2016

proofpoint™

Q4 2016 & YEAR IN REVIEW

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.

TABLE OF CONTENTS

KEY TAKEAWAYS: BIGGER, FASTER, MORE

Building on trends we saw throughout 2016, cyber attackers shifted their techniques and approaches in the fourth quarter to maximize returns on investments in malware and infrastructure. Message volume from malicious email campaigns rose dramatically. Tactics used to evade cybersecurity tools grew more sophisticated. Business email compromise (BEC) attacks evolved as attackers found new ways to impersonate executives and trick victims into sending money or sensitive data. And the market for exploit kits—easy-to-use tools for exploiting system vulnerabilities—imploded as threat actors doubled down on human exploits and social engineering.

Attacks that used traditional exploit kits (EKs) stabilized by the end of the year, with Q4 activity far lower than Q1 levels. But EKs targeting mobile devices and internet-of-things (IoT) devices such as home internet routers emerged, reflecting the growing availability of exploitable vulnerabilities in this emerging space. Social media also saw spikes in malicious activity around major events and popular trends. Negative, damaging, and malicious content increased dramatically on social channels. This activity included "angler phishing," a term we use to describe attacks that involve fake customer-support accounts that trick people seeking help into handing over their login credentials and other information. These threats all demonstrate strong ROI for attackers.

Below are key takeaways from the last quarter and an overall look at 2016.

EMAIL AND EXPLOIT KITS

Q4's largest malicious email campaign was 6.7 times the size of Q3's largest. Both campaigns involved the Locky family of ransomware and were sent using compressed files and malicious JavaScript code, marking a sharp increase in these tactics compared to earlier campaigns that used document attachments with malicious macros embedded.

Malicious JavaScript attachments regularly outnumbered attached document message volumes by a factor of four to six. Actors also used a variety of other script types like .vbs and .wsf, all in an effort to evade detection.

Overall exploit kit activity held steady in Q4 but fell 93% from its Q1 high. Some activity that might have used the popular Angler EK migrated to the RIG and Neutrino EKs. (The Angler EK—which is not related to social-media based angler phishing—disappeared at at the end of Q2.) Overall, the EK market has largely been relegated to mid-level operators of malvertising, online ads embedded with malicious code designed to exploit web browser vulnerabilities.

CEO-to-CFO spoofing dropped 28 percentage points between August (when it represented 39% of all email from attackers posing as a CEO) and December; DMARC adoption grew 33% between Q3 and Q4. Organizations are becoming more aggressive in how they address business email compromise (BEC) phishing. But BEC actors are adapting as well, employing more effective techniques such as sending spoofed emails to rank-and-file workers.

The number of new ransomware variants increased 30 times vs. the year-ago quarter. Locky was responsible for the bulk of ransomware volume, but the number of variants continues to grow quickly. Standouts include Cerber and CryptXXX, which were distributed through email and EKs.

MOBILE

Hundreds of thousands of mobile devices were potentially exposed to attacks that redirected users to malicious websites through the DNSChanger EK. Using a technique called DNS redirection, these potential attacks included malvertising and ad redirection. The EK does not exploit mobile device vulnerabilities. Instead, it takes advantage of flaws in network routers used in homes and small offices that connect mobile devices to the internet.

MOBILE (CONTINUED)

4,500 mobile apps related to the Summer Olympics and sponsor brands were risky or malicious. Threats in mobile and social often piggyback major events and popular phenomena; risky apps that potentially leak data are commonplace on both major mobile platforms.

SOCIAL MEDIA

Fraudulent accounts across social channels doubled from the third to fourth quarter. These accounts may be used for phishing, social spam, malware distribution, and more.

Social media phishing attacks increased 500% during the year. This includes angler phishing that intercepts customer support channels on social media.

Q4 HIGHLIGHTS

The fourth quarter of 2016 saw substantial variation in payloads, timing, and techniques used to deliver malware and attack businesses and consumers even beyond the volume and variety we observed throughout 2016. From Locky campaigns of unprecedented size to attacks on home routers via malvertising, threat actors continued to innovate and experiment.

MALWARE & EMAIL THREATS

Email remained the top vector for malware as exploit kits (EKs) continued to decline and vendors rapidly addressed zero-day vulnerabilities making EKs less effective. Several factors complicated detection efforts, both at the end user and antivirus levels:

- Social engineering
- High-volume spam
- Low-volume targeting and personalization
- Continued increases in the use of email attachments other than Microsoft Word and Excel (e.g., JavaScript, RAR archives, etc.)
- URL distribution via trusted platforms like Microsoft SharePoint or typosquatted variations on apparently trustworthy URLs

The malware itself continued to evolve as well, with social components appearing in the ransomware space and malicious macros getting more sophisticated.

Q4 EMAIL THREAT VOLUME AND TECHNIQUE TRENDS

Sheer volume remained an important part of the email threat landscape at the end of 2016. Locky ransomware in particular was delivered via the largest spam campaigns we have ever observed and dominated malicious email traffic for the quarter.

Key Stat: The largest email campaigns distributing Locky ransomware were 35% larger than the largest campaigns of Q3, itself a record-setting quarter.

Analysis: The erratic campaign activity from the middle of 2016 was on display again in the fourth quarter. We observed three major pauses in Locky spam: two weeks in October, one week in November, and -- consistent with last year's holiday pause -- the last week of December. However, volumes remained very high, with the use of attached JavaScript and zipped JavaScript to deliver Locky payloads driving the majority of this activity. The largest of these campaigns in Q4 exceeded the volumes of the largest Q3 campaigns by 35%.

In addition to high-volume campaigns distributing Locky via JavaScript attachments, we also observed large Locky campaigns using

- Microsoft Word and Excel document attachments with malicious macros
- URLs linking to zipped JavaScript files and malicious documents
- Zipped VBScript files

A key difference in the fourth quarter was in the combination of these techniques. Whereas during the period from February through September the large-scale Locky campaigns relied on a single type of attachment, in the fourth quarter we regularly observed two or three of these techniques at use in a single campaign.

That latter months of 2016 also marked a renewed use of URLs, albeit linking directly to malicious payloads rather than to the exploit kits that characterized campaigns of 2013 and 2014. Although still relatively rare throughout 2016, malicious URL use in email campaigns rebounded in November, led by a threat actor distributing Vawtrak in US-targeted campaigns. URLs often linked to malicious zipped JavaScript hosted or malicious documents on dedicated servers, or to SharePoint links hosting zipped JavaScript.

The largest of these campaigns by message volume were sent by an actor distributing Vawtrak. These were URLs leading to malicious document downloads and were sometimes combined with malicious document attachments. Traditionally this actor only sent email campaigns with document attachments alone and, like many of the actors we track, appeared to be experimenting with new delivery methods, finally settling on the use of links with recipient emails base-64 encoded in the URL.

The timeline below illustrates the evolution of these campaigns:

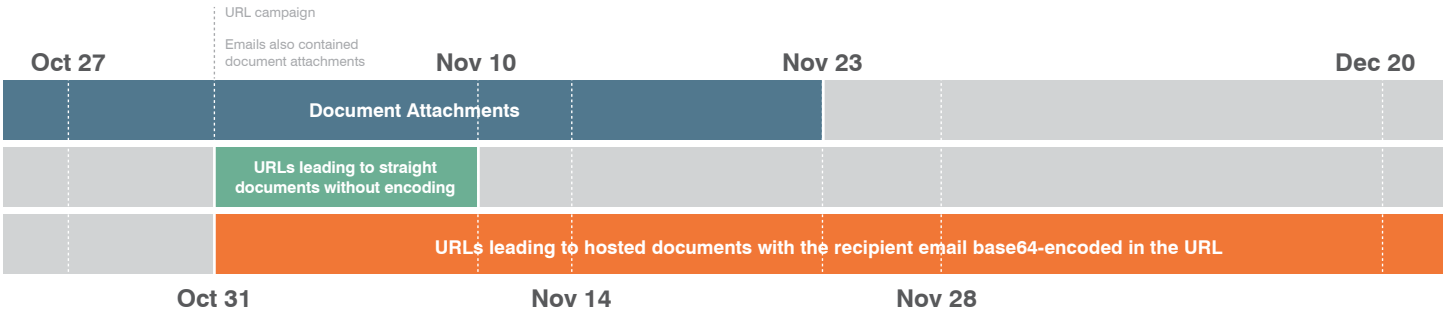

Figure 1: Timeline of evolving Vawtrak campaigns

Aside from these Vawtrak campaigns and occasional Ursnif campaigns using Microsoft SharePoint links, the use of URLs in malicious emails appeared to return to “normal”, relatively low levels in December.

The chart below shows the relative volume of document attachment and URL email campaigns during the quarter. Note that variations on the attached JavaScript files were by far the most common with most of these emails bearing Locky ransomware. Moreover, the return to a more balanced attack in December is visible in a rise of malicious document message volume that roughly matches a decrease in zipped script attachment message volume.

Indexed Weekly Malicious Message Volume by Attack Type, October - December 2016

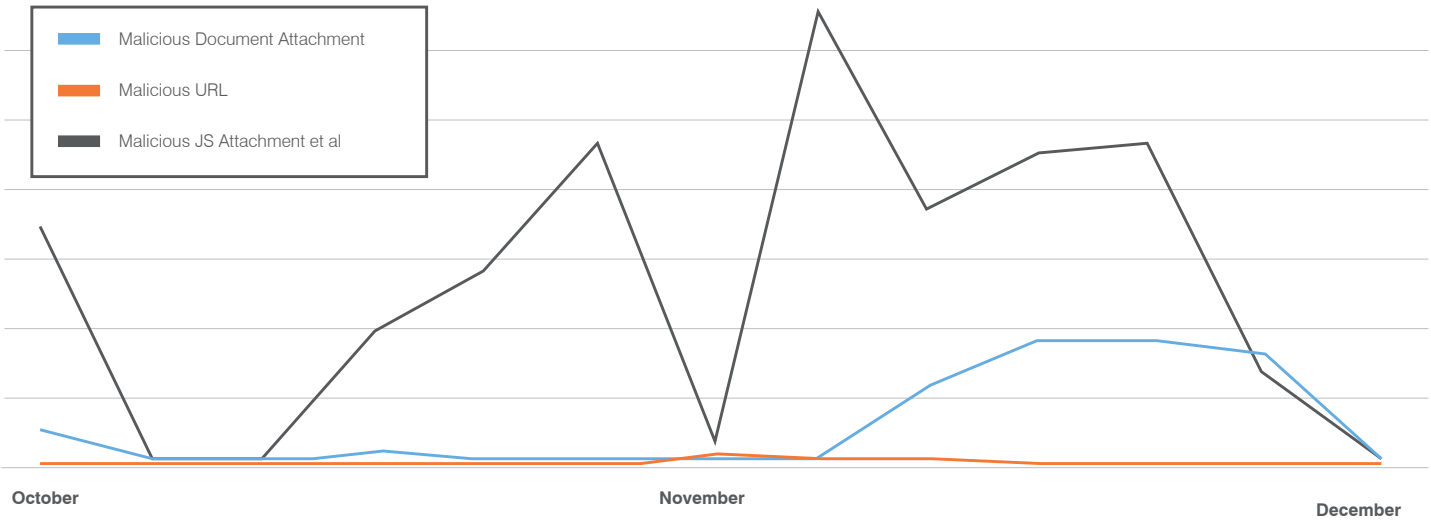

Figure 2: Indexed malicious message volume by attack type

As we observed at the end of 2015 and the beginning of 2016, the Western Christmas holiday and Russian Orthodox Christmas holidays were associated with a sustained pause in the distribution of most banking Trojans; Locky ransomware activity also entered a hiatus at the end of 2016.

TECHNIQUES

In the last three months of 2016, threat actors continued to introduce new efforts to avoid, evade, or otherwise thwart automated sandboxing and other forms of automated dynamic analysis. For example, we observed malicious document attachments with embedded VBScript and LNK objects in place of malicious macros. Other actors began using encrypted or password-protected document attachments with the password included in the email body, both increasing the sense of legitimacy and decreasing the ability of most sandboxes to detonate the documents. We observed this technique in campaigns distributing Cerber ransomware and Ursnif banking Trojan, and even in credential phishing campaigns.

Key Stat: For emails containing malicious URLs, destinations shifted almost exclusively to dedicated phishing pages; EK pages were the destination for only 1% of links in malicious emails in December.

Analysis: Credential phishing remains a timely, noteworthy, and large-scale threat, ranging from high-profile spear phishing attacks to more mundane campaigns going after Gmail, Office 365, and other cloud service credentials. These phishing attacks are generally propagated via links in email and, as shown in Figure 3, URLs linking directly to dedicated phishing pages have largely displaced links to exploit kits that were far more common in 2014 and 2015. By the end of Q4, EKs accounted for only 1% of the links in malicious emails. These changes in URL destinations are consistent with the overall decline in EK activity this year.

URL Destinations – Credential Phishing Pages vs. Exploit Kits

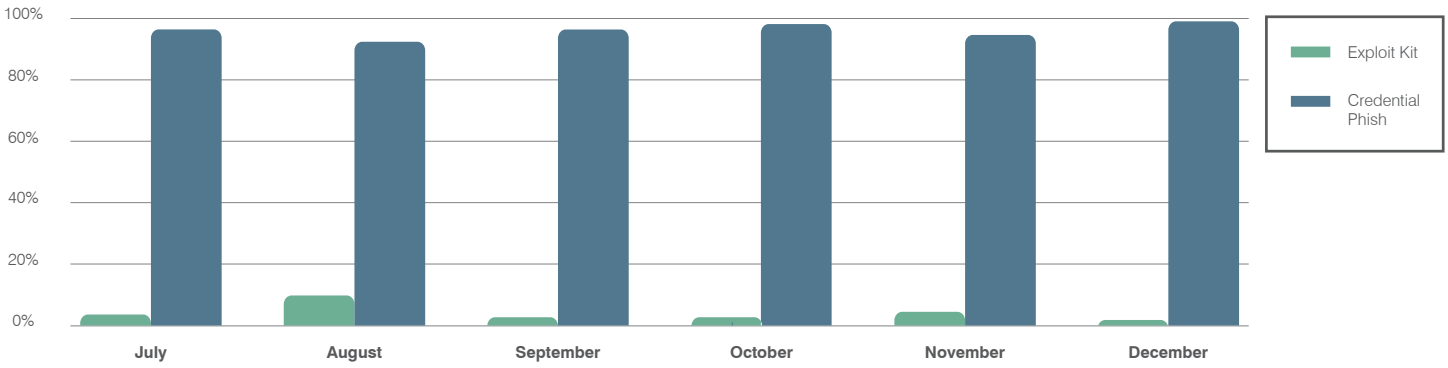

Figure 3: The use of emailed URLs for phishing versus exploit kit linking

In addition to the advent of increasingly sophisticated fake websites used for phishing, techniques have also evolved in malware campaigns. For example, we have observed a steady increase in the use of PowerShell in malicious documents over the last few months. PowerShell is generally used in conjunction with malicious macros in Microsoft Office documents and provides several advantages to threat actors over macros alone for installing or downloading malware:

- Detection evasion: While some sandboxes will generate false negatives if they do not have PowerShell installed, this advantage tends to be relatively short-lived since security vendors and tools will quickly catch up. The greater benefit is that PowerShell enables fileless installations of malicious payloads, which improve overall detection evasion.
- Flexibility: PowerShell is more robust than macros alone so can perform a greater variety of actions. Currently we only see it being used to download and execute EXE payloads, but this will likely change as attackers make greater use of this tool, including leveraging malware and tools already written in PowerShell.

Finally, actors continue to improve on and leverage the personalization techniques we identified earlier this year. Combined with sophisticated social engineering, these techniques demonstrate the enduring effectiveness of exploiting the human factor, as well as the potential for return on investment threat actors are seeking via malware and delivery innovation.

BEC

Many large organizations have begun implementing policies and procedures to avoid the massive losses that have been associated with business email compromise (BEC). BEC attacks are carefully planned, socially engineered campaigns that begin with targeted emails and then move on to other out-of-band communications, making them difficult to detect and defend against.

Organizations, however, are beginning to adopt a number of technological solutions that help identify the email spoofing that is the basis for BEC attacks. SPF, DKIM, and DMARC work in concert with a limited number of vendor solutions to stop BEC emails before they reach end users.

Key Stat: CEO-to-CFO spoofing dropped 28 percentage points by December from a high of 39% in August. DMARC adoption grew by 33% over Q3 2016.

Analysis: As shown in Figure 4, by the end of the last quarter, it was clear that BEC actors had realized that spoofing emails to the CFO from the CEO was less effective than spoofing emails from the CEO to other staff. CEO-to-CFO spoofing dropped 28 percentage points by December from a high of 39% in August.

CEO-to-CFO Spoofing for H2 2016

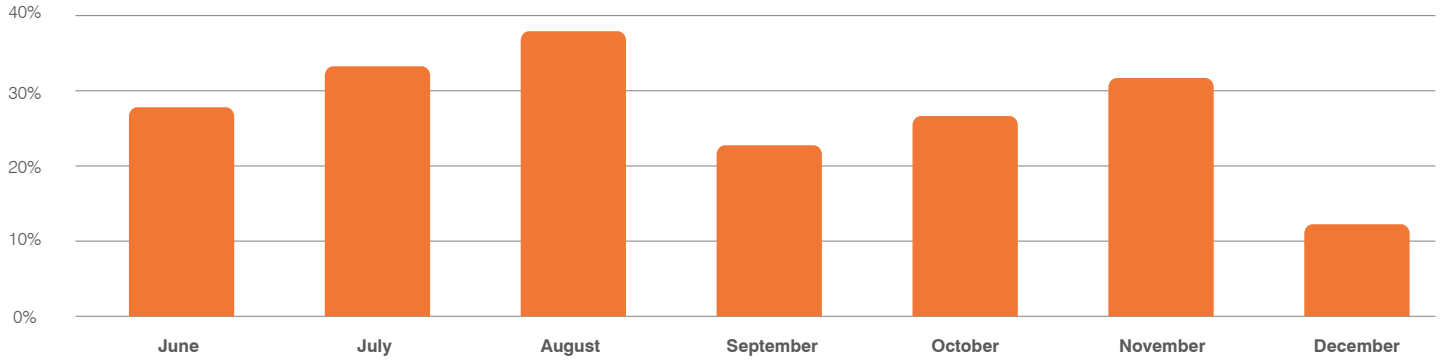

Figure 4: Percent of total BEC emails from the CEO during the last half of 2016 that were specifically sent to the CFO

Spoofing Types Observed in Q4

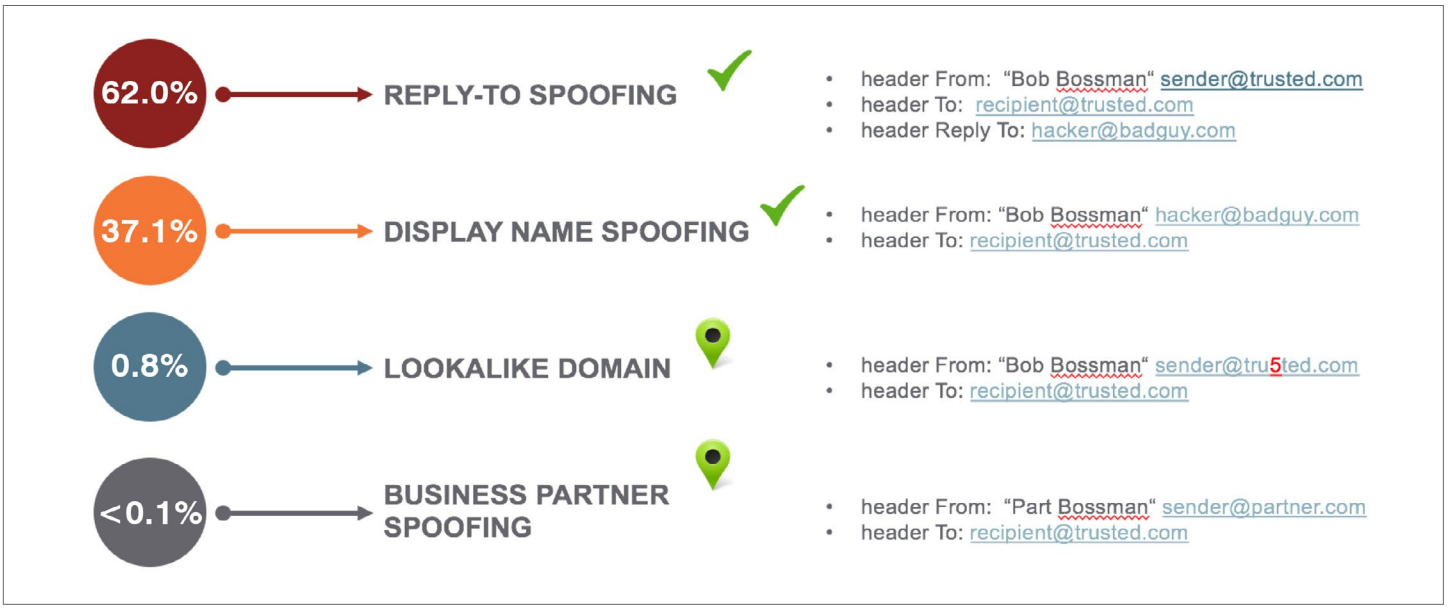

Figure 5: Additional insights into the nature of BEC attacks and the underlying spoofing techniques we observed in Q4

Moreover, Figure 6 below shows quarter over quarter DMARC adoption rates by vertical in the organizations we surveyed, suggesting that while adoption is strong, there remain many more organizations that need to fully implement these technologies.

DMARC Sender Adoption Rate by Vertical - Q416

Vertical	Q416 DMARC Adoption	Q415 DMARC Adoption	YOY Growth
Banking	36%	27%	33%
Healthcare	28%	16%	75%
ISP/Telco	29%	21%	36%
Logistics	50%	41%	22%
Payment Services	44%	32%	36%
Public Sector	50%	25%	100%
Retail/eCommerce/Gamin	33%	25%	30%
Social Media	63%	59%	36%
Technology	61%	51%	6%
Travel	39%	31%	26%
GRAND TOTAL	**38%**	**33%**	**17%**

Figure 6: DMARC adoption rates by vertical

EXPLOIT KIT LANDSCAPE

Exploit kit (EK) activity at the end of 2016 remains at levels observed in the third quarter. Overall, EKs as an infection vector have not recovered from their drop in the first half of 2016, and trends indicate they are unlikely to do so. However, we have still observed significant EK activity during the fourth quarter, primarily related to malvertising. While Angler EK, the formerly dominant exploit kit, has not reappeared, RIG EK and its variants are now the largest contributors to exploit kit traffic.

Key Stat: Exploit kit activity in Q4 remains at 93% off its January peak with no sign of future increases.

Exploit Kit Activity - Samples collected over Q4 2016

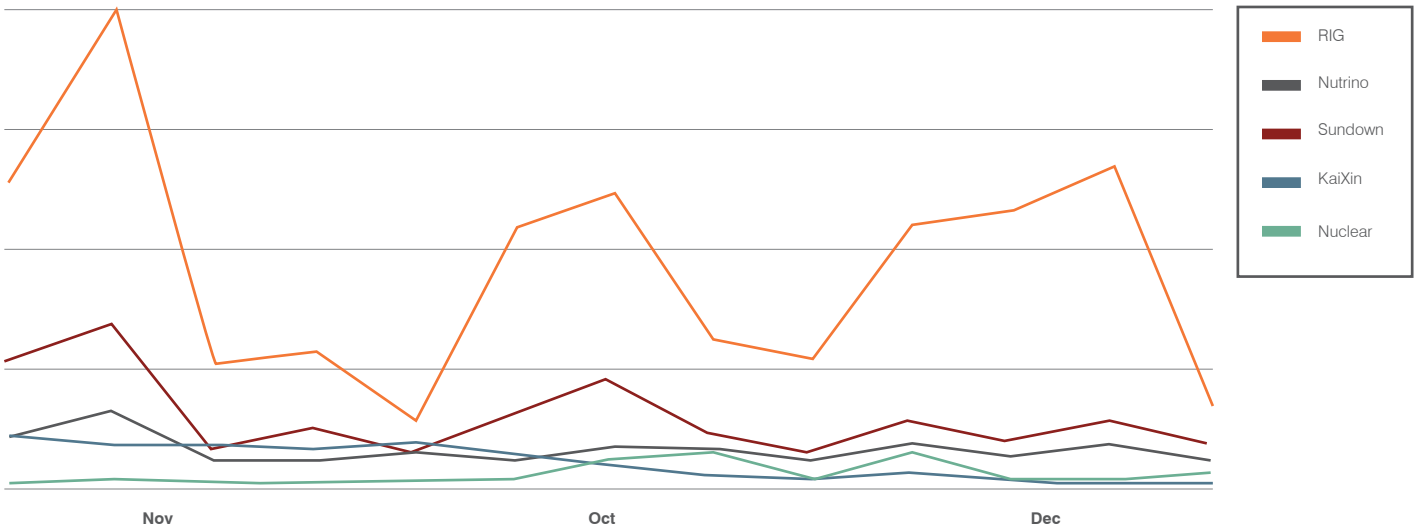

Figure 7: Q4 exploit kit activity

Analysis: However, this "new normal" of much lower EK activity compared to 2015 does not mean that this important piece of the threat infrastructure is stagnating. Evidence of ongoing innovation in the EK space can be found in DNSChanger EK. DNSChanger largely operates through malvertising and can attack SOHO routers via Windows and Android web browsers; the endpoints themselves are not infected but once the routers are compromised, their DNS records are replaced and all devices, regardless of operating system, are vulnerable to further malvertising, popups, and further attack. We observed widespread use of DNSChanger in December and expect that this may represent a new direction for exploit kits as standard exploits used to compromise PCs are quickly patched by vendors, making devices such as routers and "Internet of Things" (IoT) endpoints more attractive targets.

MOBILE

The mobile threat landscape continued its rapid evolution in Q4. Risky, malicious, and cloned apps all made their appearances while mobile attack kits and IoT exploit kits created opportunities for attackers across mobile operating systems.

Key Stat: Hundreds of thousands of mobile devices were subjected to malvertising, potential attack, etc., when DNSChanger EK.

Analysis: Mobile devices were not just affected by the actions of DNSChanger EK but also proved to be an interesting vector through which DNSChanger EK could infect home and small office routers. Proofpoint researchers confirmed that users accessing the Internet via Chrome on Android could infect a vulnerable SOHO router through which they were connected. Interestingly, the vulnerability was not within Chrome or Android, but rather relied on normal communications between the mobile device and the router; DNSChanger EK modified DNS records on the router through the device without compromising the device itself. However, once the router was compromised, both mobile and desktop devices running any operating system (including iOS and Android) were subject to browser redirection, malvertising, popups, etc.

SOCIAL MEDIA

Social media continued its rapid growth in Q4 as a brand vehicle; at the same time, threat actors took advantage of the growth to expand their footprints. We saw increasing degrees of cross-pollination between social, mobile, and malware spaces.

Key Stat: Fraudulent accounts across social channels increased by 100% from the third to fourth quarter of 2016.

Analysis: We discovered a 100% increase in general for fraudulent accounts in October 2016 compared to September 2016. These fraudulent accounts were used for everything from spamming to "angler phishing." To that end, Proofpoint researchers observed a 20% increase in spam content across Facebook and Twitter quarter over quarter. Q4 had the second highest amount of spam in terms of volume for 2016 (Q1 was first).

Legitimate Twitter support accounts sent more private messages than ever, with over a 25% increase in direct messages sent in Q4 compared to Q3. However, as support accounts send more messages and customers become accustomed to interacting with brands via direct messages, angler phishing becomes easier and customers are less likely to be suspicious. In Q4, angler phishing was the most common among financial services and entertainment accounts.

Attackers continued to gravitate towards hot topics for their fraudulent accounts, as demonstrated by the wide range of fraudulent "Super Mario Run" pages that appeared in Q4 both before and after the launch of the much-anticipated mobile game. As with Pokemon Go, many social media accounts had links to "download" the game, but the links led either to malware or to surveys such as the one shown below (Fig. 8).

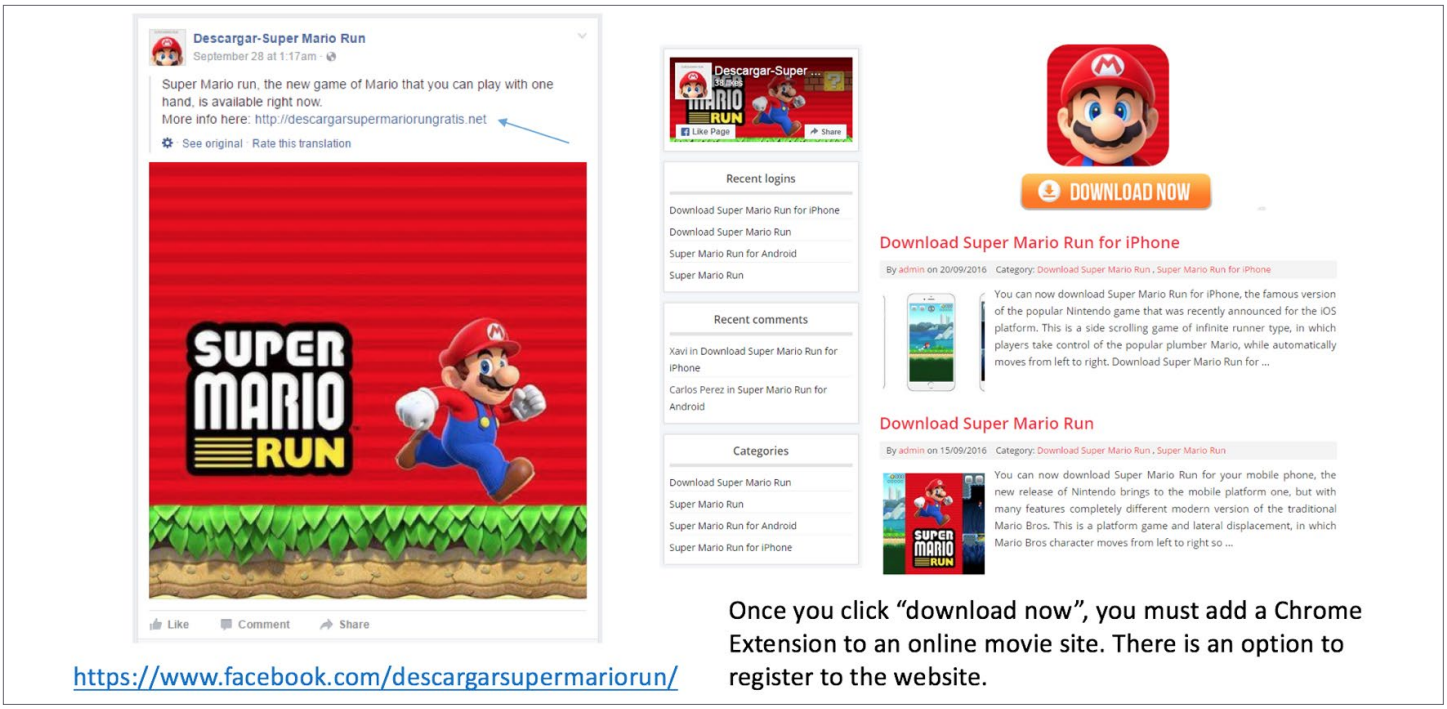

Figure 8: Fake downloads for Super Mario run

Highlighting the increasing interplay of malware and social media, Proofpoint researchers also discovered the Ransoc desktop locking software. Part of a growing trend known as “doxware”, Ransoc scrapes Skype and social media profiles for personal data while it scans files and torrents for potentially sensitive information. However, unlike the more notorious file encrypting ransomware that has dominated the threat landscape in 2016, Ransoc threatens victims with fake legal proceedings if they fail to pay the ransom should it discover objectionable or potentially illegal content.

2016 YEAR IN REVIEW

The 2016 threat landscape was characterized by extremes with little in the way of a middle ground:

- Massive email campaigns of hundreds of millions of messages dropping Locky ransomware
- Smaller, more targeted campaigns featuring the Dridex banking Trojan, 2015's top email-borne malware
- Near-silence from Locky and Dridex actors during the month-long Necurs botnet outage
- Historic highs in exploit kit (EK) traffic at the start of the year, followed by dramatic declines to a new, much lower baseline.
- Large, sustained malvertising campaigns utilizing exploit kits and sophisticated targeting and filtering affecting millions of users
- Continued, rapid growth in social and mobile threats, from angler phishing to mobile exploit kits.

For our experts' take on changes we're likely to see to the threat landscape in 2017, visit Threat Insight to read our Cybersecurity Predictions for 2017.

TOP STORIES FOR 2016

2016 brought significant changes to the threat landscape, with widespread shifts in high-volume campaigns in both the exploit kit and email spaces. Marked declines in exploit kit activity were balanced by large malvertising campaigns, while a rapidly growing body of ransomware dominated a space once the domain of banking Trojans.

Volume and variety

Key stats:

- Malicious document attachment volume increased over 600% compared to 2015
- The total volume of JavaScript attachments and their variations – which were negligible in 2015 – totaled more than 2 ½ times more than all malicious document attachments.
- Even malicious URL messages – a small fraction of total malicious email message volume – increased more than 300% compared to 2015.

Malicious email volumes increased dramatically over the course of 2016. Whereas we measured "large campaigns" in 2015 in the hundreds of thousands of messages, and in the first quarter of 2016 in the millions of messages, by the end of 2016, large campaigns regularly reached hundreds of millions of messages across the Proofpoint customer base. At the same time, these large campaigns shifted from using primarily macro-laden documents with banking Trojan payloads (often Dridex) to using primarily malicious JavaScript attachments to distribute Locky ransomware. The chart below illustrates both campaign growth and the changing distribution vectors over 2016.

Indexed Weekly Malicious Message Volume by Attack Type, 2016

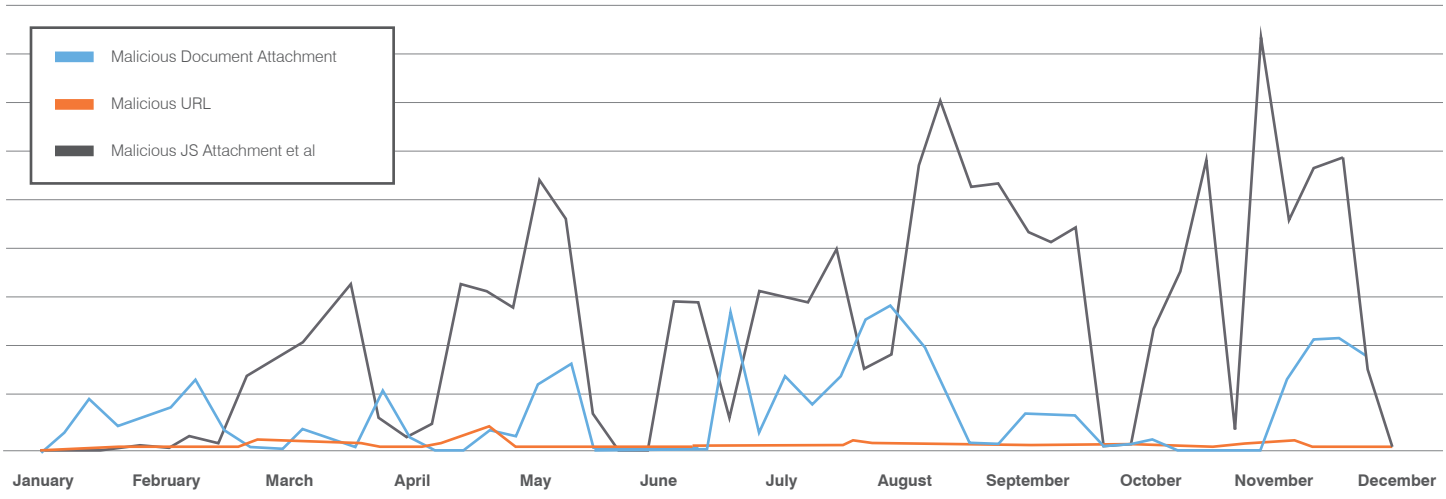

Figure 9: Relative message volume by attack type

While ransomware was the dominant malware type encountered via email across the Proofpoint customer base in 2016, banking Trojans still accounted for almost one-fourth of email-borne malware. A disproportionate number of these email messages were sent in the first quarter of 2016 before the actors distributing Dridex had fully shifted to distributing Locky ransomware, which Proofpoint researchers discovered in February 2016. Much smaller percentages of overall email-borne malware (Fig. 10) were distributing intermediate downloaders, credential stealers, spambots, and other payloads.

Malware Categories 2016 January - October

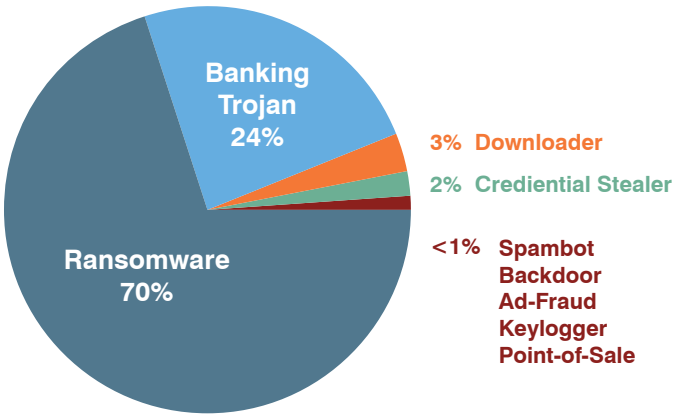

Figure 10: Malware categories distributed via email for January through October

The extremely high-volume campaigns distributing Locky did not preclude threat actor and malware author innovation in other areas, however. New banking Trojans like Panda Banker, information stealers like August Stealer, downloaders like RockLoader, and even new point-of-sale (POS) malware all contributed to considerable malware variety, despite the overwhelming noise associated with Locky ransomware.

Moreover, established malware families such as the Vawtrak and Ursnif banking Trojans were used extensively, particularly in so-called "personalized" or geographically targeted campaigns.

RANSOMWARE TAKES OVER

Key stat: The number of ransomware variants in the wild grew by a factor of almost 30X, although the vast majority of circulating ransomware was Locky.

Although Locky ransomware, with its massive email campaigns and use of JavaScript attachments at unprecedented scale, was the biggest ransomware story this year, the rise of ransomware in general in 2016 is significant. Starting from the numbers of ransomware variants in the wild at the end of 2015 – for years a relatively stable count – we have observed a roughly 30-fold increase in the number of circulating variants by the end of 2016. The majority of these did not attain the visibility or widespread distribution of variants such as CryptXXX or Cerber, but the number of variants and ease with which authors can now create and propagate this kind of malware led us to refer to ransomware as the "Hello World" of contemporary malware.

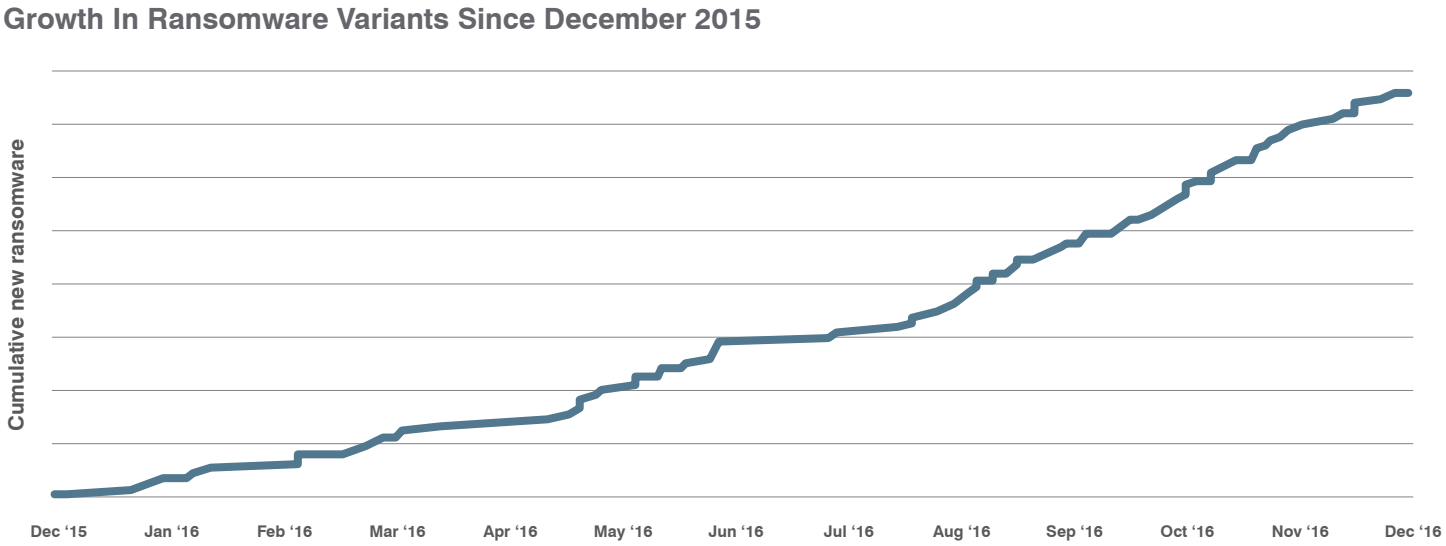

Figure 11: Cumulative growth of ransomware variants

The growth of "instant issue" malware was not limited to file-encrypting ransomware. For example, in addition to traditional types of ransomware, we also observed increases in desktop lockers. Instead of encrypting files on the PC, these simply prevent access to the computer through a full-screen application or web page and demand a ransom for restoring access. As noted above, the more sophisticated instance of so-called "doxware" – Ransoc desktop locking software – demonstrated that innovation in this variety of malware was widespread and suggests that many untapped opportunities remain for 'instant issue' malware as a category.

In general, these developments exemplify a trend in high-volume campaigns towards software that is easily monetized, as opposed to banking Trojans, keyloggers, RATs, and other malware that require far more sophistication and maintenance to generate significant return on investment for threat actors.

BIFURCATION OF EMAIL-BASED MALWARE CAMPAIGNS

Email-based malware campaigns evolved into a dichotomy in 2016. Whereas spam has always relied on high-volume, shotgun-style campaigns, the Dridex campaigns of 2015 and Locky campaigns of 2016 brought the technique to malware distribution. By the end of 2016, actors spreading Locky ransomware in particular set a high bar for large-scale malware distribution via email. Although dwarfed by Locky campaigns, Cerber ransomware was also being spread at significant scale for the last half of 2016. Ransomware lends itself to this type of distribution as it does not require the degree of region-specific customization as banking Trojans, the web injects for which must be keyed to individual banks.

In 2016, it appears that threat actors came to this same conclusion, saving banking Trojans, along with RATs, keyloggers, and other information stealers for much lower-volume, targeted campaigns. Banking Trojan campaigns became much more targeted by region and industry, with Dridex, for example, re-emerging in August with a heavy focus on Swiss banks after a period of near silence in June and July. Similarly, an unsolicited email threat actor known for highly personalized campaigns consistently distributed the Ursnif and Nymaim banking Trojans in targeted attacks throughout the last three quarters of 2016.

These lower-volume campaigns free actors to pursue more lucrative attacks and leverage stolen information more effectively while very large ransomware campaigns maximize profits, even if conversion rates are low.

SPAM, PHISHING, AND MALWARE CONVERGE AS THREAT ACTORS ADAPT

In general, threat actors tend to specialize, with spammers distributing spam, phishing actors focusing on credentials and personal information, and malware actors achieving their goals with malicious software. In 2016, however, we began to see additional cross-pollination among email-based threats. Even particular vectors and distribution mechanisms shifted as threat actors adapted to changing conditions.

For example, in December, Proofpoint researchers documented an email campaign from a known phishing actor using password-protected document attachments. This technique had previously been used by actors distributing Cerber ransomware and other malware to evade detection and increase the sense of urgency and legitimacy associated with the emails. Applying this approach to credential phishing – with the credential phishing page delivered as a password-protected web-page file attachment – highlights the hybridization of techniques in order to stay ahead of continually improving defenses.

Unlike Locky and Cerber, CryptXXX ransomware was primarily spread via exploit kit from the time of its discovery in April. Then in July, Proofpoint researchers observed the malware being distributed in email campaigns. The timing coincided with a 96% decrease in EK traffic between April and June, suggesting that threat actors were attempting to adapt to the changing landscape by shifting their distribution techniques from infrastructure with waning effectiveness to methods with the right combination of effectiveness and cost.

This continuous adaptation and adjustment applied to payloads as well as distribution and evasion techniques. For example, the threat actors behind Dridex – the malware "success story" of 2015 – effectively jumpstarted the ransomware bandwagon in early 2016 with Locky. At the same time, as ransomware took over high-volume campaign activity, the functionality of banking Trojans also added increased stealing capabilities, profiling installed applications and services, and even evolving to function as intermediate loaders. This reflects the ability of threat actors to optimize successful payloads for greatest effect: while "instant issue" payloads such as ransomware have little need to avoid detection after the initial infection, stealthy banking Trojans are well-suited to a wide range of uses – from keylogging to downloading point-of-sale malware and other payloads.

BEC

Although the FBI has reported that losses to date from business email compromise (BEC) have already reached into the billions, this threat is not exclusive to large enterprises. In fact, almost 15% of BEC attacks occur at businesses employing less than 5000 people, more than any other group in our data.

While larger organizations potentially have deeper pockets and therefore make larger targets for BEC attackers, smaller companies have fewer resources to mitigate the threat of BEC. Regardless of company size, though, organizations are looking to a variety of electronic solutions. As noted for Q4, implementation and enforcement of SPF, DKIM, and DMARC are improving efforts to combat BEC where these fraudulent attacks usually begin – with fraudulent, spoofed emails. In fact, 2016 was the "year of DMARC" with substantial adoption, especially in the public sector, where utilization was up 100% from 2015.

DMARC Implementation by Sector in 2016

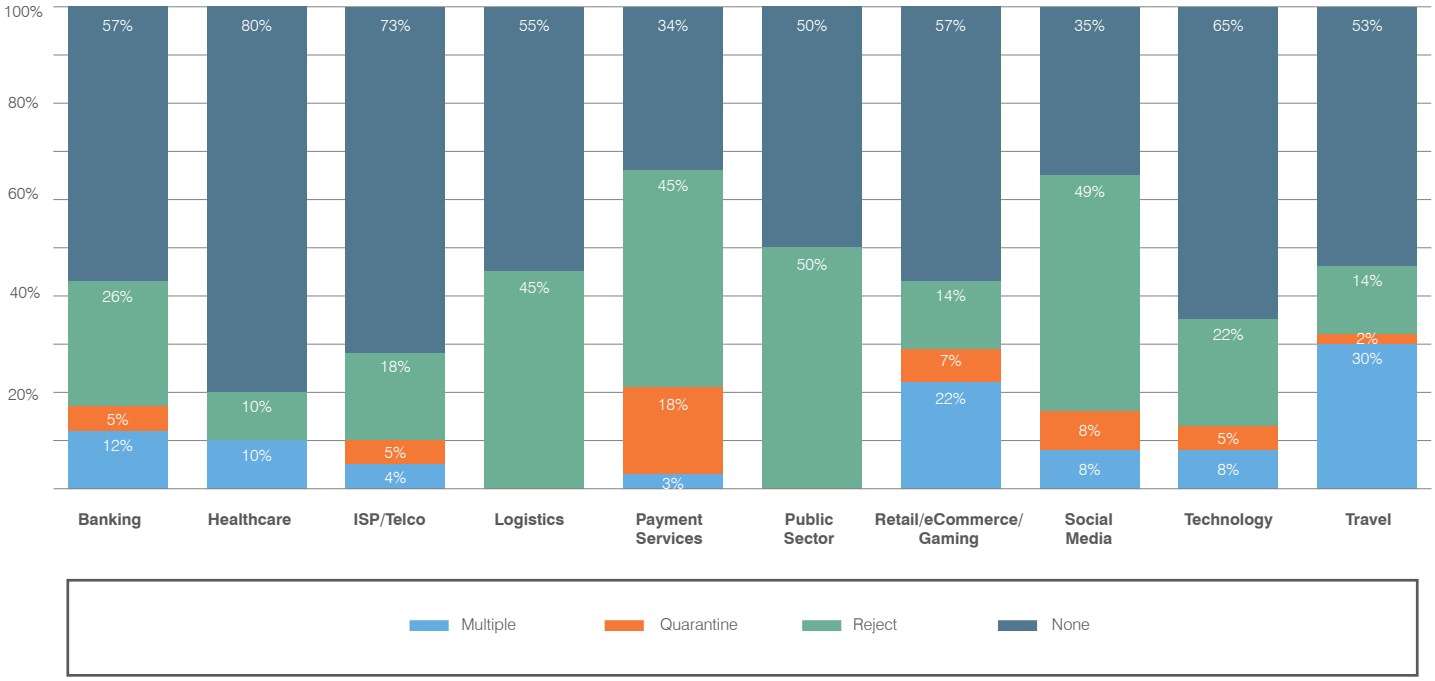

Figure 12: DMARC implementation by sector

2016 Was the Year of DMARC The widespread recognition of BEC as a genuine threat to a wide range of organizations manifested itself in a surge in adoption of DMARC across a wide variety of industries. Globally, 38% of the companies surveyed by Proofpoint are publishing a DMARC record (up from 29% a year ago and 22% two years ago). While EMEA (Europe, the Middle East, and Africa) and Australia and New Zealand are still lagging behind other regions in terms of overall adoption—with 25% and 27% respectively—their year-over-year increases are double that of North America. Over the last two years, Latin America showed the most accelerated DMARC adoption rate, but North America remains the leading region in overall DMARC usage, with an adoption rate of 51 percent, up from 42% twelve months ago.

EXPLOIT KITS

One of the most dramatic shifts in the threat landscape in 2016 was the rapid decline in exploit kit traffic after record highs in the first quarter. Angler EK, once the dominant player in the exploit kit space, led the market off a cliff in Q2 after some high-profile arrests of key actors.

Exploit Kit Activity - Samples Collected Over 2016

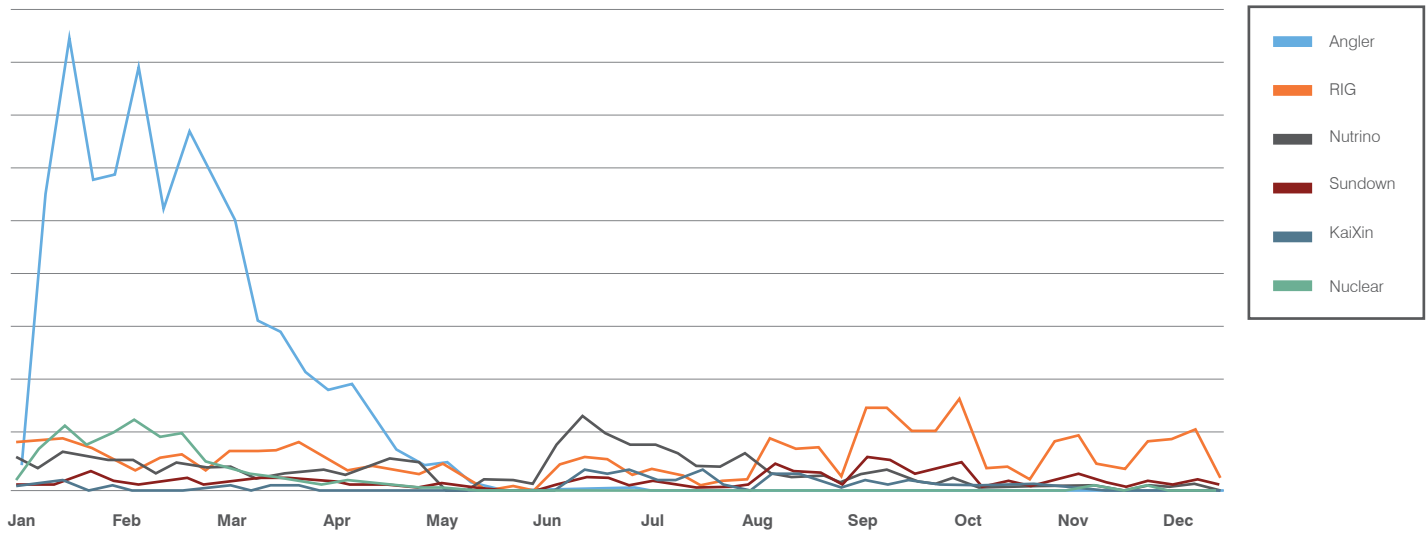

Figure 13: Overall relative volumes of EK traffic, 2016

Exploit Kit Activity - Share of Samples Collected Over 2016

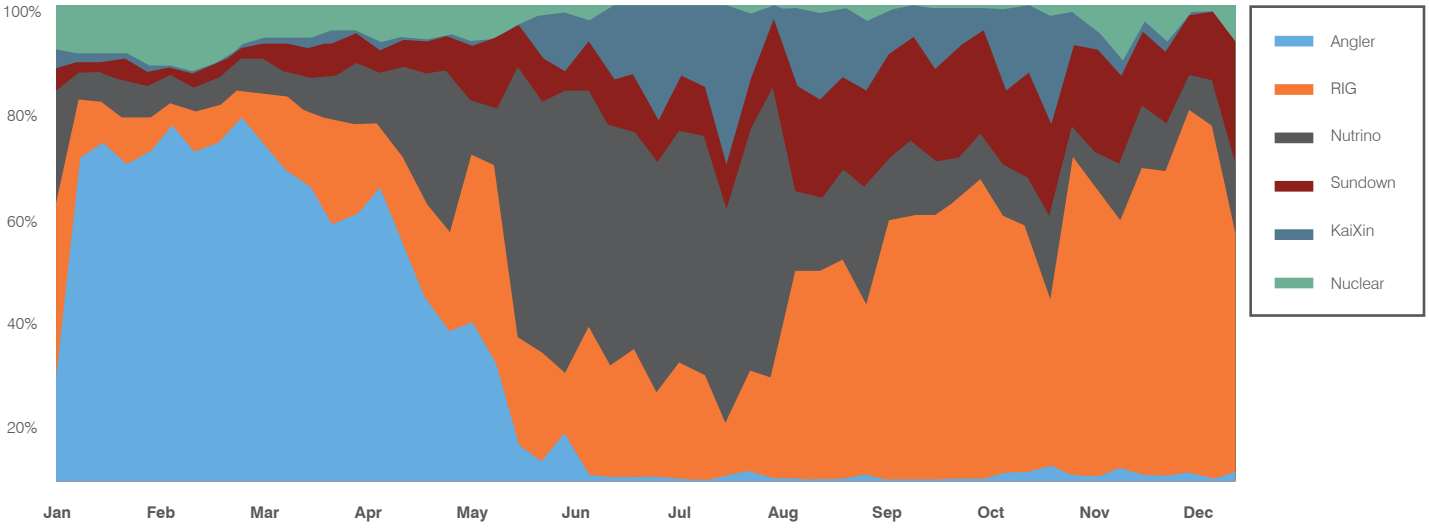

Figure 14: Weekly top-6 EK activity as a percentage of total, 2016

As shown in Figures 13 and 14, while no exploit kits completely replaced Angler in terms of sheer volume, Neutrino, Sundown, and RIG all saw substantial relative increases in volume as actors looked for alternatives. However, overall EK traffic remained at 93% of Q1 levels for much of the last half of the year.

Proofpoint experts attribute this shift to the decreasing conversion rates for exploit kits, meaning that it is increasingly difficult for actors to find exploitable visitors. Our coverage of the AdGholas group was an example of the tail end of the "golden age" of an area where EKs remained powerful tools for threat actors. AdGholas used

- Sophisticated filtering to identify high-quality users most likely to be vulnerable and exclude the security community
- Low-level vulnerabilities that flew under the security radar, allowing impressions of malicious ads to be presented to millions of users a day for extended campaigns

More recently, we observed the "DNSChanger EK" targeting small office/home office (SOHO) routers. This EK is not reliant on browser or system vulnerabilities, many of which are patched so rapidly that zero days have far less utility to threat actors than they used to, but rather on router and IoT vulnerabilities, which are far more common and exploitable.

These changes have led many of the largest threat actor groups to abandon EKs entirely, while mid-level actors continue to use them on a smaller scale. Innovation in this area continues, though, with both mobile and IoT vulnerabilities providing fertile ground for new, if smaller, campaigns.

TARGETING IMPROVES

While many of the year's headlines centered around the enormous scale of attacks, especially for Locky ransomware, dramatic improvements in targeting and automation, whether on social media, via email, or through referred traffic to exploit kits and compromised websites, present the greatest risk to end users. Socially engineered lures, personalized content, and multi-band communications for BEC attacks, all play on the human factor in ways that generic, large-scale attacks cannot.

For example, one of the most prolific spammers we track uses data harvested from LinkedIn and elsewhere to create personalized emails at scale to distribute malware with effective email lures. At a smaller scale (but with potentially higher impact) we continue to observe advanced persistent threats (APTs) operating with extremely high degrees of targeting. While the US-China Cyber Agreement signed in August appeared to lead to measurable reductions in APT threats from China against US interests, we have observed many APT actions around the globe, especially from Russia, whose APT actors were extremely active in the last half of 2016.

At the same time, as noted above, AdGholas demonstrated remarkably effective and precise targeting and filtering of potentially vulnerable users in their malvertising campaigns in the first half of the year. With the decline of EK effectiveness and reduced conversion rates, careful filtering of traffic is necessary to maximize returns on what remains of EK utilization.

Regardless of the vector or medium, attacks outside of massive Locky campaigns or the widespread malvertising campaigns we observed early in the year, are demonstrating that small has become the new big, with careful targeting helping actors maximize ROI.

SOCIAL MEDIA

Social media continued its hyper growth throughout 2016, both as a consumer platform and business tool. We observed similarly rapid growth in the attacks seen on social media platforms and, concurrently, evolving techniques in attacks that use social media as a vector. Because attacks on social media offer a significantly higher rate of ROI, this significant growth is not surprising and is expected to continue as both social platforms and related attacks mature.

In addition to the growth story, a few other trends emerged this year. In particular, we observed attacks often coinciding with major events such as the Summer Olympics. Fraudulent apps on fraudulent social media pages take advantage of new attention being paid to the event; in the case of the Olympics, we counted thousands of apps related to the event as well as a 60% increase in risky social media content. Pokemon GO, Super Mario Run, the presidential election, holidays, and major sporting events are all examples of events or phenomena that led to increases in malicious activity on social media.

Angler phishing also emerged as a significant threat to both consumers and brands. Angler phishers consistently take advantage of non-business hours, lookalike domains, and social engineering to leverage major brands and go after user credentials.

MOBILE APP THREATS

As with social media, 2016 represented a watershed year in the mobile threat landscape. Several significant risks emerged beyond the growth of malware for mobile platforms – which, in itself, continued unabated:

- Risks from malicious clones of popular apps like Pokémon GO
- Increased use of sideloading to distribute unauthorized apps
- The availability of targeted attack tools for mobile devices like Pegasus

While zero-day flaws affecting Windows PCs and traditional desktop-oriented exploit kits declined in importance during 2016, mobile zero-day vulnerabilities and attack kits grew in significance. Attacks via rogue WiFi networks became easier to implement than ever and both major mobile operating systems demonstrated vulnerability to attack.

Even the DNSChanger EK was able to attack mobile devices indirectly by changing DNS records on home routers and opening up any connected devices, regardless of OS, to pop-ups, malvertising, and further potential compromise.

Here too we saw mobile and social vectors combine with rogue apps being delivered through social channels. Again, these were often in conjunction with major events or phenomena. The Olympics, for example, spawned more than 4,500 mobile apps associated with the Olympics and sponsor brands that were either risky or malicious.

2016 RESEARCH HIGHLIGHTS

Proofpoint researchers tracked a wide range of threats throughout 2016, ranging from zero-day discoveries to investigations of novel macros for delivering malware. Our top Threat Insight posts for 2016 are aggregated below and offer a guided tour of the major evolutions and innovations in the cybersecurity threat landscape in 2016.

ADVANCED PERSISTENT THREATS

Operation Transparent Tribe - APT Targeting Indian Diplomatic and Military Interests

Bank robbery in progress: New attacks from Carbanak group target banks in Middle East and US

NetTraveler APT Targets Russian, European Interests

BANKERS, TROJANS, AND STEALERS

Updated Blackmoon banking Trojan stays focused on South Korean banking customers

Dridex, JavaScript, and Porta Johns

Vawtrak and UrlZone Banking Trojans Target Japan

Death Comes Calling: Thanatos/Alphabot Trojan Hits the Market

Panda Banker: New Banking Trojan Hits the Market

Dridex Returns To Action For Smaller, More Targeted Attacks

Nightmare on Tor Street: Ursnif variant Dreambot adds Tor functionality

Kronos Banking Trojan Used to Deliver New Point-of-Sale Malware

August in November: New Information Stealer Hits the Scene

BEC

Beyond Vanilla Phishing - Impostor Email Threats Come of Age

Scammers Exploit Turkey Coup Attempt with Timely Business Email Compromise (BEC) Lures

DELIVERY AND TECHNIQUES

Hiding in Plain Sight - Obfuscation Techniques in Phishing Attacks

,om Is Not .com – Attackers Increasing Use of Typosquatting

Phish Scales: Malicious Actor Combines Personalized Email, Variety of Malware To Target Execs

Beware the JavaScript - Malicious Email Campaigns With .js Attachments Explode

Malicious Macros Add Sandbox Evasion Techniques to Distribute New Dridex

Threat Actors Using Legitimate PayPal Accounts To Distribute Chthonic Banking Trojan

Ursnif Banking Trojan Campaign Ups the Ante with New Sandbox Evasion Techniques

Looking for Trouble: Windows Troubleshooting Platform Leveraged to Deliver Malware

Spike in Kovter Ad Fraud Malware Riding on Clever Macro Trick

Veil-Framework Infects Victims of Targeted OWA Phishing Attack

EXPLOIT KITS AND MALVERTISING

Video Malvertising Bringing New Risks to High-Profile Sites

Exploit Kit Déjà Vu: Massive Email Campaigns Spreading Dridex Via Angler

Is Angler EK Sleeping with the Fishes? Neutrino exploit kit now distributing most CryptXXX

EXPLOIT KITS AND MALVERTISING (CONTINUED)

Necurs Botnet Returns With Updated Locky Ransomware In Tow

Massive AdGholas Malvertising Campaigns Use Steganography and File Whitelisting to Hide in Plain Sight

LANDSCAPE

Two Threats For the Price of One: Credential Phishing Leads to iSpy Keylogger

It's Quiet...Too Quiet: Necurs Botnet Outage Crimps Dridex and Locky Distribution

ZeusPOS and NewPOSthings Point-of-Sale Malware Traffic Quadruples For Black Friday

Ostap Bender: 400 Ways to Make the Population Part With Their Money

MOBILE

DroidJack Uses Side-Load…It's Super Effective! Backdoored Pokemon GO Android App Found

RANSOMWARE

Dridex Actors Get In the Ransomware Game With "Locky"

New Ransomware - All Your Data Are Belong To Us

CryptXXX: New Ransomware From the Actors Behind Reveton, Dropping Via Angler

Ransomware Explosion Continues: CryptFIle2, BrLock and MM Locker Discovered

Locky Ransomware Actors Turning To XORed JavaScript to Bypass Traditional Defenses

Ransoc Desktop Locking Ransomware Ransacks Local Files and Social Media Profiles

SOCIAL MEDIA

Malicious Apps and Social Media Scams Target 2016 Rio Olympic Fans and Brands

Fraudulent Social Media Accounts Continue to Phish for Banking Credentials

Pokémon GO Mobile App Threats Are Also Social

No Shortcuts to Verification: Social Media Verification Phishing Scams Steal Credentials and Credit Card Numbers

SPAM

Spam, Now With a Side of CryptXXX Ransomware!

Election Spam Trumps Phishing As November Draws Closer

Election Spam Gets Bipartisan

ZERO-DAY AND OTHER VULNERABILITIES

Killing a Zero-Day in the Egg: Adobe CVE-2016-1019

Microsoft Patches CVE-2016-3351 Zero-Day, Exploited By AdGholas and GooNky Malvertising Groups

Peas in a pod: Microsoft patches CVE-2016-3298, a second information disclosure zero-day used in malvertising campaigns and the Neutrino Exploit Kit

Microsoft Word Intruder 8 Adds Support for Flash Vulnerability CVE-2016-4117

Home Routers Under Attack via Malvertising on Windows, Android Devices

PROOFPOINT RECOMMENDATIONS

This report reveals important developments in the threat landscape which affect your cybersecurity strategy. Here are our top recommendations for how you can protect your company and brand in 2017.

Assume users will click. Social engineering is increasingly the most popular way to launch email attacks and criminals evolve their techniques fast. 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 BEC defense. Highly-targeted, low volume business email compromise scams often have no payload at all and are thus difficult to detect. Invest in a solution that has dynamic classification capabilities that you can use to build quarantine and blocking policies.

Protect your brand reputation and customers. Fight attacks targeting your customers over social media, email, and mobile—especially fraudulent accounts that piggyback on your brand. Look for a robust social media security solution that scans all social networks and reports fraudulent activity.

Lock down mobile app environments. Mobile environments increase the risk of unauthorized apps that can steal critical corporate information. Invest in a data-driven solution that works with your mobile device management (MDM) to reveal the behavior of apps in your environment, including what data they are accessing.

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.