netskope
THREAT LABS

December 2021

Netskope Threat Labs Report

IN THIS REPORT

- **Cloud-enabled threats:** For the third consecutive month, Microsoft OneDrive was the cloud with the most malware downloads while Google Drive's share continued to fall.
- **Malware & phishing:** Blogger dominated the top five phishing domains in December, a contrast to November when four other cloud apps appeared in the top five.
- **Ransomware:** A new ransomware family named Khonsari was found exploiting the recent Apache Log4j vulnerability.

TOP STORIES

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

Multiple Apache Log4j Vulnerabilities Discovered

Exploits for zero-day vulnerability Log4Shell made public - December 10, 2021

Threat actors are exploiting Log4Shell to deploy malware - December 12, 2021

A second Apache Log4j vulnerability has been discovered - December 14, 2021

Novel ransomware called Khonsari is exploiting Log4Shell - December 14, 2021

Nation-state hackers are exploiting Log4Shell - December 15, 2021

Conti ransomware is using Log4Shell exploit to access vCenter Servers - December 17, 2021

US agencies are ordered to patch the Log4Shell vulnerability - December 17, 2021

Attackers exploiting Log4Shell revive the TellYouThePass ransomware - December 17, 2021

Apache issues a patch for third high severity Log4j vulnerability - December 18, 2021

Attackers exploit Log4Shell to deploy Dridex - December 20, 2021

Australia, Canada, New Zealand, U.K., and U.S. release a joint advisory - December 23, 2021

A fourth CVE is issued for Log4j - December 28, 2021

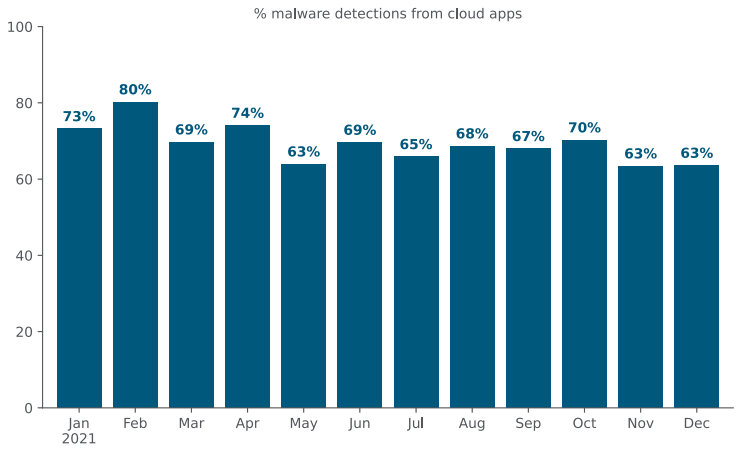
ABOUT THIS REPORT

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.

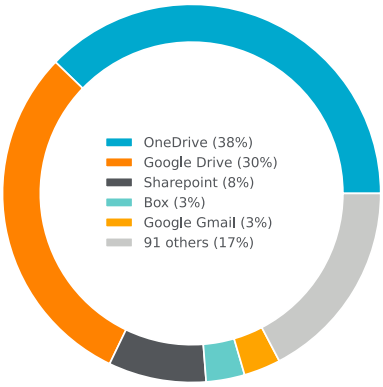
We analyze detections raised by our Next Generation Secure Web Gateway, which raises a detection when a user attempts to access malicious content. For this report, we count the total number of detections from our platform, not considering the significance of the impact of each individual threat.

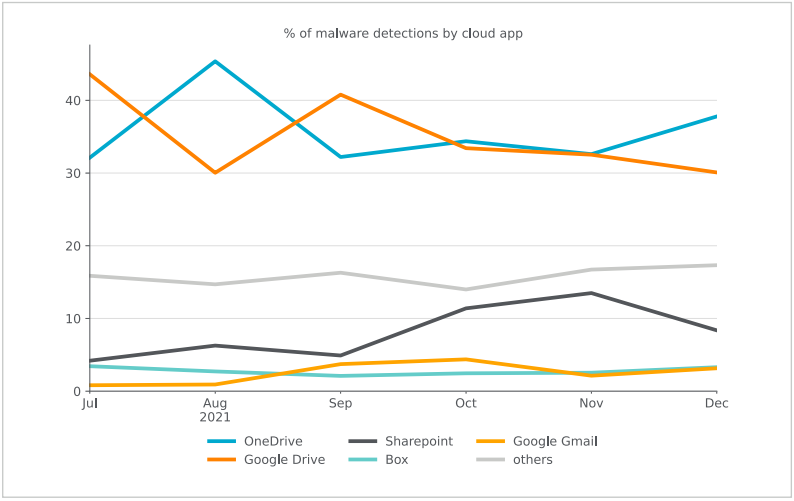
CLOUD-ENABLED THREATS

Attackers continue to abuse popular cloud apps to deliver malware to their victims. For the second straight month, 63% of all malware downloads detected and blocked by the Netskope Security Cloud platform were delivered via cloud apps as compared to traditional websites. 63% ties for the lowest share of malware downloads since the peak at 80% in February 2021.



On the left is a breakdown of the top five apps for which Netskope blocked the most malware downloads this month. On the right is a breakdown of the changes in the top five app list over the past six months. OneDrive took the top spot for the third month in a row, and by the biggest margin since August. Weebly, which appeared in the top five in November was displaced by Google Gmail. Google Drive continues to fall from its peak in September, matching its six-month low.





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

Phishing for O365 credentials

US universities have been targeted in multiple phishing attacks to steal Office 365 credentials. Details

Emotet being spread via Azure

Researchers identified Emotet being spread via fake Google Drive pages to open a file on Microsoft Azure. Details

Fake O365 notification to steal cloud credentials

A series of phishing attacks use fake Office 365 notifications to steal their Microsoft credentials. Details

Social engineering to steal cloud credentials

Attackers successfully used a social engineering campaign to steal sensitive Google, Twitter, and Facebook credentials from their targets. Details

Security flaw found in Microsoft Azure App Service

A security flaw found in Microsoft Azure App Service led to the exposure of customer source code for at least four years. Details

Aclip abuses Slack

An attacker is deploying a newly discovered backdoor named Aclip that abuses Slack for command and control. Details

Cerber ransomware targets Confluence and GitLab

Cerber ransomware has been found targeting Atlassian Confluence and GitLab servers using remote code execution vulnerabilities. Details

Malicious NPM packages steal Discord tokens

At least 17 malicious packages have been discovered on the NPM package Registry that were designed to steal Discord access tokens. Details

Twitter abused by spam accounts

Twitter removed more than 3,400 accounts accused of running manipulation or spam campaigns. Details

Ceeloader

Nobelium continues to breach networks by using a custom Ceeloader malware to target cloud and managed service providers. Details

Facebook disrupted seven different spyware-making companies

Facebook has disrupted the operations of seven different spyware-making companies that have abused the social media platform to harm vulnerable individuals. Details

MALWARE & PHISHING

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. Blogger (blogspot.com) dominated the top five phishing domains in December, a contrast to November when four other cloud apps appeared in the top five.

Malicious domains:

1. haberreport[.]xyz
2. dianches-inchor[.]com
3. kkkjs[.]xyz
4. slimshady.gotdns[.]ch
5. laudypauty[.]com

Phishing domains:

1. reikreitel.blogspot[.]com
2. soufsont.blogspot[.]com
3. citationsherbe[.]at
4. oiazeiuiazolme.blogspot[.]com
5. sefonta.blogspot[.]com

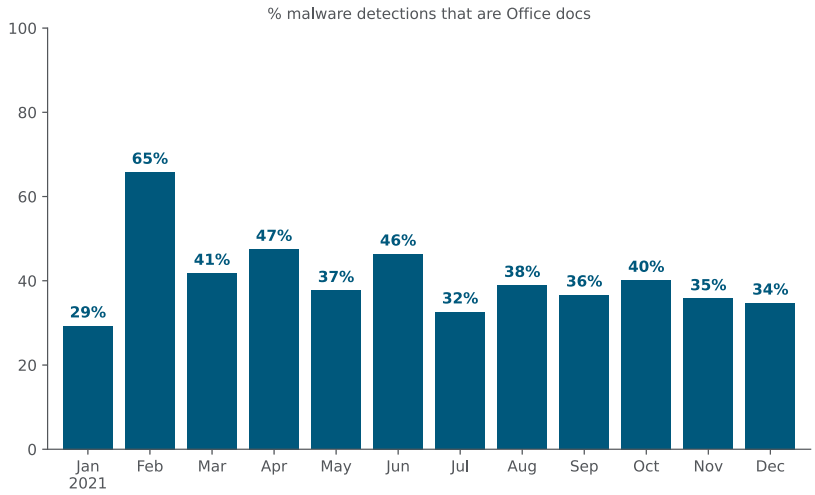
Malware distribution domains:

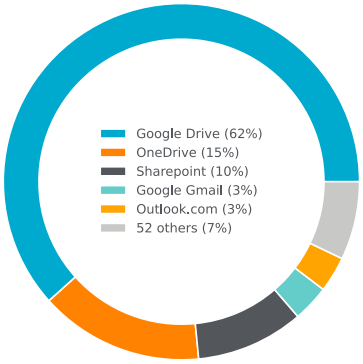
1. w.woodsome[.]xyz
2. y.sitread[.]xyz
3. hjxiaz.oss-cn-shenzhen.aliyuncs[.]com
4. p97t.oss-cn-shanghai.aliyuncs[.]com
5. p.pingpig[.]xyz

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

1. **Valyria** is a family of malicious Microsoft Office Documents that contain embedded malicious VBScripts.
2. **Wacatac** is a Trojan that exfiltrates banking data.
3. **Amphitryon** is a family of malicious Microsoft Office Documents that contains embedded malicious VBA macros.
4. **Symmi** is a browser hijacker.
5. **Ursu** contains a variety of malicious functionality and is frequently used as an infostealer.

Attackers continue to abuse Microsoft Office documents as a popular malware delivery vehicle. On the left, Office documents continue to make up approximately one-third of all malware detections on the Netskope platform. On the right, the app from which Netskope blocked the most malicious Office documents was again Google Drive.





RANSOMWARE

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

1. **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
2. **LockBit:** A ransomware group operating in the RaaS (Ransomware-as-a-Service) model, following the same architecture as other major threat groups, like REvil.
3. **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.
4. **Cerber:** Cerber is well known for performing a widespread ransomware attack in 2016 and was recently used to target Confluence and BitBucket servers.
5. **Khonsari:** A new ransomware family written in .NET and being delivered through Log4Shell.

BlackCat

BlackCat, a new ransomware written in Rust, contains a highly-customizable feature set allowing for attacks on a wide range of corporate environments. Details

BlackByte exploits ProxyShell

The BlackByte ransomware gang is breaching corporate networks by exploiting ProxyShell vulnerabilities. Details

Cuba ransomware

The FBI has revealed that the Cuba ransomware gang has compromised the networks of at least 49 organizations from US critical infrastructure sectors. Details

Glupteba botnet

Google disrupted the Glupteba botnet, a blockchain-enabled and modular malware that now controls more than 1 million Windows PCs around the world. Details

Emotet drops Cobalt Strike

Emotet malware has been seen installing Cobalt Strike beacons directly, giving immediate network access to make ransomware attacks imminent. Details

Conti ransomware

Australian Cyber Security Centre says Conti ransomware attacks have targeted multiple Australian organizations since November 2021. Details

Hancitor

Hancitor, a loader that provides Malware as a Service, has been observed using fake Docusign phishing emails to distribute malware such as FickerStealer, Pony, CobaltStrike, and Cuba Ransomware. Details

Hive ransomware

Researchers find that the Hive ransomware gang is more active and aggressive than its leak site shows, with an average attack rate of three companies every day. Details

AvosLocker uses Windows Safe Mode

The AvosLocker ransomware gang has started focusing on disabling endpoint security solutions by rebooting compromised systems into Windows Safe Mode. Details

AvosLocker gives free decryptor to government agency

AvosLocker ransomware operation provided a free decryptor after learning they encrypted a US government agency. Details

Rook ransomware

Rook, a new ransomware operation, recently appeared on the cyber-crime space, declaring a desperate need to make "a lot of money". Details

Aquatic Panda

Aquatic Panda, a Chinese threat actor, has been observed leveraging critical flaws in the Apache Log4j logging library as an access vector to perform various post-exploitation operations. Details

UPCOMING EVENTS

RSAC Learning Lab
Privilege Escalation and Persistence in AWS
6-9 June 2022
San Francisco, CA

RSAC
Defending against new phishing attacks that abuse OAuth authorization flows
6-9 June 2022
San Francisco, CA

RECENT PUBLICATIONS

CVE-2021-44228: Log4Shell Apache Log4j RCE

CVE-2021-44228 (Log4Shell or LogJam) is a recently discovered zero-day vulnerability in the ubiquitous Apache Log4j Java-based logging library. Blog

CVE-2021-45046: New Log4j Vulnerability Discovered

Shortly after the Apache Software Foundation (ASF) released the bug fix for the vulnerability known as Log4Shell or LogJam (CVE-2021-44228), a second vulnerability was discovered in Log4j Java-based logging library, tracked as CVE-2021-45046. Blog

Khonsari: New Ransomware Delivered Through Log4Shell

While many organizations are patching the two recent Apache Log4j vulnerabilities (CVE-2021-44228 and CVE-2021-45046), attackers have been exploiting them to deliver a new ransomware family called Khonsari. Blog

CVE-2021-45105: New DoS Vulnerability Found in Apache Log4j

Just a few days after CVE-2021-45046 was released and fixed, a third zero-day vulnerability was discovered in Apache Log4j, tracked as CVE-2021-45105. The bug was reported on December 15, 2021, and disclosed on December 18, 2021. Blog

CVE-2021-44832: New Vulnerability Found in Apache Log4j

A fourth vulnerability was discovered in the Apache Log4j library. Tracked as CVE-2021-44832, this bug may allow arbitrary code execution in compromised systems when the attacker has permissions to modify the logging configuration file. 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.