
netskope
CLOUD AND THREAT REPORT
JANUARY 2022 EDITION
BROUGHT TO YOU BY:
netskope
THREAT LABS

EXECUTIVE SUMMARY

In this sixth edition of the Cloud Threat Report, we take a look back at the top trends in cloud attacker activities and cloud data risks from 2021 compared to 2020. We examine changes in the malware landscape in 2021, highlighting that attackers are enjoying more success abusing cloud apps to deliver malware payloads to their victims. We quantify that success in terms of the increasing number of cloud apps from which we block malware downloads and the increasing share of the total malware downloads coming from cloud apps.

In addition, we take a look at a continuing trend of attackers abusing Microsoft Office document formats to deliver malware. In Q2 2020, we saw a sudden spike in malicious Office documents driven primarily by Emotet, who launched a large-scale and highly effective malspam campaign that delivered malicious Office documents using popular cloud apps. Since then, copycat groups have continued to abuse Office documents to deliver malware and the quantity of malicious documents remains high above pre-Emotet levels.

We also take a look at credential attacks against managed cloud apps which continue at the same rate as 2020, but with a shift in the sources of the attacks. The top source of credential attacks in 2020 were a few heavy hitters responsible for a large number of login attempts. In 2021, credential attacks came from a much larger number of sources, each responsible for fewer login attempts.

Finally, we take a look at a different type of data risk, insider threats. In 2021, we observed users leaving their jobs at twice the rate of 2020. Users leaving the organization pose a serious data security risk, with more than one out of every seven people using personal Cloud Storage apps to take data with them when they leave. Because Cloud Storage apps appear in leaderboards throughout this report, we finish by examining how their overall popularity among users is a primary driver for their appearance at the top of the malware download and insider threat leaderboards.

REPORT HIGHLIGHTS

- **Google Drive emerges as the top app for malware downloads,** taking over that spot from Microsoft OneDrive, while the percentage of malware downloads from cloud apps increased from 46%, peaked at 73% and plateaued at 66%.
- **Emotet copycats continue to abuse Microsoft Office documents,** which continue to represent one-third of all malware downloads, compared to one-fifth of all malware downloads prior to Emotet.
- **More than half of managed cloud app instances are targeted by credential attacks,** while the sources of such attacks shift from a few heavy-hitters to a more decentralized attack.
- **Employee attrition leads to data exfiltration,** as one of out overy seven users take data with them when they leave using personal app instances.
- **Cloud adoption continues to rise,** with the rising popularity of Cloud Storage apps attracting abuse by both attackers (for malware delivery) and insider threats (for data exfiltration).

ABOUT THIS REPORT

Netskope provides threat and data 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 Netskops's Next Generation Secure Web Gateway (SWG) and API Cloud Access Security Broker (CASB). When reporting about threats, we analyze detections raised by our NG SWG when malicious content is accessed. We count the total number of detections from our platform, not considering the significance of the impact of each individual threat. When reporting on insider threats, we count the total number of downloads and uploads from our platform, not considering the content or sensitivity of each individual file.

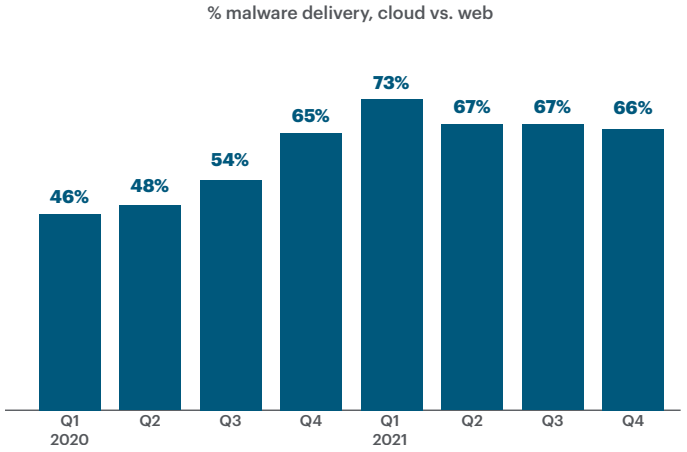
Netskope Threat Labs

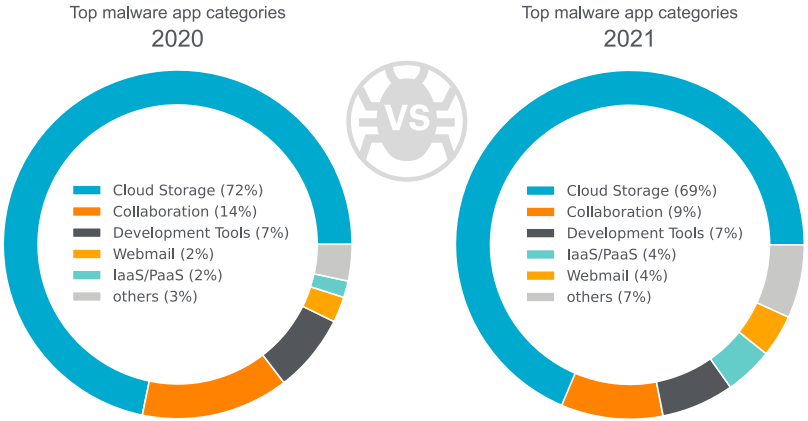
Staffed by the industry's foremost cloud threat and malware researchers, Netskope Threat Labs discovers, analyzes, and designs defenses against the latest cloud and data threats affecting enterprises. Our researchers are regular presenters and volunteers at top security conferences, including DefCon,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

GOOGLE DRIVE EMERGES AS TOP APP FOR MALWARE DOWNLOADS

Throughout 2020, the percentage of total malware downloads from cloud apps compared to traditional websites increased every quarter. This upward trend is a reflection of both attacker activity and user behavior. Attackers enjoyed greater success abusing cloud apps to deliver malicious payloads to users, led by groups such as Emotet. In 2021, we saw the percentage of malware downloads plateau, with just over two-thirds of all malware downloads for the year coming from cloud apps. We expect this plateau to continue into 2022.

Cloud Storage apps accounted for the majority of cloud malware downloads in both 2020 and 2021. The features of Cloud Storage apps that make them attractive as a malware delivery platform are their popularity and ease of use. Attackers create their own free accounts, upload malicious payloads, and share them publicly or with specific victims. While the percentage of total malware downloads from different app categories varied slightly year-over-year, the ordering of the top three categories remained unchanged.

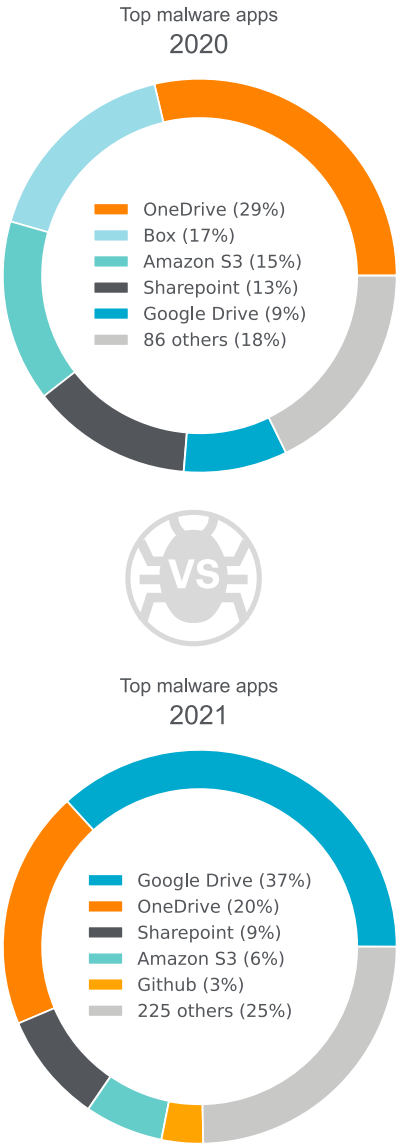




Google Drive emerged as the app with the most malware downloads in 2021, taking over that spot from Microsoft OneDrive in 2020. Google Drive and Microsoft OneDrive are the two most popular Cloud Storage apps tracked by the Netskope platform, so their presence at the top of the list is unsurprising. Attackers create their own free Google Drive or OneDrive accounts, upload malicious payloads, and share them publicly or with specific victims. The changes in the leaderboard are a reflection of changes in attacker tactics as well as user behavior. For example, Emotet delivered the majority of their malicious Office document payloads using Box in 2020, but were inactive for most of 2021, and so Box fell from 17% in 2020 to less than 3% in 2021. Other attackers trying to mimic Emotet's success shifted tactics slightly, instead abusing Google Drive to deliver similar malicious Office documents, contributing to its rise to the top of the leaderboard.

Overall, the total number of apps with malware downloads increased from 91 to 230. Outside the top five, the apps that saw the greatest increase in the number of malware downloads included a variety of Cloud Storage, Collaboration, and Web Hosting apps. Those apps include (in alphabetical order):

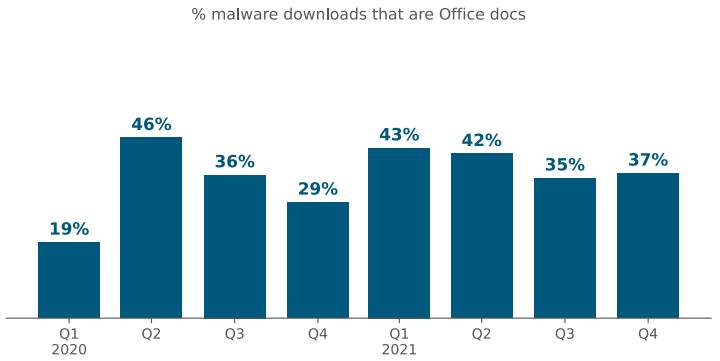
- Baidu Cloud
- Chrome Web Store
- Google Cloud Storage
- Microsoft Azure Blob Storage
- QQ Messenger
- SendSpace
- Sourceforge
- Squarespace
- Weebly
- Zippyshare

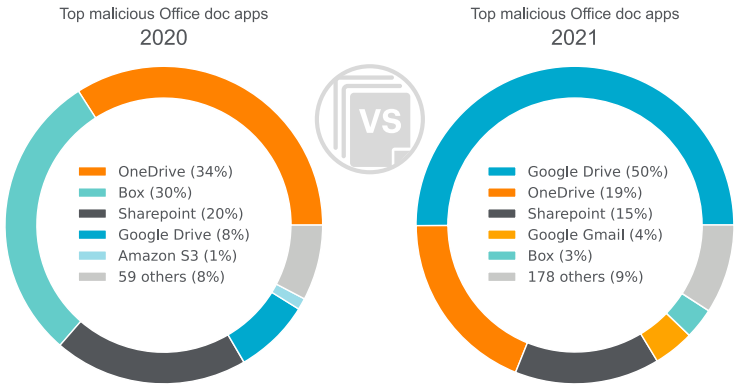


EMOTET COPYCATS CONTINUE TO ABUSE OFFICE DOCS

Malicious Office documents, representing only 19% of malware downloads at the beginning of 2020, increased to 37% at the end of 2021. This increase happened in bursts, the first of which occurred in the second quarter of 2020 when Emotet launched a large-scale and highly effective malspam campaign to deliver malware via weaponized Office documents hosted in Box. That malspam campaign was the primary driver of Box appearing as one of the top apps for malware downloads in 2020, as described in the previous section. Since then, other threat groups have attempted to recreate Emotet's success, abusing Office documents to deliver ransomware, banking Trojans, remote access Trojans, and other malware. The second burst happened at the beginning of 2021, led by an increase in malicious Office documents spread by Dridex. The success of Emotet in 2020 has caused long-term changes in the distribution of malicious file types. Prior to Q2 2020, Office documents represented one-fifth of all malware downloads. Since then, Office documents represent more than one-third of all malware downloads, a trend that we expect to continue throughout 2022.

The apps with the most malicious Office document downloads exhibited a similar trend as the overall malware downloads: Google Drive took over the top spot from Microsoft OneDrive, and Box fell significantly after the Emotet campaign of 2020. Attackers delivering malicious Office documents via cloud apps create their own free accounts, upload malicious documents, and share them publicly or with specific victims. While we expect Microsoft OneDrive and Google Drive to remain in the top spots in 2022 due to their overall popularity, we expect the proportion of each to balance out in 2022, based on attacker activity and user behavior.



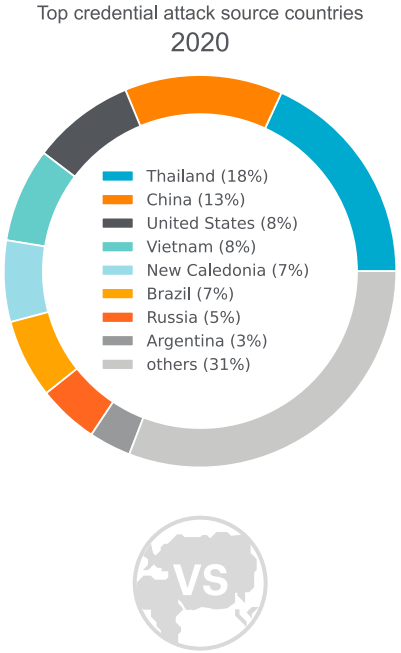


MORE THAN HALF OF MANAGED CLOUD APP INSTANCES TARGETED BY CREDENTIAL ATTACKS

From 2020 through 2021, more than half of all cloud-managed corporate instances of cloud apps were targeted by credential attacks, including password spraying and credential stuffing attacks. Attackers constantly try common passwords and leaked credentials from other services to gain access to sensitive information stored in cloud apps. The attackers attempting to break into managed cloud app instances are also generally launching credential attacks from the same IP addresses against other services, including SSH and RDP.

Year-over-year, the quantity of credential attack attempts against cloud apps remained constant, but the sources of the attacks shifted significantly. Only 2% of the login attempts in 2021 originated from IP addresses that also launched credential attacks in 2020, with the remaining 98% coming from new IP addresses.

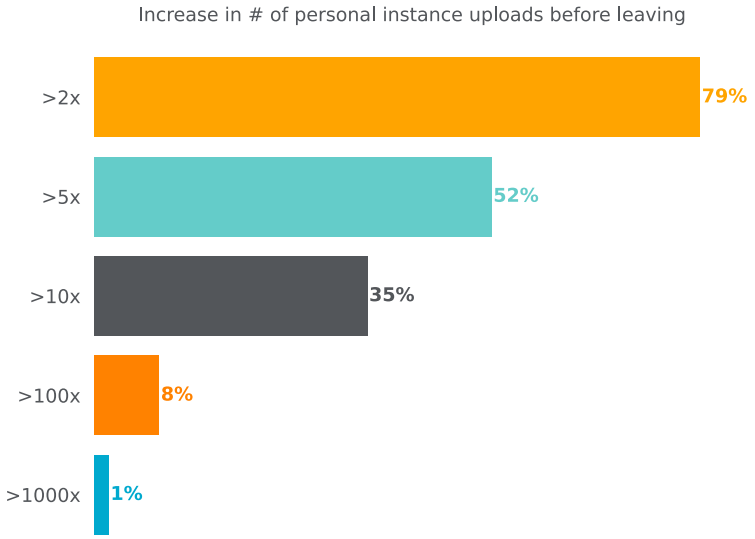
By country, the source of credential attacks also shifted, with the United States overtaking Thailand as the top source of attacker login attempts. In 2020, there were a handful of heavy-hitting IP addresses responsible for propelling Thailand to the top spot. In 2021, none of those heavy-hitters appeared to be active in Thailand. In 2021, the United States took the top spot because of a much larger number of IP addresses (64x as many as Thailand in 2020) each making a smaller total number of login attempts, coming primarily from the major ISPs in the country. This activity was likely the result of compromised devices being used to launch credential attacks.



EMPLOYEE ATTRITION LEADS TO DATA EXFILTRATION

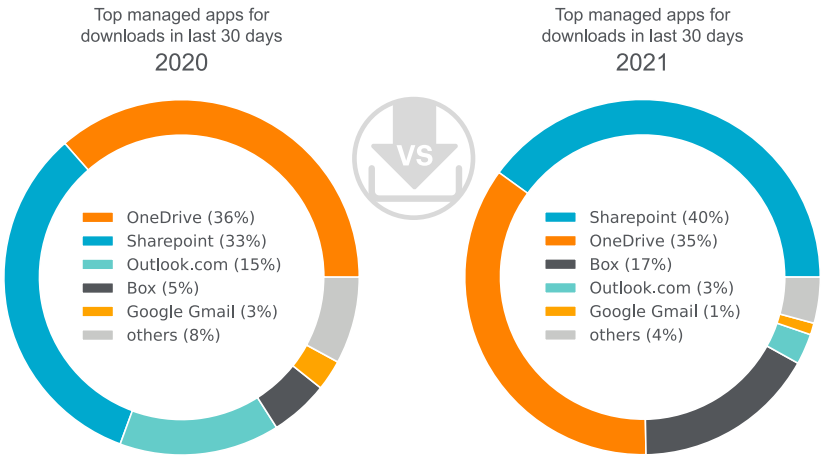
In 2021, attrition doubled, with 8% of employees leaving their jobs, compared to 4% in 2020. In their final 30 days of employment, those users tended to download more files than usual from managed corporate app instances and upload more data than usual to personal app instances. Between 2020 and 2021, an average of 29% of users downloaded more files from managed corporate app instances and 15% of users uploaded more files to personal app instances in their final 30 days.

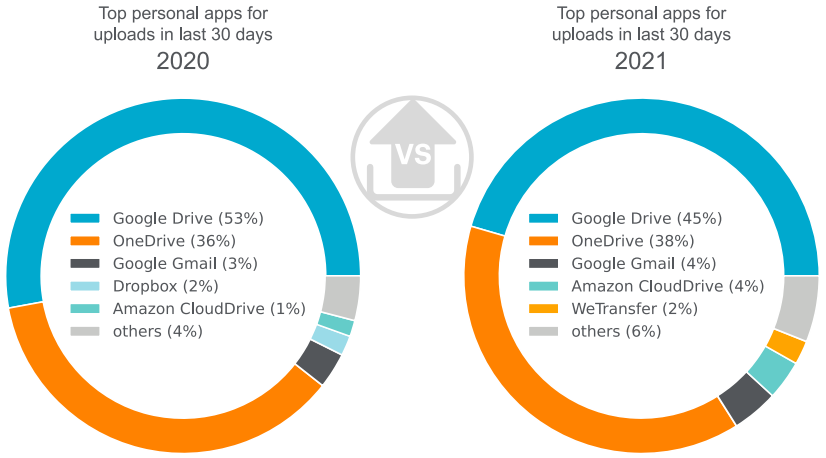
Of the users who uploaded more files to personal apps in their final 30 days, half uploaded more than 5x their normal data volume, 8% uploaded more than 100x their usual data volume, and 1% uploaded more than 1000x their baseline, indicating that there is significant and deliberate movement of data into personal instances coming from users about to leave their jobs.



The top managed apps from which users downloaded files before leaving included Cloud Storage, Collaboration, and Webmail apps. OneDrive and Sharepoint remained in the top two spots throughout the past two years, with Box rising to take the #3 spot from Outlook.com.

The top personal app instances to which users uploaded files before leaving were primarily Cloud Storage apps. Personal instances of Google Drive and Microsoft OneDrive, the two most popular Cloud Storage apps, accounted for the vast majority of the uploads in both 2020 and 2021, with Amazon CloudDrive and WeTransfer gaining in popularity in 2021.



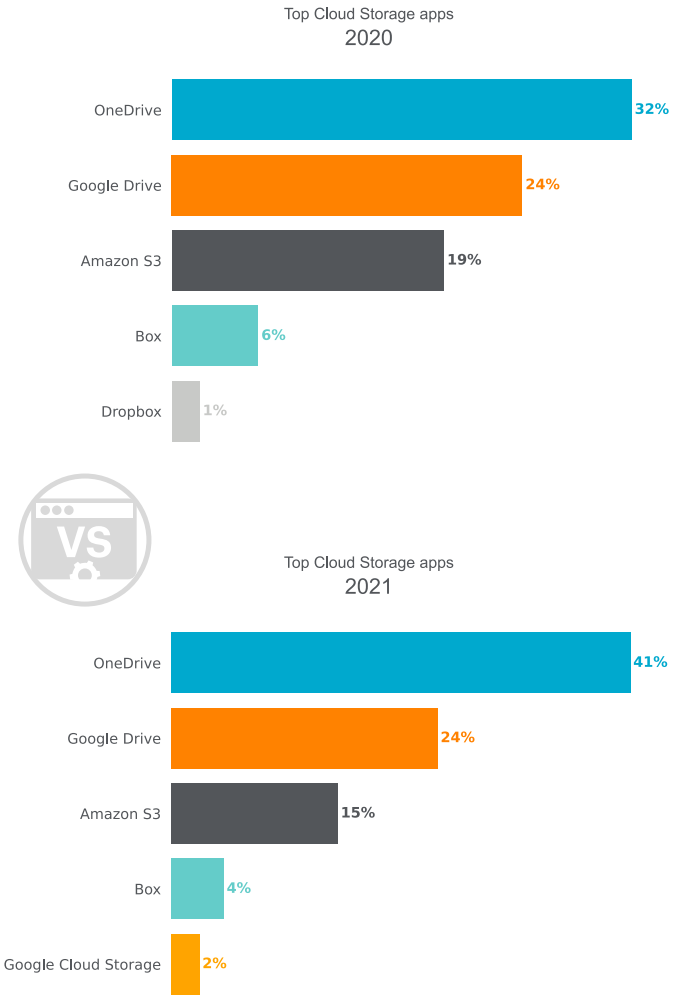


POPULARITY OF CLOUD STORAGE APPS INVITES ABUSE

Why do Cloud Storage apps appear in so many top five lists in this report, for malware downloads, for malicious Office document downloads, and for apps used by insiders to take data when they leave? And why do so many of the same apps appear in each of those lists? Cloud Storage apps are very popular among all users. In 2021, 79% of people used at least one Cloud Storage app, up from 71% of all users in 2020. The total number of Cloud Storage apps in use also increased: An organization with 500—2,000 people used, on average, 39 distinct Cloud Storage apps in 2021, up from 35 in 2020.

Attackers want to maximize the likelihood of their attacks reaching their victims, so they choose to abuse the most popular cloud apps to deliver malware payloads. Similarly, users on average will be more likely to download content hosted on familiar apps. For example, an average user would be more likely to click on a link to download a file from Microsoft OneDrive than a service like AnonFiles. Similarly, insiders taking data are going to use familiar tools to take files with them when they leave an organization.

The most popular cloud apps in terms of the percentage of users that interact with those apps each month are Microsoft OneDrive, Google Drive, Amazon S3, and Box. This leaderboard considers all instances of an app: A user is counted as using the app regardless of whether they use personal instances, company instances, or third-party instances of the app. These top four apps remained the same in 2020 and 2021, with OneDrive gaining in popularity, while Amazon S3 and Box declined in popularity. Dropbox also fell in popularity, beaten out by Google Cloud Storage for fifth place in 2021. These apps, especially Microsoft OneDrive and Google Drive, appear throughout this report due to their overall popularity among enterprise users.



RECOMMENDATIONS

The top trends in 2021 were an increase in cloud-delivered malware along with a continuing theme of Office documents being abused to deliver malware, credential attacks being launched against managed cloud apps, and insiders using personal cloud app instances to take data when they leave their jobs. To mitigate the risks these trends pose, Netskope recommends organizations implement the following controls:

1. SSO/MFA for both managed and unmanaged apps, including adaptive policy controls invoking step-up auth based on user, device, app, data, and activity.
2. Multi-layered, inline threat protection for all cloud and web traffic to block malware from making it to endpoints, plus blocking outbound malware communications.
3. Granular policy controls for data protection including data movement to and from apps, between company and personal instances, shadow IT, users, websites, devices, and locations.
4. Cloud data protection for sensitive data from internal and external threats across web, email, SaaS, shadow IT, and public cloud services, and security posture management for SaaS and IaaS.
5. Behavioral analysis to detect insider threats, data exfiltration, compromised devices, and compromised credentials.

LEARN MORE

For more information on cloud-enabled threats and our latest findings from Netskope Threat Labs, go to:
NETSKOPE.COM/NETSKOPE-THREAT-LABS

For more information on how to mitigate risk, contact us today:
WWW.NETSKOPE.COM/REQUEST-DEMO

BROUGHT TO YOU BY:

netskope
THREAT LABS