October 2022

Netskope Threat Labs Report

IN THIS REPORT

| **Cloud-enabled threats:** Microsoft OneDrive has been in the top spot for more than six months, used to download a variety of Trojans. Its position is a reflection of its overall popularity in the enterprise.

| **Malware & phishing:** Free web hosting services and content delivery networks continue to be popular tools used by attackers to deliver malware and phishing content. For the second month in a row, an IPFS service also made the top list, as attackers abused it to deliver illicit content.

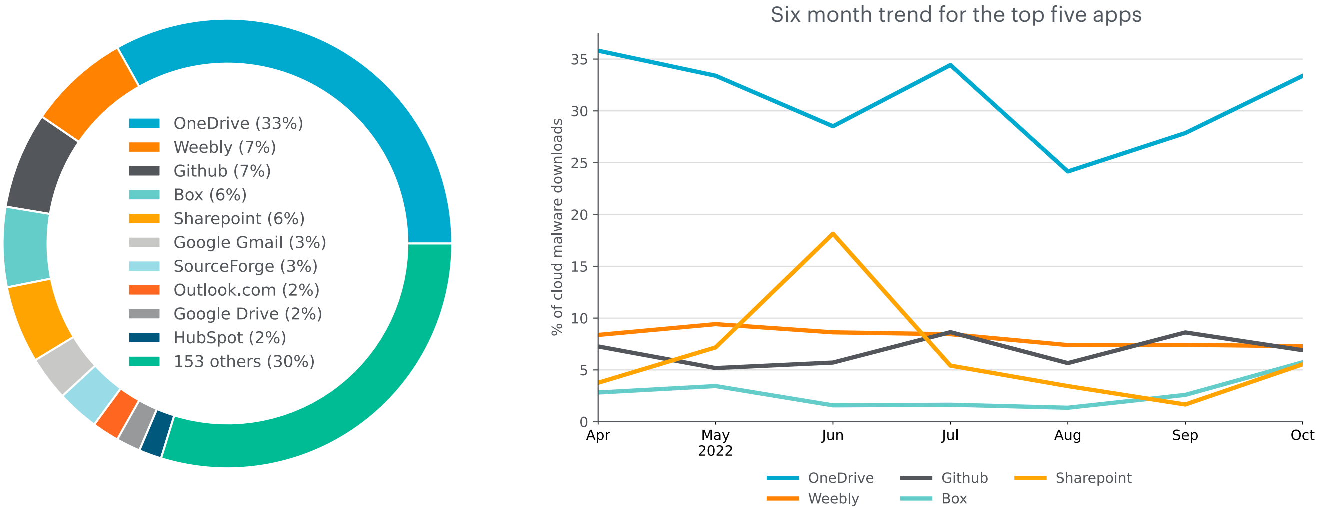
| **Ransomware:** Prestige, a ransomware family recently used to target Ukrainian organizations that were previously targeted with HermeticWiper, entered the top five this month.

netskope
THREAT LABS

CLOUD-ENABLED THREATS

In October, Netskope detected malware downloads originating from 163 distinct cloud apps. Microsoft OneDrive, used to deliver a variety of different types of malware, continues to hold the top spot, where it has been for more than six months. Compared to September, the share of cloud malware downloads from Microsoft OneDrive increased slightly. The share of cloud malware downloads coming from Box and SharePoint also increased slightly, propelling both back into the top five. HubSpot made its first appearance in the top ten due to a variety of Trojans being delivered via its CDN.

Top apps for malware downloads | October 2022



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

LofyGang abusing multiple cloud services

Researchers found over 200 malicious NPM packages linked to a group known as LofyGang, which is abusing multiple cloud services throughout the attack, including GitHub, Discord, and Glitch. Details

APT group abusing multiple cloud services

Researchers disclosed information about an APT group named POLONIUM, which abuses common cloud services for C2 communication, including Dropbox, OneDrive, and Mega. Details

Cryptomining campaign abusing cloud resources

A new and automated campaign was found abusing GitHub, Buddy, and Heroku services to mine cryptocurrency using free-tier accounts. Details

Malware attempting to steal AWS EC2 access keys and tokens

Researchers found malicious samples trying to steal Amazon Elastic Compute Cloud (EC2) access keys and tokens via typosquatting and legitimate tools. Details

RepoJacking technique abusing GitHub

Researchers disclosed a new technique named RepoJacking that consists of hijacking a renamed GitHub repository and routing the traffic to a malicious repository instead. Details

Malware abusing IIS logs for C2

A new backdoor used by Cranefly threat actors was found abusing IIS to perform C2 communication, by reading the commands from legitimate log files. 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 second month in a row, an IPFS domain appears in the toplists. Free hosting service Weebly, multiple CDNs, and free document hosting services also continue to appear in the toplists.

Malicious domains:

1. notifyoutspoken[.]com
2. radiusdressing[.]com
3. totalpopper[.]com
4. entrancementcards[.]weebly[.]com
5. zeroedglass[.]com

Phishing domains:

1. dormdolls[.]com
2. revolknfts[.]netlify[.]app
3. reyah435324login[.]weebly[.]com
4. llantasmex[.]com
5. wejibuxod[.]weebly[.]com

Malware distribution domains:

1. static[.]s123-cdn-static[.]com
2. cdn-cms[.]f-static[.]net
3. download[.]pdf00[.]com
4. docplayer[.]net
5. ipfs[.]io

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

1. **PhishingX** is a malicious PDF file used as part of a phishing campaign to redirect victims to a phishing page.
2. **Khalesi** is an infostealer that was first discovered in 2018.
3. **PDFka** is a PDF file that exploits CVE-2010-0188 for arbitrary code execution.
4. **AgentTesla** is a Remote Access Trojan (RAT) and keylogger written in .NET that has been around since 2014.
5. **Remcos** is a Remote Access Trojan (RAT) that has been around since 2016 and is typically delivered via malicious Microsoft Office documents.

RANSOMWARE

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

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. **Prestige** has been used to target victims in Ukraine who were previously targeted with HermeticWiper.
4. **Black Basta** was first discovered in April 2022 and has both Windows and Linux variants.
5. **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.

BlackByte abusing Windows driver

Operators of the BlackByte ransomware group were found abusing a vulnerable and legitimate Windows driver to bypass security solutions. Details

LockBit using zero-day to infect Microsoft Exchange

Microsoft is investigating a possible zero-day vulnerability that was used by LockBit to infect Exchange servers and deploy ransomware attacks. Details

Venus ransomware targeting public remote desktops

The recently discovered Venus ransomware was found abusing publicly-exposed remote desktop services to infect and encrypt Windows devices. Details

Black Basta ransomware using Qakbot

The Black Basta ransomware group was spotted using Qakbot malware to deploy the Brute Ratel C2 framework through the attack chain. Details

BlackByte using new exfiltration tool

An affiliate of the BlackByte ransomware group was found using a new tool to exfiltrate data named “ExByte”, able to quickly steal data from Windows devices. Details

Joint advisory about DAIXIN ransomware

The FBI, CISA, HHS, and the Department of Health released a joint advisory about DAIXIN ransomware group, which has been targeting healthcare in the U.S. Details

TommyLeaks extortion group and SchoolBoys ransomware

Researchers have found a link between a new extortion group named TommyLeaks with a new ransomware gang named SchoolBoys, which is using the leaked LockBit builder. Details

Magniber ransomware targeting home users

A new ransomware named Magniber was found targeting home computers, disguising itself as an operating system update. Details

Vice Society group targeting education sector with multiple ransomware

The threat group known as Vice Society is targeting the education sector in the U.S. and worldwide, using multiple ransomware families, including BlackCat, QuantumLocker, and Zeppelin. 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 October:

Ukraine enhanced its cybersecurity cooperation with EU agencies — October 10, 2022

The pro-Russian group KillNet claimed responsibility for DDoS attacks on US Airports — October 11, 2022

New ransomware attack targeting transportation and logistics sectors in Ukraine and Poland — October 17, 2022

Pro-Russia attackers targeting Bulgarian government with DDoS attacks — October 18, 2022

Internet in Ukraine was disrupted whilst the Russian army was conducting an operation — October 20, 2022

Ukraine is warning of a possible Cuba ransomware campaign spread through phishing emails — October 25, 2022

An unknown attacker is targeting Ukrainian military with the RomCom remote access trojan — October 26, 2022

Allegedly LAPSUS$ member arrested in Brazil

In an operation named "Dark Cloud", the Brazilian Federal Police arrested a suspect that is allegedly a member of the LAPSUS$ hacking group, after investigating the Brazilian Ministry of Health breach. Details

DDoS botnet asking ransom

A DDoS botnet known as Fodcha was found injecting ransom messages into network packets, demanding payment to stop the DDoS attack. Details

Microsoft Mark-of-the-Web zero-day

An actively exploited zero-day that allows the bypass of the Mark-of-the-Web on Windows can be unofficially patched, until Microsoft releases the official security update. Details

UPCOMING EVENTS

OWASP Global AppSec
Defending Against Chained Attacks on Your SSO/OAuth Identity System
Jenko Hwong — November 18, 2022
San Francisco, CA

BSides São Paulo
BlackCat Ransomware: Tactics and Techniques From a Targeted Attack
Gustavo Palazolo — November 20, 2022
São Paulo, Brazil

BSides London
Cloud Chatter: Defending Against Cloud C2
Dagmawi Mulugeta — December 10, 2022
London, England

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.