REPORT

proofpoint®

QUARTERLY THREAT REPORT

Q4 2017

proofpoint.com

The *Proofpoint Quarterly Threat Report* highlights the trends and key takeaways of attacks we see within our large customer base and in the wider threat landscape.

Every day, we analyze more than 1 billion email messages, hundreds of millions of social media posts, and more than 150 million malware samples to protect organizations around the world from advanced threats. We continue to see sophisticated threats across three primary vectors: email, social media, and cloud apps. That gives us a unique vantage point from which to reveal and analyze the tactics, tools, and targets of today's cyber attacks.

This report is designed to provide actionable intelligence you can use to better combat today's attacks, anticipate emerging threats, and manage your security posture. Along with our findings, the report recommends steps you can take to protect your people, data, and brand.

TABLE OF CONTENTS

KEY TAKEAWAYS: COIN MINERS AND RANSOMWARE ARE FRONT AND CENTER

Here are the key takeaways from the fourth quarter of 2017.

EMAIL

The volume of messages bearing malicious document attachments jumped 300%.
Much of this traffic stemmed from massive attack campaigns that abused Microsoft's **DYNAMIC DATA EXCHANGE** protocol and used social engineering.

RANSOMWARE remained the top payload distributed by malicious messages.
This type of attack accounted for 57% of all malicious message volume.

The number of ransomware payment demands denominated in Bitcoin fell 73% amid wide swings in the CRYPTOCURRENCY's value.
Attackers are increasingly setting ransom amounts in terms of U.S. dollars or local currency (though the payment itself is usually still in cryptocurrency).

THE TRICK was the most used banking Trojan.
It accounted for 84% of all malicious spam that contained a banking Trojan.

Lookalike and TYPOSQUATTED domains were used in a wide range of attacks
Character-swapping was the top technique used to create domains that could be confused with an established brand or organization.

EXPLOIT KITS AND WEB-BASED ATTACKS

Social engineering techniques grew as browser exploits fell among high-profile, web-based attack campaigns.
EXPLOIT KIT (EK) traffic fell 31% from the previous quarter. The RIG EK was the most used EK.

SOCIAL MEDIA

The number of fraudulent customer-support accounts on social media rose 30%.
At the same time, phishing links in social media grew 70% from the previous quarter.

DYNAMIC DATA EXCHANGE
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.

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

CRYPTOCURRENCY
A form of digital money designed to be secure and anonymous, making it well suited for ransomware payments that cannot be traced to the attacker.

THE TRICK
The Trick, also known as TrickBot, is a banking Trojan closely related to Dyre. While its operators were arrested in 2015 by Russian authorities, it saw a resurgence in 2017.

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.

EXPLOIT KIT
Exploit kits (EKs) run on the web, detecting and exploiting vulnerabilities in computers that connect to compromised sites, malicious ads, and attacker-controlled landing pages. EKs, often sold to attackers as a service, make it easy to infect PCs in "drive-by" malware downloads and are increasingly being used to deliver social engineering attacks that do not rely on active exploits.

TA505
Motivated by financial gain, this threat actor is the source of some of the largest email attack campaigns on record, including those spreading the Dridex banking Trojan, Locky ransomware, Jaff ransomware, The Trick banking Trojan, and more.

LOCKY
Locky is the most common strain of ransomware seen in malicious emails, encrypting victims' data and holding it "hostage" until the victim pays to decrypt. For most of 2016 and several months in 2017, Locky accounted for the majority of malicious email traffic.

GLOBEIMPOSTER
This ransomware variant, also known as Fake Globe, mimics and is named after an earlier ransomware strain called Globe. Initially used in small regional campaigns, GlobeImpostor became a global threat when the prolific threat actor TA505 began using it in larger campaigns.

EMAIL: MALICIOUS DOCUMENTS OVERTAKE URLS

Key stat: The volume of messages with malicious document attachments jumped 300% from the third quarter.

The global volume of messages carrying malicious attachments rebounded, surging more than 300% vs. the previous quarter. Driven by high-volume campaigns from threat actor **TA505**, these messages often distributed The Trick banking Trojan or an assortment of ransomware strains, including **LOCKY** and **GLOBEIMPOSTER**.

Several attackers seized on the disclosure of a technique for abusing Microsoft's Dynamic Data Exchange (DDE) to deliver malware in large and small campaigns.

By the end of October, attackers had largely abandoned the technique as they turned to their usual methods of exploiting malicious macros and other forms of embedded code. But sporadic campaigns using the DDE technique continued in November and December, as the technique took its place in threat actors' rotating toolkit.

Indexed Daily Malicious Message Volume by Attack Type, Q4 2017

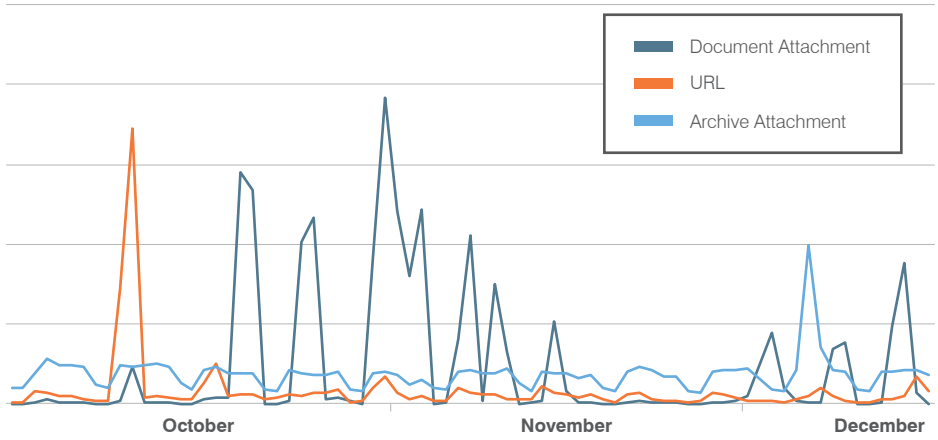

Figure 1: Indexed attack type trend, October 2017 through December 2017 (77 Days)

Conversely, malicious URL use plummeted—the exceptionally high volumes of the third quarter proved to be an anomaly. Still, all attack types remain popular with a variety of threat actors.

Figure 1 shows dramatic swings in the volume of malicious messages that use malicious URLs, document attachments, and archive file attachments (such as ZIP or 7-Zip). These constant shifts highlight attackers' flexibility. They continually vary attack types, payloads, and infection techniques to grow more effective and get the biggest returns.

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

ZEUS PANDA
Also known as Panda Banker, this banking Trojan is related to Zeus, one of the earliest banking Trojans.

COIN MINERS
Cryptocurrency 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, generating cryptocurrency for the threat actor distributing the malware.

WEBINJECT
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 (for example, with their banking credentials), that information is sent to the attacker instead of the bank.

BANKING TROJANS: NOT JUST FOR BANKING

Key stat: Messages distributing The Trick accounted for 84% of BANKING TROJAN message volume.

The Trick extended its run as the top banking Trojan by global message volume. It appeared in six times as many messages than all other observed banking Trojans combined. This is a far cry from 2016, when Dridex and Vawtrak were the top bankers and The Trick was limited to mostly small, geo-targeted campaigns.

Along with The Trick, **ZEUS PANDA** (aka Panda Banker) and Emotet also appeared frequently in Q4 campaigns. And several regular attackers quickly adopted a new Trojan called IcedID.

Some banking Trojans—most notably, The Trick—added cryptocurrency mining modules or bots. Other banker campaigns added **COIN MINERS** as later-stage payloads, expanding a trend that we reported in Q3.

In past years, the autumn months have seen more variation in targeting by banking Trojans. The fourth quarter of 2017 was the same. Zeus Panda campaigns that supplemented and expanded the bot's customary online banking **WEBINJECTS** with injects targeting the online shopping sites for a variety of popular brick-and-mortar retailers.

These changes serve as a sharp reminder that banking Trojans are by no means limited to targeting the customers of financial services firms. Online customers of *any* business or service are potential targets.

RANSOMWARE: BITCOIN VOLATILITY SHAKES UP THE BUSINESS

Key Stat: The use of Bitcoin to denominate ransomware demands fell 73%.

Despite a surge in banking Trojan message volume—largely driven by large campaigns by a single attacker using The Trick—ransomware remained the dominant malicious payload in email campaigns. It accounted for more than 57% of all malicious messages, as shown in Figure 2.

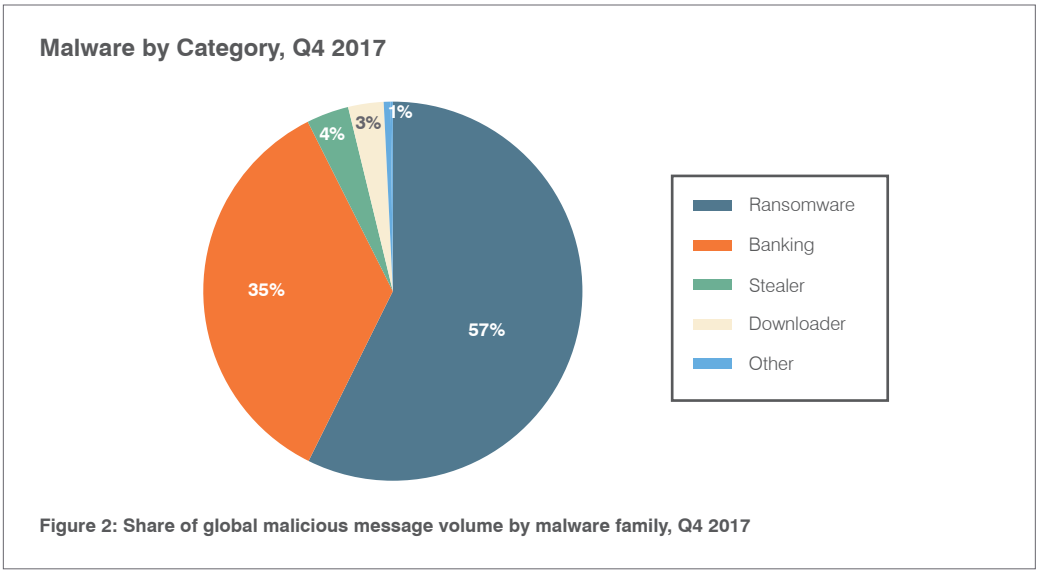

Figure 2: Share of global malicious message volume by malware family, Q4 2017

For much of the last two years, attackers' ransoms have been denominated in Bitcoin values. The amount demanded is expressed as some number of bitcoins, whether a full integer or a fraction such as "0.5" or "0.15."

Surging cryptocurrency values are a boon for holders of Bitcoin. But they are a challenge for anyone who tries to price their product or service in Bitcoin—threat actors included.

In Q4, newer ransomware strains appeared to take this into account. Sigma ransomware first appeared in mid-November demanding a payment denominated in U.S. dollars.

Denominating ransoms in a government-issued currency—even if the actual payment is made in the form of Bitcoin—has two big benefits for an attacker. It allows the threat actors to maintain pricing stability and still accept their payments anonymously, and in a currency that, for the moment, continues to appreciate quickly.

By analyzing ransomware demands over a 90-day period into mid-December, it is easy to understand that the currency switch was part of a broad trend across a range of attacks (Figure 3).

Ransomware Ransoms Denominated in Bitcoin vs Traditional Currency, 90-Day Trend

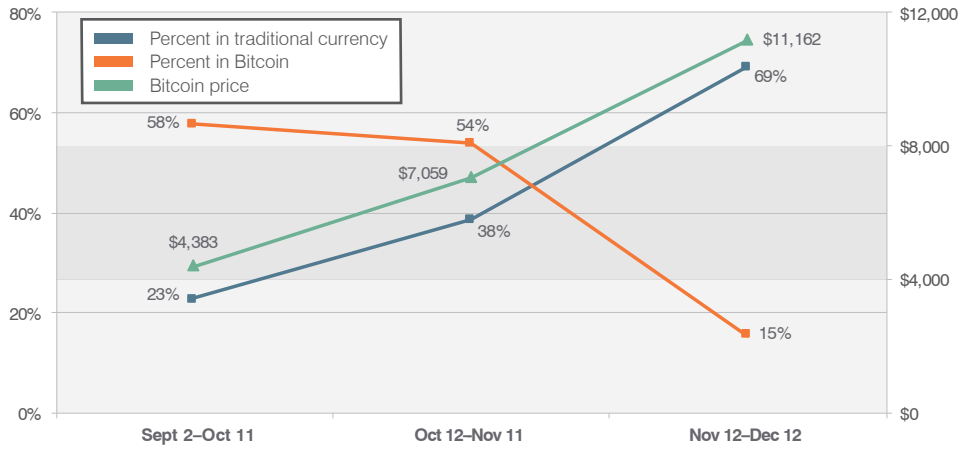

Figure 3: Ransomware ransoms denominated in Bitcoin vs. traditional currency 90-day trend

Denominating ransomware demands in traditional currency instead of or in addition to Bitcoin clearly correlates to the surge in Bitcoin valuations. Economics would suggest that the latter actually causes the former.

This trend may reverse if Bitcoin prices fall back to earth. No matter what happens, the correlation is more evidence of modern cybercriminals' profit motive. They choose the tools and techniques that will best enable them to "follow the money."

TARGETED THREAT ACTORS BREAK THE SURFACE

Many of the campaigns tracked by our researchers in Q4 were broadly distributed commodity malware payloads. But we also analyzed and reported on activities by several highly targeted threat actors, including the Lazarus Group, APT28, and a new threat actor we dubbed Leviathan.

Email and documents used in these attacks were often personalized and tailored to the interests and business of the targeted recipient. They used stolen branding and public documents. And they took advantage of typosquatted or lookalike domains to trick recipients into clicking links or downloading files.

EMAIL FRAUD THREATS: MAKING SENSE OF FRAUDULENT DOMAIN NAMING PRACTICES

DEFENSIVE DOMAIN REGISTRATION
The recommended practice of purchasing internet domains that could be mistaken for those of legitimate brands 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.

ANGLER PHISHING
In angler phishing, attackers create fake customer support accounts on social media to trick people looking for help into visiting a phishing site or providing account credentials.

Key stat: The average number of DEFENSIVE DOMAIN REGISTRATIONS is 300 domains. For large enterprises, suspiciously registered domains can outnumber brand-registered domains 20 to 1.

Our research suggests that threat actors are dramatically outpacing brands in the registration of suspicious domains vs. defensive registrations. This wide gap leaves brands open to fraud, phishing, spoofing, and more.

To defend themselves, organizations do not have to register every possible permutation of their domain or domains. Instead, they can analyze the most common changes and substitutions to prioritize their defensive registrations and manage a more reasonable subset of potential typosquatted domains.

Lookalike domains account for just over 3% of email fraud attempts overall. But they make up a disproportionate number of domains used in email fraud, phishing, **ANGLER PHISHING**, and other attacks.

While some observers pay more attention to fraudulent registrations in new or unusual top-level domains (TLDs), suspicious registrations in the standard ".com" remain by far the most common.

Nearly 82% of such registrations use ".com." Moreover, almost 90% of suspicious registrations used the same TLD as the brand they impersonated. Email fraudsters often use simple variations on the legitimate domain names within the TLD of the brand they are trying to impersonate.

Figure 4 highlights common spelling patterns in suspicious domain registrations.

Type of Cousin Domain	Different TLD	Same TLD	Grand Total
Individual character swapped	3.49%	37.60%	41.09%
Inserted additional character	0.97%	31.15%	32.12%
Added or removed leading/trailing characters	0.73%	12.51%	13.25%
Removed character	0.41%	5.10%	5.51%
Exact match hyphenated	1.23%	3.40%	4.63%
Exact match	3.40%	0.00%	3.40%
Grand Total	**10.23%**	**89.77%**	**100.00%**

Figure 4: Typosquatting techniques

Swapping individual characters of a brand name within the same TLD is the most common typosquatting technique. Figure 5 breaks out specific letter swaps.

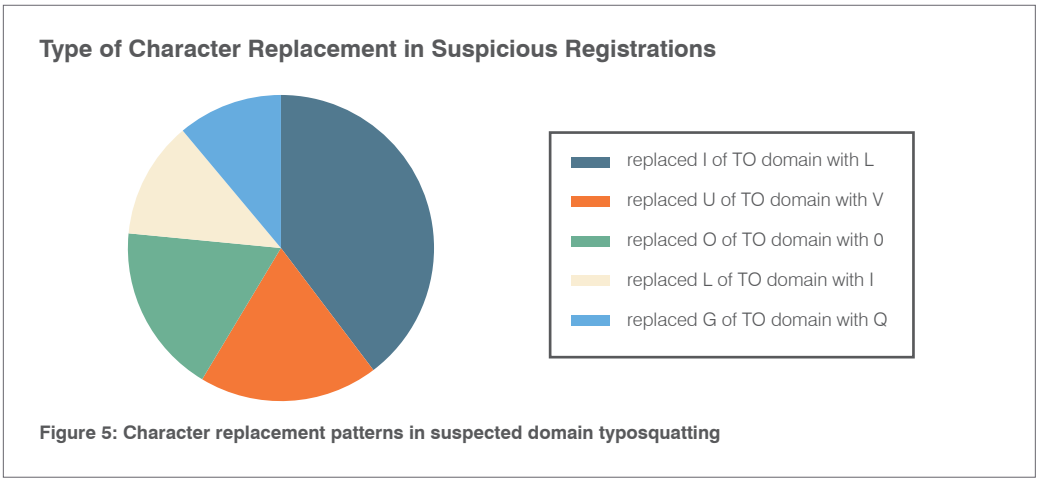

Figure 5: Character replacement patterns in suspected domain typosquatting

WEB-BASED THREATS: CONSOLIDATION AND SOCIAL ENGINEERING

Key stat: Observed exploit kit traffic decreased 31% from Q3.

RIG EK
RIG has become the most widespread exploit kits in the wake of Angler's disappearance after the arrests of its operators in June 2016.

Already subdued exploit kit traffic—which had been holding steady for several quarters at roughly 10% of its 2016 peak—fell further in Q4. The **RIG EK** accounted for almost 98% of observed exploit kit traffic in Q4 2017. But its share of overall traffic decreased at the end of the quarter in the face of a late surge by Magnitude EK (Figure 6).

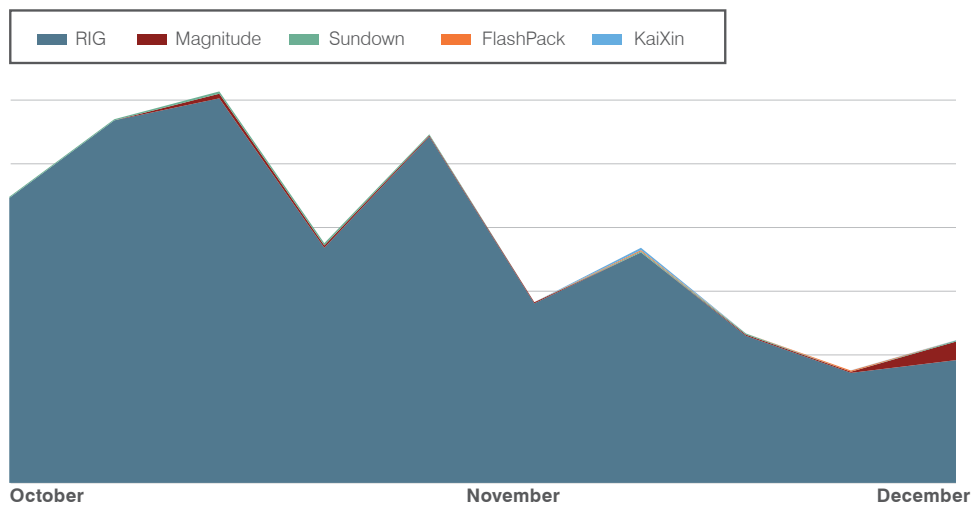

Figure 6: Top exploit kit traffic as percentage of total, October–December 2017

BAD RABBIT
The ransomware strain first appeared in October, targeting people in Russia and Ukraine. It is similar to the NotPetya strain of ransomware. Disguised as an Adobe Flash update, it infects systems through "drive-by" downloads but requires the victim to launch the bogus update.

The big story was the discovery of a large, sophisticated malvertising campaign targeting users of a popular adult video site. Instead of exploiting technical flaws in user's web browser, the attacks tricked people into installing malware themselves. Attackers used sophisticated filtering to target by location and internet provider. Targeted users were presented with a webpage asking them to download an update to their browser or Adobe Flash. Instead, they got the Kovter ad fraud malware, a technique seen in October's **BAD RABBIT** ransomware outbreak.

Attackers face a dearth of viable web browser exploits and the general limitations of exploits as an infection technique. As foreshadowed by early examples in late 2016, they have turned to social engineering-based approaches similar to those used in email attacks—often to great effect.

POINT-OF-SALE MALWARE HAS ITS UPS AND DOWNS

In 2016, we saw traffic associated with specific point-of-sale (POS) malware strains quadruple over the Black Friday weekend. In 2017, spikes were less pronounced. A mix of top POS malware strains were active at various times over the year, not just around Black Friday (see Figure 7).

For example, FindPOS was active in March, wound down through the summer, then resumed activity late in October. That was around the same time MagikPOS slowed, suggesting a single actor switched tools. On the other hand, NewPosThings traffic, aside from a June spike, has remained low and steady for much of the year.

The takeaway? We can speculate that wider chip-and-PIN implementations are making a dent in POS malware, reducing the potential success of seasonal campaigns that lead to spikes in traffic. But we need to further study the cyclical trends in POS malware to determine how, or whether, the threat landscape will coalesce around existing and new variants.

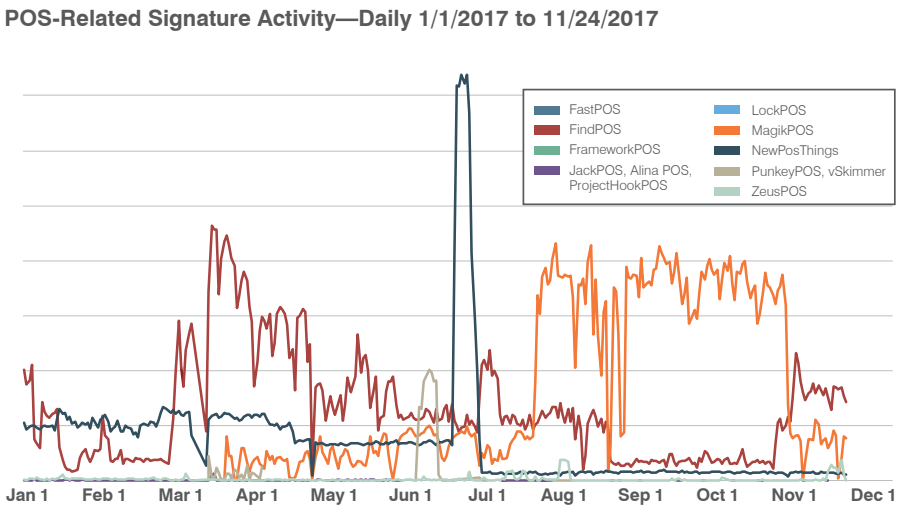

Figure 7: Point of sale (POS) malware traffic, January-November 2017

SOCIAL MEDIA THREATS SURGE INTO 2018

Key stat: Fraudulent customer support accounts on social media grew 30% over the previous quarter and year-ago totals.

Threats in social media surged last quarter. The number of fake customer support accounts grew 30% compared to both the previous quarter and to the same period in 2016.

After remaining flat for most of 2017, phishing links in social media also showed strong growth in Q4, jumping nearly 70% over Q3 (Figure 8).

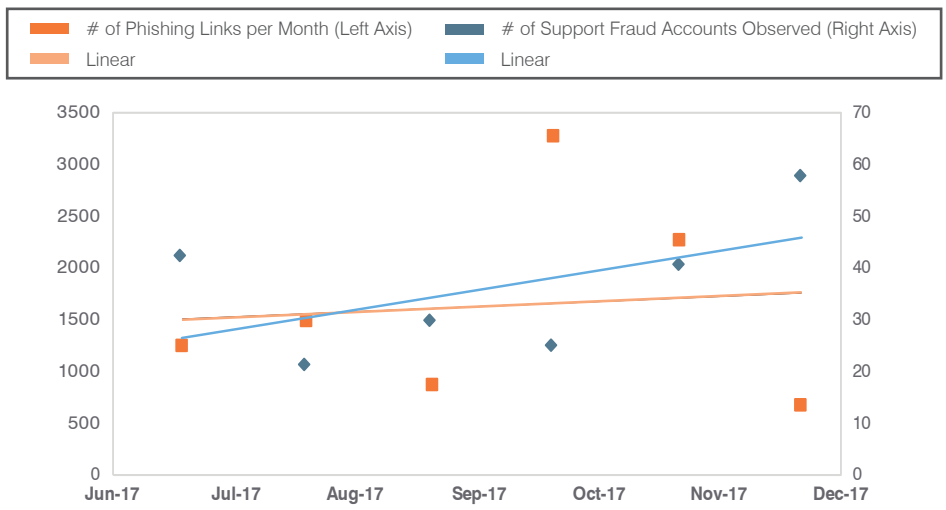

Figure 8: Relative monthly activity in phishing link distribution via social media vs. fraudulent support accounts

RECOMMENDATIONS

This report provides insight into the shifting threat landscape that can inform your cybersecurity strategy. Here are our top recommendations for how you can protect your company and brand in the coming months.

Assume users will click. Social engineering is increasingly the most popular way to launch email attacks and criminals continue to find new ways to exploit the human factor. Leverage a solution that identifies and quarantines both inbound email threats targeting employees and outbound threats targeting customers before they reach the inbox.

Build a robust email fraud defense. Highly-targeted, low volume email fraud scams often have no payload at all and are thus difficult to detect. Invest in a solution that has dynamic classification capabilities that you can use to build quarantine and blocking policies.

Protect your brand reputation and customers. Fight attacks targeting your customers over social media, email, and mobile—especially fraudulent accounts that piggyback on your brand. Look for a comprehensive social media security solution that scans all social networks and reports fraudulent activity.

Partner with a threat intelligence vendor. Smaller, more targeted attacks call for sophisticated threat intelligence. Leverage a solution that combines static and dynamic techniques to detect new attack tools, tactics, and targets, as well as a constantly shifting landscape—and then learns from them.

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

ABOUT PROOFPOINT
Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.