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 ................................................................. 4

Email ..................................................................................................................................................... 4
Web-Based Attacks .................................................................................................................................. 4
Social Media ........................................................................................................................................... 4

Email-based threat trends: Malicious URLs deliver bankers in droves, while non-malware threats grow ............................................................................................................................... 5

Emotet dominates the banking Trojan landscape ............................................................................ 7
Direct extortion scams: Why distribute ransomware when you can just trick victims into giving you money?................................................. 9
RATs infest the threat landscape ........................................................................................................ 10
Best supporting malware: Downloaders, stealers and backdoors ...................................................... 11
Email fraud threats: Q4 sees explosive growth in BEC-style attacks .............................................. 12

Web-based threats: Coinhive goes off the charts at the end of 2018 ............................................. 13

Social media threats: Support fraud continues to grow as platforms clamp down on phishing links ................................................................................................................................. 14

Proofpoint recommendations ........................................................................................................... 15
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.

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.
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.

**WHY WE TRACK THIS**

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.

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

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

**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.

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.

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.
**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.
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.

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.

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.

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

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.

```plaintext
<table>
<thead>
<tr>
<th>Malware Family</th>
<th>Q1 2017</th>
<th>Q2 2017</th>
<th>Q3 2017</th>
<th>Q4 2017</th>
<th>FY 2017</th>
<th>Q1 2018</th>
<th>Q2 2018</th>
<th>Q3 2018</th>
<th>Q4 2018</th>
<th>FY 2018</th>
<th>QoQ</th>
<th>YoY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential Stealer</td>
<td>16.40%</td>
<td>6.33%</td>
<td>5.19%</td>
<td>3.63%</td>
<td>5.75%</td>
<td>19.21%</td>
<td>17.22%</td>
<td>22.66%</td>
<td>17.18%</td>
<td>19.31%</td>
<td>-24.17%</td>
<td>235.78%</td>
</tr>
<tr>
<td>Downloader</td>
<td>26.13%</td>
<td>5.43%</td>
<td>5.95%</td>
<td>3.04%</td>
<td>6.20%</td>
<td>18.14%</td>
<td>23.05%</td>
<td>25.55%</td>
<td>16.77%</td>
<td>20.96%</td>
<td>-34.36%</td>
<td>238.06%</td>
</tr>
</tbody>
</table>
```

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.

**PERSISTENCE**

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

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.

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.
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.
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