September 2022

Netskope Threat Labs Report

IN THIS REPORT

Cloud-enabled threats: Microsoft OneDrive continues to top the list for malware downloads, while Weebly fell into third place behind GitHub.

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

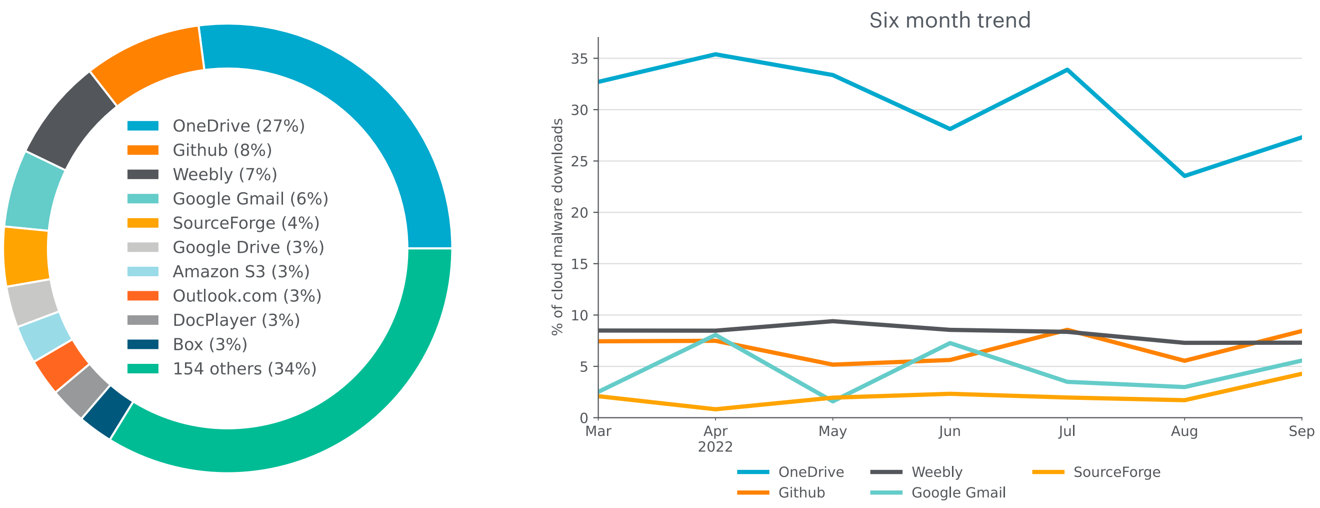
Ransomware: Zeppelin, a ransomware-as-a-service family written in Delphi and targeting Windows entered the top five this month.

netskope
THREAT LABS

CLOUD-ENABLED THREATS

In September, Netskope detected malware downloads originating from 164 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 August, Weebly fell to third as the percentage of malware downloads from GitHub increased slightly. Malware downloads from SourceForce and Gmail also increased slightly, moving both into the top five this month.

Top apps for malware downloads September 2022



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

Vulnerability in TikTok's app could allow for account hijacks

A new high severity vulnerability was found in the Android application of TikTok's app (CVE-2022-28799), which may allow attackers to remotely hijack user accounts. Details

Attackers phishing for Steam accounts

Researchers found a phishing campaign that is using the "browser in a browser" technique to steal Steam credentials. Details

Self-spreading malware abusing YouTube

A new malware was found abusing compromised YouTube channels to self-spread through fake video tutorials, delivering multiple malware including RedLine Stealer. Details

New Microsoft Teams vulnerability

Researchers found a vulnerability on Microsoft Teams that allows attackers to impersonate employees via access tokens. Details

PrivateLoader abusing vk.com

New research shows that PrivateLoader malware has shifted from Discord attachments to vk.com documents to host second stage payloads. Details

Microsoft Teams GIFShell attack

A security researcher found a new attack technique that consists of abusing Microsoft Teams features for C2 communication and data exfiltration via GIF files. Details

Attackers abusing LinkedIn to steal credit cards

A new malicious campaign was found where attackers are abusing the Smart Links feature of LinkedIn Premium to harvest credit card data through phishing pages. Details

Attackers abusing Microsoft Exchange to spread spam

Researchers disclosed an attack where Microsoft Exchange was being used to spread spam via malicious OAuth applications deployed on compromised cloud tenants. Details

Attackers targeting GitHub accounts

A phishing campaign was spotted where attackers were impersonating a DevOps platform to steal credentials and two-factor authentication codes from GitHub accounts. 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 include a domain being used to host some elements of a phishing campaign in IPFS and multiple Weebly sites.

Malicious domains:

1. financialbom[.]us
2. fdsfdfsd[.]likes[.]fans
3. bafybeiacmku4gynwzjfgophrd63sluz5m7mxbnzjuyn3nrs66dxzlisi44[.]ipfs[.]w3s[.]link
4. esa365[.]azurewebsites[.]net
5. gaknupatra[.]weebly[.]com

Phishing domains:

1. negogesi[.]weebly[.]com
2. sushi-swap-home[.]weebly[.]com
3. sbcglobal-secure[.]weebly[.]com
4. unbloockyouraccount2022[.]weebly[.]com
5. sitebuilder176428[.]dynadot[.]com

Malware distribution domains:

1. cdn[.]discordapp[.]com
2. static[.]s123-cdn-static-d[.]com
3. static[.]s123-cdn-static[.]com
4. uploads[.]strikinglycdn[.]com
5. download[.]pdf00[.]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. **Khalesi** is an infostealer that was first discovered in 2018.
3. **Emotet** is a malware strain commonly spread using malicious Office documents and LNK files.
4. **Formbook** is a malware-as-a-service infostealer recently used to target Ukrainians.
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 September.

1. **Black Basta** was first discovered in April 2022 and has both Windows and Linux variants.
2. **Zeppelin** is a ransomware-as-a-service family written in Delphi and targeting Windows.
3. **RedAlert** is a cross-platform ransomware that targets both Windows and Linux ESXi servers.
4. **Redeemer** is a free ransomware-builder being advertised on hacker forums.
5. **SiennaBlue** is associated with H0lyGh0st and written in Go.

BianLian ransomware group growing activity

New research shows that the BianLian ransomware group has become increasingly active since its discovery in late 2021, using the ProxyShell vulnerability to gain initial foothold. Details

Vice Society ransomware targeting education sector

A new Cybersecurity Advisory (CSA) warns about the Vice Society ransomware group targeting the education sector, using known tools such as PowerShell Empire and Cobalt Strike. Details

PHOSPHORUS ransomware details

Microsoft released details about multiple ransomware campaigns linked to DEV-0270 (a.k.a. Nemesis Kitten), which is a sub-group of PHOSPHORUS, an Iranian threat actor. Details

LockBit hit by DDoS attack

The LockBit ransomware-as-a-service group was a target of a DDoS attack that shut down their websites for an entire weekend, said to be in response to an attack made against the Entrust company. Details

Monti ransomware using Conti TTPs

Researchers found that the Monti ransomware group is mimicking Conti's tactics, techniques and procedures (TTPs), along with their tools and codes leaked earlier in 2022. Details

Universal decryptor for LockerGoga

BitDefender has recently released an universal decryptor for LockerGoga ransomware, identified in January 2019 after attacks against many U.S. and Norway companies. Details

Quantum and BlackCat distributed by Emotet

Researchers found that Emotet is now being used by Quantum and BlackCat ransomware-as-a-service groups, after Conti's official retirement. Details

BlackCat using new version of ExMatter exfil tool

Researchers released details about a new version of ExMatter, an exfiltration tool that is being used by BlackCat ransomware, capable of stealing data over SFTP and WebDav. Details

Bl00dy ransomware using leaked LockBit builder

A recently discovered ransomware group named Bl00dy started to use the recently leaked builder of LockBit 3.0 ransomware. Details

New ransomware named Royal

A new ransomware operation named Royal was found, targeting multiple corporations with ransom values reaching up to $2 million. 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 September:

Former members of Conti ransomware group targeting Ukrainian organizations — September 7, 2022

Cobalt Strike servers of ransomware groups targeted with anti-Russia messages — September 7, 2022

Ukraine shutters two more Russian bot farms used to spread disinformation — September 8, 2022

Russian attackers using new infostealer malware against Ukrainian organizations — September 15, 2022

The Russian Sandworm group found posing as Ukrainian telecom provider to deliver malware — September 19, 2022

Anonymous claimed to have leaked over 300,000 data of Russian reservists — September 23, 2022

Research shows details about multiple self-proclaimed hacking groups supporting Russia — September 23, 2022

Ukraine has taken down a hacking group that stole accounts of about 30 million Ukrainians — September 24, 2022

The Ukrainian military intelligence service is warning of a possible massive cyber-attack from Russia — September 25, 2022

Uber breached by Lapsus$ group

Uber has recently suffered a cyber attack by the LAPSUS$ group, where the attacker gained access through a compromised contractor account. Details

Cyber attack on Rockstar Games

The Rockstar gaming company was recently breached by the LAPSUS$ group, where the attacker leaked videos and parts of the source code related to Grand Theft Auto 6. Details

Google Chrome and Microsoft Edge leaking passwords

Researchers found that the spell-checking features present on Google Chrome and Microsoft Edge are leaking sensitive information, such as username and passwords. Details

Microsoft Exchange Zero-Day

Attackers are exploiting a new unpatched Zero-Day vulnerability in Microsoft Exchange, which allows remote code execution. Details

UPCOMING EVENTS

Swiss Cyber Storm

Detecting Cloud Command and Control
25 October 2022
Kursaal Bern, Bern, Switzerland

RECENT PUBLICATIONS

RedLine Stealer Campaign Abusing Discord via PDF Links

RedLine is an infostealer discovered in 2020, capable of stealing data such as credit card numbers, passwords, VPN and FTP credentials, gaming accounts, and even data from crypto wallets. In September 2022, Netskope Threat Labs found a RedLine Stealer campaign being spread through phishing emails. The email lures the user into opening a PDF file that redirects the victim to a URL that downloads RedLine, hosted on Discord. Netskope also found old versions of the same PDF file downloading other malware from Discord. Blog

Netskope Threat Coverage: LockBit's Ransomware Builder Leaked

The LockBit ransomware group was recently the target of two important events. The first one was a DDoS attack that took their websites down for a couple of days. And the second was a leak of the LockBit 3.0 (a.k.a LockBit Black) ransomware builder, which allows anyone to generate the necessary files to build LockBit payloads, such as the encryptor and decryptor. This blog covers both the timeline and the details of this leak. Blog

Attackers Continue to Abuse Google Sites and Microsoft Azure to Host Cryptocurrency Phishing

On August 9, 2022, Netskope released a blog post about a phishing campaign where attackers were abusing Google Sites and Microsoft Azure Web Apps to steal cryptocurrency wallets and accounts from many different targets. Over the past month, Netskope found that the attackers responsible for the phishing campaign have proven to be resilient to take-downs. Netskope also found new phishing pages mimicking Binance, Crypto.com, Gate.io, KuCoin, PancakeSwap, and Shakepay. 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.