RESEARCH PAPER

A New Era in Phishing — Games, Social, and Prizes

Research Credits:
Or Katz
Principal Lead Security Researcher,
Akamai

Akamai

Table of Contents

Overview

Phishing attacks are an extremely common attack vector that have been used for many years, and the potential impacts and risk involved are well known to most Internet users. However, it is still a highly relevant attack vector being used in the wild, affecting many victims. How can a security threat continue to have a significant impact, despite the fact that many Internet users know about the risks and potential impact? We dive deeper into several recent phishing scams and provide insights into the modern phishing scam landscape and what makes these campaigns effective — and thus a continuously dangerous security threat.

New research from the Akamai Enterprise Threat Research team shines a spotlight on some of the most prominent phishing campaigns from 2017. Our research shows that despite broad awareness of phishing attack risks, attacks are still a relevant threat. More importantly, we found the attack techniques and elements being used in recent phishing campaigns to be highly effective, highly distributed, and long lived.

We believe the threat actors have evolved and elevated their attacks to counteract the improved awareness of Internet users to phishing exploits. The techniques used in recent phishing campaigns seek to play on victims' awareness and gain higher levels of trust, while not creating antagonism. This makes the attacks more effective by creating positive interaction with the victims, and encouraging them to spread the attacks within their own social media circles. We refer to such attacks as "positive" phishing campaigns.

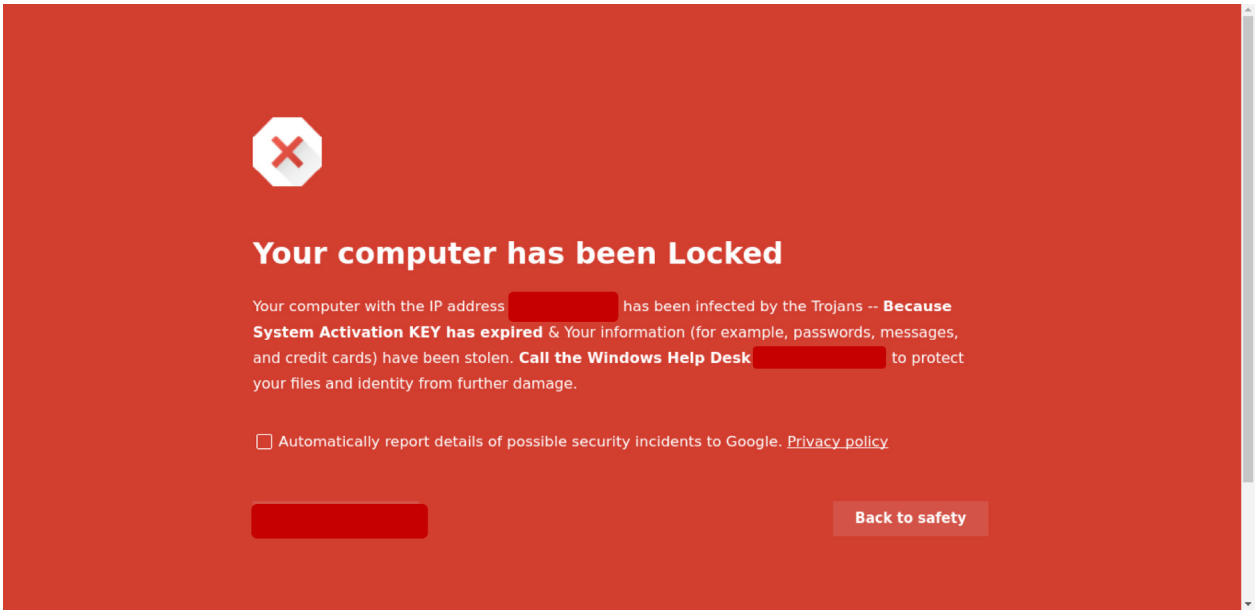

Figure 1: Example of a "negative" phishing attack — Your computer has been locked — leading users to download malicious software or call a fake help center

Negative campaigns (see Figure 1) activate the victim's negative feelings — such as fear, uncertainty, and doubt — making them highly effective, but also triggering defensive impulses in some cases. In contrast, "positive" campaigns highlight feelings of excitement, hope, and gratitude, and are gaining momentum. As "positive" campaigns interact with victims' positive feelings, they are frequently combined with elements of social networks, making these campaigns much more effective.

We are seeing growing momentum in the threat landscape of attacks that are starting to include elements of gaming, social networks, and prize winning. All of these elements serve the threat actor's main goal: to gain the user's trust and lead victims to divulge sensitive information. This trust is also used to spread the phishing campaign, by integrating steps that require the target to share the content via the target's social network, thereby increasing the campaign's impact and distribution.

Examining the way victims share phishing scams throughout social networks reveals an interesting insight. The attacks build upon the positive reputation of the targeted brands. Moreover, we can see that the "positive" campaign's victims often do not feel antagonized by the campaign. As a result, the victims are less likely to have negative feelings against the campaign and the brand, even after learning that they have been targeted.

As part of our research into recent "positive" phishing attack campaigns, we examined the two most meaningful elements leveraged by the attackers: 1) the use of games and prizes, and 2) the use of social networks and instant messaging.

Play a Game and Win a Prize

An interesting development in recent attack campaigns is the use of a gaming element. This is not surprising to observe, because it is well known that engaging users with games increases user commitment and gives a positive experience. We see gaming being introduced in areas such as customer feedback and user authentication, such as CAPTCHA challenges.

Here are some examples of the recent phishing campaigns that used gaming elements.

Wheel of Chance

The Akamai Enterprise Threat research team saw an attack campaign that included an element of gaming resembling a roulette wheel. This campaign prompts the victim to spin the wheel for a chance to win a free prize.

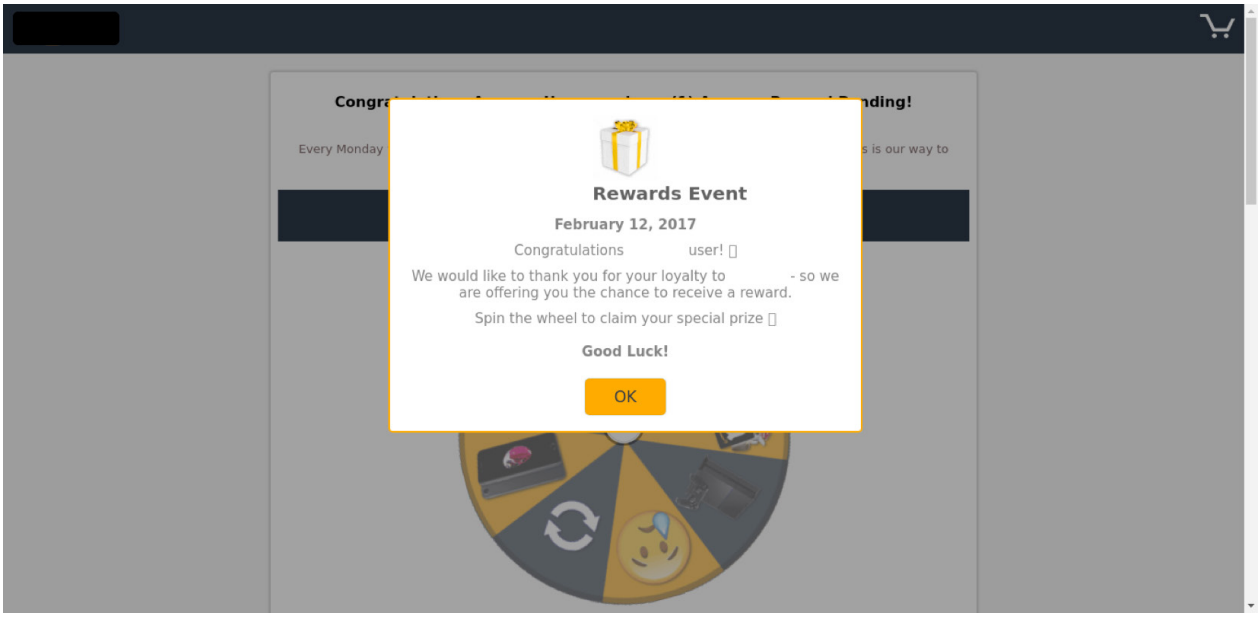

Figure 2: Wheel of fortune — "Spin the wheel to claim your special prize"

This particular attack campaign abuses the reputation of well-known companies by using their brands on the phishing website in order to gain the victim's trust.

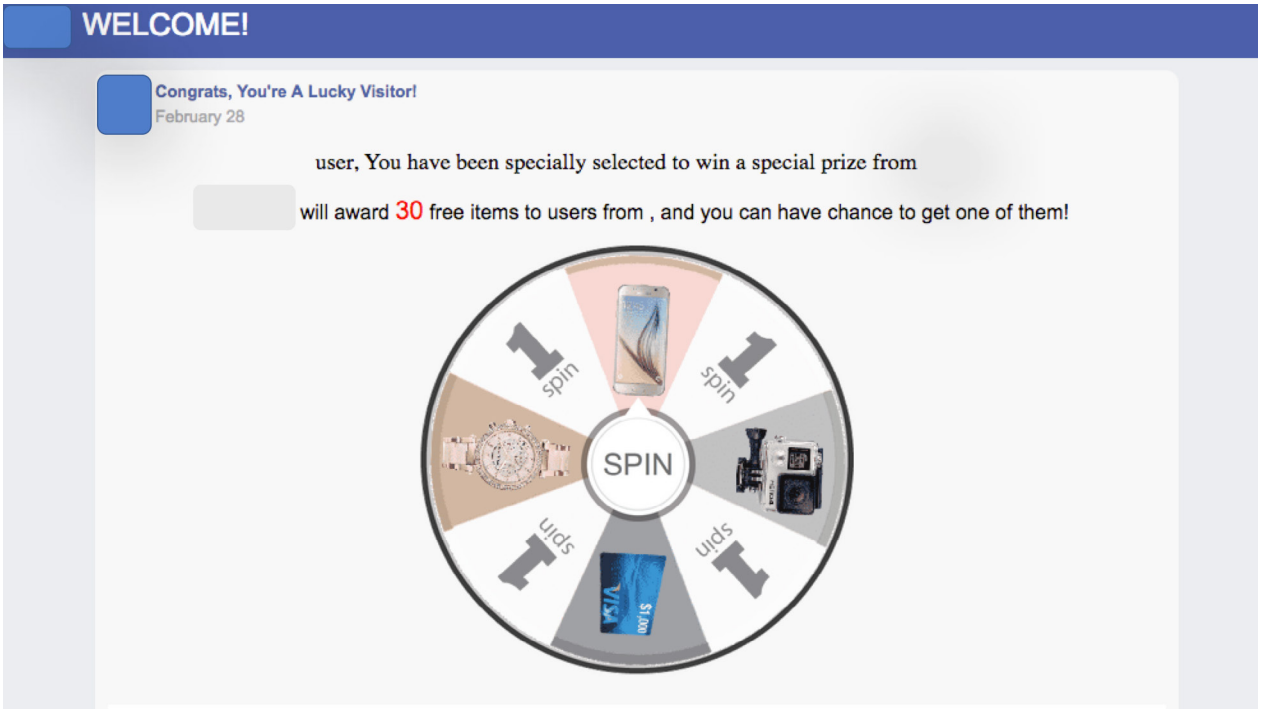

Figure 3: Wheel of fortune — "You have been specially selected to win a special prize"

All participants are declared winners and led to a website requesting private information from the victim. The phishing campaign usually targets sensitive information such as user login credentials, credit cards, email addresses, and personal information.

The Three Questions Quiz

Over the past year, we tracked the activity of more than 300 phishing campaigns, using the same toolkit that abuses more than 40 commercial brands. Each of these phishing campaigns begins with a short quiz in which a user is asked three questions related to the recognized brand. Therefore, we referred to this type of phishing scam as the "Three Questions Quiz." Regardless of the answer that is selected, the victim always wins.

The phishing campaigns share identical functionality and features, as a result of using the same toolkit. According to our analysis of toolkit usage in the wild, the evidence suggests individual phishing campaigns are being activated by different threat actors.

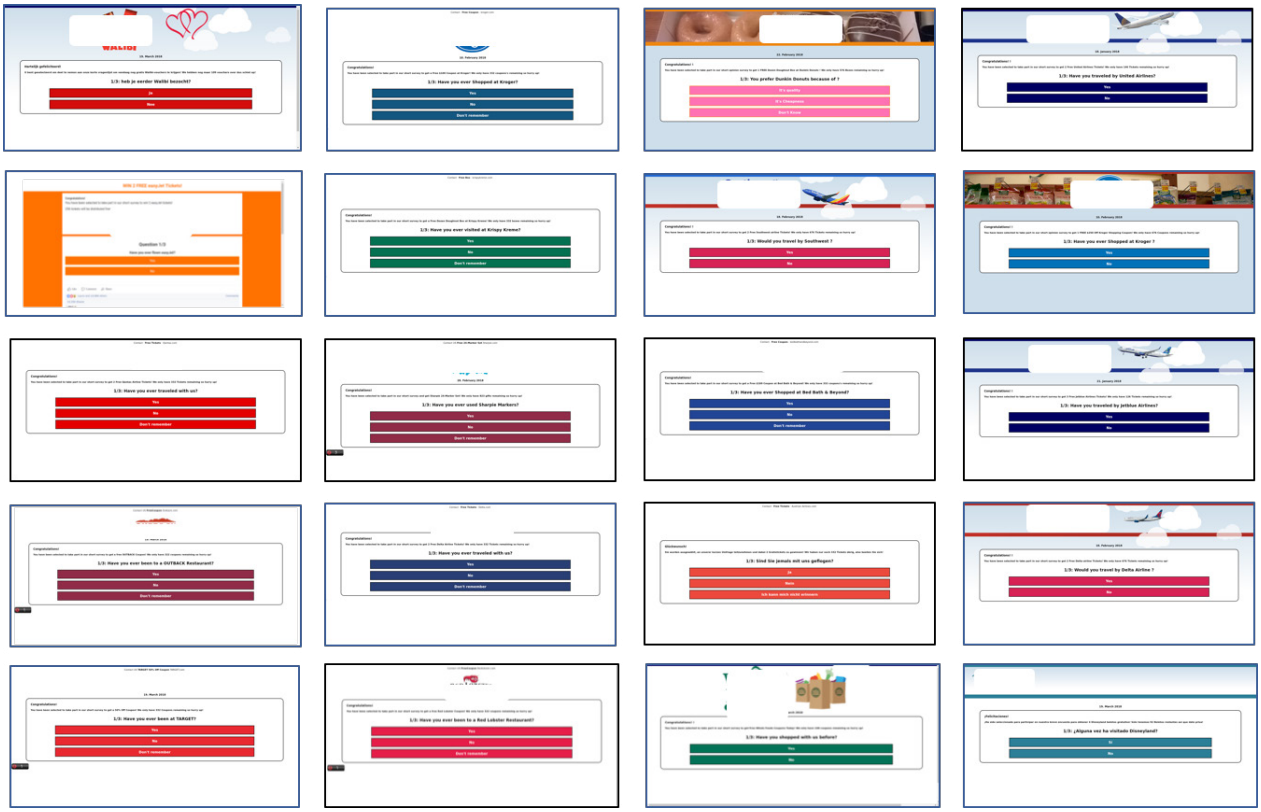

Figure 4: 20 different brands, three questions quiz, one toolkit

The campaigns abuse the reputation of a variety of brands, and although the campaigns appear similar, each was customized and contains different quiz questions in different languages. Many of the abused brands are airline companies, but retail, home decoration, amusement parks, fast food, restaurants, and coffeehouse chain brands are also commonly abused.

Figure 5: Nine different airline companies, nine different attack campaigns, same toolkit

We've seen "Three Questions Quiz" campaigns used many times over the past few years. The frequency of these campaigns is growing, and they are abusing new brands. Additionally, the integration of social networks into these phishing scams boosts the distribution of the attack, since many of the victims willingly share the quizzes with their friends.

For more technical details on the "three questions quiz," read "The Slippery Slope Starts with 'Get 2 Free Airline Tickets."

Win a Prize

The final nail in the coffin for a phishing victim occurs when they win a prize. At that point, all doubts — if some still exist — dissipate, and the victim willingly offers up all the required (and sensitive) information in order to be eligible to claim the prize.

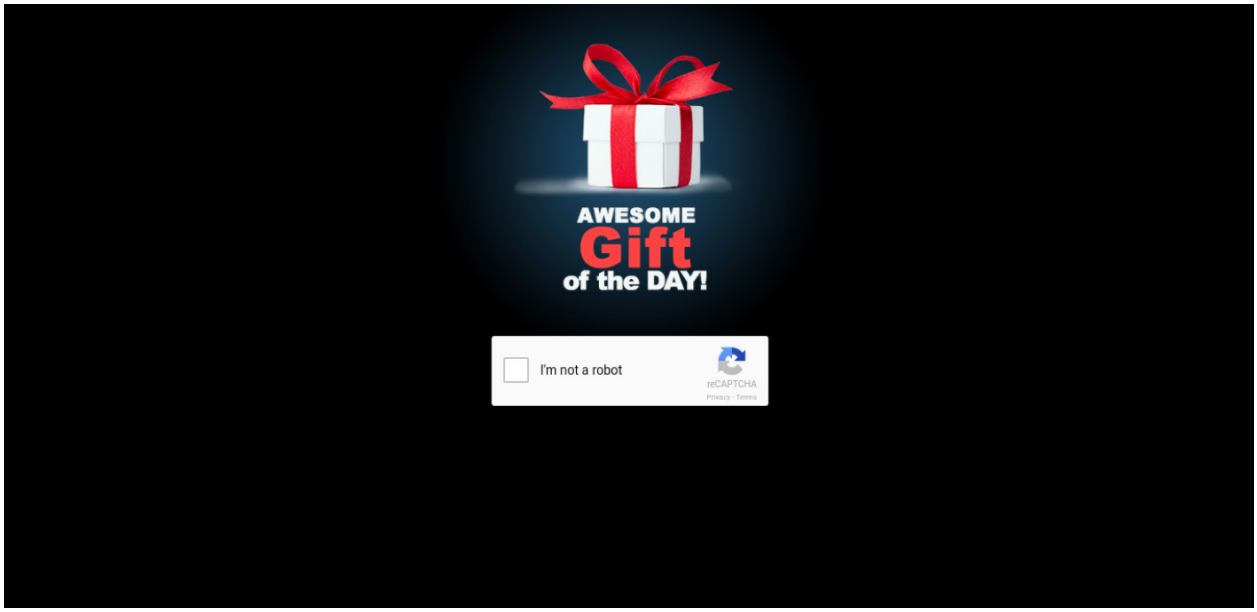

Figure 6: A typical "you just won a prize" phishing website page

Many phishing scams enhance the victim's experience by giving them an option to participate in a game in which the prize will be determined.

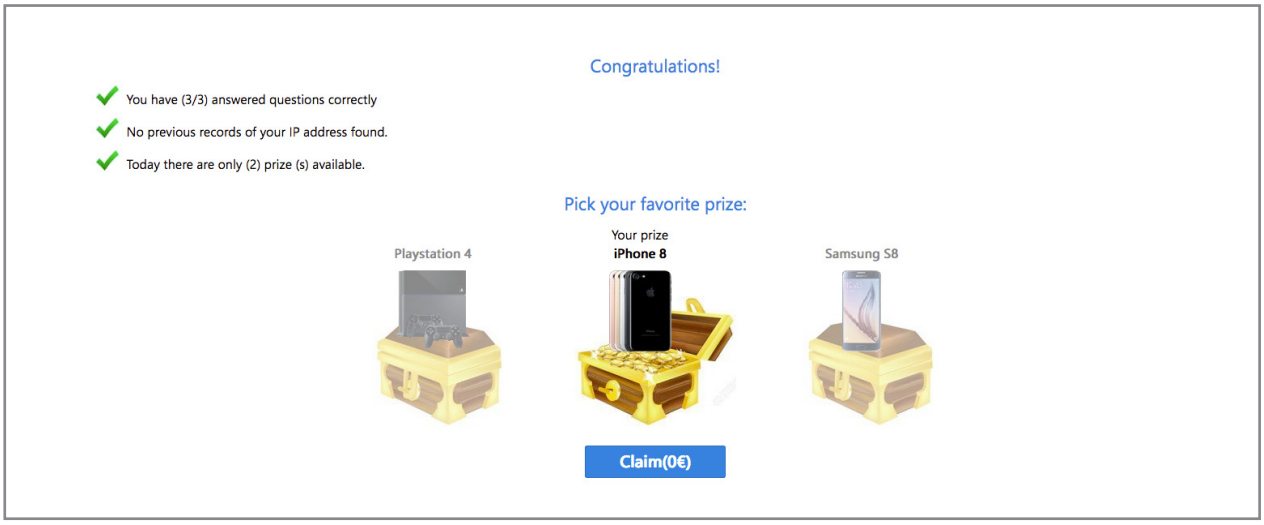

Figure 7: Winning an iPhone 8 phishing scam

As you can see in Figure 7, once a victim is eligible for a prize, the victim is asked to choose a treasure box. Regardless of his choice, the winner always wins. The prizes, in most cases, are related to the brand being abused (e.g., free airline tickets, a box of free donuts, shopping vouchers, or an iPhone 8).

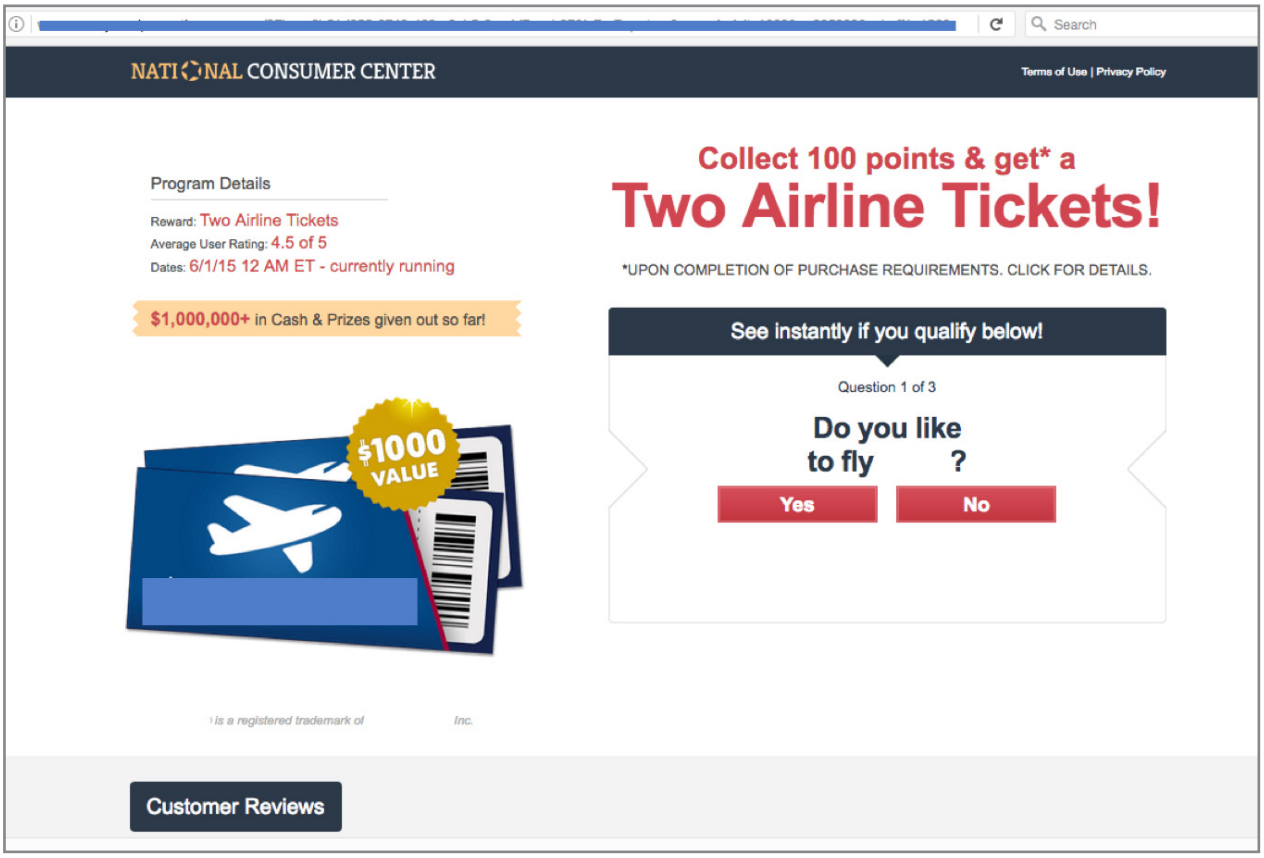

Figure 8: The famous "you've won two airline tickets" scam

Getting Social

Sharing is Caring

Another prevalent technique used in these recent campaigns includes the integration of social networks and instant messaging platforms into phishing websites. Social networks and instant messaging platforms help to amplify the distribution of the attack campaigns, enabling the threat actors to use new distribution channels and reach new victims. This augments the traditional channels of email, website spam, and adware.

A common practice in the flow of the phishing scam is to include a step where the victim, after "winning" a prize, is required to share a link to the phishing website across social networks.

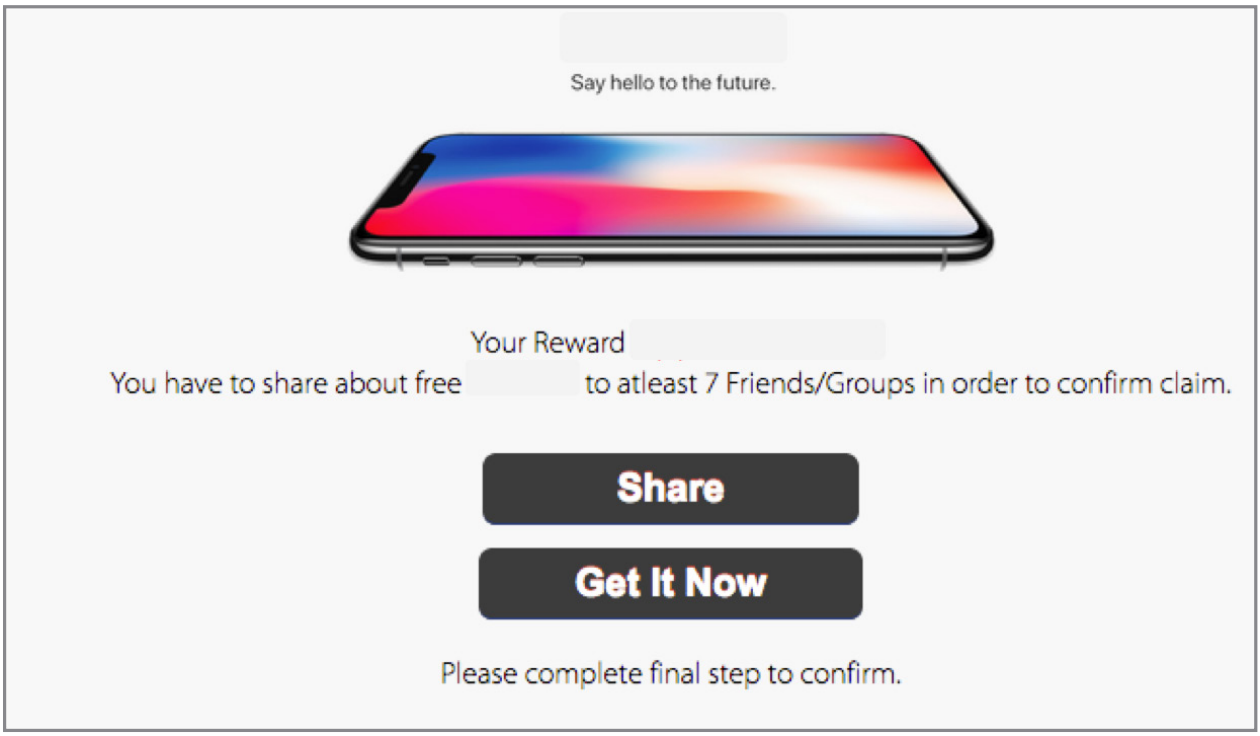

Figure 9: Phishing website indication of winning prize with sharing required

By tracking some of these campaigns, we were able to spot significant evidence of victims who decided to promote and share phishing scams through social networks and instant messaging platforms.

Sharing the phishing scam through social networks is a common way to amplify the campaign. Another approach to finding new victims uses instant messaging platforms, where the method of distribution is much more personal and reflects the nature of the instant messaging applications. Both social networks and instant messaging lead to phishing being distributed rapidly by users, with limited monitoring by security controls. This also limits mitigation capabilities, since these applications are mostly used on mobile devices.

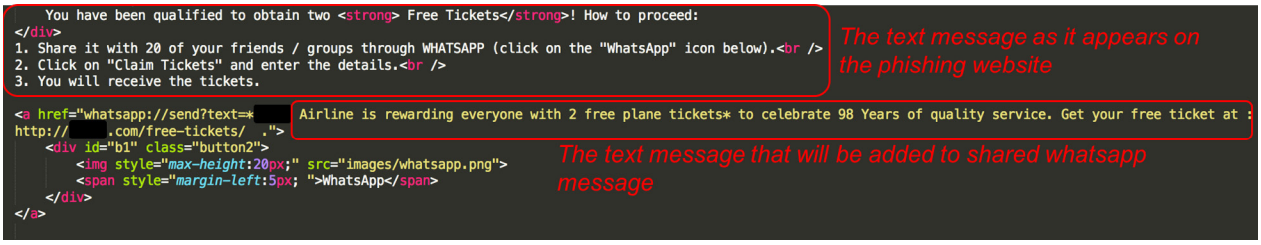

Figure 10: HTML code from phishing website "share it with 20 of your friends" condition for distributing campaign on WhatsApp

Figure 10 shows an example of a phishing website that includes a condition the user must fulfill before being able to claim the prize, which is sharing the phishing website with the victim's friends and groups.

Fake It with Fake Social Network Users

Fake users are another element being used by many of the phishing websites to strengthen trust in their victims. These users appear on the phishing website as an integrated plugin for social networks, but what the user is actually seeing is embedded JavaScript code on the phishing site presenting pre-generated accounts. In order to gain trust, those fake users are being used as a reference and evidence of "others" who have also won prizes on the phishing site.

Figure 11: Fake users that also "won" a prize

Throughout our research, we saw that the same fake users often appear in many different unrelated attack campaigns. This is not surprising, since it's the same toolkit that is used by all those attack campaigns.

Figure 12: Fake users across different phishing campaigns

As Figure 12 shows, "Bruno Pinho" and the rest of his co-fake users appear in different attack campaigns with nearly identical posts. The victim is meant to see them as other lucky users that, having won previous prizes, are thankful for winning two airline tickets, a box of donuts, or a free coupon for their favorite retailer.

The targeted brands have been obfuscated, but a closer examination of the text associated with each fake user shows that each campaign was customized with different messaging, making it appear more authentic.

There Is No Such Thing as Bad Publicity

Phishing campaigns that use social networks are highly effective, in terms of number of affected victims, when compared to more traditional phishing campaigns.

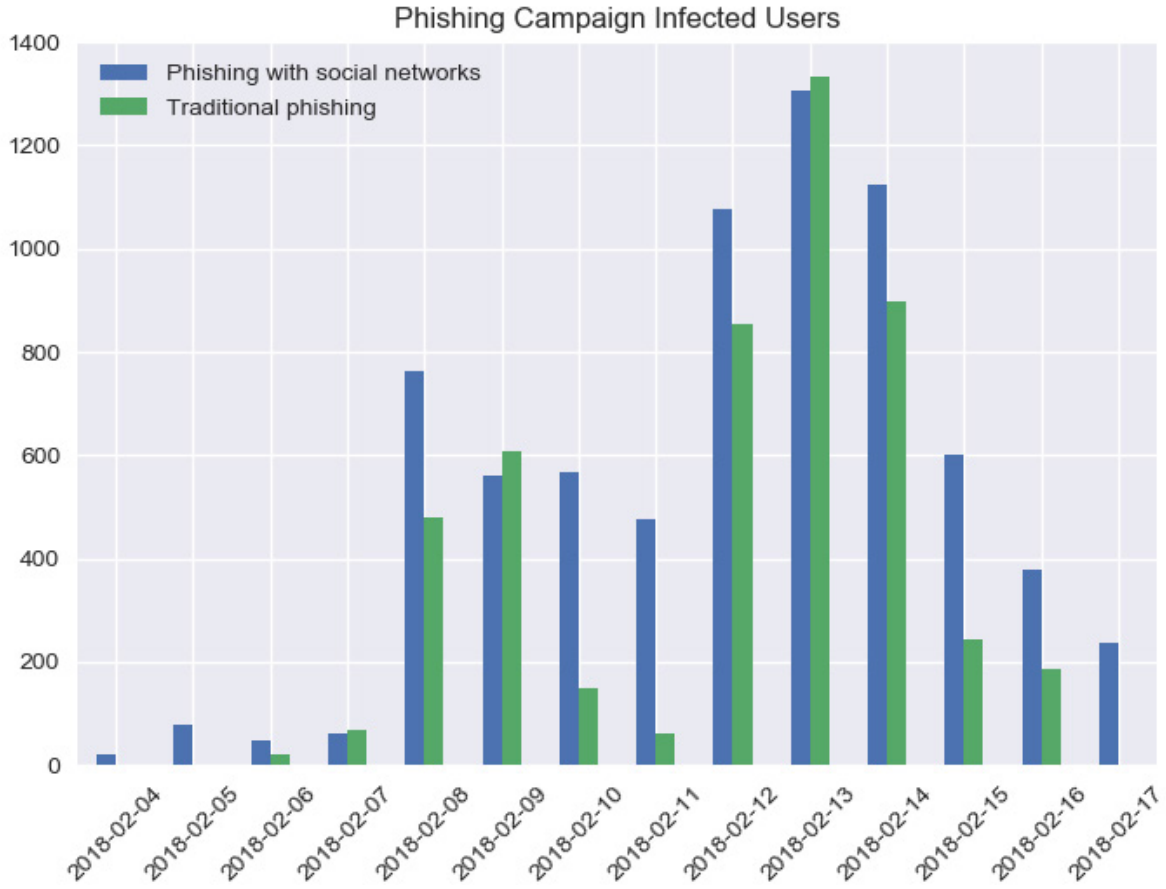

Figure 13: Phishing campaign being shared throughout social networks vs. the traditional campaign in terms of affected victims

Figure 13 shows a sample of Akamai's service provider DNS traffic that was inspected over a two-week period, comparing the number of affected victims per day for a phishing campaign that is using an obligatory step of sharing on social networks versus the traditional phishing campaign that is not using sharing techniques. We can see that campaigns using social media in their flow are more effective and long-lived, with a higher number of affected victims.

The information collected from some of the sharing messages on social media shows that many victims include good feedback and supportive messages about the abused brands. We believe that these messages, even if the result of malicious activity, are positive and support the abused brand. This also supports and strengthens the trust provided by the fake accounts created by the phishing tools.

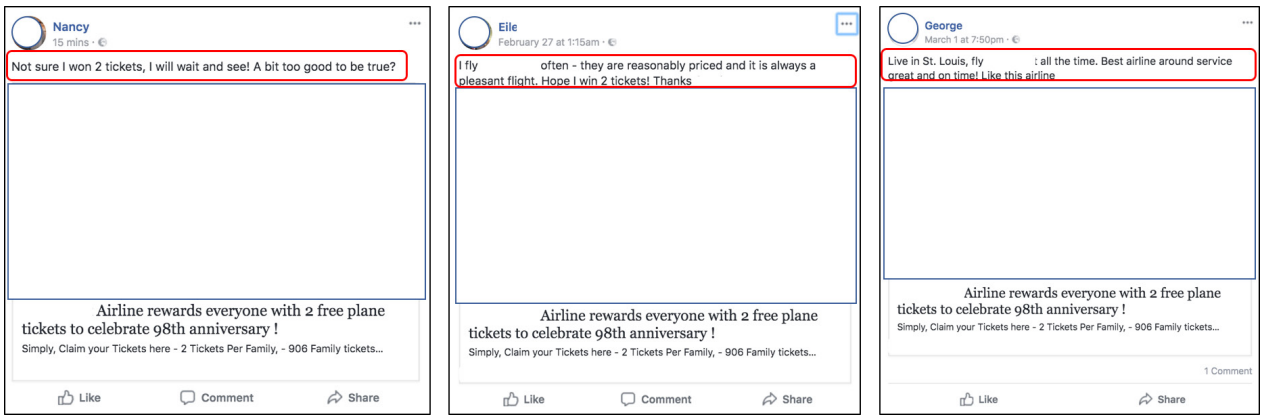

Figure 14: Phishing scam on social network sharing positive messages

Figure 14 shows three examples, with the feedback from the "get 2 free airline tickets" phishing scam victims. Messages such as: "I fly <abused airline> often—they are reasonably priced and it is always a pleasant flight" or "fly <abused airline> all the time." Best airline around service great and on time." Moreover, we were also able to see evidence that victims tend to be unconcerned even once they have realized that they were targeted by a phishing attack.

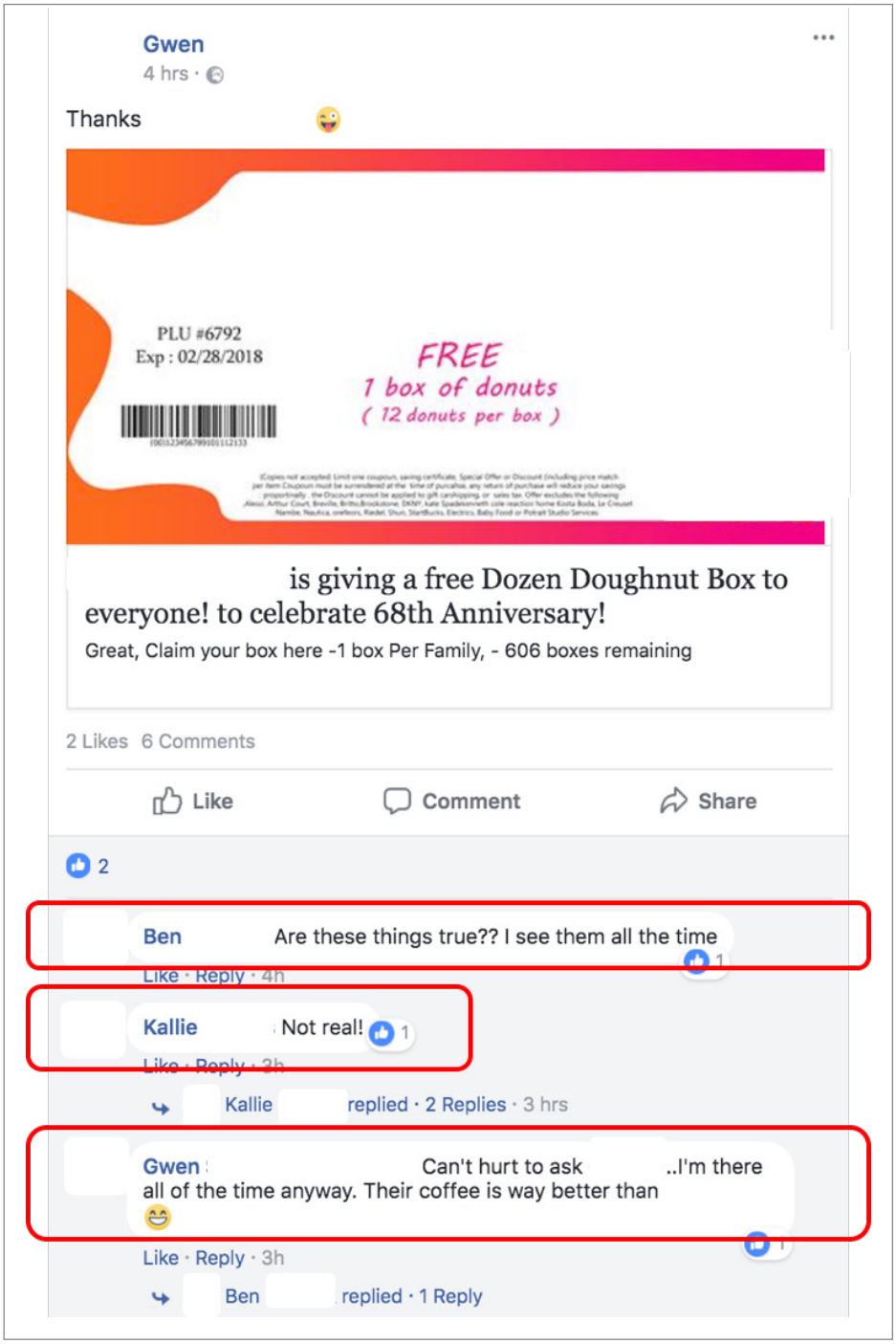

Figure 15: Social media discussion after a phishing website was shared

Figure 15 is a screenshot from a popular social media platform. We can see that even after getting feedback that the offer was "Not real!" and the user had not won a free box of donuts, the victim answered with:

"Can't hurt to ask <abused brand>... I'm there all of the time anyway. Their coffee is way better than <competitor brand>."

While it is not always the case, we were able to find many examples such as the one illustrated above in which the victims expressed no hard feelings or negative brand perception, even after they realized it was a scam and they hadn't won anything.

A key question that needs to be asked: Does this type of phishing actually lead to negative impact on the abused brands? Or is it possibly considered as a good impact to the abused brand? Perhaps the old adage of "There Is No Such Thing as Bad Publicity" holds true.

Summary

Security threats are constantly evolving, and wearing new shapes and colors to avoid detection. Phishing attacks are not new to the threat landscape, yet we can see this attack vector being continuously reinvented and reinvigorated by the distribution and amplification of campaigns through social channels.

One of the most surprising findings in our research is the huge amount of evidence that we collected about victims who shared phishing campaigns via their social networks. The level of tolerance, even once they understood they were potentially the victim of a scam, caught us by surprise. The victims often saw the risk eclipsed by the potential gain of a prize (even when it was a free donut).

The usage of new distribution channels, such as social networks and instant messaging applications, is a disturbing trend, as these applications are usually used on mobile devices. These devices are generally seen as the weakest link in an enterprise's security posture: roaming, going into and out of an enterprise's network, and rarely 100% controlled and monitored. More than that, users frequently fail to keep their devices updated with the latest security patches on their own.

We predict that mobile devices will continue to play a significant role in the future of attack vectors against enterprises, primarily because they are an easy entry point to the network. Social networks and instant messaging services will continue to be used as distribution channels. The potential of viral distribution channels that can spread campaigns in a matter of hours, or even minutes, is too much for attackers to ignore.

A key element in the ability to fight back against threats being delivered by mobile and roaming devices, and being distributed throughout social networks, is the ability to monitor all enterprise network devices' traffic in a cloud-based approach. Such an approach empowers the use of crowdsourcing techniques, where visibility to different unrelated traffic is transformed to new and unique insights in real time. In other words, by looking at the impact of campaigns across a number of enterprises, cloud-based protections can spot trends that a single enterprise might never see on its own.

The industry as a whole needs to continue to raise awareness for these lurking threats, and ensure that our peers, colleagues, friends, and families understand the risks and avoid sharing their sensitive information. After all, any offer that sounds too good to be true probably is.