netskope
THREAT LABS

February 2022

Netskope Threat Labs Report

IN THIS REPORT

- **Cloud-enabled threats:** While cloud-delivered malware continues to dominate, the share of downloads from Google Drive continues to fall, reaching a new 12-month low, while the share of downloads from Microsoft OneDrive continues to increase, reaching a 12-month high.

- **Malware & phishing:** For the third consecutive month, phishing infrastructure hosted in Blogger made the top five list, as attackers continue to create phishing infrastructure on the platform.

- **Ransomware:** BlackCat, one of the top ransomware families detected by Netskope, has been linked to BlackMatter.

TOP STORIES

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

The following outlines a timeline of cybersecurity events in Ukraine for the month of February:

Gamaredon behind spear-phishing emails targeting Ukraine since October 2021 - Feb 04, 2022

Ukrainian agencies hit by Distributed Denial-of-Service attacks - Feb 15, 2022

White House linked Ukrainian DDoS attacks to Russian GRU - Feb 18, 2022

EU countries offer Ukraine help in fighting against Russian cyber-attacks - Feb 23, 2022

Novel Hermetic Wiper used in attacks as Russia moves troops into Ukraine - Feb 23, 2022

Russia warns of cyber attacks aimed at Russian critical infrastructure operators - Feb 25, 2022

Ukraine recruits an 'IT Army' to hack Russian entities, lists 31 targets - Feb 26, 2022

A Ukrainian security researcher leaked 60,000+ internal messages from Conti - Feb 27, 2022

Facebook took down accounts used by a Belarusian-linked hacking group - Feb 28, 2022

Ukraine says its 'IT Army' has taken down key Russian sites - Feb 28, 2022

Ukrainian networks targeted with malware before Russia's invasion - Feb 28, 2022

Microsoft to disable VBA macros

Microsoft announced that it will disable running VBA macros downloaded from the Internet in several Microsoft Office apps starting in early April. Details

Hackers targeting U.S. CDCs

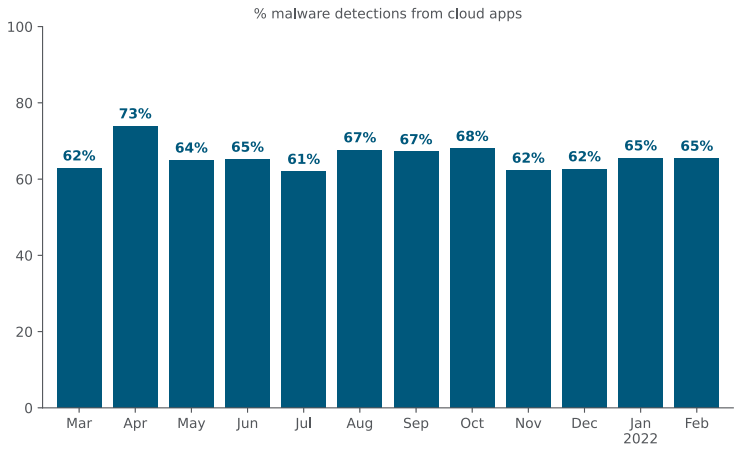
Russian-backed hackers have been targeting U.S. cleared defense contractors (CDCs) to steal sensitive info around U.S. defense and intelligence programs and capabilities. Details

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.

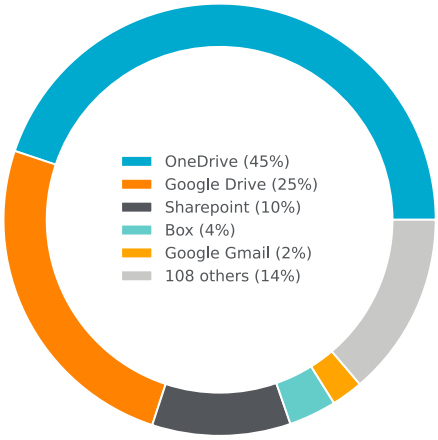
We analyze detections raised by our Next Generation Secure Web Gateway, which raises a detection when a user attempts to access malicious content. For this report, we count the total number of detections from our platform, not considering the significance of the impact of each individual threat.

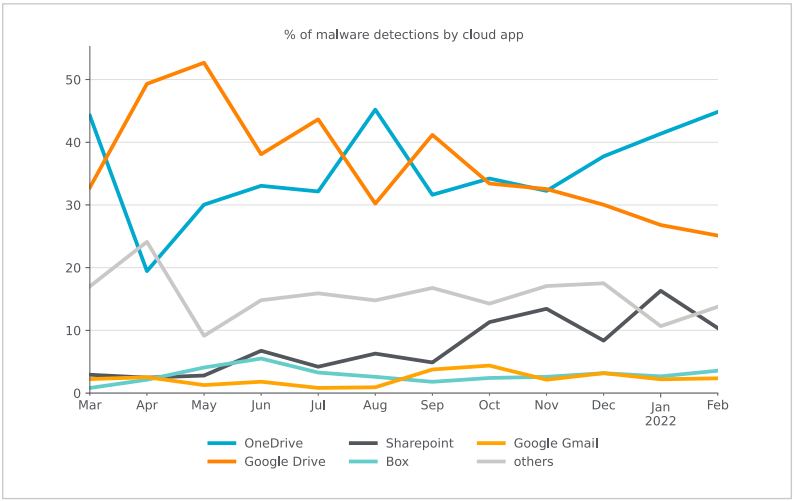
CLOUD-ENABLED THREATS



Attackers continue to abuse popular cloud apps to deliver malware to their victims. The percentage of malware downloads originating from cloud apps remained at 65%, which is below the peak of 80% observed in February 2021.

For the fifth consecutive month, the share of cloud malware downloads from Google Drive declined, reaching a 12 month low. In January, Google released a new feature that warns users of potentially malicious content, likely contributing to the diminishing share of malware downloads. At the same time, the share of cloud malware downloads from Microsoft OneDrive–as of this writing, the most popular cloud storage app among Netskope users–increased for the third consecutive month, reaching a 12-month high.





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

Public Azure Blob exposes 100k files

A publically accessible Microsoft Azure blob was discovered containing more than 100,000 sensitive files. Details

Public AWS server contains employee data

An unsecured AWS server, found open to the public Internet, caused a compromise of airport employees' data in Colombia and Peru. Details

Coin miners account for 86% of compromised GCP instances

Google researchers identified that coin miner infections account for over 86% of all cases of compromise concerning cloud instances. Details

Amazon S3 abused to host malware

Researchers identified a previously undocumented Mac trojan that abuses Amazon S3 and CloudFront to host its second-stage payloads, including adware, in the form of .DMG or .ZIP files. Details

Discord's CDN abuses for malware delivery

Threat actors are abusing Discord's CDN to distribute fake Windows 11 upgrade installers in hopes of tricking victims into downloading and executing RedLine stealer malware. Details

Attackers are abusing Teams to spread malware

Attackers are compromising Microsoft Teams accounts to spread malicious executables to participants in existing chat conversations. Details

Google Drive abused in malicious campaigns

A low-skilled attacker has been using off-the-shelf malware and payloads hosted in cloud services such as Google Drive in malicious campaigns aimed at companies in the aviation sector. Details

NimbleMamba abuses Dropbox

An APT group operating has embarked on a new campaign that takes advantage of a previously undocumented implant called NimbleMamba that uses the Dropbox API for both command-and-control as well as exfiltration. Details

Marlin abuses OneDrive for command and control

An advanced persistent threat (APT) group with ties to Iran has refreshed its malware toolset to include a new backdoor, dubbed Marlin, which makes use of Microsoft's OneDrive API for its C2 operations. Details

MuddyWater abuses Telegram for command and control

Iran's MuddyWater is using new malware that is using Telegram's API for C2 communications in worldwide cyber attacks. Details

CapraRAT disguises itself as YouTube app

An APT group has expanded to include a new RAT, dubbed CapraRAT, that disguises itself as a YouTube app in espionage attacks aimed at Indian military and diplomatic entities. Details

Malware attempted to pass for Zoom, Teamview, and Visual Studio

An SEO poisoning campaign was discovered dropping the Batloader and Atera Agent malware for searches for productivity tool downloads, such as Zoom, TeamViewer, and Visual Studio. 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) continues to be abused by attackers to host phishing infrastructure, accounting for three of the top five phishing domains.

Malicious domains:

1. launchingonsetwhirlwind[.]com
2. lousebankroll[.]com
3. softballwaiting[.]com
4. rotation.ahrealestatepr[.]com
5. soaheeme[.]net

Phishing domains:

1. facenooflogin.blogspot[.]com
2. cg.taispeed68[.]xyz
3. chase-help-support-locked.blogspot[.]com
4. chase-onlinehelp.blogspot[.]com
5. autoexprs[.]com

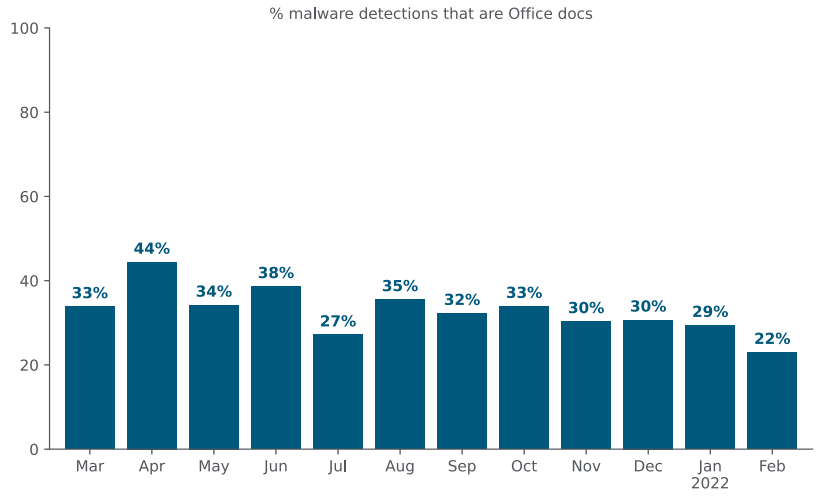
Malware distribution domains:

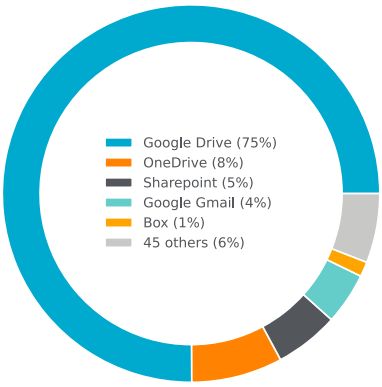
1. j.haycake[.]xyz
2. w.woodsome[.]xyz
3. www.orolk[.]space
4. g.wagegem[.]xyz
5. y.sitread[.]xyz

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

1. **Wacatac** is a Trojan that exfiltrates banking data.
2. **Valyria** is a family of malicious Microsoft Office Documents that contain embedded malicious VBScripts usually to deliver other malicious payloads.
3. **Ursu** contains a variety of malicious functionality and is frequently used as an infostealer.
4. **Barys** is a Trojan that abuses Dropbox to discreetly download payload and exfiltrate files.
5. **Nymeria,** also known as **Loda**, is both a keylogger and a remote access trojan (RAT).

Attackers continue to abuse Microsoft Office documents as a popular malware delivery vehicle. Valyria, the second most common malware family for the month, is just one example of such malicious Office documents. In February, the share of malware downloads that were Office documents decreased to its lowest value in the past year, 22%, only slightly higher than the pre-Emotet levels observed in early 2019 (19%). While Google Drive's overall share of malware downloads continues to decrease, the app continues to have a commanding lead over other apps in terms of malicious Office document downloads.





RANSOMWARE

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

1. **BlackCat** is the first ransomware written in Rust and was first seen in December 2021.
2. **Sugar** was first seen in November 2021 and targets individuals, demanding low ransoms.
3. **Hive** emerged in June 2021 and has been observed targeting organizations that many ransomware operators avoid.
4. **AvosLocker** is a ransomware that emerged in July 2021.
5. **LockBit:** A ransomware group operating in the RaaS (Ransomware-as-a-Service) model, following the same architecture as other major threat groups, like REvil.

Conti ransomware leaked

An individual connected to the Conti ransomware group has leaked a wide variety of data beginning with internal chat messages. Details

TrickBot shuts down

TrickBot malware operation has shut down after its core developers move to the Conti ransomware gang to focus development on the stealthy BazarBackdoor and Anchor malware families. Details

Log4j vulnerability exploited to deploy ransomware

A threat actor is actively exploiting the well-known Log4j vulnerability to infect unpatched VMware Horizon servers with ransomware. Details

Ransomware targeting critical infrastructure

Cyber Security authorities from Australia, the U.K., and the U.S. have published a joint advisory warning of an increase in ransomware attacks targeting critical infrastructure. Details

Sugar ransomware

A new ransomware operation, dubbed Sugar, is targeting individual computers, rather than corporate networks, with low ransom demands. Details

DeadBolt targets NAS devices

DeadBolt ransomware is now targeting ASUSTOR NAS devices by encrypting files and demanding a $1,150 ransom in bitcoin. Details

DeadBolt decryption key released

A decryption key for the DeadBolt ransomware strain has been released after QNAP NAS devices were infected. Details

TargetCompany ransomware decryption key released

Researchers have released a decryption utility to help TargetCompany ransomware victims recover their files for free. Details

Decryption keys released for multiple ransomware

The master decryption keys for the Maze, Egregor, and Sekhmet ransomware operations have been released. Details

Hive decrypted via flaw in algorithm

Researchers have used a flaw in Hive ransomware's encryption algorithm to decrypt data infected without relying on the private key used to lock access to the content. Details

Memento ransomware hackers deploy PowerLess

APT35 (aka Phosphorus or Charming Kitten), a group linked to Memento ransomware, is now deploying a new PowerShell based backdoor called PowerLess. Details

Moses Staff deploys StrifeWater

Moses Staff, a hacker group tied to a series of espionage and sabotage attacks has incorporated a previously undocumented RAT, dubbed StrifeWater, in ransomware attacks. Details

FBI releases details around LockBit

The FBI has released technical details and indicators of compromise associated with LockBit ransomware attacks. Details

Black Cat ransomware linked to BlackMatter

Black Cat ransomware gang has been confirmed to be former members of the notorious BlackMatter/DarkSide ransomware operation. Details

Entropy related to Dridex

Analysis of Entropy ransomware reveals code-level similarities with the Evil Corp's Dridex malware. Details

BlackByte attacked critical infrastructure

The FBI revealed that the BlackByte ransomware group has breached the networks of at least three organizations from US critical infrastructure sectors. Details

Cuba ransomware

Cuba ransomware operation is exploiting Microsoft Exchange vulnerabilities to gain initial access to corporate networks and encrypt devices. 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

Microsoft Office: VBA Blocked By Default in Files From the Internet

On February 7, 2022, Microsoft announced that they will start blocking VBA macros for files downloaded from the internet. In this blog post, we explained how it works and how we expect attackers will adapt to this change. Blog

Netskope Threat Coverage: HermeticWiper

On February 24, 2022, a new malware called HermeticWiper was found in hundreds of computers in Ukraine. HermeticWiper corrupts disks on infected systems, similar to WhisperGate. In this blog post, we analyze this threat to demonstrate how it works. Blog

NETSKOPE THREAT LABS

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