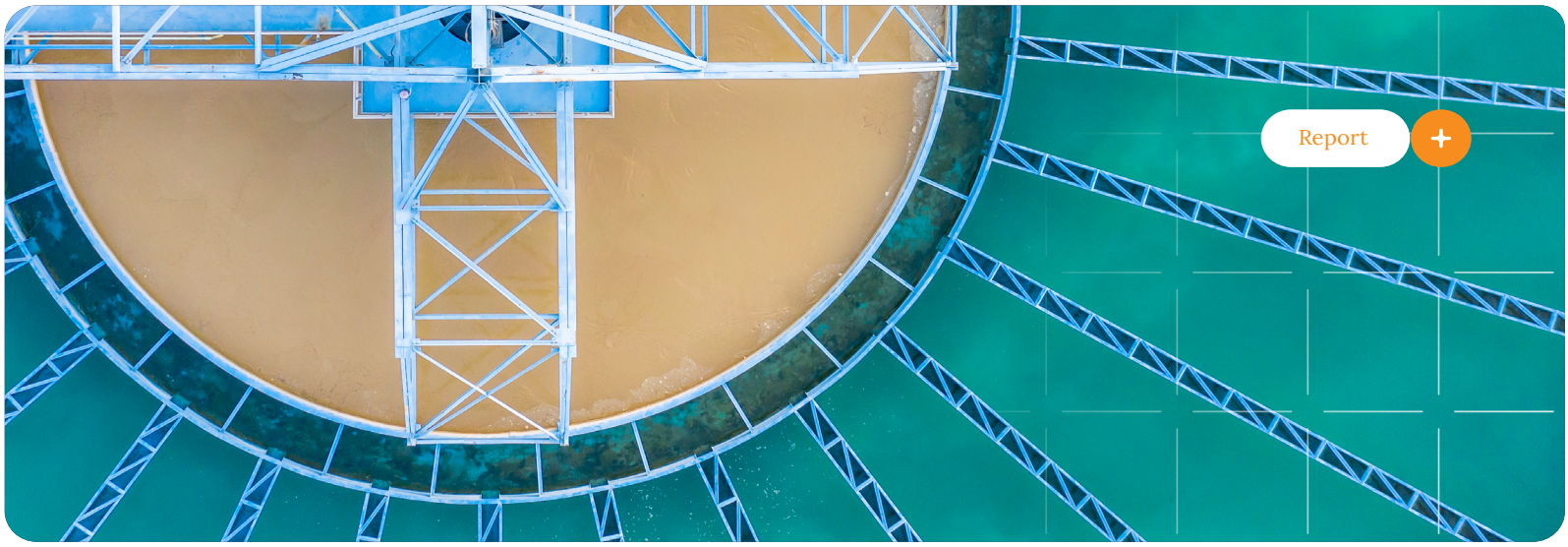
March 2023



NETSKOPE THREAT LABS REPORT
HEALTHCARE

The Netskope Threat Labs Report highlights a different segment every month. The purpose of this report series is to provide strategic, actionable intelligence on active threats against enterprise users in each segment. The segment highlighted in this report is enterprise users in healthcare.

IN THIS REPORT

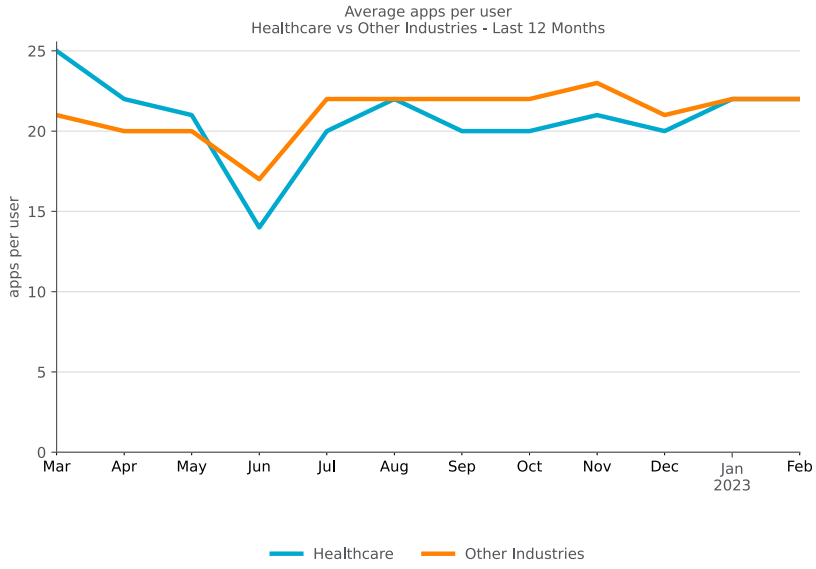
- **Cloud App Adoption:** The popularity of cloud apps in healthcare is similar to other industries, with 21 apps per user per month on average. Microsoft OneDrive, Teams, and Sharepoint are the most popular cloud apps in healthcare.

- **Cloud App Abuse:** Attackers are increasingly abusing cloud apps as a malware delivery channel in healthcare enterprises, where cloud-delivered malware increased from 38% to 42% in the past twelve months, led by malware downloads from popular apps, including Microsoft OneDrive and Weebly.

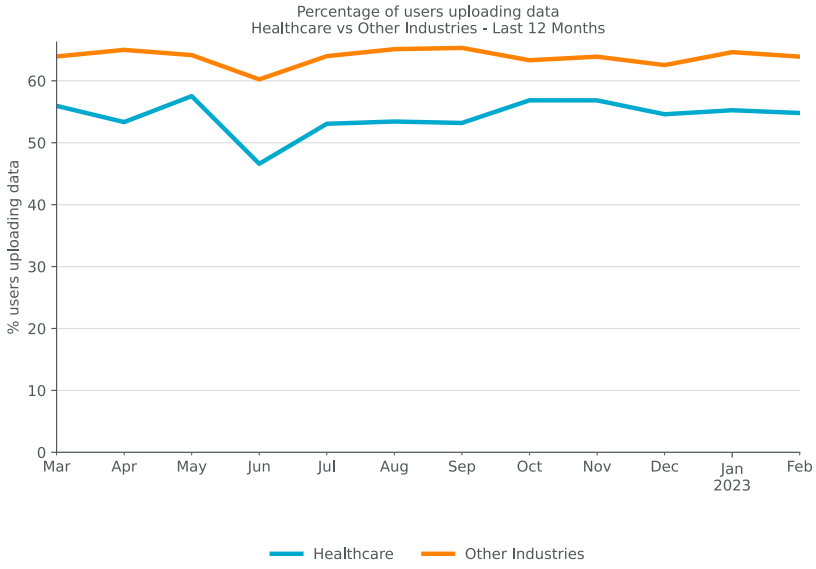
- **Malware & Ransomware:** The most common type of malware blocked by Netskope in healthcare enterprises were trojans, followed by downloaders and exploits. FormBook, Casbaneiro, Ursnif, and Remcos are among the top malware families targeting healthcare in the past twelve months.

CLOUD APP ADOPTION

Cloud apps are used in healthcare to improve productivity and enable hybrid workforces. The average number of cloud apps an enterprise user in healthcare interacts with monthly decreased slightly, from 25 in March 2022 to 22 in Feb 2023. This puts healthcare on-par with other industries in terms of cloud adoption. The top 1% of users in healthcare interacted with 92 apps per month, compared to 93 apps in other industries.

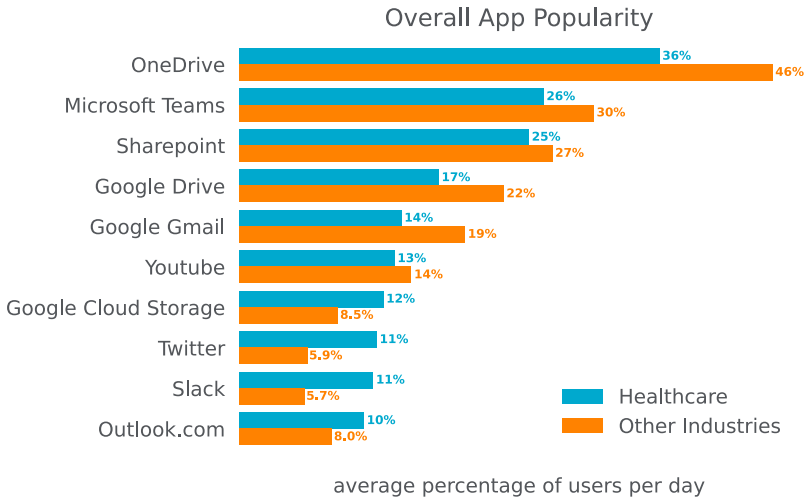


Enterprise users in healthcare download data from cloud apps at the same rate as users throughout other industries, with 94% of users downloading data from cloud apps each month, but lag behind in terms of uploads. In the last twelve months, 54% of users working in healthcare, on average, uploaded data to cloud apps, compared to 64% of users in other industries. Over the past twelve months, the number of users uploading to cloud apps remained stable, with only a 1% decrease between March 2022 and February 2023.



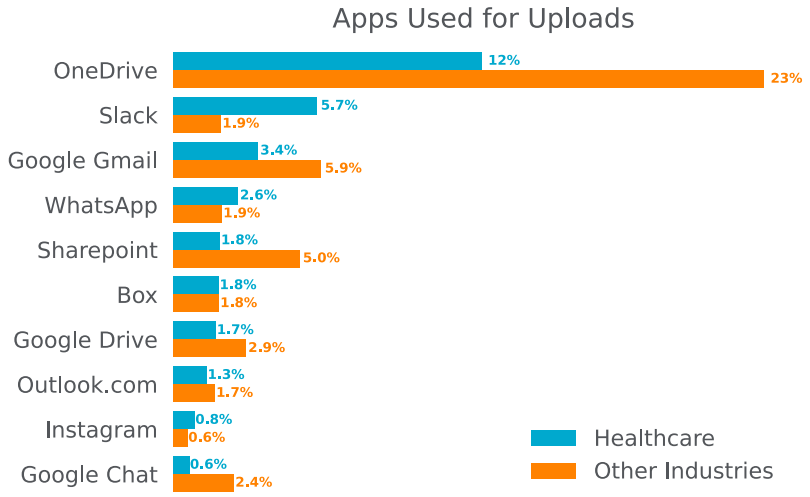
Most Popular Cloud Apps

The most popular cloud app among enterprise users in healthcare is OneDrive, with an average of 36% of users per day, followed by Microsoft Teams and Sharepoint. The majority of Microsoft apps are more popular in other industries when compared to healthcare, especially OneDrive, with an average of 46% of users per day. Google Drive and Gmail are also popular in healthcare, but also more popular in other industries. This observation indicates healthcare organizations could still be using traditional on-prem Office product software at a higher rate than other industries. Google Cloud Storage is more popular in healthcare than in other industries, and Twitter and Slack are almost twice as popular in healthcare when compared to other industries.



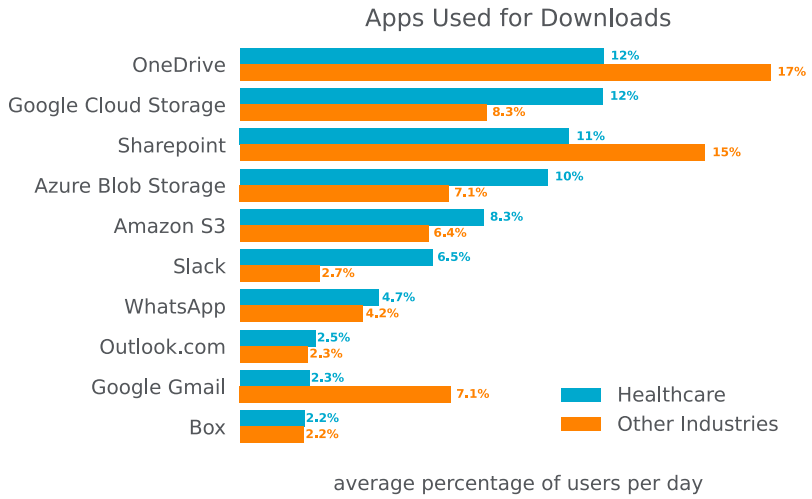
Top Apps Used for Uploads

In addition to being the most popular app, Microsoft OneDrive is also the most popular app used for uploads, but it is significantly less used in healthcare when compared to other industries. The second most popular app for uploads is Slack, with 5.7% of users per day on average, 3x more when compared to other industries. Google apps, such as Gmail, Drive, and Chat are also popular among enterprise users in healthcare for file uploads, but not as popular as they are in other industries.



Top Apps Used for Downloads

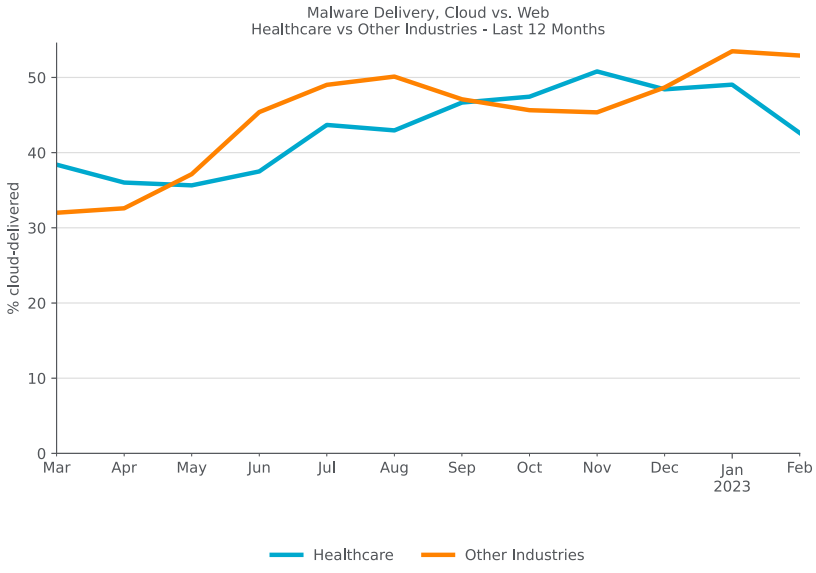
OneDrive leads the most popular cloud app for downloads by enterprise users in healthcare, with 12% of users per day on average. Microsoft apps, such as OneDrive and Sharepoint are commonly used for downloads, but with a smaller margin compared to other industries. Azure Blob Storage is an exception, as it's used 1.4x more in healthcare enterprises than the rest of the industries. Slack, which is a popular app overall in healthcare, is being used 2.4x more when compared to other industries for file downloads. In total, cloud-based productivity suites appear to be less popular across the board in healthcare compared to other industries.



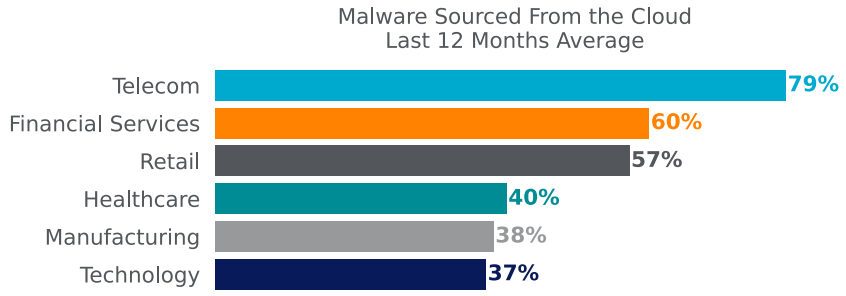
CLOUD APP ABUSE

Cloud Malware Delivery

In the past twelve months, the popularity of cloud malware delivery in healthcare organizations increased from 38% in March 2022 to 42% in February 2023. Attackers attempt to fly under the radar by delivering malicious content via popular cloud apps. Abusing cloud apps for malware delivery enables attackers to evade security controls that rely primarily on domain block lists and URL filtering, or that do not inspect cloud traffic. The twelve-month average in healthcare organizations is also almost the same compared to other organizations, with 43% of malware downloads from enterprise users in healthcare compared to 45% in other industries.



Compared to other industries, healthcare is in the middle of the pack in terms of cloud malware downloads, with only Manufacturing and Technology having a lower percentage of cloud malware downloads.

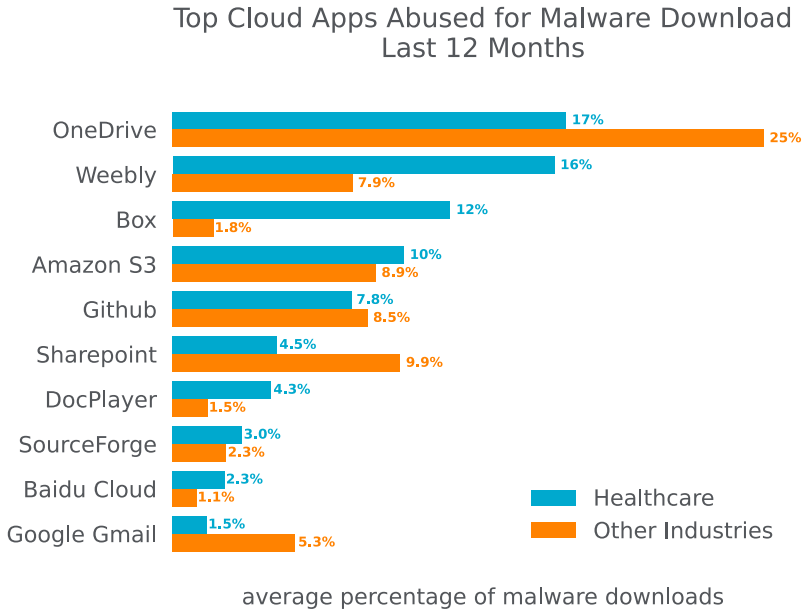


Cloud Apps Abused for Malware Delivery

In the last twelve months, Microsoft OneDrive was the most popular cloud app abused for malware downloads in healthcare organizations, representing 17% of all cloud malware downloads. As highlighted earlier in this report, Microsoft OneDrive is also the most popular app among enterprise users in healthcare, which makes it both a prime target for attackers seeking to target a wide variety of organizations using the same toolset and also makes it more likely that the malicious payloads would reach their targets.

The free web hosting service Weebly is the second most popular app abused for malware downloads in healthcare enterprises, with twice as many downloads when compared to other industries. Box holds the third place, with 12% of malware downloads, 6.6x higher than other industries.

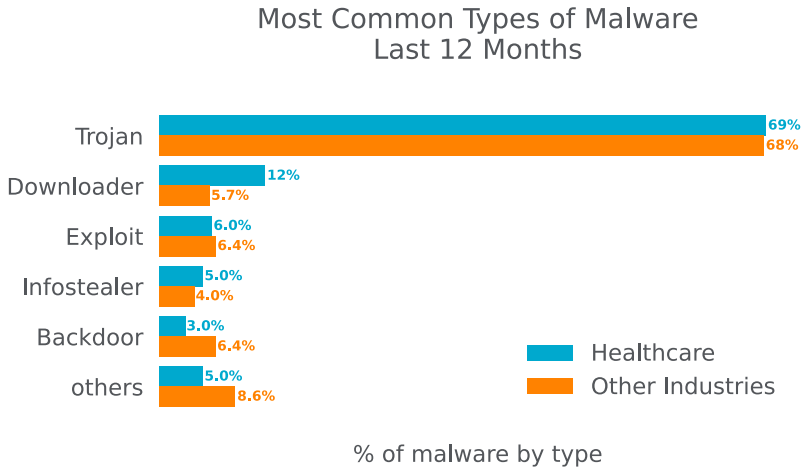
Other apps abused for malware downloads in healthcare enterprises include cloud storage apps (Amazon S3, Baidu Cloud), software hosting sites (GitHub, SourceForge), collaboration apps (Sharepoint), and mail apps (Google Gmail). DocPlayer, which is a cloud app to share online documents, is also popular for malware downloads in healthcare enterprises, with 4.3% downloads on average in the last twelve months, 2.8x higher than other industries.



Top Malware Types

The most common malware detected by Netskope in healthcare enterprises in the last twelve months were Trojans, which are commonly used by attackers to gain an initial foothold and deliver other types of malware, such as infostealers, remote access trojans, backdoors, and ransomware. The second most common type of malware were downloaders, which like trojans, are also used to deliver other types of malware.

The third place are file-based exploits, which includes documents used to exploit many known vulnerabilities, including CVE-2022-30190 (a.k.a. Follina) and other vulnerabilities that exploit unpatched versions of Adobe Acrobat and Reader and Microsoft Office.



Top Malware & Ransomware Families

This list contains the top ten malware and ransomware families detected by Netskope in healthcare in the last twelve months:

- **Backdoor.Zusy** (a.k.a. TinyBanker) is a banking trojan based on the source code of Zeus, aiming to steal personal information via code injection into websites. Details
- **Trojan.FormBook** (a.k.a. XLoader) is a malware that provides full control over infected machines, offering many functionalities such as stealing passwords and executing additional malware. Details
- **Infostealer.Casbaneiro** (a.k.a. Metamorfo) is a banking trojan that aims to steal sensitive financial data, similar to other families sourced from LATAM like Guildma, Grandoreiro, and Ousaban. Details
- **Trojan.Ursnif** (a.k.a. Gozi) is a banking trojan and backdoor, which had its source code leaked on GitHub in 2005, allowing attackers to create and distribute many variants. Details
- **Infostealer.Micropsia** is a Delphi malware created by an APT group known as Arid Viper that aims to steal sensitive information and provide remote access. Details

- **RAT.Remcos** is a remote access trojan that provides an extensive list of features to remotely control devices and is popularly abused by many attackers. Details

- **Infostealer.PonyStealer** (a.k.a. Fareit) is a malware able to steal passwords from hundreds of applications, including web browsers, emails, messaging apps, and FTP. Details

- **RAT.NetWiredRC** (a.k.a. NetWire RC) is a malware associated with APT33, aimed to provide remote access and steal sensitive information, like passwords. Details

- **Infostealer.Azorult** (a.k.a. PuffStealer) is a malware that aims to steal sensitive information such as account passwords. Details

- **Ransomware.BlackCat** (a.k.a.) is a RaaS (ransomware-as-a-family) group that emerged in November 2021, known for targeting critical sectors, such as government and healthcare. Details

RECOMMENDATIONS

This report highlighted increasing cloud adoption, including increases of data being uploaded to and downloaded from a wide variety of cloud apps. It also highlighted an increasing trend of attackers abusing a wide variety of cloud apps–especially popular enterprise apps–to deliver malware to their victims. The malware samples were primarily Trojans, but also included botnets, ransomware, backdoors, and infostealers. Netskope Threat Labs recommends enterprises in healthcare review their security posture to ensure that they are adequately protected against these trends:

- Inspect all HTTP and HTTPS downloads, including all web and cloud traffic, to prevent malware from infiltrating your network. Netskope customers can configure their Netskope NG-SWG with a Threat Protection policy that applies to downloads from all categories and applies to all file types.

- Ensure that high-risk file types like executables and archives are thoroughly inspected using a combination of static and dynamic analysis before being downloaded. Netskope Advanced Threat Protection customers can use a Patient Zero Prevention Policy to hold downloads until they have been fully inspected.

- Configure policies to block downloads from apps and instances that are not used in your organization to reduce your risk surface to only those apps and instances that are necessary for the business.

- Configure policies to block uploads to apps and instances that are not used in your organization to reduce the risk of accidental or deliberate data exposure from insiders or abuse by attackers.

- Use an Intrusion Prevention System (IPS) that can identify and block malicious traffic patterns, such as command and control traffic associated with popular malware. Blocking this type of communication can prevent further damage by limiting the attacker's ability to perform additional actions.

In addition to recommendations above, Remote Browser Isolation (RBI) technology can provide additional protection when there is a need to visit websites that fall in categories that can present higher risk, like Newly Observed and Newly Registered Domains.

NETSKOPE THREAT LABS

Staffed by the industry's foremost cloud threat and malware researchers, Netskope Threat Labs discovers, analyzes, and designs defenses against the latest cloud threats affecting enterprises. Our researchers are regular presenters and volunteers at top security conferences, including DefCon, BlackHat, and RSA.

ABOUT THIS REPORT

Netskope provides threat protection to millions of users worldwide. Information presented in this report is based on anonymized usage data collected by the Netskope Security Cloud platform relating to a subset of Netskope customers with prior authorization.

This report contains information about detections raised by Netskope's Next Generation Secure Web Gateway (SWG), not considering the significance of the impact of each individual threat. Stats in this report are based on the period starting March 1, 2022 through February 28, 2023. Stats are reflection of attacker tactics, user behavior, and organization policy.