December 2022

Netskope Threat Labs Report

IN THIS REPORT

| **Cloud-enabled threats:** Cloud malware delivery reached its highest level in the past six months, as more than half of malware downloads over HTTP and HTTPS originated from cloud apps, led by Microsoft OneDrive.

| **Malware & phishing:** Free web hosting services and content delivery networks continue to be popular tools abused by attackers to host malware, phishing, and other malicious content.

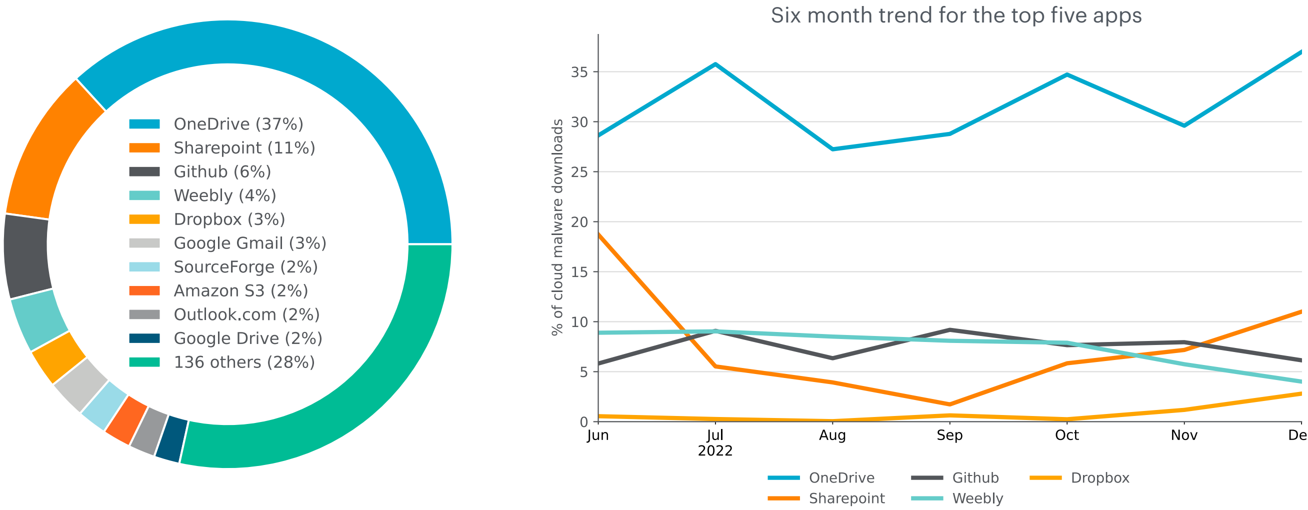
| **Ransomware:** BlackMagic, primarily targeting victims in Israel, and Royal, targeting victims worldwide, both entered the top five in December.

netskope
THREAT LABS

CLOUD-ENABLED THREATS

In December, Netskope detected malware downloads originating from 146 distinct cloud apps. Microsoft OneDrive, used to deliver a variety of different types of malware, continues to hold the top spot, where it has been for more than six months. Weebly returned to the top five after briefly falling out in November. Cloud apps accounted for 52.7% of all HTTP and HTTPS malware downloads in December, its highest level in the past six months.

Top apps for malware downloads | December 2022



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

DEV–0139 targeting cryptocurrency companies via Telegram

Researchers recently discovered a malicious campaign where the threat actor tracked as DEV–0139 abused Telegram channels to target and gain trust of cryptocurrency investment companies. Details

APT group using GitHub as a dead drop resolver

New research shows that a threat actor known as Cobalt Mirage is attacking US organizations with a custom malware named Drokbk, which uses GitHub API as a dead drop resolver. Details

Vulnerability in Amazon Elastic Container Registry (ECR) Public Gallery

A critical vulnerability could allow attackers to delete all images in the Amazon ECR Public Gallery or update the image contents to inject malicious code. Details

New phishing campaign abusing Facebook

Researchers found a new phishing campaign that abuses Facebook throughout the attack chain, evading email security solutions. Details

Malicious PyPI package targeting developers

A malicious Python package mimicking SentinelOne’s API was found in Python’s PyPI repository, trying to steal sensitive data including from AWS, GitHub, and Kubernetes. Details

Google’s WordPress plugin allowing AWS metadata theft

A server-side request forgery (SSRF) vulnerability in the Google Web Stories WordPress plugin could allow one to steal AWS metadata from websites hosted on Amazon. Details

Vulnerability in Kyverno affecting cloud environments

A critical vulnerability was discovered in Kubernetes Native Policy Management (Kyverno), which could allow one to import malicious code into cloud production environments. Details

RisePro info-stealer malware abusing Telegram

A malware downloader service known as PrivateLoader was found distributing an infostealer malware named RisePro, which abuses Telegram for C2 communication. Details

MALWARE & PHISHING

The following are the top five new malicious domains that Netskope blocked users from visiting, the top five new phishing domains that Netskope blocked users from visiting, and the top five domains from which Netskope blocked malware downloads. Free hosting services and CDNs continue to appear in the top lists as attackers abuse these services to blend in with benign traffic.

Malicious domains:

1. krjxhvyyzp[.]com
2. 8a4e8c[.]qmtfxvgkgcwfmghl[.]com
3. uuruemaish[.]fun
4. tarmlosning[.]com
5. fr33f1lex1.com

Phishing domains:

1. uthecrimorew[.]info
2. ferralpibrazz[.]weebly[.]com
3. swisspostpaket[.]wpengine[.]com
4. applikationman[.]wpengine[.]com
5. home-bltkub-petshop[.]blogspot[.]com

Malware distribution domains:

1. cdn[.]discordapp[.]com
2. static[.]s123-cdn-static[.]com
3. cdn-cms[.]f-static[.]net
4. download.wetransfer[.]com
5. docplayer[.]net

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

1. **PhishingX** is a malicious PDF file used as part of a phishing campaign to redirect victims to a phishing page.
2. **Farfli** is an old Remote Access Trojan (RAT) frequently modified and used by multiple APT groups.
3. **AgentTesla** is a Remote Access Trojan (RAT) and keylogger written in .NET that has been around since 2014.
4. **Dridex** is an infostealer that is commonly spread using malicious Office documents.
5. **Talu** is a Trojan used to deliver a variety of different types of malware, including infostealers.

RANSOMWARE

The following are the top five ransomware families blocked by Netskope in December.

1. **Black Basta** was first discovered in April 2022 and has both Windows and Linux variants.
2. **BlackMatter** was inspired by LockBit, REvil, and DarkSide.
3. **BlackMagic** has been used to target transportation and logistics in Israel.
4. **Prestige** has been used to target victims in Ukraine who were previously targeted with HermeticWiper.
5. **Royal** is a rebranded version of Zeon ransomware, linked to the Conti ransomware.

Cuba ransomware reaches $60 million in payments

A new joint security advisory between the FBI and CISA revealed that the ransomware group known as Cuba has reached over $60 million in ransoms. Details

New wiper malware targeting Russian courts and mayor's offices

A newly discovered data wiper malware named CryWiper was found masquerading as ransomware and targeting Russian courts and mayor's offices. Details

Ransomware attack forces hospital to transfer patients

A ransomware attack has forced the André-Mignot hospital to transfer some of its patients as computer systems were affected in the attack. Details

New data wiper named Fantasy

An Iranian APT group known as Agrius was spotted using a new data wiper dubbed as Fantasy in supply chain attacks, targeting organizations in Israel, Hong Kong, and South Africa. Details

Malware abusing official repositories to deploy ransomware

A new malware campaign is abusing PyPI and npm repositories with typosquatted and false libraries to target developers with a Golang-based ransomware. Details

Details about the destructive Azov ransomware

A new research shows more details about a new data wiper named Azov Ransomware, which was being distributed by SmokeLoader malware. Details

California's Department of Finance likely hit by LockBit

The Department of Finance in California has confirmed a cyber security incident claimed by LockBit, which says that 75 GB of files were stolen. Details

Windows drivers signed by Microsoft used by ransomware

A new joint research shows that multiple ransomware actors were using drivers signed by Microsoft's Windows Hardware Developer Program throughout the attack chain. Details

Microsoft fixes zero-day used by ransomware

The security vulnerability tracked as CVE–2022–44698 that was being used by attackers to deliver Magniber ransomware and Qbot malware was recently fixed by Microsoft. Details

Agenda ransomware using Rust instead of Golang

A new research shows details about the Agenda ransomware, which is now using Rust language instead of Go, targeting healthcare and education sectors in different countries. Details

Royal ransomware linked to former Conti Team One members

Researchers have found that Royal ransomware is a rebranded version of Zeon ransomware, which was associated with a group linked to Conti ransomware. Details

Vice Society ransomware group using new encryptor

A new custom ransomware named PolyVice was found being used by the Vice Society group, using a hybrid encryption scheme. Details

TOP STORIES

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

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

Microsoft warns about Russian-sponsored attacks targeting Ukrainian infrastructure throughout the winter — December 05, 2022

IT Army of Ukraine claimed a DDoS attack to the second largest bank in Russia — December 06, 2022

Ukrainian government infected with malicious ISO files that mimic Windows 10 installers — December 15, 2022

Users of an Ukrainian military system known as DELTA targeted with infostealer malware — December 19, 2022

Russian attackers targeting a large petroleum refinery in NATO country amid war — December 20, 2022

The Glupteba malware returned after Google disruption

A botnet named Glupteba has returned after Google disrupted its operation in 2021, being modular malware targeting Windows and IoT devices. Details

Facebook takes down spyware vendors in multiple countries

Facebook announced that they took down 200 covert influence operations since 2017 operating in multiple countries, including India, China, Russia, Israel, and the US. Details

Attackers abusing search engine ads to push malware

The FBI released an alert informing that attackers are creating search engine advertisements that mimic organizations, leading to info stealers and ransomware. Details

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.

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.