March 2021

# Threat Spotlight: Protecting your business in 2021

## Defend against evolving phishing and malware attacks

Your journey, secured.

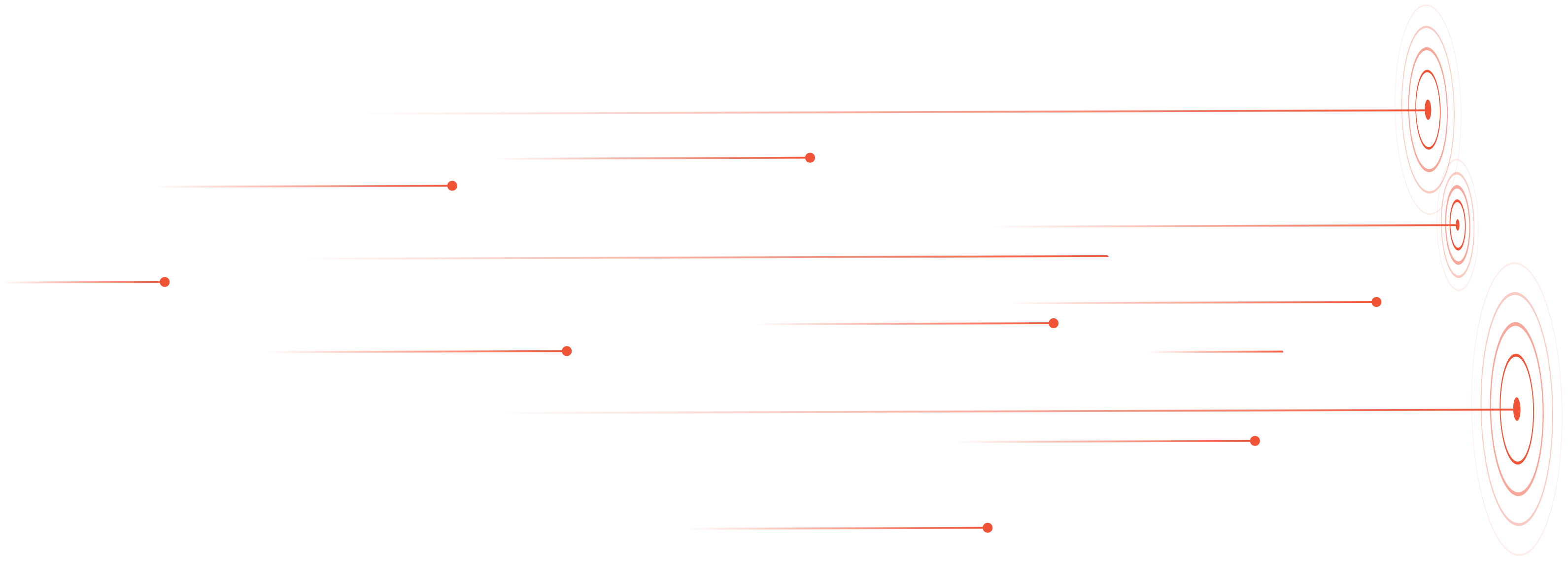
# Contents

# The evolving cyberthreat landscape

Barracuda

Beware of rapidly-emerging cybersecurity threats. Cybercriminals are morphing their attack techniques, using a range of new tactics to try to increase their success. From coronavirus-related phishing and form-based attacks to IoT malware and conversation hijacking, cybercriminals continue to evolve the threat landscape in an ongoing attempt to outsmart more potential victims and 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 block lists 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. Business email compromise attacks, which make up a small percentage of all cyberattacks, have cost organizations worldwide billions of dollars in recent years.

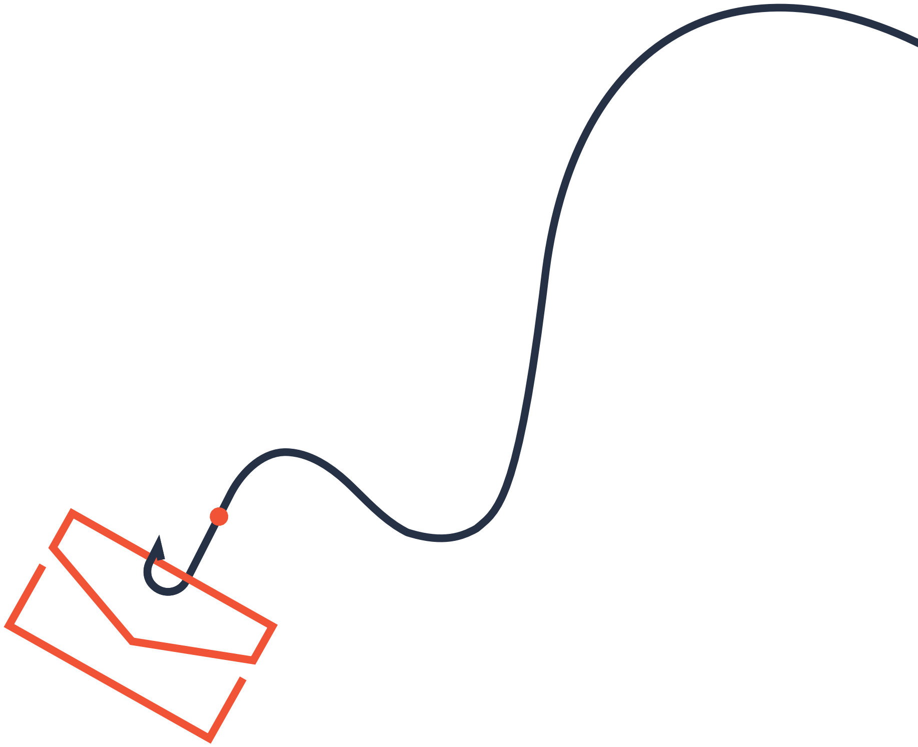
Each month, Barracuda researchers evaluate the current cybersecurity landscape and publish the detailed findings in the Threat Spotlight. This eBook analyzes that proprietary research from the past 12 months, to provide an outlook of top potential cybersecurity threats for the year ahead and effective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

# Top threat: Phishing

Don't expect phishing, including spear phishing, coronavirus-related 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 dark web 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, sometimes scammers impersonate an employee in a business, school, or other organization and request financial or personal information.



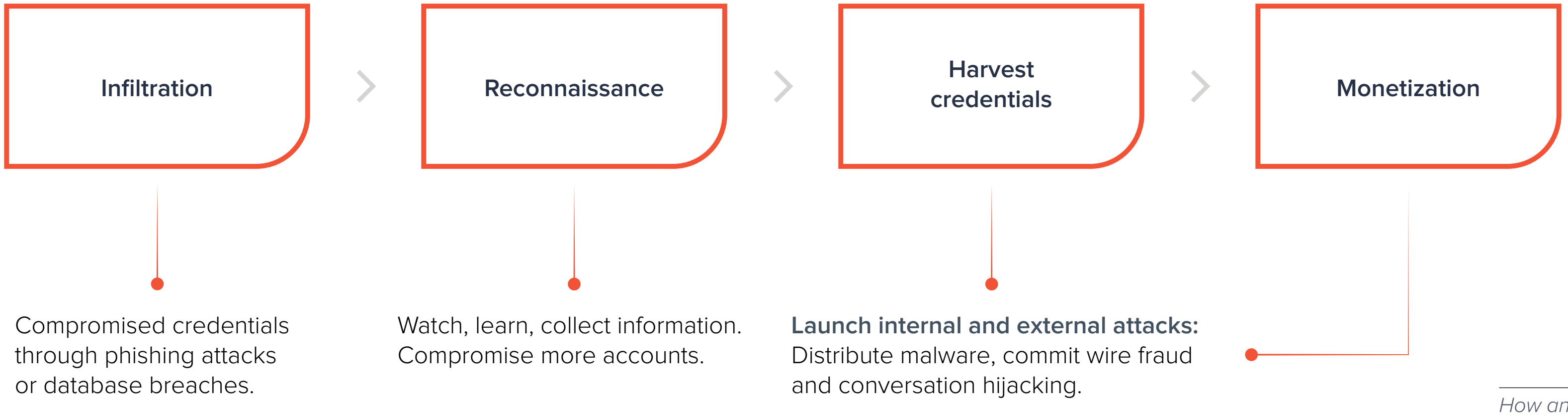
# Phishing lures account-takeover victims

Barracuda and UC Berkeley researchers conducted a large-scale analysis of email account takeover, the timelines of attacks, the behaviors hackers are using to try to avoid detection, and ways to identify suspicious activity.

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 monitor and 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 for other accounts.

In their analysis, researchers noted that attacks are spread out over a period of time; they don't always happen as soon as the account is compromised. Attackers are also getting smarter about geography; they send phishing emails and perform other actions from IPs tied to similar regions and countries of the hacked account. IP addresses and ISPs provide important clues; attackers tend to use anonymous IPs belonging to ISPs that are different from the hacked account's provider. For cybercriminals, taking over accounts and gaining access to an organization and its data provides a lucrative payoff.

See the full details in Threat Spotlight: Email account takeover.



Infiltration

Compromised credentials through phishing attacks or database breaches.

Reconnaissance

Watch, learn, collect information. Compromise more accounts.

Harvest credentials

**Launch internal and external attacks:** Distribute malware, commit wire fraud and conversation hijacking.

Monetization

*How an account-takeover attack happens*

## Hijacked conversations fuel sophisticated phishing attacks

Attackers are also using conversation hijacking to steal money and sensitive personal information. Based on information they've gathered from compromised email accounts or other sources, cybercriminals insert themselves into existing business conversations or initiate new ones. Leveraging information from the compromised accounts, including internal and external conversations between employees, partners, and customers, they craft convincing messages and send them from impersonated email domains to trick victims into wiring money or providing personal information.

Barracuda researchers saw a sharp rise in domain-impersonation attacks used to facilitate conversation hijacking in recent months. An analysis of about 500,000 monthly email attacks showed a 400-percent increase in domain-impersonation attacks used for conversation hijacking. While the use of conversation hijacking in domain-impersonation attacks is extremely low compared to other types of phishing attacks, these sophisticated attacks are very personalized, making them effective, hard to detect, and costly.

See the full details in Threat Spotlight: Conversation hijacking.

**+400%**

*Domain impersonation increase in recent months*

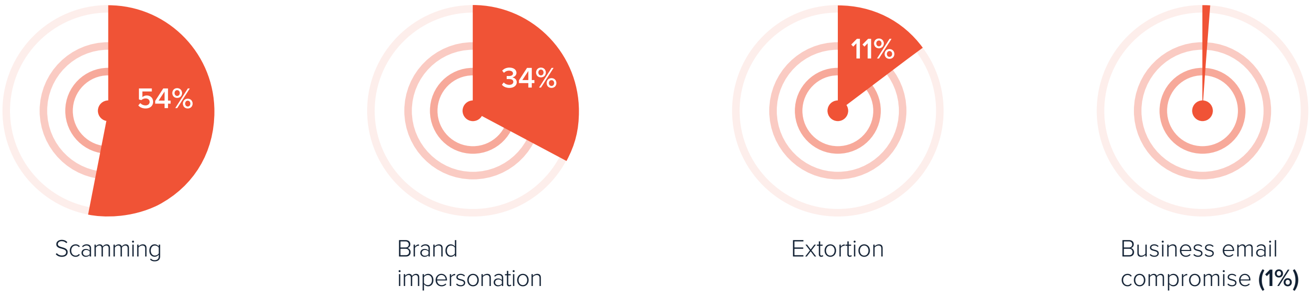
# Phishing attacks capitalize on coronavirus

As the world grapples with the coronavirus and how to handle it, attackers are taking advantage of the widespread discussion of COVID-19 in emails and across the web. A variety of phishing campaigns are leveraging the heightened focus on COVID-19 to distribute malware, steal credentials, and scam users out of money. The attacks use common phishing tactics that are seen regularly, but a growing number of campaigns are using the coronavirus as a lure to try to trick distracted users and capitalize on the fear and uncertainty of would-be victims. (The FBI issued an alert about these types of attacks.) Early on, bad actors sent emails impersonating officials from the World Health Organization or claiming to sell face masks or coronavirus cures. Now attackers are focusing more on using false updates about vaccine availability to trick people.

Between the end of February and March 23, Barracuda researchers saw a 667% spike in the number of coronavirus-related phishing attacks. They identified three main types of phishing attacks using COVID-19 themes: scamming, brand impersonation, and business email compromise. Phishing attacks using coronavirus as a hook got more sophisticated quickly, and a significant number of extortion attacks also popped up.

See all the details in Threat Spotlight: Coronavirus-related phishing.

**How businesses were affected by COVID-19 spear-phishing attacks in 2020**[1]



[1] 2020 Threat Spotlight: Coronavirus-related phishing

## Spear-phishing attacks target schools and staffers

As many schools and colleges continue to be remote, hackers understand they rely heavily on email to receive updates from teachers, principals, and department heads and they are taking advantage of the situation. Spear phishing, a highly-personalized phishing attack that targets a specific organization or individual, is being used by cybercriminals to attack a variety of different industries, including education.

Barracuda researchers evaluated more than 3.5 million spear-phishing attacks, including attacks against more than 1,000 schools, colleges, and universities. Researchers found that educational institutions are more than twice as likely to be targeted by a business email compromise (BEC) attack than other organizations. In fact, more than 25% of spear-phishing attacks targeting the education sector were carefully-crafted BEC attacks. Compromised accounts are then used to launch subsequent attacks and compromise additional accounts.

See all the details in Threat Spotlight: Spear-phishing attacks targeting education sector.

Spear-phishing attacks **evaluated**

**3.5**M

Schools **2X** more likely to be targeted by a

**BEC**
attack

# Scammers try new phishing tactics

As solutions evolve to defeat threats, scammers evolve their tactics to try to evade detection. Here's three examples.

Cybercriminals create email accounts with legitimate services and use them in impersonation and BEC attacks. They write targeted messages and, in most cases, use these email accounts only a few times, to avoid detection or being blocked by email service providers.

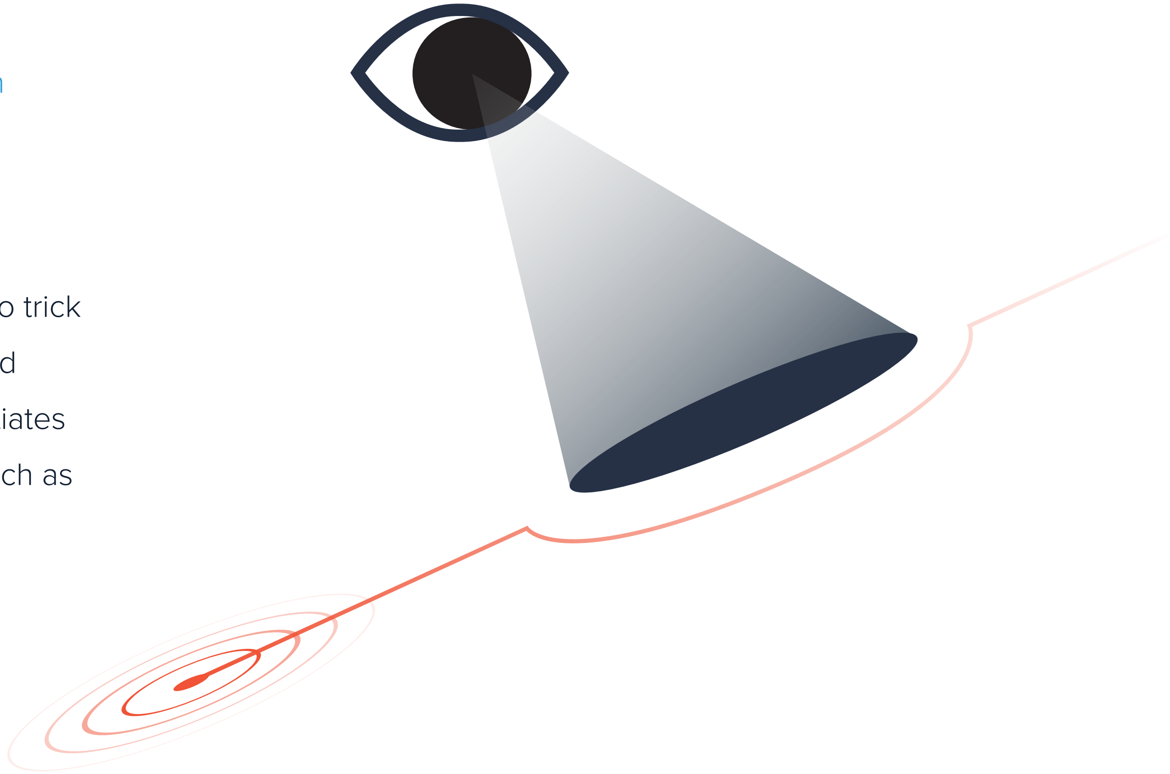
See all the details in Threat Spotlight: Malicious accounts in business email compromise.

In a unique type of brand impersonation attack, scammers leverage file, content-sharing, and other productivity sites to trick victims into sharing login credentials. This highly-specialized attack is hard to detect because the phishing email that initiates the attack usually contains a link to a legitimate website, such as docs.google.com or sway.office.com.

See all the details in Threat Spotlight: Form-based attacks.

Phishing campaigns trying to obtain email credentials have started using reCaptcha walls to block automated URL-analysis services from scanning the content of phishing website pages and to make the phishing site appear more believable for potential victims.

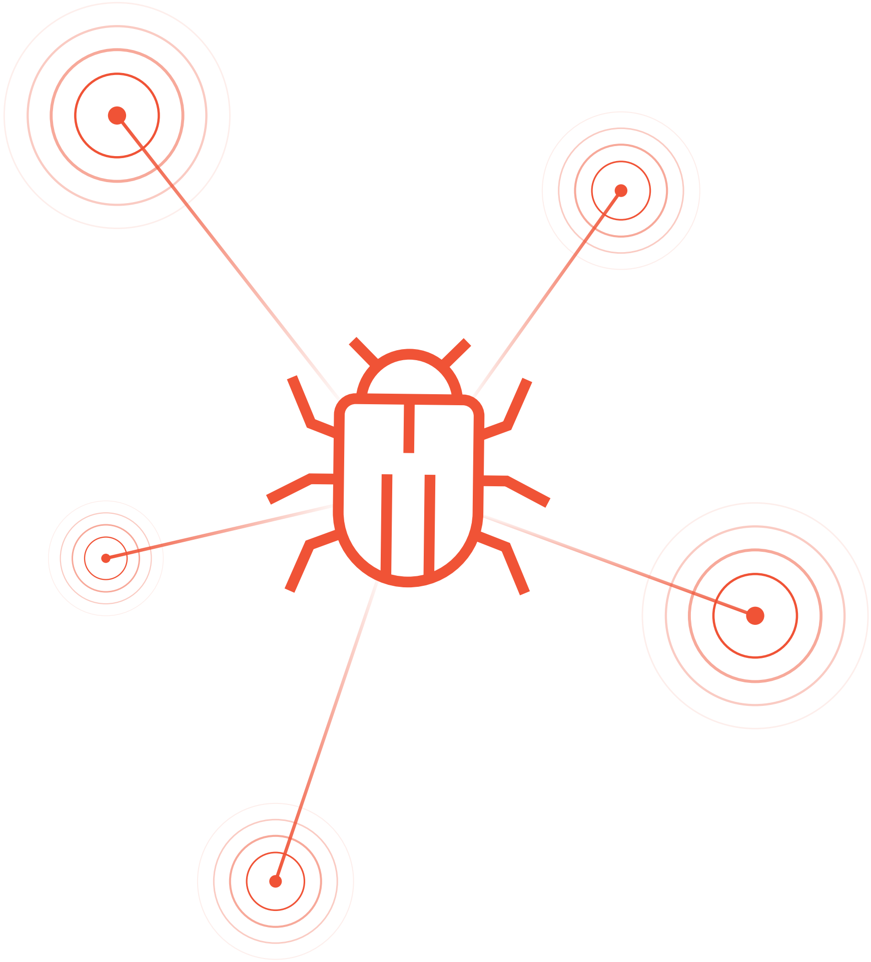
See all the details in Threat Spotlight: Malicious use of reCaptcha.



# Top threat: Malware

Cybercriminals continue to use malicious software, known as malware for short, to launch a variety of attacks. 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, 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.



## Ransomware locks critical files and causes business chaos

Cybercriminals are targeting government, healthcare, and education organizations with ransomware, a form of malware. Delivered as an email attachment or link, the malware infects the network and locks email, data, and other critical files until a ransom is paid. 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 and unanticipated expenses. For example, in 2018 the city of Atlanta got hit with a ransomware attack demanding roughly $50,000 in Bitcoin, and the city ended up spending more than $2.6 million to recover.

Although ransomware has been around for more than two decades, the threat has been growing rapidly in recent years. With the pandemic putting millions of workers at home, cybercriminals gained a larger attack surface as the result of the fast and widespread shift to remote work. The weak security of home networks makes it easier for cybercriminals to compromise them, move laterally to business networks, and launch ransomware attacks.

See all the details in Threat Spotlight: Ransomware.

## New IoT malware variant building a botnet

A new malware variant is launching attacks on Mac and Android IoT devices. Previously, only Windows and Linux machines were being attacked. The cybercriminal organization behind the malware known as InterPlanetary Storm released the new variant, which is building a botnet that Barracuda researchers estimate includes about 13,500 infected machines located in 84 countries and continues to grow.

The InterPlanetary Storm malware variant gains access to machines by running a dictionary attack against SSH servers. It can also gain entry by accessing open Android Debug Bridge (ADB) servers. The malware detects the CPU architecture and operating system, and it can run on ARM-based machines, a common architecture used for routers and other IoT devices.

See all the details in Threat Spotlight: New InterPlanetary Storm variant targeting IoT devices.

## Malware exploits servers and web application frameworks

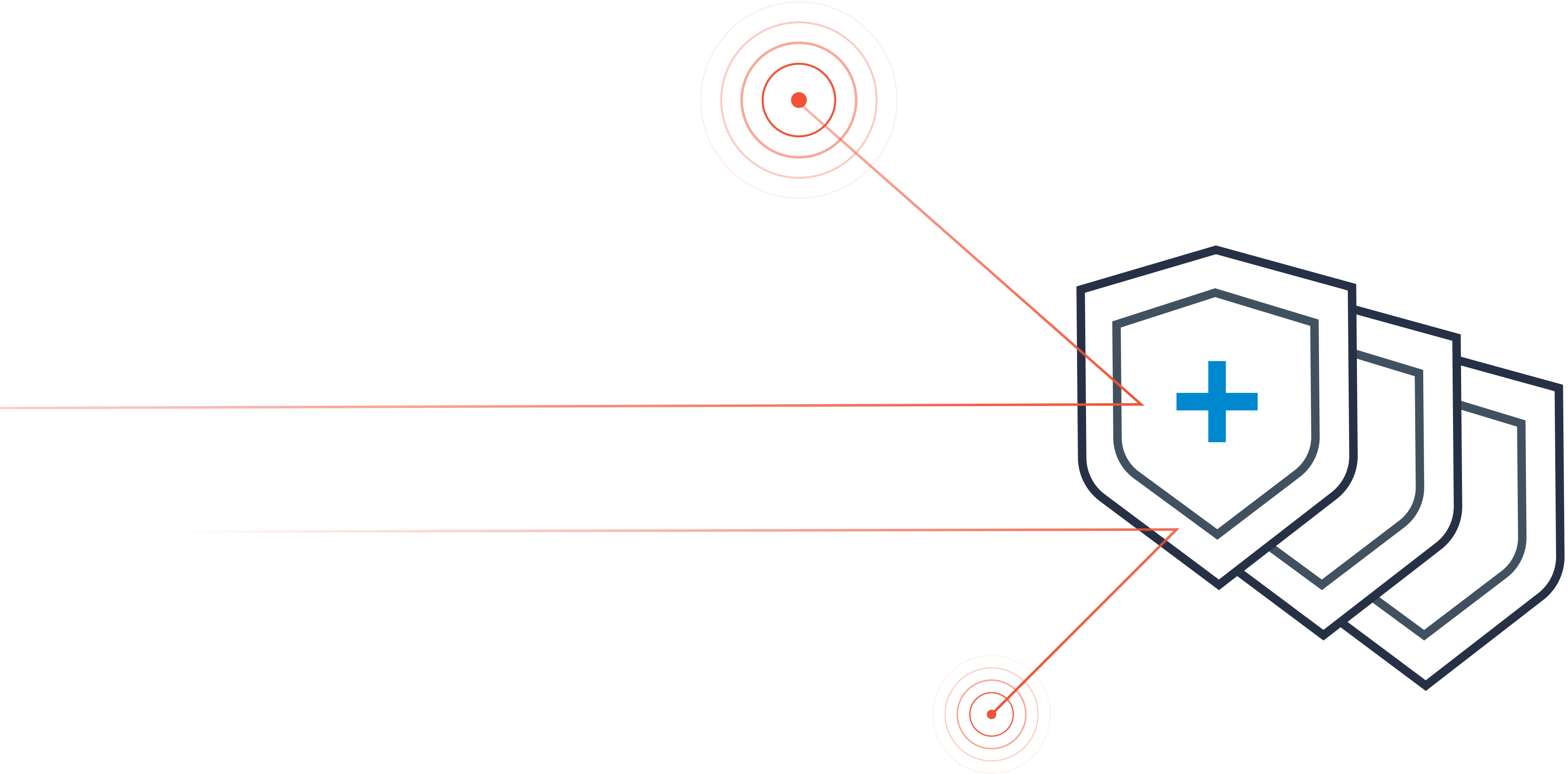
While previous variants of the cryptominer malware known as Golang attacked only Linux machines, the latest variant uses a new pool of exploits to target Windows machines. Instead of targeting end users, this new malware attacks servers.

This new malware variant attacks web application frameworks, application servers, and non-HTTP services. Its main goal is to mine cryptocurrency. Once the malware infects a machine with the initial payload, it downloads a number of files for the cryptominer, which are customized based upon the platform being attacked. The malware spreads as a worm, searching and infecting other vulnerable machines.

See all the details in Threat Spotlight: New cryptominer malware variant.

# Defending your business

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

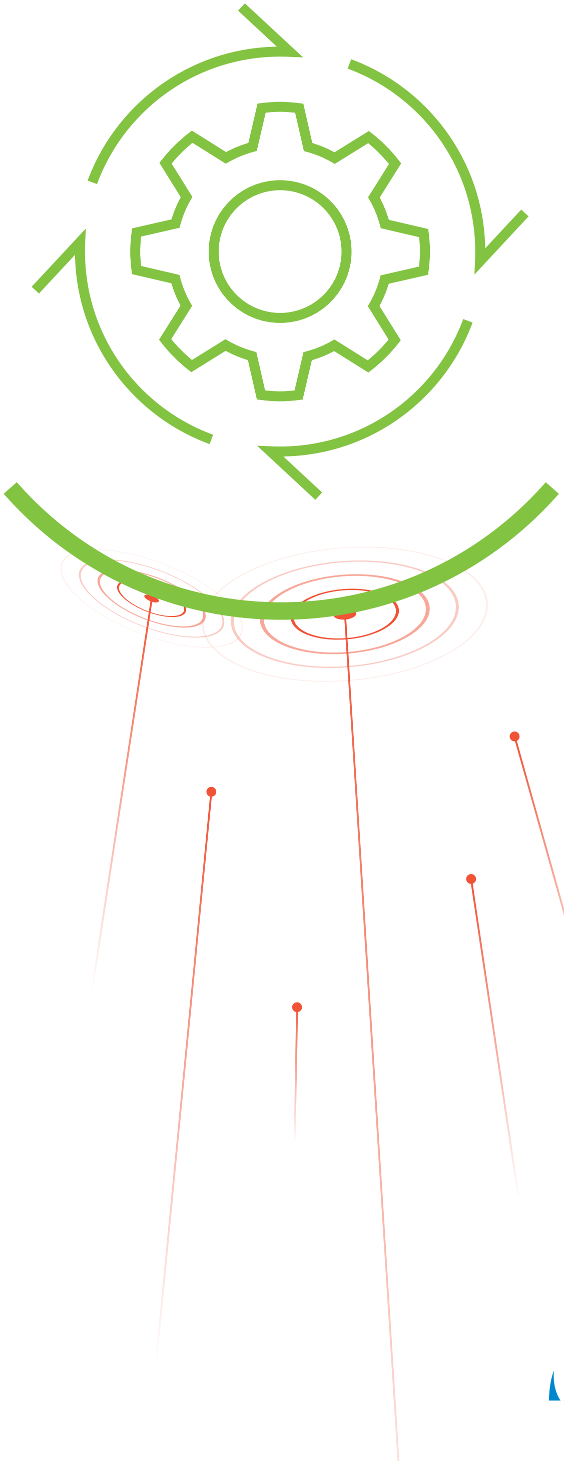


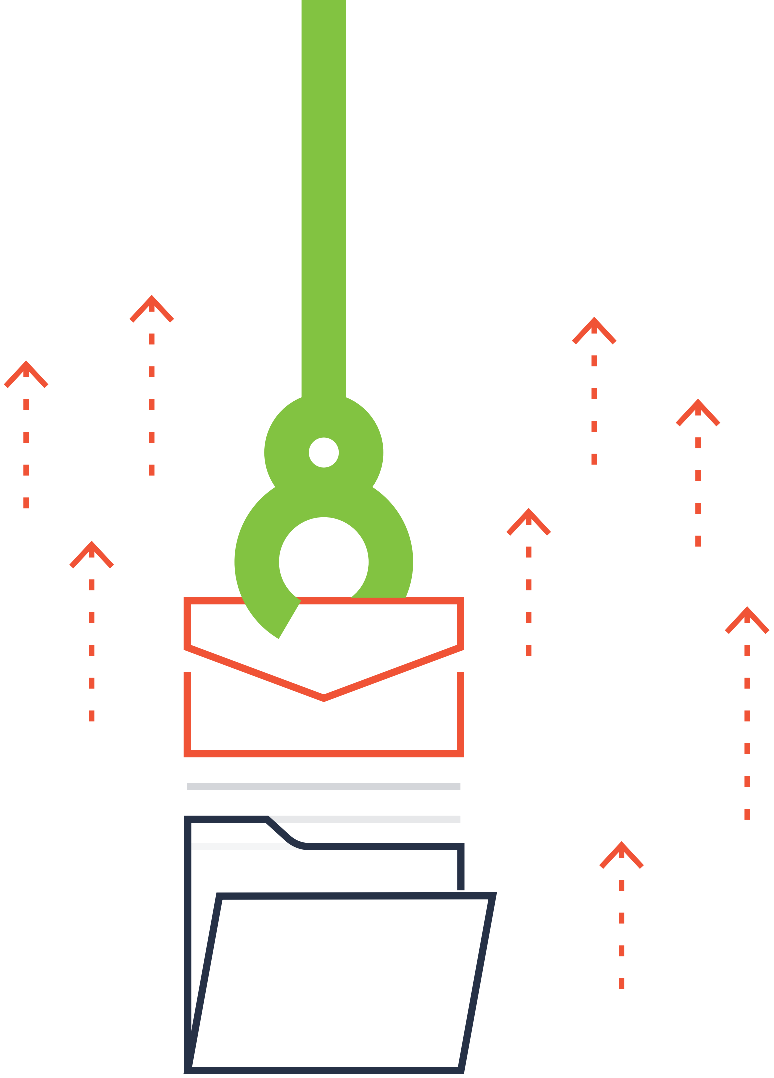
## Take advantage of artificial intelligence

Scammers are adapting email tactics to bypass gateways and spam filters, so it's critical to have a solution in place that uses artificial intelligence to detect and protect against 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 phishing, attacks are becoming increasingly difficult for even trained and knowledgeable users to detect. Organizations should invest in advanced detection techniques and services 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.

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 phishing, malware, and other 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.

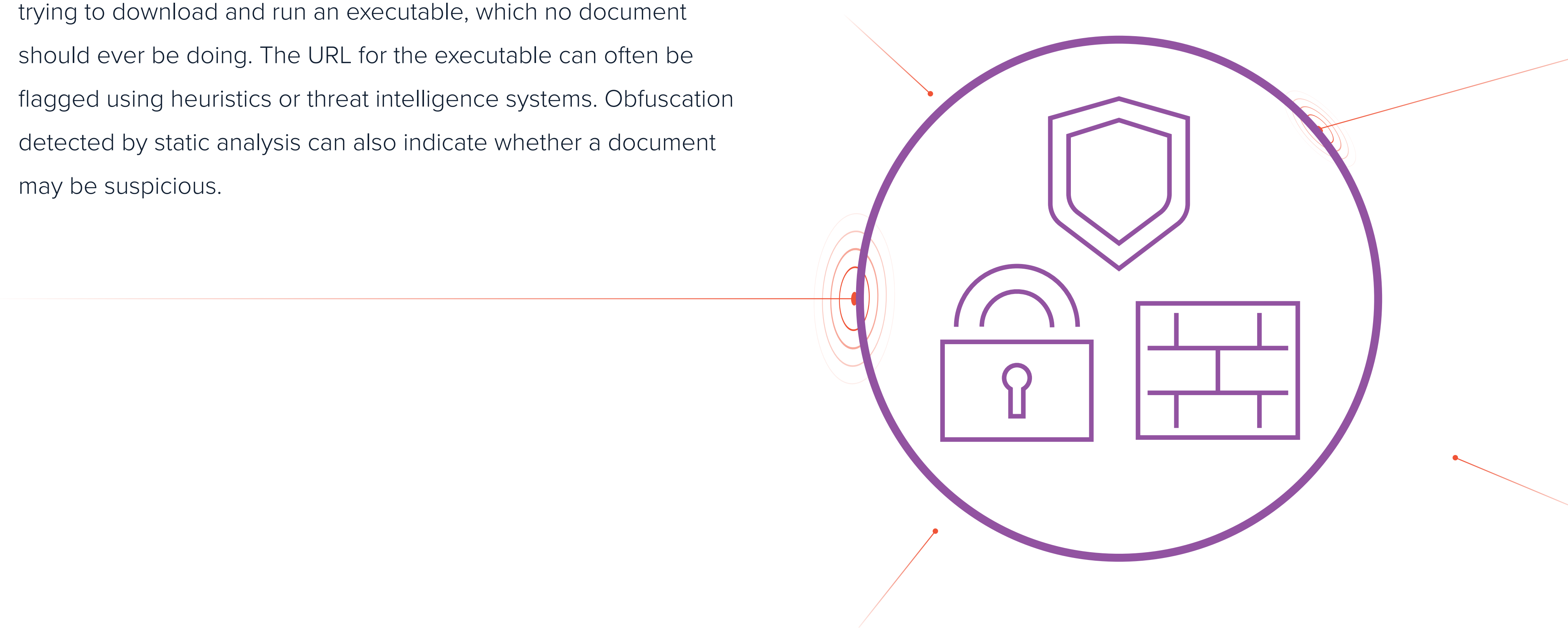
## Use a variety of advanced solutions

Deploy advanced inbound and outbound security techniques, including malware detection, spam filters, network and WAF 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.

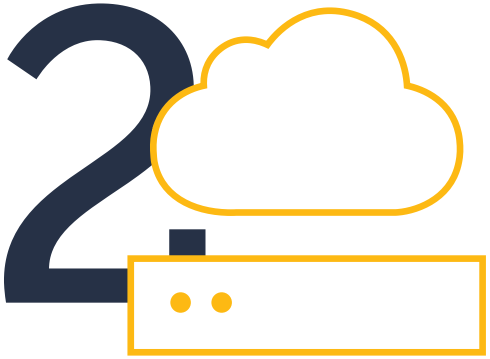


## Build in a backup plan

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.



# About Barracuda

At Barracuda we strive to make the world a safer place. We believe every business deserves access to cloud-enabled, enterprise-grade security solutions that are easy to buy, deploy, and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey. More than 200,000 organizations worldwide trust Barracuda to protect them—in ways they may not even know they are at risk—so they can focus on taking their business to the next level. For more information, visit barracuda.com.

Barracuda®
Your journey, secured.

Subscribe to the Barracuda blog for the latest insights from our monthly Threat Spotlight.

Threat Spotlight: Protecting your business in 2021 • US 1.0 • Copyright 2021 Barracuda Networks, Inc. • 3175 S. Winchester Blvd., Campbell, CA 95008 • 408-342-5400/888-268-4772 (US & Canada) • barracuda.com