proofpoint.

REPORT

The Human Factor 2022

People-centric cybersecurity in an era of user-based risks

proofpoint.com

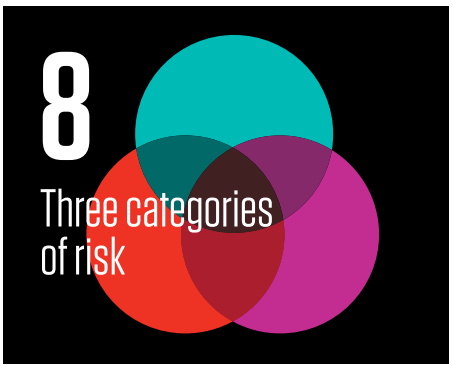
INTRODUCTION

For many of us, 2021 began on a hopeful note as COVID-19 vaccines started to roll out. And while much of the year consisted of a stuttering journey back toward normality, the story was quite different for the world's cyber criminals.

In cybersecurity terms, 2021 was the breakout year when financially motivated cyber crime became a national security issue. It was also a year marked by ceaseless creativity from threat actors who worked to undermine digital defenses and take advantage of the many opportunities presented by an uncertain world.

This report will look at how ransomware caused gas shortages on the east coast, why a Justin Bieber tour might have put you on the phone with a malware distributor, and what an increase in SMS phishing means for mobile security. We'll also explore the evolving relationship between malware distributors and one of the world's most successful ransomware gangs, and how legitimate cloud services now provide the infrastructure for a majority of malicious activity.

After a year that changed the world, it turns out that some things stayed the same. Attackers remained as unscrupulous as ever, making protecting people from cyber threats an ongoing—and often fascinating—challenge.



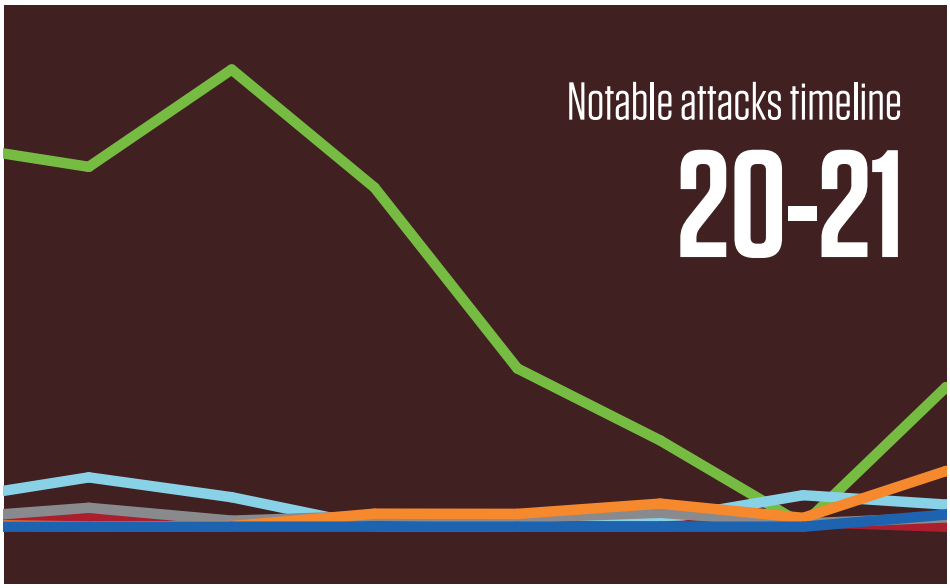


Table of Contents

ABOUT THIS REPORT

Since 2014, the Human Factor report has explored a simple premise: that people—not technology—are the most critical variable in today's cyber threats.

Since then, this once-contrarian notion has become a widely acknowledged reality. Cyber attackers target people. They exploit people. Ultimately, they are people.

To effectively prevent, detect and respond to today's threats and compliance risks, information security professionals must understand the people-centric dimensions of user risk: vulnerability, attack and privilege. In practical terms, this means knowing:

- Where users are most vulnerable
- How attackers are targeting them
- The potential harm when privileged access to data, systems and other resources is compromised

Addressing those elements—the human factor of cybersecurity—is the core pillar of a modern defense.

EACH DAY WE ANALYZE TRILLIONS OF DATA POINTS ACROSS DIGITAL CHANNELS THAT MATTER

2.6B
email messages

49B
URLs

1.9B
attachments

28.2M
cloud accounts

1.7B
suspicious mobile messages

What this report covers

This report dives deep into each of three facets of user risk. It examines key developments in the threat landscape. It explores the developing relationship between cyber criminal groups and what it means for the rest of us. And it explains how a people-centric defense can make users more resilient, mitigate attacks and manage privilege.

This report covers threats detected, mitigated and resolved during 2021 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.

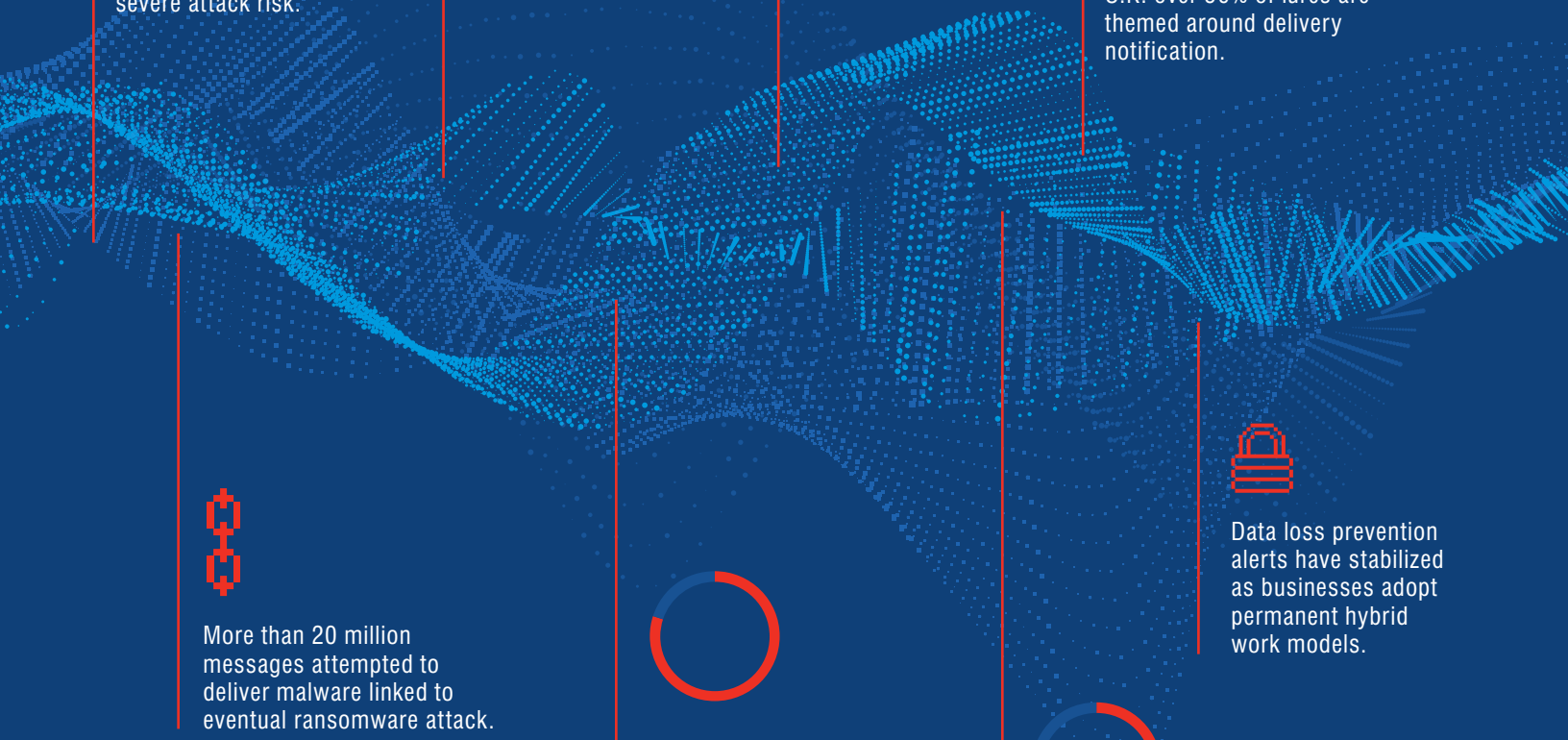
Scope

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, 28.2 million cloud accounts, 1.7 billion suspicious mobile messages and more. Together, this amounts to trillions of data points across the digital channels that matter.

This report covers January 1 to December 31, 2021. 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.

KEY FINDINGS



50%

Managers and executives make up only 10% of users, but almost 50% of the most severe attack risk.

Malicious URLs are 3-4x more common than malicious attachments.

100k

Attackers attempt to initiate more than 100,000 telephone-oriented attacks every day.

Smishing attempts more than doubled in the U.S. over the year, while in the U.K. over 50% of lures are themed around delivery notification.

Data loss prevention alerts have stabilized as businesses adopt permanent hybrid work models.

More than 20 million messages attempted to deliver malware linked to eventual ransomware attack.

+80%

of businesses are attacked by a compromised supplier account in any given month.

35%

35% of cloud tenants that received a suspicious login also saw suspicious post-access activity.

DEFINING CYBERSECURITY RISK

In cybersecurity, risk is defined as:

In other words, a people-centric risk model takes into account:

- The probability of someone being attacked (attacks)
- The likelihood that they will interact with a piece of malicious content sent to them (vulnerability)
- How severe the impact could be if their credentials are compromised (privilege)

This report focuses on each of these elements through the lens of our people-centric model of user risk—vulnerability, attacks and privilege—with recommendations on ways to mitigate each.

A deeper dive into user risk

Just as people are unique, so is their value to cyber attackers—and risk to employers. They have distinct vulnerabilities, digital habits and weak spots. They're attacked in diverse ways and with varying frequency. And they have different levels of access privileges to data, systems and resources. These intertwined factors determine a user's overall risk.

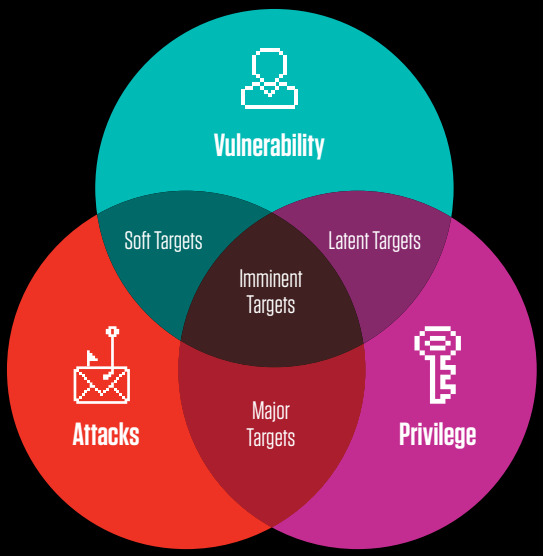


Figure 1. How three types of risk interact.

Vulnerability

Users' vulnerability starts with their digital behavior—how they work and what they click. Many employees work remotely or access company email through their personal devices. They may use cloud-based file storage and install third-party add-ons to their cloud apps. They may handle data in riskier ways than their peers. Or they may be especially receptive to attackers' email phishing tactics.

Attacks

Not all cyber attacks are created equal. While any can be harmful, some are more dangerous, targeted or sophisticated than others. For example, some malware is more closely tied to ransomware operators, while a message from a compromised supplier has higher potential for financial loss than a request for gift cards. Indiscriminate "commodity" threats might be more numerous than more advanced ones, but they're usually well understood and more easily blocked. (Make no mistake, though. They can cause just as much damage.) Other threats might appear in only a handful of attacks. But they can pose a more serious danger because of their sophistication or the people they target.

Privilege

Privilege measures all the potentially valuable things people have access to, such as data, financial authority, key relationships and more. Measuring this aspect of risk is crucial because it reflects the potential payoff for attackers—and harm to organizations if compromised. The user's position in the organizational chart is naturally a factor in scoring privilege. But it's not the only factor—and often, not even the most important one. For attackers, a valuable target can be anyone who enables them to achieve their goal.

Section 1

Vulnerabilities

Assessing user vulnerability is an essential part of good cyber defense. To manage this aspect of our risk model, you need to know who in your organization is most likely to fall for a well-crafted piece of social engineering.

Social engineering works by exploiting human nature. Most people cope with the volume of decisions they have to make day-to-day using a mixture of heuristics and cognitive biases. And as the demands on our time and attention increase, so does our reliance on these rules of thumb. Cyber attackers recognize this, choosing targets with demanding jobs or working in high-pressure departments. They know that these victims may not have the time to fully scrutinize a message before clicking a link or downloading an attachment.

Quantifying Vulnerability

The easiest way to quantify vulnerability without putting your organization at risk is to test employee responses to simulated threats. Data collected last year from our phishing simulation tool showed a failure rate range of between 4%–20% depending on the type of attack being tested.

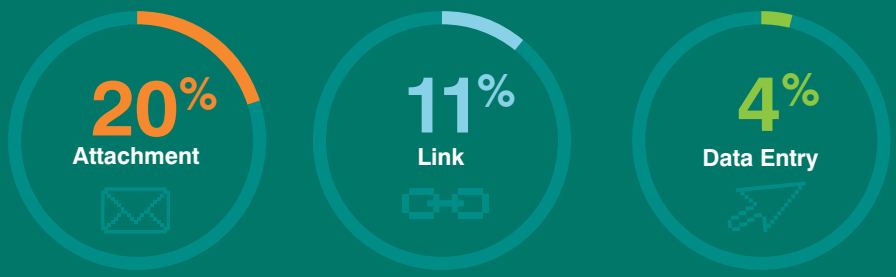


Figure 2. Failure rates for simulating phishing attack types, 2021.

Viewed by department, failure rates vary from 6%–12% with the average being 11%. Several high-profile (and highly targeted) departments fill out the lower reaches of the table, including IT, legal and finance, though there are several potentially lucrative targets at or above the average rate, including operations and purchasing.

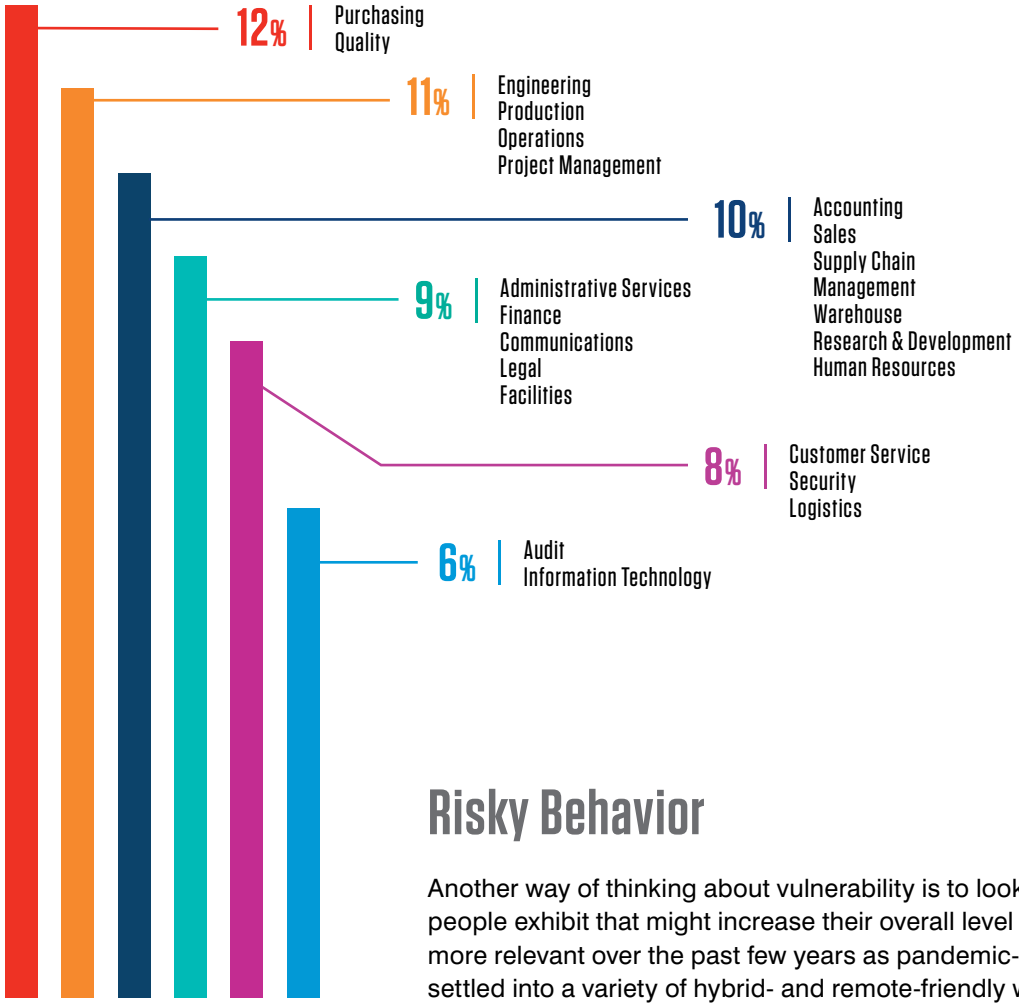


Figure 3. Average phishing simulation failure rate by department, 2021.

Risky Behavior

Another way of thinking about vulnerability is to look at the kinds of behaviors people exhibit that might increase their overall level of risk. This has become even more relevant over the past few years as pandemic-inspired work from home has settled into a variety of hybrid- and remote-friendly workplaces. One area where the pandemic has had a notable impact is the risk posed by insider threats. The Ponemon Institute's 2022 report on this subject measures a 44% increase in insider threat incidents since 2020.

According to the results of our annual **State of the Phish report**, almost half of working adults shifted to a remote working environment as a result of COVID-19. One thing to emerge clearly from this shift is a definite mingling of business and personal. And this is perhaps nowhere more apparent than in how people use their personal and work devices. Nearly three-quarters said they used a personal device for work purposes, while 77% said they accessed personal accounts on an employer-issued device. Most concerning of all, 55% of respondents admitted that they allow friends and family to use their work computers and phones.

Personal devices may not have the same level of protection as work devices, and friends and family may not be trained to an appropriate level of security awareness. How to resolve the tension between convenience and security is an ongoing question, but it's beyond doubt that work-from-home has significantly altered the stage on which most cyber crime plays out.

Section 2

Attacks

In this section we examine the specific strategies, techniques and tools used by **THREAT ACTORS** during 2021. Some of the campaigns featured in this section are noteworthy because of their sheer volume, others for the ingenuity they display. In almost every case, victims faced the possibility of severe financial loss, reputational damage or both.

In our risk model, **attacks** are the trigger point at which **vulnerability** and **privilege** are exposed. The more sneaky, sophisticated or compelling the attack, the more likely it is that even the most security-aware victim will fall prey to them. Attackers are always evolving, probing for defensive gaps. So, it's essential that automated defenses are dynamic enough to respond to novel threats. Security training should also be updated regularly with details from the latest campaigns.

We'll start out looking at some of this category's landscape features before moving onto email, mobile and cloud-based threats.

THREAT ACTOR:

An industry term describing an individual or group responsible for launching cyber attacks. Threat actors can be financially motivated cyber criminals, state-aligned advanced persistent threats (APTs) conducting espionage and sabotage, or "hacktivists" working to further a political or social agenda. In a few cases, the lines are blurred, as some APT actors have also been observed stealing money.

Russia's cyber confederates

The 2022 Russian invasion of Ukraine began as we started writing this report, and while it isn't strictly within our stated timeframe, the consequences of that event are so profound that they demand attention.

Before the invasion began, destructive wiper malware was deployed against Ukrainian organizations and key communications infrastructure. And once the invasion began, our researchers observed a significant increase in the activity of known Russia-aligned advanced persistent threat (APT) actors.

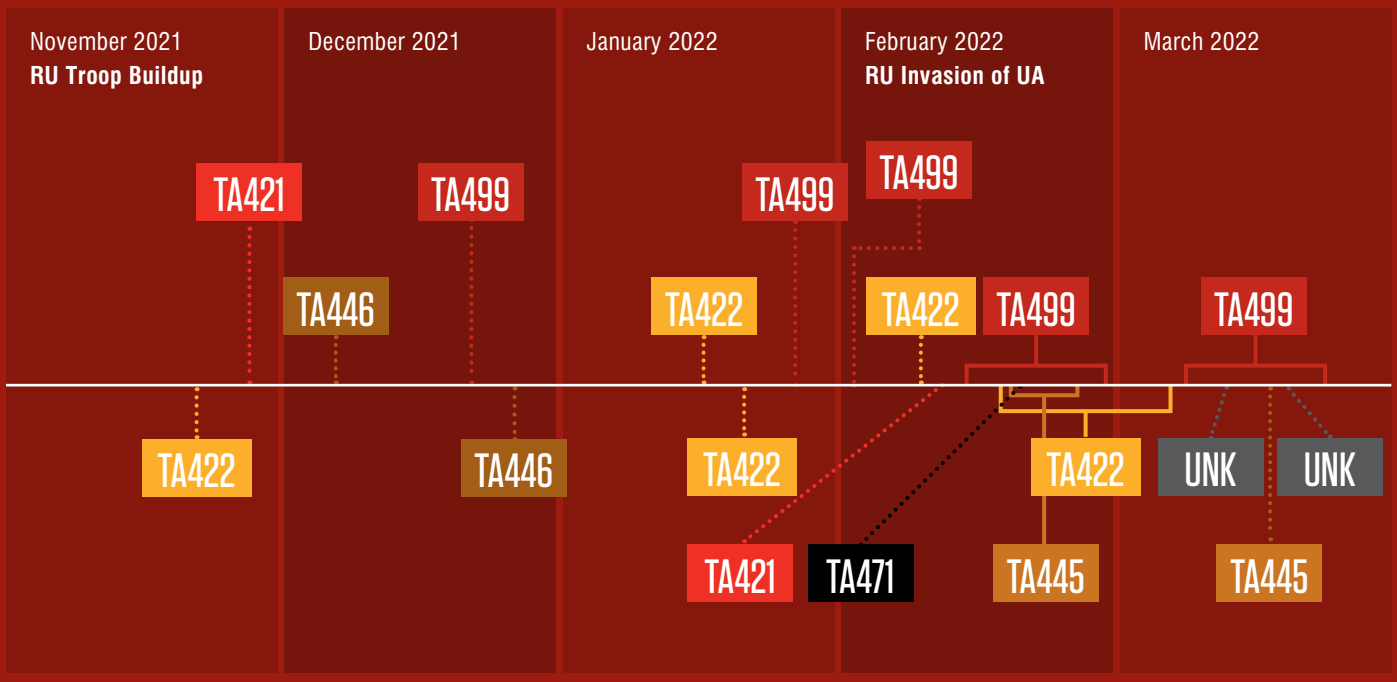


Figure 4. A timeline of Russian-aligned APT activity, November 2021 to March 2022.

APT groups aligned with other national interests have also responded to the situation. In the weeks since the invasion began, we have seen activity from Belarus- and China-aligned actors, specifically targeting European governmental organizations involved in asylum and other relief efforts.

As we'll see later in this report, the line between physical and cyber warfare isn't the only one that's been crossed during the invasion. With a large amount of financially motivated cyber crime activity originating from these two countries, many of the world's most successful cyber criminals have been forced to pick sides. Prior to the start of this conflict, most of these groups avoided targeting victims in Russia, Ukraine and neighboring territories—possibly in return for authorities turning a blind eye. But since mid-February, we've seen a sharp rise in the incidence of Russia- and Ukraine-based employees of multi-nationals being targeted. In the case of people in Russia, they are often now as likely to be attacked as employees anywhere else in the world.

Understandably, APT attention garners a lot of headlines. But it's important to remember that only a low single-digit percentage of our customers ever see activity from a state-sponsored actor (let alone one aligned with a global superpower). With a small number of exceptions, when cyber mayhem knocks at your door, it will probably look more like a common criminal than a hostile nation.

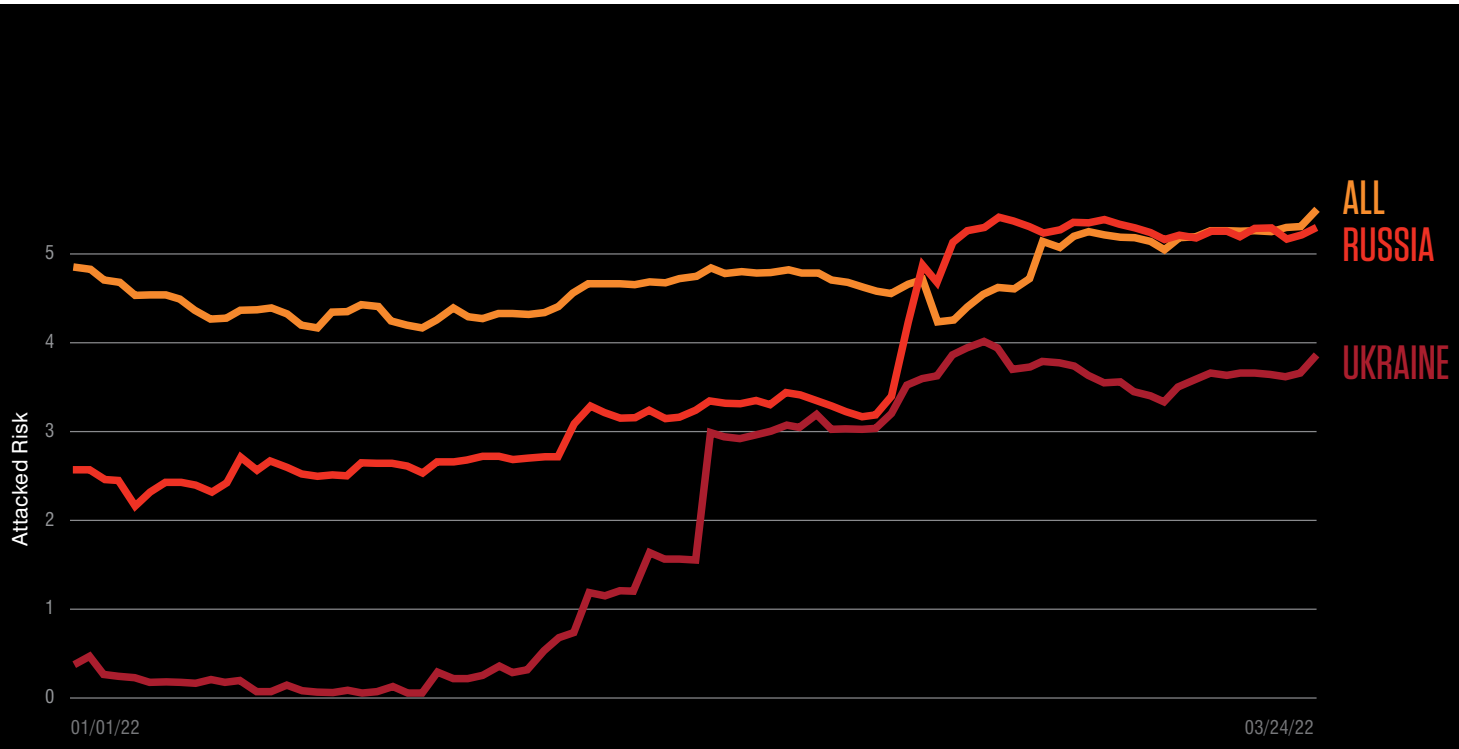


Figure 5. Attack risk on employees in Russia, Ukraine and worldwide (based on Proofpoint attack index) for employees of a large multinational company, January to March 2022.

Emotet rises again

In January 2021, an international law enforcement operation took down the **EMOTET** botnet. Overnight, a threat responsible for nearly 10% of the previous year's malicious email activity was gone.

But cyber criminals are nothing if not opportunistic, and other operators stepped up to fill the gap. In 2021, a group we call **TA511** emerged as the undisputed volume leader for malicious email, sending three times as many messages as the next most prolific attacker.

EMOTET:

Before the 2021 takedown of its infrastructure, Emotet was the world's most frequently distributed malware. Since returning at the end of the year, Emotet's developers have been linked with both TrickBot and Conti groups.

TA511:

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

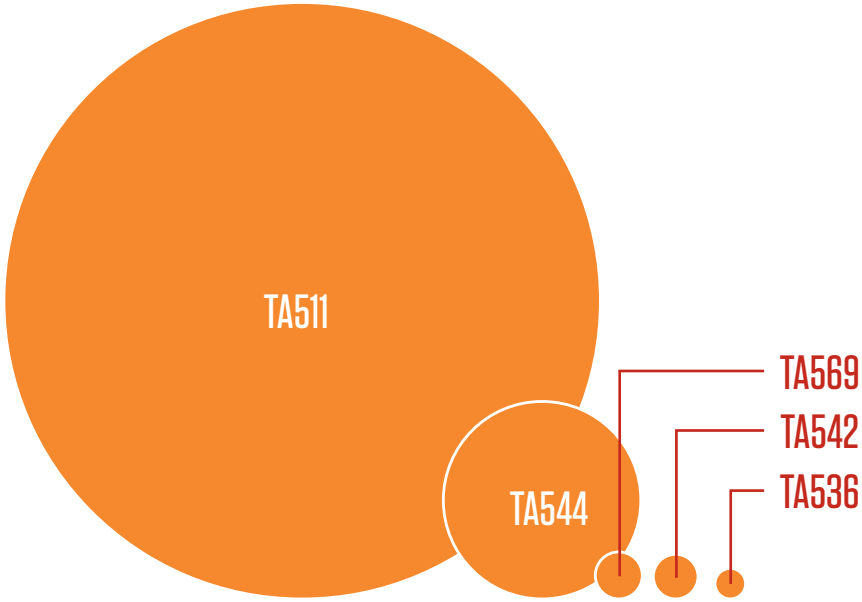


Figure 6. Top threat actors by message volume, 2021.
(Circle sizes represent relative message volume.)

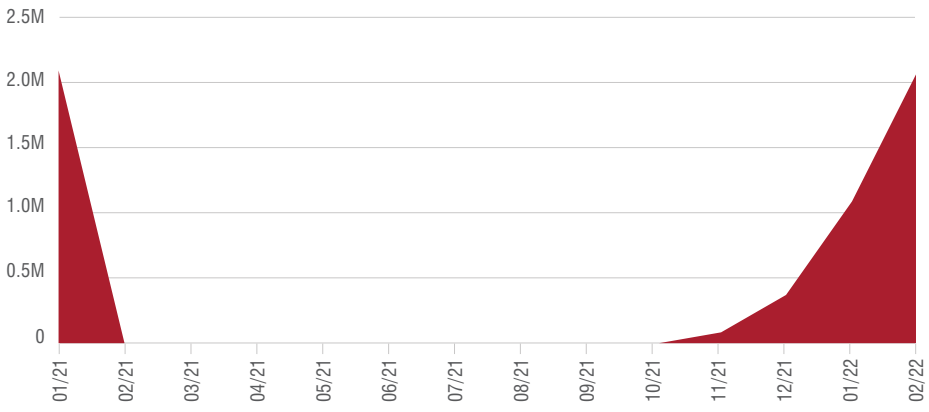


Figure 7. Emotet message volume, January 2021 to February 2022.

In November 2021, Emotet resumed activity, but the malware did not immediately reach 2020 levels. For the first few months after the group's return, TA542 (the threat actor behind Emotet) message volumes only numbered in the tens of thousands. But as of March this year, Emotet appears to be ramping back up to previous heights, with several campaigns distributing close to a million messages each. Later in this report, we'll explore the reasons behind this in detail, as recent research has established solid links between Emotet and the Conti ransomware group.

As TA511's tool of choice, **TORDAL** unsurprisingly topped our list of most common malware. While the relationship between TA511 and Tordal is exclusive, most of the other malware rounding out the top five has multiple distributors (Ficker Stealer is typically observed as a secondary payload downloaded by Tordal.) As such, they might be encountered in very different contexts depending on the attacker's preferred social engineering tactics. For example, **FORMBOOK** was distributed using COVID-19 lures, generic business request-for-information emails, and even one campaign in which the attacker masqueraded as a soccer agent representing young players from Africa and South America.

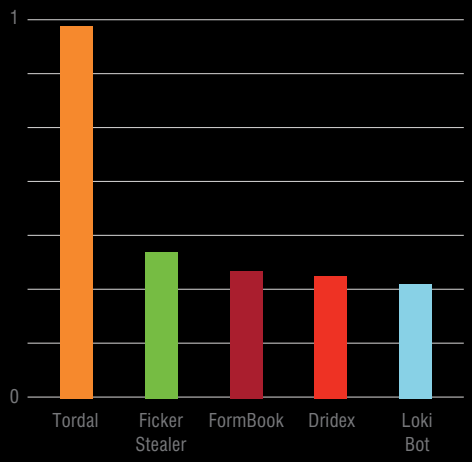


Figure 8. Top malware by message volume, 2021.
(Note: Scale is normalized to protect confidential Proofpoint data)

TORDAL:

Also known as Hancitor, Tordal is a downloader for secondary malware, including Cobalt Strike on at least one occasion. The initial version of Tordal used the anonymous Tor network for communications, while later versions have used plain HTTP.

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.

Social-engineering strategies

With the pandemic continuing to surge and recede throughout the year, COVID-19 lures remained a go-to theme. The first spike coincided with the widening availability of vaccines in the early part of the year, which led to an eventual decline in campaign volume as more of the population became vaccinated. However, the summer surge of Delta variant led to a further spike in activity.

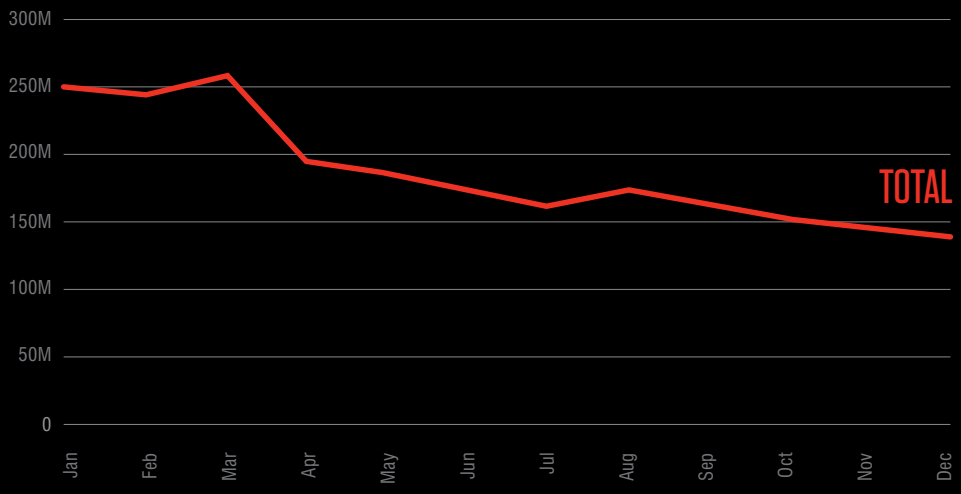


Figure 9. Volume of pandemic-themed messages, 2021.

TA451:

An Iran-aligned threat actor, active since at least 2017. This group uses phishing to gain initial access, often favoring job lures aimed at defense contractors. Over the years the group has distributed a variety of commodity and proprietary malware.

TA425:

Operating out of India, this attacker is believed to be state aligned. Typically, it targets universities, think tanks, tech companies and governments across a range of countries.

TA421:

A state-sponsored actor originating from Russia. According to FBI, CISA and NSA, this group is known to be associated with Russia's Foreign Intelligence Service (SVR). As such, its methods are sophisticated, making use of proprietary malware.

COBALT STRIKE:

This legitimate "red team" tool is used by security teams to test network security. It is also popular with threat actors, who use cracked or illicitly purchased versions of the software as part of their attack chains.

Figure 10. Landing page used by TA425 spoofing Pakistan's National Immunization Management System.

Although the majority of pandemic-themed malicious activity was conducted by financially motivated criminals, some state-sponsored attackers also used COVID-19 lures. In early 2021, Iran-aligned actor **TA451** conducted a phishing campaign against a U.S. defense contractor. Later in the year, India-aligned actor **TA425** targeted users in Pakistan with booster shot lures. Russian state-sponsored attacker **TA421** also got in on the act, targeting government organizations around the world with COVID-19 lures that ultimately tried to deliver **COBALT STRIKE**.

Squid Game swindlers: how attackers piggyback pop culture

Beyond COVID-19, 2021 also saw the usual sampling of perennial themes around tax returns, job listings and seasonal holidays. But rather than focus on the familiar, we're now going to take a closer look at an example that shows just how responsive attackers can be to social and cultural currents.

"Squid Game" was a runaway success for Netflix when it launched in late September. In less than a month, viewers spent a total of 1.65 billion hours watching the show, making it Netflix's most popular content ever. By October, cyber criminals were taking advantage, with high-volume attacker TA575 sending Squid Game-themed emails to victims in the U.S. The emails promised early access to the next season or even the opportunity to be cast in future episodes.

If victims were persuaded to download the attached Microsoft Excel file and enable macros, the Dridex banking Trojan was installed on their system.

Campaigns like this can blip in and out of the threat landscape as quickly as the cultural moments that inspired them. Keeping track of them is hard even for a well-resourced threat intelligence group, so organizations will need to rely on automated email defenses capable of spotting dynamic threats as they emerge and recede.

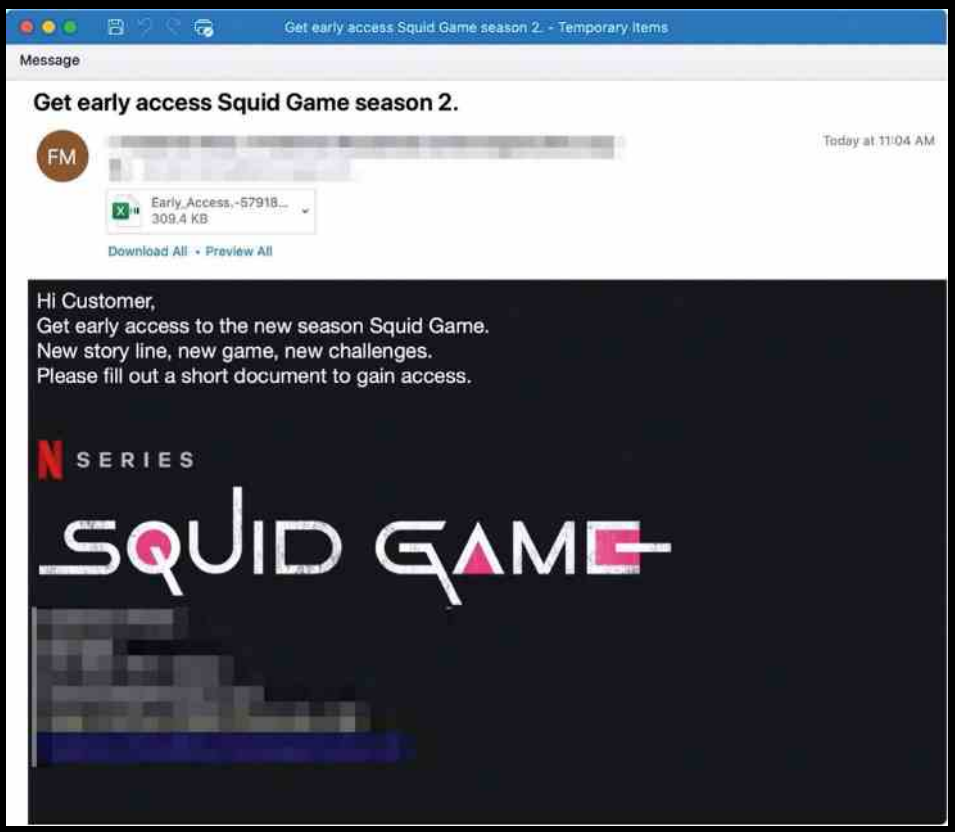


Figure 11. An example Squid Game email lure.

Ransomware: a year in review

Ransomware hit the headlines in 2021 like never before, as a series of prominent attacks showed that this cyber threat can prevent people from filling their cars with gas, putting food on the table, or even getting medical treatment. A recent report by the FBI looking back at last year counts at least 649 ransomware attacks against critical infrastructure organizations.[1]

The year did see a handful of wins in the fight against ransomware. Law enforcement recovered around half the money paid by Colonial Pipeline, while the Kaseya supply chain ransomware attack was resolved quickly with the release of a decryption key. But despite these mini-victories, the sense remained of a shadowy cyber criminal elite striking at will against some of the world's largest and most essential businesses.

But in late February 2022, an unexpected spotlight fell on the ransomware underworld. An unknown Twitter user with the handle @ContiLeaks published chat logs and other data related to the **CONTI** group. Researchers began poring over the information, quickly realizing that the leaks provided an unprecedented look at the inner workings of one of the world's most successful—and secretive—ransomware operations.

One thing that immediately stands out in the leaked chats is Conti's organizational structure. The group operates like an ordinary business, with salaried employees, vacation allowances and a human resources department. It also appears to be rigidly hierarchical, with several layers of management. The leaks also contain endless messages about working conditions, pay and other everyday complaints.

Crucially, the group's senior management seems to have created silos between departments, so the left hand doesn't always know what the right hand is doing. An exchange from October 2020 illustrates this, with two Conti associates expressing surprise at the similarity between their campaigns and those of **RYUK**, a ransomware group they believe to be entirely separate. This suggests a lack of awareness at lower levels of the many points of intersection between Conti, Ryuk and the various malware operators they use to provide initial access.

Initial access providers are now an integral part of the ransomware ecosystem. Rather than trying to deliver ransomware directly via email, the operators of Conti, REvil and others use existing malware compromise to infect devices and systems. In last year's report we talked about the relationship between various malware groups and ransomware operators, but the Conti leaks provide the firmest evidence yet of a hand-in-glove relationship between malware botnets and ransomware.

CONTI:

One of the world's most successful, and by some accounts ruthless, ransomware operators. It came to prominence in early 2021 with attacks on healthcare services in the U.S. and Ireland, a sector traditionally considered off-limits.

RYUK:

A strain of ransomware closely linked to the TrickBot banking Trojan. Recent leaks suggest that Ryuk's developers are also behind Conti ransomware.

REvil:

This ransomware group entered the public eye after its attacks on 22 municipalities in Texas. In January 2022, Russian authorities made several arrests and claimed to have dismantled REvil's infrastructure. But the group reemerged in April 2022 amid Russia's invasion of Ukraine.

DARKSIDE:

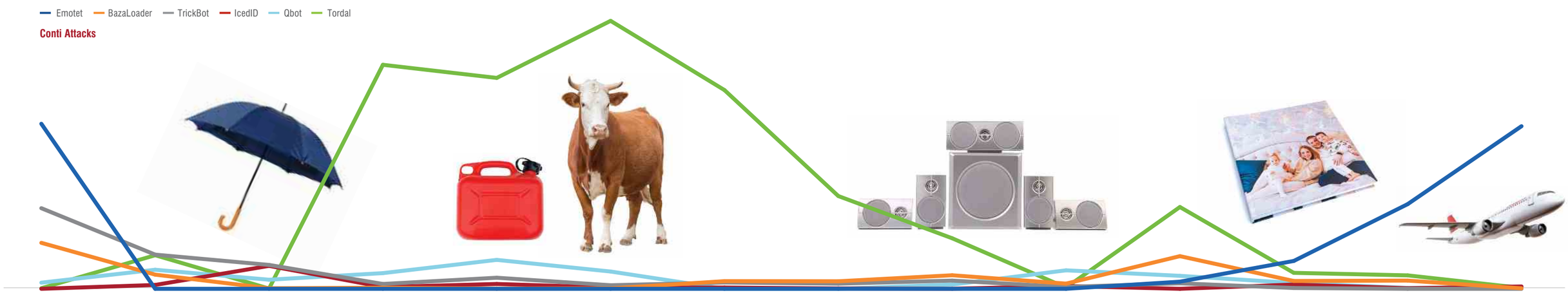
Darkside gained sudden worldwide recognition when its ransomware was named responsible for the Colonial Pipeline attack. The group claimed to be disbanding in June 2021, saying scrutiny had grown too great. But it may have simply rebranded itself as BlackMatter. The FBI has also linked Alphv and BlackCat to the group.

1 FBI. "2021 Internet Crime Report." April 2022.

THE HUMAN FACTOR 2022 \ REPORT

Initial Access Facilitator Malware + Notable Ransomware Attacks

Message volumes of malware known to be used by Conti for initial access and notable Conti attacks, January 2021 to February 2022



Jan 2021

The Polish developer behind some of the world's most popular RPG video games was hit with HelloKitty ransomware. Its servers were encrypted, and source code was stolen and put up for sale.

Feb 2021

Mar 2021

One of the largest insurance companies in the U.S. reportedly paid a ransom of $40 million after ransomware attackers accessed its systems through a fake browser update.

Apr 2021

A public school district in Florida was hit by the Conti group, which initially demanded $40 million to unlock IT systems. Attackers usually research their victims' finances, but this amount was substantially more than the district could afford to pay.

May 2021

In one of the year's most high-profile attacks, DarkSide ransomware caused a fuel pipeline serving the East Coast to shut down temporarily. The company paid a $4.4 million ransom, of which around half was recovered by law enforcement.

A European national health services provider was hit by the Conti group, causing treatment delays after around 80% of the agency's IT systems were encrypted.

Jun 2021

REvil's attack on a large meat processor led to concern about potential food shortages, forcing the company to pay an $11 million ransom.

Jul 2021

An attack on a managed software provider by REvil raised the prospect of thousands of potential downstream victims. Swift law enforcement action led to a takedown of REvil's infrastructure and the release of a decryption key to victims.

Aug 2021

A global IT and management consultancy firm had its systems encrypted and data stolen by the LockBit group. The company was able to restore from backups without paying the $50 million ransom demand, but the group retaliated by leaking the data.

Sep 2021

Two large manufacturers of audiovisual electronics were hit by the Conti and BlackMatter ransomware groups.

Oct 2021

One of the largest networks of local television stations in the U.S. was hit by an attack that caused disruption to broadcasts. Attackers used Active Directory to move between different channels owned by the network.

Nov 2021

Dec 2021

An online photography platform was hit by Conti, compromising employee data and disrupting some manufacturing. The group leaked data it stole during the breach.

Jan 2022

Feb 2022

The BlackCat group hit a global aviation operations business, disrupting flight operations. The company had contingency systems in place and was able to restore systems without significant delays.

A popular snack brand in the UK was attacked by Conti, interfering with ordering and dispatch of products to retailers.

BLACKMATTER:

Believed by some to be a rebrand of DarkSide, this ransomware-as-a-service operator has close ties to the Colonial Pipeline attacker, though members have since claimed that they are merely associates of other groups.

TRICKBOT:

After emerging in 2016, this banking Trojan achieved widespread prominence. This may have been its downfall, as TrickBot's developers announced plans to retire the malware at the start of 2022.

BAZALOADER:

First discovered in April 2020, BazaLoader is used to download other malware. It is still being actively developed and is believed to provide initial access to Conti ransomware.

The chart on pages 20–21 shows message volumes for prominent malware strains widely believed to provide initial access for one or more ransomware operators. It also lists several of last year's highest profile ransomware attacks. In most cases the connections between malware and ransomware operators are anecdotal or correlative (though researchers have begun to tease out the connections between the malware distributor commonly known as **FIN7** and ransomware operators **DARKSIDE**, **BLACKMATTER** and **REvil**). But because of the Conti leaks, we now have definitive proof that Conti makes extensive use of **BAZALOADER**, **TRICKBOT** and Emotet. In the case of the latter two, it seems likely that the decline and shutdown of TrickBot and the sudden resurgence of Emotet at the start of 2022 are directly related, with the latter now in line to be Conti's initial access malware of choice.

The overlap between TrickBot, Emotet and Conti demonstrates that one of the most important ways to defend against this kind of extortion is to prevent malware getting a foothold in the first place. And since all the malware mentioned in the chart above is distributed via malicious email and relies on human vulnerability, having strong email defenses and resilient users are vital first steps in keeping ransomware attackers out of your environment.

Big Tech will keep us safe—or will it?

Cyber attackers don't just rely on their own ingenuity to inspire trust. They also include legitimate services like Microsoft OneDrive, Google Drive and Dropbox in their campaign infrastructure, both because these services are convenient and because victims may be more inclined to trust a link from a familiar service.

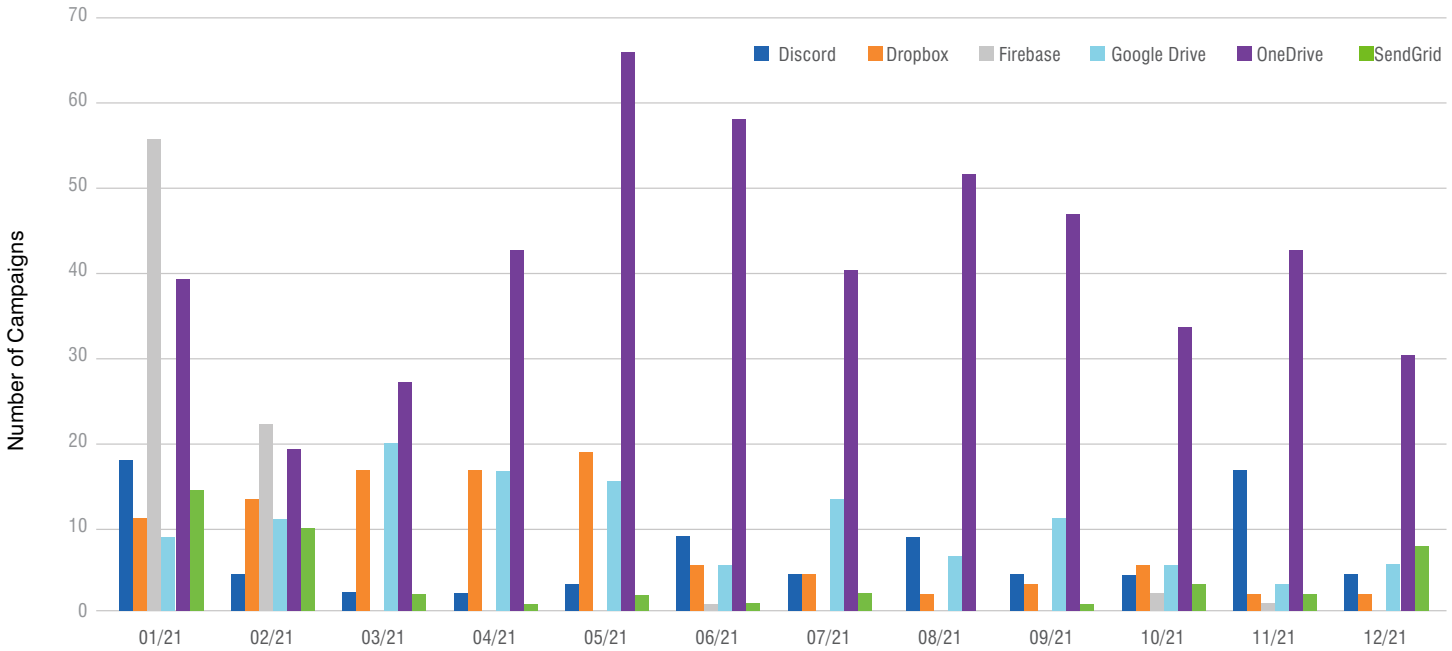


Figure 12. Campaigns using legitimate services, 2021.

TA571:

A financially motivated malware distributor targeting multiple industries in North America. First observed in mid-2019.

URSNIF:

A widely used banking Trojan that evolved from a malware strain called Gozi, whose source code leaked in 2015. Ursnif is the most popular of several Gozi-derived variants, which include Dreambot, ISFB and Papras.

TA579:

A financially motivated malware distributor targeting multiple industries in North America. First observed in mid-2021.

Microsoft OneDrive and Google Drive were the most common pieces of legitimate infrastructure used by the top-tier cyber crime actors we track. Typically, URL links pointing to these services are either included directly in the body of a malicious message or embedded in an attached PDF. As Google and Microsoft's webmail products both include in-built virus scanning, it is possible that victims assume files served using these companies' infrastructure undergo similar safety checks.

Among high-volume cyber criminals, the group we track as **TA571** makes extensive use of both OneDrive and Google Drive to distribute malware. TA571's campaigns typically involve an emailed link to a ZIP file hosted on one of the two services. The compressed folder contains an Excel file which drops **URSNIF** malware if macros are enabled.

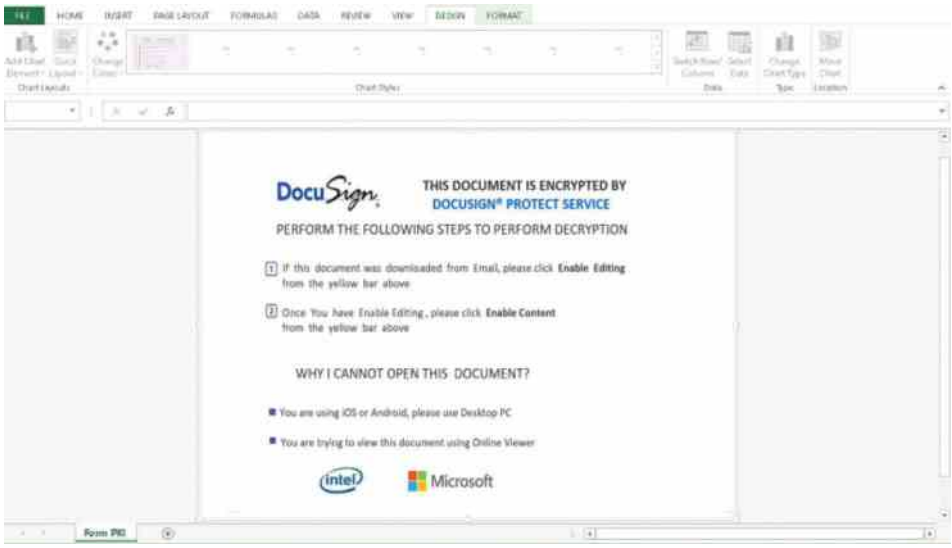


Figure 13. A TA571 payload document.

TA571 and the actor we track as **TA579** also make heavy use of OneDrive to distribute BazaLoader—making legitimate infrastructure an integral component of campaigns known to provide initial access to the likes of Conti and Ryuk.

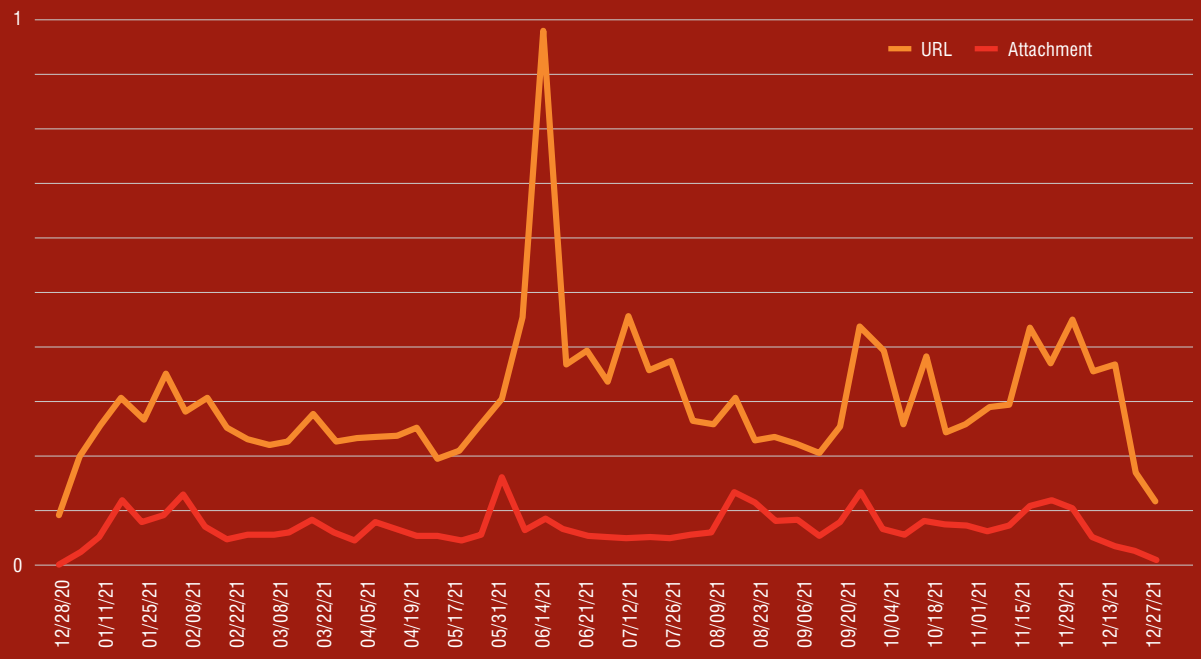


Figure 14. URL and attachment attack volume, 2021.
(Note: Scale is normalized to protect confidential Proofpoint data)

Email threats

Email is universal, critical to modern business and inherently insecure. Created long before the internet was mainstream, email was never developed with privacy or security in mind. In the 45 years since, it has become an essential pillar of modern business communications—and a magnet for all kinds of attacks.

Fear of attachment—and the links that bind

A dubious attachment arriving in your inbox is still how many of us think malware spreads. But according to our data, emails containing malicious links are between three to four times more common than attachment-based attacks.

While URL-based threats might be more prevalent, data from our recent State of The Phish report shows that failure rates for attachment-based attacks are nearly twice as high. (In other words, users are twice as likely to download a malicious file as they are to click on a malicious link.)

Most people now understand that cyber attacks are a risk to both businesses and individuals. But in such a fast-moving environment, received wisdom can be counterproductive. Regular training that emphasizes the latest tactics, techniques and procedures being used by attackers is essential to keeping people aware of the danger, bolstering your first line of defense.

"Friendly" fraudsters

Trust is an essential component of social engineering. To persuade someone to interact with a piece of malicious content, an attacker has to convince them to trust the source—or at least to suspend distrust long enough to succumb. Over the past year, we've seen a growing trend of cyber criminals going to surprising lengths to develop rapport with victims before attempting to initiate an attack.

The most common form of conversational threat involves task-oriented lures—a form of business email compromise (BEC). These attacks typically start with a benign message asking if the recipient is available to perform a simple task. If the victim engages, the attacker asks for money, gift cards or a change to an invoice. In an average month, we see around 80,000 task-oriented malicious emails.

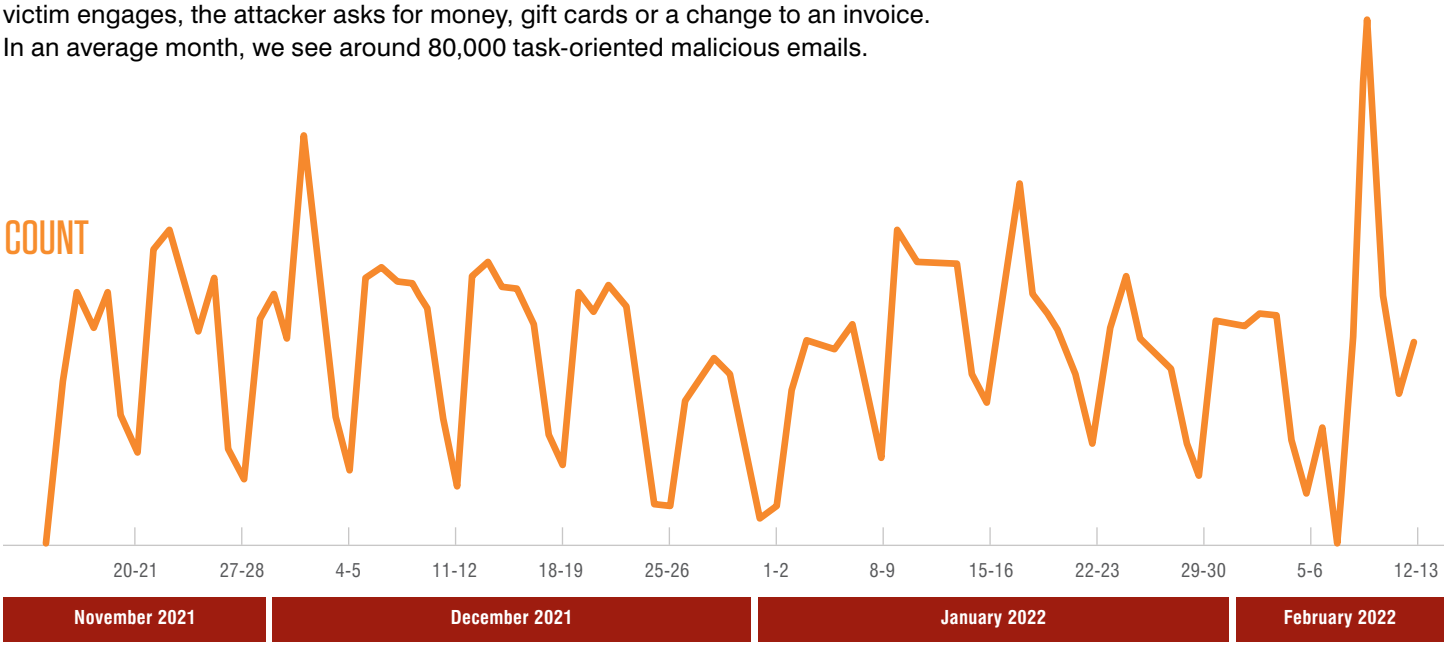


Figure 15. Quick task BEC attempts.

TA576:

Known to target accounting and financial institutions during tax season, this threat actor attempts to deliver remote access Trojans using tax-related email lures. First observed in 2018.

A conversational approach can also be used to distribute malware. The attacker we track as **TA576** is notable for low-volume campaigns that primarily target accounting and finance organizations. The lures typically purport to be requests for help preparing taxes. If someone at the victim organization responds, TA576 replies with an email containing a URL that links to the NetWire remote access Trojan.

Figure 16. Example of a task-oriented malicious email.

DEMONWARE:

A ransomware strain notable for its operator's attempts to recruit insiders to initiate attacks.

TA499:

A threat actor believed to be aligned with the Russian state. It specializes in embarrassing dissident politicians, celebrities and athletes. Attacks are initiated via benign emails that attempt to solicit information and set up bogus video chats.

TA453:

An Iran-aligned advanced persistent threat (APT) actor. The group has historically pursued Islamic Revolutionary Guard Corps (IRGC) priorities, targeting dissidents, academics, diplomats and journalists.

The biggest ransomware threats aren't typically delivered directly through email. But that doesn't mean that ransomware gangs aren't making use of the channel. In summer 2021, we saw a ransomware group called **DEMONWARE** sending out messages trying to entice employees to infect their own machines in return for a cut of the profits. Beyond inviting the recipient to join a criminal enterprise, the emails contained no other malicious elements. Interested employees were told to contact a Telegram chat address for further instruction.

Finally, 2021 also saw a number of instances where APTs, or state-sponsored attackers, used lengthy conversational phases to lay the groundwork for an attack. A campaign by Russia-aligned actor **TA499** in early 2021 used rapport-building emails to entice recipients into phone or video-chat conversations. The likely goal was to create content showing the Russian opposition in a negative light. Similarly, Iran-aligned attacker **TA453** has made frequent use of conversational campaigns, including phone calls, to build rapport ahead of trying to solicit information and steal credentials.

Hijacking the conversation

One of the easiest ways to inspire trust in a potential victim is to take on the appearance of a trusted contact. For this reason, thread or conversation hijacking is a popular technique with a number of high-volume, financially motivated attackers.

Thread hijacking relies on the attacker already having access to a compromised inbox, either through credential phishing, an existing malware infection or password spraying. In the case of the more prolific botnets, this process is automated. Scraped email including “Re:” or “Fwd:” often have content injected at the top of the thread and are sent back to users in the chain. BEC attacks frequently make use of the technique as well, with a more hands-on approach allowing for a greater degree of tailoring messages to their intended victims. Once they have access to an inbox, the attacker responds to an existing email thread, usually with a malicious attachment, URL or a request for the recipient to perform an action on the attacker’s behalf.

Because the email is being sent from a legitimate account, the message has all the hallmarks of a genuine correspondence, making it much more likely that the recipient will comply.

Malware Campaigns Using Threat Hijacking in 2021

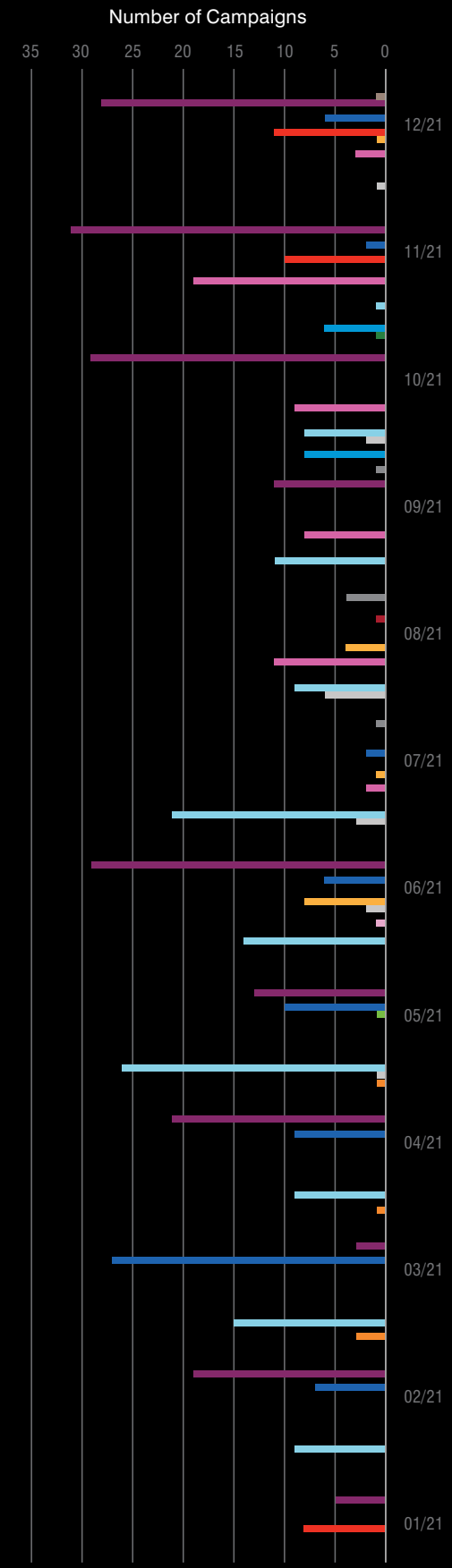


Figure 17. Malware campaigns using threat hijacking, 2021.

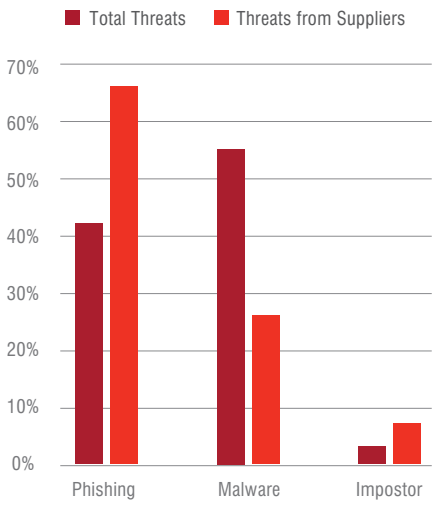


Figure 18. Supplier threats vs. general landscape threats (30-day period, February 22 to March 23, 2022).

Breaking the supply chain

Attacks sent from a supplier domain have a different complexion from other attacks. In any given month, more than 80% of our customers receive a threat that appears to originate from one of their suppliers. That figure tracks only a little lower than the percentage of customers who received a threat of any kind.

Where supply chain threats differ most is in the likely angle of attack. As this chart shows, compared to the general landscape, supplier-originating threats are more likely to be phishing or impostor attacks. And they are much less likely to involve malware.

Phishing and impostor threats are particularly reliant on exploiting the victim's trust and familiarity with the apparent sender. This dynamic becomes even more visible when we look at the distribution of high, moderate and broad[2] targeted threats sent from supplier domains. All things being equal, you might expect organizations to receive fewer highly targeted threats, as reconnaissance is time-consuming, leading to lower message volumes. However, with a spoofed or compromised supplier domain, cyber criminals are more easily able to put together detailed attacks, leading to a disproportionate number of highly targeted attacks.

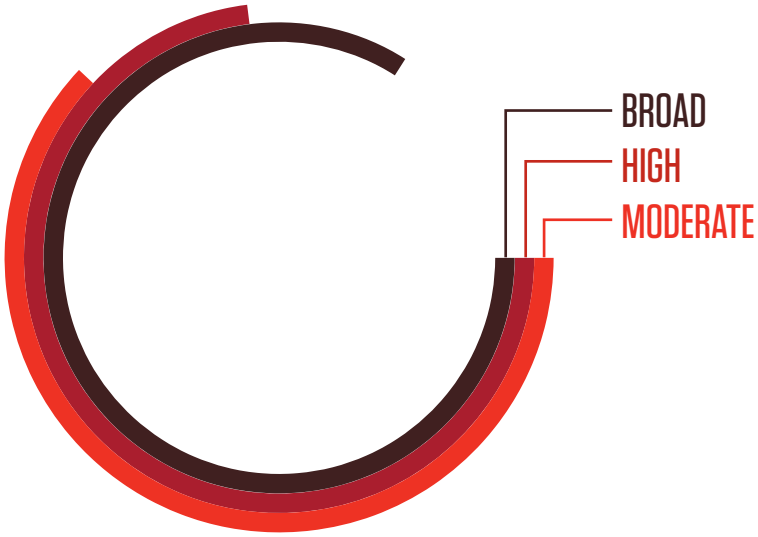


Figure 19. Distribution of attack types from supplier domains (30 days).

While malware attacks from compromised suppliers can't be ruled out, awareness training needs to pay particular attention to the risk of supplier accounts being used for targeted social engineering attacks. Cyber criminals do their homework and approach like a known partner or associate, making compromised suppliers particularly hard to defend against. But machine-learning-based email protection is trained to spot the tiny "tells" that give away these attacks.

2 High = sent to <5 unique target domains. Moderate = sent to 5-39 unique target domains. Broad = sent to 40+ unique target domains.

Where we're going, we don't need TOADs

One of the year's most unexpected developments was a sharp increase in telephone-oriented attack delivery (TOAD). These attacks require a high level of direct interaction, as the emailed lures do not contain malware or malicious URLs. Instead, the goal is to persuade the victim to call a fake customer service number. Once the victim calls, the attacker guides them into giving remote access to their computer or manually downloading malware. Our data shows more than 100,000 attempts to initiate a telephone-oriented attack every day.

Persuading victims to proactively make a phone call isn't easy, and last year's TOAD lures involved some of the most creative social engineering we've ever seen. From a fake movie streaming site to fake concert tickets for big names such as Justin Bieber and The Weeknd, distributors of BazaLoader malware have been responsible for some particularly original campaigns.

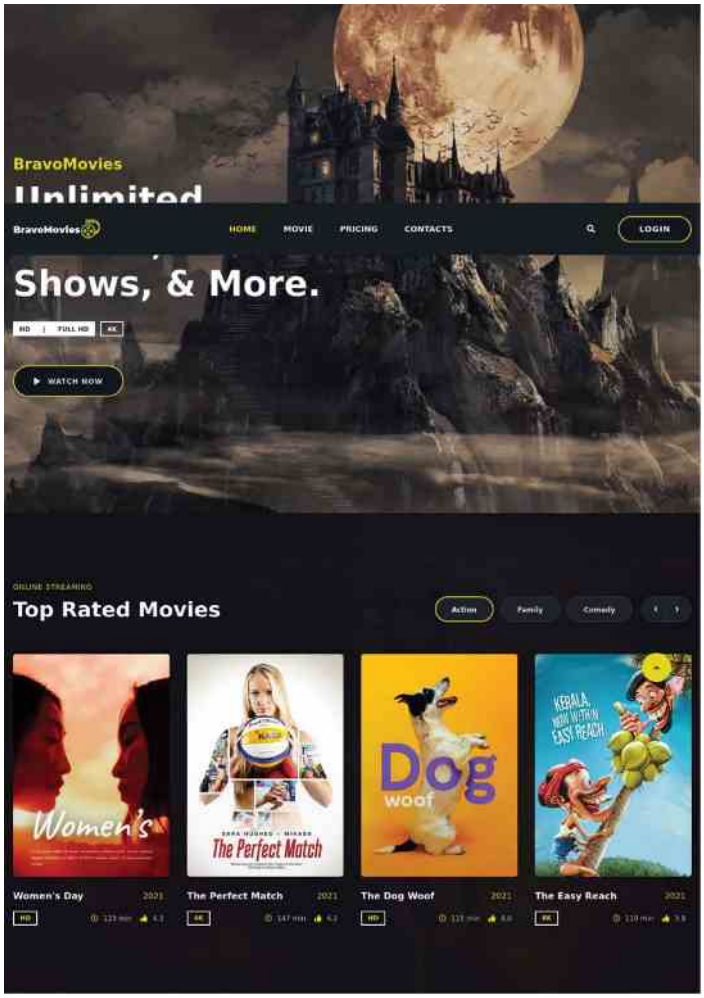


Figure 20. A fake movie-streaming services used in telephone-based attacks.

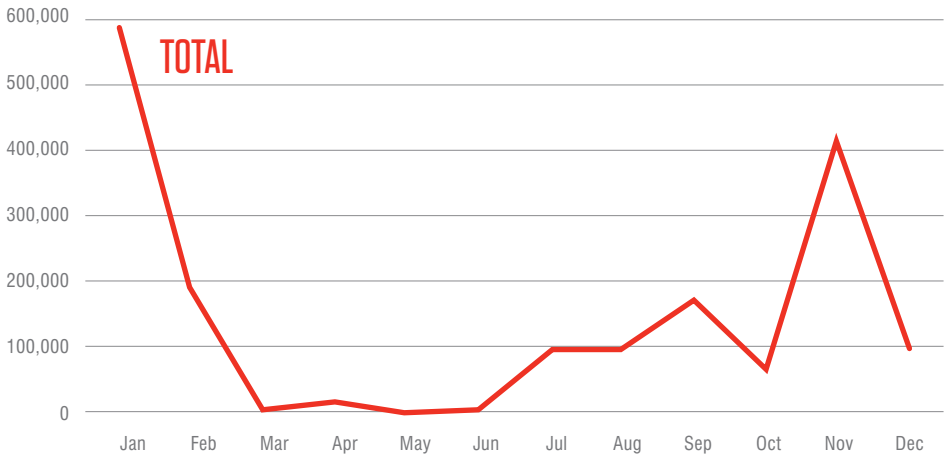


Figure 21. BazaLoader message volume, 2021. (Note: not all campaigns involved TOAD delivery method.)

Mobile threats

Smartphones are inherently personal. They contain detailed snapshots of our lives, including valuable information about our relationships, finances, likes and dislikes. But as we've already discussed, these devices also increasingly blur the line between personal and professional. From just one compromise, attackers can potentially open up a victim's finances as well as their employer's network—making phones an alluring target for cyber attack.

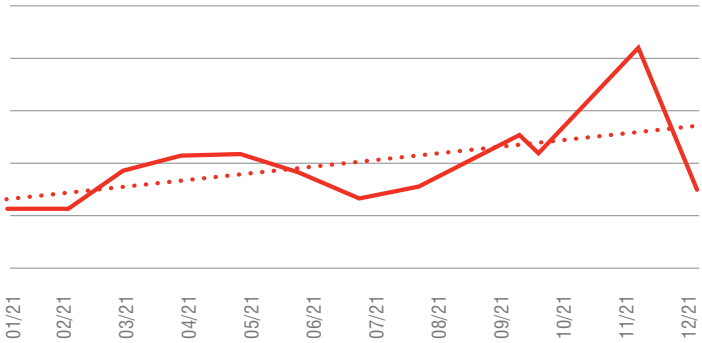


Figure 22. U.S. reports of SMS-based phishing attempts, 2021.

State of the smish

In this year's "State of the Phish" report, 54% of respondents revealed that they use their personal phone for work purposes. This means that for many of us, our smartphone contains the keys to both our personal and professional lives. Unsurprisingly, cyber criminals recognize this two-for-one opportunity and have increased targeting of mobile devices accordingly.

SMS phishing—or "smishing"—lures typically 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 the U.K., mobile attackers gradually settled on package delivery notification as the most effective theme. By the final three months of the year, these messages accounted for more than half of malicious SMS lures. At the same time, banking lures dropped sharply, possibly as a result of awareness-raising campaigns by the financial services industry.

For U.S. consumers, the smishing picture was similar. But because Amazon handles much of its own logistics, notification lures were divided between delivery and merchant categories.

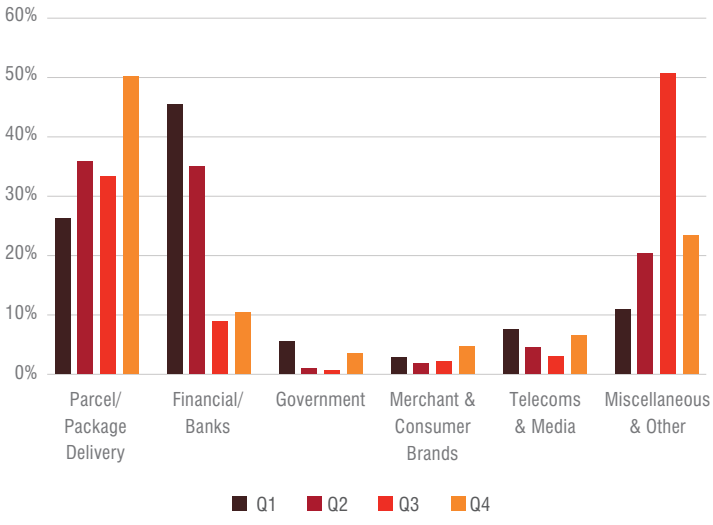


Figure 23. U.K. malicious SMS lure categories, 2021.

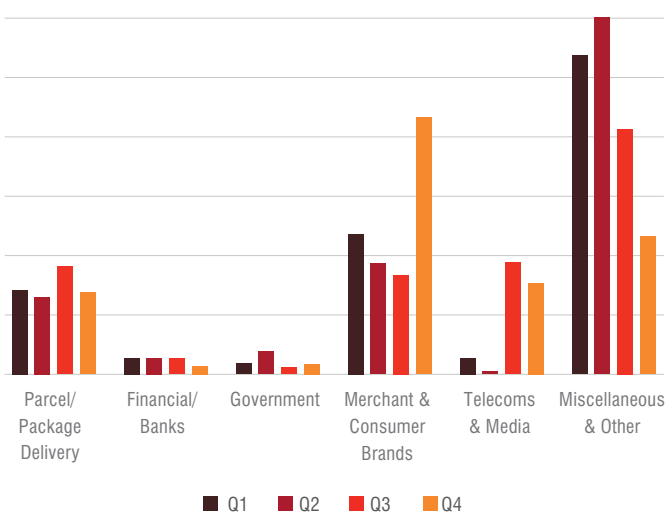


Figure 24. U.S. malicious SMS lure categories, 2021.

Catching FluBot

Smartphones aren't just a target for smishing activity—malware developers also have the devices themselves squarely in their sights.

Figure 25. FluBot reports.
(Note: Scale is normalized to protect confidential Proofpoint data)

FLUBOT:

A powerful Android malware capable of stealing data, intercepting calls and messages, and overlaying credential theft screens on top of many popular banking apps.

FLUBOT is a sophisticated, worm-like malware that emerged towards the end of 2020. It was first detected in Spain before spreading to other countries, arriving in the U.K. in March 2021. The malware spreads by accessing the address books of infected devices and sending new infected messages to numbers on the list. Coupled with a persuasive lure—such as package delivery notification—it makes for a particularly virulent piece of malware.

Once present on a system, FluBot can read and send messages, delete other installed apps, make voice calls, access the internet and overlay credential theft screens on a range of banking, brokerage and other finance apps. With the potential for multiple financial accounts to be managed from the same device, a single FluBot infection can have devastating results.

Cloud threats

Cloud infrastructure is now an essential component of most tech stacks. And as cloud technology has become ubiquitous, so have attacks on cloud accounts.

Gathering cloud attacks

Our data for 2021 shows that over 90% of monitored cloud tenants were targeted every month. Nearly a quarter (24%) of cloud tenants were successfully attacked, with the total percentage of tenants compromised during the course of the year reaching 63%. (Note: not all tenants with configured alerts have automatic remediation or protection.) In other words, like email-based phishing and malware delivery, attempted cloud account compromise has developed into a substantial and permanent feature of the threat landscape.

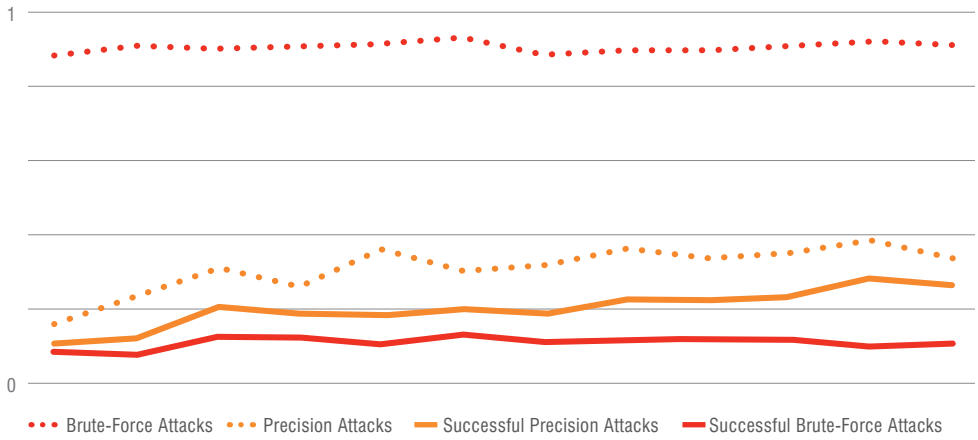


Figure 26. Brute-force vs. precision attacks against cloud accounts, volume and success rates, 2021.
(Note: Scale is normalized to protect confidential Proofpoint data)

BRUTE-FORCE ATTACKS:

95%

Brute-force attacks targeted 95% of organizations and managed to compromise nearly a third (32%) of cloud tenants during 2021.

Brute-force attacks remain the method of choice for most threat actors. These attacks targeted 95% of organizations and managed to compromise nearly a third (32%) of cloud tenants during 2021. Where we are seeing developments is in the frequency and sophistication of precision attacks. The number of cloud tenants targeted by precision attacks steadily increased over the course of the year, as did the number of tenants who experienced a resulting breach.

In total, 75% of cloud tenants were targeted with a precise attack, with 60% being compromised as a result. While brute-force attacks targeted three times as many tenants as precision attacks, the latter were twice as effective. Accounts compromised by precision attacks were also more likely to be abused later for cloud malware creation and hosting.

Section 3

Privilege

As recent cloud breaches have shown, one set of single-sign-on credentials can grant access to confidential data, organizational structures and enterprise systems. In our risk model, **privilege**—the systems and data your users have access to—allows you to quantify exactly how much damage a breach could do.

It's also perhaps the area of our model where organizations have the highest level of potential control. However, as many high-profile stories from the year reveal, auditing and managing privilege is still on the "to-do" list for some organizations.

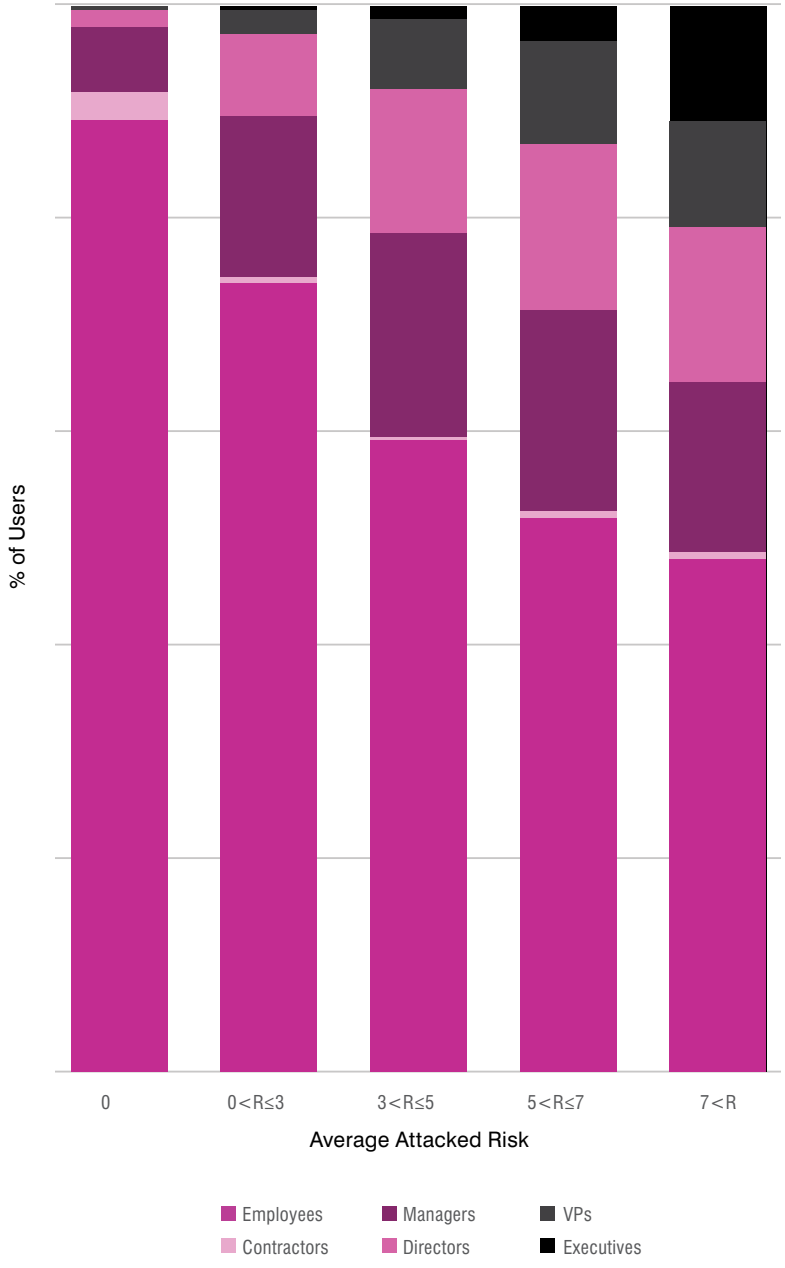


Figure 27. Averaged attacked risk by role, 2021.

High-privilege users disproportionately targeted in attacks

Across the organizations in our dataset, around 10% of users are classified as being managers, directors or executives. However, our data shows that this group represents almost 50% of the most severe risk or attack.

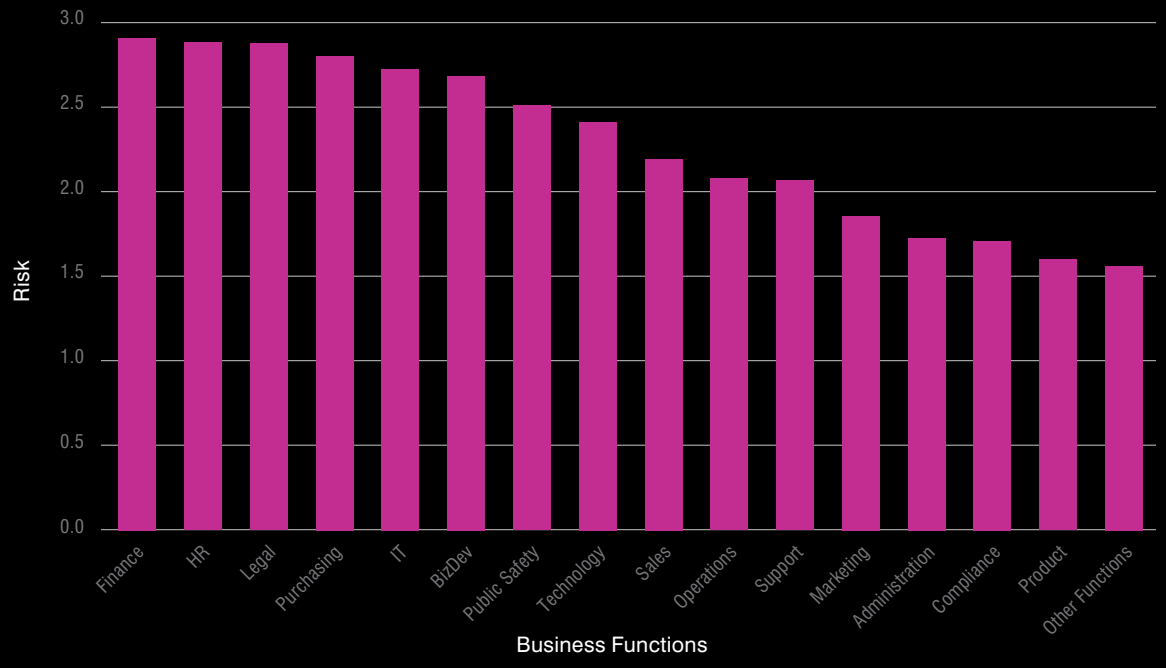


Figure 28. Average attacked risk by department, 2021.

Similarly, departments that deal with sensitive information, such as finance, human resources and legal, tend to be at higher risk than functions such as marketing and product.

Knowing where the highest privilege-based risks exist, whether that is individually or departmentally, is a crucial step in defending any organization from attack. High-privilege users can receive additional training to manage the elevated threat against them. Departments dealing with sensitive or valuable data may benefit from additional layers of security or oversight.

Suspicious cloud activity

With many enterprise systems now accessible through a single set of cloud credentials, a substantial amount of privilege-based risk is opened up. In the wrong hands, an account could be used to grant persistent access to malicious applications, manipulate and potentially exfiltrate sensitive data and files, and even commit malicious code to shared repositories. In several cases, we've seen malicious **OAUTH** applications created within compromised cloud environments. These apps were subsequently utilized by attackers to infect additional cloud accounts, leveraging their "verified publisher" status.

Over the course of the year, our cloud security team observed that 35% of tenants experiencing a suspicious log-in also experienced suspicious file activity after the breach. In addition, we detected over 200 malicious applications, targeting over 55% of cloud tenants. On average, approximately 10% of organizations were found to have at least one authorized active malicious application in their environment.

OAUTH:

An open-standard authentication protocol that uses tokens to provide access to online services without requiring passwords. Commonly encountered when using Facebook or Google credentials to access third-party sites and applications, but also found in some enterprise cloud environments.

Data loss prevention

Insider threats are a growing risk for businesses—not least because, as we've seen, cyber criminals are actively trying to recruit disgruntled employees.

In 2020, organizations were still scrambling to adjust to the sudden need for remote work. By 2021, most businesses had settled into the new pattern. And as the year wore on, many began to plan for a permanently hybrid future in which employees spend as much time working from home as in the office.

As such, we saw little movement in the configuration of data loss prevention alerts. Unlisted USB devices remained the biggest concern, while downloading potentially malicious files and exfiltrating data to USB both rose in the rankings. Printing large volumes of paper documents during irregular hours returned to the top 10 after understandably dropping out during the pandemic.

ACTION	2021 RANK	2020 RANK
Connecting unlisted USB device	1	1
Performing large file or folder copy	2	2
Exfiltrating tracked file to the web by uploading	3	3
Downloading file with potentially malicious extension	4	5
Opening a clear text file that potentially stores passwords	5	4
Exfiltrating a file to an unlisted USB device	6	7
Installing hacking or spoofing tools	7	8
Accessing upload and sharing cloud services	8	9
Opening ObserveIT Agent folder	9	10
Printing large number of pages during irregular hours	10	11

Table 1. Most popular DLP alerts configured by customers, 2021.

For many, a gradual ramp up to hybrid work is only just beginning. However, as people start the return to office, we can expect the nature of privilege risk assessment to adjust in turn. The surface area for attacks is constantly shifting, and so the priority and focus of security teams must shift with it.

Conclusion

Today's threats require a people-centric approach to prevention.

In the vast majority of cases, human factors matter more than the technical specifics of an attack. Cyber criminals are looking for relationships that can be leveraged, trust that can be abused, and access that can be exploited.

Deploy a solution that gives you visibility into who's being attacked, how they're being attacked, and whether they clicked. Consider the individual risk each user represents, including how they're targeted, what data they have access to, and whether they tend to fall prey to attacks.

We recommend the following for a people-centric defense.

Vulnerability

Most cyber attacks can't succeed unless someone falls for them. Mitigating vulnerabilities starts with security awareness training and risk-based controls.

- Train users to spot and report malicious email. Regular training and simulated attacks can stop many attacks and help identify people who are especially vulnerable. The best simulations mimic real-world attack techniques. Look for solutions that tie into current trends and the latest threat intelligence.
- At the same time, assume that users will eventually click some threats. Attackers will always find new ways to exploit human nature. Find a solution that neutralizes threats by applying additional layers of security to your most vulnerable users.
- Isolate risky websites and URLs. Keep risky web content out of your environment. Web isolation can be a critical safeguard against URL-based threats. The same technology can isolate users' personal web browsing and web-based email services.

Attacks

Cyber attacks are inevitable. But with the right mindset, tools and policies, they can be a manageable risk.

- 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.
- 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.

Privilege

The goal of every cyber attacker is access to data, systems and other resources. The more privileged the victim, the more access attackers have—and the more damage they can do.

- Deploy an insider threat management system to prevent, detect and respond to malicious, negligent and compromised users—the most common scenarios for privilege misuse—in as close to real time as possible.
- Respond quickly to potential privilege abuse with tools that can help you determine what happened before, during and after the incident and determine the user's intent—without the usual false positives.
- Enforce security policies with user training, real-time reminders, and blocking when necessary.

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.

0400-008-01-01 05/22