Legitimate SaaS Platforms Being Used to Host Phishing Attacks

unit42.paloaltonetworks.com/platform-abuse-phishing/

Lucas Hu August 23, 2022

By Lucas Hu

August 23, 2022 at 6:00 AM

Category: Malware

Tags: credential theft, Phishing, SaaS

This post is also available in: 日本語 (Japanese)

Executive Summary

Instead of creating phishing pages from scratch, more and more cybercriminals are now abusing legitimate software-as-a-service (SaaS) platforms, including various website builders or form builders, to host their phishing pages. Since these URLs are hosted on legitimate domains, they can be especially difficult for many phishing detection engines to detect. Furthermore, these platforms typically require little to no coding experience, significantly lowering the barrier to entry for creating and launching phishing attacks.

From the beginning of 2020 to June 2022, Palo Alto Networks analyzed the URLs detected by our Advanced URL Filtering service, and discovered that the number of phishing URLs hosted on legitimate SaaS platforms has continued to increase at an alarming rate. In fact,

from June 2021-June 2022, the rate of newly detected phishing URLs hosted on legitimate SaaS platforms has increased over 1100%.

The Palo Alto Networks Advanced URL Filtering uses deep learning to analyze the content of each webpage at the URL level instead of the domain level. Customers with an Advanced URL Filtering subscription therefore receive protections from these platform-abuse phishing attacks.

Related Unit 42 Topics Phishing, Credential Theft

Table of Contents

Introduction to Platform-Abuse Phishing Attacks

Today, more organizations are adopting existing SaaS tools for tasks like handling file storage, building websites, and more importantly, enabling collaboration within and outside of the organization. For example, many website builders allow users to easily create websites without having to write any code themselves, and form builders allow users to easily create and share surveys, registration forms, etc. Recently, we've seen that cybercriminals have begun to abuse these SaaS platforms for their own nefarious uses. In early 2022, we noticed an uptick in phishing URLs hosted on legitimate SaaS platforms, and we decided to further investigate this trend.

Methodology

First, we gathered a list of various SaaS platforms that could potentially be used to host phishing attacks. We then looked at the phishing URLs discovered by The Palo Alto Networks Advanced URL Filtering service from January 2020-June 2022 and used signature-based pattern matching to determine which phishing URLs were hosted on each SaaS platform.

Examples of the types of SaaS platforms we studied are shown in Table 1.

Platform Type	Description
File Sharing	Sites for hosting and/or sharing files

Form Builders	Sites for creating forms, surveys, etc.
Website Builders	Popular website builders, typically requiring no coding experience
Note Taking/Collaboration	Sites for taking notes, writing documentation, creating internal dashboards, etc. Various productivity tools.
Design/Prototyping	Sites for designing/prototyping wireframes, infographics, mockups, etc.
Personal Branding	Sites for hosting social media links, personal portfolios, etc.

Table 1. Breakdown of types ofSaaS platforms studied in this research.

Results: Platform-Abuse Phishing Is on the Rise

In Figures 1 and 2 respectively, we show the number of newly discovered phishing URLs hosted on legitimate SaaS platforms per week, as well as the percentage of all newly discovered phishing URLs that we found being hosted on legitimate SaaS platforms. We can see that the prevalence of platform-abuse phishing URLs has increased significantly from 2020, both in terms of raw numbers and percentage. Although there was a slight dip during the 2021-22 holiday season, starting in February 2022, the trend began to surge once again.

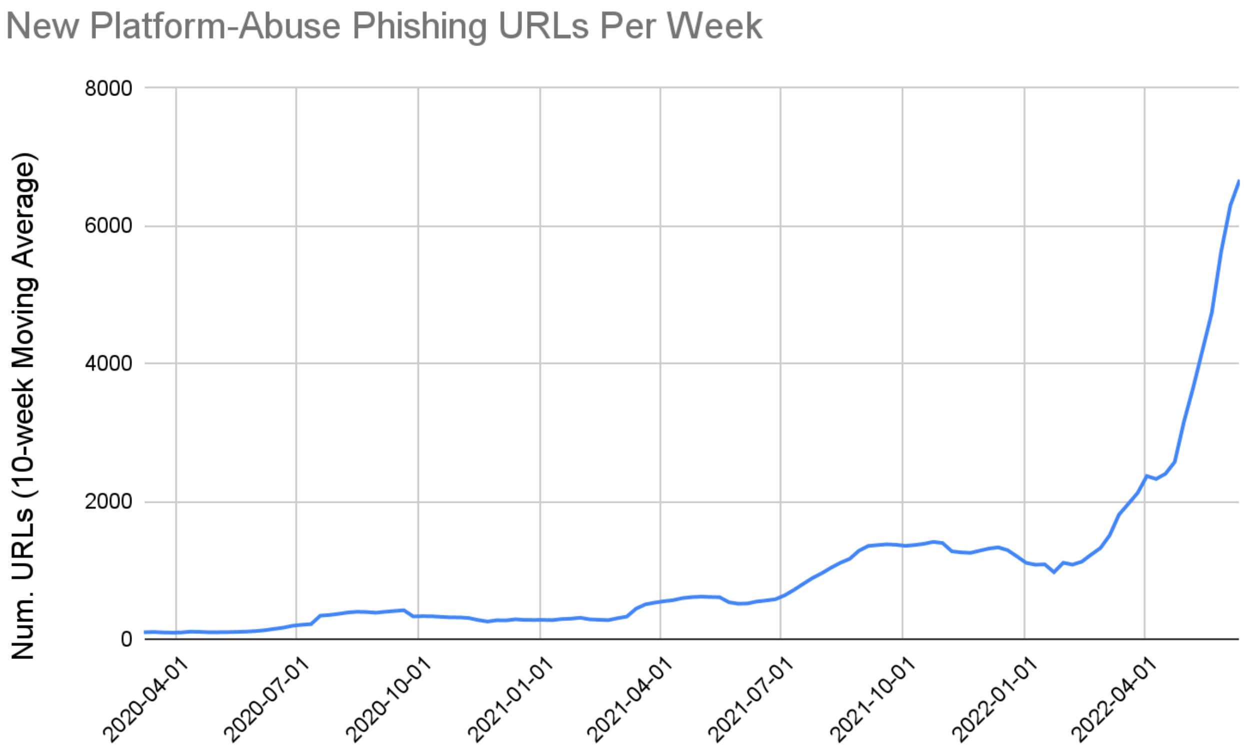


Figure 1. Newly created phishing URLs hosted on legitimate SaaS platforms per week.

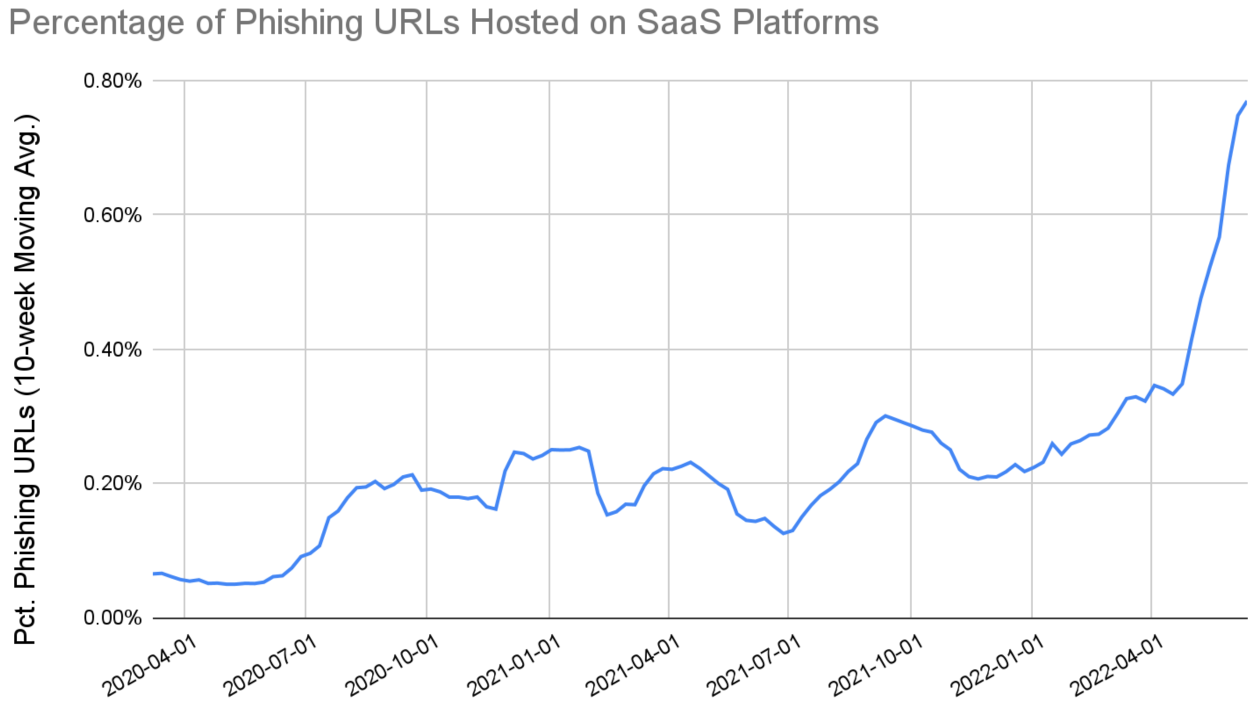


Figure 2. Percentage of newly discovered phishing URLs hosted on legitimate SaaS platforms.

Next, we separately analyzed the trends in each SaaS platform subcategory and normalized each subcategory's “platform abuse” rate to a prevalence value between 0 and 1. A value of 1 represents the week in which that platform type saw the largest number of new phishing URLs.

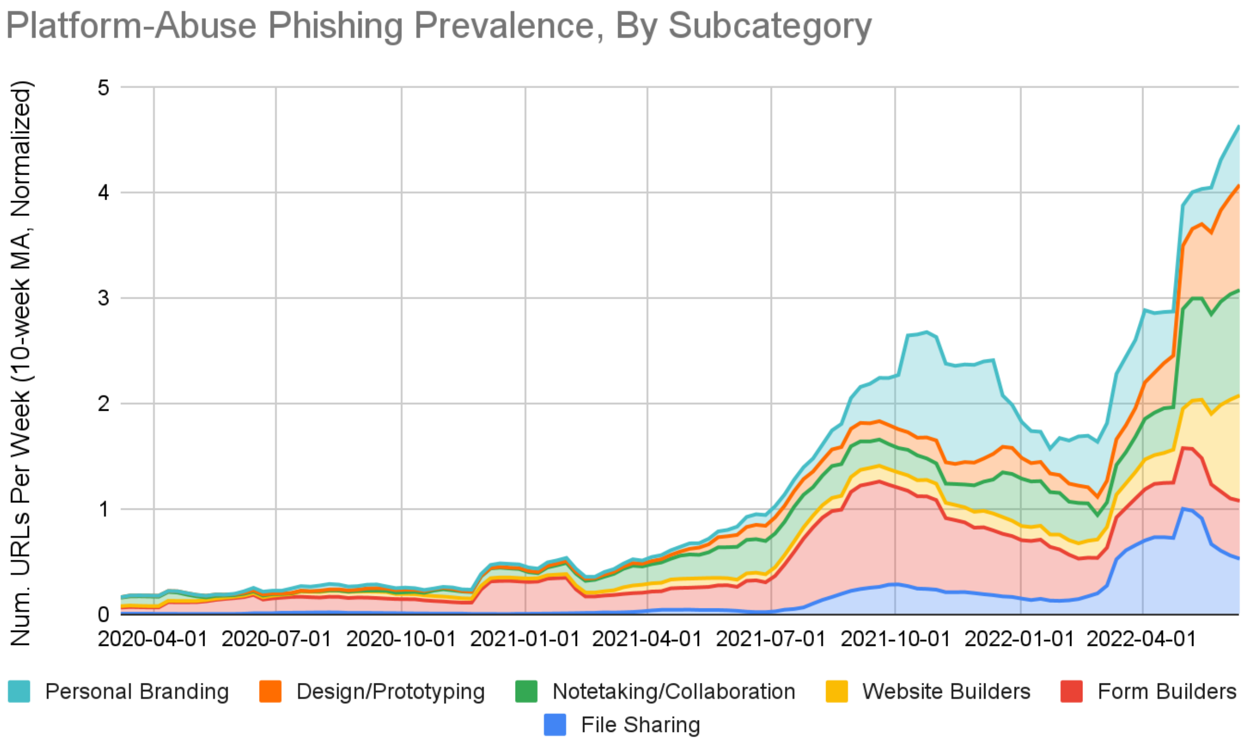


Figure 3. Phishing prevalence within each SaaS platform subcategory, normalized. Generally speaking, each type of SaaS platform saw an increase in phishing activity in the latter half of 2021, with the most noticeable increases occurring between September-October 2021. More recently, we observed a larger increase beginning in February 2022. With new SaaS platforms continuing to rise in popularity, it is likely that this trend will continue into the future, making it absolutely critical that URL Filtering products are equipped with the right capabilities to detect these types of phishing URLs.

Platform-Abuse Phishing Case Studies

We have highlighted a variety of case studies to demonstrate the types of tactics these platform-abuse phishing URLs employ.

In Figure 4, we see a file-sharing URL that shows a preview of a document related to a remittance payment. However, upon clicking the “View Now” button, the user is taken to a credential-stealing page built using a popular website builder, which prompts the user to enter their login credentials to view a sensitive document.

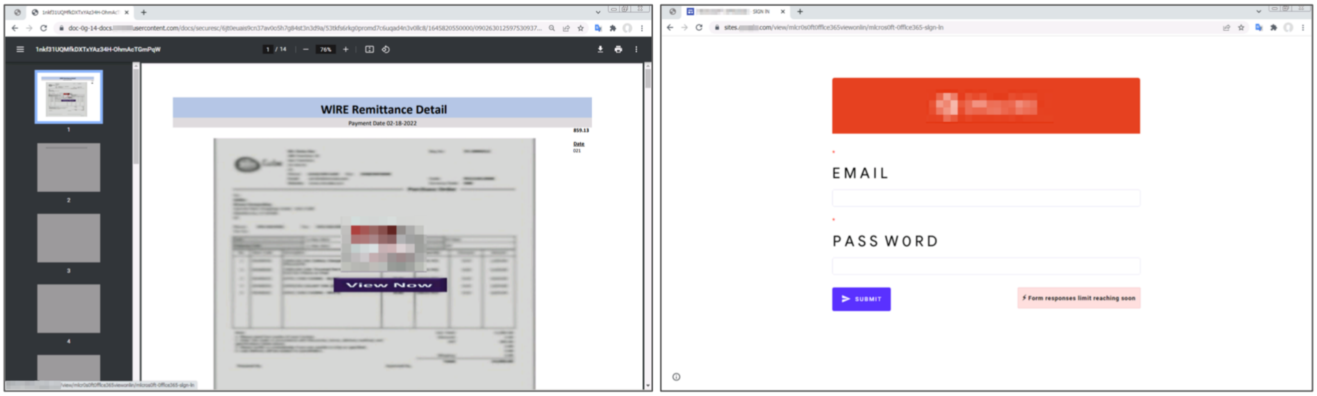


Figure 4. Left: Landing page for a phishing attack, hosted on a file-sharing site. Sent in an email with the subject line: “Re: [REDACTED COMPANY NAME] Wire.” Right: Credential-stealing page built using a popular website builder, linked to by the page on the left.In Figure 5, we see an example of a credential-stealing page hosted on a site built by a legitimate form builder. On the page where the user is prompted to enter a password, the attacker has embedded a logo, imitating a reputable brand in order to make the page appear like a legitimate login portal. Since the password prompt only appears after some user interaction (entering the email address on the first page), this phishing page may be more difficult for automated crawler-based detection engines to detect.

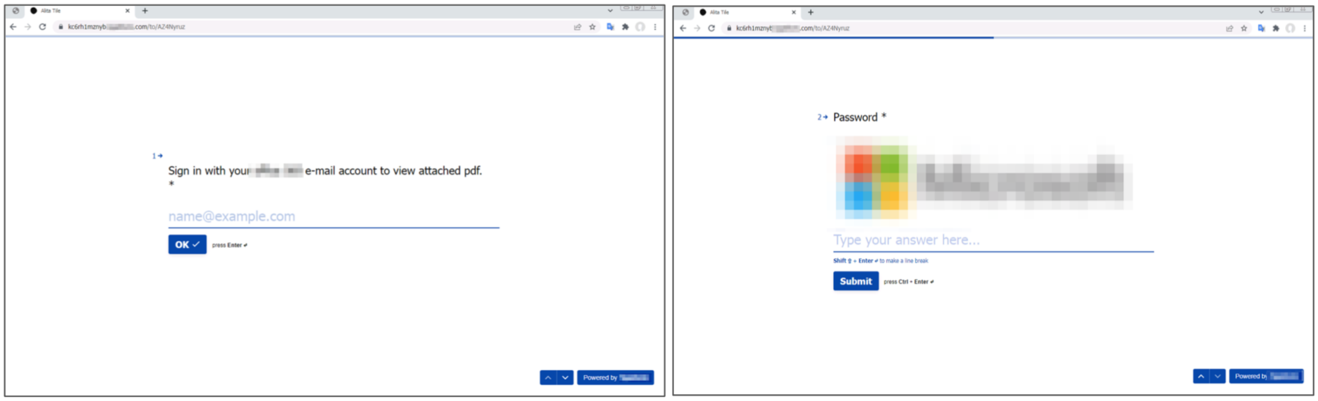
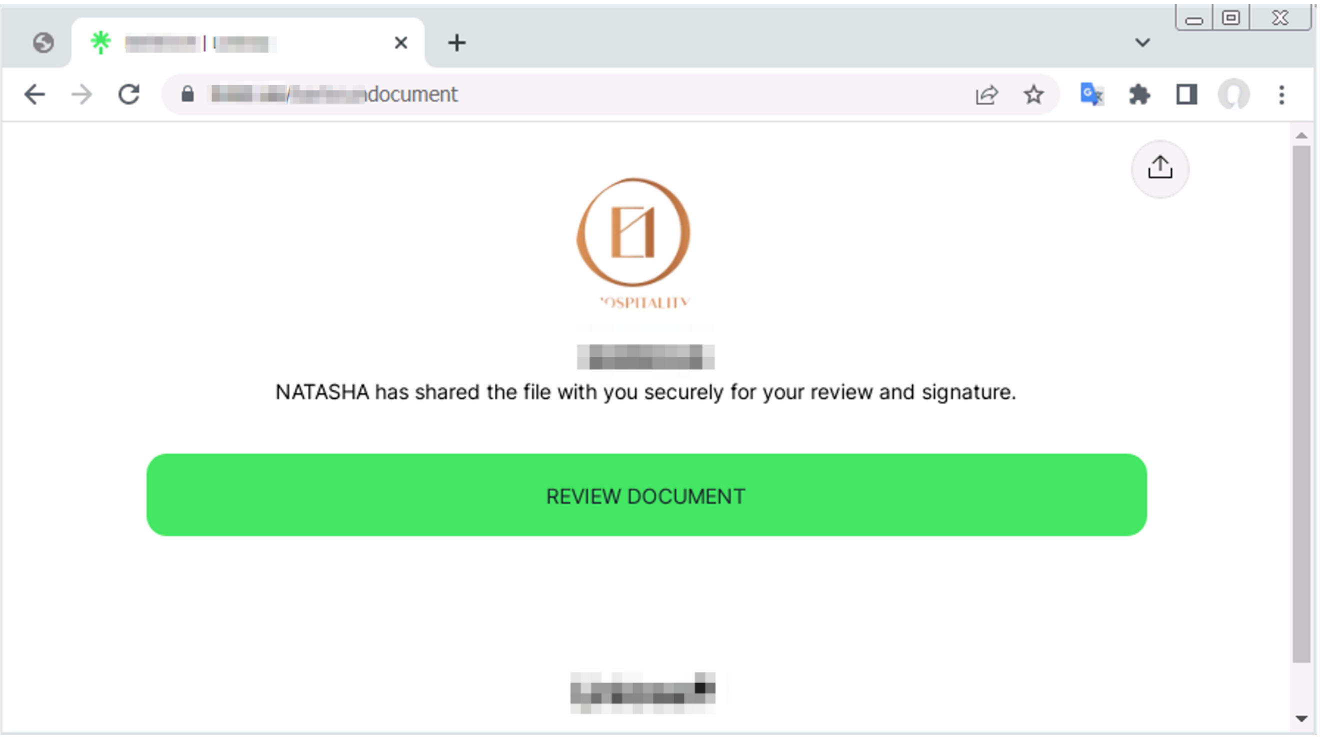

1→ Sign in with your [redacted] e-mail account to view attached pdf. *

Figure 5. Credential-stealing page built using a popular form builder. Sent in an email with the subject line: “Invoice 071158.”

Furthermore, we noticed several examples of landing pages that don’t host the credential-stealing forms themselves, but rather contain urgent-sounding language that prompts the user to click on a link or button, which then leads to a different credential-stealing page. Using landing pages in phishing campaigns may increase the number of clicks necessary to arrive at the credential-stealing page, but the practice has an important benefit: In the event that the final credential-stealing page is taken down, the attacker can simply change the link and point to a new credential-stealing page, preserving the effectiveness of the original campaign.

Link-hosting sites are an example of a type of SaaS platform that attackers can abuse to host such landing pages for phishing attacks. These platforms allow users to host links to their various social media accounts on a single page, giving them the ability to consolidate their online presence.

As one such link-hosting platform started to gain more popularity in 2021, we observed more and more landing pages for phishing attacks being hosted on the platform. (This trend can be seen in Figure 3 by observing the increase in phishing URLs hosted on “Personal Branding” platforms starting in the latter half of 2021.) An example of such a landing page is shown in Figure 6.



[redacted]

[redacted]document

'OSPITALITY

[redacted]

NATASHA has shared the file with you securely for your review and signature.

[redacted]

Figure 6. Landing page for a phishing attack created using a popular link-hosting platform, discovered on Nov. 29, 2021.

An article published by Cofense suggests that these more niche platforms may be less effective at finding hosted threats, especially compared to sites and tools from popular cloud vendors. By utilizing these niche platforms, attackers may be able to put up phishing pages that stay live for a longer period of time.

This suggests that attackers may try to take advantage of relatively new and less “obvious” platforms when deciding which platforms to use for their phishing attacks. In doing so, attackers may be attempting to take advantage of the likelihood that these platforms do not have as many resources dedicated to abuse prevention as the more established and general-purpose SaaS platforms do.

Conclusion

As seen in the case studies shown above, just because a URL is hosted on a seemingly legitimate domain or platform, doesn’t mean that the URL itself is trustworthy. More phishing URLs are being hosted on legitimate SaaS platforms, making these phishing pages both easier for attackers to create and harder for phishing detection engines to detect.

Since the Palo Alto Networks Advanced URL Filtering service analyzes web content on a URL level (using machine-learning models that study the actual content of the page), Palo Alto Networks customers who subscribe to Advanced URL Filtering receive protections from these types of phishing attacks, as well as from other web-based threats.

For end users, it is crucial to take caution when inputting one's credentials into any online type of platform. Furthermore, users should be wary of any suspicious emails that use time-sensitive language to prompt a user to take some sort of urgent action.

When in doubt, users should manually navigate to the relevant login page directly in their browser (for example, by typing login.microsoftonline.com in the navigation bar), instead of clicking any links contained in a potentially deceptive email.

Acknowledgements

The author would like to thank Seokkyung Chung, Ziqi Dong, Wei Wang, Jun Javier Wang, Claud Xiao, Billy Melicher and Ashraf Aziz for helping gather the data sources used in this report, for curating the list of SaaS platforms and for setting the direction of this research report.