

# QUARTERLY THREAT REPORT

Q1 2018

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

Every day, we analyze more than 5 billion email messages, hundreds of millions of social media posts, and more than 250 million malware samples to protect organizations around the world from advanced threats. We continue to see sophisticated threats across email, social media, and the web. 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 brands.

## TABLE OF CONTENTS

<b>Key takeaways: Banking Trojans take back the top spot while angler phishing explodes.....</b>	<b>4</b>
Email.....	4
Exploit kits and web-based attacks .....	4
Social media and domain research .....	4
<b>Email-based threat trends: Attachments ebb, banking Trojans flow.....</b>	<b>5</b>
Banking Trojans: Emotet leads bankers back to the fore .....	7
Ransomware: Down, but not out .....	7
Email fraud threats: Nobody is immune .....	9
<b>Web-based threats: Exploit kits continue their decline as new threats emerge.....</b>	<b>10</b>
<b>Social media threats: Angler phishing angles up .....</b>	<b>12</b>
<b>Recommendations .....</b>	<b>14</b>

## KEY TAKEAWAYS: BANKING TROJANS TAKE BACK THE TOP SPOT WHILE ANGLER PHISHING EXPLODES

Below are key takeaways from the first quarter of 2018.

### EMAIL

- For the first time since Q2 2016, banking Trojans displaced ransomware as the top malware in email, accounting for almost 59% of all malicious email payloads in Q1.
- Credential stealers and downloaders made up the bulk of the remaining malicious payloads, comprising 19% and 18% of malicious email, respectively.
- The lull in ransomware and generally lower volumes of malicious mail in Q1 appear to be associated with a disruption in the Necurs botnet but have been accompanied by more diverse payloads including RATs, backdoors, and more.
- Emotet was the most widely distributed banking Trojan, accounting for 57% of all bankers and 33% of all malicious payloads.
- 40% of organizations targeted by email fraud received between 10 and 50 attacks in Q1 2018, and the number of companies receiving more than 50 attacks rose 20% compared to the last quarter of 2017.

**FOR THE FIRST TIME IN YEARS, BANKING TROJANS DISPLACED RANSOMWARE AS THE TOP MALWARE IN EMAIL.**

### EXPLOIT KITS AND WEB-BASED ATTACKS

- Exploit kit (EK) traffic continued to decline, falling 71% from the previous quarter.
- Roughly 95% of web-based attacks now redirect into social engineering schemes instead of EKs.
- Proofpoint researchers played a key role in sinkholing ElTest, the web's oldest infection chain, preventing as many as two million malicious redirects a day.

### SOCIAL MEDIA AND DOMAIN RESEARCH

- Social media support fraud, or "angler phishing," exploded in Q1 2018, increasing 200% from the previous quarter.
- 30% of Bitcoin-related domain registrations were suspicious, but new registrations fell off sharply as the value of Bitcoin continued to fall through Q1.
- 84% of Fortune 500 CEOs were victims of threats and hate speech on Twitter and the dark web in February 2018.

### WHY WE TRACK THIS

Email is by far the most frequent source of advanced attacks. Studying attackers' tools, techniques and procedures helps us spot emerging threats and protect against them.

### 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.

## EMAIL-BASED THREAT TRENDS: ATTACHMENTS EBB, BANKING TROJANS FLOW

**Key stat:** URL-based malicious messages outnumbered messages with malicious attachments by a ratio of 4 to 1, marking a swing back to URLs with relative quiet from a single actor normally engaging in high-volume attachment campaigns.

As in past quarters, we observed another pendulum swing in malicious message delivery. While high-volume campaigns delivering malware via a variety of attachments predominated in Q4 2017, the first quarter of 2018 was characterized by lower-volume campaigns that used links to hosted malware. In part, this was due to only sporadic activity from a single actor, **TA505**, who is usually responsible for the highest volume attachment campaigns we see on a daily basis. Even **TA505**, though, sent two large, uncharacteristic spam campaigns linking to suspicious pharmaceutical sales landing pages this quarter.

Indexed Daily Message Volume by Attack Type, Q1 2018

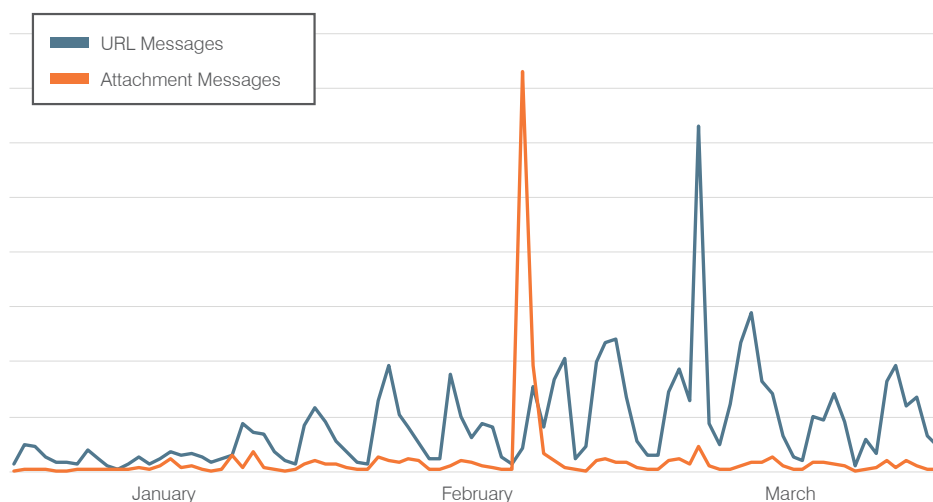


Figure 1: Indexed daily attack type trend, Q1 2018

The slowdown in **TA505** activity allows us to more closely examine trends and payloads that might otherwise be drowned out by massive message volume from a single actor. Moreover, many of the other relatively prolific actors have historically used URLs in their malicious spam, further reinforcing the predominance of URL-based messages. Overall, URL messages outnumbered those with malicious attached documents by a 4-to-1 ratio in Q1.

### REMOTE-ACCESS TROJAN

This type of malware gives attackers total control over the compromised system. Compromised systems may be infected with additional malware, be subject to information theft, or be used as part of a botnet.

The relative mix of payloads in these messages, whether delivered by attachment or URL, also saw a significant shakeup in Q1. For the first time since Q2 2016, banking Trojans displaced ransomware as the most common payload by message volume. As shown in Figure 2, reduced ransomware volumes appeared to open the door for greater payload diversity, with **remote access Trojans (RATs)**, keyloggers, and other types of malware filling the gap.

REDUCED RANSOMWARE VOLUMES APPEARED TO OPEN THE DOOR FOR **GREATER PAYLOAD DIVERSITY**, WITH REMOTE ACCESS TROJANS (RATS), KEYLOGGERS, AND OTHER TYPES OF MALWARE FILLING THE GAP.

Malware by Category, Q1 2018

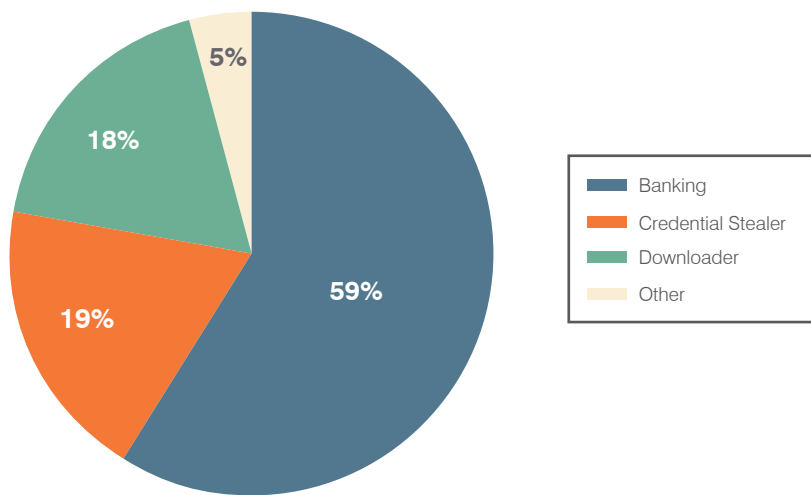


Figure 2: Relative mix of malware payloads in email by category, Q1 2018

Indexed Daily Message Volume by Malware Family

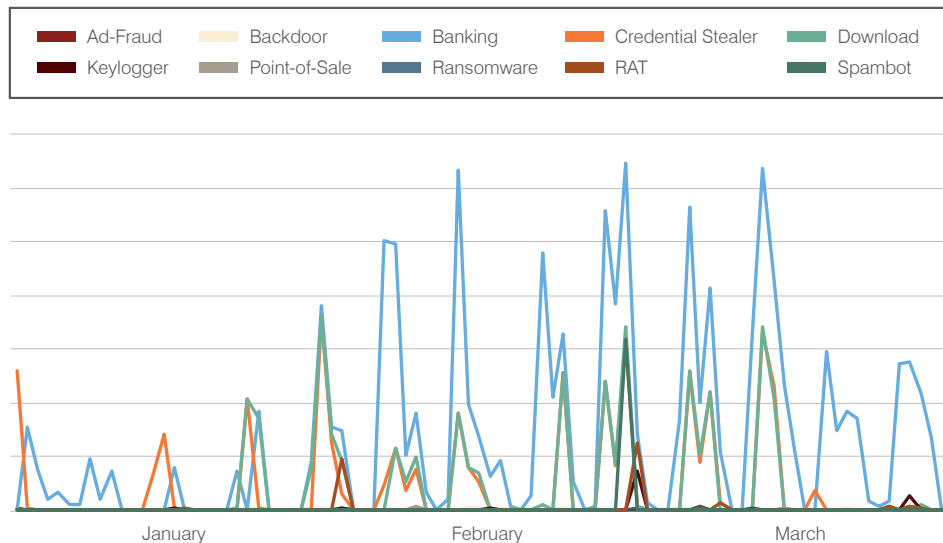


Figure 3: Relative daily message volume by malware category, Q1 2018

## BANKING TROJANS

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

### DRIDEX

Dridex is a widely used banking Trojan that spreads through a variety of vectors, primarily via email, infecting the victims and stealing banking credentials.

### EMOTET

This banking Trojan, first documented in 2014, has evolved to include anti-analysis tools and the ability to spread laterally on networks.

## BANKING TROJANS: EMOTET LEADS BANKERS BACK TO THE FORE

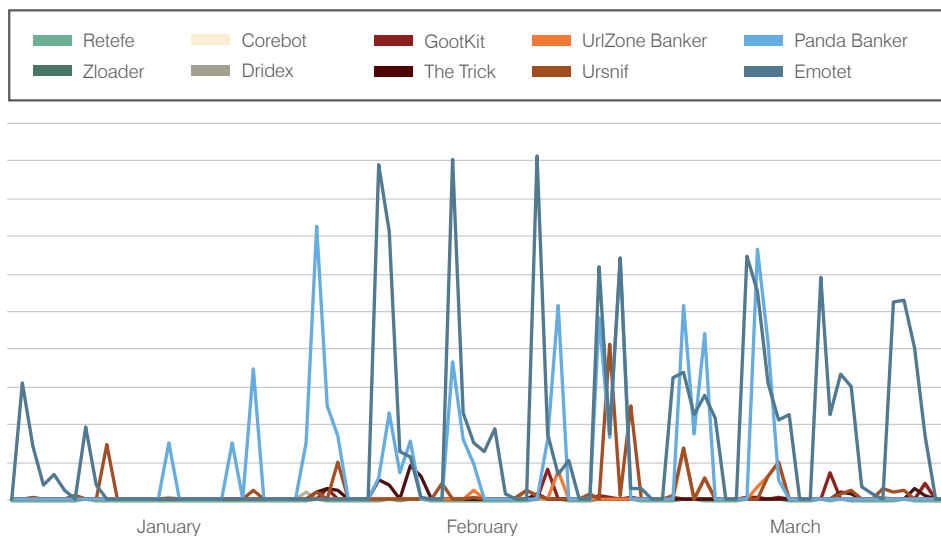
**Key stat: **BANKING TROJANS** accounted for 59% of all observed malicious messages, displacing ransomware for the first time since Q2 2016 as the top malware family by message volume.**

In 2015 and early 2016, banking Trojans, particularly **DRIDEX**, dominated the email threat landscape. While banking Trojans never disappeared, beginning in Q2 2016, ransomware became the primary payload in increasingly massive malicious spam campaigns, with bankers appearing in more focused, region-specific campaigns.

In February 2018, however, the **EMOTET** banking Trojan began appearing in large, consistent campaigns, accounting for almost 57% of banking Trojan payloads in Q1. Emotet is related to Cridex, itself a predecessor to Dridex, and may download both Dridex and Gootkit bankers as secondary payloads. Emotet also includes a spam module for further email-based propagation.

Panda Banker appeared in almost 31% of the remaining banking Trojan campaigns. Figure 4 shows the relative daily mix of banking Trojans throughout Q1.

**Indexed Relative Daily Message Volume With Banking Trojan Payloads**



**Figure 4: Indexed relative daily banking Trojan message volume, Q1 2018**

## RANSOMWARE: DOWN, BUT NOT OUT

**Key Stat: We detect hundreds of WannaCry samples every day.**

## RANSOMWARE

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

Despite a dramatic decrease in the overall volume of messages bearing **RANSOMWARE** payloads, this malware family, which has dominated headlines since early 2016, remains an active threat. In particular, two relatively new ransomware strains—Globelmposter and Sigma—continue to appear regularly in large email campaigns. At the same time, the infamous WannaCry ransomware, once thought to have been rendered ineffective by a so-called "killswitch," has seen continued network traffic, albeit at lower levels than during the 2017 global outbreak.

Figure 5 shows the relative volume of GandCrab, Globelmposter, and Sigma ransomware, the only active ransomware strains observed in email in Q1.

### Indexed Relative Daily Message Volume With Ransomware Payloads

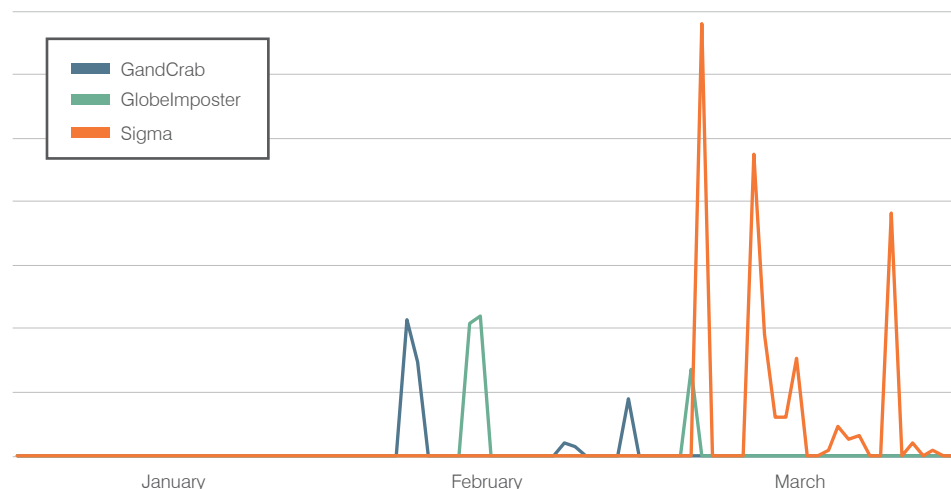


Figure 5: Relative volume of malicious messages bearing ransomware as their primary payloads, Q1 2018

While these volumes are much lower than the multi-million message campaigns that were the norm in previous quarters, they correspond to a fairly typical Q1 lull in TA505 activity, an actor who regularly distributes massive malicious spam campaigns, the volumes of which help define the threat landscape. During Q1 2018, TA505 generally ran less frequent campaigns and focused primarily on banking Trojans and RATs, launching only three ransomware campaigns this quarter.

### WANNACRY

The ransomware infected tens of thousands of systems across more than 150 countries in May 2017, one the largest cyber attacks on record. It spread through a flaw in a file-sharing component of Microsoft Windows.

**WE HAVE OBSERVED CONTINUED WANNACRY ACTIVITY, SUGGESTING THAT THE RANSOMWARE NEVER REALLY WENT AWAY.**

In 2017, our researchers were instrumental in stopping the spread of **WannaCry ransomware**, which initially affected over 100 countries and hundreds of thousands of computers. More recently, though, we have observed continued **WANNACRY** activity, suggesting that the ransomware never really went away but instead continued propagating more slowly. Figure 6 shows weekly intrusion detection system (IDS) activity and new sample detection associated with WannaCry.

### Observed WannaCry Samples

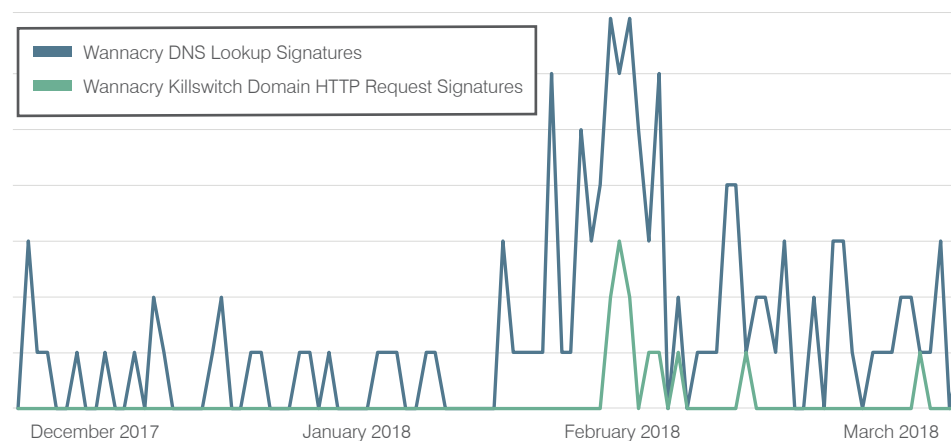


Figure 6: Ongoing WannaCry activity

We will continue to monitor both WannaCry and the larger ransomware space. Given the value of ransomware for both financial gain and creating disruption, it is unlikely that we have seen the last of this malware family.

## 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.

## W2 SCAM

In this scam, someone spoofing an executive asks the finance or HR department to send employee records, which are then used for identity theft and other attacks. It is named after the W2 tax form U.S. employers use to report each worker's wages.

## EMAIL FRAUD THREATS: NOBODY IS IMMUNE

**Key stat: Some 40% of organizations targeted by email fraud (including business email compromise, or BEC) received between 10 and 50 attacks in Q1, and the number of companies targeted by more than 50 attacks rose 20% from the previous quarter.**

**EMAIL FRAUD** continues to grow in both scale and pervasiveness. Roughly 90% of businesses were targeted and, on average, each of these organizations received 28 email fraud attacks in Q1, an increase of 36% from the previous quarter and 28% vs. the year-ago quarter. Successful attacks can result in direct losses in the tens or hundreds of thousands of dollars with lasting indirect impacts as well.

As in past quarters, we did not detect any clear correlation between company size and the likelihood of an email fraud attack. While larger organizations may have deeper pockets and more potential individual targets, smaller companies may be more vulnerable—in either case, both represent attractive targets for threat actors.

In Q1 2018, 40% of targeted organizations received between 10 and 50 email fraud attacks, an increase of nearly 18%. The number of companies targeted by fewer than 10 attacks has been steadily decreasing but, significantly, the number of organizations targeted in more than 50 attacks rose 20% vs. the fourth quarter of 2017.

This level of targeting varied substantially by country. The United Kingdom, for example, saw the highest number of attacks per targeted organization with an average of 36 such emails in Q1. The Netherlands was the lowest among observed countries, with nine attacks on average per targeted organization. For reference, targeted companies in the United States experienced 24 attacks in the quarter.

We also observed upticks in email fraud rates across most industries. In particular, entertainment and media, biotechnology, manufacturing, and transportation experienced increases of more than 50% in the average number of attacks per targeted organization compared to Q4 2017. Within our global customer base, real estate businesses saw the highest rate of email fraud attacks, with targeted organizations experiencing an average of 68 such attacks in Q1.

Social engineering underpins all of these attacks, the majority of which involve wire-transfer scams. The top three specific subject lines in Q1—“Request,” “Payment,” and “Urgent”—were consistent with this type of fraud. Moreover, while the total volume of tax-related fraud remains low, Q1 saw the same seasonal spike in **REQUESTS FOR W2 INFORMATION** that we have observed in previous years.

Similarly, threat actors have increased the number of identities they routinely spoof. As organizations train employees to be suspicious of “CEO spoofing,” threat actors are seeking to impersonate other people of authority within the company, resulting in a 36% quarter-over-quarter increase in the average number of spoofed identities in email fraud attacks. Additionally, 57% of targeted companies saw the identities of more than five employees spoofed, an increase of 10 percentage points over the previous quarter. This suggests that, with freely available information about employees widely accessible and with multiple types of assets to target, email fraud actors are getting more creative and finding new ways to unlock the target organization. Figure 7 shows the upward trend of both spoofed identities and targeted individuals since Q3 2016.

### DISPLAY-NAME SPOOFING

The display name is what appears in the "From:" field when reading the message. It is unrelated to the sender's actual email address or where any replies are sent—it can be anything. In display-name spoofing, the attacker uses a familiar name and email address to gain the recipient's trust.

### DOMAIN SPOOFING

Spoofing impersonates trusted colleagues or contacts by making an attacker's emails appear to come from a legitimate and expected address. Some domain spoofing uses lookalike domain names deceptively similar to the real ones.

### WHY WE TRACK THIS

Web-based attacks remain a major threat vector. Studying attack techniques helps identify vulnerabilities that are being exploited and new social-engineering schemes that could trick people into installing malware.

### EXPLOIT KITS (EKs)

Exploit kits (EKs) run on the web, detecting and exploiting vulnerabilities in computers that connect to it. EKs, often sold to attackers as a service, make it easy to infect PCs in "drive-by" malware downloads.

### Identities Spoofed and People Targeted Per Average Organization

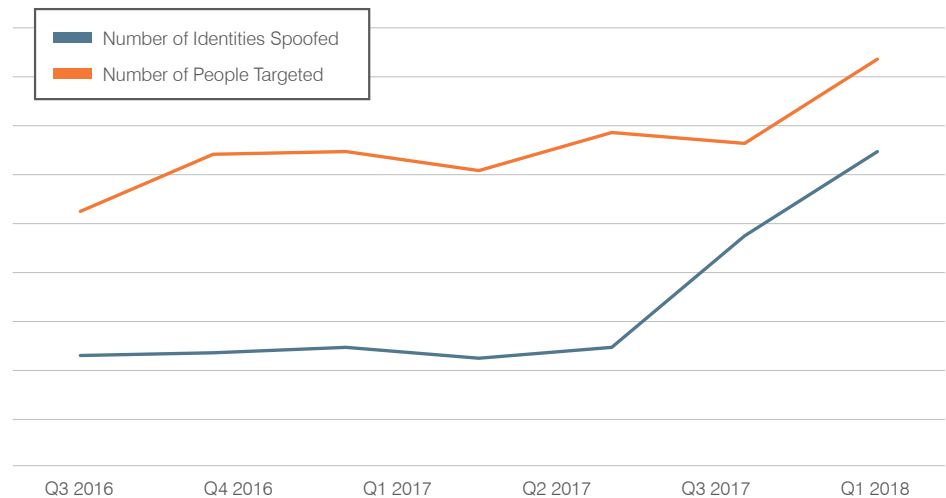


Figure 7: Average number of identities spoofed and individuals targeted per organization

Within these attacks, **DISPLAY-NAME SPOOFING** was the most commonly used fraud tactic, although it was often used in tandem with other approaches. In Q1, over 98% of all impostor email attacks used this tactic. Webmail domains, such as gmail.com and aol.com, were the most common sending domains observed, accounting for 53% of these attacks. Display-name spoofing attacks sent from webmail addresses accounted for 40% of all email fraud in Q1.

**DOMAIN SPOOFING**, in which an attacker hijacks an organization's trusted domain, accounted for about 27% of all email fraud attacks, and 70% of the organizations that were targeted by email fraud in Q1 saw at least one domain spoofing attack. Of the sending domain types used last quarter, more than a fourth of impostor emails came from the same domain used by the primary target. These are the cases in which an attacker spoofs a trusted identity within an organization to target someone from that same organization.

## WEB-BASED THREATS: EXPLOIT KITS CONTINUE THEIR DECLINE AS NEW THREATS EMERGE

**Key stat: Roughly 95% of web-based attacks now redirect into social engineering schemes instead of exploit kits.**

Through early 2016, **EXPLOIT KITS (EKs)** were a major vector for web-based malware infections, powering drive-by downloads, malvertising, and more at massive scale. Since the well-documented demise of the Angler EK, however, EK traffic has steadily declined, even as smaller exploit kit players vied for remaining market share. Threat actors have instead turned to social engineering schemes, network propagation, social media, and doubled down on email distribution to spread malware and conduct phishing operations.

Social engineering schemes rely on users encountering pop-ups and modal dialogs prompting them to install bogus software updates, fake antivirus, or special "font packs." Instead of requiring active exploits that have increasingly short shelf lives, these schemes trick users into installing malware themselves. As many as 95% of web-based attacks now redirect users to social engineering templates rather than EKs. Figure 8 shows recent samples of events and associated infrastructure in such



### Exploit Kit Activity—Samples Collected Q1 2018

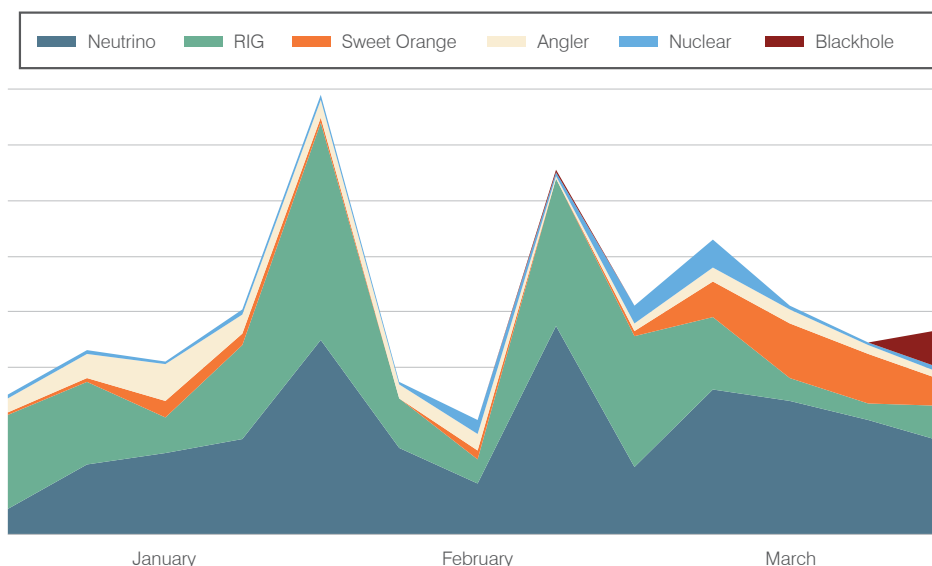


Figure 9: Relative activity for top exploit kits, Q1 2018

We also observed new infrastructure supporting a variety of web-based attacks. **BlackTDS**, a so-called “drive-by as a service,” is a new traffic distribution system used in a growing number of web-based schemes as well as in malicious email campaigns. In the latter case, URLs in emails take recipients to landing pages from which BlackTDS can redirect to the pages or malware payloads of the threat actor’s choosing.

We also discovered a new Fast Flux infrastructure, dubbed **Sandiflux**, used to spread malware and conceal malicious activity on the web, notably GandCrab ransomware.

Finally, in Q1 our researchers were instrumental in **taking down EITest**, one of the oldest and longest running infection chains used to drive traffic to EKs and social engineering schemes. At the time of the sinkholing operation, EITest was responsible for as many as two million redirects a day into malicious sites and infrastructure.

#### WHY WE TRACK THIS

Organizations are engaging customers in new digital channels they do not control, which are fertile ground for threat actors looking to cash in on trusted brands.

#### 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.

## SOCIAL MEDIA THREATS: ANGLER PHISHING ANGLES UP

**Key stat: Observed instances of social media support fraud, or “angler phishing,” exploded in Q1 2018, increasing more than 200% from the previous quarter.**

Social media threats continue to evolve as threat actors look to social platforms for personal information, malware distribution, and more. While common link spam on social media showed some seasonal variations even as the platforms themselves looked to automated solutions to address the problem, more sophisticated social media support fraud, also known as “**ANGLER PHISHING**” exploded, increasing 200% quarter over quarter (Figure 10).

**SOME 84% OF FORTUNE 500 CEOs WERE VICTIMS OF THREATS AND HATE SPEECH ON TWITTER AND THE DARK WEB IN FEBRUARY 2018.**

**Indexed Number of Support Fraud Accounts Observed**



**Figure 10: Indexed monthly volume of observed fraudulent support accounts**

Social media support fraud occurs when threat actors insert themselves into a conversation between a legitimate brand and a consumer seeking help with a particular issue, ranging from account login to product support. Since Q1 2017, we have observed a more than fivefold increase in this type of attack, which is much more difficult for social platforms to address in an automated fashion than standard link spam.

At the same time, social media is a breeding ground for a variety of hate speech and threats against organizations and their staff. Some 84% of Fortune 500 CEOs were victims of threats and hate speech on Twitter and the dark web in February 2018.

### DEFENSIVE REGISTRATIONS

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.


Suspicious domains—used in attacks over social media, the web, and email—are also proliferating rapidly. As with many social media scams, threat actors follow major trends and register domains for nefarious uses accordingly. For example, 30% of Bitcoin-related domain registrations in Q1 were suspicious, but new registrations fell off sharply as the value of Bitcoin continued to fall through Q1. As Bitcoin values climb back up from Q1 lows, we expect to see additional suspicious registrations. Aside from Bitcoin, we continue to observe suspicious domain registrations outnumbering brand-owned **DEFENSIVE REGISTRATIONS** by roughly 20 to 1, emphasizing the importance of strategic domain management.

## 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 attacks often have no payload at all and are thus difficult to detect. Preventing email fraud requires a multilayered solution that includes email authentication and domain discovery, as well as dynamic classification that can analyze the content and context of emails, stopping display-name and lookalike-domain spoofing at the email gateway.
- **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.





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

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.