netskope
THREAT LABS

January 2022

Netskope Threat Labs Report

IN THIS REPORT

- **Cloud-enabled threats:** The share of malware downloads from Google Drive continues to decrease and is now at a six-month low, while the share of malware downloads from Microsoft OneDrive is approaching a six-month high.

- **Malware & phishing:** While Blogger continues to be abused by attackers to host components of phishing pages, the number of top phishing pages hosted on Blogger decreased from December.

- **Ransomware:** Three relatively new ransomware families, AvosLocker, Hive, and BlackMatter made this month's top five list of ransomware blocked by Netskope's platform.

TOP STORIES

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

US FTC warns companies to protect against Log4J attacks

The US Federal Trade Commission warns that it will go after any US company that fails to protect its customers' data against ongoing Log4J attacks. Details

Ukrainian websites were defaced

Multiple websites belonging to various Ukrainian public institutions were compromised, defaced, and subsequently taken offline. Details

Ukraine accused Russia of defacement attacks

Ukraine formally accused Russia of masterminding the attacks that targeted websites of public institutions and government agencies. Details

Joint advisory on Russian attack response

FBI, NSA, and CISA released a joint advisory on how to respond to cyberattacks orchestrated by Russian state-sponsored actors. Details

UniCC is shutting down

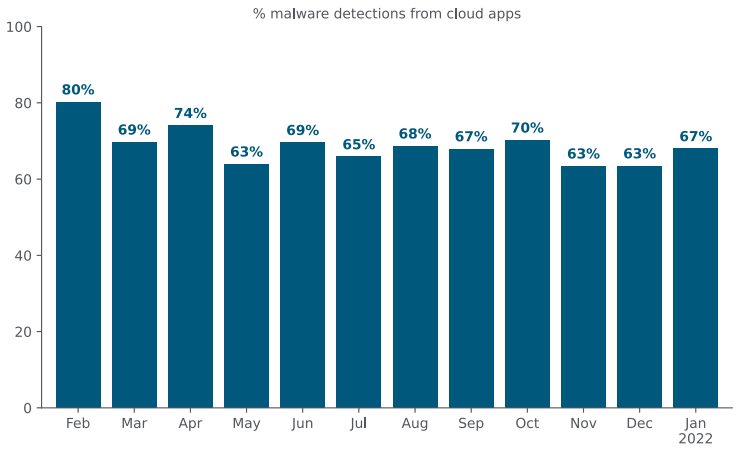
UniCC, the biggest dark web marketplace for stolen credit and debit cards, has announced that it's shutting down operations. Details

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.

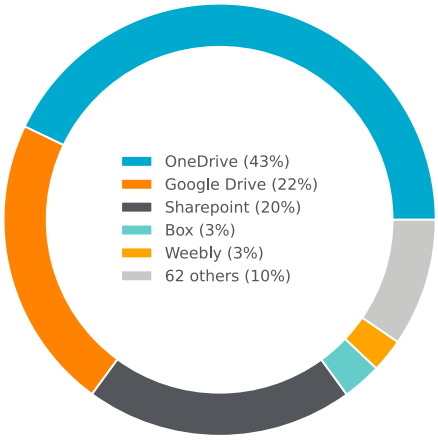
We analyze detections raised by our Next Generation Secure Web Gateway, which raises a detection when a user attempts to access malicious content. For this report, we count the total number of detections from our platform, not considering the significance of the impact of each individual threat.

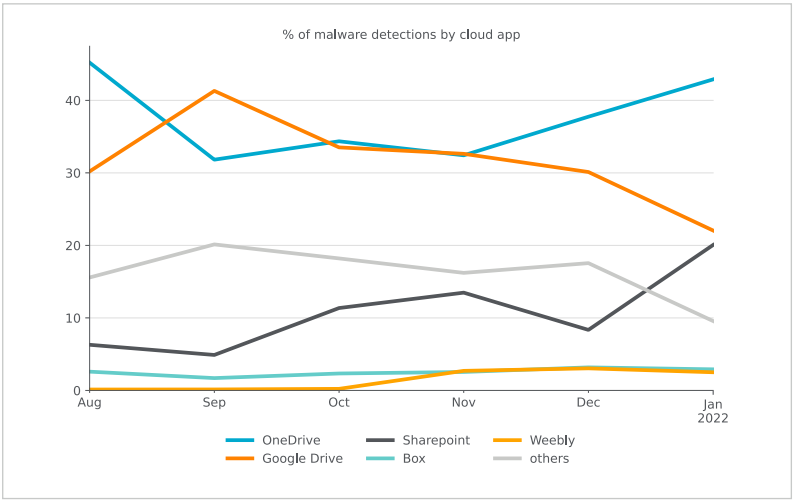
CLOUD-ENABLED THREATS



Attackers continue to abuse popular cloud apps to deliver malware to their victims. For the first time in three months, the percentage of malware downloads originating from cloud apps increased, to 67%, still far below the peak of 80% in February 2021.

The share of malware downloads from Google Drive continues to fall from its peak in September 2021 and is now at a six-month low. Google recently released a new feature that warns users of potentially malicious content, likely contributing to the diminishing share of malware downloads. At the same time, Microsoft OneDrive–the most popular cloud storage app among Netskope users–has seen an increased share of malware downloads. Weebly reappeared again on the top five list as its share of malware downloads was slightly higher than that of Google Gmail, which it once again displaced.





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

Malicious OAuth apps and phishing from hijacked O365 accounts

A new campaign named "OiVaVoii" was identified targeting company executives with malicious OAuth apps and custom phishing lures sent from hijacked Office 365 accounts. Details

Adobe Cloud suite abused to target O365 and Gmail users

Researchers identified that attackers are creating accounts within the Adobe Cloud suite to send images and PDFs that appear legitimate to target Office 365 and Gmail users. Details

Phishing campaign pilfers O365 creds

A new phishing campaign impersonating the United States Department of Labor pilfers Office 365 credentials from victims. Details

OneDrive abused for C2

Researchers identified a multi-stage espionage campaign that abuses Microsoft OneDrive for command-and-control to target high-ranking government officials in Western Asia. Details

Insecure S3 Bucket exposes sensitive information

An insecure Amazon S3 bucket exposed personal data on 500,000 Ghanaian graduates. Details

APT35 abuses S3 to deploy CharmPower

APT35 has been observed leveraging Log4Shell attacks to drop a new PowerShell backdoor, dubbed "CharmPower," from an actor-controlled Amazon S3 bucket. Details

Dark Herring abuses AWS to deliver malicious Javascript

An operation, dubbed Dark Herring, used 470 Google Play Store apps and affected over 100 million users worldwide to deploy malicious JavaScript files hosted on AWS. Details

Google Voice abuse

FBI warns about ongoing Google Voice authentication scams where attackers set up a Google Voice account in the victims' names. Details

Google Docs abused for phishing

Attackers are abusing the commenting feature of Google Docs to send out phishing emails that appear trustworthy. Details

SysJoker abuses GitHub and Google Drive

A new multi-platform backdoor malware named SysJoker that abuses GitHub and Google Drive has emerged in the wild. Details

Lazarus abuses GitHub for C2

North Korea's Lazarus APT abuses GitHub for command and control in its latest campaign. Details

Molerats abuse Google Drive and Dropbox

Molerats have been discovered abusing legitimate cloud services like Google Drive and Dropbox to host malware payloads and for command-and-control and the exfiltration of data. Details

DuckDNS abuse

Attackers are abusing DuckDNS to deploy and deliver variants of commodity RATs. Details

OceanLotus abuses Glitch

Netskope Threat Labs identified that OceanLotus hackers are now using the web archive file format (.MHT and .MHTML) and abusing Glitch to deploy backdoors. Details

Purple Fox disguised as Telegram installer

A malicious Telegram for Desktop installer distributes the Purple Fox malware. 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. While Blogger (blogspot.com) continues to be abused by attackers to host components of phishing pages, the number of top phishing pages hosted on Blogger decreased from four in December to two in January.

Malicious domains:

1. yrsii[.]xyz
2. nertablisst[.]com
3. cksxss[.]xyz
4. coinpot[.]co
5. ugroocuw[.]net

Phishing domains:

1. dezhduzedze.blogspot[.]com
2. hangovertest1.blogspot[.]com
3. eahmxz[.]com
4. pollockview[.]com
5. defenderalert[.]ga

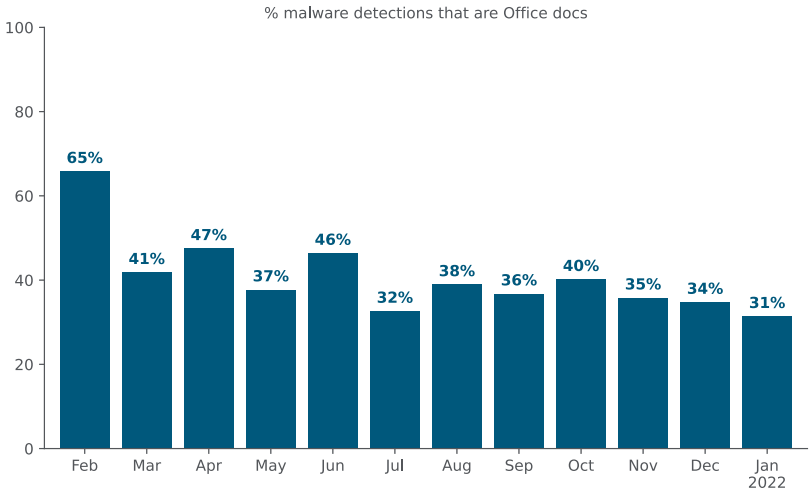
Malware distribution domains:

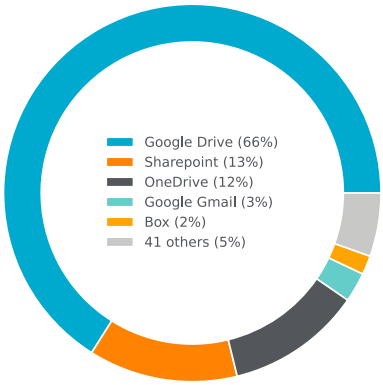
1. c.bushcash[.]xyz
2. j.haycake[.]xyz
3. w.woodsome[.]xyz
4. y.sitread[.]xyz
5. i.mythlate[.]xyz

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 usually to deliver other malicious payloads.
2. **Amphitryon** is a family of malicious Microsoft Office Documents that contain embedded malicious VBA macros, usually to redirect users to malicious websites.
3. **Wacatac** is a Trojan that exfiltrates banking data.
4. **Barys** is a Trojan that abuses Dropbox to discreetly download payload and exfiltrate files.
5. **Groooboor** is a Remote Access Trojan (RAT) that is typically spread through malicious Office documents.

Attackers continue to abuse Microsoft Office documents as a popular malware delivery vehicle. Three of the top five malware families listed above use malicious Microsoft Office files to spread. In January, the share of malware downloads that were Office Documents decreased slightly for the third consecutive month, now representing just under one-third of all malware downloads on the Netskope platform, but still remain well above their pre-Emotet levels from early 2019 (19%). While Google Drive's overall share of malware downloads continues to decrease, the share of malicious Office Document files downloaded from Google Drive remains above 50%.





RANSOMWARE

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

1. **AvosLocker** is a ransomware that emerged in July 2021.
2. **Hive** emerged in June 2021 and has been observed targeting organizations that many ransomware operators avoid.
3. **LockBit** is a ransomware group operating in the RaaS (Ransomware-as-a-Service) model, following the same architecture as other major threat groups, like REvil.
4. **BlackMatter** is a new ransomware that emerged in July 2021 after the disappearance of DarkSide.
5. **Conti** recently abused the December 2021 Log4Shell exploit to hack VMware vCenter Servers.

Diavol linked to TrickBot

The FBI has formally linked the Diavol ransomware operation to the TrickBot Group. Details

VPNLab.net has been taken down

Authorities from 10 countries took down VPNLab.net, a VPN service provider used by ransomware operators. Details

Ukrainian police arrest ransomware affiliate group

Ukrainian police officers have arrested a ransomware affiliate group responsible for attacking at least 50 companies. Details

REvil operators arrested

Russian authorities have detained 14 individuals suspected to be part of the REvil RaaS operation. Details

WhisperGate

Researchers identified a new destructive malware operation dubbed WhisperGate targeting government, non-profit, and information technology entities in Ukraine. Details

White Rabbit

White Rabbit, a new ransomware variant that appeared in the wild, is linked to the FIN8 hacking group. Details

TellYouThePass

TellYouThePass ransomware has re-emerged as a Golang-compiled malware in an effort to target more operating systems. Details

Night Sky

Researchers identified a new ransomware variant dubbed Night Sky that targets corporate networks and steals data in double-extortion attacks. Details

Magniber

Magniber ransomware is using Windows application package files (.APPX) to drop malware pretending to be Chrome and Edge web browser updates. Details

DeadBolt

Attackers claim to be using a zero-day vulnerability to hack QNAP devices and encrypt files using the DeadBolt ransomware. Details

Qlocker ransomware targeting QNAP devices

Threat actors behind the Qlocker ransomware are targeting Internet-exposed QNAP Network Attached Storage (NAS) devices. Details

Malicious USB drives used to deploy ransomware

The FBI warned that ransomware gangs are mailing malicious USB drives, posing as the U.S. Department of Health and Human Services and Amazon to target industries for ransomware infection. Details

UPCOMING EVENTS

HackCon IT-SECPRO
New Phishing Attacks – Exploiting OAuth Authorization
03 Feb 2022
Virtual

HackCon IT-SECPRO
Abusing the cloud for command and control
16 Feb 2022
Virtual

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

Abusing Microsoft Office Using Malicious Web Archive Files

Netskope Threat Labs is currently tracking a malicious campaign that uses Web Page Archive files (".mht" or ".mhtml") to deliver infected documents, which eventually deploys a backdoor that uses Glitch for C2 communication. Blog

Infected PowerPoint Files Using Cloud Services to Deliver Multiple Malware

In this blog post, we will analyze a malicious PowerPoint Add-In file detected by Netskope that delivers AveMaria (a.k.a. Warzone) and AgentTesla. These files are using Bitly to shorten URLs and different cloud services like MediaFire, Blogger, and GitHub to host the payloads. Blog

Netskope Threat Coverage: WhisperGate

A new destructive malware called WhisperGate was discovered in mid-January 2022 targeting Ukrainian organizations. This malware has a destructive nature: wiping files and corrupting disks to prevent the OS from loading. Blog

Netskope Threat Coverage: Night Sky

A new ransomware family named Night Sky was spotted working in the RaaS (Ransomware-as-a-Service) model. 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.