proofpoint.

QUARTERLY

THREAT REPORT

Q1 2019

EXECUTIVE SUMMARY

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

Every day, we analyze more than 5 billion email messages, hundreds of millions of social media posts and more than 250 million malware samples to protect organizations around the world from advanced threats. We continue to see sophisticated threats across email, social media and the web. That gives us a unique vantage point from which to reveal and analyze the tactics, tools and targets of today's cyberattacks.

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

TABLE OF CONTENTS

KEY TAKEAWAYS: BUSINESS EMAIL COMPROMISE (BEC) GROWTH CONTINUES, WHILE EMOTET DOMINATES MALWARE IN Q1

61% OF MALICIOUS PAYLOADS WERE EMOTET, A BOTNET THAT CAN LOAD A RANGE OF ADDITIONAL MODULES, FROM SPAMMING TO INFORMATION STEALING.

EMAIL

- Malicious URLs in emails outnumbered malicious attachments by roughly 5 to 1 for Q1, up 21% quarter over quarter and 180% vs. Q1 2018.
- Banking Trojans made up only 21% of malicious payloads in email during the quarter, comprised primarily of IcedID, The Trick and Qbot.
- 61% of malicious payloads were Emotet, a botnet that can load a range of additional modules, from spamming to information stealing. Volumes for downloaders, stealers and remote access Trojans (RATs) dropped 11, 8 and 7 percentage points, respectively, with Emotet making up most of the difference.
- Ransomware remained virtually absent in the first three months of 2019, as 82% of all payloads were either Emotet (formerly classified as a banking Trojan) or current bankers.
- "Payment" jumped to the top subject line in email fraud attacks, up 6 percentage points from Q4 2018.
- In Q1 2019, engineering, automotive and education were the industries most heavily targeted in email fraud attacks.
- Across all industries, targeted organizations experienced an average of 47 such attacks. These numbers were lower than the record highs of Q4 2018 but may be a sign of increasingly selective targeting and seasonal variations.

WEB-BASED ATTACKS

- Coinhive samples spiked in late January to 4.9 times the weekly average for the quarter. Not surprisingly, detected events dropped to near-zero after Coinhive shut down in March 2019. Others filled the gap in illicit coin mining, as threat actors continue to operate in this space, despite ongoing market volatility.
- Social engineering attacks via compromised websites and malvertising were off from Q4 2018 levels by roughly 50%, reflecting what appears to be a seasonal trend. However, activity was still 16 times higher than the year-ago quarter.

DOMAIN FRAUD

- Over three times as many fraudulent domains had an SSL certificate as legitimate domains in Q1 2019, lending a false sense of security to end users encountering these domains online and in email attacks.
- In Q1, the proportion of domains identified as potentially fraudulent that resolved to an IP address was 26 percentage points higher than for all domains across the web. The proportion generating HTTP responses was 43 percentage points higher than for all domains.
- March registrations of look-alike domains were almost as numerous as the previous two months combined.

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.

EMAIL-BASED THREAT TRENDS: THREAT ACTORS CONTINUE TO FAVOR MALICIOUS URLS, WHILE EMOTET KEEPS VOLUME HIGH

Key statistic: Attacks leveraging malicious URLs continued to grow relative to those bearing malicious attachments. Malicious URLs in emails outnumbered malicious attachments by roughly 5 to 1 for Q1, up 21% quarter over quarter and 180% vs. Q1 2018.

Email remains the top vector for malware distribution and phishing, while email fraud continues to grow rapidly, with threat actors adapting tools and techniques across attack types to best capitalize on a range of vulnerabilities. Overall message volume in Q1 2019 remained almost flat compared to Q4 2018, bucking the usual trend of a substantial drop in volume during the first quarter of the year.

EMOTET

Emotet is a botnet that has appeared in sustained, large-scale campaigns for several months with modules for direct theft from victim bank accounts, information theft, DDoS and more.

As shown in Figure 1, while malicious URLs outnumbered malicious attachments in email campaigns delivering malware throughout Q4 2018, the pendulum has swung even further in favor of malicious URLs. Much of this traffic, both overall and in terms of the prevalence of malicious URLs in messages, was driven by the actor distributing the **EMOTET** botnet.

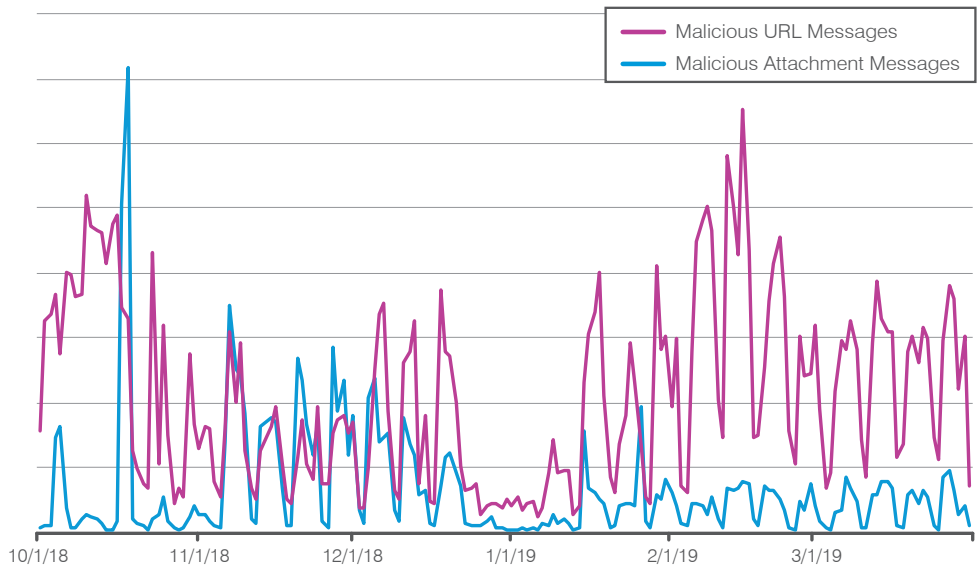

Figure 1: Indexed daily attack type trend, October 2018–March 2019

BOTNET
A botnet is a network of devices infected with malware that can be controlled as a group by threat actors without the owners' knowledge.

Although previously classified as a banking Trojan, Emotet is now widely considered a **BOTNET**, frequently downloading additional modules for sending spam and downloading additional malware. This change in classification, as well as significant increases in the volume of messages attempting to install Emotet, led to a significant change in the relative volume of messages by malware family. Figure 2 shows the relative volume by family for Q1 2019, in which 61% of malicious payloads were botnets, all of which were Emotet.

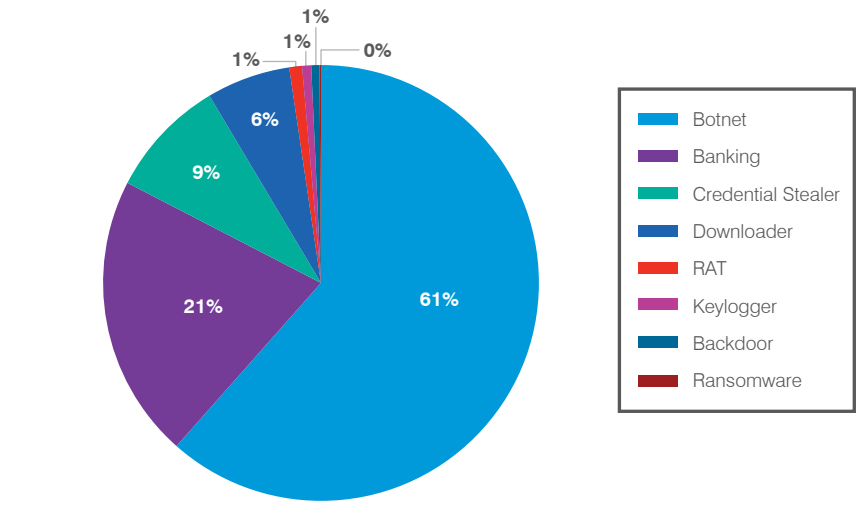

Figure 2: Relative mix of malware payloads in email by category, Q1 2019

REMOTE ACCESS TROJAN
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.

Figure 3 illustrates the dramatic shift in relative malware volumes observed between Q4 2018 and Q1 2019. While the change in Emotet's classification is responsible for the appearance of the botnet category in 2019, the figure also illustrates how Emotet displaced credential stealers, stand-alone downloaders and **RATS** in the overall landscape.

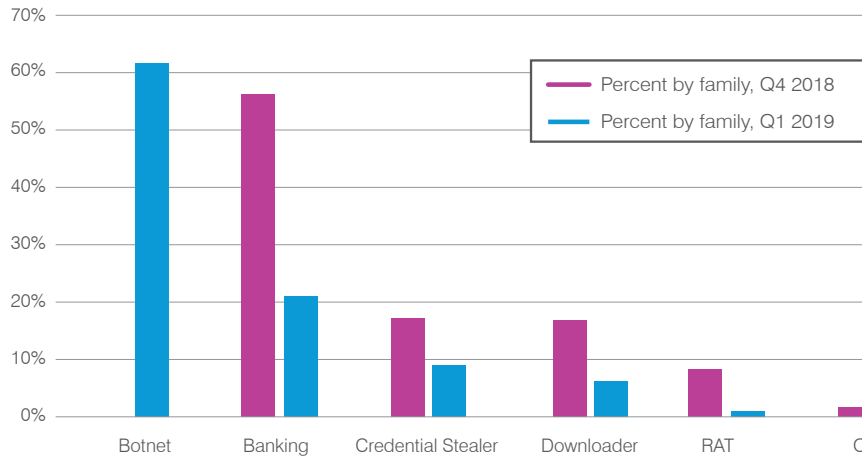

Figure 3: QoQ comparisons of relative malware volumes by family

TA505
A prolific actor that distributed extremely high-volume campaigns through 2017 and turned to lower volume campaigns focused on RATs and downloaders.

As in recent quarters, ransomware was virtually absent in the first three months of 2019 with the exception of some smaller-scale, targeted GandCrab campaigns. Remote access Trojans (RATs), which peaked at 8% of overall volume in Q4 2018, dropped to just 1% of initial malicious payloads, largely due to decreased activity by **TA505**, a frequent distributor of RATs in moderate-volume campaigns. Credential stealers and downloaders continued to decline relative to Q3 and Q4 2018, but it is still too early to know if these reflect seasonal trends of normally expected lower Q1 traffic.

A MIXED BAG FOR BANKING TROJANS AS EMOTET GOES ALL-IN ON BOTNET ACTIVITIES

Key statistic: Banking Trojans made up only 21% of malicious payloads in Q1. Combined with Emotet, however, the two comprised 82% of all email-borne malware.

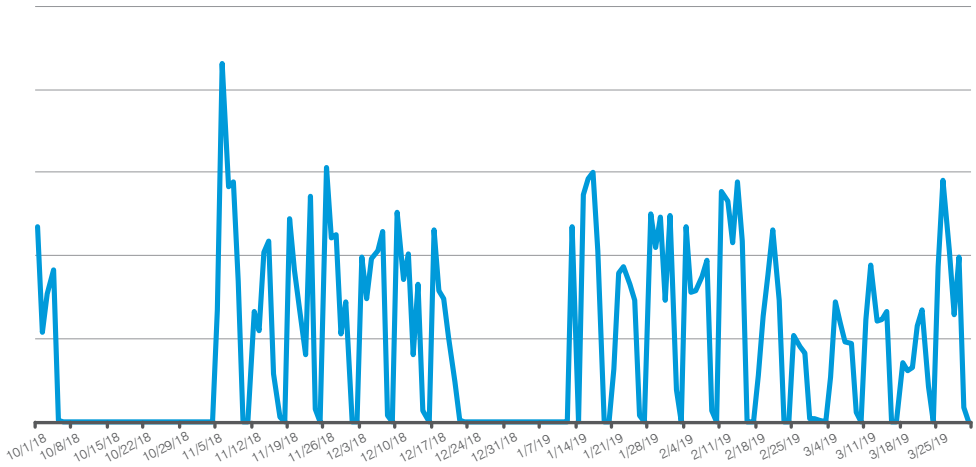

Figure 4: Indexed Emotet message volumes for Q4 2018 and Q1 2019

ICEDID
IcedID is a banking Trojan that we originally observed being distributed by Emotet in April of 2017 but is now distributed by multiple actors.

QBOT
Qbot is a banking Trojan and a backdoor that can perform several actions including stealing information and logging keystrokes.

While Emotet did not achieve the peak volumes we observed in Q4 2018, consistent campaigns throughout Q1 resulted in a nearly 27% increase in total message volumes bearing Emotet for the quarter.

Removing Emotet from Q4 2018 banking Trojan volumes and looking across the last two quarters, we see a marked shift towards **ICEDID**, The Trick and **QBOT**, while Panda Banker, the top banking Trojan in Q4 2018, was not detected in any email campaigns. In Q1, IcedID, The Trick and Qbot accounted for over 85% of banking Trojan payloads in email.

However, because Emotet has steadily shifted away from banking activities, overall volumes associated with dedicated banking Trojans now stand at 21% of malicious payloads observed in email. While we should not assume that banking Trojan volumes are down by 35 percentage points from Q4 2018, when we reported that they made up 56% of all malicious payloads (including, at that time, Emotet), the decline in banking Trojans after their 2018 resurgence is noteworthy as an indicator of a functional shift in the preferred malware payloads of crimeware threat actors.

IN Q1, ICEDID, THE TRICK AND QBOT **ACCOUNTED FOR OVER 85%** OF BANKING TROJAN PAYLOADS IN EMAIL.

Relative Banking Trojan Volumes, Q4 2018 and Q1 2019

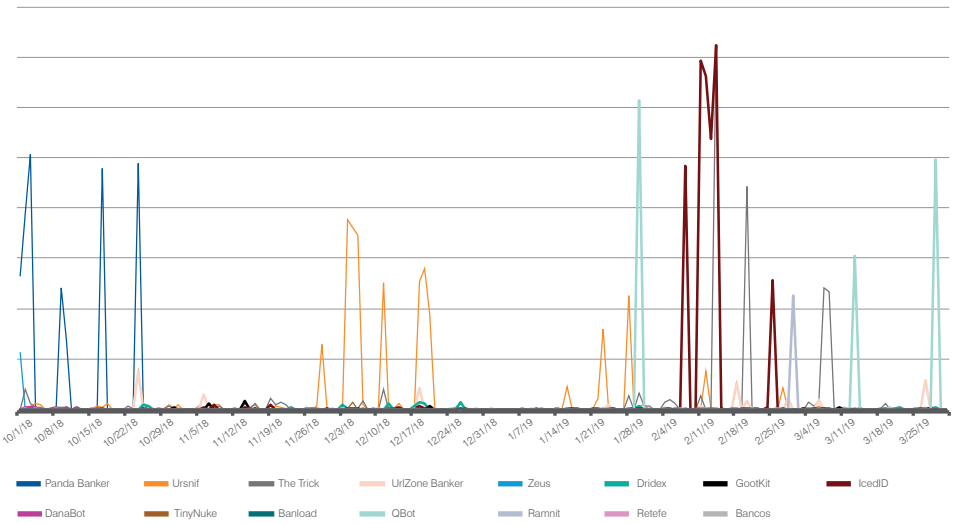

Figure 5: Indexed relative daily banking Trojan message volume, Q1 2019

Figure 6 emphasizes the frequent changes in actor activity and dominant payloads, as actors shift malware and/or exit the landscape temporarily. It is worth noting that we regularly see overall declines in activity in Q1. This quarter, ongoing large Emotet campaigns compensated for changes elsewhere, so it remains to be seen what trends will emerge in the coming quarter as actors ramp up to more typical activity levels.

Relative Volume of Banking Trojan Campaigns, Q1 2019

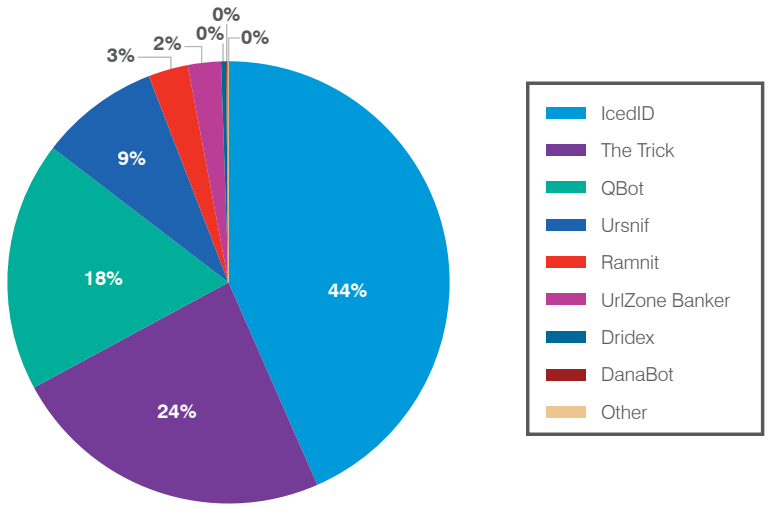

Figure 6: Relative mix of banking Trojan message volumes, Q1 2019

RANSOMWARE: OUT OF THE INBOX AND INTO HIGH-STAKES ATTACKS

In the last quarter of 2018 and the first quarter of 2019, ransomware made up just one-tenth of one percent of all malicious payloads delivered via email. This stands in stark contrast to 2016 and 2017, when ransomware regularly comprised the vast majority of malicious payloads. However, ransomware has not disappeared altogether from the threat landscape. Rather, threat actors are now using ransomware in targeted attacks against key assets for much larger ransoms instead of attacking hundreds of thousands of recipients in low-ransom, high-volume malicious email campaigns. In short, threat actors are going for quality over quantity in their ransomware attacks.

Recent high-profile ransomware infections like the LockerGoga attack on Norsk Hydro and widely reported attacks on local government agencies often occur as secondary infections on compromised networks. The ransomware may be deployed directly by attackers on vulnerable targets or may be downloaded via Trojans already resident on network devices. This fits with the trend we observed throughout 2018 of widespread deployment of RATs, downloaders and backdoors that may sit undetected on endpoints and servers. These types of malware can collect information and provide threat actors with the intelligence necessary to identify vulnerable, high-value assets that are most likely to ensure organizations are willing to pay very large ransoms instead of hundreds of dollars typically demanded to unlock an individual PC in attacks common in previous years. By shifting gears in this way, threat actors can now take advantage of deeper pockets and higher stakes to demand tens of thousands or even millions of dollars to unlock servers and other critical infrastructure.

EMOTET IS A MALWARE MULTI-TOOL: WHERE DOES THAT LEAVE RATS, DOWNLOADERS AND STEALERS?

Key statistic: Volumes for downloaders, stealers and RATs dropped 11, 8 and 7 percentage points, respectively while Emotet increased 26%.

MALWARE-AS-A-SERVICE
A paradigm in which threat actors sell access to malware and infrastructure to other actors.

For several quarters, we have tracked a steady increase in the prevalence of RATs. Prior to 2018, RATs rarely appeared in the consumer and enterprise landscapes. At the same time, 2018 saw consistently high proportions of downloaders and information stealers as ransomware volumes dropped off precipitously. Now, however, the most widely distributed malware strain is a modular botnet, capable of functioning like all of these types of malware. Emotet also appears to be available in a **"MALWARE-AS-A-SERVICE"** model, allowing threat actors to distribute malware via the botnet and leverage its large network of infected devices.

While Emotet has been observed delivering a range of secondary payloads, including banking Trojans, it is not clear if Emotet will bring about a shakeout in the malware market or simply enable more widespread infections. Of note, we have observed the actor primarily responsible for distributing Emotet switch occasionally to Qbot, another robust malware strain that, while primarily a banking Trojan, also contains information stealing and backdoor capabilities.

While this trend bears further observation, it is possible that the upsurge in RATs in 2018 portended the rise in full-featured "Swiss Army Knife" malware capable of satisfying a range of needs for multiple threat actors.

EMAIL FRAUD THREATS: Q1 SEES CONTINUED GROWTH IN BEC-STYLE ATTACKS AND IDENTITY DECEPTION TECHNIQUES

Key statistic: "Payment" jumped to the top subject line in email fraud attacks, up 6 percentage points from Q4 2018

EMAIL FRAUD
Email attacks leveraging various identity deception techniques to trick recipients into completing actions under fraudulent pretenses.

EMAIL FRAUD remains a pervasive challenge for organizations, with threat actors shifting tactics, both seasonally and based on apparent trial and error. They build off of successful techniques and back off techniques that appear to net lower returns. At the same time, these attacks, which rely on sophisticated social engineering and identity deception, exploit email personas that are not specifically verified through tools such as Domain-based Message Authentication, Reporting & Conformance (DMARC), which can help organizations understand the true identity of senders and intended recipients.

In Q1 2019, engineering, automotive and education were the most affected industries, averaging between 80 and 100 imposter messages per targeted organization (Figure 9). Across all industries, targeted organizations experienced an average of 47 such attacks. While these numbers are off from the record-high levels of Q4 2018, we regularly observe overall lower threat activity levels in Q1 as attackers retool for the new year and take time off for extended holiday seasons. This may also be a sign of increasingly selective targeting rather than a true drop in imposter activity as we also observed more attacks involving a single spoofed identity and a single attacked identity in an organization. We will continue to observe this data to determine whether this is an anomaly or a more significant adjustment.

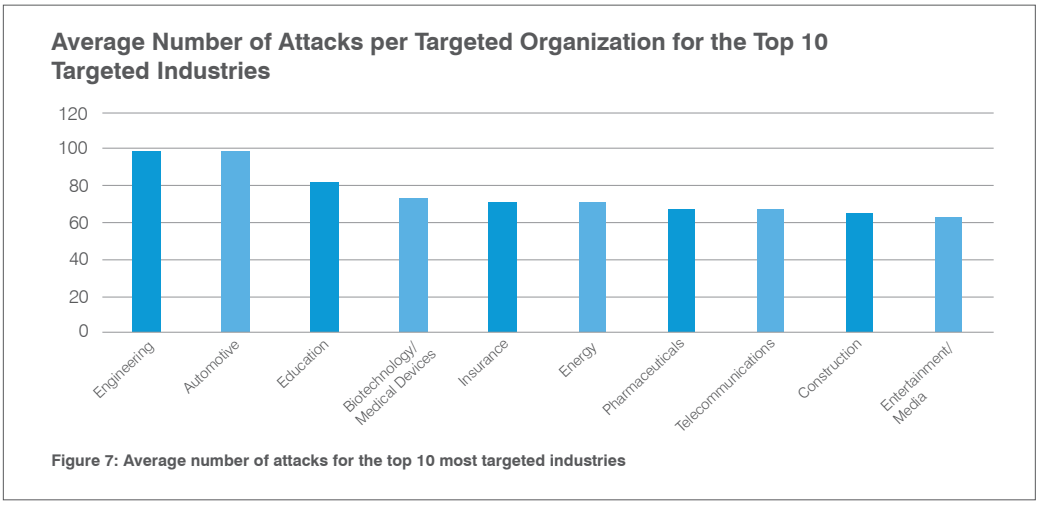

Figure 7: Average number of attacks for the top 10 most targeted industries

TOP-LEVEL DOMAIN
The portion of a domain name that follows the final "dot" such as .com, .net., .biz, etc.

Email fraud attackers continue to favor .com top-level domains **(TLDS)** in their sending addresses by a wide margin. These may include look-alike domains, spoofed domains or spoofed display names with underlying .com addresses, many of which are throwaway webmail addresses. The use of .com TLDs is up almost three percentage points from Q4 2018, with most other TLDs declining slightly. The top TLDs used in email fraud attacks in Q1 are shown in the table and chart below:

From address TLD	Percent of total TLD
com	69.29%
net	6.15%
de	3.15%
org	2.50%
lv	1.92%
mx	1.11%

From address TLD	Percent of total TLD
in	1.01%
me	0.87%
us	0.85%
biz	0.81%

Table 1: Top 10 top-level domains used in imposter messages

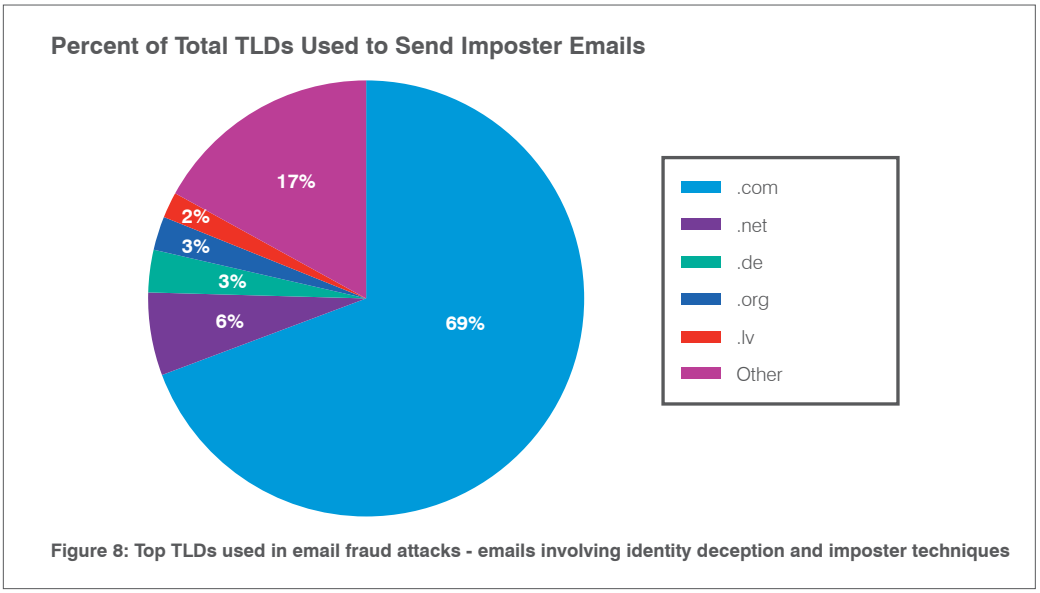

Figure 8: Top TLDs used in email fraud attacks - emails involving identity deception and imposter techniques

Subjects lines associated with these attacks also shifted from Q4, with "Payment" jumping over five percentage points to become the most common category. Conversely, "Other" dropped over six percentage points, falling to the second most common subject line category.

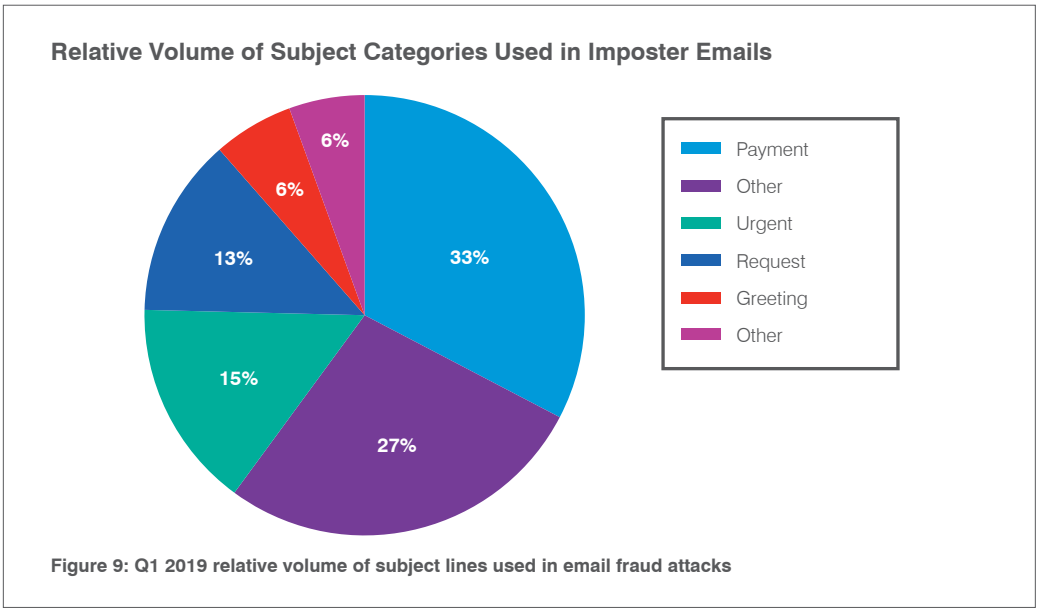

Figure 9: Q1 2019 relative volume of subject lines used in email fraud attacks

WEB-BASED THREATS: COINHIVE SHUTS DOWN, BUT ILLICIT CRYPTOCURRENCY MINING IS ALIVE AND WELL

Key statistic: Detected Coinhive samples spiked in late January to 4.9 times the weekly average for the quarter, but detected events dropped to near-zero after Coinhive shut down in March.

COINHIVE
A technology used to mine cryptocurrency by co-opting processing power on devices when surfers visit websites with the JavaScript software installed.

MODAL
A modal is an overlay on a web page that simulates the function of a pop-up without launching a new browser window.

Proofpoint researchers regularly track web-based threats including exploit kit (EK) activity, social engineering schemes and embedded cryptocurrency mining – also known as cryptojacking. While EK activity levels generally remain very low, web-based social attacks were up nearly 16 times from Q1 2018. **COINHIVE** and related cryptojacking activity dropped off dramatically after the service shut down during the last month of the quarter.

Social engineering attacks include fake antivirus and plugin updates that generally appear as **MODALS** on compromised websites or in malvertising. Such attacks were off from Q4 2018 levels by roughly 50%, reflecting what appears to be a seasonal trend: attack volumes grew rapidly each quarter of 2018 from their lowest levels in Q1. However, we detected nearly 16 times as many social engineering attacks in Q1 2019 as we did in Q1 2018, with relatively steady levels throughout the quarter (Figure 10). With exploit kits still operating at extremely low levels only in selected markets, web-based social engineering schemes remain the tool of choice for threat actors working via this vector.

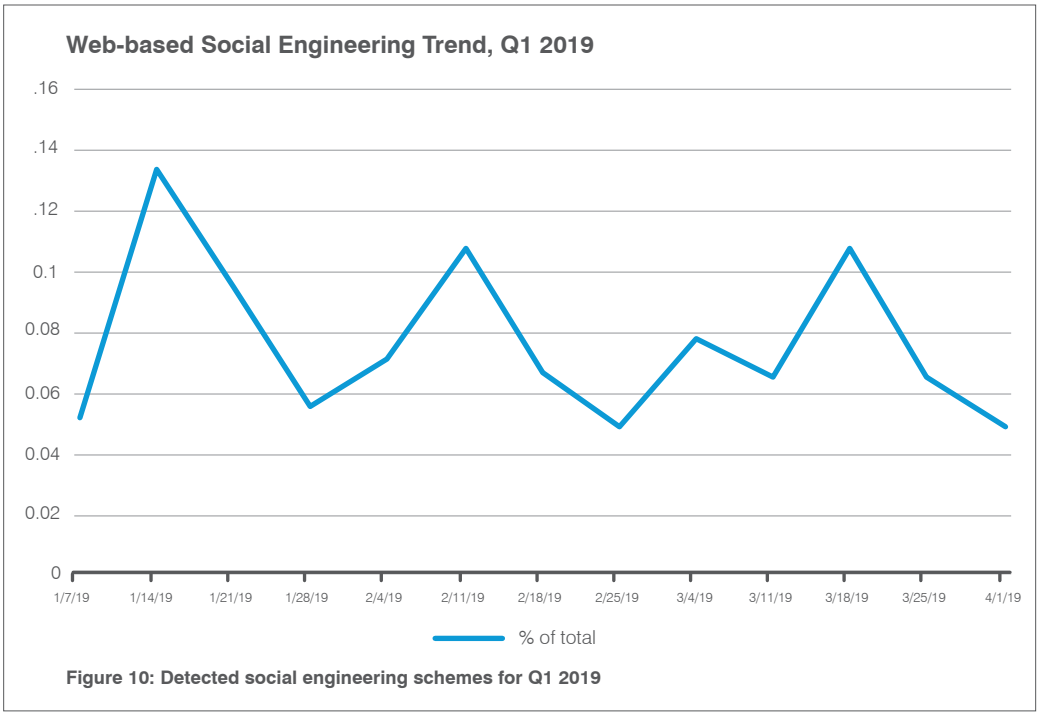

Figure 10: Detected social engineering schemes for Q1 2019

Coinhive saw a massive spike in activity at the end of 2018. We observed another spike, albeit much less pronounced relative to the quarterly average, in late January 2019, with the number of detected samples 4.9 times the weekly average. Detected events over the following two weeks were two to three times the weekly average.

However, Coinhive announced on February 26, 2019 that it would be shutting down due to a number of market factors, particularly the low value of Monero cryptocurrency and the scheduled hard fork of the currency that would make web-based mining far more difficult. As expected, we saw an abrupt decrease in Coinhive activity on the Proofpoint Emerging Threats worldwide sensor network following the March 8, 2019 shutdown, even as we continued to observe samples of the code in the wild (Figure 11).

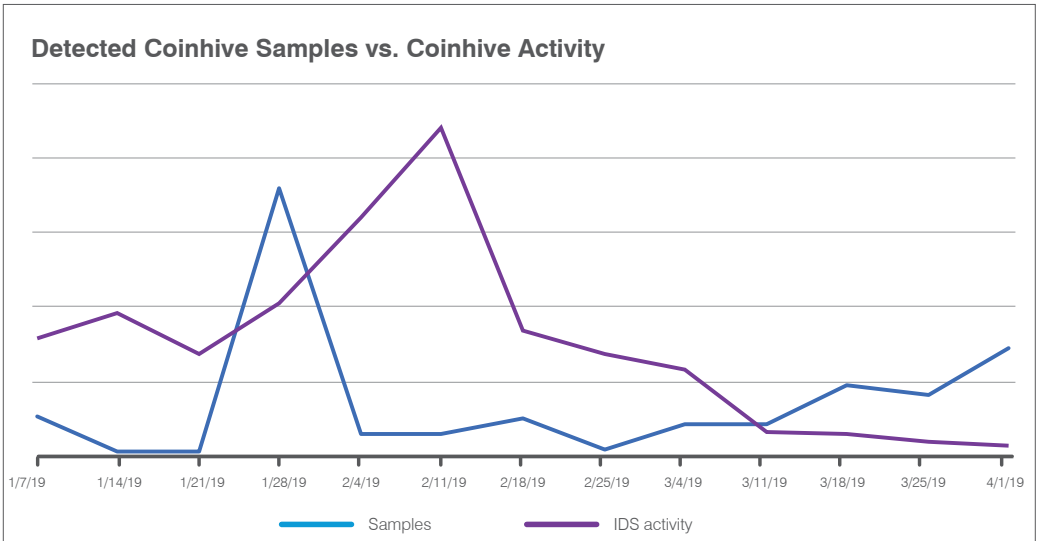

Figure 11: Indexed number of Coinhive sames detected vs. number of Coinhive events detected by IDS sensor network

Other malware and potentially abused services have stepped in to fill its place, despite the March 9 Monero fork. Threat actors continue to follow the money despite the ongoing volatility in cryptocurrency markets. Modifications to the Monero blockchain have not stopped cybercriminals from using illicit coin mining as an ongoing revenue stream, whether through installed malware or via cryptojacking.

DOMAIN THREATS: LOOK-ALIKES, FRAUDULENT HTTPS AND TRICKS ABOUND FOR CONSUMERS AND BUSINESSES

Key statistic: Over three times as many fraudulent domains had an SSL certificate as legitimate domains in Q1 2019.

Proofpoint researchers regularly scan hundreds of millions of domains for evidence of fraud and malicious intent. These domains may be used for phishing, BEC attacks, malware distribution and more. Throughout 2018 we noticed a few key trends that continued into the first quarter of 2019 and reinforce other findings around email fraud.

SSL CERTIFICATE
Small files that help cryptographically secure online transactions and data transmissions.

In particular, in 2018 fraudulent domains were 29% more likely to resolve to an IP address instead of simply being parked or generating a 404 error. The number that generated an HTTP response – for example, actually returning content of some sort – was 41% higher and, most significantly, over a quarter had an **SSL CERTIFICATE**. This is in contrast to just 6% of all domains that had such a certificate, which triggers the padlock icon in modern browsers. Web surfers have long been conditioned to associate this padlock with safety when, in fact, it is only a signal that outside actors cannot steal information being transmitted to a web server, even if that web server is controlled by a threat actor. It is also worth noting that a much smaller proportion of fraudulent domains had an associated Mail eXchange (MX) record, allowing them to send and receive email. The absence of an MX record creates a smaller footprint for threat actors and suggests that they are only likely to create an MX record if they are going to be used for sending spam or malicious mail. These findings are summarized in the table below.

Type of suspicious domain/ web property (2018)	% resolving to an IP address	% with an HTTP response	% with MX records	% with an SSL certificate
All domains	66%	53%	42%	6%
Fraudulent domains	95%	94%	16%	26%

Table 2: 2018 domain analysis

In Q1, by contrast, the individual differences varied but the trends remained clear:

Type of suspicious domain/ web property (Q1 2019)	% resolving to an IP address	% with an HTTP response	% with MX records	% with an SSL certificate
All domains	58%	38%	39%	6%
Fraudulent domains	84%	81%	32%	20%

Table 3: Q1 2019 domain analysis

Again, the MX records are noteworthy, as fraudulent domains appear to be coming in line with all domains, although it is not clear why threat actors are now more likely to create MX records for their domains.

As we noted with domains used in email fraud attacks, the .com TLD is by far the most commonly used. As the most trusted and widely recognized, it makes sense that threat actors would gravitate towards the TLD for their new registrations. The top 10 TLDs for fraudulent domains are shown below. Note that .xn--p1ai is the Unicode equivalent of .ru in Cyrillic (.РФ).

TLD	Percentage of total fraudulent domains
.com	39.4694893
.xn--p1ai	6.77803992
.co.uk	4.14461519
.fr	4.09360454
.net	2.83109099
.dev	2.82471466
.xyz	2.79920933
.online	2.78008034
.ru	2.09143659
.org	2.07868393

Table 4: Top 10 top-level domains appearing in fraudulent domains.

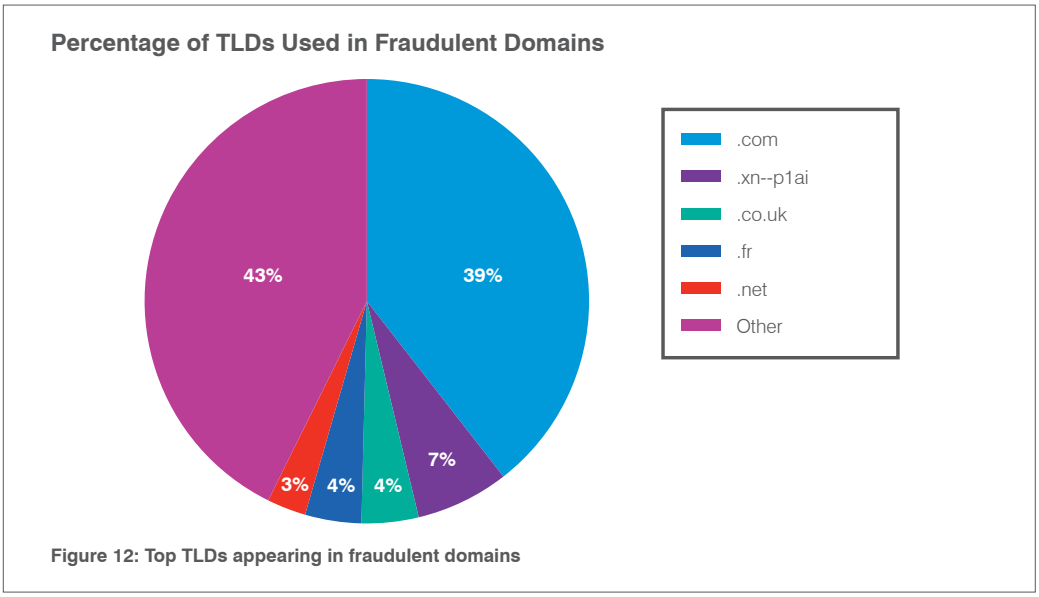

Figure 12: Top TLDs appearing in fraudulent domains

Look-alike domain registrations (example: proofp0int.com instead of proofpoint.com) also increased quickly through the quarter, with March registrations almost 50% greater than those recorded in either January or February.

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. Leverage a solution that identifies and quarantines both inbound email threats targeting employees and outbound threats targeting customers before they reach the inbox.

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

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

Partner with a threat intelligence vendor. Smaller, more targeted attacks call for sophisticated threat intelligence. Leverage a solution that combines static and dynamic techniques to detect new attack tools, tactics and targets 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) is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 100, rely on Proofpoint to mitigate their most critical security and compliance risks across email, the cloud, social media, and the web. No one protects people, the data they create, and the digital channels they use more effectively than Proofpoint.