proofpoint.

REPORT

The Human Factor 2023

Analyzing the cyber attack chain

proofpoint.com

Introduction

After two years of pandemic-induced disruption, 2022 felt like a return to business as usual for many. And that certainly seems to have been the case for the world's cyber criminals. As COVID-19 medical and economic programs began to wind down, attackers had to get back to making a living the old-fashioned way: by honing their social engineering skills, enhancing their tooling, and looking for opportunity in unexpected places.

All of this has led to an explosion in ingenuity. From the commoditization of sophisticated techniques like multifactor authentication bypass to threats that rely solely on the attacker's charm and persuasiveness, the cyber attack chain—and the landscape as a whole—has seen major development on several fronts. And with Microsoft's moves to curtail abuse of Office macros creating unignorable pressure to innovate, many threat actors are still experimenting to figure out what comes next.

But no matter which tactics or techniques attackers turn to, their victims remain stubbornly human. Cyber attackers target people. They exploit people. Ultimately, they are people. That's what makes protecting people from cyber threats such a profound and fascinating challenge.

TABLE OF CONTENTS

THE HUMAN FACTOR 2023 \ **REPORT**

Key Findings

13 million

TOAD messages peaked at more than 13 millon per month

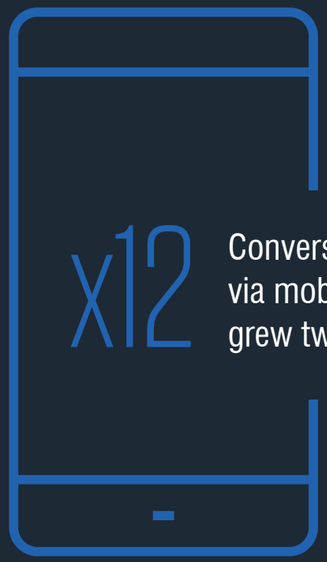
Emotet topped the charts again, sending over

25 million messages

94%

of cloud tenants were targeted every month

Office macro use collapsed after Microsoft rolled out controls to block them

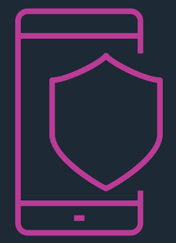


x12

Conversational attacks via mobile devices grew twelvefold

Top 5

Novel distribution pushed SocGholish into the top-five ranking for malware (by message volume)



MFA-Bypass

accounted for more than a million messages per month

About This Report

For more than 20 years, Proofpoint has been in the business of protecting people and defending data from cyber attacks. In that time, our research has consistently led us toward a simple but powerful observation: people—not technology—are the most critical variable in today's cyber threats.

This year, *Human Factor* report takes an even closer look at new developments in the threat landscape, focusing on the combination of technology and psychology that makes modern cyber attacks so dangerous.

What this report covers

This report covers threats detected, mitigated and resolved during 2022 among Proofpoint deployments around the world: one of the largest, most diverse data sets in cybersecurity.

We largely focus on threats that are part of a broader attack campaign, or series of actions taken by an attacker to accomplish a goal. Sometimes, we're able to link these campaigns to a specific threat actor, a process known as attribution.

Scope

The data in this report draws on the Proofpoint Nexus Threat Graph, using data collected from Proofpoint deployments around the globe. Each day, we analyze more than 2.6 billion email messages, 49 billion URLs, 1.9 billion attachments, 28 million cloud accounts, 1.7 billion suspicious SMS and more. Together, this amounts to trillions of data points across the digital channels that matter.

This report covers Jan. 1–Dec. 31, 2022. Where specific campaigns are discussed, this is the result of direct observation by our global network of threat researchers. Campaigns are defined as a series of common actions taken by a single attacker to accomplish a goal.

In a small number of cases, full-year data either wasn't available or might confuse the point being made. We'll make it clear where we've used a shorter time frame or a different source of data.

SECTION 1

The Threat Landscape

TA542:

The threat actor behind the Emotet malware. Financially motivated and known for extremely high-volume email campaigns.

TA511:

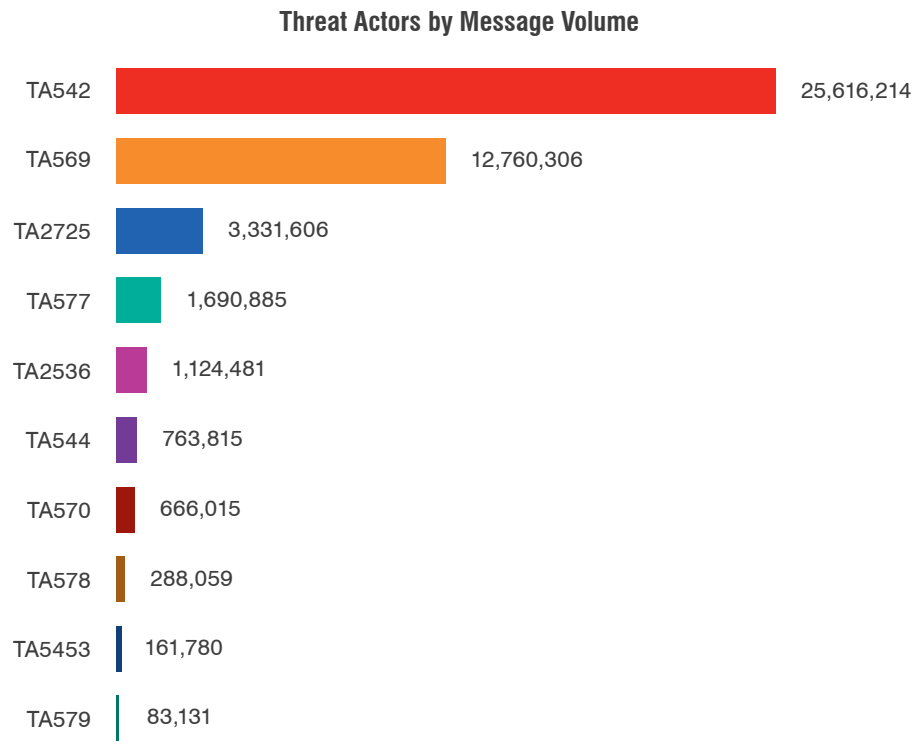
A financially motivated cyber criminal group. Known for high-volume campaigns targeting a wide range of industries. It has been associated with a number of different malware families since first being observed.

The more things change, the more they stay the same. In some respects, 2022 saw a lot of development in the threat landscape. Attack chains became more varied. Delivery mechanisms were rapidly tested and discarded. And threat actors began to match their ingenuity with new-found patience.

And yet, while techniques and tactics evolved—often at breakneck speeds—over the course of the year, the identity of the main culprits retained a degree of consistency.

Leaders and losers

Despite an erratic year, **TA542**, the entity behind Emotet, regained its place as the world's most prolific threat actor. Its return to the top comes only a year after law enforcement took the botnet offline in January 2021. Emotet's absence last year left the way clear for a new volume leader to step up for the first time in three years. But **TA511**—last year's top actor by volume—doesn't even make the top 10 this year, falling to 12th place.



TA2541:

A persistent cyber criminal group that typically targets aviation, transportation and defense industries.

TA577:

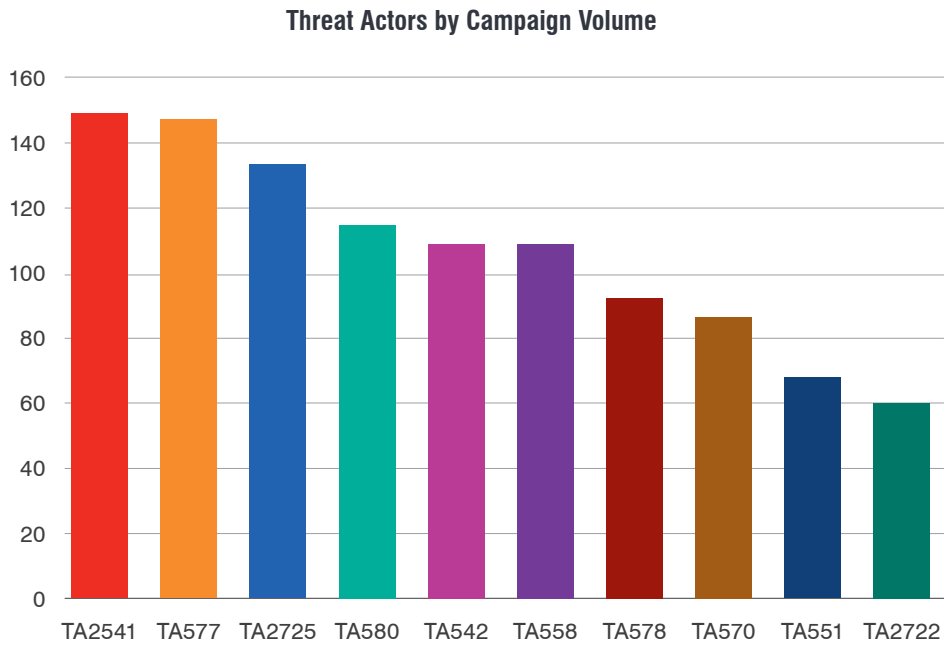
A prolific cyber criminal group tracked since 2020. One of the most notorious Qbot affiliates, this group is known to target a wide range of verticals.

initial access facilitator:

Cyber criminal groups that specialize in providing ransomware actors with access to compromised systems.

Our researchers identify threat actors by looking for patterns in the daily deluge of malicious email. When they find activity by a known actor, those messages are grouped into a campaign, usually defined by a common social engineering strategy or technique.

Ranking actors by the number of discrete campaigns they launch rather than just by sheer volume of messages can offer a useful alternative perspective. This approach allows us to see which groups are most active across the year and how they alter their tactics and lures.



The top two actors in this chart, **TA2541** and **TA577** make for an interesting comparison. TA2541 has a tight focus on aerospace, travel and defense industries. Unlike many others, this group tends to ignore current events and seasonal themes in its lures, preferring to rely on carefully crafted, industry-specific social engineering.

TA577, on the other hand, takes a completely different approach. A known **initial access facilitator**, this group targets broadly across both geographies and industries, and it has delivered a wide variety of different malware over the years.

financially motivated:

Cyber criminals who primarily seek to acquire money, either through direct theft or by monetizing stolen data and credentials.

advanced persistent threat:

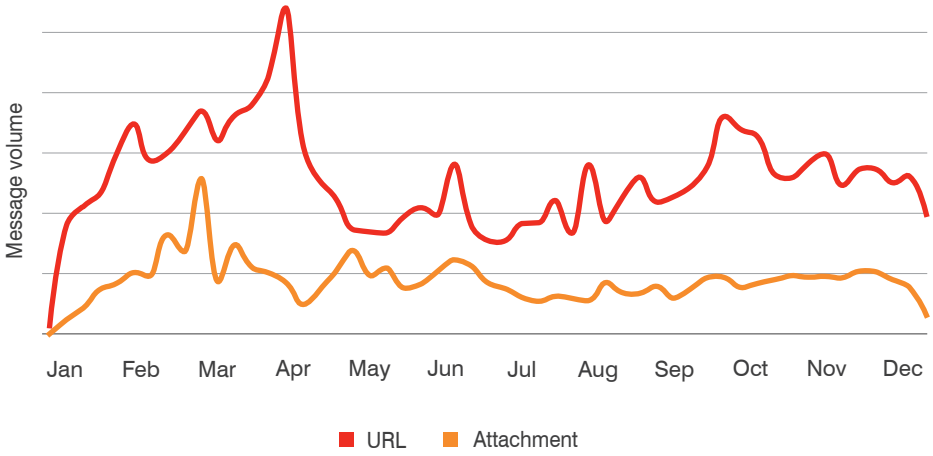
Threat actors who primarily work in support of a national interest. In some rare cases, APT actors also engage in financially motivated activity.

Emotet:

A prolific malware botnet. Apart from a period during 2021 when Emotet was shut down by law enforcement, it has typically been the world's most widely distributed malware.

Linked or attached?

The split between URLs and attachments for threat delivery also remained consistent year on year. While there were a few periods when trends grew close, URLs accounted for around three quarters of all threats overall.



When we break down campaigned threats between **financially motivated** and **advanced persistent threat** (APT) actors, we see a difference in approach, with APT actors far less likely to use attachments.

While URLs are also the most popular delivery mechanism for cybercrime, the distribution is more even. Some of this may be down to the influence of a handful of large-scale actors. As we'll see when we take a closer look at EMOTET in "Spotlight on **Emotet**" on page 27, TA542 has a strong attachment to… well, attachments.

FormBook:

This malware-as-a-service has been sold on forums since 2016. Pricing is comparatively low, making it a popular choice for attackers. Because of this, it's seen in a wide range of attacks using many different social engineering tactics and delivery methods.

NetSupport:

A legitimate remote access tool, now widely abused by cyber criminals.

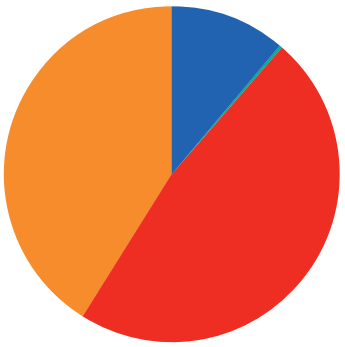
AgentTesla:

Widely available stealer malware that also acts as a loader for secondary payloads.

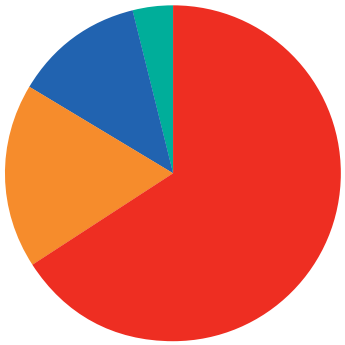
SocGholish:

An initial access malware delivered exclusively by drive-by downloads from infected websites.

Delivery Type E-Crime

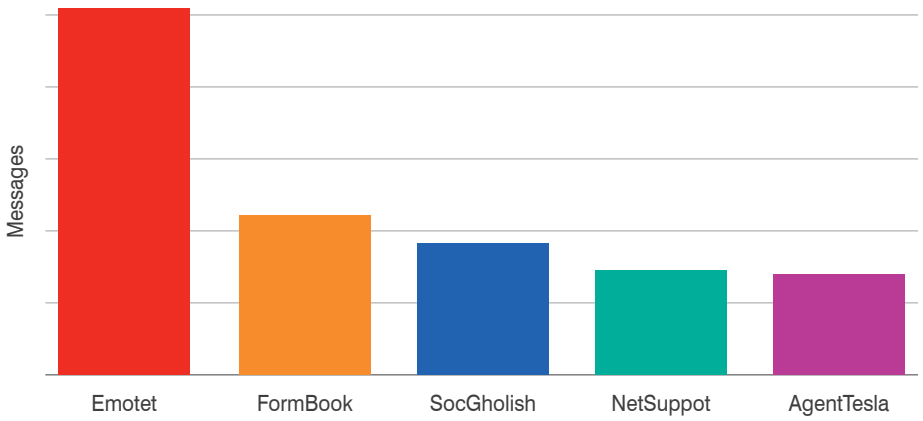


Delivery Type APT



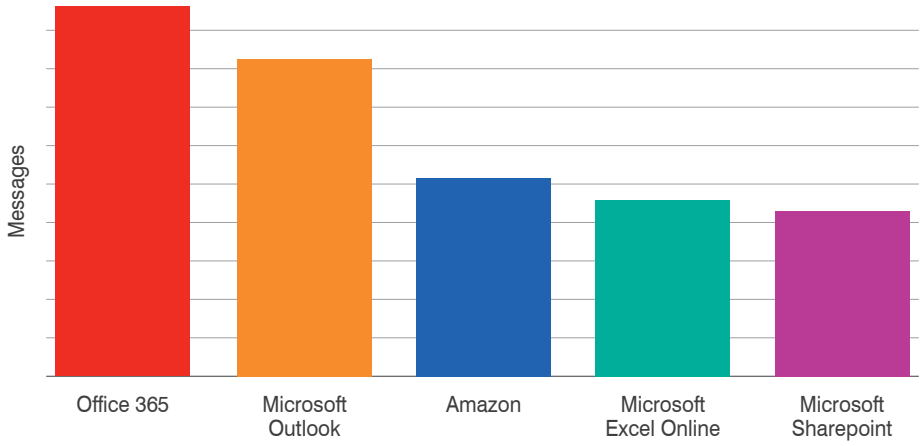
Top malware

With TA542 the leading threat actor by volume, it will come as no surprise to see Emotet at the top of the malware chart. Commodity malware used by a range of threat actors occupies three of the other four places (**FormBook**, **Netsupport** and **AgentTesla**). But the rise of **SocGholish** is noteworthy. (We take a detailed look at it in detail in "Spotlight On SocGholish" on page 22.)



Top lures

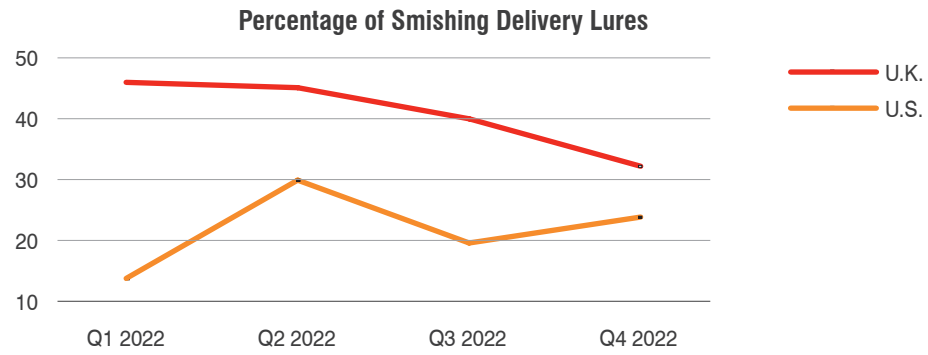
Abusing our familiarity and trust in major brands is one of the simplest forms of social engineering. And once again, cyber criminals had an overwhelming favorite when it came to brand abuse.



Microsoft products and services occupied four of the top five positions for abused brands across all threats, with Amazon taking the other spot. Among campaigns reviewed by our researchers, Amazon was actually the most abused brand, but Microsoft still dominated the rest of the top five.

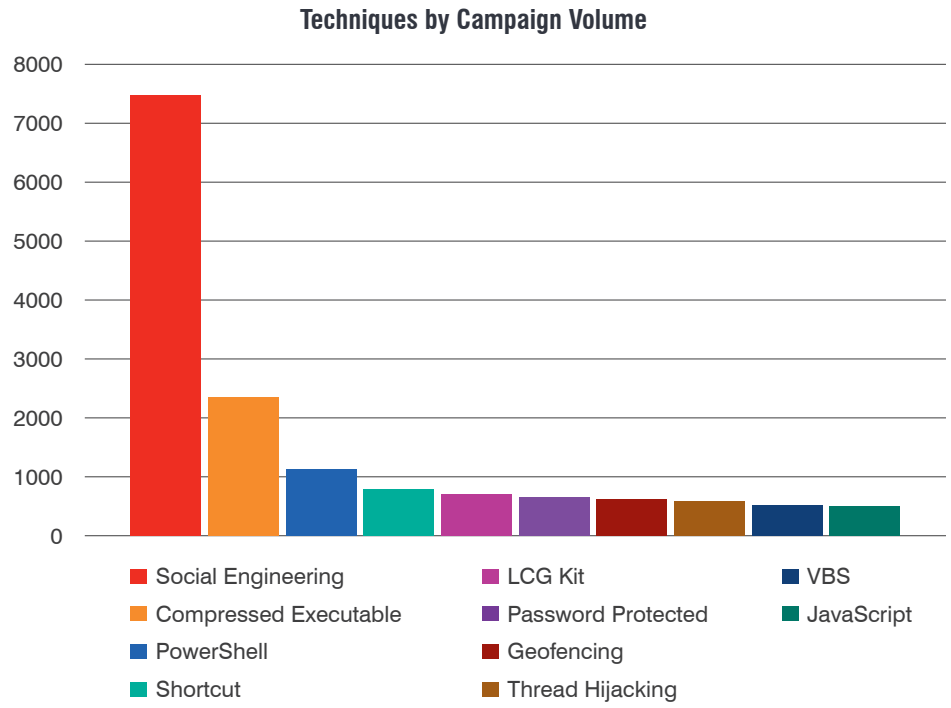
Switching focus to the topics featured in malicious messages, our researchers found that terms like “payment,” “order,” “invoice” and “purchase” were most commonly used.

In the mobile space, last year’s most popular smishing subject—package delivery notifications—remained prominent in both the U.S. and U.K. But as other lure types increased in the U.K., the overall share of delivery-related smishing messages fell.



Top techniques

When the first *Human Factor* report debuted almost 10 years ago, one of the insights we wanted to convey was the central role of social engineering in most cyber attacks. To this day, it remains the most common technique encountered by our researchers. Among the many attacks we classified, the vast majority relied on some element of psychological manipulation.



Social engineering is endlessly scalable and limited only by attackers' ingenuity. And even without the use of malware or technical exploits, the aftermath of a successful social engineering attack can be devastating.

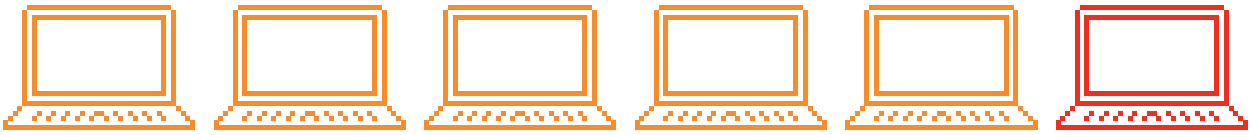
Identity Crisis

Whether their chosen mode is phishing or malware distribution, attackers invest a lot of effort into gaining access to corporate credentials and devices. So it's worth spending a moment to consider why this access is so highly prized.

User credentials are analogous to identity. Once your login and password are compromised, an attacker effectively becomes you as far as the systems you have access to are concerned. And recent research we undertook into identity risks reveals just how easily a compromised identity can become a big problem.

At many organizations, the presence of misconfigured or "shadow" admins brings additional risk to credential theft. Local administrators are often missing from privilege account management solutions. And some admin accounts may not be known to IT departments at all, with privileges either misapplied or left in place after a role change. As many as 40% of these shadow admin identities can be exploited in a single step, such as resetting a domain password to elevate privileges. And 13% of shadow admins were found to already have domain admin privileges.

The situation is equally promising for malware distributors. We've found that as many as 1 in 6 endpoints contain some kind of exploitable identity risk. Around 10% of endpoints have an unprotected privileged account password, with 26% of those exposed accounts being domain admins. So it's easy to see how successful initial access can rapidly lead to domain-wide attacks such as ransomware infection or data theft.



1 in 6
endpoints contain risk

TA471:

An advanced persistent threat actor that engages in both corporate and government espionage.

TA416:

An advanced persistent threat group aligned with the Chinese state.

TA453:

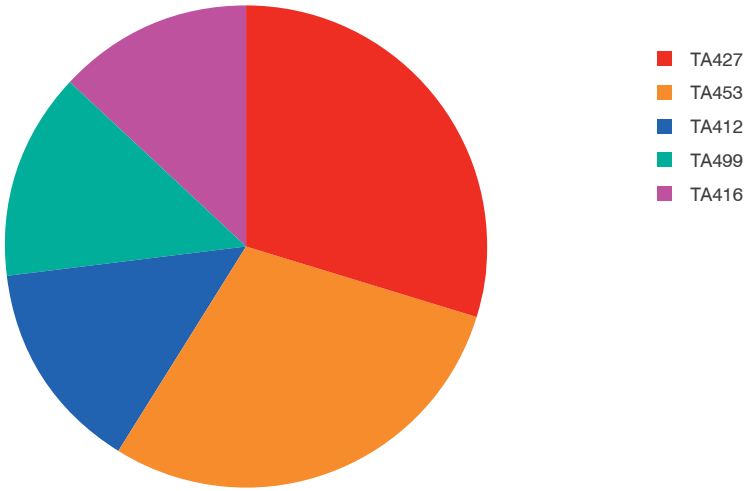
An advanced persistent threat group that supports the intelligence needs of Iran's Islamic Revolutionary Guard Corps.

APT Spotlight

As the lure themes mentioned in the last section show, financial motives dominate the threat landscape. So much so, that only a tiny fraction of our customers are targeted by state-sponsored APT actors (and even fewer are targeted by groups aligned with one of the global superpowers).

Since volumes of APT activity are low in comparison to financially motivated cyber crime, a single outlier attack can have an outsized impact on our data. This was the case in 2022, where one large campaign by **TA471** propelled that actor to the top of the APT message volume charts. Message volume can mislead; our researchers prefer to describe attributed APT activity in terms of frequency and number of campaigns. Using this measure, **TA416**, an APT actor aligned with the Chinese state, was one of the most active. In particular, our researchers noted significant new campaigns by TA416 that coincided with the start of the Russia-Ukraine war, targeting European diplomatic entities involved in refugee and migrant services.

APT Actors by Campaign Volume



Precision and patience are key to much APT activity, with many of these actors investing significant time exchanging benign messages with their targets to build rapport over weeks or even months. Most activity by **TA453**, the second most active APT group last year, follows this pattern, with the group impersonating multiple personas in some campaigns. The group, which is believed to be aligned with the Islamic Revolutionary Guard Corps of Iran, typically targets academic, dissidents, journalists and other figures of political influence. But last year, the group also targeted medical and aerospace researchers.

SECTION 2

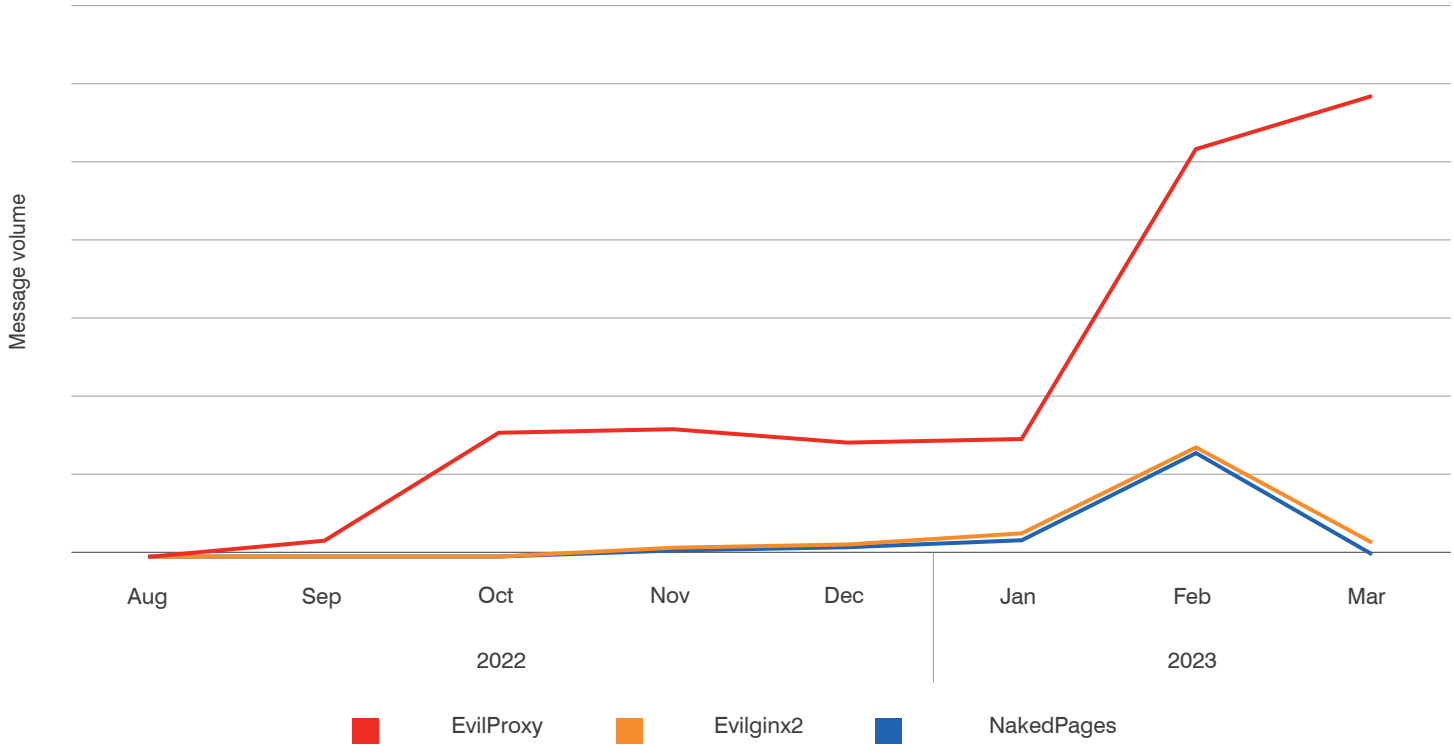
New Developments

Over the course of 2022, several technical and tactical innovations grew to become ubiquitous in the threat landscape. In their own way, each signals a dangerous escalation, whether in terms of once-inaccessible tools becoming commoditized, or new methods of manipulation becoming commonplace.

MFA bypass

With multifactor authentication (MFA) turned on, many users assume that their accounts and data are secure. After all, a cyber criminal would have to compromise your credentials and have access to the second factor of authentication, such as your mobile, landline or token generator.

But in the tug-of-war between attack and defense, one side rarely keeps hold of an advantage for long. In early 2022, our researchers reported on a new development in the world of phish kits. These off-the-shelf tools allow even non-technical criminals to spin up a phishing campaign. The existence of phish kits is nothing new, with recent years seeing the market evolve from a licensing model to operators providing fully hosted, phishing as a service. And in 2022, phish kits gained a powerful new capability: bypassing MFA.



EvilProxy:

A phishing-as-a-service platform with advanced capabilities.

Evilginx2:

A red-team tool with advanced capabilities allowing for reverse proxy attacks against multi-factor authentication.

NakedPages:

An off-the-shelf phishing kit with advanced capabilities allowing for reverse proxy attacks against multi-factor authentication.

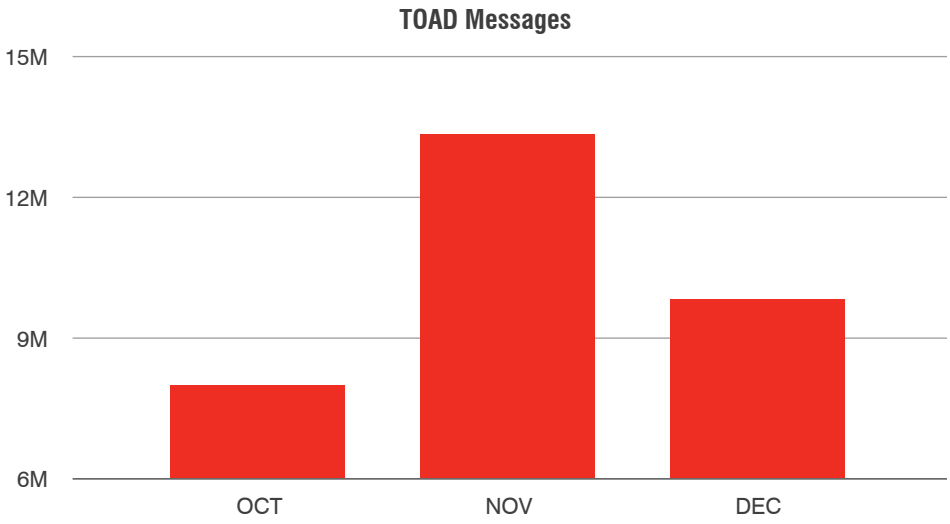
In the fourth quarter of the year, we gained visibility into attacks using three prominent MFA bypass frameworks: **EvilProxy**, **Evilginx2** and **NakedPages**. Together, these techniques account for hundreds of thousands of malicious messages every month, with EvilProxy continuing to see significant volumes into 2023.

MFA is still an integral part of defense in depth, and activating it remains best practice. But the growth of these techniques should signal a loud note of caution: attackers will take everything if you let them—even your MFA tokens.

Attack of the TOADs

Last year we reported on an increase in telephone-oriented attack delivery (TOAD), a novel technique involving a high degree of interaction between victim and attacker. The first stage of a TOAD attack uses pure social engineering. Usually, it arrives in the form of a fake subscription invoice or similar, designed to persuade victims to call a telephone helpline. But instead of customer service, the target ends up talking to a cyber criminal. Once they have a victim on the phone, cyber attackers can pursue several ploys, from guiding victims into granting remote access to their machines to instructing them to download malware.

This year our systems gained the ability to detect TOAD attacks automatically, giving us a clearer picture of just how ubiquitous this technique has become.



BazaCall:

An early prominent instance of telephone-oriented attack delivery that infected victims with the now defunct BazaLoader malware.

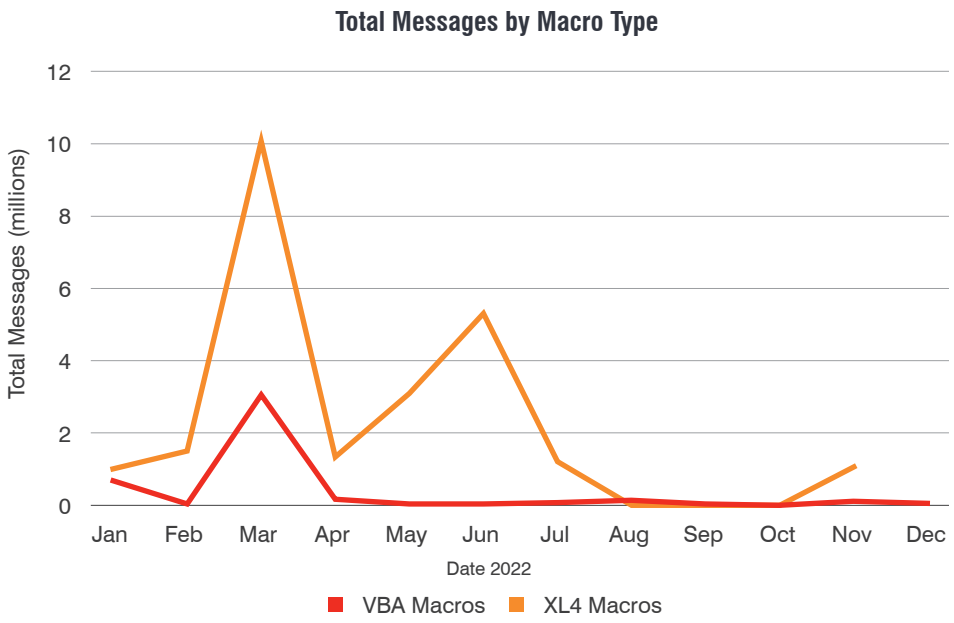
We now detect and mitigate millions of TOAD messages per month. And while a percentage of these originate with high-profile attackers like the **BazaCall** group responsible for last year's fake movie streaming sites and unannounced Justin Bieber tours, the sheer volumes now involved speak to adoption by less sophisticated groups.

TOAD is here to stay; security awareness programs had better jump to it.

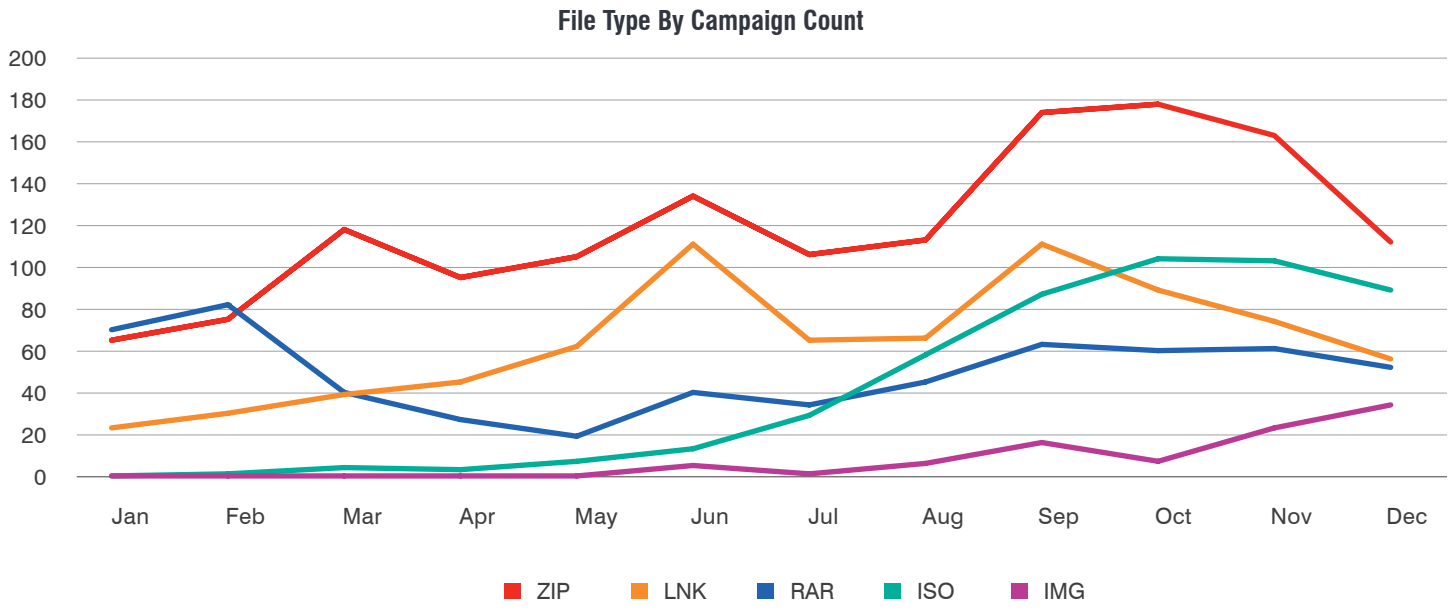
Forced evolution

Cyber criminals are innovators, but they don't innovate for the sake of it. If a tactic or technique is successful, they'll keep at it until defenders catch on. A great example of this is the use of Office macros for malware delivery. The technique was a mainstay for almost two decades—so much so that Microsoft finally decided to do something about it.

Over the course of 2022, Microsoft made changes to how its productivity suite treats files downloaded from the internet, making it much harder for cyber criminals to deliver malware through Office documents.



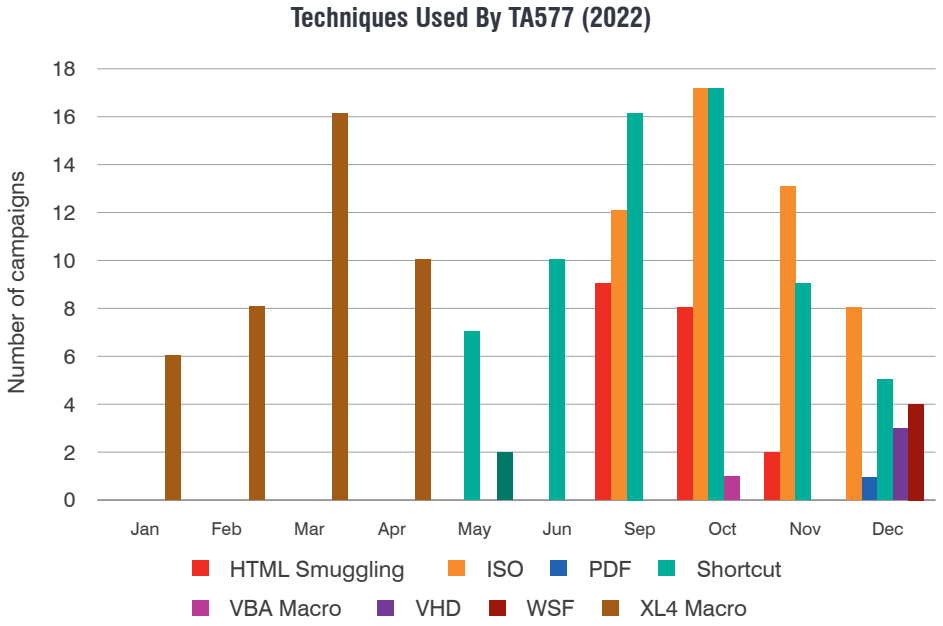
Volumes of messages containing Office macros fell sharply over the course of the year, with the large spikes in both VBA and XL4 due to Emotet-related activity. In turn, we saw other file types increasing as cyber criminals experimented with new techniques.



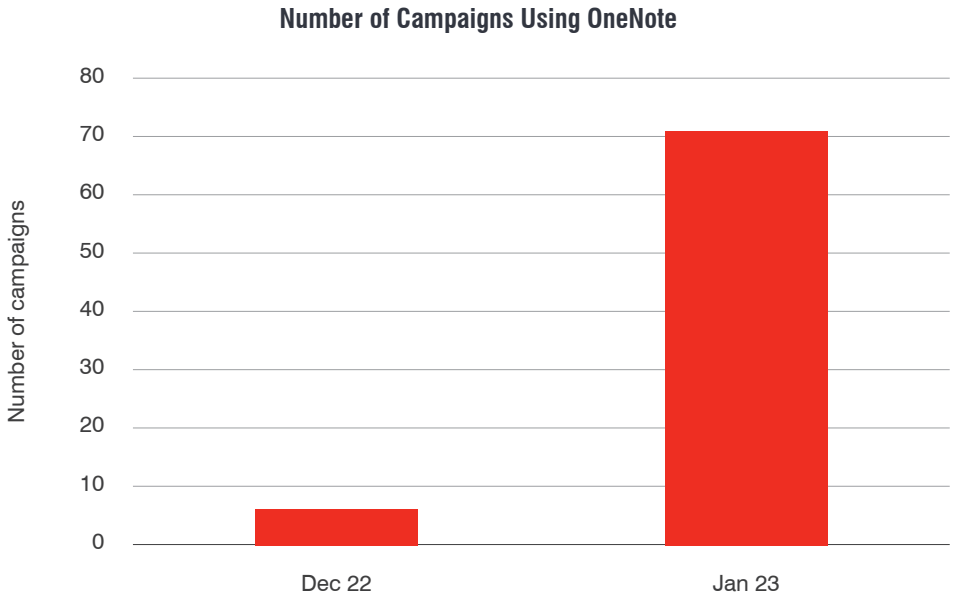
Threat actor **TA577** provides a compelling snapshot of this evolution in practice. A prolific Qbot affiliate, TA577 features in the top five threat actors for both message and campaign volume. In 2022, the group pivoted away from macros and adopted new techniques, including using various file types such as PDFs, ISOs and virtual hard disk (VHD) files.

MACROCALYPSE

With Office macros no longer a reliable malware delivery channel, threat actors turned to PDFs, ISOs and virtual hard disk (VHD) files.



But the end of Office macros doesn't mean that attackers turned their backs on Microsoft. At the end of the year, our researchers noted a sudden increase in campaigns abusing the software giant's OneNote product. Campaigns surged in early 2023, and Microsoft has announced plans to increase security measures for files embedded in OneNote documents.



Spotlight on SocGholish

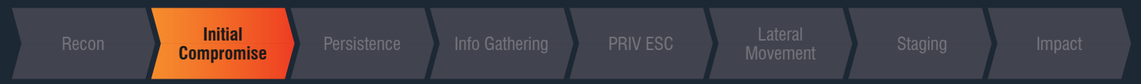
One of the year's standout threats appeared in the form of SocGholish, a malware exclusively delivered by cyber criminal group **TA569**. Among the threat actors we track, TA569 was the second most prolific after TA542/Emotet. And among malware seen in malicious email, only Emotet and the commodity malware **FormBook** had a higher message volume.

TA569:

A cyber criminal group known for compromising content management servers to deliver SocGholish. An initial access facilitator, the group has been linked to WastedLocker and may have ties to other ransomware operations.

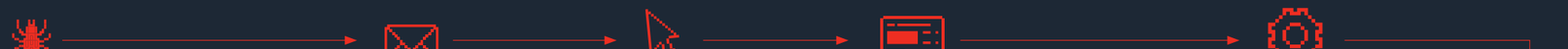
The attack chain

The cyber attack chain is a model that describes the typical progression of most threats. While every attack is unique in some way, most follow a common sequence. Let's compare and contrast the initial compromise sequence for two key strains of malware.



SocGholish attack chain: initial compromise

Unlike most of the malware discussed in this report, SocGholish isn't delivered directly 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.



Infect host

Malware can be served from infected websites. To do this, the attacker takes advantage of a vulnerability with the site or a site component, such as advertising units or embedded assets.

Legitimate email

Infected sites are often unaware that they are hosting SocGholish and will continue to send out email to users.

Click URL

If recipients click through to a site containing SocGholish, they risk infection.

Fake browser update

SocGholish typically shows users a pop-up notification asking them to download and install a "browser update" that's actually malware.

SocGholish installed

If a user follows the fake update instructions, SocGholish is installed on their machine.

Ransomware or other follow-on activity

Emotet attack chain: initial compromise

Compare that attack chain to Emotet-based attacks, which follow a more traditional pattern.

Email

Most malware is delivered by malicious email containing either links or attachments.

Has attachment

The group behind Emotet now stands almost alone among large-scale threat actors in its use of macro-enabled Office attachments.

Attachment is opened

For an email threat to pose a risk, the recipient must first open the attachment.

Interaction with attachment

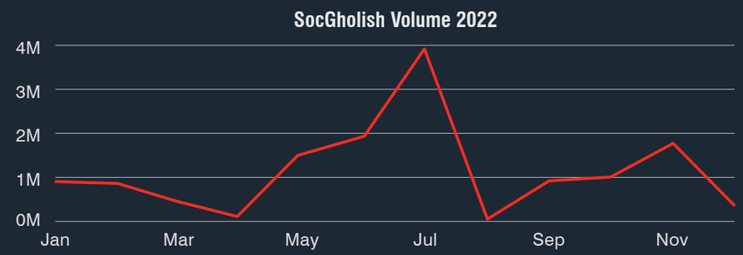
Once an attachment is opened, the recipient usually still has to go further before the threat is realized. In the case of Emotet, victims typically have to click to enable Office macros.

Emotet installed

If the recipient engages with the malicious attachment, Emotet is downloaded and installed to their machine.

This year, TA569 was successful in serving malware from some very high-traffic website, including, for a brief period, some local and national news sites. During that time, any email containing a link back to an infected—such as daily newsletters, breaking news alerts or third-party roundups—was flagged for posing a risk of SocGholish infection.

In the specific case of the news websites, administrators identified the source of the infection and removed the malicious script in a matter of hours. But many sites hosting SocGholish have no idea they are infected. And to complicate matters further, TA569 tends to cycle through the sites it has compromised, turning injects on and off, making the task of identifying infected hosts even harder.



But while SocGholish email volumes are similar to those of other high-profile malware, there is a critical difference in how this threat is spread. Understanding that difference offers not only the key to defending against SocGholish, but also a valuable insight into how social engineering can show up in unexpected areas of decision making.

Ghoulishly smart social engineering

SocGholish makes for an interesting case study because its attack chain contains both active and passive forms of social engineering. Most obviously, the fake browser update preys upon users' familiarity with computing conventions to persuade them to install malicious software. But beyond this overt manipulation, our researchers believe TA569 may also have a subtler purpose.

Eroding user patience with the systems and tools configured to defend them is an ambitious goal, but some threat actors have already experienced some success. In one of last year's highest profile breaches, attackers gained access to their target's systems by bombarding a specific user with MFA push requests on their mobile device. Sufficiently annoyed, that user eventually clicked "Yes" to authenticate the log-in attempt. A point of defense became a point of weakness, simply because the attacker made it into an irritant.

In the case of SocGholish, it's possible that high volumes of email from legitimate sources being flagged as malicious will eventually cause enough friction that users demand certain sites be safe listed. Or worse, people will start ignoring flagged email warnings altogether. If either of those happen, TA569's success will create a rising tide that lifts all cyber criminal boats.

TA2536:

A long-standing financially motivated cyber criminal group, first observed in 2015. Typically distributes malicious Office documents.

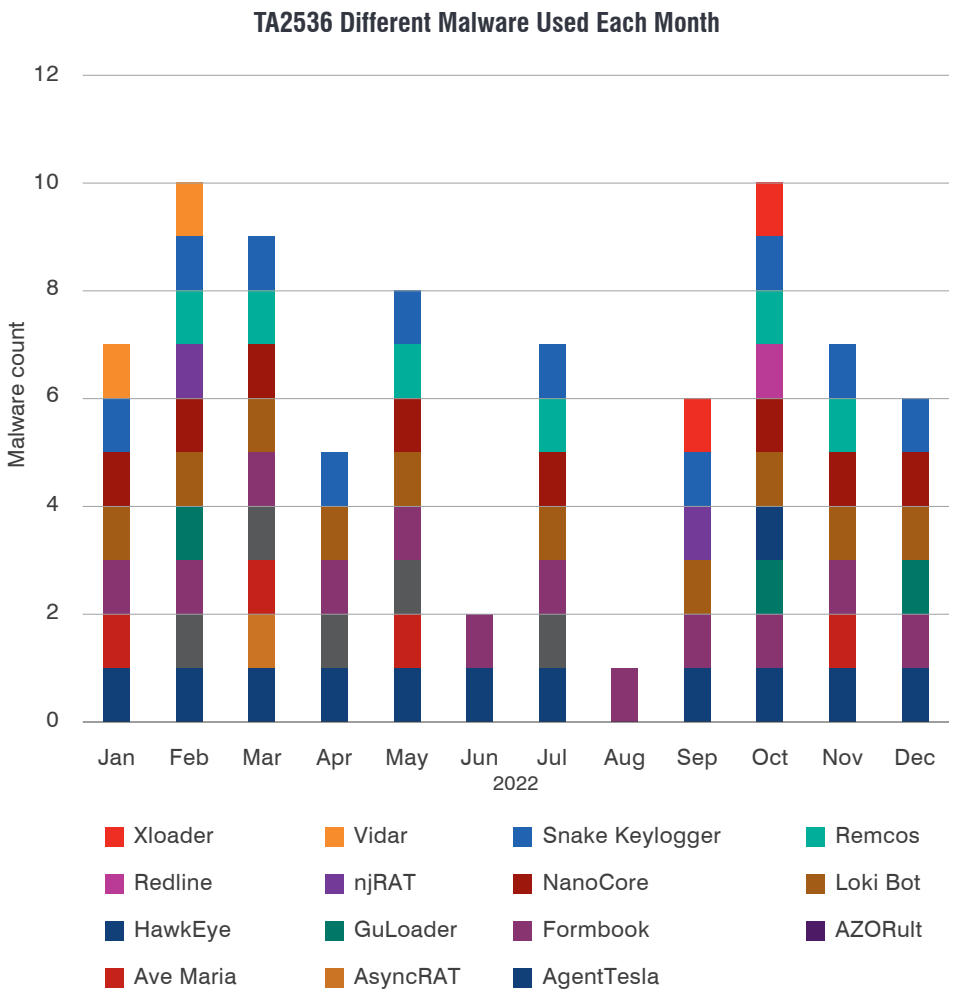
LokiBot:

Common stealer malware, first identified in 2016. Also used as a backdoor for secondary infections.

Rapid iteration

The fluctuations in the threat landscape are a constant challenge for security teams and researchers. The most agile threat actors change social engineering strategies and malware payloads regularly, making them a moving target that can be tough to pin down.

A good example of this tendency in 2022 was **TA2536**, a cyber criminal group we've been tracking since 2015. TA2536 largely uses commodity malware, delivering 15 different payloads over the course of the year. AgentTesla and **LokiBot** information stealers appeared often in the group's campaigns, but as the chart below illustrates, other payloads varied widely.



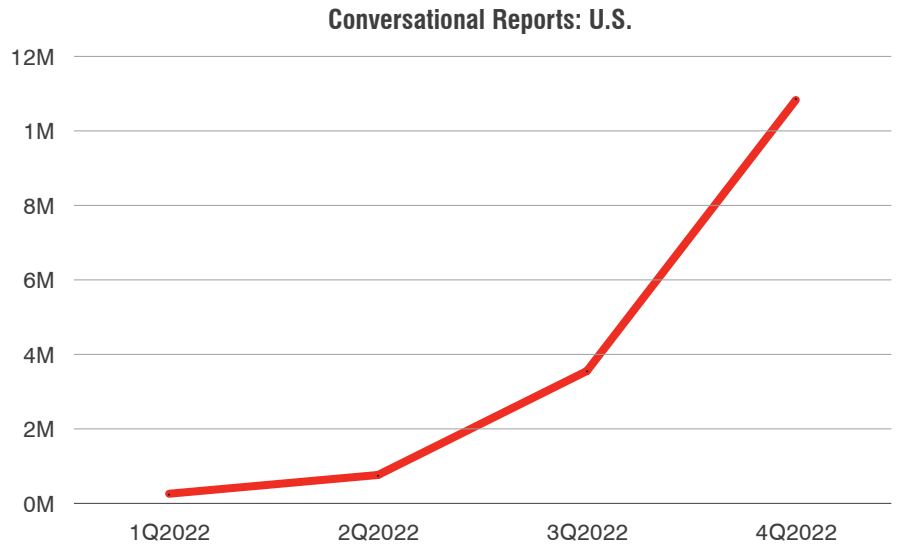
Pig Butchering:

A form of conversational threat in which benign messages are exchanged before the attacker seeks to extract money from victims by persuading them to invest in bogus cryptocurrency platforms.

Chatting with Attackers

Cyber attack and cyber defense are often deeply technical disciplines. But one of 2022's most notable developments was also arguably the least technical. Conversational attacks have been a part of the threat landscape for a while. APT attackers, for instance, are known to invest significant time and effort in building rapport with their targets before trying to steal credentials or data. But over the course of the year, our data reveals a significant increase in the number of conversational attacks from financially motivated actors.

In the mobile space, our Cloudmark division measured a twelvefold increase in conversational attacks during the first half of the year, including romance scams, fake job ads and "**Pig Butchering**" cryptocurrency fraud. This growth has made conversational lures the most common form of attack in some verticals. Even accounting for the impact of simplified abuse reporting in iOS, the data reveals a significant shift towards conversational approaches across the mobile landscape.



$2.5B

Losses due to cryptocurrency scams in 2022

$2.7B

in BEC losses to U.S. companies

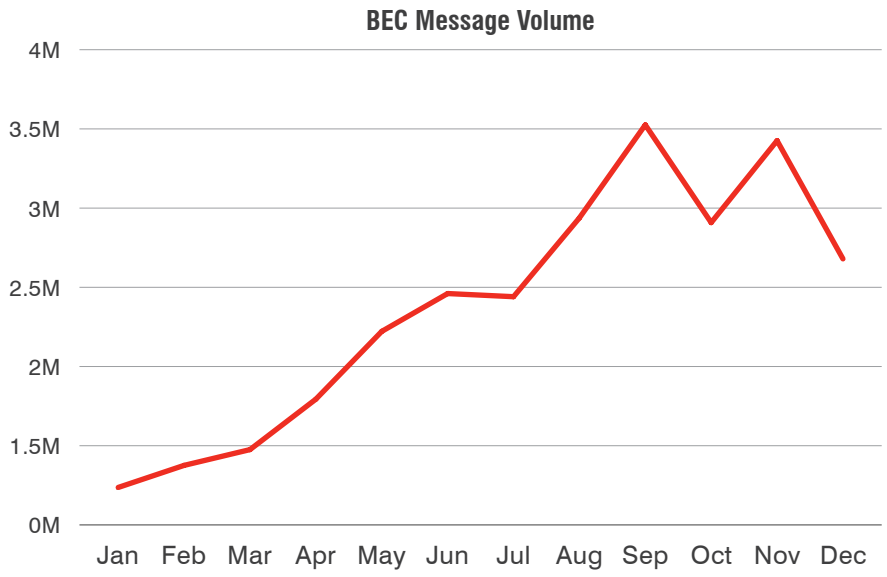
$34M

in losses from ransomware

The cost of these attacks is considerable. The most recent FBI *Internet Crime Report* cited more than $2.5 billion in losses due to cryptocurrency scams;[1] pig butchering is now among the leading examples of this trend. And the losses aren't just financial. Conversational approaches work because the victim makes an emotional investment in the attacker. In romance scams and pig butchering, the realization that this trust has been misplaced can be every bit as devastating as the monetary loss.

Business email compromise

While the chatty, informal messages typical of pig butchering and romance scams are less common in email, certain categories of email threat beyond APT still fit this pattern. Most business email compromise (BEC) does not involve phishing or malware. Instead, attackers use social engineering and other deceptive techniques to slip undetected into the normal flow of business communications, sending illegitimate invoices, money transfers and similar tasks.



BEC is a seemingly low-key threat, attracting far less attention than ransomware and data leaks. But according to the FBI *Internet Crime Report*, BEC cost American businesses $2.7 billion last year, with the global figure certain to be much higher. Ransomware victims, in contrast, lost just $34 million.

1 FBI. "Internet Crime Report 2022." March 2023.

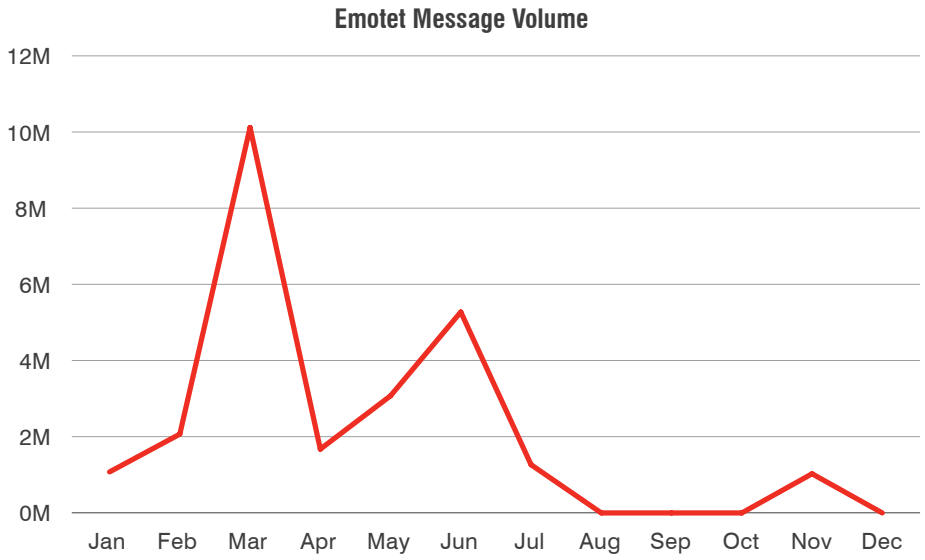
Conti:

Once the world's most infamous ransomware gang. The group disbanded in 2022 after many of its internal documents were leaked on Twitter. Research suggests many individuals associated with Conti joined other groups and continue to remain active in the cybercriminal ecosystem.

Spotlight on Emotet

In January 2021, law enforcement shut down the Emotet botnet, making arrests and seizing money and equipment. Overnight, the world's most prolific malware was taken offline. But optimism from that operation was short-lived. Last November Emotet blinked back into life and began sending out new campaigns. Independent reporting at the time drew a connection between Emotet's return and moves by the **Conti** ransomware gang to consolidate its choice of initial access malware.

Emotet activity throughout 2022 was erratic. The only two significant peaks of activity occurred in March and June, and activity shut down completely during August, September, October and December. Despite this fitful pattern, TA542, the group behind Emotet, still sent more malicious email last year than any other threat actor we track.



THE EMOTET-CONTI CONNECTION

The @ContiLeaks disclosures confirmed a close alliance between Conti and Emotet. The group may have fallen into disarray after Conti shut down.

One possible explanation for TA542's periods of dormancy can be found in the fate of the Conti ransomware group. In late May of last year, the group announced plans to shut down operations. This came after a period of intense scrutiny triggered by large amounts of the group's internal data being leaked on Twitter. The @ContiLeaks disclosures confirmed a close alliance between Conti and Emotet. Emotet may have experienced a degree of disarray as a result of the Conti closing its doors.

It's also possible that Emotet may simply be biding its time. The group is something of an outlier among large-scale threat actors. For instance, it still prefers to distribute its malware using attachments, swimming against the tide of URL-based attacks. Even so, Emotet conducted a small number of experimental campaigns involving URLs. These tests suggest that—like many dominant players—the group may just be taking its time in adapting to the changes going on around it.

SECTION 3

Opportunistic Attacks

RELIEF AGENCIES IN THE CROSSHAIRS

A likely state-sponsored phishing campaign targeted personnel involved in managing the logistics of refugees fleeing the Russia-Ukraine war. A week later, China-aligned TA416 was found targeting similar relief efforts.

Timeliness is key consideration in social engineering. Lures that refer to recent events or time-sensitive decisions can cause victims to skip some of the scrutiny they might otherwise apply. In recent years, COVID-19 provided attackers with endless headlines and policy decisions to use in their lures. This year, as the pandemic receded into the background in many countries, cyber criminals looked to apply their opportunism elsewhere.

Russia-Ukraine

When the Russia-Ukraine war ignited at the end of February, some commentators predicted a year of unprecedented cyber conflict. Thankfully, that didn't happen. But the political, economic and humanitarian upheaval was an opportunity several APT actors couldn't ignore.

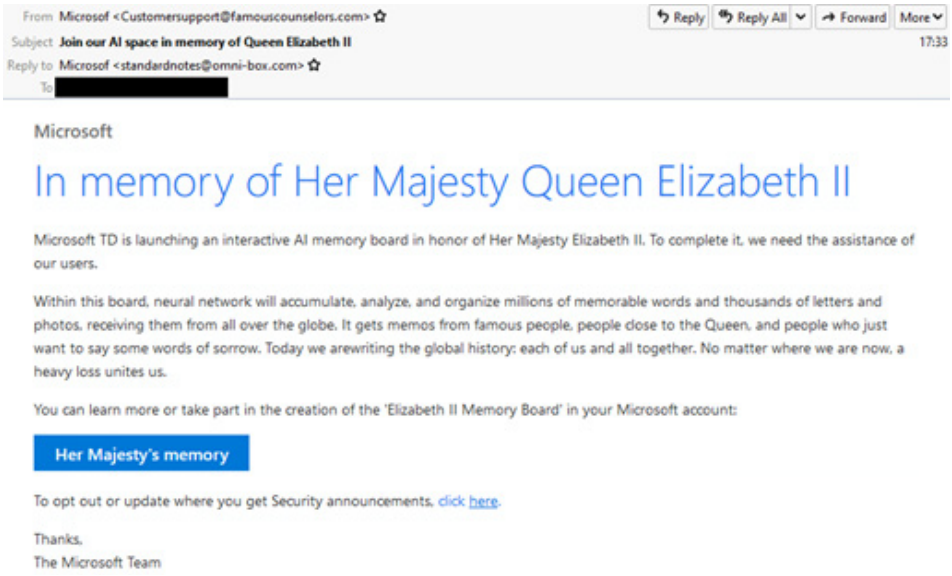
Within days of the invasion, our researchers identified a likely state-sponsored phishing attack using compromised Ukrainian armed service credentials. The campaign targeted European government personnel involved in managing the logistics of refugees fleeing the war. Only a week later, a campaign by China-aligned attacker TA416 was uncovered targeting a similar range of relief efforts.

CASHING IN ON THE CROWN

A lure purporting to be part of a digital "memorial wall" directed victims to a website that tried to harvest their login credentials.

Queen Elizabeth II

While international conflict provided opportunity for state-sponsored attackers, financially motivated cyber criminals were less choosey. In September, the death of Queen Elizabeth II led one threat actor to spin up an unusual phishing campaign. The lure purported to be part of a digital "memorial wall" being constructed by Microsoft. If users clicked through to participate, they were directed to a URL that tried to harvest their login credentials.



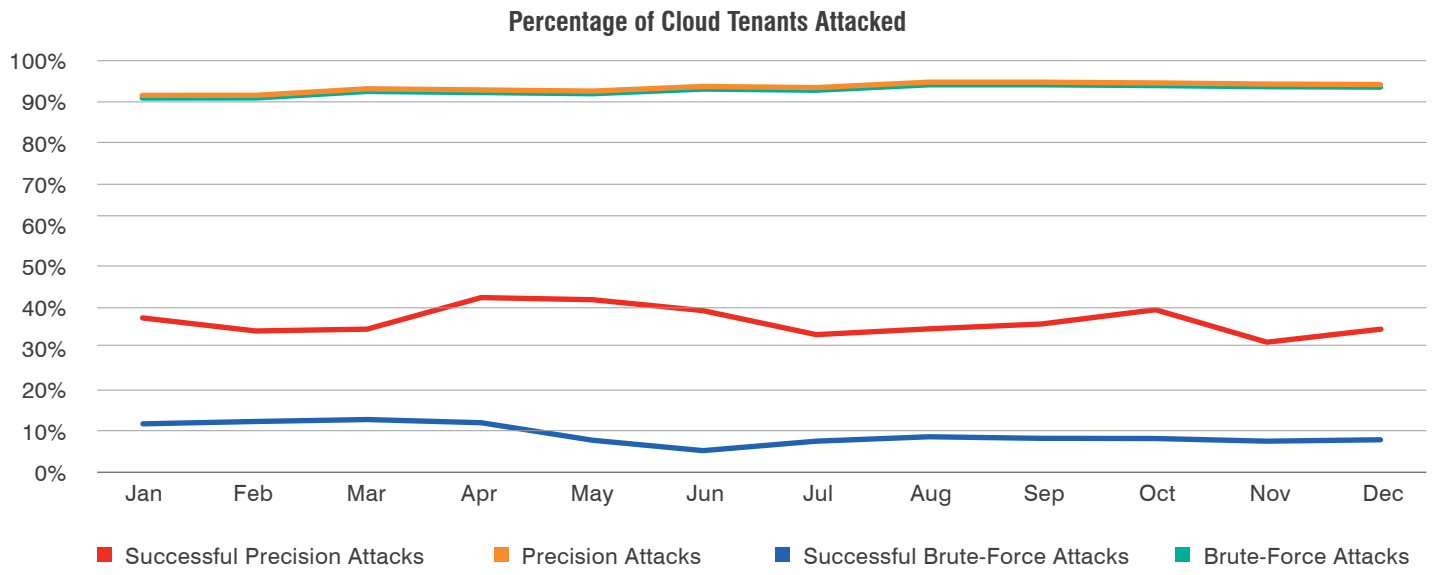
Silicon Valley Bank

The recent collapse of Silicon Valley Bank (SVB) offers a great illustration of just how quickly cyber attackers can gear up to take advantage of a crisis. Within hours of U.S. authorities taking control of the ailing bank in March, our researchers saw dozens of lookalike and typosquatting domains being registered. And almost at once, SVB customers began to receive targeted malicious email trying to incite money transfers or other illicit transactions.

SECTION 4

A Dark Cloud

Last year we reported on how the ubiquity of cloud infrastructure led to a noteworthy rise in the number of threats faced by cloud tenants. This year, that trend has continued to the point where it is now cloud threats themselves that have become truly ubiquitous



62%

of targeted cloud tenants were successfully compromised

The average monthly volume of brute-force attacks rose

400%

in early 2023 vs. the 2022 monthly average

In 2022, up to 98% of monitored tenants were targeted by either a precision or a brute-force cloud attack. Attacks were so frequent that in any given month, 94% of monitored tenants were targeted, indicating a regularity on par with email and mobile vectors.

Of these targeted cloud tenants, 62% were successfully attacked, with the monthly success rate averaging around 20%. This is slightly lower than last year's monthly figure of 24%, which suggests that cloud administrators may have noted the degree of threat escalation and taken steps to protect their systems and users.

Another contributing factor to the declining success rate might be found in Microsoft's deprecation of some legacy email protocols. Removing these less secure options led to a mid-year decline in the success rate of brute-force attacks, though precision attacks largely retained their effectiveness. The waning effectiveness of brute-force attacks may have led attackers to double down on volume. As we entered 2023, the number of brute-force attacks in our data—notably password spraying—increased from a monthly average of around 40 million to nearly 200 million. Still, it seems likely that dwindling efficacy will ultimately continue to lead attackers to pivot to other techniques and threat vectors.

14%

of successful cloud attacks led directly to post-compromise malicious email activity in the second half of 2022.

13%

of successful cloud attacks led to malicious file activity.

11%

of organizations authorized a malicious third-party app.

Post-access activities

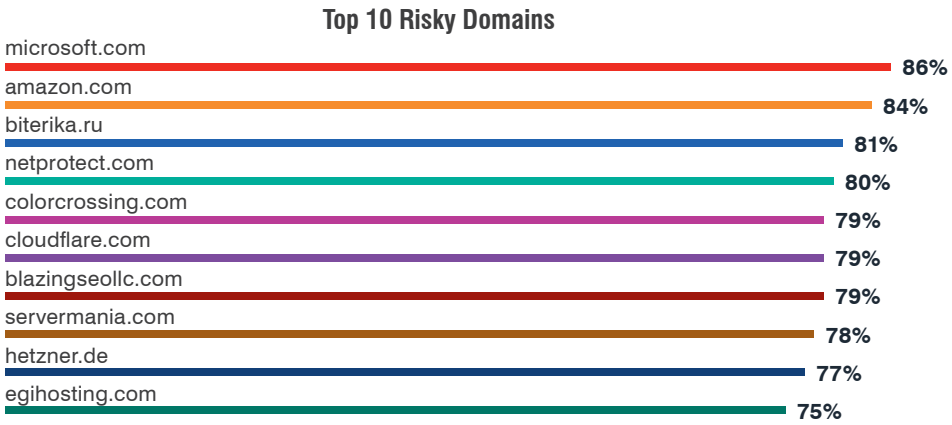
Once a cloud tenant has been compromised, threat actors have several options. With a single set of credentials often giving access to email, document storage and other single sign-on services, the effects can be severe. Among monitored cloud tenants that experienced a successful attack in the second half of last year, at least 14% saw outbound post-access malicious email activity. Thread-hijacking and impersonation are critical tools in the BEC and supply chain playbooks. So malicious mailbox access could have consequences not just for the attacked organization, but for their customers and partners.

Post-access malicious file activity rates were similar, affecting 13% of affected tenants in 2022. File activity isn't only limited to data theft—attackers can also upload malicious files containing malware or phishing threats or amend existing documents, such as supplier payment details.

Attackers' ability to persist in the compromised environment is a growing challenge in cloud-based attacks. Many attackers set up new mailbox rules such as redirects, or seek to manipulate multifactor authentication methods, granting a degree of persistence even if their access is detected and cut off. Attackers may also authorize malicious OAuth applications, potentially making their access more durable and persistent. At a conservative estimate, at least 11% of organizations authorized a malicious third-party application last year.

Traffic sources

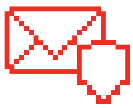
As we saw in the lure data presented earlier in this report, using legitimate infrastructure is a tried and trusted technique in social engineering. But it also plays a key role in the delivery of many cloud-based attacks. Around 8 in 10 organizations faced brute-force attacks using Microsoft, Amazon and Cloudflare infrastructure last year. While the threats originating from other domains in this list might seem like easy targets for blocklisting, the presence of cloud giants such as Microsoft, Amazon and Cloudflare—whose infrastructure hosts countless legitimate services that organizations rely upon—shows the limitations of rules-based protections.



Conclusion

No matter where attackers look next for inspiration, a people-centric approach to prevention is the key to defending against future threats. Users who are trained to expect the unexpected will be primed to spot a threat and break the attack chain, whether it comes in the form of a note-perfect phishing page or a sly text message purporting to be from an old friend.

Cyber attacks are inevitable. But with the right mindset, tools and policies, they can be a manageable risk. Deploy solutions that give you visibility into who's being attacked, how they're being attacked, and whether they clicked.



Build a robust email fraud defense. Email fraud can be hard to detect. Invest in a solution that can manage email based on custom quarantine and blocking policies. Your solution should analyze both external and internal email—attackers may use compromised accounts to trick users within the same organization.

Protect cloud accounts from takeover and malicious apps. Attackers are agile and can pivot on a dime, so every entry point into your systems needs to be covered.

Partner with a threat intelligence vendor. Focused, targeted attacks call for advanced threat intelligence. Leverage a solution that combines static and dynamic techniques to detect new attack tools, tactics and targets—and then learns from them.

Threat actors are more equipped, creative and motivated than ever. Stopping them requires a multilayered, people-centric approach that spans the entire attack chain.

To learn more about how Proofpoint can protect your people from advanced email attacks and identity-based threats, visit proofpoint.com

LEARN MORE

To learn more about how Proofpoint provides insight into your vulnerability-, attack- and privilege-based user risks and helps you mitigate them with a people-centric cybersecurity strategy, visit **proofpoint.com.**

ABOUT 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 75 percent 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**

proofpoint.

0400-014-01-01