April 2025

8 key threats to protect against now

Gain insights into the latest cyberthreats and discover practical strategies to protect your business from evolving attacks

Barracuda®

Table of contents

The evolving threat landscape

Cybercriminals and cybersecurity professionals have long been locked in a virtual arms race. Adversaries develop new attacks, security vendors develop new strategies to detect them and adversaries then respond with yet more innovations to evade the latest security.

For that reason, Barracuda researchers are constantly engaged in gathering, analyzing and reporting on the very latest threat data, which we gather from a vast global network of data collection points. Threat intelligence is published throughout the year on the Barracuda Blog, often in special Threat Spotlight posts.

Each of these threat intelligence posts contains information that can help you keep your organization protected against emerging and evolving attacker tactics, techniques and procedures (TTPs).

In this e-book, we've collected key takeaways from our most important pieces of threat intelligence from the last year, divided into three categories: threat trends, detailed analysis of specific incidents and threat types, and reports on novel attack techniques.

Taken together, the information presented here — and in the original blog posts — provides a roadmap to help you protect against key attack types.

Knowledge is power, and our goal here is to help you understand what's coming so you can allocate your security resources to keep your business as safe as possible.

Analyzing threat trends

Barracuda researchers have gathered and analyzed threat data to identify emerging trends and help guide organizations in preparing to defend against the changing threat landscape.

Barracuda

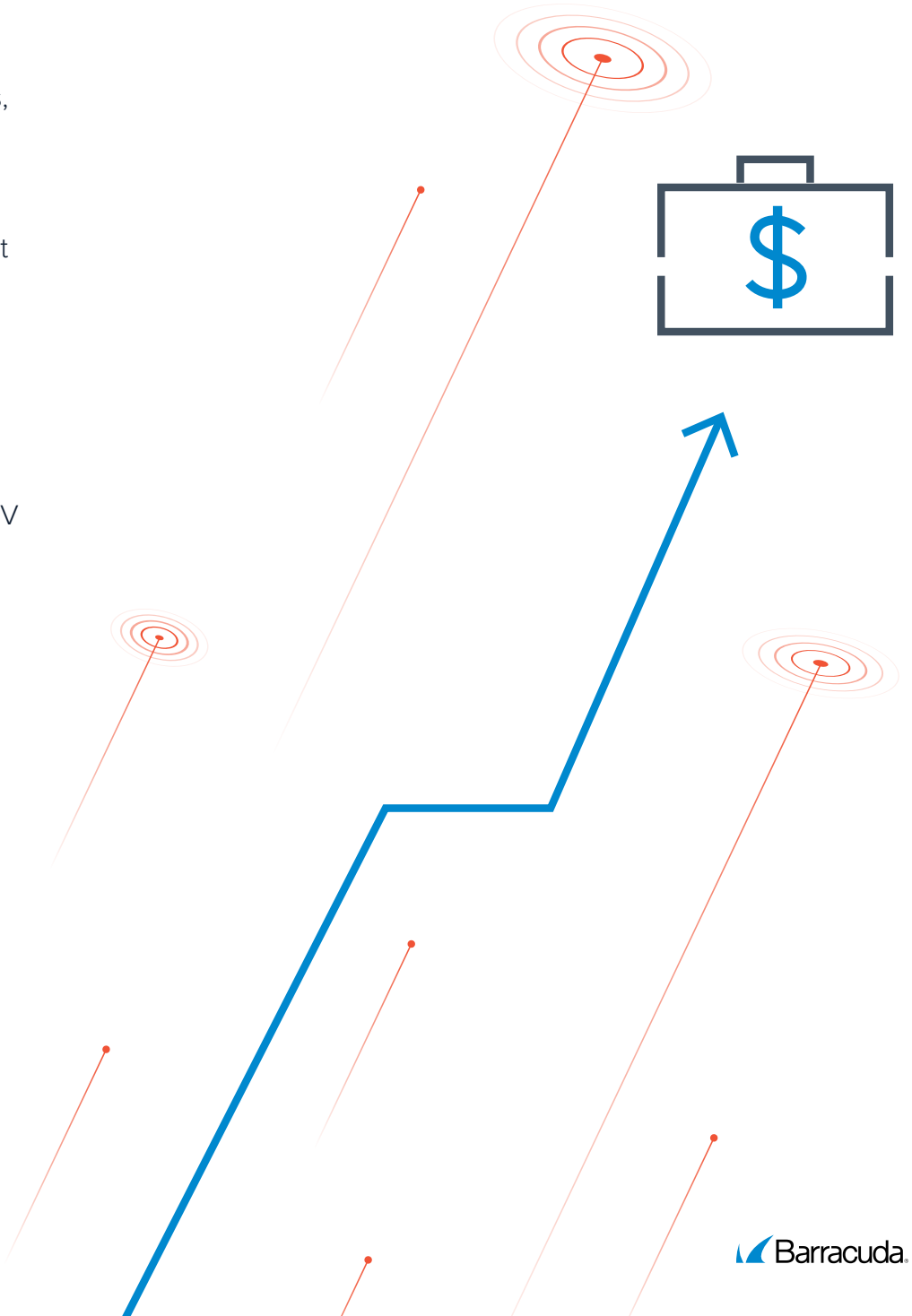
Ransomware trends

Barracuda researchers analyzed reported ransomware incidents, revealing top targets, how the business of ransomware is evolving and more. Data and insights from Barracuda Managed XDR shows how organizations can identify unfolding or imminent ransomware attacks.

The dominance of ransomware-as-a-service

A significant number of ransomware attacks leveraged common ransomware-as-a-service (RaaS) offerings such as LockBit, ALPHV or BlackCat and Rhysida.

> *"The most prevalent ransomware groups in our sample are, perhaps unsurprisingly, ransomware-as-a-service (RaaS) models. These include LockBit, which in 2023/24 was behind one in six, or 18% of the attacks where the identity of the attacker is known, despite the law enforcement takedown of the group in February 2024. Of these incidents, 28% targeted healthcare organizations, 21% municipalities, and 14% education.*



ALPHV ransomware, also known as BlackCat, accounted for 14% of attacks in 2023/24 where the identity of the attacker is known, with a third of these incidents targeting healthcare organizations, while 17% hit financial services.

Rhysida, a new ransomware group that appeared in early 2023, accounted for 8% of named attacks, with 38% of them hitting healthcare.

RaaS ransomware attacks can be hard to predict and therefore contain. The number and range of affiliates implementing attacks from the same ransomware family can lead to significant variation in observed tactics, techniques, and procedures (TTPs)."

The widespread availability of RaaS services — which make it easy for almost anyone to launch a ransomware attack — has contributed to the ongoing growth of ransomware attempts. Barracuda Managed XDR threat data finds a fourfold increase in ransomware threats over 2024.

4x increase

in ransomware threats over 2024

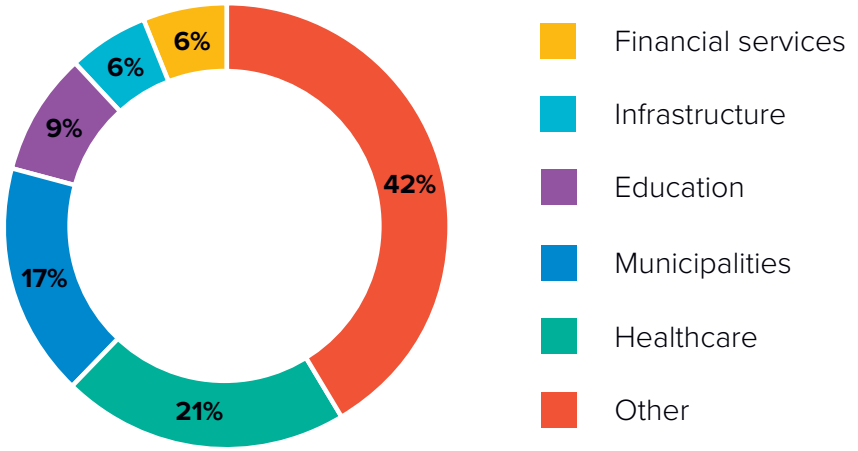
Barracuda

Healthcare and municipalities remain top targets

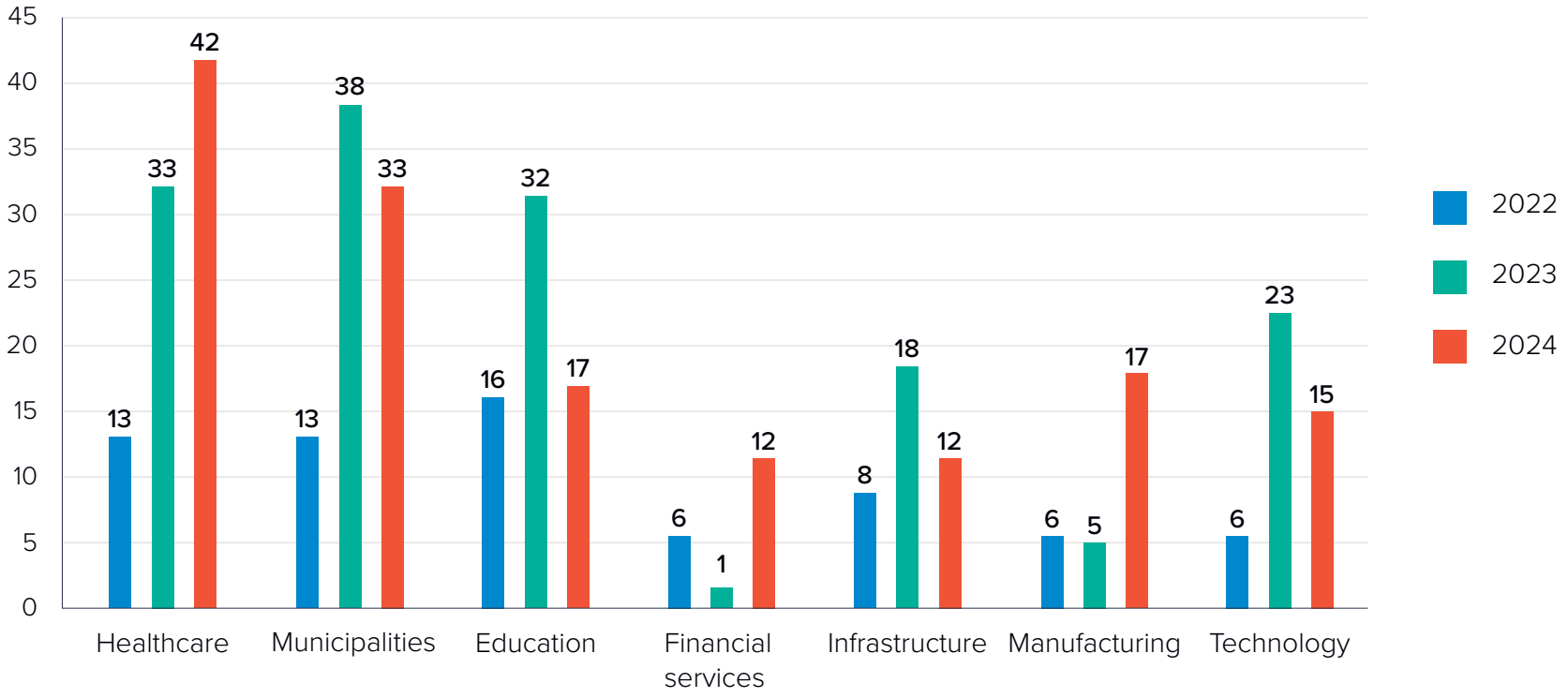
Ransomware continues to disproportionately target specific industries, primarily healthcare and municipalities. Healthcare attacks rose compared to prior years.

Education also saw a dramatic decrease in attacks, from 18% in 2023 to 9% in 2024. Attacks on financial services, while still low, saw a major increase.

Reported ransomware attacks by focused industry, 2024



Count of ransomware attacks by industry based on sample of 200 incidents



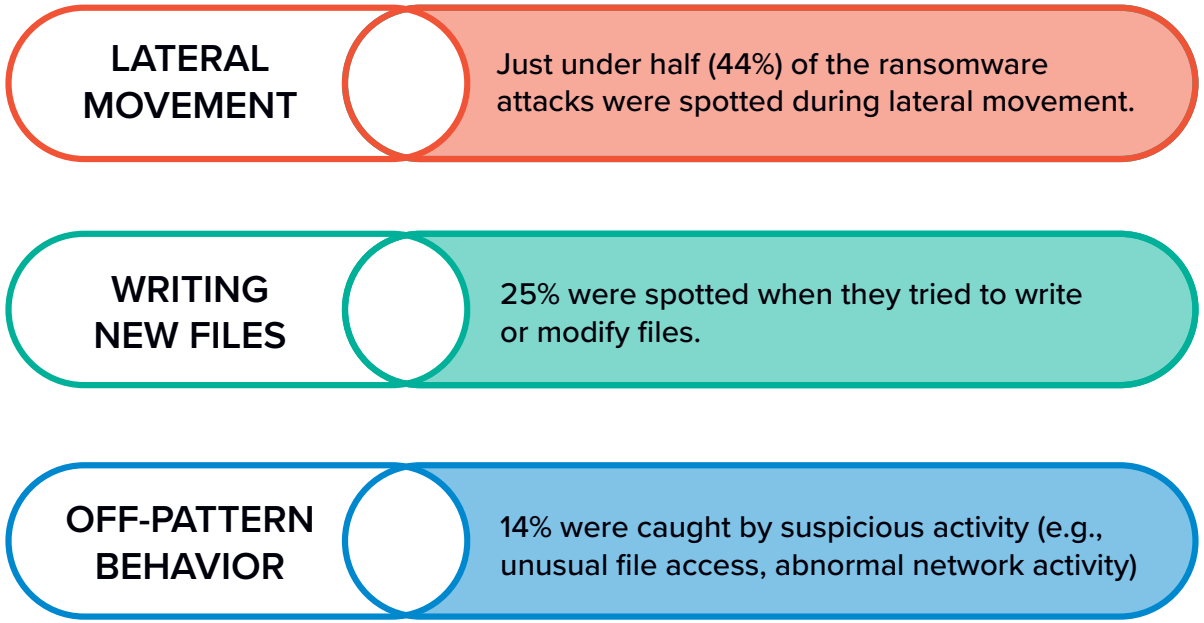
Barracuda

Most common ways ransomware is detected

Ransomware attacks can be complex and multistep. This provides several opportunities for detection. Multilayered security is critical to optimizing your ability to detect unfolding or imminent ransomware incidents and prevent attackers from accomplishing their goals.

Data from Barracuda's Security Operations Center (SOC) and Barracuda Managed XDR shows that suspicious lateral movement is the clearest sign of a ransomware incident, with 44% of attacks spotted at this stage.

A quarter of incidents were spotted when the attackers tried to write or modify files, and 14% were caught during other suspicious 'off-pattern' behavior. These were spotted by machine-learning engines that detect anomalies in normal patterns of behavior within a system.



Barracuda

Bad bots are evolving to become more human-like

Barracuda researchers also examined how bad bots are evolving to become more human-like in their behavior — and what that means for your organization's security.

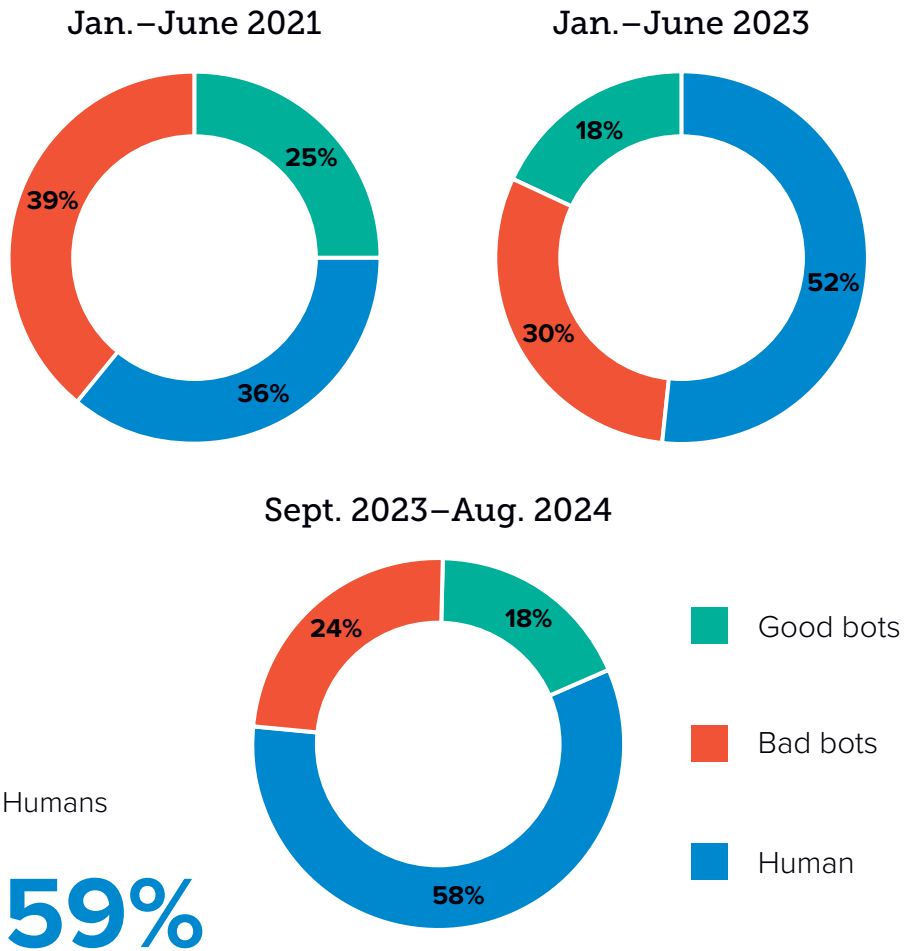
Bad bots represent growing share of internet users

Findings show that there are more individual bad bots swarming around the internet, but their volume as a share of overall internet traffic has declined.

Individual clients detected in internet traffic — Jan. to Aug. 2024

	Good bots	Bad bots	Humans
September 2023	5%	36%	59%
August 2024	7%	44%	49%

Traffic distribution — Bots vs. humans



Barracuda

This may at first seem contradictory. However, researchers believe that the reduction in bad bot traffic at the same time as an increase in the total number of bots is explained by three trends:

1. More companies have become aware of the danger of bad bots and have implemented measures to detect and block them. This, in turn, makes bad bots a less attractive method for hackers to achieve their goals.

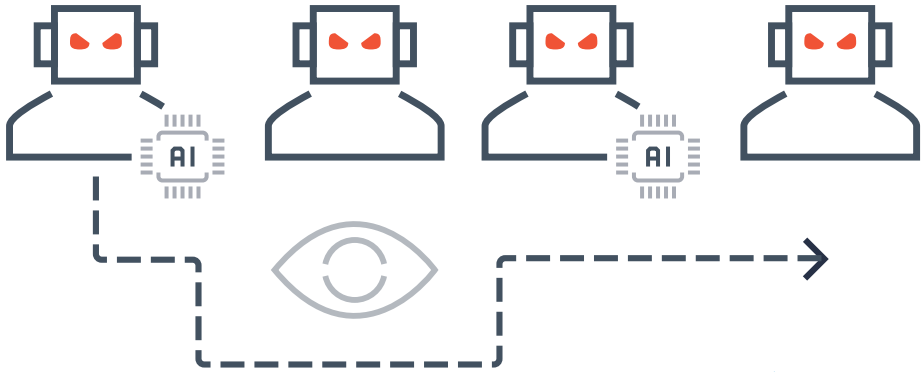
2. "In 2021, bad bot traffic included swarms of shopping bots targeting e-commerce sites to grab high-value consumer items to resell at a significantly inflated price. This included the infamous 'sneaker-bots' hunting limited edition shoes. When the market for such products collapsed during the economic downturn, the demand for mass shopping bots declined, reducing the volume of bad bot traffic."

3. The advanced and sophisticated bots that have been developed are more highly targeted than previous bots, meaning that they can achieve their goals more efficiently — requiring less traffic.

Nearly half of bots are 'advanced,' many of them are malicious

Indeed, these more advanced bots, which use AI and are capable of convincingly imitating human behavior in many types of interaction, were found to account for nearly half of all bot traffic:

"These account for 49% of bot activity, much of it malicious. The malicious bots use sophisticated techniques to mimic human behaviors, and they can navigate complex web interactions, bypassing standard controls that look at rate of traffic, error rate, CAPTCHA, and IP addresses. Examples include account takeover bots that use multiple methods to perform so-called 'low and slow' attacks, which leverage different IP/geo locations to stay under the radar and evade detection."



Barracuda

“Grey bots”

There has been an emergence of so-called “grey bots” powered by artificial intelligence. These are not necessarily malicious, but their purpose and methods may be considered questionable:

> *“These AI bots are primarily designed to extract or scrape large volumes of data from websites, for example, to train generative AI models. The bots can be aggressive when collecting data and may remove information without permission, possibly ignoring any embedded robots.txt code that is added by publishers to signal to scraper bots that they shouldn’t take that website’s data.”*

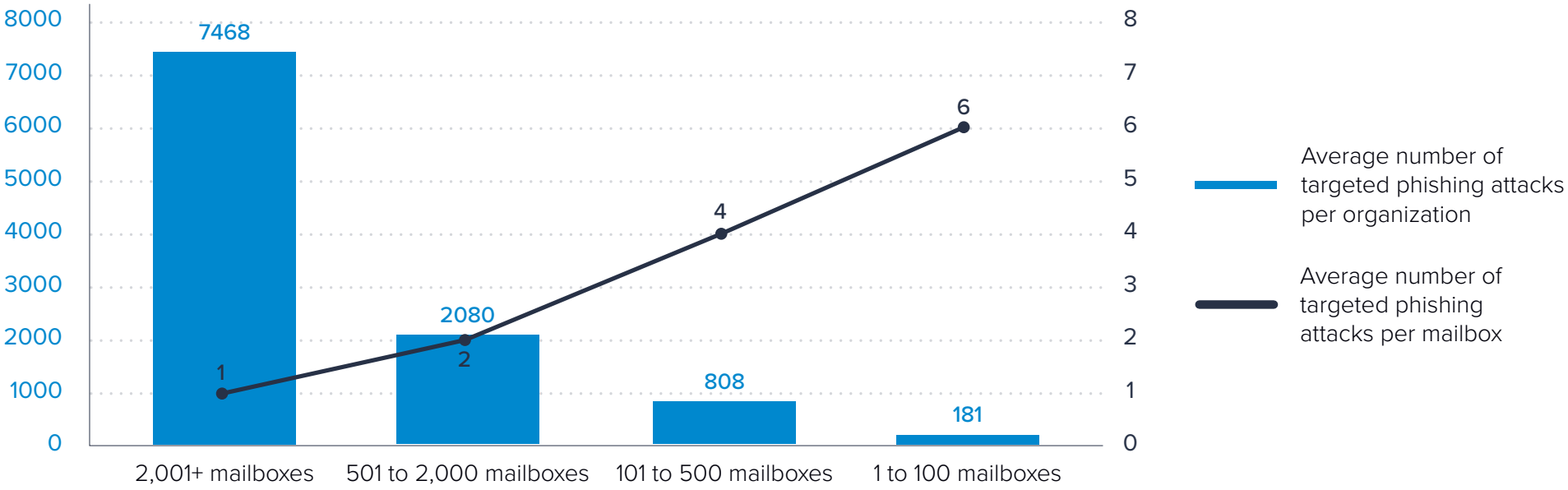
How company size affects email threat targeting

Barracuda researchers investigated whether a company's size affected the type and number of email threats that target it. They looked at the more advanced types of email attacks, including targeted phishing, business email compromise (BEC), and conversation hijacking.

The analysis was based on email threat detection data collected by our installed base of email protection solutions over a 12-month period.

When it comes to targeted phishing attacks, the total number of attacks was highest for the biggest companies and lowest for the smallest ones. However, on a per capita basis, the trend was reversed. At the smallest companies, each mailbox received an average of six attacks, while at the largest ones, the average was only one attack per mailbox.

Volume of targeted phishing threats affecting organizations (June 2023 to end May 2024)



"This disparity could be related to the different organizational structures and resourcing in companies of different sizes. For example, smaller companies tend to have flatter organizational structures with easier access to names or contact details. This could mean that attackers can target a wide range of employees.

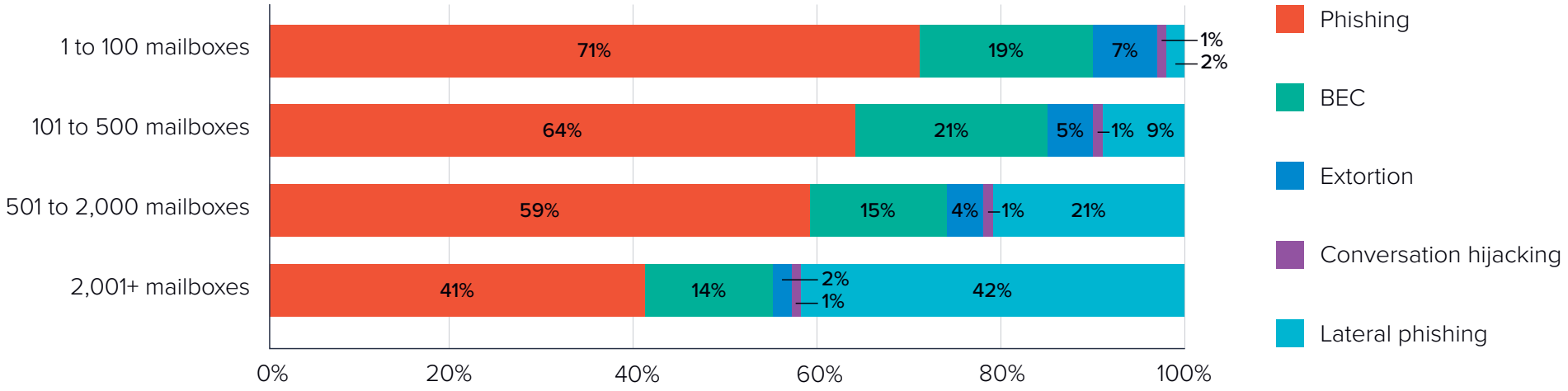
... At a larger organization, high-value, privileged accounts are usually concentrated among a few individual employees or company leaders. These users may often receive the bulk of the attacks, while many other mailboxes receive no inbound threats at all, bringing down the average."

Targeted attack profiles

BEC and conversation hijacking — sophisticated attacks that depend on the attackers already being inside the network and in control of at least one account — were found to be relatively equally distributed across companies of different sizes.

However, extortion and phishing attacks were found to be more common among smaller organizations, perhaps because they are less likely to have multilayered security that effectively detects and blocks phishing attempts.

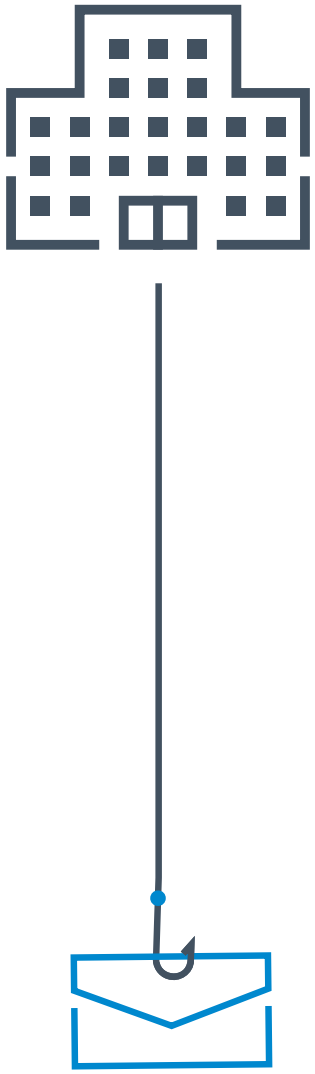
Type of targeted email threats affecting organizations (June 2023 to end May 2024)



Barracuda

Lateral phishing plagues larger companies

Another clear difference between larger and smaller companies is the prevalence of lateral phishing attacks. These are phishing attacks that originate from within an organization, usually coming from an already compromised account.



"The prevalence of account compromises among larger businesses may reflect the fact that credentials for many companies are likely already available for purchase on the dark web, making lateral phishing a straightforward attack. Larger companies are attractive targets for cybercriminals because they potentially offer a greater return on investment. These organizations often hold vast amounts of valuable sensitive, confidential, and financial data.

Larger companies present numerous exploitation opportunities for cybercriminals. With more mailboxes and employees, there are significantly more potential points of entry for attackers. Additionally, these organizations often have multiple communication channels, including distribution lists, which can rapidly disseminate malicious messages across the business, effectively hiding within the high volume of internal traffic."

Detailed analysis of evolving attacks

Barracuda researchers also looked at several well-known threat types and the ways adversaries are leveraging new technologies to adapt their tactics to make attacks more sophisticated.

Barracuda

Sextortion scams evolve to optimize results

Barracuda researchers examined the ways in which targeted sextortion scams have been evolving their tactics.

These are attacks in which the criminal attempts to extort money from victims under the threat of releasing explicit and embarrassing sexual images or videos.

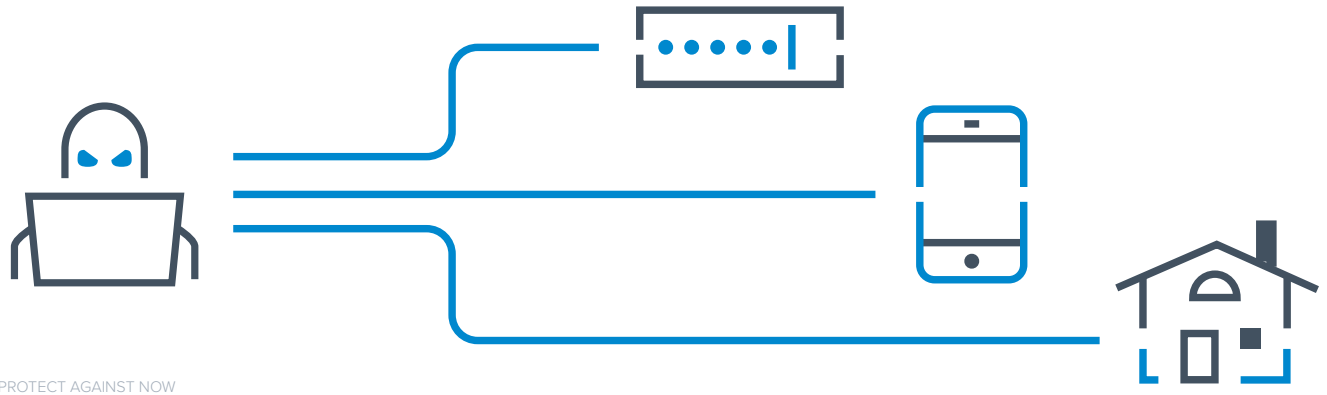
Criminals claim to have taken the compromising content from the victim's computer, and they use a variety of techniques to try to convince the victim that their claims and threats are real. Victims are often reluctant to report such attacks.

A focus on personalization using online info

The key advance that Barracuda researchers noted was the heavy leveraging of victims' personal data:

"Criminals are leveraging the personal data of targeted victims, including full names, telephone numbers, and addresses, to make their sextortion attempts more threatening and convincing. The sextortion emails address the victim by their first and last name, and the opening sentences of the email include the victim's telephone number, street address, and city.

In many cases, emails start with copy like this: 'I know that calling [telephone number] or visiting [street address] would be a better way to have a chat with you in case you don't cooperate. Don't even try to escape from this. You have no idea what I'm capable of in [city].'"



In addition, it is now very common for sextortion emails to include a Google Maps image of the target's location, whether at home or at work.

Extortion demands rising from hundreds to thousands

A few hundred dollars used to be the typical amount that sextortion crooks demanded. However, in the recent attacks that Barracuda researchers examined, the average amounts had risen to near $2,000.

Addition of QR code makes paying up easier

One key to an extortion scam is to make it as easy as possible for the victim to pay — possibly to ensure they're less likely to have second thoughts as they go through the process.

To this end, sextortion crooks have in some cases begun including a QR code that victims can scan to make their payment in bitcoin.

Average amount that sextortion crooks demanded in recent attacks

Barracuda

Possible testing

While many of the emails have nearly identical content (apart from personalization), some of them appear to be testing the effectiveness of specific variations.

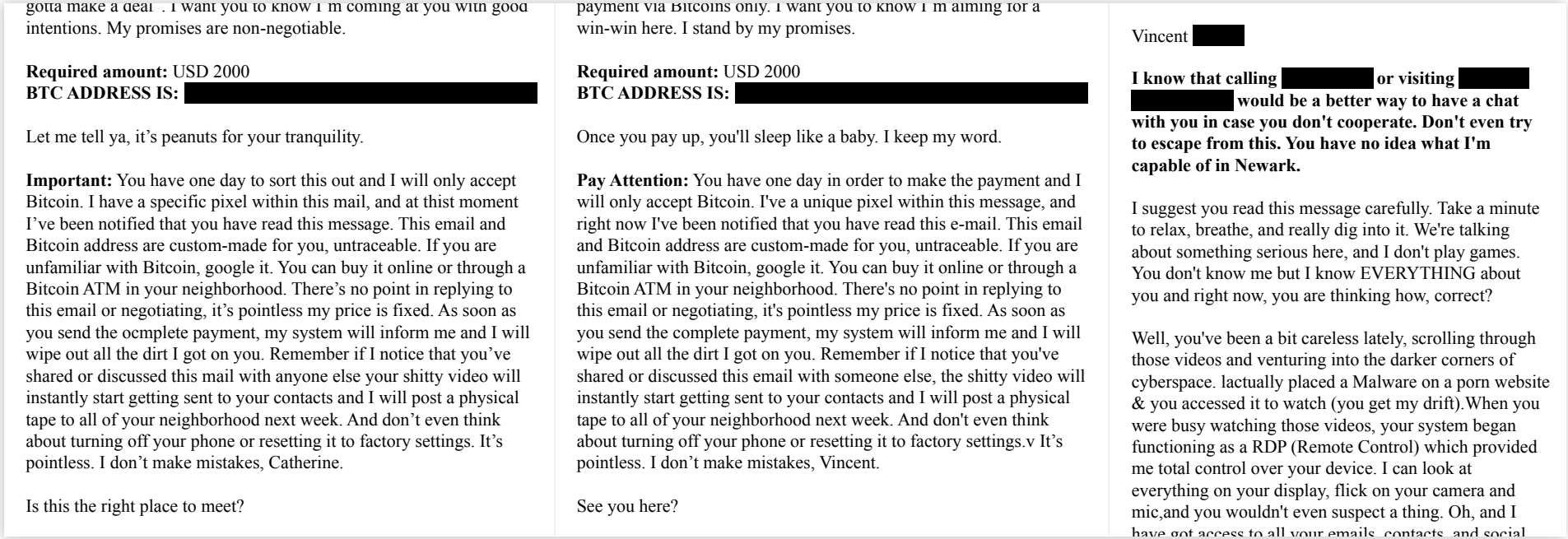
For example, several variations are being used in the line of copy that appears just before the Google Map image of the victim's address, including:

1. See you here?
2. Can you notice something here?
3. Is this the right place to meet?

Likewise, variations are being used in the line of copy that appears just below the bitcoin payment information, including:

- Once you pay up, you'll sleep like a baby. I keep my word.
- Let me tell ya, it's peanuts for your peace.
- Let me tell ya, it's peanuts for your tranquility.

These examples demonstrate how attackers are using this type of testing in their attacks:



gotta make a deal". I want you to know I'm coming at you with good intentions. My promises are non-negotiable.

Required amount: USD 2000
BTC ADDRESS IS: [redacted]

Let me tell ya, it's peanuts for your tranquility.

Important: You have one day to sort this out and I will only accept Bitcoin. I have a specific pixel within this mail, and at thist moment I've been notified that you have read this message. This email and Bitcoin address are custom-made for you, untraceable. If you are unfamiliar with Bitcoin, google it. You can buy it online or through a Bitcoin ATM in your neighborhood. There's no point in replying to this email or negotiating, it's pointless my price is fixed. As soon as you send the ocmplete payment, my system will inform me and I will wipe out all the dirt I got on you. Remember if I notice that you've shared or discussed this mail with anyone else your shitty video will instantly start getting sent to your contacts and I will post a physical tape to all of your neighborhood next week. And don't even think about turning off your phone or resetting it to factory settings. It's pointless. I don't make mistakes, Catherine.

Is this the right place to meet?

payment via Bitcoins only. I want you to know I'm aiming for a win-win here. I stand by my promises.

Required amount: USD 2000
BTC ADDRESS IS: [redacted]

Once you pay up, you'll sleep like a baby. I keep my word.

Pay Attention: You have one day in order to make the payment and I will only accept Bitcoin. I've a unique pixel within this message, and right now I've been notified that you have read this e-mail. This email and Bitcoin address are custom-made for you, untraceable. If you are unfamiliar with Bitcoin, google it. You can buy it online or through a Bitcoin ATM in your neighborhood. There's no point in replying to this email or negotiating, it's pointless my price is fixed. As soon as you send the complete payment, my system will inform me and I will wipe out all the dirt I got on you. Remember if I notice that you've shared or discussed this email with someone else, the shitty video will instantly start getting sent to your contacts and I will post a physical tape to all of your neighborhood next week. And don't even think about turning off your phone or resetting it to factory settings.v It's pointless. I don't make mistakes, Vincent.

See you here?

Vincent [redacted]

I know that calling [redacted] or visiting [redacted] would be a better way to have a chat with you in case you don't cooperate. Don't even try to escape from this. You have no idea what I'm capable of in Newark.

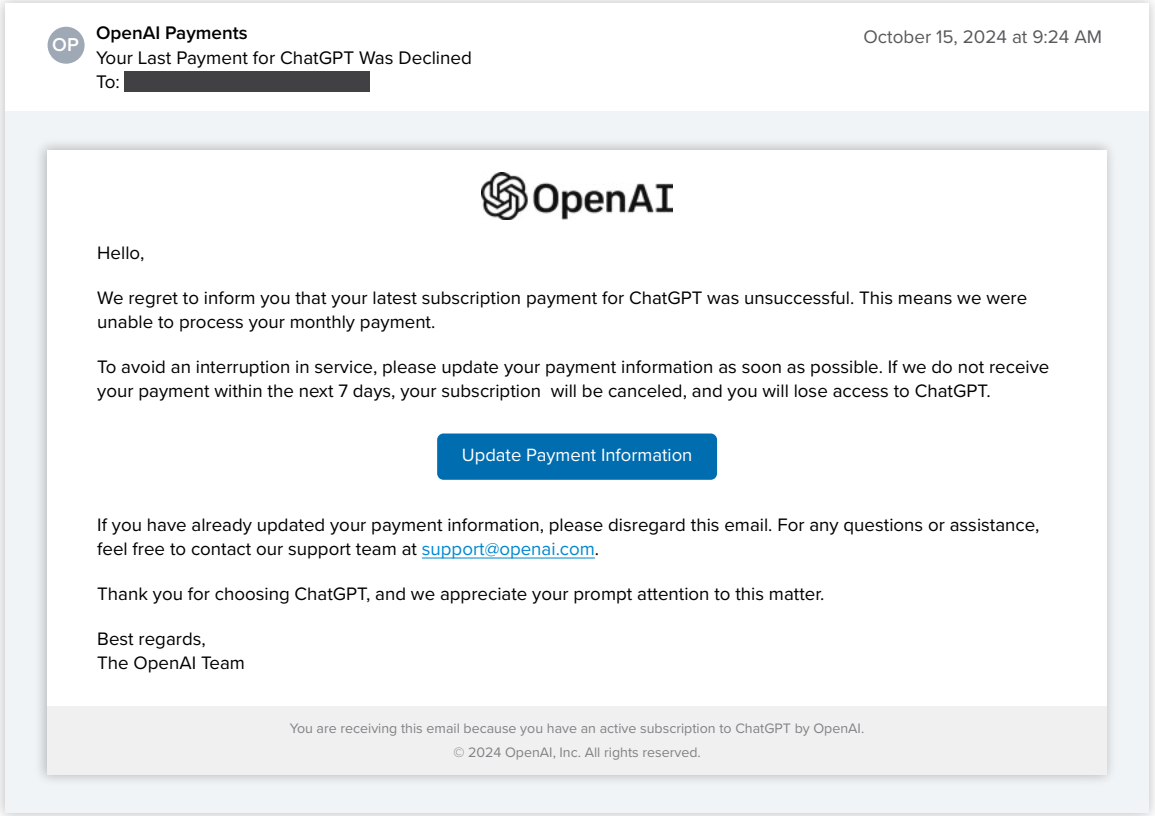
I suggest you read this message carefully. Take a minute to relax, breathe, and really dig into it. We're talking about something serious here, and I don't play games. You don't know me but I know EVERYTHING about you and right now, you are thinking how, correct?

Well, you've been a bit careless lately, scrolling through those videos and venturing into the darker corners of cyberspace. lactually placed a Malware on a porn website & you accessed it to watch (you get my drift).When you were busy watching those videos, your system began functioning as a RDP (Remote Control) which provided me total control over your device. I can look at everything on your display, flick on your camera and mic,and you wouldn't even suspect a thing. Oh, and I have got access to all your emails, contacts, and social

Phishing crooks impersonate Open AI to launch attacks

Barracuda researchers uncovered a large-scale impersonation campaign. Combining well-known and familiar tactics with techniques to exploit the exploding global interest in generative AI tools, the attack impersonated OpenAI — the company behind ChatGPT — with an urgent message requesting updated payment information to avoid the cancellation of a monthly subscription.

"This phishing attack included a suspicious sender domain, an email address designed to mimic legitimacy, and a sense of urgency in the message. The email closely resembled legitimate communication from OpenAI but relied on an obfuscated hyperlink, and the actual URL differed from one email to another."



OP **OpenAI Payments** October 15, 2024 at 9:24 AM
Your Last Payment for ChatGPT Was Declined
To: [redacted]

OpenAI

Hello,

We regret to inform you that your latest subscription payment for ChatGPT was unsuccessful. This means we were unable to process your monthly payment.

To avoid an interruption in service, please update your payment information as soon as possible. If we do not receive your payment within the next 7 days, your subscription will be canceled, and you will lose access to ChatGPT.

Update Payment Information

If you have already updated your payment information, please disregard this email. For any questions or assistance, feel free to contact our support team at support@openai.com.

Thank you for choosing ChatGPT, and we appreciate your prompt attention to this matter.

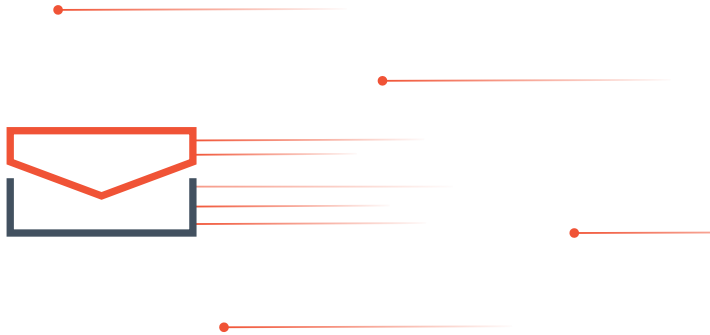
Best regards,
The OpenAI Team

You are receiving this email because you have an active subscription to ChatGPT by OpenAI.
© 2024 OpenAI, Inc. All rights reserved.

Barracuda

Key elements of the attack — tactics and giveaways

When our researchers analyzed the OpenAI impersonation attack, they found that the volume of emails sent was significant, but the lack of sophistication was surprising. The attack was sent from a single domain to over 1,000 recipients. The email used different hyperlinks within the email body, possibly to evade detection.



Here is a list of high-level attributes from the email that break down the phishing characteristics:

1. Sender's email address

   The email is from info@mta.topmarinelogistics.com, which does not match the official OpenAI domain (e.g., @openai.com). This is a significant red flag.

2. DKIM and SPF records

   The email passed domain keys identified mail (DKIM) and sender policy framework (SPF) checks, two common email authentication methods, which means that the email was sent from a server authorized to send emails on behalf of the domain. However, the domain itself is suspicious.

3. Content and language

   The language used in the email is typical of phishing attempts, urging immediate action and creating a sense of urgency. Legitimate companies usually do not pressure users in this manner.

4. Contact information

   The email provides a recognizable support email (support@openai.com), adding legitimacy to the overall message. However, the overall context and sender's address undermine its credibility.

Advanced infostealer attacks broad range of data and files

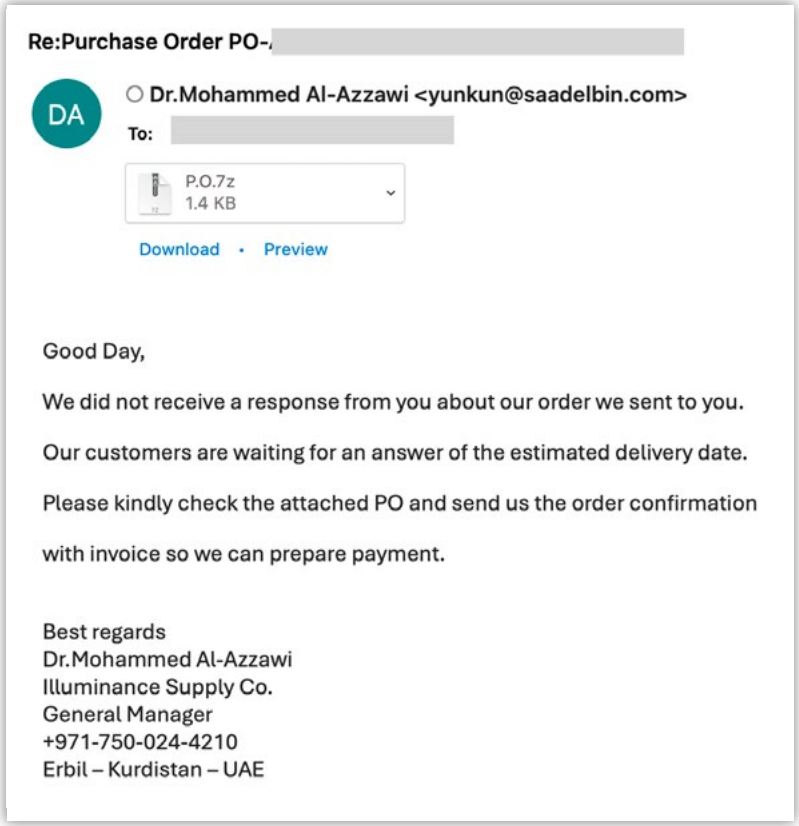
Barracuda researchers also detected a group of phishing attacks that featured an advanced, stealthy technique designed to exfiltrate a broad range of sensitive information using a sophisticated infostealer malware.

While most infostealers observed in the past focused on stealing saved browser passwords and sometimes cryptocurrency wallets, this one tried to collect PDF files and directories from most folders, as well as browser information such as session cookies, saved credit card details, bitcoin-related extensions, web history, and more, and to then transmit them to a remote email account as a zipped attachment.

Step by step analysis — from initial phish to data exfiltration

Step 1: The phishing email

The attack begins with a phishing email encouraging the recipient to open an attached purchase order. The email includes several basic grammatical errors.

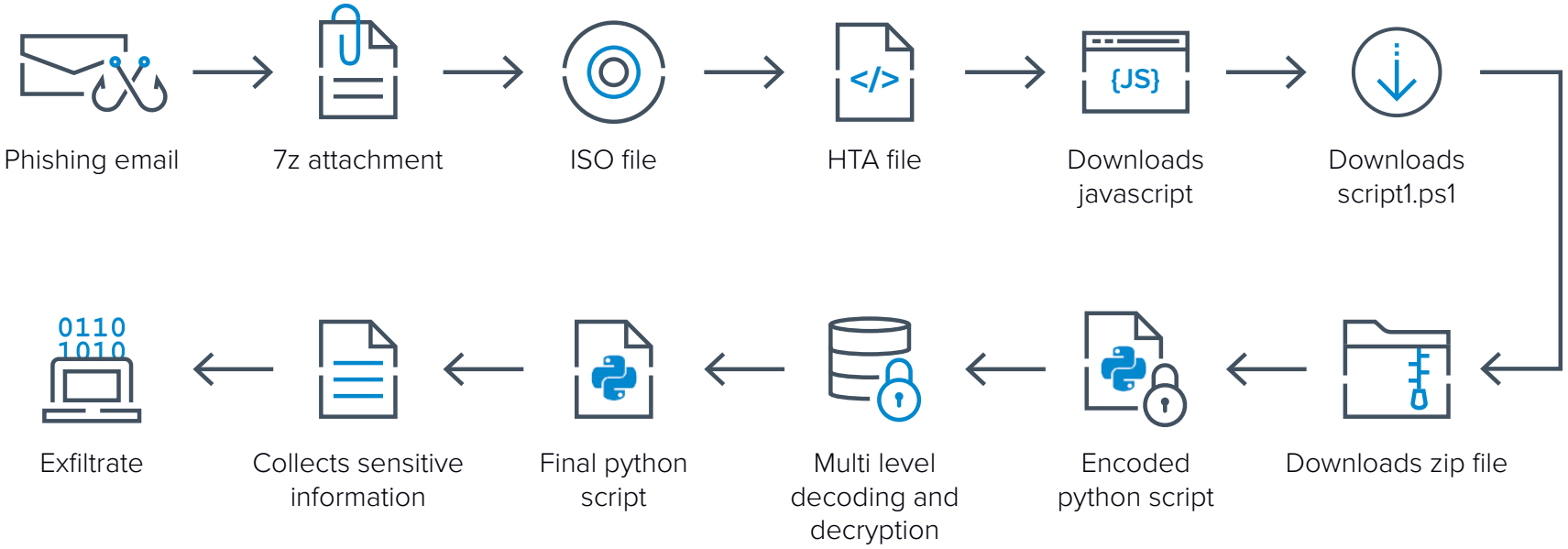


All the emails appear to be sent from the same address and the company name and contact details appear to be fictitious.

The attachment contains an archive file with an HTML application file hidden within it. Upon running this file, a series of malicious payloads are downloaded and executed.

Step 2: The malicious payloads

The file downloads and executes a number of different files to the compromised account from a remote server, with each file in turn downloading the next one.



The last one executes the infostealer malware. The file then 'sleeps' for three seconds, after which it kills and deletes all the other files before deleting itself.

The scripts are obfuscated and encrypted, making it harder for security analysts to reverse engineer the threat.

Step 3: The data exfiltration

Most phishing attacks are associated with data theft, where the attackers are looking to steal credentials, financial account details and more. Data exfiltration is also a type of theft, but it is more often associated with ransomware and the active removal of information from the network, often in significant volumes by means of tools and exploits.

In these attacks, we are looking at data exfiltration, executed by a sophisticated infostealer malware that is designed to collect and exfiltrate a wider range of information than typical infostealers.

The capabilities of the infostealer used in this attack include:

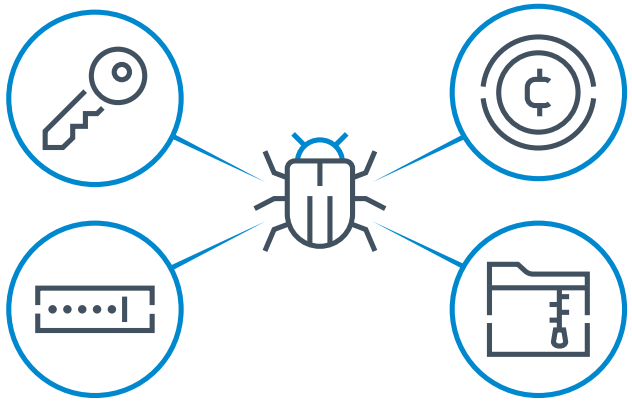
Collecting browser information

- The malware is designed to kill browser processes and collect their MasterKeys for Chrome, Edge, Yandex, and Brave.
- It can collect session cookies from the browser directories, saved passwords from web browsers, saved credit card information, web and download history, and autofill information.
- It can also copy any bitcoin-related browser extension folders, including MetaMask, BNB Chain Wallet, Coinbase Wallet, and Ronin Wallet.

Collecting files

- The infostealer tries to collect PDF files located in the following folders: Desktop, Downloads, Documents, and the ‘Recent’ folder in %AppData% and %Temp%\Browser.
- It can copy and ZIP entire directories, including %AppData%\Zcash, %AppData%\Armory, and any gaming folders.

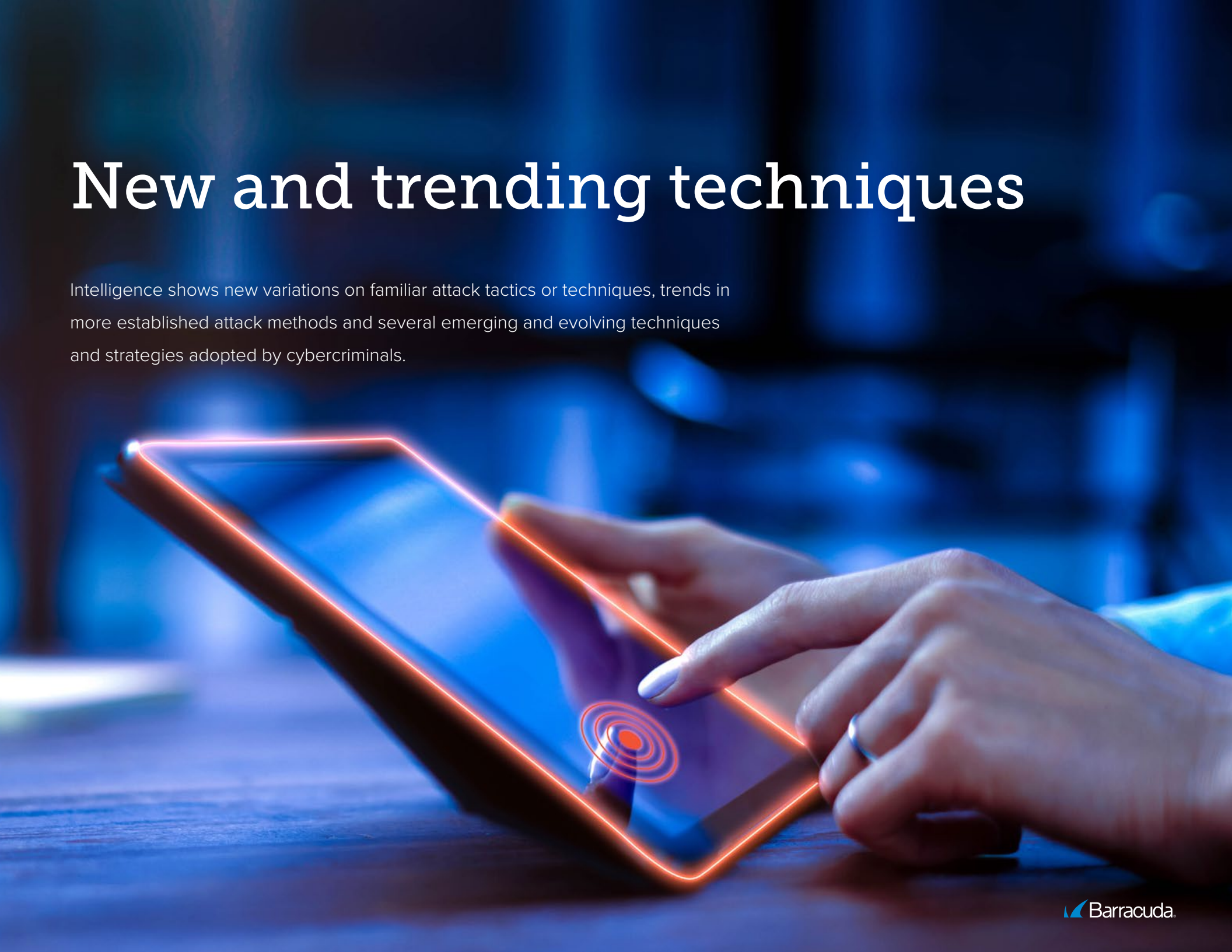
The amount of information collected is extensive and sensitive. The stolen saved passwords and cookies could help an attacker to move laterally in the organization, while credit card information and bitcoin wallet information could be used to steal money.



Barracuda

New and trending techniques

Intelligence shows new variations on familiar attack tactics or techniques, trends in more established attack methods and several emerging and evolving techniques and strategies adopted by cybercriminals.



Barracuda

Growth and evolution of QR code attacks

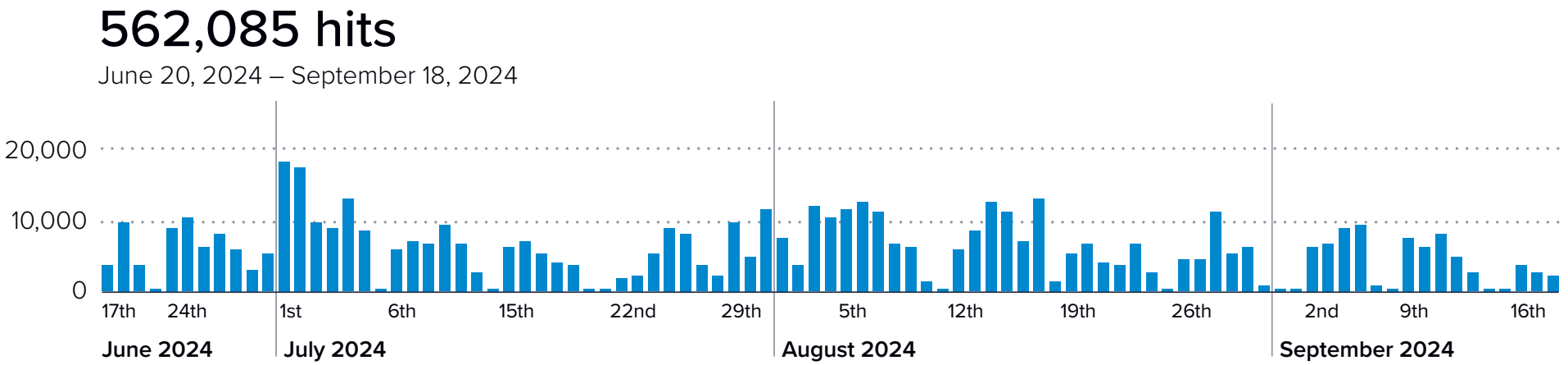
QR codes have been around for a while, and "quishing" attacks, in which criminals try to trick victims into scanning malicious QR codes, are not entirely new, but they are growing more numerous and significant. And they are using increasingly sophisticated techniques to evade detection.

One thing that makes these attacks difficult to guard against is that the target may receive the quishing email on their computer, but then they scan the QR code using their phone, which may have less robust security.

Half a million PDF-based QR code attacks

In the past, malicious QR codes were typically embedded in the body of a phishing email. But more recently, attackers have shifted to embedding the QR code into a PDF document that is attached to the phishing email. Barracuda detected more than half a million such attacks in just a three-month period.

Number of phishing emails with QR codes embedded in PDF documents

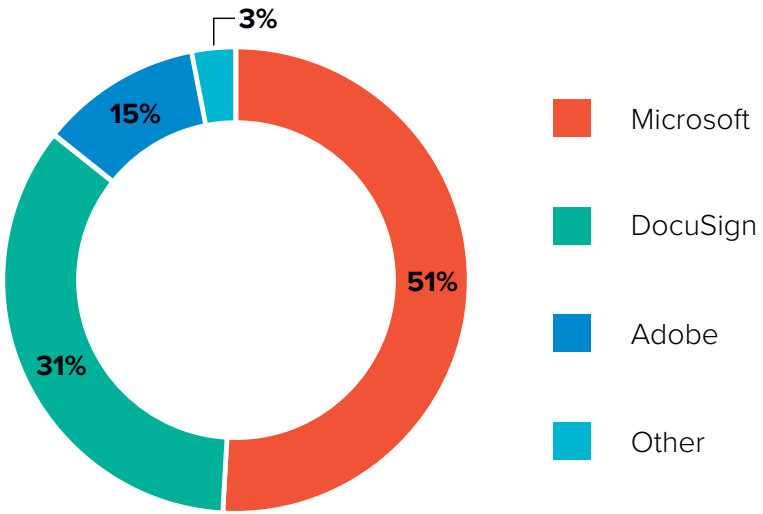


Barracuda

Attacks impersonate trusted brands

These emails mainly impersonated well known and trusted brands. 97% of them claimed to be from Microsoft (51%), DocuSign (31%) or Adobe (15%).

Brands being impersonated in QR code attacks



Even users with strong security awareness might fall victim when the attack appears to come from trusted brands with which they interact on a daily basis.

Phishing with text-based QR codes and specially crafted URLs

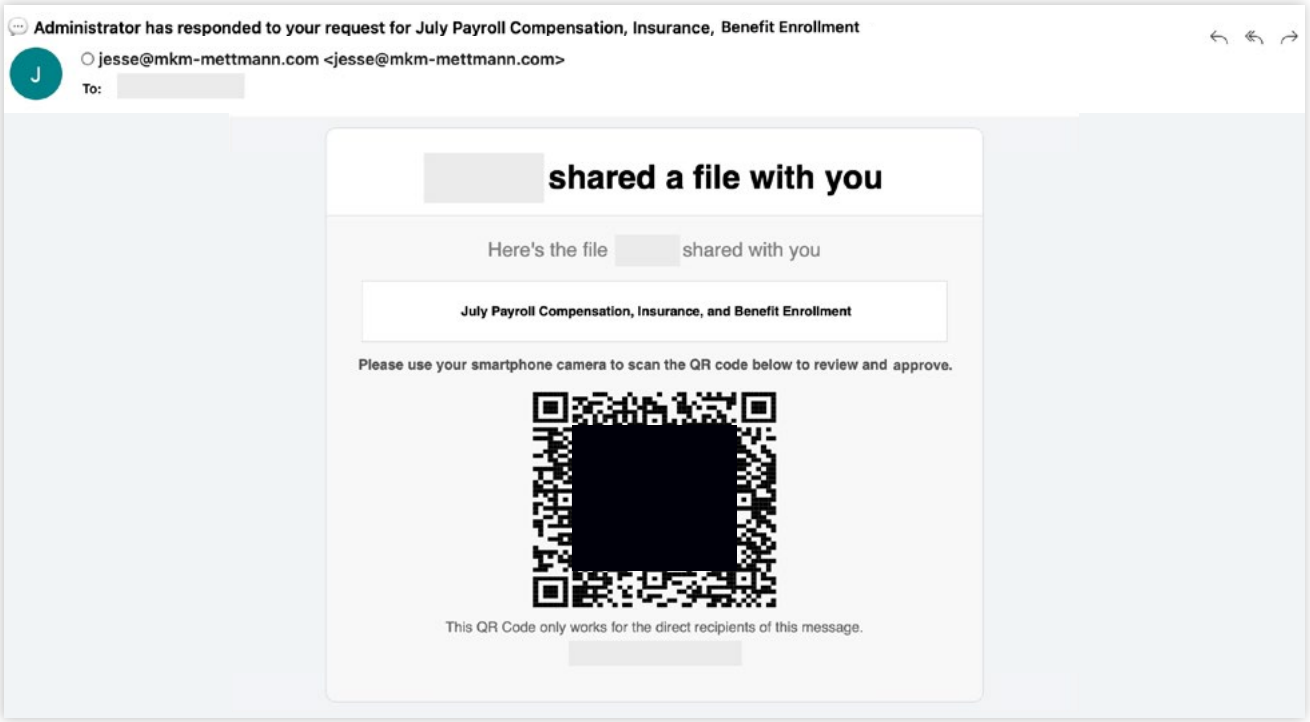
Barracuda researchers also examined two novel evasive techniques that were recently detected by Barracuda systems.

Text (ASCII)-based QR codes

As security tools adapt to the threat of QR codes, attackers evolve their approaches.

In 2024, Barracuda noted that attackers were adapting their techniques to try to evade tools such as optical character recognition (OCR) scanning, which is designed to extract, check for and block malicious URLs in QR codes.

The researchers identified a new generation of QR code phishing, where the QR code 'image' is created out of text-based ASCII/ Unicode characters. In an email, it will look like a traditional QR code. To a typical OCR detection system, it appears meaningless.

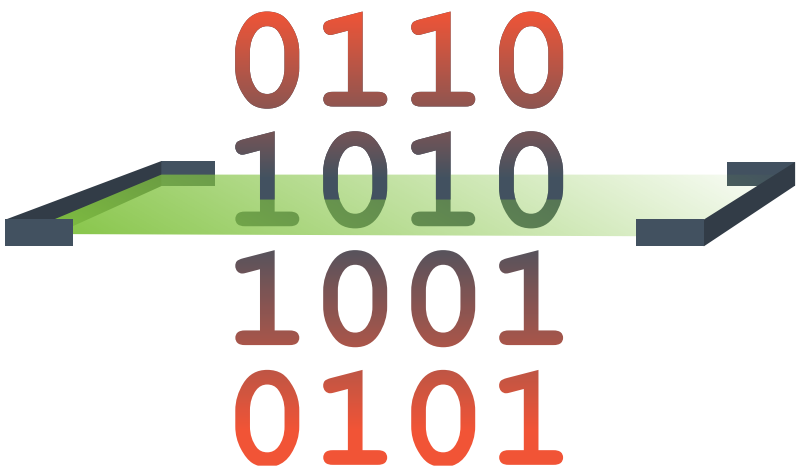


Because there are a wide variety of ways to use Unicode or ASCII character sets to build a QR code, it can be challenging to detect threats.

Barracuda recommends that if security technologies flag the potential use of ASCII QR code in a phishing attack, the easiest option is to take a screen shot of the phishing email and pass it to an OCR engine to read the URL behind the QR code.

Blob URLs used to evade detection focused on external traffic

Another novel evasive technique discovered by Barracuda researchers was the use of Blob URLs.



"A Blob URL (also known as an Object URL) is used by browsers to represent binary data or file-like objects (called Blobs) that are temporarily held in the browser's memory.
Blob URIs allow web developers to work with binary data like images, videos, or files directly within the browser, without having to send or retrieve it from an external server.

Because Blob URLs don't load data from external URLs, traditional URL filtering and scanning tools may not initially recognize the content as malicious."

Attacks using Blob URLs have so far mostly impersonated large, trusted companies — a tried and true social engineering technique.

Barracuda

Protecting your business

The cybersecurity landscape in 2025 is as complex and challenging as ever. At Barracuda, we don't just analyze and report on the latest threats. Our development teams work closely with researchers to respond promptly to them, with innovative technologies, strategies, and capabilities designed to shut down the newest attacks before they can gain a foothold in our customers' networks.

No matter what the year brings, the basic requirements of robust security remain the same:

- **Promote a culture of security throughout your organization.** This includes using a security awareness training solution that engages users, promotes good habits, and bases lessons and simulations on up-to-date threat data.
- **Email security is critical**, as that's how most attacks are launched. Look for an email security platform that seamlessly integrates a wide variety of capabilities — including advanced threat protection, AI-based impersonation protection, cloud-based backup and archiving, automated incident response, and more — and is backed up by a vendor committed to continuous improvement.
- **Modern backup capabilities** — including end-to-end encryption, immutable redundant backups, granular restore, and more — are critical to building resiliency and to ensuring swift recovery from ransomware and other attacks.
- **Ensure your devices, apps and software are always updated** — cybercriminals are constantly looking for unpatched vulnerabilities and will take advantage of any they find. Your app and API security solution should be capable of automatically patching and updating when needed. And it should include powerful bot protection capabilities and DDoS protection.
- **Robust application security.** Install advanced application protection to protect web applications and APIs and make sure it is properly configured with rate limiting and monitoring in place.

To discuss your specific security needs and how to address them, contact Barracuda or your managed security provider. Visit barracuda.com to explore our comprehensive platform, and get help now.

About Barracuda

Barracuda is a leading cybersecurity company providing complete protection against complex threats. Our platform protects email, data, applications, and networks with innovative solutions, and a managed XDR service, to strengthen cyber resilience. Hundreds of thousands of IT professionals and managed service providers worldwide trust us to protect and support them with solutions that are easy to buy, deploy, and use. For more information, visit barracuda.com.