June 2023

NETSKOPE THREAT LABS REPORT
MANUFACTURING

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 Manufacturing.

IN THIS REPORT

- **Cloud App Adoption:** OneDrive is the most popular app among users in manufacturing, followed by Google Drive and Gmail, which are more popular among users in manufacturing than in other industries. Manufacturing lags behind other industries in terms of cloud adoption on average, but is catching up as more users are adopting cloud apps.

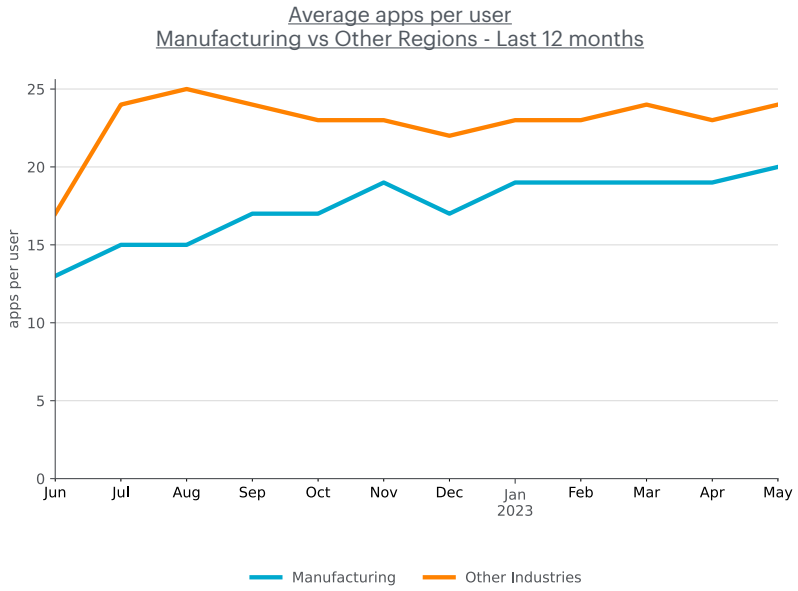
- **Cloud App Abuse:** Attackers are increasingly abusing cloud apps as a malware delivery channel in manufacturing, where cloud-delivered malware increased from 32% to 66% in the past twelve months, led by malware downloads from popular apps, including Microsoft OneDrive, Sharepoint, and GitHub.

- **Malware & Ransomware:** The most common types of malware blocked by Netskope in manufacturing were Trojans, followed by file-based exploits, and downloaders. Emotet, AgentTesla, and BlackBasta were among the top malware and ransomware families targeting manufacturing in the past twelve months.

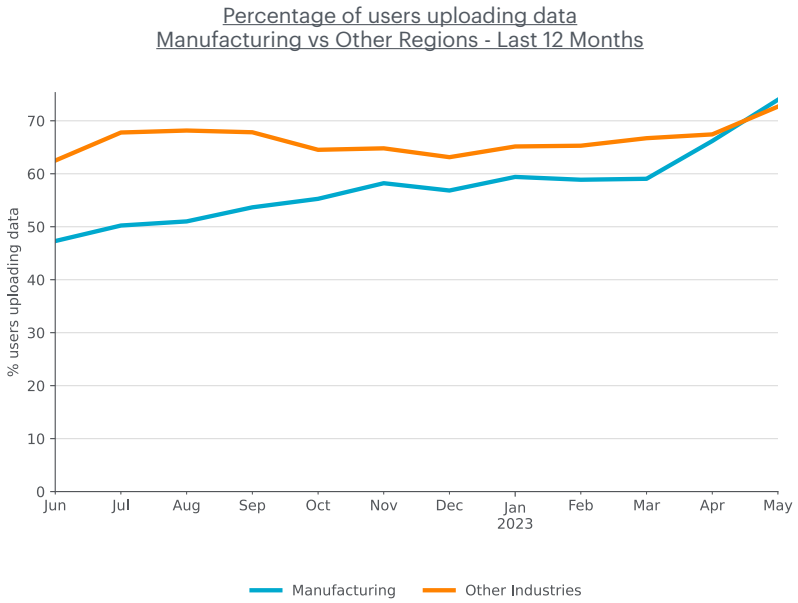
netskope
Threat Labs

CLOUD APP ADOPTION

Cloud apps are used in manufacturing and other industries to improve productivity and enable hybrid workforces. The number of apps a user in manufacturing interacts with has increased from 13 to 20 apps over the past twelve months, lagging behind other industries. The twelve month average of 17 apps in manufacturing lagged behind the average of 23 apps in other industries. The top 1% of users in manufacturing interacted with 73 apps per month, compared to 96 apps in other industries.

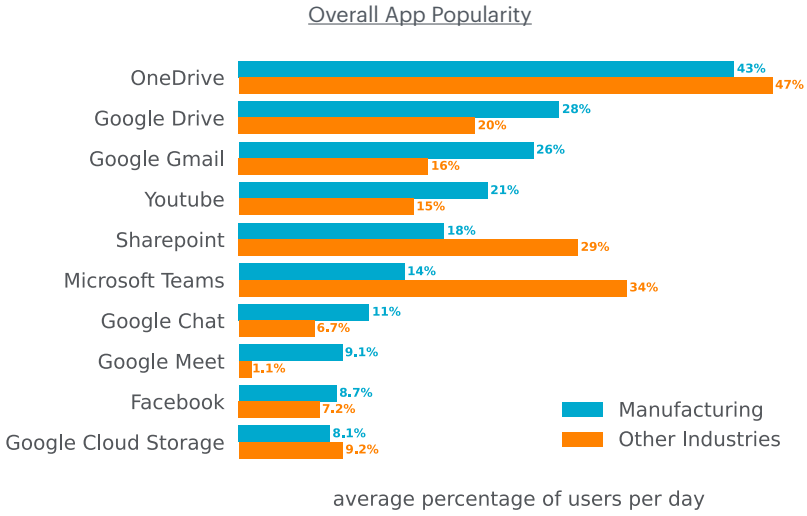


Users in manufacturing downloaded data from cloud apps at almost the same rate as users throughout other industries, with 94% of users downloading data from cloud apps in manufacturing each month, versus 93% in other industries. In the last twelve months, 58% of manufacturing users, on average, uploaded data to cloud apps, compared to 66% of users in other industries. Over the past twelve months, the number of users uploading to cloud apps in manufacturing increased 27% between June 2022 and May 2023, becoming on par with the usage in other industries.



Most Popular Cloud Apps

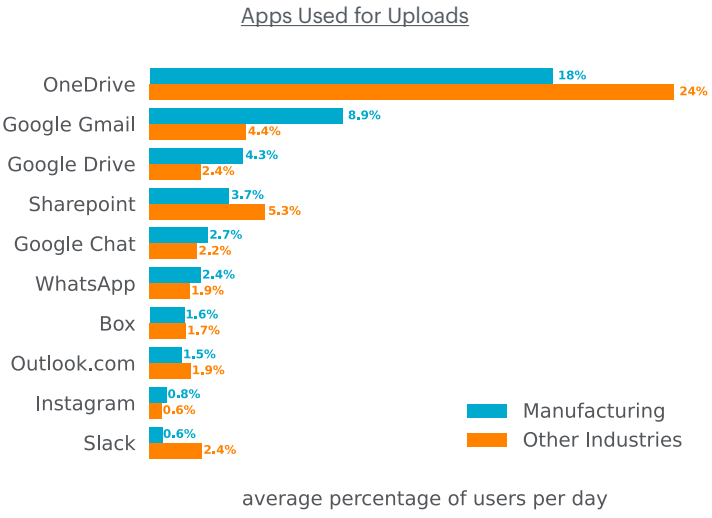
OneDrive is the most popular app in manufacturing and other industries, with an average of 43% and 47% users per day, respectively. Apart from Google Cloud Storage, Google apps are more popular among users in manufacturing than in other industries, especially Google Meet, with 8.3x more use. Microsoft apps are less popular in manufacturing than in other industries, especially Sharepoint, with 11% more usage on average in other industries. YouTube and Facebook are also popular apps among users in manufacturing, with YouTube having 1.4x more usage on average.



Top Apps Used for Uploads

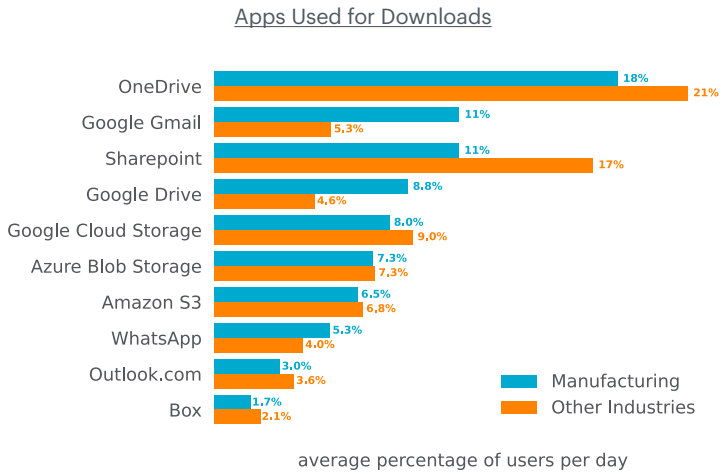
In addition to being the most popular app overall, Microsoft OneDrive is also the most popular app used for uploads, with 18% of users regularly uploading data on average per day, which is a lower percentage than other industries. Google apps are more popular among users in manufacturing for uploads, with Gmail being used twice as much as in other industries. Microsoft apps, like OneDrive, Sharepoint, and Outlook, are more popular in other industries than in manufacturing.

Communication apps are also popular for uploads, with WhatsApp being slightly more popular among users in manufacturing, and Slack more popular in other industries, with 4x more usage on average. Instagram and Box are also popular for uploads in both manufacturing and other industries, with almost the same average of use.



Top Apps Used for Downloads

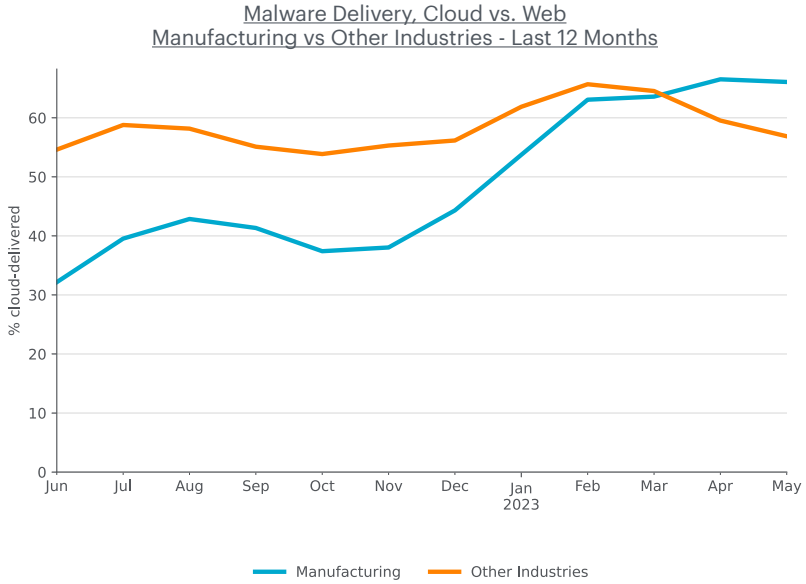
OneDrive leads the most popular cloud apps for downloads by users in manufacturing, with 18% of users per day on average. In general, cloud apps for file storing/sharing, like OneDrive, Sharepoint, Google Cloud Storage, and Amazon S3, are more popular across the board in other industries than in manufacturing. The only exceptions are Azure Blob Storage, which has the same average of downloads, and Google Drive, which like other Google apps, are more popular among users in manufacturing. Other popular apps for downloads in manufacturing include WhatsApp, Outlook, and Box.



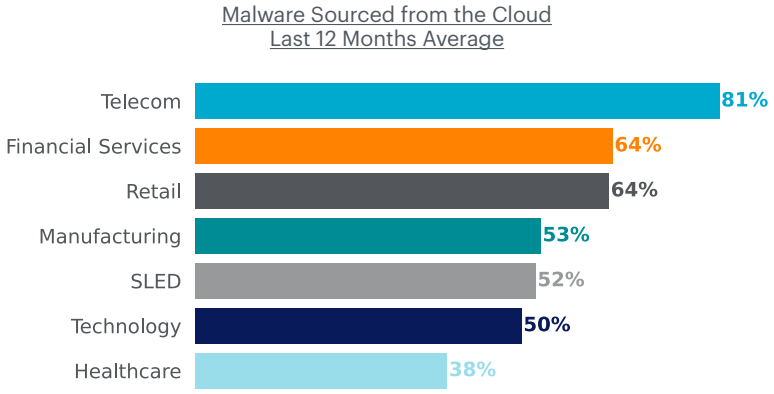
CLOUD APP ABUSE

Cloud Malware Delivery

The popularity of cloud malware delivery in manufacturing organizations has more than doubled, increasing from 32% in June 2022 to 66% in May 2023. The twelve-month average in manufacturing organizations is almost the same compared to other organizations, with 53% of malware downloads from users in manufacturing compared to 58% 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.



Manufacturing is in the middle of the pack in terms of cloud malware downloads on average in the last twelve-months, leading SLED, technology, and healthcare enterprises.

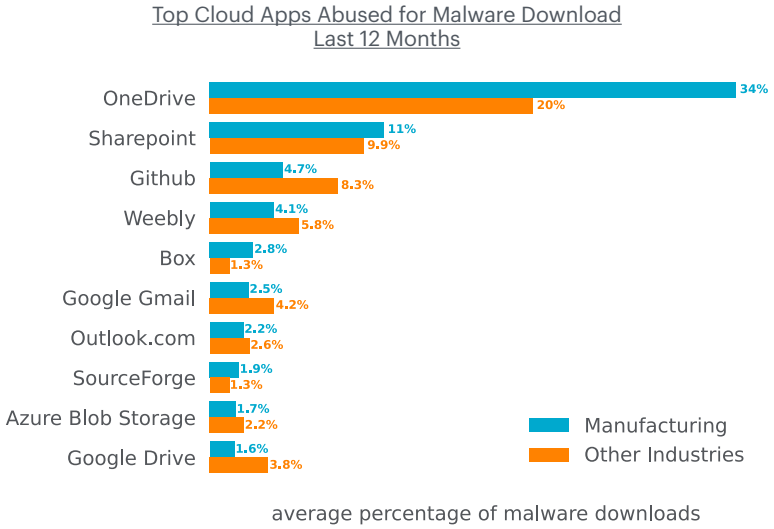


Cloud Apps Abused for Malware Delivery

In the last twelve months, Microsoft OneDrive was the most popular cloud app abused for malware downloads in manufacturing organizations, representing 34% of all cloud malware downloads. As highlighted earlier in this report, Microsoft OneDrive is also the most popular app among users in manufacturing, which makes it both an useful app 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.

Sharepoint is the second most popular app for malware downloads in manufacturing organizations, with 11% of users on average in the last twelve months, a slightly higher number when compared to other industries. Software hosting sites (GitHub, SourceForge) are also popular in manufacturing for malware downloads, though with GitHub being 1.7x more abused in other industries on average.

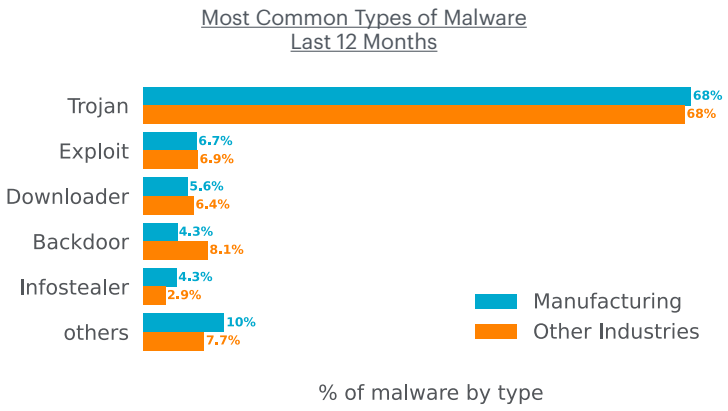
The free web hosting service Weebly is also popular for malware downloads in manufacturing organizations, but slightly more abused in other industries. Other popular apps for malware downloads include file hosting/sharing apps, such as Box, SourceForce, Azure Blob Storage, and Google Drive. Mail apps, like Google Gmail and Outlook, are also popular for malware downloads in manufacturing organizations.



Top Malware Types

The most common malware detected by Netskope in manufacturing 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 file-based exploits, which include documents used to exploit many known vulnerabilities, including CVE-2022-30190 (a.k.a. Follina), CVE-2021-40444, and other vulnerabilities that exploit unpatched versions of Adobe Acrobat, Adobe Reader, Microsoft Office, MacOS, and Linux. The third most common type of malware are downloaders, which like trojans, are also used to deliver other types of malware.



Top Malware & Ransomware Families

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

- **Infostealer.ClipBanker** is an infostealer that steals banking information, among other data, and is typically spread via emails and social media. Details
- **Infostealer.Fareit** (a.k.a Siplog, Pony) is both an infostealer and botnet, stealing credentials from VPNs, browsers, and more. Details
- **Botnet.Emotet** is one of the most prevalent botnets in the cyber threat landscape, often used to deliver other malware such as TrickBot. Details
- **Infostealer.AgentTesla** is a .NET-based remote access trojan with many capabilities, such as stealing browsers' passwords, capturing keystrokes, clipboard, etc. Details
- **Infostealer.QakBot** (a.k.a. Quakbot, QBot) is a modular malware active since 2007 capable of stealing sensitive financial data from infected systems, often delivered via malicious documents. 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

- **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. Details

- **Downloader.BanLoad** is a Java-based downloader widely used to deliver a variety of malware payloads, especially banking Trojans. Details

- **Ransomware.BlackBasta** is a ransomware group that emerged in April 2022 with both Windows and Linux variants, targeting corporate networks. Details

- **Ransomware.BlueSky** is a ransomware family that emerged in 2022 with links to other groups, like Conti, and designed to use multi threads to encrypt files faster. 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 file-based exploits, backdoors, ransomware, and infostealers. Netskope Threat Labs recommends organizations in manufacturing 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 the recommendations above, Remote Browser Isolation (RBI) technology can 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 (SWG), not considering the significance of the impact of each individual threat. Stats in this report are based on the period starting June 1, 2022 through May 31, 2023. Stats are reflection of attacker tactics, user behavior, and organization policy.