February 2023

NETSKOPE THREAT LABS REPORT
EUROPE

Starting in February 2023, the Netskope Threat Labs Report will highlight 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 we are highlighting in this inaugural edition of the report is enterprise users in Europe.

IN THIS REPORT

Cloud App Adoption: Cloud adoption in Europe increased by 29% in the past year, where 53% of users regularly upload to, and 92% regularly download data from, cloud apps, with Microsoft OneDrive and Google Drive being the two most popular apps.

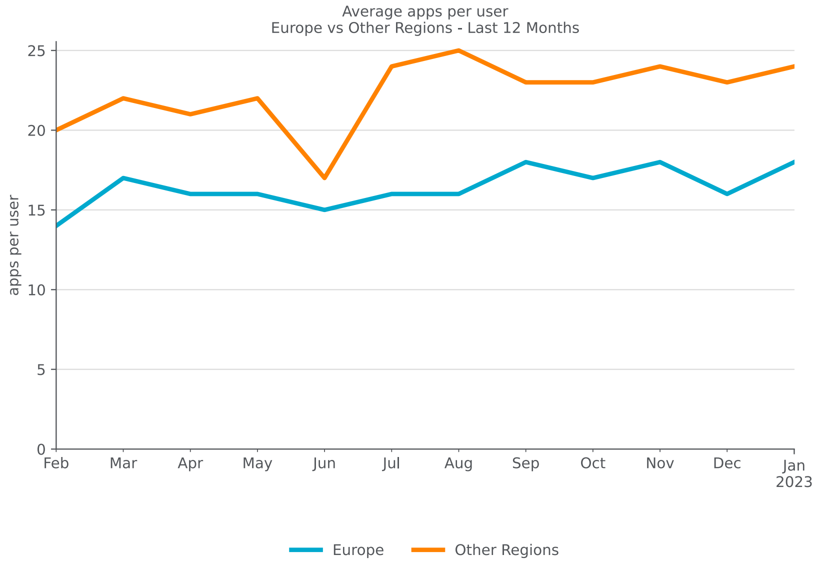
Cloud App Abuse: Attackers are increasingly abusing cloud apps as a malware delivery channel in Europe, where cloud-delivered malware increased from 33% to 53% in the past year, led by malware downloads from popular apps, including Microsoft OneDrive and Google Drive.

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

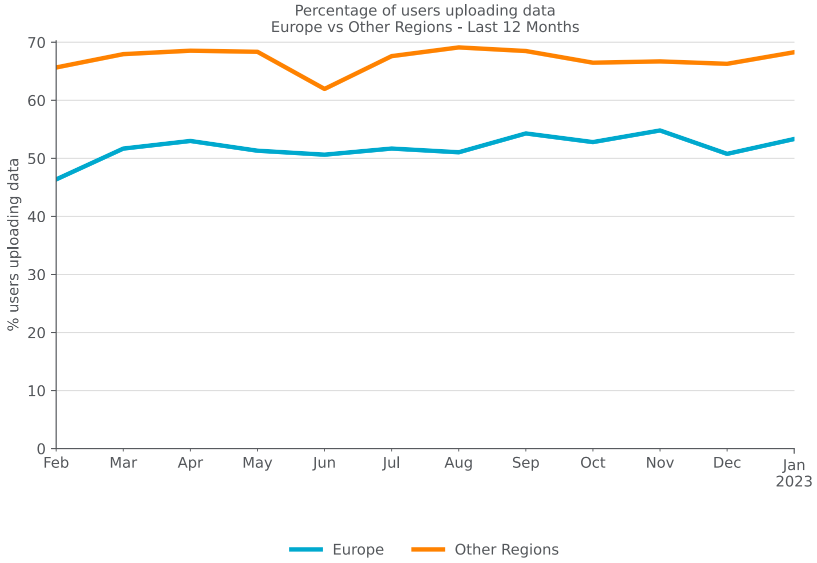
netskope
THREAT LABS

CLOUD APP ADOPTION

Cloud app adoption continues to increase in Europe, with enterprises using cloud apps to improve productivity and enable hybrid workforces. The average number of cloud apps a European enterprise user interacts with monthly increased 29% in the past 12 months. The average European user now interacts with 18 apps per month, with the top 1% of users interacting with 79 apps per month. Europe lags behind the rest of the world, where the average user interacts with 24 apps and the top 1% interact with 102 apps.

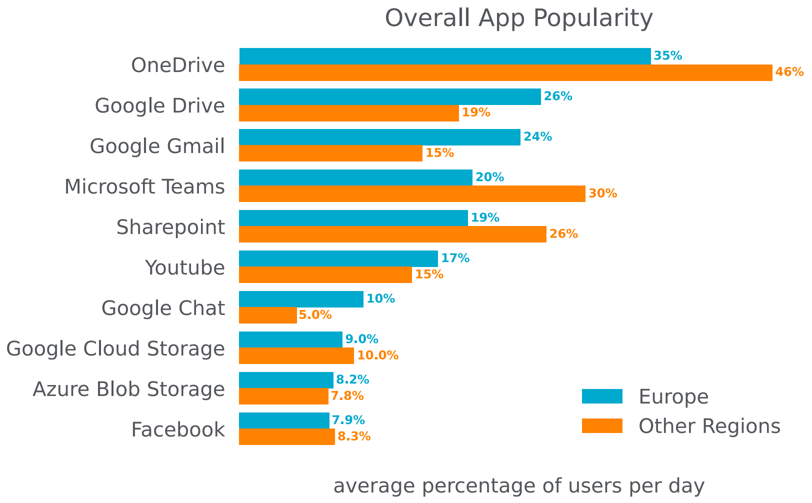


European users download data from cloud apps at the same rate as users throughout the rest of the world, with 92% of users downloading data from cloud apps each month, but lag behind the rest of the world in terms of uploads. 53% of European users upload data to cloud apps each month, while 68% of users elsewhere in the world upload data monthly. Over the past twelve months, Europe chipped away at that gap as uploads to cloud apps increased by 12%.



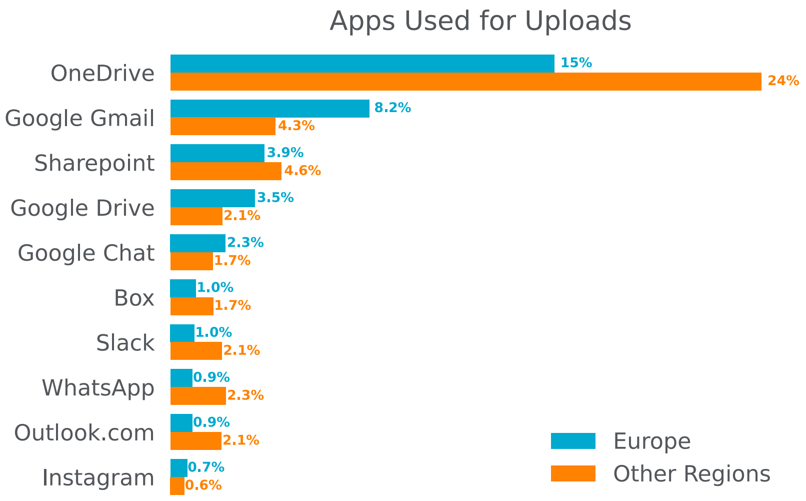
Most Popular Cloud Apps

The most popular cloud apps in Europe 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 Europe and the rest of the world. While OneDrive is still the most popular app in Europe, its lead over Google Drive is much more narrow in Europe than it is in the rest of the world. In fact, all of the Google Workspace components are more popular in Europe than the rest of the world, and all of the Microsoft 365 components are less popular in Europe than the rest of the world, except for Google Cloud Storage and Azure Blob Storage.



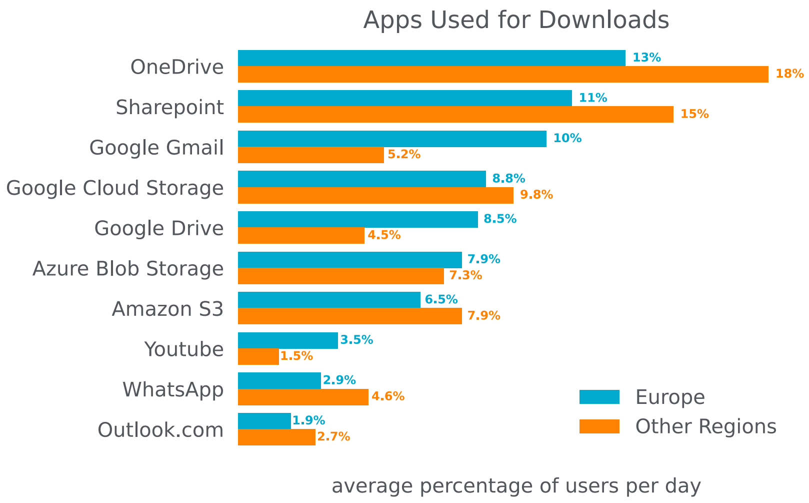
Top Apps Used for Uploads

In addition to being the most popular app, Microsoft OneDrive is also the most popular app used for uploads, but with a more narrow margin in Europe compared to the rest of the world. European enterprise users also upload files to messaging apps, such as Slack and WhatsApp, but less frequently than the rest of the world.



Top Apps Used for Downloads

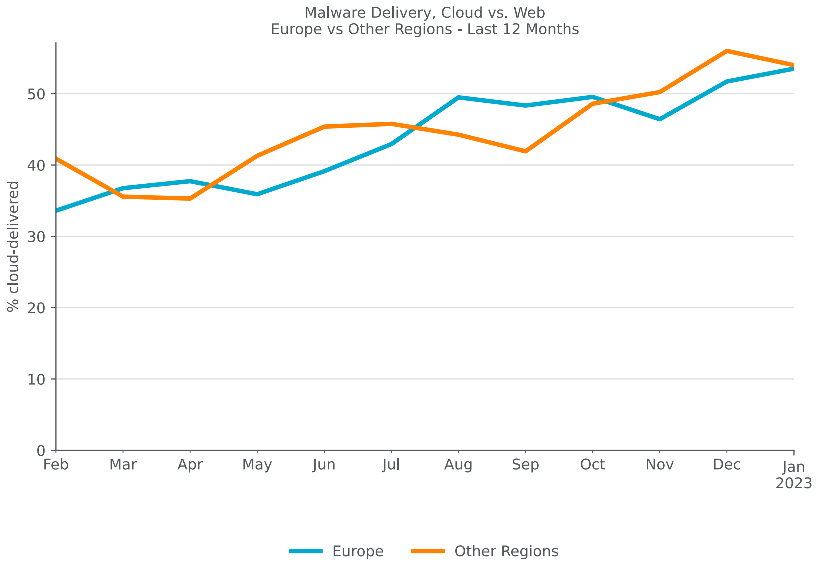
In terms of downloads, Microsoft OneDrive still leads, but with a smaller margin in Europe than the rest of the world. Gmail and Google Drive are also popular for downloading files, averaging almost twice as much usage in Europe compared to other regions. WhatsApp is also one of the most popular apps for file downloads in Europe, but lags behind the rest of the world.



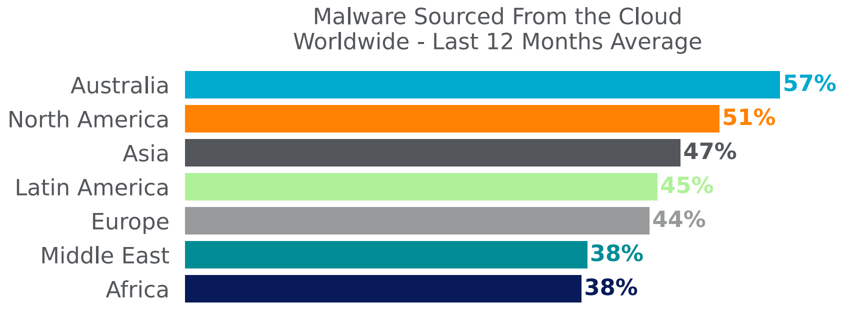
CLOUD APP ABUSE

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 twelve months, the popularity of cloud malware delivery in Europe has closely tracked the popularity of cloud malware delivery in the rest of the world, rising from 33% in February 2022 to 53% in January 2023.

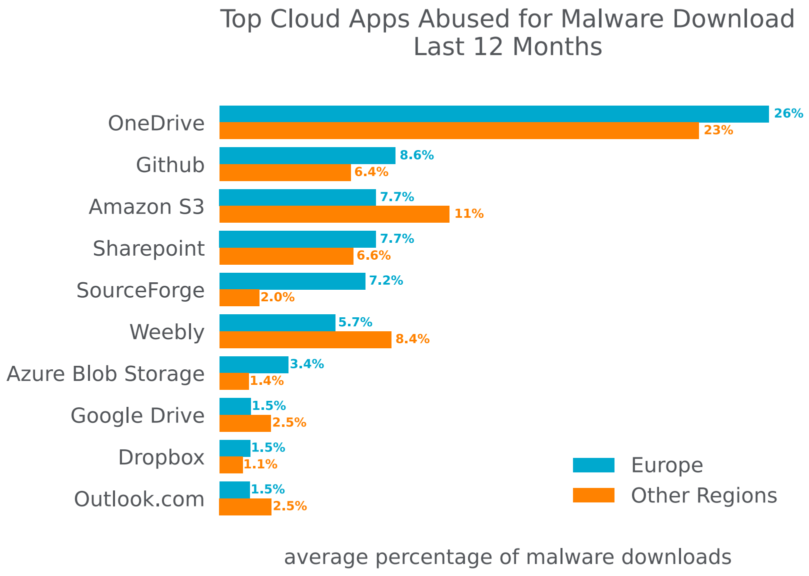


Compared to other regions, Europe is in the middle of the pack in terms of cloud malware downloads, with only the Middle East and Africa having a lower percentage of cloud malware downloads.



Cloud Apps Abused for Malware Delivery

In the last 12 months, Microsoft OneDrive was the most popular cloud app abused for malware downloads in Europe, representing 26% of all cloud malware downloads. As highlighted earlier in this report, Microsoft OneDrive is also the most popular app among enterprise users in Europe, 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. OneDrive's position at the top of this list is a reflection of attacker tactics, user behavior, and company policy. The other top apps for malware downloads include free software hosting sites (GitHub, SourceForge), cloud storage apps (Amazon S3, DropBox, Google Drive, Azure Blob Storage), collaboration apps (Sharepoint), free web hosting services (Weebly), and webmail apps (Outlook.com).



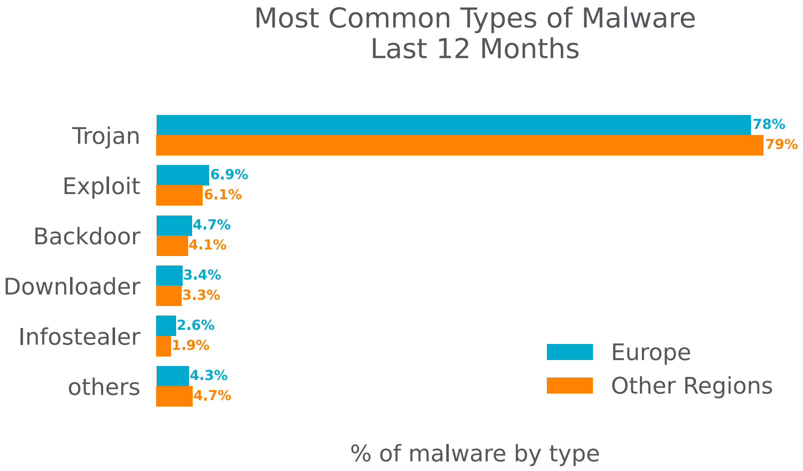
Top Malware Types

The most common malware detected by Netskope in Europe in the last 12 months were Trojans, which are commonly used by attackers to gain 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 includes a variety of scripts, documents, and executables that exploit many known vulnerabilities, including ZeroLogon (CVE-2020-1472) and other vulnerabilities that exploits unpatched versions of Adobe Acrobat and Reader and Microsoft Office.

Rounding out the top three are 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).

We have the same top five malware types blocked by Netskope in other regions, with 79% of all malware downloads being trojans, followed by 6.1% of exploits and 4.1% of backdoors.



Top Malware & Ransomware Families

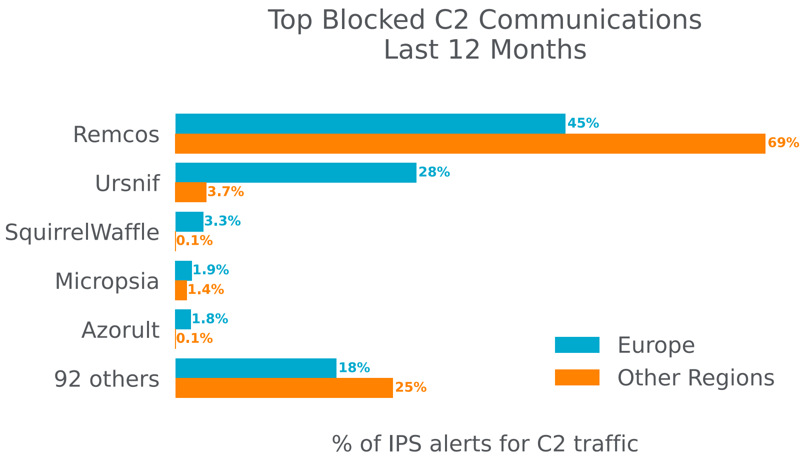
This list contains the top ten malware and ransomware families detected by Netskope in Europe in the last 12 months:

- **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
- **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
- **Infostealer.AgentTesla** is a .NET-based Remote Access Trojan with many capabilities, such as stealing browser's passwords, capturing keystrokes, and stealing the clipboard contents. Details

- **Downloader.Guloader** (a.k.a. CloudEyE) is a small downloader known for delivering RATs and infostealers, such as AgentTesla, Formbook, and Remcos. 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.Quakbot** (a.k.a. QBot) is a modular malware active since 2007 capable of stealing sensitive financial data from infected systems. Details
- **RAT.Remcos** is a remote access trojan that provides an extensive list of features to remotely control devices and is used by many different attackers. Details
- **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. Details
- **Ransomware.BlackByte** is a RaaS (ransomware-as-a-family) group active since 2021 with different targets around the world, such as the San Francisco 49ers in 2022 and critical infrastructure sectors in the US. 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

Command & Control Communication

In the last 12 months, 45% of all C2 Communications detected by Netskope in Europe came from Remcos malware, which is a remote access trojan with many capabilities. Due to its popularity, almost 69% of all C2 communication in other regions were also sourced from Remcos. Ursnif, a banking trojan also known as “Gozi”, took second place in Europe, where it is 7.5x more common than in the rest of the world. In third place, SquirrelWaffle, which is a malware loader commonly used by attackers to deploy other threats, was also more common in Europe than the rest of the world. Apart from Ursnif and SquirrelWaffle, Azorult, which is an information stealer, was also more common among enterprise users in Europe.



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 enterprises in Europe 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 February 1, 2022 through January 31, 2023. Stats are reflection of attacker tactics, user behavior, and organization policy.