netskope
THREAT LABS

March 2022

Netskope Threat Labs Report

IN THIS REPORT

Cloud-enabled threats: Among cloud apps, Weebly was responsible for the second-most malware downloads, caused by attackers hosting malicious PDFs including CAPTCHAs that redirect victims to phishing, spam, scam, and malware websites.

Malware & phishing: For the fourth consecutive month, phishing infrastructure hosted in Blogger made the top five list, accompanied by phishing pages hosted in Amazon S3 and Azure Websites, as attackers continue to abuse cloud apps to host phishing infrastructure.

Ransomware: LokiLocker, a relatively new RaaS variant first seen in the wild last summer, saw increased activity in March.

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 March:

IsaacWiper was deployed in attacks against Ukraine - Mar 01, 2022

Telegram groups have increased sixfold since the Russian invasion - Mar 03, 2022

Russia blocked Facebook after pro-Kremlin accounts were deactivated - Mar 04, 2022

Russian federal agencies' websites were compromised in a supply chain attack - Mar 09, 2022

Formbook stealer was used to target Ukrainians - Mar 09, 2022

Russia created its own TLS certificate authority to bypass sanctions - Mar 10, 2022

CaddyWiper was observed in attacks targeting Ukrainian organizations - Mar 14, 2022

Russia faces a critical IT storage crisis with two more months of data storage left - Mar 15, 2022

SBU has detained a hacker who assisted the invading Russian troops - Mar 17, 2022

Another wiper dubbed DoubleZero is targeting Ukrainian enterprises - Mar 24, 2022

Russian company Kaspersky added to the US National Security Threat List - Mar 26, 2022

Lapsus$

After the threat group Lapsus$ claimed to have breached Microsoft's internal Azure DevOps source code repositories, the City of London police arrested seven individuals allegedly connected to the gang. Details

APT41

China-affiliated APT41 breached at least six U.S. state government networks between May 2021 and February 2022 by taking advantage of vulnerable internet-facing web applications. Details

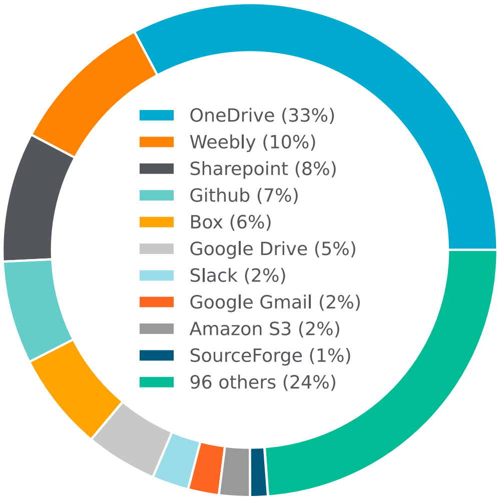
ABOUT THIS REPORT

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

In March, Netskope detected malware downloads originating from 106 distinct cloud apps. Compared to February, OneDrive remained in the top spot for the app with the most malware downloads, but there was a considerable shakeup in the top ten. Weebly ascended to second place as a result of malicious PDF files being hosted on the service, including fake CAPTCHAs that redirect victims to phishing, spam, scam, and malware websites. Netskope has seen an increase in such malicious PDF files since November, a trend that will be analyzed in more detail in our upcoming quarterly Cloud and Threat Report. Google Drive, previously in the top five, was edged out by Box and dropped to sixth.



Top apps for malware downloads
March 2022

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

Calendly abuse for O365 phishing

Phishing actors are actively abusing Calendly in a Microsoft credentials phishing campaign. Details

Increase in O365 phishing

Researchers recorded a rise in the sophistication of phishing attacks, especially those targeting Microsoft 365 credentials for the third consecutive year. Details

Azure Static Web Apps service abused

Attackers are abusing Microsoft Azure's Static Web Apps service to steal Microsoft, Office 365, Outlook, and OneDrive credentials. Details

GIMMICK abuses Google Drive

Researchers identified a macOS malware variant called GIMMICK that heavily abuses Google Drive services in multiple stages of the kill chain. Details

YouTube abuse

Researchers have identified a malware distribution campaign that uses lures on YouTube to trick victims into downloading RedLine. Details

Google Ads abuse

A large-scale campaign was discovered that abuses Google Ads and SEO to trick users into giving their personal data to fake investments schemes impersonating genuine brands. Details

Mars Stealer abuses Google Ads

Mars Stealer malware is using Google Ads advertising to rank cloned OpenOffice sites high on search results. Details

Verblecon steals Discord tokens

Researchers have identified a new complex malware loader, dubbed Verblecon, that facilitates the theft of Discord tokens. 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 malware distribution domains from which Netskope blocked malware downloads. The top malicious domains reveal an interesting trend: the use of a domain generation algorithm (DGA) that chooses three random words. All of the top five malicious domains follow this pattern. The top new phishing domains included three cloud apps this month: Blogger, Azure Websites, and Amazon S3. This was the fourth consecutive month that a Blogger site appeared in the top five. The top malware distribution domains notably contained three CDNs (content delivery networks), illustrating just how challenging it can be to try to use URL filtering alone to defend against malware. One of the three CDNs is associated with the cloud app Discord, which we have previously reported being abused to deliver the Warzone RAT.

Malicious domains:

1. snappedimpressive[.]com
2. slidecaffeinecrown[.]com
3. planningunavoidablenull[.]com
4. outlineappearbar[.]com
5. desktopnotificationshub[.]com

Phishing domains:

1. www.brookshoeus[.]com
2. trithuctre[.]org
3. soufritont.blogspot[.]com
4. farturar-agosto.azurewebsites[.]net
5. zsda28-auu8032xxs-ahu234k.s3.eu-north-1.amazonaws[.]com

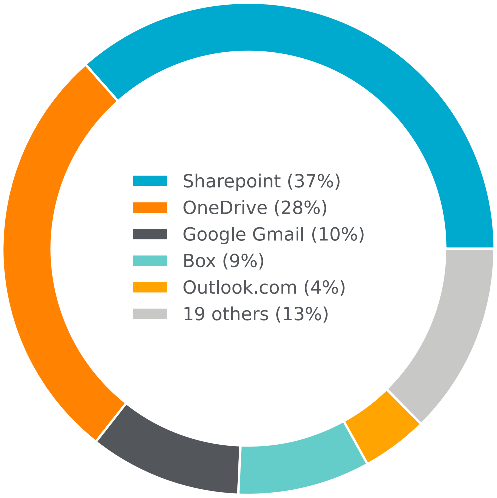
Malware distribution domains:

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. **PhishingX** is malicious PDF files that are generally used as part of a phishing campaign to redirect victims to a phishing page.
2. **Razy** is a Trojan typically distributed via malicious ads and disguised as legitimate software.
3. **Emotet** is typically distributed as a malicious Office document, often disguised as a fake invoice. Emotet's infrastructure was taken down in January 2021 but came back nine months later.
4. **RemoteShell** is a backdoor script often coupled with an exploit to provide an attacker remote access to a victim's computer.
5. **Ursu** contains a variety of malicious functionality and is frequently used as an infostealer.

Attackers continue to abuse Microsoft Office documents to deliver malware, but the format has been steadily losing popularity and has now returned to pre-Emotet levels. In March, Office documents represented less than 10% of malware downloads for the first time since 2019. This decline is driven in part by recent changes from Microsoft, including blocking VBA macros by default. Sharepoint and OneDrive were the two apps with the most malicious Office document downloads, displacing Google Drive, likely driven by a new feature on that platform that warns users of malicious content. The presence of Gmail and Outlook.com in the top five indicates that email attachments are still a popular method for delivering malicious Office documents.



Top apps for malicious Office doc downloads
March 2022

RANSOMWARE

The following were the top five ransomware families blocked by Netskope in March.

1. **LokiLocker,** unrelated to LokiBot or Locky, operates in the RaaS model and was first seen in August 2021.
2. **HermeticWiper** was first discovered targeting victims in Ukraine in February 2022.
3. **NightSky** emerged in January 2022, targeting corporate networks and stealing data in double-extortion attacks.
4. **Khonsari** was first seen in December 2021 being delivered through Log4Shell.
5. **BlackCat** is the first ransomware written in Rust and was first seen in December 2021.

Ransomware in 2021

FBI stated that ransomware gangs have breached at least 649 organizations from multiple US critical infrastructure sectors in 2021. Details

REvil ransomware affiliate extradited

U.S. DoJ announced that an alleged REvil ransomware affiliate was extradited to the United States to stand trial for the Kaseya cyberattack. Details

Ragnar Locker

The FBI stated that the Ragnar Locker ransomware group has breached the networks of at least 52 organizations from multiple US critical infrastructure sectors. Details

BlackCat and BlackMatter overlap

Researchers identified that BlackCat and BlackMatter have an overlap in the tactics, techniques, and procedures (TTPs) indicating a strong connection between the two. Details

FBI warns of AvosLocker

FBI warns of AvosLocker ransomware being used in attacks targeting multiple US critical infrastructure sectors. Details

Decryptor for Diavol ransomware

Researchers released a free decryption tool to help Diavol ransomware victims recover their files without paying a ransom. Details

Hive

Hive ransomware has converted their VMware ESXi Linux encryptor to Rust. Details

UPCOMING EVENTS

OWASP Global Appsec
Abusing Cloud Apps 101: Command and Control
6 June 2022
Virtual

OWASP Global Appsec
Defending against new phishing attacks that abuse OAuth authorization flows
6 June 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

Office Documents and Cloud Apps: Perfect for Malware Delivery

This blog demonstrates a recent Office document attack from the victim's perspective and highlights the most common types of Office document attacks seen today and shows strategies to reduce your risk of becoming the latest victim. Blog

New Formbook Campaign Delivered Through Phishing Emails

In March 2022, Netskope Threat Labs came across an interesting phishing email addressed to high-ranking government officials in Ukraine containing Formbook (a.k.a. XLoader), which is a well-known malware operating in the MaaS (Malware-as-a-Service) model. 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.