THREATSPLOIT ADVERSARY REPORT FOR SEP 2018

☎ 044-43524537

www.briskinfosec.com

✉ Contact@briskinfosec.com

BRISK INFOSEC
CYBER TRUST & ASSURANCE

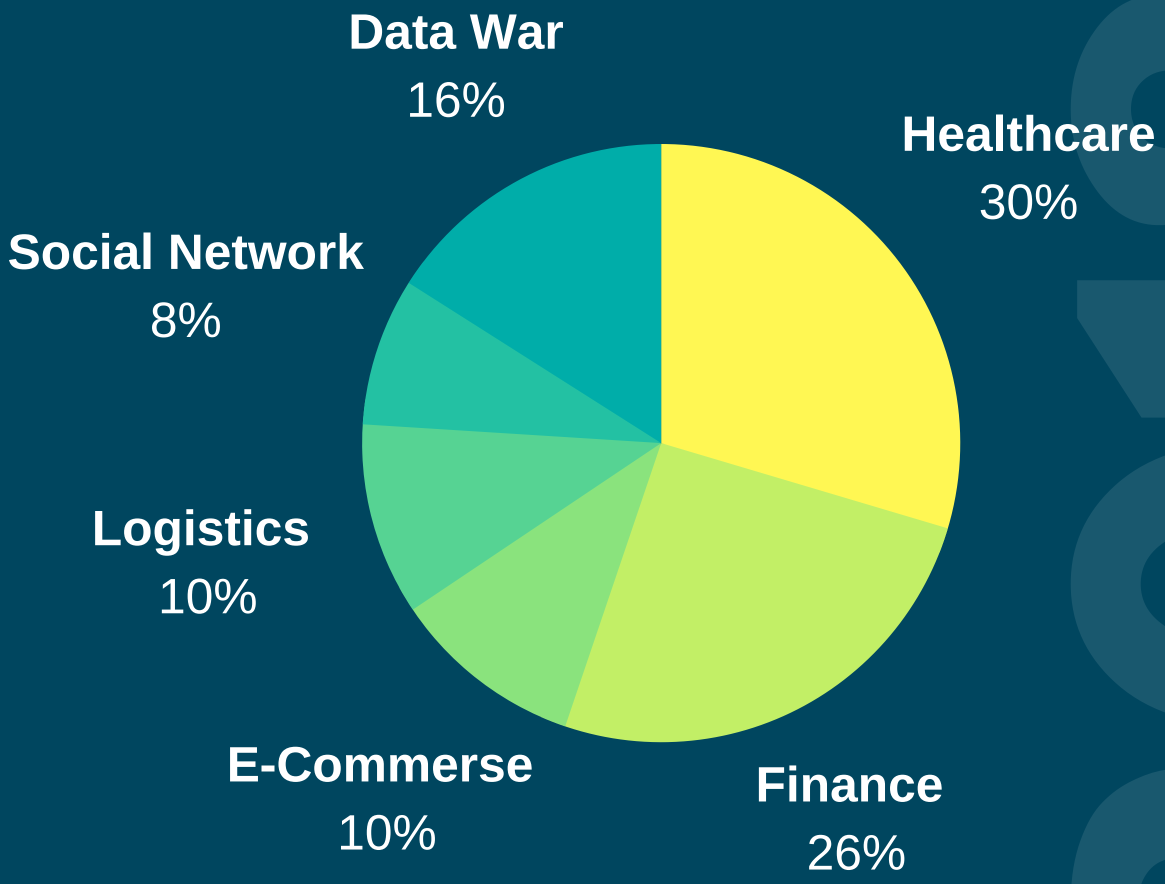
DIRECTOR'S STATEMENT

SEP 2018

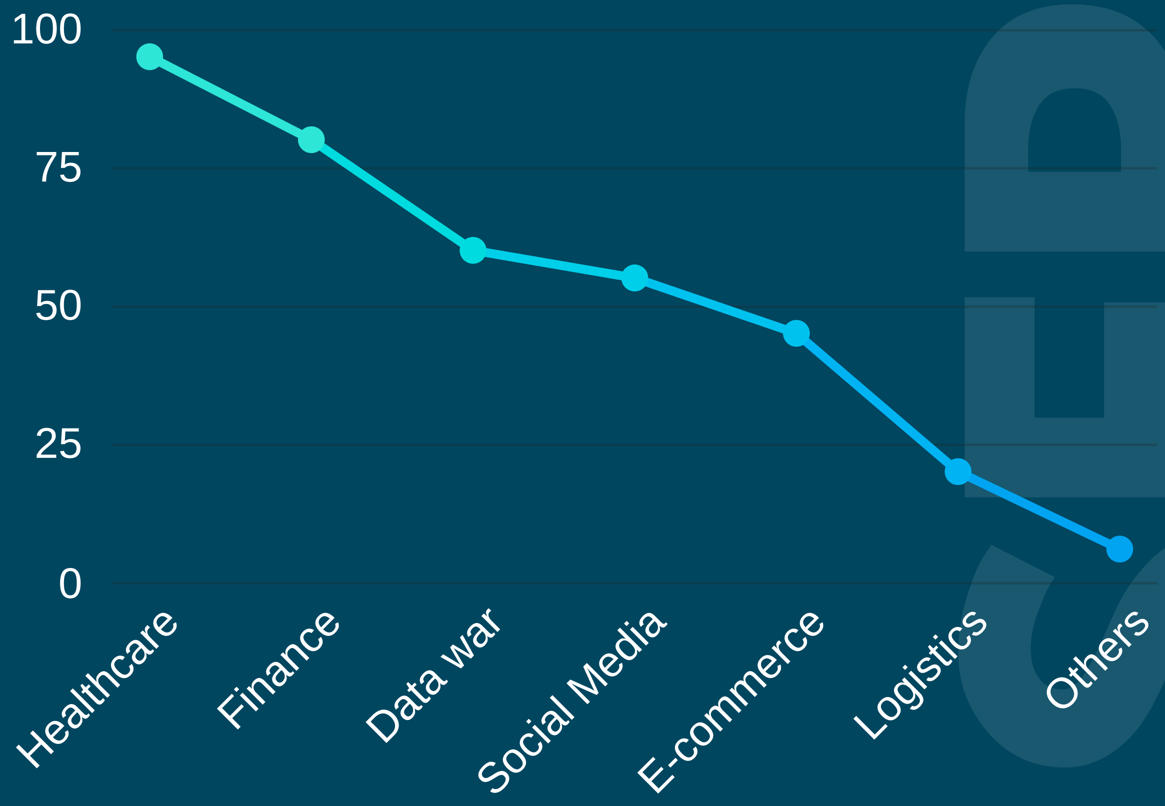
We have established a global society of universal connectivity, where individuals and organizations expect to have instant access to data and services across a variety of interconnected devices, which is creating a rich vein of valuable information, goods and computing resources for our adversaries to extract, extort and exploit. Grotesque ransomware attacks, remote mobile phone hacks and massive consumer data breaches are making it difficult to name a part of our technological framework that isn’t under assault. The number of cyber incidents registered have been increasing drastically and there are several reasons for that. Cyber-criminals take more advantage of our digital lifestyle, advances in technology to create more effective attacks. As mobile, cloud and the Internet of Things (IoT) continue to grow, new disruptive opportunities emerge for cyber-criminals as the attack surface grows.

In spite of improved awareness, The attacks are still targeted at the health sector, energy companies, and public authorities, the functioning of which affects the well-being and people’s lives. Organizations need to enhance their threat intelligence capabilities to stay ahead of cyber threats, not just activate their incident response plans when their network is breached. Organizations must focus on building a data-driven approach fuelled by threat intelligence to better anticipate potential attacks and develop a more proactive security posture for their businesses based on strategic, operational and technical demands

Statistics of Financial loss sep 2018



Statistics of Reputation loss sep 2018



ATTACKS ON HEALTH CARE

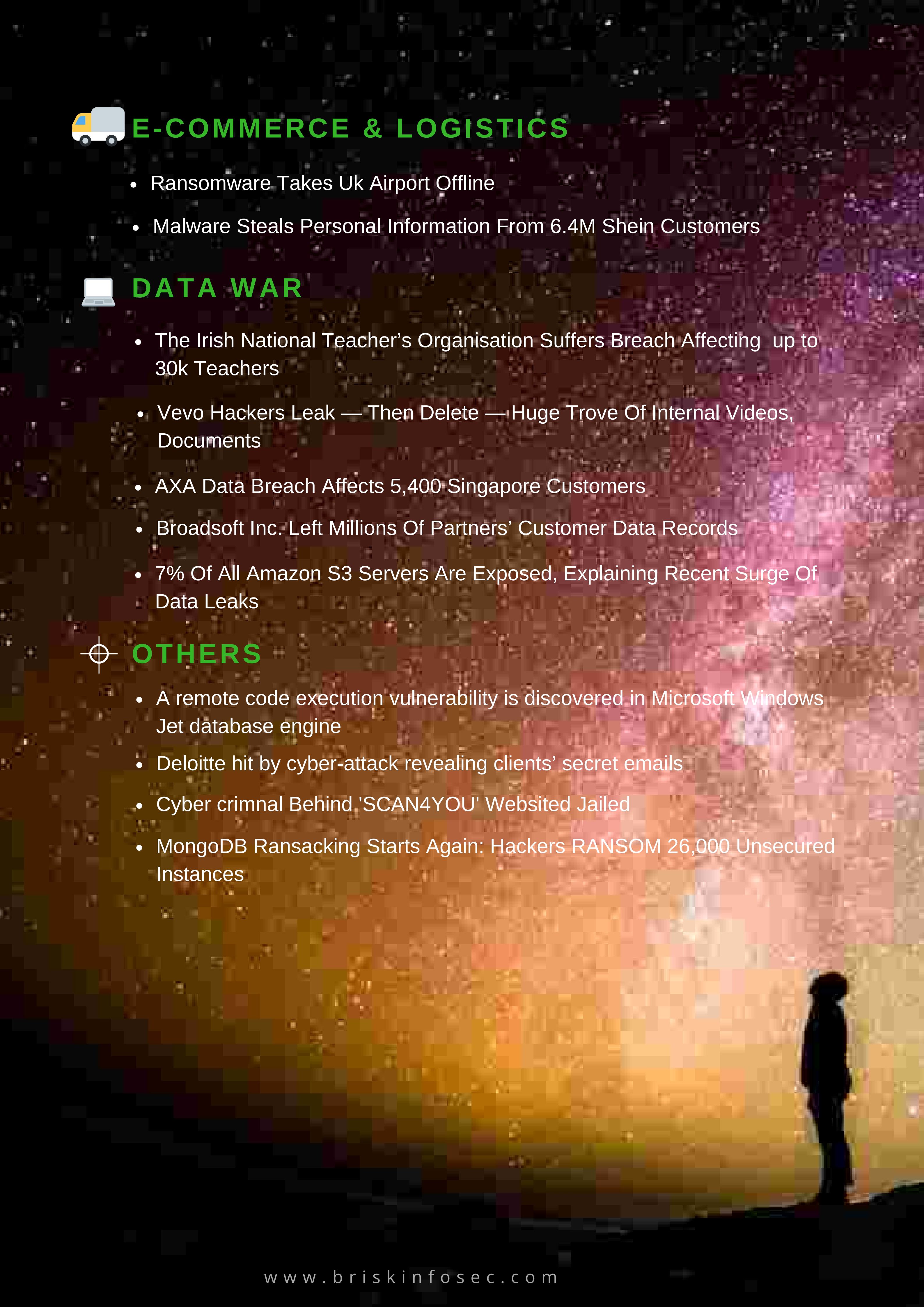
- Employee Error Exposed Data Of 16,000 Blue Cross Patients
- Respiratory Care Provider Victim Of Phishing Attack
- Peace health Employee Accessed Patient Info Unnecessarily
- Morehead Memorial Hospital's Data Breach Affects Patients
- Man Broke Into Docs' Storage Unit, Sold PatientsRecords
- Ransomware Attack Breaches 40,800 Patient Records in Hawaii
- Arkansas Oral & Facial Surgery Center Notifies 128k Patients Of Ransomware Incident
- Aspire Health Suffers Email Breach From Phishing Attack

$ BANKING & FINANCE

- AIB Loses 550 Bank Customers' Confidential Information
- New Android Banking Trojan "RED ALERT 2.0" Targeting 60 Banks
- Breach At Sonic Drive-In May Have Impacted Millions Of Credit, Debit Cards
- MacEwan University Defrauded of Nearly $12M in Phishing Scam
- Dutch Bitcoin Broker Litebit Suffers Second Data Breach In Six Weeks
- Cobalt Threat Group Serves up SpicyOmelette in Fresh Bank Attacks

SOCIAL-NETWORK

- Taringa Hacked: More Than 28 Million User Records Stolen From Popular Social Website
- Users Data Stolen After Attack On Jobs Platform Cpjobs.Com
- Facebook Security Breach Exposes Accounts Of 50 Million Users



E-COMMERCE & LOGISTICS

- Ransomware Takes Uk Airport Offline
- Malware Steals Personal Information From 6.4M Shein Customers

DATA WAR

- The Irish National Teacher’s Organisation Suffers Breach Affecting up to 30k Teachers
- Vevo Hackers Leak — Then Delete — Huge Trove Of Internal Videos, Documents
- AXA Data Breach Affects 5,400 Singapore Customers
- Broadsoft Inc. Left Millions Of Partners’ Customer Data Records
- 7% Of All Amazon S3 Servers Are Exposed, Explaining Recent Surge Of Data Leaks

OTHERS

- A remote code execution vulnerability is discovered in Microsoft Windows Jet database engine
- Deloitte hit by cyber-attack revealing clients’ secret emails
- Cyber crimnal Behind 'SCAN4YOU' Websited Jailed
- MongoDB Ransacking Starts Again: Hackers RANSOM 26,000 Unsecured Instances

HEALTHCARE

RESPIRATORY CARE PROVIDER VICTIM OF PHISHING ATTACK

REPORTED ON
SEP 2018

IMPACT
16K Patients Details exposed

COMPANY NAME
Independence Blue Cross

WEBSITE
www.ibx.com

ATTACK TYPE
Sensitive Data Leakage

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

Philadelphia-based Independence Blue Cross is notifying 16,762 patients - about 1 percent of its members that their data was exposed online for April to July, due to an employee uploading a member file online. They notified on July 19 that member information data was publically accessible between April 23 and July 20. No details were provided on whether the employee intentionally exposed the data, or whether the incident was accidental.The breached information included names, dates of birth, diagnosis codes, provider details and information used for claim processing purposes. While officials said that no Social Security numbers, financial data or credit cards were included in the breach, cyber criminals can use this type of data for medical fraud.

HEALTHCARE

RESPIRATORY CARE PROVIDER VICTIM OF PHISHING ATTACK

REPORTED ON
SEP 2018

IMPACT
Some of Patients Details exposed

COMPANY NAME
Reliable Respiratory

WEBSITE
reliablerespiratory.com

ATTACK TYPE
Phishing Attack

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
ENGLAND

Norwood, MA-based Reliable Respiratory has discovered a hacker has gained access to the email account of its employee and potentially accessed the protected some of the health information of patients. Third party security consultants were called in to investigate the phishing attack and to determine the extent of the breach. The company confirmed that the account had been compromised between June 28 and July 2. The types of information exposed differed per individual but may have included name, medical diagnoses, treatment information, medication/prescription information, medical record number, health insurance information, bank or financial account information, driver's license or state identification number, Social Security number, claims/billing information, date of birth, credit or debit card information, username and password, and passport number. Reliable Respiratory has implemented security controls to prevent phishing and other cyber attacks

HEALTHCARE

PEACEHEALTH EMPLOYEE ACCESSED PATIENT INFO UNNECESSARILY

REPORTED ON
SEP 2018

IMPACT
2000 Patients details Exposed

COMPANY NAME
PeaceHealth Medical Center

WEBSITE
www.peacehealth.org

ATTACK TYPE
Insider Threat

CAUSE OF ISSUE
Security Misconfiguration

TYPE OF LOSS
Reputation

COUNTRY
USA

Nearly 2,000 patients at PeaceHealth Southwest Medical Center are being notified. The Vancouver medical centre discovered on Aug. 9 that the employee unnecessarily accessed the electronic files containing protected health information, including patient names, ages, medical record and account numbers, admission and discharge dates, progress notes and diagnosis. The company said, PeaceHealth officials do not believe any affected patients are at risk for identity theft. Patient Social Security numbers and financial information were not accessed. An investigation revealed the employee accessed patient information between November 2011 and July 2017. The employee no longer works for PeaceHealth. They began sending out letters to the 1,969 affected patients on Monday.

HEALTHCARE

MOREHEAD MEMORIAL HOSPITAL'S DATA BREACH AFFECTS PATIENTS

REPORTED ON
SEP 2018

IMPACT
Some of Patients Data Exposed

COMPANY NAME
Morehead Memorial Hospital

WEBSITE
www.uncrockingham.org

ATTACK TYPE
Phishing Attack

CAUSE OF ISSUE
Lack of Awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

The hospital said personal data may have been obtained through a phishing attack that affected two employee email accounts. Morehead Memorial did not say how many people were affected by the data breach. An investigation into the data breach has found that information about certain patients and employees has been affected, including health insurance payment summaries, treatment overviews, health plan information, and in some cases, Social Security numbers. When the hospital learned of the attack, it cut off access to accounts, reset passwords and hired consultants to conduct an investigation The hospital has also notified the FBI and the U.S. Department of Homeland Security.

HEALTHCARE

MAN BROKE INTO DOCS' STORAGE UNIT,SOLD PATIENTS RECORDS

REPORTED ON
SEP 2018

IMPACT
1000 Medical data records exposed

COMPANY NAME
Broadsoft INC

WEBSITE
www.broadsoft.com

ATTACK TYPE
Identity Theft

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
USA

A borough man allegedly stole more than 1,000 medical records from an East Brunswick storage unit and sold them, according to authorities. Fernando Rios, 33, was charged Tuesday with identity theft, trafficking in personally identifying information and burglary, Middlesex County Prosecutor Andrew C. Carey said in a release. Rios was arrested after a joint investigation with the U.S. Department of Homeland Security, according to the release. It was unclear when the break-in occurred. Three doctors from East Brunswick and Somerset stored their patients' medical records in the storage unit, the release said.

HEALTHCARE

RANSOMWARE ATTACK BREACHES 40,800 PATIENTS RECORDS IN HAWAII

REPORTED ON
SEP 2018

IMPACT
41k Customer data records exposed

COMPANY NAME
Fetal Diagnostic Institute

WEBSITE
www.hawaiifdip.com

ATTACK TYPE
Ransomware Attack

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
USA

The Fetal Diagnostic Institute of the Pacific was hit by a ransomware attack on June 30 that potentially breached the data of 40,800 patients. hackers breached FDIP servers in June, which included some patient records. Officials took immediate action to contain the incident and enlisted a cybersecurity firm. They were able to successfully remove the virus, and confirm no malware remained. The data of both past and current patients were impacted by the breach, including names, dates of birth, addresses, medical data and other types of information. Officials said FDIP doesn’t store the financial data of patients, like credit card numbers. as the overwhelming majority agrees that organizations should not pay hackers the ransom, the right way to restore data is through offline backups.

HEALTHCARE

ARKANSAS ORAL & FACIAL SURGERY CENTER NOTIFIES 128K PATIENTS OF RANSOMWARE INCIDENT

REPORTED ON
SEP 2018

IMPACT
Virus That Locks UP

COMPANY NAME
Arkansas Oral & Facial Surgery Center

WEBSITE
ofscenter.com

ATTACK TYPE
Ransomware Attack

CAUSE OF ISSUE
Targeted That Attack

TYPE OF LOSS
Reputation

COUNTRY
USA

On July 26, 2017, Arkansas Oral & Facial Surgery Center discovered that its computer network had been impacted by ransomware, a type of computer virus that locks up, or encrypts, information and demands that a payment be made in order to unlock, or decrypt, the information. We promptly began an investigation which revealed that the ransomware had been installed on our systems by a unauthorized individual Except for a relatively limited set of patients, our patient information database was not affected by the ransomware, however, imaging files, such as x-rays, and other documents such as attachments were impacted

HEALTHCARE

ASPIRE HEALTH SUFFERS EMAIL BREACH FROM PHISHING ATTACK

REPORTED ON
SEP 2018

IMPACT
Accessed Internal Email System

COMPANY NAME
Aspire Health

WEBSITE
aspirehealthcare.com

ATTACK TYPE
Phishing Attack

CAUSE OF ISSUE
Lack of Awarness

TYPE OF LOSS
Reputation

COUNTRY
USA

The company suffered a phishing attack on Sept. 3 which gained access to Aspires internal email system. The Tennessean article cites information in the court records that indicates the hacker then forwarded 124 emails to an external email account, including emails that contained “confidential and proprietary information and files” and protected health information. “No other information about the contents of the hacked emails have been made public, so it is unclear how many patients have been exposed and what kind of information was leaked According to an email sent to the Tennessean from Cory Brown, a chief compliance officer for Aspire, the company immediately locked the compromised email account after discovering the phishing attack.Brown added that it is unknown if the stolen emails were actually opened by the hacker.

FINANCE

AIB LOSES 550 BANK CUSTOMERS' CONFIDENTIAL INFORMATION

REPORTED ON
SEP 2018

IMPACT
Some of its Users Data Leaked

COMPANY NAME
Allied Irish Bank

WEBSITE
https://aib.ie/

ATTACK TYPE
sensitive Data leakge

CAUSE OF ISSUE
Lack of Awarness

TYPE OF LOSS
Reputation

COUNTRY
Ireland

Allied Irish Banks has issued an “unreserved apology” to hundreds of customers whose private files were lost by a staff member in a significant data breach last month. An AIB staff member “mislaid” a spreadsheet relating to more than 550 AIB customers while travelling between branches in Galway on August 31. The bank has written to those affected and reported the incident to the Office of the Data Commissioner. Printed material containing names and loan and deposit balances, as well as account turnover and annual fees, were among the documents misplaced. A number of “internal bank codes” were also contained in the lost documents. The bank has said that although it is a serious incident, customer accounts cannot be accessed by a third party as a consequence.

FINANCE

NEW ANDROID BANKING TROJAN “RED ALERT 2.0” TARGETING 60 BANKS AND SOCIAL APPS

REPORTED ON
SEP 2018

IMPACT
Unauthorised access purchases

COMPANY NAME
General

WEBSITE
General

ATTACK TYPE
Tool Attack

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
USA

Your Android phone gets infected by Red Alert 2.0 banking malware, hackers start to plunder your account to make unauthorised purchases or money transfers, and your bank can't get hold of you if they suspect something suspicious is occurring. Red Alert 2.0 is said to work on phones running Android version 6.0 (Marshmallow) and earlier. As always, you would be wise to be cautious of what apps you install on your Android device – particularly if they are sourced from unofficial app marketplaces. Whether they are breaking into social media profiles to post spam or raiding online bank accounts to steal money, criminals are dead-set on exploiting innocent people's mobile devices to make money. Do everything you can to reduce the chances of putting your own smartphone at risk by taking care over what apps you install and where you source them from.

FINANCE

BREACH AT SONIC DRIVE-IN MAY HAVE IMPACTED MILLIONS OF CREDIT, DEBIT CARDS

REPORTED ON
SEP 2018

IMPACT
Possible Data Breach in Credit &debit Cards

COMPANY NAME
General

WEBSITE
General

ATTACK TYPE
Ransomware Attack

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
USA

The Oklahoma City-based chain Sonic confirmed a possible data breach involving credit cards. The thing about these data breaches is they're not stopping. We're just going to continue to see them going on into the future," said Kit Letcher with the Better Business Bureau. a security news website reported the possible breach could have led to what they're calling an online "fire sale" involving a long list of stolen credit and debit cards. It's called The Joker Stash and lists millions of cards for sale, many of which had been recently used at Sonic. What's really scary about it is who's going to take advantage of that and how many times over is your credit card information going to be sold," Letcher said. "What we need to do as consumers is really safeguard our information

FINANCE

MACEWAN UNIVERSITY DEFRAUDED OF NEARLY $12M IN PHISHING SCAM

REPORTED ON
SEP 2018

IMPACT
12 Million Bank Transfer

COMPANY NAME
Macewan University

WEBSITE
www.macewan.ca

ATTACK TYPE
Human Error

CAUSE OF ISSUE
Lack of Awareness

TYPE OF LOSS
Reputation

COUNTRY
CANADA

The defrauded of nearly $12 million in a phishing scam compounded by human error. The fraud led university staff members to transfer $11.8 million to a bank account they believed belonged to the vendor, the university said. members were involved in the transfer, there was no process in place which required staff members to phone the vendor to confirm the request to change banking information, but that will change. We are looking at the levels of staffing it must go through for authorization before somebody changes that," he said. "There is going to be a secondary and tertiary level of approval before this goes on."This incident was a result of human error resulting from a phishing attack."Beharry said three separate payments, ranging from $22,000 to $9.9 million, were made to the vendor between Aug. 10 and Aug. 19. The organizations would not have any knowledge that somebody is phishing."

FINANCE

DUTCH BITCOIN BROKER LITEBIT SUFFERS SECOND DATA BREACH IN SIX WEEKS

REPORTED ON
SEP 2018

IMPACT
Personal ands confidential data exposed

COMPANY NAME
General

WEBSITE
General

ATTACK TYPE
Ransomware Attack

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
DUTCH

Thirty-two suspected gang members were charged on suspicion of committing a “high-tech crime,” which involved hacking into credit card terminals in dental and medical offices, and stealing patient identities, the California Department of Justice announced Monday. The gangs, known as the BullyBoys and CoCo Boys, teamed up to steal at least 40 credit card terminals, which he called the “modern cash register.” The terminals which are used to process credit and debit card burglarized and hacked to process $1 million. Becerra said. Some of the debit cards were opened with stolen identities.“But remember here as well, dentists and doctors, it’s not just about money,” Becerra said. “Very personal and confidential information has now been leaked to people about six businesses in Sacramento County were broken. The gangs predominantly operate in the Bay Area and They said he did not know of any BullyBoys or CoCo Boys activity in Sacramento, but it’s not uncommon for gangs to move throughout the state as they expand their criminal activity.

FINANCE

COBALT THREAT GROUP SERVES UP SPICYOMELETTE IN FRESH BANK ATTACKS

REPORTED ON
SEP 2018

IMPACT
Loss of Finacial Creditentials

COMPANY NAME
General

WEBSITE
General

ATTACK TYPE
Ransomware Attack

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
USA

Advanced persistent threat group (APT) the Cobalt Gang, also known as Gold Kingswood, is spreading SpicyOmelette malware in campaigns targeting financial institutions worldwide.it is often financial institutions which bear the brunt. Banking customers hoodwinked by fraudulent schemes or those that become the victims of theft through the loss of their financial credentials will often try to claim back lost funds — of which, banks appear to vary when it comes to compensation. Cobalt has been connected to the theft of millions of dollars from financial institutions worldwide and is believed to have caused over €1bn in damages. Despite the arrest of the APT's suspected leader this year, the group shows no sign of stopping. Arrests of suspected Gold Kingswood operators in March 2018 did not deter the threat group's campaigns, likely due to its vast network of resources," CTU says. "[We] expect Gold Kingswood's operations and toolset to continue to evolve, and financial organizations of all sizes and geographies could be exposed to threats from this group."

SOCIAL NETWORK

TARINGA HACKED: MORE THAN 28 MILLION USER RECORDS STOLEN FROM POPULAR SOCIAL WEBSITE

REPORTED ON
SEP 2018

IMPACT
A Huge Amount of Data Leak

COMPANY NAME
General

WEBSITE
General

ATTACK TYPE
Ransomware Attack

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
USA

A data breach notification service called Leak Base obtained a copy of the database and – upon analysis – found that it contained a total of 28,722,877 records including usernames, hashed credentials and personal email addresses. The Taringa website claimed to have 28,511,984 registered users. Passwords were reportedly encrypted with MD5, an algorithm long-known to be vulnerable to attack. LeakBase, which charges customers fort to check if their details are included in hacked databases, claimed that it had already cracked 26,939,351 (93.79%) of the passwords in the trove.T here were, the service claimed, a total of 15 million unique credentials included in the database. Impacted Taringa users confirmed the records were linked to personal profiles, A notification posted to the Taringa website claimed the incident took place on 1 August 2017, They suffered an external attack that compromised the security of our databases and the code of Taringa." It said there was no evidence that the hackers still had access to servers.

SOCIAL NETWORK

CUSTOMER DATA STOLEN AFTER ATTACK ON JOBS PLATFORM CPJOBS.COM

REPORTED ON
SEP 2018

IMPACT
Users Data &Resumes exposed

COMPANY NAME
CPJOBS

WEBSITE
WWW.CPJOBS.COM

ATTACK TYPE
Security Misconfiguration

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
USA

Online jobs platform cpjobs.com has reported a security breach to police after an “unauthorised third party” stole customer data. South China Morning Post Publishers, which owns the site, said it had shut down affected pages, deactivated users’ passwords and added extra data security measures. There was no evidence to suggest users’ CVs had been compromised. We have shut down the impacted pages, deactivated all users’ passwords, and installed additional layers of data security safeguards,” a cpjobs.com spokesman said. “In addition, we have notified law enforcement and are working closely with them on their investigation.”Site representatives apologised for the incident, stressing privacy was its top priority.“Our teams are re-evaluating every part of our system to ensure maximum security,” the spokesman added. Attempts were made to breach the site’s systems on August 28 and 30, with user data and passwords stolen. Readers of scmp.com are not affected by the breach as it is protected by a separate security system, a spokesman added.

SOCIAL NETWORK

FACEBOOK SECURITY BREACH EXPOSES ACCOUNTS OF 50 MILLION USERS

REPORTED ON
SEP 2018

IMPACT
50 Million Users Data Exposed

COMPANY NAME
Facebook

WEBSITE
www.facebook.com

ATTACK TYPE
Code Injection

CAUSE OF ISSUE
Security Misconfiguration

TYPE OF LOSS
Reputation

COUNTRY
USA

A massive security breach, data of over 50 million Facebook users have been exposed following a security breach by unknown hackers. That a significant number of affected users are from India. However, Facebook did not respond to the question on the number of accounts affected in India, reported PTI. Zuckerberg said' our engineering team found an attack affecting up to 50 million accounts on Facebook. The attackers exploited a vulnerability in the code of the View As feature which is a privacy feature that lets people see what their Facebook profile would look like to another person"."The vulnerability allowed the attackers to steal Facebook access tokens - which are the equivalent of a digital key - which the attackers could have used to take over or access people's accounts," he said. that these tokens were used to access any private messages or posts or to post anything to these accounts." Facebook has invalidated access tokens for the accounts, causing those users to be logged out. Facebook said users don't need to change their passwords.

LOGISTICS

RANSOMWARE TAKES UK AIRPORT OFFLINE

REPORTED ON
SEP 2018

IMPACT
No of Applicants offline

COMPANY NAME
Bristol Airport

WEBSITE
bristolairport.co.uk

ATTACK TYPE
Ransomware Attack

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
USA

An airport spokesman said the information screens were taken offline early on Friday to contain an attack similar to so-called "ransomware".They are now working again at "key locations" including in departures and arrivals, and work is continuing to get the whole site back online. The spokesman said no "ransom" had been paid to get the systems working again. Ransomware is a form of malware in which computer viruses threaten to delete files unless a ransom is paid. Spokesman James Gore said: "We believe there was an online attempt to target part of our administrative systems and that required us to take a number of applications offline as a precautionary measure, including the one that provides our data for flight information screens. That was done to contain the problem and avoid any further impact on more critical systems.

E-COMMERCE

MALWARE STEALS PERSONAL INFORMATION FROM 6.4M SHEIN CUSTOMERS

REPORTED ON
SEP 2018

IMPACT
6.4 Million Users Data Leaked

COMPANY NAME
SheIn

WEBSITE
WWW.SheIn.com

ATTACK TYPE
Targeted Attack

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
USA

The famous online fashion retailer, SheIn.com, has notified its customers of a serious data breach after malicious hackers stole the details of more than 6.4 million people. Shein has noticed that personal information of its customers was stolen during a sophisticated criminal cyber attack on its computer network," the retailer stated on its official website. The note, released on 21 September, indicates that as a result, the retailer said it hired a well-known forensic cybersecurity firm as well as an international law firm to help it investigate the incident further. Shein said that the breach is associated with a cyber attack on its computer network that caused a malware being planted on its servers. Our investigation has confirmed that the perpetrators gained access to email addresses and encrypted password credentials of customers who registered on the company website," Shein said in its official statement, stressing that there is no evidence that credit card information was stolen. "

DATA WAR

30,000 IRISH TEACHERS HIT BY UNION BREACH

REPORTED ON
SEP 2018

IMPACT
users Resumes & Data Exposed

COMPANY NAME
Irish National Teachers Organisation

WEBSITE
Unknown

ATTACK TYPE
security Misconfiguration

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
USA

The Irish National Teachers' Organisation (INTO) warns that personal details of up to 30,000 teachers in Ireland may be at risk because of a breach. Teachers who completed online courses on the INTO's learning website (into learning.ie) in the past few years may be affected The union has announced that the breach occurred last week and allowed hackers to access names, email addresses, city, country, gender and course information. In a limited number of cases, hackers also accessed mobile numbers, school roll number, role in the school, INTO membership number and Teaching Council registration number. The union has confirmed that no payments or passwords were accessed as these are stored separately. The hack has been reported to the Office of the Data Protection Commissioner and An Garda Siochána.

DATA WAR

VEVO HACKERS LEAK — THEN DELETE — HUGE TROVE OF INTERNAL VIDEOS, DOCUMENTS

REPORTED ON
SEP 2018

IMPACT
Internal Data Exposed

COMPANY NAME
Vevo

WEBSITE
www.vevo.com

ATTACK TYPE
Phishing Scam

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
USA

A Notorious hacker group broke into the servers of music-streaming service Vevo, releasing more than 3 terabytes of internal documents and video content online — before removing them later Friday morning at Vevo's request. The purloined cache, posted by hacking and security collective OurMine, included videos, a batch of documents labelled "premieres," as well as marketing info, international social-media documents, and other internal files, as first reported by tech site Gizmodo. Vevo confirmed the hack, which it said was the result of a phishing scam via LinkedIn. "We have addressed the issue and are investigating the extent of exposure," a Vevo rep said in an emailed statement. OurMine, in a post on its site, claimed it leaked the Vevo files late Thursday after an exchange with a Vevo employee who — upon being informed of the hack — allegedly told the hackers, "F— off, you don't have anything. In an update, OurMine said that "We deleted the files because of a request from VEVO.

DATA WAR

AXA DATA BREACH AFFECTS 5,400 SINGAPORE CUSTOMERS

REPORTED ON
SEP 2018

IMPACT
5400 User Information Leaked

COMPANY NAME
AXA Insurance

WEBSITE
www.axe.ie

ATTACK TYPE
security Misconfiguration

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
USA

The personal data of 5,400 customers of AXA Insurance in Singapore has been stolen due to a cyber attack. The life insurance firm sent out an e-mail to most affected customers on Thursday (Sept 7), notifying them of the data breach..In the e-mail, AXA's data protection officer Eric Lelyon said: "We wish to inform you that because of a recent cyber attack, personal data belonging to about 5,400 of our customers, past and present, on our Health Portal was compromised."In particular, their e-mail address, mobile number and date of birth were exposed. The firm said that no other personal data - including name, NRIC number, address, credit card or bank details, health status, claims history or marital status - was leaked.CEO assured customers that the firm's Health Portal "is now secure".No financial or health data was compromised."Mr Drouffe also said that the compromised data, by themselves, will not result in identity theft. Customers are, however, advised to be vigilant against phishing, most commonly via e-mail, to trick victims into disclosing their credentials

DATA WAR

BROADSOFT INC. LEFT MILLIONS OF PARTNERS' CUSTOMER DATA RECORDS EXPOSED

REPORTED ON
SEP 2018

IMPACT
Sensitive information Leaked

COMPANY NAME
Broadsoft INC.

WEBSITE
www.broadsoft.com

ATTACK TYPE
Unknownn

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
USA

The repository contained a massive amount of sensitive information and researchers estimate It would take weeks to fully sort through all of the data. The most potentially damaging discovery was the fact that it contained internal development information such as SQL database dumps code with access credentials, access logs and more. These are all things that should not be publically available online. The two repositories contained thousands and thousands of records and reports for a number of Broadsoft clients with Time Warner Cable (TWC) appearing to be the most prominent and including applications like Phone 2 Go, TWC app, WFF etc. Much of the internal development data apparently saved by Broadsoft. For example "User Profile Dump, 07-07-2017" text file contains more than 4 million records, spanning the time period 11-26-2010 – 07-07-2017, with Transaction ID, usernames, Mac addresses, Serial Numbers, Account Numbers, Service, Category details, and more. Other databases also have billing addresses, phone numbers etc. for hundreds of thousands of TWC customers.

DATA WAR

7% OF ALL AMAZON S3 SERVERS ARE EXPOSED, EXPLAINING RECENT SURGE OF DATA LEAKS

REPORTED ON
SEP 2018

IMPACT
Unrestricted Public Access

COMPANY NAME
Amazon Servers

WEBSITE
General

ATTACK TYPE
Mitm Attack

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
USA

During the past year, there has been a surge in data breach reporting regarding Amazon S3 servers left accessible online, and which were exposing private information from all sorts of companies and their customers. most companies believe that if they're the only ones knowing the database's URL, they are safe. This is not true. Attackers can obtain these URLs using MitM attacks on corporate networks, accidental employee leaks, or by brute-forcing domains for hidden URLs. 7% of all S3 buckets have unrestricted public access According to statistics by security firm Skyhigh Networks, 7% of all S3 buckets have unrestricted public access, and 35% are unencrypted. Amazon S3 ecosystem. These lapses in security best practices have resulted in some serious breaches, from army contractors to big-time US ISPs. Below is a (most likely incomplete) list of all the major data leaks caused by companies leaving Amazon S3 buckets configured with public access during the past few months.

OTHERS

A REMOTE CODE EXECUTION VULNERABILITY IS DISCOVERED IN MICROSOFT WINDOWS JET DATABASE ENGINE

REPORTED ON
SEP 2018

IMPACT
Access to Data Sources

COMPANY NAME
Microsoft

WEBSITE
General

ATTACK TYPE
Remote Code Execution

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
USA

On 20th September 2018, The vulnerability is caused by an out-of-bounds (OOB) write in the JET database engine. Microsoft's OLE DB Provider for JET and Access ODBC only support 32-bit, which means that direct utilization is not available on 64-bit hosts. But on a 64-bit host, the 32: wedit.exe can be used to start the PoC by starting c:\ windows \ SysWOW64 \wscript.exe poc.jsAt the same time, this kind of attack can be triggered by Internet Explorer. Even on 64-bit Windows, the Internet Explorer rendering process is 32-bit. However, on IE11 – Security settings "cross-domain access to data sources" are disabled in the Internet and intranet zones, which can lead to JavaScript errors and unable to trigger the vulnerability. Launching malicious poc.html from a local drive (or USB disk) also triggers the vulnerability. However, the user needs to press "Allow Blocked Content" to trigger

OTHERS

DELOITTE HIT BY CYBER-ATTACK REVEALING CLIENTS' SECRET EMAILS

REPORTED ON
SEP 2018

IMPACT
Email System Breach

COMPANY NAME
Deloitte

WEBSITE
www2.deloitte.com

ATTACK TYPE
Server Access

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
INDIA

One of the world's "big four" accountancy firms has been targeted by a sophisticated hack that compromised the confidential emails. Their clients across all of these sectors had material in the company email system that was breached. The companies include household names as well as US government departments. The hacker compromised the firm's global email server through an "administrator's account" that, in theory, gave them privileged, unrestricted "access to all areas". The account required only a single password and did not have "two-step" verification, sources said. Emails of 244,000 staff were stored in the Azure cloud service, which was provided by Microsoft. This is Microsoft's equivalent to Amazon Web Service and Google's Cloud Platform.the hackers had potential access to usernames, passwords, IP addresses, architectural diagrams for businesses and health information. Some emails had attachments with sensitive security and design details. The breach is believed to have been US-focused and was regarded as so sensitive that only a handful of organization'ss most senior partners and lawyers were informed

OTHERS

CYBER CRIMINAL BEHIND 'SCAN4YOU' WEBSITE JAILED

REPORTED ON
SEP 2018

IMPACT
Malware INfected

COMPANY NAME
Scan4You

WEBSITE
scan4you.net

ATTACK TYPE
Ransomware Attack

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
USA

A Latvian resident was sentenced to 14 years in prison last week for his e-crime service, ‘Scan4you’.Advertised as a legitimate ‘penetration testing’ service, Scan4you was, in fact, a counter antivirus operation. The service enabled cybercriminals to test their malware against antivirus software, especially those used by the US retail sector, but also global government and financial institutions. Operating from 2009 to 2016, Scan4you is believed to have assisted with the theft of over $15 billion. The service was reportedly used by the cybercriminals behind the Citadel malware, responsible for infecting over 11 million computers and attributed with $500 million in fraud losses. Law enforcement worldwide is tackling the enablers of cybercrime. The NCSC operates CHECK, a penetration testing assurance scheme. Pen testers certified through the CHECK scheme are measured against the NCSC’s highest standards, ensuring that customers receive a high-quality service.

OTHERS

MONGODB RANSACKING STARTS AGAIN: HACKERS RANSOM 26,000 UNSECURED INSTANCES

REPORTED ON
SEP 2018

IMPACT
MongoDB Databases Left open

COMPANY NAME
Mongodb Server

WEBSITE
General

ATTACK TYPE
Database Hijacking bAttack

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
USA

Three hacking groups are once again targeting MongoDB databases, hijacking 26,000 open servers and asking for a ransom to release the data. These attackswere simple for hackers to launch: They simply scanned the internet for MongoDB databases left open to external content, wiped the content and replaced data with a ransom demand.Two healthcare organizations were part of these initial attacks.This new wave of attacks occurred over the weekend, and in total 45,000 databases were destroyed. Included among the latest victims was a database containing three years of leukemia patient data, which was used for research to improve treatments.there are about 21,000 unsecured instances of MongoDB, and he estimates that 99 percent were ransacked.Euifax said data on 143 million U.S. customers was obtained in a breach.Personal data including birth dates, credit card numbers

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.ibx.com/pdfs/privacy/ibx-data-security-notice.pdf
- https://www.hipaanswers.com/phishing-attack-on-reliable-respiratory-affects-21000-patients/
- http://www.columbian.com/news/2017/sep/15/peacehealth-employee-accessed-patient-info-unnecessarily/
- https://www.hipaajournal.com/phishing-attack-results-in-the-exposure-of-phi-at-morehead-memorial-hospital-8970/
- https://www.tapinto.net/sections/law-and-justice/articles/east-brunswick-medical-records-and-personal-info
- http://www.hawaiifdip.com/m_breach-rw.html
- https://www.databreaches.net/arkansas-oral-facial-surgery-center-notifies-128000-patients-of-ransomware-incident/
- https://healthitsecurity.com/news/hacker-steals-124-phi-laden-emails-in-aspire-phishing-attack

Finance & Banking

- https://www.breakingnews.ie/ireland/aib-loses-550-customers-confidential-information-805608.html
- https://gbhackers.com/android-banking-trojan/
- https://krebsonsecurity.com/2017/09/breach-at-sonic-drive-in-may-have-impacted-millions-of-credit-debit-cards/
- https://globalnews.ca/news/3710654/macewan-university-loses-nearly-12m-in-phishing-scam/
- https://nulltx.com/dutch-bitcoin-broker-litebit-suffers-from-second-data-breach-in-six-weeks/
- https://www.zdnet.com/article/cobalt-threat-group-serves-up-spicyomelette-in-bank-attacks/

Social Networking

- https://infowatch.com/analytics/leaks_monitoring/6857
- https://www.humanresourcesonline.net/customer-data-stolen-after-attack-on-jobs-platform-cpjobs-com/
- https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html

E-Commerce & Logistics

- https://www.theregister.co.uk/2018/09/17/bristol_airport_cyber_attack/
- https://blog.360totalsecurity.com/en/malware-steals-personal-information-from-6-4m-shein-customers/

Data War

- https://www.infosecurity-magazine.com/news/30000-irish-teachers-hit-by-union/
- https://variety.com/2017/digital/news/vevo-hack-leak-documents-videos-1202560068/
- https://www.straitstimes.com/singapore/axa-data-breach-affects-5400-singapore-customers
- https://www.databreaches.net/broadsoft-inc-left-millions-of-partners-customer-data-records-exposed/
- https://www.bleepingcomputer.com/news/security/7-percent-of-all-amazon-s3-servers-are-exposed-explaining-recent-surge-of-data-leaks/
- https://systemtek.co.uk/2018/10/cyber-criminal-behind-scan4you-website-jailed/
- https://www.zdnet.com/article/mongodb-ransacking-starts-again-hackers-ransom-26000-unsecured-instances/

Others

- https://www.cisecurity.org/advisory/a-vulnerability-in-microsoft-windows-jet-database-engine-could-allow-for-remote-code-execution_2018-105/
- https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails
- https://www.hackread.com/hacker-jailed-running-scan4you-malware-scanning-site/
- https://www.zdnet.com/article/mongodb-ransacking-starts-again-hackers-ransom-26000-unsecured-instances/

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