REPORT

proofpoint.

# QUARTERLY THREAT REPORT

Q3 2017

proofpoint.com

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

Every day, we analyze more than 1 billion email messages, hundreds of millions of social media posts, and more than 150 million malware samples to protect organizations around the world from advanced threats. We continue to see sophisticated threats across three primary vectors: email, social media, and mobile. 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: Back to the Future** ..... **4**

Email ..... 4

Exploit Kits and Web-Based Attacks ..... 4

Domain ..... 5

Social Media ..... 5

**Email-Based Threat Trends** ..... **5**

Banking Trojans: New Trends for Old Players ..... 7

Ransomware: Doubling down on Locky, While Destructive Ransomware Increases ..... 8

*Sidebar: Coinminer Mania* ..... *10*

*Email Fraud Grows While Actors Refine Techniques* ..... *10*

**Exploit Kits: Down But Now Out** ..... **11**

**Domain Trends** ..... **12**

**Social Media Tends** ..... **13**

**Recommendations** ..... **14**

# KEY TAKEAWAYS: BACK TO THE FUTURE

Over the last few years, the third quarter has become a flashpoint for threat researchers—a time of peak message volumes and a preview of tools and techniques attackers will use in the coming months. Q3 followed a similar pattern this year.

The volume of email attacks that use malicious URLs exploded, making up the highest proportion of email attacks (vs. those that use attachments) in more than two years. Ransomware and banking Trojans remain the payloads of choice.

Meanwhile, social engineering and targeting techniques further evolved in email fraud and attacks on social media.

And in our first public report of lookalike domains used for a range of attacks and fraud, attackers appear to be winning the domain-registration race. For every "defensive" registration from organizations acting proactively, we found twenty suspicious lookalike registrations by someone else.

Here are key takeaways from the quarter:

## EMAIL

**Malicious email volume soared 85% from the prior quarter, propelled by an explosion of malicious URL attacks.**

The volume of email with malicious URLs linking to hosted malware shot up nearly 600% from the previous quarter and more than 2,200% from the year-ago quarter. The upsurge amplified a trend we saw in first half of the year—volumes marked the highest proportion of URL email (vs. attachment-based email) that we have seen since 2014. Still, large campaigns that use malicious attachments also helped drive the surge—in this case, malware hidden in compressed-file archive attachments.

**Ransomware remained the top malware category.**

Across our global customer base, ransomware accounted for almost 64% of all email malware attempts. New ransomware strains appeared daily, but Locky remained the top payload. It accounted for almost 55% of total message volume and more than 86% of all ransomware volume. At the same time, strains known as Philadelphia and GlobeImposter grew from small, regionally focused variants into global threats, thanks to a few high-volume campaigns by a single attacker.

**BANKING TROJANS**
This type of malware steals victims' bank login credentials, usually by redirecting the victim's browser to a fake version of their bank's website or injecting fake login forms into the real site.

**ETERNALBLUE**
EternalBlue is a powerful hacking tool that exploits a flaw in a Windows file-sharing component. It was stolen from the U.S. National Security Agency and leaked publicly in early 2017.

**BANKING TROJANS represented 24% of all malicious email volume, with a strain called The Trick accounting for 70% of that total.**

Driven by massive campaigns from one attacker, The Trick displaced the Dridex strain as the top banking Trojan. (Dridex, after a lull for most of the first quarter, had re-emerged in large campaigns in Q2.) Dridex—along with Ursnif, Bancos, and Zloader—continued in regionally focused campaigns. Also appearing was a new version of Retefe. It used a leaked exploit from the U.S. National Security Agency known as **ETERNALBLUE** to spread across internal networks.

**Email fraud rose 29% vs. the previous quarter.**

The frequency of attacks also increased; email fraud attempts per targeted organization rose 12% from the previous quarter and 32% vs. the year-ago period. While email fraud does not discriminate by size, organizations with more complex supply chains are more frequent targets.

## EXPLOIT KITS AND WEB-BASED ATTACKS

**EXPLOIT KITS (EKS)**
Exploit kits (EKs) run on the web, detecting and exploiting vulnerabilities in computers that connect to it. EKs, often sold to attackers as a service, make it easy to infect PCs in "drive-by" malware downloads.

**Traffic from EXPLOIT KITS (EKS) held steady, but at levels a mere 10% of its 2016 peak.**

The RIG EK accounted for 76% of all EK activity. Attackers are layering social engineering schemes into their EK campaigns. The trend suggests they are looking beyond the exploits alone as they get harder to find and obtain.

**DEFENSIVE REGISTRATIONS**
The recommended practice of buying up internet domains that could be mistaken for yours before attackers do. Lookalike domains can be used to trick customers and partners with fake websites and fraudulent emails that appear to be from your organization.

**ANGLER PHISHING**
In angler phishing, attackers create fake customer-support accounts on social media to trick people looking for help into visiting a phishing site or providing account credentials.

**TA505**
Motivated by financial gain, this threat actor is the source of some of the largest email attack campaigns on record, including those spreading the Dridex banking Trojan, Locky ransomware, Jaff ransomware, The Trick banking Trojan, and more.

**LOCKY**
Locky is the most common strain of ransomware seen in malicious emails, encrypting victims' data and holding it "hostage" until the victim pays to decrypt. For most of 2016 and several months in 2017, it accounted for the majority of malicious email traffic.

## DOMAIN

**Suspicious domain registrations outnumbered DEFENSIVE REGISTRATIONS 20 to 1.**
Some organizations are aggressively registering domains to combat typosquatting and domain spoofing, but most are not. Defensive registration of brand-owned domains fell 20% vs. the year-ago period. Suspicious domain registrations grew 20%.

## SOCIAL MEDIA

**Fraudulent support accounts, used for so-called ANGLER PHISHING, doubled from the year-ago quarter.**
The number of fake customer-support accounts grew 5% over the previous quarter while the volume of phishing links on branded social channels rose 10%.

# EMAIL-BASED THREAT TRENDS

**Key stat: URL-based malware campaigns grew nearly 600% over the previous quarter and more than 2,200% over the same period last year.**

The volume of fraudulent email that delivered malware through malicious URLs grew dramatically. One of the biggest drivers: **TA505**, a highly prolific attacker best known for massive Locky campaigns, switched from attachments to URLs to deliver it. TA505 also sent Philadelphia and GlobeImposter ransomware and The Trick banking Trojan at volumes high enough to move the needle.

That surge helped push overall malicious email volume up 85% from the earlier quarter, despite a 74% drop in emails with malicious attachments.

Still, malicious attachments remain a significant part of mix. Attackers launched a smaller number of attachment campaigns, along with some exceptionally large campaigns that hid malicious code in compressed-file archives. Campaigns used RAR and 7-Zip archive file formats, usually containing malicious JavaScript or VBScript. When executed, the scripts downloaded and installed **LOCKY** ransomware.

As Figure 1 and Figure 2 show, malicious URL messages as a percentage of total global message volume reached 64%. That is a proportion we have not seen since 2014, the last year malicious URL emails made up the majority of attack campaigns messages. Ultimately, both approaches had similar objectives: whether delivered through URLs or attachments, Locky was the payload for the majority of these high-volume campaigns.

**Indexed Daily Malicious Message Volume by Attack Type, 2017 YTD**

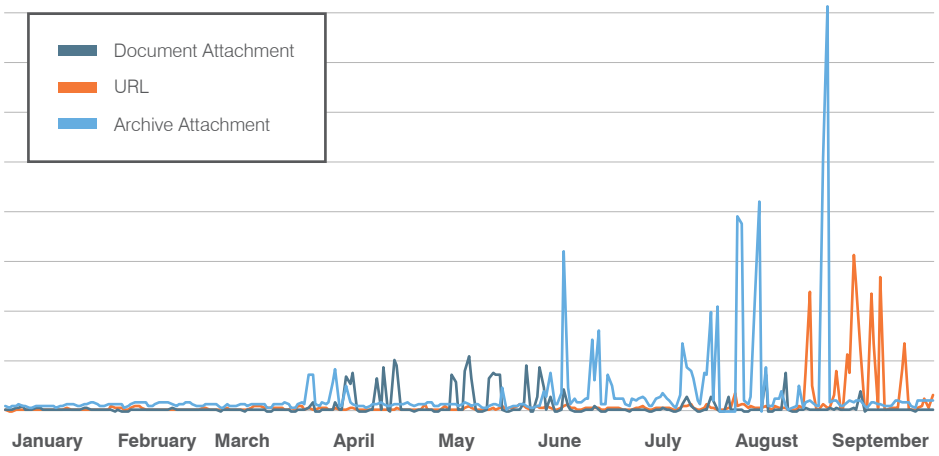



**Figure 1: Indexed attack type trend, January 2017 through September 2017 (273 Days)**

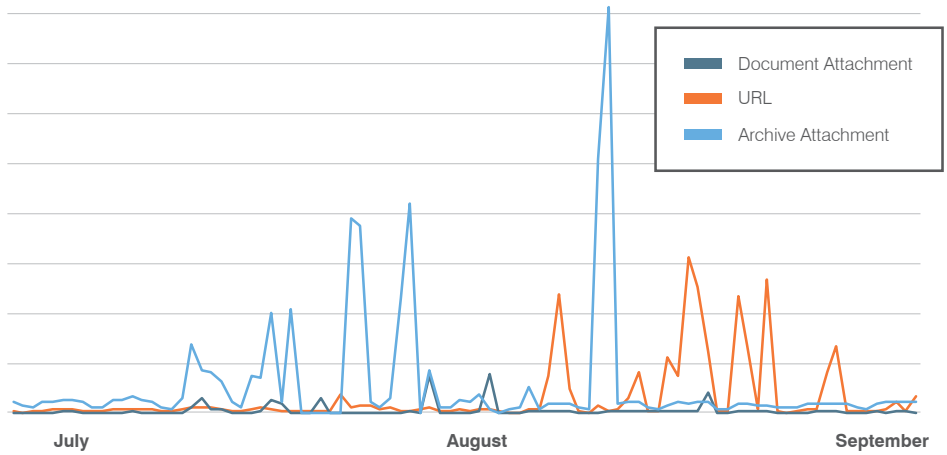



**Figure 2: Indexed attack type trend, July 2017 through September 2017 (92 Days)**

Figure 3 shows the ongoing dominance of ransomware, particularly Locky. A handful of large campaigns distributing **THE TRICK** banking Trojan created some spikes later in the quarter.

**THE TRICK**
The Trick, also known as Trickbot, is a banking Trojan closely related to Dyre. Dyre's operators were arrested in 2015 by Russian authorities but the malware resurged in 2017.

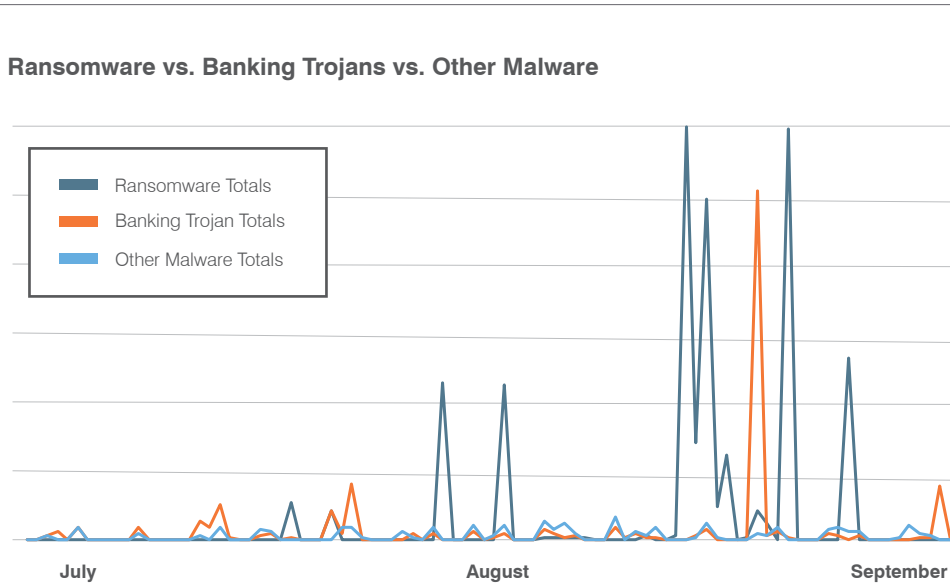



**Figure 3: July 2017 through September 2017 (92 Days)**

## BANKING TROJANS: NEW TRENDS FOR OLD PLAYERS

**Key stat: The Trick accounted for 70% of all emails sending banking Trojans.**
Most of this malware came from TA505, the threat actor behind massive email campaigns using Locky ransomware and the Dridex banking Trojan.

**DRIDEX** traffic fell sharply as TA505 switched over to The Trick. At the same time, **ZLOADER** activity held steady through much of the quarter, though at lower levels from Q2. Meanwhile, Zeus Panda, Emotet, and URLZone appeared in large, regionally focused campaigns.

In a potentially bigger development, banking Trojans such as **RETEFE** and The Trick paired with the EternalBlue exploit. This enables the Trojans to spread unaided across internal networks after the initial email infection. Retefe, which has targeted mostly Swiss banks with German-language lures, never achieved the volume or reach of Dridex or Zeus. But these "ripples" of early summer's **WANNACRY** outbreak—which also used EternalBlue—hint at a potential trend for 2018. More attackers may take advantage of the security weaknesses revealed by WannaCry and NotPetya.

Figure 4 shows the daily mix of banking Trojans. Traffic spikes from The Trick punctuate the quarter, dwarfing smaller bumps mostly from Zloader and Panda Banker.

**DRIDEX**
Dridex is a widely used banking Trojan that spreads through a variety of vectors, primarily via email, infecting victims and stealing banking credentials.

**ZLOADER**
Zloader, also known as Terdot, is a downloader often used with the Zbot banking Trojan and other malware variants.

**RETEFE**
This banking Trojan has mostly targeted areas of Europe. Instead of injecting fake login forms into legitimate banking websites to steal credentials (as many banking Trojans do), it redirects the user to a fake version of the bank website through a series of proxy servers.

**WANNACRY**
The ransomware infected tens of thousands of systems across more than 150 countries in May, one the largest cyber attacks on record. It spread through a flaw in a file-sharing component of Microsoft Windows.

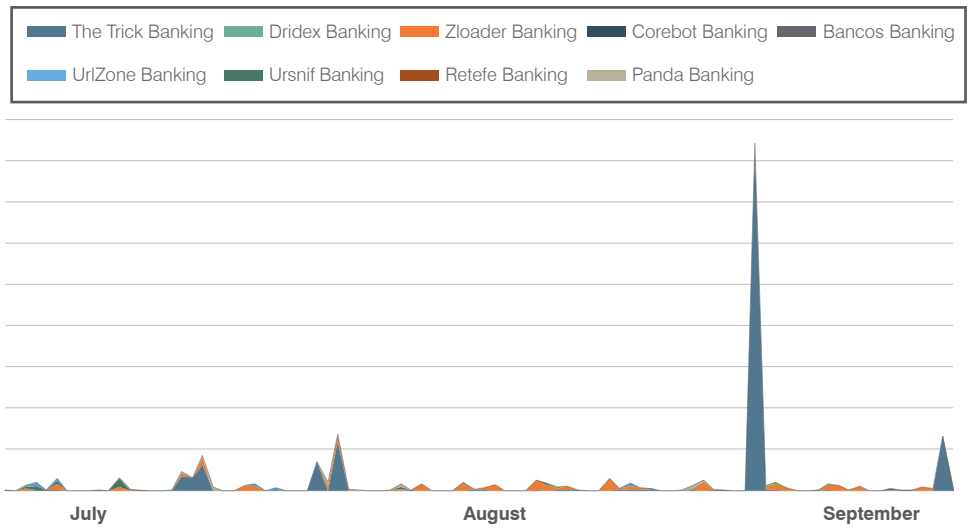



**Figure 4: Indexed daily message volumes for top banking Trojan strains, July-September 2017**

## RANSOMWARE: DOUBLING DOWN ON LOCKY, WHILE DESTRUCTIVE RANSOMWARE INCREASES

**Key Stat: Ransomware attempts accounted for almost 64% of total malicious message volume across our global customer base.**

Ransomware continued to dominate the threat landscape. New variants emerged daily, development of destructive ransomware persisted, and targeted attacks grew.

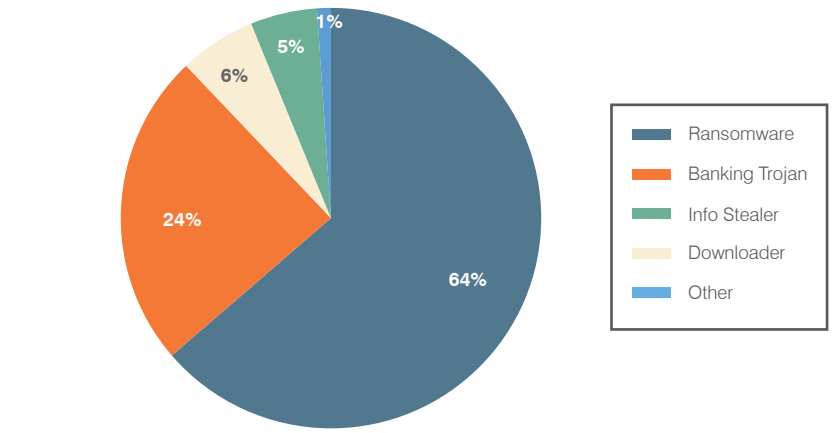



**Figure 5: Comparison of quarterly overall message volume**

Most ransomware appeared in very large Locky campaigns from TA505. But TA505 also sent out GlobeImposter and Philadelphia ransomware variants. Notably, one of those strains included an "offline" version of Locky that did not require a central command-and-control (C&C) infrastructure to encrypt victims' files.

**AFFILIATE IDS**
Malware authors often pay affiliates to spread their malware. The affiliate ID is hardcoded into versions of the malware to ensure that the right people get credit for the infection.

Other attackers shifted further from indiscriminate high-volume campaigns to more targeted attacks. One introduced the Defray ransomware strain in small-scale attacks on healthcare and education targets in August. Other attackers followed suit. Several new Locky **AFFILIATE IDS** that appeared in campaigns targeted mostly at higher education and healthcare. At least one of these (Affid=36) distributed the offline version of Locky.

**NOTPETYA**
This strain of malware masqueraded as Petya ransomware but appears to be a state-sponsored tool to cause turmoil rather than collect a ransom.

On the heels of WannaCry and Petya-like attacks in Ukraine in late Q2, other strains emerged. Hell (discovered in July) and IsraByte (discovered in August) failed to gain traction or publicity. But like **NOTPETYA** and WannaCry, they appeared to be designed more for destruction than financial gain.

As Figure 6 shows, high-volume attackers consolidated around a smaller number of ransomware strains in Q3, despite new strains and uses. Driven by TA505, Locky, GlobeImposter, and Philadelphia dominated, while new Locky distributors added to the totals. Strains such as SAGE and TorrentLocker largely disappeared.

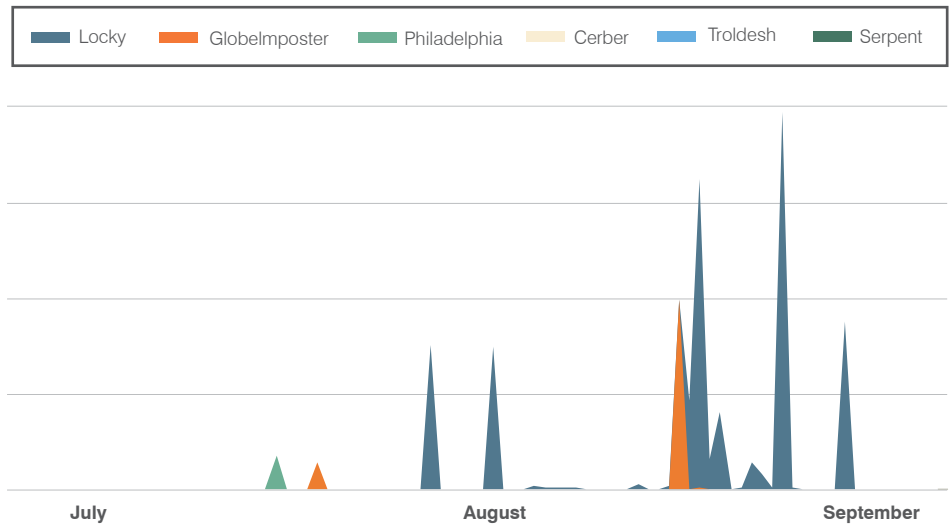



**Figure 6: Indexed daily message volume of top ransomware strains, July-September 2017**

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

The nearly exponential growth of new **RANSOMWARE** strains over the last year appears to finally be slowing slightly—but not because of any reduced threat.

On average, 1.4 new ransomware strains appeared every day. That's down from 1.8 new strains per day in the earlier quarter. The decrease is likely due to a drop in large numbers of "minor project," proof-of-concept, experimental, and "script kiddie" ransomware strains that helped inflate earlier totals.

In other words, this slowing does not point to a lower threat from ransomware. Instead, it suggests that attackers are consolidating around a few more effective strains, using ransomware in new ways, and growing more sophisticated (Figure 7).

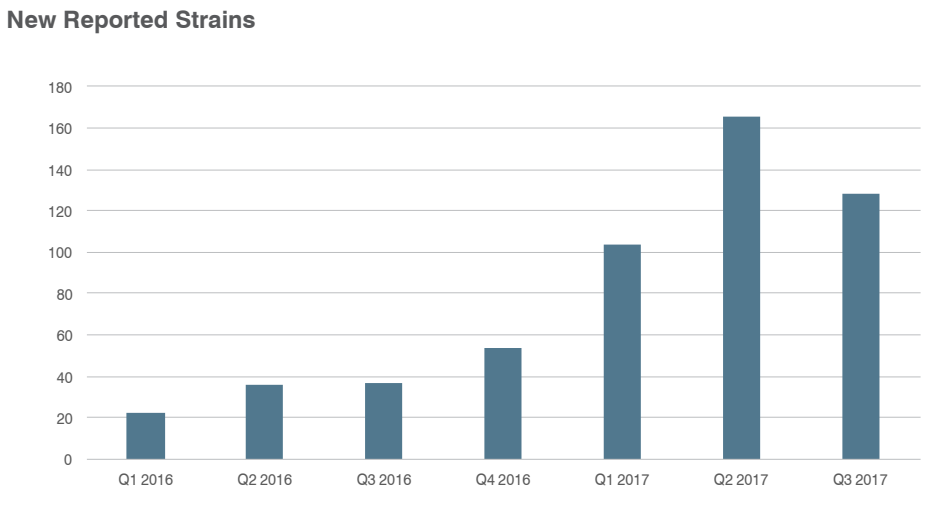



**Figure 7: Newly reported ransomware strains by quarter, 2016 and 2017 year-to-date**

# COINMINER MANIA

**CRYPTOCURRENCY** miners, or "coinminers," are malware strains that use system resources on infected machines to generate electronic cash for threat actors. Cryptocurrencies such as Bitcoin and Litecoin have built-in mechanisms to create scarcity and ensure the value of the currency. That makes completing the computations required to "mine" new units of the currency ever more difficult. The most popular mainstream cryptocurrency, Bitcoin, now requires near-supercomputer computational power to mine. But other cryptocurrencies such as Litecoin and Monero can still be mined on a desktop-class computer—or by stealing CPU cycles from a large number of client systems.

As a result, coinmining malware for these currencies is growing. They are spread through exploit kits, social engineering schemes, and even NSA exploits such as EternalBlue. The Pirate Bay recently made headlines by using visitors' CPU cycles to mine Monero currency.

The threat is multi-pronged. Some attacks target server-side web vulnerabilities to embed scripts that pull in coinminers to use CPU resources of visiting browsers. Other attacks use phishing to steal users' cryptocurrency wallet credentials, a broad-based, fast-growing trend. Still others use malware to turn victims' PCs into coinminers.

Regardless of what methods they use, threat actors will likely explore new means of exploiting victim PCs to mine. Until the smaller currencies reach the saturation levels of Bitcoin, the prospects are highly lucrative. Threat actors have revealed time and again their willingness to "follow the money."

**CRYPTOCURRENCY**
A form of digital money designed to be secure and anonymous. Currency—which can be used to buy and sell goods or exchanged for government-issued currency—is created through a "mining" process that uses computer power to solve complex math problems.

**DOMAIN SPOOFING**
Domain spoofing impersonates trusted colleagues or contacts by making an attacker's emails appear to come from a legitimate and expected address. Some domain spoofing uses lookalike domain names deceptively similar to the real ones.

## EMAIL FRAUD GROWS WHILE ACTORS REFINE TECHNIQUES

**Key stat: Attempted email fraud attacks grew 29% from the previous quarter across our global customer base.**

As the total number email fraud attacks rose, so did the frequency of attacks on targeted organizations—email fraud attempts grew 12% from the previous quarter and 32% from the year-ago quarter.

**DOMAIN SPOOFING,** a common email fraud technique, further increased as well. This type of attack can be prevented completely with email authentication. Still, 89% of organizations experienced at least one domain spoofing attack this quarter.

### Industry targeting

All industries continue to be targeted by email fraud. But attackers did appear to favor organizations with more complex supply chains, as they have in past quarters. Manufacturing, for example, continues to be targeted more often than other industries. Figure 8 shows the relative frequency of targeting by vertical. It compares Q3 2017, Q2 2017, and the year-ago quarter—all of which revealed similar relationships.

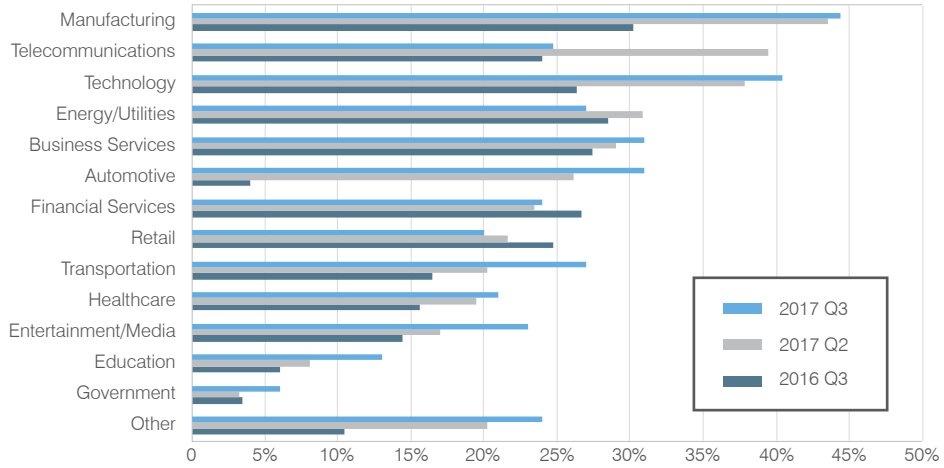



**Figure 8: Average number of email fraud attacks/company, by targeted industry, Q3 2017 vs Q2 2017 and Q3 2016**

**EMAIL FRAUD**
In email fraud attacks, an email purporting to come from a top executive asks the recipient to wire money or send sensitive information. It doesn't use attachments or URLs, so it can be hard to detect and stop.

Our analysis of **EMAIL FRAUD** found no correlation between a company's size and the frequency of email fraud attempts. In Q2, we saw some signs that cyber criminals were prioritizing larger organizations, but not to a statistically significant degree. This quarter, any apparent relationship disappeared altogether. Companies of all sizes were targeted uniformly.

### Individual targeting shows refinement

By its nature, email fraud is highly targeted. That fact was clearer than ever as attackers spoofed more identities and targeted more employees per organization. Almost three quarters of targeted organizations had more than one identity spoofed and more than one employee targeted. So-called "whaling," or attacks in which the spoofed email of a C-level executive is used to target another C-level exec, is still common. (This type of attacks is represented in Figure 9 as a "one-to-one" attack.) But cyber criminals are expanding their reach and targeting more people within each organization.

**Identities Spoofed by Number of Staff Targeted, Q3 2017 vs. Q2 2017 and Q3 2016**

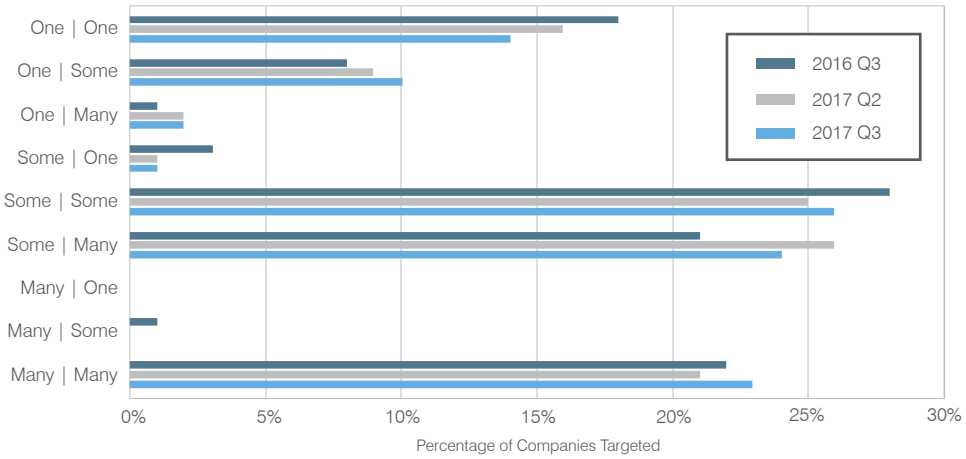



**Figure 9: Attack types by number of executive identities spoofed vs. number of people targeted. For example, a company that saw email fraud attacks that spoofed four executive identities and targeted 10 members of the finance team would be classified as a "some-to-many" attack.**

Attackers also continue to use a fake chain of emails to make their emails more convincing. About 10% percent of all email fraud used this tactic in Q3.

# EXPLOIT KITS: DOWN BUT NOT OUT

**RIG EK**
RIG has become the most popular EK in the wake of Angler's disappearance after the arrests of its operators in June 2016.

**Key stat: 73% of all Q3 exploit activity involved RIG EK.**
Exploit kits suffered a dramatic and well-publicized decline after peaking in early 2016. While activity has muddled along at a mere 10% of 2016 levels, EKs remain an important part of the threat landscape. This is especially true in regions where high levels of software piracy prevent regular patching.

New social engineering schemes are also being used with EKs, which means attackers do not have to rely on the newest exploits to get the job done. But we are seeing increased activity from "traffers," networks designed to drive traffic to exploit kit landing pages. The change hints at a possible resurgence in exploit kit (EK) activity in the months to come.

For now, RIG EK remains the dominant exploit kit, accounting for 73% of all EK traffic we saw this quarter. By the end of the quarter, already-feeble traffic associated with Angler EK had all but disappeared. Even Neutrino, which vied with RIG for the top spot for a few periods in the quarter had given way almost entirely to RIG by the end. Figure 10 shows the traffic for the top exploit kits.

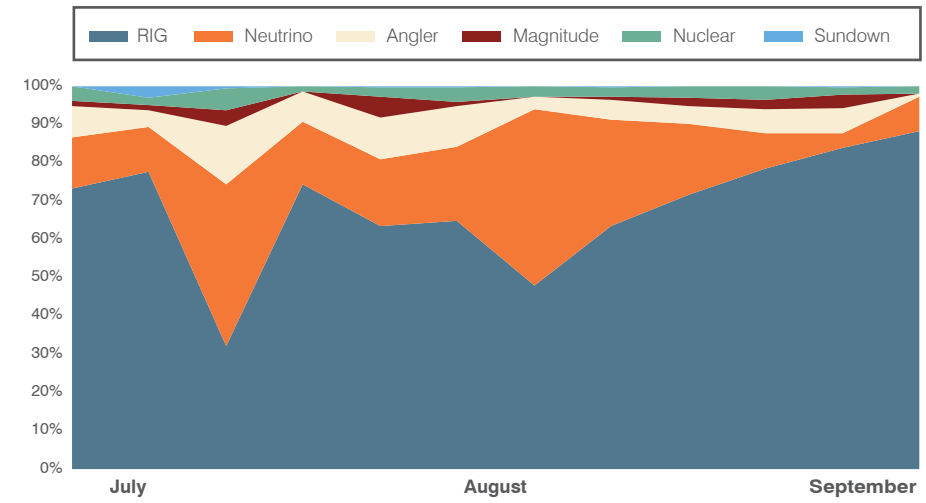



**Figure 10: Top exploit kit traffic as percentage of total, April-May 2017**

# DOMAIN TRENDS

**Key stat: Suspicious domain registrations outnumbered defensive registrations 20 to 1, widening the gap between companies looking to protect their brand and attackers looking to exploit it.**

**TYPOSQUATTING**
Fraudsters register domains that are misspellings or typographically mangled versions of a legitimate domain to trick users who mistype the URL or don't look closely at email headers.

In Q3 we extended our research to examine the registration of "suspicious domains" for the Fortune 50. Suspicious domains are those that are likely to be used for **TYPOSQUATTING** and spoofing.

From the beginning of 2015 until end of August 2017, brand-owned defensive domains have fallen while suspicious domains registered by someone other than the brand have grown (Figure 11). From January through August 2017, suspicious domain registrations rose 20% vs. the year-ago period as brand-owned defensive registrations fell 20%.

Even with these defensive registrations, suspicious domains have historically far outpaced brand-owned domains. For every defensive registration in 2016, we found 10 suspicious lookalike registrations by someone else. This year, suspicious registrations outnumbered defensive ones 20-to-1.

Moreover, spikes in defensive registrations are usually tied to a major event related to the brand, such as a new product launch, rather than an ongoing defense.

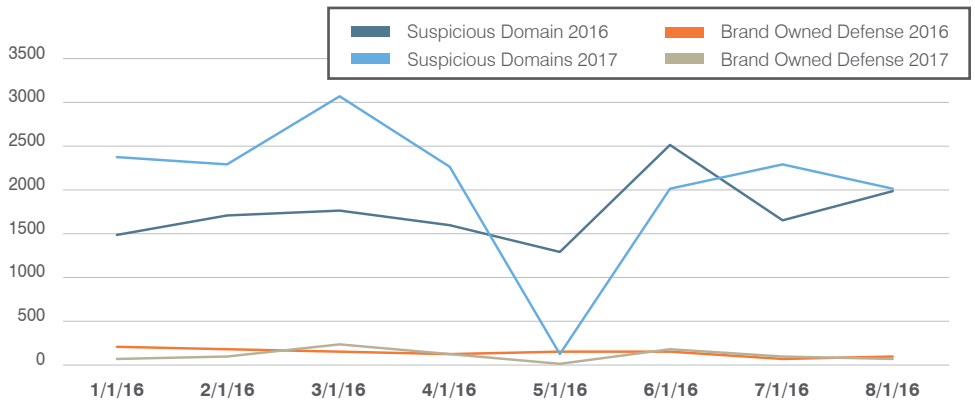



**Figure 11: Year-over-year comparison (Q1-Q3 2016 and 2017, respectively) of suspicious domain registrations vs. brand-owned defensive registrations for Fortune 50 firms**

# SOCIAL MEDIA TRENDS

**Key stat: Fraudulent customer-support accounts doubled from the year-ago quarter.**

Social media threats are numerous and varied, from malware distribution to fraud. We track two major categories:

- Support fraud accounts used for so-called "angler phishing"
- More traditional phishing links that lead users to pages that steal credentials and personal information

The number of fake customer-support accounts grew 5% from the previous quarter and doubled from the year-ago period. Phishing links on branded social media accounts grew 10% from the previous quarter (Figure 12) and was roughly flat from the year-ago period.

Together, these details suggest a broad shift in social media attacks. While attackers may respond to events or seasonal trends with conventional phishing, they are turning their attention to more lucrative angler phishing.

Standard credential phishing through social media may be easier. But targeted angler phishing has a better chance of success because it feels legitimate to the victim—much more human than random links posted in comments on branded social media pages.

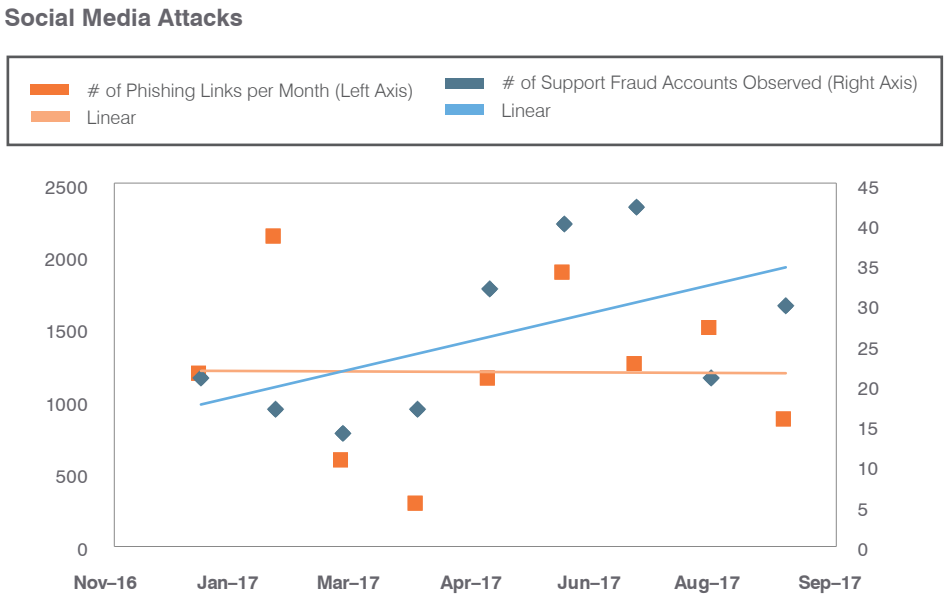



**Figure 12: Relative monthly activity in phishing link distribution via social media versus fraudulent support accounts**

# 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 data, people, and brand in the coming months.

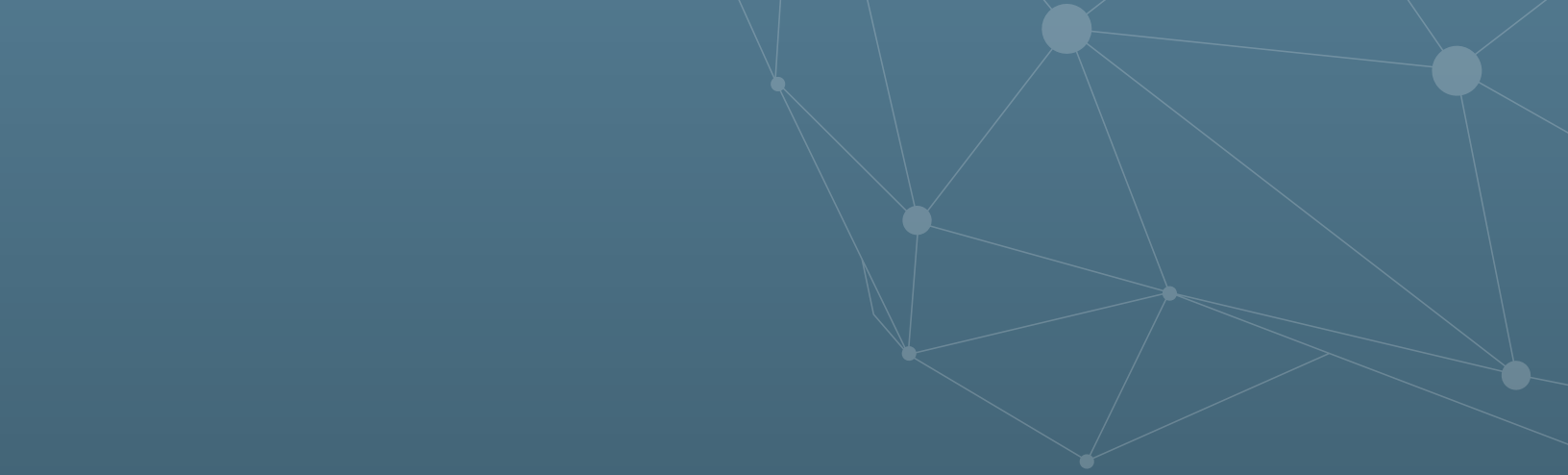
**Combat typosquatting on the web.**
Defensive domain registration is a simple and cost-effective tactic to keep attackers from creating look-alike domains for email fraud and credential phishing. Work with your business leaders to define a list of potential look-alike domains to register. Include conference and marketing campaign websites, which are frequent targets.

**Deploy email authentication to stop domain spoofing techniques used in email fraud.**
With protocols such as DMARC (Domain-based Message Authentication, Reporting & Conformance), you can stop fraudsters from using your email domain. For email attacks that use lookalike domains, your solution should be able to find domains that could be mistaken for yours—and work with third-party services to take them down.

**Protect your users from email attacks of all types.**
Whether they're malware attachments, malicious URLs or socially engineered email fraud, your email defenses should cover the widest range of email-based threats. Robust protection includes robust analysis capabilities to preemptively identify and sandbox suspicious URLs and attachments. It should use multi-stage sandbox analysis to identify malicious attachments and URLs—at the delivery point and later when employees click. And it should identify and block non-malware threats, such as emails that could trick your employees from sending money and sensitive information to impostors.

**Partner with a threat intelligence vendor.**
Smaller, more targeted attacks call for sophisticated threat intelligence. Leverage a solution that brings together analysis data with threat intelligence, combines static and dynamic techniques to detect new attack tools, tactics, and targets—and then learns from them. By correlating analysis results with threat intelligence feeds, these difficult-to-detect emails can be caught before a user has a chance to click.

**Protect your brand from impostors on social media.**
Look for a security solution that alerts you to lookalike social media accounts, especially those offering fraudulent "customer-support" services. The solution should not just detect infringing accounts but work with takedown services to stop them from defrauding your customers and partners.



For the latest threat intelligence and insight,
visit the Proofpoint Threat Insight blog at
**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 percent 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.

www.proofpoint.com