proofpoint™

THE HUMAN FACTOR 2016

1. PEOPLE ARE REPLACING AUTOMATED EXPLOITS AS ATTACKERS' PREFERRED ENTRY TACTIC

Attackers infected computers by tricking people into doing it themselves. 99.7% of documents used in attachment-based campaigns relied on social engineering and macros. At the same time, 98% of URLs in malicious messages linked to hosted malware, either as an executable or an executable inside an archive.

2. DRIDEX BANKING TROJAN CAMPAIGNS WERE THE DOMINANT TECHNIQUE FOR MAKING PEOPLE CENTRAL TO THE INFECTION CHAIN

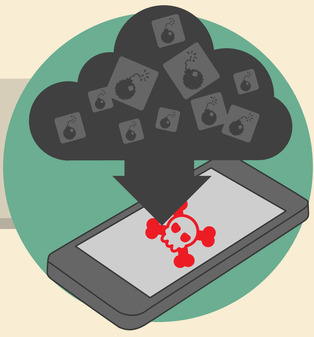
Banking Trojans were the most popular type of malicious document attachment payload, accounting for 74% of all payloads. Dridex-based email volume was almost 10 times greater than the next most-used payload in such attacks. Attackers use social engineering and mimicking familiar processes such as invoices and statements to trick a user into clicking on the messages in their email.

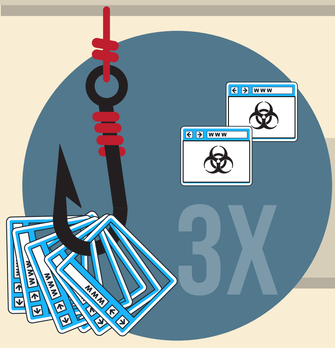
3. ATTACKERS TIMED EMAIL AND SOCIAL MEDIA CAMPAIGNS TO ALIGN WITH THE TIMES THAT PEOPLE ARE MOST ENGAGED

As they shifted from malware exploits to clicks by humans, attackers optimized campaign delivery times to match the times when people click. Email messages are delivered at the start of the business day (9-10 a.m.) in the target regions. Social media spam posting times likewise mirror the peak usage times for legitimate social media activity.

4. PEOPLE WILLINGLY DOWNLOADED MORE THAN 2 BILLION MOBILE APPS THAT STEAL THEIR PERSONAL DATA

Attackers used social media threats and mobile apps, not just email, to trick users into infecting their own systems. Our analysis of authorized Android app stores discovered more than 12,000 malicious mobile apps— capable of stealing information, creating backdoors, and more—accounting for more than 2 billion downloads.



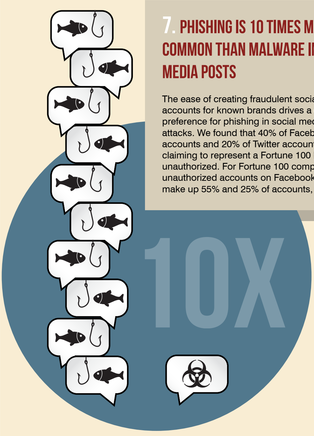


5. URLS LINKING TO CREDENTIAL-PHISHING PAGES WERE ALMOST 3 TIMES MORE COMMON THAN LINKS TO PAGES HOSTING MALWARE

On average, 74% of URLs used in email-based attacks linked to credential-phishing pages, rather than to sites hosting malware.

6. ACCOUNTS USED TO SHARE FILES AND IMAGES — SUCH AS GOOGLE DRIVE, ADOBE, AND DROPBOX — ARE THE MOST EFFECTIVE LURES FOR CREDENTIAL THEFT

Google Drive links were the most clicked credential-phishing lures. Using these brands can trick the user into clicking, especially if the victim receives the message from someone in their contacts list.



7. PHISHING IS 10 TIMES MORE COMMON THAN MALWARE IN SOCIAL MEDIA POSTS

The ease of creating fraudulent social media accounts for known brands drives a clear preference for phishing in social media-based attacks. We found that 40% of Facebook accounts and 20% of Twitter accounts claiming to represent a Fortune 100 brand are unauthorized. For Fortune 100 companies, unauthorized accounts on Facebook and Twitter make up 55% and 25% of accounts, respectively.

8. DANGEROUS MOBILE APPS FROM ROGUE MARKETPLACES AFFECT 2 IN 5 ENTERPRISES

We identified rogue app stores that allowed users to download malicious apps onto iOS devices. These apps can steal personal information, passwords, and data. About 40% of large enterprises sampled by Proofpoint TAP Mobile Defense researchers had malicious apps from DarkSideLoader marketplaces on them.

9. LOW-VOLUME CAMPAIGNS OF HIGHLY TARGETED PHISHING EMAILS FOCUSED ON ONE OR TWO PEOPLE WITHIN AN ORGANIZATION TO TRANSFER FUNDS DIRECTLY TO ATTACKERS

Highly targeted phishing messages to people with access to wire transfers hit organizations of every size across all industries. Often called "wire transfer phishing" or "CEO phishing," these scams involve deep background research by the attackers. These emails have spoofed senders so they appear to be from the CEO, CFO, or other executive; they rarely have links or attachments; and they include urgent instructions to the recipient to transfer funds to a designated account.

DOWNLOAD THE COMPLETE REPORT

proofpoint.com/humanreport