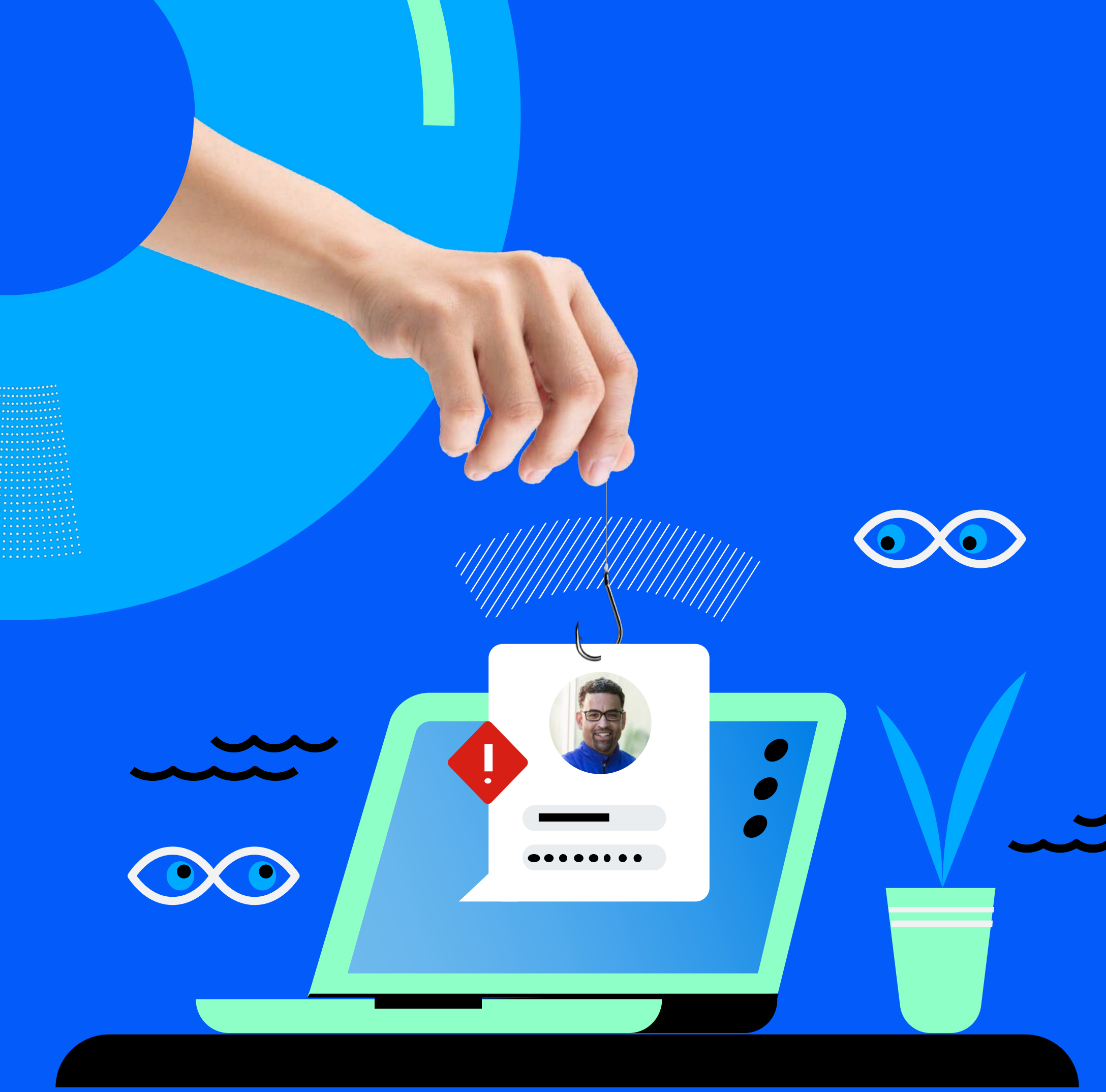


# THE Human Factor 2025

VOL. 2 | **PHISHING AND URL-BASED THREATS**

proofpoint®

# Introduction

Attacks that target people are all about hacking human nature. As we saw in our first report, one of the ways that cybercriminals accomplish this is through pure social engineering. This means they might pretend to be a person's colleague and have seemingly innocent conversations or tell believable stories. They don't rely on a malicious payload.

But social engineering isn't always so cut and dried. While it's a component of the overwhelming majority of cyberattacks today, pure social engineering isn't as widespread as other types of threats, like malicious URLs. With these threats, cybercriminals send URLs to people and use social engineering tactics to trick them into opening those links and initiating a wider attack.

Whether their goal is to launch a phishing attack and steal credentials or direct users to malware-laden websites and unleash ransomware, cybercriminals count URL-based threats as one of their primary, go-to tactics.

Many of today's most targeted URL-based threats are well researched, expertly crafted and too psychologically potent to resist. These threats are particularly insidious because they bear little resemblance to what people have come to expect. At first glance, some look innocuous because they're generated using legitimate file sharing services, such as Microsoft OneDrive. Others take people to malicious websites that look incredibly real thanks to AI tools.

How are people holding up against this onslaught? To answer this question, we looked at data from our own Proofpoint Nexus® threat intelligence platform to understand the scale of the challenges that organizations face in addressing these threats.

# Key findings

## 4x

**URLs are used 4x more often** in malicious emails than in attachments[1]

## 55%

**At least 55% of suspected SMS** phishing ("smishing") messages contained malicious URLs

## 400%

ClickFix **URL-based malware campaigns increased** nearly 400% year over year

## 34%

Approximately 34% of URL-based malware campaigns **delivered remote access software**

## 4.2M

There were **4.2 million QR code threats** identified by Proofpoint in the first half of 2025

1. Observed by Proofpoint in data from October 2024 to May 2025.

# **About** this report

Historically, the *Human Factor* report has been a comprehensive look at the human-centric threats that Proofpoint has detected, mitigated and resolved in the previous 12 months. This year, we are changing the format. Rather than bringing all our insights into a single report, we're breaking them up into a multipart series.

While each volume will explore one category of threats, they will all share the same theme: new developments in the threat landscape and how technology and psychology are combining to make modern cyberattacks so dangerous.

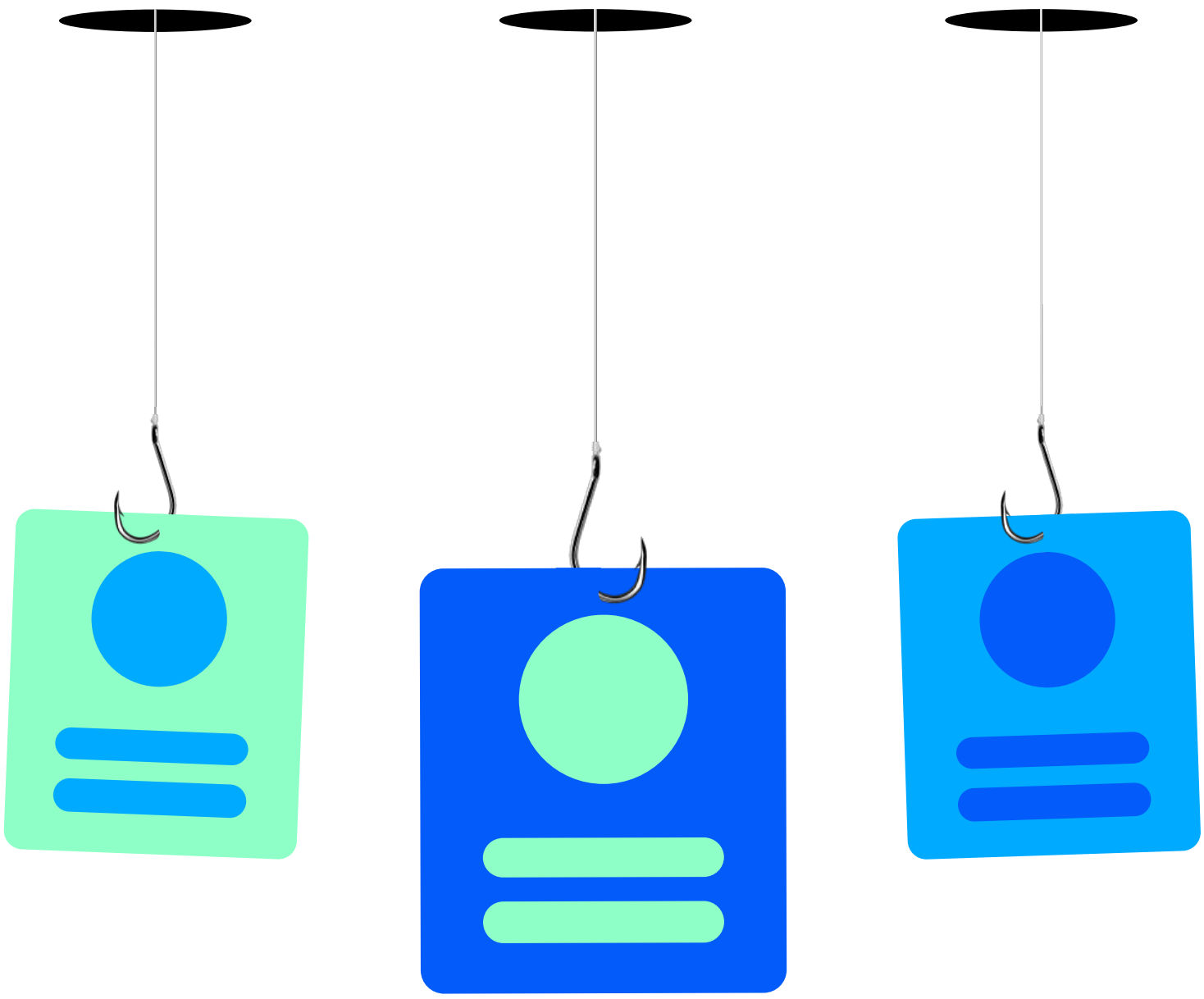
**Scope:**

This report draws on data collected from Proofpoint deployments around the world: one of the largest, most diverse data sets in cybersecurity.

Every year, we analyze more than **3.4 trillion** email messages, **21 trillion** URLs, **800 billion** attachments, **1.4 trillion** suspicious SMS messages and more. Data is pulled from across all the digital channels that matter.

*It covers May 1, 2024–May. 1, 2025.*[2]

2. When campaign data is referenced, it should be understood as a timebound set of related activity that's analyzed and contextualized by threat researchers. Campaigns represent a subset of threat data.



# **Phishing** trends

Part of the reason that cybercriminals innovate so quickly is because people are constantly catching on to their scams. Over the past 12 months, much of the development seen in phishing and URL-based threats can be viewed as a response to this constant game of wits between defenders and attackers, with attacks growing ever more subtle.

Fake login pages, malicious URLs and attachments, and compromised brand assets look so legitimate that they easily slip past people's psychological defenses when security measures don't keep them safe. And with AI tools like large language models (LLMs) being used to generate many of these lures, threat actors can iterate almost endlessly until they hit on something that works.

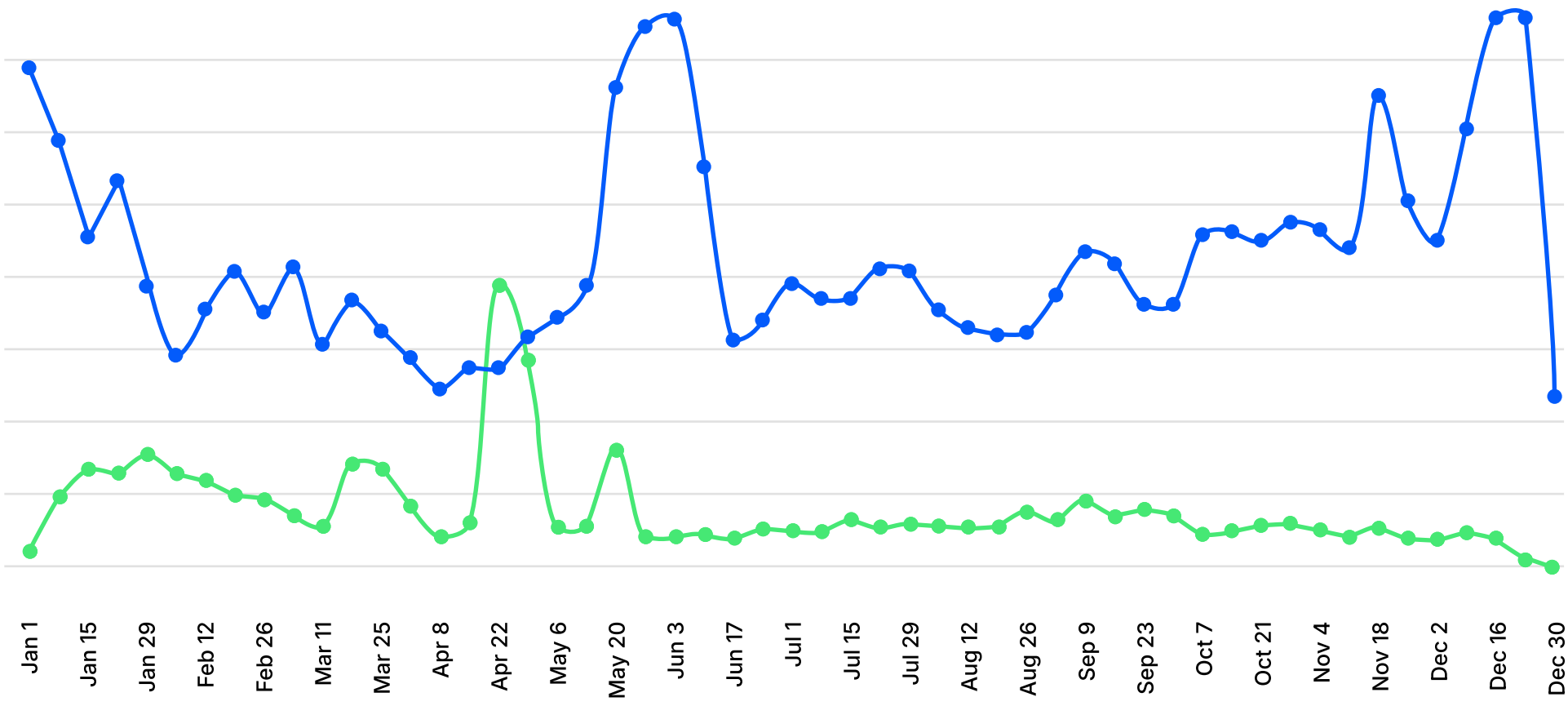
# URLs vs. attachments

The gap between URLs and attachments for threat delivery has continued to grow in opposite directions over the past few years, with the volume of URLs far outweighing the volume of attachments.

Over a six-month period in 2024–2025, our researchers observed URL threats four times more often than attachments. Campaign data in this report only accounts for email threats with malicious URLs. It does not account for how many hybrid threats we see.

**Hybrid threats are emails that contain an attachment, like a Word document or PDF, with a URL inside. Typically, those URLs lead to either a credential phishing page or a malware payload.**

**Global URL vs. attachment threats 2024**




URLs were most commonly delivered in email as a direct link within the body text or as hyperlinked text. They were also embedded in “View Document” or “Click to View” buttons. Common attachment types delivering URLs include Word documents, PDFs, ISOs and HTML files.

# Credential harvesting vs. malware

It's important to remember that URLs are just one tool that cybercriminals use to achieve their overarching objectives. Attackers want to steal credentials as part of a larger effort at taking over accounts and burrowing into networks. They are also aiming to deliver malware via URLs, which could lead to follow-on payloads such as ransomware.

Over a six-month period, our researchers observed approximately 3.7 billion URL-based threats leveraged in attempts to steal credentials (or other sensitive information). Notably, only 8.3 million of those threats were intended to deliver malware.

The numbers speak for themselves: at over four times the volume of malware, phishing for "creds" is by far the most common attack.

# The more you know

Today's phishing and malicious URLs are more underhanded and effective than ever.

### Extremely common

Most phishing threats are delivered through malicious URLs.

### Highly targeted

URLs can be customized with filtering based on location or host data to ensure only the designated target is served malicious content.

### Appear legitimate

Malicious URLs can be indistinguishable from harmless ones. Threat actors commonly abuse services such as Microsoft, Dropbox or Google Drive to increase their chances of engagement.

### An entry point

When users click on phishing URLs, it's often just the start of a much bigger attack chain that leads to account takeover, unauthorized system access and control, data breach and exfiltration, ransomware and more.

### Easy to share

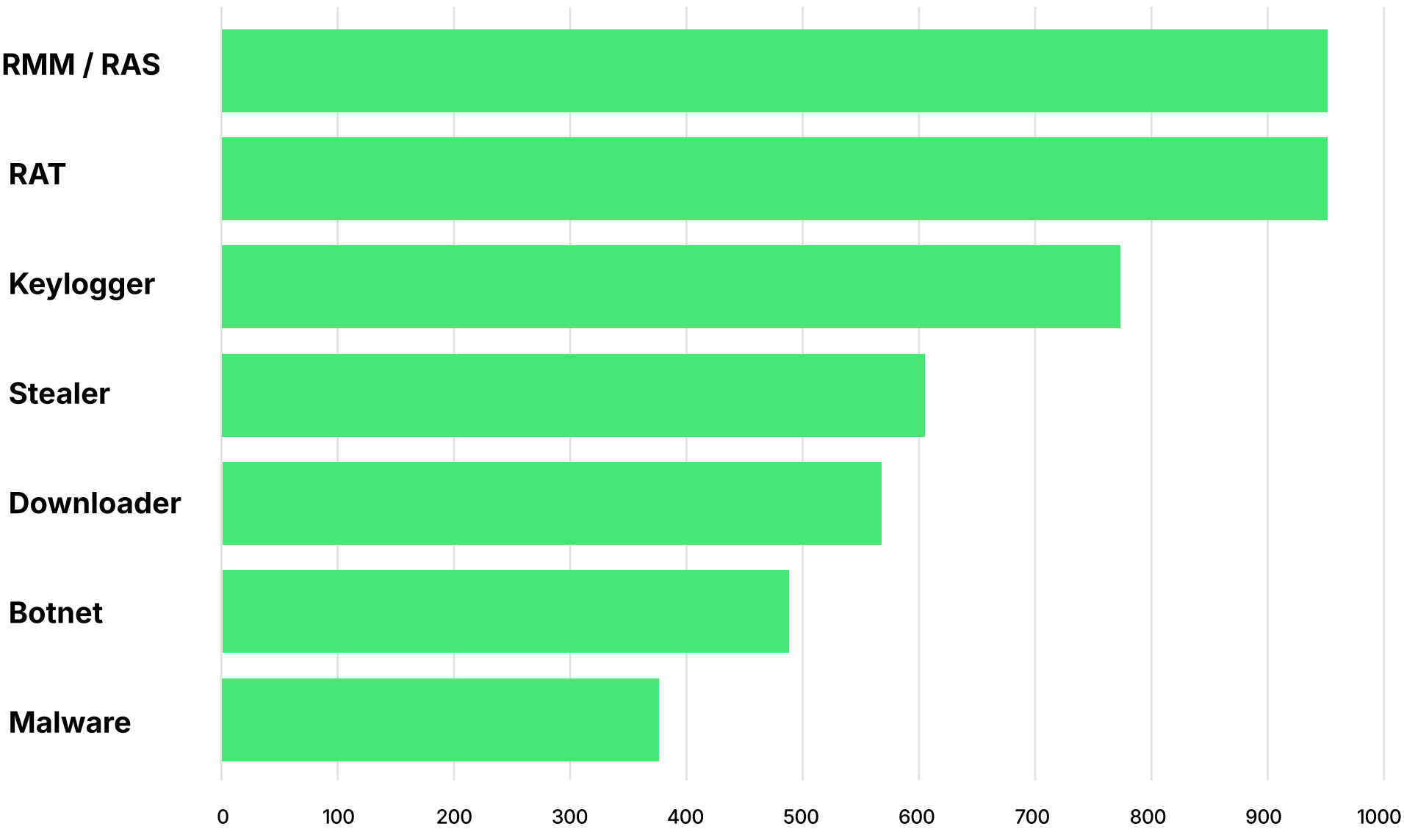
Malicious URLs are not just email threats—it's very common to receive these links via SMS as well as across tools such as Microsoft Teams, LinkedIn, Google Drive and more.

# Top malware families

Remote monitoring and management (RMM) tools and remote access software (RAS) were the most frequently observed payloads in URL-based campaigns from the second half of our reporting period. Approximately 34% of URL-based phishing campaigns delivered this payload in individual campaigns.

Remote management tools are legitimate software commonly used by IT teams. Unfortunately, they've also been adopted by threat actors to gain control of the victim's endpoints and download additional malicious software. RMMs can be used for data collection, financial fraud, lateral movement, and to install follow-on malware like ransomware.

**Campaigns by malware family**




**Note:** Some campaigns involve multiple types of malware, making it difficult to classify them into a single family. For example, if a malware functions as both a "stealer" and a "keylogger," it is counted in both categories. As a result, the graph includes more data points than the actual number of distinct campaigns.

# Popular and notable tactics

In this section, we examine specific URL-based phishing and malware tactics used by threat actors during the last 12 months. Some of these campaigns are noteworthy because of their sheer volume, while others display impressive ingenuity.

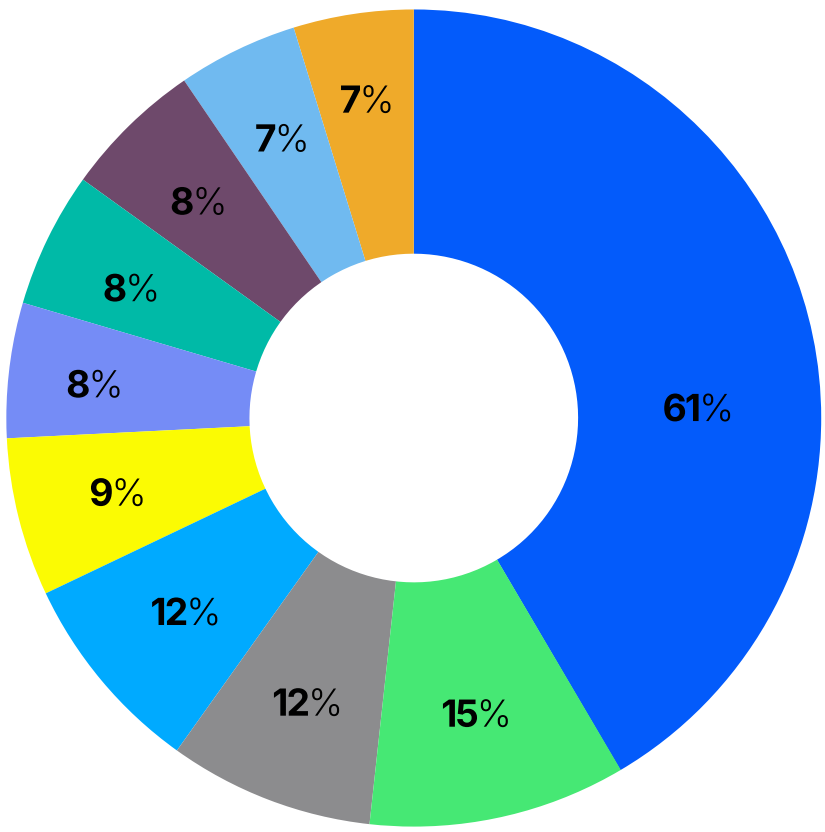
## Phishing for credentials

Cybercriminals want to be invisible and unnoticed. In account takeovers (ATOs), they use phishing attacks to steal an individual's account credentials and effectively become that person—as far as the systems that they have access to are concerned. Attackers are then free to perpetrate malware attacks, steal data with impunity, and launch additional phishing threats to expand their reach.

Our research shows that some of the URL-based credential phishing campaigns with the highest volumes in the past 12 months have been facilitated by "phish kits" like CoGUI and Darcula. Phish kits are off-the-shelf tools that enable even non-technical criminals to spin up phishing campaigns. Many kits are even capable of intercepting multifactor (MFA) authentication codes. By removing technical barriers of entry, these types of kits have significantly contributed to the rise in phishing seen over the last several years.

CoGUI is primarily used by Chinese-speaking threat actors. Campaigns are typically high-volume, with message counts ranging from hundreds of thousands to tens of millions per campaign. These campaigns include malicious URLs that, when clicked, typically lead to credential phishing websites. To avoid being detected by automated browsing systems and sandboxes, they use geofencing, headers fencing and fingerprinting. Before directing users to the final objective, victims are profiled to ensure they are located within the targeted region, which is typically Japan.

CoGUI has been observed in the threat landscape since at least October 2024 and has been tracked by Proofpoint since December 2024. Most of the observed campaigns abuse popular consumer or payment brands in phishing lures to appear more convincing to users.




**Top 10 impersonated brands in campaigns**

| | |
|---|---|
| Amazon | 61 |
| PayPay | 15 |
| MyJCB | 12 |
| Apple | 12 |
| Orico | 9 |
| Rakuten | 8 |
| SMBC | 8 |
| Saison Card | 8 |
| UC Card | 7 |
| Aeon Card | 7 |

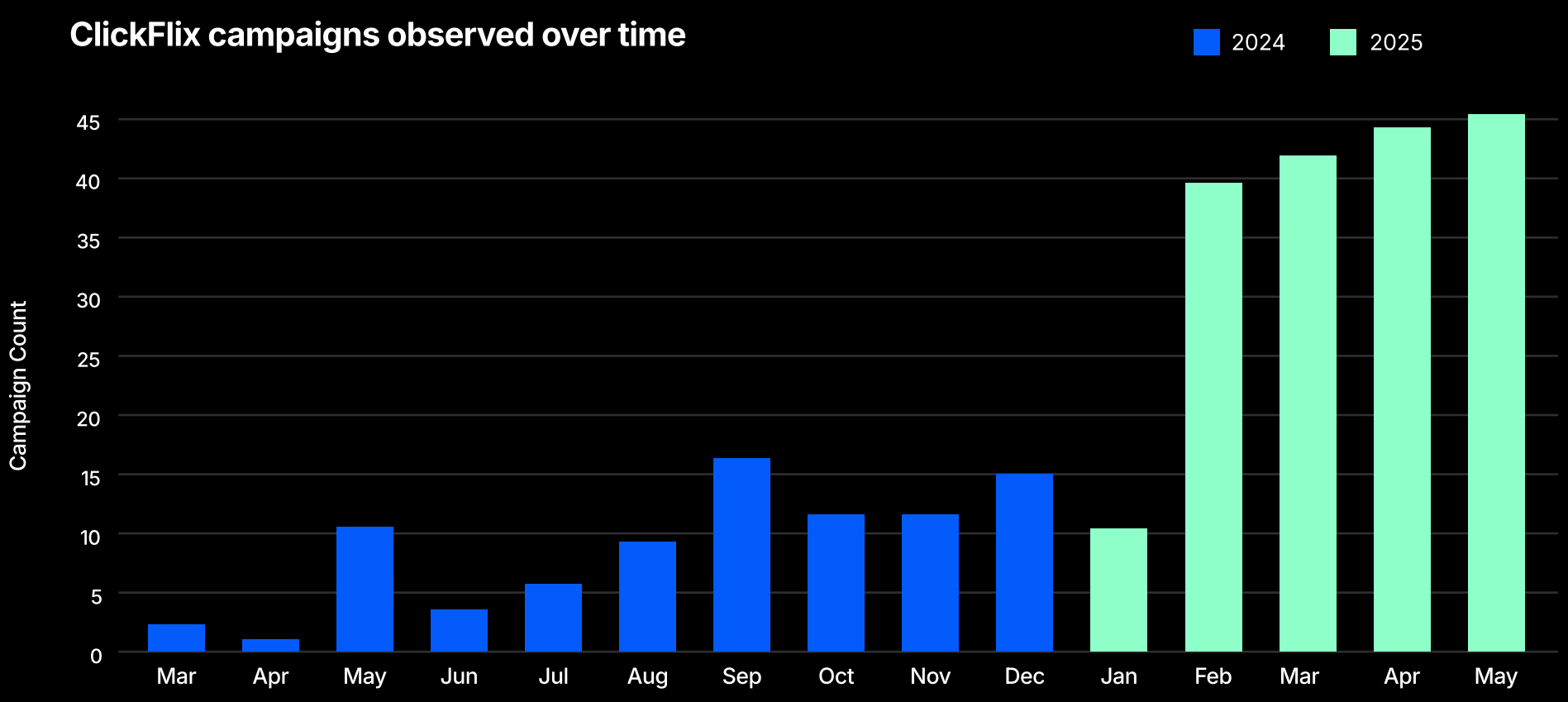
Count of top brands spoofed in CoGUI campaigns, December 2024 through April 2025.

Darcula, another popular phish kit with many similarities to GoGUI, is primarily used in smishing campaigns. Since early 2025, it has been most frequently observed in smishing campaigns that impersonate government entities, such as road toll scams. It operates similarly to CoGUI, as described above, and is used to steal PII and credit card information.

# Faking a fix

One of the past year's standout URL-based threats has been ClickFix. First observed in early 2024, this unique phishing technique has exploded like a viral trend and has been embraced by bad actors across genres, whether they're operating in support of nation-state objectives or motivated by financial gain.

ClickFix campaign volumes have increased by nearly 400% year over year, making it one of the most common URL-based techniques used by malware threat actors.




Benign conversations versus malicious campaigns observed over one year.

This exponential growth can at least partly be explained by how well these campaigns use social engineering to tap into people's impulse to quickly resolve their own technical issues. Typically, users are directed to a malicious URL or file by a phishing lure. When they click on the link to open a document or webpage, they see a dialog box containing an error message which attempts to trick them into copying, pasting and running malicious content on their devices. Compromised web pages, documents, HTML attachments, malicious URLs and more are all potential infection points.

The primary objective across these campaigns has been to deliver malware, including Remote Access Trojans (RATs), infostealers and loaders. Web injection clusters have also been known to use this technique. The most popular kind of ClickFix lure includes a fake CAPTCHA, giving victims a false sense of security.

# Laying a trap

Web inject campaigns, like SocGholish and its copycats, continue to thrive in the current threat landscape.

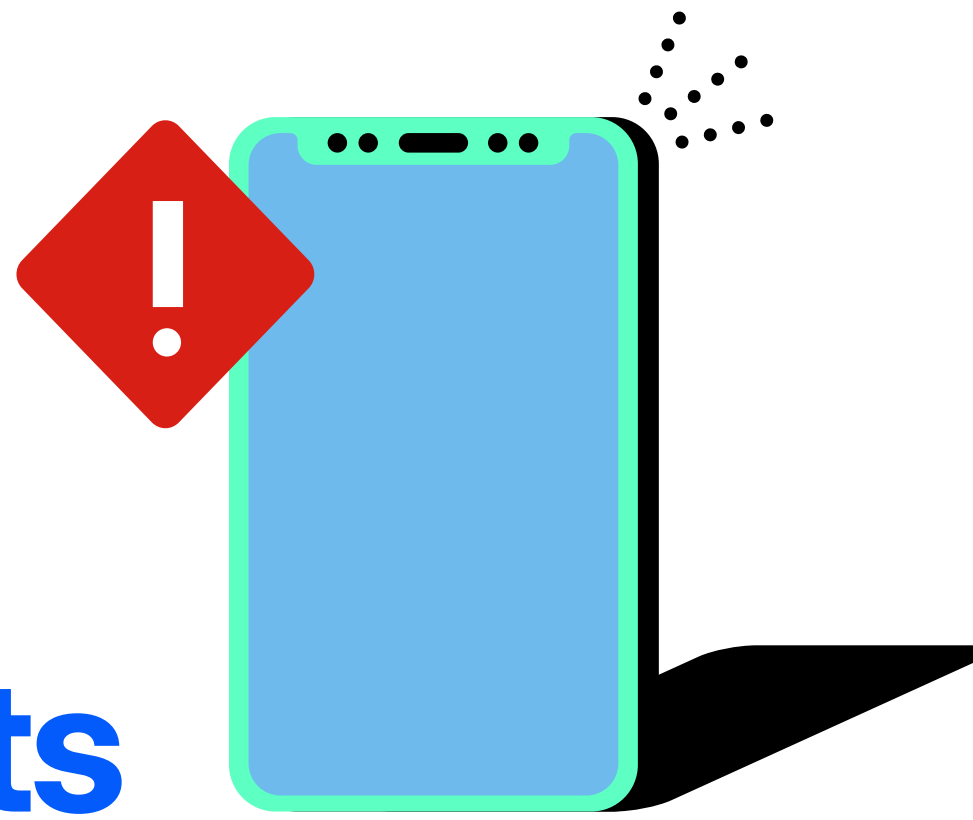
SocGholish is unlike most of the malware discussed in this report. These threats aren't directly sent by threat actors to victims in the form of an emailed URL or attachment. In fact, most emails flagged as SocGholish by our systems come from legitimate senders. Instead, SocGholish is a "drive-by" malware, which sits on infected websites and tricks victims into downloading it with fake browser update alerts.

People can get directed to these pages from links that are sent via email, text or collaboration platforms like Microsoft Teams, and anywhere else people share URLs. They're even encountered by people visiting compromised websites directly from search engines.

The security landscape for these threats is incredibly dynamic with multiple threat actors using this malware delivery method. In some cases, each part of the attack chain is managed by the same threat actor. But frequently, individual parts of the chain are managed by different actors working in collaboration.

| Name | Definition |
|---|---|
| TA569 | Threat actor associated with the SocGholish inject and Gholoader malware, uses fake update themed lures. The actor can either inject their own code directly on compromised websites or use a TDS such as TA2726 to serve their inject.[3] |
| TA2726 | A malicious TDS operator that facilitates traffic distribution for other threat actors to enable malware delivery. |
| TA2727 | A threat actor that uses fake update themed lures to distribute a variety of malware payloads. |
| TA582 | Threat actor that uses web injects and direct email to distribute malware. |
| LandUpdate808 | AKA Kongtuke, a JavaScript injection activity cluster, delivers multiple payloads including TA582 malware and according to external research has a close relationship to Interlock ransomware. |
| ZPHP | AKA SmartApeSG, a web inject activity cluster delivering malware including remote monitoring and management (RMMs). |
| ClearFake | Web inject activity cluster distributing information stealers notable for its use of a malicious script hosted on the blockchain via Binance's Smart Chain contract. |
| CoreSecThree | JavaScript injection activity cluster that uses clever fake CAPTCHA, filtering, and advanced rotating infrastructure to deliver information stealers. |

3. A TDS, or traffic distribution system, is a technology stack that enables its operators to develop complex and dynamic flows of web traffic. TDS platforms are often used by cybercriminals to redirect users to phishing websites.



# **Mobile threats** on the rise

For many of us, our smartphone contains the keys to both our personal and professional lives. Unsurprisingly, cybercriminals have recognized this is a two-for-one opportunity and increased their targeting of mobile devices. When it comes to attacking users across multiple devices, URL-based threats are the perfect tool.

## Smishing

Typically, SMS-based threats use lures that prey on our bias towards urgency and loss aversion. These psychological triggers are especially powerful in the context of phones, as we tend to be much more responsive to mobile messages than to email or computer messaging. In 2024, there was a 2,534% increase in URL threats delivered via smishing attacks.[4]

Our research shows that at least 55% of suspected smishing messages contained URLs, and 75% of organizations reported receiving smishing attacks.[5] The most popular SMS scams that featured URLs were road toll scams followed by fake delivery messages that impersonated logistics and mail companies. Many of these scams used the Darcula phish kit.

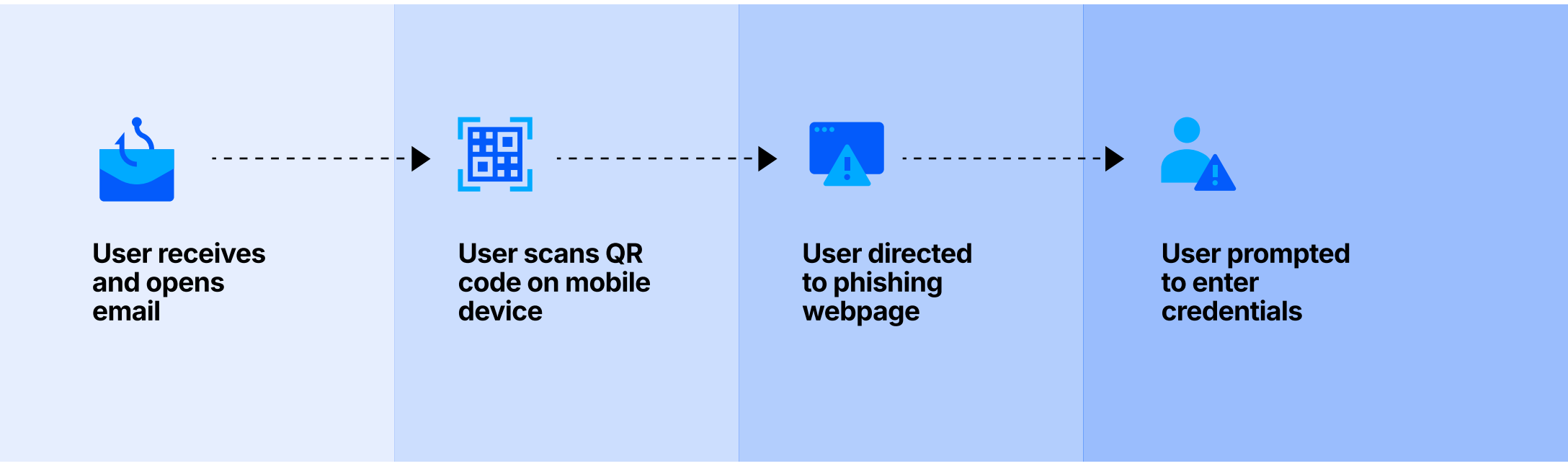
4. APWG. *Phishing Activity Trends Report.* 2024.
5. Proofpoint. *State of the Phish report.* 2024.

# QR code phishing

QR code-based URL threats burst on the scene in 2023. Since then, our researchers have seen these threats increasingly adopted by threat actors as a way to remove the victim from the enterprise detection pipeline and bypass traditional URL scanning and filters. In fact, Proofpoint observed almost 4.2M attacks exploiting QR codes in the first half of 2025 alone.

These threats are particularly dangerous, as they present users with a familiar format in a context they may not have seen before. People have grown accustomed to scanning QR codes with their phone cameras for everything from instructions to menus.

It is impossible to tell if a QR code is a threat just by looking at it. The way they work is an attacker will disguise a malicious URL within a QR code and embed it in a message. The message is socially engineered to convince the victim to scan the code. Once they do, they are then redirected to a fraudulent website designed to steal sensitive data, such as login credentials, credit card numbers or personal data.




*Typical QR code attack sequence.*

# Conclusion

The most damaging cyberthreats today don't target machines or systems. They target people. Threats like phishing and URL-based threats are often extremely difficult for users to spot. What's more, these attacks can't be accomplished without a human click. And cybercriminals are no longer limiting these attacks to just inboxes—they appear across digital channels, including collaboration and communication apps, and SaaS tools.

Proofpoint data shows that URL-based attacks can be carried out anywhere. That's why we recommend you protect your organization against these threats everywhere.

## Across the email life cycle

**Pre-delivery**

All suspected malicious URLs should be sandboxed, not just those identified to lead to direct payloads like malware.

**Post-delivery**

Some URLs can turn malicious after delivery, and a few bad ones may slip through your defenses.

**Click-time**

URL threats can detonate when clicked, so isolate them in case they've been rewritten.

## Beyond email

You need phishing protection against malicious URLs that are delivered via any messaging, collaboration or social media platforms.

## Your people

When you have visibility into who's being attacked and whether they click on URLs, you can protect everyone. This means applying the appropriate controls, like targeted learning, and protecting Very Attacked People (VAPs) with enhanced security.

## Your customers, partners and suppliers

You must protect all your trusted communications against impersonation attacks. This includes spoofed domains, lookalike domains and compromised supplier accounts.

To tackle today's evolving and emerging human-centric threats at scale, you need multilayered, AI-driven detection. Only an advanced AI-powered solution can spot the most subtle malicious indicators for threats that appear within any channel—whether that's email, messaging, SaaS apps or collaboration tools.

To learn more about how Proofpoint can protect your people from URL-based phishing threats, visit proofpoint.com.

proofpoint.

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 85% of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com

**Connect with Proofpoint:** LinkedIn



DISCOVER THE PROOFPOINT PLATFORM →