APRIL |2019

EDITION 8

# THREATSPLOIT

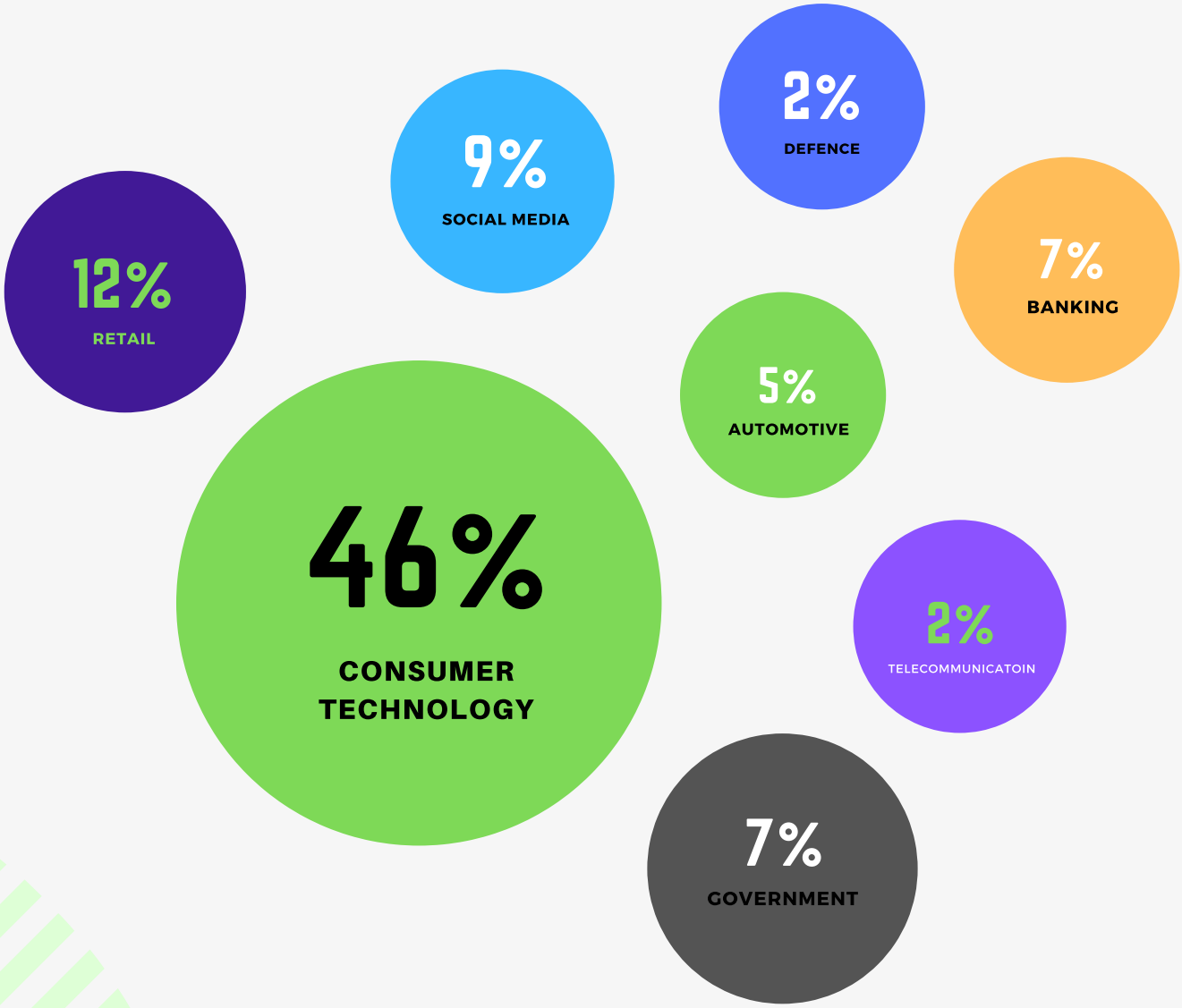
# ADVERSARY REPORT

PREPARED BY

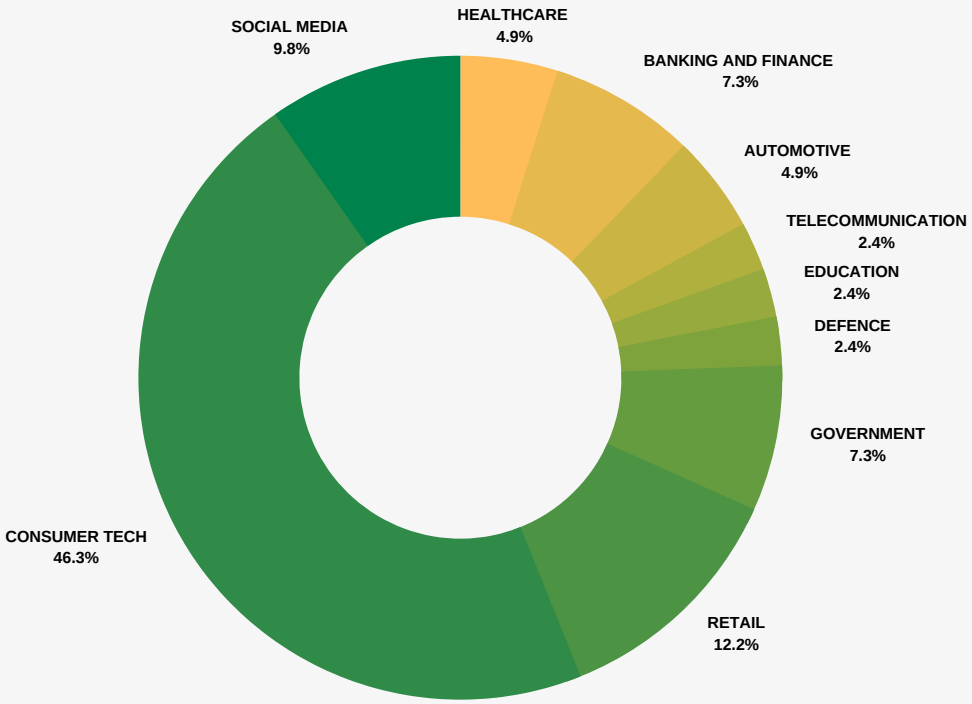

WWW.BRISKINFOSEC.COM

# INTRODUCTION

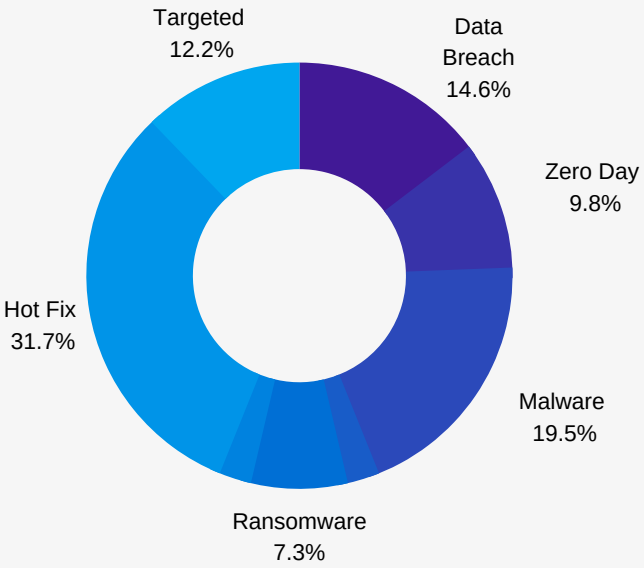
Cyber attackers demonstrated new levels of ambition and an unperturbed determination to achieve their hacking notions in the month of March 2019. When it comes to global cyber landscape, cyber risks are proliferating beyond horizons as technology innovations are increasing and social media dependencies are expanding. The ultimate and honest goal of our Threatsploit Adversary Report is to create awareness for organisations about the major attacks, both existing and emerging, and in helping them to equip best security defences to secure their internal businesses and data.



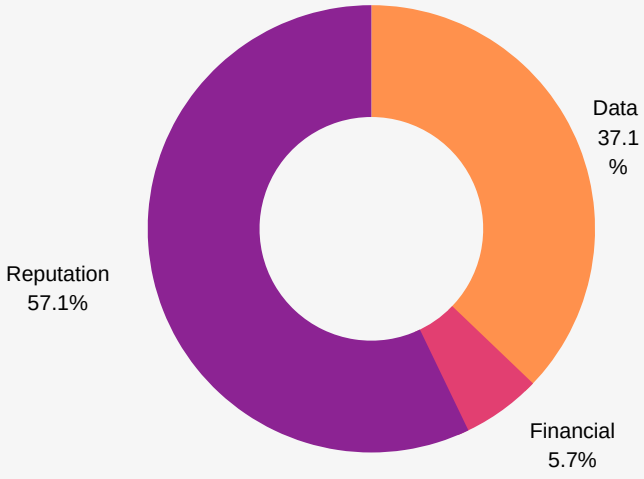
# SECTORS AFFECTED BY ATTACKS




# TYPE OF ATTACKS




# TYPE OF LOSS




Many cyberattacks initiate from various sectors. But, a majority of them originate from consumer technology sector, holding 46% from other sectors. To prevent these, it's evident that cyber security is mandatory.

01

## HEALTHCARE

- Unsecure Fax Server Leaked Patients Data
- Blood Donors, Android Shoppers and Patients Exposed in Trio of Breaches

02

## AUTOMOTIVE

- Hackers Hacked Tesla Model 3 in Pwn2Own
- Notice of the possibility of customer information leak in Tokyo area dealers

03

## BANKING AND FINANCE

- Georgia County Pays $400,000 to Ransomware Attackers
- Citrix Internal Network Hacked by International Criminals
- Gustuff Android banking trojan targets 125+ banking, IM, and cryptocurrency apps

04

## CONSUMER TECHNOLOGY

- OpJerusalem 2019 – JCry ransomware is now infecting Windows users
- Malicious Counter-Strike 1.6 servers used zero-days to infect users with malware
- Libssh Releases Update to Patch 9 New Security Vulnerabilities
- PuTTY Releases Important Software Update to Patch 8 High-Severity Flaws
- Microsoft addresses 18 critical security issues
- Mysterious open database included 'BreedReady' status for 1.8 Million Women
- Patched WinRAR Bug Still Under Active Attack—Thanks to No Auto-Updates
- Cisco Patches High-Severity Flaws in IP Phones
- New Mirai Variant Comes with 27 Exploits, Targets Enterprise Devices
- Cisco Patches Critical 'Default Password' Bug
- Stranger Danger: X-Force Red Finds 19 Vulnerabilities in Visitor Management Systems
- Google's Project Zero reveals zero-day macOS vulnerability to the public
- Severe Java bugs found in IBM Watson and its components
- DMSniff Point-of-Sale Malware Silently Attacked SMBs for Years
- Chinese hacking group backdoors products from three Asian gaming companies
- Remove PirateMatryoshka Trojan From Your PC
- Insecure UC Browser 'Feature' Lets Hackers Hijack Android Phones Remotely
- Zero-day In WordPress SMTP Plug-in
- Apache Bug Lets Normal Users Gain Root Access Via Scripts

05

## RETAIL

- Brace yourselves: Exploit published for serious Magento bug allowing card skimming
- Unprotected Elasticsearch DB exposed 33 Million job profiles in China
- Aluminium producer switches to manual operations after ransomware infection
- Security Lapse Exposed Sensitive Customer Records In Gearbest Data Breach
- Planet Hollywood Owner Suffers Major POS Data Breach

06

## SOCIAL MEDIA

- Facebook Mistakenly Stored Millions of Users' Passwords in Plaintext
- Cybercrime: Over 60000 Facebook users' data leaked; Facebook files lawsuit against Ukrainian hackers
- ExBigg Boss contestant Somi Khan's Instagram hacked
- Man Steals $122m From Facebook And Google By Simply Sending Them Random Bills Which They Paid

07

## DEFENCE

- Hacked tornado sirens taken offline in two Texas cities ahead of major storm

08

## GOVERNMENT

- Police Federation hit by ransomware attack
- BJP official website hacked!
- Gujarat Congress Website Hacked, Hardik's Picture from Purported Sex Tape Uploaded

09

## TELECOMMUNICATION

- Saudi caller ID app leaves data of 5+ million users in unsecured MongoDB server

10

## EDUCATION

- Hackers access applicant data at three U.S. colleges

HEALTH CARE

## Unsecure Fax Server Leaked Patients Data

One of the familiar company in California, Health tech, maintained a fax that wasn't properly secured, reports a Dubai based cybersecurity Company, named as SpiderSilk. The fax server was running an Elasticsearch database that contained more than 6 million records. The server was left unprotected without a password. According to HIPAA, if any other medical company fails to implement competent security, hefty fine will be levied on them.

ATTACK TYPE
*Data Breach*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*USA*

## Blood Donors, Android Shoppers and Patients Exposed in Trio of Breaches

800,000 blood donors in Singapore, a Californian medical software company, and electronics smartphone retailer Gearbest, all these three have suffered cyber breaches recently. The cause of breach is due to misconfigured and insecure servers, and fragile security controls. Due to this, many customers data were pilfered. To thwart such attacks, companies must equip flexible and cost effective solutions.

ATTACK TYPE
*Data Breach*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*SINGAPORE*

AUTOMOTIVE

## Hackers Hacked Tesla Model 3 in Pwn2Own

A bug named as JIT was discovered in Tesla Model 3 in a Pwn2Own contest. The hack guys were named as Richard Zhu and Amat Cam. Together, they're known as Fluoroacetate and triumphantly demonstrated their research one Model 3 internet browser. For their remarkable work, they were gifted with a whopping bounty of $375,000.  Just like honey on cream, they were also gifted with a splendid electric sedan vehicle.

ATTACK TYPE
*Zero day*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*USA*

## Notice of the possibility of customer information leak in Tokyo area dealers

Toyota Motor Corporation (TMC), a car company in Japan was affected by a data breach. The breach exposed the personal information of a million Japanese customers. The exposed information encompassed names, dates of birth, occupation, and much more. The little consoling factor was that, no financial information was disclosed. This is the 2nd time Toyota has been hacked. Officials confirmed that they were working on mitigations.

ATTACK TYPE
*Data Breach*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*Japan*

BANKING AND FINANCE

## Georgia County Pays $400,000 to Ransomware Attackers

Ransomware attack has once again struck a place called Jackson County in Georgia, crippling IT systems over two weeks. The ransomware was named as 'Ryuk', and is said to have originated from the Eastern European group. Unable to redeem from attacks, the companies paid a whopping ransom of $400,000 to the hacking team responsible for this, confirms the officials in Jackson County.

ATTACK TYPE
*Malware*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*SINGAPORE*

## Citrix Internal Network Hacked by International Criminals

On 6th March 2019, FBI officials informed Citrix that their internal Citrix network had been compromised. Without procrastination, Citrix hired some cybersecurity officials and initiated a forensic investigation, took remedial actions to secure their internal network and, carried on their cooperation in FBI. Citrix also informed its customers and conveyed their sincere apologies.

ATTACK TYPE
*Security Breach*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*SINGAPORE*

## Gustuff Android banking trojan targets 125+ banking, IM, and cryptocurrency apps

An Android Banking Trojan named as Gustuff, is now outsmarting the notoriety of other top Trojans like Anubis, Red Alert, Exobot, LokiBot and BankBot. Gustuff uses social engineering attacks to trick the users, turns off Google Play Protect, does phishing attacks, and most significantly can hide its presence, if it fears to be detected. It also has an ATS (Automatic Transfer Service) system right on the user's phone which can open apps, fill in transaction details, and approve money transfers on its own. This Trojan is mostly distributed through SMS spam with its installation link.

ATTACK TYPE
*Malware*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*Global*

## OpJerusalem 2019 – JCry ransomware is now infecting Windows users

ATTACK TYPE
*Malware*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*Israel*

Jcry is a new type of ransomware that is written in Go (Golang) language, a latest language for building ransomware. This attack was a part of OpJerusalem (Operation Jerusalem) campaign. This ransomware targeted hundreds of renowned Israeli websites. To enamour the victims, malicious link was sent as an image, containing message "Your abode flash player version is outdated." Click on the update button to update your player. When users clicked, the malicious code gets downloaded.

## Malicious Counter-Strike 1.6 servers used zero-days to infect users with malware

ATTACK TYPE
*Zero day*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*USA*

Security researchers from a Russian antivirus firm Dr.Web, revealed the fact that a network of malicious Counter-Strike 1.6 multiplayer servers had exploited Remote Code Execution (RCE) vulnerabilities in users with a malware named as Belonard. The computers affected by Belonard were added to a botnet like structure. However, security researchers later confirmed that the network was shutdown.

## Libssh Releases Update to Patch 9 New Security Vulnerabilities

ATTACK TYPE
*Hot Fix*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation*

COUNTRY
*Global*

Libssh2, a popular open source client-side C library implementing the SSHv2 protocol, has released its latest software. The latest software was the version 1.8.1. This newest version patched totally nine security vulnerabilities which could have caused memory corruption issues, arbitrary code execution on the client side. To be away from these, users are requested to upgrade to the latest version.

## PuTTY Releases Important Software Update to Patch 8 High-Severity Flaws

ATTACK TYPE
*Hot fix*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation*

COUNTRY
*Global*

PuTTY, one of the highly familiar open-source client side programs which allows users to remotely access systems over SSH, Telnet, and Rlogin network protocols has released the contemporary version of its software. The latest release version was PuTTY 0.71. It comprised the patch for 8 highly critical security vulnerabilities.

CONSUMER TECHNOLOGY

## Microsoft addresses 18 critical security issues

ATTACK TYPE
*Zero day*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation*

COUNTRY
*USA*

Microsoft patch released on a Tuesday of March, featured patches for 18 vulnerabilities. If those vulnerabilities remain unpatched, they could lead to Remote Code Execution (RCE). The security patches covered a wide range of Microsoft products, with edge being the most notable one.

## Mysterious open database included 'BreedReady' status for 1.8 Million Women

ATTACK TYPE
*Data Breach*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*China*

Victor Gevers, a popular security researcher discovered the startling fact of 29808 databases exposed openly. This was found in China. Further, it was figured out that all those databases contained details of 1.8 million Chinese women. The collected details included names, date of birth, addresses, marital status and more. It was also found that 89% of collected data, were of unmarried woman whom were under the age of 30.

## Patched WinRAR Bug Still Under Active Attack—Thanks to No Auto-Updates

ATTACK TYPE
*Hot Fix*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*USA*

A new WinRaR version 5.70 beta 1 was released by the WinRaR team. This new version patched the critical vulnerability (CVE-2018-20250) which had been existing in the previous WinRaR versions, over a period of 19 years. Many cyber criminals worldwide are still persuading to exploit this recently patched vulnerability. You may ask why? The main reason is the fact that WinRaR software is devoid of an auto-update feature, making it easily vulnerable to cyberattacks.

## Cisco Patches High-Severity Flaws in IP Phones

ATTACK TYPE
*Hot Fix*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*USA*

Cisco systems urged their customers to update many of their IP phones of 8800 series to the latest version. The phones in this series were meant for business purposes. Unfortunately, the IP phones in this series were affected by 5 highly dreadful flaws. Cisco released the latest version alongside the patches on Wednesday. One of the flaws present were CSRF (Cross Site Request Forgery), which forces an end user to execute malicious actions

## New Mirai Variant Comes with 27 Exploits, Targets Enterprise Devices

ATTACK TYPE
*Hot Fix*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation*

COUNTRY
*Global*

A new Mirai variant comes with 11 new exploits. This Mirai version detected during January 2019, targeted WePresent WiPG-1000 wireless presentation system and the LG Supersign TV. These two were the most notable devices that were targeted, reports the Palo Alto Networks Unit 42. The malicious payload is hosted on a Colombian server. With many more exploits added recently, the total sums up to 27.

## Cisco Patches Critical 'Default Password' Bug

ATTACK TYPE
*Hot Fix*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*USA*

Cisco Systems warned customers about a discovery tool named as Cisco Common Service Platform Collector (CSPC). The flaw could allow an adversary to log into the system and collect sensitive data, tied to host operating systems and hardware. The vulnerability is rated as critical, holding a CVSS rating of 9.8. Like adding fuel to the flame, two more critical level vulnerabilities were also found by Cisco. One is related to Cisco Email Security Appliances while the other is related to Cisco Small Business SPA514G IP Phones.

## Stranger Danger: X-Force Red Finds 19 Vulnerabilities in Visitor Management Systems

ATTACK TYPE
*Hot Fix*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*USA*

Two X-Force Red summer interns scrutinized the security of 5 familiar visitor management systems and with much of surprise, they figured out 19 undisclosed vulnerabilities. Few of their findings encompassed the sensitive data leakage, keys to the kingdom, and significant breakout. Further, they also discovered these systems were capable to cause a foothold in destroying corporate networks.

## Google's Project Zero reveals zero-day macOS vulnerability to the public

ATTACK TYPE
*Hot Fix*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation*

COUNTRY
*USA*

Google's project Zero team has recently discovered a critical vulnerability in macOS kernel. The discovered vulnerability is said to grant intruders access to users system without their acknowledgement. Google has earnestly reported this issue to Apple on November 2018 itself. More than 4 months have passed, remedial actions weren't taken. However, Apple is now working on Google's project Zero on a fix.

## Severe Java bugs found in IBM Watson and its components

IBM has announced fixes for five flaws in Java runtime that leave multiple versions of Watson Explorer and IBM Watson Content Analytics vulnerable to various attacks. Post this, the company's Product Security Incident Response Team (PSIRT) has posted an alert about the "high severity" bugs affecting various Watson analytics products, consoles, and the content analytics studio. The best solution is to download and install the IBM Java SDK as soon as possible

ATTACK TYPE
*Hot Fix*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation*

COUNTRY
*USA*

## DMSniff Point-of-Sale Malware Silently Attacked SMBs for Years

ATTACK TYPE
*Malware*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*USA*

A Point of Sale (POS) malware which uses a domain generation algorithm was deployed against small and mid-sized organisations since four years, says a team of security researchers from flashpoint. The malware was identified as DMSniff which gained access of the users systems by launching brute-force attacks or, by scanning for vulnerabilities and exploiting those.

## Chinese hacking group backdoors products from three Asian gaming companies

A dreadful Chinese cyber-espionage team known as the Winneti group has breached the networks of two game makers and a gaming platform to include a backdoor Trojan within their products. However, even a third game named as infestation, has been found vulnerable. Infestation gamers are asked to reinstall their systems as quick as possible

ATTACK TYPE
*Hot Fix*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*Global Asia*

## Remove PirateMatryoshka Trojan From Your PC

ATTACK TYPE
*Malware*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation*

COUNTRY
*Russia*

The PirateMatryoshka is a dreadful malware used to infect computers worldwide. It is primarily distributed by the The Pirate Bay torrent tracker. As per the released security reports, it has been downloaded already about 10,000 times. To get rid of this malware if affected, primary aiding factor is to boot your PC into safe mode and to quarantine it, and its other related objects.

CONSUMER TECHNOLOGY

## Insecure UC Browser 'Feature' Lets Hackers Hijack Android Phones Remotely

UC Browser on smart phones must be immediately uninstalled because the China-made UC Browser contains a "questionable" ability that could be exploited by remote attackers to automatically download and execute code on your Android devices. This hidden feature has been lurking in UC browser since 2016.

ATTACK TYPE
*Remote Code*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation*

COUNTRY
*China*

## Zero-day In WordPress SMTP Plug-in

ATTACK TYPE
*Zero day*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*Global*

The Easy WP SMTP Plug-in is used by WordPress site owners to configure the SMTP settings of their site server's outgoing emails. It's being leveraged by hacker groups to create backdoor admin accounts and redirecting users to tech support scams. Both, NinTechNet and Defiant – cybersecurity companies have reported about the attacks.

## Apache Bug Lets Normal Users Gain Root Access Via Scripts

An important privilege escalation vulnerability (CVE-2019-0211) affects the Apache HTTP server and can be exploited by users whom can write and run scripts to gain root on Unix systems, via scoreboard manipulation. Charles Fol was the first to discover this vulnerability. This flaw is said to impact all the Apache HTTP Server releases from 2.4.17 to 2.4.38.

ATTACK TYPE
*Hot Fix*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*USA*

RETAIL

## Brace yourselves: Exploit published for serious Magento bug allowing card skimming

ATTACK TYPE
*Hot Fix*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation*

COUNTRY
*Global*

An attack code was published on Friday that exploits a critical vulnerability in the Magento e-commerce platform. This exploit affects the following versions:

· Magento Commerce < 1.14.4.1
· Magento Open Source < 1.9.4.1
· Magento < 2.1.17
· Magento < 2.2.8
· Magento < 2.3.1

To protect from this vulnerability, one can install a stand-alone patch. To be fully protected against all vulnerabilities, sites must be upgraded to Magento Commerce or Open Source 2.3.1 or 2.2.8.

## Unprotected Elasticsearch DB exposed 33 Million job profiles in China

A database named as Elasticsearch contained 57GB data of Chinese user's profiles comprised of jobseeker's name, age, city, gender, marital status, phone number, and salary. The database was discovered by Sanyam Jain on 10th March 2019, a security researcher and an active member in GDI foundation. The database was exposed through a search engine called as Shodan.

ATTACK TYPE
*Data Leak*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation*

COUNTRY
*China*

RETAIL

## Aluminium producer switches to manual operations after ransomware infection

ATTACK TYPE
*Ransomware*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*Europe*

This time, a ransomware attack identified as LockerGoga has struck one of the world's largest Aluminium producer named as Norsk Hydro. This ransomware had crippled some of the company's infrastructure and has damaged many operations of its various businesses. The company said that the attack was caused by ransomware infection. They also announced their plans to restore impacted systems using backups. However, the country's Computer Emergency Response Team (CERT) is now cautioning other companies about this obnoxious attack.

## Security Lapse Exposed Sensitive Customer Records In Gearbest Data Breach

Noam Rotem, a renounced white-hat and an activist of VPN mentor's security team has discovered a major security breach in one of the most successful Chinese e-commerce company, named as Gearbest. The company exposed databases that contained unencrypted data like email addresses, passwords of over thousands of users, order details of many sex toys, vouchers, and much more.

ATTACK TYPE
*Data Breach*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*China*

## Planet Hollywood Owner Suffers Major POS Data Breach

ATTACK TYPE
*Data Breach*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation*

COUNTRY
*USA*

Earl Enterprises, the parent company of a popular restaurant chain Planet Hollywood, got hacked and the payment information of more than two million users have been compromised. This included card numbers, customer names, and card expiration dates. Hackers accessed data from restaurant goers at Buca di Beppo, Earl of Sandwich, and Planet Hollywood (Las Vegas, New York and Orlando). They later reported that this incident has been contained.

## Facebook Mistakenly Stored Millions of Users' Passwords in Plaintext

Facebook, once again is hit by a privacy controversy as the passwords of hundred million users unfortunately, were left unencrypted. Apropos of that, even Instagram users were affected. Pedro Canahuati, Facebook's vice president of engineering revealed to press that the company will notify victims, without much delay

ATTACK TYPE
*Hot Fix*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation*

COUNTRY
*USA*

## Cybercrime: Over 60000 Facebook users' data leaked; Facebook files lawsuit against Ukrainian hackers

ATTACK TYPE
*Malware*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*USA*

On 8th March, a federal lawsuit has been filed by one of the most powerful tech beast, Facebook, against two hackers from Ukraine. They had enticed more than 60,000 Facebook users into installing malicious browser extensions. Facebook also claimed that the perpetrators caused a damage of more than $75,000. Facebook sued those hackers whom were found to be affiliated with a tech company named as Web Sun Group.

## ExBigg Boss contestant Somi Khan's Instagram hacked

A former Bigg Boss 12 contestant from Jaipur, Somi Khan got her Instagram account hacked on Saturday. She came to know about this hack incident on Saturday night and informed the Cyber Cell department. She also cautioned people not to believe anything that comes from her Instagram account.

ATTACK TYPE
*Targeted*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*India*

## Man Steals $122m From Facebook And Google By Simply Sending Them Random Bills Which They Paid

ATTACK TYPE
*Targeted*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/financial*

COUNTRY
*Lithuania*

A man from Lithuania named as Evaldas Rimausauskas stole between 2013_2015, a whopping amount of $122 m from two biggest corporate giants. From Facebook, he stole $99m dollars and from Google, he stole $23m. He agreed to forfeit $50m. But, it isn't evident of what he had done with the remaining $72m. Evaldas will be sentenced on July 29th, and faces 30 years in prison.

DEFENCE

## Hacked tornado sirens taken offline in two Texas cities ahead of major storm

Two North Texas towns in Dallas County named as DeSoto and Lancaster, got their tornado emergency sirens turned off by a hacker on the night of March 12th, between 02:30 A.M-04:00 A.M. Over 30 sirens went on and off, with 10 in DeSoto and 20 in Lancaster. According to CBS Dallas, DeSoto and Lancaster officials confirmed it as a hack incident. The two hacked systems were taken offline and have remained offline, ever since then.

ATTACK TYPE
*Malware*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation*

COUNTRY
*Texas*

## Police Federation hit by ransomware attack

ATTACK TYPE
*Ransomware*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*UK*

The Police Federation of England and Wales (PFEW) have been astonishingly struck by a ransomware attack on March 9th 2019. The gruesome attack has swiftly encrypted many databases, servers and made the data and email services inaccessible. The number of police officials who fell in this trap have accounted to 119,000 people. However, a statement was issued by PFEW stating that "instant steps are taken to isolate the attack".

GOVERNMENT

## BJP official website hacked!

Bhartiya Janata Party's (BJP) official website (www.bjp.org) has been hacked by anonymous hackers. No hacker group has claimed responsibility of the attack, till now. When accessed at 11.30 am on Tuesday, the website was hacked with profane language being posted on the website. Later, the site became inaccessible with an error message on it.

ATTACK TYPE
*Targeted*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*India*

## Gujarat Congress Website Hacked, Hardik's Picture from Purported Sex Tape Uploaded

ATTACK TYPE
*Targeted*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation*

COUNTRY
*India*

Kamal Nath late night decision to withdraw security cover from RSS office with just few days before Lok Sabha elections gained intense criticisms from many quarters. Post this, former chief minister and Congress veteran Digvijaya singh rebuked the decision. With government taking no word of mouth on this, Police officials confirmed that additional security measures are kept at booths.

TELECOMMUNICATION

## Saudi caller ID app leaves data of 5+ million users in unsecured MongoDB server

Similar to Truecaller app, Dalil is an Android app that provides caller ID services but only for Saudi and other Arabian users. Security researchers Ran Locar and Noam Rotem, discovered that this app has been leaking user's data like cell phone numbers, device details, telecom operator details, GPS coordinates, and much more, over a week. Roughly, 208,000 unique phone numbers and 44 million app events of data have been leaked. The cause is identified to be a MongoDB database, which has been left accessible online without a password.

ATTACK TYPE
*Malware*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation*

COUNTRY
*Texas*

EDUCATION

ATTACK TYPE
*Ransomware*

CAUSE OF ISSUE
*Lack of awareness*

TYPE OF LOSS
*Reputation/Data*

COUNTRY
*UK*

## Hackers access applicant data at three U.S. colleges

Hackers recently accessed student's data from Hamilton College and from other two colleges. After identification, an official investigation was launched by cybersecurity professionals. It was figured out that a ransomware attack had damaged some of their systems. However, College executives have reached out to those, whose data were accessed and swore safety measures, to safeguard them.

# REFERENCES


- https://techcrunch.com/2019/03/17/medical-health-data-leak/
- https://www.cbronline.com/news/gearbest-elasticsearch
- https://www.bleepingcomputer.com/news/security/2-million-emails-of-350k-clients-possibly-exposed-in-oregon-dhs-data-breach/
- https://www.bankinfosecurity.com/georgia-county-pays-400000-to-ransomware-attackers-a-12159
- https://www.citrix.com/blogs/2019/03/08/citrix-investigating-unauthorized-access-to-internal-network/
- https://www.zdnet.com/article/gustuff-android-banking-trojan-targets-100-banking-im-and-cryptocurrency-apps/
- https://securityaffairs.co/wordpress/83056/data-breach/toyota-data-breach.html
- https://hackersonlineclub.com/hackers-hacked-tesla-model-3-in-pwn2own/?fbclid=IwAR3WBgp9S-ZLAHhPSpk-klPspKbb8-aVuoHLDhM_8x0C45GEpOomazdYdJw
- https://www.zdnet.com/article/saudi-caller-id-app-leaves-data-of-5-million-users-in-unsecured-mongodb-server/
- https://www.securityinfowatch.com/cybersecurity/information-security/news/21071531/hackers-access-applicant-data-at-three-us-colleges
- https://statescoop.com/tornado-sirens-in-dallas-suburbs-deactivated-after-being-hacked-and-set-off
- https://www.zdnet.com/article/police-federation-hit-by-ransomware-attack/
- https://hwnews.in/news/national-news/bjp-official-website-hacked/80960
- https://www.news18.com/news/politics/gujarat-congress-website-hacked-hardiks-picture-from-purported-sex-tape-uploaded-2068255.html
- https://www.terabitweb.com/2019/03/18/unprotected-elasticsearch-db-china-html-2/
- https://www.suchtv.pk/technology/item/83881-huge-norwegian-aluminium-plants-been-hacked.html
- https://www.vpnmentor.com/blog/gearbest-hack/
- https://www.suchtv.pk/technology/item/83881-huge-norwegian-aluminium-plants-been-hacked.html
- https://www.itproportal.com/news/planet-hollywood-owner-suffers-major-user-data-breach/
- https://blog.sucuri.net/2019/03/sql-injection-in-magento-core.html
- https://thehackernews.com/2019/03/uc-browser-android-hacking.html
- https://www.informationsecuritybuzz.com/expert-comments/zero-day-in-wordpress-smtp-plug-in/
- https://securityaffairs.co/wordpress/82030/hacking/opjerusalem-2019-jcry-ransomware.html
- https://securityaffairs.co/wordpress/82293/data-breach/mongodb-open-database.html
- https://www.zdnet.com/article/malicious-counter-strike-1-6-servers-used-zero-days-to-infect-users-with-malware/
- https://thehackernews.com/2019/03/libssh2-vulnerabilities.html
- https://thehackernews.com/2019/03/putty-software-hacking.html
- https://thehackernews.com/2019/03/winrar-hacking-malware.html
- https://threatpost.com/cisco-patches-high-severity-flaws-in-ip-phones/143016/
- https://www.zdnet.com/article/new-mirai-malware-variant-targets-signage-tvs-and-presentation-systems/
- https://threatpost.com/cisco-patches-critical-default-password-bug/142814/
- https://techcrunch.com/2019/03/04/vulnerable-visitor-check-in-systems/
- https://9to5google.com/2019/03/04/google-project-zero-macos-kernel-flaw/
- https://www.zdnet.com/article/ibm-patch-these-critical-java-openj9-java-bugs-in-watson-analytics-products/
- https://latesthackingnews.com/2019/03/18/39-of-counter-strike-1-6-servers-found-to-be-delivering-malware
- https://www.bleepingcomputer.com/news/security/dmsniff-point-of-sale-malware-silently-attacked-smbs-for-years/
- https://www.zdnet.com/article/chinese-hacking-group-backdoors-products-from-three-asian-gaming-companies/
- https://sensorstechforum.com/remove-piratematryoshka-trojan/
- https://www.scmagazine.com/home/security-news/vulnerabilities/march-patch-tuesday-microsoft-addresses-18-critical-security-issues/
- https://securityaffairs.co/wordpress/82030/hacking/opjerusalem-2019-jcry-ransomware.html
- https://thehackernews.com/2019/03/facebook-account-passwords.html?fbclid=IwAR0XFciX-xOOJHCrk_vUJUl7U5fZ_L4W7NL42JQhN78eHPGLGnenW1f8wH0
- https://www.ibtimes.sg/cybercrime-over-60000-facebook-users-data-leaked-facebook-files-lawsuit-against-ukrainian-hackers-29764
- https://timesofindia.indiatimes.com/city/jaipur/ex-bigg-boss-contestant-somis-instagram-hacked/articleshow/68253835.cms
- https://www.sickchirpse.com/man-steals-122m-facebook-google/

# CONCLUSION

Cyberattacks are increasingly sophisticated, innovative, organized, relentless, expert in lurking surreptitiously, and nefarious in their repercussions, costing organizations trillions of losses globally. Our latest reports brings you the latest attacks from different sectors. The chances of avoiding an attempted breach is almost uncertain. We suggest organizations to reach out a competent cybersecurity vendor whom can correctly help them in planning a proper and suitable cybersecurity strategy accordingly. Business executives need to find the right balance between cybersecurity investments, and in sculpting fitting plans that fulfils the unique needs of their organizations.

## TO KNOW MORE ABOUT BRISKINFOSEC

CASE STUDIES

SOLUTIONS

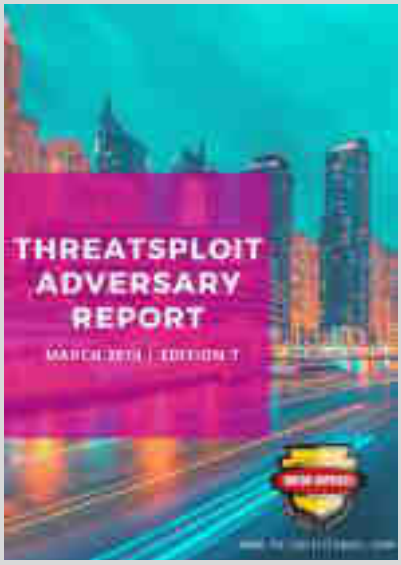
SERVICES

RESEARCH

COMPLIANCES

BLOGS

# YOU MAY INTERESTED ON OUR PREVIOUS WORKS









FEEL FREE TO REACH US FOR ALL YOUR CYBERSECURITY NEEDS

CONTACT@BRISKINFOSEC.COM | WWW.BRISKINFOSEC.COM