REPORT

proofpoint.

QUARTERLY THREAT REPORT

Q2 2018

proofpoint.com

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 250,000 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 gives you actionable intelligence you can use. Our research can help you to better combat today's attacks, anticipate emerging threats and manage your security posture. Along with our findings, we recommend steps you can take to protect your people and your organization.

TABLE OF CONTENTS

KEY TAKEAWAYS: RANSOMWARE IS BACK BUT BANKERS AND MINERS REIGN SUPREME

Below are key takeaways from the second quarter of 2018.

EMAIL

- Malicious message volume in Q2 increased 36% vs. Q1 2018. While still lower than peak volumes experienced in 2016 and 2017, payload variety from a large group of threat actors rather than massive campaigns from a small group of high-volume attackers characterized Q2.
- Ransomware returned with commensurate drops in credential stealers and banking Trojans. However, at just over 11% of total malicious message volume, ransomware appears to be a normal part of threat actors' rotating toolkits rather than the dominant payloads of the quarter. We also continued to observe consolidation around major strains like GandCrab--introduced in Q1 2018--and Sigma, another relative newcomer to the ransomware landscape.
- On average, customers targeted in email fraud attacks received 35 business email compromise (BEC) messages in Q2, a 26% increase over Q1 and an 87% increase over Q2 2017. As in previous quarters, these increases were not correlated with the size of the organization being attacked; companies of all sizes were targeted equally, although some industries such as retail, healthcare and government all experienced larger increases in BEC activity than their counterparts.

EMAIL FRAUD (AKA BEC) MESSAGE VOLUME AMONG TARGETED ORGANIZATIONS **INCREASED 87% YOY.**

EXPLOIT KITS AND WEB-BASED ATTACKS

- As observed over the last several quarters, exploit kit (EK) activity remains a small fraction of its early 2016 peak.
- Traffic associated with social engineering schemes and so-called "cryptojacking" spiked in Q2, with Coinhive events jumping 460% vs. Q1 2018.
- Social engineering schemes on the web, particularly those involving fake antivirus and browser plugins, continue to grow rapidly, increasing 500% over Q1.

SOCIAL MEDIA AND DOMAIN RESEARCH

- After growing by 200% between Q4 2017 and Q1 2018, support fraud again grew by 38% quarter over quarter in Q2 2018. And it grew 400% vs. Q2 of 2017.
- Proofpoint researchers also detected a 30% increase in phishing links on social media. This comes after months of decline as social platforms developed automated means of remediating this threat.

EMAIL-BASED THREAT TRENDS: THE SAME BUT DIFFERENT

Key stat: Malicious message volume in Q2 increased 36% vs. Q1 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.

Much of 2017 was characterized by massive email campaigns bearing malicious attachments. The largest of these were consistently sent by a single actor known as **TA505.** In contrast, 2018 campaigns to date have generally been smaller, more diverse in their payloads, and more likely to rely on URLs linking to malicious files than attached documents (Figure 1).

TA505
TA505 is a financially motivated actor responsible for many of the largest campaigns we have observed, regularly distributing millions of malicious messages at their peak in 2016 and 2017.

Indexed Daily Message Volume by Attack Type, Q1 and Q2 2018

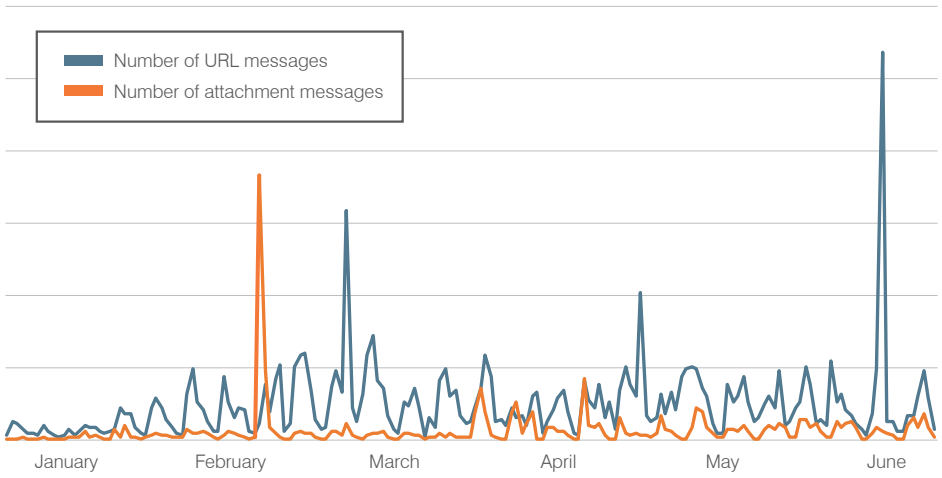

Figure 1: Indexed daily attack type trend, January–June 2018

The second quarter of 2018 saw a 36% increase in total malicious message volume over the first quarter. The reappearance of regular ransomware campaigns created a more even mix of malware families (Figure 2), whether they were distributed as attachments or via links. A 7 percentage point increase in **DOWNLOADER** payloads vs. Q1, as well as an 11 percentage point increase in ransomware payloads were accompanied by drops in the proportion of credential stealers and banking Trojans.

DOWNLOADER
Malware with a generally small footprint used to download other malicious software on a victim's device.

Malware by Category, Q2 2018

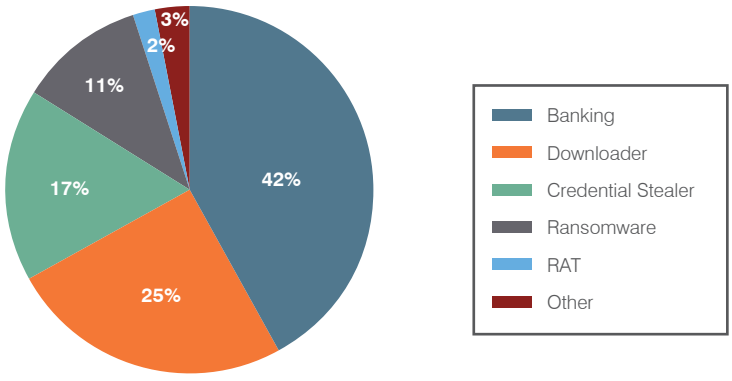

Figure 2: Relative mix of malware payloads in email by category, Q2 2018

REMOTE ACCESS TROJANS

Remote Access Trojans, or RATs, provide attackers with complete administrative control of the victim's system. RATs are used for reconnaissance, espionage, financial gain, credential theft, loading additional malware, and more.

FLAWEDAMMYY

FlawedAmmy is a RAT based on leaked source code for the legitimate remote access software, Ammy Admin. Discovered by Proofpoint Researchers in 2018, the RAT is now widely distributed.

Figure 3 shows the shifting daily mix of malware across the first half of 2018. Note that **REMOTE ACCESS TROJANS** (RATs), appeared in almost daily campaigns in Q1. They doubled their associated relative message volume in Q2, accounting for 2% of the malicious messages we saw. While overall volumes remain relatively low, high-volume actors like TA505 are now distributing RATs like **FLAWEDAMMYY** on a regular basis. This suggests that a wider range of financially motivated actors see potential value in infecting large numbers of clients with this type of malware.

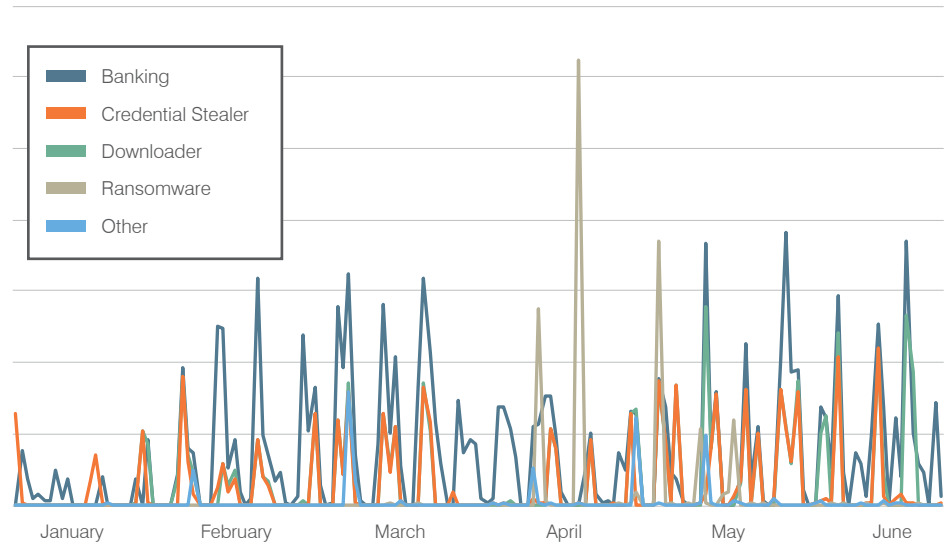

Figure 3: Relative daily message volume by malware category, H1 2018

COIN MINERS MEET COMMODITY MALWARE

Mainstream uses for cryptocurrency are often mired in controversy, with frequent headlines about currency manipulation, underground markets for illegal goods and services, and more. However, it remains the currency of choice for anyone attracted by the promise of both anonymous transactions and potential profits. As ransomware infection rates have slowed, cybercriminals are now turning to other options. These include standalone strains of coin mining malware, add-on modules for banking Trojans, and in-browser mining software to generate cryptocurrency revenue.

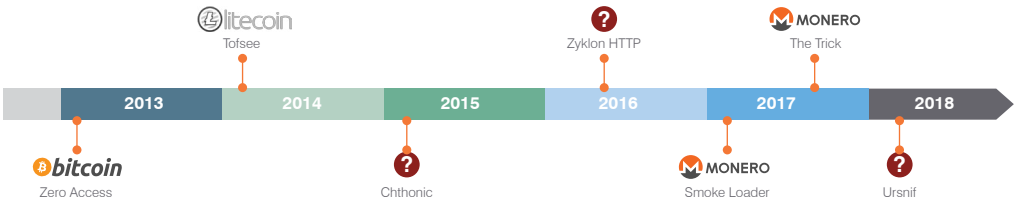

Figure 4: Timeline of cryptocurrency mining introductions to commodity malware

The evolution of banking Trojans in particular provides insight into the importance of cryptocurrency in the threat landscape. The timeline above shows when we first observed the addition of coin mining capabilities to mainstream or commodity banking Trojans. Historically, bankers have generally used webinjects that either modify or replace web pages from online banking sites to steal login credentials, conduct fraudulent transactions, and otherwise monetize infections. Most banking Trojan campaigns are regionally targeted, as the webinjects must be configured for individual banks. However, many banking Trojan campaigns have added cryptocurrency mining modules or bots, known as coin miners, as later-stage payloads. This expands a trend that we first reported in Q3 2017. Other bankers—most notably, The Trick—added cryptocurrency mining modules to the primary payload.

At the same time, we have seen webinjects increasingly target cryptocurrency wallets and exchanges, as well as international online payment sites. This makes regional targeting less critical.

BANKERS' HOLIDAY: BANKING TROJANS CONTINUE TO DOMINATE, WITH PANDA EMERGING FROM THE SHADOW OF EMOTET

Key stat: Banking Trojans accounted for 42% of all observed malicious messages, dropping 17% as ransomware campaigns picked back up.

Banking Trojans remained the top payload in the second quarter of 2018, exceeding the next largest category, downloaders, by 17%. While bankers decreased proportionally over Q2 relative to other malware families, overall message volume increases meant that banking Trojan volumes stayed relatively flat vs. Q1. However, the changing mix of banking Trojan strains was noteworthy. This is shown in Figure 5.

Relative Indexed Message Volumes, Banking Trojans, Q1 vs. Q2

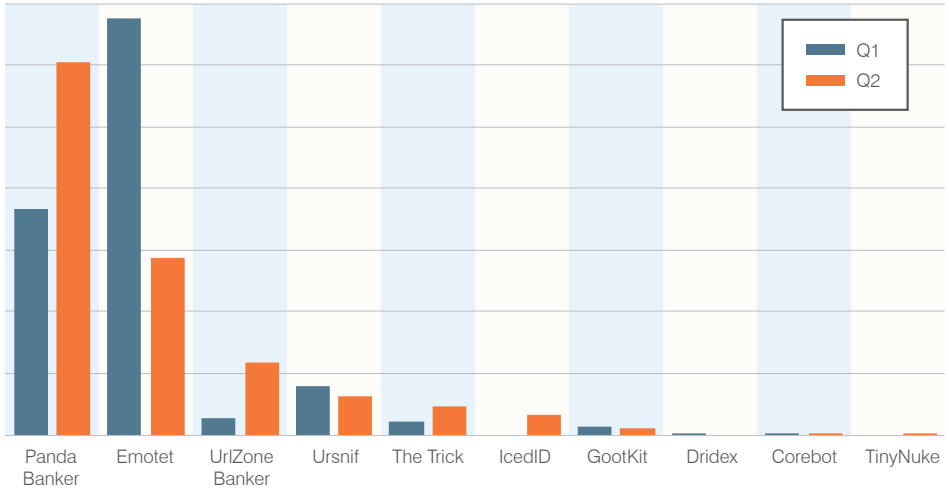

Figure 5: Indexed relative quarterly banking Trojan message volume, Q1 vs. Q2 2018 for the top 10 banking Trojans to date

EMOTET
Emotet is a banking Trojan that peaked in distribution in Q1 2018 with modules for direct theft from victim bank accounts, information theft, DDoS, and more.

Panda Banker (aka Zeus Panda) appeared in several large campaigns in Q2, while **EMOTET** volumes dropped precipitously. The URLZone banking Trojan appeared in regular campaigns targeting Japan throughout Q2; these campaigns all downloaded the Ursnif banking Trojan as a secondary payload. Another banker known as IcedID also appeared at scale in Q2, frequently as a secondary payload associated with Ursnif and The Trick infections.

RANSOMWARE: YOU KNEW IT WASN'T GONE

Key stat: Ransomware accounted for 11% of malicious campaigns in Q2, up from a fraction of 1% in Q1

Ransomware was largely absent from malicious email campaigns in Q1, particularly compared to the previous 18 months. During that time it dominated the threat landscape. The reason for its decline has been the subject of significant speculation. Potential explanations range from market saturation to reduced activity by TA505, an actor responsible for the largest ransomware campaigns we have ever seen.

GANDCRAB
GandCrab is a recently discovered ransomware strain distributed in an affiliate model, allowing multiple actors to distribute the malware through a variety of vectors.

While message volume with ransomware payloads is far from 2016 and 2017 levels, ransomware did return to more regular campaigns in the second quarter of 2018. Proofpoint researchers observed **GANDCRAB**, Sigma and GlobeImposter ransomware in Q2, with GandCrab campaigns driving overall volumes to 11% of malicious email volume.

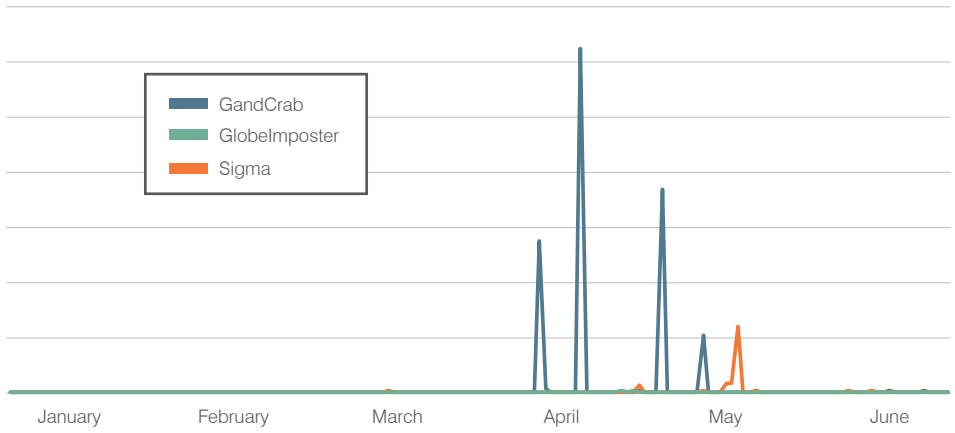

Figure 6: Relative volume of malicious messages bearing ransomware as their primary payloads, Q1 and Q2 2018

It remains to be seen how ransomware campaigns will evolve in the coming months. Threat actors continue to diversify beyond the ransomware that had previously proved so lucrative. A year ago, the rapid introduction of new ransomware strains peaked, with almost two new strains appearing each day. Since then, the rate at which new variants were introduced by malware authors and attackers has steadily declined. Even as ransomware began appearing more frequently again in malicious email campaigns, we continued to see consolidation around major strains. These include GandCrab—introduced in Q1 2018—and Sigma, another relative newcomer to the ransomware landscape. This is in contrast to the frequent appearance of one-offs, proofs of concept, and minor variants that largely followed on the heels of massive **LOCKY** campaigns from 2016 and early 2017 (Figure 7).

LOCKY
Locky ransomware was introduced in early 2016 by TA505; it became a dominant feature of the threat landscape over the next two years.

Figure 7: New ransomware strains by quarter

Ransomware by nature is extremely noisy -- for the time being, it appears that threat actors are still favoring malware that can persist on infected machines and potentially generate longer term value than ransomware. However, the reintroduction of ransomware in Q2, albeit at lower volumes than in years past, suggests that ransomware is becoming a more regular feature of the threat landscape and a standard part of the rotating toolkit employed by threat actors rather than their bread and butter.

EMAIL FRAUD THREATS: GROWTH CONTINUES AS THREAT ACTORS TWEAK TECHNIQUES

Key stat: On average, targeted organizations received 35 BEC emails in Q2, a 26% increase quarter over quarter and 87% year over year.

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.

EMAIL FRAUD, also known as business email compromise or BEC, continues to accumulate billions in reported losses. We continue to see substantial growth both in several metrics related to email fraud, as well as shifts in technique and targeting throughout Q2.

On average, customers targeted in email fraud attacks received 35 BEC messages in Q2. This is a 26% increase over Q1 and an 87% increase over Q2 2017. As in previous quarters, these increases were not correlated with the size of the organization being attacked; companies of all sizes were targeted equally. However, some industries such as retail, healthcare, and government all experienced larger increases in BEC activity than their counterparts (Figure 8). In each of these outlier industries, email fraud attackers began systematically targeting larger numbers of staff at affected organizations.

COMPANIES OF ALL SIZES WERE TARGETED EQUALLY. HOWEVER, SOME INDUSTRIES **SUCH AS RETAIL, HEALTHCARE, AND GOVERNMENT** ALL EXPERIENCED LARGER INCREASES IN BEC ACTIVITY THAN THEIR COUNTERPARTS.

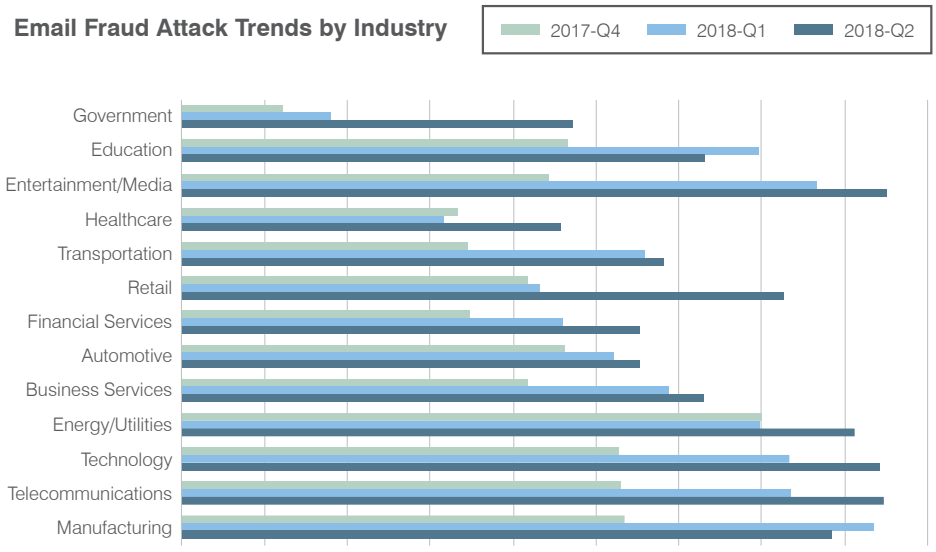

Figure 8: Number of BEC attacks per targeted organization by industry

Similarly, attackers changed tactics around lures in email fraud attacks as well. The term "document" was used in almost 12% of attacks, up 14 times from Q1. This was accompanied by decreases in blank subject lines, requests for payment, and—perhaps predictably—W2-related subjects, among others (Figure 9).

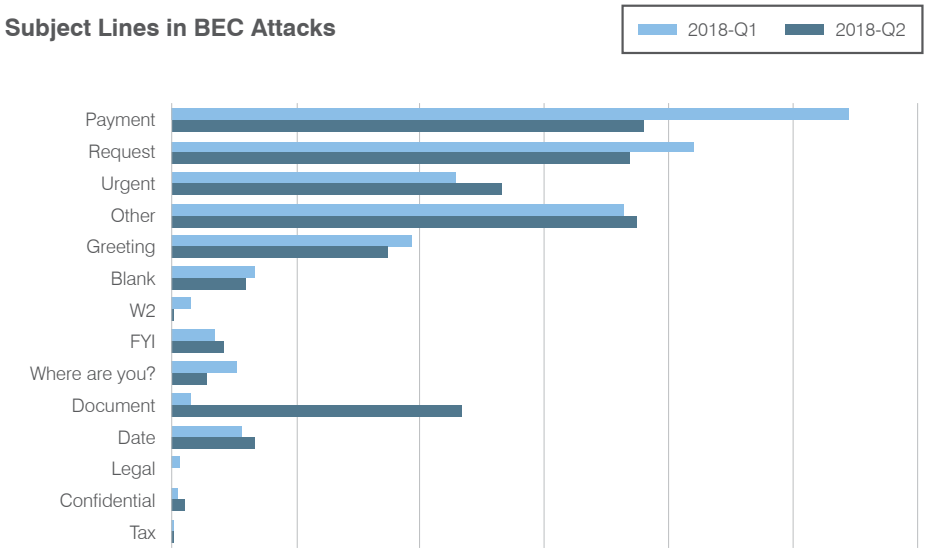

Figure 9: Q1 vs. Q2 email fraud attacks by subject header

Other measures of email fraud tools and techniques remained largely unchanged vs. Q1. The number of identities spoofed in targeted organizations, the number of unique individuals within those organizations who were targeted, and the ratio of spoofed identities to targeted individuals all held steady.

The presence of fake chains—tactics used to create the appearance of an email history and legitimate interactions—dropped by just over three percentage points that threat actors are no longer finding the technique to be as useful or necessary from a social engineering perspective.

WEB-BASED THREATS: COINHIVE AND SOCIAL ENGINEERING EVENTS SPIKE, EXPLOIT KITS LIMP ALONG

Key stat: Detected Coinhive events jumped by 460% vs. Q1 2018

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-engineeing schemes that could trick people into installing malware.

As we have seen over the last several quarters, exploit kit (EK) activity remains a small fraction of its early 2016 peak. However, the traffic that is associated with social engineering schemes and so-called "cryptojacking" spiked in Q2, with **COINHIVE** events jumping 460% vs. Q1 2018.

COINHIVE
JavaScript code designed to allow website operators to mine cryptocurrency using site visitor CPUs.

Figure 10 shows relative activity from major EKs for the first half of 2018. Neutrino and RIG continue to dominate what remains of the EK market. In one notable campaign, we observed RIG EK being used in a combination phishing and malware attack to infect machines with TeamViewer. This suggests that threat actors are still innovating in their use of exploit kits.

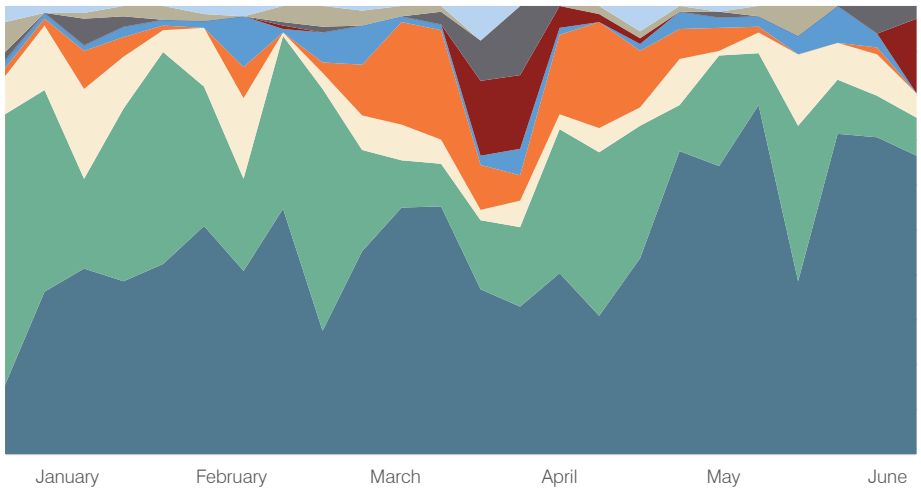

Figure 10: Relative activity for top exploit kits, year to date

BLACKTDS
A new traffic distribution system used in a growing number of web-based schemes and malicious email campaigns in which threat actors can redirect victims to the pages or malware payloads of their choice.

Despite these declines in more traditional web-based attacks, we continue to see increased activity around **BLACKTDS**, a so-called "drive-by as a service". BlackTDS is appearing frequently. And it delivers malware for a growing group of financially motivated actors we regularly track.

Social engineering schemes on the web, particularly those involving fake antivirus and browser plugins, continue to grow rapidly. These rose 500% over Q1, as shown in Figure 11.

Figure 11: Indexed IDS events related to social engineering schemes

Throughout Q2 2018, we have also observed steady growth of events on our IDS sensor network relating to Coinhive. And, beginning in late May, we saw a rapid increase in Coinhive traffic. This resulted in a 460% jump quarter over quarter, as shown in Figure 12.

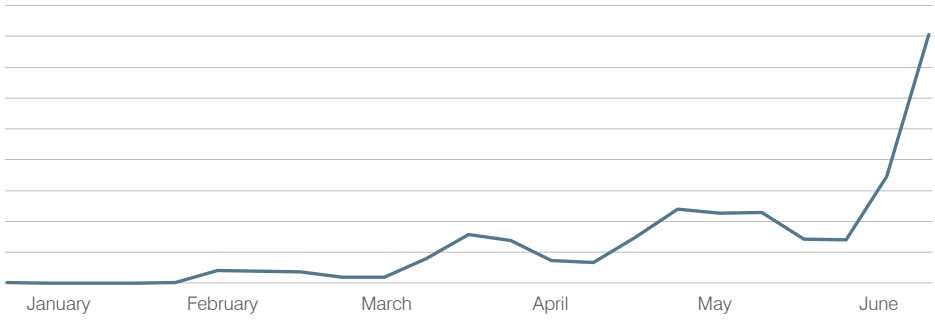

Figure 12: Coinhive events, H1 2018, shown as a percent of total observed IDS events

Coinhive was originally developed to allow website operators to monetize their sites. It did this by co-opting visitor CPUs to mine Monero cryptocurrency. Some sites have already implemented the JavaScript code, following the best practice of informing users of the activity. In some cases, they have done away with advertisements for a revenue stream. In many other cases, though, attackers have modified the code and inserted it on websites without informing users in a practice known as cryptojacking.

SOCIAL MEDIA THREATS: SUPPORT FRAUD REACHES NEW LEVELS

Key stat: Support fraud phishing grew 38% vs. Q1 of 2018 and over 400% year over year.

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.

Social media continues to be a critical point of engagement between brands and customers. It is also a "Wild West" of digital risk. Support fraud, also known as angler phishing, is when attackers attempt to insert themselves in legitimate conversations between consumers and brand-owned social media accounts. This continued to grow rapidly in the second quarter.

After growing by 200% between Q4 2017 and Q1 2018, support fraud again grew by 38% in Q2 2018. This is a 400% growth vs. Q2 of 2017, even with what appears to be a seasonal dip in support fraud activity in June.

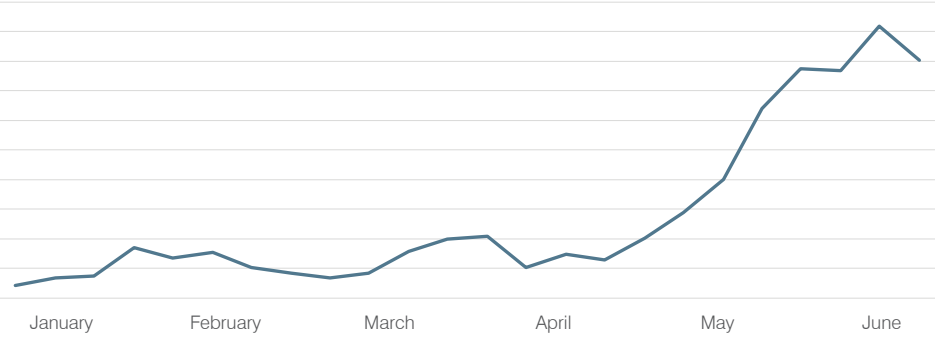

Figure 13: Indexed support fraud phishing account volume

Proofpoint researchers also detected a 30% increase in phishing links on social media. Phishing links had been steadily declining as social platforms developed automated means of remediating this threat. We will continue to monitor for the presence of phishing links to see if this represents a trend or overall shift in techniques.

2018 WORLD CUP—ATTACKERS TIP THEIR HANDS IN SOCIAL CHANNELS

For years we have seen attackers exploit major events and trends for social engineering. These exploits target fans, brands, participants and other interested parties. They target anyone who might click through malicious links, inadvertently install malware, or divulge personal or financial information. The World Cup and its associated brands captured the attention of millions of fans worldwide. And they also provided countless examples of brand theft, suspicious behavior, and other risks to businesses and their constituents.

A look at Twitter and Facebook accounts with keywords related to the World Cup revealed almost 250 accounts representing potential brand risk or malicious intent for the competition and its sponsors.

World Cup-related social media accounts by risk type

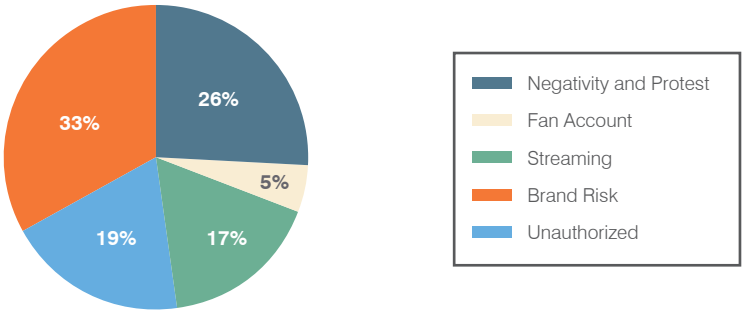

Figure 14: Percentage of social media accounts related to the World Cup

Streaming accounts, for example, represented almost 17% of the suspicious accounts we identified associated with the World Cup. These featured:

- Hosted malware on linked sites
- Phishing for user's personal information or credentials
- Direct monetization by serving large numbers of online ads

Social media accounts that we dub "brand risk," on the other hand, accounted for over a third of the suspicious accounts we detected in connection with the World Cup. These pages were the most likely to include links to malicious content or engage in malicious activity with fans and followers. Stolen branding and social engineering contributed to their sense of legitimacy, but many included fake giveaways, phishing attempts, links to malicious pages and more. The brand risk was a result of fans believing they have been scammed, infected or phished via pages they expected to be legitimate.

Social media channels are new breeding grounds for these kinds of threats, with hundreds of suspicious accounts cropping up to take advantage of an event's popularity. It was easy for attackers to create accounts co-opting World Cup-related brands on social media. This created a complex landscape for people to navigate as they consumed a range of media and information during this summer's competition.

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.** Email fraud scams are often difficult to detect. Invest in a solution that has dynamic classification capabilities that you can use to build quarantine and blocking policies.

- **Protect your brand reputation and customers.** Fight attacks that target your customers over social media, email, and mobile. Especially the fraudulent accounts that piggyback on your brand. Look for a comprehensive social media security solution that scans all social networks and reports fraudulent activity.

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

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

ABOUT PROOFPOINT
Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50% 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.