

BIGGER, FASTER, MORE DIVERSE

A SURVEY OF THE 2016 THREAT LANDSCAPE



The threat landscape is constantly changing, and 2016 was another high watermark for threats across email, social media, and mobile devices. Here are some of the key trends Proofpoint observed during the year.

EMAIL

6.7X
THE LARGEST EMAIL ATTACK CAMPAIGN IN THE LAST QUARTER OF THE YEAR WAS 6.7 TIMES THE SIZE OF PREVIOUS QUARTER'S

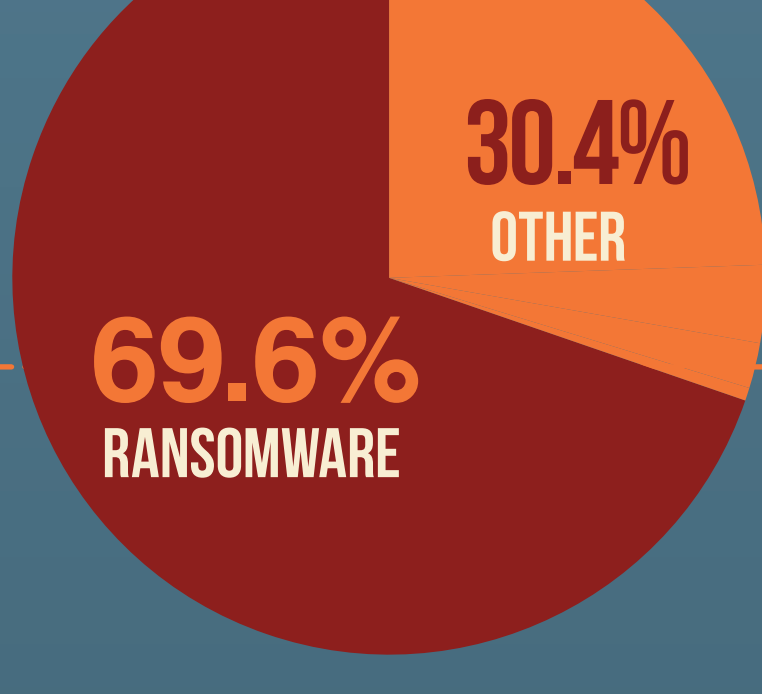
>90%
MORE THAN 90% OF TODAY'S ATTACKS START WITH EMAIL*

*PhishMe, "2016 Enterprise Phishing Susceptibility and Resiliency Report," December 2016.

RANSOMWARE TAKES OVER

The record-setting campaigns of Q3 and Q4 delivered ransomware. As a category, **ransomware appeared more than twice as often** as all other malware categories combined.

TYPES OF MALWARE SENT TO PROOFPOINT CUSTOMERS, JANUARY-OCTOBER 2016



Locky, sent mostly through malicious JavaScript attachments, was by far the most popular form of ransomware.

But while Locky reigns, the number of ransomware variants is growing quickly. The number of new **ransomware variants multiplied 30 times** in 2016 vs. the year-ago quarter.



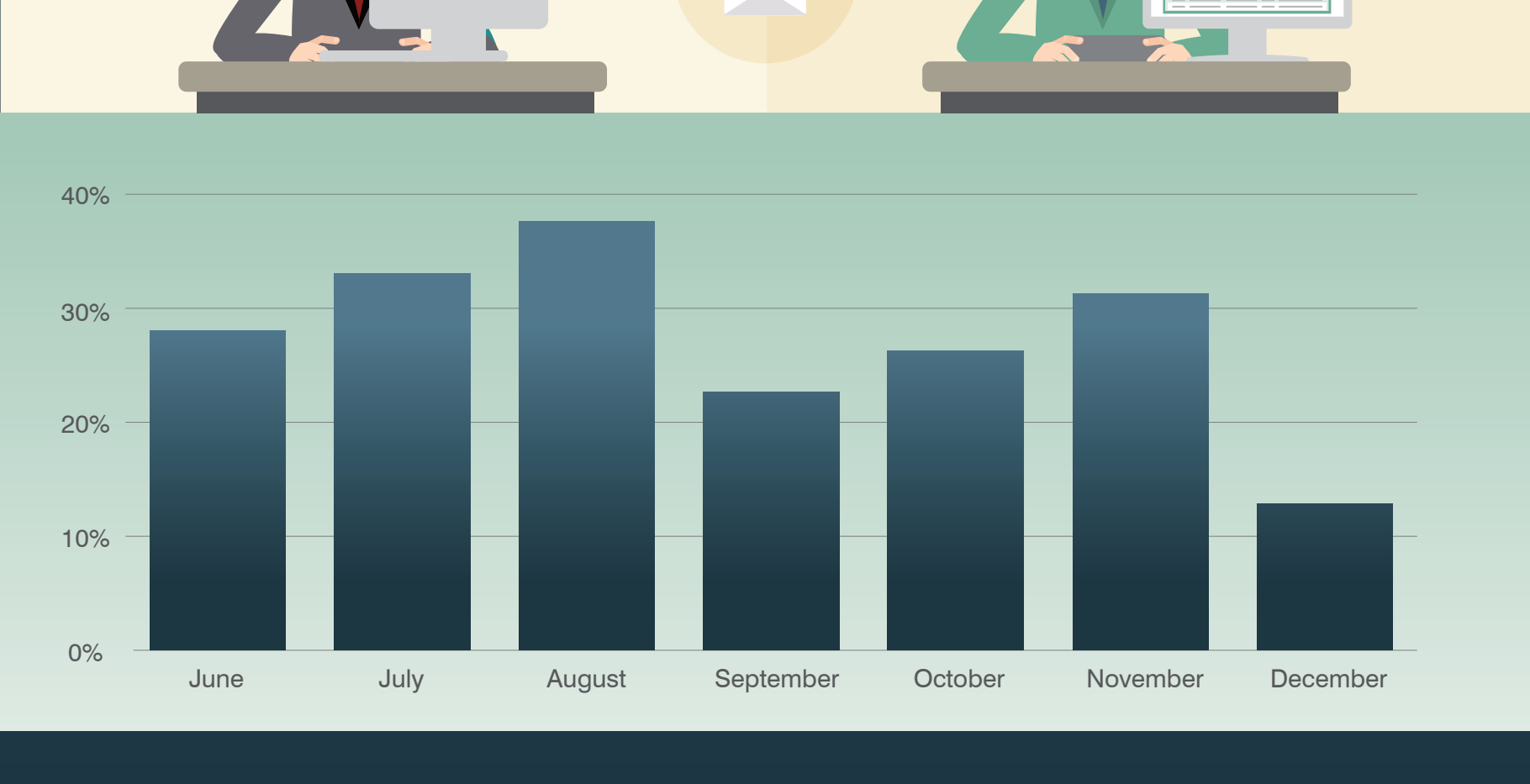
BUSINESS EMAIL COMPROMISE EVOLVES

Business email compromise (BEC), in which fraudsters posing as a company executive trick victims into wiring money or sending sensitive corporate information, is evolving.

OTHER 89%
By December, **89% of attacks targeted non-CFO executives** and rank-and-file workers.

CFO 39%
Attacks from a spoofed CEO account to the CFO peaked in August, accounting for **39%** of all BEC attacks.

CEO-TO-CFO SPOOFING AS A PERCENT OF TOTAL BEC AMONG FORTUNE 1000 CUSTOMERS



BEC attacks rely on convincing victims that the email is coming from an executive. Here's a breakdown of the techniques they use.

60% REPLY-TO SPOOFING

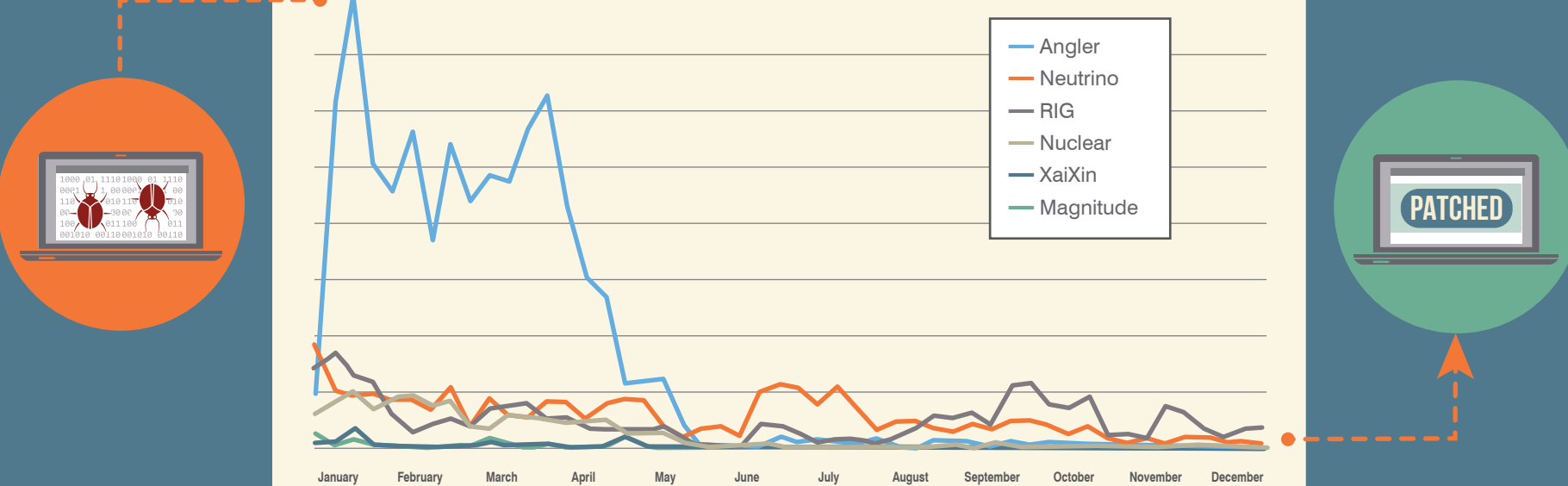
37% DISPLAY NAME SPOOFING

2% LOOKALIKE DOMAIN

1% BUSINESS PARTNER SPOOFING

EXPLOIT KIT ACTIVITY IMPLODES

Exploit kits (EKs), which make it easy to exploit software and system flaws in attacks, once ruled the threat landscape. But **traffic flatlined in 2016 as vendors patched vulnerabilities** more quickly.



FOR CREDENTIAL PHISHING, ATTACKERS HAVE TURNED TO MALICIOUS URLS

Attackers are using emailed URLs to send victims to dedicated phishing pages

By the end of Q4, **EKs accounted for only 1%** of the links in malicious emails

SOCIAL

SOCIAL MEDIA IS EMERGING AS ANOTHER KEY THREAT VECTOR

Between Q3 and Q4 alone, fraudulent accounts doubled. **Spam across Facebook and Twitter grew 20%** during the same period.

↑20%

For the year, **Social media phishing attacks increased 500%**. This includes "angler phishing," in which fraudsters pose as a brand's customer support to trick users into handing over account credentials and other information.

↑500%

MOBILE

Hundreds of thousands of mobile devices were potentially exposed to attacks that redirected users to malicious websites through the DNSChanger EK. And this EK relied only on router vulnerabilities rather than mobile exploits.

Attackers also piggybacked on popular events and trends.

For the **Summer Olympics alone**, we saw **4500 mobile risky or malicious apps** related to the event and sponsor brands.

FOR MORE DETAILS ABOUT 2016 THREAT TRENDS—AND WHAT YOU CAN DO TO PROTECT YOUR PEOPLE, DATA, AND BRAND—**DOWNLOAD OUR FULL Q4 THREAT SUMMARY AND YEAR IN REVIEW**