Protecting your business from cyberthreats in 2020

How to fight phishing, ransomware and other top attacks

Barracuda
Your journey, secured.

barracuda.com

Table of Contents

The Evolving Cyberthreat Landscape

Cybercriminals are launching more attacks than ever. They're also morphing their techniques; in 2019, they unleashed a variety of new types of attacks and used a range of new tactics to try to increase their success. From spear phishing and sextortion to account takeover and ransomware, cybercriminals continue to evolve the threat landscape in an ongoing attempt to outsmart more potential victims and further monetize their attacks.

As cybercriminals hone their approaches, attacks are becoming more targeted, sophisticated and costly. With spear-phishing attacks, for example, which are highly personalized, cybercriminals research their targets and craft carefully-designed messages, often impersonating a trusted colleague, website or business. Like other attacks, spear-phishing emails typically try to steal sensitive information, such as login credentials or financial information, which is then used to commit fraud, identity theft and other crimes. Cybercriminals also take advantage of social-engineering tactics in attacks, using urgency, brevity and pressure to increase the likelihood of success.

Costly attacks are skirting security

Many attacks are designed to evade traditional email security, including gateways and spam filters. Attacks are often sent from high-reputation domains or already-compromised email accounts and don't always include a malicious link or attachment. Since most traditional email-security techniques rely on blacklists and reputation analysis, these attacks get through. Attacks typically use spoofing techniques and sometimes include "zero-day" links, URLs hosted on domains that haven't been used in previous attacks or that have been inserted into hijacked legitimate websites; they are unlikely to be blocked by URL-protection technologies.

The costs and damages associated with attacks can be extreme. There are a wide range of financial impacts, including business interruption, reduced productivity, data loss, regulatory fines and brand damage. According to a recent FBI warning, business email compromise attacks, which make up a small percentage of all cyberattacks, cost organizations worldwide more than $26 billion in the past three years.

Each month, Barracuda researchers evaluate the current cybersecurity landscape and publish the detailed findings in the Threat Spotlight. This eBook analyzes that proprietary research from the past 12 months, to provide an outlook of top potential cybersecurity threats for 2020 and effective solutions that businesses can use to help defend against them in the year ahead.

Business email compromise attacks cost organizations more than $26 billion in the past three years.

Top Threat: Phishing

Don't expect phishing, including spear phishing, lateral phishing and related attacks, to go away any time soon. **Phishing remains a persistent threat, and attacks continue to evolve.**

Phishing emails are sent to very large numbers of recipients, more or less at random, with the expectation that only a small percentage will respond. Here's an example: An apparently official email from a well-known delivery company says your package has been delayed and tells you to click a link to get more details. If you click the link, malware could be downloaded onto your device. The link could also go to a fake website where you're asked to enter your name, address and social-security number. That information would be sold on the black market and used to commit identity theft, fraud and other crimes.

On the other hand, spear-phishing attacks are very personalized. Cybercriminals research their targets and often impersonate a trusted colleague, website or business. Like other phishing attacks, spear-phishing emails typically try to steal sensitive information, such as login credentials or financial information. For example, scammers impersonate an employee in the organization requesting a wire transfer.

While phishing emails are sent to large numbers of recipients, spear-phishing attacks are more personalized.

Phishing lures account-takeover victims

Barracuda researchers revealed a startling rise in account takeover, one of the fastest growing email security threats. To execute account-takeover attacks, cybercriminals use brand impersonation, social engineering and phishing to steal login credentials and access accounts. Once an account is compromised, hackers track activity to learn how the company does business, the email signatures they use, and the way financial transactions are handled, so they can launch successful attacks, including harvesting additional login credentials.

An analysis of account-takeover attacks found that 29 percent of organizations had their Office 365 accounts compromised in March 2019. **More than 1.5 million malicious and spam emails were sent from the hacked Office 365 accounts** in that one month. With more than half of all global businesses already using Office 365 and adoption continuing to grow quickly, hackers want to take over accounts because they serve as a gateway to an organization and its data—a lucrative payoff for the criminals.

See the full details in Threat Spotlight: Account Takeover »

Hackers exploit vulnerabilities with IoT devices

Cybercriminals are also harvesting login credentials for IoT devices. Attackers use vulnerabilities in web apps and mobile apps used by some IoT devices to acquire credentials and take control of devices. The credentials can also be used to push firmware updates to the devices, changing their functionality and using the compromised devices to attack other devices on the same network.

Barracuda researchers used an IoT security camera to help illustrate the threat of IoT credential compromise. By identifying and exploiting multiple vulnerabilities in the camera's web app and mobile app ecosystem, researchers were able to compromise it, without any direct connection to the camera itself, and could view the video feed, set/receive/delete alarms, remove saved video clips from cloud storage and read account information. **The threat of IoT credential compromise could affect many types of IoT devices, regardless of their function,** because it takes advantage of the way the devices communicate with the cloud.

See the full details in Threat Spotlight: IoT Credential Compromise »

Phishing moves in new direction

Attackers are adapting and introducing new ways to exploit compromised accounts.

Barracuda researchers, teaming up with leading researchers at UC Berkeley and UC San Diego, uncovered a new and growing type of account-takeover attack: lateral phishing. Attackers use accounts they've recently compromised to send phishing emails to an array of recipients, ranging from close contacts within the company to partners at other organizations. The study found that **1 in 7 organizations experienced lateral-phishing attacks in the previous seven months**.

Of the organizations that experienced lateral phishing, more than 60 percent had multiple compromised accounts. Some had dozens of compromised accounts that sent lateral phishing attacks to additional employee accounts and users at other organizations. In total, lateral phishing emails were sent to more than 100,000 unique recipients from the compromised accounts that were analyzed.

See the full details in Threat Spotlight: Lateral Phishing »

Phishing attacks are remediated too slowly

Inefficient incident response to email attacks is costing businesses billions in losses annually.

For many organizations, finding, identifying and removing email threats is a slow and manual process that takes too long and uses too many resources. As a result, attacks often have time to spread and cause more damage. After all, in most phishing campaigns, it takes just 16 minutes for someone to click on a malicious link. **With manual incident response, however, it takes about three and a half hours for organizations to respond.** In many cases, by that time, the attack has spread further, requiring additional investigation and remediation.

Barracuda researchers performed email threat scans on 383,790 mailboxes across 654 organizations. Using the Barracuda Email Threat Scanner, a free tool that an organization can use to analyze its Office 365 environment and detect threats that got past the email gateway, nearly 500,000 malicious messages were identified in those mailboxes in a 30-day period. **On average, each organization had more than 700 malicious emails that users could access anytime.**

Automated incident response is more important than ever, especially considering the rise in spear-phishing attacks that are designed to evade email security. For example, business email compromise attacks, which include no malicious links or attachments, have been shockingly effective; in the past three years, these attacks have resulted in losses of $26 billion, according to the FBI.

See the full details in Threat Spotlight: Inefficient Incident Response »

In most phishing campaigns, it takes just 16 minutes for someone to click on a malicious link, but manual incident response can take hours.

Top Threat: Malware

Cybercriminals continue to use malicious software, known as malware for short, to launch a variety of attacks. **Modern malware attacks are complex, layered and continuing to evolve.** Most malware is sent as spam to widely-circulated email lists that are sold, traded, aggregated and revised as they move through the dark web. Typically, the malware is hidden in a document attached to an email. Once the document is opened, either the malware is automatically installed or a heavily obfuscated macro/script is used to download and install it from an external source. Common types of malware include viruses, Trojans, spyware, worms and ransomware.

Malware is constantly updated to include new evasion and backdoor techniques designed to fool users and security services. Some of these evasion techniques rely on simple tactics, such as using web proxies to hide malicious traffic or source IP addresses.

More sophisticated evasion techniques include polymorphic malware, which constantly changes its code to side-step detection from most anti-malware tools.

Most malware is sent as spam to widely-circulated email lists that are sold, traded, aggregated and revised as they move through the dark web.

Email attachments popular for malware delivery

In a document-based malware attack, cybercriminals use email to deliver a document containing malware. Attackers use social-engineering tactics, including urgency, to get users to open the malicious attachment.

Barracuda researchers uncovered an alarming increase in the frequency of document-based malware attacks. **An email analysis in April 2019 revealed that 48 percent of all malicious files detected in the previous 12 months were some kind of document.** More than 300,000 unique malicious documents were identified.

Microsoft and Adobe file types are the most commonly used in document-based malware attacks, including Word, Excel, PowerPoint, Acrobat and PDF files. Attackers often play tricks with file extensions to try to confuse users and get them to open malicious documents.

See the full details in Threat Spotlight: Document-Based Malware »

Malware attacks take a modular twist

Cybercriminals are also using email to launch modular-malware attacks. An increasing trend, modular malware provides an architecture that is more robust, evasive and dangerous than typical document-based or web-based malware. Modular malware includes—and can selectively launch—different payloads and functionality, depending on the target and the goal of the attack.

Barracuda researchers have seen a spike in the use of modular malware. **An analysis of email attacks targeting Barracuda customers identified more than 150,000 unique malicious files in the first five months of the year.**

Typically, modular malware involves a very basic initial payload. Once a foothold is established, the payload connects to a remote command-and-control (C2) server. This enables information about the system to be sent and processed by the C2 server; additional payloads can be chosen, based on that information. This approach has been used in banking Trojans, including Emotet, TrickBot and CoreBot, as well as in infostealers, like LokiBot and Pony.

See the full details in Threat Spotlight: Modular Malware »

Top Threat: Ransomware

Ransomware is one of the largest modern security challenges, and many businesses lack the resources to effectively combat it. A type of malware that infects your system, ransomware locks or encrypts important data, allowing attackers to ask for a ransom. The attackers will offer to provide the decryption key only if you pay a certain amount of money within a short time.

Ransomware usually finds its way into a system through a malicious email attachment or a malicious website that will download infected software.

Once the ransomware is on the system, it may lock down the system, encrypt the user's files, or restrict the user from accessing any of the computer's main features. While the system is locked down, the ransomware will pop up messages asking for a certain amount of money to lift the lock. **Paying the ransom is not a guarantee that the system will be unlocked or that the ransomware will be removed.**

Ransomware attacks are widespread, and they have become a preferred tool of hackers due to their success. Effectively combatting ransomware requires a team of knowledgeable people making frequent updates to cybersecurity, something most small and medium-sized businesses don't have the resources to do.

Ransomware has been around for about 20 years, but the threat has grown rapidly recently.

Ransomware attacks move beyond businesses

Cybercriminals are targeting government agencies across the United States with ransomware. These evolving and sophisticated attacks are damaging and costly. They can cripple day-to-day operations, cause chaos and result in financial losses from downtime, ransom payments, recovery costs and other unbudgeted expenses.

While ransomware has been around for about 20 years, the threat has been growing rapidly recently, especially when it comes to attacks on government.

Barracuda analyzed hundreds of attacks across a broad set of targets, revealing that **government organizations are the intended victims of nearly two-thirds of all ransomware attacks**. Local, county, and state governments have all been targets, including schools, libraries, courts, and other entities.

An in-depth look at 55 ransomware attacks on state, county, and local governments showed that, while all types of governments were affected, most victims were small towns or big cities. About **45 percent of the municipalities attacked had populations of less than 50,000 residents**, and 24 percent had less than 15,000 residents. Smaller towns are often more vulnerable because they lack the technology or resources to protect against ransomware attacks. Nearly 16 percent of the municipalities attacked were cities with populations of more than 300,000 residents. Ransomware used in recent attacks against state and local governments includes Ryuk, SamSam, LockerGoga and RobbinHood.

See all the details in Threat Spotlight: Government-Ransomware Attacks »

Attackers use blackmail to make money, too

With sextortion, a form of blackmail, attackers leverage usernames and passwords stolen in data breaches, using the information to contact and try to trick employees, individuals and other victims into giving them money. The scammers claim to have a compromising video, allegedly recorded on the victim's computer, and threaten to share it with all their contacts unless they pay up.

Sextortion scams have expanded in scope, increased in frequency and become more sophisticated. Attackers prey on a victim's fears in a threatening email. Often, attackers spoof their victim's email address, pretending to have access to it, to make the attack even more convincing. Bitcoin is the form of payment typically demanded.

Barracuda researchers uncovered some startling revelations about sextortion scams. An analysis of spear-phishing attacks targeted at Barracuda customers found that 1 in 10 were blackmail or sextortion attacks. **In fact, employees are twice as likely to be targeted in a sextortion scam than a business email compromise attack.**

Sextortion emails are typically sent to thousands of people at a time, as part of larger spam campaigns, so most get caught in spam filters. But scammers are continually evolving their email-fraud techniques, including using social-engineering tactics to bypass traditional email-security gateways. Sextortion emails that end up in inboxes typically do so because they originate from high-reputation senders and IPs; hackers use already-compromised Office 365 or Gmail accounts. Attackers have also started to vary and personalize the content of the emails, making it more difficult for spam filters to stop them.

Sextortion scams are under-reported due to the intentionally-embarrassing and sensitive nature of the threats. IT teams are often unaware of these attacks because employees don't report the emails, regardless of whether they pay the ransom.

See all the details in Threat Spotlight: Sextortion »

Defending Your Business

The rapidly evolving threat environment requires a multi-layered protection strategy—one that closes the technical and human gaps—for every organization to maximize its cybersecurity performance and minimize the risk of falling victim to sophisticated attacks, including phishing, malware and ransomware.

Take advantage of artificial intelligence

Scammers are adapting email tactics to bypass gateways and spam filters, so it's critical to have a solution in place that use artificial intelligence to detect and protect against sextortion, phishing and spear-phishing attacks, including business email compromise and brand impersonation. Deploy purpose-built technology that doesn't solely rely on looking for malicious links or attachments. **Use machine learning to analyze normal communication patterns within your organization and spot anomalies that may indicate an attack.**

With the evolution of lateral phishing, attacks are becoming increasingly difficult for even trained and knowledgeable users to detect. Organizations should invest in advanced detection techniques and services that leverage artificial intelligence and machine learning to automatically identify phishing emails and block potentially-threatening messages and attachments from reaching email inboxes, without relying on users to identify them on their own.

Get more information about AI-based protection from phishing and account takeover »

Proactively investigate and remediate

While many malicious emails appear convincing, phishing-detection systems and related security software can pick up subtle clues and help block potentially-threatening messages and attachments from reaching email inboxes.

Given the nature of sextortion scams, employees might be reluctant to report these attacks. Conduct regular searches on delivered mail to detect emails related to password changes and security alerts. Many sextortion emails originate from outside North America or Western Europe. Evaluate where delivered mail is coming from, review any of suspicious origin, and remediate.

Some of the most devastating and successful spear-phishing attacks originate from compromised accounts, so be sure scammers aren't using your organization as a base camp to launch these attacks. Use technology to identify suspicious activity, including logins from unusual locations and IP addresses, a potential sign of a compromised account. Be sure to also monitor email accounts for malicious inbox rules, as they are often used as part of account takeover. Criminals log into the account, create forwarding rules and hide or delete any email they send from the account, to try to cover their tracks. **Deploy technology that recognizes when accounts have been compromised and remediates in real time** by alerting users and automatically removing malicious emails sent from compromised accounts.

Get more information about proactive threat identification and automated incident response »

Train staffers to recognize and report attacks

Educate your employees about spear-phishing, sextortion, and other new types of attacks by making it part of security-awareness training. Ensure they can recognize potential threats, understand their fraudulent nature, and know how to report them.

Help employees avoid making costly mistakes by creating guidelines that put procedures in place to confirm requests that come in by email, including making wire transfers and buying gift cards.

Use phishing simulation to transform staffers from a security liability into a line of defense. Show them how to identify email, voicemail, and SMS attacks. Test the effectiveness of your training with in-the-moment simulations. Evaluate the users most vulnerable to attacks.

Get more information about phishing simulation and training »

Use a variety of advanced solutions

Deploy advanced inbound and outbound security techniques like malware detection, spam filters, firewalls, and sandboxing.

Encryption and DLP help secure against accidental and malicious data loss. Email archiving is critical as well for compliance and business-continuity purposes.

For emails with malicious documents attached, both static and dynamic analysis can pick up on indicators that the document is trying to download and run an executable, which no document should ever be doing. The URL for the executable can often be flagged using heuristics or threat intelligence systems. Obfuscation detected by static analysis can also indicate whether a document may be suspicious.

If a user opens a malicious attachment or clicks a link to a drive-by download, an advanced network firewall capable of malware analysis provides a chance to stop the attack by flagging the executable as it tries to pass through.

Get more information about protection that goes beyond next-generation firewalls »

Build in a backup plan

In the event of a ransomware attack, a backup solution can minimize downtime, prevent data loss, and get your systems restored quickly, whether your files are located on physical devices, in virtual environments, or the public cloud.

To avoid having backups affected by a ransomware attack, follow the 3-2-1 rule: keep three copies of your files on two different media types with at least one offsite.

Get more information about data backup and recovery »

Barracuda
Your journey, secured.