netskope
THREAT LABS

October 2021

Netskope Threat Labs Report

IN THIS REPORT

| **Cloud-enabled threats:** Google Drive remains the app from which Netskope blocked the most malware, despite an 11-point decrease from September.

| **Malware:** Box made the top five apps from which Netskope blocked malicious Office document downloads.

| **Ransomware:** President Biden stated that the US will bring together 30 countries to jointly crack down on ransomware gangs.

TOP STORIES

This section lists the top cybersecurity news in the last month.

Joint effort to stop ransomware gangs

US President Joe Biden stated that the US will bring together 30 countries to jointly crack down on ransomware gangs. Details

$5.2 billion USD of crypto transactions attributed to ransomware

US FinCEN has attributed $5.2 billion worth of outgoing Bitcoin transactions to the top 10 commonly reported ransomware variants. Details

Ransom Disclosure Act

According to the new legislation proposal titled the ‘Ransom Disclosure Act’, victims of ransomware attacks in the US may have to report any payments to hackers within 48 hours. Details

Civil Cyber-Fraud Initiative

The US Department of Justice’s new Civil Cyber-Fraud Initiative states that government contractors are accountable in a civil court if they fail to meet required cybersecurity standards. Details

EU to stop anonymous domain registrations

The European Union is drafting legislation to end anonymous domain registrations on the continent. Details

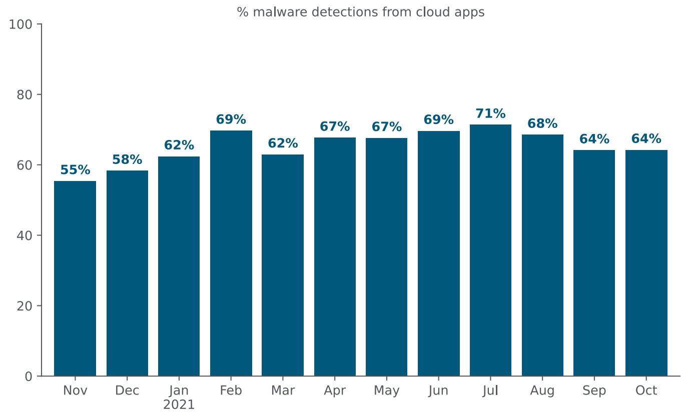
ABOUT THIS REPORT

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.

We analyze detections raised by our Next Generation Secure Web Gateway, which raises a detection when a user attempts to access malicious content. For this report, we count the total number of detections from our platform, not considering the significance of the impact of each individual threat.

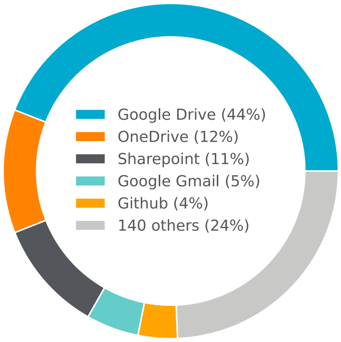
Cloud-enabled threats:

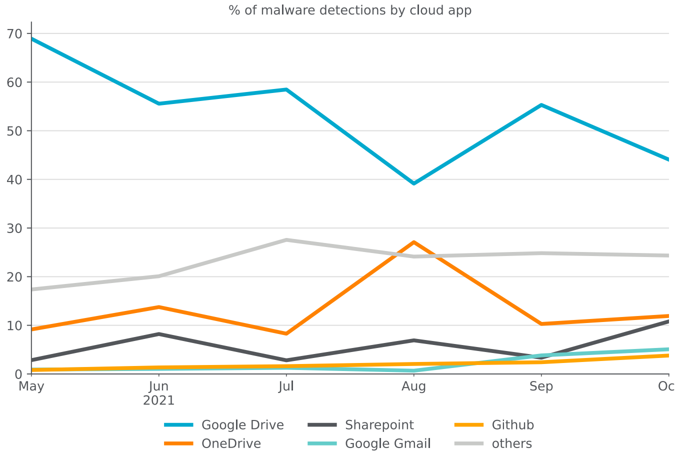
Attackers abuse popular cloud apps to deliver malware to their victims. For the second consecutive month, 64% of all malware downloads detected and blocked by the Netskope Security Cloud platform were delivered via cloud apps as compared to traditional websites.



On the left is a breakdown of the top 5 apps for which Netskope blocked the most malware downloads this month. The top 5 apps accounted for 76% of all cloud-delivered malware.

On the right is a breakdown of the changes in the top five app list over the past six months. Google Drive remains in the top spot despite an 11-point decrease from September.





The remainder of this section highlights additional ways attackers are abusing cloud apps.

Harvester abuses Microsoft Infrastructure

A new threat actor, tracked as Harvester, is using a custom backdoor, dubbed Graphon, that abuses Microsoft infrastructure for its C&C activity. Details

DEV-0343 targets Office 365 credentials

Researchers uncovered a malicious activity cluster, tracked as DEV-0343, that is targeting the Office 365 tenants of US and Israeli defense technology companies. Details

Amazon SES abused as part of Office 365 campaign

An Office 365 credential phishing campaign abuses a stolen Amazon SES token. Details

YouTube abuse

Malware campaigns are creating YouTube videos to distribute password-stealing trojans. Details

TA505 lures via OneDrive shared files

Researchers identified a mass volume email attack staged by TA505, a prolific cybercriminal gang that sends notifications about Microsoft OneDrive shared files. Details

Phishing via DocuSign imitation

Threat actors are following a new trend of targeting non-executive employees with phishing emails that are crafted to look like legitimate DocuSign messages but are not being sent from the platform. Details

Discord abuse

Threat actors are abusing Discord to deliver various types of malware. Details

Dropbox abuse for C2

A new cyber espionage campaign, dubbed Operation Ghostshell, abuses cloud storage services such as Dropbox for command-and-control (C2) communications in an attempt to stay under the radar. Details

Airflow misconfigurations

Researchers discovered Apache Airflow misconfigurations resulting in the exposure of sensitive credentials for platforms such as Amazon Web Services (AWS), Google Cloud Platform (GCP), PayPal, Slack, and Stripe. Details

Malware hones in on Huawei Cloud

A new version of a Linux crypto-mining malware is now focusing on new cloud service providers like Huawei Cloud. Details

Vidar stealer

Vidar stealer has started abusing the Mastodon social media network to get C2 configuration details and evade detections. Details

SquirrelWaffle

A new threat referred to as SquirrelWaffle is being spread via spam campaigns to infect systems with a new malware loader. Details

Ransomware group abuse SEOs

Researchers have spotted two campaigns linked to either the REvil or SolarMarker that utilize SEO poisoning. Details

Malware:

The following are the top five malicious domains that Netskope blocked users from visiting, the top five phishing domains that Netskope blocked users from visiting, and the top five malware distribution domains from which Netskope blocked malware downloads.

Malicious domains:

1. beibitao[.]website
2. iekx[.]xyz
3. wonderfulprofitforyou[.]life
4. clonyjohn[.]com
5. billyjons[.]net

Phishing domains:

1. bancaporinternet.interban.pe.novadigio[.]com
2. webdineroalinstantebcp[.]com
3. check-securepayment[.]com
4. anazon.co.ip.r5bvnxo[.]cn
5. www.mpaypal[.]cf

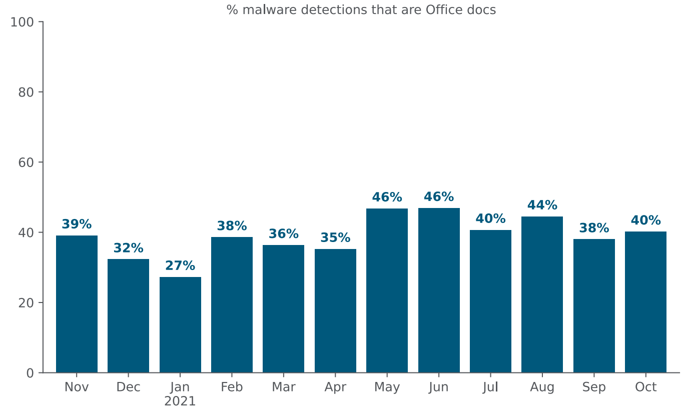
Malware distribution domains:

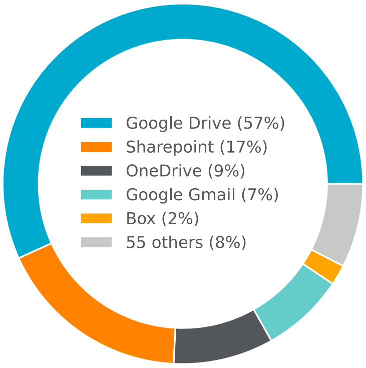
1. kan-web-am.s3.tebi[.]io
2. a.aruncorp[.]xyz
3. n21ald.oss-cn-shanghai.aliyuncs[.]com
4. memuplay[.]com
5. j.haycake[.]xyz

The following are the top five malware families blocked by Netskope:

1. **Win32.Trojan.Wacatac:** Wacatac is a Trojan that exfiltrates banking data.
2. **Win32.Trojan.Barys:** Barys is a Trojan that abuses Dropbox to discreetly download payload and exfiltrate files.
3. **Win32.Trojan.Razy:** Razy is a Trojan typically distributed via advertising blocks disguised as legitimate software.
4. **Document-PDF.Phishing.PhishingX:** PhishingX refers to PDF documents that are used as part of a phishing campaign.
5. **ByteCode-MSIL.Trojan.AgentTesla:** AgentTesla is a RAT and keylogger written in .NET.

Attackers continue to abuse Microsoft Office documents as a popular malware delivery vehicle. On the left, the percentage of Office document malware downloads increased just 2 points from last month as Office docs continue to account for around 40% of all malware downloads. On the right, the app from which Netskope blocked the most malicious Office document was again Google Drive, although the percentage delivered via Google Drive fell 20 points from September as SharePoint and OneDrive rose. Box edged out Outlook.com for the #5 spot.





Ransomware:

The following are the top 5 ransomware families blocked by Netskope.

1. **WannaCryptor:** Also known as WannaCry, is ransomware that is propagated through an exploit called EternalBlue that targeted a critical vulnerability in an outdated version of Microsoft's implementation of the Server Message Block (SMB) protocol.
2. **Sodinokibi:** Also known as REvil, launched a supply chain ransomware attack using an exploit in Kaseya's VSA remote management software on July 2, 2021.
3. **Cerber:** Cerber was being spread via the cloud productivity platform, Microsoft Office 365, and is well known for performing a widespread ransomware attack in 2016.
4. **Phobos:** Phobos tends to target smaller organizations and demand lower ransoms than other families.
5. **WastedLocker:** WastedLocker is attributed to the threat group Evil Corp and has been active since early 2020.

Nobelium has targeted 140 MSPs

Nobelium, behind last year's SolarWinds hack, is still targeting 140 managed service providers and cloud service providers and at least 14 have been breached since May 2021. Details

Europol made 12 ransomware related arrests

Europol has announced the arrest of 12 individuals believed to be linked to ransomware attacks against 1,800 victims in 71 countries. Details

DarkSide involved in money laundering scheme

DarkSide ransomware operators moved $7 million worth of Bitcoin in what looks like a money-laundering scheme. Details

REvil shut down again

The REvil ransomware operation has likely shut down after an unknown individual hijacked their Tor payment portal and data leak blog. Details

REvil ransomware operator arrested

German investigators have identified a Russian man believed to be one of REvil ransomware gang's core members. Details

FIN7 sends pen testing lures

FIN7 is attempting to join the ransomware space by creating fake pen testing companies to recruit individuals for conducting network attacks. Details

FIN12

Researchers state that the FIN12 gang executes a file-encrypting payload, most of the time Ryuk ransomware, on target networks in less than two days. Details

BlackMatter M.O.

The US CISA, FBI, and NSA published an advisory that details how the BlackMatter ransomware gang operates. Details

Hive encrypts Linux and FreeBSD

The Hive ransomware gang now also encrypts Linux and FreeBSD using new malware variants. Details

Karma ransomware related to Nemty

Researchers have found evidence of the Karma ransomware being just another evolutionary step in the Nemty strain. Details

Two ransomware operators arrested

Europol arrested two men in Ukraine that are said to be members of a prolific ransomware operation with demands ranging up to €70 million. Details

BillQuick Web Suite vulnerability abused to deploy ransomware

An unknown threat group is exploiting a SQL injection vulnerability BillQuick Web Suite time and billing solution to deploy ransomware. Details

Ranzy Locker ransomware

FBI states that Ranzy Locker ransomware had compromised more than 30 US businesses as of July 2021. Details

Yanluowang ransomware

A new ransomware strain, dubbed Yanluowang, is reportedly being used in highly targeted attacks. Details

Atom Silo

Atom Silo, a newly spotted ransomware group, is targeting a recently patched and actively exploited Confluence Server and Data Center vulnerability to deploy their ransomware payloads. Details

SnapMC

SnapMC, a new threat actor, has emerged in the cybercrime space performing data-stealing extortion but without performing any file encryption. Details

Macaw Locker

Evil Corp has launched Macaw Locker, a new ransomware to evade US ransom payment sanctions. Details

Groove ransomware calls on ransomware attacks on the US

Groove ransomware gang called on other extortion groups to attack US interests after law enforcement took down REvil's infrastructure. Details

Ransomware hits VMware ESXi VMs

An unknown ransomware gang is using a Python script to encrypt VMware ESXi virtual machines. Details

BlackByte decryptor

A BlackByte decryptor has been released which allows victims to recover their files for free. Details

Babuk decryptor

Researchers have created and released a decryption tool to help Babuk ransomware victims recover their files for free. Details

AtomSilo and LockFile decryptors

Researchers released a decryption tool that will help AtomSilo and LockFile ransomware victims recover some of their files for free without having to pay a ransom. Details

RECENT PUBLICATIONS

A DBatLoader: Abusing Discord to Deliver Warzone RAT

In this blog post, we analyze a recent DBatLoader sample that abuses Discord to deliver malware known as Warzone, a Remote Access Trojan created in 2018. Blog

What Happens When Facebook Goes Down?

On Monday, October 4, 2021, Facebook suffered a prolonged outage when, during routine maintenance, all connections to their global backbone network were mistakenly taken down. Blog

SquirrelWaffle: New Malware Loader Delivering Cobalt Strike and QakBot

In this blog post, we analyze two variants of the malicious Office documents that deliver SquirrelWaffle, the final SquirrelWaffle payload, and how the last stage URLs are being protected inside the binary. Blog

NETSKOPE THREAT LABS

Staffed by the industry's foremost cloud threat and malware researchers, the 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.

netskope

The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and takes a data-centric approach that empowers security teams with the right balance of protection and speed they need to secure their digital transformation journey. Reimagine your perimeter with Netskope.