June 2022

Netskope Threat Labs Report

IN THIS REPORT

Cloud-enabled threats: Weebly continues to hold one of the top spots for malware downloads, caused by a continuing pattern of malicious PDFs that redirect victims to phishing, spam, scam, and malware distribution websites. The same types of PDFs are also being distributed using Squarespace, Wordpress, and other platforms.

Malware & phishing: The top five phishing sites in June were all hosted on Weebly and Blogger, as those platforms continue to be favored by attackers. While Azure Blob storage did not make the top five, we saw an increase in traffic to phishing sites hosted on that platform.

Ransomware: Pandora and Black Basta, both newcomers in 2022, took the top two spots, followed by three families that have been around much longer: LokiLocker, Hive, and Lockbit.

netskope
THREAT LABS

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 June:

Anonymous group continues to target Russian organizations **- June 4, 2022**

Russia's Ministry of Construction, Housing and Utilities website reportedly hacked **- June 6, 2022**

Russian attackers are using the Follina exploit to deliver CredoMap and Cobalt Strike **- June 21, 2022**

Microsoft detected Russian attackers in multiple pro-Ukraine countries **- June 22,2022**

DarkCrystal RAT campaign targeting Ukrainian telecommunications operators **- June 24, 2022**

Ukrainian cyberpolice force arrested people behind over 400 phishing websites **- June 29, 2022**

Ukraine suffered almost 800 cyberattacks since February 2022 **- June 30, 2022**

New malware loader discovered

A new loader named SVCReady was discovered by researchers, using hidden shellcode inside Microsoft Office documents to deliver its payloads. Details

LNK files used for malware delivery

The use of LNK files to deliver malware has increased significantly since Microsoft released the protections against VBA and Excel 4.0 Macros (XLM). Details

New malware builder discovered

A new malware builder named Quantum Software was discovered, allowing the creation of loaders in multiple formats, including LNK, HTA, and ISO. Details

Racoon Stealer 2.0

After shutting down its operations in March 2022, Raccoon Stealer is back with a new version allegedly coded from scratch and sold in the MaaS model on underground forums. Details

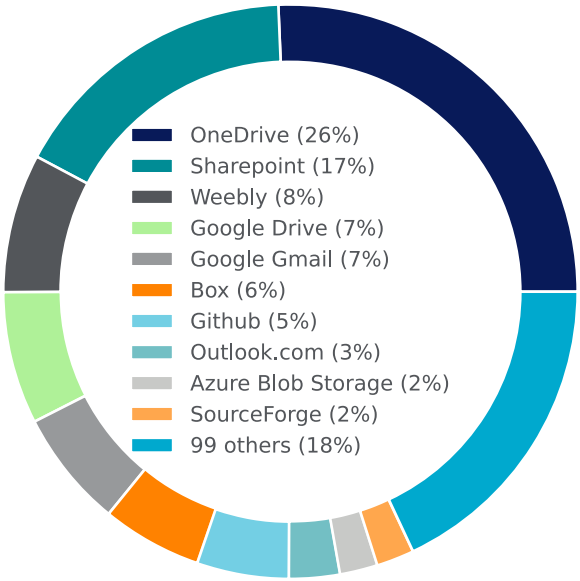
ABOUT THIS REPORT

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.

CLOUD-ENABLED THREATS

In June, Netskope detected malware downloads originating from 105 distinct cloud apps. Compared to May, OneDrive, Sharepoint, and Weebly remained in the top three spots. Weebly continues to be abused to deliver malicious PDF files that redirect victims to phishing, spam, scam, and malware websites. The same type of PDF files are also being spread by attackers on other platforms, including Squarespace and WordPress. Neither Amazon S3 nor Baidu Object Storage made the top 10 this month, supplanted by Azure Blob Storage and Outlook.com. Both Google Gmail and Outlook.com rose in the rankings, the result of an increase in malware being spread through email campaigns in June.



Top apps for malware downloads June 2022

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

Ransomware abusing multiple cloud services

Researchers have uncovered a ransomware named YourCyanide, which abuses multiple cloud services such as Discord, PasteBin and Microsoft throughout the payload download routine. Details

Python PyPI packages infected with infostealer

The PyPI packages “keep”, “pyanxdns”, and “'api-res-py” were infected with a backdoor present in a fake module named “request”. Details

Attackers using Log4Shell against VMware Horizon

The United States Coast Guard Cyber Command (CGCYBER) and CISA warned against attackers exploiting Log4Shell in VMware Horizon systems. Details

Attackers abusing QuickBooks Cloud Service

Researchers found phishing emails sent by attackers from QuickBooks cloud service, targeting companies across multiple industries. Details

Phishing campaign targeting Microsoft 365 users

Attackers are targeting Microsoft 365 users via phishing emails spoofing the MetaMask cryptocurrency support. Details

Python libraries targeting AWS data

Multiple Python packages available on PyPI repository were found stealing sensitive data such as AWS credentials, relaying the stolen data to publicly exposed endpoints. Details

YTStealer malware targeting YouTube

Researchers have uncovered a new malware named YTStealer, which was designed to steal authentication cookies from YouTube content creators. Details

Stealthy backdoor abusing Microsoft IIS

Researchers have discovered a backdoor that was created as a malicious module within Microsoft Internet Information Services (IIS). 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. In March and April, the top malicious domains were dominated by domain generation algorithm (DGA) domains consisting of two or three random words. In May and June, only one of the top malicious domains followed that pattern. For the first time in four months, some of the top domains came from TLDs other than com (co and xyz). The top new phishing domains included two cloud apps that have frequented the top five, Weebly and Blogger. Although it did not make the top five, we also saw an increase in traffic to phishing sites hosted in Azure Blob Storage in June (*.blob.core.windows.net). The Discord CDN did not make the top malware distribution domain list for the second month in a row, with the list dominated instead by other CDNs.

Malicious domains:

1. miamiblue[.]co
2. hospicalada[.]xyz
3. ukenthasc[.]xyz
4. mo9jr8ie6sier3an[.]com
5. sender.petanitest[.]com

Phishing domains:

1. www-bitflyer-go-com-br.blogspot[.]com
2. polygonxls-raylson.blogspot[.]com
3. biogbtge.weebly[.]com
4. hgdeuheijklw.weebly[.]com
5. spectrumonlineweb.weebly[.]com

Malware distribution domains:

1. static.s123-cdn-static[.]com
2. static1.squarespace[.]com
3. uploads.strikinglycdn[.]com
4. d6bqwyojjrctq.cloudfront[.]net
5. d38dspngxyp0cd.cloudfront[.]net

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

1. **PhishingX** is malicious PDF files that are generally 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. **Zmutzy** is an information stealer written in .NET that steals saved credentials and crypto wallets.
4. **Abracadabra** is a family of Excel spreadsheets containing malicious macros and using encryption to evade analysis.
5. **Razy** typically takes the form of malicious browser extensions that display malicious ads and steal data.

Abracadabra is one example of attackers continuing to abuse Microsoft Office documents to deliver malware. However, the format has been steadily losing popularity, driven in part by recent changes from Microsoft, including blocking VBA macros by default. In June, Office documents accounted for just 4% of all malware downloads, a marked decrease from the end of 2021, when malicious Office Documents represented more than 25% of all malware downloads.

RANSOMWARE

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

1. **Pandora** is likely based on the Babuk ransomware, and was actively targeting high-profile organizations in early 2022.
2. **Black Basta** was first discovered in April 2022 and has both Windows and Linux variants.
3. **LokiLocker,** unrelated to LokiBot or Locky, operates in the RaaS model and was first seen in August 2021.
4. **Hive** emerged in June 2021 and has been observed targeting organizations that many ransomware operators avoid.
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.

UNC2165 using LockBit

An APT group tracked as UNC2165 shifted to Lockbit ransomware probably to evade U.S. sanctions against the Evil Corp group, which overlaps with UNC2165. Details

Black Basta using QBot

The ransomware group known as Black Basta was found using Qbot malware (a.k.a. Qakbot) to extend their lateral movement capabilities. Details

New variant of Cuba ransomware

Researchers have observed a new version of Cuba ransomware, which emerged between March and April 2022. Details

Confluence RCE exploited to deliver ransomware

Internet-exposed Confluence servers are being targeted by attackers that are exploiting CVE-2022-26134 to deploy AvosLocker and Cerber2021 ransomware. Details

APT group deploying ransomware as decoy

Researchers found that the China-based APT group Bronze Starlight (a.k.a. APT10) is deploying multiple ransomware families to cover espionage operations. Details

AstraLocker 2.0 abusing Microsoft Office

A new version of the AstraLocker ransomware was found being distributed through malicious Microsoft Office files via phishing attacks. Details

LockBit 3.0

The ransomware group LockBit has released a new version (3.0), containing new characteristics including a bug bounty program and Zcash payment. Details

MedusaLocker alert

The FBI, CISA, and FinCEN released a cybersecurity advisory (AA22-181A) to provide information about MedusaLocker ransomware, observed in May 2022. Details

UPCOMING EVENTS

Roadsec
Quem habilitou as macros? Cenário de ataques via arquivos Microsoft Office
9 July 2022
São Paulo, SP - Brazil

DEF CON Cloud Village
OAuth-some Security Tricks: Yet more OAuth abuse
13 August 2022
San Francisco, CA

RECENT PUBLICATIONS

Emotet: Still Abusing Microsoft Office Macros

Netskope Threat Labs recently came across hundreds of malicious Office documents that are being used to download and execute Emotet via Excel 4.0 Macros (XLM), indicating that some attackers are still using old delivery methods in the wild despite the protections Microsoft released in 2022. 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.