REPORT

single point of contact

proofpoint

The Human FACTOR 2018

People-centered threats define the landscape

proofpoint.com

Over the last year, cyber criminals have continued to increase their use of social engineering rather than automated exploits, scaling up people-centered threats and attacks that rely on human interaction. They have found new ways to exploit "the human factor"—the instincts of curiosity and trust that lead well-intentioned people to click, download, install, move funds, and more every day.

These threats focused on people and their roles within an organization rather than just computer systems and IT infrastructure.

Threat actors (cyber attackers and their sponsors) attacked people at both macro and micro scales.

At the macro level, they waged massive, indiscriminate campaigns in email and social channels. Ransomware was the biggest email-borne threat of 2017. And broad, multimillion-message malicious campaigns defined the new normal for the year.

At the micro level, state-sponsored groups and financially motivated email fraudsters launched highly targeted attacks. Even attacks on cloud-based platforms relied on human error, carelessness, and credulity to penetrate systems of value.

Whether they are broad-based or targeted; whether delivered via email, social media, the web, cloud apps, or other vectors; whether they are motivated by financial gain or national interests, the social engineering tactics used in these attacks work time and time again. Victims clicked malicious links, downloaded unsafe files, installed malware, transferred funds, and disclosed sensitive information at scale.

single point of contact

Table of Contents

single point of contact

KEY FINDINGS

CRYPTOCURRENCY
This form of electronic money is created through a "mining" process that uses computer power to solve complex math problems. Coin miners are malware strains that hijack infected systems for this purpose.

Email remains the top attack vector. Threats range from spam that clogs inboxes and wastes resources to email fraud that can cost organizations and people millions of dollars. The modern threat landscape also includes a variety of web-based threats that span social channels and cloud applications. And mainstream interest in **CRYPTOCURRENCY** is driving advances in malware and new approaches to phishing and cyber crime.

Here are the key findings from Proofpoint research over the last year. The results, based on data collected across our global customer base and analysis of over one billion messages per day, highlight the ways actors are stepping up attacks that exploit "the human factor."

Social engineering

Social engineering underpins the Human Factor. Attackers are adept at exploiting our natural curiosity, desire to be helpful, love of a good bargain, and even our time constraints to persuade us to click.

DEFENSIVE DOMAIN REGISTRATION
The recommended practice of buying up internet domains that could be mistaken for yours before attackers do. Lookalike domains can be used to trick customers and partners with fake websites and fraudulent emails that appear to be from your organization.

- Suspiciously registered domains of large enterprises outnumbered **BRAND-REGISTERED DOMAINS** 20 to 1. That means targets of phishing attacks are more likely to mistake typosquatted and suspicious domains for their legitimate counterparts.
- Fake browser and plugin updates appeared in massive malvertising campaigns affecting millions of users. As many as 95% of observed web-based attacks like these, including those involving exploit kits, incorporated social engineering to trick users into installing malware rather than relying on exploits with short shelf lives. Two years ago, social engineering in web-based attacks was much less widely deployed.
- About 55% of social media attacks that impersonated customer-support accounts—a trend known as "angler phishing"—targeted customers of financial services companies.
- Some 35% of social media scams that used links and "clickbait" brought users to video streaming and movie download sites. In-browser coin mining, in which attackers hijack victims' computers to generate cryptocurrency, also went mainstreams. These attacks converged largely around pirated video streaming sites; users' long viewing sessions gave the miners extended access to victims' PCs, netting more income for their operators.

PHISHING
In the broadest sense, phishing is any attempt to persuade someone to interact with an unsafe email. Phishing emails are used to trick recipients into opening unsafe attachments, clicking unsafe URLs, handing over account credentials and other sensitive information, wiring money, and more.

Recommendations:

Train employees to spot attacks that use social engineering through email, social media, and on websites—even those seemingly tied to well-known brands or current events. Use **PHISHING** simulations (fake attacks that test use real-world tactics) to see who in your organizations clicks. Paired with awareness training, these simulations can reduce the impact of real attacks.

Email threats: malware, phishing, and fraud

Analyzing the vast number of malicious messages sent every day, we saw new trends in how attackers target victims and the volume of email they send.

- Dropbox phishing was the top lure for phishing attacks. Twice as many phishing messages used the file-sharing service to entice victims than next most popular lure. However, click rates for Docusign lures were the highest at over five times the average click rate for the top 20 lures, demonstrating that volume did not necessarily equate to effectiveness.
- Observed network traffic of coin mining bots jumped almost 90% between September and November. This threat activity closely mirrored the rise and fall of the value of Bitcoin, the best-known cryptocurrency.
- Ransomware and banking Trojans accounted for more than 82% of all malicious email messages, making them the most widely distributed malware types. But by the end of 2017, many campaigns also included coin miner modules or secondary payloads.
- Microsoft Office exploits appeared regularly in email campaigns but they usually came in short bursts. This pattern highlights the short shelf life of exploits before they are rendered ineffective due to organizations patching their systems to fix the vulnerability.

Recommendations:

Invest in an advanced email security solution that protects against the full range of tools and techniques used in attacks. Your solution should include awareness training. And it must protect against credential phishing, fraud, and unsafe URLs and attachments.

Targeting trends

EMAIL FRAUD
In email fraud attacks, an email or series of emails purporting to come from a top executive or partner firm asks the recipient to wire money or send sensitive information. It does not use malicious attachments or URLs, so it can be hard to detect and stop.

Attacks throughout the year ranged from massive malicious spam campaigns to highly targeted email fraud attacks. While no industries were immune, we did observe noteworthy targeting trends.

- Education, management consulting, entertainment, and media firms experienced the greatest number of **EMAIL FRAUD** attacks, averaging over 250 attacks per organization.
- Construction, manufacturing, and technology topped the most phished industries. Manufacturing, healthcare, and technology firms were the top targets of crimeware.
- Ransomware predominated worldwide, but Europe and Japan saw the highest regional proportions of banking Trojans, with 36% and 37% of all malicious mail in those regions respectively.

Recommendations
Deploy email gateway solutions that prevent unsafe emails from reaching users in the first place. And have tools and processes in place that help you quickly detect and resolve any threats that get through.

New infrastructure, new digital risks

Businesses are embracing cloud services to improve worker collaboration, streamline operations and engage customers. With these new benefits come new risks, including accidental sharing, credential theft, and unsafe third-party app add-ons. Here are the top trends we saw:

- Nearly 25% of all suspicious login attempts to cloud services were successful.
- About 1% of all cloud service credentials have been in leaked in our sample of hundreds of thousands of SaaS accounts examined during risk assessments conducted across industries.
- Roughly half of all cloud app users have installed third-party add-ons. About 18% of these add-ons have access to email and files.
- Around 60% of cloud service users, including 37% of privileged users, did not have a password policy or multi-factor authentication enforced.

Recommendations
Assess cloud apps and users based on objective, people-centered, risk-aware scoring measures. Find potential data compromises, compliance violations, and more. Then deploy services to monitor ongoing security and compliance risks that come with cloud apps.

Good cloud services, bad actors

Users are accustomed to frequent email notifications from cloud services and apps. Attackers are using these services to send malicious messages and host malware. These attacks are hard for users and defenders to recognize because they come from legitimate services and platforms.

- No major cloud services avoided abuse. For example, threat actors used Microsoft SharePoint to host malware distributed in millions of messages across hundreds of campaigns through 2017.
- Other services, ranging from G Suite to Evernote, were used to send phishing emails and malware.
- Most cloud platforms are extensible. Third-party add-ons open up new features, but they also create possibilities for abuse. We found a vulnerability in Google Apps Script, for example, that allowed attackers to send malware through legitimate emails that came from G Suite accounts.

DYNAMIC DETECTION
Dynamic detection identifies new threats based on the actions of suspect attachments, clicked URLs, network traffic, logins, data transfers, and other behavioral factors.

BANKING TROJANS,
This type of malware steals victims' bank login credentials, usually by redirecting victims' browser to a fake version of their bank's website browsers or injecting fake login forms into the real site.

WEBINJECTS
A technique that alters web pages as they are displayed to the users. Attackers use webinjects to append insecure forms to seemingly secure websites. When users fill out the forms (say, with their banking credentials), that information is sent to the attacker instead of the bank.

CREDENTIAL PHISHING
A type of phishing that tries to trick users into providing account credentials, such as user names and passwords.

Recommendations

The sheer volume of cloud apps and services—many of them useful and safe—makes visibility into security and compliance risks difficult. Be especially mindful of third-party add-ons that connect to popular business apps; they may host threats or misuse your data. **DYNAMIC DETECTION** solutions from a threat intelligence partner can identify potential risks, unusual activity, and emerging threats.

BY THE NUMBERS

Social engineering approaches further matured in both phishing and malware attacks. Geotargeted malware attacks (beyond those we expect with **BANKING TROJANS,** which usually require region-specific **WEBINJECTS**) also increased.

Phishing

A disproportionately high volume of phishing that used lures associated with the Dropbox file-sharing service was the biggest change from 2016. But users were far more likely to click those that purported to be from DocuSign, the electronic signature service.

Figure 1 shows the relative volumes for the top 20 **CREDENTIAL PHISHING** lures in 2017.

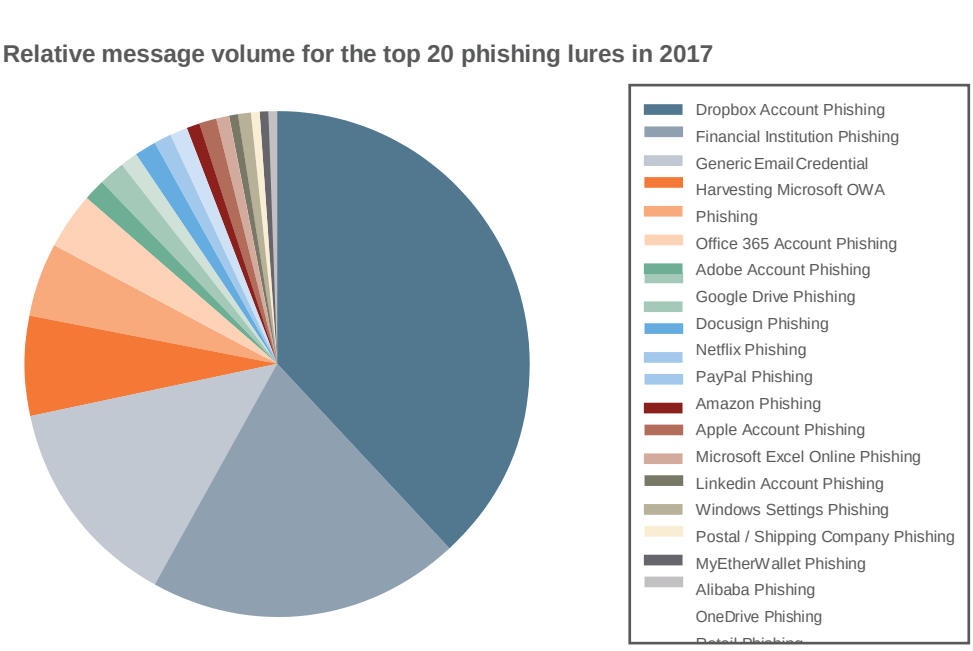


Figure 1: Relative volumes associated with the top phishing attack lures

We saw some differentiation in targeting, but most of it stems from inherent differences install bases, use cases, and user profiles.

Microsoft Outlook Web App (OWA) phishing was more common in healthcare and media. Financial institution account credential phishing predominated in education. And generic email account credentials were a more frequent target for business services. But in general, we saw few significant differences among industries.

The volume of threats does not always equate their effectiveness. Threat actors often compensate for less effective but potentially more lucrative lures with volume. By the same token, lures more likely to generate a higher percentage of clicks may not need large campaigns.

For instance, Dropbox phishing volumes dominated throughout 2017, compounded by isolated instances of extremely large campaign activity (see Figure 1). But as Figure 2 shows, click rates for DocuSign phishing exceeded those for Dropbox phishing despite much lower overall volume. In fact, DocuSign click rates beat out all other credential phishing email lures.

single point of contact

Dropbox-related lures appeared in **more phishing email overall**, but DocuSign-related lures were far more effective at getting people to click.

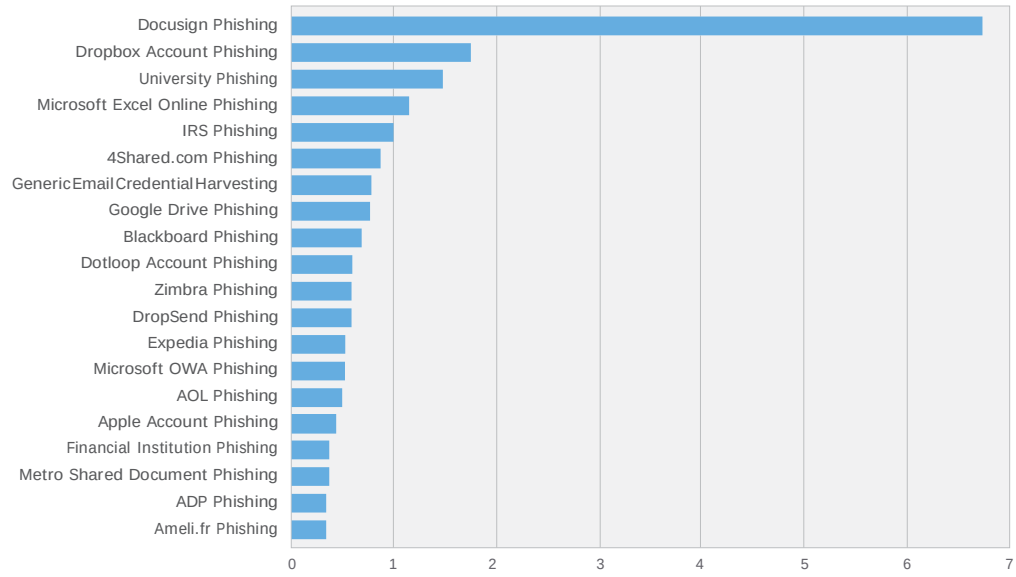


Figure 2: Average click rates for the top 10 lures

Click rates also vary by industry, with predictable trends based on likely user profiles and use cases.

Figure 3 plots click rates by industry and lure type. It shows that while the volume of phishing threats was consistent across industries, click rates were highest in automotive, aerospace, defense, and commercial banking. These industries were associated with very high Dropbox click rates. DocuSign click rates were generally high across the board with notable exceptions such as education.

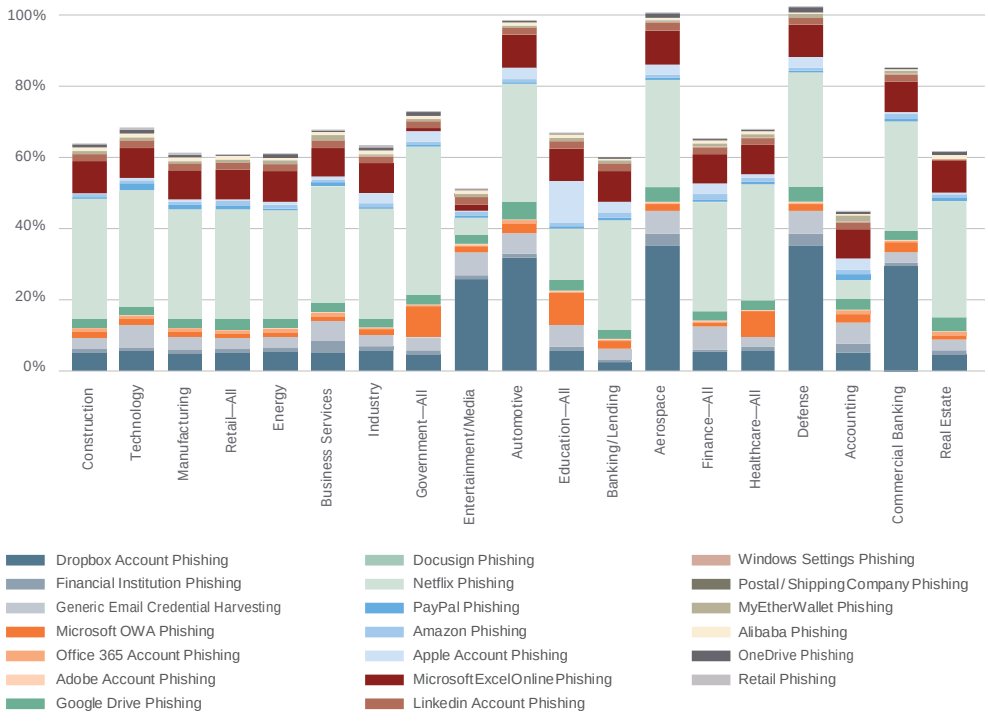


Figure 3: Most clicked lures by industry

single point of contact

Malware

Our researchers see periodic pendulum swings between malware delivered by malicious document attachments and those sent using URLs. Within those categories, we observe similar swings—among the types of attached or linked files.

DYNAMIC DATA EXCHANGE
DDE is a 20-year-old communications protocol in Microsoft Windows that allows documents to pull information from other documents. The technique has been largely replaced by newer protocols but is still supported in Windows.

For example, attached documents abusing **DYNAMIC DATA EXCHANGE (DDE)** exploded in October and then settled into a pattern of more occasional use. But amid these swings overall use of malicious attachments—ranging from compressed script files to exploit documents—exceeded URLs by almost 28%. Figure 4 breaks down the differences in aggregated malicious attachments vs. malicous URLs in email campaigns by malware family.

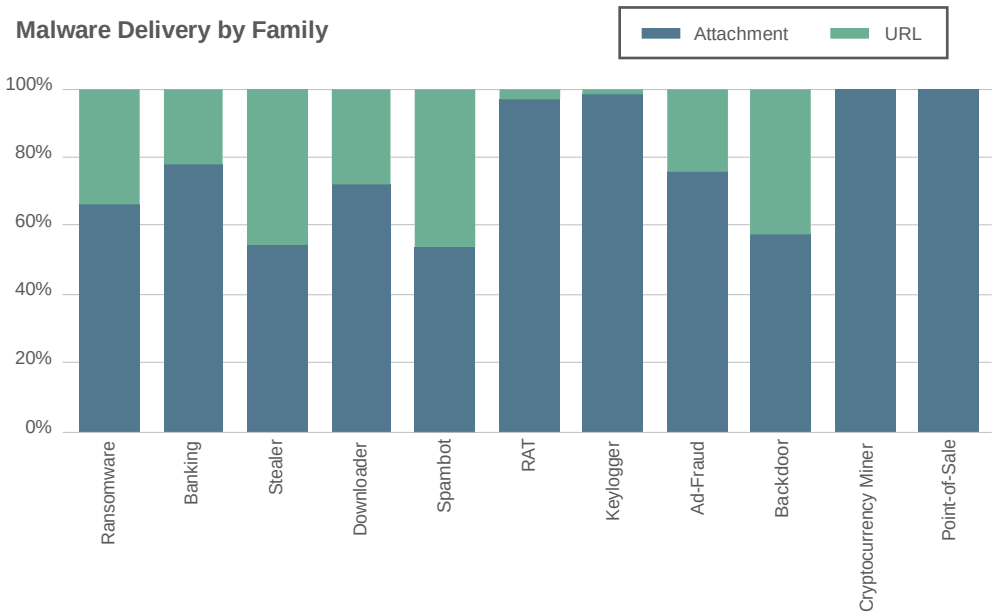


Figure 4: Malware delivery via URL vs. attachment by malware family

In contrast to the roller coaster pattern of malicious URL message volume, messages bearing malicious macro documents or attached scripts were used steadily throughout the year. These emails deliver malware that is not easily thwarted by robust patching regimens.

In all cases, though, email-based malware delivery still relied on the human factor. Recipients generally needed to download an attachment or click a link. Even when attackers attempted to exploit a vulnerability, they often embedded their exploit documents in PDFs or other document attachments. These attacks required the user to take the step of double-clicking the embedded document, akin to enabling macros.

Schemes like this underscore the human factor's status as the richest vulnerability targeted by cyber criminals. That held true even in the case of attacks that use DDE, the most abused Office feature in 2017. Recipients had to—and did—click through multiple security warnings to run the exploit and infect their PCs with malware.

RANSOMWARE
This type of malware locks away victims' data by encrypting it, then demands a "ransom" to unlock it with a decryption key.

Whether via URL or attachment, malware targeting via email varied by region, albeit by modest margins." **RANSOMWARE** predominated worldwide. But banking Trojans appeared in more than 30% of malicious emails in Europe, Japan, and Australia (Figure 5).

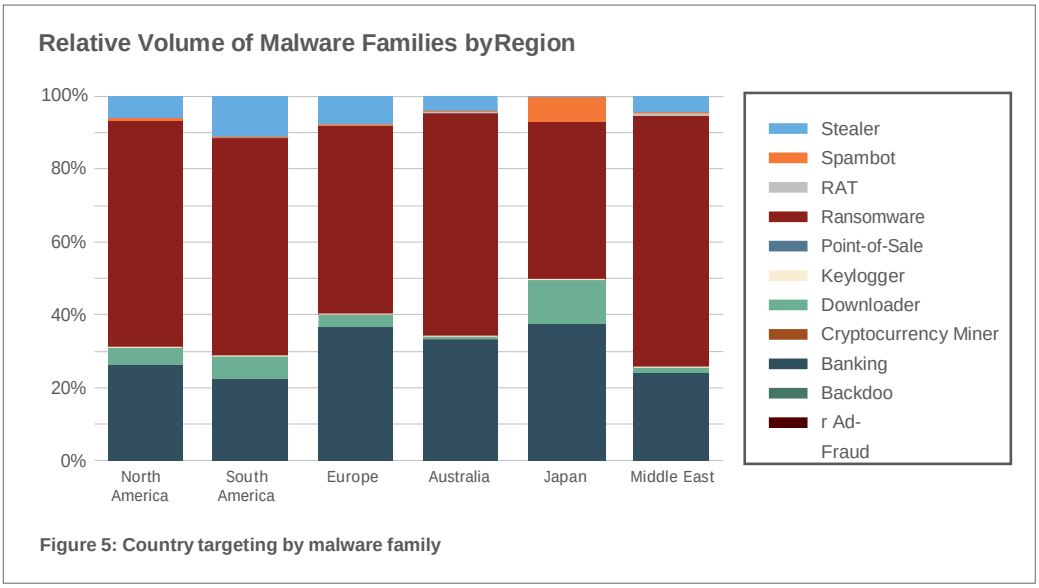


Figure 5: Country targeting by malware family

CRIMEWARE
This term encompasses a wide range of malware used for cyber crime such as stealing credit card numbers, raiding online bank accounts, corporate intellectual property theft, and more.

INFORMATION STEALERS
Malware used to collect information from compromised systems and send it to the attacker. Keyloggers, which record users' keystrokes (hoping they will type their usernames, passwords, credit card numbers, and so on), are a common type.

DOWNLOADER
Downloaders are snippets of code or scripts used to gain a foothold on a targeted system and download other malware components.

In a similar vein, **CRIMEWARE** activity varied by industry, with a few standout trends. No industries escaped attacks. Malware families included ransomware, banking Trojans, **INFORMATION STEALERS**, and **DOWNLOADERS**, and others.

Ransomware was especially prevalent in messages targeting educational institutions. Business services and marketing/advertising saw the least ransomware. Business services, media/entertainment, insurance, and others experienced higher proportions of stealer attacks. But again, aside from variability among industries, no single vertical experienced disproportionate attacks with particular malware families.

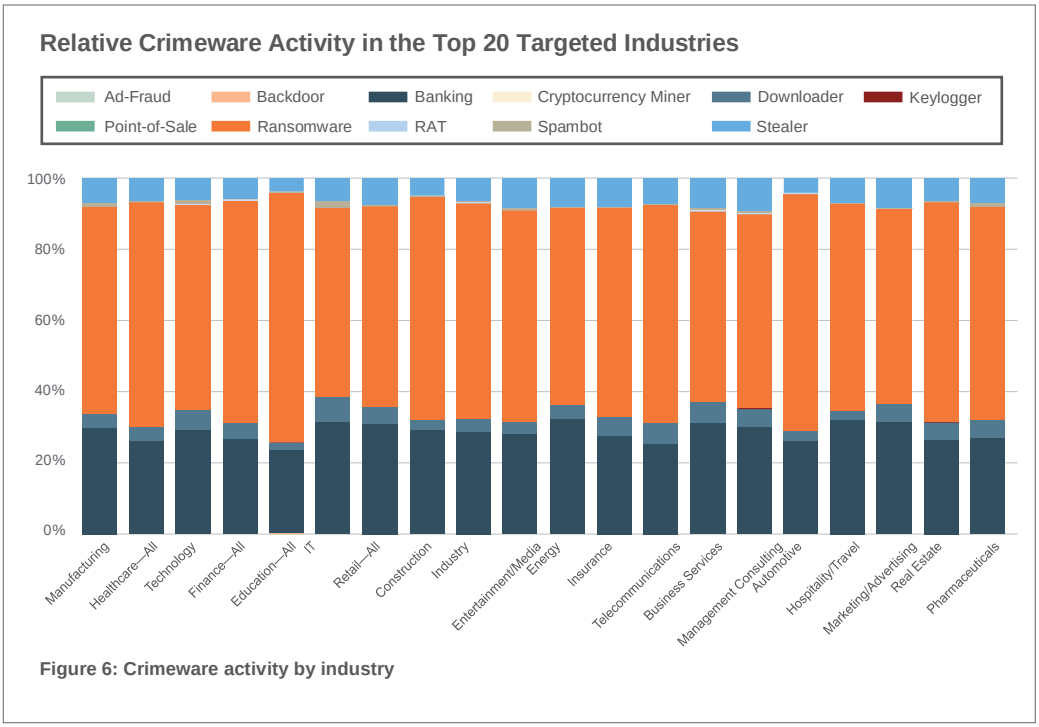


Figure 6: Crimeware activity by industry

Who clickswhen?

We also examined how people behaved in response to these threats. We tracked how soon people clicked on the attachment or URL after it was delivered. We looked at when those clicks occurred. And we uncovered regional differences that can help defenders deploy the right resources at the right time.

Figure 7 shows that North American employees tended to click around three time windows: the beginning of the work day, lunch, and the end of the work day.

Australian employees, on the other hand, were more likely to click in the morning and then activity tapered off throughout the day. South America followed a similar, though less pronounced, pattern as North America.

Almost a quarter of clicks occurred within the **first five minutes of the message being delivered.** And 52% occurred within the first hour.

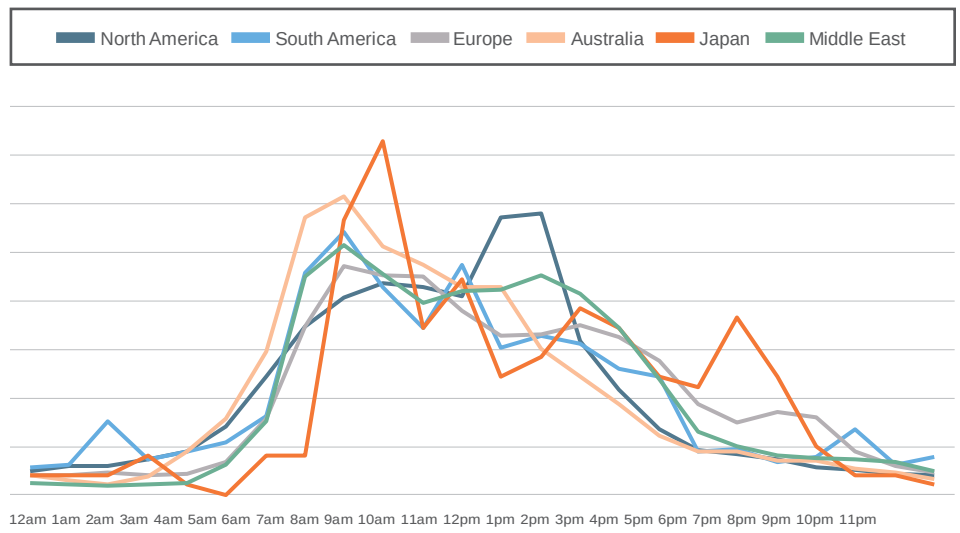


Figure 7: Regional clicks by hour of day

Despite these regional differences, 52% of clicks occurred within one hour of the message being delivered. Figure 8 shows that delays between delivery and click follow a nearly logarithmic curve—clicks taper off sharply after delivery of malicious messages. Within one minute of delivery, more than 11% of recipients had already clicked on a malicious URL. Almost one quarter of clicks occurred within five minutes. That means defenders have very little time to neutralize or mitigate threats. They need to prevent malicious messages from reaching user inboxes in the first place.

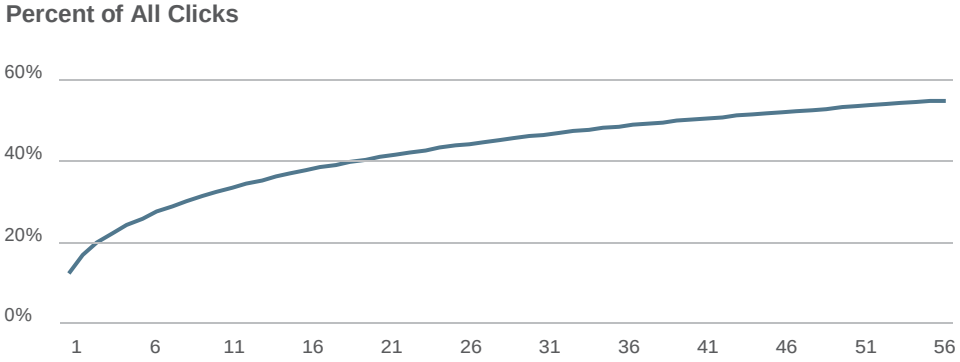


Figure 8: Delay between message delivery and click

SOCIAL ENGINEERING: ALL YOU HAVE TO DO IS CLICK

Businesses have improved their system-patching regimens. They have rolled out new security tools and have deployed layered defenses across networks and endpoints.

So why are security breaches still a problem?

Because cybersecurity is not strictly an IT and operations issue. As recent headline-grabbing attacks have shown, it goes far beyond the back office. In today's threat landscape, information security has a number of distinctly human elements. And as exploiting software and hardware vulnerabilities grows more difficult, attackers are turning to people. Human nature is the vulnerability.

Even the best defenses can be thwarted by one wayward click on a link or attachment or one innocent response to a well-crafted email lure. People remain the weakest link in the security chain, a fact not lost on cyber criminals.

Social engineering 101

Attackers have relied more and more on social engineering to trick users into revealing credentials, installing malware, or wiring funds. Few of us are still tempted to send money to distressed Nigerian princes anymore. But the basic principles behind those early email scams are alive and well. We see them in large malicious email campaigns, web-based attacks, on social media, in email fraud, and elsewhere.

Today, social engineering tends to take one of two forms:

- Simple lures used in large campaigns. These may simply be file names for malicious attached documents, such as "resume.doc" or "invoice.xls." Only a small fraction (among hundreds of thousands or millions of recipients) will be curious enough to open them.
- Highly sophisticated, persuasive schemes designed to generate a higher response rate. These use precisely rendered graphics and stolen branding or create well-crafted email lures and fake documents that appear legitimate.

The latter are more likely to appear in smaller, more targeted attacks, but we are seeing even larger campaigns and web-based social engineering schemes that create very convincing collateral.

Several tactics fall under the umbrella of social engineering:

- Conveying a sense of urgency
- Replicating trusted brands
- Preying on our natural curiosity
- Taking advantage of conditioned responses to frequent events such as software updates

These techniques work every day. Users click, install, and reply without threat actors needing to develop expensive and short-lived **EXPLOITS**.

EXPLOITS
An attack on a software or hardware vulnerability that hasn't been fixed (patched) with an update.

WHY WE TRACK THIS

Studying the newest techniques used in brand fraud helps determine how to prevent, detect, and contain it.

Brand theft and typosquatting fool even savvy users

Many threat actors who used to invest time and resources creating automated exploits have turned to brand theft instead. Brand theft is a highly effective means of tricking users into believing they are interacting with legitimate sites and services. As shown in Figure 9, this kind of attack uses professional-grade graphics and strategic **TYPOSQUATTING** that can fool even security-conscious users.

Typosquatting goes hand-in-hand with brand theft. Attackers register web domains similar to those owned and used by legitimate brands. Typosquatting allows cyber criminals to send emails from what seems to be a trusted brand and direct victims to a website that looks like the real thing.

For example, Figure 9 shows a fake Litecoin website distributing a modified version of the Litecoin wallet (an app that allows people to manage the encryption keys to their Litecoin account). The fake version of the Litecoin app lets attackers harvest credentials and steal funds. The website copies the real Litecoin website almost exactly. The only difference: the malicious site's domain name is "itecoin[.]com" instead of "litecoin[.]com".

TYPOSQUATTING
Fraudsters register domains that are misspellings or typographically mangled versions of a legitimate domain to trick users who mistype the URL or do not look closely at email headers.

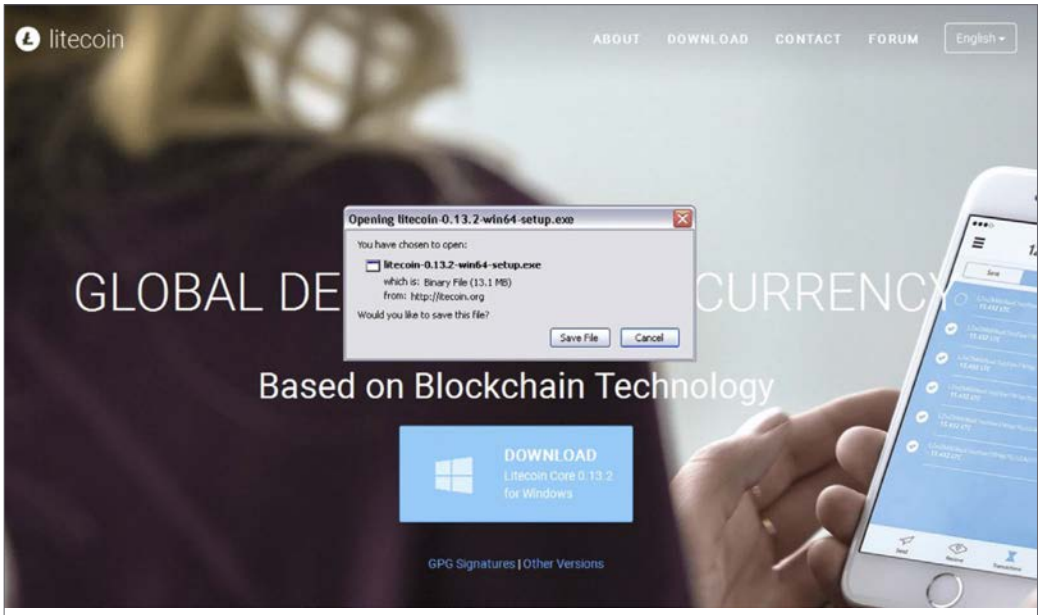


Figure 9: Sophisticated template used to distribute a backdoored cryptocurrency wallet leveraging stolen Litecoin branding

Our research suggests that threat actors are dramatically outpacing brands in registering domains that could be confused with those used by trusted brands. For large enterprises, suspiciously registered domains can outnumber brand-registered domains 20 to 1.

(We label domain registrations as "suspicious" if they look confusingly similar to ones owned by a known brand but haven't yet been used in an attack. Defensive registrations are lookalike domains claimed by the brands themselves to pre-empt typosquatting attempts.)

SPOOFING
A technique to trick workers, partners and customers by using email and web addresses that look like those of trusted brands.

This wide gap between suspicious and defensive registrations leaves brands open to fraud, phishing, **SPOOFING**, and more. Even savvy users may click on links and respond to phishing scams when typosquatting is involved.

Figure 10 shows the relative frequency of domain variations used for typosquatting.

Most often, threat actors simply swap an individual character. They might register "myc0mpany.com" (using the numeral 0 in place of the letter O) to fool customers and employees of "mycompany.com".

The litecoin.com example in Figure 9 used the third most popular approach, adding or removing leading or trailing characters.

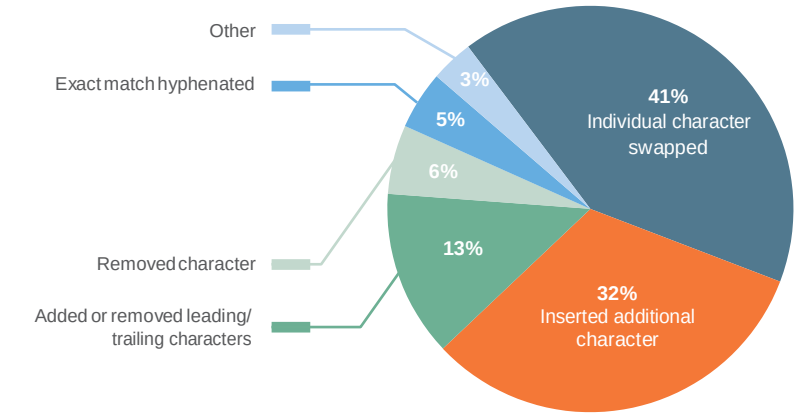


Figure 10: Common variations used in suspicious domain registrations and typosquatting

Threat actors are registering suspicious domains by the score.

The 2018 Winter Olympics in Pyeongchang, South Korea, and the 2020 Summer Olympics in Tokyo, Japan, provide a few high-profile examples of suspicious domain registrations.

Since 2010, the year the official site of https://www.pyeongchang2018.com/ was registered, more than 100 similar domains have been registered. Of those, only three were legitimate (though unofficial) domains related to medal-tracking.

We have seen similar trends for the upcoming 2020 games. In most cases, the sites have been registered by unauthorized ticket sellers, streaming sites, and more—all intended to capitalize on interest around the games.

Lookalike domains are only part of the picture. Attackers also use polished graphics and familiar visuals to hijack consumers' trust in popular brands.

Figure 11 shows a real-world example this approach. The images, which impersonate a well-known airline ticket sales website in Russia, were part of a massive **MALVERTISING** campaign by a threat group called **ADGHOLAS.** The campaign reached millions of potential victims with the goal of installing mole ransomware.

MALVERTISING
Malvertising, short for malicious advertising, embeds malicious code into online display ads. These ads often appear on legitimate, widely trusted websites, making them difficult to block at the gateway or endpoint.

ADGHOLAS
A threat group responsible for some of the largest malvertising campaigns we have ever observed.

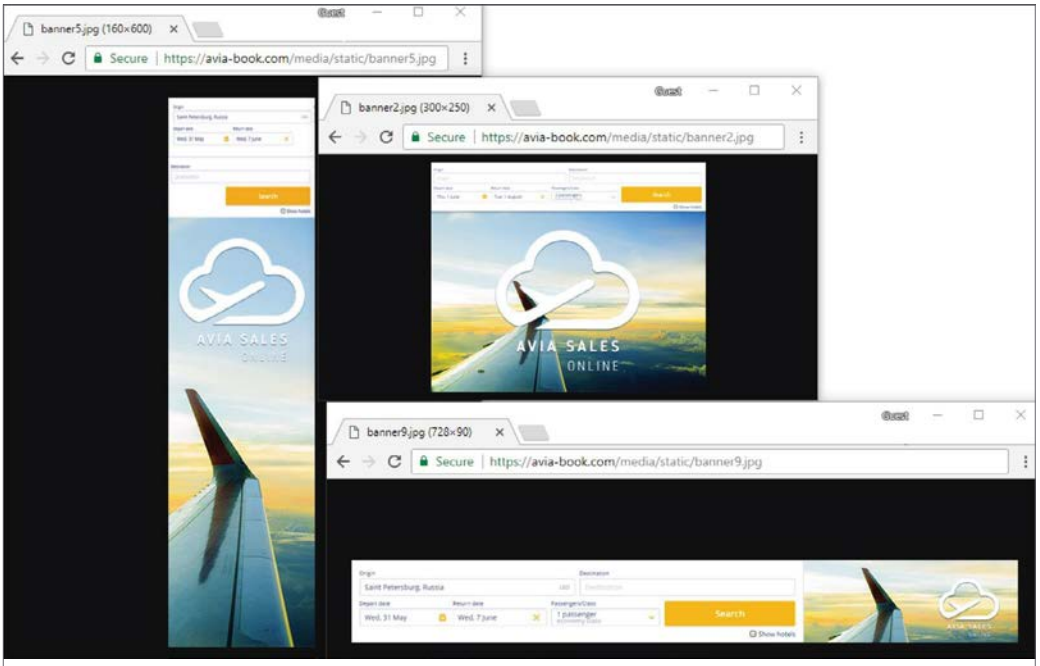


Figure 11: Brand theft examples

Brand theft can extend to phishing schemes for financial institutions, media sites, and even targeted, state-sponsored attacks. The practice has become pervasive. And attackers have grown adept at it, making it difficult for users to distinguish scams from legitimate marketing.

Even exploits get the human touch

We often talk about "the human factor" in contrast to automated exploits—fully automated exploits such as malvertising and other web-based attacks that have not relied on human interaction.

That distinction is getting fuzzier.

In the wake of plunging traffic to automated exploit kits, as many as 95% of web-based attacks now incorporate social engineering. They may offer users fake updates, bogus security alerts, or other tricks to persuade users to download and install malware.

And for document exploits more common in email attacks, recipients still need to be convinced to open the file. Even last year's WannaCry and NotPetya attacks exploited vulnerabilities that had available patches.

Figures 12 and 13 details how attackers used document exploits throughout 2017. For each exploit, activity spikes soon after the associated vulnerability is publicly disclosed.

But those bursts of activity are just spikes, not steady increases. Exploits have an inherently short shelf life. Cyber criminals quickly make use of them before potential targets patch their systems and render the exploits less effective. Rather than marking long-term shifts, new exploits are simply added to threat actors' rotating toolkits.

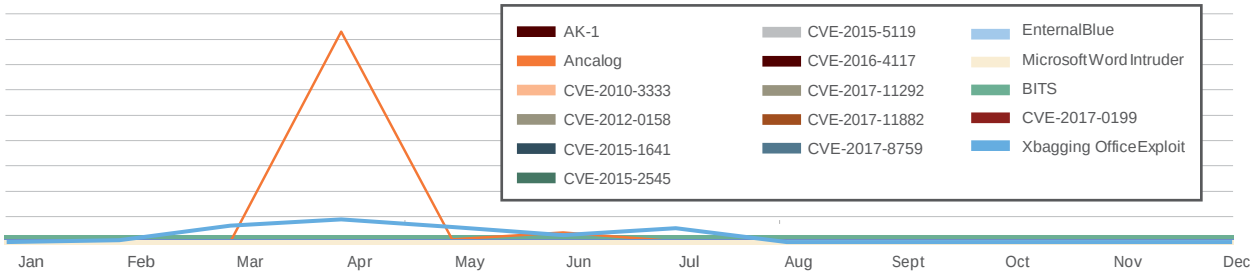


Figure 12: Document exploit activity in email campaigns with all major exploits observed in the wild

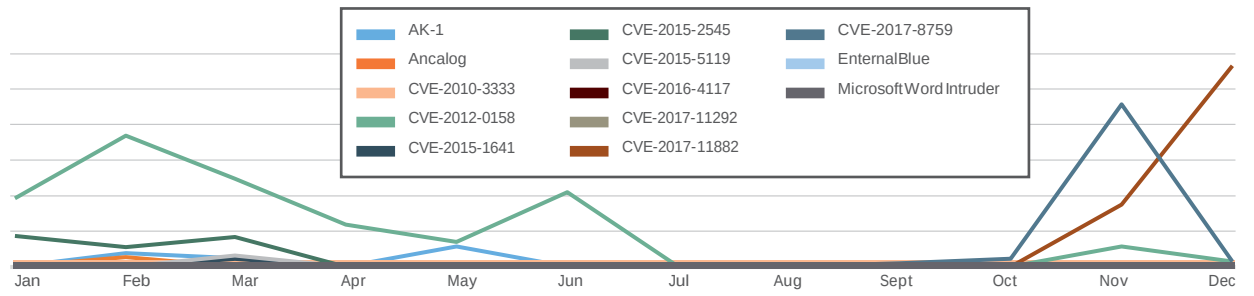


Figure 13: Document exploit activity in email campaigns, removing the top three exploits to better show usage trends for less common exploits

Exploits are not going away. But all signs point to the human factor as a main component in most attacks going forward. Malicious macros and attached scripts (which require someone to click) will dominate most email-based attacks. And more web-based attacks will use social engineering.

The human factor is simply more reliable—and therefore more lucrative—for attackers.

single point of contact

WHY WE TRACK THIS

Noting similarities and differences in industries targeted in email fraud helps reveal possible motivations of attackers and what might help safeguard against this growing threat.

EMAIL FRAUD: THE ULTIMATE HUMAN EXPLOIT?

Email fraud, also known as business email compromise (BEC), arguably relies more on the human factor than any other kind of cyber attack. It uses no malware; it incorporates social engineering; and it often uses out-of-band communications between the attacker and target to add a veneer of legitimacy and evade detection. All of these elements are designed to thwart security tools and persuade recipients to transfer funds or send sensitive data—rather than install malware.

Industry targeting: attackers get personal with educators and consultants

Companies of all sizes are about as equally likely to be targeted by an email fraud attack. But some industries were clearly in the sights of attackers.

Education was the most-targeted vertical, with **four times as many attacks** per organization than average (across all industries).

Education was the most-targeted vertical, with four times as many attacks per organization than average (across all industries). Figure 14 shows the average number of attacks per organization in each industry we track. Education also saw the largest year-over-year increase; the average number of attacks per institution jumped 120% vs. the previous year's average.

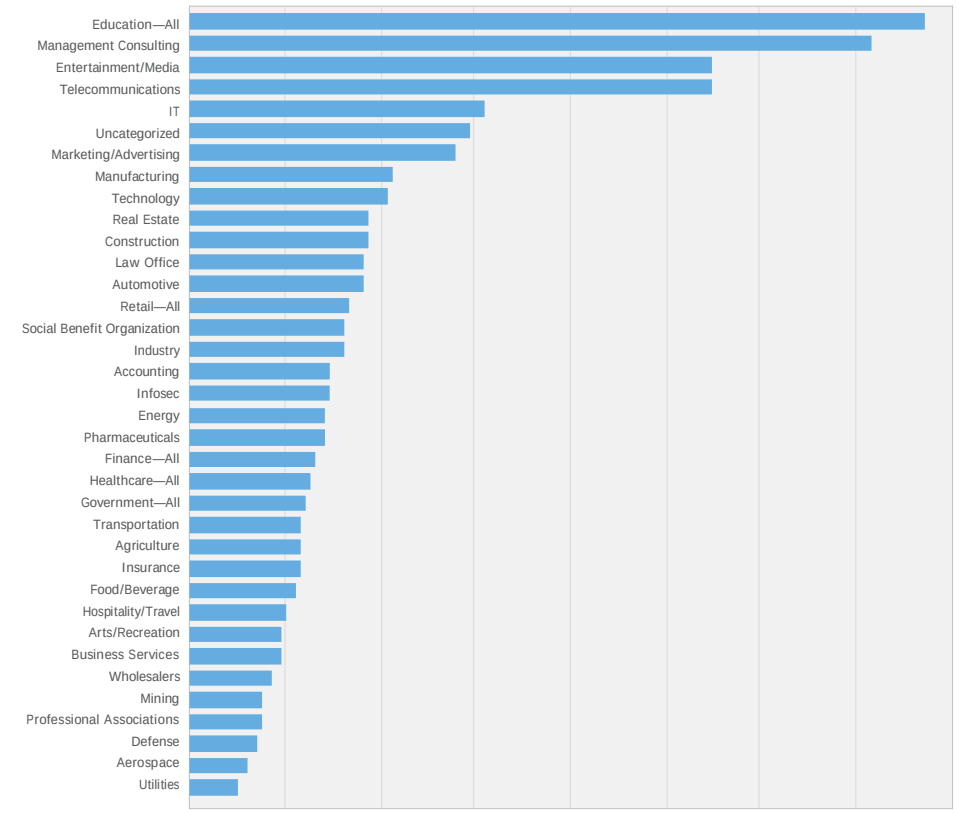


Figure 14: Average number of email fraud attacks per company targeted by industry

Management consulting, entertainment/media, and telecommunications rounded out the four most targeted sectors.

Seemingly natural targets for cyber crime, such as the defense and aerospace industries, ranked near the bottom of list. The reason: most email fraudsters are after money, not corporate secrets. That makes these low-ranking industries less attractive than those frequently engaged in high-value transactions with complex and multifaceted supply-chain and customer relationships that may be more easily exploited for financial gain.

But no industry was immune to email fraud. Even the lowest-ranked industries experienced dozens of email fraud attacks per organization in 2017. Overall, roughly 80% of businesses experienced an email fraud attack.

WHY WE TRACK THIS

Examining the subject lines used in email fraud attempts provides some insight into seasonal trends and evolving techniques among email fraudsters.

Subject lines introduce new email fraud techniques

Figure 15 outlines the most common email subject lines by quarter. It reveals a spike in W2 and tax-related lures in Q1.

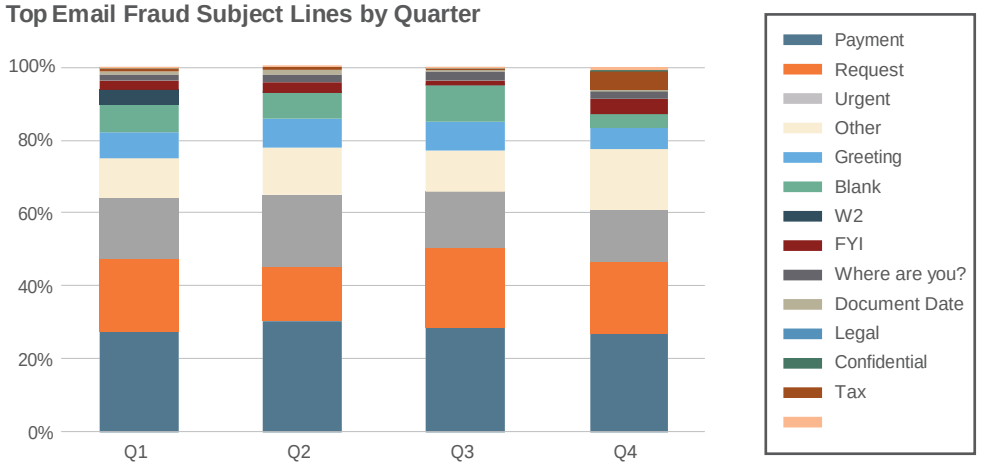


Figure 15: Distribution of most common email subjects in BEC attacks

The number of attacks using legal language **increased 1,850% year-over-year.** The subject "Lawyer's call" was the most popular.

Note the increase in subject lines related to legal work. While still small overall, the number of attacks using legal language increased 1,850% year-over-year. Of these, the subject "Lawyer's call" was the most popular. In most cases, these emails attempted to start an out-of-band discussion with someone in authority to convince the victim to transfer information or money.

Throughout 2017, we also saw email fraudsters increase their use of "fake chains." They prepended subject lines with "Re:" or "Fwd:" and, in some cases, included a bogus email history to establish legitimacy. Fraud attempts that used this technique grew more than 50% year-over-year. By the end of 2017, more than 11% of all email fraud attempts were using it.

We also saw a dramatic rise in the number of "many-to-many" fraud attacks. Targeting multiple employees has been common for some time. But most only spoofed the sender identity of a senior executive or high-ranking individual in a partner company. By the end of 2017, however, 41% of attacks involved more than five spoofed senders. Within these attacks, the average number of spoofed senders doubled from five people to 10 between Q3 and Q4 2017. The trend suggests that email fraudsters are adapting as organizations become more aware of email fraud and move to prevent it.

single point of contact

WHY WE TRACK THIS

Advanced persistent threats (APTs) are far more difficult to detect and defend against than other types of cyber attacks. They have significant resources, proven capabilities, and sophisticated tools. They can more easily target the human factor and warrant close scrutiny.

BIG ACTORS TARGET THE LITTLE GUYS

State-sponsored attackers and established cyber criminals usually reserve their efforts for the biggest, most high-profile targets. But in 2017, they began going after smaller targets.

The Lazarus Group

The Lazarus Group is widely recognized as a threat actor affiliated with by North Korea. It has launched both financially motivated and espionage activities against banks, governments, and many other agencies before.

But in 2017, it initiated multistage attacks against individual people to steal cryptocurrency and against point-of-sale (POS) infrastructure to steal consumer credit card data. To our knowledge, this was the first documented case of a state-sponsored attack against POS systems for financial gain.

FIN7

FIN7, on the other hand, is a financially motivated cyber crime group linked to major thefts. It uses sophisticated techniques and tools often associated with APT actors. FIN7 has proven to be highly adaptable. It recently stepped up attacks against a variety of individuals within restaurant chains using a new backdoor and malicious macros.

The CobaltGroup

The Cobalt Group provides another example of a threat actor carefully targeting people within organizations. The group incorporated new malware and document exploits in attacks against financial institutions. It sent malicious emails to specific people in information security and fraud departments. Well-crafted lures, combined with anti-sandbox features, made these attacks difficult to detect by both automated systems and human recipients.

APT groups also rely on the human factor

Cobalt and FIN7 use some APT-style techniques, and Lazarus is recognized as a state-sponsored APT actor. But all of these groups engage in some financially motivated activities.

However, most APT actors tend to focus more on espionage and disruption. While APT tools and resources tend to be more sophisticated than those of crimeware actors, all still work to exploit the human factor. As shown in Figure 16, APT activity observed across the our customer base is far more likely to target government and defense industries. But no industries were exempt.

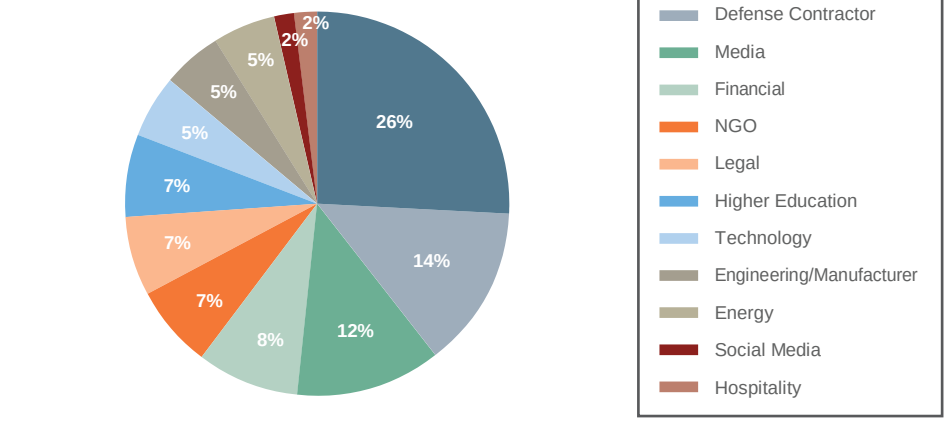


Figure 16: Observed APT activity by industry

single point of contact

WHY WE TRACK THIS

Cryptocurrency has become a prime target for threat actors looking to directly monetize their efforts. Following phishing, malware, and network activities related to cryptocurrencies gives us significant insight into the latest trends among cyber criminals.

CRYPTOCURRENCY IN THE CROSSHAIRS

Attackers continue to prove their adaptability. They shift lures and payloads to follow trends, interests, and, most importantly, money.

With its volatile but still-meteoric rise in value and popularity, cryptocurrency quickly became a target of phishing, malware, and web-based attacks in 2017. Cryptocurrency-related attacks went so far as to manipulate internet searches to lure victims. In one case, a group bought ads on Google and other search engines to direct potential victims to fake cryptocurrency wallet sites designed to steal wallet credentials.

Our network sensors tracked upticks in coin mining malware activity that corresponded to the sharp rise in Bitcoin values at the end of 2017. Coin miners are running on client PCs, embedded in websites, and running on networked servers. At the same time, DNS requests for "Monero mining pool" steadily ramped up through November. Then they dropped off in early December as values of cryptocurrency across the board followed Bitcoin downward (Figure 17).

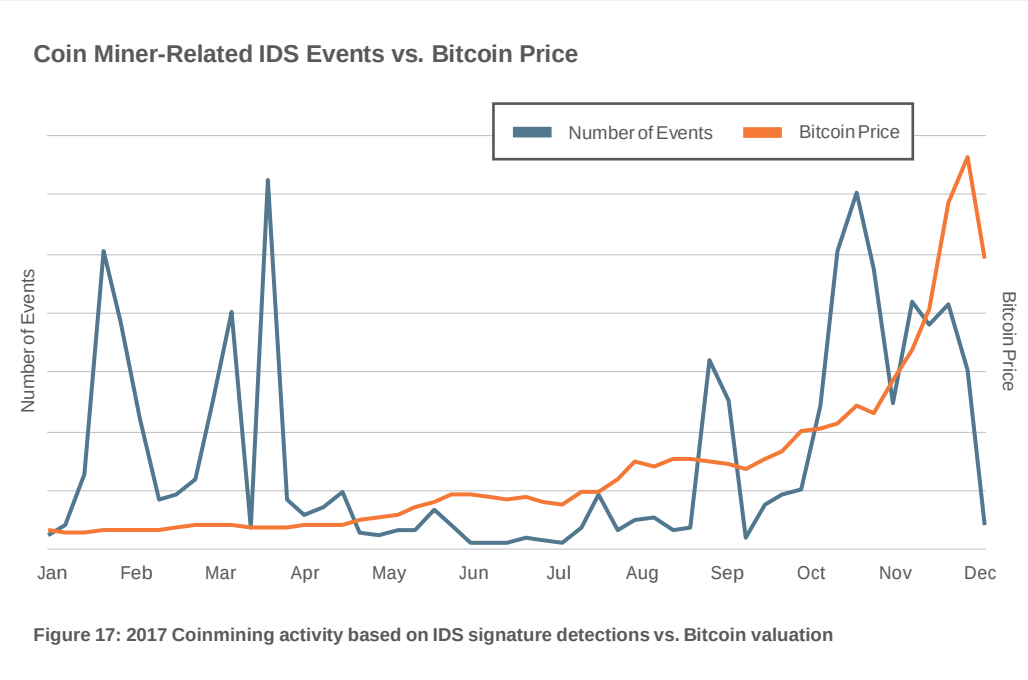


Figure 17: 2017 Coinmining activity based on IDS signature detections vs. Bitcoin valuation

GOOTKIT
The highly persistent banking Trojan, first reported in 2014, has been linked to attacks.

Cryptocurrency phishing campaigns continued in email. Our researchers identified sophisticated phishing templates targeting wallets and exchanges. These included a campaign that tried to trick users into opening a malicious document attachment. The document exploited a vulnerability in Microsoft Office to install the **GOOTKIT** banking Trojan (Figure 18) on affected PCs.

Our researchers found **over 100,000 Bitcoin-related domains.**

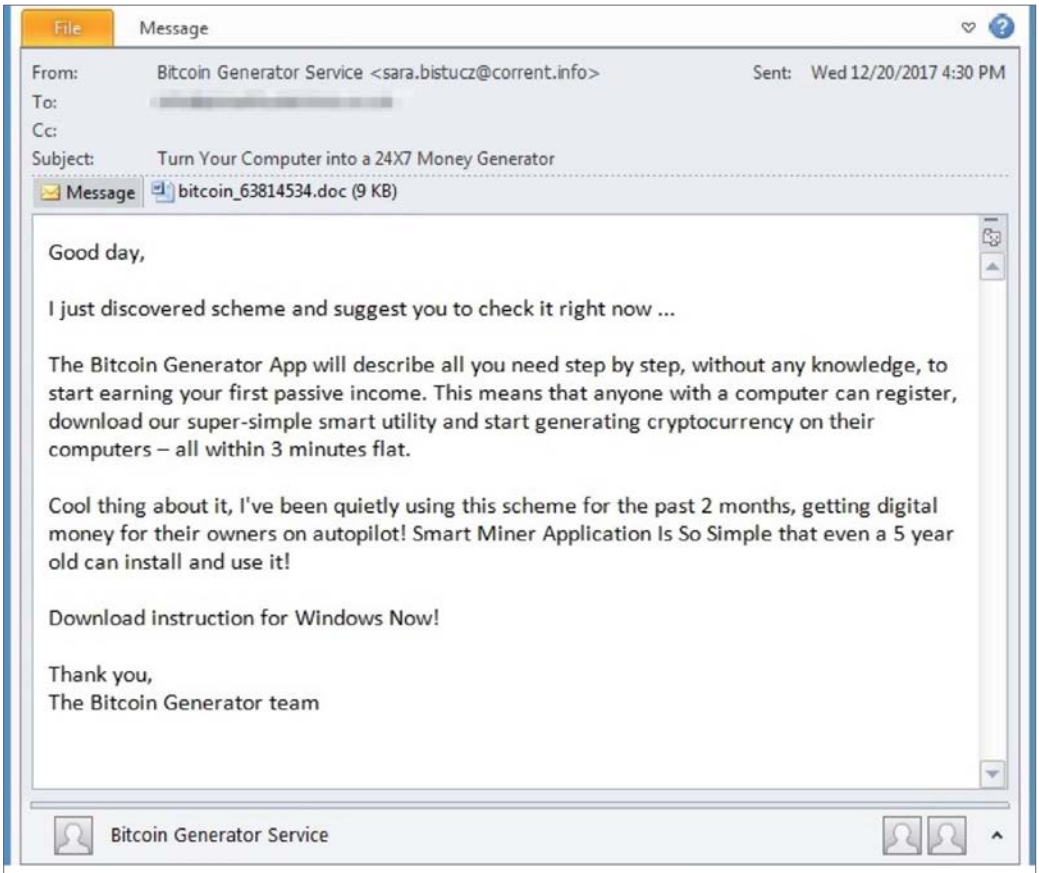


Figure 18: Bitcoin-themed email lure and attachment distributing Gootkit (from December 2017)

At the same time, suspicious domain registrations using “bitcoin” and other cryptocurrency terms increased. Threat actors were building a repository of domains that could be used in a variety of email and web-based attacks.

Our researchers found over 100,000 Bitcoin-related domains (those that contain the word “bitcoin” or variations of that word) as of January 12, 2018. Variations of the word “bitcoin” may include typosquatting and the use of Punycode. Punycode takes advantage of a quirk in the internet’s domain naming system to create lookalike URLs. For example, Punycode for domain “xn--9naa4azkq66k5ba2d.com” is displayed as “bitcoin.com” in Unicode.

As with Bitcoin-related related network traffic, the number of suspicious domain registrations has risen and fallen in step with Bitcoin prices (Figure 19).

Threat actors were building a **repository of domains** that could be used in a variety of email and web-based attacks.

Number of Registrations, Price of Bitcoin in U.S. Dollars, and Number of Suspicious Registrations

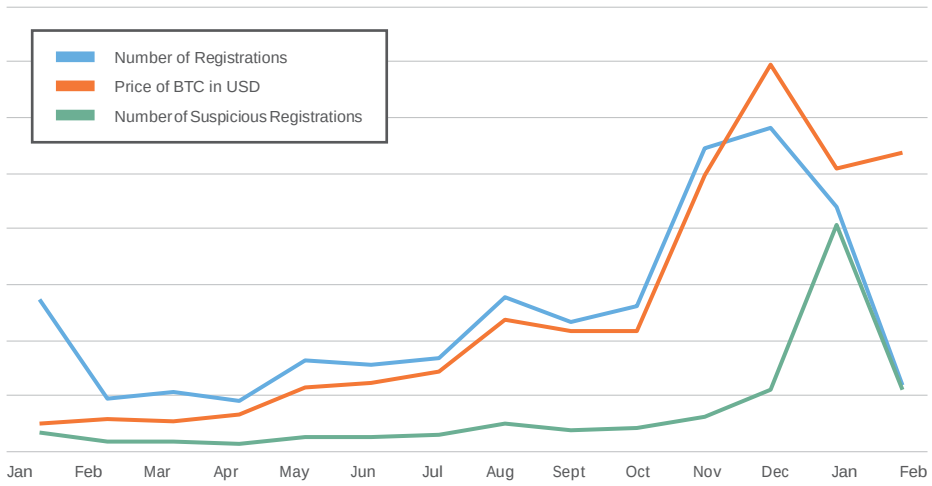


Figure 19: Bitcoin-related domain registrations vs. Bitcoin price over time

CONSIDERING DIGITAL RISK: SOCIAL MEDIA, FRAUDULENT DOMAINS AND BEYOND

WHY WE TRACK THIS

As business processes and commerce go digital, attackers are finding new ways to exploit them. Researching suspicious domain registrations, scams and social engineering techniques—and who they target—helps anticipate and stop future attacks.

BOTNET
A collection of computers that have been compromised and are under the control of attackers. The compromised machines are spread around, have "clean" IP addresses, "and, harnessed together, make the botnets useful in large attacks and spam campaigns.

Human interaction and commerce are increasingly digital, and threat actors are adapting to that reality. They are following shifting trends, usage patterns, and popular interests to attack people through social media channels.

Many of these attacks rely on social engineering. Others simply take advantage of inclinations for immediate gratification, improved status, or even the reward of "getting something for nothing."

But as the old adage goes, there is no such thing as a free lunch. The hidden costs of a bargain in social media channels can often be credential loss to phishing, coin mining through browser hijacking, and malware infections.

Our researchers, for example, identified a large social media **BOTNET** built by exploiting an early version of the Facebook API and a legitimate but outdated version of a third-party app. The botnet operators convinced Facebook users to install the third-party app and provide an API access token in exchange for more likes on their posts.

In reality, the app supported a botnet used to generate spam on a variety of branded Facebook pages. Facebook has since made changes to prevent this type of abuse. But the scheme is a window into the myriad ways threat actors can prey on social media users.

Angler phishing, also known as social media support fraud, is another risk to social media users. In angler phishing, attackers insert themselves into conversations between people and brands they trust using lookalike social media handles to steal personal information.

Financial services brands are the most likely to be abused in this way. About 55% of all angler phishing attacks we observed targeted financial institutions and their customers.

Customers of entertainment and media companies experience less than half of this. They accounted for 25% of all social media support fraud. The remaining 20% of angler phishing targets customers of technology, food, and telecommunications brands.

More traditional social engineering scams include posting bogus coupons and links to malicious pages claiming to be free offers, often for movies or performances. In other cases, attackers send carefully engineered phishing scams as direct messages to social media users.

Figure 20 shows the distribution of scam types we observe on social channels, either posted as links or fake social media pages.

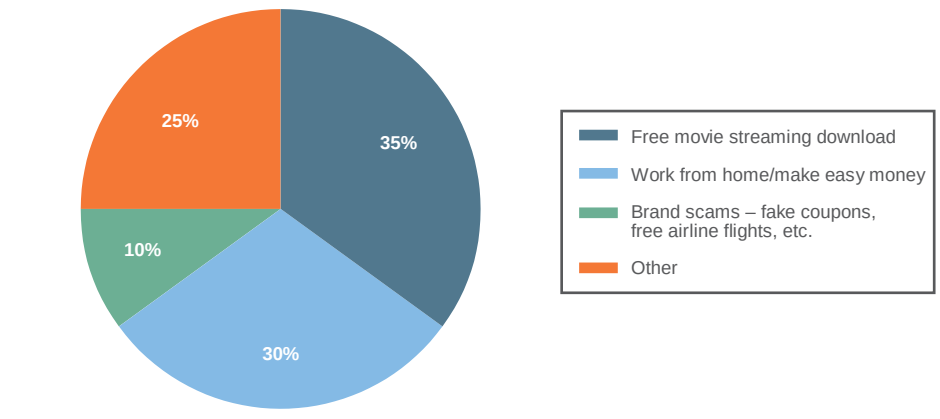


Figure 20: Types of scams seen on social media

Figure 21 shows a large spike in scam activity tied to media brands coinciding with major entertainment and media launches.

The movie-related scams we observed did one or more of the following:

- Hosted malware on linked sites
- Phished for user's personal information or credentials
- Made money more directly by serving large numbers of online ads

The ads are often circular, leading to more ad-filled pages. For each click, the fraudster makes money. The spike in Figure 21 is an extreme example. But it represents one more case in which threat actors adapt their lures and attacks to major events and trends.

We've already seen **more than 500 suspicious domains** that relate to "tokyo2020," about 100 for "beijing2022" and roughly 200 for "paris2024."

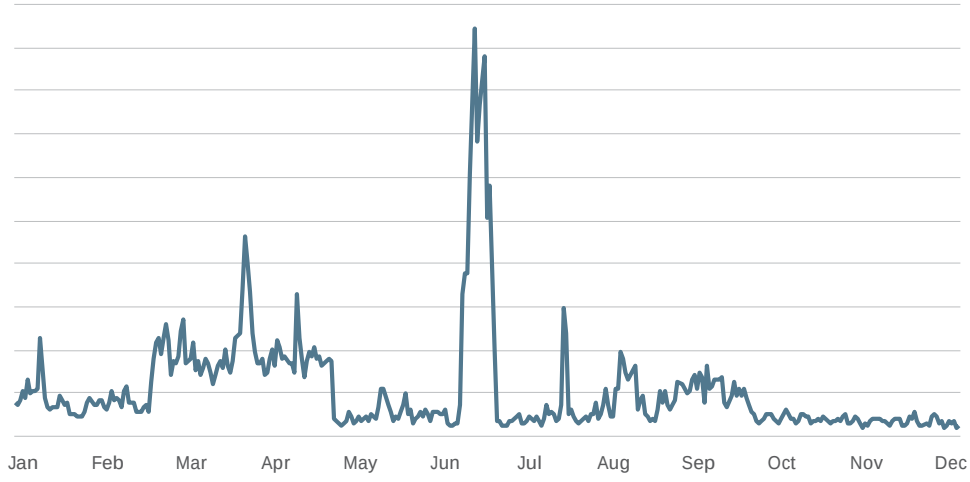


Figure 21: Social media scam volume by day

As noted earlier, scammers used the 2018 Winter Olympics for similar activities. This trend continues for upcoming Olympic games. We have already seen more than 500 suspicious domains that relate to "tokyo2020," about 100 for "beijing2022" and roughly 200 for "paris2024."

Most recently, a large number of websites are impersonating major brands but residing on unrelated domains. Attacker and fraudsters are buying "clean," unused and expired domains from a robust secondary market. These URLs are valid and have solid reputation scores, making detection by security tools more difficult.

Threat actors count on users simply clicking links and being fooled by the content of the sites rather than noticing the unrelated URLs. We have seen this kind of brand impersonation across industries, though it is often focused on selling luxury goods and clothing items at a too-good-to-be-true discount. Once users provide credit card information, the site operators rarely deliver what they promise. They deliver cheap counterfeit merchandise and may even resell credit card information.

WHY WE TRACK THIS

More businesses are moving to the cloud, creating new kinds of risk. Analyzing how attackers are getting access to this infrastructure—and how some users are inadvertently misusing it—provides critical insight into how to better protect against these new threats.

CLOUD SERVICES AS A THREAT VECTOR

The cloud and software-as-a-service (SaaS) apps are mainstays of modern business and consumer computing. They are also quickly becoming the latest frontier of innovation for threat actors.

24% of all suspicious logins to cloud services were successful

In a recent sample of prospective customers, about 1% of SaaS credentials were compromised and 24% of all logins to cloud services were suspicious. Suspicious logins included:

- Malicious sources such as bots, scanning hosts, Tor nodes, and more
- Non-human logins from cloud infrastructure and third-party services
- "Too-fast-to-travel" events

Malicious logins, such as those from bots, are common in "traditional" cyber crime. Non-human logins into cloud-based infrastructure and services are a more recent phenomenon. These come from a service or app—some of which may not have been explicitly authorized by a user or organization.

Too-fast-to-travel events refer to situations in which someone logs into an account from one region—and then another login is detected from somewhere the first person couldn't have traveled too that soon. For example, say a legitimate login occurs from a U.S.-based IP address. Then two hours later, someone logs in from a Chinese IP address. At least one of those logins is suspicious.

Risky apps and add-ons

OAUTH
This open standard allows internet users to grant websites or apps permission to connect to cloud-base services without giving them their passwords.

For authorized apps and third-party add-ons, users are often unaware of the hidden layers of access—and risks. For example, if someone authorizes a third-party cloud email add-on, an **OAUTH** token may allow the app to synchronize the user's email on a separate, less-than-secure server. Once authorized, these apps continue to have access—even after the user deletes the app or quits the service.

We saw danger signs when examining third-party apps accessing core cloud services. Most of the organizations we surveyed had hundreds of apps installed on cloud platforms. Roughly 18% of these apps could access email or files. In many cases, this access may be legitimate and useful. But often, organizations are unaware that the apps have unfettered access to critical communications and data.

Sharing made easy. Too easy.

Anytime, anywhere access and easy integration with a variety of third-party add-ons are among the greatest strengths of cloud apps. But they also represent the greatest risks to personal and corporate data.

In many cases, we also see people failing to follow best practices for cloud apps. This behavior may stem from convenience, lack of governing policy, or ignorance.

For example, in our sample:

- Thousands of files were shared with personal, non-business accounts (see Figure 22)
- Hundreds of thousands of files were shared openly with the entire organization rather than being limited to those who needed access.
- Tens of thousands of files were shared publicly

In the emerging cloud era, the human factor is alive and well. Carelessness, ignorance, or lack of guidance can all lead to oversharing and new risks to data. Personal and public file sharing can pose a particular risk—especially after employees leave an organization but retain access.

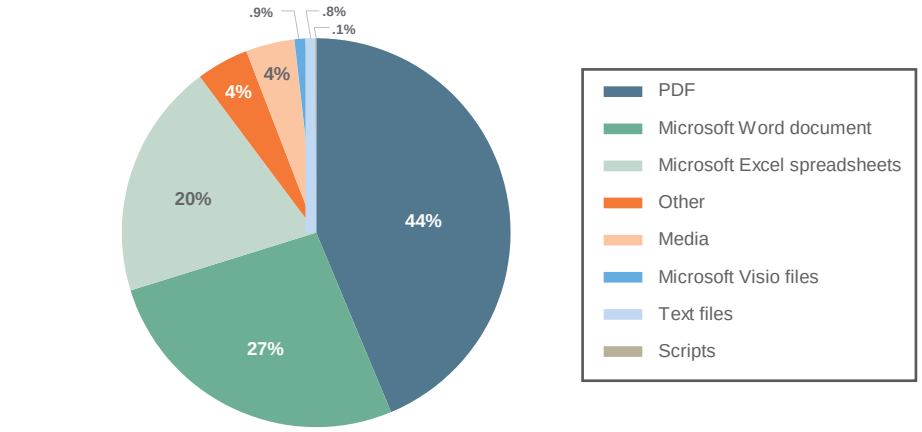


Figure 22: Distribution of file types shared via personal accounts

Using good for bad: abuse and compromise of legitimate services to fool users and defenders

As we adopt cloud apps and services at scale across organizations and use them frequently in our daily lives, our habits are changing. Our security tools are not changing as quickly.

We have become accustomed to receiving everything from emailed surveys to shared files from a variety of services. The tools and services we rely on to defend ourselves from cyber threats are often configured to trust email and other content from major, reputable email providers. So when attackers abuse "good services for bad purposes," we often are not prepared. That makes these services useful vectors for attackers.

Many of these platforms are extensible by design. That versatility opens up new features for organizations. It also creates wide-ranging possibilities for abuse.

MACRO
Macros allow users to create complex sets of actions through simple triggers. Attackers use these powerful features to compromise vulnerable PCs.

Google Apps Script, for example, allows users to add **MACRO**-like functionality to its G Suite platform and control many core functions through code. In 2017, our researchers identified a vulnerability in Google Apps Script that allowed attackers to spread malicious code through legitimate emails originating from G Suite accounts.

Google has since made changes preventing this type of abuse. But as is the case with Microsoft Office macros, most vendors and organizations will opt for powerful features rather than disabling such functions completely, even if they might be abused.

Abusing legitimate services goes beyond exploiting vulnerabilities or misusing extensibility features. For much of 2017, attackers used Microsoft SharePoint to host malware that was sent in millions of messages across hundreds of campaigns.

By the end of 2017, Microsoft made changes to mitigate this sort of abuse, such as limiting the number of anonymous downloads of files hosted on SharePoint. Attackers again proved adaptable. They simply sent malware through other services such MailChimp, ConstantContact, and Sendgrid, all of which had been abused in earlier campaigns as well.

Abusing legitimate services has other benefits for threat actors beyond the inherent trust people and tools place in them. Legitimate email service providers (ESPs) operate at massive scale. They are frequently used by legitimate marketers to send large email blasts. And they are used by organizations ripe for abuse.

As a result, ESPs themselves have a hard time detecting malicious activity. And shutting it down often amounts to an unwinnable game of whack-a-mole.

REPUTATION-BASED DEFENSES
This category of analysis, which assesses the reputation of the sender, can quickly identify known threats. But is often blind to new and emerging threats.

Detecting malicious activity from legitimate services requires deeper, dynamic analysis than **REPUTATION-BASED DEFENSES** can offer alone. Attacks that leverage legitimate services exploit the human factor. And like other people-centered attacks, they challenge automated defenses as and the people being targeted.

CONCLUSION

As the threat landscape continues to evolve, new tools and approaches are emerging regularly. But one thing remains constant: the human factor. More than ever, cyber criminals rely on people to download and install malware or send funds and information on their behalf. And as the shelf lives of automated exploits get shorter, the potential return on investment from social engineering will further outpace that of automated attacks.

Social engineering is at the heart of most attacks today. It can come through something as simple as a bogus invoice lure in a multimillion message malicious spam campaign. It may appear as an intricate fake chain of emails and out-of-band communications in email fraud. Even web-based attacks—which once depended almost exclusively on exploit kits and drive-by downloads—are now built around social engineering templates. People willingly download bogus software updates or fake anti-malware software.

These opportunistic attacks extend to social media channels and cloud-based tools as well. Fraudsters and other attackers capitalize on major events and trends and leverage legitimate services to trick defenders and victims.

Threat actors themselves are focusing more on individuals rather than entire organization. No industries were exempt from attack. But in some cases, risk varied by industry and over time by a number of measure, including roles within an organization, the severity of threats received, and the types of datato which users had access.

We also saw state-sponsored attacks against individuals for financial gain and APT-style tools groups looking to key personnel in restaurants and other targets. In many cases, these smaller targets may not be prepared to defend against sophisticated threats.

Regardless of the vector or approach attackers use, defenders in security operations must understand threat actors and how they operate. Threats may come from what appear to be legitimate sources. They may not involve easily recognized malware. And they will frequently leverage channels ranging from social media to web-based attack chains.

Attackers are opportunistic and adaptable. They take advantage of new options, vectors, and tools to increase their chances of success.

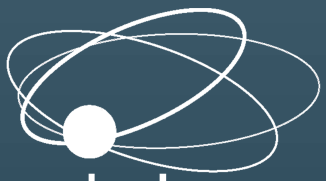
RECOMMENDATIONS

Today's attacks target people, not just technology. They exploit the human factor: our natural curiosity, desire to be helpful, love of a good bargain, time constraints and respect for authority. Protecting against these threats requires a new, people-centered approach to security.

We recommend the following:

- **Train your people to spot attacks that target them.**
  Your security awareness training should include phishing simulations that use real-world tactics to see who's most at risk. Teach them to recognize attacks on email, cloud apps, mobile devices, the web, and social media.
- **Get advanced threat analysis that learns and adapts to changing threats.**
  Today's fast-moving, people-centered attacks are immune to conventional signature- and reputation-based defenses. Be sure your defenses adapt as quickly as attackers do.
- **Deploy DMARC authentication and lookalike domain (typosquatting) defenses.**
  These technologies stop many attacks that use your trusted brand to trick employees, partners, vendors, and customers.
- **Get visibility into the cloud apps, services and add-ons your people use.**
  Deploy tools to detect unsafe files and content, credential theft, data theft, third-party data access, and abuse by cloud scripting apps.
- **Automate some aspects of detection and response.**
  Automated tools can proactively detect security threats and other risks posed by the ever-growing volume of apps your people use in the enterprise. And security orchestration and automation solutions can help you respond faster and more effectively. Consider solutions that connect, enrich, and automate many steps of the incident response process. That frees up security teams to focus on tasks that people do best, boosting awareness and security.

Single Point of Contact provides comprehensive IT security consulting services to ensure the impact of a potential cyberattack is minimal. We tailor our services to ensure our clients stay secure around the clock, so you can rest assured that your network is secure. Email or call us at **800-791-4300** to learn more about how our services can protect you from a security breach or the dreaded compliance violation.



single point of contact

For the latest threat research and guidance about today's advanced threats and digital risks, visit **proofpoint.com/us/threat-insight.**