proofpoint™

RESEARCH REPORT

THE HUMAN FACTOR 2016

Today's advanced attacks focus more on exploiting human flaws than system flaws. Proofpoint developed The Human Factor to explore this under-reported aspect of enterprise threats.

This paper presents original field research using data gathered by Proofpoint products deployed in customer settings around the world. It covers the latest trends in the top vectors for targeting people: email, social media, and mobile apps. The Human Factor reveals not just who is clicking what, but how threat actors are using social engineering to get people to perform the work of automated exploits. Because as the data make clear, the weakest link in security is all of us.

EXECUTIVE SUMMARY

Life imitated art in 2015 as real-world cyber criminals every day applied the mantra of the anti-hero hacker of the cable TV series Mr. Robot: "People make the best exploits." Social engineering became the No. 1 attack technique. Attackers shifted away from automated exploits and instead engaged people to do the dirty work—infecting systems, stealing credentials, and transferring funds. Across all vectors and in attacks of all sizes, threat actors used social engineering to trick people into doing things that once depended on malicious code.

Attackers use people in three progressively controlling ways:

Running attackers' code for them.
These attacks comprised mainly high-volume campaigns distributed to broad groups of users. They used a variety of ruses to evade technical detection and convinced people to disable or ignore security, click links, open documents, or download files that installed malware on laptops, tablets, and smart phones.

Handing over credentials to them.
These attacks appeared frequently in medium-volume campaigns. They targeted key people who had valued credentials, such as usernames and passwords to crucial systems or useful services, tricking them into turning over their "keys to the castle."

Directly working for them, transferring funds to them.
These attacks were narrow and highly targeted. They aimed for users with the right job duties and ability act directly on behalf of attackers. These users, thinking they were following orders from higher-ups, most often made wire transfers to fraudulent bank accounts.

These attacks differed in scale and volume. But they all shared one common thread: using social engineering to persuade people to do the work of malware—and deliver big dividends for the attackers.

IN 2015, SOCIAL ENGINEERING WAS THE #1 ATTACK TECHNIQUE. PEOPLE REPLACED EXPLOITS AS ATTACKERS' FAVORITE WAY TO BEAT CYBERSECURITY.

TABLE OF CONTENTS

KEY FINDINGS & DEFENSIVE RECOMMENDATIONS

1. People are replacing automated exploits as attackers' preferred entry tactic

By an overwhelming margin, attackers infected computers by tricking people into doing it themselves, not through automated exploits. A whopping 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 link to hosted malware, either as an executable or an executable inside an archive. To work, these files have to be opened by the user. So attackers trick users into double-clicking them and infecting themselves.

Recommendation: *While dynamic malware analysis can be especially effective in detecting never-before-seen threats, consider a solution that also includes predictive analysis to prevent malicious threats from ever reaching the user. By examining suspicious URLs and attachments using a wide range of techniques, dynamic and predictive malware analysis approaches detect and block today's complex threats more effectively. To address the "human factor" of attacks, make users aware of the latest social engineering and credential-phishing schemes through regular training. Done right, "phishing" your own employees can also be a useful test of how effective your user-awareness efforts are.*

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. The document files in these messages contained malicious macros that tricked the recipient into running code to infect their computer. Employees' inboxes continued to be the primary way banking Trojans gain entry into your organization. Attackers use social engineering and mimicking familiar processes like invoices and statements to trick a user into clicking on the messages in their email. With social engineering, these messages may be even appear to be coming from a colleague or manager.

Recommendation: *Deploy robust security measures and controls that operate within your email flow. Consider real-time malware analysis services at the email gateway to detect and block threats before they reach your people.*

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. Even so, there was no time of day or day of week when malicious content was not being sent to people—or being clicked by them.

Recommendation: *Given that network-based security solutions cannot consistently detect threats within email and social media posts, consider solutions that integrate with these platforms. Automation can help you scale your security operations, quickly respond to system alerts, and discern high-priority threats. Look for a solution that can automatically block verified threats, quarantine infected users, and protect others from being infected.*

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. One in five clicks on malicious URLs occurred off the network, many of them from social media and mobile devices. Malicious mobile apps are no longer corner cases—they're real-world threats. Our analysis of authorized Android app stores discovered more than 12,000 malicious mobile apps— capable of stealing information, creating backdoors, and other functions—accounting for more than 2 billion downloads.

Recommendation: *To detect these risks and prevent attacks, consider a mobile-focused threat intelligence and defense solution. In addition to malicious apps, the solution should address riskware—apps that, while not always overtly malicious, engage in risky behavior. Riskware is invisible to mobile device management tools, which is why they're found on so many employee- and company-owned mobile devices. These apps exhibit a wide range of dangerous behavior that leads to leaked sensitive enterprise data, stolen credentials, or exfiltrated data—often used to target employees in future attacks. Look for a solution that can assess, detect, and control risky behavior in a way that doesn't interfere with users' legitimate productivity and privacy needs.*

5. URLs linking to credential-phishing pages were almost three 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. In email phishing campaigns, attackers link to pages designed to entice people to provide their logins and other personal information. In effect, the victim does the work of keyloggers, infostealers, and other automated malware.

Recommendation: *Adopt a solution that combines deep analysis, content inspection, and robust URL intelligence services. To stop these threats before they reach your people, consider an agentless, cloud-based service that rewrites all URLs contained in email and tests every URL at the time a user clicks. Attacks target people wherever they work. Be sure your defenses extend to users regardless of whether they are accessing a URL on the corporate VPN, an unsecured public connection, or on their own mobile device.*

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. Phishing emails that use these brands are more likely to succeed at tricking the user into clicking, especially if the victim receives the message from someone in their contacts list. These brand lures are effective because these services are familiar, and the user is used to clicking to sign in to view shared content.

Recommendation: *Get ahead of threats and respond to them faster with better insight and intelligence. Visibility into the nature of campaigns targeting your company is key to reducing the time and effort required to stop an attack and contain the damage. When security teams understand the size, type, and urgency of the threats—along with a detailed view of affected users—they can act more quickly. Consider predictive defenses to get ahead of attack campaigns: proactively sandboxing suspect URLs can preemptively identify URLs that are likely malicious—before users even get the chance to click and compromise their machine.*

7. Phishing is 10 times more common than malware in social media posts

The fastest growing social media threat was fraudulent customer-service account phishing, which uses social engineering to trick users to divulge logins and personal information. The ease of creating fraudulent social media accounts for known brands drives a clear preference for phishing in social media-based attacks. Distinguishing fraudulent social media accounts from legitimate ones is difficult: 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.

Recommendation: *Don't allow fake social media accounts to become a conduit for phishing and social engineering. Start by choosing a solution that can discover, notify, and continuously monitor social media accounts linked to your brand. Your solution should be able to detect and analyze fake accounts to protect your customers and reputation.*

8. Dangerous mobile apps from rogue marketplaces affect two in five enterprises

Our researchers identified rogue app stores that allowed users to download malicious apps onto iOS devices – even those not "jailbroken," or configured to run apps not offered through Apple's iTunes store. Lured in by "free" clones of popular games and banned apps, users who download apps from rogue marketplaces—and bypass multiple security warnings in the process—are four times more likely to download an app that is malicious. 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—that is, rogue app stores—on them.

Recommendation: *Deploy a solution that can continuously detect and control risky app behavior on mobile devices, because users can download apps from almost anywhere, even on devices that aren't "jailbroken." Few, if any, of these rogue app stores police their contents; even sanctioned app stores come with their own security and compliance risks. For one, they don't require apps to have privacy policies. And the stores usually vet each app only once. So once an app is approved, subsequent updates can easily introduce risky or malicious behavior—which can go undetected for months after the initial download.*

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 Business Email Compromise (BEC) scams involve deep background research by the attackers. The 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.

Recommendation: *Stopping this threat requires a combination of technology solutions and procedural controls. From a technical perspective, you need an email gateway that supports advanced configuration options for flagging suspicious messages based on attributes (such as direction and Subject line) and email authentication techniques. For procedural controls, ensure that internal finance and purchasing controls are in place to authenticate legitimate requests, including addition of a secondary, out-of-band in-person or phone approval by another individual in the organization.*

General Recommendations

At the same time, get better visibility into the nature of attacks against your organization so you can quickly distinguish between targeted and indiscriminate campaigns. Your tools should be able to reveal:

- *Who has received a malicious email*
- *How many versions of the same message was delivered*
- *When they were received*
- *Which users clicked*
- *Which users reached the malicious destination*

Having this information readily available is critical to prioritizing your response

SECTION 1

BY THE NUMBERS

TARGETING PEOPLE WHEN AND WHERE THEY CLICK

In 2015, the majority of attacks were high-volume email campaigns. Marked by their use of mass-customization for evasion purposes, high volume campaigns focused on reaching as many people as possible, blanketing regions with millions of messages sent from hundreds of thousands of compromised legitimate IP addresses in minutes. No organization, industry, or user role escaped exposure to advanced threats.

THREAT TARGETING BY GEOGRAPHIC REGION

The high-volume campaigns of 2015 were much more targeted by region than by organization or individual user, with threat actors often focusing resources on a single country at a time.

- Broad-based campaigns are highly targeted by region, with localized email lures, malicious document templates, and payloads. This tailoring of campaigns to their target regions makes them more realistic to recipients and thus more effective at driving clicks, as demonstrated by infection rates for campaigns.

- Botnets and payloads that are observed primarily in a single country or region can move to others. This variation became more common later in 2015; these shifts in resources and targeting often used accompanied by email lures and attachments that were adapted to the new target region.

While the high-volume campaigns of 2015 have generally been highly targeted by geography, within their targeted region they were much less selective: email campaigns targeted every person and department in an organization.[1]

Distribution of Top Campaigns by Region

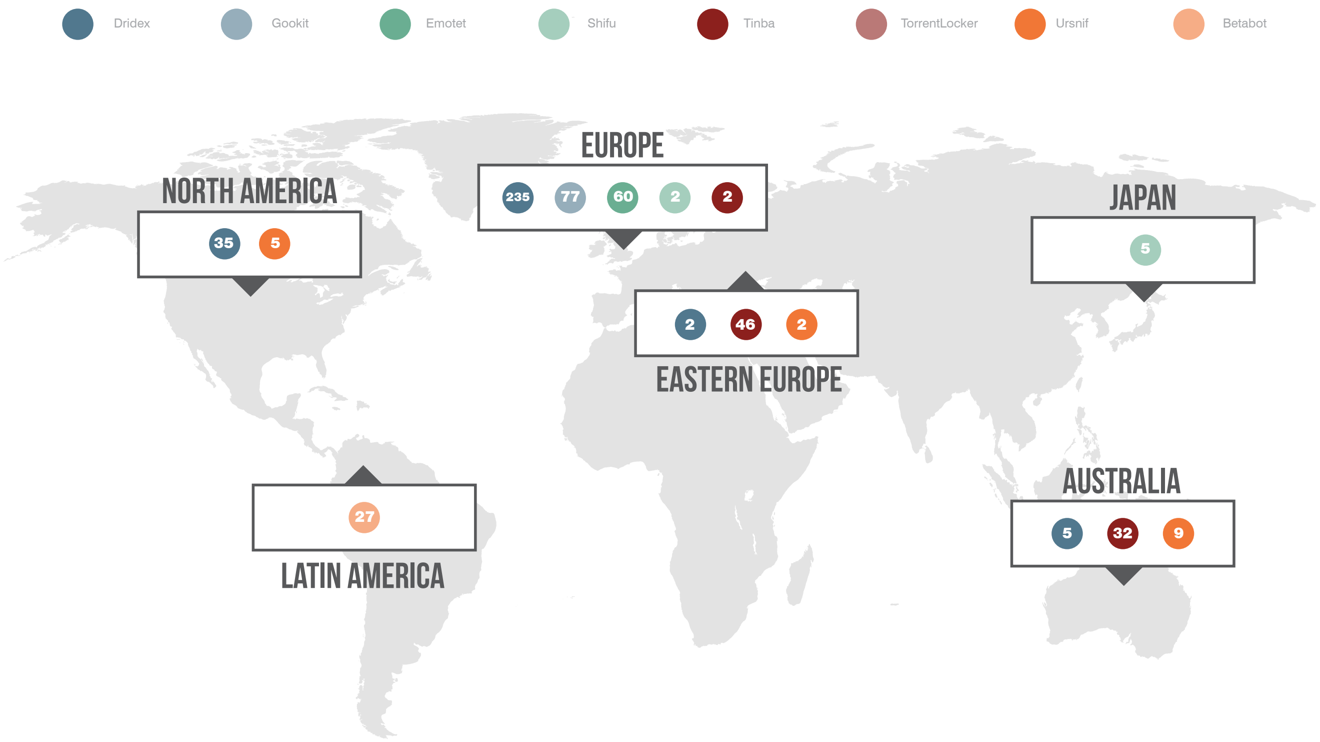


Figure 1: Number of campaigns per malware payload by geographic region, 2015

[1] Surprisingly, the distribution of messages by department is not flat, as would be expected if attackers were blasting messages at every available address for users and departments in a given organization. This is likely an effect of the fact that the longer a person is with a company, the more likely it is that their address will be on a spammer's list of valid email addresses for that company. Departments (and industries) with lower rates of employee turnover will have a higher percentage of their employees' email addresses on the lists purchased by the spamming services used by these broad-based campaigns.

EMAIL THREAT TARGETING BY DAY OF WEEK

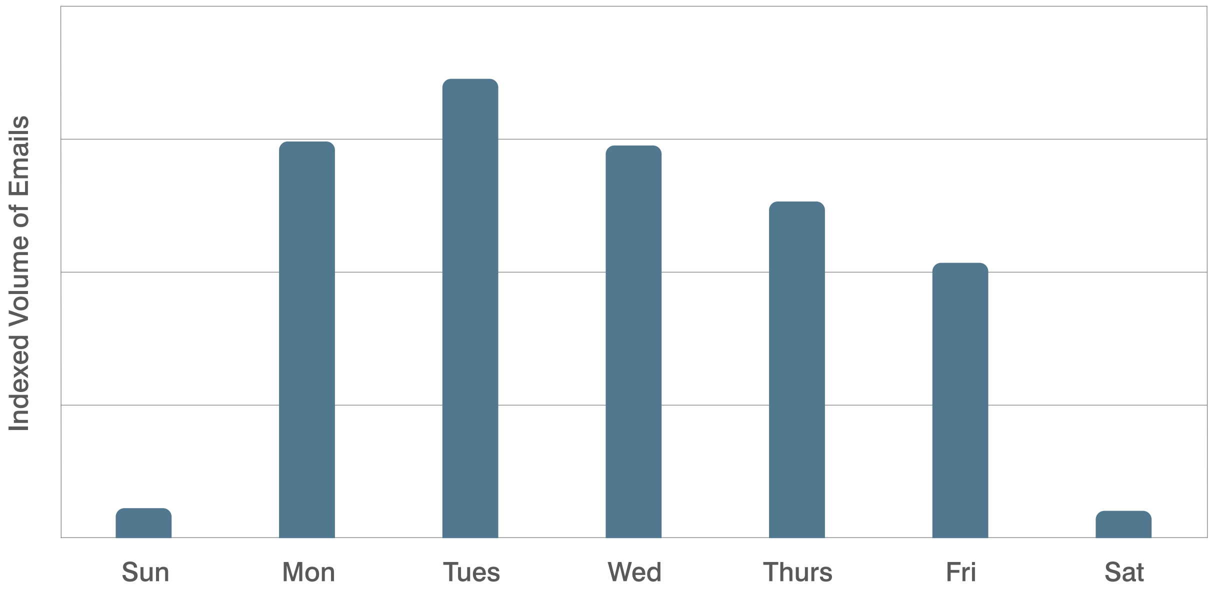


Figure 2: Indexed average daily volume of malicious messages sent per day of the week

- As they did in 2014, threat actors continued to make Tuesday their heaviest delivery day for campaigns in 2015, though the difference compared to other days of the week was less pronounced.
- We saw a clear emphasis on the first half of the week. Monday through Wednesday were the most popular days to launch spam campaigns.
- Click counts per day of the week followed a similar trend: Monday and Tuesday switched places as the top days, and volume of clicked URLs gradually decreased over the course of the work week.
- Though lower than during the work week, message volume and click rates for weekends (Saturday and Sunday) showed that users are still receiving and clicking on malicious URLs in spam emails. That means organizations need to be able to protect users regardless of whether they are on the corporate network or clicking from a smartphone or tablet.

Late 2015 saw several massive campaigns launched on Monday, possibly to capitalize on Monday's higher click-through rates. Although at first these appeared to be isolated incidents, campaigns in the first months of 2016 suggest that this marked the start of a long-term change in the timing of spam email campaigns.

EMAIL THREAT TARGETING BY HOUR OF DAY

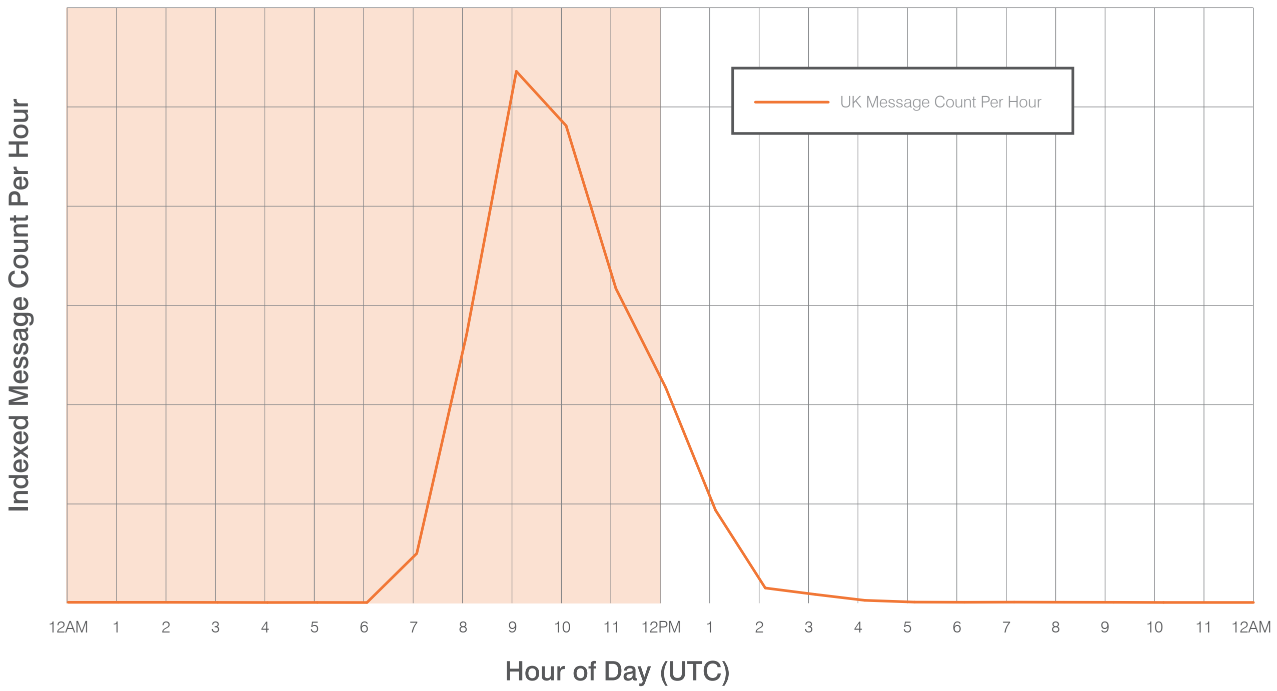


Figure 3: Example of malicious message delivery by hour of day, UK Dridex campaigns

- Email campaigns were timed to arrive at their target organization between 9-10 a.m. local time. The goal: catch people as they arrive at work but before IT teams have had a chance to detect and remove malicious messages.

- The most-used email lures took advantage of this timing: invoices, receipts, and scanned document lures targeted corporate users and were designed to get their attention at the start of the workday.

- The distribution of emails during the course of the day followed a pattern similar to that we saw in 2014, with spikes that correspond to the start of the day in the targeted time zone.

- The longer an email sits in a user's inbox, the less likely it is to be clicked. And over the course of both the day and the week, click rates decrease. With that in mind, attackers front loaded delivery for both the day-of-week and time-of-day.

SOCIAL MEDIA THREAT TARGETING BY HOUR OF DAY

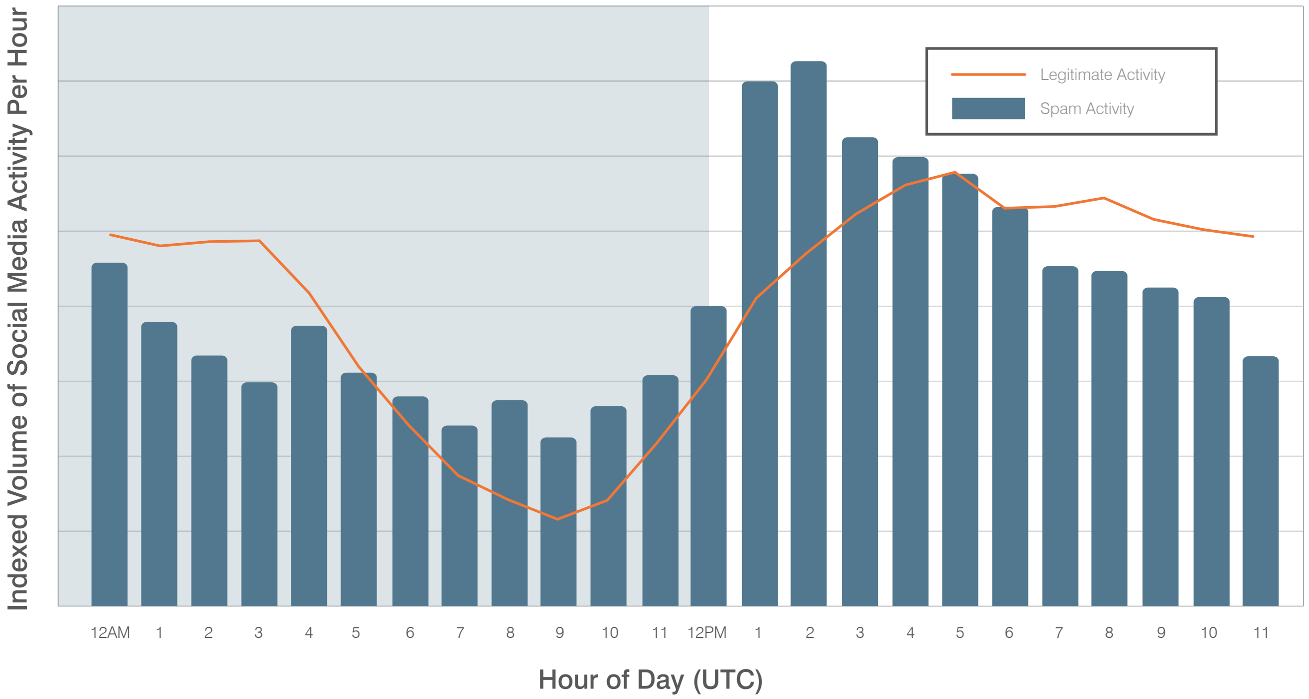


Figure 4: Legitimate and spam social media activity by hour of the day

- Attackers optimize their activity to match the peak engagement hours of the targeted venue. As they target organizations, they take into account both audience and time zone.
- The peak hours for social media spam begin around 8 a.m. ET and continue for about five more hours to 2 p.m. ET, gradually decreasing over the course of the U.S. business day. This peak activity period represents most of the morning through lunch, when people are most active on Facebook and other social media.
- Social media spam activity never ceases completely. Day-in and day-out, a spammer somewhere is posting fraudulent and potentially malicious content.

21.5% OF CLICKS WERE OFF-NETWORK

SUMMARY

Advanced threat actors are clearly targeting users based on users' moments of weakness amid peak traffic and fatigue. Social media threats and mobile apps joined email in convincing users to infect their own systems. One in every five clicks on malicious URLs occurred off the network. And this year, the off-network threat of malicious emails was complemented by the rise of social media and mobile app threats.

THREAT TARGETING BY MALICIOUS MOBILE APPS

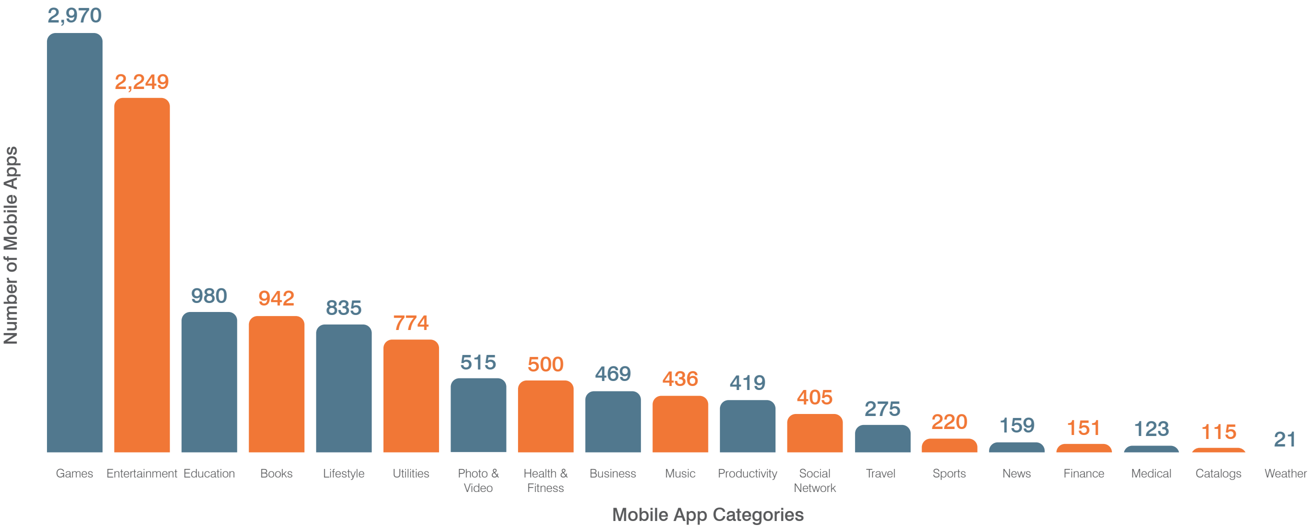


Figure 5: Malicious mobile apps by category

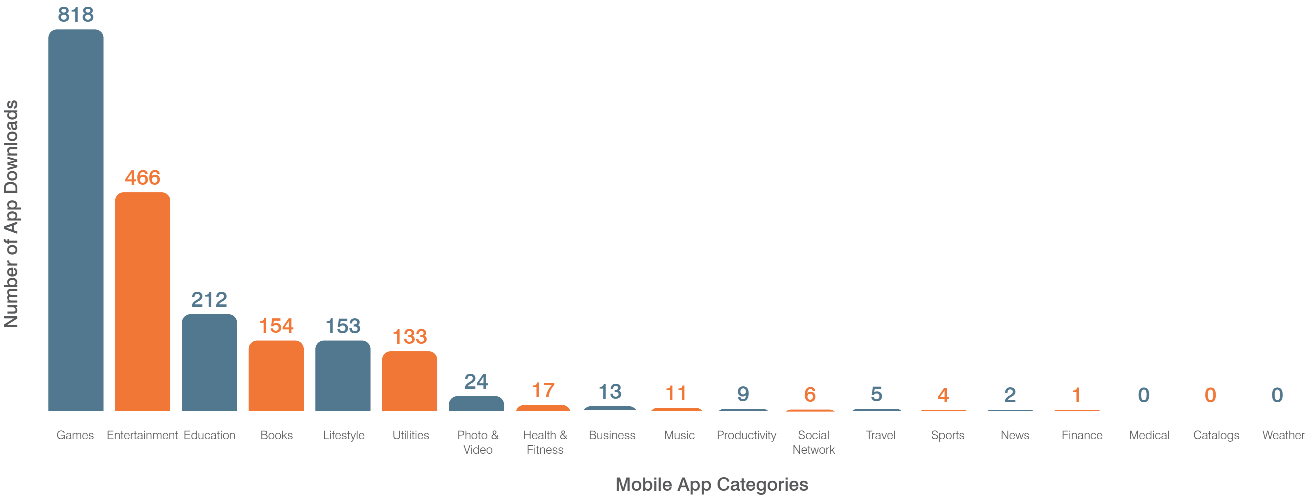


Figure 6: Malicious mobile app downloads by category

- People downloaded malicious mobile apps for Android alone over 2 billion times.
- Malicious apps heavily target the games and entertainment app categories.
- Many of these malicious apps pose as free or pirated versions of popular for-pay apps, from games to productivity tools. This lure entices users to willingly download malware onto their smartphones and tablets.

Malicious apps are an attractive vector for attackers. Unlike email-based campaigns, which rely on spam messages to millions of users, an app placed in a single store can reach millions of potential users.

SUMMARY

Dangerous mobile apps from rogue marketplaces affect 2 in 5 enterprises.

Our researchers identified rogue app stores from which users could download malicious apps onto iOS devices. The rogue app stores worked even for devices that were not configured to run apps not offered through Apple's iTunes store (also known as "jailbroken" devices). Lured in by free clones of popular games and banned apps, users who download apps from rogue marketplaces – and bypass multiple security warnings in the process – are four times more likely to download an app that is malicious. These apps steal personal information, passwords or data. Some 40% of large enterprises sampled by Proofpoint TAP Mobile Defense researchers had malicious apps from DarkSideLoader marketplaces – that is, rogue app stores – on them.

PEOPLE DOWNLOADED MALICIOUS MOBILE APPS FOR ANDROID ALONE OVER 2 BILLION TIMES.

SECTION 2

EXPLOITING PEOPLE

Findings in previous Human Factor reports demonstrated that “every organization clicks.” Regardless of size, location, or industry, the rate of clicking on malicious URLs was never zero. In past years, user clicks on malicious URLs in unsolicited emails drew their system into a sophisticated cybercrime infrastructure. These campaigns used automated exploits to infect the user’s system with a malware payload or steal their information.

That’s changing. In 2015, attackers engaged users – people – to do the work of automated exploits. This section shows how this shift appeared in everything from the kinds of malware threat actors used to the emails, lures, and social media posts that made up their campaigns.

PEOPLE RUNNING ATTACKERS' CODE FOR THEM

In 2015 attackers overwhelmingly infected computers by tricking people into doing it themselves instead of using automated exploits.

- **99.7% of documents used in attachment-based campaigns relied on social engineering and macros, rather than automated exploits.** (See ”Enable (Malicious) Content” for a detailed look at how these campaigns worked.)

- **98% of URLs in malicious messages link to hosted malware, either as an executable or an executable inside an archive.** Exploit kits use malicious code to automatically infect the user; hosted malicious archive and executables files require tricking the user into infecting themselves by double-clicking on the malware

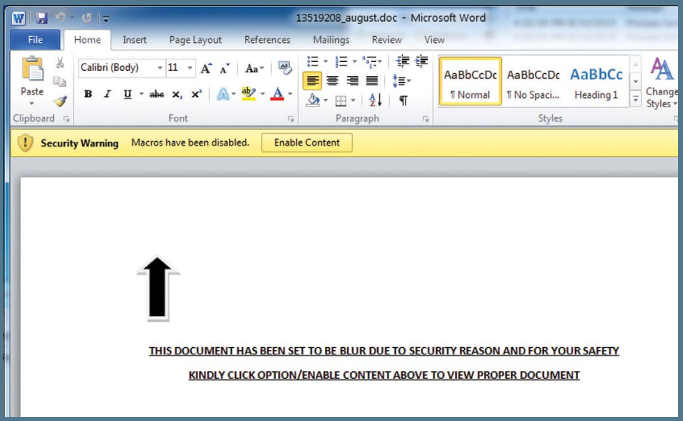
Exacerbating this issue was the dramatic scale of the Dridex banking Trojan campaigns, which made people central to the infection chain. In 2015, banking Trojans were the most popular type of malicious document attachment payload (Fig. 9). They accounted for 74% of all payloads, and Dridex message volume was almost 10 times greater than the next most-used payload in attacks that used malicious document attachments. The documents themselves used malicious macros extensively and relied on social engineering to trick the user into running the malicious code to infect their computer.

98% OF URLS & 99.7% OF DOCUMENT-BASED ATTACKS RELIED ON PEOPLE TO EXPLICITLY CLICK TO DISABLE SECURITY.

ENABLE (MALICIOUS) CONTENT

Malicious Microsoft Office macros, also known as VBA (Visual Basic for Applications) viruses, are snippets of code that can be embedded within an Office document such as Word or Excel. When the document is opened, these macros can execute a variety of operations—including automatically running the downloader for a piece of malware. VBA viruses dominated as an attack method in the late 1990s. But they quickly faded almost a decade ago, when Office 2007 began disabling macros by default. This remains the default setting for Microsoft Office. When a user opens an Office document with macros, they see a warning that enabling macros “makes your computer vulnerable to potentially malicious code and is not recommended.” (See Figure 7.)

Despite this protection, malicious macros came roaring back to life in late 2014 and early 2015. They spread through phishing campaigns, bolstered by a variety of social engineering techniques that trick recipients into enabling macros themselves. Once enabled, the macros install a variety of malware payloads on victims’ computers.



THIS DOCUMENT HAS BEEN SET TO BE BLUR DUE TO SECURITY REASON AND FOR YOUR SAFETY

KINDLY CLICK OPTION/ENABLE CONTENT ABOVE TO VIEW PROPER DOCUMENT

Figure 7: Example of Microsoft Word attachment with prompt to enable malicious macro

Because this technique requires the victim to directly enable macros—in most cases by clicking the “Enable Content“ button—social engineering is central to these campaigns.

Document attachments with malicious macros are most often tied to attackers who use the Dridex banking Trojan. But this technique is widely used to distribute a range of other malware, including malware used by sophisticated advanced persistent threat (APT) attackers. The great advantage of this approach is that the vector people cannot be patched — instead turning the user’s willingness to click into a central part of the infection chain.

EMAIL THREAT VECTOR TRENDS: URL VS ATTACHMENTS

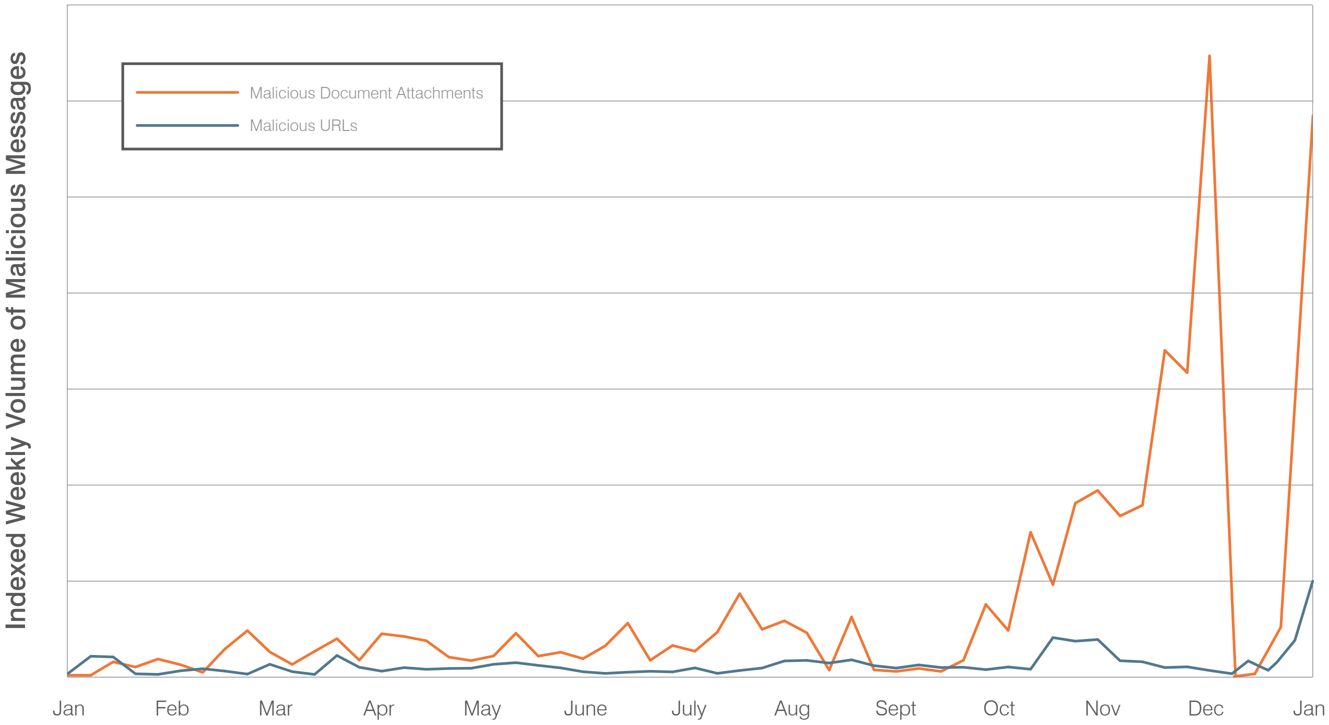


Figure 8: Indexed trend of malicious URLs vs document attachments, 2015

- Threat actors preferred malicious document attachments over URLs by a wide margin for email-based attacks in 2015.
- Rather than switching back to URL-based campaigns later in 2015 as defenses adapted, attackers instead dramatically increased the size of their campaigns and aggressively targeted organizations in the UK and Europe.
- URL-based campaigns of the type observed in previous years were virtually non-existent compared to document attachment-based campaigns.
- Dridex threat actors went quiet during September after the arrest of key figures of a crime ring accused of using the malware to steal millions of dollars from victims. The arrests impacted their sending infrastructure and may have contributed to the high volume of the November-December campaigns.

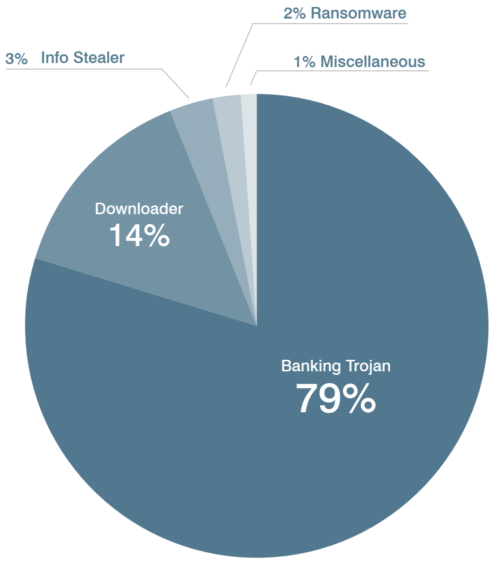


Figure 9: Malware payloads most frequently delivered by malicious document attachments

THREAT TYPES: ATTACHMENT MALWARE PAYLOADS

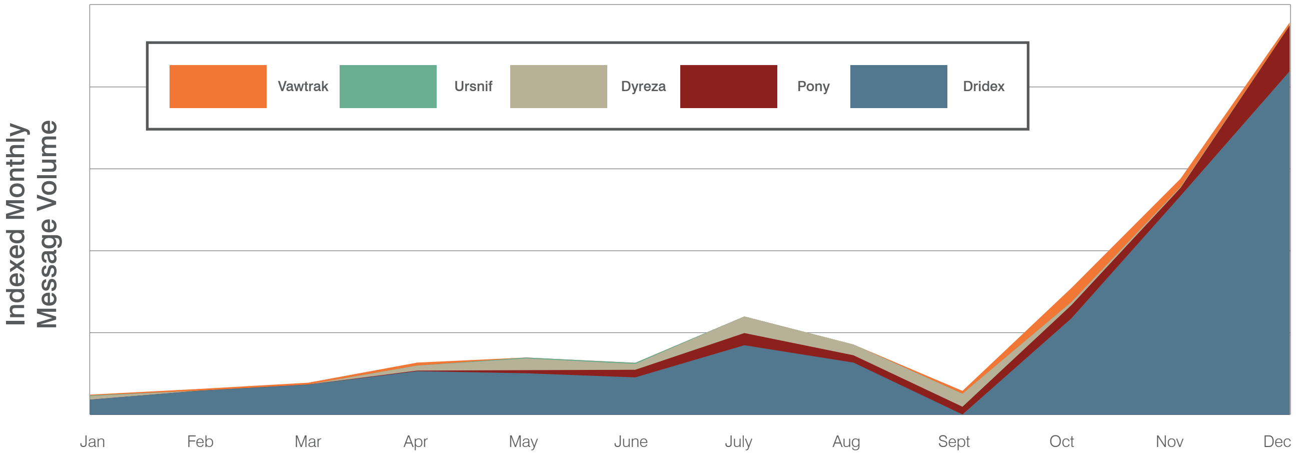


Figure 10: Weekly phishing document attachment malware payload as a percentage of total malware for top-5 payloads of 2015

Threat actors often align payloads with distribution techniques. For example, while banking Trojans were the dominant payload of campaigns using malicious document attachments, they were relatively rarely observed being distributed by exploit kits. Ransomware, on the other hand, rarely appeared in malicious document attachment campaigns but was very common in exploit-kit and archive-attachment campaigns. But by the end of 2015, these specializations began to broaden. We saw attackers begin to use payloads and distribution techniques that had not been associated before.[2] By the end of 2015, banking Trojans configurations changed and targeted credentials for users of a much wider range of services, everything from shipping and distribution accounts to cloud services.[3]

THREAT VECTOR TACTICS: MOST USED EMAIL LURES

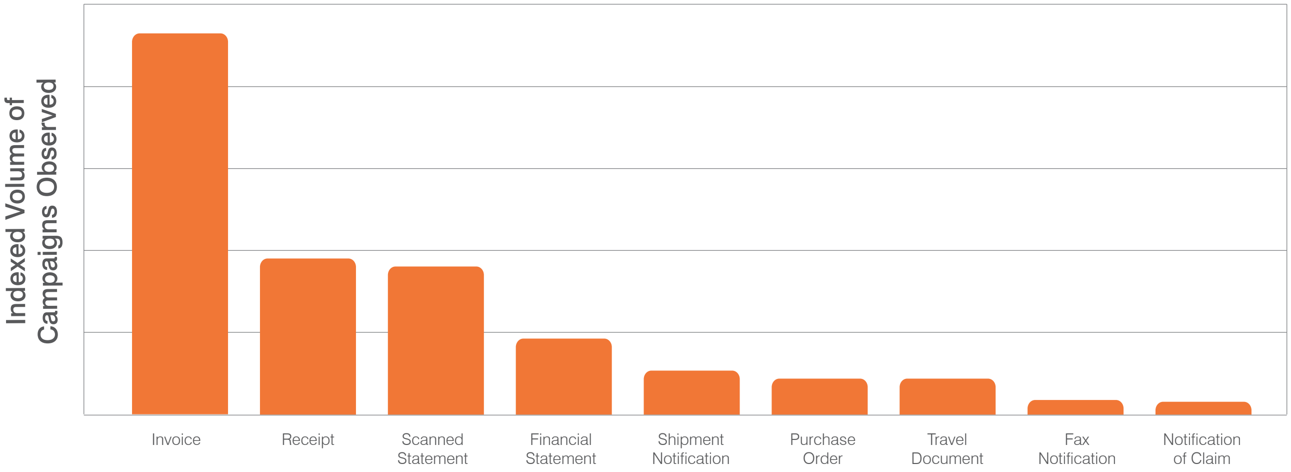


Figure 11: Most common email lures in document attachment campaigns

[2] "Dridex and Shifu give spam bots the day off and spread via exploit kits," November 18, 2015, http://www.proofpoint.com/us/threat-insight/post/dridex-shifu-give-spam-bots-day-off

[3] "Dyre malware campaigners innovate with distribution techniques," October 9, 2015, http://www.proofpoint.com/us/dyre-malware-campaigners-innovate-distribution-techniques

THREAT TYPES: MALICIOUS ATTACHMENT DOCUMENT FORMATS

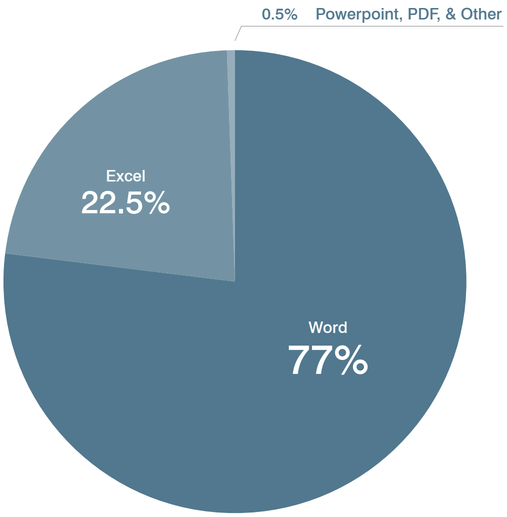


Figure 12: Top document attachments formats

- Not counting malicious and archived executables, document attachment campaigns were the most used technique of the year, with most of these documents relying on malicious macros to deliver their payloads. (See Figure 12.) The dominance of malicious documents in 2015 attests their effectiveness at enticing user to click.

- Excel files became more popular as the year went on. XLS attachments make it easy to create realistic order and billing documents, and end users are more accustomed to using active content to automatically update data in spreadsheets.

ROGUE APPS STORES: A DANGEROUS GAME

Mobile users are not immune to threats that target the human factor. For many, the lure of free games and other apps is enough to overpower normal safeguards. Offered through unsanctioned app stores, these rogue apps often come with an unwelcome feature: they install code that can steal personal information and create backdoors in corporate networks.

In 2015, an unauthorized app marketplace known as vShare found a way to serve unapproved apps to non-jailbroken iOS devices. We dubbed this type of rogue app store a "DarkSideLoader" marketplace, because it circumvented Apple's normal vetting process to sideload dangerous or unapproved apps. The apps can tap into private iOS APIs to access powerful operating system functions that Apple doesn't normally permit.

DarkSideLoader marketplaces make money through ads. More critically, they also embed malicious code such as remote access Trojans into otherwise legitimate apps and sell that access to attackers looking to infiltrate businesses and governments.

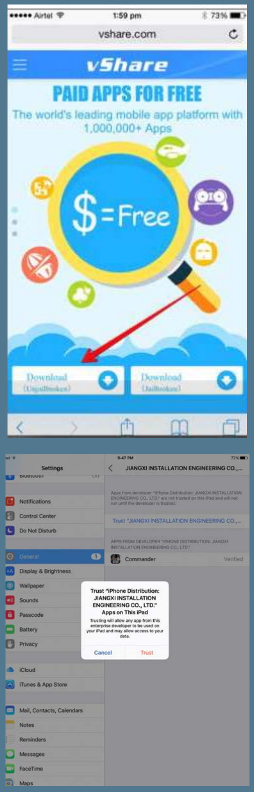
Users (or their children) often access a rogue app marketplace for a number of reasons:

- To download games, wallpaper, and other media for free
- Get free movies and other content
- Get free productivity apps
- Get apps not available on Apple's official app store

The top-ten paid apps on the Apple App Store are all available for free on the vShare marketplace, including well-known titles such as Minecraft and Geometry Dash, as well as business apps from publishers including Adobe and Microsoft.

To install these apps, people must – and do – click through multiple confirmation messages and warnings (see figures). Free downloads of popular paid apps draw people to DarkSideLoader marketplaces and entice them to click. This attraction is strong enough to outweigh the user's normal security concerns.

The vShare marketplace claims to offer 1 million apps, and Proofpoint has found over 15,000 iOS apps available through this DarkSideLoader site. The site claims over 40 million users. We have found that about 25% of those users are on iOS devices.



Apps from developer "iPhone Distribution: JIANGXI INSTALLATION ENGINEERING CO., LTD." are not trusted on this iPad and will not run until the developer is trusted.

APPS FROM DEVELOPER "IPHONE DISTRIBUTION: JIANGXI INSTALLATION ENGINEERING CO., LTD."

Trust "iPhone Distribution: JIANGXI INSTALLATION ENGINEERING CO., LTD." Apps on This iPad

Trusting will allow any app from this enterprise developer to be used on your iPad and may allow access to your data.

Figure 13: Installing apps from rogue app store

PEOPLE HANDING OVER CREDENTIALS TO ATTACKERS

URLs linking to credential phishing pages were almost three times more common than links to pages hosting malware. Our researchers found that on average, 74% of URLs used in email-based attacks linked to credential phishing pages, rather than to sites hosting malware (Fig. 14). In email phishing campaigns, attackers link to pages designed to entice people to provide their logins and other personal information. In effect, the victim does the work of keyloggers, info stealers, and other automated malware that would have been used to steal this information in past campaigns.

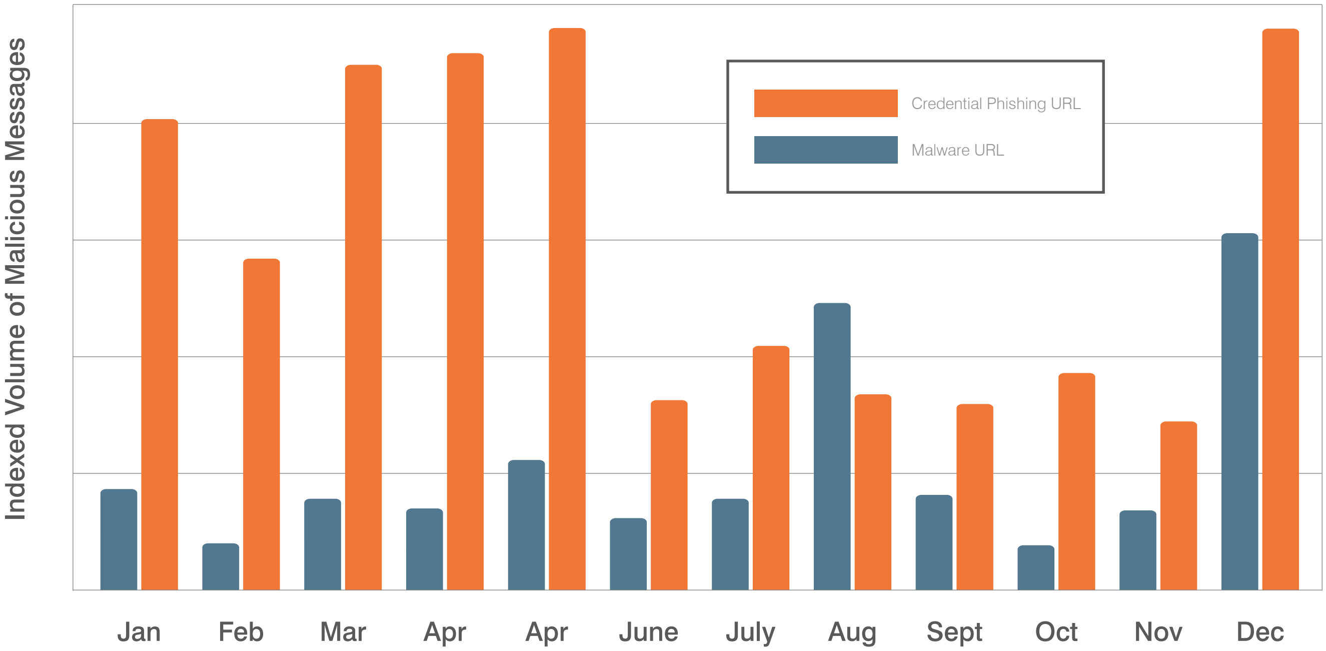


Figure 14: URLs linking to hosted malware vs credential phishing pages, 2015

- For most of the year, URLs linking to phishing sites outnumbered those linking to sites hosting malware by a factor of 4-6 times

- The seasonal decrease in use of credential phishing URL during the summer extended into the fall months

Apple-branded lures are the most used in credential phishing. But by a wide margin, accounts used to share files and images – such as Google Drive, Adobe, and Dropbox – were the most effective lures.

Google Drive phishing links were the most clicked credential-phishing lures. The presence of these brands can trick the user into clicking, especially if the victim receives the message from someone in their contacts. These brand lures are effective because users are familiar with these services and used to signing in with a click to view shared content.

THREAT VECTOR TACTICS: CREDENTIAL PHISHING

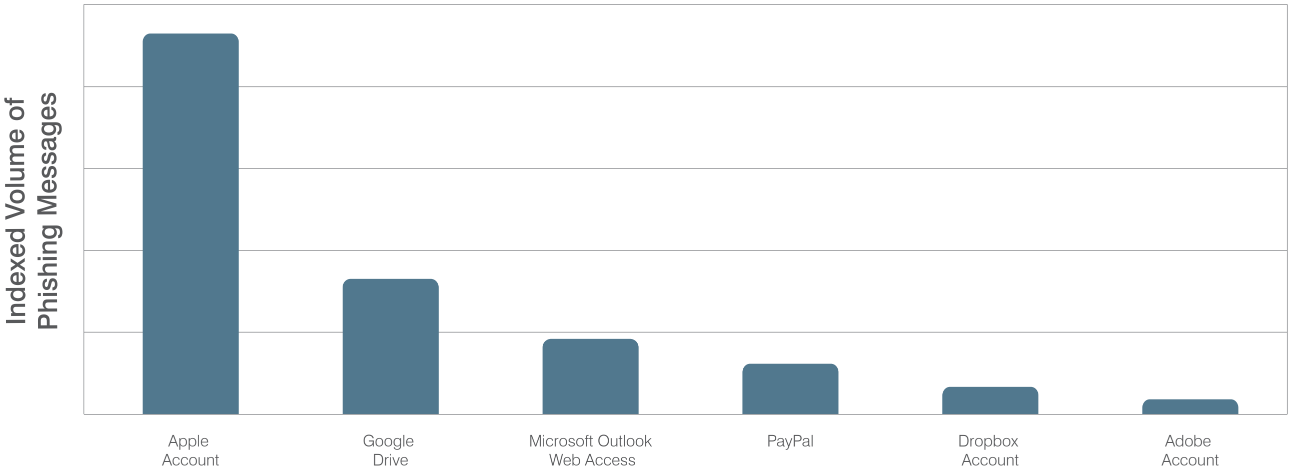


Figure 15: Most used brand lures in credential phishing

- Delivery volume does not correlate to click rates. Some brands are more effective than others in driving clicks on URLs in phishing messages. Although Apple ID phishing messages were the most sent, Google Drive phishing links were the most clicked. Conversely, Apple ID phishing URLs are the largest by volume but fifth by click rate.

- Accounts used to share files and images – such as Google Drive, Adobe, and Dropbox – are the most effective lures.

- Social networking invitation lures are no longer as effective they once were. The most clicked lures of the 2014 Human Factor report all but disappeared from credential phishing in 2016, through a combination of user education and changes by the social networking service providers to identify and mitigate the impact of phished user credentials.

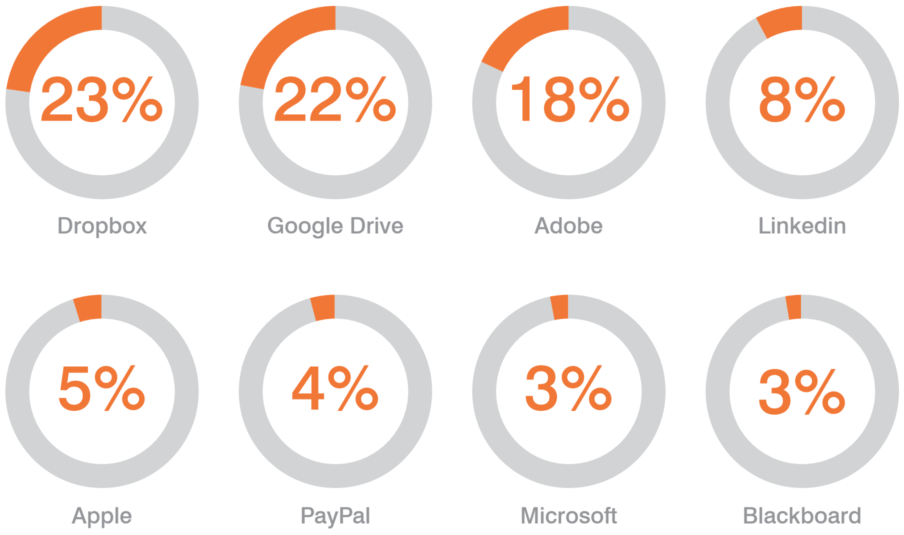


Figure 16: Most clicked brand lures in credential phishing

MOBILE APP THREATS COME OF AGE

2015 was the year that mobile attack vectors went from corner cases to pervasive threats. Data theft and misuse of resources apply to a wide range of mobile apps with suspect capabilities, from with known malware to the broader category of "riskware."

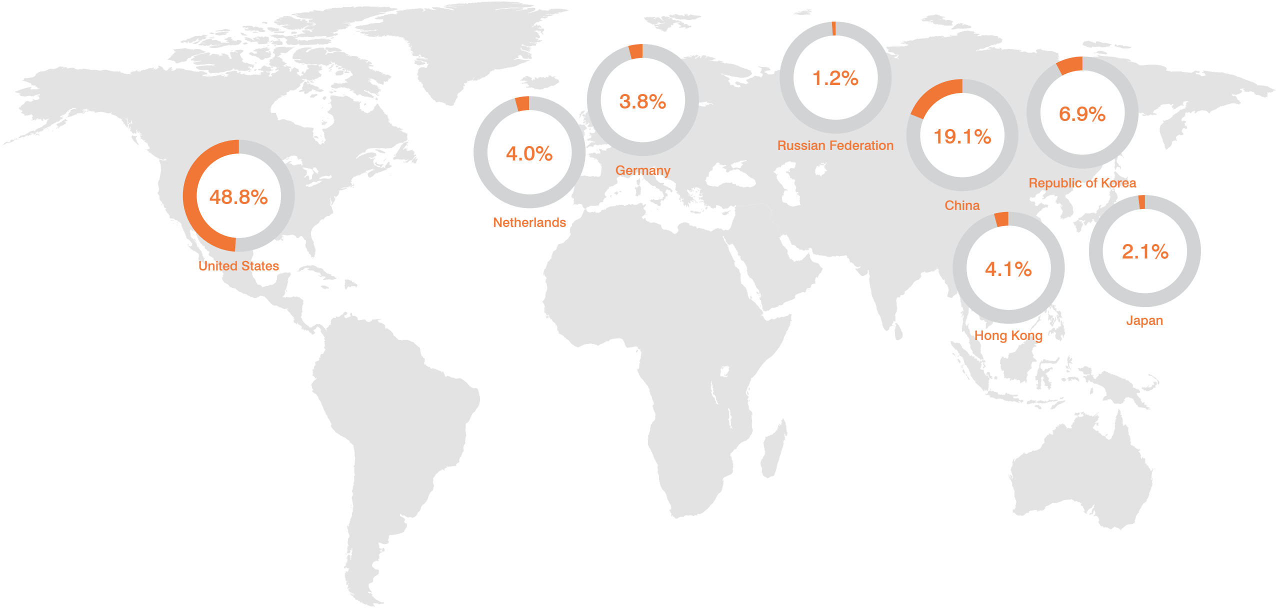


Figure 17: Top destinations for data sent by mobile apps, by percentage of apps sending to each country

- Data sent to the U.S. is not automatically safer.
- Malicious apps send data to servers in 56 countries outside the U.S. The top 10 destinations came from 86% of malicious apps.
- China is the No. 1 destination outside the U.S. for data from malicious apps.

PHISHING DOMINATES SOCIAL MEDIA ATTACKS

Phishing is 10 times more common than malware in social media posts. The ease of creating fraudulent social media accounts for known brands makes phishing the preferred technique in social media-based attacks.

The fastest growing social media threat was fraudulent customer-service account phishing, which uses social engineering to trick users into divulging personal information and logins. Distinguishing fraudulent social media accounts from legitimate ones is difficult. We found that 40% of Facebook accounts and 20% of Twitter accounts claiming to represent a Fortune 100 brand are unauthorized. And for Fortune 100 companies, unauthorized accounts on Facebook and Twitter make up 55% and 25% of accounts, respectively. (See inset "Phish in a Social Barrel".)

- Based on the fourth-quarter sample, a typical top brand on social media has an average of 340 Facebook Pages and 235 Twitter accounts. The top active financial-services brands have an average of 265 Facebook Pages and 200 Twitter accounts.
- Across top brands on social media, only 5% of those Facebook Pages are verified Facebook accounts, and only 20% of those Twitter accounts are verified Twitter accounts. (This was also true across top financial service brands.) That means up to 80% of accounts on Twitter and 95% of Facebook accounts are not verified by the brand.
- On average, we found five suspicious Facebook accounts and 30 suspicious Twitter accounts per brand. Financial-services brands had 50% more suspicious Facebook and Twitter accounts.
- Unauthorized accounts advertising giveaways of free gifts or membership points are among the most common. We found up to 330 such accounts for a single brand.
- 72% of malicious URLs leading to compromised sites are found on child-targeted accounts, such as those of cartoon shows.

PHISH IN A SOCIAL BARREL

Many brands are embracing social media to better serve customers. Already a preferred communications channel for many consumers, social media provides a fast, low-cost way to respond to questions and complaints. Now, hackers, scammers and pranksters are finding them useful, too.

Proofpoint Nexgate researchers saw a surge of fraudulent customer service accounts on social media in 2015. These accounts are used to phish credentials, steal personally identifiable information (PII), and tarnish respected brands.

One of the most significant attacks we see: fake retail banking customer service accounts that attackers use to phish bank account credentials. These attacks typically work like this:

1. A customer tweets a question (for example, “I lost my lost password”) to a bank’s Twitter customer service account.
2. An attacker, who has set up a convincing fake Twitter account and is monitoring the real one, sees the question. The attacker immediately tweets a “response” directly to the customer from the fake account. The account appears identical to the real account—logos, images, and so on. And the attackers often work after-hours to engage the victim before the real company sees the request.
3. The attacker’s tweet includes a link to a malicious website asking the customer to login to resolve their issue (reset their password, for example). When the customer logs in to the fake site, the attacker captures credentials to the customer’s bank account.

This approach lets attackers access customer account data without the trouble of penetrating bank infrastructure—they don’t even have to send a phishing email to bank customers.

These social media attacks are far more effective than similar email-borne threats. Most consumers have been warned many times by their bank to ignore unexpected email. But social media gives attackers an edge—customers are usually initiating the contact and often need help with their account. Social media enables them to craft a highly convincing phishing lure that the target expects to receive.

PEOPLE TRANSFERRING FUNDS DIRECTLY TO ATTACKERS

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 targeting people with wire-transfer access touched organizations of every size across all industries. Often called “wire transfer phishing” or “CEO phishing,” these scams usually show a high degree of background research on the part of 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 urgently instruct the recipient to transfer funds to an account (the attacker’s).

Among these attacks, we observed four different variants of message types:

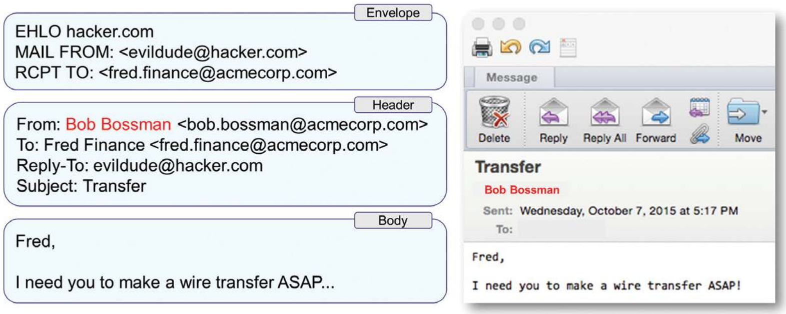
- Reply-to spoofing (75% of samples): Messages where the ”From” address is spoofed to be the real email address of the targeted sender (typically the CEO), but also contain a ”Reply-to” address where any replies are sent. Usually, the reply-to name is the same as the spoofed ”From,” but the address is unrelated, resembling something like ”ceo.executive@ presidentmail.com.”

- Spoofed name (21% of samples): Messages where the name of the ”From” address is the name of the CEO or similar, but the actual address is pointing at a third-party mail service such as Gmail.

- Spoofed sender with no “Reply-to”: In this instance, the message was spoofed to come from the CEO’s email address with no reply-to. This approach made it impossible for the attacker to carry on a conversation with the victim. So in this instance, the message contained complete wire instructions so that no further emails were required.

- Look alike domain: In this instance, the message used a ”From” address that spoofed the name of the CEO, but used a domain was one letter different from the customer domain. For example, a spoofed email from the CEO of legitcompany.com would be rendered legtcompany.com.

The broad-based campaigns of 2015 did not appear to target specific people or organizations. In contrast, low-volume campaigns of highly targeted phishing emails focused on one or two people within an organization. According to the FBI, the Internet Crime Complaint Center (IC3) began receiving complaints from businesses about trusted suppliers requesting wire transfers. These transfers ended up in banks overseas—and turned out to be fraudulent requests. Since then, “losses from the business e-mail compromise (BEC) scam have been significant.”



EHLO hacker.com
MAIL FROM: <evildude@hacker.com>
RCPT TO: <fred.finance@acmecorp.com>

From: Bob Bossman <bob.bossman@acmecorp.com>
To: Fred Finance <fred.finance@acmecorp.com>
Reply-To: evildude@hacker.com
Subject: Transfer

Fred,

I need you to make a wire transfer ASAP...

Transfer
Bob Bossman
Sent: Wednesday, October 7, 2015 at 5:17 PM
To:

Fred,

I need you to make a wire transfer ASAP!

Figure 18: Illustration of sender spoofing techniques in BEC phishing

These attacks embrace a “blockbuster” approach on the part of the attackers. While many of these messages will be quickly recognized by recipients as phishing, the small few that succeed can yield millions of dollars in fraudulent transfers. Unfortunately, these types of emails only rarely trigger typical spam rules. That’s because they look and feel legitimate, do not include a link or attachment, and do not arrive in high enough volumes to raise flags for anti spam services and applications.

CONCLUSION & RECOMMENDATIONS

UNDERSTANDING ADVANCED THREATS

As this analysis of attack trends shows, 2015 was a year in which attackers embraced the view that “people make the best exploits,” pivoting quickly and effectively to focus on techniques that put people at the center of the infection chain. From high-volume email campaigns to targeted attacks, and from email to mobile apps, attackers built social engineering into their lures and their vectors to exploit the people’s willingness to click and open an attachment, run someone else’s code, download an app, or hand over their credentials.

To understand the nature of the threats targeting the human factor, we must place them in the context of the larger framework used by many modern cyberattackers. It may be too early to tell whether this focus will continue through 2016, or if attackers will pivot just as rapidly to a new set of tools and techniques. What is certain, however, is that they will continue to use a threat framework that has proven to be flexible, adaptable, and resilient. This advanced threat framework consists of five elements: actor, vector, hosts, payload, and command-and-control channel.

This framework enables attackers to operate in robust, segmented ecosystems. They can specialize in certain parts of the framework and sell or lease it to others. And as Dridex takedown efforts in 2015 showed, such frameworks are resilient, surviving disruptions or failures of individual components.

But such frameworks also increase attackers' detection surface—and make them easier to detect. By tracking each of these elements, defenders can know what to expect in other elements and take the right countermeasures. Detecting and defending against today's advanced threats, organizations must adopt solutions that include the intelligence necessary to analyze each of these elements and respond effectively across the three main vectors that attackers use to exploit people: email, social media, and mobile.

RECOMMENDATIONS

Organizations need to take action to defend themselves against this wide range of threats; immediate actions include:

- Adopt advanced threat solutions to identify and block targeted attacks that travel over email, the No. 1 threat vector. These solutions must take into account the increasing sophistication of emerging threats and socially engineered attacks.
- Deploy automated incident response capabilities to rapidly identify and mitigate infections, including detecting and blocking command- and-control (C2) communication of infected systems.
- Patch client systems for all known operating system and application vulnerabilities to protect against aggressive exploit kits that reach clients via email, malvertising, and drive-by downloads.
- Update email gateway rules and internal financial controls to improve resistance against wire transfer fraud scams.
- Police social media activity for potentially fraudulent accounts that can hijack conversations with customers, steal personal and financial information, and damage brands ever-more reliant on social channels.

THE ADVANCED THREAT FRAMEWORK

ACTOR

The attacker organization; real humans driven by various motivations, often financial for cybercriminals.

VECTOR

The delivery mechanism; email via attacker-controlled or leased spam botnet is a dominant vector, though social media is growing.

HOSTS

The sites hosting malware; if malware is not directly attached to email, macro- enabled documents or exploit-kit emplaced droppers will source from these sites.

PAYLOAD

The malware; software that will enable the attacker to make use of (control, exfiltrate data from, download more software to) the target computer.

C2

The command and control channel that serves to relay commands between the emplaced malware and attackers.

proofpoint™

ABOUT PROOFPOINT

Proofpoint Inc. (NASDAQ:PFPT) is a leading next-generation security and compliance company that provides cloud-based solutions for comprehensive threat protection, incident response, secure communications, social media security, compliance, archiving and governance. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system. Proofpoint protects against phishing, malware and spam, while safeguarding privacy, encrypting sensitive information, and archiving and governing messages and critical enterprise information.

More information is available at www.proofpoint.com.