REPORT

proofpoint.

QUARTERLY THREAT REPORT

Q1 2017

proofpoint.com

The *Proofpoint Quarterly Threat Report* captures threats, trends and transformations we see within our customer base and in the wider security market. Each 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 from advanced threats. That gives us a unique vantage point from which see data and trends outside across the entire threat landscape.

Analyzing how these threats shift quarter over quarter helps identify larger trends and equip organizations with actionable intelligence and advice for managing their security posture. We continue to see sophisticated threats across three primary vectors: email, social media, and mobile.

TABLE OF CONTENTS

Key Takeaways: Back to the Future 4

Email 4

Web-Based Attacks, including Exploit Kits 4

Mobile 5

Social Media 5

Recommendations 5

Email-based Threat Trends 6

Banking Trojans: Vawtrak out, ZLoader in, and Dridex Back with a Vengeance 8

Ransomware: Getting Targeted 8

Business Email Compromise (BEC) Attacks are not Going Away 10

Web-based Threats Embrace Social Engineering 11

Social Media 13

Mobile Apps 13

Proofpoint Recommendations 14

KEY TAKEAWAYS: BACK TO THE FUTURE

In the first quarter of 2017, Locky ransomware failed to re-emerge in large volumes after an expected holiday break. But threat actors appeared to double down on smaller, more targeted campaigns with banking Trojans and information stealers. At the same time, mobile and social threats continued to evolve, drawing more people to phishing pages and malicious software.

Whether through email, social media, or mobile apps, threats in the first quarter were marked more by their diversity than by their volume. A wide variety of ransomware circulated in the wild. Web-based attacks added social engineering elements. Email-based attacks featured a mix of malicious URLs and attachments—a change from massive campaigns in 2016 that used attachments alone. And **BUSINESS EMAIL COMPROMISE (BEC)** actors continued to hone their techniques.

Here are key takeaways from the quarter.

EMAIL

- **The quarter ended with large-scale attack campaigns distributing Dridex; however high-volume Locky campaigns did not return.** The first quarter ended with two days of multimillion-message Dridex campaigns, the largest malware campaigns since December. The spike followed an apparent disruption for most of the quarter in the Necurs botnet. Necurs is widely believed to be the sending infrastructure behind large Dridex campaigns in 2015 and 2016 and massive Locky campaigns in 2016.

- **URL and hybrid campaigns that used URL and attachments together re-emerged.** Campaigns that used malicious URLs regularly accounted for 60% to 70% of total malicious message volume.

- **More than four times as many new ransomware variants appeared in Q1 2017 than in the year-ago quarter.** Even without Locky, ransomware remained a serious and widespread threat. New variants emerged daily. Ransomware was the primary payload in 22% of malicious email campaigns.

- **BEC attack types continued to evolve.** Reply-to and display name spoofing remained the dominant techniques in Q1, but BEC actors moved still closer to an even split between the two approaches. Reply-to spoofing decreased by 6 percentage points from Q4 2016 to 56% of total BEC attacks. Display name spoofing increased 7% to 43% of total BEC.

- **Credential phishing is alive and well.** Conventional credential phishing continues at high volumes, with malicious URLs increasingly leading to phishing pages rather than exploit kits.

- **Banking Trojans were a payload in 33% of all malicious emails.** With the near-disappearance of Locky, banking Trojans were often distributed in both smaller, personalized or targeted campaigns as well as larger "spray and pray" campaigns.

EXPLOIT KITS AND WEB-BASED ATTACKS

- **Exploit kit activity remained relatively low, at roughly 10% of the levels detected in Q1 2016.** **EXPLOIT KIT** traffic has never rebounded from its peak in Q1 2016, but **MALVERTISING** activity remains widespread. The trend is especially pronounced in Asia, where pirated software creates a larger pool of vulnerable PCs.

- **Attackers are beginning to use social engineering in web-based attacks.** We observed social engineering attacks in the **EITEST** infection chain and **MAGNITUDE EK**, suggesting that attackers are finding new ways to leverage the technology, even as new browser and operating system vulnerabilities have become harder to exploit.

BUSINESS EMAIL COMPROMISE (BEC)
In BEC attacks, an email purporting to come from a top executive asks the recipient to wire money or send sensitive information. BEC doesn't use attachments or URLs, so it can be hard to detect and stop.

EXPLOIT KITS
Exploit kits (EKs) run on the web, detecting and exploiting vulnerabilities in computers that visit pages where the EK has been installed. EKs, often sold to attackers as a service, make it easy to infect PCs in "drive-by" malware downloads.

MALVERTISING
Malvertising, short for malicious advertising, embeds malicious code into online display ads. These ads often appear on legitimate, widely trusted websites, making them hard to block with web controls.

EITEST
EITest is an infection chain, or chain of actions that constitutes a malware delivery technique, that redirects users browsing compromised websites to an exploit kit to infect PCs.

MAGNITUDE EK
Magnitude is one of the oldest and most widely used exploit kits in active development. It's used mostly in attacks in Asia.

MOBILE

- **Nearly 16,000 publishers offered malicious apps through both vendor-sanctioned and third-party app stores.** This represents over 1% of worldwide app developers, many of whom published malware that masqueraded as legitimate apps.

- **SMS phishing bypasses traditional security measures.** Threat actors continued to refine their approaches to this type of attack. They used stolen branding and multiple vectors including URLs and multi-step phishing sites for attacks that bypass many security products.

SOCIAL MEDIA

- **Social media support phishing increased by 167% over Q2 2016.** So-called "**ANGLER PHISHING**" decreased from the previous quarter. But it continues to show an overall upward trend since we began tracking this threat last year.

- **Distribution of phishing links through social media decreased by 20% since Q2 2016.** URL-based phishing continues to decline as attackers' methods in social channels evolve further while they explore multichannel attacks and new means of brand fraud.

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.

RECOMMENDATIONS

- **Be aware of increasingly sophisticated social engineering approaches in both email and web-based threats.** Adopt solutions that identify and quarantine both inbound and outbound email threats including BEC and provide access to best-of-breed threat intelligence.

- **Deploy solutions that address a range of social media threats.** The social media threat landscape continues to shift rapidly and solutions that protect both brands and their customers are critical.

- **Create environments that are safe for mobile users.** Mobile threats are varied and evolving rapidly and solutions must address a range of attack vectors, closely integrated with MDM platforms.

EMAIL-BASED THREAT TRENDS

Key stat: URL-based campaigns now make up 60-70% of total daily malicious message volume

Compared to 2016, malicious message traffic volume was dramatically lower, due largely to the absence of massive **DRIDEX** and **LOCKY** campaigns observed last year. Threat actors took a more balanced approach to their email campaigns, spreading malware through URLs, attached documents, and attached archives (such as compressed JavaScript files). The quarter ended with a bang, though, thanks to several very large Dridex campaigns in the last two days of March.

DRIDEX
Dridex is a popular banking Trojan that uses malicious macros in Microsoft Office to infect victims and steal banking credentials.

LOCKY
Locky is the top strain of ransomware, which encrypts victims' data and holds it "hostage" until the victim pays to get it back. For most of 2016, Locky had accounted for a surge in malicious email traffic.

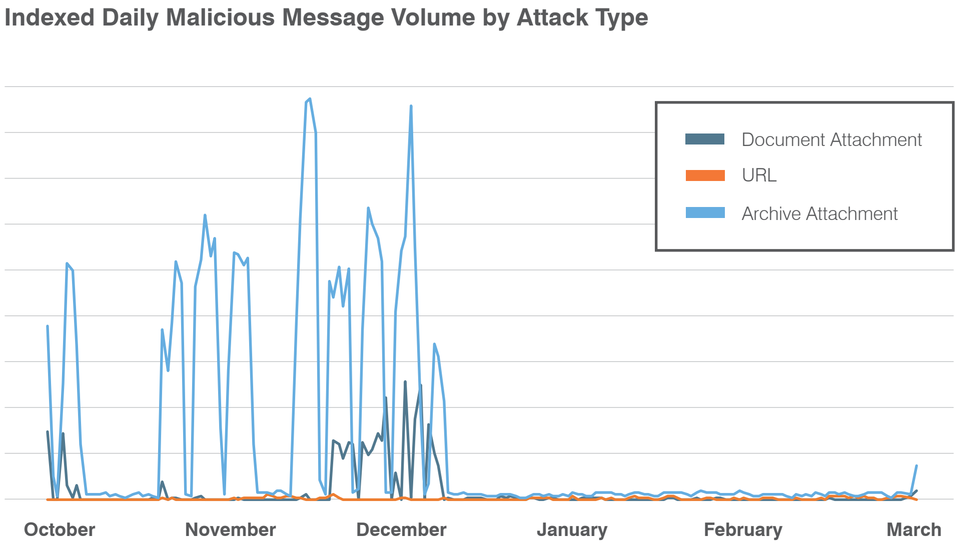

Figure 1: Indexed attack type trend, October 2016 through March 31, 2017 (180 Days)

Looking at traffic since January 1, 2017, allows us to remove the distorting effect of the absent high-volume Locky campaigns and observe the new patterns in email threats. One of those trends was an end-of-quarter spike in Dridex distribution (see Figure 2).

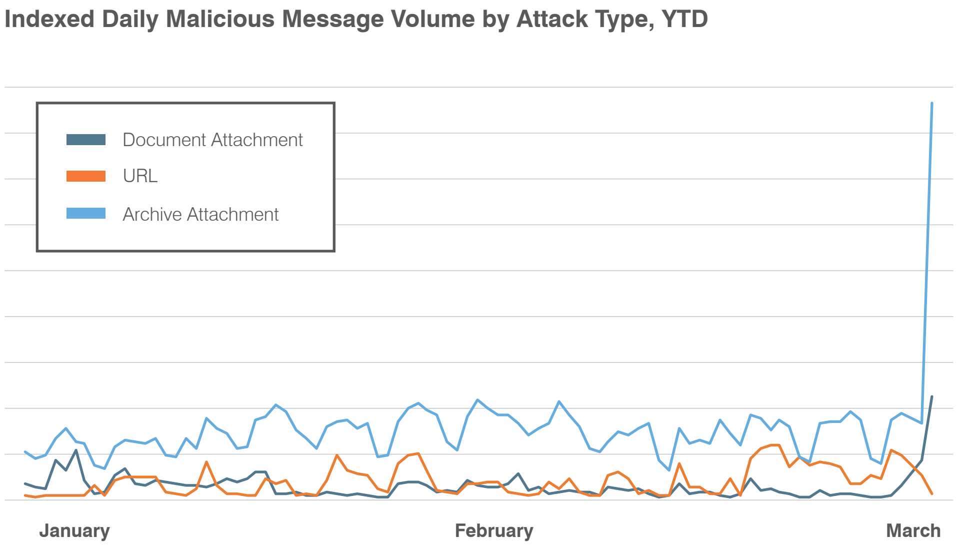

Figure 2: Indexed attack type trend, January 2017 through March 31, 2017 (90 Days)

URL-based campaigns have predominated since January. Malicious URL messages made up 60-70% of total malicious message volume observed by our Targeted Attack Protection (TAP) sensors on a typical day. That held true even as daily volumes fluctuated and higher proportions of unique URLs appeared in these campaigns. At the same time, we continue to see a strong mix of techniques, including:

- **URLs linking to malicious documents or compressed JavaScript files** hosted on compromised servers, Google Drive folders, and SharePoint. In February more of these attacks used Dropbox, the SendGrid email service, and Streamcast video service.
- **Malicious document attachments with macros or embedded scripts.** Many now run **POWERSHELL** commands to execute the download and installation of the payload.
- **Password-protected document attachments.** These were rare during late January and most of February, but became much more common again late in February.
- **Compressed JavaScript attachments** and other scripting and executable attachments.
- **Document attachments with embedded Microsoft Office exploits.** Of these, one that exploits a nearly 6-year-old patched vulnerability in Microsoft Windows common controls (CVE-2012-0158) remains among the most widely used.

POWERSHELL

PowerShell is a scripting tool built in to Windows. It gives users—or attackers—control over many system commands. PowerShell is part of the OS, so attacks that use it are hard to detect.

The disappearance of high-volume campaigns distributing Locky was widely ascribed to issues with the Necurs botnet, the infrastructure believed to have powered the campaigns. But just before the end of March, we observed multiple very large campaigns by the attackers behind earlier Dridex and Locky campaigns. In these attacks, they distributed newer Dridex botnet IDs (7200 and 7500) using multiple attachment types to drop the malware payloads. Whether these high-volume campaigns will continue is unclear. But their use of Dridex instead of Locky as the main payload represents a return to their roots.

Ransomware vs. Banking Trojans vs. Other Malware

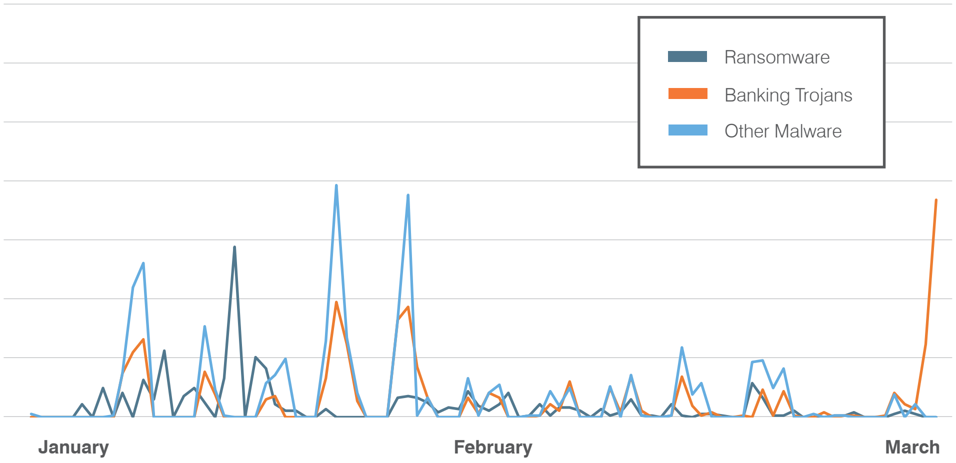

Figure 3: Indexed daily message volumes by top malware categories, January-March 2017

BANKING TROJANS: VAWTRAK OUT, ZLOADER IN, AND DRIDEX BACK WITH A VENGEANCE

Key stat: Banking Trojans appeared in 33% of all Q1 malicious attachment email campaigns, up from 25% in 2016.

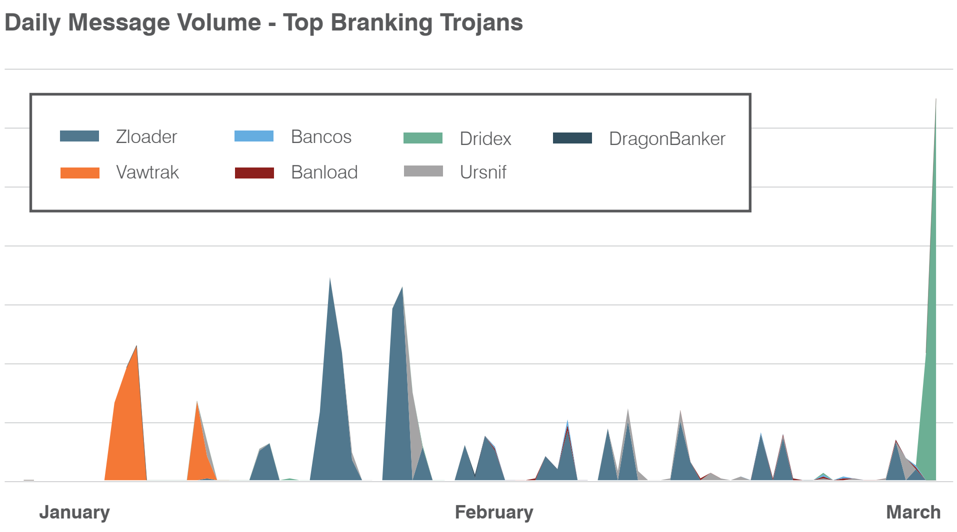
Daily Message Volume - Top Branking Trojans

Figure 4: Indexed daily message volumes for top banking Trojan strains, January-March 2017

VAWTRAK
VAWTRAK is popular banking Trojan that has used malicious Office macros and Windows PowerShell to infect victims and evade detection by security tools.

ZLOADER
Zloader, a banking Trojan also known as DELoader and Terdot.A, is a variant of Zeus.

One of the most visible changes from January to February was the disappearance of **VAWTRAK** and the rapid rise of **ZLOADER.** This is most likely attributable to the January 13 arrest in Spain of a malware developer alleged to be central to the Vawtrak banking Trojan (also known as NeverQuest or Snifula).

We observed the last campaign distributing Vawtrak on January 19. Within a few days, the threat actor alternately known as TA511, MAN1, and Moskalvzapoe switched to Zloader.

Zloader continues to drop with the Tordal (or Hancitor) downloader and Pony information stealer. This combination makes the campaigns a potent "triple threat" that should be on the radar of any organization with offices or employees in the U.S.

The Ursnif banking Trojan also continued to spread using a wide variety of techniques and cleverly integrated social engineering. Actors distributing Ursnif primarily targeted English-speaking victims and customers of banks in the U.S., U.K., Canada, and Australia.

TRICKBOT
Trickbot is a banking Trojan closely related to Drye, whose operators were arrested in 2015 by Russian authorities.

Meanwhile, **TRICKBOT** variant The Trick maintained its new, wider geographic targeting. It had appeared almost exclusively in Australia for most of 2016. But late last year it began to show up in campaigns targeting customers of banks and other payment services in the U.S., Canada, U.K., and parts of Europe. This trend continued in the first quarter.

RANSOMWARE: GETTING TARGETED

Key Stat: Ransomware was the primary payload in 22% of Q1 malicious email campaigns.

Ransomware campaigns of 2016 were generally regarded as non-targeted: like ad-fraud campaigns, they sent messages in high volumes to as many industries and organizations as possible. Locky was the best example of this, but we observed similar behavior in campaigns distributing Cerber and other ransomware families.

The changes and variety in banking Trojan activity have been complemented by continued growth in the ransomware space. None of the top 10 ransomware variants we tracked this quarter approached the distribution volumes associated with Locky ransomware in 2016. But distribution of multiple ransomware strains in moderate-volume campaigns continued almost daily.

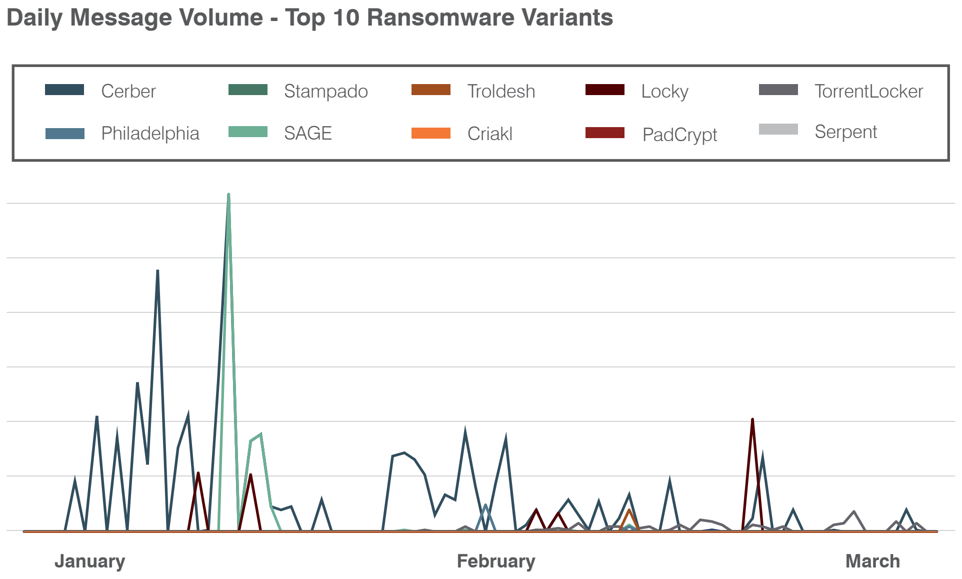

Figure 5: Indexed daily message volume of top ransomware strains, January-March 2017

As we have observed for a year now, new ransomware strains continues to multiply. We saw 4.3 times as many new ransomware variants emerge in Q1 2017 as we did in the year-ago quarter.

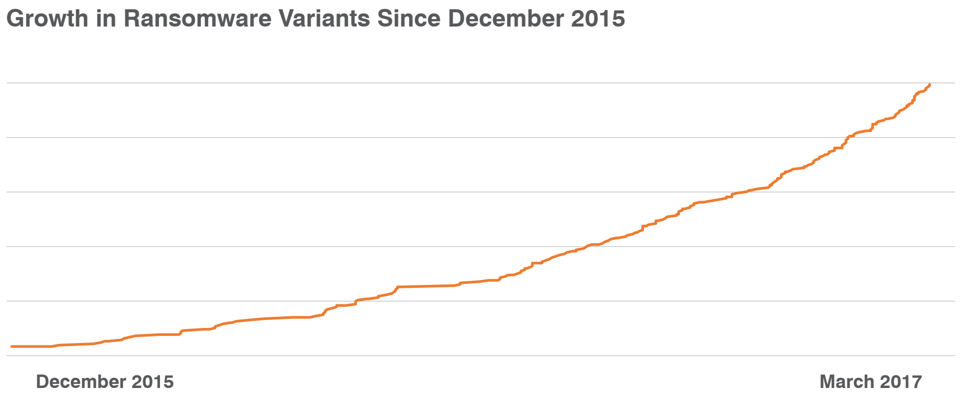

Figure 6: Indexed growth in total number of observed ransomware strains, December 2015-March 2017

Other Locky **AFFILIATE IDS** (such as 5 and 23) remain active, albeit in lower-volume campaigns. At the same time, new versions of ransomware continued to appear in February. They included Philadelphia and Serpent, the latter still limited to campaigns with narrow geographic targeting.

AFFILIATE IDS

Malware authors often pay affiliates to spread their malware. The affiliate ID is hardcoded into versions of the malware to ensure that the right people get credit for the infection.

We also saw a change and increase in campaigns distributing TorrentLocker ransomware: geographically targeted TorrentLocker campaigns have been occurring since at least late 2015, but typically erratically on only a handful of days each month. But in February and March, TorrentLocker campaigns occurred almost daily and used a wider variety of infection techniques, including HTML, Word and Excel attachments, and Dropbox links.

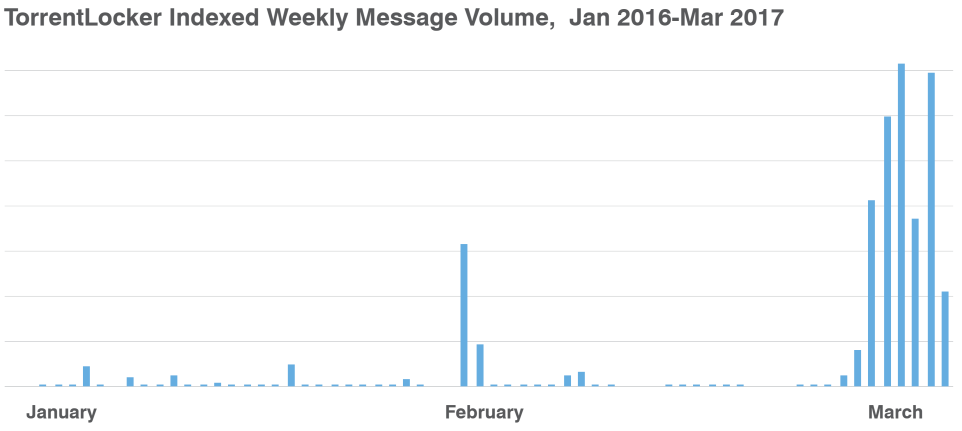

Figure 7: TorrentLocker indexed weekly message volume, 15 months to March 31, 2017

TorrentLocker is not the only example of this trend. We also observed campaigns distributing Serpent targeting Belgium and the Netherlands on separate days. And very narrow Philadelphia campaigns targeted a handful of organizations. In other examples of targeted ransomware campaigns, we observed the use of physical addresses and other personal details in email lures. This suggests that even attackers distributing ransomware, which has spread mostly through wide-net campaigns, are finding value in convincing lures, social engineering, and better targeting to increase click and infection rates.

BUSINESS EMAIL COMPROMISE (BEC) ATTACKS ARE NOT GOING AWAY

Key stat: Simple display name or domain spoofing increased 7% over Q4. The technique was used in 43% of total BEC attacks in the first quarter.

BEC losses continue to grow. As of the end of 2016, the FBI reported a 1,300% increase in "identified exposed losses" and noted that unreported losses could drive figures higher. Reported BEC attacks are now responsible for more than $3 billion in actual and potential losses. The FBI also suggests that the number may be higher because not all BEC gets reported.

We have observed BEC attacks on organizations across verticals and in companies of all sizes. Attacks range from requests for employee W2s to urgent, long-term, multichannel efforts to convince employees to transfer millions of dollars into fraudulent accounts. Attacks are not just increasing in number. Their techniques are also shifting and evolving.

Reply-to and display name **SPOOFING** remained the dominant techniques in Q1, but moved closer to an even split. Reply-to spoofing fell by 6 percentage points from Q4 2016 to 56% of total BEC attacks. Display name spoofing rose 7% to 43% of total BEC. Display name spoofing is easy to carry out—attackers simply change the name shown on most email clients. Its effectiveness gives BEC actors little incentive to use more complex techniques.

SPOOFING

Spoofing impersonates trusted colleagues by using their name in the "from" field seen by the recipient. But the "reply-to" address—where any replies are actually sent—belongs to the attacker.

Spoofing types observed in Q1

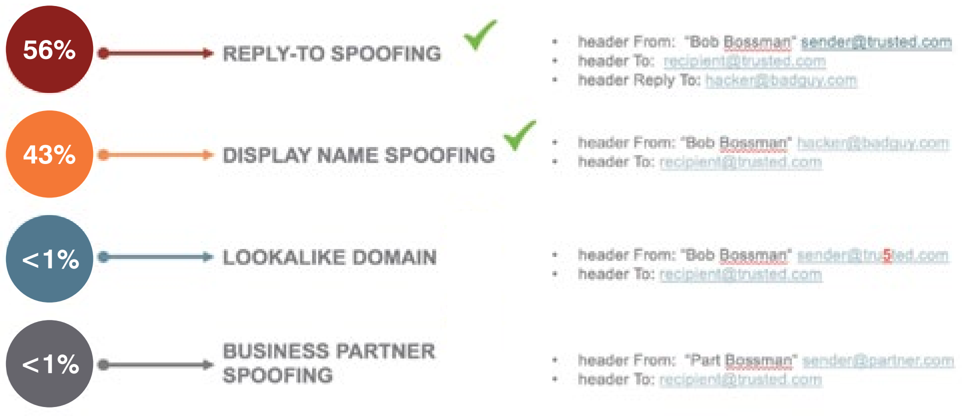
56%
REPLY-TO SPOOFING
✓
• header From: "Bob Bossman" sender@trusted.com
• header To: recipient@trusted.com
• header Reply To: hacker@badguy.com
43%
DISPLAY NAME SPOOFING
✓
• header From: "Bob Bossman" hacker@badguy.com
• header To: recipient@trusted.com
<1%
LOOKALIKE DOMAIN
• header From: "Bob Bossman" sender@tru5ted.com
• header To: recipient@trusted.com
<1%
BUSINESS PARTNER SPOOFING
• header From: "Part Bossman" sender@partner.com
• header To: recipient@trusted.com

Figure 8: Additional insights into the nature of BEC attacks and the underlying spoofing techniques we observed in Q1

Organizations continued to respond to increased BEC and advanced phishing threats by adopting Domain-based Message Authentication, Reporting and Conformance (**DMARC**). The email authentication protocol allows them to identify a range of spoofing techniques. DMARC implementation continued to slowly increase in Q1 - 4% quarter-over-quarter. At the same time, the number of organizations implementing more sophisticated policies based on the protocol continued to increase. For example, the number of organizations that rejected emails they received because they violated a DMARC policy grew 9% quarter-over-quarter.

DMARC

DMARC, which stands for "Domain-based Message Authentication, Reporting & Conformance," is an email authentication protocol that can prevent many BEC attacks.

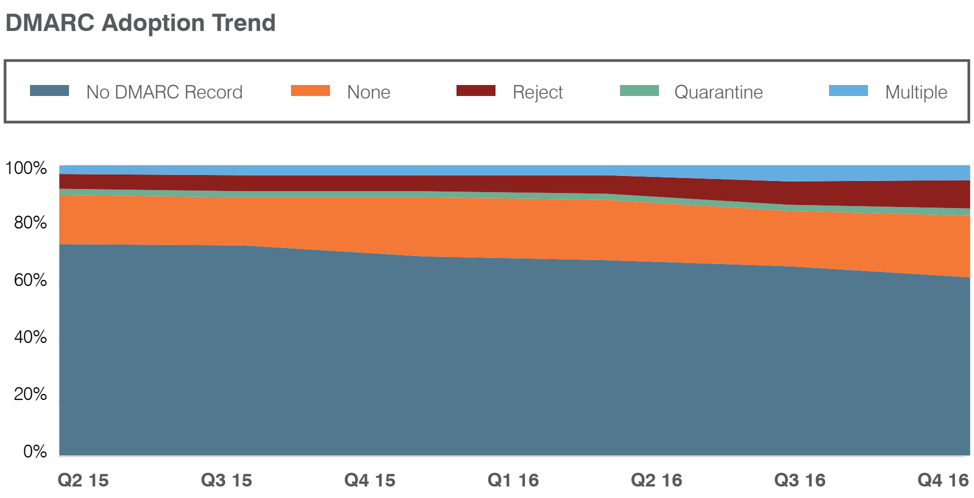

Figure 9: Implementation of DMARC across surveyed organizations.
None = DMARC record present but no active policies, Multiple = More than one active policy

WEB-BASED THREATS EMBRACE SOCIAL ENGINEERING

Key stat: Exploit kit activity remains less than 10% of Q1 2016 levels.

Exploit kit traffic has declined substantially for a variety of reasons. One big reason: finding active, unpatched zero-day vulnerabilities that can be exploited long enough to justify investments in developing the exploits is difficult. Social engineering approaches make active exploits less important. Instead, they exploit users to click, bypass sandboxes, run PowerShell code, and more to infect their own systems on behalf of attackers.

We observed two web-based attacks incorporating social engineering in Q1. The first occurred in EITest, a well-documented infection chain that mostly relies on compromised websites to direct users to exploit kit (EK) landing pages. EITest has been involved in delivering a variety of ransomware, information stealers, and other malware. Evidence points to EITest being used as far back as 2014. Most recently, the infection chain was used to deliver **FLEERCIVET** ad-fraud malware using a socially engineered font-pack download for Chrome users on Windows 10. For targeted users, a script is inserted in the page that rewrites the compromised website on a potential victim's browser. The script makes the page unreadable, creating a fake issue for the user to resolve. They resolve the issue by downloading a supposed Chrome font pack that is, in fact, malicious software. It is installed through user interaction rather than an active exploit.

FLEERCIVET
Fleercivet is a malware Trojan that opens hidden Chrome browser windows to produce fake clicks on web ads and generate revenue.

The second occurred in Magnitude, an established exploit kit that has operated for several years. Since September 2016, the actor behind Magnitude has focused primarily on Asia, almost exclusively distributing Cerber in Korea and Taiwan. Like many EKs, Magnitude is fed by malvertising traffic with pre-filtering redirectors that allow targeting based on geography, user agent, and internet service provider. But in the first quarter of 2016, we observed a new social engineering chain in Magnitude that affects Internet Explorer users on Windows 10.

Targeted web surfers are redirected to a landing page for the social engineering scheme. The page uses code that prevents users from closing or bypassing dialog boxes. Instead, it forces the user to choose options that lead them to eventually download a shortcut containing Windows PowerShell commands, which in turn download and execute Cerber ransomware. Users could choose to shut down Internet Explorer. But the social engineering and software dialogs keep the victim engaged. The attack not only allows execution of code outside the **APPCONTAINER** for Microsoft Edge (launched in an intermediate step) but also prepare users psychologically for familiar download dialogs.

APPCOUNTAINER
AppContainer is a security framework in Windows 8 and above to isolate processes, files, and more on a per-application basis for better security.

The social engineering scheme outlined here lacks the refinement of others we have observed in email distribution. Still, the addition of a social engineering attack chain to a major exploit kit is noteworthy.

Other EKs showed considerable variability. **RIG EK** was dominant throughout the quarter; **SUNDOWN** and **NEUTRINO** were also involved in a variety of malvertising. Magnitude was active but regionally limited as noted above. As social engineering becomes more prevalent in web-based attacks, we will continue to monitor EK activity and the effects of this evolution on the landscape.

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

SUNDOWN
The Sundown EK has grown amid the demise of Angler. It was one of the first to exploit newly revealed vulnerabilities in Microsoft's Edge web browser.

NEUTRINO
The Neutrino EK has become popular in the wake of Angler's demise but its use has dwindled in recent weeks.

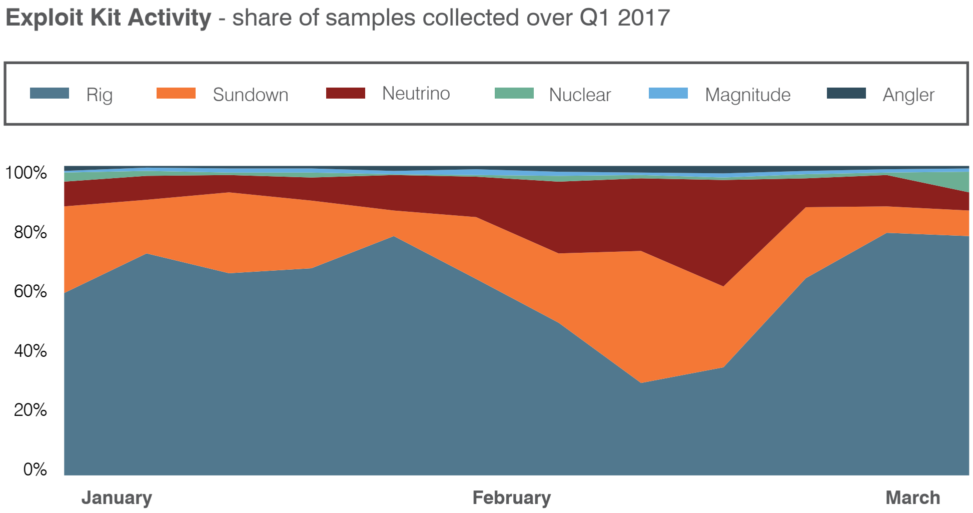
Exploit Kit Activity - share of samples collected over Q1 2017

Figure 10: Top exploit kit traffic as percentage of total, January-March 2017

SOCIAL MEDIA

Key stat: Social media support phishing increased by 167% over Q2 2016.

Social media remains a breeding ground for a variety of threats ranging from malware distribution to phishing. We observed shifting trends in support account or "angler phishing" that bear watching in the coming quarters.

Social media support phishing, also known as angler phishing, increased by 167% over Q2 2016, the first quarter in which we began tracking this threat. Although this type of social phishing decreased sharply from Q4 2016, it continues to show an overall upward trend. The spike in Q4 2016 may reflect seasonal fluctuations or continued tweaking of attack methods by actors in this space.

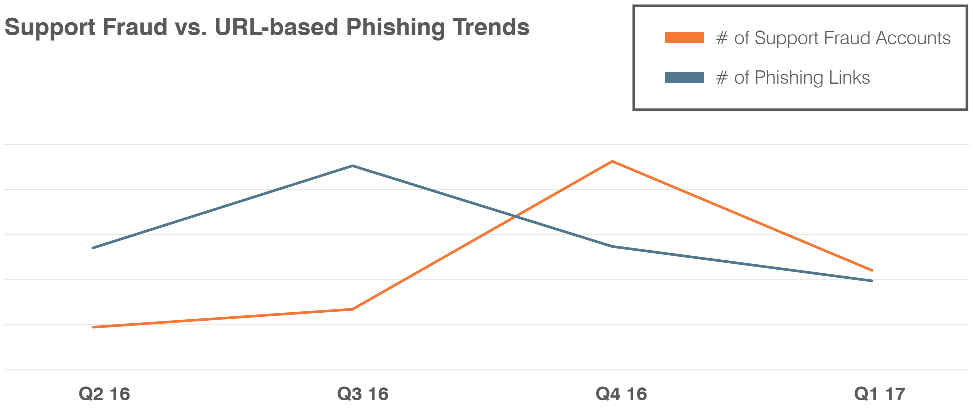

Figure 11: Relative quarterly activity in phishing link distribution via social media vs fraudulent support accounts

On the other hand, distribution of phishing links via social media decreased by 20% since Q2 2016 and by 47% from its peak in Q3. The continued decrease in URL-based phishing again suggests that attackers' methods via social channels continue to evolve.

MOBILE APPS

Key stat: 16,000 mobile app publishers are distributing malware.

Mobile threats continue to range from "leaky apps" that can transmit personal data unsafely or unnecessarily to malicious apps that masquerade as legitimate, useful applications.

We identified malicious apps on both mainstream mobile app stores and third-party app stores around the world. Many of the third-party stores promote **SIDELOADING** of apps. Sideloading is never a best practice, but it is common among those looking for free games or business applications. Increasingly, though, we are observing what appear to be legitimate business apps but are, in fact, information stealers, remote access Trojans (RATs), and other malware designed to steal sensitive information.

SIDELOADING
Sideloading is the practice of installing apps using a downloaded file rather than through a vendor-sanctioned app store.

In one case, we identified a robust information stealer masquerading as a point-of-sale (POS) system controller. Because the app was specialized in its purported function, it was an inherently targeted attack on people with access to credit card and customer data.

Mobile threats go beyond apps that are overtly malicious. A growing percentage of clicks to phishing pages come from mobile apps. And the established practice of SMS phishing continues to evolve. Attackers use stolen branding, social engineering, and links to images that bypass many sandboxes. These practices allow SMS phishers to bypass many network and mobile device management controls while presenting convincing lures for recipients.

PROOFPOINT 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. Deploy 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 BEC defense. Highly-targeted, low volume BEC 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. At the same time, implement authentication to stop supply chain and partner payment fraud.

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.

Lock down mobile app environments. Mobile environments increase the risk of rogue apps that can steal critical corporate information. Invest in a data-driven solution that works with your mobile device management (MDM) to reveal the behavior of apps in your environment, including what data they are accessing.

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

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.

www.proofpoint.com