April 2022

Netskope Threat Labs Report

IN THIS REPORT

| **Cloud-enabled threats:** Squarespace joined Weebly in the top ten this month, caused by downloads of malicious PDFs that redirect victims to phishing, spam, scam, and malware distribution websites.

| **Malware & phishing:** For the first time in five months, there were no Blogger pages in the phishing top five, replaced by Amazon S3, Azure Websites, and Weebly, as attackers continue to host phishing infrastructure in popular cloud apps.

| **Ransomware:** NightSky, first discovered in January, saw increased activity in April.

netskope
THREAT LABS

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 April:

Russians bypassing website blocks to access Western news **- Apr 4, 2022**

Armageddon APT group targeting EU government and Ukraine organizations **- Apr 5, 2022**

U.S. eased sanctions on Russia likely to avoid internet isolation **- Apr 8, 2022**

NB65 APT group used the leaked Conti ransomware to attack Russian companies **- Apr 9, 2022**

Russian APT Sandworm tried to take down a large Ukrainian energy provider **- Apr 12, 2022**

Ukrainian government targeted with IceID malware and Zimbra exploits **- Apr 14, 2022**

Gamaredon APT group targeting Ukraine with new variants of Pteredo backdoor **- Apr 20, 2022**

A U.S. advisory warns of Russian hackers targeting critical infrastructure **- Apr 20, 2022**

Research shows a high number of cyber attacks from Russia against Ukraine **- Apr 27, 2022**

Compromised WordPress websites used to target pro-Ukraine and gov websites **- Apr 28, 2022**

Emotet switches to LNK files

Emotet replaces the payload delivery system from malicious Office document format to LNK files that abuse PowerShell to download payloads. Details

Zloader

Microsoft announced the disruption of Zloader, a large botnet offered in the Malware-as-a-Service (MaaS) model. Details

Qbot opts for MSI deployments

After Microsoft disabled VBA macros by default in files downloaded from the internet, the Qbot botnet started to push its payload via MSI files within password-protected ZIP, instead of the usual malicious Office documents. Details

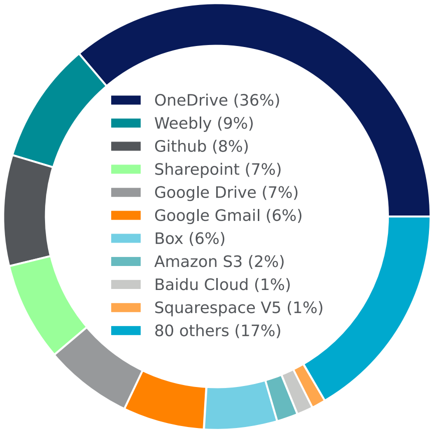
ABOUT THIS REPORT

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 April, Netskope detected malware downloads originating from 90 distinct cloud apps. Compared to March, OneDrive and Weebly remained in the top two spots. Weebly continues to be abused to deliver malicious PDF files that redirect victims to phishing, spam, scam, and malware websites. Attackers are also using Squarespace to deliver the same types of malicious PDF files, causing Squarespace to enter the top ten for the first time. Baidu Cloud (namely Baidu Object Storage) also entered the top ten this month, the result of a variety of different Trojans that were downloaded from the platform.



Top apps for malware downloads
April 2022

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

Prynt Stealer abuses Discord and Telegram

New infostealer malware named Prynt abuses Telegram to exfiltrate data and targets multiple browsers and other apps, such as Discord and Pidgin. Details

Snake Keylogger abuses MediaFire

A threat campaign was found using simple PDF files that linked to a Snake Keylogger payload hosted on MediaFire. Details

Goldbackdoor abuses multiple cloud services

A novel backdoor linked to the APT37 group was found targeting journalists, abusing Microsoft OneDrive, Graph APIs, Azure, and Google Drive throughout the attack. Details

MetaStealer abuses GitHub and Transfer.sh

A new campaign of the Windows MetaStealer malware was spotted, abusing GitHub and Transfer.sh services to host its payloads. Details

AWS Lambda abused by cryptominer

A new malware named Denonia is targeting AWS Lambda cloud environments with an XMRig variant to mine for Monero. Details

Borat RAT steals Discord tokens

Researchers have found a new RAT called Borat that provides many advanced features, such as ransomware deployment and Discord token theft. Details

New OldGremlin backdoor abuses Dropbox

A threat actor known as OldGremlin is targeting Russia with a new backdoor named TinyFluff, which uses Dropbox to store its payloads. 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. The top malicious domains reveal a continuing trend: the use of a domain generation algorithm (DGA) that chooses two or three random words. For the second month in a row, all of the top five malicious domains follow this pattern. Also for the second month in a row, all the top file malicious domains are in the com TLD. The top new phishing domains included three cloud apps this month: Weebly, Azure Websites, and Amazon S3. This was the first time in five months that a Blogger website did not appear in the top five. The top malware distribution domains continue to include popular file-sharing services, including Discord, which we have previously reported being abused to deliver the Warzone RAT.

Malicious domains:

1. unforgivablegrowl[.]com
2. visiblejoseph[.]com
3. lotteryhibernateauthorized[.]com
4. saunasupposedly[.]com
5. residenceseeingstanding[.]com

Phishing domains:

1. attethuifgyuxty.weebly[.]com
2. www.m.epsocnsznerd[.]icu
3. heavenly231.s3.eu-west-2.amazonaws[.]com
4. pemblokiran0023.weebly[.]com
5. exoduswllerkt.azurewebsites[.]net

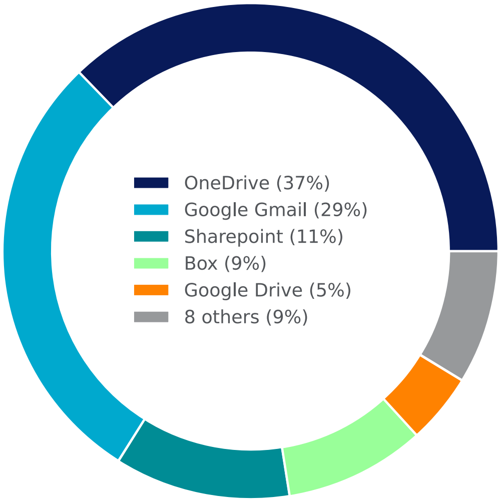
Malware distribution domains:

1. puu[.]sh
2. cdn.discordapp[.]com
3. download.pdf00[.]com
4. static.s123-cdn-static[.]com
5. uploads.strikinglycdn[.]com

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. **Quakbot** also known as Qbot, is a banking Trojan that has been around since 2008 and is typically spread through malspam campaigns.
3. **Valyria** is a family of malicious Microsoft Office documents that contain embedded malicious VBScripts usually to deliver other malicious payloads.
4. **Ursnif** is an information-stealing Trojan born from the Gozi trojan.
5. **Prometei** is a cryptocurrency mining botnet.

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. For the second month in a row, Office documents represented less than 10% of malware downloads. This decline is driven in part by recent changes from Microsoft, including blocking VBA macros by default. Compared to March, Google Gmail increased from 10% to 29%, indicating that email links and attachments are still a popular method for delivering malicious Office documents.



Top apps for malicious Office doc downloads
April 2022

RANSOMWARE

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

1. **NightSky** emerged in January 2022, targeting corporate networks and stealing data in double-extortion attacks.
2. **Somhoveran** is a screen locker ransomware commonly spread through Discord.
3. **Hive** emerged in June 2021 and has been observed targeting organizations that many ransomware operators avoid.
4. **LokiLocker,** unrelated to LokiBot or Locky, operates in the RaaS model and was first seen in August 2021.
5. **BlackCat** is the first ransomware written in Rust and was first seen in December 2021.

NotPetya

The U.S. State Department was offering up to $10 million for information about six GRU officers and hackers linked to NotPetya attacks. Details

LockBit

Evidence in logs shows the presence of the LockBit group for five months before the ransomware was deployed in a regional U.S. government agency. Details

Leaked Conti ransomware

Russian organizations were targeted with a new ransomware based on Conti's source code, which was leaked after Conti sided with Russia after Russia's invasion of Ukraine. Details

FIN7

Researchers found a connection between the FIN7 (a.k.a. Carbanak) APT group and multiple ransomware gangs, such as Maze, Ryuk, Darkside, and BlackCat. Details

UPCOMING EVENTS

You Sh0t The Sheriff
Who enabled the macros? Attack landscape via Microsoft Office files
23 May 2022
São Paulo, SP - Brazil

OWASP Global Appsec
Abusing Cloud Apps 101: Command and Control
Defending against new phishing attacks that abuse OAuth authorization flows
6 June 2022
Virtual

RSAC Learning Lab
Privilege Escalation and Persistence in AWS
Defending against new phishing attacks that abuse OAuth authorization flows
6-9 June 2022
San Francisco, CA

RECENT PUBLICATIONS

Multi-Factor Authentication (MFA) Bypass Through Man-in-the-Middle Phishing Attacks

One of the key tools at the center of social engineering attacks against organizations is phishing. The use of multi-factor authentication (MFA) can often mitigate cases where sensitive data is stolen through common phishing attacks. This is where a more modern phishing method comes into play, the man-in-the-middle (MITM) phishing attack. This blog post explains how MITM phishing works and describes mitigation techniques against this attack. Blog

Two RCE Vulnerabilities Found in Spring Framework

At the end of March 2022, two critical vulnerabilities (CVE-2022-22963 and CVE-2022-22965) were discovered in different components of VMware Spring. Spring is a popular framework focused on facilitating the development of Java applications, including cloud-based apps, eliminating the need for additional code or concerns related to server requirements. 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.