EDITION - 23 | JULY 2020

THREATSPLOIT ADVERSARY REPORT

AN INITIATIVE BY BRISKINFOSEC

WWW.BRISKINFOSEC.COM

INTRODUCTION

At this New Normal situation keeping our data and systems safe is been a great challenge for several companies. Nowadays most of the organizations are stuck in the hands of the hackers. In this Report we have compiled few threats that are currently faced by several companies to give you a small walkthrough about the day today cyber issues. At present, companies are looking to have security embedded in their strategy and solutions, In order to minimize their exposure to risk as much as possible.

As Covid 19 is a threat to human life, currently cyber attack equally threatens all Public and Private Companies. They are also not aware, if their data is safe or is been watched by the hacker. To be away from those kinds of security issues, just contact a best Security Company. As several companies have not yet decided to get back to office in this pandemic situation contacting a security company is the best way for them to keep their system and data safe.

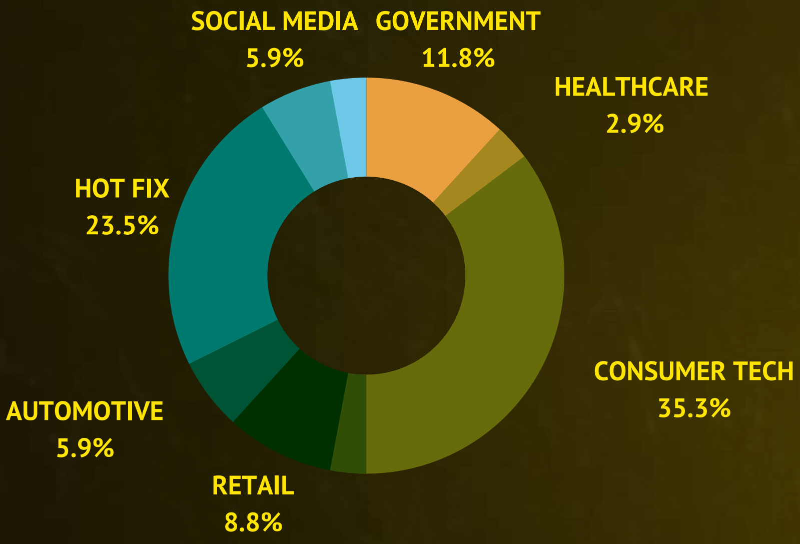
Cyber issues has been a huge concern for businesses in this WFH situation. Recent trends and cybersecurity statistics reveal a massive increase in hacked and breached data from sources that are increasingly common in the workplace, like mobile and IoT devices. According to a recent security research, most of the companies have unprotected data and poor cybersecurity practices in place, making them vulnerable to data loss.

To keep their business safe companies should have cybersecurity awareness, prevention and security best practices as a part of their culture.

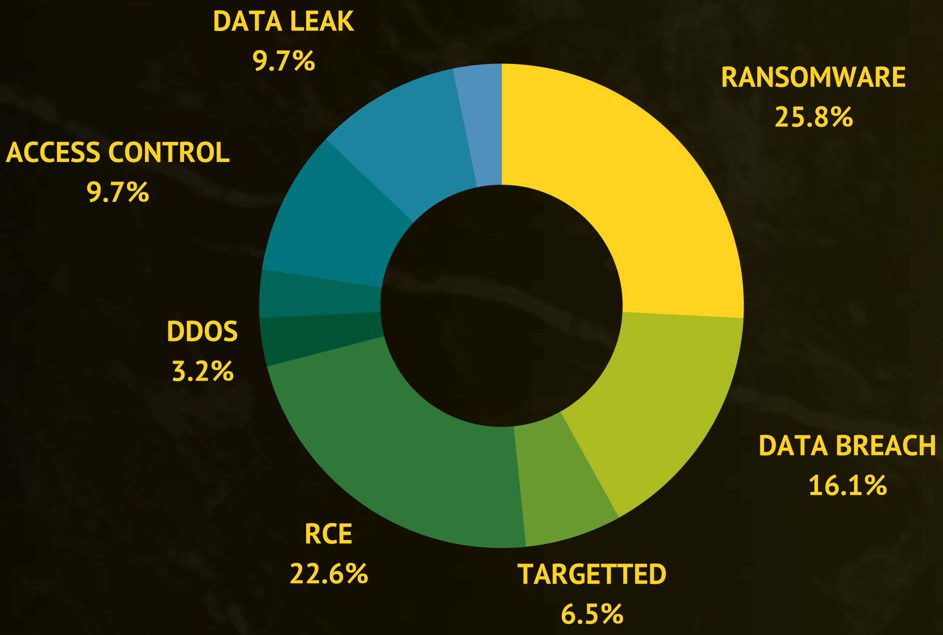
12%	GOVERNMENT
3%	EDUCATION
3%	HEALTHCARE
9%	RETAIL
6%	SOCIALMEDIA
24%	HOT FIX
35%	CONSUMER TECH
6%	AUTOMOTIVE

SECTORS AFFECTED BY ATTACKS

The below Pie-chart shows the percentage of distinctive sectors that've fallen as victims to the horrendous cyber threats. From it, it's evident that the Consumer Technology has been hit the most.



TYPES OF ATTACK VECTORS



Below, there's a bar-chart that indicates the percentage of nefarious cyber attacks that have broken the security mechanisms of distinct organizations.

Many cyberattacks initiate from various sectors. But, a majority of them seemed to have originated from consumer technology sector, holding about 35%. To prevent these, it's evident that top-notch reliable security is mandatory.

35%

GOVERNMENT

- Data from 200 US police departments & fusion centers published online
- Serious vulnerability existed in SWARCO Traffic Systems
- Keizer city computers hacked
- Vulnerability in Secure Document Wallet DigiLocker Could Bypass OTP Authentication

RETAIL

- Oracle E-Business Suite flaws allows hackers to hijack business operations
- An Indian conglomerate hit by CLOP Ransomware
- Europe’s Largest Private Hospital Operator Hit by Ransomware

EDUCATION

- Hackers ‘Hijack’ Samsung And Oxford University Servers To Defeat Microsoft 365 Security

HOT FIX

- 'SMBleed' Vulnerability Impacts Windows SMB Protocol
- Microsoft released new Security Patches for 129 Vulnerabilities
- Newly Patched SAP ASE Flaws Could Let Attackers Hack Database Servers
- Critical flaw fixed in bbPress forum plugin
- Cloud infrastructure operators should quickly patch VMware Cloud Director flaw
- Flaws found in Apple’s authentication technology
- Black Kingdom ransomware hacks networks with Pulse VPN flaws
- Grafana fixed incorrect access control vulnerability

SOCIAL MEDIA

- Twitter’s few business users had their private data exposed
- Facebook Messenger App for Windows Vulnerability Let Hackers Hijack a Call & Install Malware

AUTOMOTIVE

- Radio-frequency chip maker Hit by 'Maze' Ransomware Attack
- Honda's global operations hit by cyber-attack

CONSUMER TECH

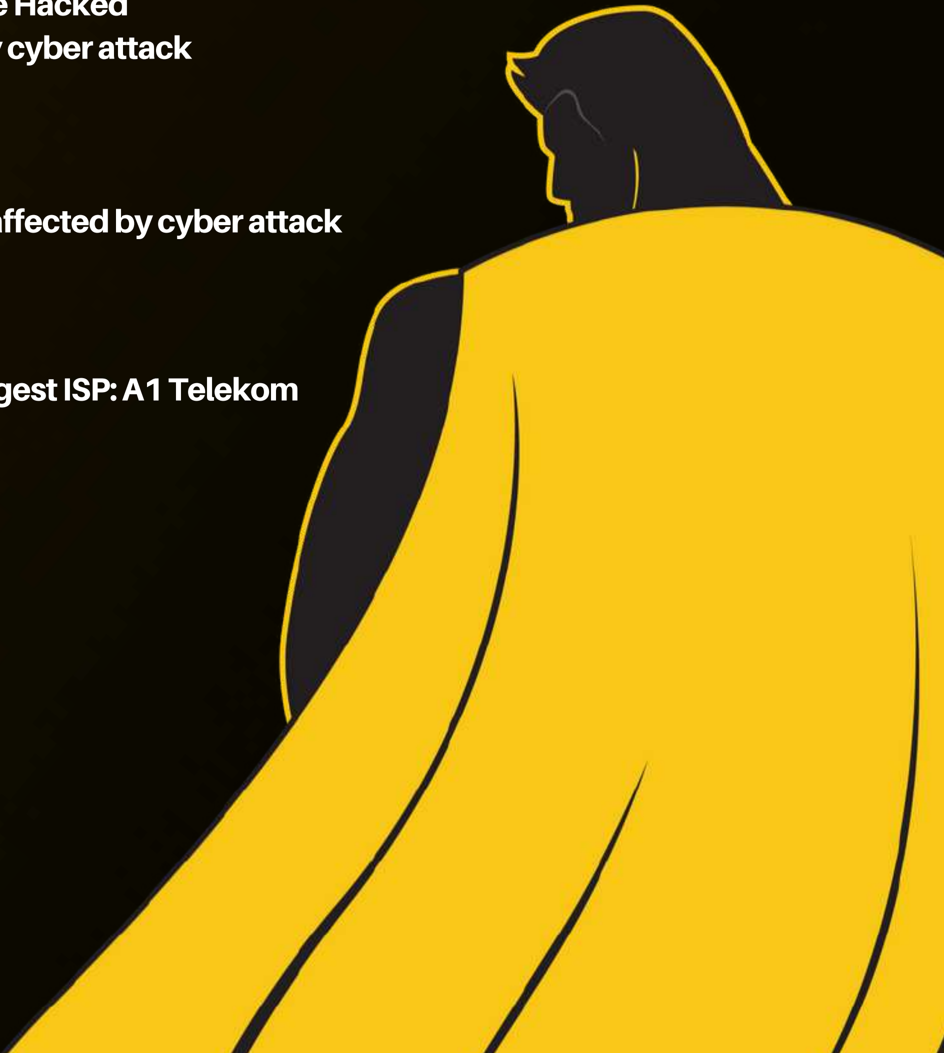
- New Magecart attacks leverage misconfigured S3 buckets to infect over 17K sites
- Joomla Resources Directory (JRD) Portal Suffers Data Breach
- Over 100 New Chrome Browser Extensions Caught Spying On Users
- Fitness Depot reported data breach
- Printers are exposing their IPP port online
- New Lamphone attack Can Listen to Your Conversations by Watching a Light Bulb in the Room
- Two Critical Flaws in Zoom may Let Attackers Hack Systems via Chat
- Nexus switches hit by a serious security flaw
- Akamai Registers Massive 1.44 Terabit-per-second DDoS Attack
- BitDefender fixes bug allowing attackers to run commands remotely
- Maneka Gandhi’s NGO Website Hacked
- Australia, NZ drinks giant hit by cyber attack

HEALTHCARE

- South Africa’s Life Healthcare affected by cyber attack

TELECOMMUNICATION

- Hackers breached Austria's largest ISP: A1 Telekom



Data from 200 US police departments & fusion centers published online

An activist group published the data they claim have been stolen from US law enforcement agencies and fusion centers. The files, dubbed BlueLeaks, have been published by DDoSecrets. The data has been made available online on a searchable portal. The leaked data contains more than one million files, such as scanned documents, videos, emails, audio files. The ten years-worth of files belonging to more than 200 police departments and law enforcement fusion centers from across the US.

ATTACK TYPE

Data Leak

CAUSE OF ISSUE

Lack of maintaince

TYPE OF LOSS

Reputation/Data

Serious vulnerability existed in SWARCO Traffic Systems

Researcher from ProtectEM found a critical vulnerability (CVE-2020-12493) affecting SWARCO Traffic Systems. Even a low-skilled attacker could easily exploit the bug and disrupt traffic controllers. Though, exploiting the flaw required physical access to the target controllers. In case of such an incident, the attacker could deactivate traffic lights causing huge traffic disruptions. The patch has released and users should make sure to update their systems.

ATTACK TYPE

Unauthorized access

CAUSE OF ISSUE

Existing Vulnerability

TYPE OF LOSS

Reputation/Data

Keizer city computers hacked

The city of Keizer's computer system was hacked and officials were only able to regain access to the data by paying the perpetrators a $48,000 ransom. The digital strike was discovered when city employees could not access some data and programs. "We believe that the forensic investigation could provide critical information to defend against attacks in the future," the city's statement read.

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Lack of awarness

TYPE OF LOSS

Reputation/Data

Vulnerability in Secure Document Wallet DigiLocker Could Bypass OTP Authentication

The Indian Government fixed a critical vulnerability in the secure document wallet service Digilocker which could have permitted anyone to bypass mobile one-time passwords (OTP) and sign in as another user to access their saved documents. The OTP function did not have authorization to perform OTP validation with submitting any valid users' details and then manipulation allow signing in as a different user. Finally, the cyber agency had fixed the issues immediately on getting the alert from CERT-In.

ATTACK TYPE

Broken authentication

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

RETAIL

Oracle E-Business Suite flaws allows hackers to hijack business operations

Oracle's E-Business Suite (EBS) were found to have two vulnerabilities, dubbed BigDebIT which were patched in a critical patch update by Oracle in January 2020. The security flaws could be exploited by threat actors to target accounting tools such as General Ledger to steal sensitive information and perform financial fraud. It is confirmed that even the systems up to date are vulnerable to these attacks. If the flaws are left unpatched, financial fraud and confidential information theft can be performed by attacking a firm's accounting systems.

ATTACK TYPE
Data Leak

CAUSE OF ISSUE
Lack of maintainces

TYPE OF LOSS
Reputation/Data

An Indian conglomerate hit by CLOP Ransomware

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Indiabulls Group has allegedly been hit with a cyberattack from the CLOP Ransomware operators who have leaked screenshots of stolen data. The CLOP Ransomware operators claimed to have breached Indiabulls and posted screenshots of files that they have allegedly stolen during the attack. When performing a ransomware attack, the CLOP threat actors are known to steal unencrypted files before deploying the ransomware. These files are then posted on their data leak site with a threat that more data will be leaked if the ransom demand is not paid.

Ripple20 vulnerabilities will haunt the IoT landscape for years to come

Cyber-security experts revealed 19 vulnerabilities in a small library designed in the 90s that has been widely used and integrated into countless of enterprise and consumer-grade products over the last two decades. The number if impacted products is estimated at "hundreds of millions" and includes products such as smart home devices, power grid equipment, healthcare systems, industrial gear, transportation systems, printers, routers,mobile/satellite communications equipment, data center devices, commercial aircraft devices, various enterprise solutions, and many others.

ATTACK TYPE
Vulnerability

CAUSE OF ISSUE
Poor security pratice

TYPE OF LOSS
Reputation

EDUCATION

Hackers 'Hijack' Samsung And Oxford University Servers To Defeat Microsoft 365 Security

ATTACK TYPE
Phishing

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Researchers at Check Point have exposed a sophisticated phishing campaign designed to harvest enterprise login credentials stored in Microsoft Office 365 accounts. To evade detection by security software, the campaign leveraged reputable web domain names such as Oxford University, Adobe and Samsung. Hackers hijacked Oxford University's email server to send malicious emails to victims. The emails contained links that redirected to an Adobe server used by Samsung in the past, enabling hackers to leverage the façade of a legitimate Samsung domain to successfully trick victims.

'SMBleed' Vulnerability Impacts Windows SMB Protocol

In early June 2020, Cybersecurity researchers uncovered a new critical vulnerability affecting the Server Message Block (SMB) protocol that allows attackers to leak kernel memory remotely, and when combined with a previously disclosed "wormable" bug, the flaw can be exploited to achieve remote code execution attacks. This impacts Windows 10 versions 1903 and 1909, for which Microsoft released security patches.

ATTACK TYPE

RCE

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

Microsoft released new Security Patches for 129 Vulnerabilities

ATTACK TYPE

RCE

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

Microsoft released its June 2020 batch of software security updates that patches a total of 129 NEW vulnerabilities affecting various versions of Windows OS and related products. The update also includes a patch for a new critical remote code execution flaw (CVE-2020-9633) affecting Adobe Flash Player for Windows systems.

Newly Patched SAP ASE Flaws Could Let Attackers Hack Database Servers

A new set of critical vulnerabilities uncovered in SAP's Sybase database software grants unprivileged attackers complete control over a targeted database and even the underlying operating system in certain scenarios. A cybersecurity company, Trustwave disclosed six flaws reside in Sybase Adaptive Server Enterprise (ASE) The company said the issues both specific to the OS and the platform were discovered during a security testing of the product. The users are recommended to update to the latest version of ASE to resolve the flaws.

ATTACK TYPE

Remote control

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

Critical flaw fixed in bbPress forum plugin

ATTACK TYPE

Privilege escalation

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation

A popular WordPress forum plugin, patched a critical security vulnerability that could lead to unauthenticated privilege escalation. Attackers who exploit the logic bug could grant themselves authorization to delete forum activities, import or export forum users, and create new forum moderators. The researcher caveated the bug's severity by pointing out that exploitation was conditional on user registration being enabled on a target site, and a BBPress registration form being embedded so that a nonce can be retrieved.

Cloud infrastructure operators should quickly patch VMware Cloud Director flaw

Public and private cloud administrators who are using VMware Cloud Director should immediately apply the patch for a high-risk vulnerability that can be used by hackers to take full control of virtualized cloud infrastructure, security experts warn. VMware released fixes for the command injection flaw previously, but if left unpatched, it can be easily exploited through customer trial accounts. VMware rated the issue high in the CVSS and said that it can lead to arbitrary remote code execution.

ATTACK TYPE

Command injection

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

Flaws found in Apple's authentication technology

Security researcher discovered that Sign in with Apple' authentication technology is flawed, such that it was possible for an attacker to hijack user accounts with web properties that relied on 'Sign in with Apple'. Researcher demonstrated a flawed web authentication mechanism rather than a confirmed ability to take over accounts. "These applications were not tested but could have been vulnerable to a full account takeover if there weren't any other security measures in place while verifying a user," according to Jain.

ATTACK TYPE

Broken authentication

CAUSE OF ISSUE

Security Misconfiguration

TYPE OF LOSS

Reputation/Data

Black Kingdom ransomware hacks networks with Pulse VPN flaws

The security researchers found that the operators of Black Kingdom ransomware are targeting enterprises with unpatched Pulse Secure VPN software or initial access on the network. The malware got caught in a honeypot, allowing researchers to analyse and document the tactics used by the threat actors. From the researchers' observations, the ransomware established persistence by impersonating a legitimate scheduled task for Google Chrome, with a single letter making the difference.

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Lack of maintenance

TYPE OF LOSS

Reputation/Data

Grafana fixed incorrect access control vulnerability

Grafana released the patches that include an important security fix for an issue that affects all versions from 3.0.1 to 7.0.1. The company received a security report on May 14, 2020, about vulnerability in Grafana regarding the avatar feature. This vulnerability allows any unauthenticated user/client to make Grafana send HTTP requests to any URL and return its result to the user/client. This can be used to gain information about the network that Grafana is running on.

ATTACK TYPE

Access control

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation

SOCIALMEDIA

Twitter’s few business users had their private data exposed

Twitter emailed its business customers, to warn that their information may have been compromised in a security lapse. The company said that business users’ billing information was inadvertently stored in the browser’s cache, and it was “possible” that others, such as those who share computers, could have accessed it. That data includes the business users’ email addresses, phone numbers and the last four-digits of their credit card number associated with the account.

ATTACK TYPE

Data exposed

CAUSE OF ISSUE

misconfiguration

TYPE OF LOSS

Reputation

Facebook Messenger App for Windows Vulnerability Let Hackers Hijack a Call & Install Malware

ATTACK TYPE

Remote access

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

Researchers disclosed a severe vulnerability in the Facebook messenger for Windows that lets hackers to hijack calls easily and then install malware. This vulnerability has a code that was executed by the app, which helps the hackers to get access to the application efficiently; once they gain control over the app. The bug has been fixed by the social media giant with its latest updated version 480.5.

Radio-frequency chip maker Hit by 'Maze' Ransomware Attack

MaxLinear said it was hit by a "Maze" ransomware attack, with a hacker releasing some proprietary information about the company online. The company said that it was working with a third party for advice on the content of information posted and that MaxLinear was also able to re-establish some affected systems and equipment. The company does not expect the incident to adversely impact its operating expenses.

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

AUTOMOTIVE

Honda's global operations hit by cyber-attack

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

Honda said it is dealing with a cyber-attack that is impacting its operations around the world. It added that the problem was affecting its ability to access its computer servers, use email and otherwise make use of its internal systems. Honda added that "work is being undertaken to minimize the impact and to restore full functionality of production, sales, and development activities." Experts identified that hackers used Snake ransomware, which scrambles files and holds them for ransom payments in crypto currency.

New Magecart attacks leverage misconfigured S3 buckets to infect over 17K sites

Few Magecart groups are changing tactics, moving from targeted attacks against carefully selected targets to a "spray-and-pray" approach, hacking everything in their sight, and hoping they manage to place their malicious code on an online store. The company reported that Magecart hackers have managed to compromise and plant malicious code on over 17,000 domains over the last few months.

ATTACK TYPE

Data leak

CAUSE OF ISSUE

Security misconfiguration

TYPE OF LOSS

Reputation/Data

Joomla Resources Directory (JRD) Portal Suffers Data Breach

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

The team behind the Joomla open source CMS announced a security breach, it took place after a member of the Joomla Resources Directory (JRD) team left a full backup of the JRD site on an Amazon Web Services S3 bucket owned by their own company. The Joomla team is now recommending that all JRD users change their password on the JRD portal, but also on other sites where they reused the password. The team also carried out a full security audit of the JRD portal.

Over 100 New Chrome Browser Extensions Caught Spying On Users

A newly discovered spyware effort attacked users through 32 million downloads of extensions to Google Chrome web browser. Google said it removed more than 70 of the malicious add-ons from its official Chrome Web Store after being alerted by the researchers in May 2020. Most of the free extensions purported to warn users about questionable websites or convert files from one format to another. Instead, they siphoned off browsing history and data that provided credentials for access to internal business tools.

ATTACK TYPE

Remote access

CAUSE OF ISSUE

Unknown

TYPE OF LOSS

Reputation/Data

Fitness Depot reported data breach

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

Fitness Depot revealed that the personal and financial information of customers were stolen following a breach that affected the company's e-commerce platform in May 2020. The company sent breach notification letter to all the affected customers. The attack is believed to be a Magecart attack in which the attackers managed to compromise Fitness Depot's online store and inject a malicious form designed to collect and exfiltrate customer information.

Printers are exposing their IPP port online

Security researchers from the Shadowserver Foundation, published a warning about companies that are leaving printers exposed online. The experts scanned all the four billion routable IPv4 addresses for printers that are exposing their IPP port, and specifically scanned the internet for IPP-capable printers that were left exposed without being protected by a firewall and allowed attackers to query for local details via the "Get-Printer-Attributes" function. In total, they usually found an average of around 80,000 printers exposing themselves online via the IPP port on a daily basis.

ATTACK TYPE
Data exposed

CAUSE OF ISSUE
Poor security practice

TYPE OF LOSS
Data

New Lamphone attack Can Listen to Your Conversations by Watching a Light Bulb in the Room

ATTACK TYPE
Eavesdropping

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
None

Lamphone the new attack method allows an adversary to record light bulb vibrations for eavesdropping. The attack works by recording the vibrations of a light bulb that generate when sound waves strike it. Using a remote electro-optical sensor, it becomes possible for an attacker to record the vibrations, segregate audio signals from the optical signals and then reverse-engineer them to get to the real audio.

Two Critical Flaws in Zoom may Let Attackers Hack Systems via Chat

Cybersecurity researchers from Cisco Talos discovered two critical vulnerabilities in the Zoom software that could have allowed attackers to hack into the systems of group chat participants or an individual recipient remotely. Cisco Talos researchers tested both flaws on version 4.6.10 of the Zoom client application and reported it to the company. Following which, Zoom patched both critical vulnerabilities with the release of version 4.6.12 of its video conferencing software for Windows, macOS, or Linux computers.

ATTACK TYPE
Remote access

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation/Data

Nexus switches hit by a serious security flaw

ATTACK TYPE
Network access control

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation/Data

Cisco warned customers with Nexus switches running its NX-OS software to install updates to address a serious flaw that allows a remote attacker to bypass network access controls and route malicious internet traffic to internal networks. CERT/CC's Sarvepalli said affected customers can prevent IP-in-IP packets by filtering IP protocol 4 packets at the upstream router or another device. Cisco also suggests this measure, but first advises customers to use iACLs to allow only strictly required management and control plane traffic that is destined to the affected device".

Akamai Registers Massive 1.44 Terabit-per-second DDoS Attack

In the mid of June 2020, an unnamed webhost was hit with one of the largest DDoS attacks ever registered by Akamai. The attack was directed at a large hosting provider used by a number of political and social sites. An Akamai executive said, "The methods involved volumetric attacks, or floods, of ACK, SYN, UDP, NTP, TCP reset, and SSDP packets, multiple botnet attack tools, and CLDAP reflection, TCP anomaly, and UDP fragments. There were no zero-day vulnerabilities and novel techniques." The attack also required a lot of planning and coordination.

ATTACK TYPE

DDOS

CAUSE OF ISSUE

Security vulnerability

TYPE OF LOSS

None

BitDefender fixes bug allowing attackers to run commands remotely

ATTACK TYPE

Remote commands

CAUSE OF ISSUE

Improper input validation

TYPE OF LOSS

None

An improper Input Validation vulnerability in the Safepay browser component of Bitdefender Total Security 2020 allows an external, specially crafted web page to run remote commands inside the Safepay Utility process. This issue affected Bitdefender Total Security 2020 versions prior to 24.0.20.116. Recently, Bitdefender has pushed out an automatic update that fixes this vulnerability in versions 24.0.20.116 and later.

Maneka Gandhi's NGO Website Hacked

The official website of BJP MP Maneka Gandhi's animal rights NGO People For Animals (PFA) was hacked by a group of 'ethical hackers.' The website that had been defaced read, "Maneka Gandhi dragged the sad death of pregnant elephant for dirty politics." Spreading false information by a person especially being an ex-minister and a Lok Sabha member is a real threat to the nation and not acceptable. The bond between Hindu and Muslim in Malappuram is strong."

ATTACK TYPE

Targetted

CAUSE OF ISSUE

Unknown

TYPE OF LOSS

Reputation/Data

Australia, NZ drinks giant hit by cyber attack

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

A ransomware attack has shut down Drinks manufacturer Lion, cutting supplies to pubs and restaurants. Investigators at the company said the outage was caused by ransomware, a cyberhack which freezes a target's computer systems until a payment is made. The company immediately shut down all their systems as a precaution, and they continued to work with cyber experts to determine how much longer their systems will be impacted. Lion also said that it was taking longer than expected to bring its production systems back online.

HEALTHCARE

South Africa’s Life Healthcare affected by cyber attack

South Africa’s Life Healthcare was hit by a cyber attack affecting its admissions systems, business processing systems and email servers, but is yet to determine the extent to which data has been compromised. The patient care was not impacted and an investigation into the incident is underway. The company’s CEO said, “We are deeply disappointed and saddened that criminals would attack our facilities during such a time, when we are all working tirelessly and collectively to fight the COVID-19 pandemic.”

ATTACK TYPE

Targetted

CAUSE OF ISSUE

Unknown

TYPE OF LOSS

Reputation/Data

TELECOMMUNICATION

ATTACK TYPE

Security breach

CAUSE OF ISSUE

Malware

TYPE OF LOSS

None

Hackers breached Austria's largest ISP: A1 Telekom

A1 Telekom was hit by a security breach in November 2019. A1’s security team detected the malware a month later, but removing the infection was more problematic than it initially anticipated. Until May 2020 the security team battled with the malware's operators attempting to remove all of their hidden backdoor components and kick out the intruders.

CONCLUSION

According to an article, online threats has risen by as much as six-times their usual levels recently, as the Covid 19 pandemic provides new ballast for cyber attacks. A journal analysed the UK traffic figures for four weeks and reported that hacking and phishing attempts were up to 37% month-on-month.

As mentioned previously, it's smart to develop strong cyber safety habits to help prepare for a cyberattack or data breach. Large-scale attacks and breaches would occur at major organizations, but it's also important to secure your personal information and networks too. So, in order to protect your files and system, keep your software up to date, secure your files, encrypt your devices, use strong passwords and keep changing it frequently.

In addition to these steps the most important step to be followed is contacting a best security company like us.

Here we would give you a clear view regarding the security issues and we would also help you out to keep your data secure at this New Normal.

Contact us for more information.

REFERENCES

- https://thehackernews.com/2020/06/SMBleed-smb-vulnerability.html
- https://thehackernews.com/2020/06/windows-update-june.html
- https://cybersecuritynews.com/facebook-messenger-app-for-windows-vulnerability/
- https://latesthackingnews.com/2020/06/19/lamphone-attack-exploits-vibrations-from-light-bulb-to-spy-on-users/
- https://www.cybersafe.news/critical-vulnerability-in-india-digilocker-patched/
- https://www.zdnet.com/article/joomla-team-discloses-data-breach/
- https://www.csoonline.com/article/3546235/cloud-infrastructure-operators-should-quickly-patch-vmware-cloud-director-flaw.html
- https://in.reuters.com/article/us-life-healthcare-cyber/south-africas-life-healthcare-hit-by-cyber-attack-idINKBN23G0MY
- https://www.zdnet.com/article/new-magecart-attacks-leverage-misconfigured-s3-buckets-to-infect-over-17k-sites/
- https://www.cybersafe.news/canadas-fitness-depot-hit-by-data-breach/
- https://www.zdnet.com/article/hackers-breached-a1-telekom-austrias-largest-isp/
- https://thehackernews.com/2020/06/newly-patched-sap-ase-flaws-could-let.html
- https://thehackernews.com/2020/06/zoom-video-software-hacking.html
- https://latesthackingnews.com/2020/06/08/swarco-traffic-systems-vulnerability-could-allow-signal-hijacking/
- https://grafana.com/blog/2020/06/03/grafana-6.7.4-and-7.0.2-released-with-important-security-fix/
- https://portswigger.net/daily-swig/wordpress-security-critical-flaw-fixed-in-bbpress-forum-plugin
- https://portswigger.net/daily-swig/sign-in-with-apple-vulnerability-find-earns-100k-bug-bounty
- https://www.zdnet.com/article/cisco-warns-these-nexus-switches-have-been-hit-by-a-serious-security-flaw/
- https://www.keizertimes.com/posts/1639/keizer-city-computers-hacked
- https://www.cybersafe.news/oracle-e-business-suite-flaws-allows-hackers-to-hijack-business-operations/
- https://www.bleepingcomputer.com/news/security/black-kingdom-ransomware-hacks-networks-with-pulse-vpn-flaws/
- https://bdaily.co.uk/articles/2020/06/18/office-365-phishing-campaign-exploited-samsung-adobe-and-oxford-university-servers
- https://www.nytimes.com/reuters/2020/06/16/technology/16reuters-maxlinear-cyber.html
- https://www.zdnet.com/article/blueleaks-data-from-200-us-police-departments-fusion-centers-published-online/
- https://www.reuters.com/article/us-alphabet-google-chrome-exclusive/exclusive-massive-spying-on-users-of-googles-chrome-shows-new-security-weakness-idUSKBN23P0JO
- https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years-to-come/
- https://www.bleepingcomputer.com/news/security/indiabulls-group-hit-by-clop-ransomware-gets-24h-leak-deadline/?&web_view=true
- https://www.zdnet.com/article/80000-printers-are-exposing-their-ipp-port-online/?&web_view=true
- https://www.bbc.com/news/technology-52982427
- https://www.techrepublic.com/article/honda-hit-by-cyberattack-that-impacted-its-global-operations/
- https://securityboulevard.com/2020/06/akamai-registers-massive-1-44-terabit-per-second-ddos-attack/
- https://www.bleepingcomputer.com/news/security/bitdefender-fixes-bug-allowing-attackers-to-run-commands-remotely/?&web_view=true
- https://www.thequint.com/news/india/maneka-gandhis-ngo-website-hacked-due-to-comments-on-mallapuram
- https://www.thequint.com/news/india/maneka-gandhis-ngo-website-hacked-due-to-comments-on-mallapuram

CLICK HERE

CLICK HERE

YOU MAY ALSO BE INTERESTED IN OUR PREVIOUS REPORTS

EDITION 22
THREATSPLOIT ADVERSARY REPORT
JUNE 2020

EDITION 21
THREATSPLOIT ADVERSARY REPORT
MAY 2020
PREPARED BY - BRISKINFOSEC

EDITION 20
THREATSPLOIT ADVERSARY REPORT
APRIL 2020
- COVID-19 CYBER ATTACKS ARE ADDING
- AWARENESS IS KEY TO SUCCESS

www.briskinfosec.com

THREATSPLOIT ADVERSARY REPORT
MARCH 2020 | EDITION 19
www.briskinfosec.com

CLICK HERE

FEB 2020 | EDITION 18
THREATSPLOIT ADVERSARY REPORT

Edition 17
THREATSPLOIT ADVERSARY REPORT
January -2020
Wishing you a Happy New Year

THREATSPLOIT ADVERSARY REPORT

EDITION 15
THREATSPLOIT
ADVERSARY REPORT

CyberSecurity Awareness Weekly

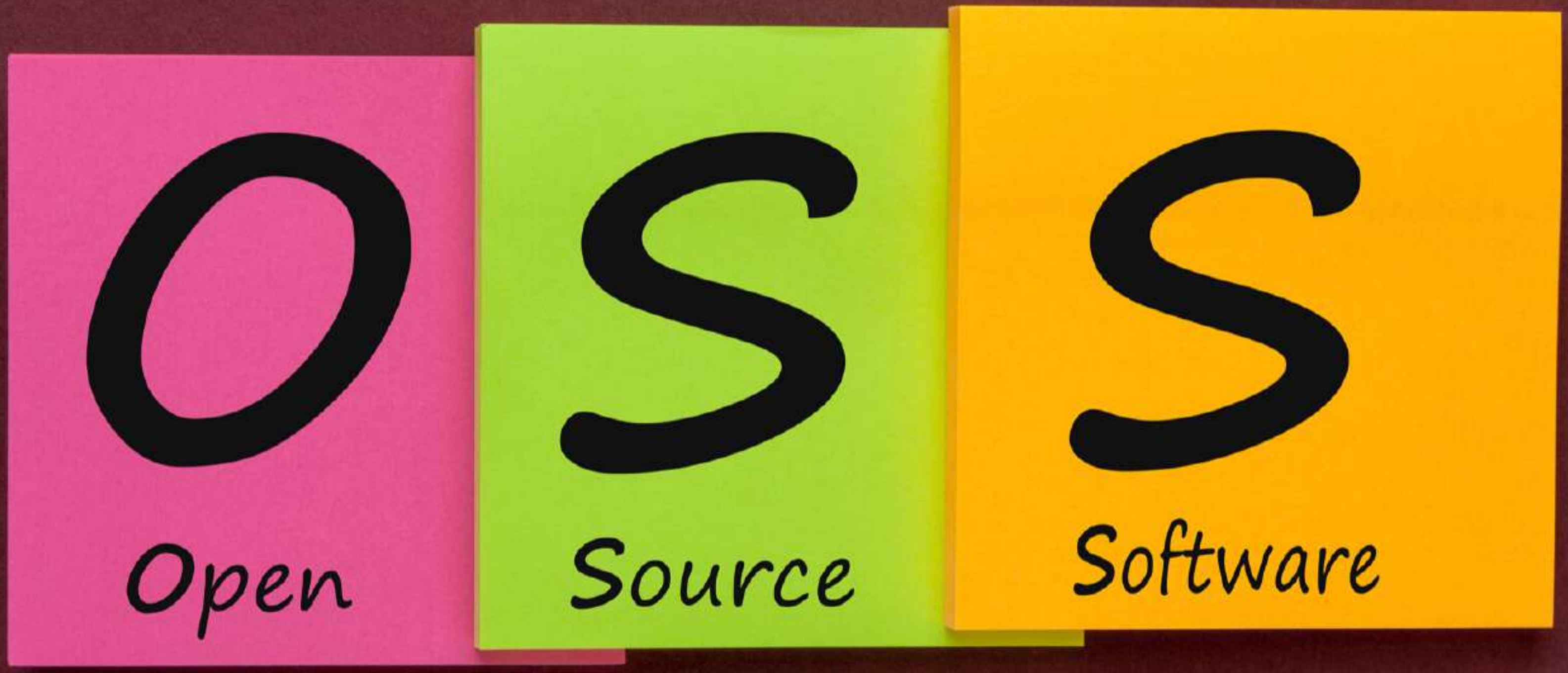
briskinfosec.com

CLICK HERE

CLICK HERE

Briskinfosec

CLICK HERE



Tool set's

BRISK INFOSEC

CYBER TRUST & ASSURANCE

Your Cybersecurity is Our Responsibility!!

contact@briskinfosec.com | www.briskinfosec.com

Affiliated by

certin www.cert-in.org.in

BQS ASQS Bureau of Quality Standard ISO/IEC 27001 ISMS CERTIFIED

Awards

CIO Review 10 MOST PROMISING CYBERSECURITY SOLUTION PROVIDER 2019

THE LEADERS GLOBE THE MOST POWERFUL CYBER SECURITY SOLUTION PROVIDER