SEPTEMBER
2016

WORLDWIDE
EDITION

netskope

# CLOUD REPORT

## **43.7** PERCENT OF CLOUD MALWARE KNOWN TO DELIVER RANSOMWARE

More than half of malware-infected files are shared with others

# REPORT HIGHLIGHTS

- **43.7** percent of cloud malware types make up some of the most common delivery vehicles for ransomware. They include Javascript exploits and droppers, Microsoft Office macros, and PDF exploits.
- **55.9** percent of cloud malware files discovered in sanctioned apps are shared with internal or external users, or publicly.
- Enterprises have an average of **977** cloud apps in use, compared to 935 last quarter.
- Microsoft still leads with the most apps in the top 20 list; collaboration app Slack makes its debut on the list.

# EXECUTIVE SUMMARY

In this Netskope Cloud Report™, we've compiled the most interesting trends on cloud app adoption and usage based on aggregated, anonymized data from the Netskope Active Platform™. Report findings are based on usage seen across millions of users in hundreds of accounts globally and represent usage trends from April 1 through June 30, 2016.

The focus of this quarter's report is on ransomware and the increasingly popular types of cloud malware that deliver ransomware. We found that of the various malware types detected in cloud apps, 43.7 percent of them are common delivery vehicles for ransomware. These common types of cloud malware that deliver ransomware are: Javascript exploits and droppers, Microsoft Office macros, and PDF exploits. We augment the list of cloud malware types this quarter to include PDF exploits and Linux malware. Javascript exploits and droppers made up 17.1 percent of malware detected, Microsoft Office macros were 15.8 percent, PDF exploits comprised 10.8 percent, backdoors 23.1 percent, Linux malware 18.4 percent, and finally Other was 14.8 percent. Ranging from one to hundreds of pieces of cloud malware at each organization, for enterprises infected with malware, the average amount found in cloud apps was 26 pieces of malware. 55.9 percent of the malware was shared with others, including internal or external users, or publicly, a significant increase from last quarter's 26.2 percent.

The average number of cloud apps in use per enterprise increased again to 977 from 935 last quarter. 94.7 percent of cloud services are not enterprise-ready, a negligible increase from last quarter's 94.6 percent. Microsoft Office 365 OneDrive for Business took the top spot in our quarterly top-used cloud apps list, for the first time beating out Facebook in terms of app sessions. Office 365 apps again had a strong showing on the list with Outlook.com and SharePoint taking the number 2 and 11 spots, respectively. For the first time ever, Slack appears on the list at number 20.

In terms of activities, view, share, and download were the top activities in Cloud Storage apps. Download was the top activity in HR and Collaboration apps this quarter, while share and edit nabbed the top spots for Business Intelligence and Finance, respectively. Delete just edged out other activities such as upload and view in Finance, a good reminder for compliance-oriented companies to gain visibility into Finance apps that may affect them in terms of Sarbanes-Oxley compliance, etc.

Looking into DLP violations this quarter, Cloud Storage unsurprisingly remains the top app category for DLP violations at 76.5 percent, followed by Webmail at 18.6 percent, and a combination of Collaboration and Social making up the remaining 4.9 percent. Upload was the top activity associated with policy violations, with 43.4 percent, follow by send, download, and other at 38.1 percent, 15.2 percent, and 3.3 percent, respectively. The majority of DLP violations involved personally-identifiable information (PII) at 53.4 percent. Protected health information (PHI) made up 14.9 percent, payment card industry (PCI) data 10.1 percent, Source Code 13.6 percent, and Other was 8.0 percent.

# **43.7** PERCENT OF CLOUD MALWARE TYPES COMMONLY DELIVER RANSOMWARE

This quarter, we augment the list of cloud malware types that the Netskope Threat Research Labs maintains to include PDF exploits and Linux malware. Javascript exploits and droppers, Microsoft Office macros, and PDF exploits make up 43.7 percent of the total detected cloud malware. Backdoors and Linux malware rose this quarter from 4.9 percent and negligible last quarter to 23.1 percent and 18.4 percent, respectively. The Other type at 14.8 percent consists of mobile malware, spy- and adware, Mac malware, and more.

Javascript exploits and droppers, Microsoft Office macros, and PDF exploits are some of the most common ransomware delivery vehicles and as such, we recommend security teams focus on addressing these threats. With these threats often delivered through phishing and email attacks, security teams should consider training sessions for employees on spotting suspicious emails and not opening attachments from unknown sources or suspicious email addresses. Within a cloud context, files that have been encrypted can easily affect other users when they are in sync folders – following a similar path as the fan-out model we described in our February 2016 Cloud Report. We also recommend using a cloud access security broker (CASB) to detect and remediate ransomware that affects files in cloud applications, as well as enabling the versioning function in Box, Dropbox, Microsoft OneDrive, Google Drive, and other file-sharing applications in order to roll encrypted files back to their last known good version and fully recover from ransomware attacks.

Enterprises that found malware in cloud apps had an average of 26 pieces of malware. The figure ranged from one to hundreds, with one in ten enterprises actually having sanctioned apps laced with malware. Finally, this quarter had 55.9 percent of malware-infected files shared with others, including internal or external users, or publicly. In terms of severity, 80.3 percent of detections were categorized as “high” severity, 5.5 percent were “medium,” and 14.2 percent were “low.”

**26**

average pieces of cloud malware in enterprises

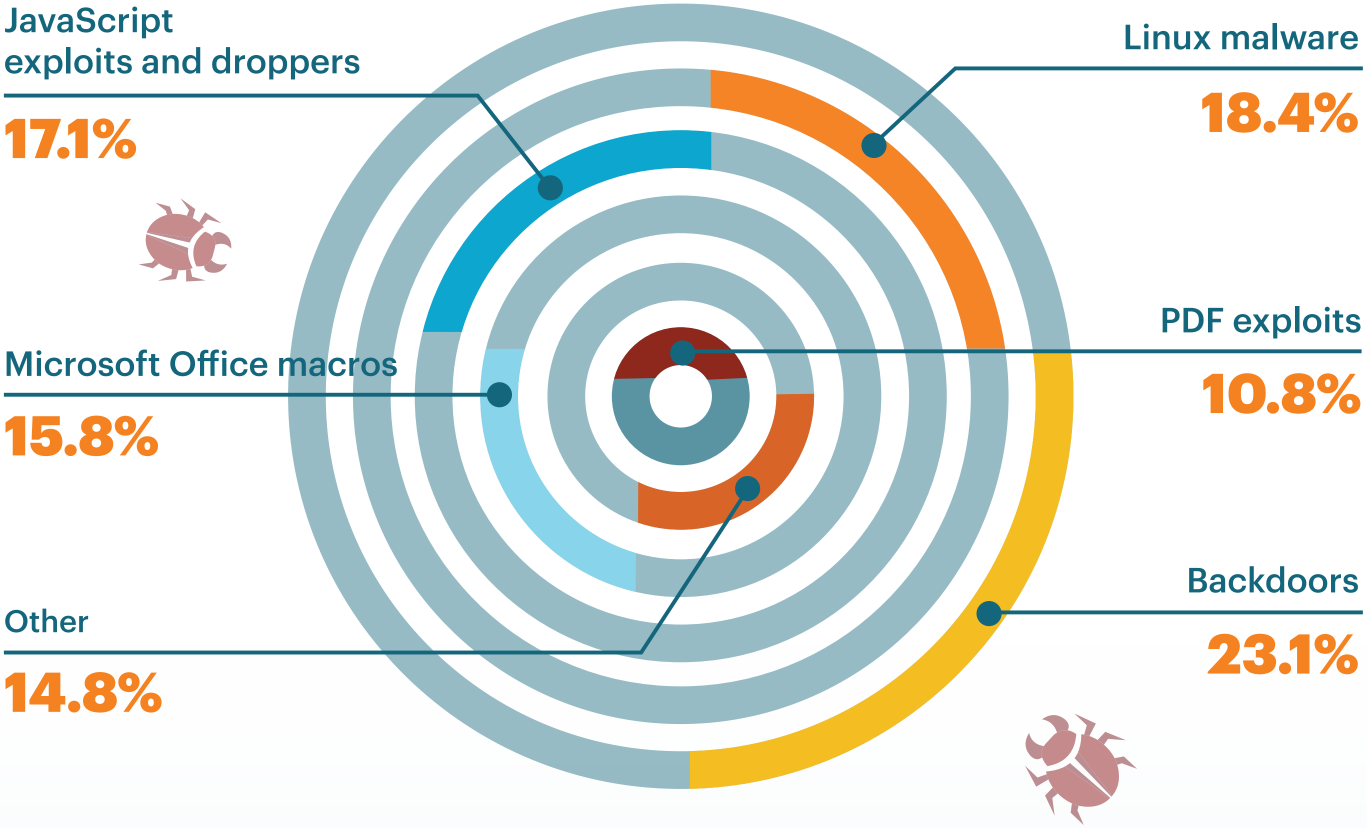
**55.9**

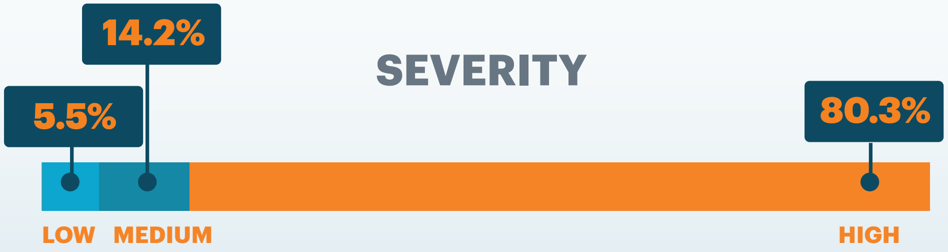
percent of malware-infected files shared with others, including internal or external users or publicly

**43.7**

percent of malware detection types are common ransomware delivery vehicles

# TYPES OF CLOUD MALWARE DETECTED



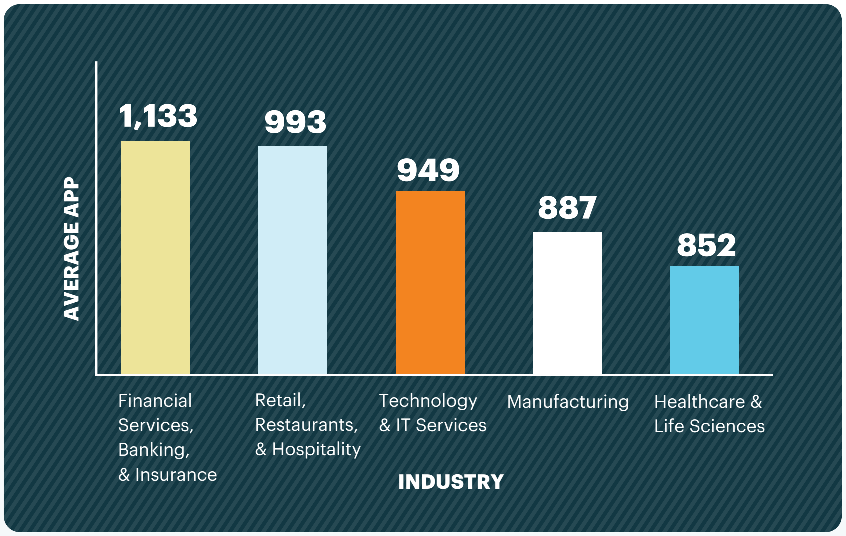


# 977 CLOUD APPS PER ENTERPRISE

Last quarter's 935 average number of apps per enterprise increased again to 977 this quarter. 94.7 percent of these apps are not enterprise-ready, earning a rating of "medium" or below in the Netskope Cloud Confidence Index™ (CCI).

This quarter, Financial Services, Banking, and Insurance remains on top as the industry with the highest average number of cloud apps used. Retail, Restaurants, and Hospitality surged ahead to second this quarter while there were slight decreases in the others. On average, as we onboard new customers, we've noticed that these numbers have remained steady with only slight deviations from customers who actively encourage cloud use balancing customers who place more restrictions on how the cloud is used with granular policy setting on the Netskope Active Platform.

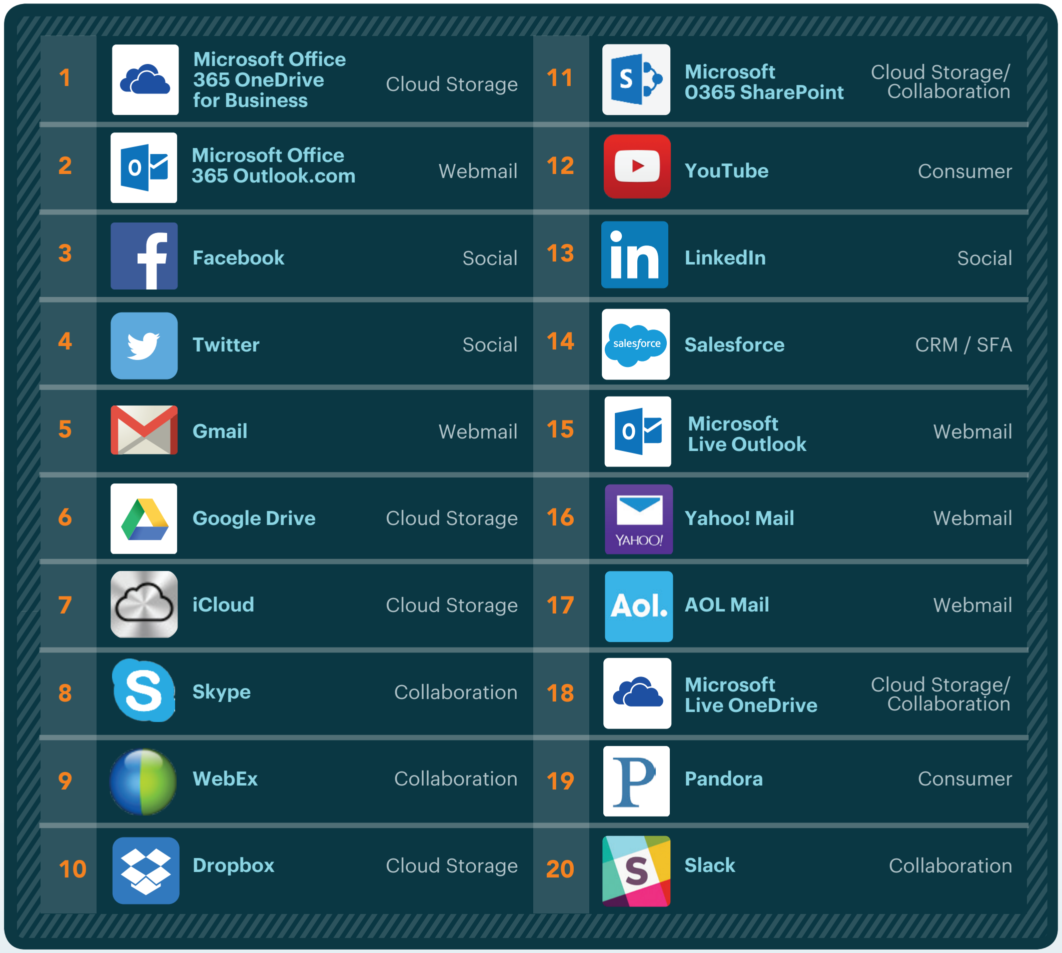
The Marketing category has the highest amount used per enterprise at 103 apps, ahead of the other categories. This is follow by Collaboration and Productivity apps at 71 and 65, respectively. And per our CCI, most categories have greater than 90 percent of apps that are not enterprise-ready. Cloud Storage remains the exception as it is usually a category for which enterprises take time to do due diligence before sanctioning.



| CATEGORY | # PER ENTERPRISE | % NOT ENTERPRISE-READY |
|---|---|---|
| Marketing | 103 | 97% |
| Collaboration | 71 | 90% |
| Productivity | 65 | 99% |
| Finance/Accounting | 60 | 96% |
| HR | 54 | 96% |
| CRM / SFA | 36 | 94% |
| Social | 31 | 92% |
| Software Development | 31 | 96% |
| IT/Application Management | 30 | 98% |
| Cloud Storage | 29 | 77% |

# MICROSOFT CONTINUES TO DOMINATE IN PRODUCTIVITY APPS

This quarter, Microsoft has 6 apps in the top 20 apps list, including Office 365 apps, Skype, and LinkedIn. Facebook was actually overtaken this quarter by Microsoft, which is a first. In this list, Slack cracks the top 20. Security teams should keep in mind that sensitive information might be exposed in Collaboration apps that are gaining in popularity with enterprises, such as Slack. Besides visibility and control of sensitive data within high-profile apps, security teams will need to note what ecosystem apps are integrated and sharing data with those popular apps, and place the appropriate access and data controls in them as well so sensitive data are not leaked via an app's ecosystem.



| | | | | | |
|---|---|---|---|---|---|
| 1 | Microsoft Office 365 OneDrive for Business | Cloud Storage | 11 | Microsoft 0365 SharePoint | Cloud Storage/ Collaboration |
| 2 | Microsoft Office 365 Outlook.com | Webmail | 12 | YouTube | Consumer |
| 3 | Facebook | Social | 13 | LinkedIn | Social |
| 4 | Twitter | Social | 14 | Salesforce | CRM / SFA |
| 5 | Gmail | Webmail | 15 | Microsoft Live Outlook | Webmail |
| 6 | Google Drive | Cloud Storage | 16 | Yahoo! Mail | Webmail |
| 7 | iCloud | Cloud Storage | 17 | AOL Mail | Webmail |
| 8 | Skype | Collaboration | 18 | Microsoft Live OneDrive | Cloud Storage/ Collaboration |
| 9 | WebEx | Collaboration | 19 | Pandora | Consumer |
| 10 | Dropbox | Cloud Storage | 20 | Slack | Collaboration |

# TOP CLOUD ACTIVITIES

The top activities in the Netskope Active Platform are send, create, edit, login, download, invite, view, share, upload, and post, respectively. Netskope normalizes more than 50 possible cloud activities across apps within categories and even across categories, so whether a user shares a file from a Cloud Storage app or a report from a Business Intelligence one, each of those are recognized as a share activity. This is useful in understanding risk, auditing user activity, and being able to say deterministically whether a data policy violation has occurred. It is also useful in isolating policy enforcement to a risky activity like share, rather than only being able to allow or block an app. Examining cloud app activities in the context of the app category, we call out the top three activities besides login for each of five important business app categories, Cloud Storage, HR, Business Intelligence, Finance, and Collaboration.

What's interesting in this quarter's cloud activity section is that in Finance, "Delete" just edged out other activities such as upload, view, and share. This is a good reminder that for companies with strict compliance requirements such as financial services with Sarbanes-Oxley, security teams need to audit the activity of employees in apps that contain sensitive data and possible place appropriate controls to mitigate risk.

### Top Activities in Cloud Storage Apps

1. View
2. Share
3. Download

### Top Activities in Finance Apps

1. Edit
2. Create
3. Delete

### Top Activities in HR Apps

1. Download
2. Create
3. Edit

### Top Activities in Collaboration

1. Download
2. View
3. Creat

### Top Activities in Business Intelligence Apps

1. Share
2. View
3. Download

# TOP POLICY VIOLATIONS IN THE NETSKOPE ACTIVE PLATFORM

Beyond measuring usage and activity, we also look at policy violations within cloud apps. Policies can be enforced based on a number of factors, including user, group, location, device, browser, app, instance, category, enterprise-readiness score, DLP profile, activity, and more. Through data abstraction and normalization of those factors, we're able to discern the apps, categories, and activities surrounding a violation. Policies observed include blocking the download of PII from an HR app to a mobile device, alerting when users share documents in Cloud Storage apps with someone outside of the company, and blocking unauthorized users from modifying financial fields in Finance apps.

Here are the top activities globally that constituted a policy violation per cloud app category, with DLP violations noted where they apply. Just as activities can vary between apps, policy violations involving those activities can vary. For example, a policy violation involving downloading from a Cloud Storage app can be the improper downloading of a non-public press release, whereas in a CRM/SFA app, it could signal theft of customer data by a departing employee.

| APP CATEGORY | Download | Upload | Post | View | Login | Send | Share | Delete | Edit |
|---|---|---|---|---|---|---|---|---|---|
| Cloud Storage | 4! | 5! | 8 | 1 | 7 | – | 2 | 6 | 3! |
| Collaboration | 2! | 4! | 8! | 1 | 7 | 9 | 3 | 6 | 5 |
| CRM and SFA | 4! | 7! | 3! | 6 | 2 | 9 | 1 | 8 | 5 |
| Finance/ Accounting | 7 | 5 | – | 3 | 2 | – | 6 | 4 | 1 |
| HR | 3 | 5 | – | 1 | 2 | – | 7 | 6 | 4 |
| Productivity | 2 | 7! | – | 5 | 1 | – | 4 | 6 | 3 |
| Social | 7! | 6! | 3! | 1 | 2 | – | 8 | 5 | 4! |
| Software Development | 3 | 5 | 8 | 2 | 4 | – | 7 | 6 | 1 |
| Webmail | 4! | 5! | 6! | 3 | 9 | 1! | 8 | 7 | 2 |

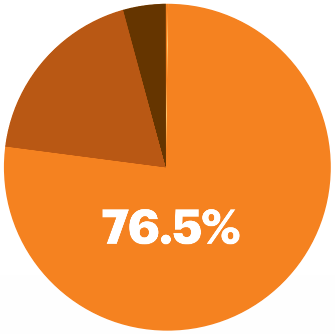
! Policy violation included in data loss prevention profile

**1** Indicates highest occurrence of policy-violating activity for the category

# CLOUD DLP POLICY VIOLATIONS

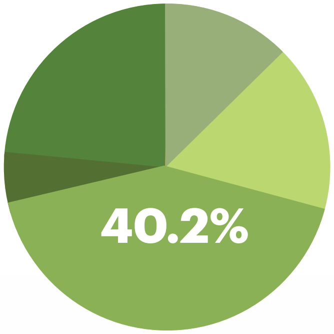
This quarter, Cloud Storage continues to make up the majority of DLP violations at 76.5 percent, followed by Webmail at 18.6 percent, and other app categories making up the final 4.9 percent. This is expected and is worth noting as security teams prioritize security policies for various apps – the focus should be first on Cloud Storage and Webmail.

Also of note, we take a look at an industry level cut this quarter of DLP violations in the total files of each industry. Manufacturing had the highest at 24 percent of total files constituting a violation, followed by Technology and IT Services at 15 percent and Healthcare and Life Sciences at 11 percent. Retail, Restaurants, and Hospitality and Financial Services, Banking, and Insurance round it out at 8 percent each. For the top two industries, DLP violations can consist of confidential documents like design plans or source code, highlighting the importance of proper access controls and cloud DLP policies to protect sensitive information.



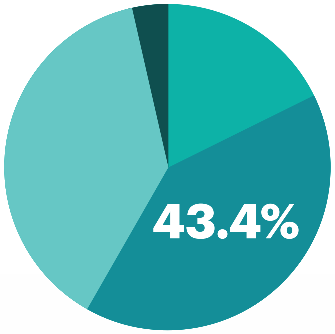
## CATEGORY

- Cloud Storage **76.5%**
- Webmail **18.6%**
- Other (e.g., CRM/SFA, Social, and Collaboration) **4.9%**



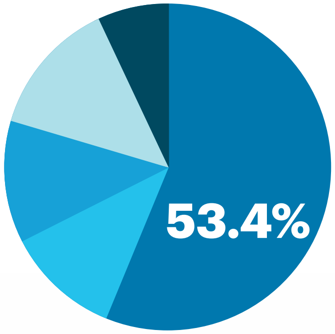
## INDUSTRY

- Retail, Restaurants and Hospitality **40.2%**
- Technology and IT Services **23.6%**
- Healthcare and Life Sciences **19.5%**
- Manufacturing **11.6%**
- Financial Services, Banking, and Insurance **5.1%**



## ACTIVITY

- Upload **43.4%**
- Send **38.1%**
- Download **15.2%**
- Other (including view) **3.3%**



## TYPE

- PII **53.4%**
- PHI **14.9%**
- Source Code **13.6%**
- PCI **10.1%**
- Other (including Confidential and Profanity) **8.0%**

# THREE QUICK WINS FOR ENTERPRISE IT

1 Implement security training and programs to guard against cloud threats and cloud malware such as ransomware. Store mission-critical data in Cloud Storage apps with versioning turned on for easy roll-back of files in case of a ransomware attack.

2 With the rising popularity of collaboration and messaging apps such as Slack, don’t forget to track ecosystem apps associated with them to reduce leak of sensitive data.

3 Enterprises should govern activities such as uploading and sharing within cloud apps to ensure sensitive data such as PII, PHI, PCI, and more are properly handled and in compliance with your organization’s rules and regulations.