JULY-SEPT 2016

proofpoint™

Q3 2016 THREAT SUMMARY

The Proofpoint Quarterly Threat Summary captures threats, trends and transformations we see within our customer base and in the wider security market. Each 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 from advanced threats. That gives us a unique vantage point from which see data and trends outside across the entire threat landscape.

Analyzing how these threats shift quarter over quarter helps identify larger trends and equip organizations with actionable intelligence and advice for managing their security posture. We continue to see sophisticated threats across three primary vectors: email, social media and mobile.

KEY TAKEAWAYS: THE STORM AFTER THE CALM

Cyber threats shifted dramatically in the third quarter, as the relative quiet of the second quarter gave way to explosions in both the volume of campaigns and the variety of threats. Attackers further honed their ability to target attacks and evade conventional cyber defenses. Ransomware came roaring back in record volumes and new forms. At the same time, malware designed to steal bank account credentials surged in highly tailored attack campaigns.

As users continued to flock to social media and mobile devices, attackers followed—often using the two technologies together. Cyber criminals piggybacked off popular brands and apps to trick people into downloading malware and hand over login credentials.

Below are key takeaways from the quarter.

EMAIL AND EXPLOIT KITS

- **The volume of malicious email that used JavaScript attachments rose 69% vs. Q2 to their highest levels ever.** New campaigns bearing varied attachment types broke volume records set in Q2, peaking at hundreds of millions of messages per day. JavaScript attachments continued to lead these very large email campaigns, with Locky ransomware actors also introducing new file attachment types—likely in attempts to bypass traditional defenses. JavaScript attachments, often disguised as other attachment types, can be confusing to users, making them especially effective in email attacks.
- **Most emails with malicious documents attached featured the popular ransomware strain Locky.** Among the billions of messages that used malicious document attachments, 97% featured Locky ransomware, up 28% from Q2 and 64% from Q1, when Locky was discovered. Like other strains of ransomware, Locky encrypts victims' data, demanding a payment to unlock it.
- **The variety of new ransomware variants grew tenfold over Q4 2015.** . The variety of ransomware continued to increase, especially strains delivered by exploit kits (EK). Among these EK-distributed variants, and in smaller email campaigns, CryptXXX remained the dominant ransomware payload, even appearing in a spam campaign. Ransomware can be disruptive and costly, especially as new variants make detection trickier.
- **Cyber criminals continue to hone their techniques in business email compromise (BEC) attacks.** In BEC attacks, impostors pose as a high-ranking executive to trick his or her colleagues into wiring money. "Reply-to" spoofing has fallen roughly 30% since early 2016, while "display name" spoofing rose, making up about a third of all BEC attacks.[1] The shift shows that attackers continue to evolve and adjust their techniques. None of this has displaced "ordinary" credential phishing, which continues to get more sophisticated. BEC and many phishing attacks do not involve or malicious attachments, relying instead on social engineering, which makes detecting them with conventional security tools especially hard.

1 In reply-to spoofing, the "From" name, address field, and reply-to name are legitimate, but the "Reply-to" address is the impostor's. Victims, not noticing the discrepancy, think they're emailing the real executive. Display-name spoofing relies on a similar inattention; the "From" name field is legitimate, but the "From" address is the impostor's.

- **Banking Trojans diversified and personalized.** . After a period of relative quiet, the popular banking Trojan Dridex reemerged in larger campaigns. Dridex, had appeared in smaller-scale and targeted campaigns in Q2. Other banking Trojans such as Ursnif also appeared in highly personalized campaigns totaling tens to hundreds of thousands of messages, a trend that began in Q2 and continued into Q3. At the same time, a wide range of banking Trojans were used in malvertising—malicious code embedded into online ads—or dropped by EKs in other browser-based attacks. These large but highly targeted campaigns are difficult to detect without intelligent protection.
- **Exploit kit activity held steady but remains far below the peaks of 2015.** Total observed EK activity fell 65% in Q3 from Q2 and is down 93% from its 2016 high in January, though the slide appears to have leveled off. With once-popular Angler gone, Neutrino gave way to RIG as the dominant EK over the course of Q3. The shift portends a greater number and variety of exploit kits, which could pose a challenge to cybersecurity tools.

MOBILE

- **Pokémon GO-related malware spawned malicious counterfeits.** Malware in the form of malicious side-loaded clone apps, dangerous add-ons, and other risky apps grew out of the game's popularity. Users can download apps from anywhere, and even the major app stores offer only limited screening of apps and updates. That means many users have no way of knowing whether the apps they download are truly secure.
- **Mobile exploit kits and zero-day attacks targeted iOS and Android.** Most mobile devices today have 10-20 exploitable zero-days. Roughly 30% of those are serious and could allow attackers to run malicious code on infected devices. Because many devices in the workplace are employee-owned, most enterprises have little visibility into mobile threats in their environment.

SOCIAL MEDIA

- **Negative content is up.** Negative or potentially damaging content such as spam, adult language, and pornography rose 50% over Q2. When this type of content appears on a brand's social media account—or one set up by an impostor—customers flee.
- **Social phishing has doubled since Q2.** Social media is a breeding ground for credential and financial phishing, where attackers trick social media users into handing over account credentials. Fraudulent accounts—used for a type of attack we call angler phishing—led the way. Because these attacks take place on social media networks, well outside the network parameter and not on enterprise-owned accounts, traditional security tools are blind to them.
- **Cross-pollination between mobile and social takes off.** High-profile phenomena such as the Rio Olympics and Pokémon GO created openings to spread mobile malware, including mobile zero-day exploits, over social media. Traditional security tools have little visibility into either channel.

TOP THREATS & TRENDS, JULY - SEPTEMBER 2016

Some of the trends we highlighted in the second quarter continued in the third, with a few notable additions. The volume associated with major email campaigns, especially those distributing Locky, continued to increase. At the same time, the explosion of new forms of ransomware continued. Malicious attachments remained the dominant vector for email-based threats. But we did begin to see the re-emergence of larger URL-based campaigns pointing directly to hosted malware. Exploit kit activity leveled off near its June rate, leaving RIG as the primary EK player.

High-volume daily campaigns and high-profile ransomware infections dominated headlines throughout the first half of the year. But threat actors also continued to use email to establish beachheads for advanced persistent threats (APTs) and targeted attacks. Once malware is delivered through email, it opens the door for large paydays and further attacks.

Volume trends: Locky campaigns make Q3 the Everest of 2016… so far

Although volumes fell at the end of Q3, Locky remains a lucrative and successful strain of malware. It's no wonder it remains widely distributed by multiple attackers all over the world through email. The massive volume of messages and shifting attachment types are huge hurdles for anyone looking to stop it from reaching users.

Key stat: Messages delivering Locky accounted for 97% of malicious message volume in Q3.

Analysis: Locky utterly dominated malicious message payloads in Q3, appearing in 97% of them. August alone accounted for 63% of both Locky-bearing messages and overall malicious message volume for the quarter. Messages spreading malware through malicious document attachments rose 184% over Q2, but accounted for just 25% of total malicious message volume. Instead, more and more messages distributed Locky using zipped JavaScript files (a trend we also observed in Q2) as well attached .hta (HTML executable file) and .wsf (Windows Script File) files.

Message volumes fell sharply in September. As shown in Figure 1, the month started strong. Attack campaigns were among the largest we have ever observed, peaking at hundreds of millions of messages in a single day. But a subsequent drop left total volumes for the month short of their August peaks. In addition to the changes in distribution method, Locky itself also saw several updates, including new extensions for encrypted files.

Indexed Weekly Malicious Volume by Attack Type, 2016 YTD

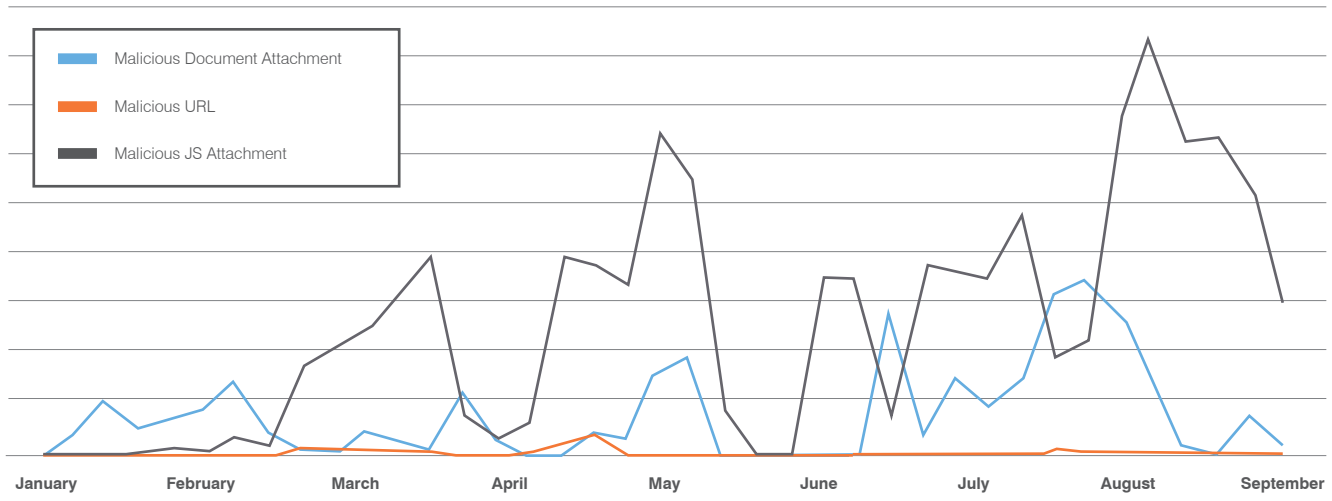

Figure 1: Year-to-date weekly malicious message volume by attack type

While Locky dwarfed all other types of email-distributed malware, it was the only ransomware strain in the top five malware types, as noted in Figure 2. The remaining four are all banking Trojans—or in the case of Pony, intermediate loaders associated with banking Trojans.

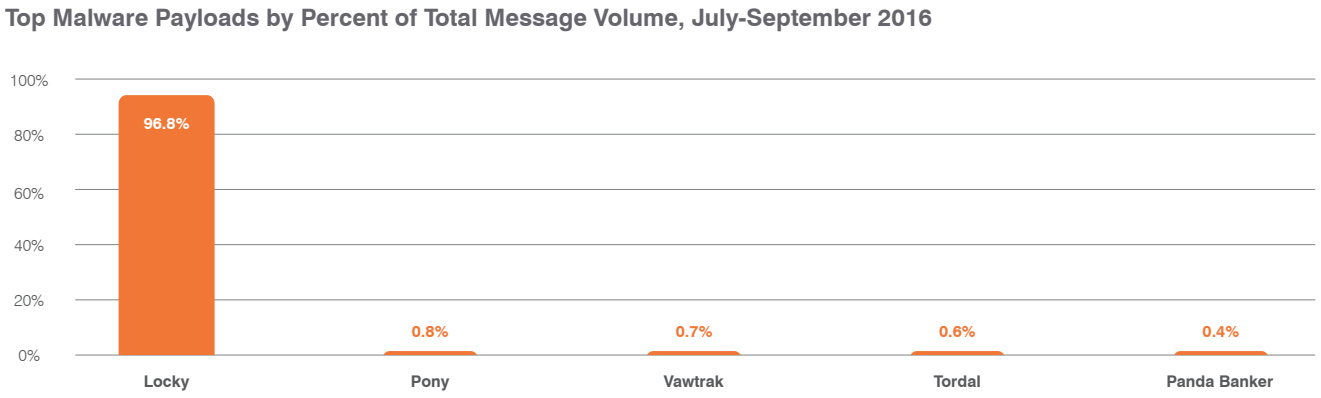

Figure 2: Top malware payloads distributed via email in Q3

Ransomware: Go big or go home

Ransomware can be costly. The FBI reported criminals collected $209 million in ransomware payments in the first quarter of 2016 alone, with estimated payments to surpass $1 billion by the end of the year. The direct costs of paying large ransoms to recover data can be significant. But greater indirect losses often stem from system downtime and loss of business, even if robust backup regimens allow data to be restored without paying a ransom.

Key stat: Observed ransomware families increased by 53% in Q3 vs. Q2, growing by a factor of 10x since 2015.

Analysis: Throughout Q3, ransomware remained a dynamic threat. Several new families appeared on the scene, and volume continued to grow. Other families all but disappeared. Still others failed to gain traction. Ultimately, Locky and CryptXXX were the two dominant ransomware families with Locky distribution predominantly through email and CryptXXX through EKs.

The disruption of the Necurs botnet in June dried up message volumes in Q2. But Locky reemerged in a big way in Q3, with message volumes growing 370% vs. Q2 volumes with appearances in several high-volume campaigns.

In Q3, Locky continued the trend of delivery via JavaScript attachments. The volume of malicious JavaScript attachments grew 69% quarter-over-quarter. Threat actors also began sending instances of Locky that can work “offline.” These variants can begin encrypting infected machines without checking into a command-and-control (C&C) server first.

Locky was the most widespread email threat. But other ransomware variants also appeared in high-volume campaigns, including CryptFile2, MarsJoke, and Cerber. MarsJoke was notable for using malicious documents hosted online—it was delivered via URLs rather than attached directly to email. This change appears to be a growing trend. Petya ransomware also reemerged near the end of the quarter; it’s one of the few variants that targets low-level disk structures, encrypting a system’s master boot record instead of encrypting files one by one. In addition, the ability to detect and encrypt network drives has become a standard feature of many ransomware variants, further increasing the risk to victims.

Figure 3 shows the rapid growth of ransomware variants since the end of 2015—nearly a tenfold increase. Although we estimate that half of ransomware families are inactive, the growth trend suggests that old families are being replaced by new variants at a steady rate. It’s tempting to think that these older variants no longer appearing in the wild are retired or deactivated, but experience shows that attackers can easily reactivate “old” malware, sometimes with minor or even no updates or to reuse code in new variants.

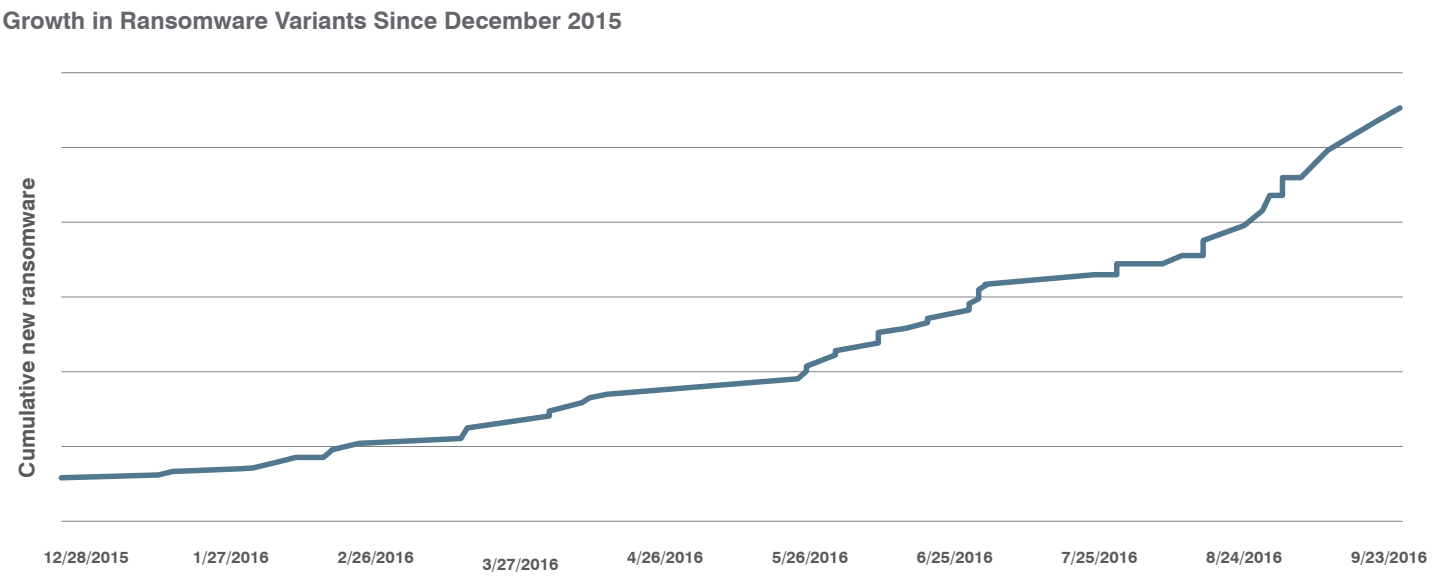

Figure 3: Indexed growth of ransomware families since December 2015

BEC adjusts tactics while generic phishing gets smarter too

The challenges of massive message volumes are compounded by fast-changing threats and advanced techniques that go beyond malware. Case in point: BEC. These carefully planned, socially engineered attacks go after single, large payouts. Manual security processes and regular updates are not enough to address these dynamic, hard-to-identify threats. Instead, they call for scalable, automated defenses against BEC and other advanced email threats. Large-scale credential phishing campaigns are also evolving, making them harder to detect without automated defenses. Gone are the days of clunky "419" schemes. Today's phishing attacks are sophisticated, socially engineered strikes.

Key stat: Display-name spoofing increased to almost 1-in-3 BEC messages.

Analysis: Reply-to spoofing—in which the "From" field is legitimate but the "reply-to" address belongs to the attacker—was used more than two times as often as display-name spoofing. This represents a slight shift from the 3:1 ratio we reported in The Human Factor 2016 report. Display-name spoofing, meanwhile, now appears in almost 1-in-3 BEC messages. This shift suggests that BEC scammers are shifting tactics as people and businesses grow wiser to these attacks.

By a large margin, the top subject line used in BEC attacks was once again "Request." The top five subject lines account for more than 20% of all observed BEC subject lines. While attackers have a handful of clear favorites, they employ a wide variety of subject lines. Figure 4 shows the relative volumes of the top subject lines associated BEC phishing attempts during July-September 2016.

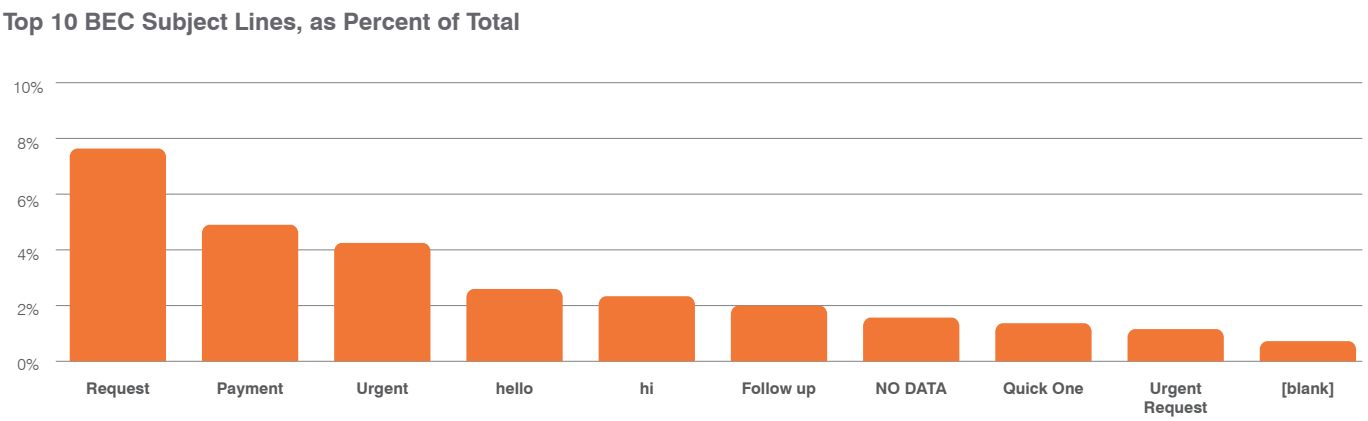

Figure 4: Top 10 BEC Subject lines as a percent of total observed incidents, July-September 2016

BEC and similar instances of email fraud capture headlines and yield FBI warnings because of the scale of the losses. But "traditional" phishing is increasingly sophisticated and remains widespread. We regularly observe campaigns that combine social engineering with carefully crafted pages that mimic banking sites, online services, social media logins, and more. Most are intended to capture login credentials. Others may steal more detailed banking or account information. Whether BEC or more broad-based, less targeted phishing, the potential damage to individuals and organizations can range from identity theft to substantial direct financial losses.

Banking Trojans diversify

The size of banking Trojan campaigns has shriveled with the shift to high-volume ransomware campaigns in the email space. Still, banking Trojans remain a serious threat, causing billions of dollars in losses. With improved targeting and evasion techniques—and better information-stealing abilities—they could pose a serious risk to organizations that lack intelligent protection.

Key stat: Banking Trojans made up only about 3% of all email-based threats this quarter by message volume. But these types of malware were increasingly targeted and delivered with personalized techniques and evasive macros.

Analysis: As high-volume malicious email campaigns have shifted to distributing ransomware, the once ubiquitous banking Trojans showed up in lower volume, increasingly personalized campaigns, a trend we first spotted in Q2. These Trojans were also observed being used heavily in massive malvertising operations, delivered via exploit kits and sophisticated targeting.

Without the lopsided dominance of Dridex that we observed in 2015 and the first quarter of 2016, banking Trojans also demonstrated a higher degree of diversity. Dridex rebounded in a number of personalized campaigns. At the same time, we also observed Ursnif, Panda Banker, Zeus, Gootkit, Cthonic, and several other banking Trojans in regional attacks. Two key trends emerged from these campaigns.

First, the Trojans themselves continue to add more features. They include:

- The ability to steal additional credentials and information
- Communication with C&C infrastructure via the Tor network, possibly making them harder to detect

Second, threat actors distributing the bankers are using more sophisticated techniques. Examples include:

- Using distribution methods that evade detection
- Building evasion techniques into macros
- Using low-profile exploits and steganography
- Co-opting trusted third parties like PayPal
- Improving targeting

Given that their web-injects must be configured for specific banks, banking Trojans always require a degree of regional targeting. But we have observed even stronger regionalization lately. For example, Ursnif is heavily focused on Australia, and Gootkit propagates mostly in Central and Southern Europe (Germany, Italy, and France).

Exploit kits: Where did everybody go?

Organizations should be prepared to monitor for threats from a greater number and variety of exploit kits. Smaller, more competitive malvertising and "drive-by download" markets are pushing attackers to innovate and jockey for market share. At the same time, due to malvertising campaigns explicitly targeting victims in Asian countries, organizations in Asia should verify that their defenses are ready for the campaigns' new geographic focus. Specifically, they must be able to detect traffic for new Asia-specific exploit kit variants.

Key stat: Total exploit kit activity fell by 65% in Q3 vs. Q2 and by 93% from January (the biggest month of 2016) to September.

Analysis: After seeming poised to take the place of Angler, the Neutrino EK faded in Q3. RIG, meanwhile, took more share in its place, growing from 5% to 50% of observed exploit-kit traffic. Still, these changes are taking place against the backdrop of a much smaller overall traffic volume. While the overall volume seems to have stabilized in Q3, it is 93% percent lower than what we saw for the first three months of 2016.

Large-scale malvertising campaigns of 2015 and early 2016— exemplified by the AdGholas campaign—have ceded to smaller-scale campaigns and a shift in geographic targeting. The widespread malvertising campaigns that we do see are targeting victims in Asian countries; examples include Magnitude, GooNky, and a variant of Neutrino. This regional shift appears to stem at least in part by efforts to avoid detection and exposure to online ad networks. In some cases, the campaigns include specific features or variants for Asia.

The disappearance of major players and the overall contraction in the space has disrupted the field. As the remaining players work to hang onto market share, new variants of major exploit kits such as RIG and Neutrino have emerged. Attackers that had used other EKs before are now also building new kits.

At the same time, smaller EKs such as Sundown are staying active, and some older or more obscure kits are resurfacing. The result: a more competitive environment.

Top Exploit Kit Activity as Percent Total, June-September 2016

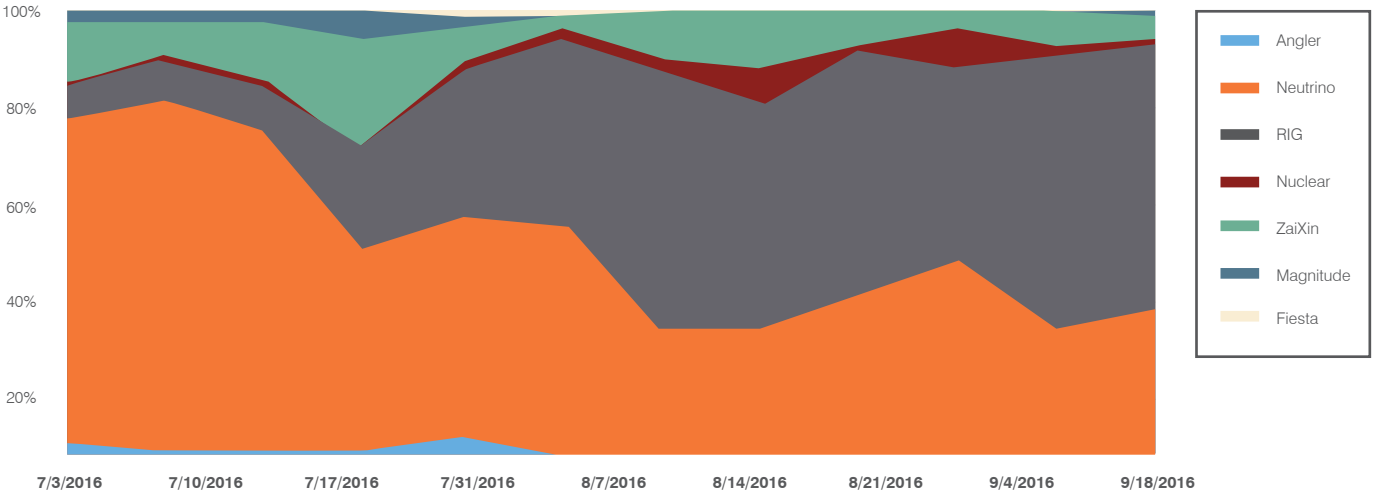

Figure 5: Top exploit kit activity as a percent of total observed EK traffic, July-September 2016

Indexed Trend of Top Exploit Kit Activity, 2016 YTD

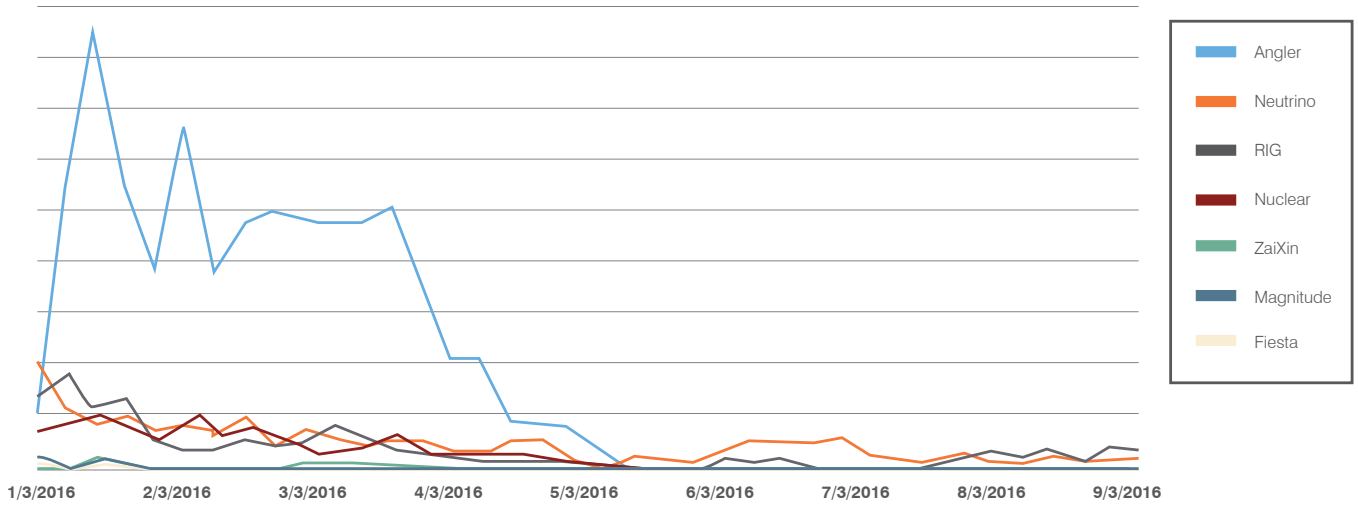

Figure 6: Indexed trend of top exploit kit observed activity, July-September 2016

Mobile app threats: Not playing games

Pokémon GO is one high-profile example of an app whose popularity has created an ecosystem of mobile threats. Games are a major target, as are apps related to major events. Some apps are overtly malicious, and others create business risks by requiring excessive permissions or handling data poorly. Whether downloaded by employees or their family members, malicious and other risky apps are following users into the workplace.

Key stat: Nearly 5% of mobile devices on corporate networks are running Pokémon GO.

Analysis: Released in July, Pokémon GO was an immediate international sensation. Because of its staggered global release, pent-up demand led users who could not access it through legitimate app stores to sideload the app through third parties and direct downloads. Within three days of Pokémon GO's release in Australia and New Zealand, we identified a cloned version of the Android app in a malware repository. The counterfeit copy included DroidJack, a remote access Trojan capable of taking over the device, and modified app permissions indicated in Figure 7. Though not observed in the wild, this version of Pokémon GO showed just how easily attackers could modify a popular app and distribute a malicious version to users.

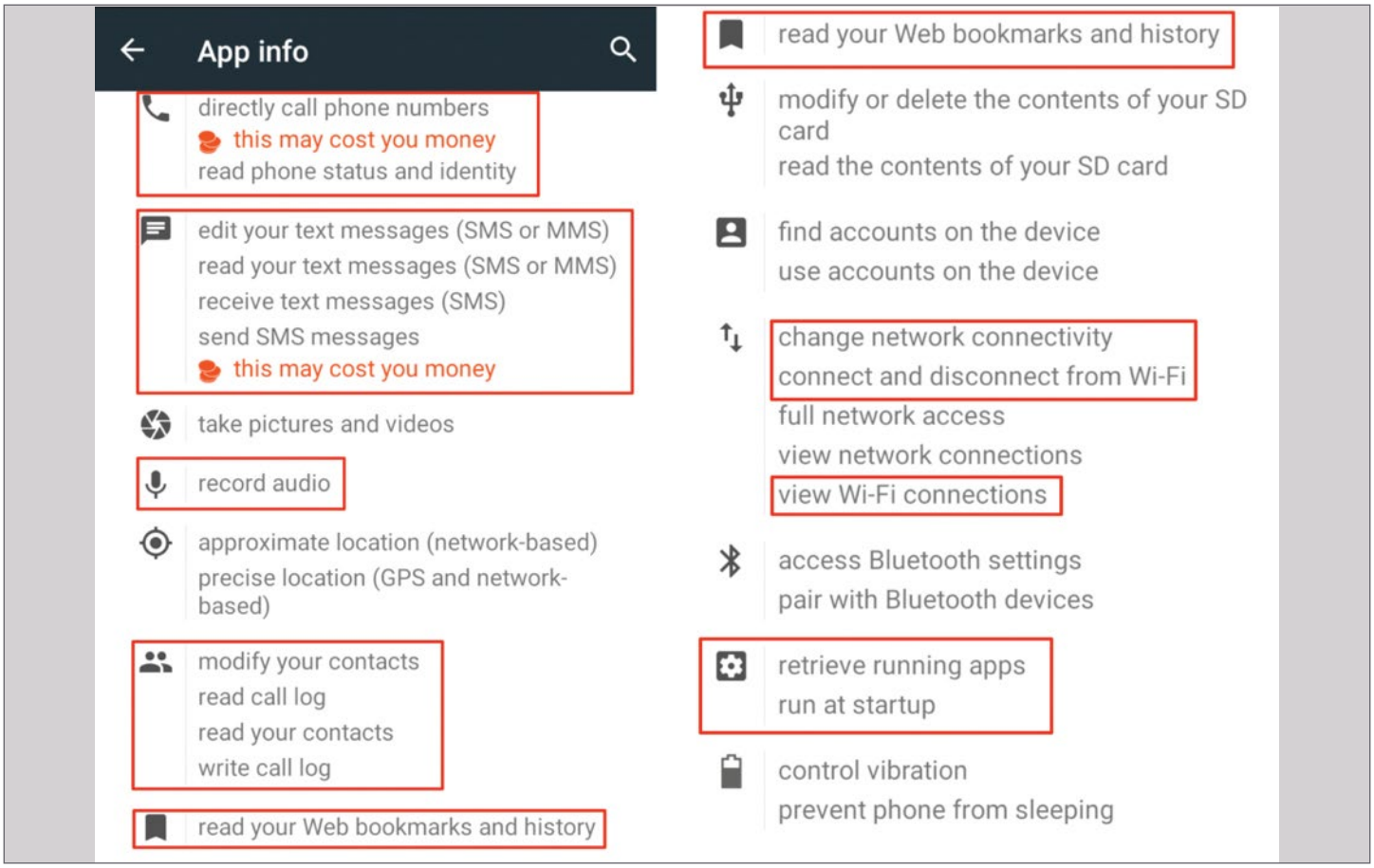

Figure 7: Modified app permissions for a malicious clone of Pokémon GO

A recent survey showed that Pokémon GO is installed on nearly 5% of mobile devices accessing corporate networks. Like many popular games, Pokémon GO has spawned numerous game guides, cheats, and add-ons. Many of them are risky or malicious, potentially exposing networked resources to attackers. We have identified at least three malicious versions of Pokémon GO this quarter along with numerous malicious companion apps. Even among legitimate installations, 4% of devices accessing corporate networks were an early version of the game that granted excessive permissions.

The Olympic Games in Rio also provided further examples of ways in which threat actors co-opted popular phenomena for malicious purposes. We identified over 4,000 Android apps and over 500 iOS apps related to the Olympics that exhibited risky or malicious behaviors.

Mobile threats continue with Pegasus and other zero-day tools

Most mobile devices have multiple serious, unpatched vulnerabilities that could expose them to a slew of malware and attack vectors. This includes both Android and iOS devices. As mobile devices become primary means of daily work and regular communication, these vulnerabilities can have serious consequences. That's why organizations need dynamic, intelligent protection and management.

Key stat: The average mobile device has between 10 and 20 exploitable zero-day vulnerabilities.

Analysis: In August, we found that the so-called "Pegasus mobile device attack kit" was available in both the criminal underground and the research community. This kit can be used to attack any device that is running any iOS version between iOS 7 and iOS 9.3.5. Although the malware originally surfaced as a result of a high-profile attack on a political dissident in the United Arab Emirates, it can be used against any person or enterprise with a vulnerable device.

Like many other types of both mobile and desktop malware, Pegasus can be delivered through a URL with a convincing lure. Because it targets mobile devices, the link can be distributed via SMS, email, social media, malicious search results or even other apps. When installed, Pegasus exploits a vulnerability in many versions of iOS. It silently roots the phone and gains unencrypted access to a variety of apps and communication on the phone.

Apple's rapid response with an update to iOS and the significant public attention the issue received helped mitigate the immediate risk. But Pegasus was only the best known of such malware: the average mobile device has 10 to 20 exploitable zero-day vulnerabilities that can be targeted by mobile malware. Roughly a third of these are serious flaws that enable attackers run malicious code. Figure 8 shows the number of mobile operating system vulnerabilities that have already been fixed in 2016.

Mobile OS vulnerabilities fixed in 2016

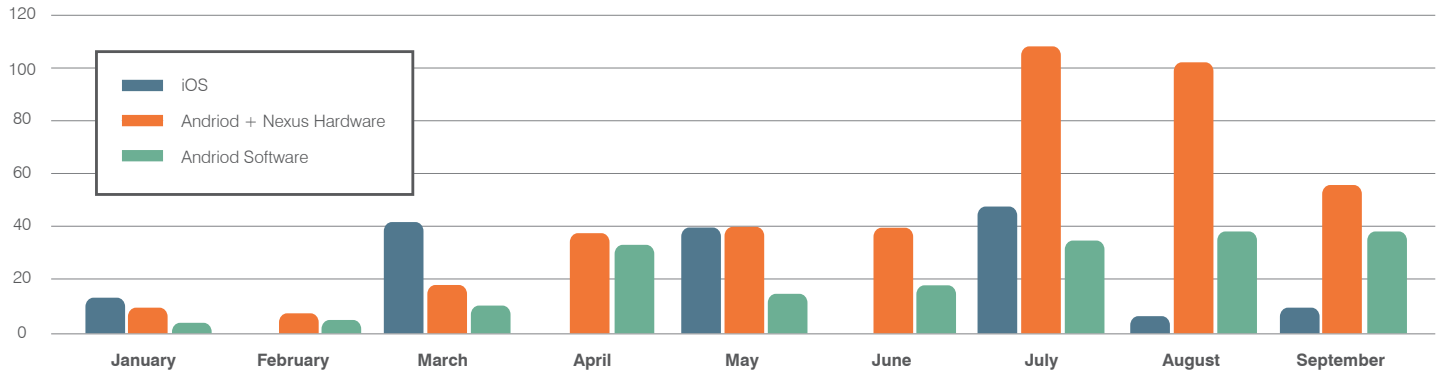

Figure 8: Mobile OS vulnerabilities fixed to date in 2016

Social media: Breeding ground for phishing and malware

Social media channels present a myriad of opportunities for threat actors to attack users, brands, and organizations. Popular trends and events drive traffic to fraudulent pages and accounts. At the same time, organizations must contend regularly with high volumes of spam and objectionable content. Regardless of the underlying motivation, the risks to both brands and people are significant, exposing them to phishing, malware, and potential harm.

Key stat: Between Q2 and Q3, social phishing increased by over 100%

Analysis: Q2 phishing on Facebook, YouTube, LinkedIn, Twitter, and Instagram more than doubled vs. Q2 and quadrupled vs. the year-ago period. This includes both general phishing and "angler phishing," where attackers use fake support accounts to intercept customers asking for help through an organization's social media account.

Phishing Attempts in Social Media, January – August 2016

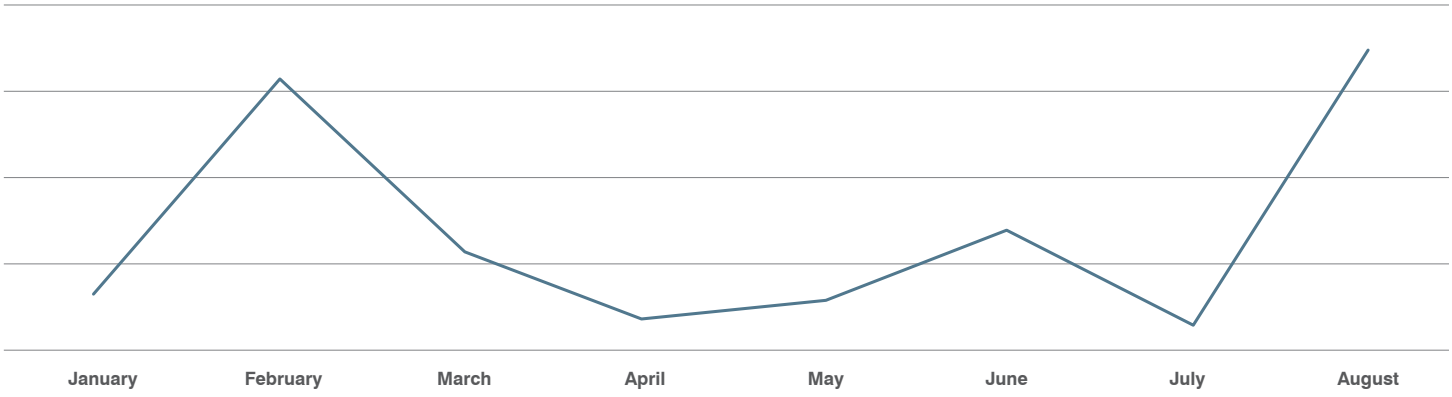

Figure 9: Social phishing by month

Aside from phishing, spam, adult language, and malicious links continue to be a key part of the social threat landscape. Such incidents increased 50% in Q3.

The Rio Olympics proved to be fertile ground for social media scams and malicious content. Along with social media attention surrounding Pokémon GO, popular trends fueled phishing, scams, and malware distribution through social channels. For example:

- Of 1,310 social media accounts with ties to the Olympics and sponsoring brands, 15% were fraudulent with 400,000 subscribers among them.
- Of 543 social media accounts related to Pokémon GO across Facebook, Twitter, and Tumblr, 167—over 30%—were fraudulent. Many distributed either desktop or mobile malware.

PROOFPOINT RECOMMENDATIONS

Based on the developments in the threat landscape detailed in this report, we recommend the following to protect yourself against the latest attacks:

- Preventing ransomware infections at the email and network gateways remains the best strategy for reducing costs and ensuring business continuity. Ransomware variants that do not rely on communication to C&C servers can evade network and endpoint-based solutions that focus detection on attempts to communicate with malicious IPs. Use security solutions that can share intelligence across various attack vectors (email, network, endpoint, and so on). Focus on catching threats before they enter your network and reach people.
- Ransomware also has a people and process component that technology alone cannot solve. The large volume of ransomware-dominated email campaigns makes it doubly important to regularly back up your organization's data. IT and security departments should also have a plan and process in place for restoring data in case of an attack. With ransomware, backing up data is both a prevention and remediation step. So are education and training to recognize and report it.
- Low-volume, personalized campaigns can be more difficult to detect. Invest in security solutions with predictive and behavioral detection capabilities so similar threats with different hash values can still be recognized and stopped.
- Be aware of fake, malicious apps piggybacking off popular apps. Never download apps from rogue marketplaces, even if they look like the real thing. Your mobile device can be infected even without jailbreaking the OS.
- Mobile vulnerabilities are more common than you think. Updating apps to their latest version is always wise. But that alone won't tell you if you already have a risky or malicious app on your device. Invest in mobile threat defense solutions to scan for compromised apps on devices in your environment and alert you to risky and malicious app behavior.
- Be aware of risks to your brand through attackers' use of fraudulent social media sites. Invest in tools that provide visibility into your organization's social media footprint and alert on fraudulent uses of your brand. Train your people to be mindful of clicking on links on social media sites, especially those advertising downloads to "too good to be true" deals or cashing in on popular trends. Have them always double-check that the social media site they visit is an organization's official site and not a fraudulent lookalike. Look for clues such as number of followers, verified account badges, and registered domains listed in web links.