APR-JUN 2016

proofpoint™

QUARTERLY THREAT SUMMARY

The Proofpoint Quarterly Threat Summary captures threats, trends and transformations we see within our customer base and in the wider security marketplace. Each day, we analyse more than one billion email messages, hundreds of millions of social media posts, and more than 150 million malware samples to protect organisations from advanced threats.

Analysing how these threats shift quarter over quarter provides ample opportunity to identify larger trends and equip organisations with actionable intelligence and recommendations for managing their security posture. We continue to see sophisticated threats across three primary vectors: email, social media and mobile.

www.proofpoint.com

KEY TAKEAWAYS

Volume, variation, and then silence
The first five months of 2016 were dominated by malicious email campaigns of unprecedented volume. New ransomware variants emerged quickly. Meanwhile, Dridex actors began distributing Locky ransomware and repeatedly shifted tactics with new loaders, document attachment types, and obfuscation techniques to evade detection.

Then at the end of May, one of the largest botnets in the world suddenly went dark. The change brought Dridex and Locky distribution to a near halt. At the same time, the hugely popular Angler exploit kit (EK)—an all-in-one toolkit that largely automates web-based cyber attacks—went silent. Together, these shifts led to an eerily quiet June.

Social media threats such as fraudulent customer service accounts continued to proliferate.

Mobile threats targeted multiple vulnerabilities. These threats focused largely on taking over victims' devices and on malicious adware, especially in older versions of Android. Below are key takeaways from the second quarter of 2016.

EMAIL AND EXPLOIT KITS

- **JavaScript attachments led an explosion of malicious message volume – 230% quarter over quarter.** Many Locky and Dridex actors turned to JavaScript files attached to email messages to install payloads. These attacks were among the largest campaigns we have ever observed, peaking at hundreds of millions of messages a day.
- **Ransomware: Locky dominated email, while CryptXXX dominated EK traffic.** Among email attacks that used malicious document attachments, 69% featured the new Locky ransomware in Q2, versus 24% in Q1. That surge propelled Locky into the top spot for email-based malware, displacing Dridex. CryptXXX appeared on the scene in Q2 and quickly dominated the EK landscape. Overall, the number of new ransomware variants (most distributed by EKs) grew by a factor of 5 to 6 since Q4 2015.
- **Highly personalised campaigns scale up.** Threat actors conducted highly personalised campaigns at scales of tens to hundreds of thousands of messages. This is a change from the much smaller campaigns that have used personalised and targeted lures in the past.
- **Business email compromise (BEC) attempts surprisingly common.** 80% of a representative sample of Proofpoint customers experienced at least one BEC phishing attack in the last month. Attackers also changed lures based on seasonal events such as tax reporting and varied their approaches to increase the effectiveness and scale of the attacks.
- **June idyll?** Exploit kit traffic observed by Proofpoint dropped by 96% between April and mid-June. The Necurs botnet went offline in June, silencing the massive Locky and Dridex campaigns that defined the first half of 2016. Traffic from the Angler EK had completely disappeared by early June, shortly after the Nuclear EK had shuttered operations. That left Neutrino as the top EK by the end of June.
- **Locky ransomware returns.** By the end of June, the first large Locky email campaigns were beginning again with all signs pointing to a return of the Necurs botnet. It remains to be seen whether the exploit kit landscape will see a similar return to form over the coming quarter.

MOBILE

- **As many as 10 million Android devices were compromised by exploit kits.** The EKs targeted multiple vulnerabilities that let attackers take control of the devices. In most cases this control was used to download adware that generated profits for threat actors.
- **98% of mobile malware is still associated with the Android platform.** This proportion is holding steady from last quarter.

SOCIAL MEDIA

- **Social media phishing attempts rose by 150%.** Organisations continued to cope with spam, adult content, and other issues that overwhelmed their ability to resolve the issues manually.

TOP THREATS & TRENDS, APRIL - JUNE 2016

The second quarter saw a continuation of the trends we highlighted in the first quarter. In particular, the volume associated with major email campaigns, especially those distributing Locky and Dridex, continued to increase. At the same time, the explosion of new ransomware that we observed in Q1 only accelerated. Malicious attachments remained the dominant vector for email-based threats. Still, we did see some crossover in the exploit kit space with URLs in emails leading to compromised sites and even direct downloads of malware.

High-volume daily campaigns and high-profile ransomware infections have dominated headlines throughout the first half of the year. But email continues to sit on the front lines of advanced persistent threats (APTs) and targeted attacks. Once malware is delivered via email, it opens the door for large paydays and further attacks.

BEC phishing keeps reeling them in

Key stat: 80% of a representative sample of Proofpoint customers were targeted with at least one BEC message in the last 30 days.

BEC attacks continue to evolve. Attackers are experimenting with new techniques and approaches. For example, BEC attempts have begun to feature broad-swath attacks, in which threat actors broadcast emails to a larger group of recipients within a target audience. Attackers also appear to be mixing legitimate emails more often with BEC to better evade detection.

The top BEC subject line was “Request”, representing 11% of BEC attacks seen across our customer base in Q2. This occurred as frequently as the next three subject lines (“URGENT”, “w2”, and “Follow up”) combined. Figure 1 shows the relative volumes of the top subject lines associated BEC phishing attempts during May.

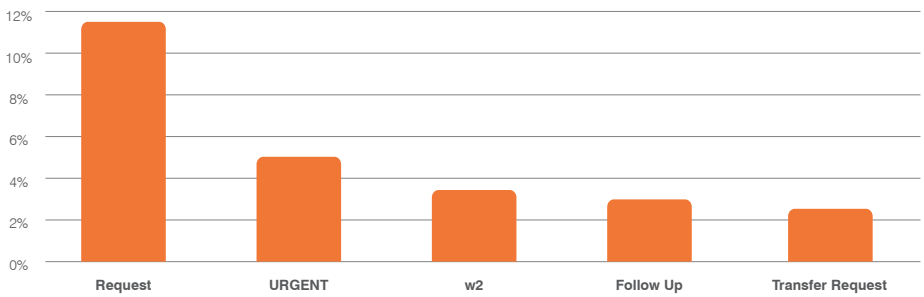

Figure 1: Top subject lines from mail identified as BEC phishing during May 2016

What this means: Technical defenses such as enhanced email firewall rules, combined with user training, can significantly reduce the risk from these threats. At the same time, attackers are improving their effectiveness faster than people can be trained to look for new threats. BEC attacks are also increasingly common. That is why automated advanced email threat defenses are essential to staying ahead of this high-yield threat.

Growth in Ransomware Variants Since December 2015

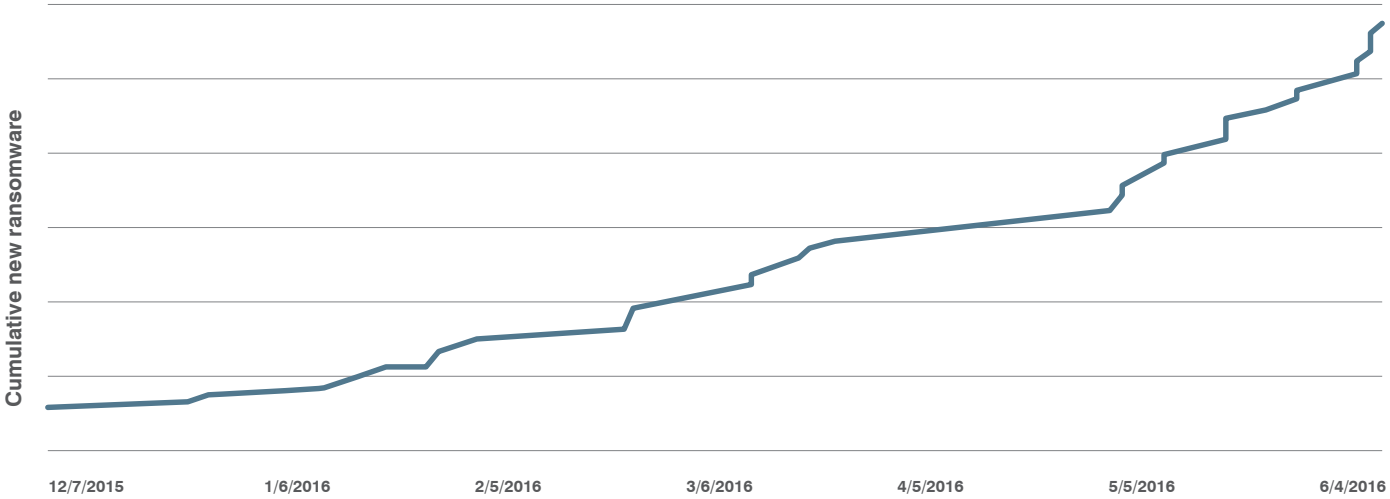

Figure 2: Ransomware family growth since December 2015

Ransomware everywhere

Key stat: Among email attacks we observed in Q2 that used malicious document attachments, 69% featured Locky ransomware. This is a 45% increase over Q1 for Locky alone. Meanwhile, the number of ransomware families has grown by as much as 600% since December.

Measured by raw message volume, Locky ransomware overtook the infamous Dridex banking Trojan in Q2. When the Necurs botnet returned to activity after its June outage, the first observed payload was Locky. Cerber emerged as a frequent Locky alternative during the June outage, but neither it nor any other ransomware variants were among the top 10 payloads during that period.

Exploit kit activity also heavily favored ransomware. CryptXXX dominated the ransomware space with widespread propagation, first via Angler exploit kit and then, later in the quarter, via Neutrino. Moreover, CryptXXX was the biggest fish in an increasingly crowded pond.

Figure 2 shows the growth of a representative sample of new ransomware families since December. These figures are not exhaustive, but they do reflect the growing diversity of ransomware, whether distributed via email, exploit kit, or other vector. At the end of June, threat actors who had been distributing instances of Dridex and Locky appeared to initiate a large-scale test of a new ransomware family called “Bart.” Unlike many other variants, Bart does not require a connection to a command-and-control infrastructure to encrypt files.

What this means: Ransomware is back in a big way with new variants and techniques emerging regularly. Organisations need defenses that can stop these destructive attacks before they can encrypt data and take critical systems offline.

JavaScript attachments led explosion of malicious message volume

Key stat: Malicious email message volume using attached JavaScript files jumped 230% from Q1. Hundreds of millions of messages targeted our customer base across multiple campaigns.

The volume of messages with malicious URLs changed little from Q1. Malicious attachment volumes actually decreased, primarily because of the June Necurs disruption. But even with the Necurs outage, malicious attached JavaScript files rose more than 230% vs. Q1. These messages were virtually unseen in 2015.

What this means: The already massive volume of malicious messages hitting organisations continues to increase, despite a nearly month-long disruption in one of the world’s largest botnets. The volume of malicious JavaScript attachments in particular has reached levels never seen before, representing a threat that far exceeds the means of most security teams and manual processes. Organisations must have a scalable, automated defense against email-based advanced threats that can adapt to new techniques and approaches.

Indexed Weekly Malicious Volume by Attack Type, 2016 YTD

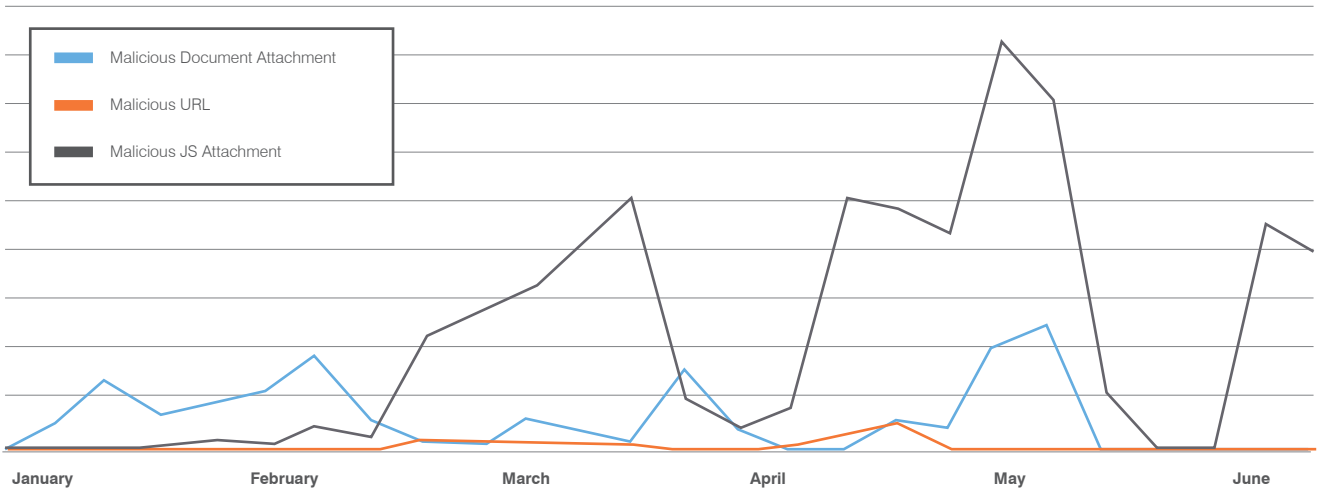

Figure 3: Indexed weekly volume of malicious messages by attack type, January-June 2016

Variation of distribution, infection chains, and payloads

Key stat: Locky displaced Dridex as the top malware payload. Among the top 10 malicious email we observed in Q2, the ransomware strain accounted for 41% of all payloads.

Locky displaced Dridex in Q2 as the top malware payload, nearly doubling its share in the top 10 email-based threats. The landscape is not as skewed towards a single type of malware as in the past, though. Two malware loaders (RockLoader and Pony) and an information stealer (Kegotip) round out the top five payloads. RockLoader is used mostly to deliver Locky and Dridex; the share of Locky/Dridex malware might have been considerably higher without the Necurs botnet disruption.

Still, RockLoader is just one example of the recent surge in new methods of delivery. These methods include links to exploit kits on compromised content management systems and multiple infections chains that combine malicious documents and JavaScript.

Our researchers have also observed:

- Multiple payloads being distributed in a single campaign,
- Highly personalised large scale attacks
- Rotating and geo-targeted lure documents
- A “crossover” campaign that attached malware to credential phishing

In short, threat actors are using a wide variety of techniques to expand attack surfaces and capitalise on clicks in socially engineered attacks.

Top Malware Payloads by Indexed Message Volume (April-June 2016)

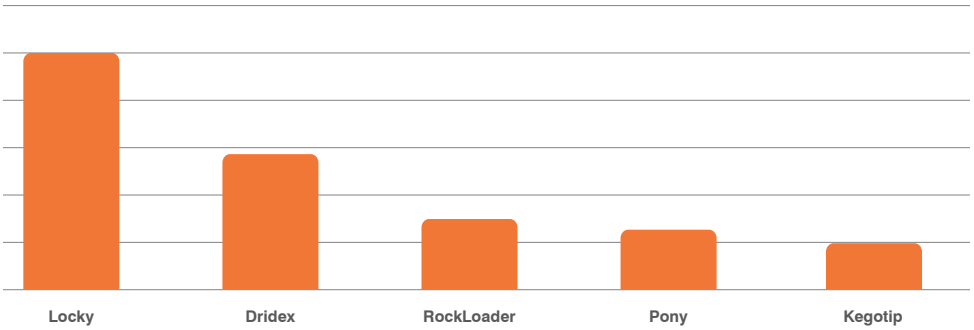

Figure 4: Relative volumes of the top five email-based malware threats

What this means: The challenges to organisations from massive message volumes are now being compounded by fast-changing threats and innovative techniques for delivering malware to users. Manual processes and periodic updates are not sufficient to address the dynamic, diverse nature of these threats. Instead, organisations must have scalable, automated defenses against email-based advanced threats.

Top Exploit Kit Activity (Indexed), April-June 2016

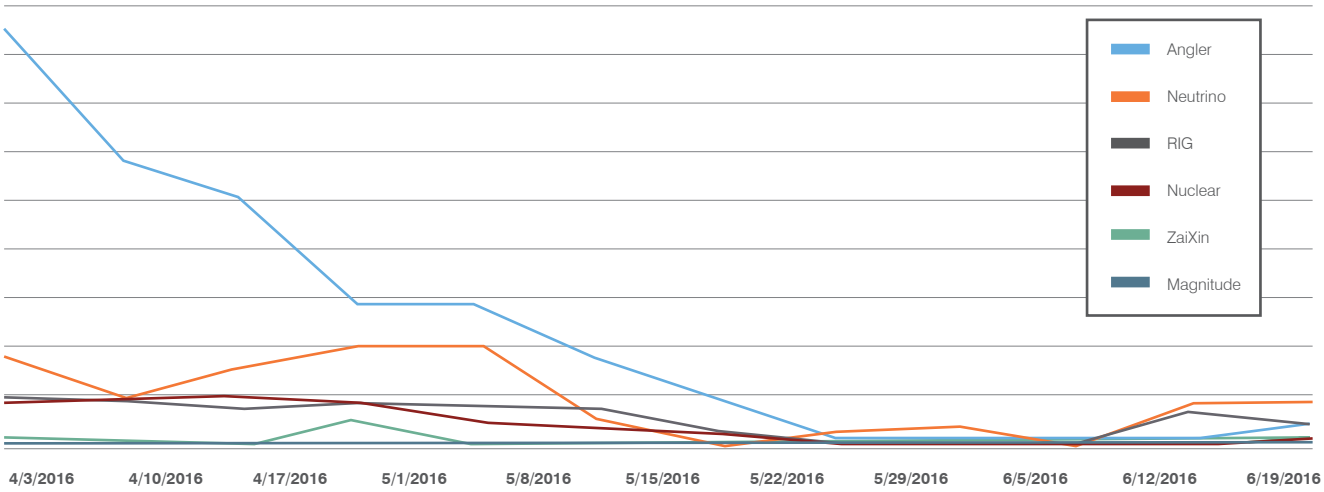

Figure 5: Exploit kit activity dropped precipitously during Q2

Angler takes a break and exploit kit volume plummets

Key stat: Exploit kit traffic observed by Proofpoint dropped 96% from April to mid-June.

Attackers consolidated around Angler EK in 2015 through Q1 2016, when it accounted for 60% of total EK traffic. But Angler activity dropped precipitously in Q2 helping drag total EK activity down 96% by mid-June.

With Angler going dark, many actors (include those distributing CryptXXX ransomware) shifted their malware to Neutrino, an EK we observed gaining traction in Q1. Other threat actors suspended projects that leveraged exploit kits entirely. As Q2 drew to a close, overall EK activity began to slowly rebound but remained a fraction of Q1 levels.

What this means: While temporary lulls in activity are not uncommon; the Q2 pause is the third (and largest) in the last year. These lulls can reflect law enforcement activity, seasonal changes, and other unexplained disruptions to criminal infrastructure. In every case, activity rebounded to levels exceeding those before the disruption. We do not expect this change in the EK landscape to be permanent, but it remains to be seen if another player will reach Angler-like levels of dominance and activity in the near future.

The relative quiet from Angler has also given other EKs like Neutrino and RIG an infusion of activity and, presumably, development efforts. For targets, EKs continue to be an important infection vector that sometimes crosses over into email-based URL threats, varied roles in advanced persistent threats, and a thriving malvertising ecosystem. Beyond their normal patching efforts, organisations need to continually monitor threat intelligence sources to track and patch the vulnerabilities exploited by EKs.

Mobile Malicious Apps Focus on Device Takeover and Malicious Ads

Key stat: As many as 10 million Android devices were infected by a mobile exploit kit targeting multiple vulnerabilities.

In the second quarter, we saw an increase in apps that are using known rooting exploit vulnerabilities to compromise devices, install fake apps, and push advertising to users without their consent.

In particular, we saw apps that used a “cocktail” approach, blending multiple vulnerabilities, each capable of taking over a device, to compromise as many versions of devices as possible. This type of activity targeted Android, and apps that use the EKs infected as many as 10 million devices. They typically target devices running versions of Android 5.1 and older. Once a device is compromised, other apps are downloaded to the device without the user’s consent. These apps display malicious ads, generating profits for the attackers.

The malicious apps are available on numerous app stores. But we have also found links to download apps advertised in spam email and SMS messages distributed to users around the world. For example, we found the HummingBad-infected “Swiping Whale” app on several app stores. But it was also offered to users through links in spam messages, hosted directly on a variety of private websites—in much the same way that Windows malware is distributed.

What this means: While mobile malware is an evolving field, the threat landscape on mobile increasingly looks like the landscape for desktops. Exploit kits, malicious downloads, and adware are all making an appearance, especially on Android platforms. As mobile devices increasingly replace or reach parity with desktops in the enterprise, organisations need to adopt mobile defenses that integrate with MDM solutions and dynamically inspect mobile apps for risk and malicious intent. At the same time, these mobile defenses need to be backed up with the same types of threat intelligence that characterise our approach to the rest of the enterprise.

Social Media Phishing on the Rise

Key stat: In the first six months of 2016, we have already seen a 150% increase in social media phishing attacks when compared to the same period last year.

Social media is increasingly the public face of many brands—in many cases more so than a traditional web presence. It's no wonder that cyber criminals are leveraging social media to attack customers. Like an anglerfish uses a bioluminescent lure to entice and attack smaller prey, the glowing lure in this case is a fake customer support account that promises to help a brand's customers but secretly steals their credentials instead.

At the same time, social media spam, adult language, and malicious links continue to plague social media channels. They all create risk to brands and threaten the value these channels provide.

What this means: Social media provides an excellent channel to engage with customers. However, if interactions are threatened by phishing attacks or risky content, customers walk away and brands struggle to manage their social channels. Automated solutions for identifying and mitigating risks like angler phishing and spam are critical to keeping social channel clean and useful to their associated brands.

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:

- Given the sheer volume of attacks coming through email, invest in mail gateway solutions capable of detecting and preventing advanced attacks and those that do not involve malware. This step helps minimise the number of threats coming into the network. Once these threats are the network, malware and malicious traffic may be more difficult to detect and distinguish from legitimate business traffic.
- Never allow emails with attached executable code to be delivered. Likewise, do not allow people to share code over email. Enact simple rules that block .exe or .js attachments to prevent obvious malicious exploits from entering your environment.
- With the increase of social media phishing, be aware of external risks targeting your users, especially using fraudulent accounts. Deploy security solutions that give you visibility into your social media risks. Train your people to recognise social media phishing attempts.
- Attackers use a variety of methods to target your organisation and colleagues; deploy security solutions that can correlate activity across threat vectors. That capability gives you deeper insight into attacks to help you resolve them, block future attacks, and more easily detect those that do get through.