adware starts to become malware.

MALWARE VS ADWARE

Some malware functions like adware, serving ads to you in order to use a piece of software. Except, in many cases, malware installs itself without the knowledge or consent of the user. Often, malware presents unwanted advertisements to the user, forcing them to engage it to close the ad. You may have seen these kinds of ads before - they're the ones with the unclosable boxes that force you to close the browser tab, curse the dregs of society, and move on.

In other cases, it may track user activity and display ads in places where it shouldn't have access. Worse, sometimes this malware becomes spyware, and actually observes a user's behavior, before reporting it back to the software developer. At best, these things can be a mild nuisance. At worse, they expose a vector for attack.

MALVERTISING

One way this malware can be installed on a machine is by downloading infected software, perhaps from a seemingly legitimate mirror site or via TOR. In other instances, they can be installed via a Drive-by-Download event. In still others, they may be installed via completely innocuous activities like reading, say, the New York Times or listening to Spotify.

In these instances, the user doesn't click anything. They may not even interact with the ad directly. Enter the world of malvertising (malicious advertising).

With malvertising, malicious code is hidden inside an online (often display or popup) ad and, when your browser makes a request, the malicious payload is delivered alongside the other (legitimate) requests.

The malvertisement's code may register an iframe that navigates to another page, where malware is hosted. The malware then infects the user's system, looking for vulnerabilities. Finding them, it installs it's payload and the user's system is compromised.

IT'S NOT UNCOMMON FOR A SINGLE WEBPAGE TO MAKE DOZENS OF REQUESTS TO THIRD-PARTY APPLICATIONS, LIBRARIES, OR EVEN IFRAMES.

MALVERTISING OFTEN WORKS BECAUSE MALICIOUS CODE CAN BE HIDDEN IN ONE OF THESE KINDS OF REQUESTS.

HOW TO PREVENT THIS THREAT

1 First, make sure you have control over what kind of software the users in your organization are allowed to download. At the very least, consider limiting download authorization to a few people in your organization. When a user needs a new piece of software installed, have them file a ticket or request help from someone with the appropriate authority to download the software. Sure, your users will find that annoying. But, it's the best way to make sure they don't inadvertently download something that may contain adware.

2 Secondly, make sure you've got good protections in place, including virus protection, anti- exploit, and/or anti-malware software. At a minimum, install ad blockers on user browsers and install tools to scan downloads before they're downloaded. These practices reduce the vectors available for malicious advertising to take root.

3 Thirdly, make sure you provide your users with the proper education needed to understand the risks they - and the organization - are exposed to. Oftentimes, users are merely unaware of the threats that are out there. You want to make sure you educate them. You may not only save the organization, but also their personal data if they take some of those lessons to heart when they go home for the evening.

What makes malvertising-delivered malware so bad is its ability to infiltrate an organization so surreptitiously. While media providers are responsible for - and take action towards - preventing malvertisers on their network, they are hard to catch.

4 Finally, having a good SIEM that's mining system logs and monitored by a security operations team with expertise in deciphering events from incidents (and preventing the latter) will help to ensure that you catch threats before they become problems.

USING TOR

A common misconception on the web is that using the Tor browser can keep you safe from cyberthreats. That's not true. TOR was built for anonymity; not explicitly for security. It's important to understand the difference, if you want to protect your users and your organization.

WHAT IS TOR

Tor is software designed to enable anonymous communication. Pioneered by the United States Naval Research Laboratory in the 90s, it was designed to protect U.S. intelligence communications online. It was later taken over by DARPA and was subsequently made open-source and available to the public.

HOW TOR WORKS

Tor employs a practice called "onion routing" to anonymize communication over the network ("The Onion Router", hence Tor). Onion routing works by encapsulating messages in layers of encryptions, then transmitting the encrypted information through a series of nodes (called "onion routers").

At each node, a layer of encryption is peeled away, including information about the next node the packet is destined for. When the final layer is decrypted, the message arrives at it's destination. The sender remains anonymous because each node knows only the location of the immediately preceding and immediately following nodes. It doesn't know anything about who the sender is or what the encrypted message says.

TOR VULNERABILITIES

Because the messages sent are encrypted and the sender remains anonymous, many assume that Tor is inherently secure. In some ways, it is. After all, messages are encrypted and the content of the transmissions are obscured to each of the members of the network responsible for decrypting their layer and sending it forth to the next node.

> “Anonymity is not the same as security. And Tor, like all software, has vulnerabilities.”

Tor, when used properly, may offer some additional security over other browsers. But there are A LOT of caveats, even from the Tor Project itself. Some of these caveats include:

- Tor only protects applications that are properly configured to send their Internet traffic through Tor. They recommend using the Tor browser in order to protect privacy and anonymity, but don’t mention anything about security.
- Don’t torrent over Tor. File-sharing applications on Tor have notoriously ignored proxy settings and deanonymize your Tor torrent and your other Tor web traffic when you do.
- Don’t use browser plugins.
- Only visit HTTPS versions of websites
- Don’t open documents downloaded through Tor while online. DO NOT IGNORE THIS WARNING.
- Use a bridge relay rather than connecting directly to the public Tor network.

TOR EXIT NODE EAVESDROPPING

Exit nodes are the points in the network where an encrypted communication leaves the network for the target server. Attackers, identifying nodes (They're not hard to find), can monitor traffic coming off of the node and inject malicious code in presumably safe, encrypted transmissions.

In reality, this may not even be that hard to set up. In 2014, a group of Playstation hackers showed how easy it was to spin up nodes. Sure, Tor has gotten more secure since then, but hackers have gotten more sophisticated too. The point is that exit nodes are vulnerable. Moreover, much of the network is, in fact, hostile.

THE TOR COMMUNITY

Tor was initially conceived as a tool for U.S. intelligence services to communicate anonymously across the Internet. Other countries use it for the same purpose. And state-sponsored actors watch state-sponsored actors on the network.

On the Georgian Impact Podcast, one security expert went so far as to say:

"You should assume that when you're sending traffic in the Tor network, that there's somebody that's looking at it."

"...I can sit down and I can run a Tor exit node. I can offer to the Tor Foundation, like, 'Hey, I have, you know, a box of co-lo and I'd be happy to let you pump like 10 megabits per second of traffic through it. Here's what you need to hook me up. Go ahead and send some traffic.'

I can do that and I can get access to tens of thousands of people's network traffic that way. What I can't do is I can't call up Verizon and say, 'Hey, can you route customer x, y, z's Web browsing through my machine now?' I would have to break into Verizon to do that."

// GEORGIAN IMPACT PODCAST

While you may not be hiding state secrets, the reality is that there are several people on the network who have a vested interest in actively monitoring and trying to “hack” the network.

Additionally, it’s presumed that up to 57% of the active services on the Tor network belong to organizations carrying out illicit activity such as selling drugs, credit card information, violence-for-pay, or child pornography. It’s not called “the dark web” for nothing. Proceed with caution in this web territory, for you may come back with a virus.

Although the sender and messaging information propagated through the network is encrypted, there are ways to use what’s called “timing analysis” to monitor traffic, anticipate it’s flow through the network, and break the anonymity of the chain as it reaches an exit node.

There have been times when other weaknesses have exploited vulnerabilities in the Tor network. In many cases, attackers have been able to exploit weaknesses in the Tor architecture or an exit node to uncover IP addresses, decrypt messages, or hijack communications.

HOW TO PREVENT THIS THREAT

Use of the Tor browser and Tor network can expose uninformed users to malvertising, drive- by-download attacks, or worse. It is not, contrary to what some people think, a wholly secure experience.

In general, you likely don’t need anyone in your organization on the Tor network or using the Tor browser. So, don’t enable it. If, however, you do, then make sure they heed the Tor project’s warnings. Maybe separate them from your organization’s core network.

At the very least, you want to make sure you’ve got a high-quality SIEM backed by an actively engaged security operations team monitoring traffic in the hidden regions of your network, identifying aberrations, and responding to security events before they become incidents.

DDOS ATTACKS

Denial-of-Service (DoS) and, more commonly Distributed-Denial-of-Service (DDoS), attacks are among the most common cyber threats on the Internet. Recognizing how they work and preventing the threat can help to reduce the chance that a DoS attack is carried out against or with your organization.

WHAT IS A DoS ATTACK

The purpose of a Denial-of-Service attack is to shut down a machine or network, rendering it inaccessible or unusable to it's target users. This is accomplished by sending a flood of Internet traffic to a server, effectively overloading it. The server - incapable of processing the requests coming in at the rate they're arriving - stalls or crashes. The organizational result of a DoS attack is often lost time and money.

WHAT IS A DDoS ATTACK

In the old days of the Internet, it might be possible to flood a server with a single machine. A security monitor could recognize that all the traffic was coming from a single IP address and then move to block access.

Now, when an attacker wants to carry out a Denial-of-Service attack, they employ the help of thousands of machines to make it happen. When that happens, it's not just a Denial-of- Service attack, but rather a Distributed-Denial-of-Service attack. Because the attack is being distributed across a broad network of machines all homed in on one goal: overloading the target server. Most of the time, these machines are unwitting accomplices.

HOW THIS HAPPENS

A machine can become an unwitting accomplice to a DDoS attack if it's been infected with malware, perhaps from a Drive-by-Download or Malvertisement.

In these instances, the malware provides a vector for an attacker to take control of a machine and use it to create a botnet.
While the name sounds cool, the implication is not. These machines are taken over (effectively, "zombie-fied") and become part of the network of bots used to carry out the attacker's bidding.

It's a bit like the way Emperor Palpatine controlled the Galactic Senate and the entire clone army; each thought they were free, but, in reality, they were merely doing the bidding of the Sith lord.

APPLICATION LAYER ATTACKS

In this form of attack, bots are directed to a specific part of a web application, rather than the entire network. This can often be used as a deception; while security or network engineers are paying attention to the part of the network under attack, an attacker can slip through a 'back door' to the system and steal sensitive information.

ADVANCED PERSISTENT DOS

This occurs when the attack lasts for a protracted period of time (the longest (so far) being 38 days as part of a corporate feud (ostensibly). These are sophisticated attacks because the attacker may toggle attacks towards different parts of an application layer, while concentrating the thrust of effort on a single part of the system. They attack the middle and the flanks at the same time.

WHO ARE THE DDOS VICTIMS

While large companies are more likely direct targets, small and medium-sized organizations also make good targets for DDoS attacks, especially for those “script kiddies” trying to earn their stripes.

Many of these organizations have valuable data and either very small (or no security operations teams) available to monitor when they’re under attack. They also don’t have the sophistication to catch, for instance, when an attack is merely a diversion and the real threat is hidden, happening behind their back.

In other instances, employees at these companies, without proper employee training can become unwitting accomplices. Again, because these organizations don’t often have the sophistication to recognize or prevent against various security threats, their users get exposed to Malware that turns their machines into botnet zombies.

HOW TO PREVENT THIS THREAT

Look for unusually slow network performance, unavailability of the website, and inability to access a website. If any of these symptoms are occurring, check your server logs and review your net statistics (netstat -an). If you see thousands of IP addresses statused at TIME_WAIT, the server is likely timing out and crash is imminent.

By monitoring your logs, your SIEM can do some of this lifting for you and clue you into what’s happening quickly. If backed by a solid security operations team, you may be able to be back on your feet before any real damage is done. Similarly, DNS providers like Cloudflare can provide a layer of protection to prevent attacks or mitigate them when they’re underway.

Good security habits, combined with vigilant monitoring of your logs and responsive security protocols can go a long way in preventing an attack before it occurs.

PHISHING

We all should know by now that Nigerian princes don't need our saving through email campaigns. But what if it was an email that looked like it was from Gmail saying that someone had tried to login to your account and you needed to immediately change your password? The practice of phishing isn't gone. It's just evolving.

WHAT IS PHISHING

Phishing traditionally refers to the practice of sending out fraudulent emails in order to get an individual to reveal personal information, such as passwords or credit card information. Yet, as the Internet has evolved, so have attack vectors. Now, phishing can be done through phone, text, or even social media.

HOW DOES IT WORK

Now, phishing emails (or calls or texts) come as messages purporting to be from your bank or familiar company. Sometimes they come from a colleague who desperately needs you to open an attachment. Phishers take advantage of the trust garnered between people and institutions in order to exploit it. It's a practice called social engineering and exploitation.

Attackers mirror relationships you have in your life, then exploit them. Really savvy attackers will even go so far as to spoof a landing page that looks like the genuine thing in order to reinforce trust. For example, you click a link to reset your compromised Gmail password and are taken to a page that looks like Gmail. (In fact, this kind of congruent attack is getting even easier, with the prevalence of phishing kits.)

Depending on your browser and device, the actual URL may be hidden once the page loads. Even so, they often use 'similar sounding' URLs so that they overcome any skepticism the user might have.

Of course, there's always a form on the page and, as the user enters their information, keystrokes are recorded, information is recorded, and/or malware is loaded onto the user's system. Perhaps for later use in a DDoS attack.

Phishing works in large part by the law of averages. Cast large nets, get some people to respond. According to Phishing.org, there are over 100 Billion (yes, with a "B"!) phishing emails sent every day.

Users who fall prey to phishing attacks are not only at risk of having malware loaded onto their machine, but also compromising their friends and contacts whose information might also be on the machine. Attackers can then use this more specific information to carry out more targeted attacks.

With more specific information and more targeted attacks, phishers can make emails, texts, and messages seem that much more authentic, raising the trust quotient that much more, compounding the vicious cycle.

THERE ARE OVER 100 BILLION PHISHING EMAILS SENT EVERY DAY.

HOW TO PREVENT THIS THREAT

Naturally, you want to make sure you have your bases covered; use spam filters, set up user's browser to prevent fraudulent websites from opening, and force users to change passwords frequently. Ensure you have a firewall and that it's properly configured.

As with so many potential threats, one of the largest liabilities is your people. You have to make sure that you have a good user education program that helps individuals to recognize what phishing emails look like and how to discern legitimate emails/texts/calls from illegitmate ones. At the very least, circulate phishing.org's list of 10 ways to avoid phishing scams.

You may even want to check the database at isitphishing.ai to see what brands are most frequently represented in phishing attacks. You can also see, in real time, examples of phishing attacks the software is catching.

KnowBe4.com is another great resource for training, education, and company-wide user scoring.

IF A USER IS COMPROMISED

While preventative software can take you part of the way towards stopping successful phishing attacks, the reality is that users are often your most vulnerable attack vector.

In order to mitigate any potential liability, you want to make sure you've not only got preventive software, but good backend software to recognize if a threat has taken place. For example, a good SIEM can mine your logs to find aberrations in behavior, browser activity, or other indicators that a phishing attack may be underway or have occurred. If backed by a good security team, the appropriate measures can be taken quickly to prevent any real harm - or loss - from occurring to your organization, your employees, or your stakeholders.

RANSOMWARE

Having your files encrypted and held at ransom is now more common than it ever has been. According to Verizon Data Breach Investigations Report of 2021, there were close to 3,710 reported incidents of ransomware.

WHAT IS RANSOMWARE

Ransomware is a cyber threat where a malicious piece of software infiltrates a system and locks some - or all - of it until a ransom is paid. During the attack, users are unable to carry out tasks using the infected areas of the system. Typically, the ransom is a 'no-brainer' amount designed to get the target company to 'just pay up,' rather than drag out the attack. After all, a lot of people paying a nominal amount leads to a lot of money for the attacker.

WHAT IS SAMSAM RANSOMWARE

The SamSam Ransomware attack is a type of ransomware attack released in 2016 that targeted JBoss servers. Unlike other ransomware attacks, which might use phishing, or drive-by-downloads to infect machines and find vulnerabilities, SamSam used a remote desktop brute-force attack to guess passwords.

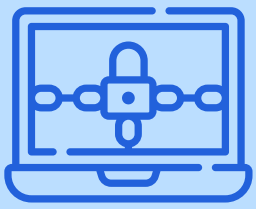
Once a password was identified, the malware made its way through the rest of the network, using brute force and sophisticated algorithms to guess the passwords of other machines. When the malware has enough of a toe-hold in the network, it encrypts the information on the network, effectively preventing legitimate users from being able to access their machines until a ransom is paid.

WARNING SIGNS OF RANSOMWARE

In the case of SamSam, the malware does its best to 'blend in' until the network is significantly compromised. After a machine is compromised, the virus may sit silently for a few days or even more.

Then, when the timing is right, the attackers download hacking tools onto the computers in an organization. For example, they loaded PSInfo and Mimikatz onto several machines to monitor information and steal passwords. Then go silent again. Until a few days later, when the encryption malware is loaded into the organization and executed across the organization. In the case of the Atlanta attack, two versions of SamSam were loaded on they system, in case one was detected by security software.

Unfortunately, this kind of 'random' activity can be difficult to track which is why it's important to have a great SIEM being monitored by a skilled security operations team working together to identify and catch these aberrant events before they become incidents.



RANSOMWARE, LIKE MANY OTHER KINDS OF ATTACKS, IS MADE EASIER WHEN LAX SECURITY CONTROLS ARE IN PLACE.

ENFORCE STRONG PASSWORDS, ROTATE PASSWORDS, USE TWO-FACTOR AUTHENTICATION, AND INVEST IN USER TRAINING TO MINIMIZE VULNERABILITIES.

HOW TO PREVENT THIS THREAT

Below is a list of suggestions to help prevent ransomware threats. Additionally, a SIEM tool, paired with an active security operations team can help to see and response to events in real time.

Audit your network for systems that use Remote Desktop Protocols (RDP) for remote communication and disabling.

Verify that all cloud-based virtual machine instances with public IPs have no open RDP ports, especially port 3389, unless there is a valid business reason to keep open RDP ports.

Secure any system with an open RDP port behind a firewall and require users to use a virtual private network (VPN) to access that system.

Enable strong passwords and account lockout policies to defend against brute force attacks.

Use and enforce two-factor authentication.

Maintain a good back-up and recovery strategy.

Enable logging and ensure that logging mechanisms capture RDP logins. Keep logs for a minimum of 90 days and review them regularly to detect intrusion attempts.

When creating cloud-based virtual machines, adhere to the cloud provider's best practices for remote access.

Ensure that third parties that require RDP access follow internal policies on remote access.

Minimize network exposure for all control system devices. Where possible, disable RDP on critical devices.

Regulate and limit external-to-internal RDP connections. When external access to internal resources is required, use secure methods such as VPNs. Of course, VPNs are only as secure as the connected devices.

Restrict users' ability (permissions) to install and run unwanted software applications.

Scan for and remove suspicious email attachments; ensure the scanned attachment is its "true file type"

Disable file and printer sharing services or require strong passwords or AD authentication.

COMPROMISED ACCOUNTS

So you've taken responsibility for ensuring you've educated your users about the potential ways in which they can be hacked. You've educated them about drive- by-downloads, adware, phishing, the dangers of tor, and ransomware. Everyone knows the threats. And yet, an account still gets compromised.

SPOTTING COMPROMISED ACCOUNTS

A compromised account is one that is accessed by a person not authorized to use the account. Typically, compromised accounts leave clues. This might include suspicious activity such as:

- Missing or deleted emails
- Bogus emails being sent from the account
- Unusual mail forwarding set up
- User information is changed
- Unusual credential changes

In many cases, users themselves may self-report the compromise when they start getting feedback from their own network about the 'bogus' activity. Here, it's good to have a liberal "if you see something, say something" policy. Better safe than sorry. Also, make sure to reward and encourage reporting, so people remain motivated to communicate. If employees are chastised or berated because they "invited" a threat, it may make other employees less willing to report suspicious activity.

If a user doesn't catch an account compromise, it's possible that you may see a rise in 'abuse' complaints from third parties about spam or suspicious behavior. Again, it's good to invite the information early and respond quickly.

Still, it's possible a user - or their contacts - may be unaware that their account is compromised. This might be especially true if the attacker is planning a patient, deliberate attack as in the case of the SamSam Ransomware attack, where the malicious code sat dormant for days or weeks at a time in order to elude security software.

While no security software is perfect, it can often play a critical role in identifying account compromise quickly. For example, a good SIEM with robust system monitoring and log analysis can clue you (or your security operations team) into a potential problem early, before the compromise propagates throughout the network.

PASSWORD COMPROMISE

Possibly as a result of phishing, possibly as a result of a hack on another site, or possibly through carelessness, a compromised password makes it easy for an attacker to infiltrate an account. Requiring strong passwords, enforcing frequent password changes, and using two-factor authentication can reduce instances of passwords being stolen.

MALWARE

If a user uses a machine that's been infected or been exposed to a machine that's been infected with malware (possibly through a drive-by-download attack), an account can become compromised. Using ad blockers, limiting download authority, and using virus protection software can help to prevent malware from being loaded on to user machines.

BRUTE FORCE ATTACKS

A brute force attack is one in which an attacker uses an automated script to "guess" a user's password. Often, there are algorithms that help to "sniff out" weak passwords and, if a user's password is ascertained, the account can be compromised. Minimize this risk by limiting login attempts over a given password, enforcing strong passwords, and logging all failed attempts. That way, if there is a trace of a brute force attack, your logs have information you can use to identify the threat and respond.

EDUCATING PEOPLE

While having the right tools is essential to securing your organization, we've seen that one of the largest attack vectors is your people. Providing a robust cybersecurity awareness and training program is an important component of any sincere effort to protect your organization from cybercrime.

THE PEOPLE PROBLEM

If you're in the world of IT/IS, it may be hard to imagine, but many of the people in the organization don't often think about cybersecurity or how systems and technology work.

They're more concerned with how to use it to get the job done, a need met, or a desire fulfilled. And, for most of them, they've experienced the rate of change in technology as one of conveniences and not one of malfeasance or risk. That's probably why, according to MediaPRO's State of Privacy & Security Awareness Report, 75% of professionals pose a moderate-to-severe risk to the security of their company's data. Heck, phishing attacks are credited as being responsible for as many as 91% of system breaches.

It should be stated from the outset, training your team will take time. What's often needed are behavior changes, not simply "information." How many of us, for instance, know that we should eat well and exercise, yet still don't make it a priority.

Habit change is hard. But, there are things an organization can do in order to build a culture of security and reinforce good cyber hygiene.

UNDERSTAND SCOPE OF THE THREAT

In order for behavior change to occur, people need to understand why the change matters. While a strong “why” isn’t sufficient for behavioral change, it is necessary that they have the appropriate information and context.

ADDRESS COMMON CULPRITS

As a matter of practicality, you want to make sure that your training addresses the most common threats that a user is likely to encounter, some of which include:

- Phishing
- Browser Injections • Adware
- Ransomware
- Social Engineering

Arming users with the vocabulary will help them become aware of the threats you likely think about all the time (and they’ve probably never heard of). Then, as you develop the rest of the training materials, you can make sure everybody is working from the same playbook.

USE ANECDOTES

People learn more from stories than PowerPoints, memos, or the like. As you prepare your training materials, make sure you have good stories and case studies available to help describe the impact of various threats. Unfortunately, it’s not hard to find the stories.

For example, if you’re teaching your people about SamSam Ransomware, share about the attack on Atlanta in 2018 that shut down large parts of the city. If you’re teaching about phishing, share an annotated example of a phishing email and maybe the story of how Jim Podesta fell victim.

MAKE IT CONCRETE

While anecdotes are great for creating sticky mental maps in the minds of your users, it's always possible to think "well, that could never happen here...".

Dispel these fallacies by making your training concrete. Draw analogies between what happened in the cases you're presenting and their work or department. For example, if you're training customer service reps who answer outside emails, make sure they understand the role they play in minimizing - or exposing - the organization to a cybersecurity risk.

KEEP IT SIMPLE

Most people don't speak "techie." When communicating your message(s), use simple language that the audience can relate to and comprehend. Good, concrete anecdotes will help with this. But remember, they don't need to understand all of the facets of cybersecurity. They only need to know what's necessary to fulfill their role-specific responsibility to keep the organization safe.

Similarly, your security policies and any artifacts that go out should be communicated simply and clearly. Instead of a detailed memo, for instance, you might consider an infographic. Instead of a policy manual, a set of videos on Vimeo. It's unlikely that users will read long, dense documents. But, clear, concise, engaging, relevant material? You bet.

TEST THEM

Remember when you were a kid and had to do fire drills? At some undisclosed time, the fire marshall would show up, an alarm would go off, and you'd practice lining up and marching outside in an orderly fashion.

Most of us never experienced a fire in school. But all of us were prepared. They say experience is often the best teacher and that may be true here as all. After the initial sessions, it can be helpful to do some drills and "put the organization to the test."

Because phishing is so prevalent, it may be helpful to mock up some phishing emails and circulate them throughout the organization. Then, measure the responses of who clicked, who forwarded, and who caught it.

Then, debrief the results with employees (and their supervisors). Use it as an opportunity for coaching, not punishment. Point out what clues the user might have caught and determine what they should do differently in the future.

Then, drill them again at some indeterminate point in the future. Did they do better? Mistakes are often the best teacher. You may also consider something like leaving an unmarked flash drive laying around in a public place. Monitor what happens to it. How long until it ends up being reported "up the chain?" Or, does someone take it and load it into their computer to "see what's on it?"

You know your organization and the ways in which there may be gaps; the point is to test those gaps consistently and with little warning, so that you can reinforce vigilance and good habits.

MAKE IS EASY TO COMMUNICATE

If a user suspects malicious activity, what should they do? Part of your cybersecurity plan should be a documented process that users learn to follow when they suspect something "phishy" (see what we did there?).

Because the front-line users have their own jobs (which don't involved thinking about cybersecurity 24/7), it's important that reporting dubious communication through the organization is easy and efficient. If someone has to reference a memo or a process map in order to communicate a potential threat, there's a good chance they won't.

Maybe there's a dedicated threat email address or Slack channel. Maybe they alert a supervisor, who ropes in IT. Whatever the process, make it quick and easy for the frontline user to communicate suspicious activity. Also, reward and encourage them when they do - even if it ends up being nothing. You want to incentivize people to be vigilant and reinforcing the desired behavior goes a long way in helping to do so.

MEASURE AND REPEAT

Cultivating habits takes mindfulness and repetition. It also takes measurement. If we don't know how we've done in the past, how can we know if we're getting better at reducing risks in the present? As you begin to build a culture of vigilance, report on the results of the drills you ran. How many phishing emails did you send out? How many were opened? Is that better or worse than last time?

Or, if timeliness of response is an important metric, how long did it take for the first user to report the suspicious activity? These kinds of measurements help you to know not only if you're improving, but also where the gaps are in your policies and response playbook. Use the information gathered (and questions raised) to iterate on your approach to cybersecurity.

Remember education it's a journey, not a destination. Building a culture of vigilant users, well-educated about the realistic threats they may face, and well-formed enough to carry out their responsibilities will take time and energy. It's also never done. Hackers will continue to devise new tactics and you will have to stay vigilant yourself. That way, your organization stands a fighting chance at minimizing the risk "people" play in inadvertently compromising the system.

REMINDER: NO SYSTEM IS PERFECT

Even with all the best technology and well-trained staff, no system is perfect. As a failsafe, you want to make sure that you've got good, secure infrastructure, including a SIEM monitoring system internals at all times, and a dedicated security operations team monitoring it to catch security events before they escalate into real problems.

CYBERSECURITY TOOLBOX

Vigilance, good processes, and user education are essential components of protecting your network. However, you also need the right set of tools to help protect, catch, and mitigate cyber threats. Below is a list of tools to consider adding or reinforcing in your stack to fend off threats.

FIREWALL

Firewalls have been around forever. In fact, if there's one security tool you likely have; it's this one. It's job is simple: prevent unauthorized access to your system. Firewalls work by monitoring network traffic and connection attempts through your network before determining whether to allow a packet can pass freely.

That said, firewalls have their limitations. They can't, for instance, catch malware that makes it's way onto your system because a user succumbed to a phishing attack.

Newer firewalls, however, are becoming more sophisticated. Many (dubbed "Next- Generation Firewall"s (NGFW)) offer deep packet inspection and application-level traffic inspection, in addition to intrusion prevention.

Still, the migration towards more cloud-based applications and integrations is pushing more firewall solutions into the cloud. For example, Barracuda has discontinued it's NGFW in favor of a cloud-based solution.

FIREWALL OPTIONS

There are a variety of popular firewall options for mid-to-large sized organizations. Some of these include:

Fortigate Next Generation Firewall - it boasts high threat-protection with automated visibility designed to stop attacks before they happen.

Cisco Adaptive Security Appliance (ASA) Software - Cisco has been a leader in building security devices for decades. Their firewall and security platform has more than 1 million deployments throughout the world.

ANTIVIRUS

Antivirus tools, like firewalls, have been around for a long time. These tools are designed to alert you to a virus or malware infection on a given machine, scan incoming email attachments and links to make sure they aren't infected, then quarantine viruses that they discover. In the event they find malware, they will remove them. There is no shortage of antivirus software out there. Some of the most popular include:

Avast Antivirus - More than antivirus, this software acts as a firewall, web shield, anti-spam filter, and more.

Bitdefender Endpoint Security - Bitdefender's widely recognized nextgen endpoint security protection platform features a suite of tools including anti-virus, ransomware protection, and more.

Kaspersky's Endpoint Security for Business Suite - Kaspersky's suite provides next-gen protection, automatic rollback (in the event of an attack), and an easy-to-use management consoles. All from one of the original companies in the cyber security industry.

PENETRATION TESTING

Some hackers are bad. Others are helpful. The helpful ones use a variety to tools to carry out what's known as penetration testing on a company's IT infrastructure. The goal of this testing is to identify vulnerabilities before the bad hackers do. Penetration tests are an essential component of the modern cybersecurity toolbox. You may choose to run penetration tests on:

Specific applications: Are the applications vulnerable to Cross Site Scripting? Injection Flaws? Weak Session Management? Something else?

The network: Are there configuration files improperly configured? Maybe with default or weak passwords?

IoT/Device penetration testing: Are there weak passwords or vulnerabilities in the APIs underlying your connected devices? Penetration testing should be a part of every cybersecurity arsenal and may involve a series of steps:

- Planning & Recon
- Vulnerability Analysis
- Exploitation
- Analysis
- Reporting

PENETRATION TESTING TOOLS

Penetration testing can be carried out with a variety of off-the-shelf and proprietary tools. Some of the more popular tools for penetration testing include:

Metasploit - According to their website, Metasploit is the most used penetration-testing framework. It's a collaboration of the open-source community and Rapid7 and boasts a large database of exploits available to put your organization to the test.

Nmap - A free, open-source tool designed for vulnerability scanning and network discovery, this tools is considered the de facto standard for port scanning and network mapping. It sends packets to system ports, listens for responses, and then determines whether the ports are open, closed, or filtered (e.g., via a firewall).

Wireshark - Another free and open-source packet analyzer, this tool is used for network analysis and troubleshooting. Their claim to fame is that it allows you to see what's happening on your network at a deep level.

PUBLIC KEY INFRASTRUCTURE (PKI)

You've probably seen the little padlock in the top of a browser bar when surfing the net. That "lock" means the connection to the server is encrypted, adding a layer of security that wouldn't be there, but for PKI technology. But while most are familiar with the public-facing aspect of PKI technology via the browser bar, the technology can also be used to encrypt connections on internal networks as well.

For instance, it can be used to enable multi-factor authentication and access control, encrypt email communication (mitigating phishing attempts), authenticating endpoints in an IoT environment, and more.

SECURITY INFORMATION EVENT MANAGEMENT

While preventative efforts, such as user education training and using some of the tools mentioned above are helpful, they often aren't enough. A good SIEM aggregates information from every layer of your security stack, including your firewall and system logs to identify discrepancies that may indicate a breach. If you're working with a managed SIEM, then when such a discrepancy is discovered, the logs are reviewed, false positives eliminated, and a game plan for moving forward put forth.

Your SIEM & SOC team serve as the brain of your cybersecurity operation; gathering information from the entirety of the system, parsing it, prioritizing it, and then directing action accordingly.

FINAL THOUGHTS

The threats are real. And they're not just limited to big companies or organizations either. Very often, attackers are using bots to troll the Internet for vulnerabilities. When the bot finds the vulnerability (or an employee engages with a malicious actor), then the attacker exploits that attack vector. So, how do you protect your organization from being attacked? Here are a few common sense tips.

INVEST IN USER EDUCATION

Your people represent one of the largest attack vectors - not because they want to bring the organization down, but because they don't know what they don't know.

Unlike you, your employees don't lie awake at night thinking about cybersecurity. Most of them are probably much more interested in Facebook than public key infrastructure. And while they may not fall for the "Nigerian prince" phishing email, they may fall victim to one that looks like a trusted colleague, vendor, or friend.

To mitigate against this threat, you want to invest in high quality cybersecurity education for your team. Make sure the curriculum is concrete, replete with good anecdotes, and be sure to follow up with good testing to make sure the concepts stuck.

UNDERSTAND THE THREATS

Many IT professionals started out in the industry doing things like network and system administration. While this provides them with a good understanding how the component parts of their networks fit together, many are less aware of the risks abounding on the Internet.

You should know about some of the more common threats, such as phishing, malvertising, and browser injections. You should also follow security experts like us and OWASP in order to stay up-to-date on the threats facing your organization.

PRACTICE GOOD USER ACCOUNT MANAGEMENT

While forcing users to use two-factor authentication or asking that they create unique passwords frequently can seem 'annoying' to users, good cyber hygiene is essential to reducing risk. With practices in place that require users to rotate passwords, VPN from outside the organization, and undergo compliance audits, even account compromises can be contained.

KEEP YOUR SOFTWARE UPDATED

Old software is fertile ground for attackers. Many attackers keep databases of software vulnerabilities, which they steer their malicious bots towards. As software companies identify their own vulnerabilities, they release patches to prevent exploitation. You want to make sure you have a process for routinely monitoring the state of your software and keeping it current.

KEEP BACKUPS

While keeping backups can't prevent attacks, they can help to reduce the impact should one occur. Importantly, you want your backups keep separate from your primary network, so that the backups aren't compromised if your network is.

SEGMENT YOUR NETWORK

Not all parts of your network are equally critical. But, an attack in one part of the network could harm another, more critical part of the network. A good practice is to thoughtfully segment your network and prevent interaction where its not necessary. A common, obvious example is using a 'guest' network for wifi connections for customers or vendors (or anyone who doesn't "need" to be on your core network).

Depending on your IT infrastructure, there may be other areas to segment your network. In this case, you'll want to make sure you double down on cybersecurity infrastructure for the most critical parts of your business infrastructure.

ESTABLISH A BYOD POLICY

We live in an age of the personal device. Most of us can no longer imagine life without our smartphones or tablets. Yet, when these devices are on your network, a compromise can pose a threat to other devices on the network. If you don't segment employee devices from your core network, you want to make sure you have a policy about how devices should be allowed to interact with your network. In some cases, that may mean limiting access, requiring the use of security certificates, or even disallowing devices altogether.

RETIRE OLD DEVICES & SERVICES

As your organization grows and your business IT needs shift, you may find that old devices become obsolete or superfluous. When that happens, retire them and remove them from the network. Not only is it less to manage, but it also reduces access points and attack vectors on the network.

TEST YOUR PEOPLE & YOUR PROCESSES

As you become aware of new threats, you want to update your user education plan and roll out the information in a systematic way. In a sense, your user education "plan" is really more of a "process:" it's never complete. As you roll out your education process, you want to make sure you're testing it's effectiveness consistently.

For example, are people following the incident report strategy? Are they being properly encouraged? Is IT getting back to them quickly when a concern is reported? You may want to identify an individual whose job is to become a cyber hygiene trainer and is accountable for this part of your operation as a whole.

ENCRYPT CRITICAL INFORMATION

In the event an attacker gains access to your IT infrastructure, you can reduce the risk of critical data loss by having it be encrypted in the first place. If your information is encrypted, then attackers won't be able to gain access to the content of the information without the keys. At the very least, your most sensitive, confidential information should be encrypted.

CYBER INSURANCE

It's impossible to mitigate 100% of the risk associated with cybercrime and data loss, even with the best people, processes, and technology. Standard insurance policies don't cover the loss of data in the event of a breach. If an attack happens, your organization could be held liable to third-parties and lawsuits could be fiscally ruinous. Having cyber insurance is an essential component of the modern organization.

MONITOR YOUR NETWORK(S)

You should know what devices are on your network at all times. You should also know how they typically interact with the network and be able to identify aberrant behavior. Your SIEM plays a vital role in this function. If unusual behavior is detected, make sure it's addressed swiftly and decisively.

The cybersecurity landscape is constantly changing; attackers develop new techniques as quickly as new protections and patches are developed. Because so much cybercrime happens in 'hidden spots' in the network - and between endpoints - threats often go unnoticed...until it's too late.

The Bitlyft cybersecurity team works with organizations to monitor their networks for unusual behavior and prevent threats before they happen. With their team of highly-trained cybersecurity experts, they may be able to help you keep your network safe from harm. Contact us today for a complimentary assessment of your IT infrastructure.