November 2022

Netskope Threat Labs Report

IN THIS REPORT

Cloud-enabled threats: For the first time in more than six months, Weebly fell out of the top five as the share of cloud malware downloads originating from Weebly decreased relative to other apps.

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 third month in a row, an IPFS service also made the top list, as attackers abused it to deliver illicit content.

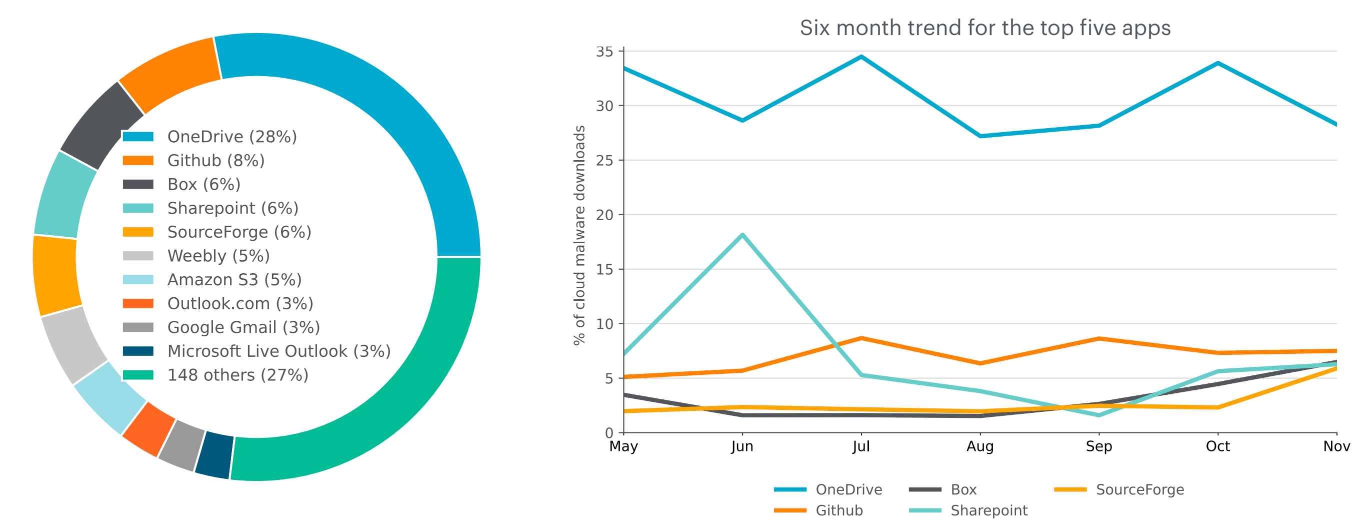
Ransomware: Black Basta was the top ransomware family in November, targeted primarily at companies based in the US.

netskope
THREAT LABS

CLOUD-ENABLED THREATS

In November, Netskope detected malware downloads originating from 158 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 October, Weebly fell out of the top five and was supplanted by SourceForge. Weebly had been in the top five for the past six months.

Top apps for malware downloads | November 2022



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

Worok hackers abuse Dropbox API to exfiltrate data

Worok Hackers use DropboxControl, an information-stealing implant that uses a Dropbox account for command-and-control, enabling the threat actor to upload and download files to specific folders as well as run commands. Details

North Korean hackers use Dolphin backdoor that abuses Google Drive

North Korea-linked ScarCruft group has been linked to a previously undocumented backdoor called Dolphin that abuses cloud services like Google Drive for data exfiltration as well as command-and-control. Details

Chinese hackers use Google Drive to drop malware

State-backed Chinese hackers launched a spear phishing campaign to deliver custom malware stored in Google Drive. Details

Attackers abusing Google Ads to deliver infostealer malware

Malicious Google Ad was sending victims to a GIMP.org look alike website that was hosting malware. Details

Hackers abusing Google Ads to distribute Royal Ransomware

Attackers were using Google Ads in a campaign to distribute various post-compromise payloads, including the recently discovered Royal ransomware. Details

AXLocker ransomware found stealing Discord credentials

The new AXLocker ransomware family is not only encrypting victims' files and demanding a ransom payment but also stealing victims' Discord accounts. Details

Attackers are abusing Microsoft Azure Web Apps services to bypass MFA

Attackers are conducting a crypto-stealing phishing campaign that abuses Microsoft Azure Web Apps service to bypass multi-factor authentication and gain access to accounts on Coinbase, MetaMask, Crypto.com, and KuCoin. Details

Cyber criminals use of Go-based Aurora Stealer malware

A novel Go-based malware dubbed Aurora Stealer is being deployed through the use of YouTube videos and cracked software download websites. Details

Ducktail hackers now use WhatsApp to phish for Facebook ad accounts

A cybercriminal operation tracked as Ducktail has been abusing WhatsApp to lure victims into executing malicious payloads or provide access to their Facebook business account. Details

Hackers are using trending TikTok "Invisible Challenge" to spread malware

Threat actors are capitalizing on a popular TikTok challenge to trick users into downloading information-stealing malware. Details

Attackers abusing Microsoft Voicemail in phishing campaigns

Researchers are warning of a new phishing campaign that abuses Microsoft Dynamics 365 Customer Voice to trick recipients into handing over their credentials. Details

Malicious packages hosted in PyPI delivering W4SP stealer

Researchers have discovered 29 packages in the official Python Package Index (PyPI) repository designed to infect developers' systems with an info-stealing malware dubbed W4SP 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. 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. wastedinvaluable[.]com
2. specialistinsensitive[.]com
3. fastofferspot[.]com
4. bafybeiehpya3iydyrpoaxdbfc2tfpdq24ofrssqvfxugbuyfqjlwkhvz5a[.]ipfs[.]w3s[.]link
5. ayvalikbalikcisikusadasi[.]com

Phishing domains:

1. kavachauthentication[.]blogspot[.]com
2. brunutssopo[.]live
3. personalizados-carimbos[.]blogspot[.]com
4. livrariacaritatem[.]blogspot[.]com
5. xtrip-com[.]blogspot[.]com

Malware distribution domains:

1. cdn[.]discordapp[.]com
2. static[.]s123-cdn-static[.]com
3. cdn-cms[.]f-static[.]net
4. s1-filecr[.]xyz
5. docplayer[.]net

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. **AgentTesla** is a Remote Access Trojan (RAT) and keylogger written in .NET that has been around since 2014.
3. **PDFka** is a PDF file that exploits CVE–2010–0188 for arbitrary code execution.
4. **Kutaki** is an infostealer and keylogger first seen in 2019.
5. **Farfli** is an old Remote Access Trojan (RAT) frequently modified and used by multiple APT groups.

RANSOMWARE

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

1. **Black Basta** was first discovered in April 2022 and has both Windows and Linux variants.
2. **Prestige** has been used to target victims in Ukraine who were previously targeted with HermeticWiper.
3. **LockBit** is a ransomware group whose builder was leaked in September 2022.
4. **ChileLocker** is a ransomware variant used to target government agencies in Chile.
5. **SiennaBlue** is associated with H0lyGh0st and written in Go.

Black Basta ransomware linked to FIN7

The individuals behind the Black Basta ransomware have been linked to hacking operations conducted by the FIN7 threat actors. Details

Black Basta is actively infiltrating companies with Qakbot

A Qakbot malware campaign has been targeting U.S. companies to install Black Basta ransomware. Details

Black Basta and BlackByte continue to target critical infrastructure

Researchers found that from the victim organizations listed on the BlackByte and Black Basta data leak sites, many are part of critical infrastructure sectors. Details

Azov ransomware is a data wiper

The Azov Ransomware has been found to be a data wiper that intentionally destroys victims' data. Details

Amadey malware deploying LockBit 3.0 ransomware

A LockBit 3.0 ransomware affiliate is using phishing emails to install the Amadey Bot and take control of devices. Details

Alleged LockBit ransomware member arrested in Ontario

A Russian and Canadian national has been charged with conspiracy in connection with LockBit. Details

DEV-0569 delivering Royal ransomware

DEV-0569, a new threat actor whose activity can be traced back as early as August 2022, developed new tools to deliver the Royal ransomware. Details

Hive ransomware makes $100 million

The Hive ransomware gang has victimized more than 1,300 businesses, receiving over $100 million in ransom payments over the past year and a half. Details

Donut extortion group also targets victims with ransomware

The Donut extortion group has been confirmed to deploy ransomware in double-extortion attacks on the enterprise. Details

RansomExx ransomware variant rewritten in Rust

The operators of the RansomExx ransomware have become the latest to develop a new variant fully rewritten in the Rust programming language. Details

Ransomware gang targets Belgian municipality but hits police instead

The Ragnar Locker ransomware gang has accidentally published stolen data from Zwijndrecht police, a local police unit in Antwerp, Belgium. Details

Trigona ransomware spotted in increasing attacks worldwide

A previously unnamed ransomware group has rebranded under the name Trigona, launching a new Tor negotiation site where they accept Monero as ransom payments. Details

Quantum Locker gang conducting ransomware extortion on Microsoft Azure

Quantum Locker gang demonstrated capabilities to operate ransomware extortion even on cloud environments such as Microsoft Azure. 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 November:

RomCom threat group, previously targeting Ukraine, is now targeting UK — November 04, 2022
Microsoft reports a disturbing rise in nation state activity — November 04, 2022
Russian Hackers blamed for Prestige ransomware attacks on Ukraine — November 11, 2022
Earth Longzhi APT targeting Ukraine and Asian countries — November 14, 2022
Ukrainian CERT discovered new data-wiping campaign — November 14, 2022
Ukraine's army stops 1,300 cyberattacks — November 16, 2022
Botnets, Trojans, and DDoS from Ukraine and Russia have increased — November 16, 2022
Pro-Russian hacktivists take down EU Parliament site in DDoS attack — November 23, 2022
New ransomware attacks in Ukraine linked to Russian Sandworm hackers — November 25, 2022
RansomBoggs ransomware targeted several Ukrainian organizations — November 26, 2022

Emotet returns with high-volume malspam campaign

The notorious Emotet malware has returned as part of a malspam campaign designed to drop payloads like IcedID and Bumblebee. Details

Cyber attack blocked trains in Denmark

A cyber attack caused trains operated by DSB to stop in Denmark. Details

StrelaStealer malware steals Outlook and Thunderbird credentials

A new information-stealing malware named StrelaStealer is actively stealing email account credentials from Outlook and Thunderbird. Details

Over 250 US news websites deliver malware via supply chain attack

Hundreds of regional and national news websites in the United States are delivering malware as a result of a supply chain attack involving one of their service providers. Details

RECENT NETSKOPE PUBLICATIONS

BlackCat Ransomware: Tactics and Techniques From a Targeted Attack

Netskope Threat Labs analyzes BlackCat and shows some of the tactics and techniques from a recent ransomware incident. The evidence shows that this was a targeted attack, where the attackers were mainly focused on stealing sensitive data from the organization and infecting as many devices as possible. Blog

Cloud Abuse: New Technique Using Adobe Acrobat to Host Phishing

Netskope Threat Labs recently discovered a phishing campaign that is abusing Adobe Acrobat to host a Microsoft Office phishing page. While abusing free cloud services to host malicious content is a popular attack technique, this is the first time we have seen Adobe Acrobat used to deliver malicious content. Blog

New Phishing Technique Targeting Over 20 Crypto Wallets

Netskope Threat Labs spotted a new crypto-phishing attack that aims to steal sensitive data from crypto wallets, including private keys and security recovery phrases, disguising itself as a service to revoke stolen ERC (Ethereum Request for Comments) assets. The page was created and hosted with Netlify, which is a free cloud service to create websites and apps. Blog

Netskope Threat Coverage: Prestige Ransomware

In October 2022, a novel ransomware named Prestige was found targeting logistics and transportation sectors in Ukraine and Poland. Blog

Netskope Threat Labs: What We'll See In 2023

Continuing our ongoing series of expert predictions, our 2023 predictions include what we see on the horizon for software supply chain, phishing, and ransomware. 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.