cyber plural

...focus on cybersecurity

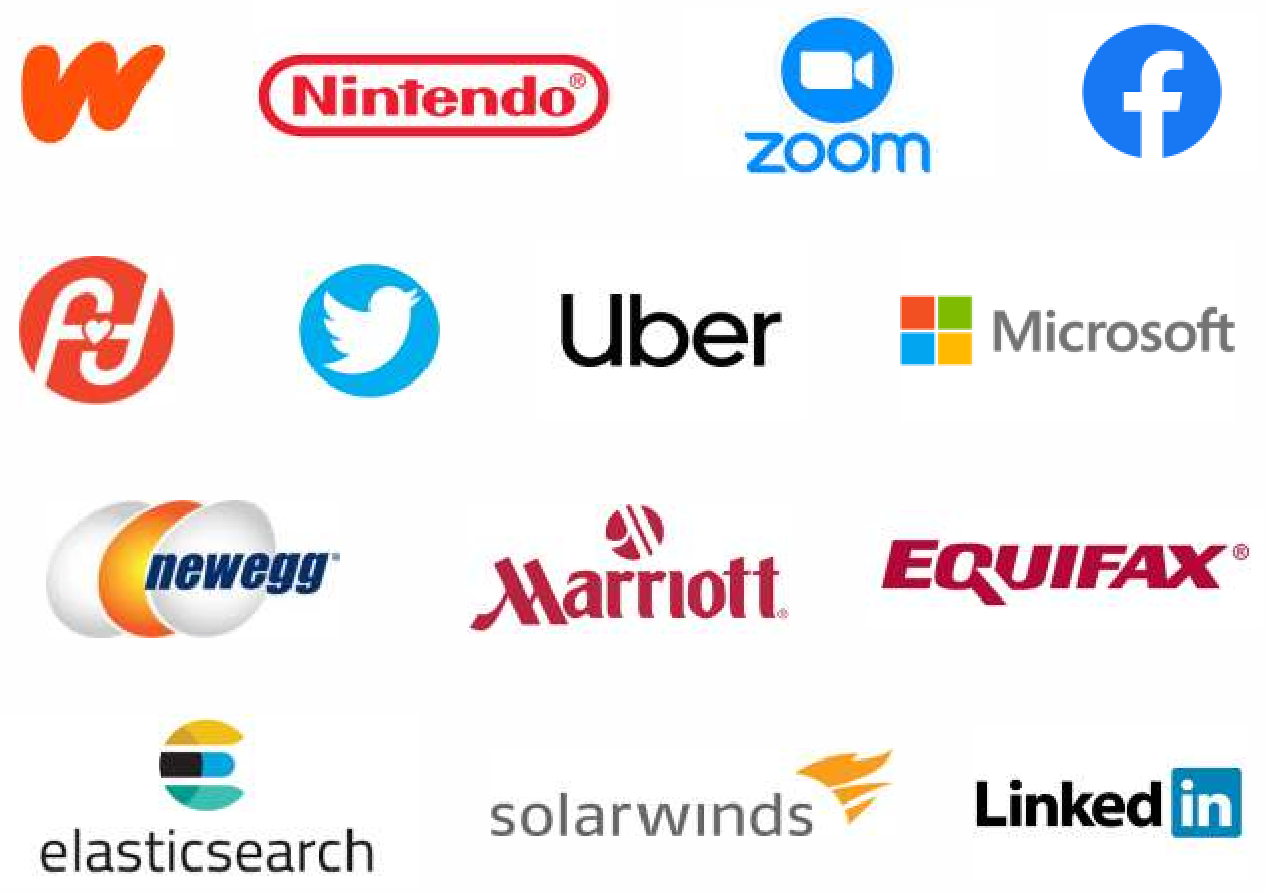
RC:1730380

TOP BREACHES

(2015 - 2021)

A BRIEF REPORT

Some of the Top Breaches of the last 5 years.



Marriot Hotels fines £18.4m for data breach that hit millions

In 2014, an attacker breached systems belonging to Starwood Hotel brands.

After acquisition by Marriott hotels, the attacker's presence persisted but now with access to Marriott Hotel's data.

The attacker gained access to data of 500 million users through the credentials of two employees at a franchise property.

More than 100 million users had their combination of contact information, card numbers and expiry dates stolen.

"Marriot remains committed to the privacy and security of its guests information and continues to make significant investments in security measures for its systems.

2014 - 2018

MITRE | ATT&CK®

IMPACT

Persistence

Exposure of 500m guests data and $18.4m fine

Ashley Madison Breach could expose Privates of 37 Million Cheaters

In 2015, the world's leading extra-marital affair website was hacked, with the attackers gaining access to the PII of 37 million users.

The attackers demanded the site be shut down or else the stolen data will be published.

When attackers breached the site, they performed a dictionary attack on the passwords stored on the database and managed to revealing over 11 million passwords.

The impacts of the attack are still felt today with scammers utilizing the exposed data for extortion.

July 2015

MITRE | ATT&CK®

IMPACT

Credential Access

PII of 37 million users exposed

Anthem to pay nearly $40 million to settle data breach probe by U.S. States

Anthem is a health insurance provider in the U.S. that suffered a major breach in 2015.

Attackers managed to get away with 78.8 million present and past customers

A single user at anthem subsidiary clicked on a phishing link which gave attackers access to the data.

Remarkably, the data was not encrypted and attackers extracted information over a course of weeks a month before the breach was discovered.

February 2015

MITRE | ATT&CK®

IMPACT

Phishing

Exposure of users' PII and multiple fines totalling in almost $260 million

Hacker Selling 1 Billion user accounts stolen from Chinese Internet Giants

The Chinese internet technology company which provides online services centered on content, community, communications, and commerce was hacked in 2015, exposing the data of 234 million users

The entries in the database were leaked in plain text, MD5 was used to hash passwords which made it very easy to crack.

And in 2017, data exfiltrated from the hack was amalgamated with the data compromised from other Chinese internet providers to create a huge list of compromised accounts which was put up for sale on the deep web.

October 2015

MITRE | ATT&CK®

IMPACT

Credential Access

PII of 234 million users exposed

Standard Bank

Standard Bank Computer was hacked in R300 million ATM fraud hit

Standard Bank Group is a financial institution that offers banking and financial services in Africa and abroad.

And in 2016, they suffered a major ATM fraud in japan that resulted in a huge loss.

May 2016

It was reported that about 100 people reportedly used forged Standard Bank credit cards to withdraw ¥1.8 billion (over $17 million) from 1,400 ATMs in Tokyo and other areas in Japan in under three hours.

MITRE | ATT&CK®

IMPACT

Forged credentials

$17 million lost in ATM fraud

Uber

Hacker Selling 1 Billion user accounts stolen from Chinese Internet Giants

In 2016, hackers gained access to personal information of 57 million drivers and riders.

This was only made public in 2018 due to some shady dealings on Uber's part

2016

Two hackers used credentials mistakenly left behind by an Uber engineer to gain access to an Amazon web server owned by Uber.

They then proceeded to download log files, backup files containing the leaked information, and according to one of the hackers "Some backend code".

" Our outside forensics experts have not seen any indication that trip location history, credit card numbers, bank account numbers, Social Security or dates of birth were downloaded."

MITRE | ATT&CK®

IMPACT

Credential Access

PII of 234 million users exposed

dailymotion

DailyMotion Hacked 85 Million User Accounts Stolen

Dailymotion is a video sharing website owned by a french group called Vivendi.

In 2016, they suffered an attack that resulted in 85 million unique usernames and password leaked

October 2016

In October 2016, Dailymotion a video sharing platform exposed more than 85 million user accounts including emails, usernames and bcrypt hashes of passwords

" The hack appears to be limited, and no personal data has been compromised. Your account security is extremely important to us and, to be on the safe side, we are strongly advising all of our partners and users to reset their passwords."

MITRE | ATT&CK

IMPACT

Forged credentials

PII of 85 million users exposed

Adult FriendFinder hit with one of the biggest data breaches ever, report says

The casual hookup and adult content website had 20 years worth of data stolen from across 6 databases.

Attackers gained access to over 137 million credentials, names and addresses.

October 2016

The exploit made use use of a local file inclusion (LFI) vulnerability which allowed the attackers to run code uploaded to separate part of the server.

The stolen data also included 15 million deleted accounts that were not purged from the database.

" Immediately upon learning this information, we took several steps to review the situation and bring in the right external partners to support our investigation"

MITRE | ATT&CK

IMPACT

Execution

412.2 million accounts exposed

Yahoo hack: 1bn accounts compromised by biggest data breach in history

Yahoo!, a well known search engine and internet service company disclosed in December 2016 that they suffered an which leaked the information of over 1 billion users

The database compromise led to the theft of users' passwords in clear text, security questions and answers, payment card data and bank information.

Yahoo! Subsequently required users to change their passwords and security questions before letting them access any of their services but in the end still had to pay a $206.8million GDPR penalty

August 2013 - December 2016

MITRE | ATT&CK®

IMPACT

Forged credentials

$206.8million in GDPR penalty and 1 billion user accounts compromised.

Deep Root Analytics behind data on 198 million US voters: security firm

Deep Root Analytics is a firm that specialises in providing analytics to other companies.

In 2017, they suffered a breach that resulted in 1.1TB of data being exposed and had to pay a $700,000 fine.

The breach data from Deep Root Analytics, a firm working on behalf of the Republican National Committee (RNC) also contains comprehensive voter analysis based on Reddit post activity which could be used to predict how somebody would vote on a particular issue

June 2017

MITRE | ATT&CK®

IMPACT

Forged credentials

200 million US voters PII, $700,000 loss

“WannaCry” ransomware attack losses could reach $4 billion

The WannaCry ransomware attack was a worldwide cyber attack that occurred in 2017.

It resulted in global monetary losses of $4B and lives lost in hospital downtime

WannaCry exploited the Eternal Blue Microsoft windows vulnerability. It spreads quickly on computers that are unpatched of the vulnerability and encrypts the files until a ransom ($300-$600 in bitcoin per affected computer) is paid

The Eternal Blue exploit used a vulnerability present in SMBv1 protocol that allowed attackers to spread malware via specially crafted packets.

May 2017

MITRE | ATT&CK®

IMPACT

Forged credentials

$4 billion and lives lost

EQUIFAX®

Massive Equifax data breach hits 143 million

Equifax, one of the three largest consumer credit reporting agencies in the US had its systems breached.

The sensitive personal data of 148 million Americans was compromised.

The exploited vulnerability was found on July 29th 2019, the system’s inadequate segmentation made lateral movement easy for attackers.

This compromised the personal information of users such as social security numbers, birth dates, addresses, driver numbers and also exposed credit card details.

“ We pride ourselves on being a leader in managing and protecting data, and we are conducting a thorough review of all our overall security operations”

2017

MITRE | ATT&CK®

IMPACT

Lateral movement

PII of 143m users exposed and nearly $700m in compensation

Aadhaar: ‘Leak’ in world’s biggest database worries Indians

Aadhaar is a 12 digit identification number provided by the government of India which can be voluntarily requested by citizens.

It provides information on the holder’s residence and biometrics.

January 2017

In January, it was discovered that attackers were selling a huge database of 1 billion registered users for a price of 500 rupees which converts to about $8

The data breach was the result of a data leak on a system run by a state-owned utility company. The breach allowed access to PII of Aadhaar holders, their bank details and biometric data

MITRE | ATT&CK

IMPACT

Credential Access

PII of 1 billion users exposed

Exactis said to have exposed 340 million records, more tha Equifax breach

Exactis is an analysis firm based in Florida which is similar to Equifax.

And just like their peers they exposed the data of millions of users including phone numbers, home and email addresses.

June 2018

The marketing and data aggregation firm Exactis exposed a database containing nearly 340 million records on a publicly accessible server. The breach exposed PII of millions of US adults and their children.

MITRE | ATT&CK

IMPACT

Credential Access

PII of 340 million users exposed

Hack Brief: 885 Million Sensitive Financial Record Exposed Online

First American is a Finance and real estate giant based in the United states.

In May 2019, a data leak was reported by an independent security journalist.

May 2019

The data leak exposed 885 million users' sensitive records that date back more than 16 years, including bank account records, PII, wire transactions, and other mortgage paperwork.

MITRE | ATT&CK®

IMPACT

Credential Access

PII of 1 billion users exposed

Verifications.io breach: Database with 2 billion records leaked

Verifications.io is an email validation service that offers its services to companies and marketing institutions as well.

The data is said to contain 2 billion records.

February 2019

Verifications.io exposed 763 million unique email addresses in a MongoDB instance that was left publicly facing with no password as well as their PIIs

The database was found by a security researcher and the exact time at which attackers got hold of the data is unknown.

MITRE | ATT&CK®

IMPACT

Exploit Public Facing Application

PII of 2 billion users exposed

Canva criticised after data breach exposed 139m user details

Canva is a high profile technology company in Australia that specializes in providing graphics design services.

On the 25th of May 2019, it suffered a huge breach that compromised 139 million user details.

May 2019

The exposed data included PIIs and passwords stored as bcrypt hashes. The culprit, Gnosticplayers boasted about the incident and also claimed to have gained OAuth login tokens for users who signed in via Google

MITRE | ATT&CK®

IMPACT

Credential Access

PII of 139 million users exposed

SolarWinds hack was ‘largest and most sophisticated attack’ ever: Microsoft president

In early 2020, hackers secretly broke into Texas-based Solarwind's systems and added malicious code into the company's software system.

Cybersecurity experts say that Russia's Foreign Intelligence Service, known as the SVR, is probably responsible for the attack.

2020 - Ongoing

The inserted code created a backdoor to customer's information technology systems, which hackers then used to install even more malware that helped them spy on companies and organizations. These include, Nvidia, Microsoft and select U.S government institutions.

The attack is still being investigated as of April 16th of 2021 with new malicious code still being discovered.

MITRE | ATT&CK®

IMPACT

Execution

Sensitive government data exposed

In 2020, the popularity of online meetings shot up due to ongoing pandemic.

At its peak, ZOOM had 300 million monthly users.

April 2020

Zoom Gets Stuffed: Here’s How Hackers Got Hold of 500,000 Passwords

Attackers referenced multiple leaked databases going all the way back to 2013 to put together a list of user credentials. This is called credential stuffing.

“ We expect to see the total number of Zoom hacked accounts offered in these forums hitting millions”

A breach not of their own fault.

MITRE | ATT&CK

IMPACT

Credential Access

500, 000 credential pairs exposed

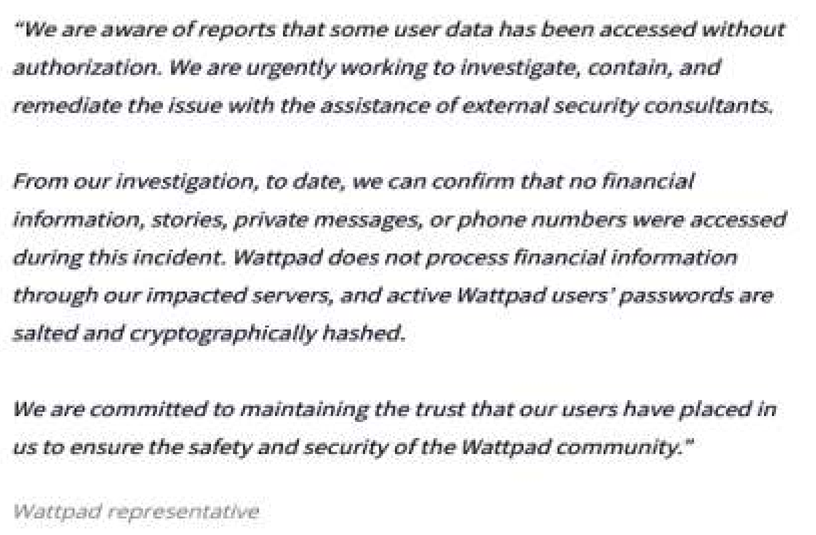
And this is not the first time.

In 2015, Wattpad was also involved in a data breach that leaked an “Unknown” amount of user data.

June 2020

Personal Data and Credentials of 268 Million Users Exposed in Recent Wattpad Hack

Including data belonging to military and government officials!!!



“We are aware of reports that some user data has been accessed without authorization. We are urgently working to investigate, contain, and remediate the issue with the assistance of external security consultants.

From our investigation, to date, we can confirm that no financial information, stories, private messages, or phone numbers were accessed during this incident. Wattpad does not process financial information through our impacted servers, and active Wattpad users’ passwords are salted and cryptographically hashed.

We are committed to maintaining the trust that our users have placed in us to ensure the safety and security of the Wattpad community.”

Wattpad representative

MITRE | ATT&CK

IMPACT

Exploit Public Facing Application

PII of 2 billion users exposed

Major US Twitter accounts hacked in Bitcoin scam

At the height of the pandemic, Twitter suffered a breach that compromised 130 major accounts.

The attackers gained access to these accounts by spear-phishing a Twitter employee.

July 2020

The attackers spear-phished a Twitter employee through a phone call and got access to specific employee systems and gained information on internal processes.

After gaining access, the attackers used 45 accounts to for tweeting a bitcoin scam and read the inboxes of 36.

As our investigation continues, we're sharing an update to answer some of the remaining questions based on what we've discovered to date. We will provide a more detailed technical report on what occured at a later date given the ongoing law enforcement investigation and after we've completed work to further safeguard our service.

MITRE | ATT&CK®

IMPACT

Phishing

$121,000 worth of bitcoin stolen

CAM4 Data Breach: 7 Terabytes of Highly Sensitive User Data Exposed

CAM4 is an adult streaming website owned by a company called Granity Entertainment.

They suffered a data breach that exposed 7TB of highly sensitive user data.

May 2020

CAM4 has had its Elasticsearch server breached exposing over 10 billion records and sensitive information which the hackers can use for prospective phishing attacks.

Apparently, the CAM4 user records contained various PII in different combinations, including names, sexual orientation, emails, IP addresses, email message transcripts, and even private conversations of users.

MITRE | ATT&CK®

IMPACT

Forged credentials

7 Terabytes of user data exposed

MGM resorts is well-known for having a number of hotels in Las Vegas.

And in February 2020 they acknowledged that personal information of about 10.7 million hotel guests was published on a hacking forum.

February 2020

MGM Resorts confirms data breach of 10.7 million guets

Hackers gained access to over 10 million guest records from MGM Grand. The records exposed the contact information of former hotel guests including Justin Bieber, Twitter CEO Jack Dorsey, and government officials.

MITRE | ATT&CK®

IMPACT

Forged credentials

PII of 10.7 million users exposed

Accellion, Inc. is an American technology company specializing in secure file sharing and collaboration, targeted towards businesses.

The company suffered a breach which exposed the data of 1.4 million people.

December 2020

Bug in Accellion's Software Exposes Data of 1.4Mn Washington State Residents

A vulnerability in Accellion's file transfer software was exploited leading to compromise of all their customers using the software. The affected product is a legacy product that the company was planning to retire support.

MITRE | ATT&CK®

IMPACT

Forged credentials

1.4 million PII exposed

Microsoft

250 Million Microsoft Customer Service Record Exposed; Exactly How Bad Was it?

On January 5th 2021, four zero-day vulnerabilities were reported to Microsoft which they confirmed on the 8th.

It is believed that 70,000 U.S. companies had their servers hacked as a result of this.

January 2021

Hackers took advantage of four zero day vulnerabilities which allowed them to compromise the server's Outlook Web Access by logging in as a normal user to then perform a privilege escalation.

According to a blog post by Microsoft, the attack was perpetrated by a Chinese group called HAFNIUM.

The blog post also showed how the attackers would potentially get credentials by dumping the server's authentication service memory.

MITRE | ATT&CK®

IMPACT

Privilege escalation

Sensitive government data exposed

MOLSON COORS beverage company

One of America's biggest beer makers had to stop making beer due to cyber security breach

Molson Coors is a multinational drink and brewing company headquartered in Chicago in the United States.

In 2021 they suffered a huge ransomware attack that resulted in them needing to shut down their operation

March 2021

The ransomware attack took control of the systems controlling about 20 of their brewery facilities.

The ransomware could end up costing the company up to $140 million.

MITRE | ATT&CK®

IMPACT

Forged credentials

$140 million lost

533 million Facebook users' phone numbers and personal data have been leaked online

This is also not the first time the social media giant was involved in a data breach.

In 2018, 50 million users had their details leaked.

The first breach (2018) occurred due to a loophole in Facebook's authentication system which used an access token with no expiry date.

The most recent breach occurred due to a flaw in the Instagram contact importer which exposed names, phone numbers, Instagram handles, and account ID numbers.

"We have changed the contact importer on Instagram to help prevent potential abuse. We are grateful to the researcher who raised this issue.

April 2021

MITRE | ATT&CK®

IMPACT

Discovery

533 million accounts exposed

One of America's biggest beer makers had to stop making beer due to cyber security breach

Molson Coors is a multinational drink and brewing company headquartered in Chicago in the United States.

In 2021 they suffered a huge ransomware attack that resulted in them needing to shut down their operation

The ransomware attack took control of the systems controlling about 20 of their brewery facilities.

The ransomware could end up costing the company up to $140 million.

March 2021

MITRE | ATT&CK®

IMPACT

Forged credentials

$140 million lost

Hackers scrapped data from 500 million LinkedIn Users

LinkedIn has 740 million users, according to its website , so the reported data scraping of 500 million users means about two-thirds of the platform's user base could be affected.

The data includes account IDs, full names, email addresses, phone numbers, workplace information, genders, and links to other social media accounts.

“While we're still investigating this issue, the posted dataset appears to include publicly viewable information that was scraped from LinkedIn combined with data aggregated from other websites or companies," - LinkedIn spokesperson. "Scraping our members' data from LinkedIn violates our terms of service and we are constantly working to protect our members and their data."

April 2021

MITRE | ATT&CK®

IMPACT

Discovery

500 million PII scraped

Apple supplier Quanta Computer from Taiwan hit by ransomware attack

Quanta, one of Apple’s major suppliers, said on Wednesday that it had been hit by a cyber attack and was trying to “recover data” after one of the world’s most notorious hacking gangs said it was attempting to extort both companies.

The admission came after REvil, one of the most prolific criminal ransomware hacking groups, said on its dark web site that it had compromised Quanta and was now extorting Apple.

“Our team is negotiating the sale of large quantities of confidential drawings and gigabytes of personal data with several major brands,” the REvil post added.

April 2021

MITRE | ATT&CK®

IMPACT

Discovery

533 million accounts exposed

Some of the most relevant breaches back home

Arik Air grounded by an Amazon S3 leak

Arik air is a west-african airline company based in Nigeria.

In October 2018, and independent security researcher found an unsecure Amazon S3 bucket containing data that belonged to them.

The researcher discovered the data when running a routine check for exposed and unsecure Amazon s3 buckets. The data was a bunch of CSV files that contained credit cards, customer names, email addresses and other valuable PII.

After finding this, they reported it to Arik air but it took them an entire month to secure the data.

October 2018

MITRE | ATT&CK®

IMPACT

Exploit Public Facing Application

PII of 80000 users exposed

Nigeria’s SureBet247 has suffered a potential security breach

Molson Coors is a multinational drink and brewing company headquartered in Chicago in the United States.

In 2021 they suffered a huge ransomware attack that resulted in them needing to shut down their operation

The data was sent to Trevor Hunt, haveibeenpwned’s founder, by an anonymous source who stated that they wanted the incident to come to light after they’d tried to make contect with surebet support with no success.

The data was extensive spanning over 32GB of backups across 6 databases of various online betting assets.

December 2019

MITRE | ATT&CK®

IMPACT

Discovery

PII of over 300 thousand users exposed

Fraudster Steals $64,822 from Unity Bank’s ATMs

Bank Security, a Twitter handle focused on bank security threats, reported that the database of Unity Bank, a Nigerian commercial bank, was being shared online on hacker forums.

The attacker claimed to have access to the entire database and that the initial leak was a small dump with “more coming soon”.

A close check of the SQL script and data posted online, contained 53K recruitment data from a possible past enrollment exercise.
Bank later issued a statement assuring customers of protection of PII as mandated by data protection regulation but did not explicitly deny the breach or associated data.

Also in 2017 hackers were able to compromise Unity bank and made away with $64,822.97 (about N23.3million allegedly perpetrated by hacking several Unity Bank accounts with an Automated Teller Machine (ATM) card.

August 2020

MITRE | ATT&CK®

IMPACT

Exploit Public Facing Application

PII of 53 thousand users exposed and N23.3 million lost

Hackers gain access into JAMB's site, diver over N10m

The Joint Admissions and Matriculation Board in April disclosed that they lost a total of N10 million as a result of an attack.

JAMB alleged that hackers who have been apprehended, ploughed into the JAMB website and changed the account details and phone numbers of their staffs diverting several millions meant for the payment of their allowances.

April 2021

MITRE | ATT&CK®

IMPACT

Stolen Application Credentials

N10 million lost

RC:1730380

CyberPlural Limited was founded to help small- and large-scale businesses pay attention to cybersecurity. With the current rise in cyber-attacks and its devastating effect on businesses.

Our approach to cybersecurity is not a one-size-fit-all but a multi-faceted approach taking into consideration the people, processes and technology implemented to suit all our customers' situation and environment.

CyberPlural Limited solutions are tailored to our client's specific needs. We identify your challenges quickly and design impactful strategies to address them. Our strategies and approaches are tightly structured aim to provide the overall security required for business continuity.

Visit our website to learn more.

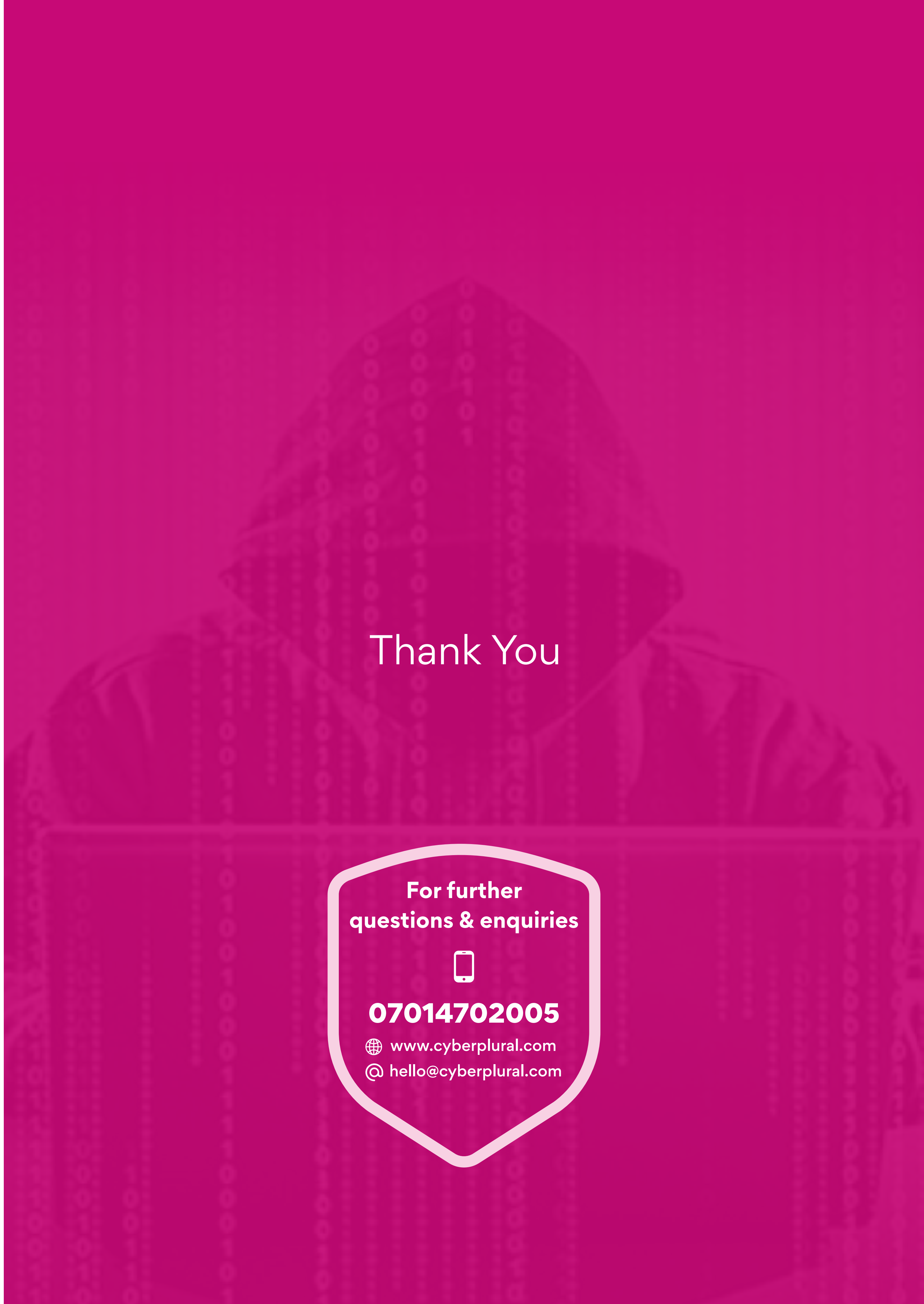
www.cyberplural.com

Follow us:

cyberplural

Top Breaches from 2015-2021

Compiled by Mainasara Tsowa, Chioma Andeh, and Muktar Suleiman



Thank You

For further questions & enquiries

☎

07014702005

www.cyberplural.com

@ hello@cyberplural.com