August 2022

Netskope Threat Labs Report

IN THIS REPORT

Cloud-enabled threats: Weebly and Microsoft OneDrive continue to top the list for malware downloads, joined this month by Azure Blob Storage, from which Netskope detected an increase in malware downloads spanning multiple Trojan families.

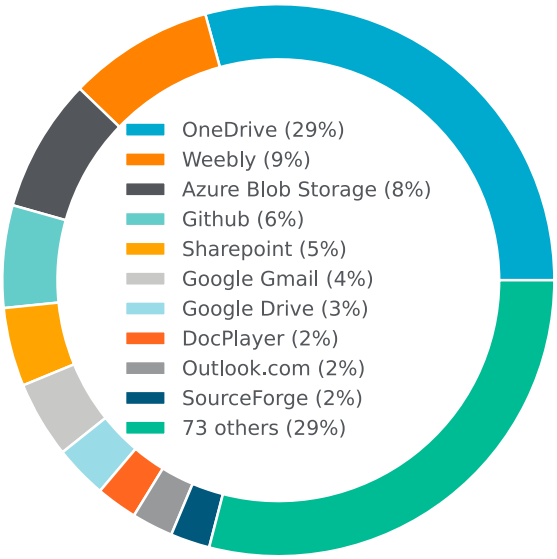
Malware & phishing: Free web hosting services Azure Web Apps, Weebly, and Netlify made the top five phishing domains as those and other free hosting services continue to be abused by phishers and scammers.

Ransomware: The cross-platform ransomware RedAlert was the most frequently detected ransomware family on the Netskope Security Cloud platform in August.

netskope
THREAT LABS

CLOUD-ENABLED THREATS

In August, Netskope detected malware downloads originating from 83 distinct cloud apps. Compared to July, OneDrive remained in the top spot, used to deliver a variety of different types of malware. Weebly moved up into the number two spot, as it continues to be abused to deliver malicious PDF files that redirect victims to phishing, spam, scam, and malware websites. Azure Blob Storage moved up to the number three spot, caused by a variety of different Trojans being distributed on that platform.



Top apps for malware downloads August 2022

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

New vulnerability named "ParseThru"

Researchers found a new vulnerability named "ParseThru," which allows attackers to gain unauthorized access to cloud-based applications developed with Golang. Details

Malicious PyPI packages delivering infostealer

New malicious Python packages were found in the PyPI repository delivering multiple malware, including infostealers that abuse Discord to exfiltrate data. Details

Scam-as-a-Service platform abusing Telegram

Researchers found a credit card stealing campaign that uses valid one-time-passcodes (OTP) to transfer funds, part of a Scam-as-a-Service platform that abuses Telegram in the operation. Details

New HTTP request issue allowing multiple attacks

New research shows how attackers may abuse HTTP request handling issues to install backdoors, compromise systems, and steal information from websites, such as authentication tokens from Amazon. Details

PyPI package delivering fileless crypto miner

Another malicious Python package was found in the official PyPI repository, delivering a Linux crypto miner that runs directly in-memory. Details

Malicious PyPI package abusing Discord

Multiple malicious PyPI packages were found installing malware that infects the Discord client, transforming it into a backdoor that can be used to steal information from web browsers and Roblox. Details

TeamTNT targeting cloud instances and services

Researchers disclosed that TeamTNT group has been targeting cloud environments and services for at least two years, recently adding credential-stealing capabilities that target AWS, GitHub, and Filezilla. Details

Fake P2E project delivering multiple infostealers

A fake play-to-earn project named "Cthulhu World" was found abusing Dropbox to distribute multiple malware such as Raccoon Stealer, AsyncRAT, and RedLine Stealer. 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 and phishing domains feature a newcomer this month, Netlify, a free web hosting service being abused to create phishing, scam, and malware delivery pages. Netlify joins Azure Web Apps and Weebly in the top five, as these free services continue to be popular among phishers and scammers.

Malicious domains:

1. attaccountforum.netlify[.]app
2. chimerical-peony-090abb.netlify[.]app
3. cruize.updogtechnologies[.]com
4. parasuasegurancacaixa.azurewebsites[.]net
5. verifikasi-security.weebly[.]com

Phishing domains:

1. parasuasegurancacaixa.azurewebsites[.]net
2. unbloockyouraccount2022.weebly[.]com
3. attoiuyaaduiesdfuyescxgc78387etdx.weebly[.]com
4. officedomaindlfnjndkjwwxxdbnbhc22.weebly[.]com
5. dashing-tapioca-233450.netlify[.]app

Malware distribution domains:

1. docplayer[.]net
2. static1.squarespace[.]com
3. static.s123-cdn-static[.]com
4. data.docslib[.]org
5. uploads.strikinglycdn[.]com

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

1. **PhishingX** are malicious PDF files 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. **Tiggre** is a malicious coin miner that disables common security software.
4. **Upatre** is a downloader spotted in 2013, with new variants popping up occasionally and delivering a variety of different payloads.
5. **PDFka** is a PDF file that exploits CVE-2010-0188 for arbitrary code execution.

RANSOMWARE

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

1. **RedAlert** is a cross-platform ransomware that targets both Windows and Linux ESXi servers.
2. **SiennaBlue** is associated with H0lyGh0st and written in Go.
3. **LockBit** is a ransomware group operating in the RaaS (Ransomware-as-a-Service) model, following the same architecture as other major threat groups, like REvil.
4. **Redeemer** is a free ransomware-builder being advertised on hacker forums.
5. **Black Basta** was first discovered in April 2022 and has both Windows and Linux variants.

Zeppelin ransomware alert

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released a new alert containing IOCs and TTPs related to Zeppelin ransomware. Details

$10M reward for Conti ransomware information

A $10M reward was announced by the U.S. State Department for information about members of the Conti ransomware group and its affiliates TrickBot and Wizard Spider. Details

SolidBit ransomware recruiting new members

Researchers released a warning stating that SolidBit ransomware group is actively recruiting new affiliates on dark web forums, and suggested that SolidBit may be a copycat of LockBit. Details

Conti ransomware using BazarCall phishing attack

The Conti ransomware group is using BaazarCall (a.k.a. Call Back Phishing) as the initial attack vector, which is a targeted attack composed in four stages. Details

BlackByte ransomware returns after hiatus

After a brief disappearance, the BlackByte ransomware group is back with a 2.0 version that includes a new data leak site and many Twitter accounts controlled by the attackers. Details

New Golang-based ransomware

Researchers found a new ransomware named “Agenda” that is written in Go language and targeting specific enterprises in Asia and Africa. Details

LockBit ransomware and its triple-extortion tactic

After being hit by DDoS attacks, the LockBit ransomware group announced that they are improving defenses and working to implement a triple-extortion strategy. 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 August:

Ukrainian cyber-activists are hijacking movie torrents to spread tips on bypassing Russian censorship — August 1, 2022

Ukraine shuts down a large bot farm used by Russian special services to spread disinformation — August 4, 2022

A new politically motivated hacker forum emerged to support Ukraine — August 11, 2022

Gamaredon APT group targeting Ukraine with a technique that hijacks Word's default template — August 15, 2022

Gamaredon APT group targeting Ukrainian entities with GammaLoad infostealer — August 16, 2022

Montenegro's security agent reported cyberattacks sourced from Russia — August 27, 2022

Ukrainian authorities exposed fraudulent call centers used for financial scams — August 31, 2022

Twitter data breach

Twitter has confirmed a data breach that affects over 5 million users which occurred through a now-patched Zero-Day vulnerability. Details

Slack bug exposed user's hashed passwords

Slack reseted the password for approximately 0.5% of its users in response to an issue that was exposing hashed passwords to workspace members. Details

GitHub Copilot AI generating unsecure code

Researchers found that code suggestions made by the GitHub AI-based development bot "Copilot" contained exploited vulnerabilities about 40% of the time. Details

Google Chrome Zero-Day

Google releases a fix for an actively exploited zero-day vulnerability (CVE-2022-2856), which consists in a flaw in user-input validation. Details

UPCOMING EVENTS

BSides Montreal

Gray Cover: The dangers of CloudShells

10 September 2022

Montreal, QC, CA

Swiss Cyber Storm

Detecting Cloud Command and Control

25 October 2022

Kursaal Bern, Bern, Switzerland

RECENT PUBLICATIONS

Detecting Ransomware on Unmanaged Devices

If an unmanaged device is infected with ransomware, will the security operations team receive an alert? In this blog post, we illustrate how you can detect a ransomware infection on an unmanaged device by monitoring uploads to managed cloud apps. Blog

AsyncRAT: Using Fully Undetected Downloader

AsyncRAT is an open-source remote administration tool released on GitHub in January 2019. Netskope Threat Labs recently came across a FUD (Fully Undetected) Batch script which is downloading AsyncRAT from an Amazon S3 Bucket. Blog

Abusing Google Sites and Microsoft Azure for Crypto Phishing

Throughout 2022, Netskope Threat Labs found that attackers have been creating phishing pages in Google Sites and Microsoft Azure Web App to steal cryptocurrency wallets and accounts from Coinbase, MetaMask, Kraken, and Gemini. These phishing pages are mimicking the real websites, avoiding typos to make the page look real, and even interacting with victims through a live web chat. Blog

Ousaban: LATAM Banking Malware Abusing Cloud Services

Ousaban (a.k.a. Javali) is a banking malware that emerged between 2017 and 2018, with the primary goal of stealing sensitive data from financial institutions in Brazil. Netskope Threat Labs came across recent Ousaban samples that are abusing multiple cloud services throughout the attack flow, targeting more than 50 financial institutions in Brazil. 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.

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.