netskope
THREAT LABS

March 2021

Netskope Threat Labs Report

TOP THREATS

From February 15, 2021, through March 15, 2021, the top five malicious domains included adware and phishing sites. The top five malware families included PDF documents used in phishing campaigns, remote access Trojans, and other Trojans. The top five cloud apps are those that were abused to deliver the most malicious content, including phishing baits and malware, as cybercriminals generally target the popular apps most aggressively.

Domains

1. agafurretor[.]com
2. crlink[.]cool
3. click[.]clickanalytics208[.]com
4. blameworthy[.]buzz
5. tracksmall[.]com

Malware

1. Document-PDF.Trojan.Phishing
2. Win32.Malware.Symmi
3. Win32.Trojan.Wacatac
4. Win32.Trojan.AgentTesla
5. Win64.Trojan.Glupteba

Apps

1. Amazon S3
2. OneDrive
3. SourceForge
4. Google Drive
5. GitHub

RECENT PUBLICATIONS

Understanding Cloud as an Attack Vector

In December, Netskope Threat Labs presented our work, "Cloud as an Attack Vector," at the 23rd International AVAR Cybersecurity Conference. You can find all the details in our AVAR blog post. Blog

Cloud and Threat Report: Shadow IT in the Cloud

The number of cloud apps in use in the enterprise increased by 20% in 2020 and 97% of apps in use in the enterprise are Shadow IT, or apps freely adopted by end users and business units. Blog

How Has Remote Work Changed After 1 Year of the COVID-19 Pandemic?

On this one-year anniversary of the COVID-19 pandemic declaration from the World Health Organization (WHO), we check back in on the remote work stats from the past year. Blog

Netskope Threat Coverage: DearCry Ransomware

On March 2, Microsoft released patches for four zero-day vulnerabilities affecting Exchange Server 2013, 2016, and 2019. In the following weeks, attackers have been aggressively targeting vulnerable servers to install web shells. Report

Cloud and Threat Report: Was 2020 the Year of the Malicious Office Document?

In the summer of 2020, there was a big, short-lived spike in malicious Office documents. Those documents contained malicious code that installed backdoors, ransomware, bankers, and other malware on unsuspecting victims' computers. Blog

THREAT ROUNDUP

A roundup of the top threats from February 15, 2021, through March 15, 2021.

Top stories:

HAFNIUM & MS Exchange exploits

Threat actor group HAFNIUM has been identified exploiting vulnerabilities in Microsoft Exchange servers. Details

DearCry ransomware

DearCry ransomware attacks Microsoft Exchange with ProxyLogon exploits. Details

Cloud-enabled threats:

MFA bypass to gain access to Microsoft accounts

Researchers identified an MFA bypass bug that could have allowed access to any Microsoft account. Details

Public Azure server

An insecure Azure server led to a data breach at Ticketcounter. Details

ServiceNow credentials exposed

Hundreds of ServiceNow credentials were exposed due to cloud misconfiguration issues. Details

NimzaLoader

New malware strain, dubbed NimzaLoader, makes use of phishing to download an executable hosted on Slack. Details

Hog ransomware

A new ransomware, called Hog, is abusing Discord to verify payment of ransom before decrypting files. Details

SendGrid abuse

SendGrid, a cloud mail provider, was abused by attackers to collect more than 400K Outlook and Office 365 credentials. Details

TeamTNT

Previously identified threat actor, TeamTNT, continues attacks in the cloud by targeting AWS credentials. Details

Earth Vetala

Researchers identified a new threat group, dubbed Earth Vetala, that leverages Onehub to distribute malware. Details

Google reCAPTCHA abuse

Phishing attacks use fake Google reCAPTCHA to swipe Office 365 credentials. Details

Google Apps Script abuse

Hackers are abusing Google Apps Script to bypass CSP and steal credit card information from victims. Details

Gootkit leverages Google SEO

Gootkit RAT expands delivery mechanisms by using Google SEO to distribute malware through compromised sites. Details

Google Alerts abuse

Threat actors are abusing Google Alerts to push fake Adobe Flash updates. Details

SolarWinds:

SolarWinds hackers downloaded Microsoft source code

Microsoft stated that SolarWinds hackers downloaded some Azure and Exchange source code. Details

SUNSHUTTLE

A new backdoor, dubbed SUNSHUTTLE, has been uncovered targeting a U.S.-based entity with possible connections to UNC2452. Details

New malware used by SolarWinds hackers

Researchers identified three new malware samples used by SolarWinds hackers. Details

SolarWinds webshell linked to Chinese hackers

New evidence suggests that malicious webshell deployed via zero-day in SolarWinds' Orion is linked to Chinese hackers. Details

Ransomware and cyber attacks:

Reported attacks

Reports of successful ransomware and cyber attacks against technology firms, transport agencies, financial entities, food supply agencies, research institutes, pharmaceuticals, and governments.

Automatic Funds Transfer Services (AFTS) hit by Cuba ransomware

Bombardier hit by Clop ransomware

Cashalo suffered a data breach

CompuCom has been hit by DarkSide ransomware

Dutch Research Council (NWO) confirms DoppelPaymer ransomware attack

European Banking Authority discloses Exchange server hack

Flagstar hit by Clop ransomware gang

Kia Motors has been hit by DoppelPaymer ransomware

Kroger has suffered a data breach due to vulnerable Accellion FTA software

Lactalis Group hit by cyberattack

Lakehead University shuts down campus network after cyberattack

Molson Coors brewing operations disrupted by cyberattack

Norway parliament data stolen in Microsoft Exchange attack

NSW Transport agency extorted by Clop ransomware gang after Accellion attack

Polecat hit by Meow attack and exposed 30TB of records

Spanish government agency for labor hit by Ryuk ransomware

TietoEVRY has suffered a ransomware attack

US building contractor Hoffman Construction suffered a data breach

Underwriters Laboratories (UL) hit by a ransomware attack

Accellion attacks linked to Clop
The recent, and highly effective, Accellion attacks linked to the Clop ransomware gang and FIN11. Details

Ryuk gets worm-like features

Ryuk ransomware variant discovered that uses scheduled tasks to spread to other Windows LAN devices. Details

SunCrypt and QNAPCrypt

Researchers identified links between SunCrypt and QNAPCrypt ransomware. Details

Malware:

Malicious Firefox extension

Researchers have identified a new campaign targeting Tibetan communities' Gmail accounts with a malicious Firefox extension, similar to Linkr. Details

ObliqueRAT

Researchers identified a new campaign that uses malicious Microsoft Office documents to spread ObliqueRAT. Details

APOMarcoSploit

The threat actors behind APOMarcoSploit, a tool used to generate Advanced Malicious Office Documents have been unmasked. Details

Verkada

Hackers access live surveillance cameras at numerous organizations due to exposed credentials. Details

Masslogger upgrades

Masslogger Trojan receives a new upgrade to steal credentials from Outlook, Discord, Chromium browsers, and many other applications. Details

Apple M1 malware

As covered in a Netskope Memo, the first malware sample designed for Apple M1 was discovered in the wild and was soon followed by more.

Shadow brokers exploit tools accessed before leak

Researchers identify new evidence that shows Chinese threat actors may have had access to the same tools leaked by The Shadow Brokers before they were published. Details

OceanLotus

OceanLotus targeted Human Rights Activists with sophisticated spyware. Details

LazyScripter

Researchers discover a new APT, dubbed LazyScripter, that uses phishing to target airlines. Details

PowerShell to pilfer QuickBooks files

Threat actors have been spotted using PowerShell scripts and malicious documents to exfiltrate QuickBooks data files. Details

NSDC links hacks to Russian-backed group

The National Security and Defense Council of Ukraine (NSDC) linked the hack of the government's document management system to Russian-backed hackers. Details

ThreatNeedle

Lazarus Group, North Korean-backed threat actor, has been spotted using a custom backdoor dubbed ThreatNeedle. Details

RedXOR

A new Linux malware, dubbed RedXOR, has been linked to Chinese Hackers. Details

zoMiner

zoMiner botnet probes for open ElasticSearch and Jenkins servers. Details

COVID-19 phishing

The US Department of Justice has seized its fifth domain with links to COVID-19 phishing. Details

Malvertistment

Malvertisers exploited browser-based WebKit zero-day to redirect users to scams. Details

Hotarus Corp

Ecuador's largest private bank and Ministry of Finance attacked by Hotarus Corp. Details