JAN-MAR 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 analyze more than 1 billion email messages, hundreds of millions of social media posts, and more than 150 million malware samples to protect people, data, and brands from advanced threats.

Analyzing how these threats shift each quarter allows us to identify larger trends and equip readers with intelligence they can act on and advice for managing their security posture. We continue to see advanced threats across three key vectors: email, social media and mobile.

KEY TAKEAWAYS

Banking Trojans and ransomware dominated the email malware landscape in the fist quarter, while impostor phishing (also known as business email compromise, or BEC) gained speed. The massive email message volumes associated with Dridex banking Trojan malware gave way to the newly discovered Locky ransomware. Social media content from top brands increased, further exposing brands through social channels. Meanwhile, risky mobile apps continued to expose sensitive data, especially on Android devices. Below are key takeaways from the first quarter of 2016.

EMAIL

- **Impostor email threats are increasingly mature and specialized.** About 75% of impostor email phishing attacks rely on "reply-to" spoofing to trick users into thinking messages are from someone in authority.

- **Ransomware vaulted into the top ranks of malware most preferred by cyber criminals.** 24% of email attacks, based on attached-document files, featured the new Locky ransomware. Dridex was the only malware payload used more frequently.

- **Email continues to be the top threat vector, and malicious message volume rose sharply.** First quarter volume increased by 66% over the fourth quarter of 2015—and more than 800% over the year-ago quarter. Dridex accounted for 74% of total attachment-based malicious email volume.

- **Java and Flash Player vulnerabilities continue to pay dividends for cyber criminals. Angler was the most used exploit kit, accounting for 60% of total exploit kit traffic.** Neutrino and RIG exploit kit use was also up last quarter of 86% and 136%, respectively.

SOCIAL MEDIA

- **Every major brand we examined[1] increased social media content by at least 30%.** As the volume of fan- and brand-generated content increases, higher risk follows. Businesses are constantly challenged to protect their brand reputation and stop spam, pornography, and adult language from diluting their message.

MOBILE

- **98% of all malicious mobile apps examined in the first quarter targeted Android devices.** This remains true despite the high-profile discovery of an iOS Trojan and the continuing presence of risky iOS apps and rogue app stores.

1 The top five English-language Twitter and Facebook brands as tracked by Socialbakers.

TOP THREATS & TRENDS: EMAIL THREATS ESCALATE, FURTHER EVOLVE

Email continues to represent the first line of attack for advanced threats and targeted attacks. It serves as a beachhead from which threat actors can pursue further malicious activities.

Impostor phishing gains sophistication

Key stat: 75% of impostor phishing attacks rely on "reply-to" sender spoofing to trick users into believing the messages are authentic.

Threat actors employ a variety of highly effective lures that target departments (such as human resources and accounting) and specific people. These lures use a variety of mechanisms to convince users that attackers' requests for information or money transfers are legitimate.

What this means: Technical defenses (such as enhanced email firewall rules) and user training can greatly reduce the risk from these threats. Even so, attackers are improving their effectiveness faster than people can be trained to look for new threats. As a result, automated advanced email threat defenses are essential to staying ahead of this high-yield threat.

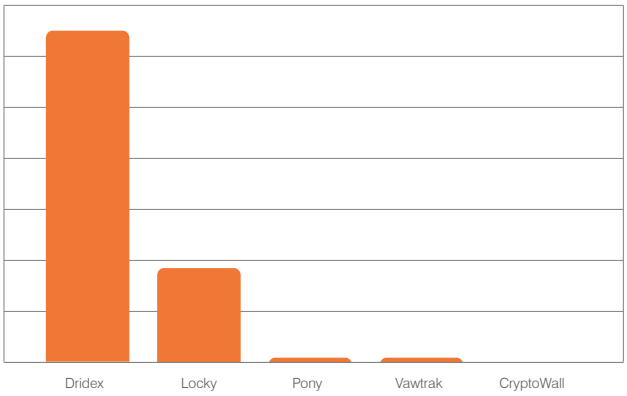
Top malware payloads, featuring new ransomware

Key stat: 24% of document attachment-based email attacks in the first quarter featured the new Locky ransomware.

Cyber criminals used only the infamous Dridex banking Trojan more—Dridex accounted for 74% of total message volume. Other payloads appeared mostly in short bursts. Nymaim entered the top 10, and Vawtrak remained a frequent alternative to Dridex.

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

Top Malware Payloads by Message Volume
Document attachment campaigns, January-March 2016



Malicious email volume skyrockets

Key stat: First quarter malicious email message volume (emails that contain harmful URLs and file attachments) increased by 66% over the fouth quarter 2015—and more than 800% vs. the year-ago quarter.

Messages with malicious URLs surged in February and March. They rose 54% quarter over quarter and almost 700% over the year-ago quarter. Many of these URLs pointed to hosted archive files. A key trend we saw in 2015 continued: threat actors favored malicious document attachments over malicious URLs.

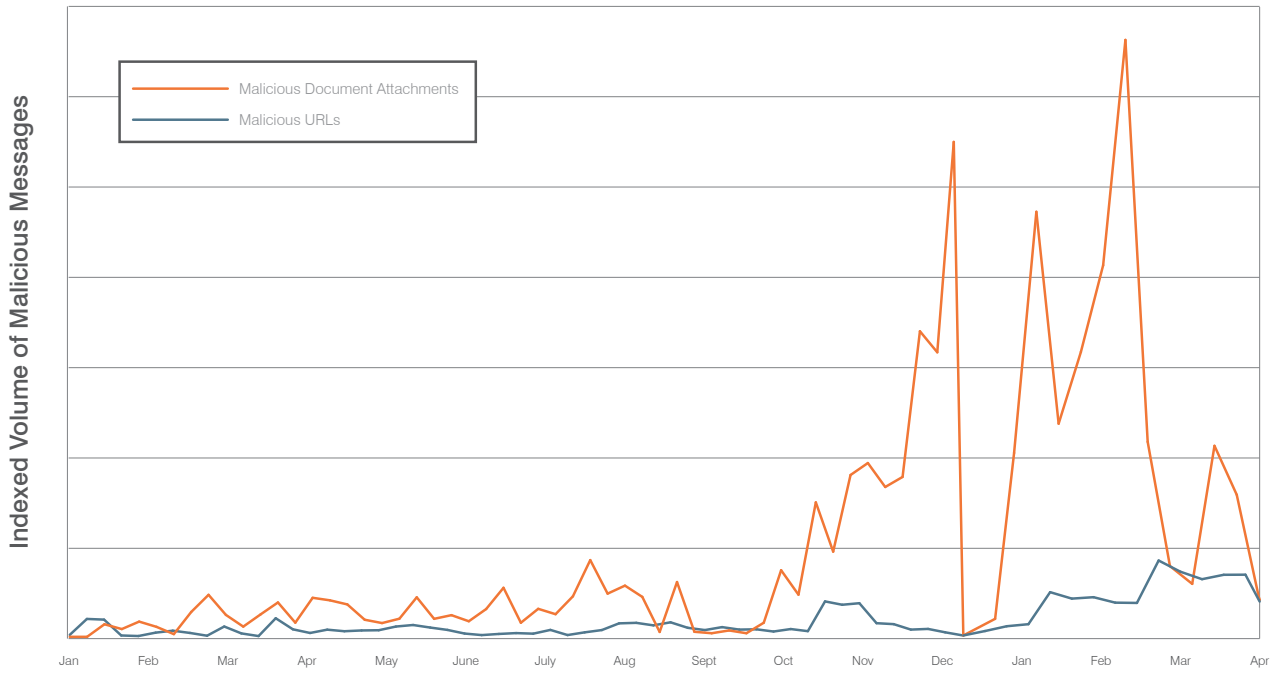
What this means: The already-massive volume of malicious messages continues to rise. This threat far exceeds the capacities of most security teams and manual processes. Organizations must have a scalable, automated defense against email-based advanced threats.

Angler Dominates Exploit Kit Traffic, but Others on the Rise

Key stat: Java and Flash Player vulnerabilities continue to pay dividends for cyber criminals through EK (EKs). EK are tools that allow attackers to more easily take advantage of security flaws in targeted systems. Angler was the most used EK, accounting for 60% of total EK traffic.

Neutrino and RIG exploit kit use was also up with 86% and 136% increases, respectively. Nuclear exploit kit traffic volume fell by a slight 8%. KaiXin and Magnitude EK rose more than 50% compared to the previous quarter, but volumes are still very low compared with the rest of the top five EKs.

What this means: In addition to normal patching efforts, organizations need to continually monitor threat intelligence sources to track and patch the vulnerabilities exploited by Angler and other EKs. The black market continues to consolidate around Angler, providing resources and motivation for active, rapid development by Angler's developers. But other EKs remain key infection tools. EK installed on compromised and malicious websites continue to power URL-based email campaigns, malvertising, drive-by downloads, advanced threats, and other attacks.



Increase in Social Media Content Drives Risk

Key stat: Every major brand we examined increased social media content by at least 30%.

Pornography and adult language stayed the same or increased vs. the fourth quarter of 2015. The trend was especially pronounced on Twitter, where adult language increased by 300%. The problem requires increasing vigilance (or automation) to deal with the issue.

In some cases, spam has plummeted, falling 70% on Facebook. But Twitter spam grew 30% for financial services brands. Spam remains a serious distraction for fans of these brands, again pointing to the need for automated solutions.

What this means: Brands are using social media more than ever to interact with their audiences. But if those interactions are muddled by spam, pornography, and adult language, customers walk away. Brands struggle to manage their social channels. Many also risk costly compliance violations.

Malicious Mobile Apps Target Android Devices

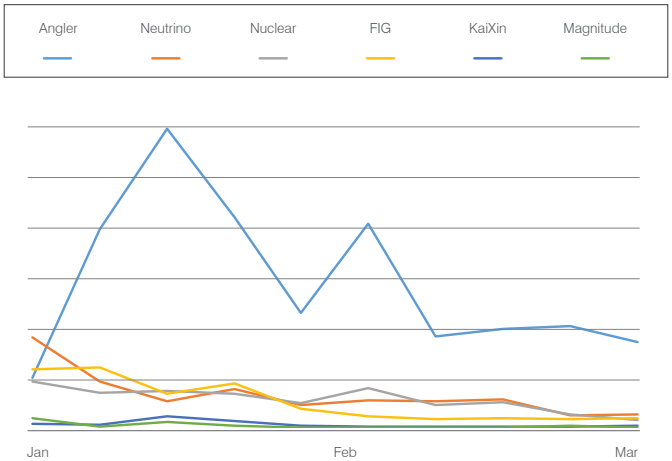
Key stat: 98% of all malicious mobile apps we examined in the first quarter targeted Android devices.

While the discovery of an iOS Trojan and rogue app stores available to iOS users made headlines, Android remains the mobile target of choice. But we expect mobile app threats to expand their footprints in other operating systems; we've already seen some incursions into Apple's "walled garden" this quarter.

Regardless of OS, we saw a number of common elements in malicious mobile apps, including:

- Known malware signatures
- Access to the Internet without permission
- Means for siphoning phone data
- Inappropriate elevation of privileges
- Access to media interfaces

Top Exploit Kits Trend by Traffic Volume
January-March 2016



What this means: Organizations need up-to-date, detailed assessments of mobile apps to identify apps that put their users, data, and networks at risk. This need is especially pressing for those that allow Android devices in their environments.

PROOFPOINT RECOMMENDATIONS

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

- Invest in an email security solution that can detect and protect against both malware and non-malware-based threats. As attackers use more social engineering to persuade users to complete tasks or run malware, solutions that can detect non-malware-based threats like imposter email can help prevent costly mistakes and breaches. User education is also key.

- Be aware of your organization's social media footprint; take steps to monitor content and activity of your social media accounts. As attackers leverage spoofed social media accounts, you must be aware of the social media footprint associated with your brand— not just owned by the brand. Close monitoring of activity on organization-owned accounts will also help prevent malicious or inappropriate content that dilutes your brand value.

- Enhance mobile device management (MDM) with security solutions that can spot and monitor potentially harmful apps. These solutions should be able to detect both malicious apps and apps that exhibit risky behavior such as exfiltrating data and communicating with unknown servers.

For more insights visit us at www.proofpoint.com/us/threat-operations-center