netskope
THREAT LABS

January 2021

Netskope Threat Labs Report

TOP THREATS

The top 5 malicious domains and malware samples that the Netskope Security Cloud platform blocked, and the top 5 apps for cloud malware delivery from which we blocked malicious downloads for 15 December 2020 through 15 January 2021.

Domains

1. d24ak3f2b[.]top
2. dgafgadsgkjg[.]top
3. popcorntime-upd[.]xyz
4. dnemkhkbsdbl[.]com
5. dolohen[.]com

Malware

1. Gen:Variant.Razy
2. JS:Trojan.Cryxos
3. Trojan.Emotet
4. VBA:Amphitryon
5. Win32.Rootkit.Connectscreen

Apps

1. Amazon S3
2. Dropbox
3. Box
4. OneDrive
5. Sharepoint

RECENT PUBLICATION

You Can Run, But You Can't Hide: Advanced Emotet Updates

Novel malware samples utilize two new techniques, namely Embedded XSL script and a Squiblytwo Attack, to evade detection.

Blog

THREAT ROUNDUP

A roundup of the top threats from 15 December 2020 through 15 January 2021.

Ransomware attacks

Reports of successful ransomware attacks against schools, technology firms, retail & appliance companies, pharmaceuticals, food supply agencies, transport agencies, and governments.

Aurora Cannabis's data sold by hacker after breaching their systems

Capcom disclosed that 390K people maybe affected by ransomware data breach

Dassault Falcon Jet reports data breach after being hit by Ragnar Locker ransomware attack

Forward Air hit by Hades ransomware

Funke Media Group, Germany's third largest publisher, hit by a ransomware attack

Kawasaki Heavy Industries reports a possibly year long data breach

Koei Tecmo hit with a cyber attack and hackers leaks stolen data

Lithuania's National Public Health Center hit by Emotet

Ransomware attack against GenRx Pharmacy leads to HIPAA disclosure

Reserve Bank of New Zealand suffered a data breach after exposed third party storage service

Roanoke College hit by likely ransomware attack

Sangoma hit with Conti ransomware attack

Scottish Environment Protection Agency (SEPA) hit by Conti ransomware

Symrise hit by Clop ransomware

T-Mobile data breach exposed phone numbers and call records

TransLink's confirms its recent Egregor ransomware attack was coupled with data theft

Vodafone's ho. Mobile has been the victim of a data breach

Whirlpool hit by Nefilim ransomware attack

SolarWinds attack

The following timeline shows the relevant events in the SolarWinds attack:

CISA officially confirm US govt hacks after SolarWinds breach — December 17, 2020

Hackers breached US govt using more than SolarWinds backdoor — December 17, 2020

SolarWinds hackers breach US nuclear weapons agency — December 17, 2020

Microsoft confirms breach in SolarWinds hack — December 17, 2020

US think tank breached three times by SolarWinds hackers — December 17, 2020

Microsoft identifies 40+ victims of SolarWinds hack — December 18, 2020

New SUPERNOVA backdoor found in SolarWinds cyberattack analysis — December 21, 2020

VMware confirms breach in SolarWinds hacking campaign — December 21, 2020

Microsoft says second hacker group may have also breached SolarWinds — December 22, 2020

SolarWinds victims revealed after cracking the Sunburst malware DGA — December 22, 2020

SolarWinds hackers breached US Treasury officials' email accounts — December 22, 2020

Microsoft says that SolarWinds hackers' goal was the victims' cloud data — December 29, 2020

US govt says Russian state hackers likely behind SolarWinds hack — January 5, 2021

SolarWinds hackers had access to over 3,000 US DOJ email accounts — January 5, 2021

US Judiciary adds safeguards for Office 365 email accounts after breach — January 7, 2021

Sunburst backdoor — code overlaps with Russian's Kazuar malware — January 11, 2021

SUNSPOT malware was used to inject SolarWinds backdoor — January 11, 2021

SolarLeaks site claims to sell data stolen in SolarWinds attacks — January 12, 2021

Babuk Locker

A new ransomware operation, named Babuk Locker, that uses strong Elliptic-curve encryption compromised 5 companies in 2021. Details

Chimera abuses cloud services

Researchers identified a threat group, Chimera, that abused Google and Microsoft cloud services like OneDrive and AzureEdge. Details

Gitpaste-12

Gitpaste-12, which abuses GitHub and Pastebin for its malicious campaign, has received an upgrade with a combined total of over 30 vulnerability exploits. Details

NSA guidance on temporary tokens

Similar to what Netskope has previously identified, the NSA has issued guidance to threat actors looking to access cloud resources by forging temporary SSO tokens. Details

GitHub and Imgur used to deploy Cobalt Strike payload

GitHub-hosted malware uses a PowerShell script that executes a malicious image downloaded from Imgur to deploy a Cobalt Strike payload. Details

Google Docs vulnerability affords screenshots of private documents

Recently patched vulnerability in Google Docs could have allowed hackers to grab screenshots of private documents. Details

Botnet steals Docker and AWS credentials

New malware botnet that is linked to a cybercrime operation, TeamTNT, steals Docker and AWS credentials. Details

Loki Bot

Researchers identified a new Loki Bot campaign that uses a technique of blurring images in documents to lure victims to enabling macros. Details

Malicious Chrome and Edge extensions

Similar to Lnkr, researchers have identified information stealing malware hidden in at least 28 third-party Google Chrome and Microsoft Edge extensions affecting around three million people. Details

CrowdStrike email compromise attempt

Attempts have been discovered to compromise cybersecurity firm Crowdstrike and access the company's perceived Office 365 email accounts. Details

Hackers bypassed MFA to access cloud service accounts

CISA pointed out that threat actors bypassed MFA to compromise cloud service accounts via a possible *'pass-the-cookie'* attack. Details

Mimecast SSL compromise

Email security company, Mimecast, disclosed a Microsoft 365 SSL certificate compromise that affected roughly 3,600 customers. Details

Pay2Key – Fox Kitten

Pay2Key ransomware operation has been attributed to Iranian threat group, Fox Kitten. Details

Joker's stash proxy seizure and shutdown

FBI and Interpol have allegedly seized proxy servers associated with Joker's Stash, the largest dark web marketplace, after which, Joker's Stash, announced its shutdown. Seizure Details, Shutdown Details

Safe-Inet

Safe-Inet, many cyber criminals' VPN of choice, has been shut down as part of Operation Nova, coordinated by US, Germany, Netherlands, Switzerland, France, and Europol. Details

SignSight

A supply chain attack, dubbed SignSight, was discovered targeting the Vietnam Government Certification Authority (VGCA) to compromise the software installers, hosted on the main website, with PhantomNet (SManager). Details

Operation Spalax

Researchers disclosed an ongoing surveillance campaign, Operation Spalax, directed against Colombian institutions in the energy and metallurgical industries. Details

PgMiner

Researchers discovered a new cryptojacking botnet operation, named PgMiner, that targets PostgreSQL database servers to install Monero miners. Details

IcedID

Threat actor TA551 has used IcedID malware as part of a malspam campaign that hosts Office documents that execute malicious macro code. Details

BumbleBee – xHunt webshell

Researchers have found a new webshell, named BumbleBee, as part of an ongoing xHunt espionage campaign that targeted Microsoft Exchange servers at Kuwaiti organizations. Details

Lazarus group

Lazarus group compromised government and pharmaceutical companies involved in COVID-19 research to deploy BookCodes and wAgent malware. Details

ElectroRAT

Researchers discovered a new RAT, dubbed ElectroRAT, written in Golang and compiled for Windows, Linux, and MacOS using Electron. Details

Dridex

Dridex campaign lures victims via fake Amazon gift card emails. Details

Wasabi knocked offline

Wasabi cloud storage knocked offline by DNS registrar for hosting malicious content. Details

XMRig

Golang-based worm has been actively dropping XMRig Monero miners on Windows and Linux servers. Details

Trump tape lure spreads QNode

New malspam campaign that lures victims with a fake Trump scandal tape spreads QNode malware. Details

Ezuri

Linux malware authors are using Ezuri, a crypter and memory loader written in Golang, to evade antivirus detection. Details

VBA self decode technique to inject RokRAT

Researchers identified malicious documents created in January, 2020 by North Korean threat group, APT 37, that used VBA self decode technique to inject RokRat. Details

OSAMiner

MacOS malware, OSAMiner, utilizes 'run-only' AppleScripts to complicate the decompiling process and evade analysis. Details

Google discloses hacking campaign

Google disclosed a highly sophisticated hacking campaign that targeted Windows and Android users. Details

Skimmers on popular ecommerce engines

Credit card skimmer found on stores powered by Shopify, BigCommerce, Zencart, and Woocommerce. Details

AutoHotkey credential stealer

Threat actors are distributing a new credential stealer written in AutoHotkey that targets US and Canadian banking users. Details

Winnti (APT 41)

Researchers have attributed a campaign that targets organizations that utilises Zeplin, a collaboration tool for designers and developers, to deploy a shellcode loader and a backdoor called Crosswalk. Details