REPORT

proofpoint.

QUARTERLY THREAT REPORT

Q2 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 analyse more than 1 billion email messages, hundreds of millions of social media posts, and more than 150 million malware samples to protect organisations from advanced threats. That gives us a unique vantage point from which see data and trends outside across the entire threat landscape.

Analysing how these threats shift quarter over quarter helps identify larger trends and equip organisations with actionable intelligence and advice for managing their security posture. We continue to see sophisticated threats across email, the web, social media, and mobile.

TABLE OF CONTENTS

KEY TAKEAWAYS: HIGH-VOLUME CAMPAIGNS RETURN AND RANSOMWARE GOES VIRAL

High-volume attack campaigns returned in the second quarter, stark contrast from the smaller, more targeted attacks we saw in the first quarter. Attackers spread a variety of ransomware and banking Trojans in high volumes. At the same time, email fraud has further evolved. **EXPLOIT KITS (EKS)** and web-based attacks grew more sophisticated. And more attacks used social engineering, especially those carried out through email, EKs, and social media. Like most of today's cyber attacks, they preyed on human nature, not just technical exploits.

Here are key takeaways from the second quarter of 2017.

EXPLOIT KITS
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.

EMAIL

Ransomware accounted for 68% of all malicious messages containing malware.
Ransomware was the big story, but it wasn't just because of the high-profile outbreaks of WannaCry and a new Petya variant. Those strains—which unlike most ransomware, were not spread through email—got the most media attention. But email-based ransomware attacks remain the vector of choice for profit-minded attackers, and they continued to grow.

Q2 malicious message volume soared 250% vs. the previous quarter.
Threat actors known for their high-volume email campaigns were out in full force with new payloads and attack types. Some campaigns even approached the massive scale of record-setting attacks seen in 2016.

Dridex is back.
Thanks to high-volume email campaigns, the venerable banking Trojan accounted for 72% of total malicious messages containing banking Trojans—and almost 15% of malicious messages overall.

"One-to-one" email fraud attacks surged almost 30% from Q1.
Cyber criminals took a more targeted approach to email fraud known as **BUSINESS EMAIL COMPROMISE (BEC)** or "whaling." Meanwhile, 87% of organisations targeted by email fraud experienced at least one attack that spoofed their own domain. This finding further highlights the importance of adopting **DMARC** email authentication. When deployed effectively, authentication can prevent domain spoofing.

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.

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

EXPLOIT KITS AND WEB-BASED ATTACKS

Exploit kit traffic held steady at levels set last year, led by the RIG EK.
The "new normal" of EK activity includes regional targeting and new advances in filtering, targeting, and evading security defenses.

EKs spread disruptive ransomware through malicious web ads.
These so-called "malvertising" campaigns by the AdGholas actor and Astrum EK infected many victims. They also highlighted a dangerous misconception about drive-by malvertising: that ads are harmless unless you click them. On the contrary, you don't need to click on the ad to be infected; merely loading the ad in your web browser is enough. If the machine is vulnerable and targeted, the infection occurs without any user interaction.

SOCIAL MEDIA

Fake social-media support accounts quadrupled vs. Q1.
This increase, and the sheer number of phishing links on social media, show just how much "angler phishing" is thriving.

Attackers are using social engineering to trick users into giving access to their accounts and personal details.
We exposed a Facebook spambot exploit that offered users "likes" if they let a spammer's app access their Facebook account. The scheme highlights how quickly cyber crime is evolving on social media and how well it targets the "human factor"—in this case, people's need for attention—on social media.

EMAIL-BASED THREAT TRENDS

Key stat: Malicious message volume increased 250% over the year-ago quarter.
High-volume email campaigns returned, featuring familiar actors and malware, new threats, and new forms of geo-targeting.

The previous quarter ended with the return of high-volume Dridex banking Trojan campaigns from the threat actor responsible for the large-scale Dridex and Locky campaigns of 2015 and 2016. In April, the same attacker—which we designate as TA505—resumed massive Locky **RANSOMWARE** campaigns.

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

In a shift from the first quarter, these campaigns used email attachments rather than URLs. And they were much larger, driving a 250% jump in overall malicious message volume. Despite this spike, volume was still less than half of year-ago levels. The contrast highlights the truly massive scale and abrupt nose-dive of last year's campaigns. But what the quarter lacked in volume—relative to 2016 peaks, at least—it made up for in diversity. We saw new ransomware strains, new attachment types, and a flowering variety of new malware observed across our customer base.

LOCKY
Locky is the top strain of ransomware. For most of 2016, Locky had accounted for a surge in malicious email traffic.

The **LOCKY** ransomware campaigns weren't as steady as those we saw in November and December. After just three campaigns, the threat actor behind them began using another ransomware strain called Jaff. The attacker stuck with the Necurs botnet to spread Dridex and then Locky. This suggests that as a sending infrastructure, Necurs has returned at least to its mid-2016 capacity, though it is being used for less frequent campaigns.

Message volumes sank in mid-June and remained well below the peaks of late May and early June. The drop-off stemmed most from TA505's smaller—though no less frequent—campaigns.

Indexed Daily Malicious Message Volume by Attack Type, 2017 YTD

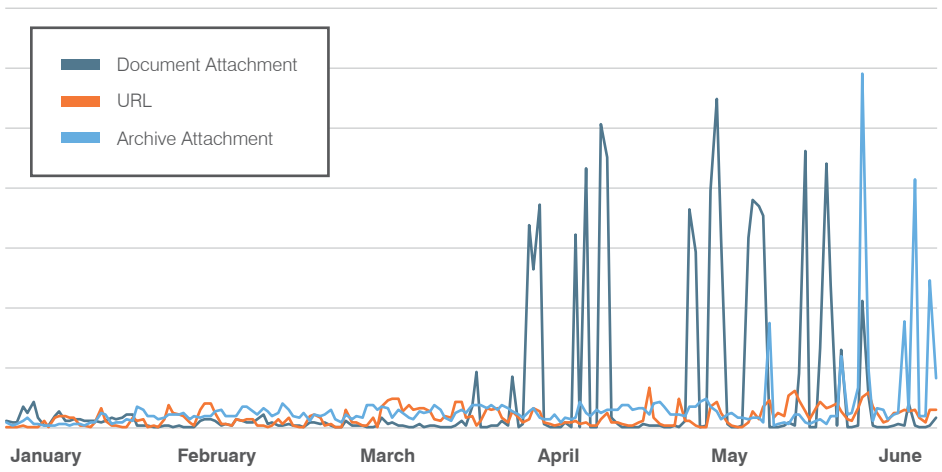

Figure 1: Indexed attack type trend, January 2017 through June 2017 (181 Days)

Malicious attachment messages dominated overall message volume throughout the quarter. But as the period drew to a close, URLs and attachments were reversing course. Malicious URL message volume jumped 57% from May to June, continuing a two-month surge. Over the same period, the average daily volume of malicious attachment messages fell 44% as total malicious attachment messages fell 45%. While most malicious emails still use attachments, malicious URLs remain a clear threat.

The URL resurgence advanced a trend that emerged last fall and gained strength in the first months of the year. At least half of daily malware campaigns rely on malicious URLs, and we also saw daily campaigns that use both URLs and attachments. The large, sporadic spikes attachment campaigns shown in Figure 1 obscure the steadily increasing volume of URL campaigns.

In URL campaigns, attackers often include malicious URLs linked to compressed programming code scripts (usually JavaScript) or to documents embedded malicious macros hosted on legitimate file-sharing services such as SharePoint and Dropbox.

In June, we also saw malicious files hosted on Evernote, a popular notetaking service. Rather than hosting the malware payload on the file-sharing site, where it is likely to be detected, attackers often host it on a separate server; running the script or macro linked in the email messages calls the download of the actual payload from another server. In other cases, malicious URLs simply link to credential-phishing pages instead of malware or intermediate downloaders.

But attachment-based attacks remain overwhelmingly popular. A recent rebound in the use of large-scale compressed script campaigns incldued compressed Windows Script File (WSF) and malicious Office document attachments (alone or embedded in PDFs).

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.

MICROSOFT WORD INTRUDER
As the name implies, this tool targets flaws in Microsoft Word by creating ready-made malicious documents.

Macros that run **POWERSHELL** are the most common attachment type. One trend that stands out from last year is the use of malicious Word-format documents with exploits targeting a vulnerability identified in CVE-2017-0199. As we noted in June, the recent addition of this vulnerability to the **MICROSOFT WORD INTRUDER** document exploit builder shows that threat actors still regard this as one of the more effective exploit opportunities in recent years.

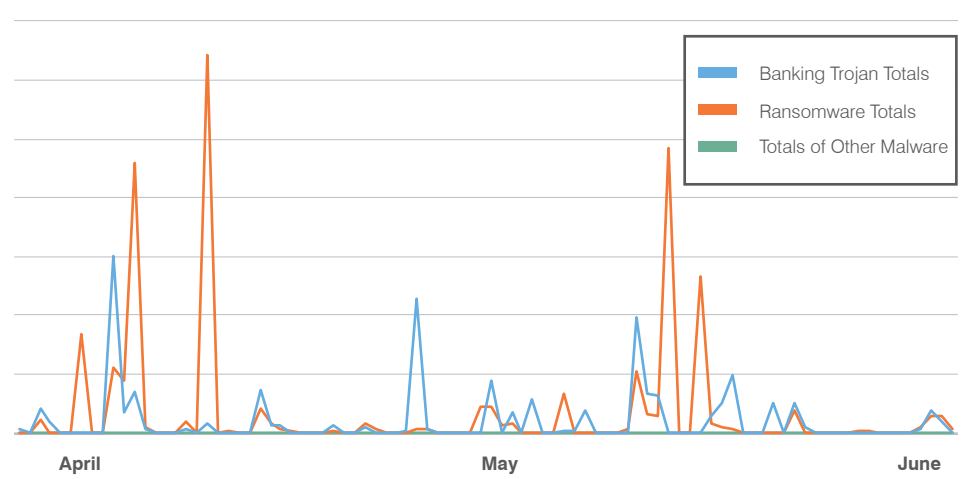

Figure 2: Indexed attack type trend, April 2017 through June 2017 (91 Days)

BANKING TROJANS: VARIETY, VOLUME, AND TARGETING

Key stat: Banking Trojans made up 20% of message volume distributing malware. Messages distributing the Dridex banking Trojan accounted for 76% of overall banking Trojan messages.

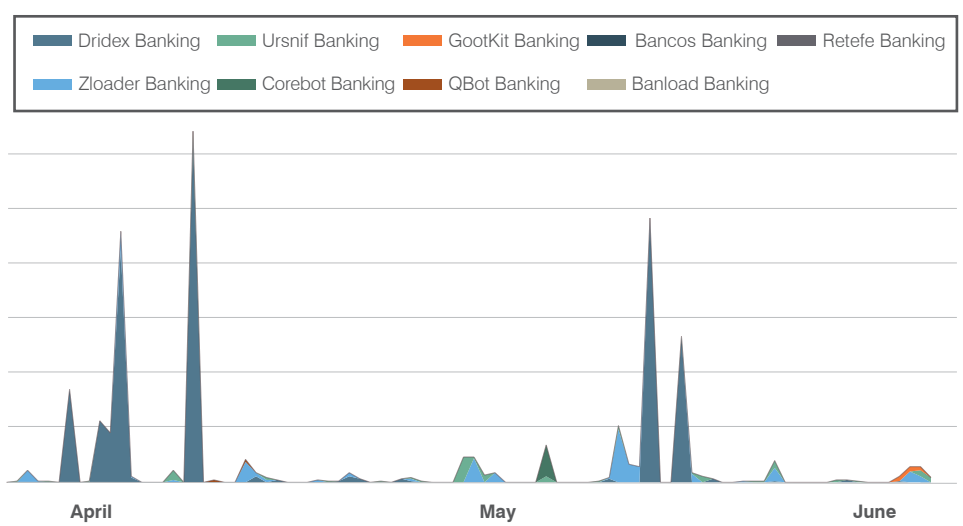

Figure 3: Indexed daily message volumes for top banking Trojan strains, April-June 2017

DRIDEX
Dridex is a popular banking Trojan that is often distributed via malicious macros in Microsoft Office and steals banking credentials among other malicious actions.

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

The return of TA505 in the last days of Q1 marked the start of a surge in **DRIDEX** activity that made it the most distributed banking Trojan of Q2. As Figure 3 shows, this volume was driven by a few mammoth campaigns.

Though they dominated in total message volume, Dridex campaigns were less frequent than those distributing other banking Trojans. Dridex campaigns were active 26 days of the quarter vs. 45 days for those distributing Zloader, 37 for Ursnif and 36 days The Trick (or **TRICKBOT**).

U.S.-targeted Zloader campaigns by a threat actor we identify as TA511 (also known as Man/Dyre) were again the largest non-TA505 campaigns we observed throughout the quarter.

We saw more geographic targeting in these regions:

- Emotet and TorrentLocker (also known as Crypt0Locker) campaigns in the U.S. and Europe—until stopping entirely in mid-May
- Gootkit in France and Italy
- Dridex in the UK and Australia
- A resurgent Nymaim in Poland
- Betabot in Brazil and, interestingly, the U.S.
- The Trick in Australia
- Ursnif in regular campaigns alternately targeting the UK, Canada, Australia, and even Japan

Reinforcing this trend were “geo-fencing” techniques for campaigns. Malicious scripts checked the IP address, system language, and other attributes of the compromised machine. The goal: verify that the machine was in the targeted region—rather than a researcher or other non-target—before downloading the malware payload. We saw this approach from several attackers in campaigns targeting Latin America, Japan, and the UK.

At the same time, we also saw more malware strains being distributed outside of their regional strongholds. For example, Emotet appeared outside of Germany; Betabot outside of Latin America; TorrentLocker outside of Europe; and most notably, The Trick outside of Australia.

The Trick is a banking Trojan that resembles Dyreza in many ways—including network patterns, encoding, web injection, techniques, and overall design. The main threat from The Trick is its ability to intercept and log traffic to banking sites. It is also used to load **AFFILIATE PAYLOADS.**

AFFILIATE PAYLOADS
Malware authors often pay affiliates to spread their malware, usually on a per-infection basis.

Starting in late summer of 2016 and through the first few months of 2017 The Trick appeared mostly in campaigns targeting Australia, with an occasional appearance in Canada and the UK. This changed in Q2. TA505 started distributing it in high-volume, global campaigns that included Europe and North America. In early June message volumes exploded.

TA505 also used a variety of packaging techniques. First, it used a Microsoft Word document with malicious macros embedded in a PDF attachment. Then it shifted to a variety of compressed script attachments. (All of these techniques are hallmarks of TA505.)

As a result, The Trick went from being a regional threat in Australia to a global threat with massive campaign volumes driving an 890% jump in message volume between Q1 and Q2. This development illustrates attackers' ability to quickly pivot to new payloads and bring lesser-known threats onto center stage.

RANSOMWARE: MAYDAY! RANSOMWARE EXPLODES IN MAY WITH JAFF & WANNACRY

Key Stat: Jaff ransomware, which first appeared on May 11, accounted for 72% of malicious messages distributing ransomware.

Ransomware dominated the threat landscape—and news headlines—in May.

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

WORM
This type of computer virus propagates itself through networks rather than through email and other means. They have become rarer as network security has improved. Before WannaCry, the last large-scale worm attack was Conficker in 2009.

But unlike most ransomware, which is distributed through email, **WANNACRY** (also known as Wcry) spread through a network **WORM** that our researchers also analysed in the context of another attack, This incident highlighted how rare these worms have become since the days of Code Red and SQL Slammer (Conficker stands out as another rare exception in the meantime).

WannCry also highlighted the limitations of using worm-based distribution: infections that spread too quickly can outrun the ability of the attacker. They also draw attention to the danger of unpatched vulnerabilities, thus limiting the useful life of the very exploits that are so effective at spreading them.

Email still the preferred vector

Despite the high-profile outbreaks of WannaCry—and one month later, Petya—email remains the preferred vector for attackers focused more on making a profit than upending their victims' business.

Discovered by our researchers on May 11 (the day the WannaCry outbreak began), campaigns by threat actor TA505 distributing Jaff ransomware quickly and quietly eclipsed the largest Dridex and Locky campaigns we had seen this year. By the end of May, Jaff was by far the top malware payload by message volume among our customers around the globe. It accounted for 49% of all malicious messages distributing malware overall, and 72% of ransomware messages.

The campaigns stopped as soon as a decryptor became available in mid-June. But the attacker behind them switched back to Locky and continued distributing The Trick. This quick pivot underscores how easily attackers can adjust to changing conditions and defenses.

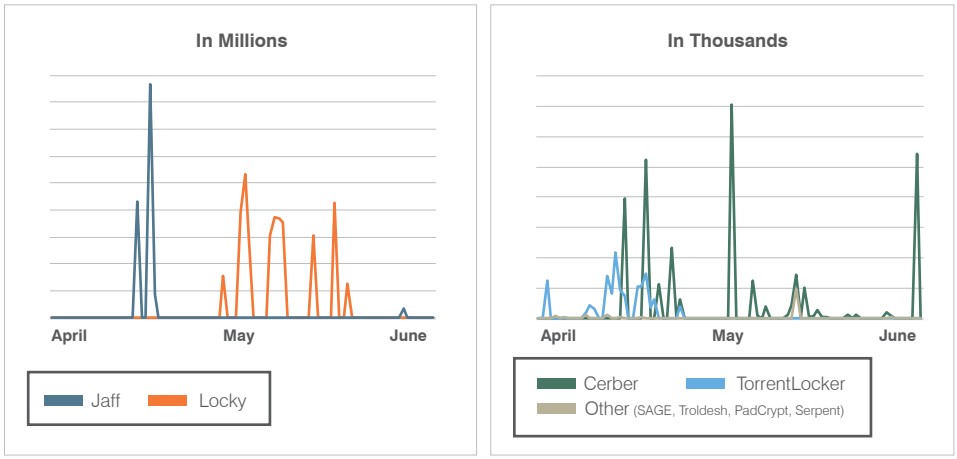

Figure 4: Indexed daily message volume of top ransomware strains, April-June 2017

Ransomware gets more targeted

Jaff and Locky have been indiscriminate in their targeting. But we continue to see many other ransomware strains opting for smaller, more targeted distribution. They range from broader regional targeting of Cerber (within the U.S.) and TorrentLocker (generally regions of Europe) to the narrower targeting of Serpent (Belgium and Netherlands) and Philadelphia (smaller U.S. regions). We even observed hyper-targeting in strains such as XData and "new **PETYA**" (Ukraine).

PETYA
Petya is a ransomware strain that works by encrypting a computer's Master Boot Record rather than individual files. A variant of Petya with an added worm component was used in the widespread WannaCry outbreak.

Of these ransomware strains, Philadelphia was one of the most targeted, with campaigns focused on specific metropolitan regions. Email lures, document attachments, and even ransom messages and amounts were tailored to the specific organisations being targeted.

In this regard, email-distributed ransomware is following a pattern we noted last year among banking Trojans: large, indiscriminate campaigns and smaller, targeted ones. This bifurcation seems likely to continue at least as long as ransomware remains profitable.

Overall, ransomware was the top malware payload in Q2 (Figure 5). It accounted for up to 68% of malicious messages with malware.

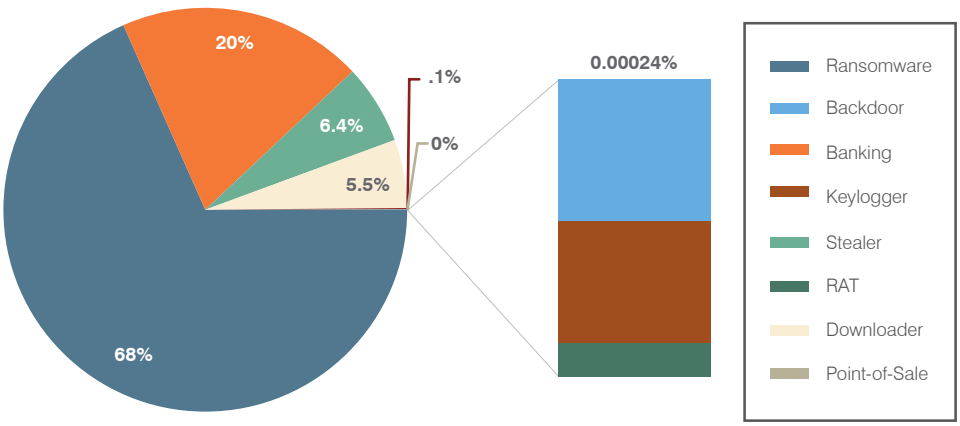

Figure 5: Comparison of quarterly overall message volume

New ransomware strains are multiplying quickly; almost five times as many new ransomware variants appeared vs. the year-ago quarter.

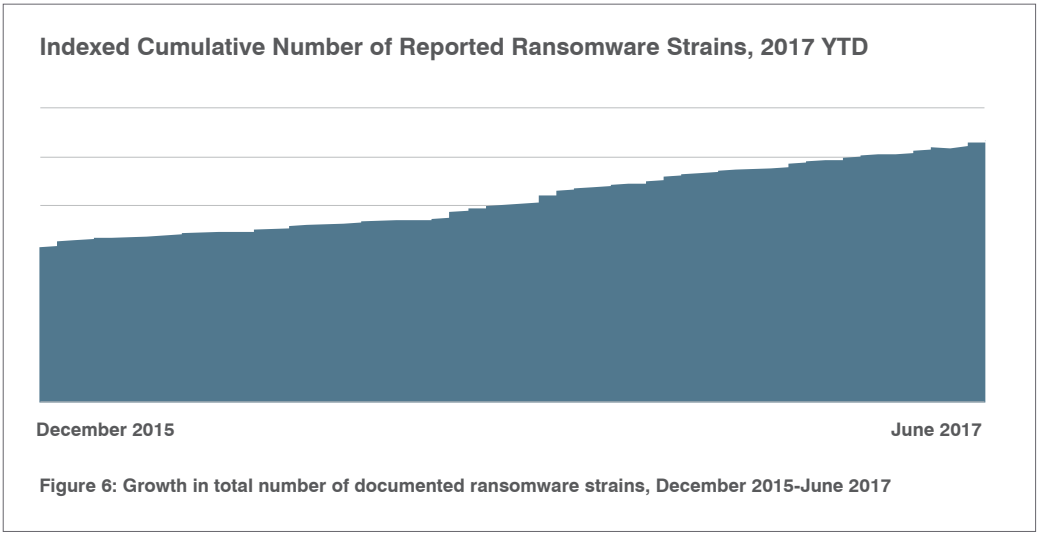

Figure 6: Growth in total number of documented ransomware strains, December 2015-June 2017

In addition to Jaff, we saw new ransomware strains such as Karo (also known as KaroCrypt) emerge. Even as some strains of ransomware have fallen out of use, total ransomware activity remains strong.

Enter the 'ransomworm'

At the same time, ransomware has moved beyond the profit motive. Outbreaks of WannaCry in May and a new Petya variant in June were highly disruptive. Unlike most ransomware, which spreads through email and the web, this pair of attacks borrowed the automated techniques of computer worms to spread within and between vulnerable networks at lightning speed.

These so-called "ransomworms" infected systems faster than the ransomware authors would have been able to collect and process ransom payments and unlock victims' files. In these cases, the focus may have been pure disruption rather than the ransom money. It is too early to say whether attackers' payment infrastructure simply has not caught up with their ability to spread ransomware—or whether ransomworms represent a new, destructive attack.

EMAIL FRAUD GETS FOCUSED

Key stat: 87% of organisations targeted with email fraud messages such as BEC saw at least one attack that spoofed their own domain.

Through the end of 2016, the FBI reported total BEC-related losses of over $5 billion. Our own data suggest that email fraudsters are refining their techniques and targeting businesses more deliberately. In a break from past quarters, we are beginning to see a moderate correlation between company size and the likelihood of an email fraud attempt.

Industry targeting

Our researchers and fraud detection systems continue to observe email fraud across all industries. But as we have noted before, some appear to be disproportionately targeted.

Technology firms and companies with more complex supply chains (such as manufacturing) are targeted more often. And in most industries, email fraud remains close to mid-2016 levels, bucking expectations of spikes around the winter holidays and spring U.S. tax season. Email fraud attempts were actually higher in Q2 vs. a year ago in technology, telecommunications, automotive, and education.

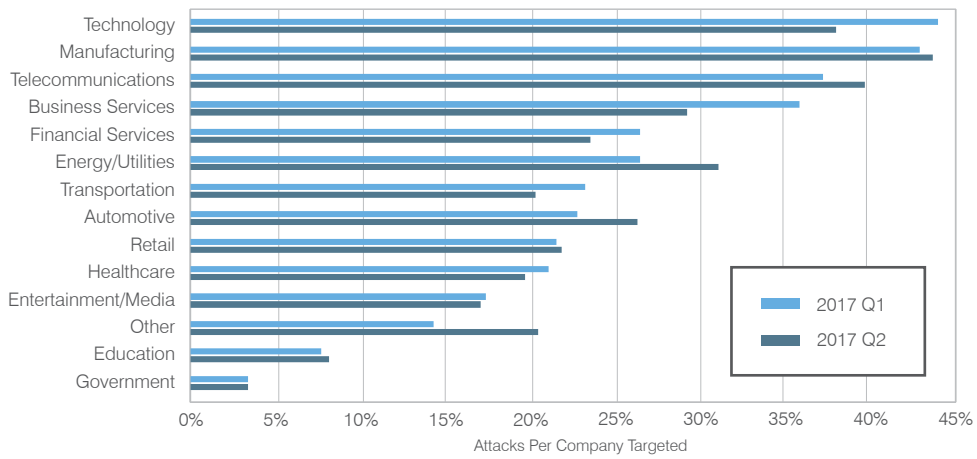

Figure 7: Average number of BEC attacks per company, by targeted industry, Q1 vs Q2 2017

Individual targeting grows more refined

Over the previous three quarters, the number of people receiving fraudulent email at targeted organisations grew steadily. In Q2, the number leveled off at just over 12 people per company per attack. But the number fluctuated by industry between Q1 and Q2, as Figure 7 shows.

This trend reflects differences between quarters in whom fraudsters spoofed and targeted (Figure 8)—specifically, a clear increase in one-to-one attacks in the most recent quarter. (A one-to-one attack refers to email fraud in which a single executive's identity is spoofed in an email sent to a single employee.)

One-to-some attacks, in which a single executive is spoofed in an email sent to multiple employees, also increased over the last quarter, although not as dramatically. Broadly distributed email fraud (some-to-many and many-to-many) fell slightly from the prior quarter.

We saw a moderate correlation between the size of a company and how often it was targeted. Email fraudsters are likely starting to widen their net to more companies—but starting to test with targeted emails to individual employees.

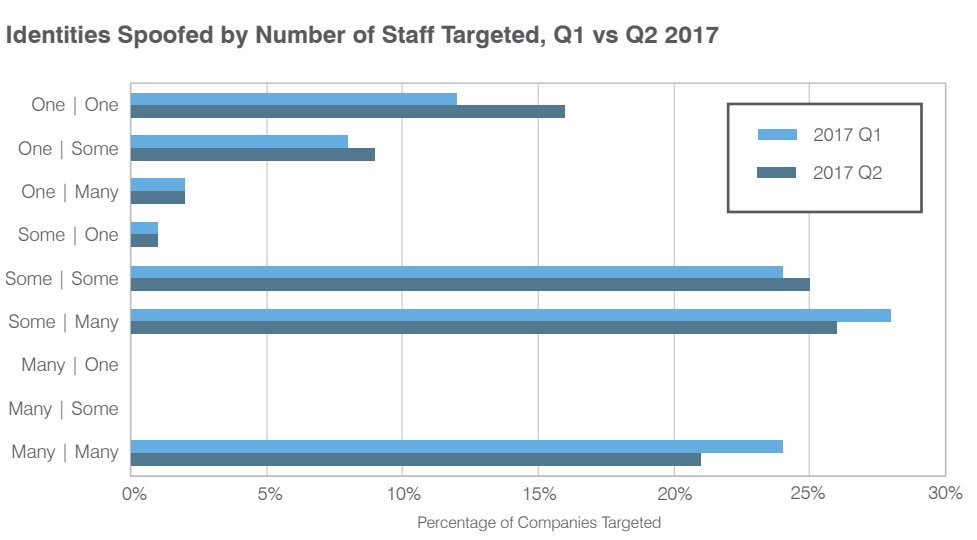

Figure 8: Attack types by number of executive identities spoofed vs. number of individuals targeted. For example, a company that saw BEC attacks in a given quarter that spoofed four executive identities and targeted 10 members of the finance team would be classified in the "some-to-many" bucket.

BEC subject types remain consistent but reflect seasonal trends

Across industries and throughout our customer base, the subject lines most commonly associated with email fraud have held steady over the last several quarters.

Subjects referencing "payments," for example, have held the top spot since we began tracking these categories last year. Payment-related subjects more broadly fall into the category of wire fraud, which continues to be the crime of choice for email fraudsters.

Not surprisingly, however, W2 and other tax season-themed lures reflected the highest degrees of seasonality. The subject lines "W-2", "Tax", and "Legal" all plunged vs. Q1, the tail end of the U.S. tax season. "W-2" fell almost 95%.

Fraudsters tend to use innocuous subjects (see Figure 9) to avoid being detected by anti-fraud tools. But many subjects also include elements of urgency—a psychological trick to get recipients to act without second-guessing the instructions. Subject lines that fall into the "Urgent" category have shown the most dramatic growth.

Most Popular Subject Lines for Observed BEC attacks, Q1 vs Q2 2017

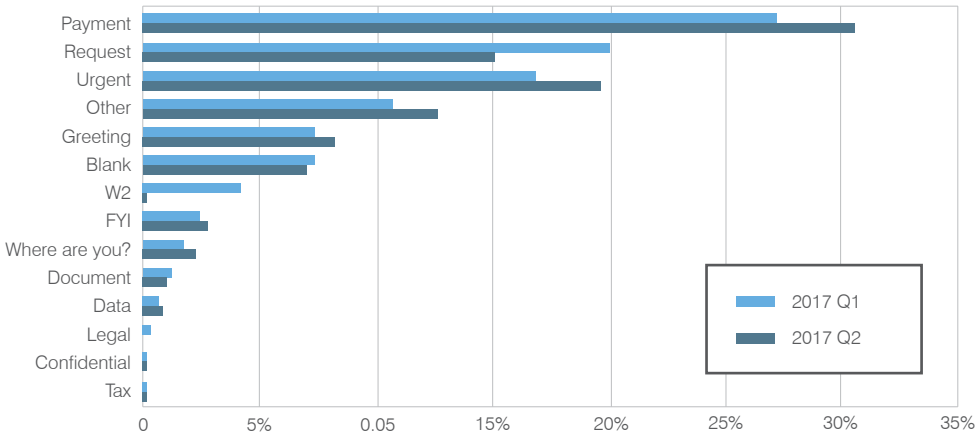

Figure 9: Relative percentages of top subject lines used in BEC attacks in Q2 2017

DMARC makes its mark on email fraud

As more organisations adopt DMARC, domain spoofing has fallen to 40% of all **SPOOFING** attacks, down from over 70% last year.

SPOOFING
Spoofing refers to attackers who disguise their email to appear as if they're from a person or brand that the recipient trusts.

Even the smaller percentage represents a significant risk. One-to-one attacks are on the rise and 87% of organisations that were targeted saw at least one attack that used domain spoofing. The average financial impact of a single successful BEC attack is about US$130,000, according to the FBI.[1]

Spoofing Technique from Q3 2016 to Q2 2017

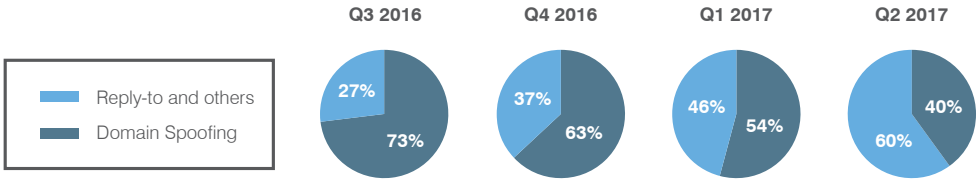

Figure 10: Domain Spoofing percentage versus Reply-to and others

1 FBI. "Business Email Compromise: An Emerging Global Threat." August 2015.

EXPLOIT KITS: WEB-BASED THREATS ARE DOWN, BUT FAR FROM OUT

Key stat: It has been over one year since an unpatched vulnerability appeared in an exploit kit.

Given recent ransomware and malware trends, one might be tempted to think that exploit kits have lost their appeal to attackers and their sting to victims. Indeed, it almost seems like the best days of exploit kits are past; more than a year has passed since the last unpatched vulnerability appeared in an exploit kit. But EK activity in the quarter shows that they still enjoy considerable appeal—and success in dispensing malware.

Overall, exploit kit traffic is holding steady around year-ago levels, which had fallen 95% after a popular EK called Angler shut down (Figure 11).

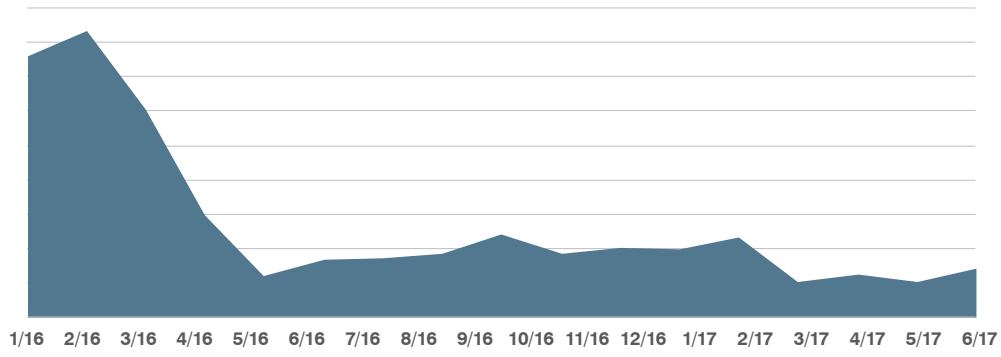

Figure 11: Indexed trend of observed EK activity, January 2016 to June 2017

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

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

Geographic targeting focused on systems in Asian countries. Meanwhile, sophisticated filtering schemes have become an important part of the EK landscape. After some fluctuations and the short-lived rise of an EK called **NEUTRINO**, attackers appear to have coalesced around **RIG**, an EK that accounts for 60%-80% of observed EK traffic in the quarter (Figure 12).

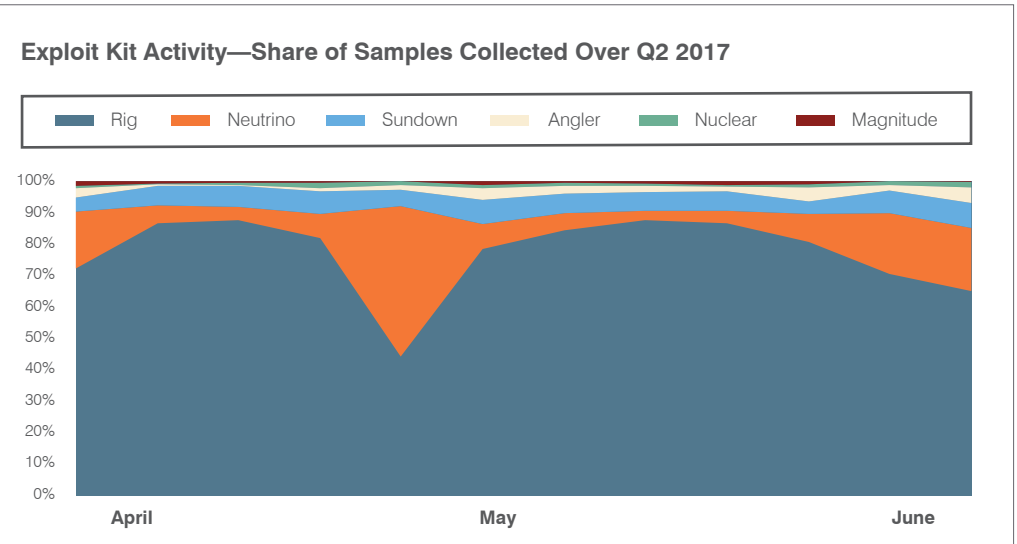

Figure 12: Top exploit kit traffic as percentage of total, April-May 2017

Neutrino and a newer EK entrant called Sundown round out the top three exploit kits. The consistency and stability of the underground EK market suggest strong demand for these services from cyber criminals.

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.

And as if to prove any doubters wrong, exploit kits demonstrated their knack for spreading damage and disruption in June with a high-profile ransomware outbreak in the UK. Initially deemed an email attack, our researchers traced the outbreak to a **MALVERTISING** campaign from the AdGholas threat actor and using the Astrum exploit kit.

Besides serving as a reminder of the real threat exploit kits still pose, the campaign showcased the newest advancements in the EK landscape. Astrum still has not reached the volume of activity associated with the other EKs shown in Figure 11. But AdGholas malvertising being used to redirect to the Astrum Exploit Kit is the most evolved blind mass infection chain known today.

Here are some of the advanced techniques it used, all in a single package:

- Full HTTPS encryption
- Heavy smart filtering
- Domain shadowing
- Diffie-Hellman key exchange algorithm

The attack also suggested a deep knowledge of the online ad industry. This understanding enabled the attackers to lure large agencies to bring in high volumes of traffic from valuable website and targets.

Perhaps most important, it corrected a common misconception about drive-by malvertising: that malicious ads are harmless unless clicked. Contrary to popular belief, there is no need to click on the advertisement to be infected. Simply loading the ad into the browser will compromise the machine if it is vulnerable and targeted—the infection occurs without any user interaction.

SOCIAL MEDIA

Key stat: Fraudulent support accounts soared 300%.

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 remains a breeding ground for a variety of threats, from malware to phishing. The number of phishing links alone in social media grew 70% from the previous quarter, and fake customer-support accounts used for **ANGLER PHISHING** jumped 300%.

The bulk of the growth occurred in May and then held steady in June. We saw similar numbers of phishing links a year ago, but the number of support fraud accounts has grown. With recent research showing that users are twice as likely to click links in social media as they are in email, the channel represents a growing threat.

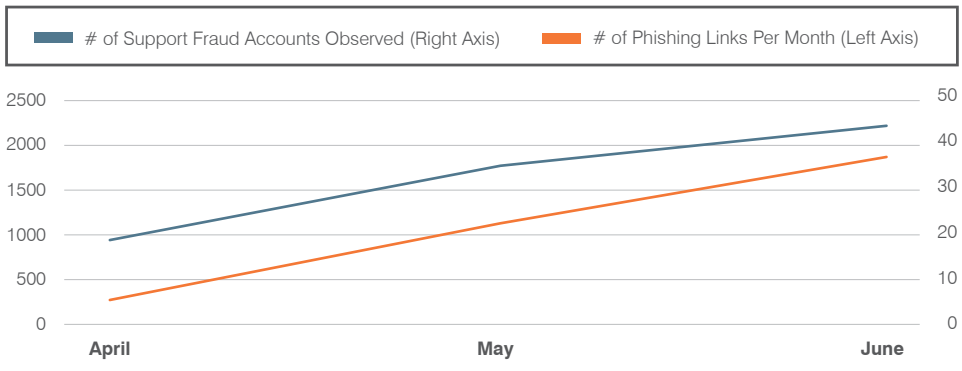

Figure 13: Relative monthly activity in phishing link distribution via social media versus fraudulent support accounts

Cyber criminals also continued to develop new techniques to take advantage of apps and valid accounts to send spam and hijack conversations. We detected a social media spambot campaign that leveraged social engineering to trick end-users into giving threat actors access to their Facebook accounts.

In this case, the compromised accounts were used to make spam posts on the social media pages of major brands. But their access to the victims' accounts would have enabled them to do much more. This technique is exploding, growing from just 40 spam comments in April 2016 to 16,000 in January 2017 from a single app. The trend highlights the accelerating pace of innovation in social media cyber crime and its ability to cash in on social media's "human factor."

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.

Revisit your patching practices
The WannaCry exploit is another example of an advanced threat that takes advantage of legacy systems that are unpatched or poorly configured. As these attacks become more frequent, your best bet is to install the latest patches, validate your security setup and test your backup infrastructure to ensure that you can restore individual machines and company-wide data.

Deploy advanced email gateway analysis
Attackers are constantly finding ways to get around the latest defenses. To detect and stop new attack tools, tactics, and techniques, deploy advanced analysis at the email gateway. Your gateway should draw on advanced threat intelligence to inspect the entire attack chain using static and dynamic techniques. And it should constantly adapt to new threats as they emerge with fast, continual updates.

Use DMARC authentication
DMARC (Domain-based Message Authentication, Reporting and Conformance) authentication can instantly stop email fraud that uses domain spoofing. With DMARC, you can be sure that email using your domain is really from your organisation.

Get visibility into geo-targeted threats
Full visibility within the flow of email can make all the difference in a targeted attack. Visibility means being able to distinguish broad attack campaigns from targeted threats. You should be able to see attacks directed at your executives and other high-value employees so you can prioritise alerts and act on them.

Secure all of your channels from digital fraud
If your organisation uses social media to support or collaborate with customers and partners, it's time to bring your social media channels into the fold of your security program. To protect your brand and the people who trust it, consider solutions that can find and mitigate risks across all the digital channels that matter.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organisations 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 organisations of all sises, 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