May 2023

NETSKOPE THREAT LABS REPORT
ASIA

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 Asia.

IN THIS REPORT

- **Cloud App Adoption:** Cloud adoption in Asia increased by 11% in the past year, where 66% of users regularly upload data to cloud apps, and 92% regularly download data from cloud apps, with Microsoft OneDrive as the most popular app, and WhatsApp used 2x more in Asia than other regions.

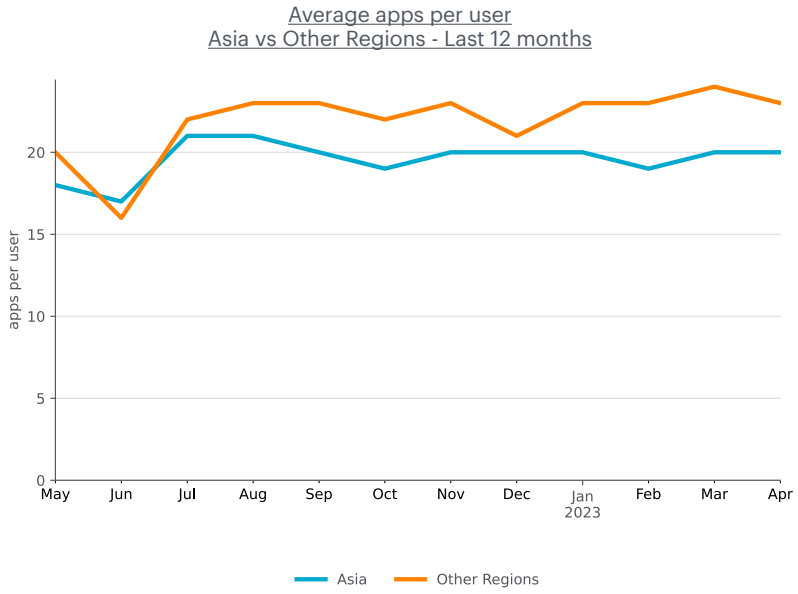
- **Cloud App Abuse:** Attackers are increasingly abusing cloud apps as a malware delivery channel in Asia, where cloud-delivered malware increased from 33% to 58% in the past year, led by malware downloads from popular apps, including Microsoft OneDrive and Google Gmail.

- **Malware & Ransomware:** The most common type of malware blocked by Netskope in Asia were trojans, followed by backdoors, exploits, and downloaders. Emotet, AgentTesla, LockBit, and RedAlert are among the top families blocked by Netskope in Asia in the past year.

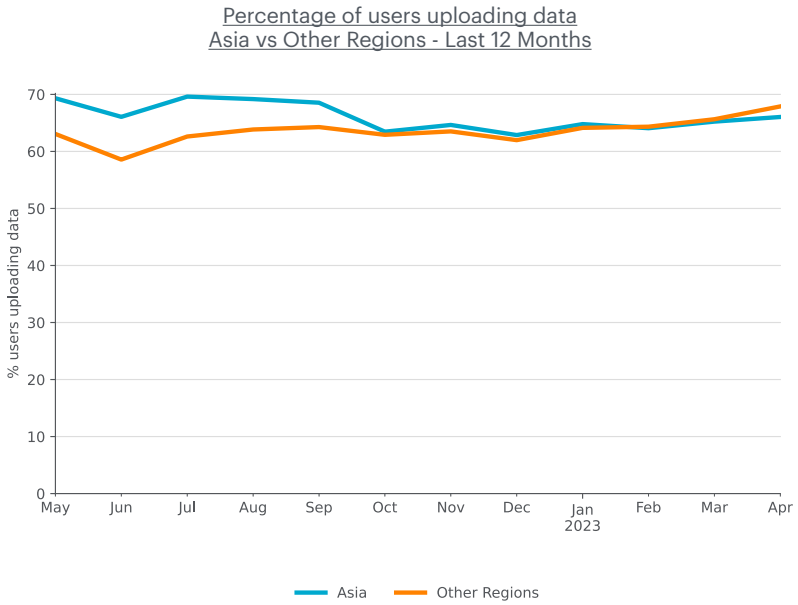
netskope
Threat Labs

CLOUD APP ADOPTION

Cloud app adoption continues to increase in Asia, with enterprises using cloud apps to improve productivity and enable hybrid workforces. The average number of cloud apps an enterprise user in Asia interacts with monthly increased 11% in the past 12 months. The average enterprise user in Asia interacts with 20 apps per month, with the top 1% of users interacting with 79 apps per month. Asia lags behind the rest of the world, where the average user interacts with 22 apps and the top 1% interact with 96 apps in the past 12 months.

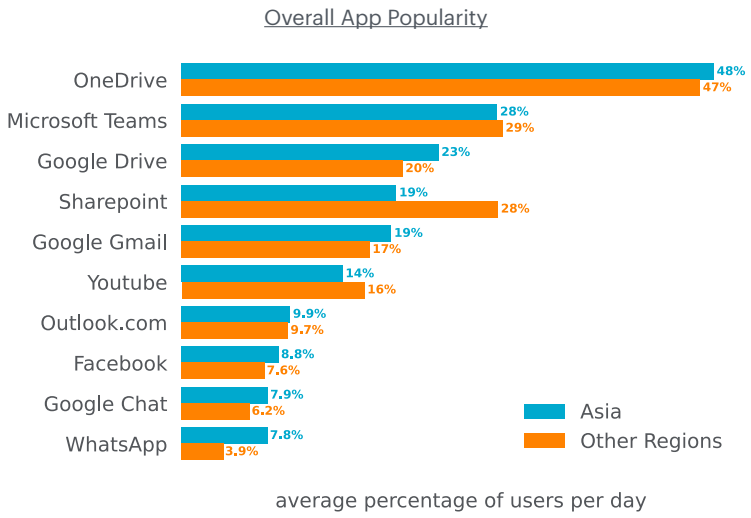


Enterprise users in Asia download data from cloud apps at almost the same rate as users in other regions, with 92% of users downloading data from cloud apps in Asia each month, versus 94% in other regions. Enterprise users in Asia also upload data to cloud apps almost at the same rate as users in other regions with a slightly higher average. Over the past 12 months, 66% of users in Asia uploaded data to cloud apps on average every month, against 64% of users in other regions.



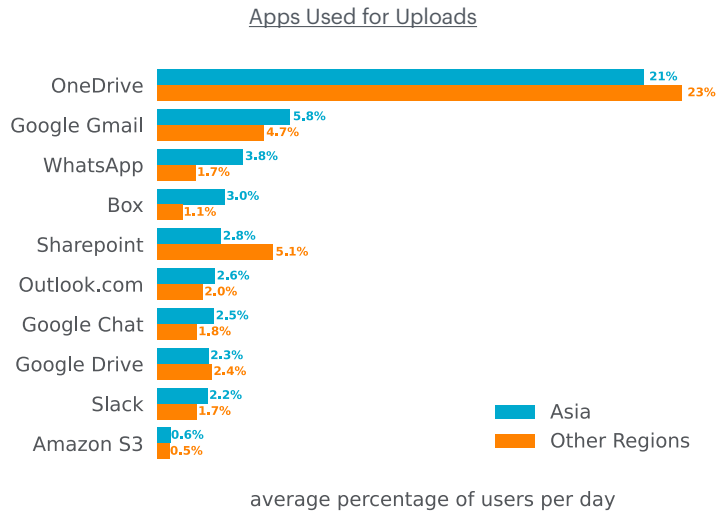
Most Popular Cloud Apps

The most popular cloud apps in Asia are mostly the same as the cloud apps throughout the rest of the world. For example, Microsoft OneDrive is the most popular app both in Asia and the rest of the world. Google Workspace components are slightly more popular in Asia than the rest of the world. Microsoft 365 components (with the exception of Sharepoint) share the same popularity in Asia with the rest of the world. WhatsApp is more popular among users in Asia than other regions, with 2x more usage on average per day.



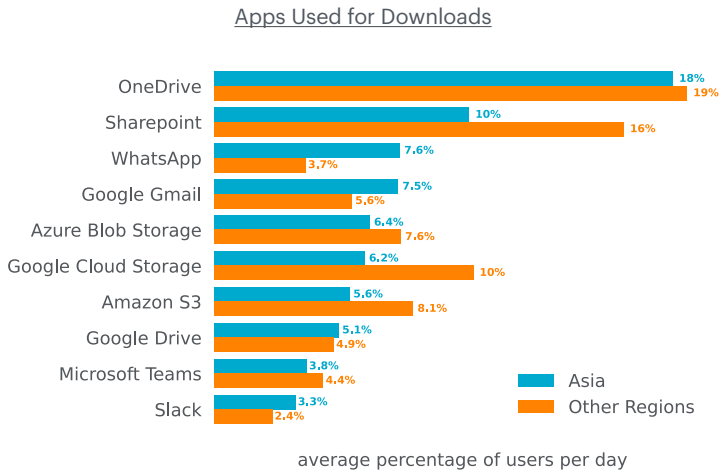
Top Apps Used for Uploads

In addition to being the most popular app among users in Asia, Microsoft OneDrive is also the most popular app used for uploads. Communication apps, such as WhatsApp, Google Chat, and Slack, are more popular for uploads in Asia compared to other regions, especially WhatsApp, with over 2x more usage. Box is more popular for file uploads in Asia compared to other regions, with 3% of users on average per day.



Top Apps Used for Downloads

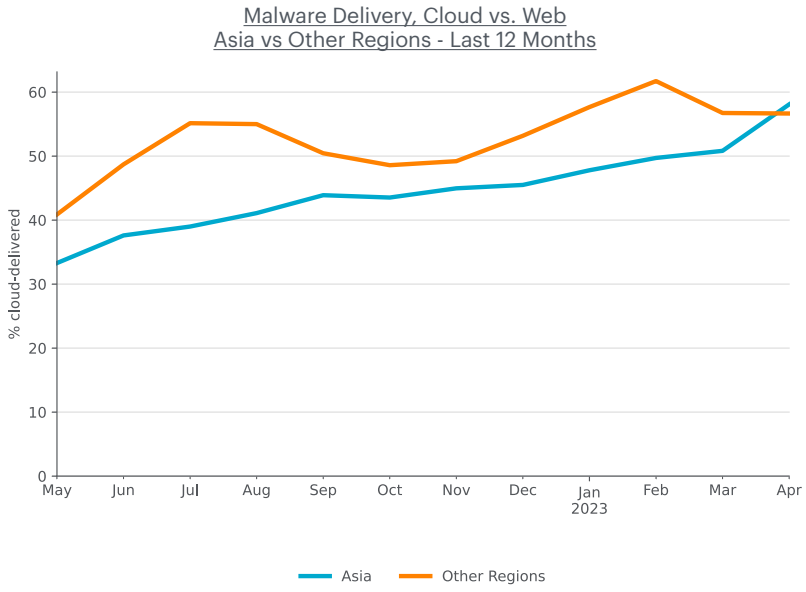
In terms of downloads, Microsoft OneDrive still leads, but with a smaller margin in Asia than the rest of the world. Sharepoint is more popular for downloads in other regions than Asia, with 16% of users on average. Aside from Microsoft Teams, communication apps are more popular in Asia than other regions for downloads, especially WhatsApp, with 7.6% of users on average. Cloud storage apps, except for Google Drive, are more popular in other regions for downloads, with Google Cloud Storage having 10% of users on average.



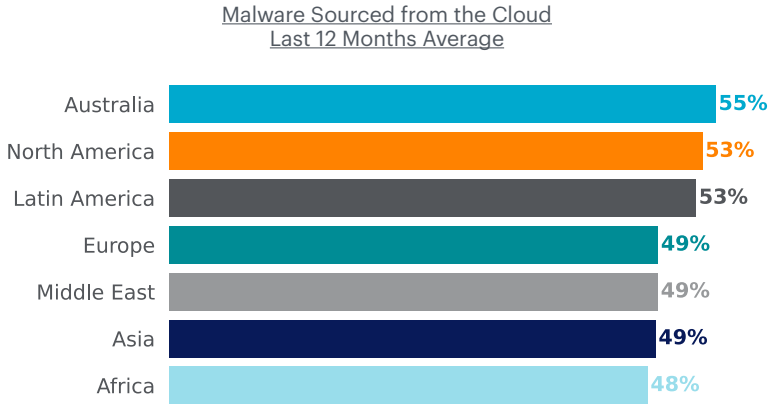
CLOUD APP ABUSE

Cloud Malware Delivery

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. In the past 12 months, the popularity of cloud malware delivery in Asia has closely tracked the tendency of cloud malware delivery in the rest of the world, rising from 33% in May 2022 to 58% in April 2023.

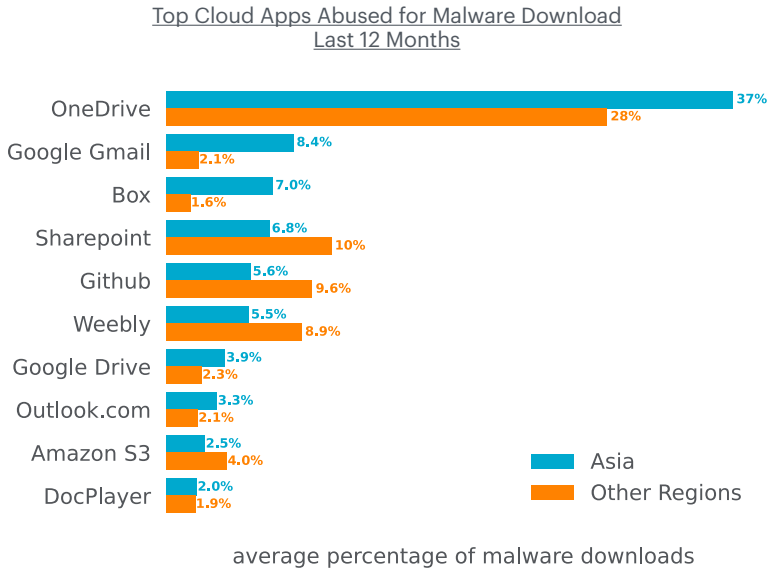


Compared to other regions, Asia is ahead of Africa in terms of cloud malware downloads, and behind other regions of the world, where there is a slightly higher percentage of cloud malware downloads.



Cloud Apps Abused for Malware Delivery

In the last 12 months, Microsoft OneDrive was the most popular cloud app abused for malware downloads in Asia, representing 37% of all cloud malware downloads. As highlighted earlier in this report, Microsoft OneDrive is also the most popular app among enterprise users in Asia, which makes it both a prime choice 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. Google Workspace components have more malware downloads in Asia than in other regions, especially Gmail, with 4x more malware downloads. Box is also a more popular app for malware delivery in Asia compared to other regions, with 7% of downloads on average. Other top apps for malware downloads include collaboration apps (Sharepoint), free software and web hosting sites (GitHub, Weebly), cloud storage apps (Google Drive, Amazon S3), webmail apps (Outlook.com), and file sharing apps (DocPlayer).



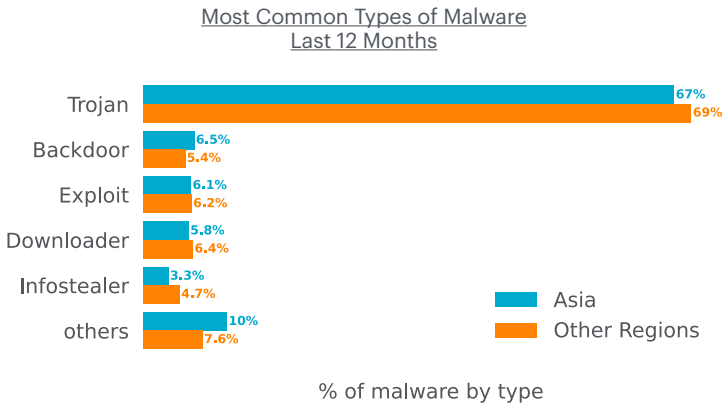
Top Malware Types

The most common malware detected by Netskope in Asia in the last 12 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 backdoors. Like trojans, some malware payloads blocked in this category can also fit other categories, because they provide not only clandestine remote access, but also keylogging, file manipulation, registry manipulation, and other malicious features. Malware in this category include Remcos, Quakbot and NjRAT (a.k.a Bladabindi).

Rounding out the top three are file-based exploits, which include a variety of scripts, documents, and executables that exploit many known vulnerabilities, including Follina (CVE-2022-30190), ZeroLogon (CVE-2020-1472), and other vulnerabilities that exploit unpatched versions of Adobe Acrobat and Reader, Java Runtime Environment (JRE), and Microsoft Office.

The most common types of malware blocked by Netskope in other regions are almost the same as Asia, with 69% of all malware downloads being trojans, followed by 6.4% of downloaders and 6.2% of exploits.



Top Malware & Ransomware Families

This list contains the top ten malware and ransomware families detected by Netskope in Asia in the last 12 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
- **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.Fareit** (a.k.a Siplog, Pony) is both an infostealer and botnet, stealing credentials from VPNs, browsers, and more. Details

- **Infostealer.AgentTesla** is a .NET-based Remote Access Trojan with many capabilities, such as stealing browsers' passwords, capturing keystrokes, clipboard, etc. 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

- **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

- **Ransomware.RagnarLocker** is a RaaS (ransomware-as-a-service) group active since 2020 with different targets around the world, including companies from critical sectors. Details

- **Ransomware.RansomEXX** (a.k.a. Defray777) is a RaaS (ransomware-as-a-service) group responsible for a large attack against the Brazilian Superior Court of Justice in 2020. Details

- **Ransomware.LockBit 3.0** (a.k.a. Black) is the latest version of the LockBit ransomware, emerged in September 2019, becoming one of the most relevant RaaS groups in the world. Details

- **Ransomware.RedAlert** (a.k.a. N13V) is a ransomware operation that emerged in 2022 targeting Windows, and Linux VMWare ESXi servers on corporate networks. 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, infostealers, ransomware, and backdoors. Netskope Threat Labs recommends enterprises with users in Asia 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 May 1, 2022 through April 30, 2023. Stats are reflection of attacker tactics, user behavior, and organization policy.