netskope

CLOUDY WITH A CHANCE OF MALICE

Forecasting the new era of cloud-enabled threats

BROUGHT TO YOU BY:

netskope

THREAT LABS

EXECUTIVE SUMMARY

The usage of cloud apps in the enterprise continues to rise, with the average number in use increasing by 20% in 2020 and where cloud activity now represents **53% of secure web gateway traffic**. This app growth comes primarily from personal apps and apps with a **"Poor" Cloud Confidence Index™ (CCI)** rating, putting sensitive data at risk. At the same time, attackers continue to abuse cloud services to lend legitimacy to their attacks with cloud-provided trusted domains and valid certificates, exploiting user trust and evading detection.

OF WEB TRAFFIC IS CLOUD RELATED

OF MALWARE IS CLOUD DELIVERED

Research was performed on anonymized usage data collected by the Netskope Security Cloud platform for millions of users from January 1, 2020 through December 31, 2020 relating to a subset of Netskope customers with prior authorization.

REPORT HIGHLIGHTS

- Malware delivery continues to shift into the cloud, with **61% of all malware delivered** via a cloud app.
- **36% of phishing campaigns** target cloud app credentials and **13% of campaigns use phishing lures** hosted in the cloud, as attackers continue to use cloud apps to gain footholds in organizations.
- Malicious Office documents **increased by 58%** in 2020 and now make up **27% of all malware downloads**, using cloud app delivery to evade legacy email and web defenses.
- **83% of users** in the enterprise use personal app instances, increasing the risk of unintentional or unapproved data movement.
- **47.5% of apps** have a **"Poor"** Cloud Confidence Index™ (CCI) rating where the most popular of these is Yahoo Mail.

KEY POINTS

Cloud Use on the Rise

In 2020, the number of apps in use by the average enterprise **increased by 20%**. Of those apps, **47.5% have a "Poor" Cloud Confidence Index™ (CCI) rating**. A "Poor" rating is what Netskope assigns to apps enterprises should avoid using and take steps to migrate to safer app alternatives.

Malware in the Cloud

Malware originating from the cloud continues to grow, with the percentage of **malware delivered using cloud apps topping 61%** at the end of 2020. The most popular apps among enterprise users continue to be the most popular among attackers.

Cloud Phishing

The popularity of cloud apps in the enterprise makes them a popular target for phishing attacks. Cloud apps are now the target of **36% of all phishing campaigns**. While the majority of phishing lures are still hosted on traditional websites, attackers are increasingly using cloud apps, with **13% hosted in cloud apps**.

Malicious Office Documents

Attackers are increasingly using malicious Office documents as Trojans to deliver next stage payloads including ransomware and backdoors. Malicious Office documents represent **27% of all malware downloads detected and blocked** by the Netskope Security Cloud.

Sensitive Data in Personal Apps

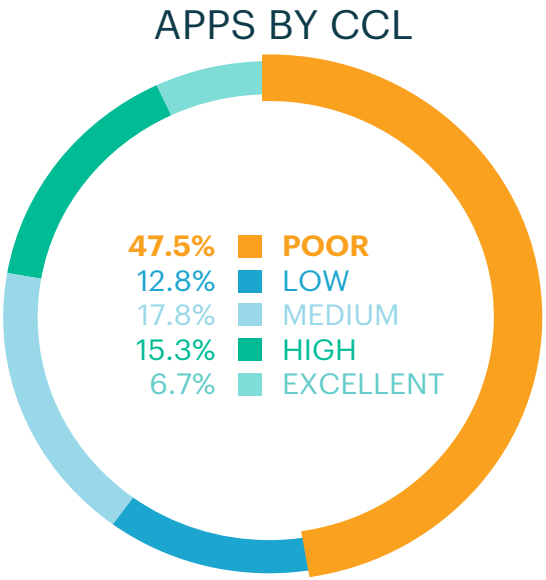
Personal cloud app instances continue to present a data security risk in the enterprise. **83% of users use personal instances of cloud apps** on managed devices, uploading an average of 20 files to personal instances each month.

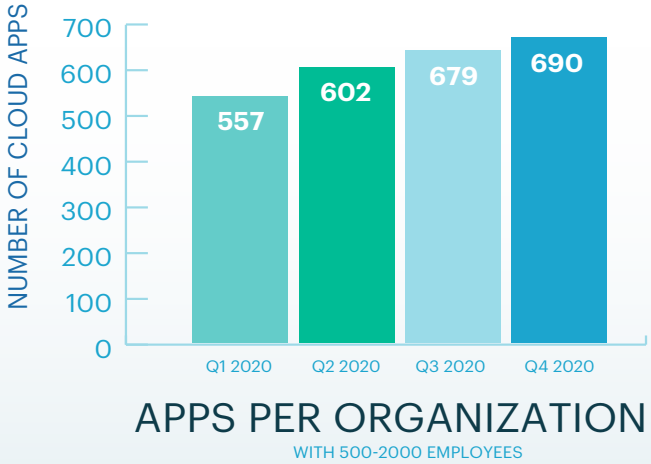
CLOUD USE ON THE RISE

Over the course of the year, the number of **cloud apps in use per organization increased 20%**. Organizations with 500 — 2,000 employees now use on average 690 distinct cloud apps per month, 97% of which are shadow IT apps that are freely adopted by business units and users. Cloud activity now represents **53% of secure web gateway traffic**. Of the cloud apps in use in the enterprise, **47.5%** have a Cloud Confidence Index™ (CCI) rating of "Poor," a rating that Netskope assigns to apps that enterprises should avoid using and instead migrate to safer alternatives. Common reasons for apps being assigned a "Poor" rating include not encrypting data at rest, claiming ownership of user-uploaded data, and lacking compliance and data center standards certifications. On the other end of the spectrum, only 22% of apps have a rating of "High" or "Excellent," a rating reserved for apps reviewed by Netskope and determined to be ready for enterprise use.

The **top five "Poor" CCI rated apps** to which enterprise users upload data are:

1. Yahoo Mail
2. PDF to PNG
3. PDF2Go.com
4. AOL Mail

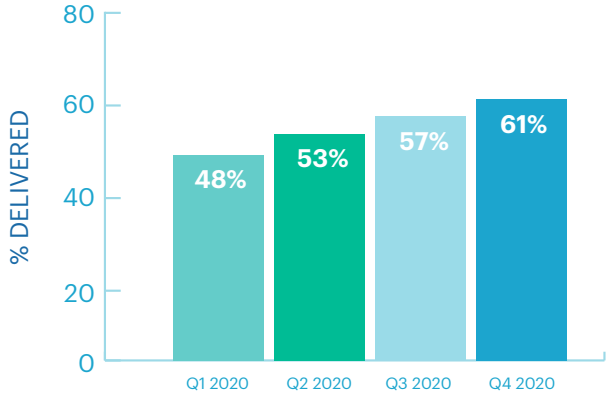




MALWARE IN THE CLOUD

Trojans and next stage malware hosted in cloud apps continue to be popular techniques used by cybercriminals, who seek to leverage the popularity of these apps to avoid blocklists. For example, the GuLoader downloader, one of the top malware delivery mechanisms of 2020, used **Microsoft OneDrive and Google Drive to deliver its payloads**. The percentage of malware delivered via cloud apps increased from **48% to 61% in 2020**.

% MALWARE DELIVERED VIA CLOUD APP

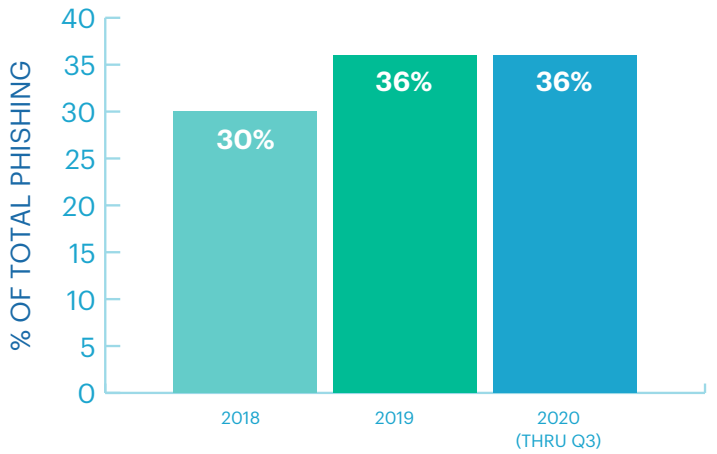


Attackers use a wide variety of apps to target their victims. In 2020, the **Netskope Security Cloud blocked malware hosted in 95 different apps**. However, attackers still tend to favor using apps that are popular in the enterprise. The majority of the blocked malware was uploaded by cybercriminals to the most popular cloud storage and collaboration apps in the enterprise.

CLOUD PHISHING

Cloud app credentials remain a top target for phishing campaigns, with **36% of campaigns in 2020 targeting cloud app credentials**[1]. At the same time, attackers are also finding creative ways to launch phishing campaigns. While the majority of phishing campaigns are still launched using traditional websites, many cybercriminals have begun using cloud apps to host their phishing lures. Cloud-hosted phishing lures often help make a phishing attack look more convincing and bypass traditional phishing detection software. Overall, **13% of phishing pages** in 2020 were hosted in cloud services.

PHISHING FOR CLOUD CREDENTIALS

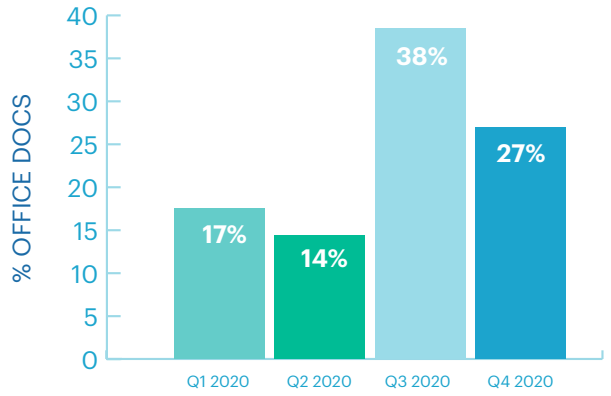


[1] Information sourced from the Anti Phishing Working Group (APWG), https://apwg.org/trendsreports/ https://apwg.org/trendsreports/

MALICIOUS OFFICE DOCUMENTS

Summer 2020 brought with it a massive spike in malicious Microsoft Office documents as the Emotet crew became active again, primarily using malicious Office documents to gain an initial foothold into their victims' networks. Malicious Office documents represented **17% of all malware detected** by the Netskope Security Cloud platform at the beginning of the year, increasing to **38% at the peak** of the Emotet activity in Q3 and **ending the year at 27%**. In 2020, the Netskope Security Cloud blocked downloads of malicious Office documents from 64 different cloud apps, with the majority coming from the most popular cloud storage and collaboration apps used in the enterprise.

% MALWARE DELIVERED VIA OFFICE DOCS



SENSITIVE DATA IN PERSONAL APPS

Personal app instances are widely used in the enterprise, with **83% of users accessing personal app instances** on corporate devices. The average enterprise user uploads 20 files to personal apps each month. Personal app usage in the enterprise increases the likelihood of data being mishandled or leaked. One common type of mishandling occurs when a user downloads data from a corporate app instance and uploads it to a personal app instance.

The top corporate apps from which users copy data to personal instances are:

1. Microsoft OneDrive
2. Box
3. Google Gmail
4. Microsoft Sharepoint
5. Google Drive

And the most popular apps to which users then upload the sensitive data are:

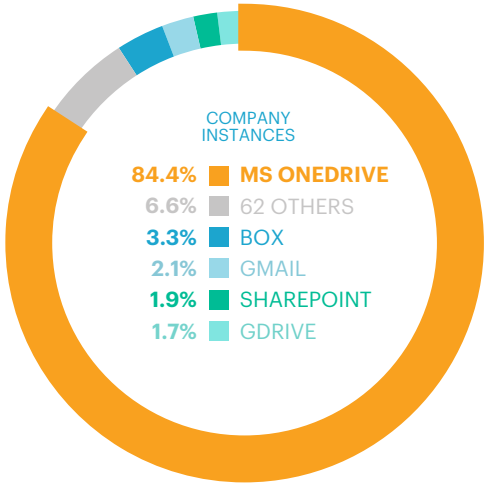
1. Microsoft OneDrive
2. Google Drive
3. Google Gmail
4. iCloud
5. WeTransfer

The most common type of cross-instance movement occurs within **Microsoft OneDrive**, users download data from the corporate instance and upload it to their own personal instance. The types of sensitive data uploaded to personal apps included source code, PII, intellectual property, and passwords and credentials.

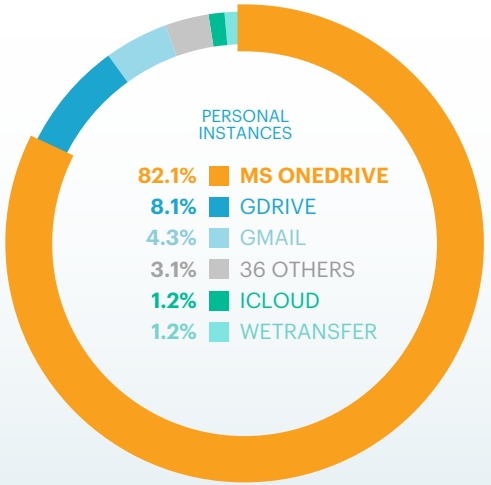
The top five types of files uploaded to personal app instances are:

1. PDFs
2. Office Documents
3. Source code
4. Images
5. Zip files

TOP SENSITIVE DATA DOWNLOADED FROM



TOP SENSITIVE DATA UPLOADED TO



SUMMARY

The scale and complexity of cloud app usage in the enterprise continues to grow with a mix of business-led and personal app instances, along with **widespread usage of "Poor" CCI apps**, presenting a risk to enterprise data security.

Cybercriminals continue to increase their abuse of the most trusted and popular cloud apps, especially for cloud phishing and cloud malware delivery. Leveraging trusted domains, valid certificates, and the practice of allow-listing popular apps to bypass inline defenses only reduces friction for attack success.

Allow/deny no longer works as you need to safely enable cloud and web access because there are many boundary crossings for data movement, plus the delivery of threats that increasingly seek credentials for access to cloud data. The coarse-grained policy is one of the driving factors for why cloud-hosted phishing techniques succeed, due to the lack of precision identifying when the user is visiting a legitimate corporate managed login page or a cloud-hosted form controlled by an attacker. Understanding the data content and context for apps, cloud services, and web user activity is the core of a single-pass SASE architecture for data and threat protection.

CLOUD SECURITY TEN BEST PRACTICES TO PROTECT YOUR DATA AND USERS INCLUDE:

1. Strong authentication and access controls (SSO, MFA, etc.) federated to managed and unmanaged apps
2. Adaptive access controls based on the user, app, instance, device, location, data, and destination to selectively grant access to specific activities
3. Zero Trust Network Access to private apps in data centers and public cloud services to reduce exposure of apps and limit network lateral movement
4. Continuous security assessment of public cloud services to detect misconfigurations and publicly exposed data, plus storage scans for data-at-rest for data and threat protection
5. Cloud inline analysis of managed and unmanaged cloud apps for data context, plus web traffic within a single-pass SASE architecture to enable data and threat protection defenses with a fast user experience
6. Selective and safe enablement of cloud apps based on a third-party risk assessment with the ability to recommend safer app alternatives via real-time coaching
7. Granular policy controls for data protection including data movement to and from apps, instances, users, websites, devices, and locations
8. Cloud data protection (DLP) for sensitive data from internal and external threats
9. Behavior analysis for anomalies, plus confidence index scores for users with event correlation timelines to visualize changes in behavior
10. Real-time coaching to users on activity and data movement with justification collection, proceed/cancel, or warning alerts to change user behavior

LEARN MORE

For more information on cloud-enabled threats and our latest findings from Netskope Threat Labs, go to:
NETSKOPE.COM/NETSKOPE-THREAT-LABS

For more information on tools to help you mitigate risks, please visit:
NETSKOPE.COM/REQUEST-DEMO