Netskope Threat Labs Report

Telecom

June 2024

The Netskope Threat Labs Report highlights a different segment every month and aims to provide strategic, actionable intelligence on active threats against users in each segment. This month, we look at users working in Telecom.

IN THIS REPORT

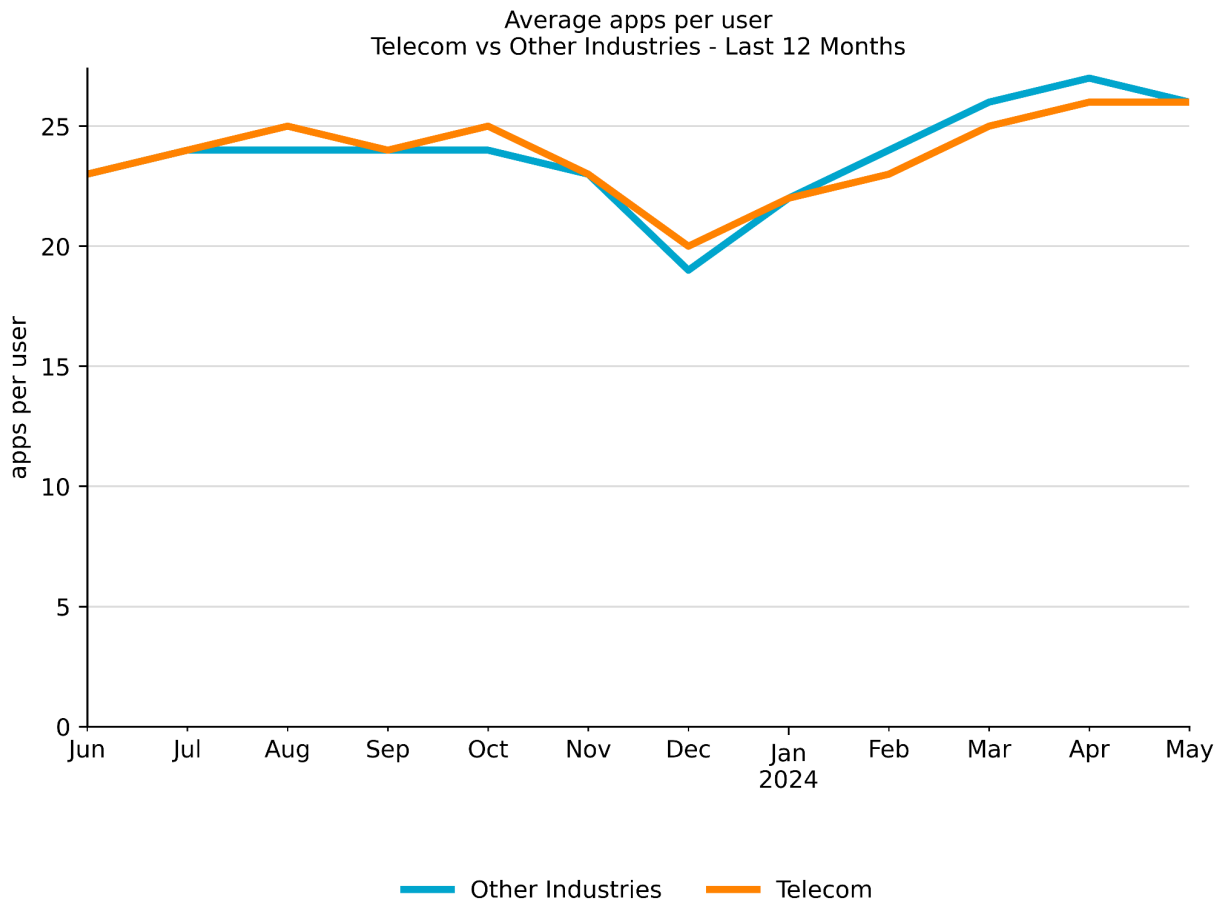
Cloud App Adoption: Users in Telecom upload and download files to cloud apps at almost the same frequency as users in other segments worldwide, but tend to interact with fewer cloud apps on average. Telecom also strongly prefers Microsoft apps, with Microsoft OneDrive, Teams, and Outlook being the industry's top three most popular apps.

Cloud App Abuse: Microsoft OneDrive and GitHub had the most malware downloads in Telecom, followed by Outlook.

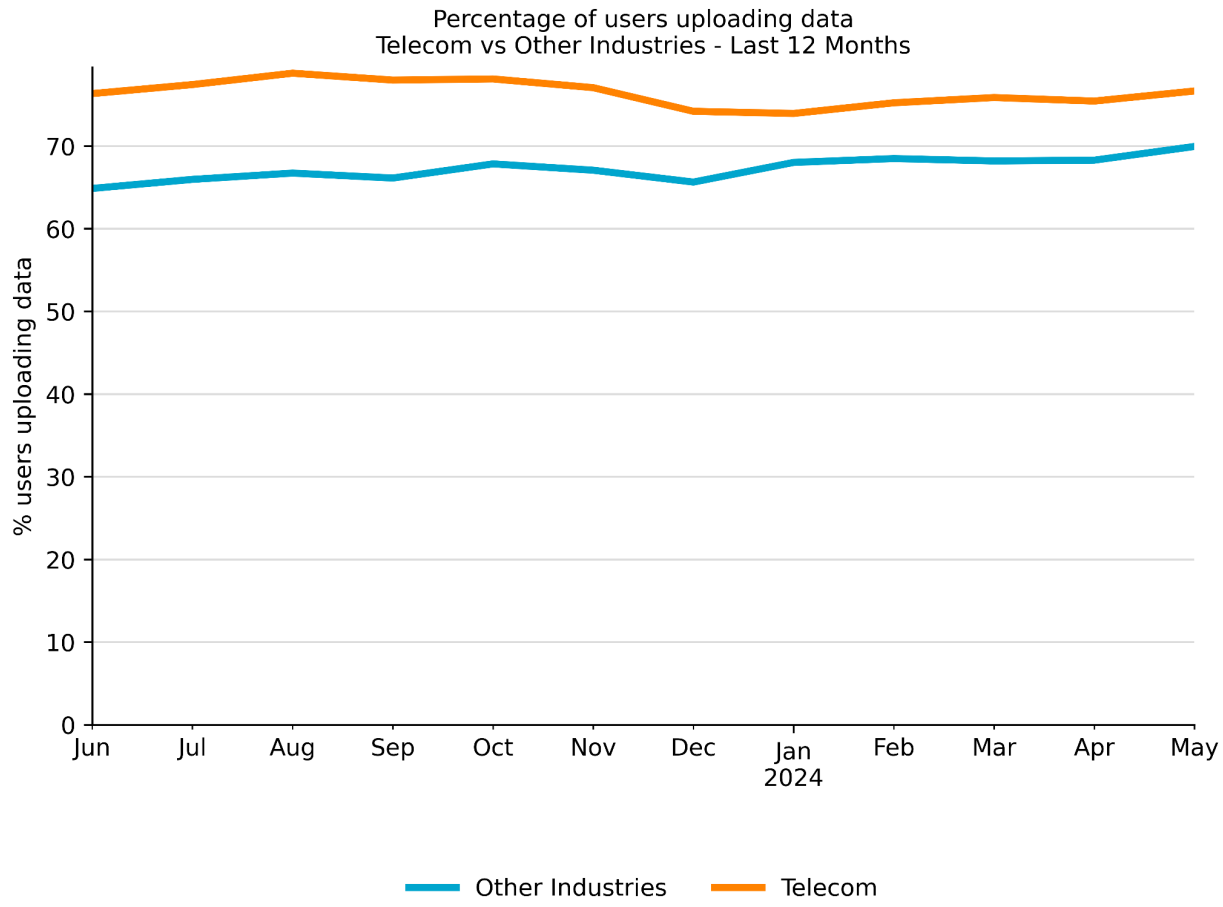
Malware & Ransomware: Among the most prevalent malware families targeting victims in Telecom were the remote access Trojan Remcos, the downloader Guloader, and the infostealer AgentTesla.

Cloud App Adoption

The average user in Telecom interacts with 24 cloud apps per month, while the top 1% interacts with 77 apps per month.

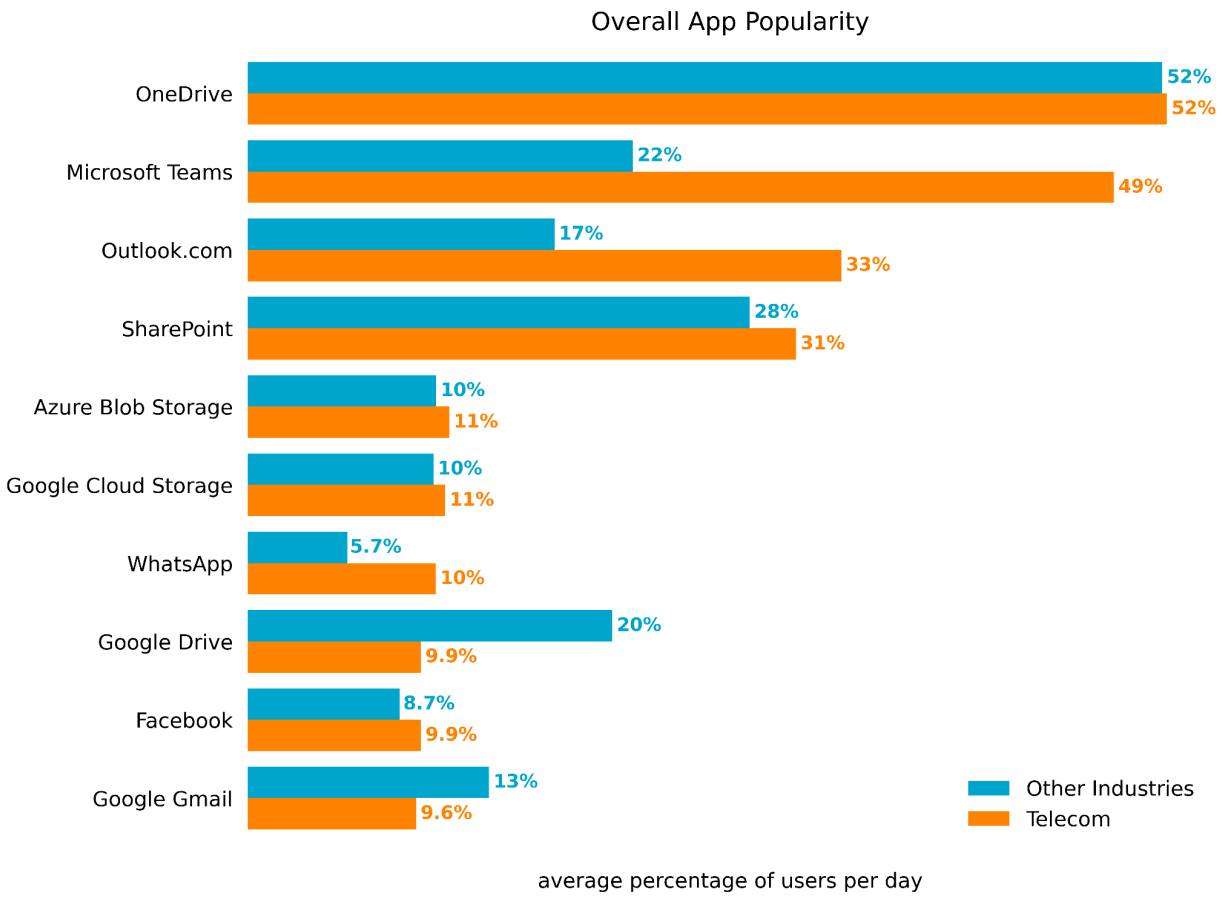


Users in Telecom download data from cloud apps at a similar rate as other industries, with 97% of Telecom users downloading data from cloud apps versus 95% in other industries. When it comes to uploading data, 76% of users in Telecom upload data to cloud apps versus 67% from other industries.



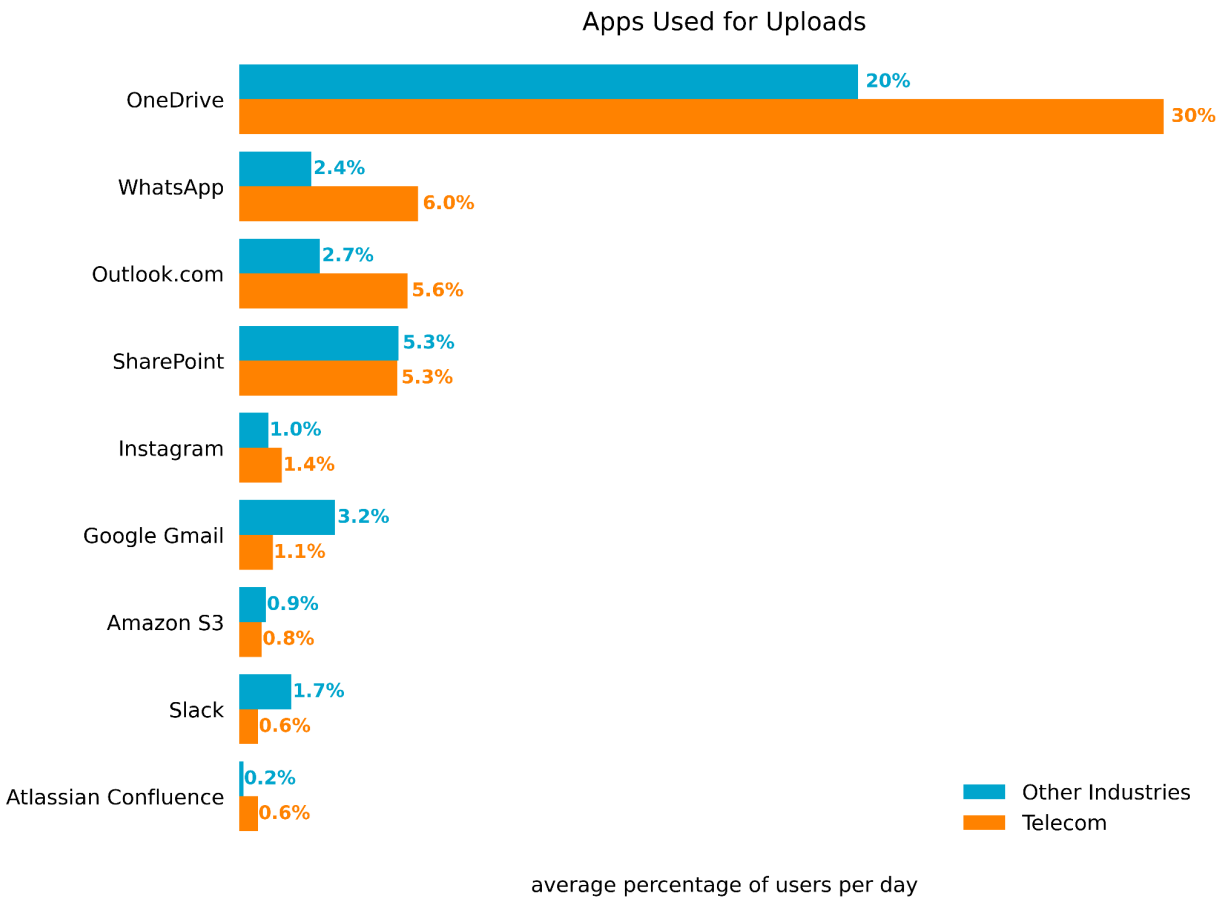
Most Popular Cloud Apps

The top three most popular cloud apps in Telecom are all Microsoft apps, with Microsoft OneDrive being the leader for all the industries. Microsoft Teams is very popular, with more than twice as many daily users. Email app Outlook.com and messaging app WhatsApp are also nearly twice as popular as other industries.



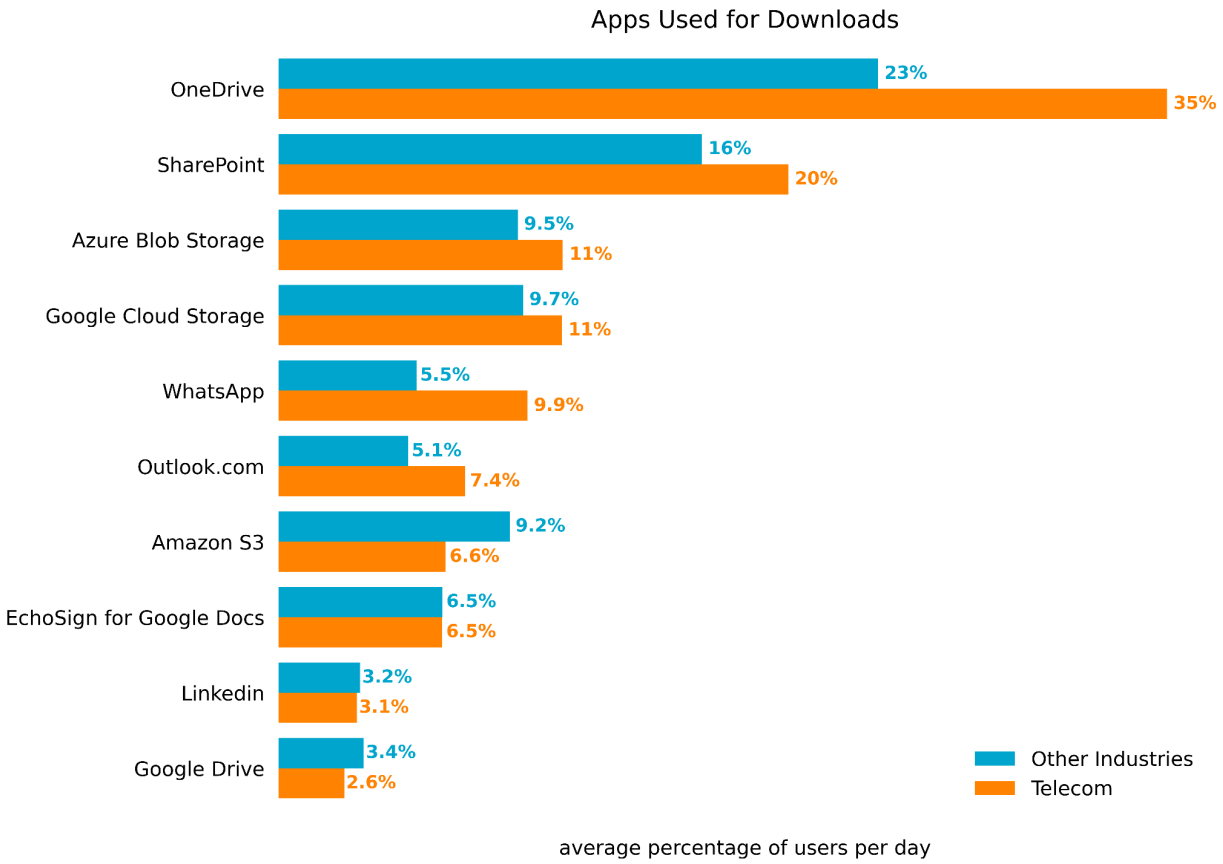
Top Apps Used for Uploads

Microsoft OneDrive is also the app most used for uploading data, with 30% of Telecom users uploading data to OneDrive daily, 50% more than other industries. The messaging app WhatsApp and the email app Outlook.com also stand out, with more than twice as many daily users as in other industries. By comparison, the messaging app Slack and email app Gmail are less popular in Telecom than in other industries.



Top Apps Used for Downloads

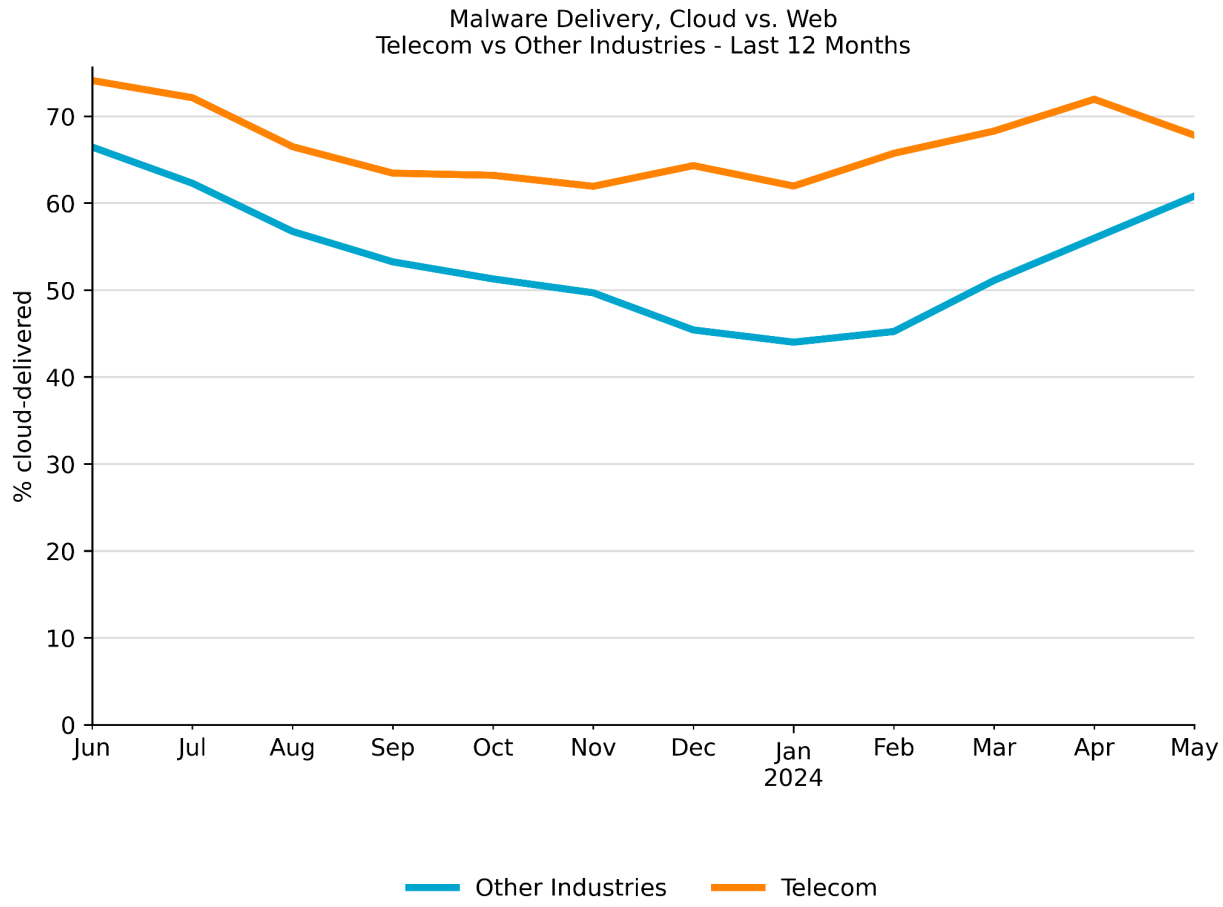
Similarly, Microsoft OneDrive is also the most popular app for downloads in Telecom, with 35% of users downloading from it. Telecom also has a slight edge in downloads from Outlook.com and Whatsapp, which are more popular than in other industries.



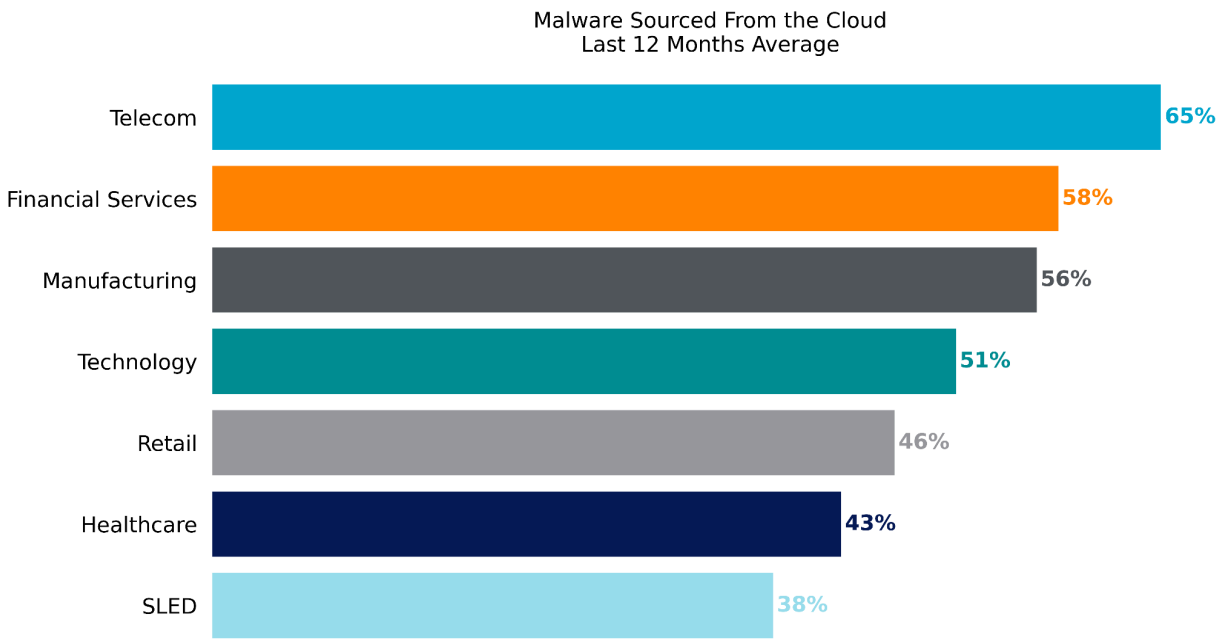
Cloud App Abuse

Cloud Malware Delivery

The percentage of malware downloads has fluctuated over the past year, driven by seasonal changes in which adversaries are active and how they choose to deliver their malware payloads to their victims. Today, the percentage of malware downloads is slightly down from where it was a year ago. In Telecom, the percentage of malware downloads fell in line with the global trend, bottoming out in the second half of 2023 and beginning to increase again in early 2024. The abuse of cloud apps allows malware to fly under the radar and evade regular security controls relying on tools, such as domain block lists, or not inspecting cloud traffic.

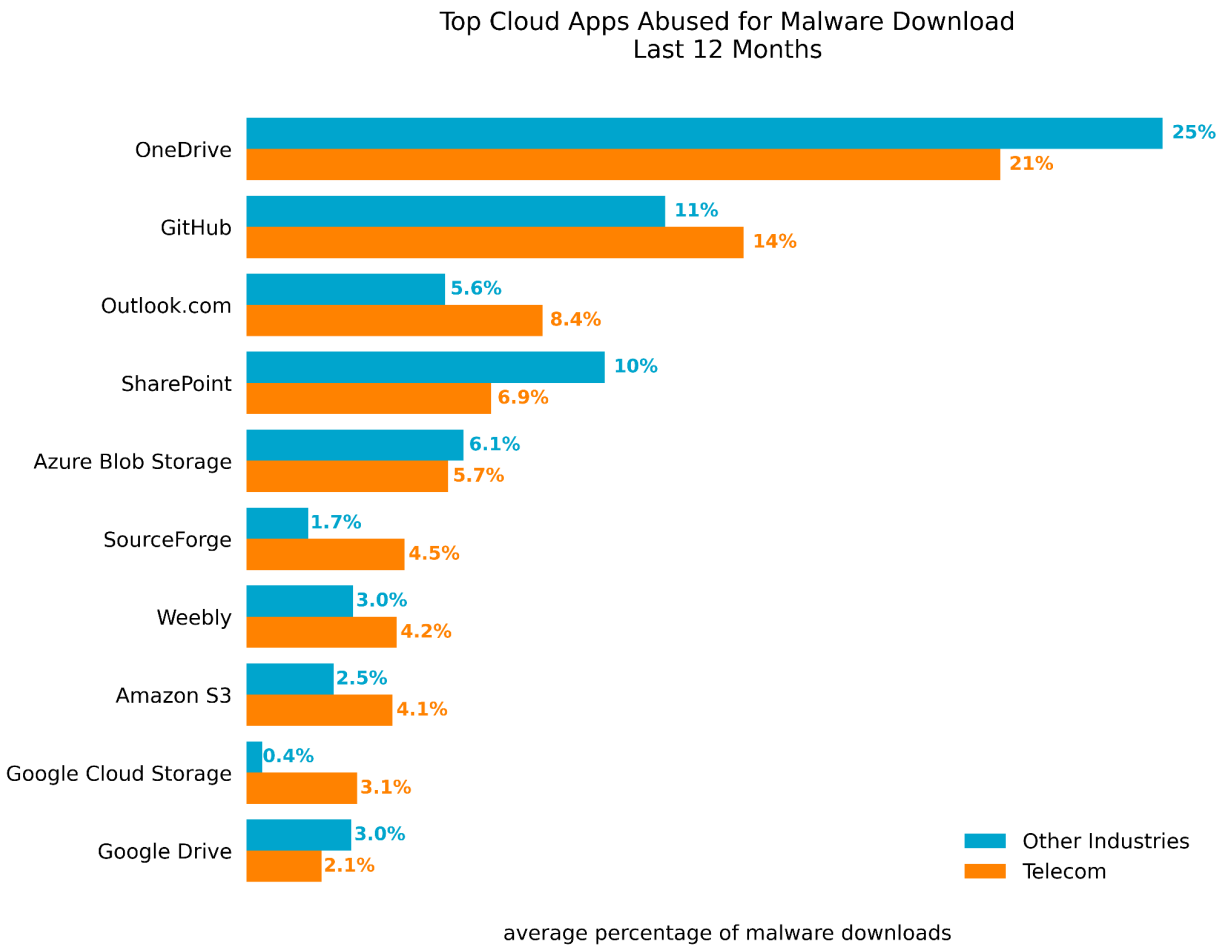


When it comes to malware sourced from the cloud, Telecom leads the pack by a considerable margin of 7 percentage points. These differences among industries are driven by differences in the adversaries targeting those industries and the behavior of users working in those industries.



Cloud Apps Abused for Malware Delivery

Microsoft OneDrive takes the top spot for the most malware downloads in Telecom, although by a smaller margin than other industries. In general, adversaries abuse Microsoft OneDrive because it is the most popular cloud storage app. Meanwhile, people who regularly use Microsoft OneDrive are more likely to click on links to download files shared with them on that platform. Therefore, the number of malware downloads Netskope detects and blocks from Microsoft OneDrive reflects adversary tactics (abusing OneDrive to distribute malware) and victim behavior (their likelihood to click on the links and download the malware). In second place, GitHub is as popular for malware downloads in Telecom as it is in the rest of the world. The other apps in the top 10 are similar to those in other industries with minor differences, including more malware downloads from SourceForce and Google Cloud Storage.



Top Malware & Ransomware Families

This list contains the top 10 malware and ransomware families detected by Netskope targeting users in Telecom in the last 12 months:

- **Botnet.Mirai** is one of the most famous botnets, targeting exposed Linux networking devices. Discovered in 2016, this malware has been targeting a wide range of devices, such as routers, cameras, and other IoT devices. Since its source code leak, the number of variants of this malware has increased considerably.
- **Downloader.BanLoad** is a Java-based downloader widely used to deliver a variety of malware payloads, especially banking Trojans.
- **Downloader.Guloader** is a small downloader known for delivering RAT and infostealers, such as AgentTesla, Formbook, and Remcos.
- **Infostealer.AgentTesla** is a .NET-based remote access Trojan with many capabilities, such as stealing browser passwords, capturing keystrokes, and stealing the clipboard.
- **Infostealer.RedLine** is a malware designed to steal data such as credit card numbers, passwords, VPN and FTP credentials, gaming accounts, and even data from crypto wallets.

- **Phishing.PhishingX** is a malicious PDF file used as part of a phishing campaign to redirect victims to a phishing page.
- **RAT.NjRAT** (a.k.a. Bladabindi) is a remote access Trojan with many capabilities, including logging keystrokes, stealing credentials from browsers, accessing the victim's camera, and managing files.
- **RAT.Remcos** is a remote access Trojan popular among many attackers that provides an extensive list of features to control devices remotely.
- **Trojan.Grandoreiro** is a LATAM banking trojan with the goal of stealing sensitive banking information, commonly targeting Brazil, Mexico, Spain, and Peru.
- **Trojan.ModernLoader** (a.k.a Avatar Bot) collects basic system information and delivers cryptominers, RATs, and other malware payloads.

Recommendations

This report highlighted increasing cloud adoption, including increased data uploaded to, and downloaded from, various cloud apps. It also highlighted an increasing trend of attackers abusing various cloud apps, especially popular enterprise apps, to deliver malware (mostly Trojans) to their victims. Netskope Threat Labs recommends organizations in Telecom 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.
- Use Remote Browser Isolation (RBI) technology to provide additional protection when there is a need to visit websites that fall into 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 (NG-SWG), not considering the significance of the impact of each individual threat. Stats in this report are based on the period starting June 1, 2023 through May 31, 2024. Stats are a reflection of attacker tactics, user behavior, and organization policy.
