May 2022

Netskope Threat Labs Report

IN THIS REPORT

Cloud-enabled threats: Weebly continues to hold one of the top spots for malware downloads, caused by a continuing pattern of malicious PDFs that redirect victims to phishing, spam, scam, and malware distribution websites.

Malware & phishing: For the first time since January, the Discord CDN did not make the top malware distribution domain list, which was instead dominated by other CDNs and software download sites.

Ransomware: LokiLocker, first discovered in August 2021, saw increased activity in May.

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 May:

Russian military targeted by a state-backed group from China **- May 3, 2022**

DDoS attacks against multiple Russian and Belarusian websites **- May 4, 2022**

Hacktivists disrupting the distribution of alcoholic beverages in Russia via DDoS **- May 5, 2022**

JesterStealer malware using "chemical attack" subject to target Ukrainian citizens **- May 7, 2022**

The online Russian TV hacked to display pro-Ukrainian and anti-war messages **- May 9, 2022**

Attackers targeting Germans who seeks information about Ukraine with RAT **- May 16, 2022**

Sandworm APT group using new version of ArguePatch loader to target Ukraine **- May 20, 2022**

Anonymous group declares cyber war against pro-Russian Killnet group **- May 23, 2022**

Unknown APT group repeatedly targeting Russia since Ukraine invasion **- May 24, 2022**

Scammers are exploiting Ukraine crisis to steal donations **- May 31, 2022**

Zero-Day vulnerability in MSDT

A Zero-Day RCE vulnerability was discovered in Microsoft Support Diagnostic Tool, tracked as CVE-2022-30190 and publicly called Follina. Details

GitHub breach

GitHub disclosed that an attacker stole about 100k npm user accounts, after breaching private repositories using stolen OAuth tokens and compromised AWS access key. Details

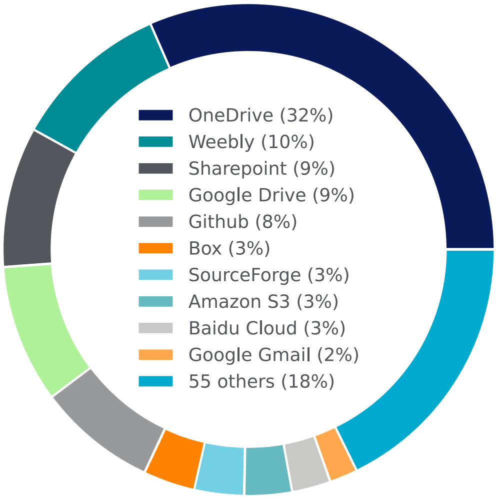
ABOUT THIS REPORT

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 May, Netskope detected malware downloads originating from 65 distinct cloud apps. Compared to April, 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. Baidu Cloud (namely Baidu Object Storage) remained in the top ten for the second straight month, the result of a variety of different Trojans that were downloaded from the platform.



Top apps for malware downloads May 2022

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

Python library infected to steal AWS data

The python "ctx" library was infected with code to steal data from AWS, such as the access key, and the secret access key. Details

Attackers may pre-hijack cloud accounts

Researchers have released a paper that shows how attackers may pre-hijack online accounts before they are created by users. Details

New technique to takeover Facebook accounts

A security researcher found a way to hack Facebook accounts via Gmail OAuth token which is used in the login process. Details

Bumblebee malware abusing Google

New campaign from TA578 threat group abusing Google Storage APIs to deliver Bumblebee malware via thread-hijacked emails. Details

New malware abusing Discord

Researchers found a new malware builder, dubbed as KurayStealer, which leverages Discord webhooks to steal sensitive data, including passwords and Discord tokens. Details

BEATDROP abusing Atlassian's Trello

Russian-based group APT29 spreading BEATDROP malware in phishing campaigns, which abuses Atlassian's Trello for C2 communication. Details

UNC3524 abusing Microsoft Exchange

New threat actor tracked as UNC3524 abusing Microsoft Exchange Web Services (EWS) API to steal data from targeted mailboxes. 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. For the past two months, the top malicious domains were dominated by domain generation algorithm (DGA) domains consisting of two or three random words. This month, only one of the top 5 follows that pattern. For the third month in a row, all the top file malicious domains are in the com TLD. The top new phishing domains included just one cloud app this month, Weebly. This is the first time since January that the Discord CDN did not make the top malware distribution domain list, dominated instead by other CDNs and software download sites.

Malicious domains:

1. openstartfive[.]com
2. www.top-dump-truck-blog[.]com
3. ocformation[.]com
4. truth-info[.]com
5. disappointingbeef[.]com

Phishing domains:

1. ydsfdsffgfdgrg[.]xyz
2. ff.member.garenav[.]vn
3. receivablessecuredocs.weebly[.]com
4. nnnnnndddnn.weebly[.]com
5. ekl-neetit[.]live

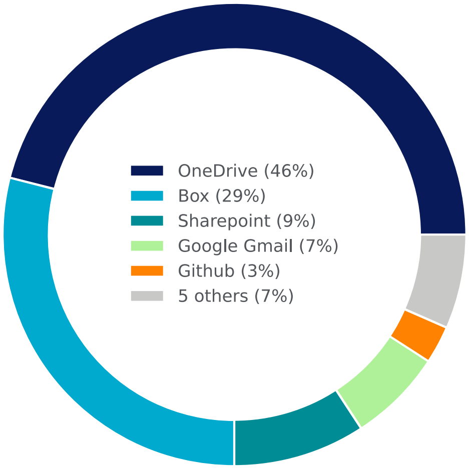
Malware distribution domains:

1. static1.squarespace[.]com
2. uploads.strikinglycdn[.]com
3. static.s123-cdn-static[.]com
4. d6bqwyojjrctq.cloudfront[.]net
5. v1.install80[.]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. **Valyria** is a family of malicious Microsoft Office documents that contain embedded malicious VBScripts usually to deliver other malicious payloads.
3. **Tiggre** is a malicious cryptominer.
4. **RemoteShell** is PHP-based malware that provides remote access.
5. **Donoff** is a family of malicious Microsoft Office DOC or DOCM files that use macros to download other malicious payloads.

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 third 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 April, Google Gmail decreased from 29% to 7% as we saw fewer malicious docs delivered via email, while Box increased from 9% to 29%.



Top apps for malicious Office doc downloads May 2022

RANSOMWARE

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

1. **LokiLocker,** unrelated to LokiBot or Locky, operates in the RaaS model and was first seen in August 2021.
2. **KillDisk** is a destructive ransomware recently used by Russia against organizations in Ukraine.
3. **Hive** emerged in June 2021 and has been observed targeting organizations that many ransomware operators avoid.
4. **Pandora** is likely based on the Babuk ransomware, and was actively targeting high-profile organizations in early 2022.
5. **Nokoyawa** was first seen in March 2022 and is likely related to Hive.

Conti ransomware shutting down

After Conti's ransomware leak, the group officially announced that it's shutting down its operations as some affiliates are migrating to smaller groups. Details

RansomHouse

New group called RansomHouse emerged in the wild, drawing attention for not encrypting any files in the operation, but only using extortion of stolen data. Details

Vulnerabilities in multiple ransomware strains

A researcher found a way to stop ransomware execution from multiple families, such as REvil and LockBit, by using DLL hijacking attacks. Details

AvosLocker

The ransomware-as-a-service group AvosLocker launched a variant which is using a new trick to bypass antivirus protections. Details

RECENT PUBLICATIONS

GoodWill Ransomware? Or Just Another Jasmin Variant?

In March 2022, GoodWill ransomware was spotted and made some headlines due its unusual ransom method, by asking victims to help less fortunate people by following a sequence of actions. After analyzing a few samples, Netskope Threat Labs found that GoodWill is based on an open-source project named Jasmin, which is a red team tool to simulate ransomware attacks. Blog

CVE-2022-30190: New Zero-Day Vulnerability (Follina) in Microsoft Support Diagnostic Tool

On May 27, 2022, a Microsoft Office document was submitted from Belarus to VirusTotal, using a novel method to deliver its payload. This new technique was identified as a Zero-Day RCE (Remote Code Execution) vulnerability in Microsoft Support Diagnostic Tool (MSDT), tracked as CVE-2022-30190 and also publicly called as Follina. Blog

RedLine Stealer Campaign Using Binance Mystery Box Videos to Spread GitHub-Hosted Payload

In April 2022, Netskope Threat Labs identified a new RedLine Stealer campaign spread on YouTube, using a fake bot to buy Mystery Box NFT from Binance. The video description leads the victim to download the fake bot, which is hosted on GitHub. RedLine Stealer is a malware that emerged in 2020, offering many capabilities for device reconnaissance, remote control, and information stealing. 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.