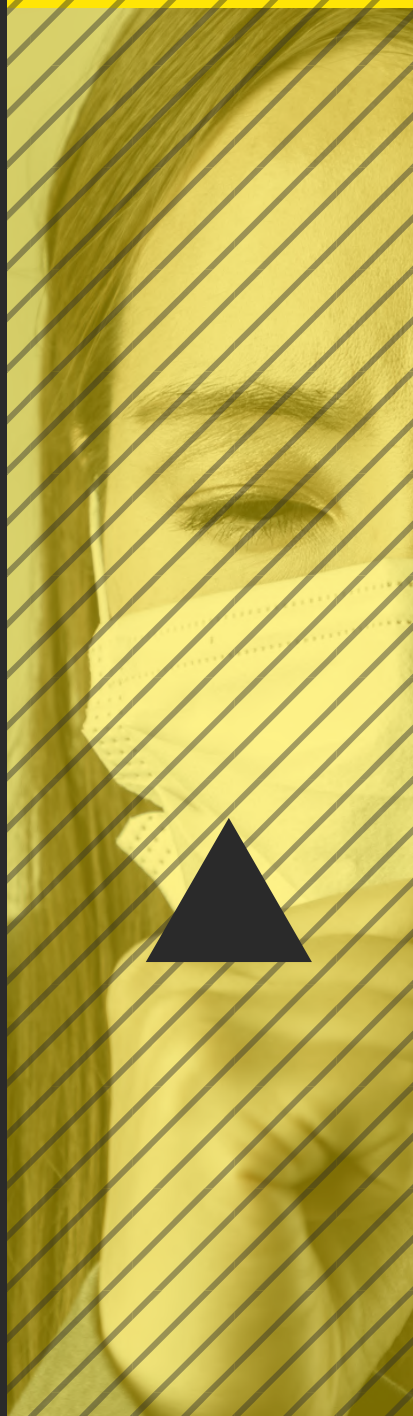
EDITION 20

THREATSPLOIT ADVERSARY REPORT

APRIL 2020

- COVID-19 CYBER ATTACKS ARE ADDED
- AWARENESS IS KEY TO SUCCESS



BRISK INFOSEC

CYBER TRUST & ASSURANCE

www.briskinfosec.com

INTRODUCTION

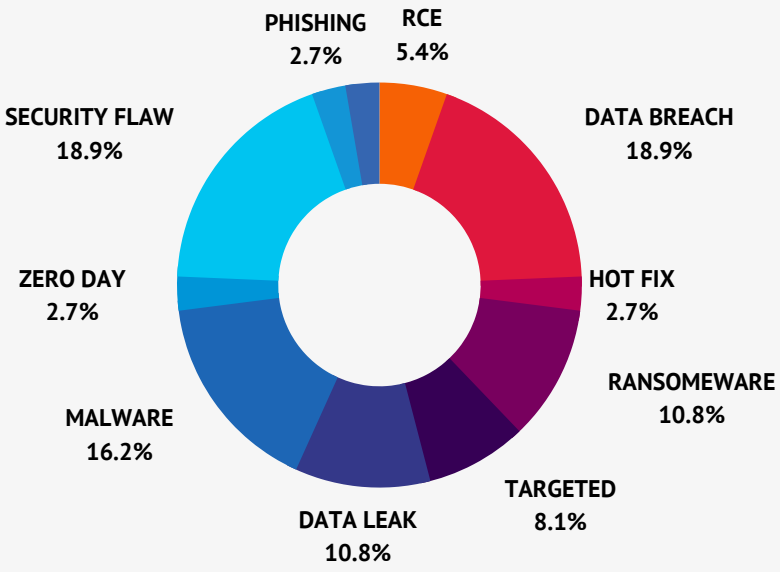
Threatsploit report March 2020, As always we have put together few Cyber Attacks of this month. Here we provide you a brief about threats which would make you be aware on how to keep your data safe. So now, 'COVID-19' is really challenging for all key industries to run their business.

According to the UN Conference on Trade and Development, the corona virus outbreak might cost the global economy $1-2 trillion in2020. This virus not only does damage to human lives but also been used as a trap in IT industry where the hackers use this to hack your data. As mentioned there are several hackers who have used this COVID-19 as a key to unlock few confidential data and have put the IT industry in trouble.

Mostly, they attack the social media accounts and have also accessed information by creating fake Application, Word Document etc., These threats are mentioned in this report in detail. Another big impact is for the employees who work from home where their data is not secured. It is still risky during data transfer. But we would help you out in keeping your data safe and secure wherever you are. we are working hard during these difficulties to keep your data safe.

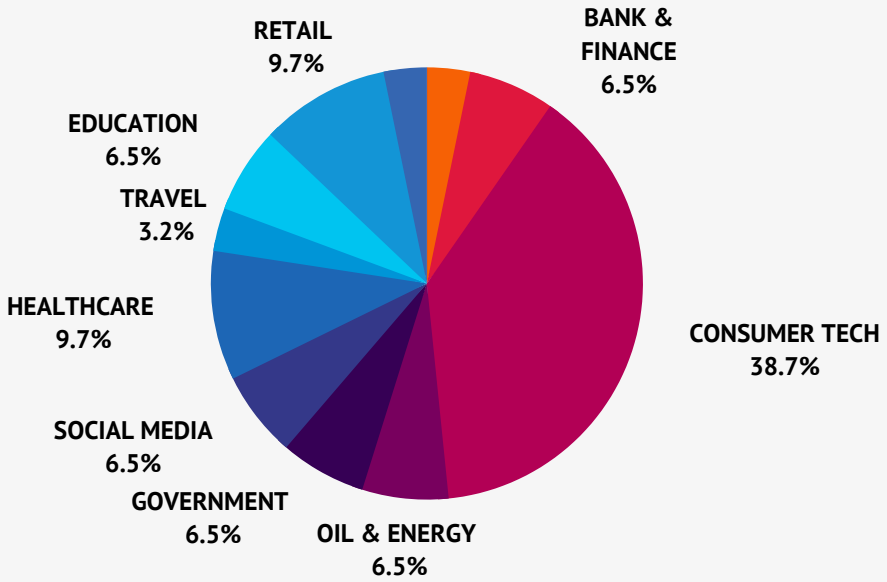
TYPES OF ATTACK VECTORS

The Pie-chart indicates the percentage of nefarious cyber attacks that have broken the security mechanisms of distinct organizations.



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.



Many cyberattacks initiate from various sectors. But, a majority of them seemed to have originated from consumer technology sector, holding about 39%. To prevent these, it's evident that top-notch reliable security is mandatory.

39%

consumer Tech

CORONA COVID19

- Several Coronavirus Scammers Went Into Overdrive
- Coronavirus used in Malicious Campaigns
- Malicious Coronavirus Tracker Application
- APT36 Uses Coronavirus to Spread Crimson RAT

TELECOMMUNICATION

- Virgin Media exposes data of 900,000 users via unprotected marketing database
- Hackers Compromise T-Mobile Employee' Email Accounts and Steal User' Data

BANKING AND FINANCE

- Financial companies leak 425GB in company, client data through open database
- Finastra, World's Third Largest Fintech, Hit by Ransomware

EDUCATION

- Truefire Data Breach Exposed Credit Cards and Personal Information of Use
- Illinois College Suffers Data Breach

OIL & ENEGRY

- Evraz faces massive ransomware attack
- Epiq Global suffered a Ransomware attack

GOVERNMENT

- Maharashtra Police's CID website hacked
- Israel's Defense Minister twitter hacked

SOCIAL MEDIA

- Coronavirus used in Malicious Campaigns
- WWE's Twitter Account Hacked

HEALTHCARE

- University of Kentucky and its health system affected by Cyber attack
- Healthcare data breach: Medical device manufacturer discloses phishing attack
- COVID-19 Vaccine Test Center Hit By Cyber Attack

TRAVEL

- Princess Cruises Confirms Data Breach

CONSUMER TECH

- Financial companies leak 425GB in company, client data through open database
- "LVI" attack broke the secure enclave of Intel's CPU
- AMD Processors Vulnerable to 2 New Side-Channel Attacks
- Critical PPP Daemon Flaw Affects Most Linux Distros
- Serious Security Vulnerability Found in Avast's Antitrack Tools
- Blisk browser vendor left an Elasticsearch server exposed online without a password
- Slack fixed vulnerability exploitable for session hijacking, account takeovers
- Intel faces new Snoop attack
- Mukashi botnet takes advantage of a known vulnerability
- Multiple botnets are spreading using LILIN DVR 0-day
- Bug in OpenWrt OS Affects Millions of Network Devices
- Critical Bugs in Rockwell, Johnson Controls ICS Gear

RETAIL

- Koodo Mobile Faced a Data Breach
- Foodmandu portal hacked
- Both Boots Advantage and Tesco Clubcard face data breaches

AUTOMOTIVE

- SpaceX and Tesla documents leaked online by hackers

CORONA COVID19

01

Several Coronavirus Scammers Went Into Overdrive

Jiri Kropac, a researcher at ESET found a wave of 2,500 infections of just two strains of malware which was delivered in COVID-19-themed emails. The malware either tries to get leverage on a computer in order to download more malicious software, or it steals personal information from an infected computer. According to Kropac, this is the biggest Coronavirus or COVID-19-themed malware campaign that was registered so far.

ATTACK TYPE
Malware

CAUSE OF ISSUE
Social Engg

TYPE OF LOSS
Reputation/Data

Coronavirus used in Malicious Campaigns

ATTACK TYPE
Malware

CAUSE OF ISSUE
Malicious Campaigns

TYPE OF LOSS
Reputation/Data

According to a Trent Micro article, COVID-19 is being used in a variety of malicious campaigns including email spam, BEC, malware, ransomware, and malicious domains. As the number of those afflicted continue to surge by thousands, campaigns that use the disease as a lure likewise increase. Experts estimate that more than three percent of Coronavirus websites created since the beginning of the year contains malicious content, reported EURACTIV Slovakia.

Malicious Coronavirus Tracker Application

Researchers from mobile security company Lookout discovered an Android app called "corona live 1.1," that is linked to SpyMax, which pretends to be the real "corona live" app and uses the Johns Hopkins coronavirus tracker. The app actually tracks the user device's photos, videos, location and camera. The camera access would allow the attackers to take photos and record videos and audio, Lookout said.

ATTACK TYPE
Malware (Tracker)

CAUSE OF ISSUE
Malicious Campaigns

TYPE OF LOSS
Reputation/Data

APT36 Uses Coronavirus to Spread Crimson RAT

ATTACK TYPE
Remote Access Trojan

CAUSE OF ISSUE
Lack of awarness

TYPE OF LOSS
Reputation/Data

A Pakistani-linked threat actor, APT36, was using a decoy health advisory that taps into global panic around the coronavirus pandemic to spread the Crimson RAT which would steal credentials from victims' browsers. Once downloaded, Crimson RAT connects to its hardcoded command and control (C2) IP addresses and sends collected information about the victim back to the server. Researchers said that making employees aware of these ongoing scams is key – particularly with more businesses moving to a work from home model in response to the coronavirus pandemic.

TELECOMMUNICATION

02

Virgin Media exposes data of 900,000 users via unprotected marketing database

Virgin Media announced that it has also suffered a data leak incident exposing the personal information of roughly 900,000 customers. The company said the unauthorized access to the database has been shut down immediately following the discovery and that it launched a full independent forensic investigation to determine the extent of the breach incident. The company is also contacting affected customers of security failure and has already notified the Information Commissioner's Office.

ATTACK TYPE
Data Breach

CAUSE OF ISSUE
Unauthorized access

TYPE OF LOSS
Reputation/Data

Hackers Compromise T-Mobile Employee' Email Accounts and Steal User' Data

ATTACK TYPE
Data Breach

CAUSE OF ISSUE
Unauthorized access

TYPE OF LOSS
Reputation/Data

T-Mobile faced a data breach in which the hackers gained access to the user's personal information. The company took necessary steps to shut down the unauthorized access upon discovery and immediately notified law enforcement of the security breach incident. It also notified the customers about the breach incident.

BANKING AND FINANCE

03

Financial companies leak 425GB in company, client data through open database

According to a ZdNet article, an open database is the source of a data leak leading to the exposure of 425GB in sensitive documents belonging to financial companies. Security researchers found over 500,000 "highly sensitive" documents, including private legal and financial files that originated from Advantage and Argus. Entries related to the companies' businesses, including credit reports, bank statements, contracts, legal documents, driver license copies, purchase orders and receipts, tax returns, Social Security information, and transaction reports.

ATTACK TYPE
Data Leak

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Finastra, World's Third Largest Fintech, Hit by Ransomware

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation

Finastra said that it was shutting down key systems in response to a security breach. The company acknowledged an incident via a notice on its Web site that offers somewhat less information and refers to the incident merely as the detection of anomalous activity. COO Tom Kilroy said, "In order to safeguard our customers and employees, we have made the decision to take a number of our servers offline while we investigate. This, of course, has an impact on some of our customers and we are in touch directly with those who may be affected."

EDUCATION

04

Truefire Data Breach Exposed Credit Cards and Personal Information of Use

Guitar Instruction Website, Truefire identified a breach in their database that involved an unauthorised user gaining access to information that customers entered through the website. The hacker accesed the personal and financial information of users who paid using their credit cards on the company's website between August 3, 2019 and January 14, 2020. Truefire said that it is working with a computer forensic specialist to identify the extent of the breach.

ATTACK TYPE
Data Breach

CAUSE OF ISSUE
Unauthorised access gain

TYPE OF LOSS
Reputation/Data

Illinois College Suffers Data Breach

ATTACK TYPE
Data Breach

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

Officials at the College of DuPage confirmed that a cybersecurity incident had taken place. College president Brian Caputo said that personal and tax information belonging to 1,755 staff had been compromised. Data exposed in the incident included 2018 W-2 tax forms. In addition to issuing breach notifications, the Glen Ellyn college is offering credit monitoring and identity protection services to current and former employees free of charge. An investigation into how the breach occurred is yet to produce any conclusive results.

OIL & ENERGY

05

Evraz faces massive ransomware attack

Evraz North America hit by a ransomware attack that impacted operations across the United States and Canada, including in Regina. Employees of its Queen City steel mill have been temporarily laid off. A company spokesperson Patrick Waldron said, “There is no indication of any breach of confidential or personal customer or employee information.” While Waldron wouldn’t comment on when operations may resume in full another executive said that the company has optimistically expressed to the union that it could happen in near future.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awarness

TYPE OF LOSS
Reputation

Epiq Global suffered a Ransomware attack

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Poor Security Pratice

TYPE OF LOSS
Reputation/Data

Epiq globally took their systems offline after detecting a cyberattack, which began encrypting devices on their network. As part of the company’s comprehensive response plan, they began working with a third-party forensic firm to conduct an independent investigation. Their technical team was working closely with world class third-party experts to address this matter, and bring their systems back online in a secure manner, as quickly as possible.

GOVERNMENT

06

Maharashtra Police's CID website hacked

In early March 2020, website of the Maharashtra police's CID was apparently hacked with a message warning the "Indian police and Modi government" against "hurting" Muslims being displayed. A group identifying itself as 'Legion' claimed responsibility for the hacking. A Cyber police officer said that the efforts are under way to trace the hack.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Poor Security Pratice

TYPE OF LOSS
Reputation/Data

Israel's Defense Minister twitter hacked

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awarness

TYPE OF LOSS
Reputation/Data

Twitter account of Israel's defense minister suffered a hack, in which the hacker posted a tweet demanding "freedom for Palestine" with the Palestinian flag. The tweets were swiftly deleted after being sent out at around 2 a.m. Bennett's office said in a statement that, "The content was immediately erased and the account password was replaced...The matter was brought to the authorized cyber elements in the security forces to be dealt with."

SOCIAL MEDIA

07

Coronavirus used in Malicious Campaigns

According to a Trent Micro article, COVID-19 is being used in a variety of malicious campaigns including email spam, BEC, malware, ransomware, and malicious domains. As the number of those afflicted continue to surge by thousands, campaigns that use the disease as a lure likewise increase. Experts estimate that more than three percent of Coronavirus websites created since the beginning of the year contains malicious content, reported EURACTIV Slovakia.

ATTACK TYPE
Malware

CAUSE OF ISSUE
Malicious Campaigns

TYPE OF LOSS
Reputation/Data

WWE's Twitter Account Hacked

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awarness

TYPE OF LOSS
Reputation/Data

Recently, WWE'S Twitter account was hacked. Its profile picture was changed to a black circle, its header was amended to a white background, and the bio was altered to "Expose. W a t c h i n g. //." The account then tweeted "The Truth Will Be Heard" upside down. It is unclear whether WWE's account was hacked or if the message is part of a larger storyline.

University of Kentucky and its health system affected by Cyber attack

According to a Health IT Security article the University of Kentucky (UK) and UK Healthcare faced a cyberattack. Hackers first installed the malware on university's system in early February causing temporary system failures, especially with UK Healthcare. Patient safety and care was not impacted by the attack. The University said that it was working to remove cryptocurrency malware from its network.

ATTACK TYPE
Malware

CAUSE OF ISSUE
Poor Security Pratice

TYPE OF LOSS
Reputation/Data

HEALTHCARE

08

Healthcare data breach: Medical device manufacturer discloses phishing attack

ATTACK TYPE
Phishing

CAUSE OF ISSUE
Lack of Awarness

TYPE OF LOSS
Reputation/Data

Back in January 2020 Tandem Diabetes Care revealed that customer data was exposed during a phishing attack that breached five employee email accounts. After discovering the attack, the company immediately secured the affected email accounts and launched an investigation, which found that an unauthorized user had gained access to the affected accounts Recently the company said the compromised email accounts contained "customer contact information, information related to the use of Tandem's products or services, and/or clinical data regarding customer diabetes therapy."

COVID-19 Vaccine Test Center Hit By Cyber Attack

A medical facility on standby to help test any coronavirus vaccine was hit by a ransomware group who were behind the Maze ransomware attack. Through this they stole the data from a victim and then publishing it online to get them to pay the ransom demanded.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Malicious Campaigns

TYPE OF LOSS
Reputation/Data

Princess Cruises Confirms Data Breach

ATTACK TYPE
Data Breach

CAUSE OF ISSUE
Lack of Maintances

TYPE OF LOSS
Reputation/Data

Recently, Princess Cruises identified a series of deceptive emails sent to employees resulting in unauthorized third-party access to some employee email accounts. So the company retained a major cybersecurity firm to investigate the matter while reinforcing security and privacy protocols to further protect systems and information. As part of its ongoing operations, the company is reviewing security & privacy policies and procedures and implementing changes when needed to enhance information security.

TRAVEL

09

Microsoft Released Patch for Wormable Bug That Threatens Corporate LANs

Microsoft released a patch for vulnerability in the SMBv3 protocol that was accidentally leaked online earlier this month. The fix KB4551762, is an update for Windows 10, versions 1903 and 1909, and Windows Server 2019, versions 1903 and 1909. In this case, "to exploit the vulnerability against an SMB server, an unauthenticated attacker could send a specially crafted packet to a targeted SMBv3 server," Microsoft said that, "To exploit the vulnerability against an SMB client, an unauthenticated attacker would need to configure a malicious SMBv3 server and convince a user to connect to it."

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Security Loopholes

TYPE OF LOSS
None

"LVI" attack broke the secure enclave of Intel's CPU

ATTACK TYPE
Security Flaw

CAUSE OF ISSUE
Vulnerability

TYPE OF LOSS
None

Earlier this month a new security flaw in Intel processors was found. Named Load Value Injection (LVI), this is a new class of theoretical attacks against Intel CPUs. Although the attack was just a theoretical threat at that time, Intel has already released firmware patches to mitigate attacks against its current CPUs and the company plans to deploy fixes at the hardware level in future generations.

AMD Processors Vulnerable to 2 New Side-Channel Attacks

AMD is seeking to downplay side-channel attacks that can leak potentially sensitive data from its processors released between 2011 and 2019. "Take A Way," the new potential attack extract sensitive information from signals created by electronic activity within computing devices as they carry out computation. The flaws reportedly affect some older Athlon CPUs as well as all Ryzen and Threadripper processors.

ATTACK TYPE
Side Channel

CAUSE OF ISSUE
Vulnerability

TYPE OF LOSS
Data

Critical PPP Daemon Flaw Affects Most Linux Distros

ATTACK TYPE
Daemon Flaw

CAUSE OF ISSUE
Security Flaw

TYPE OF LOSS
Reputation/Data

In early March 2020 the following popular Linux distros have been affected by a Critical PPP Daemon Flaw: Debian, Ubuntu, SUSE Linux, Fedora, NetBSD, and Red Hat Enterprise Linux. Other affected applications and devices include Cisco CallManager, TP-Link products, OpenWRT Embedded OS, and Synology products. The ultimate advice was to update the affected software with the latest available patches provided by the specific software vendor.

CONSUMER TECH

Serious Security Vulnerability Found in Avast's Antitrack Tools

Web researcher David Eade found and reported CVE-2020-8987 to Avast: this is a trio of blunders that, when combined, can be exploited by a snooper to silently intercept and tamper with an AntiTrack user's connections to even the most heavily secured websites. The flaws affect both the Avast and AVG versions of AntiTrack, and punters were advised to update their software as a fix for both tools has been released.

ATTACK TYPE
Security Flaw

CAUSE OF ISSUE
Security Vulnerability

TYPE OF LOSS
None

Blisk browser vendor left an Elasticsearch server exposed online without a password

ATTACK TYPE
Human Error

CAUSE OF ISSUE
Lack of awarness

TYPE OF LOSS
Reputation/Data

Blisk Browser vendors leaked user data after it accidentally left an Elasticsearch server exposed on the internet without a password. In total, they found 2.9 million records, amounting for 3.4 GB of data, left exposed online. The data appeared to be log entries for actions developers were taking inside the browser, such as registering profiles or inviting friends. Personal details leaked via the exposed servers included email addresses and user-agent strings.

Slack fixed vulnerability exploitable for session hijacking, account takeovers

In early March 2020, Slack fixed a bug that allowed attackers to hijack user accounts by tampering with their HTTP sessions. The flaw could have allowed attackers to pilfer users' cookies, giving them full account access. They could also have automated those attacks at scale, said the researcher Evan Custodio.

ATTACK TYPE
Session Hijacking

CAUSE OF ISSUE
Security Flaw

TYPE OF LOSS
Reputation/Data

Intel faces new Snoop attack

ATTACK TYPE
Data Leak

CAUSE OF ISSUE
Security Flaw

TYPE OF LOSS
Reputation/Data

A new attack that can leak data from a CPU's internal memory or cache has been discovered which affects many popular Intel processors, Tech Radar reported. Pawel Wieczorkiewicz, a software engineer at AWS found the "Snoop-assisted L1 Data Sampling" (Snoop) attack promptly reported the issue to Intel. Following its own investigations into the matter, Intel realized that patches released to fix the Foreshadow vulnerability could also be applied to this new attack.

CONSUMER TECH

Mukashi botnet takes advantage of a known vulnerability

A new variant of Mirai malware (Mukashi) is targeting a recently uncovered critical vulnerability in network-attached storage devices and exploiting them to rope the machines into an Internet of Things botnet. The Mukashi code also has the potential to conduct large scale DDoS attacks against selected targets.

ATTACK TYPE
DDOS

CAUSE OF ISSUE
Security Vulnerability

TYPE OF LOSS
Reputation/Data

Multiple botnets are spreading using LILIN DVR 0-day

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Security Flaw

TYPE OF LOSS
Reputation/Data

Multiple zero-day vulnerabilities in DVRs for surveillance systems manufactured by LILIN have been exploited by botnet operators to infect and co-opt vulnerable devices into a family of denial-of-service bots. The flaw in itself concerns a chain of vulnerabilities that make use of hard-coded login credentials, potentially granting an attacker the ability to modify a DVR's configuration file and inject backdoor commands when the FTP or NTP server configurations are synchronized.

Bug in OpenWrt OS Affects Millions of Network Devices

Researchers found vulnerability in OpenWrt operating system that allows attackers to inject the malicious payload on the vulnerable systems. The RCE bug addressed in the package list parse the logic of OpenWrt's opkg (Opkg Package Manager) The vulnerability has been fixed and assigned CVE-2020-7982 and the users are urged to upgrade to the latest OpenWrt version.

ATTACK TYPE
RCE

CAUSE OF ISSUE
Security Flaw

TYPE OF LOSS
Reputation/Data

Critical Bugs in Rockwell, Johnson Controls ICS Gear

ATTACK TYPE
Malicious Code Execution

CAUSE OF ISSUE
Security Flaw

TYPE OF LOSS
Reputation/Data

Security vulnerabilities that require very little skill to exploit have been found in industrial control systems (ICS) gear from Rockwell Automation and Johnson Controls, which anchor a flurry of bug disclosures impacting critical infrastructure. The bugs could allow an attacker to gain access to sensitive project file information, including passwords. According to an advisory, "Successful exploitation of this vulnerability could allow malicious code execution with system-level privileges."

Koodo Mobile Faced a Data Breach

Koodo Mobile's customer data was breached and was sold on various Dark Web websites. This information can be used by scammers to port Koodo Mobile numbers to attacker's devices to receive two-factor authentication codes, which could allow attackers to gain access to email and bank accounts. To prevent this, Koodo has enabled the 'Port Protection' feature.

ATTACK TYPE
Data Breach

CAUSE OF ISSUE
Security Flaw

TYPE OF LOSS
Reputation/Data

Foodmandu portal hacked

ATTACK TYPE
unauthorised access

CAUSE OF ISSUE
Security Flaw

TYPE OF LOSS
Reputation/Data

A Kathmandu-based food delivery service Foodmandu, was hacked, The Himalayan Times reported. The company stated that they detected a cyber-attack which resulted in unauthorised access of customers' data, particularly name, address, email address and phone number. They also claimed that the loophole was immediately addressed and the company is conducting further investigations

RETAIL

11

Both Boots Advantage and Tesco Clubcard face data breaches

Boots has blocked all Advantage card holders from 'paying with points' after 150,000 accounts were subjected to attempted hacks using stolen passwords. The company is writing to the customers whose accounts are believed to have been affected, and that no credit card details were accessed by the cyber attackers. Meanwhile, Tesco was also hit with a security breach where it said that it would issue replacement Clubcards to more than 620,000 customers after the breach.

ATTACK TYPE
Data Breaches

CAUSE OF ISSUE
Security Flaw

TYPE OF LOSS
Reputation/Data

SpaceX and Tesla documents leaked online by hackers

ATTACK TYPE
Data Leak

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

An American manufacturer which works with SpaceX and Tesla was being extorted by cyber criminals who are leaking documents relating to these companies. The cyber crime group known as DoppelPaymer has already leaked non-disclosure agreements signed between Visser Precision and SpaceX & Tesla. More documents stolen from Visser's network will be released unless the Denver-based firm pays a ransom, the criminals have claimed.

AUTOMOTIVE

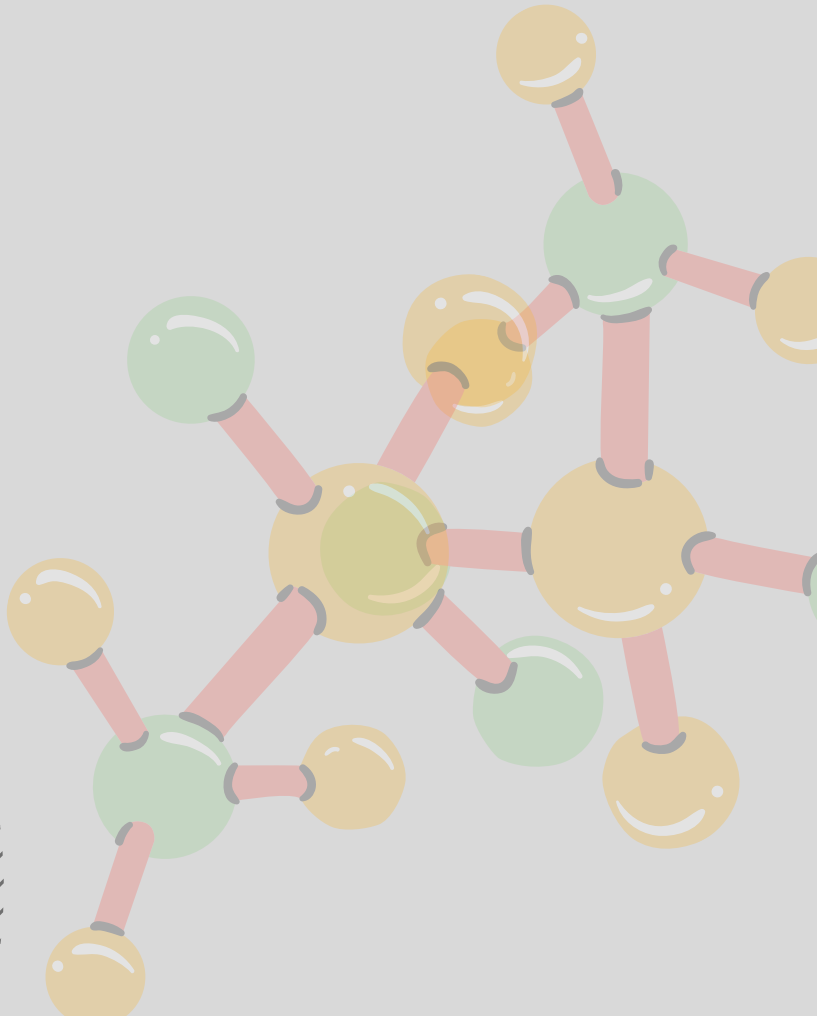
12

CONCLUSION

We hope that the above mentioned threats would have given you a heads up on our tech industry's current scenario, nowadays cyber-attacks have become a day to day struggle and COVID-19 has become an add-on, where it is been misused to spike data-breaches and ransomware attacks.

In order to be away from these data threats and to keep your data safe, just get connected to us and we would help you in keeping your data safe.

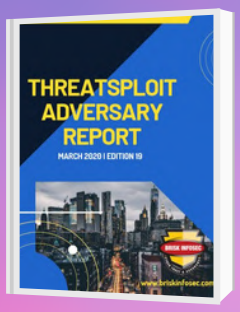
Contact us for more information.

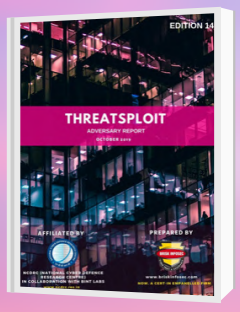


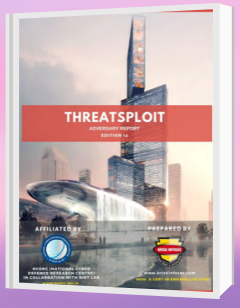
REFERENCES

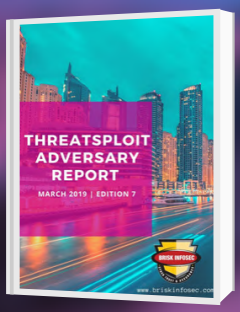
- https://blog.malwarebytes.com/threat-analysis/2020/03/apt36-jumps-on-the-coronavirus-bandwagon-delivers-crimson-rat/
- https://www.forbes.com/sites/zakdoffman/2020/03/16/new-warning-you-must-not-open-this-malicious-coronavirus-app/#345fda015763
- https://www.forbes.com/sites/thomasbrewster/2020/03/16/2500-attacks-in-less-than-a-day-coronavirus-scammers-just-went-into-overdrive/#3840e92e1f0b
- https://www.forbes.com/sites/daveywinder/2020/03/23/covid-19-vaccine-test-center-hit-by-cyber-attack-stolen-data-posted-online/#51722a1218e5
- https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains
- https://thehackernews.com/2020/03/virgin-media-data-breach.html
- https://www.zdnet.com/article/virgin-media-exposes-data-of-900000-users-via-unprotected-marketing-database/
- https://thehackernews.com/2020/03/hackers-compromise-t-mobile-employees.html
- https://www.zdnet.com/article/financial-apps-leak-425gb-in-company-data-through-open-database/?&web_view=true
- https://securityboulevard.com/2020/03/security-breach-disrupts-fintech-firm-finastra/?utm_source=dlvr.it&utm_medium=twitter
- https://www.cbronline.com/news/finastra-hacked
- https://thehackernews.com/2020/03/truefire-guitar-tutoring-data-breach.html
- https://www.infosecurity-magazine.com/news/illinois-college-suffers-data/
- https://globalnews.ca/news/6640313/evraz-regina-cyberattack-layoffs/
- https://www.bleepingcomputer.com/news/security/ryuk-ransomware-attacked-epiq-global-via-trickbot-infection/
- https://www.zdnet.com/article/ryuk-ransomware-hits-fortune-500-company-emcor/
- https://www.middleeastmonitor.com/20200307-israel-defense-ministers-twitter-account-hacked/
- https://www.haaretz.com/israel-news/israeli-defense-minister-s-twitter-account-hacked-feed-features-palestinian-flag-1.8636793
- https://www.timesofisrael.com/bennetts-twitter-page-posts-palestinian-flag-turkish-anthem-in-apparent-hack/
- https://www.thehindu.com/news/cities/mumbai/maharashtra-cid-website-hacked-defaced/article31005341.ece
- https://www.newindianexpress.com/nation/2020/mar/06/maharashtra-polices-cid-website-hacked-message-warning-modi-government-shows-up-2113287.html
- https://punemirror.indiatimes.com/pune/others/maharashtra-cids-website-hacked-we-are-warning-to-modi-govt-indian-police/articleshow/74505000.cms
- https://news-sky-com.cdn.ampproject.org/c/s/news.sky.com/story/amp/spacex-and-tesla-documents-leaked-online-by-hackers-11947792
- https://clutchpoints.com/nuggets-news-jamal-murray-responds-hacked-account/
- https://www.jordanthrilla.com/post/jamal-murray-responds-to-his-adult-tape-leaking-on-instagram
- https://healthitsecurity.com/news/monthlong-cyberattack-disrupts-operations-at-ukentucky-health.
- https://www.healthcareitnews.com/news/europe/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak
- https://portswigger.net/daily-swig/healthcare-data-breach-medical-device-manufacturer-discloses-phishing-attack
- https://www.prnewswire.com/news-releases/princess-cruises-statement-on-cyber-incident-301014787.html
- https://www.infosecurity-magazine.com/news/carnival-cruise-lines-hacked/
- https://www.zdnet.com/article/microsoft-patches-smbv3-wormable-bug-that-leaked-earlier-this-week/
- https://www.techspot.com/news/84345-intel-cpus-vulnerable-new-lvi-attack-breaks-secure.html
- https://www.techspot.com/news/84309-amd-cpus-vulnerable-severe-new-side-channel-attack.html
- https://thehackernews.com/2020/03/amd-processors-vulnerability.html
- https://thehackernews.com/2020/03/ppp-daemon-vulnerability.html
- https://latesthackingnews.com/2020/03/12/avast-antitrack-vulnerability-exposed-users-to-mitm-attacks/
- https://latesthackingnews.com/2020/03/12/avast-antitrack-vulnerability-exposed-users-to-mitm-attacks/
- https://www.bleepingcomputer.com/news/security/blackwater-malware-abuses-cloudflare-workers-for-c2-communication/
- https://latesthackingnews.com/2020/03/18/blisk-browser-vendors-leaked-data-via-unsecured-database-server/
- https://www.zdnet.com/article/slack-vulnerability-allowed-session-hijacking-account-takeovers/
- https://www.techradar.com/news/intel-cpus-at-risk-from-new-snoop-attack
- https://thehackernews.com/2020/03/zyxel-mukashi-mirai-iot-botnet.html
- https://thehackernews.com/2020/03/ddos-botnets-lilin-dvr.html
- https://gbhackers.com/severe-rce-vulnerability-in-openwrt/
- https://thehackernews.com/2020/03/windows-adobe-font-vulnerability.html
- https://threatpost.com/microsoft-warns-of-critical-windows-zero-day-flaws/154040/
- https://www.scmagazine.com/home/security-news/vulnerabilities/news-of-critical-microsoft-bug-leaks-despite-not-making-patch-tuesday-list/?
- https://threatpost.com/critical-bugs-in-rockwell-johnson-controls-ics-gear/153602/
- https://www.securitymagazine.com/articles/91926-koodo-mobiles-data-breach-notification-customer-accounts-and-data-sold-on-dark-web
- https://thehimalayantimes.com/business/foodmandu-portal-hacked/
- https://ictframe.com/foodmandu-a-kathmandu-based-food-delivery-service-has-been-hacked/
- https://www.which.co.uk/news/2020/03/boots-advantage-card-tesco-clubcard-both-suffer-data-breaches-in-same-week/
- https://wrestlingnews.co/wwe-news/wwes-twitter-account-hacked/

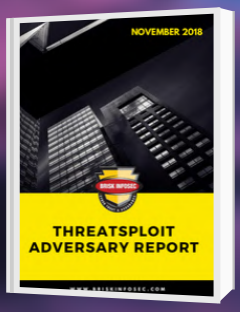
YOU MAY ALSO BE INTERESTED IN OUR PREVIOUS WORKS











FEEL FREE TO REACH US FOR ALL YOUR CYBERSECURITY NEEDS

contact@briskinfosec.com | www.briskinfosec.com

Affiliated by

certin
www.cert-in.org.in

BQS
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