QUARTERLY REPORT

proofpoint.

QUARTERLY

THREAT REPORT

Q4 2018

proofpoint.com

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 cyber attacks.

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

TABLE OF CONTENTS

KEY TAKEAWAYS: BEC GROWTH CONTINUES, WHILE RANSOMWARE HAS GIVEN WAY TO STRAIGHT EXTORTION FOR Q4

Below are key takeaways from the fourth quarter of 2018.

EMAIL

- Banking Trojans remain the top email-borne threat in Q4, making up 56% of all malicious payloads in Q4; Emotet comprised 76% of all banking Trojan payloads.
- Remote access Trojans accounted for 8.4% of all malicious payloads in Q4 and 5.2% for the year, marking a significant change from previous years in which they were rarely used by crimeware actors.
- Ransomware dropped even further in Q4 to just one tenth of 1% of overall malicious message volume.
- Malicious messages bearing credential stealers or downloaders collectively jumped more than 230% year over year
- Email fraud, also known as BEC, continued its dramatic growth. The number of email fraud attacks against targeted companies increased 226% QoQ and 476% vs. Q4 2017.

THE NUMBER OF EMAIL FRAUD ATTACKS AGAINST **TARGETED COMPANIES INCREASED 226%** QOQ AND **476% VS. Q4 2017.**

WEB-BASED ATTACKS

- Coinhive activity spiked to 23 times the average for the year for two weeks in December; overall, Coinhive activity continued to grow slowly aside from this spike.
- In Q4, we still observed a 150% increase in social engineering detections on our worldwide network of IDS sensors; while this is a slower growth rate than observed in previous quarters, it continues to demonstrate a trend towards social engineering even as EK activity has remained low.

SOCIAL MEDIA

- Fraudulent social media support account phishing, or ”angler phishing,” has increased 442% year over year
- Phishing links on social channels continue to drop as platforms address this issue algorithmically.

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: MALICIOUS URLS DELIVER BANKERS IN DROVES, WHILE NON-MALWARE THREATS GROW

Key stat: Messages leveraging malicious URLs outnumbered malicious attachments by roughly 2:1 for Q4 and 3:1 for the entire year.

Email remains the top vector for malware distribution and phishing, while email fraud, also known as BEC, continues to grow rapidly, with threat actors adapting tools and techniques across attack types to best capitalize on a range of vulnerabilities.

As shown in Figure 1, malicious URLs continued to outnumber malicious attachments in email campaigns delivering malware throughout Q4. Proofpoint observed over twice as many URL messages as attachment messages during this period, although this constituted a decrease from 2018 as a whole. For the entire year, malicious URLs appeared over three times as often as messages with malicious attachments (Figure 2), suggesting that the pendulum may be swinging back toward attachments as it tends to do periodically.

Indexed Daily Malicious Message Volume by Attack Type, Q4 2018

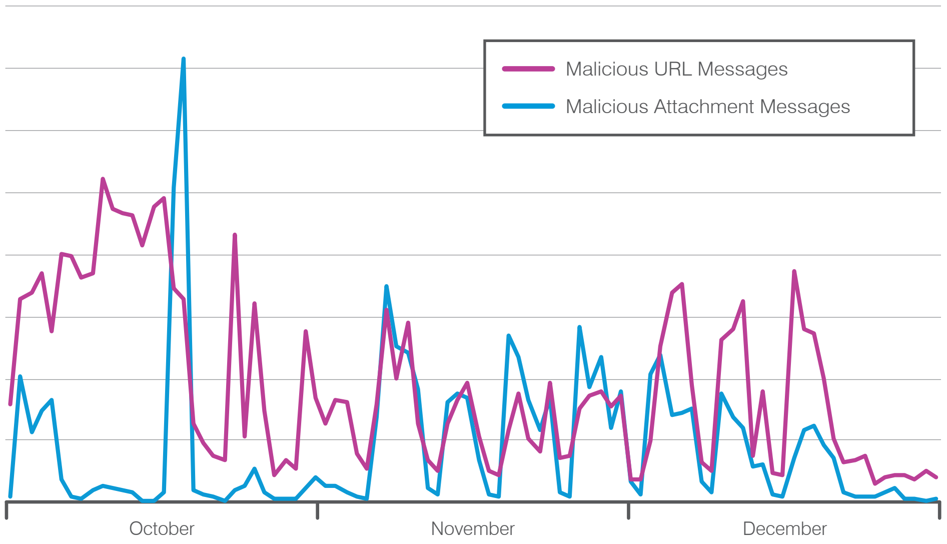


Figure 1: Indexed daily attack type trend, October-December 2018

Overall, Q4 was characterized by more even distribution of attack types, with some notable disparities throughout October.

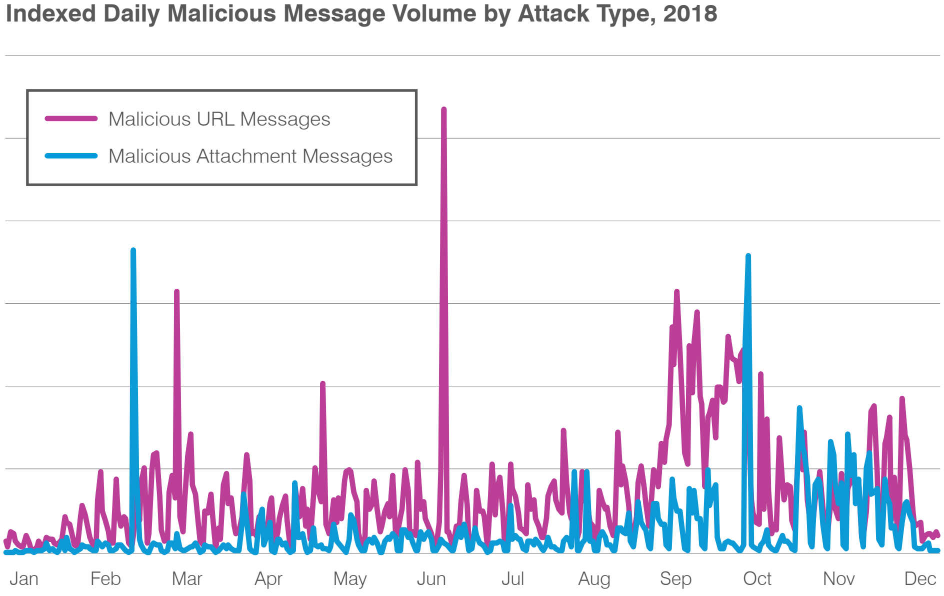


Figure 2: Indexed daily attack type trend, 2018

RANSOMWARE

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

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.

While differences in attack types moderated as the quarter progressed and frequently shift from year to year, the relative mix of malware families looked very different from 2017 and even from the third quarter of 2018. **RANSOMWARE** was virtually absent, while dramatic fourth quarter increases in banking Trojans, **REMOTE ACCESS TROJANS** and "other" malware like keyloggers compensated for drops in credential stealers and downloaders.

In particular, as shown in Figure 3, RATs, once a small proportion of the overall crimeware landscape, went mainstream in 2018, with sophisticated, prolific actors driving volumes to over 8% of all malicious payloads. At the same time, banking Trojans, stealers and downloaders together accounted for over 90% of all initial payloads in Q4.

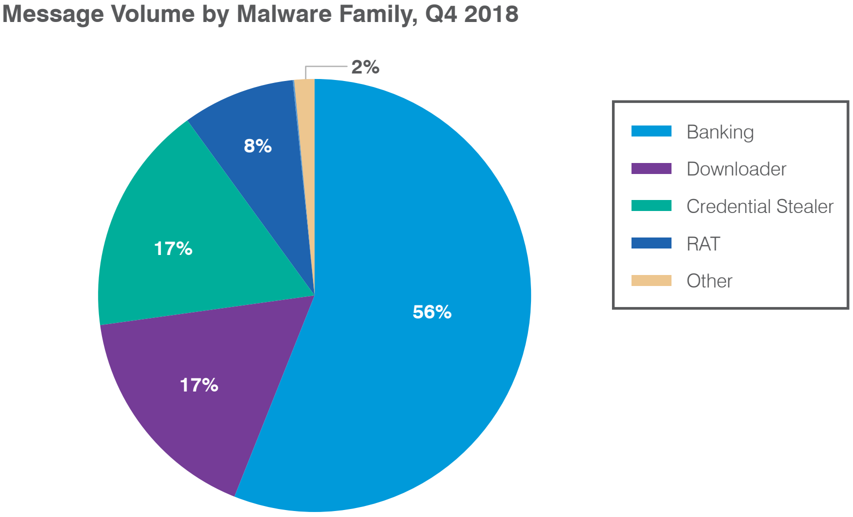


Figure 3: Relative mix of malware payloads in email by category, Q4 2018

Figure 4 illustrates how the relative mix of malicious payloads has changed throughout 2018. While each quarter experienced variability, the basic formula remained the same, with bankers, downloaders and credential stealers comprising a minimum of 85% of initial payloads.

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

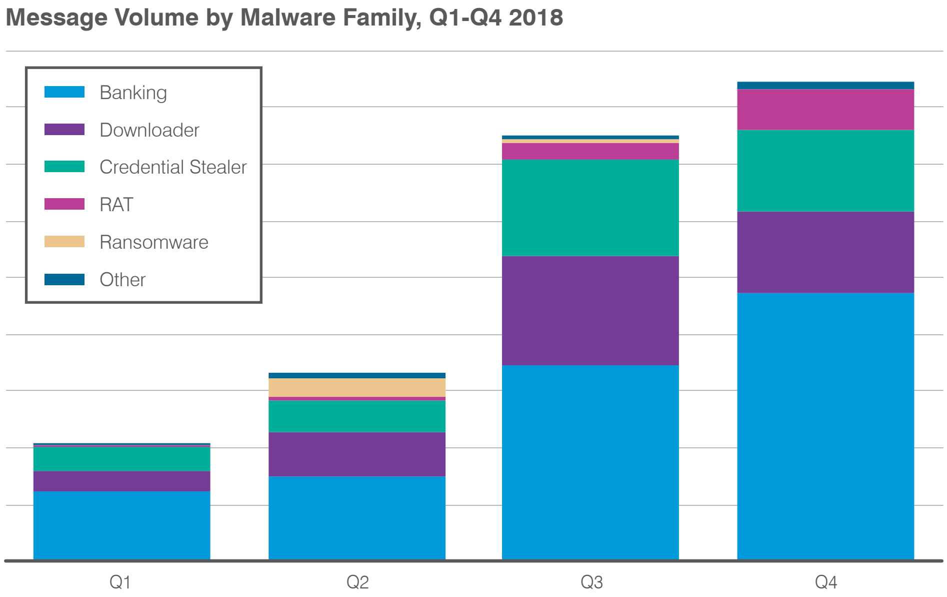


Figure 4: Relative mix of malware payloads in email by category and quarter, 2018

EMOTET DOMINATES THE BANKING TROJAN LANDSCAPE

Key stat: Banking Trojans made up 56% of all malicious payloads in Q4; of those, 76% were Emotet.

EMOTET
Emotet is a banking Trojan that peaked in distribution in Q4 2018 with modules for direct theft from victim bank accounts, information theft, DDoS and more.

Banking Trojans have been the dominant malware family appearing in malicious email campaigns throughout 2018. Although Panda Banker appeared in multiple relatively large campaigns in October, **EMOTET** predominated for the remainder of the month, as it has for much of 2018. Banking Trojans are increasingly versatile tools employed by threat actors for delivering secondary payloads, mining cryptocurrency and collecting a range of user data beyond the banking credentials often associated with this type of malware.

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.

> For the purposes of this report and for consistency with volume metrics throughout 2018, we are treating Emotet as a banking Trojan. However, its capabilities continue to evolve, and the malware is more appropriately classified as a **BOTNET**, with extensive capabilities for downloading additional payloads, exfiltrating data, performing coordinated actions and more.

As we observed in Q3, despite the presence of a range of banking Trojans appearing in the wild, threat actors continue to coalesce around known malware. Taken together, Emotet, Panda Banker and Ursnif comprised almost 97% of observed banking Trojans in Q4. Figure 5 shows that Emotet traffic, while far more consistent and appearing in higher volumes than other bankers in Q4, was quiet for most of October; the actor primarily responsible for high-volume Emotet campaigns was also inactive for most of April. Aside from these two periods, however, Emotet steadily increased in the volume and frequency of associated email campaigns throughout 2018.

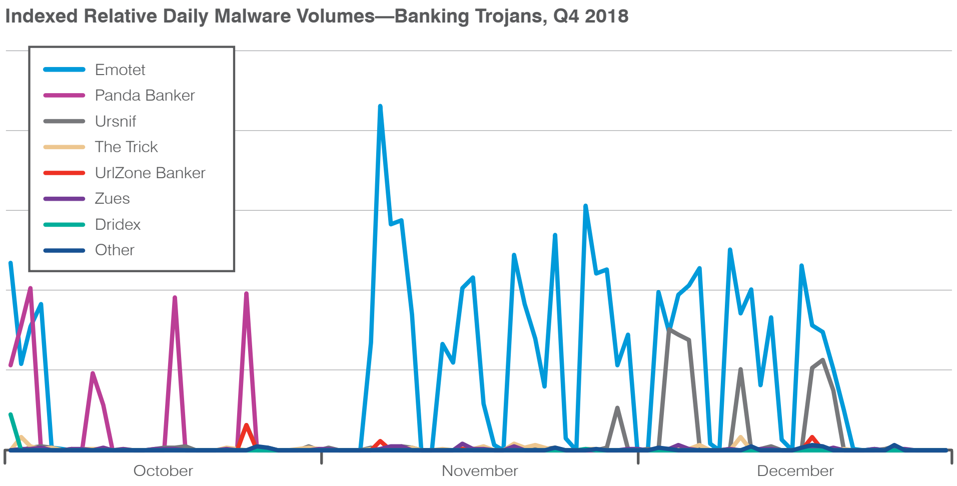


Figure 5: Indexed relative daily banking Trojan message volume, Q4 2018

THE TRICK

A banking Trojan originally seen primarily in Australia, The Trick became a global threat when TA505 began distributing the malware at scale in 2017.

Figure 6 spotlights the shifts we regularly observe in the threat landscape. In Q4 2017, **THE TRICK** represented 84% of all banking Trojan payloads. One year later, The Trick appeared in just 1% of malicious email campaigns bearing bankers.

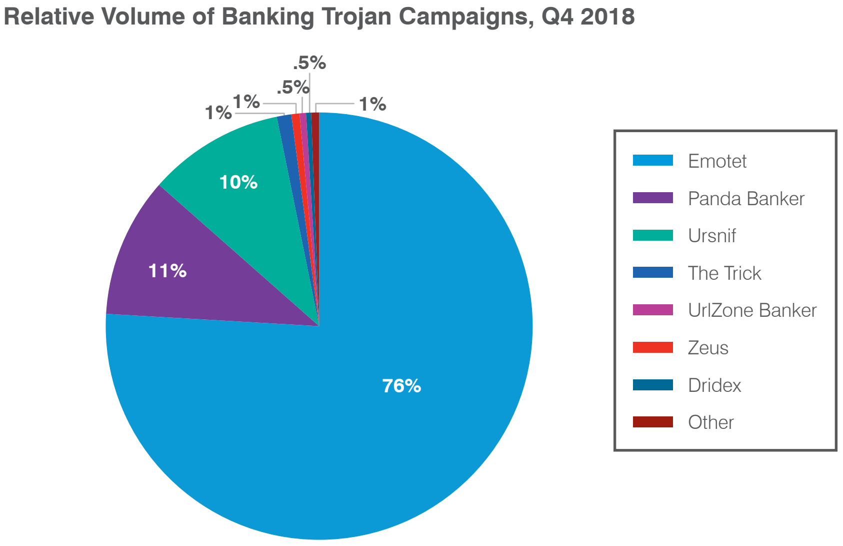


Figure 6: Relative mix of banking Trojan message volumes, Q4 2018

DIRECT EXTORTION SCAMS: WHY DISTRIBUTE RANSOMWARE WHEN YOU CAN JUST TRICK VICTIMS INTO GIVING YOU MONEY?

After dominating the threat landscape in 2016 and much of 2017, ransomware nearly disappeared in Q1 2018. In Q2, we observed a return of ransomware, albeit at much lower levels than we saw in 2017. However, this spike appeared to be a "testing of the waters," since ransomware message volumes dropped by 10 percentage points from Q2. This suggests that ransomware campaigns did not generate sufficient returns for threat actors to continue distributing them at scale. Ransomware dropped even further in Q4 to just one tenth of 1% of overall malicious message volume.

As shown in Figure 7, only three ransomware strains appeared in relatively small, sporadic email campaigns in Q4.

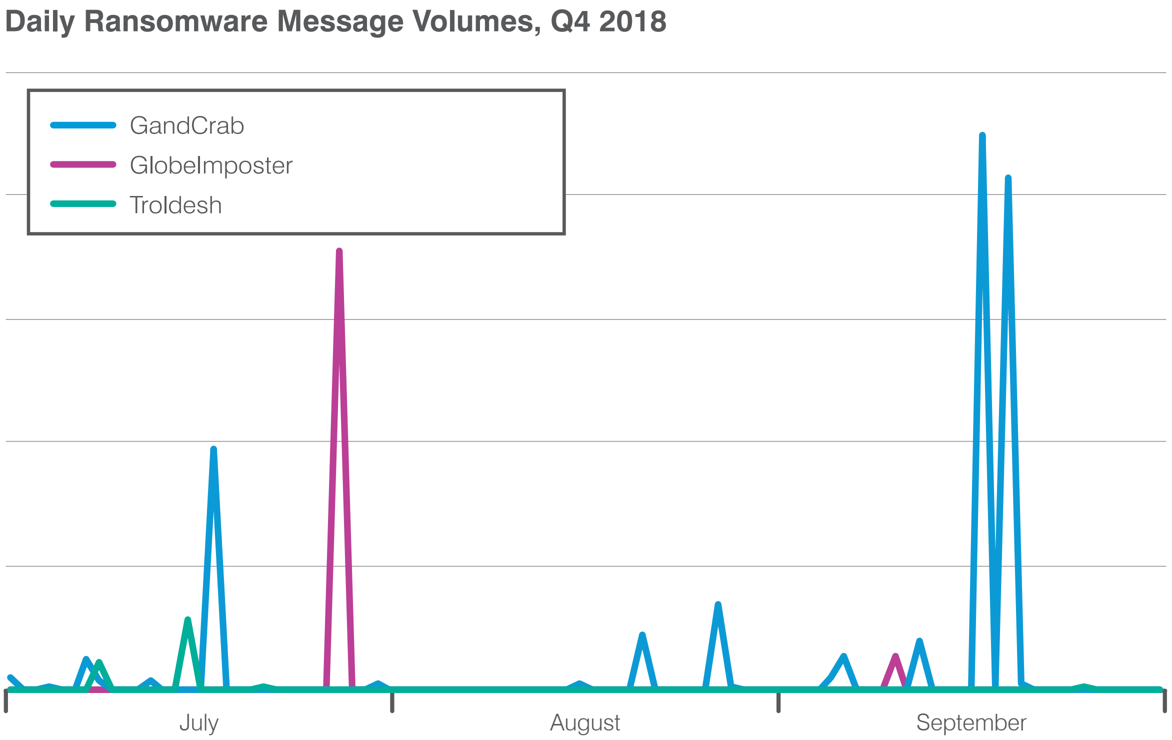

Daily Ransomware Message Volumes, Q4 2018

Figure 7: Relative volume of malicious messages bearing ransomware as their primary payloads, Q4 2018

However, even as ransomware waned, we observed a new threat become increasingly common: direct extortion. These campaigns may take the form of so-called "sextortion" or some other form of blackmail in which actors threaten to reveal compromising information or take destructive action if the victim does not pay a fee. With **rare exceptions**, these emails do not contain malware or malicious links and rely on the human factor to trick recipients. Often, the threatening emails include "evidence" of compromise, such as an old password that the actor may have obtained from a data breach or simply guessed.

Regardless of the particular scenario, it appears that threat actors have discovered that it is easier and less expensive to attempt to extort payments directly from victims rather than to distribute ransomware.

RATS INFEST THE THREAT LANDSCAPE

Key stat: Remote access Trojans comprised 8.4% of all malicious payloads in Q4 and 5.2% for the year.

Remote access Trojans rarely appeared in the consumer and enterprise landscapes prior to 2018. In Q4 2017, for example, RATs comprised just 0.04% of all observed malicious payloads in email. While banking Trojans and other commodity malware continue to dominate, RATs are noteworthy for their power and versatility for threat actors who can use them as everything from simple downloaders to tools for completely controlling and exfiltrating all of the data from a device.

TA505, one of the most prolific actors we track, has been distributing RATs such as **FLAWEDAMMYY**, **FLAWEDGRACE** and RMS RAT at scale since March 2018. Figure 8 shows that, while FlawedAmmyy has been the dominant strain of RAT appearing in malicious emails, several other RATs are also in circulation.

FLAWEDAMMYY
A RAT based on leaked source code from the legitimate AmmyyAdmin remote administration tool.

FLAWEDGRACE
A robust RAT first observed in the wild in Q4 2018.

Breakdown of Relative RAT Volume, Q4 2018

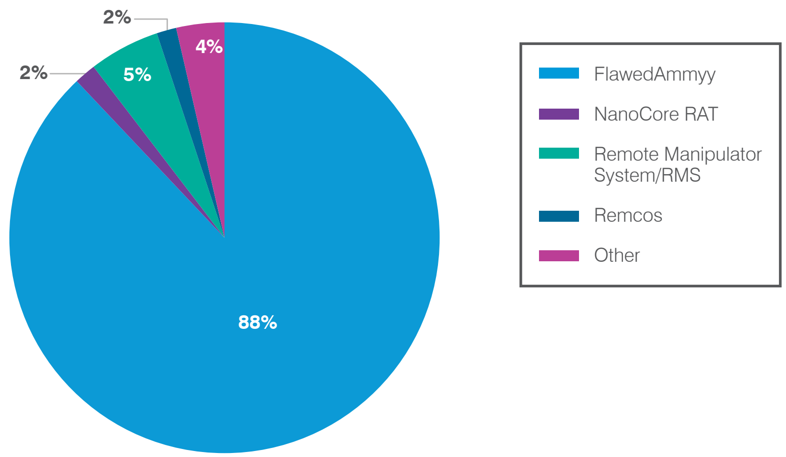


Figure 8: Indexed relative volume of malicious messages bearing RATs as their primary payloads, Q4 2018

It remains to be seen how threat actors will monetize the growing number of devices infected with RATs, but the proportion of malicious messages bearing this malware family has roughly doubled each quarter of 2018. Threat actors follow the money, meaning that they would not be increasing distribution of RATs without achieving a return on their investments in malware, command and control, and sending infrastructure.

BEST SUPPORTING MALWARE: DOWNLOADERS, STEALERS AND BACKDOORS

Key stat: Malicious messages bearing credential stealers and downloaders both jumped over 230% year over year.

Malware Family	Q1 2017	Q2 2017	Q3 2017	Q4 2017	FY 2017	Q1 2018	Q2 2018	Q3 2018	Q4 2018	FY 2018	QoQ	YoY
Credential Stealer	16.40%	6.33%	5.19%	3.63%	5.75%	19.21%	17.22%	22.66%	17.18%	19.31%	-24.17%	235.78%
Downloader	26.13%	5.43%	5.95%	3.04%	6.20%	18.14%	23.05%	25.55%	16.77%	20.96%	-34.36%	238.06%

PERSISTENCE
This refers to the ability of a piece of malware to remain installed on a device, generally without detection.

Throughout 2018, we observed the introduction of several new downloaders and stealers such as **Marap**, **Advisorsbot** and **Cobint**, as well as increased development and distribution of existing strains like **AZORult**. As with the RATs described above, this appears to be part of a broader trend toward malware infections focused on long-term **PERSISTENCE** and ongoing exploitation of infected systems.

Figure 9 shows daily message volumes for credential stealers and downloaders during Q4. While overall volumes of credential stealers and downloaders were down 24% and 34%, respectively, for the quarter, they were up over 230% vs. 2017 volumes.

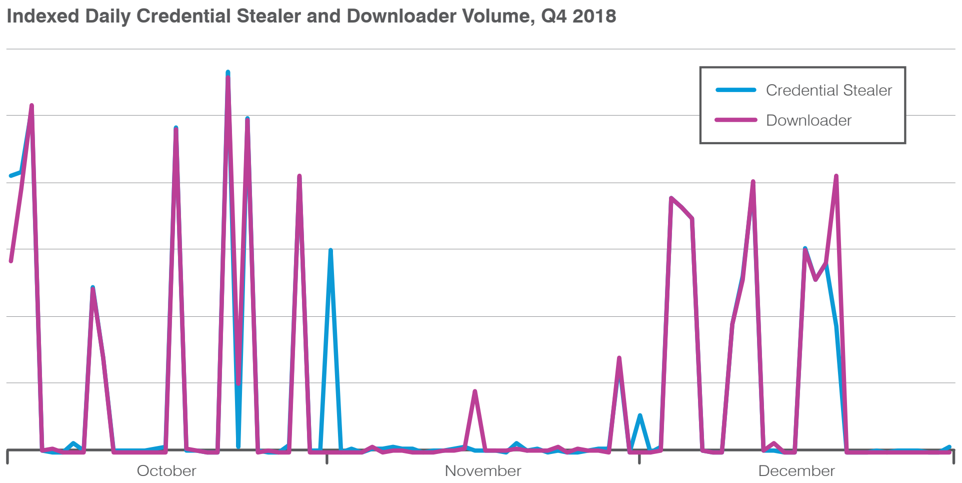


Figure 9: Indexed relative volume of malicious messages bearing downloaders or information stealers as their primary payloads, Q4 2018

Moreover, in a number of cases we observed Emotet, a robust banking Trojan, being used as a downloader. Near the end of Q4, we observed a new, stripped down version of the **ServHelper** backdoor emerge with most functions removed—except those used to download secondary payloads.

Again, it appears that threat actors were increasingly focused on the ability to compromise devices and remain resident for extended periods without detection. This is unlike the highly destructive ransomware that characterized so many campaigns in 2016 and 2017.

EMAIL FRAUD THREATS: Q4 SEES EXPLOSIVE GROWTH IN BEC-STYLE ATTACKS

Key stat: The number of email fraud attacks against targeted companies increased 226% QoQ and 476% vs. Q4 2017.

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 (BEC), remains far more targeted and far lower volume than the large-scale phishing attacks we observe every day. However, Q4 saw a massive increase in email fraud volumes as well as the number of attacks per targeted organization. On average, companies targeted by BEC received about 120 fraudulent emails in the fourth quarter of the year, up from 36 in Q3 2018 and up from 21 in the year-ago quarter.

These represent 226% and 476% increases respectively, across all industries and in companies of all sizes. As we have regularly observed, email fraud attack rates do not vary by the size of the targeted organization. However, the rates do vary by industry. Figure 10 shows increases in BEC-style attack rates for the most-targeted industries in Q4.

NOTABLY, **60% OF COMPANIES SAW THEIR OWN DOMAINS SPOOFED** BY EMAIL FRAUD ACTORS, AN **INCREASE OF ALMOST 10 PERCENTAGE POINTS** FROM THE PREVIOUS QUARTER.

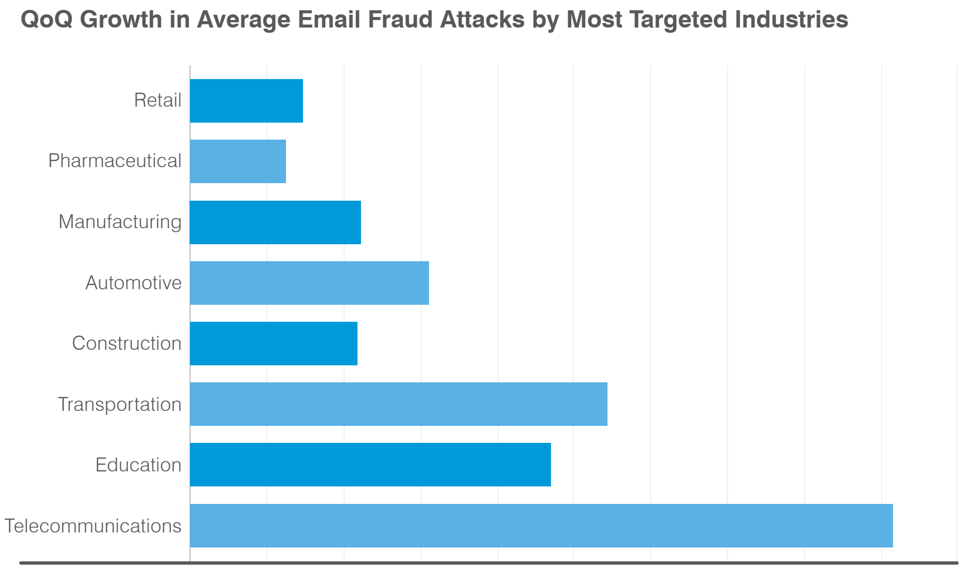


Figure 10: Increases in average email fraud attack rates between Q3 and Q4 2018 for the most attacked industries

As we noted in Q3 2018, email fraud has shifted towards a "many-to-many" challenge: attackers spoof many identities to target many people within the organizations; 59% of attacks followed this pattern in Q4. Notably, 60% of companies saw their own domains spoofed by email fraud actors, an increase of almost 10 percentage points from the previous quarter.

WEB-BASED THREATS: COINHIVE GOES OFF THE CHARTS AT THE END OF 2018

Key stat: Coinhive activity spiked to 23 times the average for the year for two weeks in December.

Web-based threats we track include **EXPLOIT KIT (EK)** activity, social engineering schemes and embedded cryptocurrency mining on the web. Aside from minor spikes in activity associated with RIG EK, exploit kits remain steady at the same low levels we have observed for the last two years. Social engineering attacks on the web continue to represent a far more pervasive threat. These types of attacks present web surfers with fake antivirus notifications and fake software updates that lead to malware downloads, phishing landing pages and more. While growth rates for these types of web-based threats have moderated in Q4, we still observed a 150% increase in social engineering detections on our worldwide network of **IDS** sensors. The steep drop at the end of December may be a seasonal trend and bears further observation in 2019.

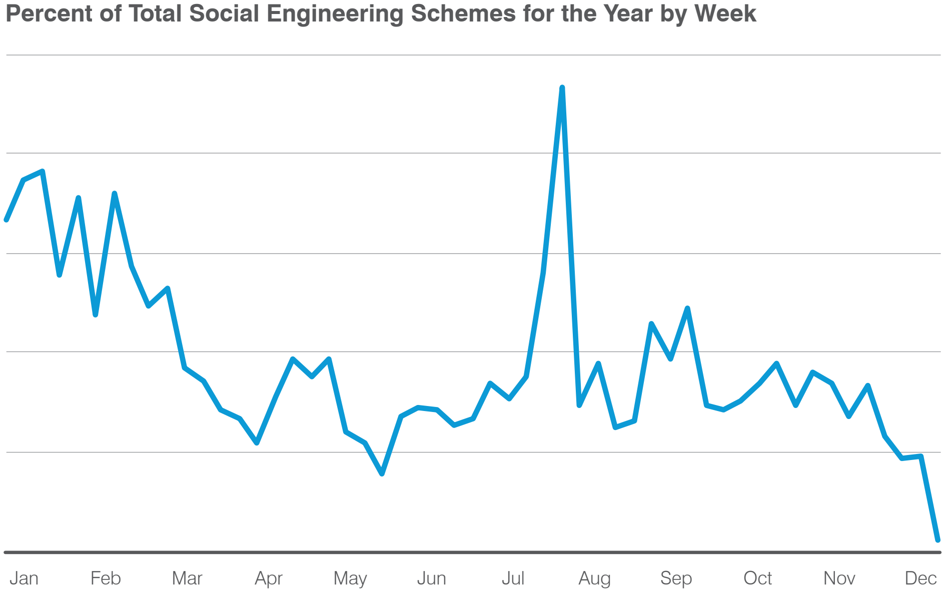


Figure 11: Indexed IDS events related to social engineering schemes for 2018

Coinhive, a technology used to mine cryptocurrency by co-opting processing power on devices when surfers visit websites with the JavaScript software installed, has also continued to increase in adoption and associated traffic throughout the quarter. As shown in Figure 12, though, Coinhive activity jumped dramatically at the end of Q4, increasing to 23 times the average for the year. Again, we will continue to observe this trend to determine if this is a seasonal spike. However, interest in Coinhive remains strong despite ongoing volatility in the cryptocurrency market.

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.

EXPLOIT KIT (EK)

This is an attack vector in which compromised web pages can be used to directly load malware on a vulnerable device; EK activity has largely given way to social engineering after reaching epidemic proportions in the middle of the decade.

IDS

An intrusion detection system, or IDS, operates at the network's edge to report potentially malicious activity such as malware check-ins or penetration attempts.

Percentage of Total Coinhive Samples Detected by Week, 2018

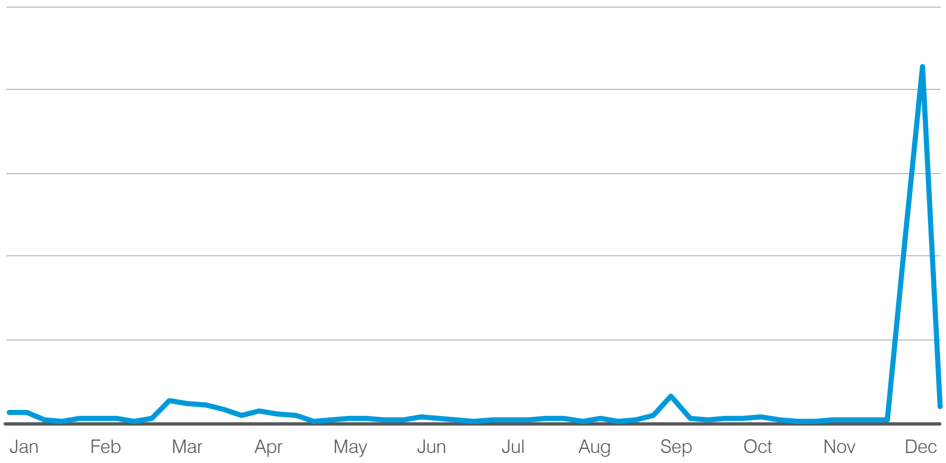


Figure 12: Coinhive events, 2018, shown as a percent of total observed samples

SOCIAL MEDIA THREATS: SUPPORT FRAUD CONTINUES TO GROW AS PLATFORMS CLAMP DOWN ON PHISHING LINKS

Key stat: Angler Phishing has increased 442% year over year.

Social media channels remain key vectors for fraud and theft. While the platforms themselves continue to develop automated protections, **SOCIAL MEDIA SUPPORT FRAUD** remains a key challenge for consumers and the brands with which they interact.

In Q4, suspected support fraud—also known as “angler phishing”—accounts increased by about 40% over the previous quarter. As shown in Figure 13, accounts potentially associated with support fraud phishing, in which threat actors insert themselves into legitimate interactions between consumers and brands, increased 40% from the previous quarter. Over the course of 2018, angler phishing accounts have increased by over 500%.

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 SUPPORT FRAUD

This a type of phishing in which attackers attempt to insert themselves in legitimate conversations between consumers and brand-owned social media accounts.

Cumulative QoQ Increases in Support Fraud Accounts

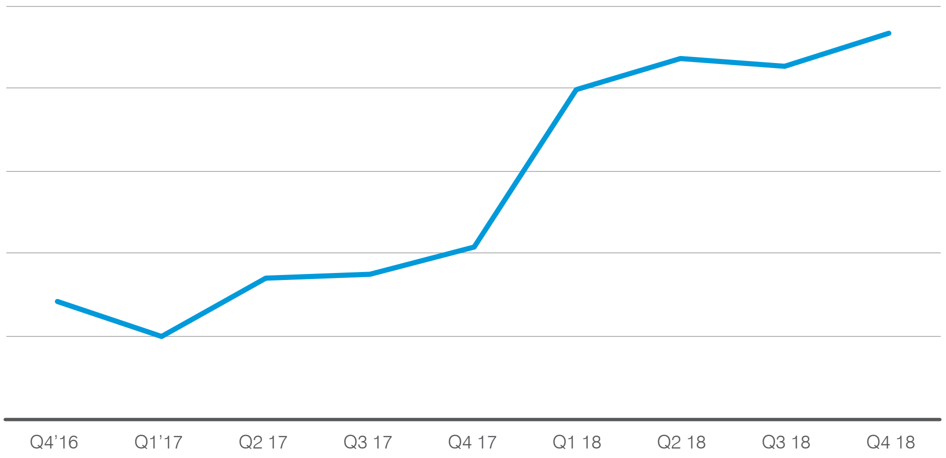


Figure 13: Cumulative change by quarter in observed support fraud accounts

PROOFPOINT RECOMMENDATIONS

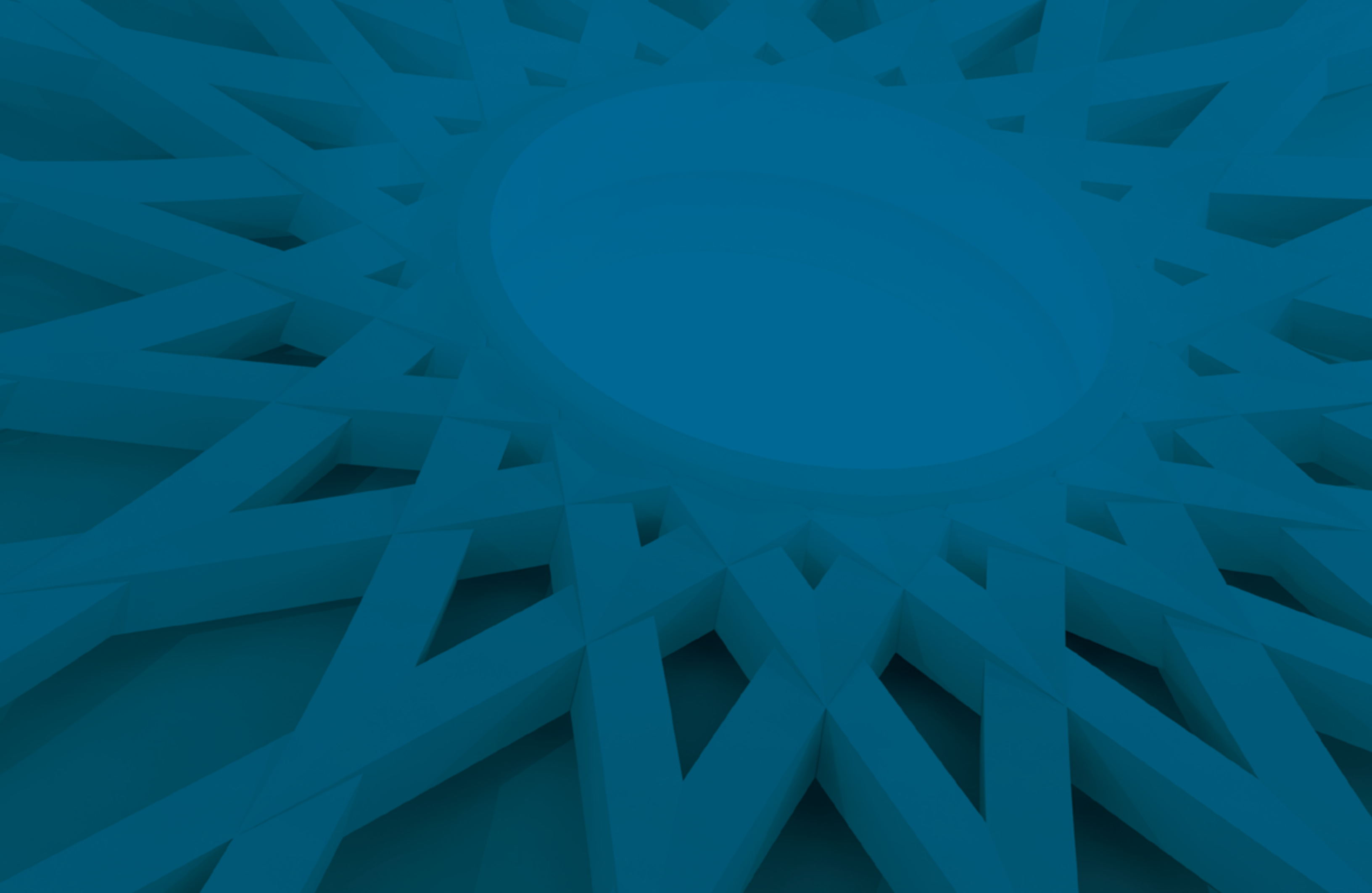
This report provides insight into the shifting threat landscape that can inform your cybersecurity strategy. Here are our top recommendations for how you can protect your company and brand in the coming months.

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.