proofpoint

QUARTERLY

THREAT REPORT

Q3 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 brand.

TABLE OF CONTENTS

KEY TAKEAWAYS: FROM BANKERS TO SOCIAL ENGINEERING SCHEMES, ACTORS DOUBLE DOWN FOR Q3

Below are key takeaways from the third quarter of 2018.

EMAIL

- Banking Trojans, downloaders and credential stealers made up 94% of malicious payloads. Ransomware dropped to less than 1% of all email-borne payloads, while remote access Trojans (RATs) doubled their presence from Q2, making up 4% of all malicious payloads in email.
- The pendulum of malware delivery mechanisms in email continued to swing towards URLs; malicious URLs outnumbered attachments like macro-laden documents by over 370%. However, many of these malicious URLs led to macro documents themselves.
- While new malware often makes headlines, corporate credential phishing via email increased over 300% between Q2 and Q3 2018.
- The number of email fraud attacks per targeted organization increased 77% over Q3 2017. While the frequency of attacks and the number of individuals targeted per organization both continue to increase, the number of identities spoofed in these attacks decreased significantly as email fraud actors doubled down on leveraging high-profile identities.

WHILE NEW MALWARE OFTEN MAKES HEADLINES, CORPORATE CREDENTIAL **PHISHING VIA EMAIL INCREASED OVER 300%** BETWEEN Q2 AND Q3 2018

WEB-BASED ATTACKS

- Web-based threats have shifted almost entirely away from exploit kits to social engineering schemes, with fake antivirus and bogus plugins appearing more than twice as often as in Q2 and over 20 times as often as in Q1.
- The total incidence of Coinhive-based cryptojacking held steady between Q2 and Q3, with the number of detected events in both quarters roughly six times that of Q1.
- Despite a brief spike in Neutrino EK activity in August, overall exploit kit activity held steady at a small fraction of its 2016 peak. Of this remaining activity, Neutrino and RIG EK accounted for 85% of total EK traffic for the quarter.

SOCIAL MEDIA

- Social media platforms continue to excel at combating phishing links; phishing links have decreased 90% vs. Q3 2017.
- Social media support fraud, also known as “angler phishing,” however, reached its highest level ever in September. Overall, this type of phishing increased 486% compared to Q3 2017.

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: BANKING TROJANS LEAD THE WAY AS DOWNLOADERS GET STEALTHIER AND PHISHING EXPLODES

Key stat: Corporate credential phishing increased over 300% between Q2 and Q3 2018.

Email remains the top vector for malware distribution and phishing. 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.

In particular, we regularly observe pendulum swings between the general use of URLs and distribution of malicious attachments in email. As shown in Figures 1 and 2, threat actors have favored URLs throughout 2018. In Q3, malicious URLs outnumbered attachments by over 370%. It is worth noting that many of these URLs campaigns were driven by large campaigns from established actors, many of which used URLs that led to malicious macro documents.

While September appears to show a substantial spike in malicious URLs, the increase was accompanied by a proportional increase in malicious attachment messages. Overall, malicious message volumes in September exceeded total volumes for all of Q1, with both high-frequency and high-volume campaigns appearing regularly.

Indexed Daily Malicious Message Volume by Attack Type, Q3 2018

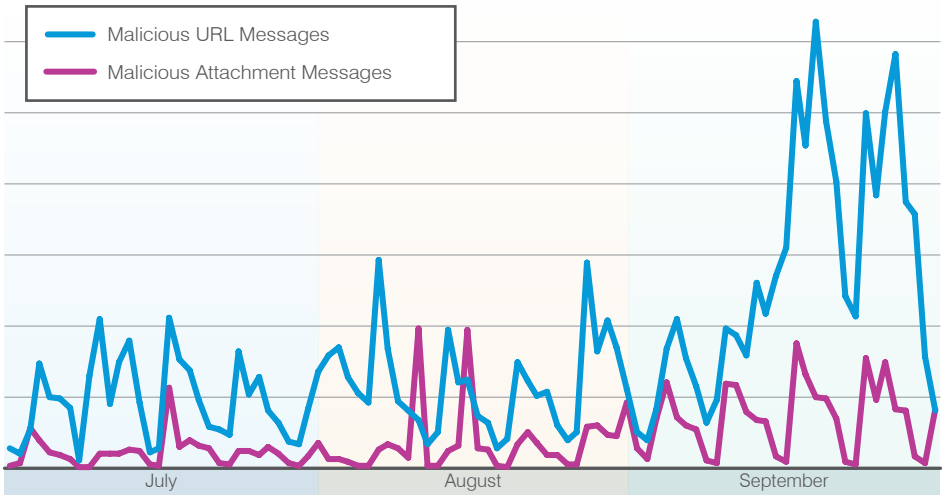

Figure 1: Indexed daily attack type trend, July-September 2018

While it remains to be seen whether the September volume increases represent a trend, a seasonal spike, or another anomalous condition, Figure 2 shows that the disparity between URLs and attachments has been present for most of 2018. On average this year, URLs have exceeded malicious attachments by almost 380%.

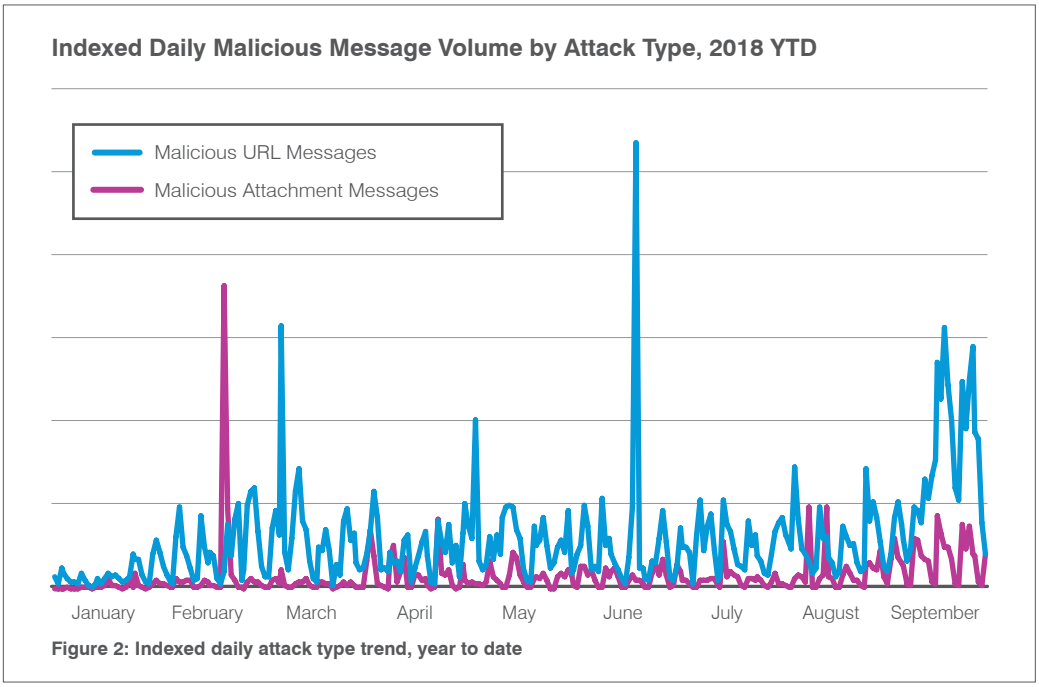

Figure 2: Indexed daily attack type trend, year to date

Regardless of delivery method—malicious attachment or URL—payloads in Q3 remained diverse with a range of banking Trojans, credential stealers, and downloaders appearing in both large and small campaigns (Figure 3). Ransomware dropped by 10 percentage points from Q2, comprising only 1% of malicious email volume, while **REMOTE ACCESS TROJANS** (RATs) nearly doubled relative to other malware families compared to Q2. Although RATs still only represent 4% of total message volume, threat actors continue to distribute RATs at unexpected scale. RATs appeared in just 1% of malicious messages in Q1 and 2% in Q2.

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.

The growing prevalence of malware like RATs and bankers vs. "smash and grab" ransomware represents a continued shift towards large investment, large return campaigns. It appears that threat actors are currently seeing greater rewards for investing the time and effort into monitoring and managing hosts infected with relatively quiet malware designed for stealthy persistence and ongoing exploitation. This shift has also accompanied the introduction of new regulations and security measures around cryptocurrencies, the booming value of which helped drive ransomware campaign volumes in 2016 and 2017.

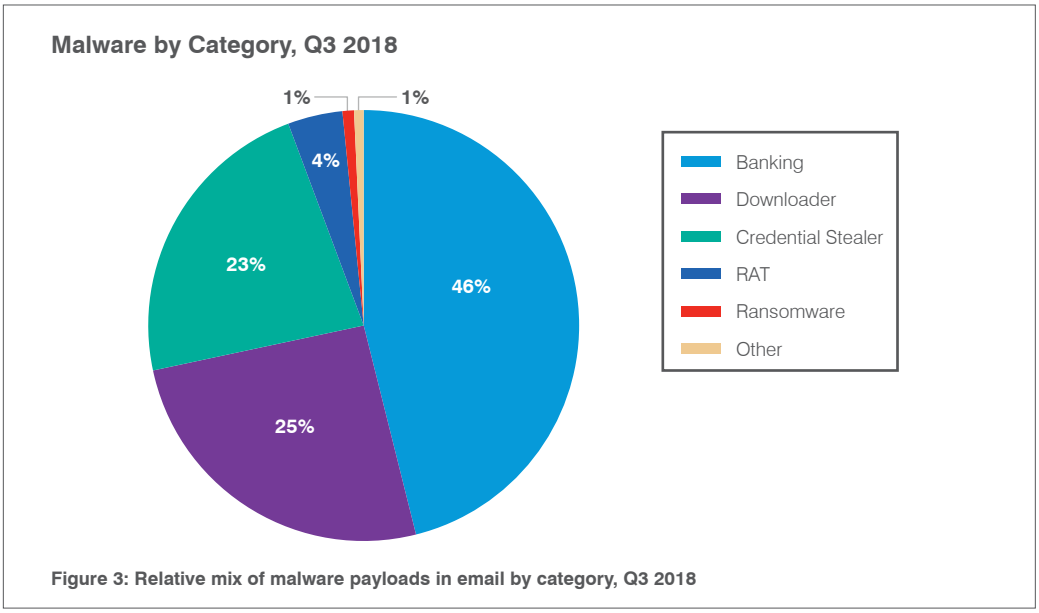

Figure 3: Relative mix of malware payloads in email by category, Q3 2018

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

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

Looking across quarters in 2018, we can pick out a number of additional trends beyond the relative increases in RATs and the near disappearance of **RANSOMWARE** after a moderate resurgence in Q2 (Figure 4). In particular, after Q1's disproportionately high volume of banking Trojans, the overall mix of malware families has skewed less towards any one family, with downloaders and stealers making up for declines in ransomware and leveling off of bankers.

Moreover, while new **DOWNLOADERS** and stealers appeared, increasing the payload diversity within these families, the proportion of malware classified as "other" has decreased and threat actors have continued to consolidate around well-known malware families.

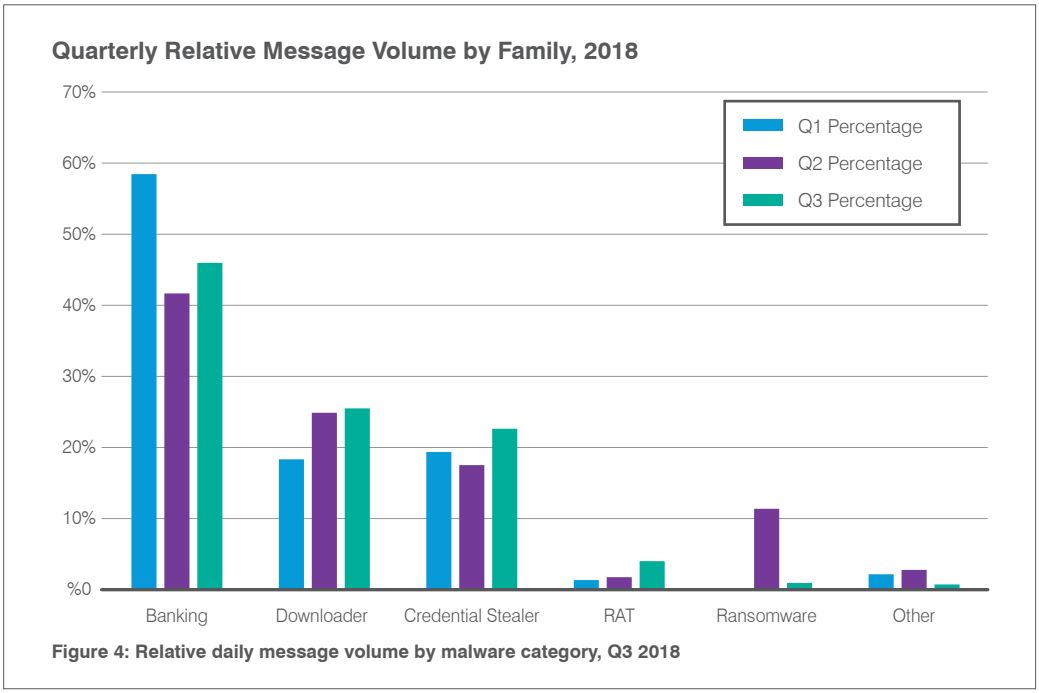

Figure 4: Relative daily message volume by malware category, Q3 2018

Like malware campaigns distributing corporate credential stealers, corporate credential phishing schemes also increased between Q2 and Q3. Credential phishing schemes, however, skyrocketed by over 300% quarter over quarter (Figure 5). As with other trends, this may be seasonal in nature.

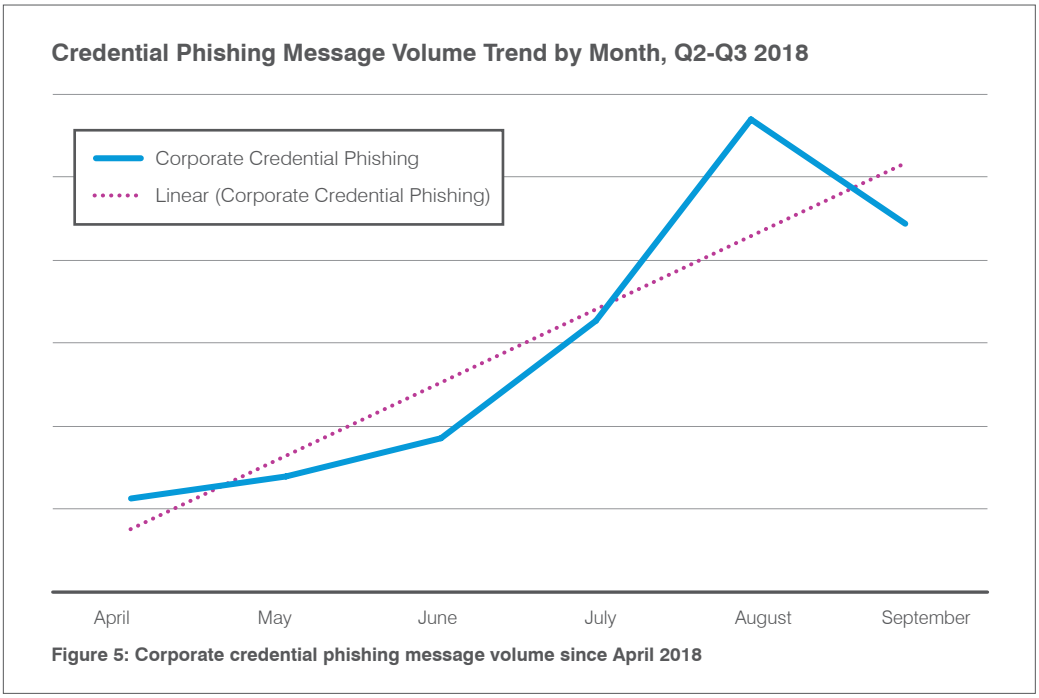

Figure 5: Corporate credential phishing message volume since April 2018

BANKERS DIVERSIFY BUT PANDA AND EMOTET DOMINATE THE LANDSCAPE

Key stat: Banking Trojans made up 46% of all malicious payloads; of those, 90% were Emotet and Panda Banker.

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.

As with the ransomware campaigns of 2016 and 2017, a small number of actors drove the majority of campaign volume, even as the number of distinct actors and banking Trojan payloads remained high. **EMOTET**, for example, was distributed in consistent, near-daily, large campaigns by the actor we track as TA542. Panda Banker (aka Zeus Panda) appeared in large campaigns distributed by the actors TA511 and TA544. While other actors distributed Panda Banker, these two actors were responsible for the majority of large-scale email campaigns with Panda as the primary payload. Overall, as shown in Figure 6, the volume of messages bearing banking Trojans trended upwards throughout Q3.

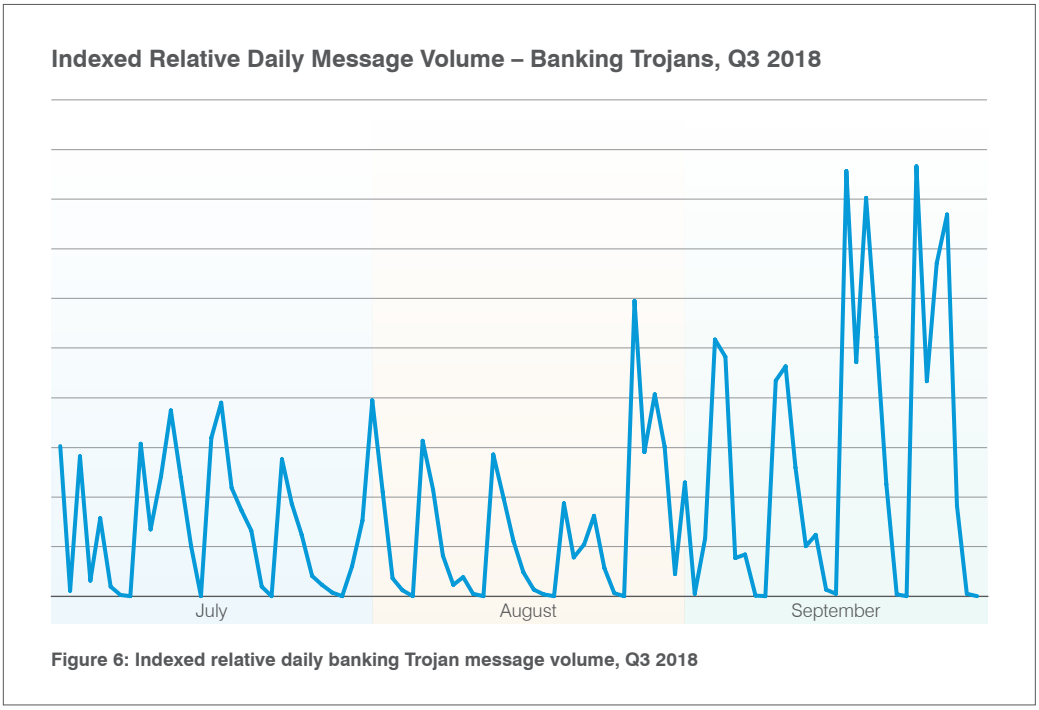

Figure 6: Indexed relative daily banking Trojan message volume, Q3 2018

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.

As noted above, Panda Banker and Emotet comprised the vast majority of banking Trojan campaigns (Figure 7), capturing market share from URLZone, Ursnif and **THE TRICK**. In Q2, Panda and Emotet appeared in 77% of banker campaigns vs. 90% in Q3.

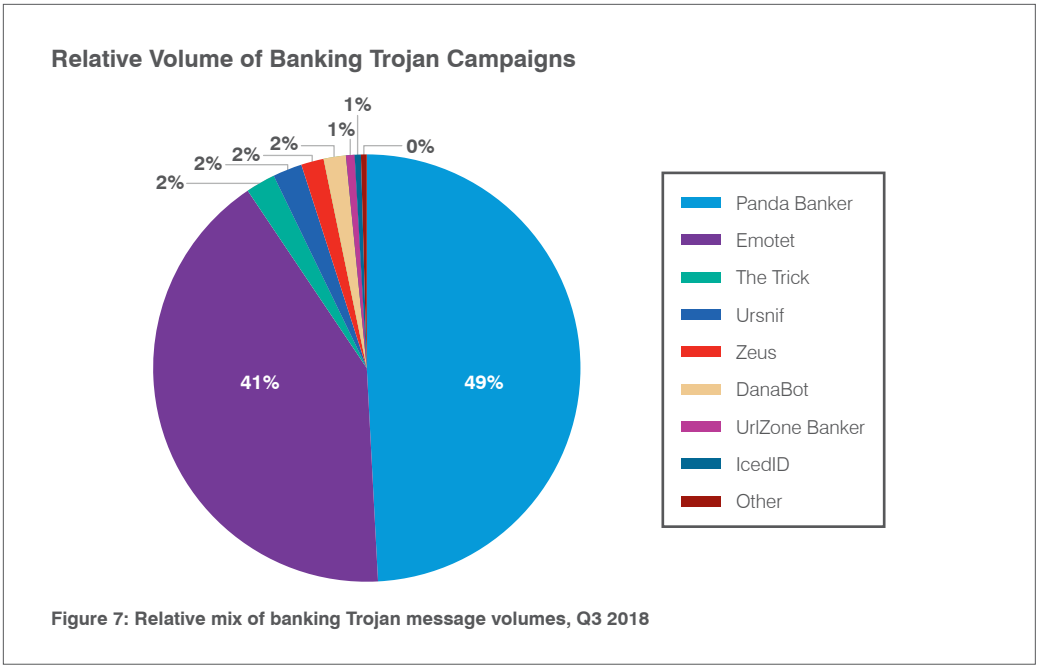

Figure 7: Relative mix of banking Trojan message volumes, Q3 2018

RANSOMWARE: GONE BUT NOT FORGOTTEN

Key Stat: Ransomware message volume dropped 10 percentage points from Q2, making up only 1% of overall malicious message volume.

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

After dominating the threat landscape in 2017 and much of 2016, **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.

GANDCRAB
GandCrab is one of the few strains of ransomware still active in 2018; it is distributed in an affiliate model, allowing multiple threat actors to distribute the malware through a variety of vectors.

The only exceptions to this appear to be **GANDCRAB** and Hermes ransomware, both of which appeared in occasional campaigns in Q3 (Figure 8).

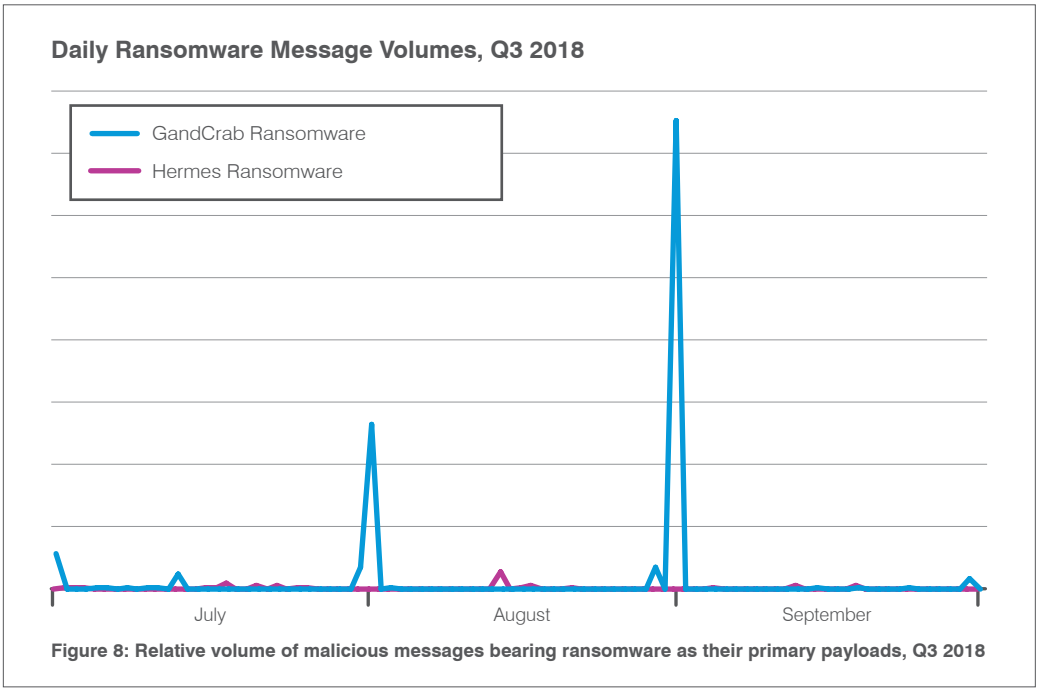

Figure 8: Relative volume of malicious messages bearing ransomware as their primary payloads, Q3 2018

DOWNLOADERS AND STEALERS: FILLING IN FOR RANSOMWARE

In Q3, Proofpoint researchers discovered three new downloaders, all of which were part of a trend towards distribution of small-footprint, stealthy malware used initially for reconnaissance. Credential stealers and downloaders accounted for 48% of all malicious payloads in Q3, compared to just 11% in Q3 2017. At that time, ransomware comprised nearly 64% of malicious payloads, driven primarily by massive Locky and GlobeImposter campaigns distributed by TA505.

Marap, Advisorsbot and Cobint, however, were all part of the shift away from a single dominant malware family like ransomware or banking Trojans. Figure 9 shows the relative daily volume of downloaders and information stealers, the latter of which regularly jockeyed for position with downloaders and represented another layer of malware infections focused on long-term persistence and ongoing exploitation of infected systems.

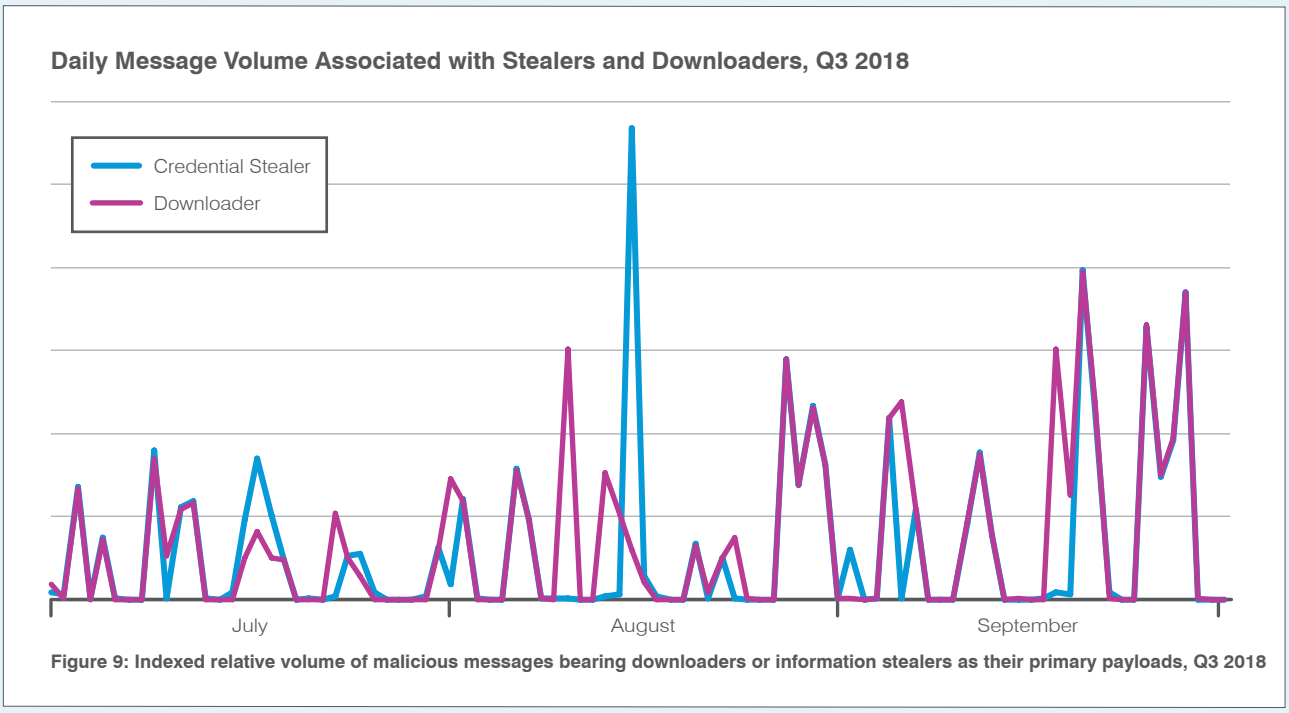

Figure 9: Indexed relative volume of malicious messages bearing downloaders or information stealers as their primary payloads, Q3 2018

Threat actors—from newer players we featured in our **AdvisorsBot blog** to established actors like TA505 and Cobalt Group—are increasingly looking to stealthy downloaders to initially infect systems and then only install additional malware on systems of interest. As defenses improve across the board, threat actors must innovate to improve the returns on their investments in malware and infection vectors. This approach is consistent with the "follow the money" theme we have associated with a range of financially motivated campaigns over the years. It appears to be the latest trend as threat actors look to increase their effectiveness and differentiate final payloads based on user profiles.

EMAIL FRAUD THREATS: ACTORS CONSOLIDATE AROUND PROVEN TECHNIQUES

Key stat: Over half of companies saw their own domain spoofed to launch an attack against their employees.

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 continued to grow as a business problem, with targeted organizations receiving an average of over 36 such attacks in Q3. This represents a 77% increase over Q3 2017. And while we saw a few industries like pharmaceuticals and construction increase significantly in apparent email fraud targeting (Figure 10) this quarter, organization size continued to have no bearing on attack rates. Overall, complex supply chains were a far better indicator of the likelihood of an email fraud attack.

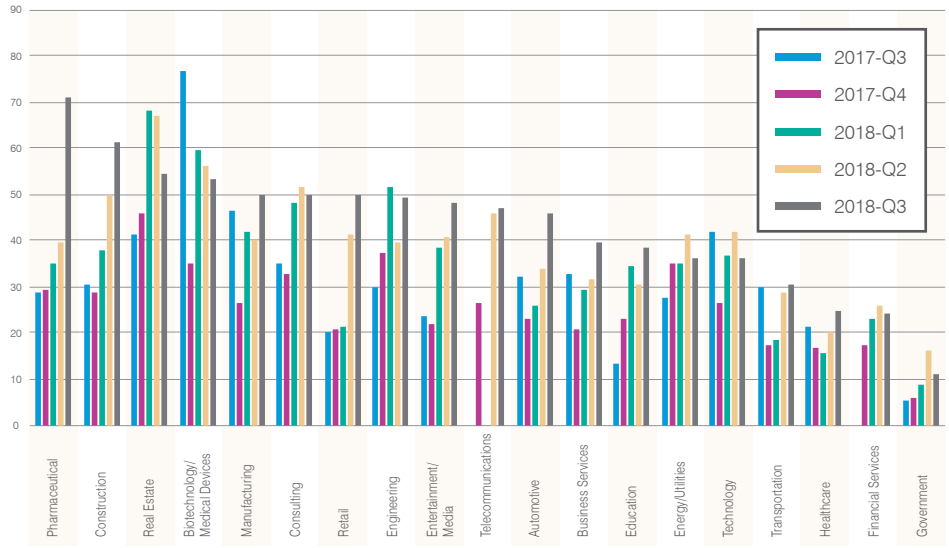

Figure 10: Number of email fraud attacks per targeted organization by industry

Aside from shifts in prevalence by industry, Q3 was marked by a few other noteworthy changes in the email fraud space. First, we found that email fraud actors were conveying a greater sense of urgency in the wording of their emails—making their requests timebound and warning employees of consequences for delay. Second, while it only represented only a small percentage of the total, we saw a 549% increase in payroll-related scams quarter over quarter, as hundreds of companies were targeted with emails featuring subjects such as “Payroll update.” Although the Q2 spike in attacks referring to documents in the subject line proved to be anomalous, the payroll-related jump serves as a reminder that changes in subject lines do not need to be tied to specific events like tax filing or the close of the fiscal year.

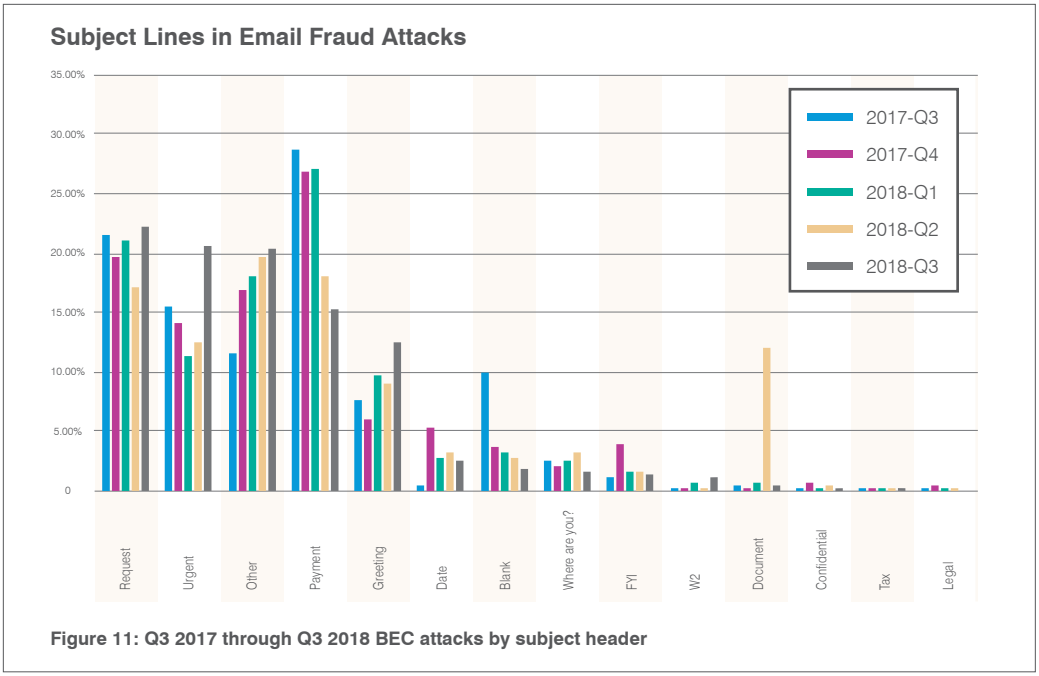

Figure 11: Q3 2017 through Q3 2018 BEC attacks by subject header

WE SAW A **68% REDUCTION** IN THE NUMBER OF SENDING IDENTITIES THAT WERE SPOOFED

Compared to Q2, we saw a 68% reduction in the number of sending identities that were spoofed (Figure 12) in these attacks. In Q3, BEC actors impersonated an average of five users, returning to levels common throughout 2017. Given that the number of attacks has increased but the number of identities spoofed has decreased, we expect that threat actors were experimenting during the first half of 2018, spoofing a wider range of employee and partner identities. These actors have returned to the tactic of spoofing those employees with the greatest authority. Moreover, over half of companies saw their own domain spoofed to launch an attack against their employees, marking less reliance on spoofed external partners who may be less recognizable to employees.

While the number of identities spoofed declined, an average of 27 people were targeted per attack, matching Q2 levels and representing a 96% increase in target victims year over year.

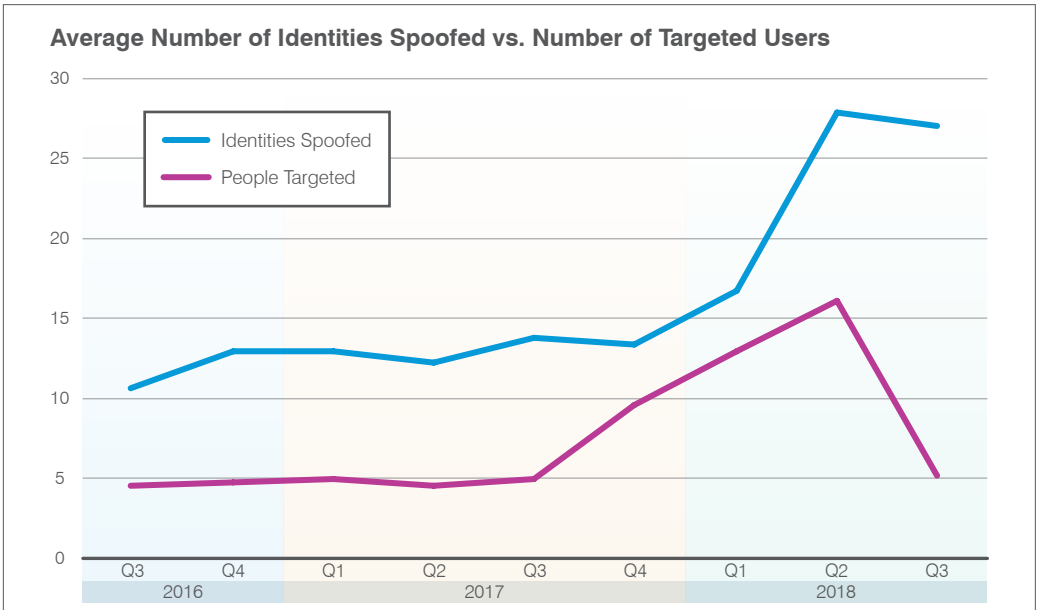

Figure 12: Average number of identities spoofed per targeted organization vs. average number of targeted users in email fraud attacks

Finally, while email fraud continues to be a highly targeted scam, the proportion of companies that received more than 50 BEC emails almost doubled from 11% to 20% year over year. Taken together,

these changes allow threat actors to spend their time on employee targeting to improve their chances of successfully exploiting the human factor.

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.

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.

WEB-BASED THREATS: SOCIAL ENGINEERING CONTINUES TO DOMINATE

Key stat: Web-based social engineering schemes grew 233% vs. Q2.

While we continue to see ongoing low-level exploit kit activity, as noted in Q2, social engineering attacks on the web represented 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. Between Q1 and Q2, we observed over a 9x increase in social engineering detections on our worldwide network of **IDS** sensors. As shown in Figure 13, social engineering detections continued to increase in Q3, growing an additional 233% quarter over quarter.

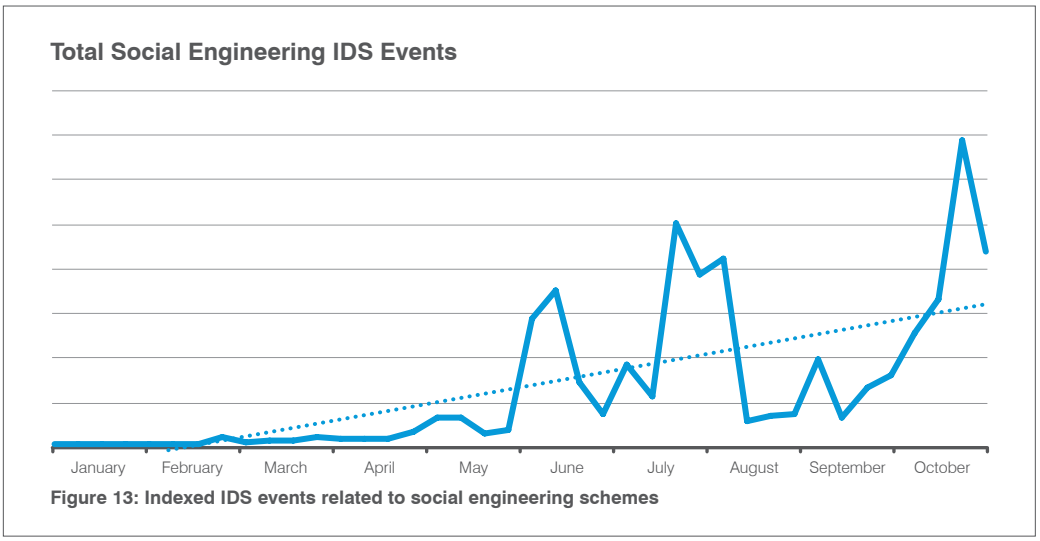

Figure 13: Indexed IDS events related to social engineering schemes

Coinhive is JavaScript code that webmasters can install on legitimate sites—or that attackers can install on compromised sites—that co-opts users' CPUs to mine cryptocurrency while they view a web page. Coinhive-related activity exploded at the end of Q2 2018, with the sheer volume and speed of adoption, suggesting that much of this activity was malicious cryptojacking. Although the spike in June was not sustained, overall Coinhive activity continued to trend upward throughout Q3 (Figure 14).

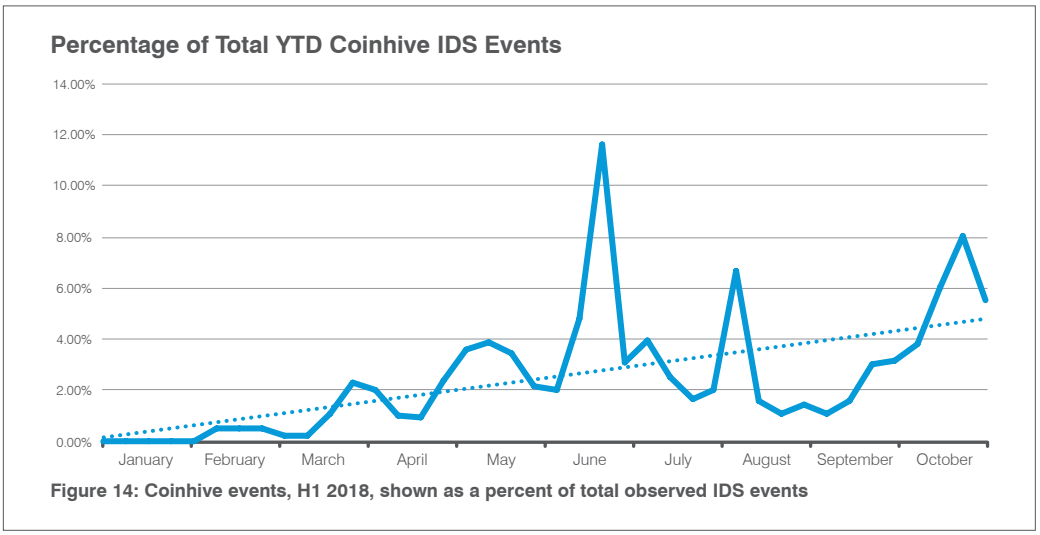

Figure 14: Coinhive events, H1 2018, shown as a percent of total observed IDS events

Despite a brief spike in Neutrino activity in August, overall EK activity held steady at a small fraction of its 2016 peak. Of this remaining activity, Neutrino and RIG EK accounted for 85% of total EK traffic for the quarter.

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

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

SOCIAL MEDIA THREATS: SUPPORT FRAUD REELS IN THE PHISH

Key stat: Social media support fraud increased by 486% vs. Q3 2017.

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.

For the last year, we have seen a fairly consistent inverse relationship between **SOCIAL MEDIA SUPPORT FRAUD**, also known as "angler phishing," and the presence of phishing links. Social media generally excel at combating phishing links, with this tactic decreasing 90% vs. Q3 2017. However, as shown in Figure 15, angler phishing—in which actors insert themselves into legitimate conversations between consumers and brands on social media—reached its highest level ever in September. The dip in August appears to be a seasonal artifact, with this type of phishing increasing overall by 486% compared to this quarter last year.

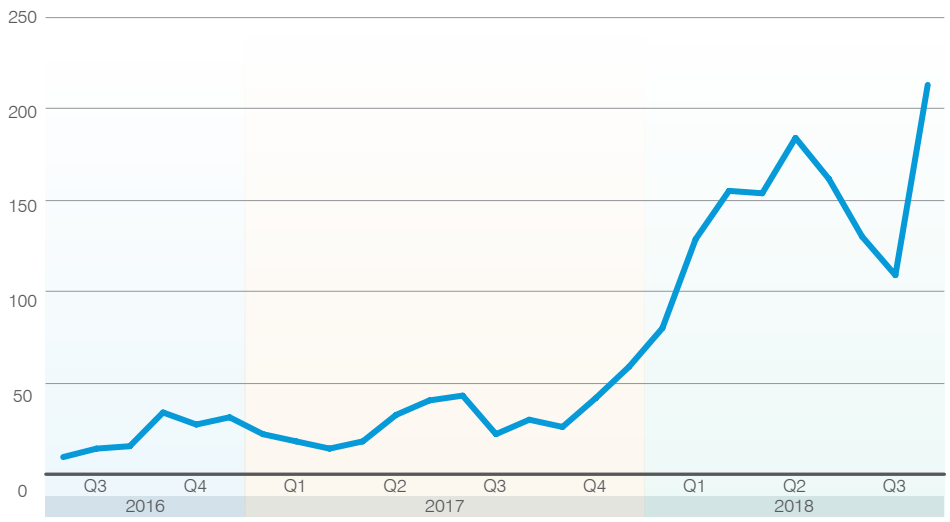

Figure 15: Indexed support fraud phishing account volume

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 email fraud 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), 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.

proofpoint.

proofpoint.com

1018-037