WING.security

The 2023 State of SaaS

Navigating Through the Risks

Table of Contents

Executive Summary

Last August, the cloud service provider DigitalOcean announced that their Mailchimp email marketing account had been compromised, and as a result, a very small number of its customers had experienced attempts to compromise their accounts by password resets. In addition, DigitalOcean halted from working with Mailchimp and migrated all their email services away from Mailchimp.

This example demonstrates the importance of diving into the threat landscape of software-as-a-service (SaaS) when addressing SaaS security. First, as users of SaaS services on a daily basis, we are all vulnerable to threats on these platforms. Second, even if we do our best to keep the best security practices, we might still be influenced by cyber attacks that target our SaaS providers, since our data and permissions might be exposed or leaked during those attacks, exactly as DigitalOcean experienced in the breach of Mailchimp, among other companies.

The popularity of SaaS platforms has been skyrocketing in recent years, but this rapid growth has also led to a corresponding increase in emerging cyber threats targeting these platforms. However, along with this rapid growth comes a corresponding rise in emerging cyber threats targeting these platforms, and new attack methods have been evolving.

We are delighted to present Wing Security's first annual report, where we will take a closer look at the tactics, techniques, and procedures (TTPs) used by cyber threat actors to attack SaaS platforms in 2022. We have observed last year an increase in cyber attacks that involve SaaS platforms, specifically in Identity and Access Management (IAM) platforms such as Okta, Microsoft 365, OneLogin, etc. The report covers relevant attack techniques for SaaS such as MFA fatigue and OAuth token abuse, among others. In addition, we will provide an overview of the extent of usage of SaaS as we have seen in 2022 among our customers, offer our 2023 predictions and highlight our "golden tips" to address SaaS security.

THE YEAR THAT WAS:

Top Trends in SaaS Attacks in 2022

1. Stolen Credentials

As the popularity of SaaS continues to grow, so does the willingness of threat actors to gain access to SaaS accounts, particularly for Identity and Access Management (IAM) platforms such as Okta, Microsoft 365, and OneLogin. This is because gaining access to one central service can potentially give access to multiple sources of data, some of which may be confidential.

There are various methods for stealing or using stolen credentials, but in the cases seen in 2022, phishing and obtaining leaked or purchased credentials from the darknet were among the most common techniques. According to Auth0 by Okta, in the first quarter of 2022, 34% of all login attempts were made by credential stuffing, a technique that leverages credentials that were already leaked in the darknet.

0ktapus Campaign

The 0ktapus campaign lasted a few months and targeted employees of technology companies that use Okta. The threat actor successfully compromised nearly 10,000 accounts and over 5,000 MFA codes in more than 130 organizations, including Twilio, Evernote, Klaviyo, Cloudflare, Slack, AT&T, Microsoft, HubSpot.

The threat actor sent SMS messages to employees of the targeted companies, containing a custom link to a phishing site that appeared to be the Okta login page of their company. Once the victim entered their credentials and MFA codes, the information was automatically sent to the threat actor via a Telegram bot, allowing them to log into the victims' accounts.

August 2022

Uber's Breach

The notorious cybercrime group known as Lapsu$ successfully gained access to Uber's network and data through various SaaS applications, including Slack, Google Admin Console, AWS, SentinelOne, and Duo.

The group initially gained access by logging into an external employee account on OneLogin using credentials that were purchased on the darknet. Once they had access, the group then initiated a MFA fatigue attack on the victim and successfully bypassed the MFA obstacle.

September 2022

Circle-CI Phishing Campaign

An unknown actor executed a phishing campaign targeting GitHub users, with a goal to extract victims' credentials and their MFA codes for their GitHub accounts. The threat actor impersonated the CI/CD platform Circle-CI, and sent the victims emails with an alert that urged them to deliver their credentials on a phishing site.

According to GitHub, many organizations were infected in this campaign, including Dropbox, in which 130 of its GitHub private code repositories were stolen.

September 2022

2. MFA Fatigue

Multi-Factor Authentication (MFA), the mechanism that requires users to provide at least two forms of identification to log in, is facing increasing attacks in various creative ways. As the use of MFA as a security measure grows, so do the attempts by threat actors to bypass it. Auth0 by Okta reported that in the first 90 days of 2022, it observed nearly 113 million attacks against MFA.

The leading technique in 2022 was MFA fatigue, where the threat actor floods the victim with multiple push verification requests until the victim, accidentally or not, approves the threat actor's access in order to stop the notifications, only to find out later that the threat actor has entered their account. An increase in MFA fatigue attacks was recorded during 2022. For example, Microsoft reported that there were more than 30,000 MFA fatigue attacks per month on Azure AD alone. However, it's not only the numbers themselves that are interesting, but also the trend of these numbers, which is on the rise.

Cisco

A threat actor affiliated with the cybercrime group Lapsu$ gained access to Cisco's network by compromising a Cisco employee's personal Google account, and extracting Cisco's VPN credentials that were synced with the employee's Google account through Chrome's stored passwords. Once the threat actor obtained the credentials, they attempted to bypass the MFA challenge using various techniques.

In this case, like many others, the MFA fatigue was accompanied by voice phishing, where the threat actor called the victim and engaged in a conversation to manipulate the victim into cooperating. Once the threat actors bypassed the MFA, they enrolled new devices for the MFA mechanism and successfully connected to Cisco's VPN. From there, the actors executed tactics to maintain and expand their access to the network.

CISCO

May 2022

Uber Breach

According to Uber, Lapsu$ successfully gained access to Uber's network by buying corporate credentials of one of Uber's external employees in the darknet.

After that, the actor initiated a MFA fatigue attack on the victim, accompanied with Whatsapp messages, impersonating Uber's IT personnel, convincing the employee to approve the MFA push notification request, which resulted in Lapsu$ successfully bypassing the MFA challenge.

Uber

September 2022

3. OAuth Tokens Theft and Abuse

As awareness of the importance of using strong and unique credentials, as well as MFA, increases, threat actors are finding creative ways to bypass these obstacles. Therefore, the trend of using tokens, particularly OAuth tokens, illegally to gain access to data is on the rise. OAuth is a standard protocol for authorization and is commonly used in SaaS platforms, where users allow applications to access their data in other applications. From a threat actor's perspective, using such a token saves the effort of obtaining credentials and MFA information, as the token includes the authorization and permissions needed for the desired access by default. In the past year, we have seen various methods used to achieve this goal, such as stealing OAuth tokens from third-parties, OAuth phishing consent, using old tokens, and Man-in-the-Middle phishing attacks, among others.

Microsoft 365 OAuth Phishing Consent Campaign

In the beginning of 2022, hundreds of organizations were targeted in a wide OAuth phishing attack, in which the victims received emails encouraging them to grant read and write permissions for their Microsoft 365 accounts to a new OAuth application, created and controlled by the threat actor.

In this method, the victim single-handedly issues the access token for the threat actor.

January 2022

GitHub

GitHub disclosed that an unknown threat actor authenticated to GitHub's API by using stolen OAuth tokens that were issued by GitHub users to third-party integrators, Heroku and Travis-CI.

This was done in order to extract data from private repositories from dozens of organizations that use GitHub, including npm. In some cases the actor managed to extract the victim's code repository as well as API keys, such as for AWS.

April 2022

Azure Active Directory Powershell and Exchange Online 365

Microsoft disclosed an attack where an unknown, financially motivated threat actor compromised cloud tenants with high permissions that didn't use MFA, by using a method called credential stuffing.

Once the threat actor gained access to the compromised tenant, they deployed malicious OAuth applications that added an inbound connector to the Exchange Online settings. This allowed the threat actor to make future spam campaigns appear as if they were originating from the organizational domain.

September 2022

4. Malicious Web Extensions

Web extensions for browsers and application add-ins are popular among users, as they enhance the user experience, allow for personal customization, and provide additional functionality. The trend of using malicious web extensions by threat actors is not new, but it is still relevant. In a special report on the phenomenon of malicious web extensions published in August, Kaspersky reported that in the first half of 2022 alone, the number of victims of malicious web extensions reached over 3 million, which is 70% of the total number of victims in all of 2021. Additionally, there were several high-profile reports of malicious web extensions with millions of infected users in the second half of 2022.

The cyber security company **Volexity** revealed that the North Korean Advanced Persistent Threat (APT) cyber actor, known as Kimsuky, used a malicious web extension to exfiltrate Gmail and AOL email data from victims. It's worth noting that in this campaign, the actor used the malicious extension as a post-exploitation tool, rather than as an initial access tactic, which is more commonly seen in attacks involving malicious web extensions.

July 2022

McAfee disclosed five malicious web extensions that were downloaded by more than 1.4 million users. The extensions purported to be benign, offering users the ability to watch Netflix together, take screenshots, and access website coupons. However, they all had the same function, which was to track users' browsing history and enable the threat actor to modify cookies on eCommerce sites, allowing the actor to receive affiliate payments for the items the user purchased.

August 2022

Guardio Labs discovered a malvertising campaign that involved 30 different malicious web extensions for Google Chrome and Microsoft Edge, which were downloaded by over a million users. The extensions offered color customization but actually hijacked users' searches and redirected them to the website they intended to visit, but with a customized URL that provided the actor with commission benefits.

October 2022

5. SaaS As Malicious Infrastructure

As the popularity of SaaS grows, threat actors, both state-sponsored and non-state-sponsored, have been using SaaS platforms as an infrastructure for their attacks to disguise their malicious activities. This trend is on the rise and includes traditional phishing campaigns and command and control for malware. Utilizing SaaS as infrastructure for cyber attacks gives threat actors two main advantages.

Firstly, it allows them to blend their activities in with normal network traffic as legitimate SaaS communication, thus minimizing the risk of detection. Secondly, they can use the credibility of the SaaS platforms they impersonate in their attacks, which increases the likelihood that the victim will unknowingly cooperate with the threat actor.

GitHub

The North Korean APT group Lazarus used GitHub as a command and control (C2) infrastructure as part of a phishing campaign, in which they sent victims emails with documents, allegedly job offers from Lockheed Martin, with embedded malicious macros in the Word documents.

This was disclosed by the cybersecurity company Malwarebytes.

January 2022

Microsoft Teams

An unknown actor executed a campaign of spreading malwares through Microsoft Teams, targeting local media outlets in the Great Lakes region, as discovered by Avanan. Once inside, the actor attached a malicious malware, “User Centric”, to a chat thread to increase the likelihood that victims would open it.

Researchers believe that the access to Teams was via stealing credentials by phishing or compromising one of the target’s partners.

February 2022

Trello, Google Drive and Dropbox

The cybersecurity company Mandiant, revealed in April that the Russian APT29 cyber group operated a spear phishing campaign targeting diplomatic organizations in Europe, Americas and Asia, while using Trello, as a C2 to communicate with their malware.

In another campaign during the spring of 2022 and disclosed by Palo-Alto, APT29 leveraged Google Drive and Dropbox as C2.

Spring 2022

THE STATE OF SAAS:

2022 in Numbers

1. SaaS Applications

The average organization had

07

new apps in its environment each month

13%

increase in SaaS applications during 2022

The average user had

28

SaaS Applications

07

Web Extensions

SaaS applications most prominent risks

13%

of the applications found in organizations have high permissions

Categories that usually require high permissions: Communication, Email, CRM

88%

of the organizations using Wing Security had applications with unused high permissions

89

of applications have unused high permissions, in an average organization over the course of one year

TOP APPLICATION CATEGORIES

1 Analytics

2 E-commerce

3 Collaboration

4 Developer Tools

5 Productivity Tools

2. SaaS Users

28%

of users in an average organization are external and don't belong to the organization's domain but to vendors, sub-contractors, customers, etc

60%

of organizations have external users on Slack

45%

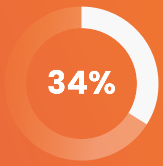
of organizations have external users with high permissions

3. Exposed Data

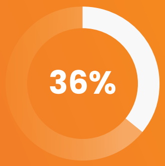
The average organization had

150K

files shared externally with collaborators from outside the organization



In organizations that use Slack, over 34% of files are shared in Slack, despite it not being a file-management

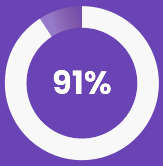


of files were externally shared for over a year

Exposed data potential risks

50K

In the average organization, almost 50K of files shared in 2022 were shared to "anyone with a link", meaning anyone who has access to the file's link could see, edit and download its content



of organizations had sensitive files shared externally or on a public Slack channel

WING SECURITY'S PREDICTIONS:

A Forecast For 2023 Security Trends

As the use of SaaS applications and their connectivity increases, so do the TTPs.
As 2023 begins, we have identified the top 5 trends that we expect to see in the upcoming year:

01 **Threat actors will likely focus on targeting identity applications (IAMs and IDMs)** as they offer a valuable target for hackers seeking to gain unauthorized access to sensitive information in different resources at once. We have already seen this trend rising and expect it to continue.

02 In order to bypass multi-factor authentication (MFA) systems, threat actors will likely continue to come up with new and creative methods. **Organizations must enforce the proper use of MFA** by their employees and stay vigilant, updating their MFA policy regularly to defend against these types of attacks.

03 **The implications of SaaS supply chain attacks are also expected to increase** in the coming year. As more companies rely on SaaS providers for their critical business functions, the risk of these types of attacks and their consequences are likely to increase.

04 **SaaS platforms will continue to be utilized by threat actors** as a means of creating malicious infrastructure, executing phishing campaigns, hosting malwares, and managing command and control on SaaS platforms. As it becomes more difficult for organizations to detect and defend against these types of attacks, actors will develop more sophisticated ways to utilize SaaS applications for malicious activities.

05 **Ensuring that former employees no longer have access to sensitive data will be a major task for organizations in the coming year.** As the global economy forecasts for 2023 suggest that the number of employees changing jobs or leaving a company is likely to increase, companies must take steps to revoke their former employees' access to sensitive information in order to reduce the risk of a security breach. This task becomes even more challenging when SaaS activity is not regularly monitored and managed.

Wing Security's "Golden Tips" For SaaS Security

In today's digital workspace, SaaS applications have become an integral part of many businesses. These cloud-based solutions offer convenience and flexibility, but also come with their own set of security considerations. In order to reduce the risks related to SaaS, it is important to follow some key practical tips for securing your SaaS applications and protecting your company's data.

1 Prefer login with SSO over login with user and password

Single-Sign-On (SSO) is much more secure than logging in with a user and password, as it allows for centralized authentication and authorization. Users are able to access multiple systems and applications at once without having to remember multiple sets of credentials, reducing the risk of password reuse and phishing.

2 Set a strong password organizational policy in place where SSO is not supported

In cases where SSO is not implemented, make sure that your organizational password policy requires users to choose complex, long and unique passwords to make it more difficult for threat actors to guess.

3 Enforce proper use of MFA, including limiting push notifications and adding a number challenge

Make sure that all users set and use Multi-Factor Authentication, and limit the number of times a push request can be sent to the user to avoid MFA fatigue attacks. A number challenge in the push message, where the user types a number received in the push message, is also recommended.

4 Manage your SaaS posture to eliminate "Shadow IT" - discover all applications, users and issued tokens

In order to eliminate Shadow IT and fully manage the risk of using SaaS applications, it is important to discover all the SaaS applications in use in your organization and manage their usage on a regular basis. This includes tracking permissions given to each application by tokens and identifying any security issues that may arise.

5 Permit only web browser extensions that exist in official marketplaces and monitor them regularly

It is recommended to install web extensions from official marketplaces to reduce the chances of malicious extensions. However, it is still important to monitor extensions regularly, even if they were installed from an official marketplace, as malicious extensions can still be found and removed.

6 Make sure you off-board former employees and revoke all their access to company assets

When an employee leaves the company, it is crucial to close all their access to the company's assets, including SaaS applications, files and data, in order to avoid data leakage. Make sure that you have a mechanism in place to ensure the off-boarding process is done in its entirety.

7 Close file sharing when it is no longer needed to avoid data leakage

People share files with both internal and external users to collaborate on a daily basis. However, when a project ends or a shared file is no longer needed, people tend to forget to close the share. It is recommended to monitor shared files and make sure they are closed once they are no longer needed to reduce the potential damage of data leakage.

As we have seen throughout this report, the growing popularity of SaaS has created new areas of attack that require special attention from security and IT teams.

We discussed the top five trends in cyber attacks related to SaaS and provided a forecast for the top trends in 2023.

We are confident that SaaS is a great model for both personal and business use, and with the right security attitude and management, the risks it poses can be significantly mitigated.

Sources and Additional Reading

- https://explodingtopics.com/blog/saas-statistics/
- https://www.digitalocean.com/blog/digitalocean-response-to-mailchimp-security-incident/
- https://assets.ctfassets.net/2ntc334xpx65/5B8jmyTUmE1P6SDCaBh8mz/78d75730fa2ff69637181a075542eb06/The_State_of_Secure_Identity_2022_Ebook.pdf/
- https://blog.group-ib.com/0ktapus/
- https://www.uber.com/newsroom/security-update/
- https://www.darkreading.com/attacks-breaches/circleci-and-github-customers-targeted-phishing-campaign/
- https://dropbox.tech/security/a-recent-phishing-campaign-targeting-dropbox/
- https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us/
- https://blog.talosintelligence.com/recent-cyber-attack/
- https://www.zdnet.com/article/microsoft-warns-about-this-phishing-attack-that-wants-to-read-your-emails/
- https://github.blog/2022-04-15-security-alert-stolen-oauth-user-tokens/
- https://www.microsoft.com/en-us/security/blog/2022/09/22/malicious-oauth-applications-used-to-compromise-email-servers-and-spread-spam/
- https://www.kaspersky.com/about/press-releases/2022_13-million-users-encountered-browser-extension-threats-in-the-first-half-of-2022/
- https://www.volexity.com/blog/2022/07/28/sharptongue-deploys-clever-mail-stealing-browser-extension-sharpext/
- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/malicious-cookie-stuffing-chrome-extensions-with-1-4-million-users/
- https://labs.guard.io/dormant-colors-live-campaign-with-over-1m-data-stealing-extensions-installed-9a9a459b5849/
- https://www.malwarebytes.com/blog/threat-intelligence/2022/01/north-koreas-lazarus-apt-leverages-windows-update-client-github-in-latest-campaign/
- https://www.avanan.com/blog/hackers-attach-malicious-.exe-files-to-teams-conversations/
- https://www.mandiant.com/resources/blog/tracking-apt29-phishing-campaigns/
- https://unit42.paloaltonetworks.com/cloaked-ursa-online-storage-services-campaigns/

For more information reach out to hello@wing.security