Sunrise to Sunset: Analyzing the End-to-end Life Cycle and Effectiveness of Phishing Attacks at Scale

Written Report

Navoda Senavirathne

March 31, 2021

Background

Phishing is a type of social engineering attack often used to steal sensitive information where an attacker masquerading as a legitimate entity. The attackers in this case make use of numerous means to reach the potential victims (e.g., e-mails, social-media, instant messaging, text messages, telephone calls, search engine listing or spoofed mobile or cloud applications and QR codes). Despite the sophisticated anti-phishing ecosystem in place, phishing attacks continue to be successful in deceiving Internet users into exposing their sensitive information. This could result in both direct and collateral damages such as financial fraud, identity theft, harming the reputation of the involved organization or people, and working as a stepping stone to other cybercrimes.

Based on target victims, phishing attacks can be divided into two categories as *spearphishing* and *large scale phishing*. In *spearphishing* the attackers target specific high-value individuals or groups whereas in *large scale phishing* a broad range of potential victims is targeted. In this paper, the focus is given to *large scale phishing* attacks. In a typical phishing attack, victims are duped into a fraudulent website that impersonates a well-known brand with the aim of stealing their sensitive information. In the process of *large scale phishing* attacks, the first step is to configure a deceptive website that has the similar look and feel of a legitimate website. Once the phishing website is launched, the attacker distributes the link of the phishing website embedded in a convincing message (e.g., e-mail). Once the victim submits the required information on the fraudulent web page (in case of a successful attack), the attacker downloads and utilize them for a malicious purpose which could be financial or otherwise.

Due to the versatility and menacing nature of phishing attacks, a multitude of detection and mitigation technologies have been developed which has given rise to an anti-abuse ecosystem. This ecosystem comprises different techniques and methods belongs to multiple layers of defence such as spam filters, URL and content blacklisting, content removal, malware and vulnerability scanners, user awareness training etc. Among them, browser-based phishing detection works as the foremost mitigation strategy.

Phishing attacks have a low barrier to entry and are easy to scale. Moreover, the attackers can use a myriad of illicit services to deploy phishing websites while *phishing kits*, all-in-one packages with the necessary software to create a phishing website, are readily available. Further, such kits incorporate features to evade detection by automated anti-phishing systems. Therefore, attackers can launch a phishing attack with minimal effort. Thus, despite the sophisticated anti-phishing ecosystem phishing attacks still pose a significant threat to Internet users. In this paper [1], the authors identify the gaps in the existing anti-phishing ecosystem that leads to successful phishing attacks by passively analysing the victim traffic to phishing websites.

Contribution

The study carried out in the paper relies on two key observations that were noted by the authors in a preliminary study with respect to live phishing websites.

- Phishing websites often embed resources (e.g., images, fonts, or JavaScript) hosted on third-party domains, including domains that belong to the organizations being impersonated.
- Some phishing websites redirect the victim back to the organization's legitimate website after retrieving their information.

Based on the observations mentioned above, the authors argue that by using the right methodology it is possible to track the visitors' activity directly on certain phishing websites by, a) inspecting HTTP/HTTPS requests for the aforementioned embedded web resources within their own systems, and b) by identifying page referrals from suspicious sources. As explained by the authors, by using such a method both victim interactions with phishing websites and the visits from the attackers themselves at the testing phase of the phishing website can be identified. In other words, this can be used to proactively identify phishing threats. However, the main challenge in developing such a method based on the above criteria is the lack of access to web traffic data. To overcome this challenge the authors have collaborated with one of the most targeted financial services brands for phishing in order to develop a re-usable, passive framework named as the *Golden Hour*, to meaningfully analyze the victim traffic flow to live phishing pages. Specifically, it first analyzes web traffic data belongs to the selected organization to find the web events of interest. After filtering out the benign events, it matches the URLs of the remaining events with known phishing URLs obtained from trusted, external data sources. This enables the discovery of phishing attempts and further analysis of the selected web events enable them to determine the progression, characteristics and longevity of the successful phishing attacks. It is shown that by using the proposed method more than $1/3^{rd}$ of the phishing attacks targeting the particular organization can be identified.

Review

I think the significance of the paper can be attributed to the observations on the phishing web sites and the dataset that the authors have used to analyze the end to end life cycle of real world phishing attacks at scale. Thus, providing new insights to the organizations on how they can utilize their web traffic data in conjunction with external data sources to proactively detect phishing attacks and secure the victim accounts. Also, this method proposes a concrete approach to assess the impact of phishing attacks in monetization terms thus the organizations can isolate and identify which phishing attacks are the most successful and why? Further, they have discussed the limitations of their work thus providing the readers with a better understanding of any threats to the validity of their findings.

As mentioned above, the paper discusses the limitations of the proposed work in details. However, a discussion on the efficiency of the proposed framework in terms of analyzing the web traffic data would have provided the readers with a comprehensive picture of the computational cost involved in deploying this solution. Further, the frame-work is completely reliant on the quality of the external data sources that contain information about the phishing URLs. Even though the authors claim that the proposed framework can be used in general with respect to any organization, it seems somewhat unrealistic to expect that phishing URLs will get updated in the external data sources at the same rate for all organizations as similar to the large scale, global organization that they have used in this work.

References

1. Adam Oest, Penghui Zhang, Brad Wardman, Eric Nunes, Jakub Burgis, Ali Zand, Kurt Thomas, Adam Doupé, and Gail-Joon Ahn. Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale. In *29th {USENIX} Security Symposium ({USENIX} Security 20)*, pages 361–377, 2020.