July 2022

Netskope Threat Labs Report

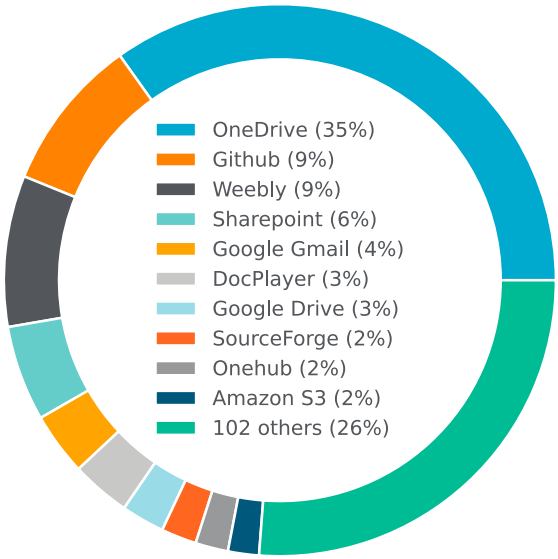
IN THIS REPORT

- **Cloud-enabled threats:** Weebly continues to hold one of the top spots for malware downloads and was joined by DocPlayer, with both being abused to deliver malicious PDFs that redirect victims to phishing, spam, scam, and malware distribution websites.
- **Malware & phishing:** The top five phishing sites continue to be hosted on Weebly and Blogger, as those platforms continue to be favored by attackers.
- **Ransomware:** The top ransomware families included the cross-platform RedAlert and Redeemer, a free ransomware builder being advertised on hacker forums.

netskope
THREAT LABS

CLOUD-ENABLED THREATS

In July, Netskope detected malware downloads originating from 112 distinct cloud apps. Compared to June, OneDrive remained in the top spot, used to deliver a variety of different types of malware, and Weebly remained in the number three spot as it continues to be abused to deliver malicious PDF files that redirect victims to phishing, spam, scam, and malware websites. DocPlayer, a document-sharing service, made its first-ever appearance in the top ten as the result of malicious PDF files being shared on the service.



Top apps for malware downloads July 2022

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

NPM software supply chain attack

Researchers uncovered a supply chain attack that delivers malicious JavaScript via the NPM package manager. Details

Sensitive airport data exposed via S3 bucket

A misconfigured S3 bucket was publicly exposing 3TB of sensitive data, including employee PII, information about planes, GPS coordinates, and fuel lines. Details

Known scam reaches Discord

Attackers are using known scam techniques, including scaring the person with fake messages, to steal Discord accounts. Details

Rozena backdoor abusing Discord

Researchers found a phishing campaign that uses the Follina vulnerability to deliver the Rozena backdoor, which is hosted on Discord. Details

Cryptocurrency-mining malware abusing cloud

Recent research shows how attackers are abusing cloud-based systems to deploy cryptocurrency-mining malware and generate profit from their attacks. Details

Attackers abusing GitHub metadata

Research shows how attackers can abuse GitHub metadata to deceive users into using a malicious repository. Details

MacOS spyware abusing cloud

A new MacOS malware named CloudMensis was discovered, which is a spyware that abuses cloud apps to download payloads and conduct C2 communication. Details

New malware targeting Facebook

A new infostealer malware targeting Facebook Business accounts was discovered, used by a threat actor in an operation named as DUCKTAIL. Details

NPM package abusing Discord

Researchers identified a new malicious campaign named LofyLife, delivering malware via NPM packages that are able to steal Discord tokens and bank card data. 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 new phishing domains continue to be dominated by Weebly and Blogger. After a two-month absence, the Discord CDN once again returned to the top five malware distribution domains.

Malicious domains:

1. laconicgrains[.]com
2. hunter.libertylawaz[.]com
3. perfectway[.]me
4. secure.etym6cero[.]com
5. amigodlex[.]com

Phishing domains:

1. to-exploregate.blogspot[.]com
2. shutterislandsid4.blogspot[.]com
3. lebftegfbst.weebly[.]com
4. plbebgdtb.weebly[.]com
5. securemybtapp000.weebly[.]com

Malware distribution domains:

1. static.s123-cdn-static[.]com
2. static1.squarespace[.]com
3. cdn.discordapp[.]com
4. uploads.strikinglycdn[.]com
5. d14jiafrlzkcus.cloudfront[.]net

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. **Emotet** is a malware strain commonly spread using malicious Office documents and LNK files.
3. **Zusy** is a banking Trojan that targets Microsoft Windows and is derived from Zeus.
4. **Talu** is a Trojan used to deliver a variety of different types of malware, including infostealers.
5. **Duba** is a browser hijacker that redirects search engine traffic.

RANSOMWARE

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

1. **Black Basta** was first discovered in April 2022 and has both Windows and Linux variants.
2. **Mauicrypt** was first discovered in early 2021 and is linked to North Korea.
3. **RedAlert** is a cross-platform ransomware that targets both Windows and ESXi servers.
4. **Redeemer** is a free ransomware-builder being advertised on hacker forums.
5. **SiennaBlue** is associated with H0lyGh0st and written in Go.

Hive ransomware upgraded to Rust

Researchers spotted a new version of Hive which includes a full code migration from GoLang to Rust, also containing improvements in the encryption method. Details

APT group targeting healthcare with ransomware

A new joint cybersecurity advisory provides information about Maui ransomware, which is being used by attackers to target healthcare organizations. Details

Decryptor for AstraLocker

Researchers released a free decryption tool for AstraLocker ransomware, which announced its retirement on the 4th of July weekend. Details

New ransomware named Lilith

A new ransomware named Lilith emerged in July 2022, developed with C/C++ and targeting 64-bit versions of Windows. Details

New ransomware named HavanaCrypt

HavanaCrypt is a new ransomware family that emerged in July 2022, disguising itself as a "Google Software Update" application. Details

H0lyGh0st ransomware targeting businesses

North Korean attackers tracked as DEV-0530 (a.k.a. H0lyGh0st) found targeting small and midsize businesses with ransomware. Details

Lockbit 3.0 and Blackmatter

Researchers found similarities between Lockbit 3.0, which was released in June 2022, and Blackmatter ransomware. Details

LockBit 3.0 abusing Windows Defender

Attackers are abusing the Microsoft Defender's command line tool to side-load a DLL that delivers Cobalt Strike beacons. 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 July:

Attackers behind the TrickBot malware have shifted its focus to target Ukraine — July 7, 2022

The UAC-0056 group (a.k.a. TA471) is targeting Ukraine with Cobalt Strike — July 13, 2022

A report shows an increase in the number of cyber attacks against Ukraine on Q2 of 2022 — July 13, 2022

A state-sponsored group known as Tonto Team is increasing espionage activity against Russia — July 13, 2022

Russian attackers using fake DoS tool to target pro-Ukrainian activists — July 19, 2022

The U.S. CNMF released a list of IOCs related to malware seen in Ukraine — July 21, 2022

Attackers hacked a Ukrainian radio station to spread false news about Zelensky health — July 22, 2022

The United States and Ukraine are expanding the cooperation on cybersecurity — July 27, 2022

Industrial control systems infected via "cracking" tools

Attackers are using malicious password recovery tools to infect industrial control systems (ICS) with Sality malware, creating a peer-to-peer botnet. Details

Microsoft resumes VBA protection

After quietly reversing the protection against VBA macros on files downloaded from the internet, Microsoft re-enables the protection. Details

UPCOMING EVENTS

DEF CON Cloud Village

OAuth-some Security Tricks: Yet more OAuth abuse

13 August 2022

Las Vegas, NV

BSides Montreal

Gray Cover: The dangers of CloudShells

10 September 2022

Montreal, QC, Canada

RECENT PUBLICATIONS

Netskope Threat Coverage: Microsoft Discloses New Adversary-in-the-Middle (AiTM) Phishing Attack

On July 12, 2022, Microsoft researchers disclosed a large-scale phishing campaign that has targeted more than 10,000 organizations since September 2021. The campaign used adversary-in-the-middle (AiTM) phishing sites to proxy the authentication process and hijack the victims' Office 365 session cookies. Blog

Microsoft's Macro Reversal Invites a Resurgence of Office Malware

In January 2022, Microsoft announced that Excel 4.0 macros would be restricted by default, to protect users from malicious macros. In February 2022, Microsoft announced that VBA macros would also be blocked for files downloaded from the internet. Cybersecurity professionals and enthusiasts rejoiced at the news! Then, on July 7, 2022, Microsoft quietly reversed course, re-enabling VBA macros for files downloaded from the internet. 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.