AUG 2018

THREATSPLOIT ADVERSARY REPORT

044-4352 4537

www.briskinfosec.com

contact@briskinfosec.com

SECTORS WE FOCUSED

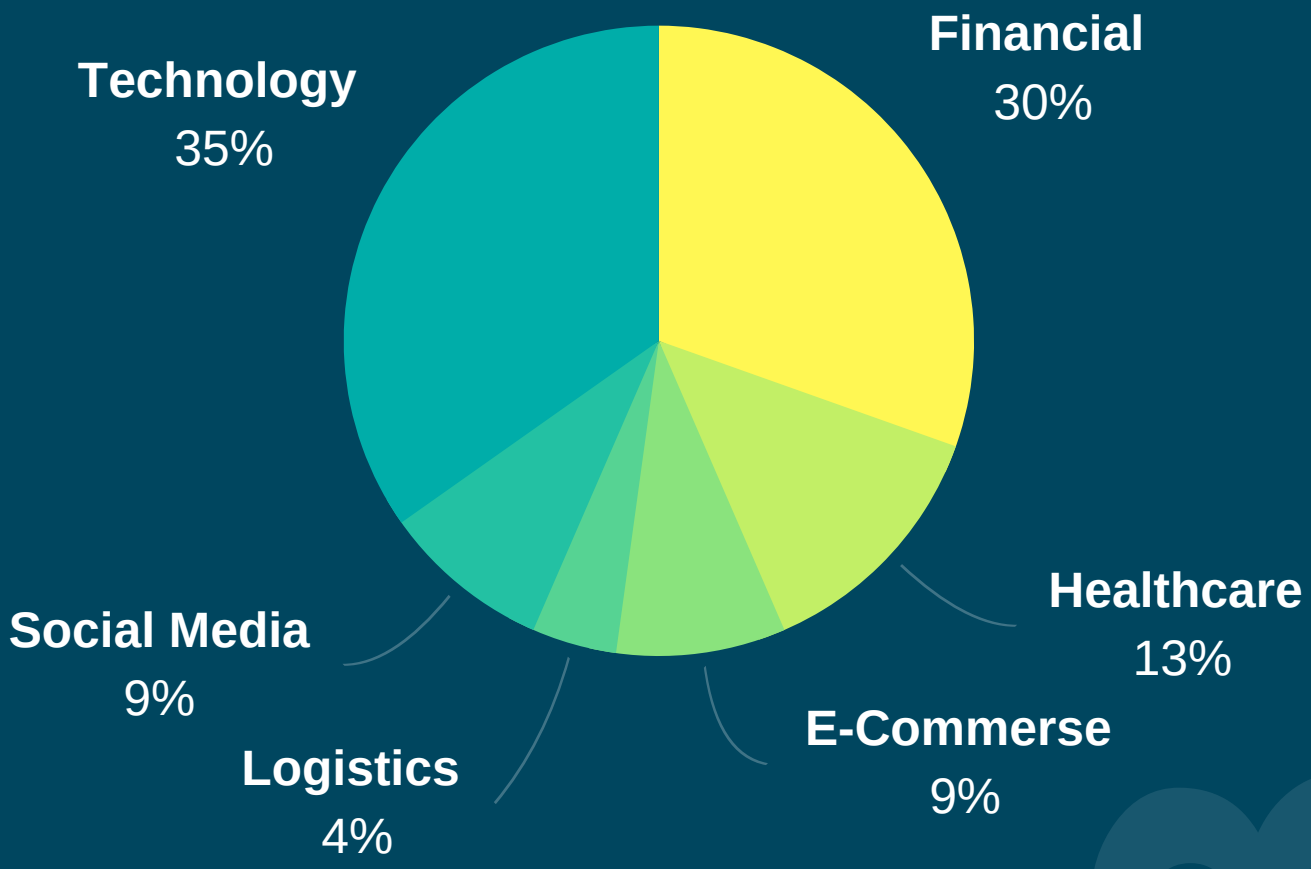
- HEALTH CARE
- FINANCE AND BANKING
- E-COMMERCE
- LOGISTICS
- SOCIAL MEDIA
- TECHNOLOGY

EXECUTIVE SUMMARY

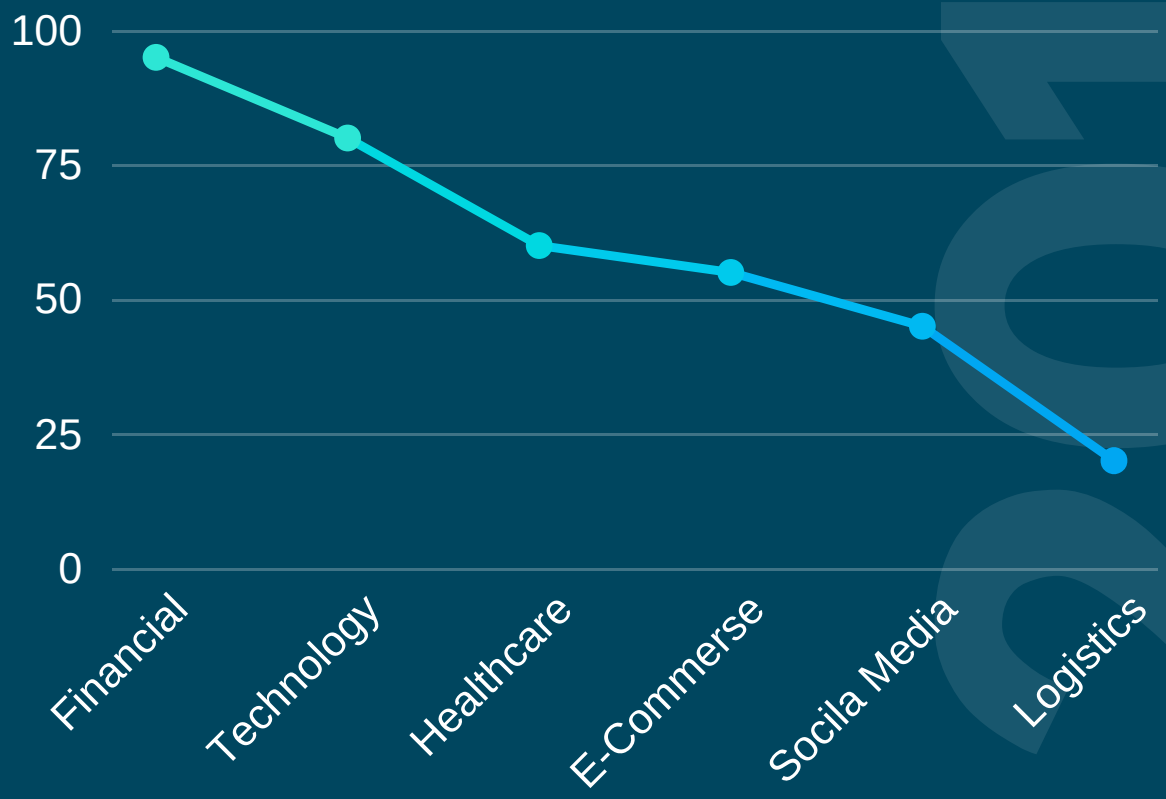
Cyber attackers revealed new levels of ambition in the month of August 2018. When it comes to global cyber landscape Cyber risk continues to grow as technology innovation increases and social dependence on information technology expands. The progression of events has demonstrated the interconnectedness of risks and shared reliance on common internet infrastructure, service providers, and technologies. Goal of the Briskinfosec's Threatsploit Adversary Report - Aug 2018 to educate corporates on major attacks and identify key takeaways to secure their won internal business.

We at BINT LAB explore some longer-term trends, many of which have evolved. We look at organizations that have been targeted or re-compromised after remediating a previous attack .BINT Research Lab conducted the research across north America,Europe,India/Middle-East and the APAC region. We take a detailed look to explore how we leverage sophisticated attacker tactics, techniques and procedures to show organizations what they need to do to stay ahead of those threats

Statistics of Financial loss Aug 2018



Statistics of Reputation loss Aug 2018



ATTACKS ON HEALTH CARE

- Legacy Health E-mail Breach Exposes 38000 Patient's Information
- 417,000 Augusta University Health Patient Records Breached Nearly One Year Ago
- Third-Party Vendor Error Exposes Data Of 19k Patients For 2 Months
- Cyber Vulnerabilities Found In Two Commonly Used Medical Devices

$ BANKING & FINANCE

- Bank Of Spain Hit With DDOS Attack
- Indian Bank Hit in $13.5M Cyberheist After FBI ATM Cashout Warning
- Union Bank Was Hacked And Got Its Money Back
- In Rostov, Hacker Stole More Than A Million Rubles From An ATM
- Brazilian Banking Customers Targeted By IOT DNS Hijacking
- New Phishing Scam Targets Paypal Users
- Third-Party Web Manager Exposes TCM Bank Data

E-COMMERCE

- T-Mobile Hacked — 2 Million Customers Personal Data Stolen
- Hacker Claims To Have 20,000 Customer Records, But Evidence Casts Doubt
- Data Hacked At web Provider Fashion Nexus

LOGISTICS

- Personal Data Leakage Of Russian Railways Passengers
- Air Canada Suffers Data Breach - 20000 Mobile App Users

SOCIAL MEDIA

- Reddit Suffers Data Breach With Hackers Obataining Email Addresses From Some Users
- Widespred Instagram Hack Locking Users Out Of Their Account

TECHNOLOGY

- DNC Calls FBI Attempt To Hack Its voter Database
- Iranian Hackers Target 76 Universities Worldwide To Steal Research
- The Most Profitable RYUK Ransware Attack in the Last Two Weeks
- SAMSAM Ransomware Attacks Extorted Nearly $6Million
- Babysitting App Suffers Temporary Data Breach Of 93000 Users
- Leaked Data From Chinese Hotel Chain May Affect 130 Million Customers
- 16-Year-Old Teen Hacked Apple Servers
- New Php Code Execution Attack Puts Wordspress Site At Risk
- Alleged 19-Year-Old SIM Swapper Used Stolen Bitcoin To Buy Luxury Cars
- EX-NSA Hacker Discloses Macos High Sierra Zero Day Vulnerability

HEALTHCARE

LEGACY HEALTH E-MAIL BREACH EXPOSES 38000 PATIENT'S INFORMATION

Legacy Health submitted a HIPAA Email Breach to the U.S. Department of Health and Human Services (HHS). In the health system, there are 38,000 legacy health patients' personal, medical and billing information might have been accessed in "Email breach".The Portland-based non-profit health system said someone accessed multiple employees' email accounts, some of which contained patient information. Legacy, which operates 6 hospitals and 70 clinics in Oregon and southwest Washington, said Not all of the system's patients are affected by the breach. It also said it's implementing new policies to prevent future breaches.

REPORTED ON
AUG 2018

IMPACT
38000 patients information leaked

COMPANY NAME
Legacy health

WEBSITE
www.legacyhealth.org

ATTACK TYPE
E-mail breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

HEALTHCARE

417,000 AUGUSTA UNIVERSITY HEALTH PATIENT RECORDS BREACHED NEARLY ONE YEAR AGO

A phishing attack aimed at the email accounts of 24 university faculty and administrators at Augusta University Health led to the exposure of medical and personal information on about 417,000 individuals. The hackers solicited usernames and passwords, giving them access to a number of internal email accounts for a small percentage of patients, Social Security and driver's license numbers were included. Notifications will be sent to impacted patients in the coming weeks and will include one year of free credit monitoring. The health system also implemented software to screen emails for protected health or other personal data to prevent a similar incident in the future. Officials said they've also increased security training and enhanced compliance-related policies.

REPORTED ON
AUG 2018

IMPACT
417000 patients and medical information exposed

COMPANY NAME
Augusta university medical center

WEBSITE
www.augustahealth.org

ATTACK TYPE
Phishing attack

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

HEALTHCARE

THIRD-PARTY VENDOR ERROR EXPOSES DATA OF 19K PATIENTS FOR 2 MONTHS

A transcriptionist vendor for Orlando Orthopaedic Center made an error during a software upgrade in dec 2017. But in the process, the server was left open to the public and allowed access without authentication. they became aware of the breach in February 2018. The investigation revealed patient names, dates of birth, insurance details, employers and medical treatment were all included in the exposed data. Social Security numbers were breached for a “limited number of patients.” Officials could not rule out theft or unauthorized access. The HHS Office of Civil Rights takes delayed notification very seriously. Presence Health was hit with a $475,000 fine in January 2017 for waiting about 100 days to report a breach. The fine is pretty severe, given Presence was just 40 days late.

REPORTED ON
AUG 2018

IMPACT
19101 patient’s data exposed by breach

COMPANY NAME
Orlando orthopaedic

WEBSITE
www.orlandoortho.com

ATTACK TYPE
Phishing attack

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
financial/Reputation

COUNTRY
USA

HEALTHCARE

CYBER VULNERABILITIES FOUND IN TWO COMMONLY USED MEDICAL DEVICES

Cyber-security researchers at CyberMDX have discovered two major security flaw in medical devices: Becton Dickinson (BD)’s Alaris TIVA syringe pump and Qualcomm Life Capsule’s Datacaptor Terminal Server (DTS). The researchers worked closely with both the vendors and the vulnerabilities were publically disclosed via the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). They called the flaws as Misfortune Cookie, assigned them a severity rating of 9.8. A potential vulnerability is found in the BD Alaris TIVA syringe pump's software version 2.3.6 and later ones, which were sold outside the United States. The team found out that if a hacker could gain access to a hospital’s network and the Alaris TIVA syringe pump is connected to the server, then the hacker can malicious activity without being caught

REPORTED ON
AUG 2018

IMPACT
Two medical devices

COMPANY NAME
Qualcomm Life Capsule

WEBSITE
qualcommlife.com

ATTACK TYPE
Cyber Threat

CAUSE OF ISSUE
security misconfiguration

TYPE OF LOSS
Reputation

COUNTRY
UK

HEALTHCARE

1.4 MILLION PATIENT RECORDS BREACHED IN UNITYPOINT HEALTH PHISHING ATTACK

UnityPoint Health is notifying 1.4 million patients that their records may have been breached when its business system was compromised by a phishing attack. This is the second breach for UnityPoint this year. the health system's business email system was hit by a series of targeted phishing emails that looked like they were sent from an executive within UnityPoint. An employee fell victim to the emails, which gave hackers access to internal email accounts. The hacked accounts included protected health information, including names, addresses, medical data, treatment information, lab results and/or insurance information. For some of the 1.4 million patients, their payment card and Social Security number were included in the breach. This breach is the largest in the U.S. this year by a landslide.

REPORTED ON
AUG 2018

IMPACT
1.4 million patients data stolen

COMPANY NAME
Unitypoint Health's Meriter Hospital

WEBSITE
www.legacyhealth.org

ATTACK TYPE
E-mail breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

FINANCE

CYBER ATTACK ON COSMOS BANK- 94 CRORE STOLEN

In cosmos bank, the 78 crores were withdrawn through various ATMs located across 28 countries. The bank said this includes 12,000 VISA card transactions. In the same way, the bank said about Rs 2.50 crore was withdrawn through 2,800 debit card transactions in India at various locations. According to reports, Rs 13.9 crore was transferred through SWIFT (Society for Worldwide Interbank Financial Telecommunication) transaction. The bank came to know about the malware attack on its debit card payment system on August 11. It observed that unusual repeated transactions were taking place through ATM VISA and RuPay card for nearly two hours. As soon as the suspicious transactions were reported, the bank immediately shut down its VISA and RuPay debit card payment system.

REPORTED ON
AUG 2018

IMPACT
1300000 dollor stolen

COMPANY NAME
The cosomos co-operative bank limited

WEBSITE
www.cosmosbank.co

ATTACK TYPE
Malware attack

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/financial

COUNTRY
INDIA

FINANCE

BANK OF SPAIN HIT WITH DDOS ATTACK

The Bank of Spain's website hit by a distributed denial-of-service attack which disrupted access to the site. The attack didn't affect the bank's services or communications with the European Central Bank or other institutions. DDoS attack main aims to exhaust the resources of a network, application or service that leads an organization to face the various technical impacts. It is a denial of service attack that intermittently affects access to the website, but it has had no effect on the normal functioning or data breach of the entity. This kind of Powerful DDoS attacks always ends up costing your organization tens of thousands of dollars in man-hours, lost business and reputation damages.

REPORTED ON
AUG 2018

IMPACT
Hackers access the website

COMPANY NAME
Bank of spain

WEBSITE
www.bde.es/bde/es/

ATTACK TYPE
DDOS Attack

CAUSE OF ISSUE
Lack of Awareness

TYPE OF LOSS
Reputation

COUNTRY
SPAIN

FINANCE

INDIAN BANK HIT IN $13.5M CYBERHEIST AFTER FBI ATM CASHOUT WARNING

On Sunday, Aug. 12, The FBI was warning banks about an imminent "ATM cashout" scheme about to unfold across the globe, thanks to a data breach at an unknown financial institution. On Aug. 14, a bank in India disclosed hackers had broken into its servers, stealing nearly $2 million in fraudulent bank transfers and $11.5 million unauthorized ATM withdrawals from cash machines in more than two dozen countries.

REPORTED ON
AUG 2018

IMPACT
1300000 dollor stolen

COMPANY NAME
The cosomos co-operative bank limited

WEBSITE
www.cosmosbank.co

ATTACK TYPE
malware attack

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/financial

COUNTRY
INDIA

FINANCE

UNION BANK WAS HACKED AND GOT ITS MONEY BACK

The Union Bank of India hacking was triggered after an employee clicked on a phishing email that released malware into the bank's servers. The unidentified hacker was attempting to swindle us of $171 million (about Rs1,100 crore at today's rates) from our Nostro account.
The "phishing" an attempt to obtain sensitive information such as usernames, passwords and other financial details by pretending to be a trustworthy entity—mails were sent to 15 email IDs. Unfortunately phishing email and clicked on the link which released the malware that went viral on the bank's servers. The hackers would have got their way and swindled the cash but for a silly mistake, they made, according to Shinde.

REPORTED ON
AUG 2018

IMPACT
sensitive information leaked

COMPANY NAME
union bank

WEBSITE
www.unionbankofindia.co.in

ATTACK TYPE
phishing attack

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

FINANCE

IN ROSTOV, HACKER STOLE MORE THAN A MILLION RUBLES FROM AN ATM

Rostov police are looking for an unknown hacker who deftly stole from the ATM 1 million 264 thousand rubles without breaking the ATM. Presumably, on August 14, the hacker opened the ATM's pin-keyboard then connected to it and withdrew a large sum of money. It is interesting to note that the loss of money was noticed only two weeks later, as the hacker did not damage the device. Only on August 29, the head of the security service of the Bank appealed to the police and reported the theft of a large sum of money. The hacker hasn't been caught yet.

REPORTED ON
AUG 2018

IMPACT
1300000 dollor stolen

COMPANY NAME
the cosomos co-operative bank limited

WEBSITE
www.cosmosbank.co

ATTACK TYPE
malware attack

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/financial

COUNTRY
RUSSIA

FINANCE

BRAZILIAN BANKING CUSTOMERS TARGETED BY IOT DNS HIJACKING

The researchers discovered malicious servers attempting to reconfigure vulnerable IoT devices in Brazil using an unauthenticated remote configuration URL which changes the DNS server settings of the modems/routers and resulting in all name resolution within the home of the affected consumers to be routed through malicious DNS servers.The attack redirects users seeking popular financial site, such as those used to pay a bill or check a bank statement. Researchers said the malicious DNS server controlling the attacks effectively becomes the middleman that provides the malicious actor to bring up fake portals and web fonts to collect sensitive information from users whose routers were infected. these attacks target the IoT device owner rather than other entities.

REPORTED ON
AUG 2018

IMPACT
sensitive information leaked

COMPANY NAME
General

WEBSITE
general

ATTACK TYPE
DNS hijacking

CAUSE OF ISSUE
Targeted attack

TYPE OF LOSS
Reputation

COUNTRY
BRAZIL

FINANCE

NEW PHISHING SCAM TARGETS PAYPAL USERS

New email-based phishing attack designed to steal the login and password credentials for their Internet payment accounts. The scam email, which is just the latest hoax targeting the PayPal community, tells users that several different computers have recently tried to access their account with numerous failed password attempts.
In order to "restore" access, users are advised to fill out an attached form, identified Restore_your_account_PayPal.html. Entering your confidential information into the form is only going to pass your private data to the cybercriminals behind this spam campaign who will use it to phish your account for money and perhaps steal your identity

REPORTED ON
AUG 2018

IMPACT
steal login and password credentials

COMPANY NAME
paypal

WEBSITE
www.paypal.com

ATTACK TYPE
Phishing attack

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
US

FINANCE

THIRD-PARTY WEB MANAGER EXPOSES TCM BANK DATA

The TCM Bank, a limited-purpose credit card bank wholly owned by ICBA Bancard, revealed recently that a website misconfiguration by the third party has leaked personal information of credit card applicants for 16 months. The victims are those who have applied in between March 2017 – July 2018, which is the time period the breach had hit the bank. The breach has exposed the applicants' names, addresses, DOBs and social security numbers. The data revealed that only less than 10,000 applicants were victims among the whole of the applicants. It was less than 25% of the applications we processed during the relevant time period that were potentially affected, and less than one per cent of our cardholder base was affected here

REPORTED ON
AUG 2018

IMPACT
10000 applicants are victims

COMPANY NAME
TCM Bank

WEBSITE
www.icba.org/corporate-members/tcm-bank/home

ATTACK TYPE
Third Party data breach

CAUSE OF ISSUE
Security misconfiguration

TYPE OF LOSS
Reputation

COUNTRY
USA

E-commerc

T-MOBILE HACKED — 2 MILLION CUSTOMERS' PERSONAL DATA STOLEN

T-Mobile confirmed that the telecom giant suffered a security breach on its US servers. The hackers were able to exploit an internal API (application programming interface) on its servers that handled personal information. The leaked information includes customers' name, billing zip code, phone number, email address, account number, and account type. T-Mobile said more than 2 million people may have had their information stolen, representing about 3 per cent of its 75 million-plus customer base. However, the good news is that no financial information like credit card numbers, social security numbers, or passwords, were compromised in the security breach.

REPORTED ON
AUG 2018

IMPACT
2 million customers personal data stolen

COMPANY NAME
General

WEBSITE
General

ATTACK TYPE
security Breach

CAUSE OF ISSUE
Security misconfiguration

TYPE OF LOSS
Reputation

COUNTRY
US

E-COMMERCE

HACKER CLAIMS TO HAVE 20,000 CUSTOMER RECORDS, BUT EVIDENCE CASTS DOUBT

Hackers claim to have stolen personal information belonging to 20000 Superdrug customers in a targeted cyber attack. The details of 20,000 users, including names, dates of birth and contact numbers. Credit or debit card information linked to the accounts were not accessed, it added. Superdrug had evidence that 386 accounts had been affected by the breach, and urged its online customers to change their passwords. The group attempted to force the company to pay a ransom, it confirmed. We believe the hacker obtained customers' email addresses and passwords from other websites and then used those credentials to access accounts on our website," Superdrug said in a statement.

REPORTED ON
AUG 2018

IMPACT
Exposed 20k users details

COMPANY NAME
Superdrug

WEBSITE
www.superdrug.com

ATTACK TYPE
Sensitive data exposer

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
USA

E-COMMERCE

DATA HACKED AT WEB PROVIDER FASHION NEXUS

The email and home addresses of around 650,000 fashion shoppers were stolen following a security breach at e-commerce platform provider Fashion Nexus. The data breach allowed hackers to access customer details from fashion brands including Elle Belle Attire, AX Paris and Traffic People. Online fashion retailers Perfect Handbags and DLSB were also believed to be affected. Fashion Nexus said that on or around 9 July a "white hat hacker" or "ethical hacker" breached one of the company's web servers.

REPORTED ON
AUG 2018

IMPACT
650K users affected by hack

COMPANY NAME
Fashion nexus

WEBSITE
www.fashionnexus.co.uk

ATTACK TYPE
E-mail Breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
UK

ILOGISTICS

PERSONAL DATA LEAKAGE OF RUSSIAN RAILWAYS PASSENGERS

people who serve the Internet resources of companies make stupid mistakes. The reasons behind data leakage are Unprofessionalism and incompetence of IT professionals and the attempts of companies to save money.
How can it be dangerous? For example, a person buys a train ticket with a departure date in six months. He receives an SMS with a link to his personal account to view and edit information. At the same time, "Yandex. Browser", Android or metric counter tells the search engine that a previously unknown page has appeared. The search engine sees that the page is working and indexes it. Hackers who do searches related to train ticket booking gets the data and access the user's personal account

REPORTED ON
AUG 2018

IMPACT
users personal accounts exposes

COMPANY NAME
Russian railways

WEBSITE
eng.rzd.ru

ATTACK TYPE
Security Misconfiguration

CAUSE OF ISSUE
security misconfiguration

TYPE OF LOSS
Reputation

COUNTRY
RUSSIA

LOGISTICS

AIR CANADA SUFFERS DATA BREACH - 20,000 MOBILE APP USERS AFFECTED

Air Canada says personal information of 20,000 of its mobile app users may have been affected by a data breach. In a news release, the airline explained that it noticed “unusual login activity” between Aug. 22-24. All users of the app — about 1.7 million customers — have been locked out of their accounts until they update their passwords. Users have also been emailed instructions on how to log in to the app and change passwords. The app stores names and contact information, which may have been accessed.
It also may hold information such as passport and NEXUS card numbers, gender, birth date, nationality and credit card numbers. While Aeroplan passwords are not stored on the Air Canada app, it is also asking users to track activity out of precaution. Air Canada added that the breach does not affect those who have an account on aircanada.com.

REPORTED ON
AUG 2018

IMPACT
20000 users information leakeds

COMPANY NAME
Air Canada

WEBSITE
www.aircanada.com

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Broken Authentication

TYPE OF LOSS
Reputation

COUNTRY
CANADA

SOCIAL MEDIA

REDDIT SUFFERS DATA BREACH WITH HACKERS OBTAINING EMAIL ADDRESSES FROM SOME USERS

Reddit announced that it suffered a security breach in June that exposed some of its users' data, including their current email addresses and an old 2007 database backup containing usernames and hashed passwords. hacker(s) managed to gain read-only access to some of its systems that contained its users' backup data, source code, internal logs, and other files. The hack was accomplished by intercepting SMS messages that were meant to reach Reddit employees with one-time passcodes, eventually circumventing the two-factor authentication (2FA)

REPORTED ON
AUG 2018

IMPACT
Exposed user's data

COMPANY NAME
Reddit

WEBSITE
www.reddit.com

ATTACK TYPE
Security Misconfiguration

CAUSE OF ISSUE
Authentication bypassed

TYPE OF LOSS
Reputation

COUNTRY
USA

SOCIAL MEDIA

WIDESPREAD INSTAGRAM HACK LOCKING USERS OUT OF THEIR ACCOUNTS

A growing number of Instagram users are taking to social media, including Twitter and Reddit, to report a mysterious hack which involves locking them out of their account with their email addresses changed to .ru domains. According to victims, their account names, profile pictures, passwords, email addresses associated with their Instagram accounts, and even connected Facebook accounts are being changed in the attack. Many of the affected Instagram users are also complaining about their profile photos replaced with stills from popular films, including Despicable Me 3 and Pirates of the Caribbean. Although it is still unknown who is behind the widespread hack of Instagram accounts, the use of the email addresses originating from Russian email provider mail.ru may indicate a Russian hacker or hacking group is behind the attack, or perhaps hackers pretending to be from Russia.

REPORTED ON
AUG 2018

IMPACT
Gaining access on accounts

COMPANY NAME
Instagram

WEBSITE
www.paypal.com

ATTACK TYPE
Data tampring

CAUSE OF ISSUE
security Misconfiguration

TYPE OF LOSS
Reputation

COUNTRY
USA

TECHNOLOGY

DNC CALLS FBI AFTER DETECTING ATTEMPT TO HACK ITS VOTER DATABASE

The DNC said that it now believes a phishing attempt that was part of an unauthorized test on its Vote Builder system was performed by a third-party and it had worked with its service provider to help thwart the suspected attack
The Democratic National Committee said Wednesday that it has thwarted a hacking attempt on its database holding information on tens of millions of voters across the country.

REPORTED ON
AUG 2018
IMPACT
Voter database information
COMPANY NAME
General
WEBSITE
General
ATTACK TYPE
Phishing Attackr
CAUSE OF ISSUE
Lack of awareness
TYPE OF LOSS
Reputation
COUNTRY
USA

TECHNOLOGY

IRANIAN HACKERS TARGET 76 UNIVERSITIES WORLDWIDE TO STEAL RESEARCH

A total of 76 universities in 14 countries have been targeted including institutions. The Mabna Institute, working as part of Cobalt Dickens, allegedly stole information from 76 universities across 21 countries, as well as 47 US and foreign private sector companies, including the US Department of Labor and the United Nations. After discovering a spoof website which masqueraded as one of the target universities, CTU uncovered a wider campaign designed to steal credentials from academic staff.In total, 16 domains have been used by the threat actors to host over 300 spoofed websites, including university login pages and online libraries. The majority of the domains were registered between May and August 2018. The campaign appears to be ongoing, as the latest domain registration took place on August 19.

REPORTED ON
AUG 2018
IMPACT
76 university impacted for ransomware
COMPANY NAME
General
WEBSITE
General
ATTACK TYPE
E-mail Breach
CAUSE OF ISSUE
Lack of awareness
TYPE OF LOSS
Reputation
COUNTRY
General

TECHNOLOGY

THE MOST PROFITABLE RYUK RANSOMWARE ATTACK IN THE LAST TWO WEEKS

$640,000 in just 2 weeks and still counting, that is the estimated total revenue of the Ryuk ransomware that attacked various enterprise PCsHermes ransomware which originated from the infamous Lazarus Group of North Korea, it is strongly believed that Ryuk is also the creation of the same group. A malware commonly attributed to the notorious North Korean APT Lazarus Group, which was also used in massive targeted attacks.The malware will attempt to write a dummy file to the Windows directory, which would only be allowed with Admin privileges. If the creation of the file failed, it will sleep for a while and attempt the same another five times. If failure persists beyond these attempts, Ryuk will simply terminate. If the file was successfully created, it will write two more files to a subfolder in the Windows directory.

REPORTED ON
AUG 2018

IMPACT
$640,000 and still counting

COMPANY NAME
General

WEBSITE
General

ATTACK TYPE
Ryuk ransomware

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation/Financial

COUNTRY
General

TECHNOLOGY

SAMSAM RANSOMWARE ATTACKS EXTORTED NEARLY $6 MILLION

By tracking all the Bitcoin addresses researchers were able to find, Sophos says it identified at least 233 victims who paid a ransom to the SamSam crew. Half of the victims who paid were private sector companies, while around a quarter was healthcare organization, followed by 13% of victims being government agencies, and around 11% being institutions in the education sector. The Sophos team says it identified 157 Bitcoin addresses used in SamSam ransom notes that received payments, and another 88 who did not receive any money. The total funds stored in these addresses is around $5.9 million, which is way more than previous estimates about the group's financial prowess that had its earnings at only $850,000.Sophos says that SamSam usually makes around one victim per day, and one in four victims pay the ransom.

REPORTED ON
AUG 2018

IMPACT
$6 million paid to hackers

COMPANY NAME
General

WEBSITE
General

ATTACK TYPE
Ransomware Attack

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation/Financial

COUNTRY
General

TECHNOLOGY

BABYSITTING APP SUFFERS 'TEMPORARY DATA BREACH' OF 93,000 USERS

Babysitting-booking app Sitter "temporarily" exposed the personal data of 93,000 account holders, according to a researcher who recently discovered the trove of data using the Shodan Internet of Things (IoT) search engine.
Bob Diachenko explains how he found the 2GB MongoDB database on August 13, which contained phone numbers, addresses, transaction details, phonebook contacts, partial credit card numbers, and encrypted account passwords. Other information included in-app chat and notification history, plus details of which users needed a babysitter at what time and at which address.

REPORTED ON
AUG 2018

IMPACT
93000 users data breached

COMPANY NAME
unknown

WEBSITE
unknown

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
Unknown

TECHNOLOGY

LEAKED DATA FROM CHINESE HOTEL CHAIN MAY AFFECT 130 MILLION CUSTOMERS

Personal data and booking information from 13 hotels operated by Huazhu Hotels Group has reportedly been leaked in data breach A post on a Chinese dark web forum titled "Huazhu-owned hotels booking data" claimed to be selling personal data and information of customers from Huazhu-owned hotels including Hanting Inns, Hi Inn, and JI Hotel. According to local reports, 130 million customers are believed to be affected by the breach. Leaked information potentially includes 240 million lines of data containing phone numbers, email addresses, bank account numbers, and booking details are selling for 8 bitcoins per individual.T he seller reportedly lowered its asking price to 1 bitcoin after the news spread quickly across local media. Huazhu Hotels Group released an official statement (in Chinese) saying that an internal investigation is underway and the public security bureau is investigating the case

REPORTED ON
AUG 2018

IMPACT
$6 million paid to hackers

COMPANY NAME
General

WEBSITE
General

ATTACK TYPE
Ransomware Attack

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation/Financial

COUNTRY
CHINA

TECHNOLOGY

16-YEAR-OLD TEEN HACKED APPLE SERVERS

The 16 age teenager from Melbourne, Australia, managed to break into Apple servers and downloaded some 90GB of secure files, including extremely secure authorized keys used to grant login access to users, as well as access multiple user accounts. The teen, whose name is being withheld as he's still a minor, hacked the company's servers not once, but numerous times over the course of more than a year, and Apple's system administrators failed to stop their users' data from being stolen. When Apple finally noticed the intrusion, the company contacted the FBI, after detecting his presence on their servers and blocking him. The Australian Federal Police AFP caught the teenager last year after a raid on his residence and seized two Apple laptops, a mobile phone, and a hard drive. IP address matched the intrusions into the organization.

REPORTED ON
AUG 2018
IMPACT
90GB of secure files
COMPANY NAME
Apple
WEBSITE
www.apple.com
ATTACK TYPE
Improper access control
CAUSE OF ISSUE
Authorised key exposed
TYPE OF LOSS
Reputation
COUNTRY
USA

TECHNOLOGY

NEW PHP CODE EXECUTION ATTACK PUTS WORDPRESS SITES AT RISK

A new exploitation technique that could make it easier for hackers to trigger critical deserialization vulnerabilities in PHP programming language using previously low-risk considered functions. The new technique leaves hundreds of thousands of web applications open to remote code execution attacks, including websites powered by some popular content management systems like WordPress and Typo3. PHP unserialization or object injection vulnerabilities were initially documented in 2009, which could allow an attacker to perform different kinds of attacks by supplying malicious inputs to the unserialize() PHP function.

REPORTED ON
AUG 2018
IMPACT
Attcker could view, change or even cre a new account according to his privilages
COMPANY NAME
General
WEBSITE
General
ATTACK TYPE
Ransomware Attack
CAUSE OF ISSUE
Targeted Attack
TYPE OF LOSS
Reputation/Financial
COUNTRY
CHINA

TECHNOLOGY

ALLEGED 19-YEAR-OLD SIM SWAPPER USED STOLEN BITCOIN TO BUY LUXURY CARS

It appears that Narvaez spent some of the Bitcoin he stole on sports cars. Through DMV records, the police found that Narvaez purchased a 2018 McLaren paying partly in Bitcoin and partly by trading-in a 2012 Audi R8, which Narvaez purchased with Bitcoin in June 2017. The investigators obtained records from Bitcoin payment provider BitPay, and cryptocurrency exchanges Bittrex. According to the document, AT&T provided authorities with the unique identifying numbers—or IMEI—of cell phones used to take over victim's numbers, the coordinates of cell phone towers which those phones connected to, and Narvaez's call records. This information revealed that Narvaez's phone was connected to the same cell phone tower, and at the same time, as one of the phones used to SIM swap victims.

REPORTED ON
AUG 2018
IMPACT
Stolen bitcoins
COMPANY NAME
general
WEBSITE
general
ATTACK TYPE
Sim swapping
CAUSE OF ISSUE
Targeted Attack
TYPE OF LOSS
Reputation/financial
COUNTRY
USA

TECHNOLOGY

EX-NSA HACKER DISCLOSES MACOS HIGH SIERRA ZERO-DAY VULNERABILITY

A safety researcher has demonstrated, on the current Def Con safety convention, Mac pc working Apple's Excessive Sierra working system may be very simply hacked by merely tweaking two strains of the code. This revelation was made by Patrick Wardle, an ex-NSA hacker. Report dated August 13, 2018, provides an in-depth rationalization of this vulnerability and its detection. The report says- "Your Mac pc working the Apple's newest Excessive Sierra working system may be hacked by tweaking simply two strains of code, a researcher demonstrated on the Def Con safety convention Patrick Wardle himself explains: "By way of a single click on, numerous safety mechanisms could also be fully bypassed. Run the untrusted app? click on …allowed. Authorize keychain entry? click on …allowed. Load Third-party kernel extension? click on …allowed. Authorize an outgoing community connection? click on allowed."

REPORTED ON
AUG 2018
IMPACT
Allowing to install malisious files
COMPANY NAME
Apple
WEBSITE
www.apple.com
ATTACK TYPE
Zero day vulnerability
CAUSE OF ISSUE
MAC OS
TYPE OF LOSS
Reputation
COUNTRY
USA

CONCLUSION

Cyber adversaries are increasingly sophisticated, innovative, organized, and relentless in developing new and nefarious ways costing organizations trillions globally with an Expected increase to the trillion annually. Our latest reports bring you the latest attacks from different sectors. The chance of avoiding an attempted breach is almost non-existent. We suggest that organizations ascertain their own risk tolerance and plan a Cybersecurity strategy accordingly. Business executives need to find the right balance between Cybersecurity investments and securing appropriate plans suitable for the unique needs of their Industry or organization.

Reference Link

Health Care

- https://www.legacyhealth.org/our-legacy/stay-connected/newsroom/notice-of-email-phishing-incident.aspx
- https://www.augusta.edu/notice/?campaign_url=https%253A%252F%252Fwww.augustahealth.org%252F&ga_cid=2142552651.1534519563#notice
- https://www.orlandosentinel.com/health/os-orlando-ortho-center-breach-20180720-story.html#
- https://www.medicalplasticsnews.com/mpn-north-america/cyber-vulnerabilities-found-in-two-major-medical-devices/

Finance & Banking

- https://www.cybersecurity-insiders.com/bank-of-spain-website-hit-by-ddos-cyber-attack/
- https://forums.hardwarezone.com.sg/eat-drink-man-woman-16/indian-bank-hit-%2413-5m-cyberheist-after-fbi-atm-cashout-warning-5886731.html
- http://bankersdaily.in/hacked-how-171-mn-stolen-from-union-bank-was-recovered-every-bankers-must-know/
- http://www.ehackingnews.com/2018/09/in-Rostov-hacker-stole-more-than.html
- https://www.scmagazineuk.com/brazilian-banking-customers-targeted-iot-dns-hijacking-attacks/article/1490426
- https://www.esecurityplanet.com/news/article.php/3920031/New-Phishing-Scam-Targets-PayPal-Users.htm
- http://ago.vermont.gov/blog/2018/08/07/tcm-bank-n-a-data-security-incident-notice-to-consumers/

E-commerce

- https://thehackernews.com/2018/08/t-mobile-hack-breach.html
- https://www.mirror.co.uk/tech/superdrug-targeted-hackers-who-claim-13119820

Logistics

- https://www.fastnethost.com/blog/personal-data-leakage-of-russian-railways-passengers/
- https://www.aircanada.com/us/en/aco/home/book/travel-news-and-updates/2018/notice-air-canada-mobile-app-users.html

Social Media

- https://www.reddit.com/r/announcements/comments/93qnm5/we_had_a_security_incident_heres_what_you_need_to/
- https://instagram-press.com/blog/2018/08/14/issue-affecting-access-to-instagram-accounts/

Technology

- https://www.telegraph.co.uk/news/2018/08/22/democratic-national-committee-calls-fbi-new-hacking-attempt/
- https://www.zdnet.com/article/iran-hackers-target-70-universities-in-14-countries/
- https://hackercombat.com/north-koreas-ryuk-ransomware-the-most-profitable-ransomware-in-the-last-two-weeks/
- https://www.bleepingcomputer.com/news/security/samsam-ransomware-crew-made-nearly-6-million-from-ransom-payments/
- https://cyware.com/news/babysitting-app-sitters-exposed-2gb-data-and-93000-users-personal-details-56ccf63a
- https://securityaffairs.co/wordpress/75741/deep-web/chinese-hotel-chain-data-leak.html
- https://thehackernews.com/2018/08/apple-hack-servers.html
- https://thehackernews.com/2018/08/php-deserialization-wordpress.html
- https://motherboard.vice.com/en_us/article/wjka95/sim-swapper-arrest-bitcoin-luxury-cars
- https://thehackernews.com/2018/08/macos-mouse-click-hack.html

This adversary research report is proudly presented by

BRISKINFOSEC TECHNOLOGY AND CONSULTING PVT LTD

Feel free to reach us for all your cybersecurity needs
contact@briskinfosec.com | www.briskinfosec.com |
USA|INDIA|UK