April 2023

NETSKOPE THREAT LABS REPORT
SLED

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 users in each segment. The segment highlighted in this report is users in SLED (state, local, and education).

IN THIS REPORT

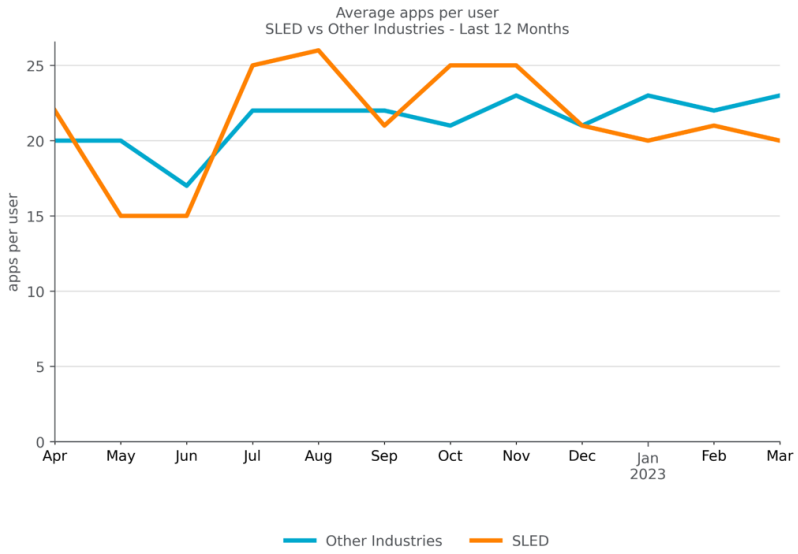
- **Cloud App Adoption:** Enterprise apps such as OneDrive, Sharepoint, and Google Drive are used in SLED with the same frequency as other industries, while social media and video sites are more popular in SLED.

- **Cloud App Abuse:** Attackers are increasingly abusing cloud apps as a malware delivery channel in SLED, where cloud-delivered malware increased from 45% to 52% in the past twelve months, led by malware downloads from popular apps, including Microsoft OneDrive, Weebly, and GitHub.

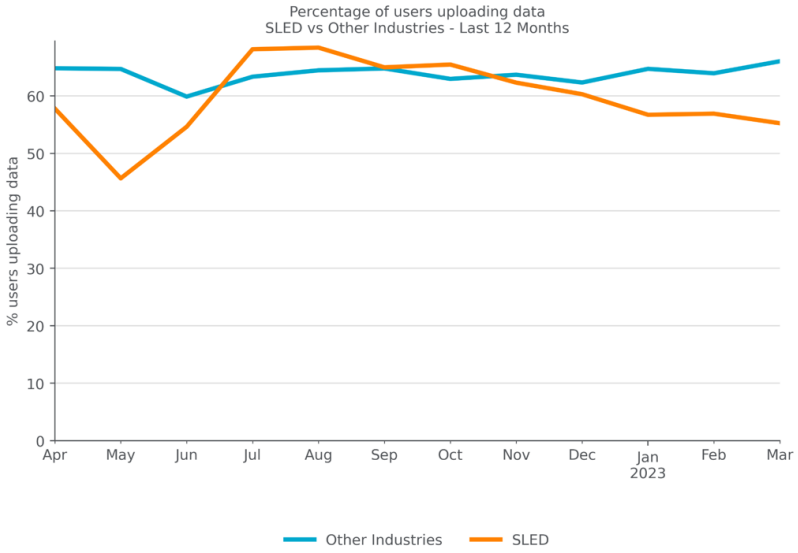
- **Malware & Ransomware:** The most common type of malware blocked by Netskope in SLED were trojans, followed by downloaders and exploits. Emotet, AsyncRAT, and Hive were among the top malware and ransomware families targeting SLED in the past twelve months.

CLOUD APP ADOPTION

Cloud apps are used in SLED and other industries to improve productivity and enable hybrid workforces. The number of apps a SLED user interacts with has fluctuated between 15 and 26 apps over the past twelve months, which is in-line with the averages across other industries. The top 1% of users in SLED interacted with 95 apps per month, compared to 92 apps in other industries.

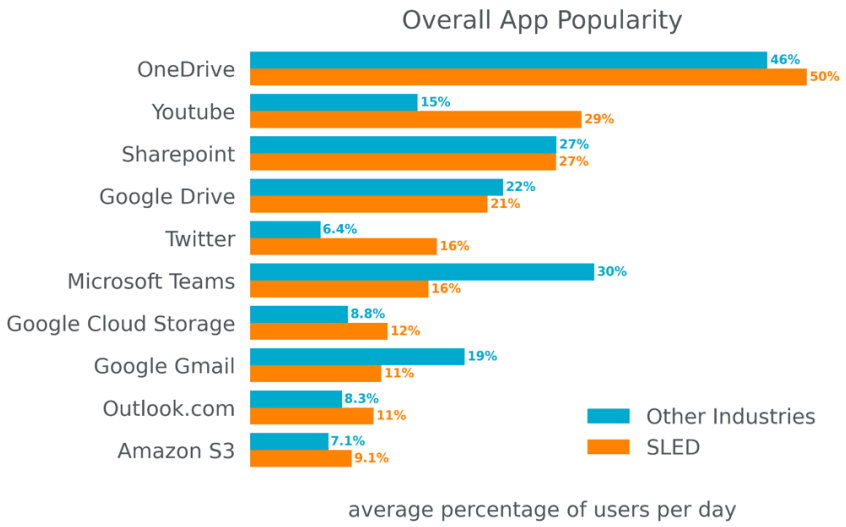


Users in SLED download data from cloud apps almost at the same rate as users throughout other industries, with 95% of users downloading data from cloud apps in SLED each month, versus 94% in other industries. In the last twelve months, 60% of SLED users, on average, uploaded data to cloud apps, compared 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 2% decrease between April 2022 and March 2023.



Most Popular Cloud Apps

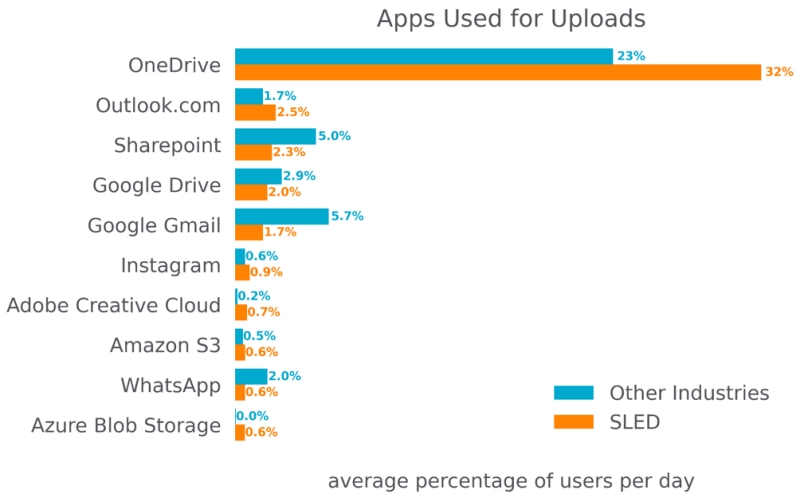
The most popular cloud app among users in SLED is OneDrive, with an average of 50% of users per day. SLED is on par with other industries when it comes to the use of enterprise apps for file sharing/storage, such as OneDrive, Sharepoint, and Google Drive. Social media and video sites are more popular among SLED users than other industries, with YouTube used almost twice as much and Twitter with 2.5x more usage in SLED. Microsoft Teams is much less popular among SLED users when compared to other industries, with nearly half users on average per day.



Top Apps Used for Uploads

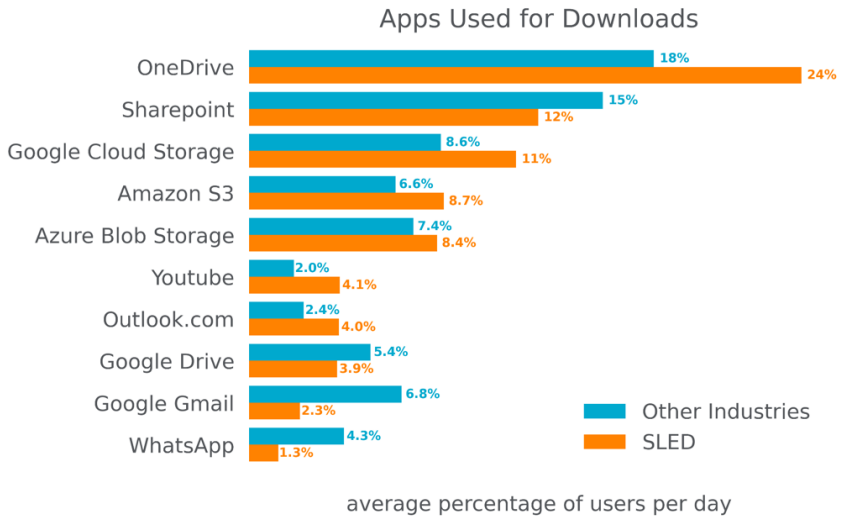
In addition to being the most popular app, Microsoft OneDrive is also the most popular app used for uploads, with 32% of users regularly uploading data on average per day, which is a higher percentage than other industries. Outlook is also popular for uploads in SLED, being used 1.4x more when compared to other industries. Sharepoint is also a popular app for uploads, but way less popular when compared to other industries, with less than half of usage.

Google apps, such as Drive and Gmail are popular among users in SLED, but more popular in other industries, with Gmail with more than triple of usage. WhatsApp is popular in SLED, but it's used more frequently in other industries, with 2% of users on average per day. Adobe Creative Cloud is 3.5x more popular for uploads among users in SLED when compared to other industries, but still used by a very small percentage of users.



Top Apps Used for Downloads

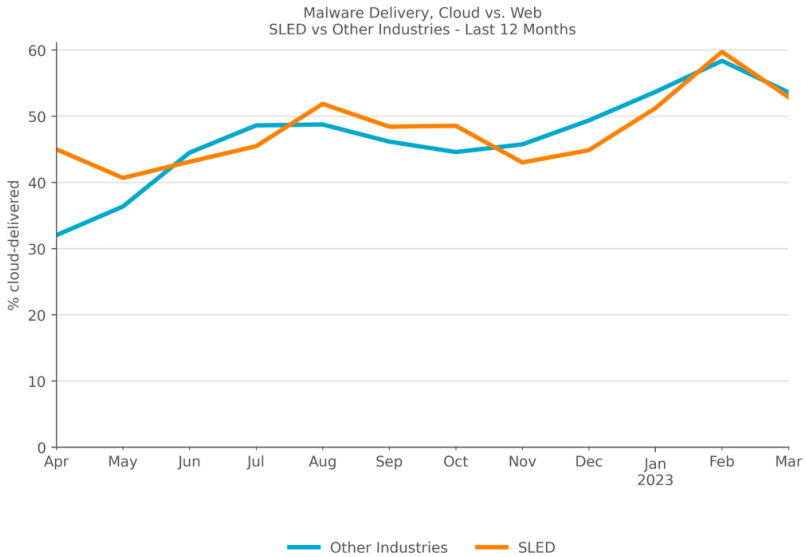
OneDrive leads the most popular cloud apps for downloads by users in SLED, with 24% of users per day on average. In general, cloud apps for file storing/sharing, like OneDrive, Google Cloud Storage, Amazon S3, and Azure Blob Storage, are more popular across the board in SLED when compared to other industries. The only exceptions are Sharepoint and Google Drive, which are more popular in other industries. Google Gmail and WhatsApp are also popular apps in SLED for downloads, but heavily more used in other industries.



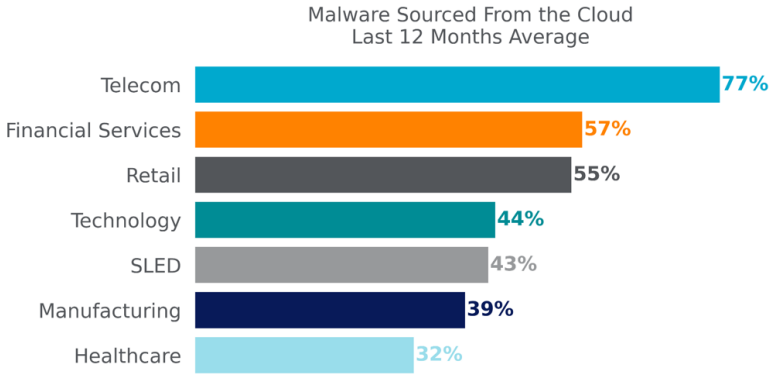
CLOUD APP ABUSE

Cloud Malware Delivery

In the past twelve months, the popularity of cloud malware delivery in SLED organizations increased from 45% in April 2022 to 52% in March 2023. The twelve-month average in SLED organizations is almost the same compared to other organizations, with 43% of malware downloads from users in SLED compared to 48% in other industries. 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.



SLED is average in terms of cloud malware downloads, only one percentage point behind technology and leading both manufacturing and healthcare.

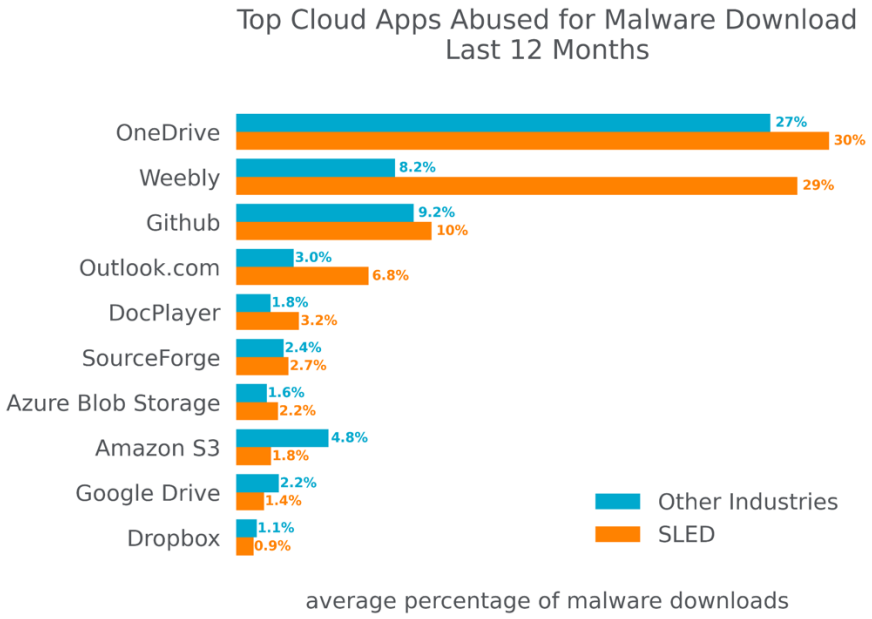


Cloud Apps Abused for Malware Delivery

In the last twelve months, Microsoft OneDrive was the most popular cloud app abused for malware downloads in SLED organizations, representing 30% of all cloud malware downloads. As highlighted earlier in this report, Microsoft OneDrive is also the most popular app among users in SLED, 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 SLED, with 3.5x more downloads when compared to other industries. Software hosting sites (GitHub, SourceForge) are also popular in SLED for malware downloads, with almost the same average compared to other industries.

Outlook users in SLED are downloading malware more than twice when compared to other industries. DocPlayer, which is a cloud app to share online documents, is also popular for malware downloads in SLED, with 3.2% downloads on average in the last twelve months. Other apps abused for malware downloads in SLED include file sharing and storage, such as Azure Blob Storage, Amazon S3, Google Drive, and Dropbox, with only Azure Blob Storage having a higher presence in SLED.



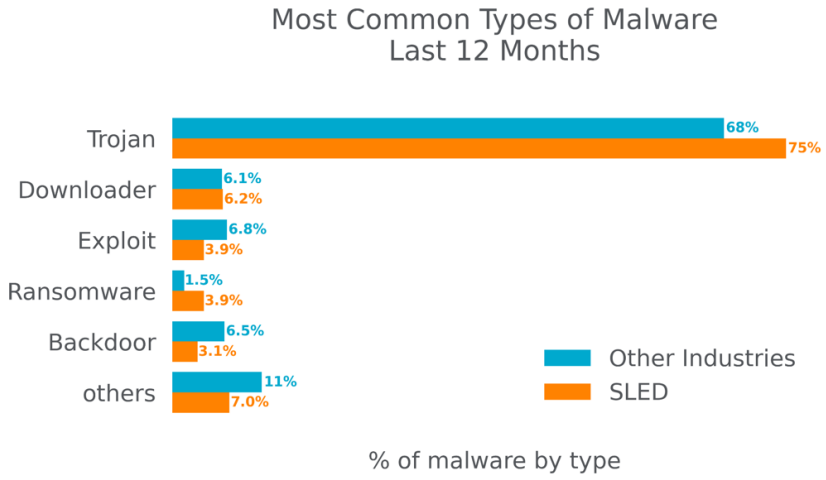
MALWARE & RANSOMWARE

Top Malware Types

The most common malware detected by Netskope in SLED 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.

In 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 MacOS and Windows.

Top Malware & Ransomware Families



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

- **Trojan.Razy** is a Trojan typically distributed via malicious ads disguised as legitimate software, often used to steal cryptocurrency data. Details
- **Trojan.Valyria** (a.k.a. POWERSTATS) is a family of malicious Microsoft Office Documents that contain embedded malicious VBScripts, usually to deliver other malicious payloads. 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
- **Infostealer.ClipBanker** is an infostealer that steals banking information, among other data, and is typically spread via emails and social media. Details
- **RAT.AsyncRAT** is an open-source remote administration tool released on GitHub in 2019, designed to remotely control computers via encrypted connection. Details

- **Botnet.Emotet** is one of the most relevant botnets in the cyber threat landscape, often used to deliver other malware such as TrickBot. Details

- **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

- **Adware.Spigot** is a malware able to hijack browsers on both Windows and MacOS to display misleading advertising. Details

- **Ransomware.Conti** is a Russian-based RaaS (ransomware-as-a-service) group that had its source code leaked in 2021 by a disgruntled affiliate, allowing attackers to create variants or incorporate parts of the code into existing families. Details

- **Ransomware.Hive** is a RaaS (ransomware-as-a-service) group active since 2021, known for targeting critical infrastructure such as healthcare and energy providers. 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 organizations in SLED 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 April 1, 2022 through March 31, 2023. Stats are reflection of attacker tactics, user behavior, and organization policy.