Stone Forest

SGSECURE@WORKPLACE WEBINAR:

Cybersecurity – Adapting Business to the New Normal

Hoi Wai Khin, Stone Forest | CISSP, CISM, CDPSE, CRISC, CBCP, PSCMC, FCMI, ISO 27001 LA

31 August 2021

Disclaimer

While utmost care has been taken to ensure content accuracy at the time of writing, no person should rely on the contents in this presentation without first obtaining advice from a qualified professional. These presentation slides are issued on the terms and understanding that (1) the author is not responsible for the results of any actions taken on the basis of information in these slides, nor for any error in or omission from these slides; and (2) the author expressly disclaims all and any liability and responsibility to any person, whether a reader of these slides or not, in respect of anything, and of the consequences of anything, done, or omitted to be done by any such person in reliance, whether wholly or partially, upon the whole or any part of the contents of these slides. Information contained herein is proprietary to Stone Forest and no part should be reproduced without prior permission and due acknowledgement.

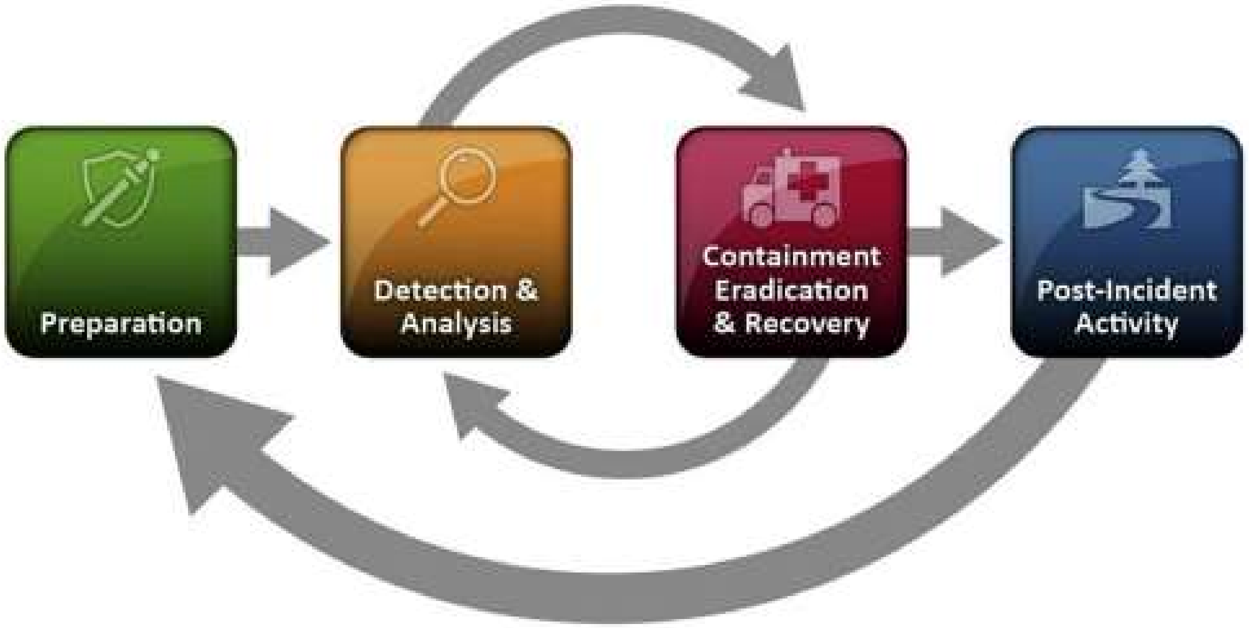
This presentation is for general purposes only and may not be accurate, suitable for, or applicable in your specific circumstances. You are advised to obtain your own independent advice.

Cyber Incident Case Study – The Background

A client contracted us to perform a **forensic investigation into a cyber security breach.**

WHAT WE DID:
Conducted an analysis on the security incident following the **NIST Incident Response framework**.

OBJECTIVE:
This analysis aims to perform a triage on the incident so that a strategy can be provided on the next step for the client.



Source https://www.nist.gov/cyberframework

Incident #1 – Hela Ransomware

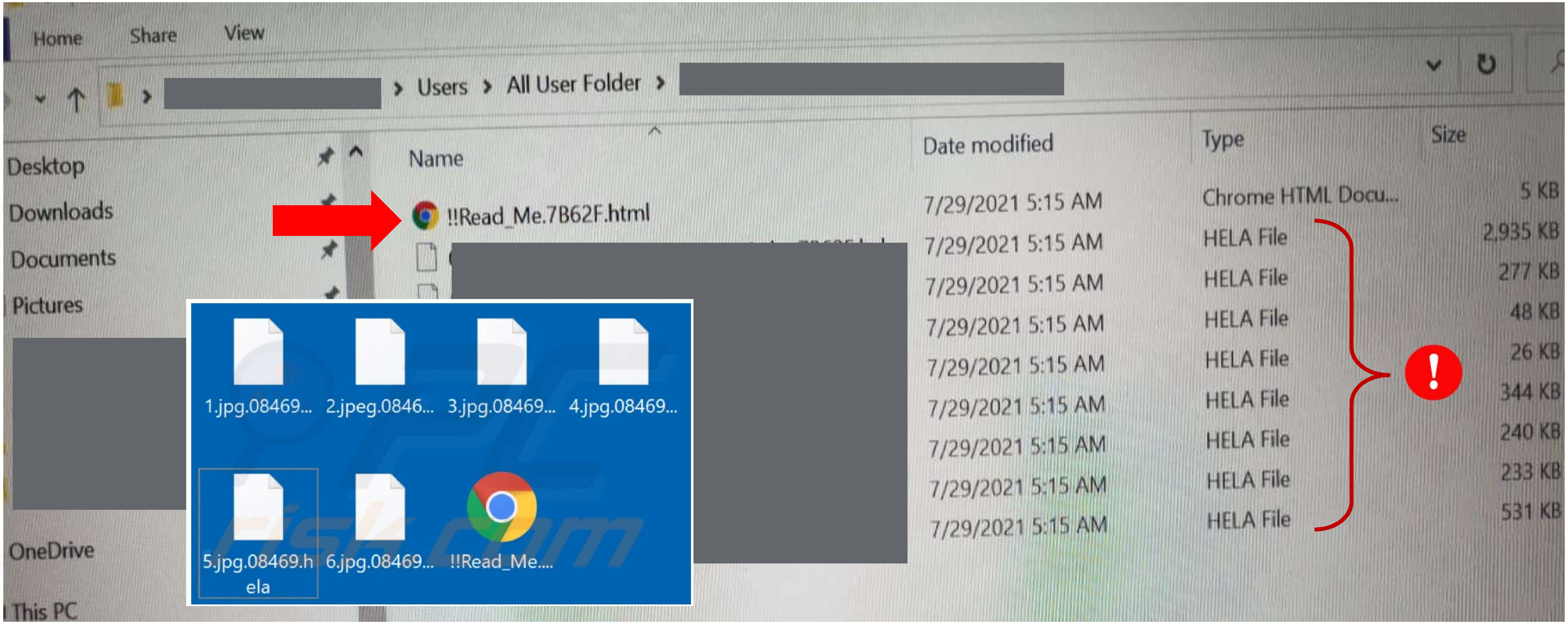
WHO: **A listed company**

WHEN: 28 July 2021

WHAT HAPPENED:

- Users reported that they cannot login and access to the company network
- IT team checked and discovered that they was a large number of the files in the domain controller and network drive with an **‘.hela’ extension**
- Their domain controller is located on premise
- IT team later discovered that their backup drive on the same domain controller was also affected
- There was a **“!!Read_me.7B62F.html”** file

Incident #1 – Hela Ransomware Analysis



[redacted] > Users > All User Folder > [redacted]

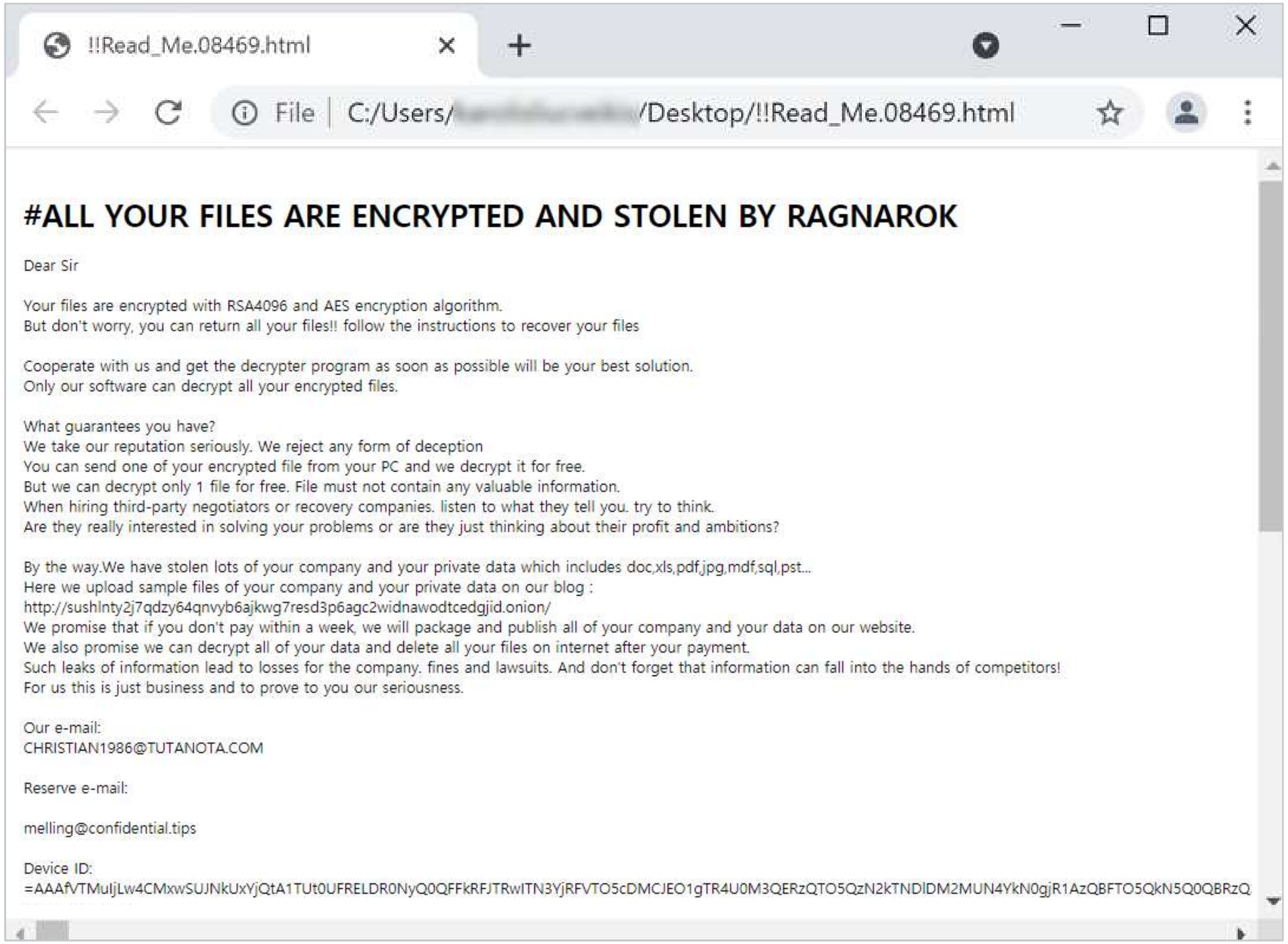
Name	Date modified	Type	Size
!!Read_Me.7B62F.html	7/29/2021 5:15 AM	Chrome HTML Docu...	5 KB
[redacted]	7/29/2021 5:15 AM	HELA File	2,935 KB
[redacted]	7/29/2021 5:15 AM	HELA File	277 KB
[redacted]	7/29/2021 5:15 AM	HELA File	48 KB
[redacted]	7/29/2021 5:15 AM	HELA File	26 KB
[redacted]	7/29/2021 5:15 AM	HELA File	344 KB
[redacted]	7/29/2021 5:15 AM	HELA File	240 KB
[redacted]	7/29/2021 5:15 AM	HELA File	233 KB
[redacted]	7/29/2021 5:15 AM	HELA File	531 KB

1.jpg.08469... 2.jpeg.0846... 3.jpg.08469... 4.jpg.08469...

5.jpg.08469.hela 6.jpg.08469... !!Read_Me....

Incident #1 – Hela Ransomware Analysis

IT clicked on the Read_me file and the message is as follows



#ALL YOUR FILES ARE ENCRYPTED AND STOLEN BY RAGNAROK

Dear Sir

Your files are encrypted with RSA4096 and AES encryption algorithm.
But don't worry, you can return all your files!! follow the instructions to recover your files

Cooperate with us and get the decrypter program as soon as possible will be your best solution.
Only our software can decrypt all your encrypted files.

What guarantees you have?
We take our reputation seriously. We reject any form of deception
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain any valuable information.
When hiring third-party negotiators or recovery companies. listen to what they tell you. try to think.
Are they really interested in solving your problems or are they just thinking about their profit and ambitions?

By the way.We have stolen lots of your company and your private data which includes doc,xls,pdf,jpg,mdf,sql,pst...
Here we upload sample files of your company and your private data on our blog :
http://sushlnty2j7qdzy64qnvyb6ajkwg7resd3p6agc2widnawodtcedgjid.onion/
We promise that if you don't pay within a week, we will package and publish all of your company and your data on our website.
We also promise we can decrypt all of your data and delete all your files on internet after your payment.
Such leaks of information lead to losses for the company. fines and lawsuits. And don't forget that information can fall into the hands of competitors!
For us this is just business and to prove to you our seriousness.

Our e-mail:
CHRISTIAN1986@TUTANOTA.COM

Reserve e-mail:

melling@confidential.tips

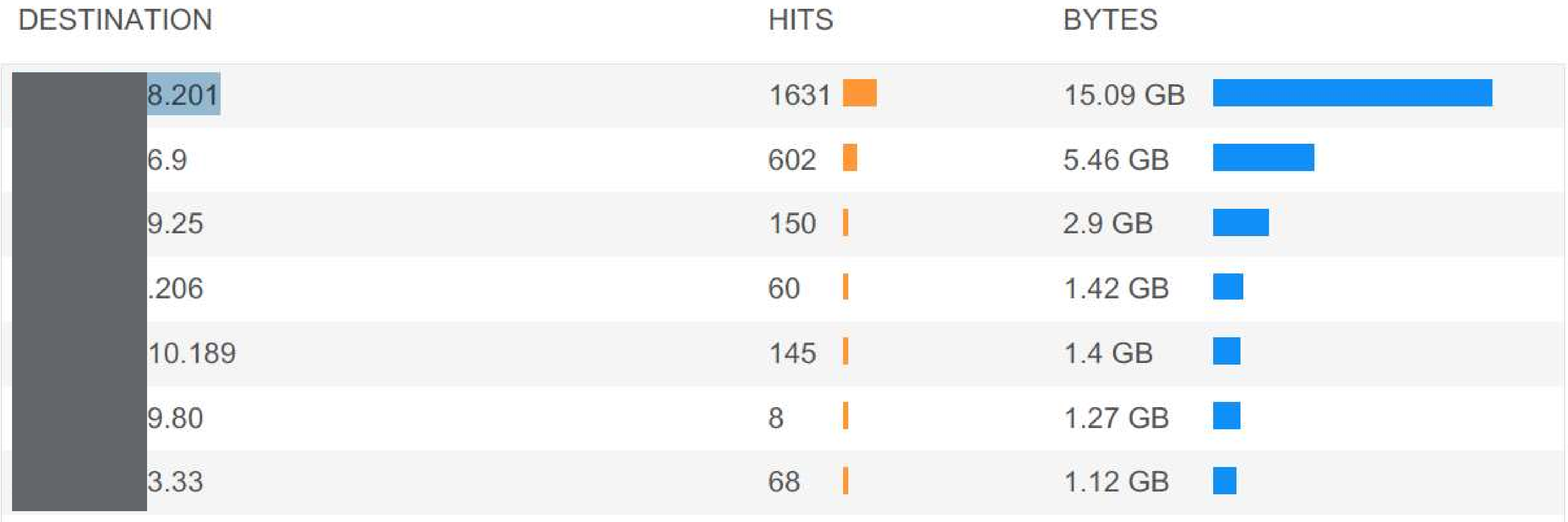
Device ID:
=AAAfVTMuIjLw4CMxwSUJNkUxYjQtA1TUt0UFRELDR0NyQ0QFFkRFJTRwITN3YjRFVTO5cDMCJEO1gTR4U0M3QERzQTO5QzN2kTNDlDM2MUN4YkN0gjR1AzQBFTO5QkN5Q0QBRzQ

Stone Forest

What to do next?

Firewall Analysis

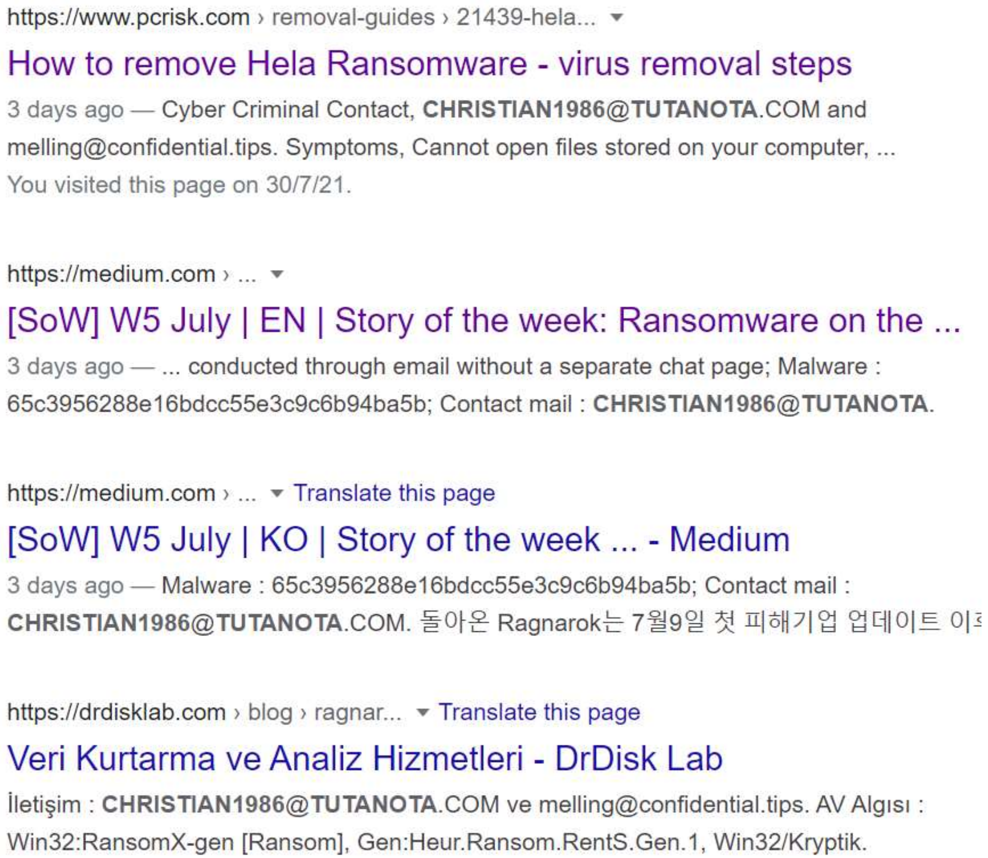
We advised the IT team to check the firewall logs to determine if any data was copied out of the network. If personal data is involved, the company will need to inform PDPC.



DESTINATION	HITS	BYTES
[redacted]8.201	1631	15.09 GB
[redacted]6.9	602	5.46 GB
[redacted]9.25	150	2.9 GB
[redacted].206	60	1.42 GB
[redacted]10.189	145	1.4 GB
[redacted]9.80	8	1.27 GB
[redacted]3.33	68	1.12 GB

Internet Research

We did a web research on the email address in the Read-me message



https://www.pcrisk.com › removal-guides › 21439-hela... ▾

How to remove Hela Ransomware - virus removal steps

3 days ago — Cyber Criminal Contact, **CHRISTIAN1986@TUTANOTA**.COM and melling@confidential.tips. Symptoms, Cannot open files stored on your computer, ...

You visited this page on 30/7/21.

https://medium.com › ... ▾

[SoW] W5 July | EN | Story of the week: Ransomware on the ...

3 days ago — ... conducted through email without a separate chat page; Malware : 65c3956288e16bdcc55e3c9c6b94ba5b; Contact mail : **CHRISTIAN1986@TUTANOTA**.

https://medium.com › ... ▾ Translate this page

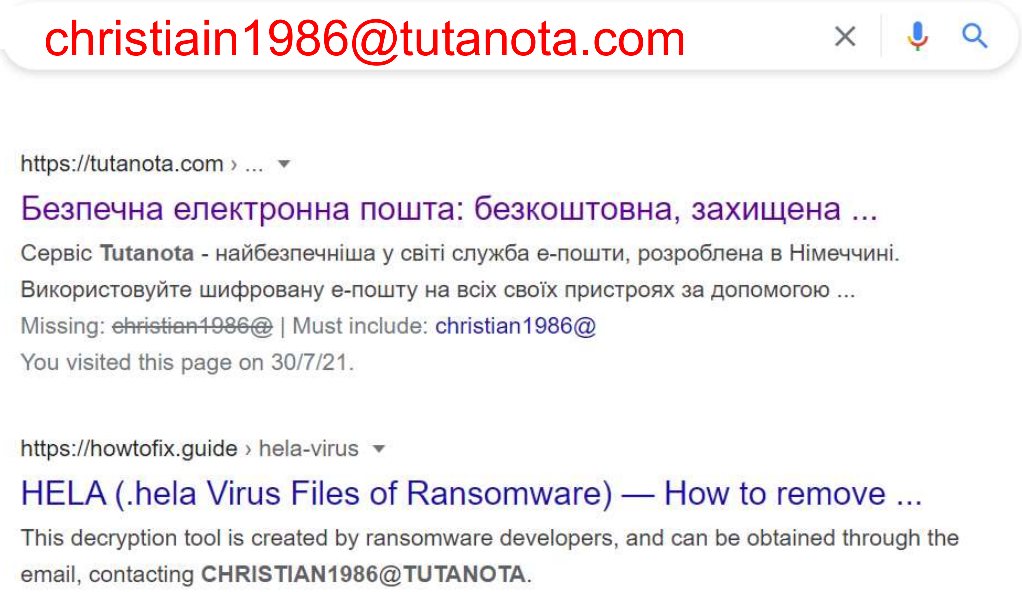
[SoW] W5 July | KO | Story of the week ... - Medium

3 days ago — Malware : 65c3956288e16bdcc55e3c9c6b94ba5b; Contact mail : **CHRISTIAN1986@TUTANOTA**.COM. 돌아온 Ragnarok는 7월9일 첫 피해기업 업데이트 이

https://drdisklab.com › blog › ragnar... ▾ Translate this page

Veri Kurtarma ve Analiz Hizmetleri - DrDisk Lab

İletişim : **CHRISTIAN1986@TUTANOTA**.COM ve melling@confidential.tips. AV Algısı : Win32:RansomX-gen [Ransom], Gen:Heur.Ransom.RentS.Gen.1, Win32/Kryptik.



christiain1986@tutanota.com

https://tutanota.com › ... ▾

Безпечна електронна пошта: безкоштовна, захищена ...

Сервіс **Tutanota** - найбезпечніша у світі служба е-пошти, розроблена в Німеччині. Використовуйте шифровану е-пошту на всіх своїх пристроях за допомогою ...

Missing: ~~christian1986@~~ | Must include: christian1986@

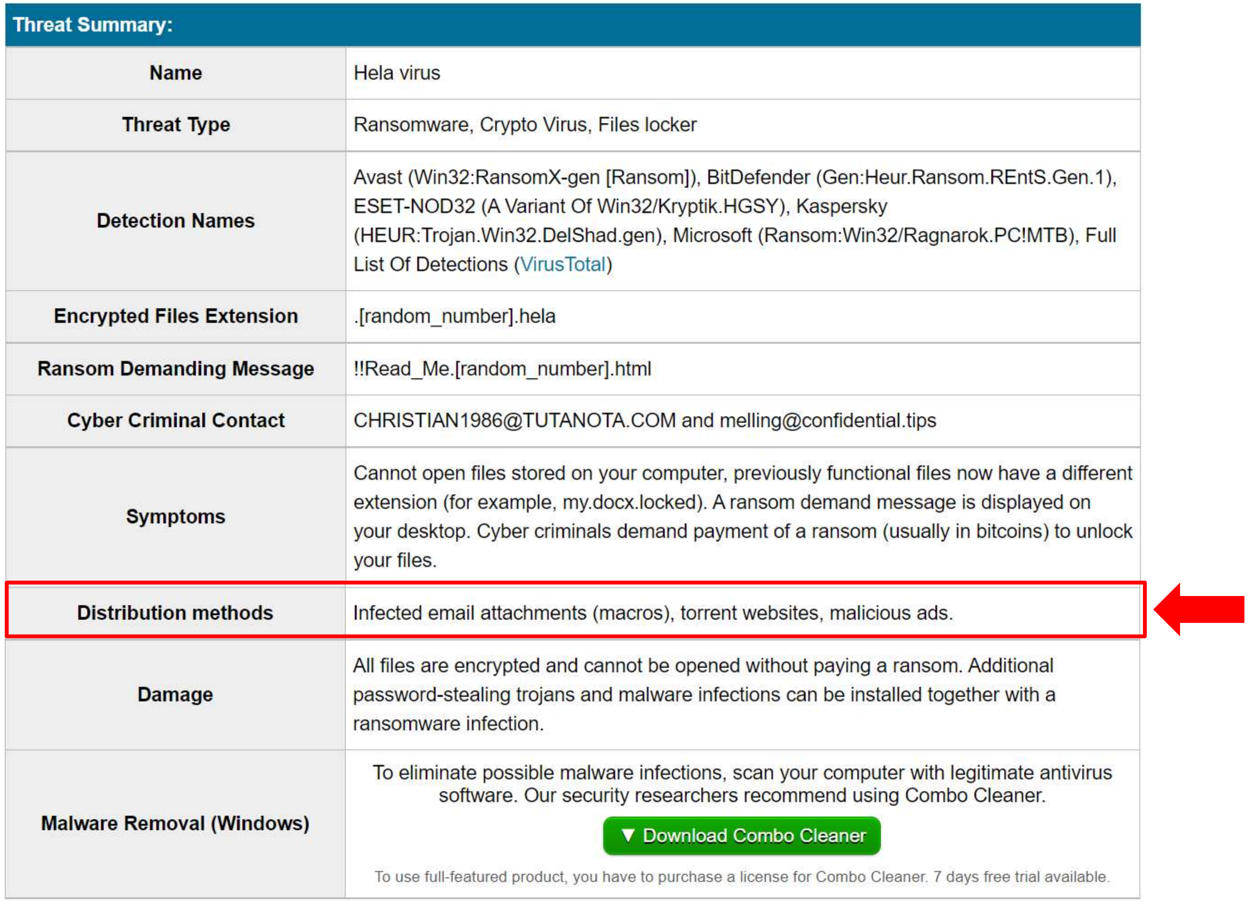
You visited this page on 30/7/21.

https://howtofix.guide › hela-virus ▾

HELA (.hela Virus Files of Ransomware) — How to remove ...

This decryption tool is created by ransomware developers, and can be obtained through the email, contacting **CHRISTIAN1986@TUTANOTA**.

Internet Research



Threat Summary:	
Name	Hela virus
Threat Type	Ransomware, Crypto Virus, Files locker
Detection Names	Avast (Win32:RansomX-gen [Ransom]), BitDefender (Gen:Heur.Ransom.REntS.Gen.1), ESET-NOD32 (A Variant Of Win32/Kryptik.HGSY), Kaspersky (HEUR:Trojan.Win32.DelShad.gen), Microsoft (Ransom:Win32/Ragnarok.PC!MTB), Full List Of Detections (VirusTotal)
Encrypted Files Extension	.[random_number].hela
Ransom Demanding Message	!!Read_Me.[random_number].html
Cyber Criminal Contact	CHRISTIAN1986@TUTANOTA.COM and melling@confidential.tips
Symptoms	Cannot open files stored on your computer, previously functional files now have a different extension (for example, my.docx.locked). A ransom demand message is displayed on your desktop. Cyber criminals demand payment of a ransom (usually in bitcoins) to unlock your files.
Distribution methods	Infected email attachments (macros), torrent websites, malicious ads.
Damage	All files are encrypted and cannot be opened without paying a ransom. Additional password-stealing trojans and malware infections can be installed together with a ransomware infection.
Malware Removal (Windows)	To eliminate possible malware infections, scan your computer with legitimate antivirus software. Our security researchers recommend using Combo Cleaner. ▼ Download Combo Cleaner To use full-featured product, you have to purchase a license for Combo Cleaner. 7 days free trial available.

https://medium.com/s2wlab/sow-w5-july-en-story-of-the-week-ransomware-on-the-darkweb-d142ea4a3fe2

Stone Forest

Next Action Steps

Notification to relevant authorities on the cyber incident

- IT team reported the case to the Singapore Police Force (“SPF”) and Cyber Security Agency (“CSA”)
- The SPF proposed a list of decryptor tools to decrypt the files but it did not work
- The CSA informed the company that they will revert back again in a few days

Backup and recovery process

- We advised their IT team to perform a cloud backup of their SaaS HR and Finance data
- Their file server contained a lot of operational data which included Contracts, Projects files, Marketing data, etc.

Next Action Steps

- IT updated the Board and Management that a lot of the files in the file server were encrypted with an '.hela' extension.
- These files consisted of the day-to-day internal business operations, HR details and customers personal details.

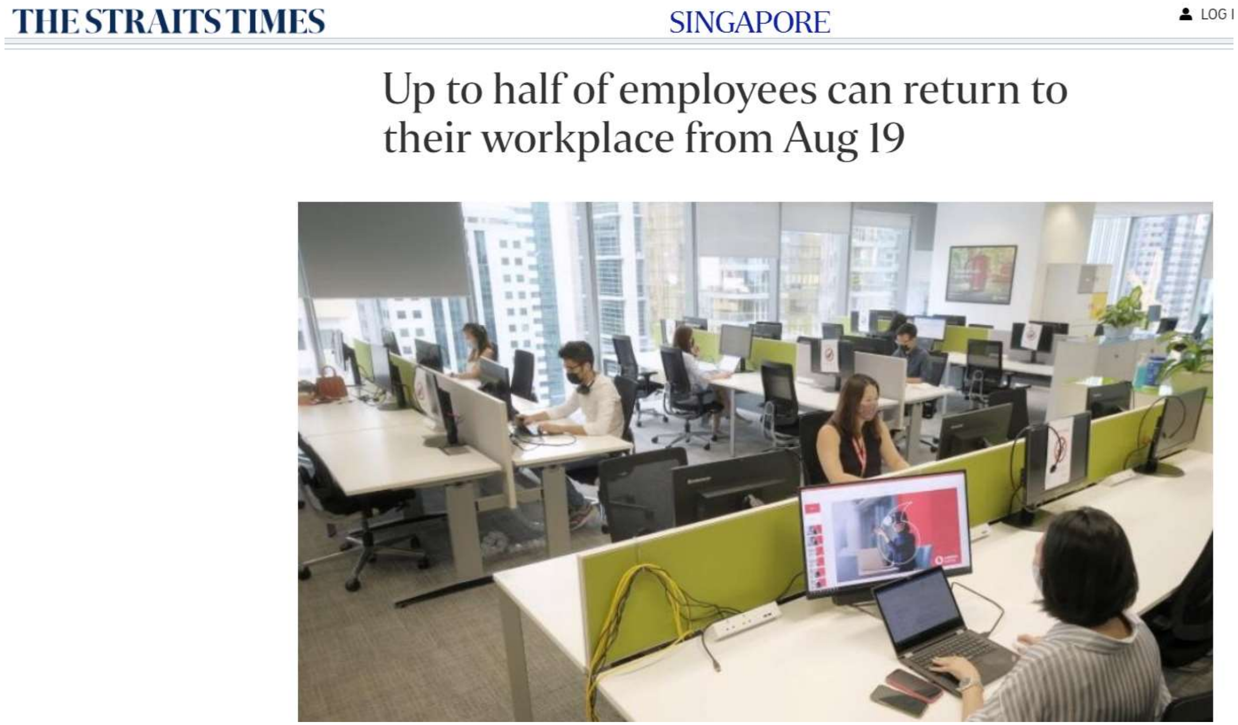
What will be your next course of action?

The Story Continues

- IT tried to perform data restoration from their backup
- But discover that their backup had been also encrypted
- They did not receive any follow up email from the attackers demanding ransom
- STORY ENDING - **Company data is encrypted forever!**

Hot News

What is the biggest news on the internet NOW?

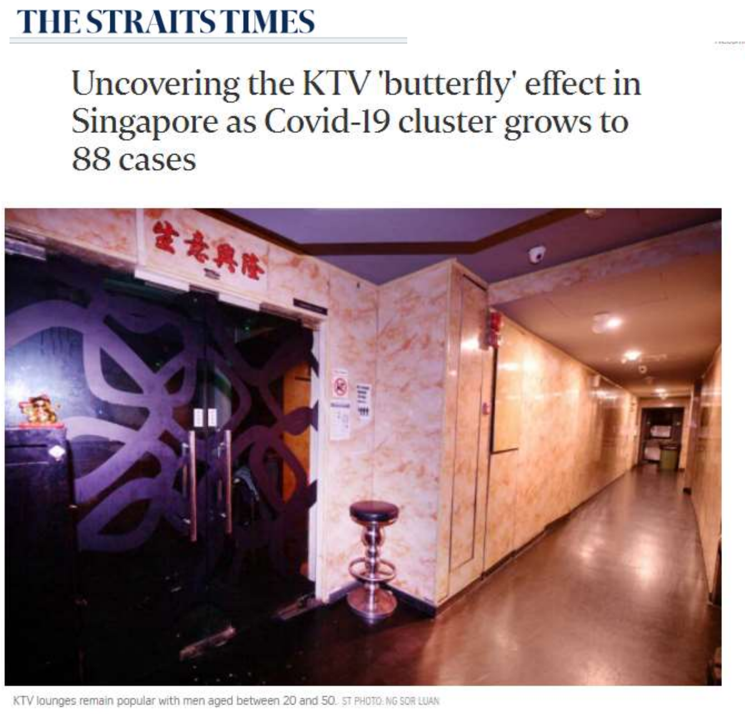


THE STRAITS TIMES SINGAPORE

Up to half of employees can return to their workplace from Aug 19

Hot News

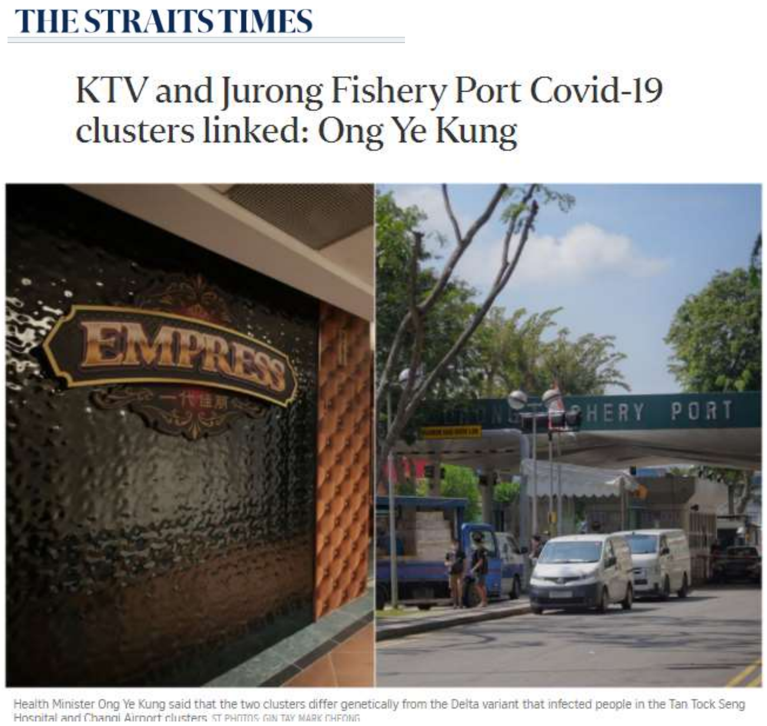
Previously, it was…



THE STRAITS TIMES

Uncovering the KTV 'butterfly' effect in Singapore as Covid-19 cluster grows to 88 cases

KTV lounges remain popular with men aged between 20 and 50. ST PHOTO: NG SOR LUAN



THE STRAITS TIMES

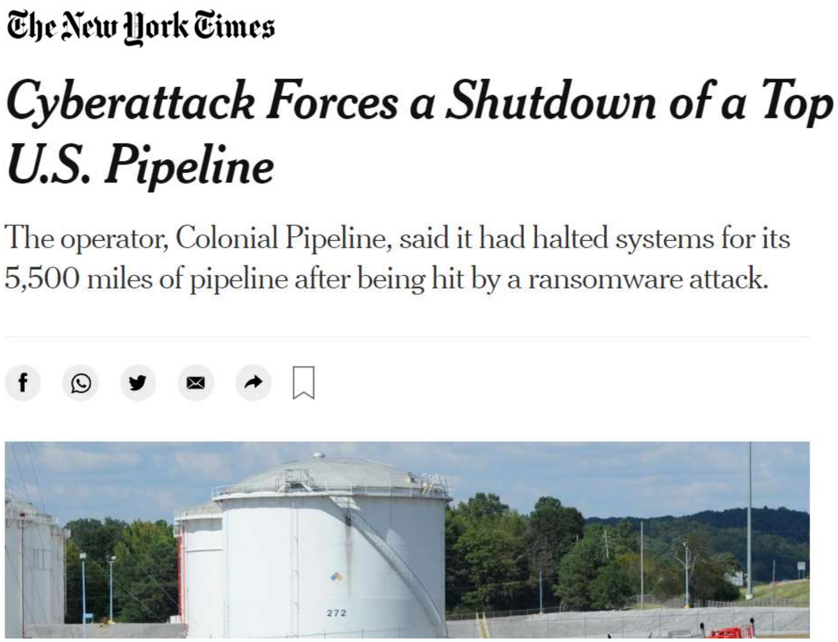
KTV and Jurong Fishery Port Covid-19 clusters linked: Ong Ye Kung

Health Minister Ong Ye Kung said that the two clusters differ genetically from the Delta variant that infected people in the Tan Tock Seng Hospital and Changi Airport clusters. ST PHOTOS: GIN TAY, MARK CHEONG

Stone Forest

Hot News

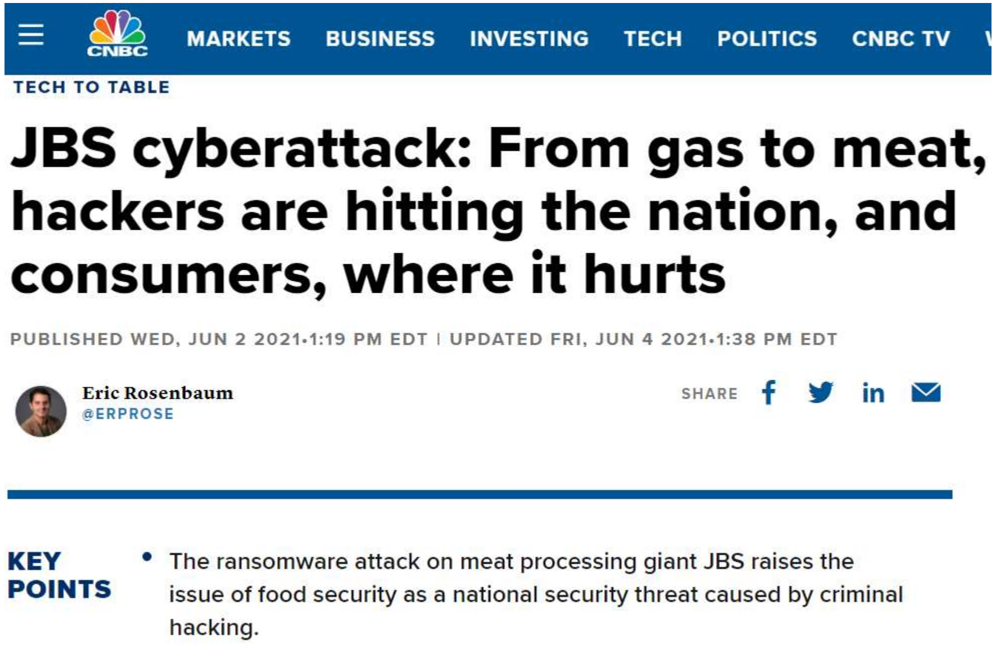
Just a few MONTHS ago



The New York Times

Cyberattack Forces a Shutdown of a Top U.S. Pipeline

The operator, Colonial Pipeline, said it had halted systems for its 5,500 miles of pipeline after being hit by a ransomware attack.



TECH TO TABLE

JBS cyberattack: From gas to meat, hackers are hitting the nation, and consumers, where it hurts

PUBLISHED WED, JUN 2 2021•1:19 PM EDT | UPDATED FRI, JUN 4 2021•1:38 PM EDT

Eric Rosenbaum
@ERPROSE

KEY POINTS

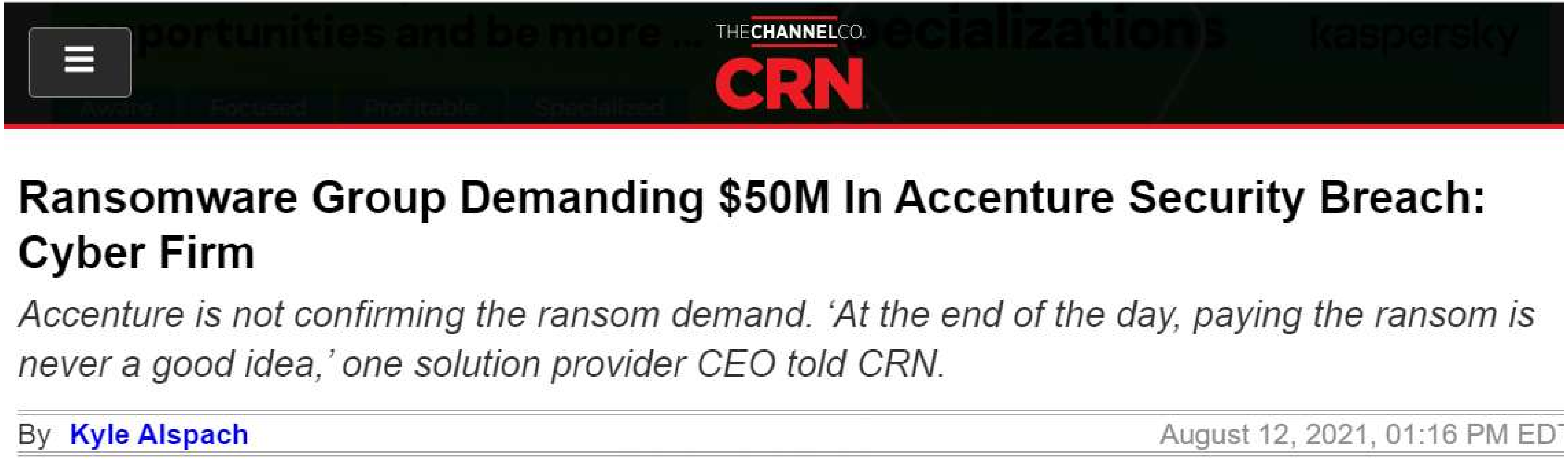
- The ransomware attack on meat processing giant JBS raises the issue of food security as a national security threat caused by criminal hacking.

Hot News

Another big company hit by a ransomware attack

By Brian Fung, CNN Business

Updated 1855 GMT (0255 HKT) August 11, 2021



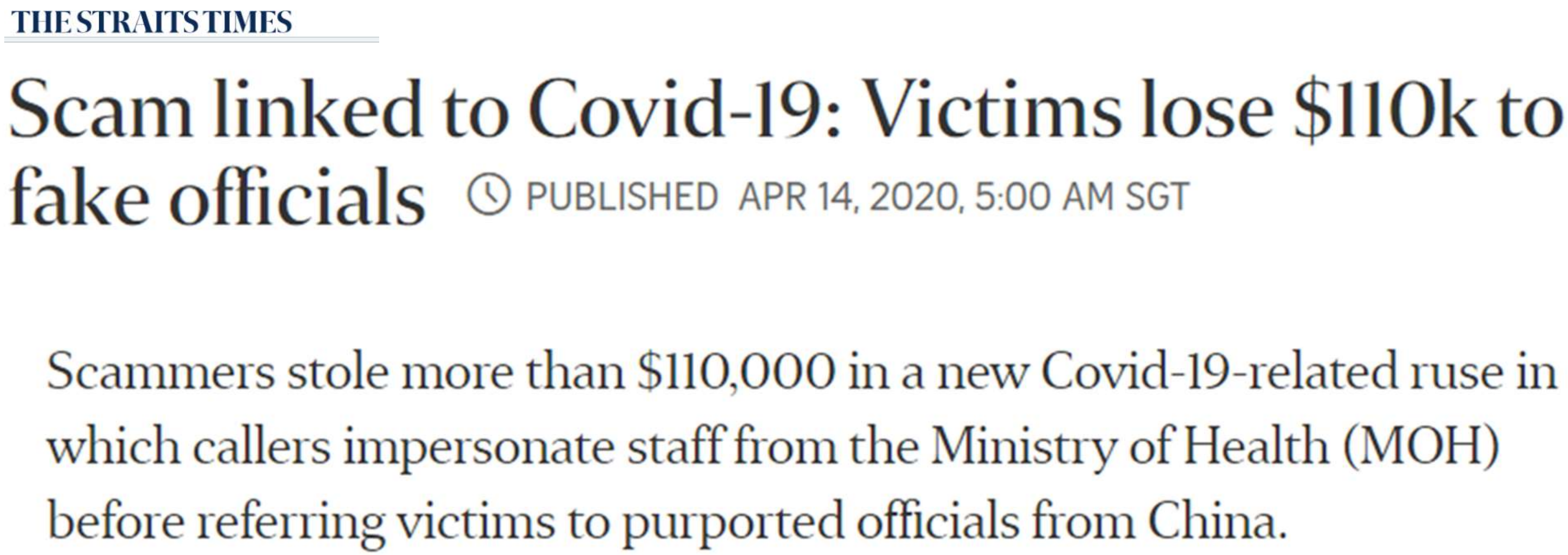
Ransomware Group Demanding $50M In Accenture Security Breach: Cyber Firm

Accenture is not confirming the ransom demand. 'At the end of the day, paying the ransom is never a good idea,' one solution provider CEO told CRN.

By Kyle Alspach

August 12, 2021, 01:16 PM EDT

Started a Long Time Ago



THE STRAITS TIMES

Scam linked to Covid-19: Victims lose $110k to fake officials

PUBLISHED APR 14, 2020, 5:00 AM SGT

Scammers stole more than $110,000 in a new Covid-19-related ruse in which callers impersonate staff from the Ministry of Health (MOH) before referring victims to purported officials from China.

Source : https://www.straitstimes.com/singapore/courts-crime/scam-linked-to-covid-19-victims-lose-110k-to-fake-officials

Incident #2

WHAT HAPPENED:

- **CEO received an anonymous email with personal data of 5 senior members**. These included their addresses, phone numbers, emails, and date of births.
- Head of IT was asked to investigate and there were no abnormal activities.
- There were abnormal incoming and outgoing traffic information on the logs.
- CEO received a **2nd anonymous email with a link to a video file**.
- IT downloaded the file onto a standalone computer and clicked on the video file.
- The video plays showing that the attacker have access to a spreadsheet that contained all their customer information and internal HR information.
- CEO received a **3rd anonymous email that asked for 2 bit coins within 24 hours**. If not, their confidential data would be released on the dark web.

SingCERT

Singapore Computer Emergency Response Team

Should you pay the ransom?

SingCERT **does not recommend** paying the ransom. Doing so does not guarantee that the data will be decrypted or that your data will not be published by threat actors.

It also encourages the threat actors to continue their criminal activities and target more victims. Threat actors may also see your organisation as a soft target and may strike again in the future.

Impact

- **Personal information** related to HR or any others could be compromised and this could be a violation of the Personal Data Protection Act. If there is a confirmed compromise of personal data, the DPO will need to activate the data breach response plan and notify PDPC within 3 calendar days if there is a material impact.

pdpc
PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

- **Confidential financial information** could be compromised and this could be used to the advantage of the attacker and this could be a violation of the SGX listing Act on "Insider trading".

SGX

- **Confidential business/operation information** could be compromised and this might be disadvantage to the company if there is/are any potential business collaboration activities.

Opportunity
Cost

Security Tips

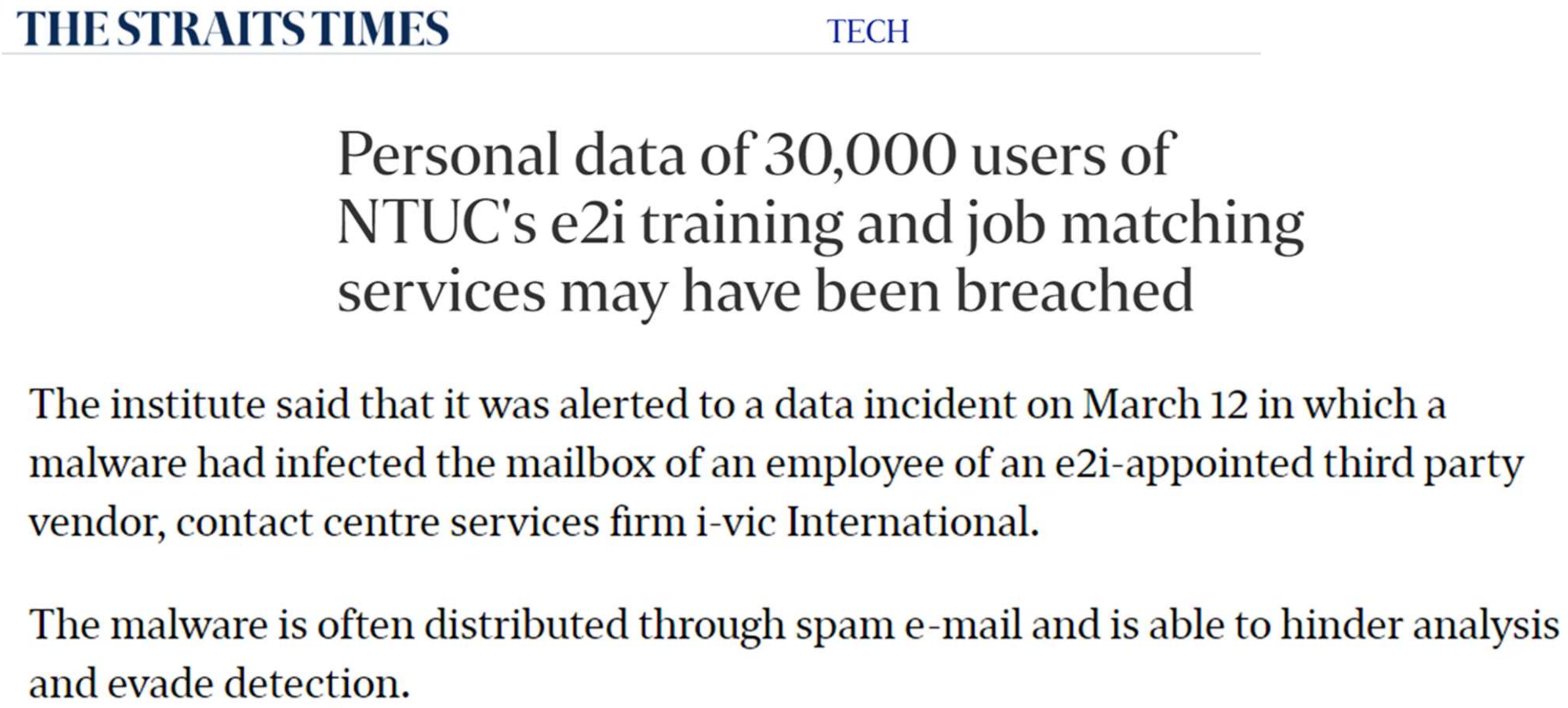
Make sure you **protect all personal information**, not only yours but those that you are handling as well

Do not send to your personal account any confidential information

Protect your personal email account with **2FA**

Stone Forest

Vendor Considerations



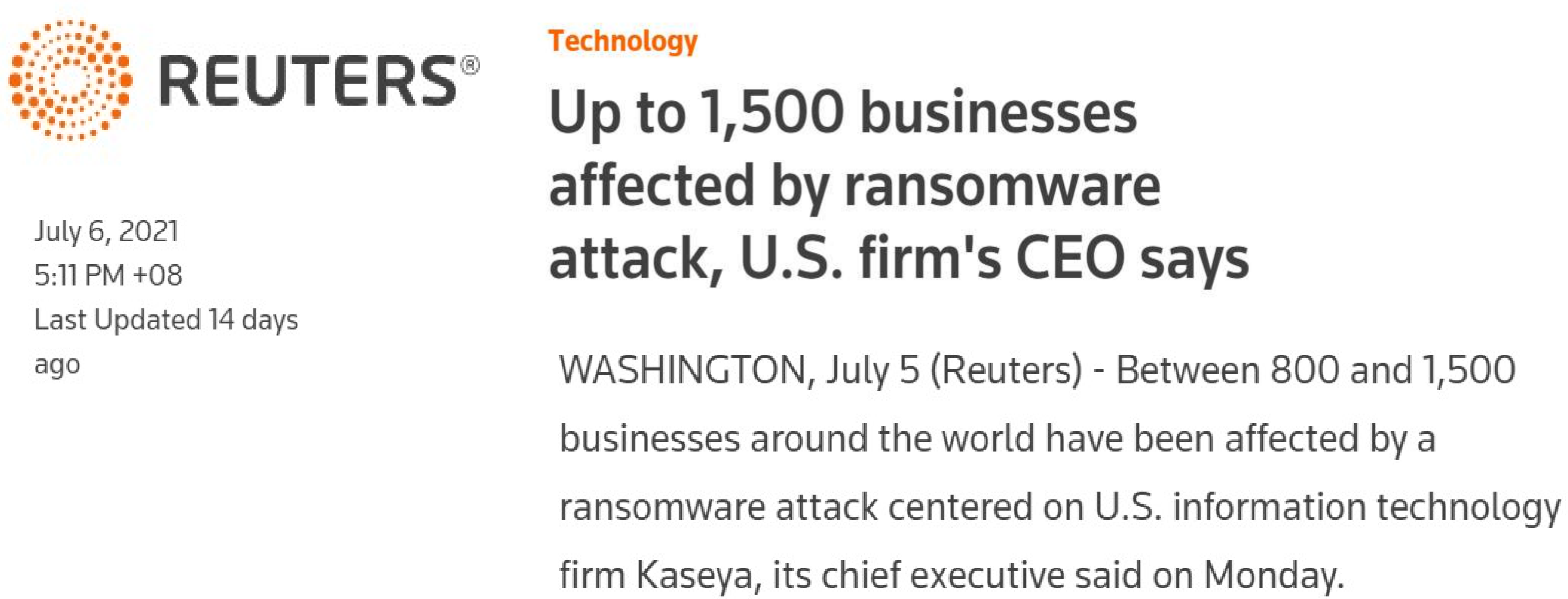
THE STRAITS TIMES TECH

Personal data of 30,000 users of NTUC's e2i training and job matching services may have been breached

The institute said that it was alerted to a data incident on March 12 in which a malware had infected the mailbox of an employee of an e2i-appointed third party vendor, contact centre services firm i-vic International.

The malware is often distributed through spam e-mail and is able to hinder analysis and evade detection.

Hot News



REUTERS®

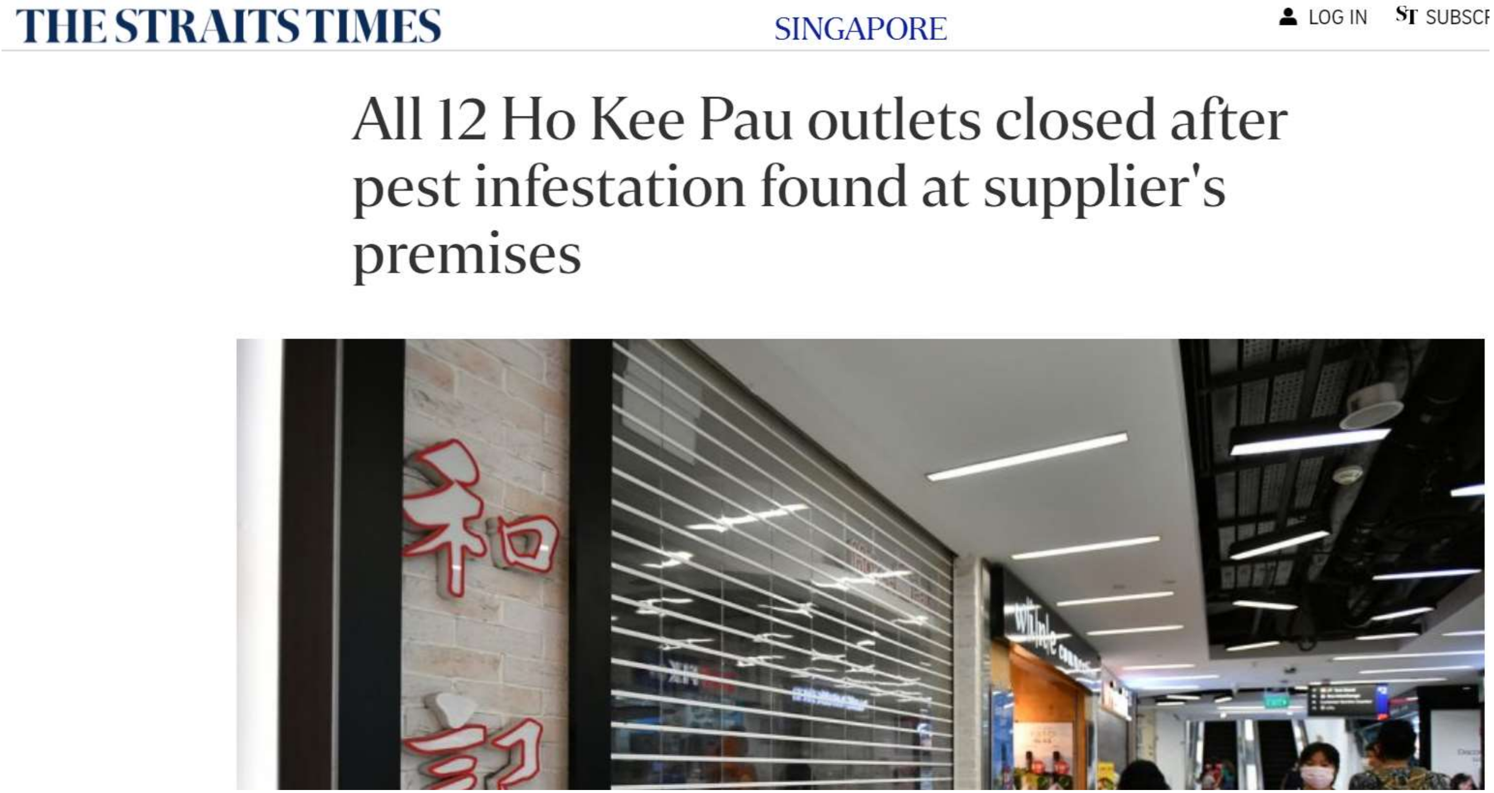
July 6, 2021
5:11 PM +08
Last Updated 14 days ago

Technology

Up to 1,500 businesses affected by ransomware attack, U.S. firm's CEO says

WASHINGTON, July 5 (Reuters) - Between 800 and 1,500 businesses around the world have been affected by a ransomware attack centered on U.S. information technology firm Kaseya, its chief executive said on Monday.

Hot News



THE STRAITS TIMES

SINGAPORE

All 12 Ho Kee Pau outlets closed after pest infestation found at supplier's premises

CSA Cyber Security Landscape 2020

The below key malicious cyber activities in 2020 are referenced from the Cyber Security Agency Singapore Cyber Security Landscape 2020 report.

Key malicious cyber security threats	Descriptions	Risk index
Ransomware	89 ransomware cases were reported to CSA in 2020, a sharp rise of 154 per cent from the 35 cases reported in 2019. The cases affected mostly Small-and-Medium Enterprises (SMEs), and hailed from sectors such as manufacturing, retail and healthcare.	High
Malicious Command and Control (C&C) Servers & Botnet Drones	CSA detected about 6,600 botnet drones with Singapore IP addresses daily, an increase from 2019's daily average of 2,300. Variants of the Mirai and Gamarue malware were prevalent among infected botnet IP addresses in 2020, with Mirai malware, which primarily targets Internet-of-Things (IoT) devices, staying strong due to the continuing growth of IoT devices locally.	Low
Phishing	Globally, 2020 saw a surge in COVID-19-related phishing campaigns. COVID-19 themes very likely accounted for over 4,700 of malicious URLs spoofing local entities and services that were in greater demand during Singapore's circuit breaker period, which included online retail and payment portals.	High

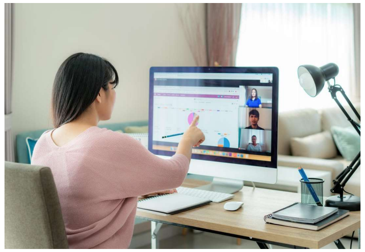
CSA Cyber Security Landscape 2020

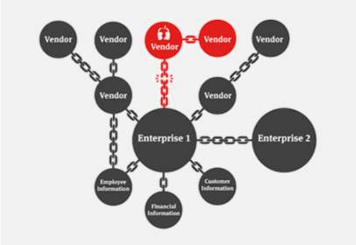
The below key malicious cyber activities in 2020 are referenced from the Cyber Security Agency Singapore Cyber Security Landscape 2020 report.

Key malicious cyber security threats	Descriptions	Risk index
Website Defacements	495 '.sg' websites were defaced in 2020, a decrease of 43 per cent from 873 in 2019. The majority of victims were SMEs, and no government websites were affected. The significant fall in 2020 is consistent with global trends and suggests that activist groups could have chosen other platforms with potentially wider reach (e.g. social media) to embarrass their victims.	Moderate
Cybercrime	Online cheating2 cases made up the top cybercrime category in Singapore, recording a rise of almost 62 per cent from 7,580 cases in 2019, to 12,251 cases in 2020. This trend is attributed to the rapid growth of e-commerce	Low

Anticipated Cybersecurity Trends

RANSOMWARE ATTACK
Your personal files are encrypted
You have 5 days to submit the payment!!!
To retrieve the Private key you need to pay
Your files will be lost





The report highlighted several emerging cybersecurity trends to watch against the backdrop of an increasingly complex and dynamic cyber threat landscape. Near-term trends include:

(a) Evolving Traits of Ransomware Attacks. Ransomware has evolved into a massive and systemic threat, and is no longer restricted to the sporadic and isolated incidents observed. Globally, the recent spate of high-profile ransomware incidents affecting essential service providers and key firms – such as the fuel pipeline company Colonial Pipeline (United States) and meat processing company, JBS (Brazil) - have demonstrated that the attacks could cause real-world effects and harm, and may have the potential to become national security concerns. The proliferation of such attacks spells an urgency for businesses to review their cybersecurity posture and ensure that they build their systems to be resilient in recovering from any successful cyber-attacks.

(b) Targeting of Remote Workforce. Social distancing measures during the COVID-19 pandemic have led to the rapid adoption of remote working. However, poorly configured network and software systems - which are part of the new remote work ecosystems - have widened the attack surface and exposed organisations to greater risk of cyber-attacks.

(c) Increased Targeting of Supply Chains. A successful breach in the supply chain, as seen in the high-profile SolarWinds supply-chain breach at the tail end of 2020, provided cyber threat actors a single pivoting point to multiple victims. While such attacks are not new, they are becoming more sophisticated. The compromise of a trusted supplier or software can result in widespread repercussions worldwide, as victims could include major vendors with huge customer bases.

Overview of

Cyber Threats in 2020

CYBERCRIME IN SINGAPORE

16,117

Cybercrime cases accounted for

43%

of overall crime in 2020

ONLINE CHEATING

2020: **12,251**
2019: 7,580
2018: 4,928

COMPUTER MISUSE ACT

2020: **3,621**
2019: 1,701
2018: 1,207

CYBER EXTORTION

2020: **245**
2019: 68
2018: 80

WEBSITE DEFACEMENTS

495

'.sg' websites were defaced, a sharp decrease of 43% from 873 cases in 2019

RANSOMWARE

89 ransomware cases were reported to CSA, with cases hailing from the manufacturing, retail and healthcare sectors. This was a significant rise of 154% in cases over the whole of 2019

C&C SERVERS AND BOTNET DRONES

1,026 unique and locally hosted C&C servers were discovered, a spike from 530 recorded in 2019

About **6,600** botnet drones were observed daily on average in 2020, also a significant increase from 2019's daily average of 2,300

PHISHING

47,000 phishing URLs[1] with a Singapore-link were detected. A slight decrease of 1% as compared to 2019

NUMBER OF CASES SINGCERT HANDLED IN

2020: **9,080**

2019: **8,491**

COMMONLY SPOOFED GOVERNMENT ORGANISATIONS IN SINGAPORE:

- MINISTRY OF EDUCATION (MOE)
- MINISTRY OF MANPOWER (MOM)
- SINGAPORE POLICE FORCE (SPF)

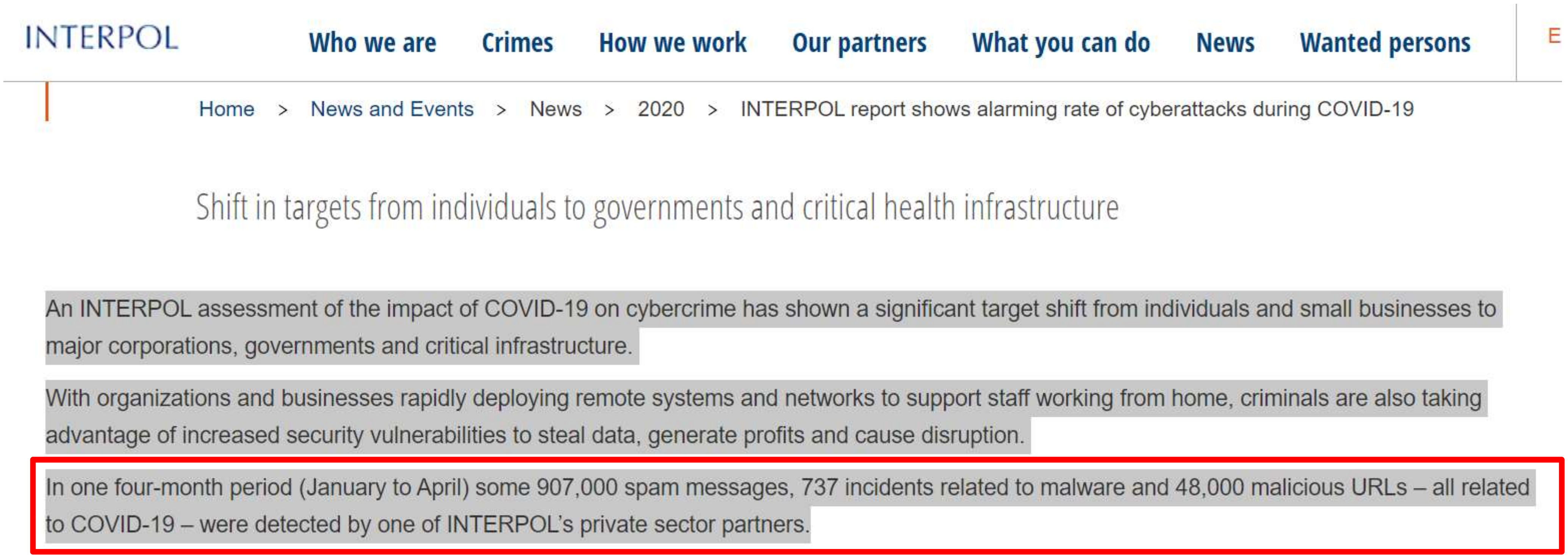
COMMONLY SPOOFED SECTORS

- TECHNOLOGY
- BANKING AND FINANCIAL SERVICES
- SOCIAL NETWORKING FIRMS

AMAZON, PAYPAL AND FACEBOOK WERE COMMONLY SPOOFED BRANDS

[1] URLs — Uniform Resource Locators, colloquially termed web addresses.

COVID-19 Impact


INTERPOL
Who we are
Crimes
How we work
Our partners
What you can do
News
Wanted persons
E
Home > News and Events > News > 2020 > INTERPOL report shows alarming rate of cyberattacks during COVID-19

Shift in targets from individuals to governments and critical health infrastructure

An INTERPOL assessment of the impact of COVID-19 on cybercrime has shown a significant target shift from individuals and small businesses to major corporations, governments and critical infrastructure.

With organizations and businesses rapidly deploying remote systems and networks to support staff working from home, criminals are also taking advantage of increased security vulnerabilities to steal data, generate profits and cause disruption.

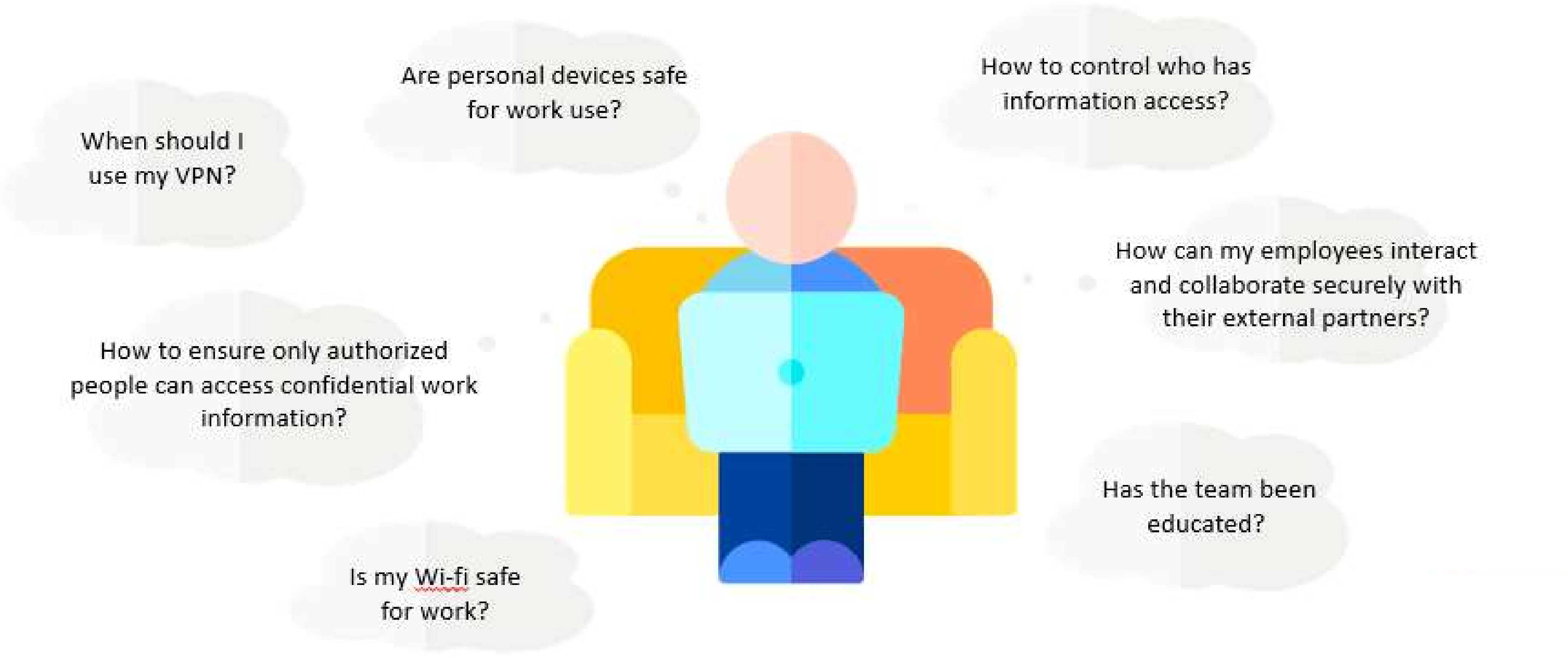
In one four-month period (January to April) some 907,000 spam messages, 737 incidents related to malware and 48,000 malicious URLs – all related to COVID-19 – were detected by one of INTERPOL's private sector partners.

Are you able to IDENTIFY a phishing or fake email?

If unsure, please VERIFY!

Stone Forest

WFH Risks



When should I use my VPN?

Are personal devices safe for work use?

How to control who has information access?

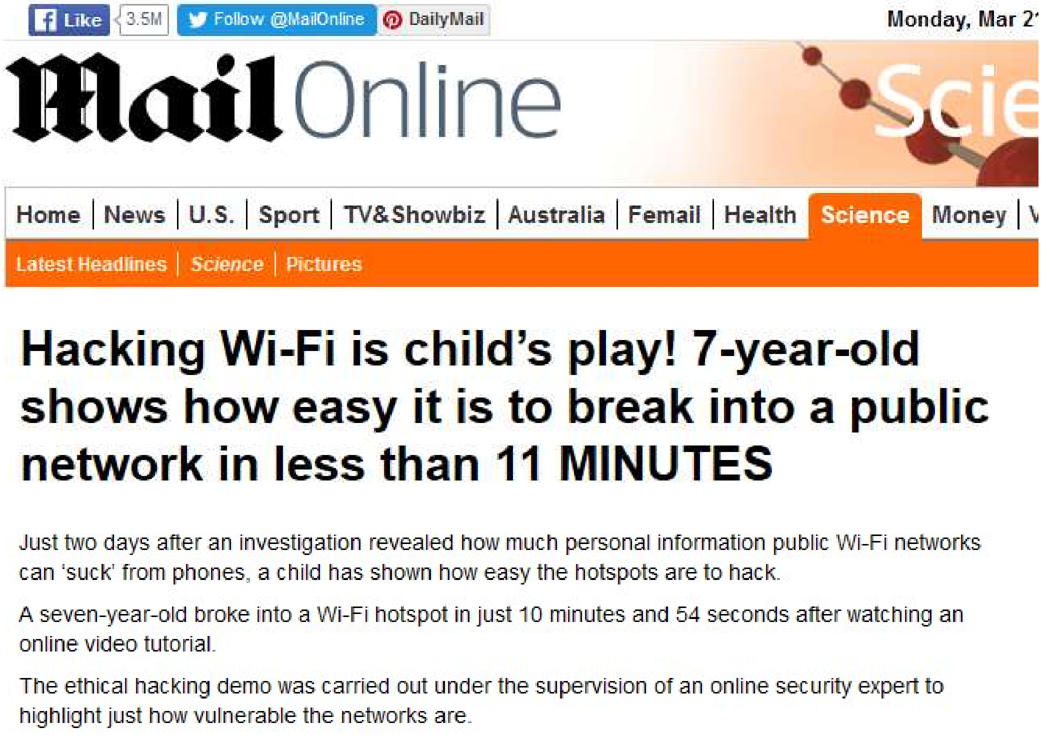
How can my employees interact and collaborate securely with their external partners?

How to ensure only authorized people can access confidential work information?

Has the team been educated?

Is my Wi-fi safe for work?

WFH Risks


Like
3.5M
Follow @MailOnline
DailyMail
Monday, Mar 2
Mail Online
Scie
Home | News | U.S. | Sport | TV&Showbiz | Australia | Femail | Health | Science | Money | V
Latest Headlines | Science | Pictures

Hacking Wi-Fi is child's play! 7-year-old shows how easy it is to break into a public network in less than 11 MINUTES

Just two days after an investigation revealed how much personal information public Wi-Fi networks can 'suck' from phones, a child has shown how easy the hotspots are to hack.

A seven-year-old broke into a Wi-Fi hotspot in just 10 minutes and 54 seconds after watching an online video tutorial.

The ethical hacking demo was carried out under the supervision of an online security expert to highlight just how vulnerable the networks are.

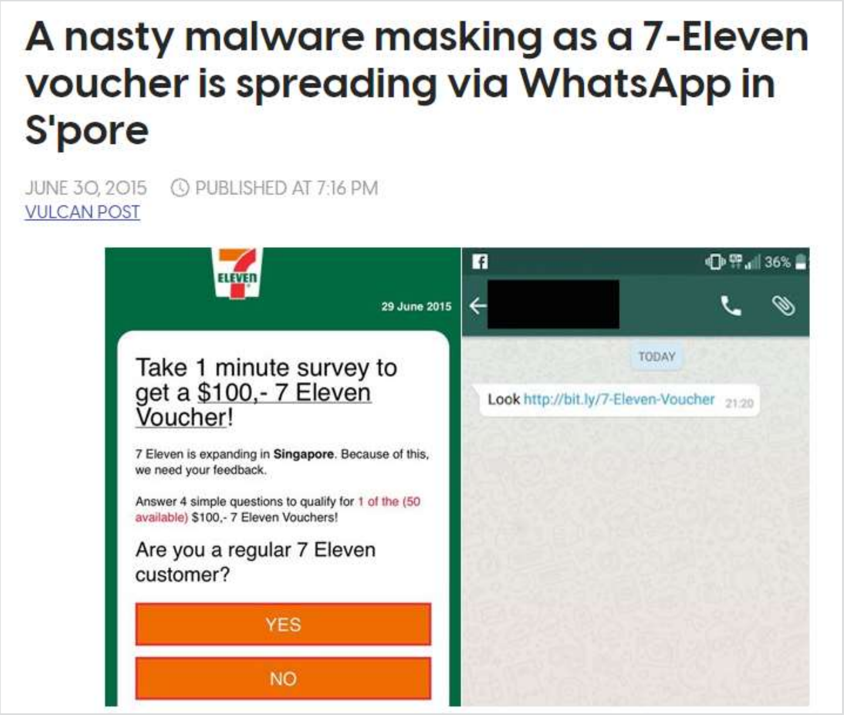
Betsy Davies (pictured) watched an online video tutorial before being asked to hack into a Wi-Fi hotspot. It took the seven-year-old 11 minutes to infiltrate the network by setting up a rogue access point - frequently used by attackers to activate a 'man in the middle' attack, and begin eavesdropping on - or 'sniffing' - traffic

Stone Forest

When you are working from home, ensure PASSWORD CONTROL to connect to your WIFI?

Ensure ENCRYPTION is enabled.

Collaboration Tools Risk



A nasty malware masking as a 7-Eleven voucher is spreading via WhatsApp in S'pore

JUNE 30, 2015 PUBLISHED AT 7:16 PM
VULCAN POST

29 June 2015

Take 1 minute survey to get a $100,- 7 Eleven Voucher!

7 Eleven is expanding in **Singapore**. Because of this, we need your feedback.

Answer 4 simple questions to qualify for 1 of the (50 available) $100,- 7 Eleven Vouchers!

Are you a regular 7 Eleven customer?

YES

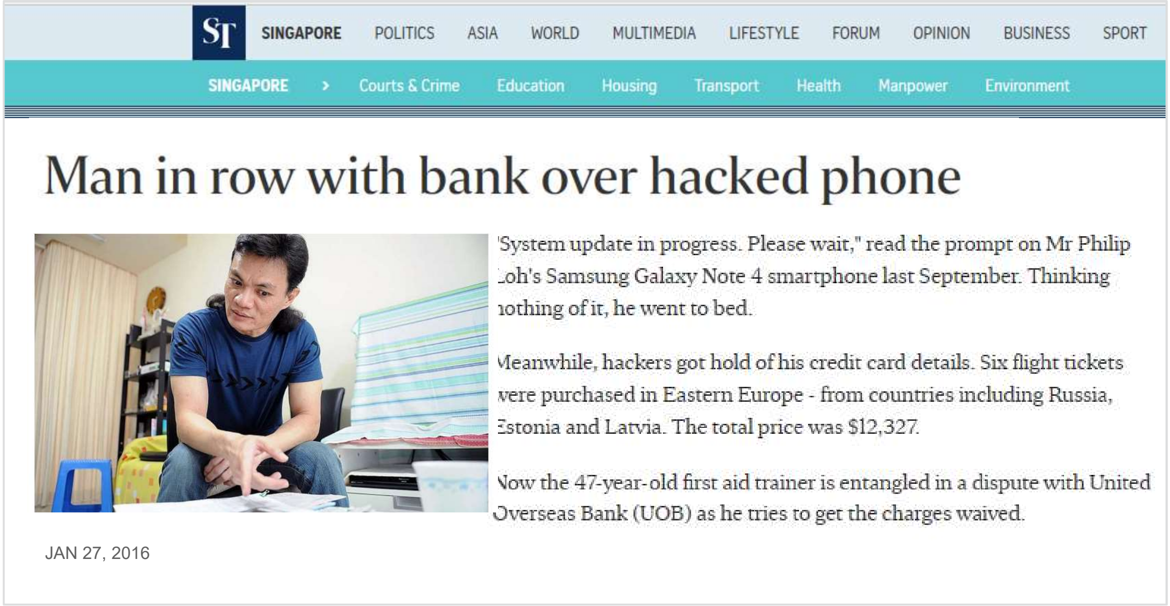
NO

36%

[redacted]

TODAY

Look http://bit.ly/7-Eleven-Voucher 21:20



Man in row with bank over hacked phone

'System update in progress. Please wait," read the prompt on Mr Philip Loh's Samsung Galaxy Note 4 smartphone last September. Thinking nothing of it, he went to bed.

Meanwhile, hackers got hold of his credit card details. Six flight tickets were purchased in Eastern Europe - from countries including Russia, Estonia and Latvia. The total price was $12,327.

Now the 47-year-old first aid trainer is entangled in a dispute with United Overseas Bank (UOB) as he tries to get the charges waived.

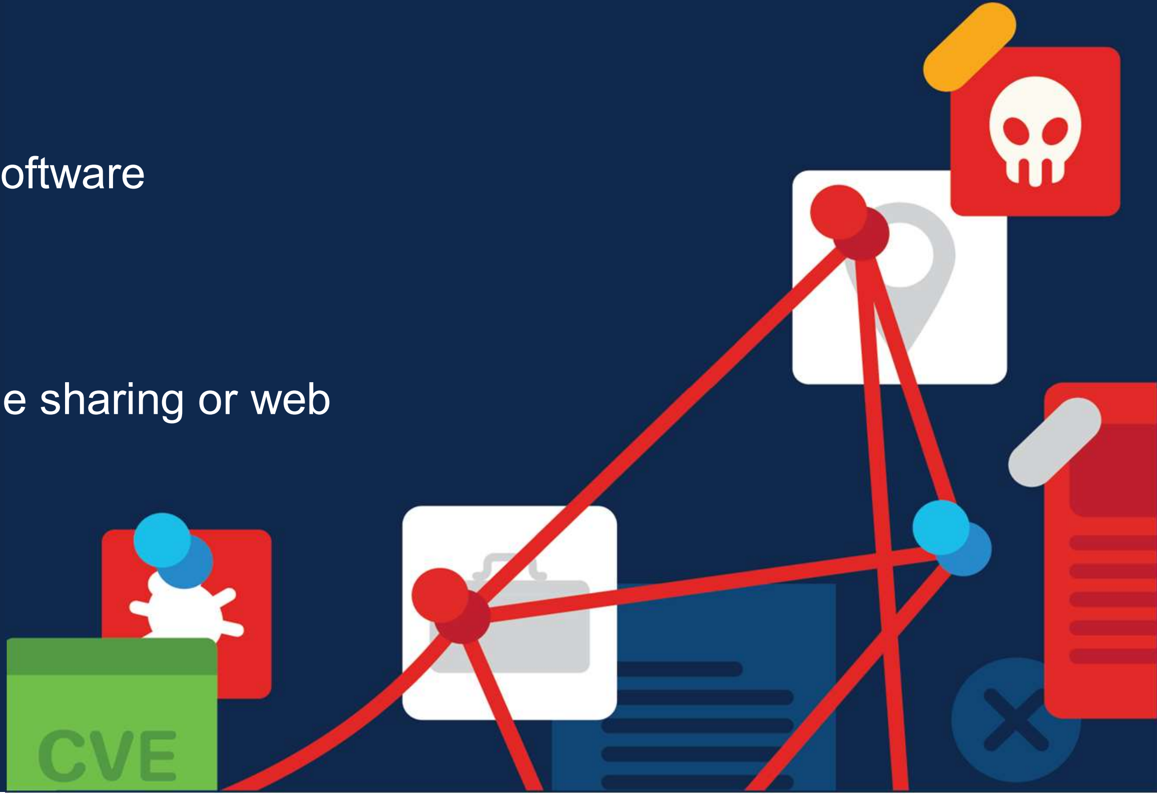
JAN 27, 2016

Stone Forest

DOUDLE VERIFY with the sender
if you are asked to click or
download any links or files.

How to Keep Malicious Software Off My Computer?

- ✓ Be suspicious
- ✓ Comply with security policies and procedures
- ✓ Never disable or tamper with virus protection software
- ✓ Always scan files from external storage media
- ✓ Never re-configure your computer to provide file sharing or web application services
- ✓ Report any suspicious programs found running on your PC



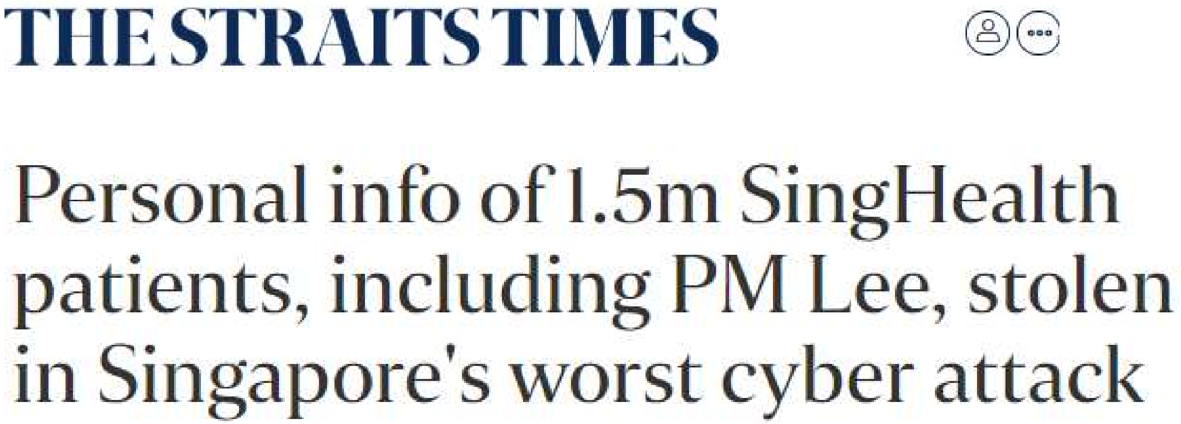
As a General Good Practice

DO NOT open any files and/or click on links from **unknown email**

If you received such email, please **immediately delete** the email

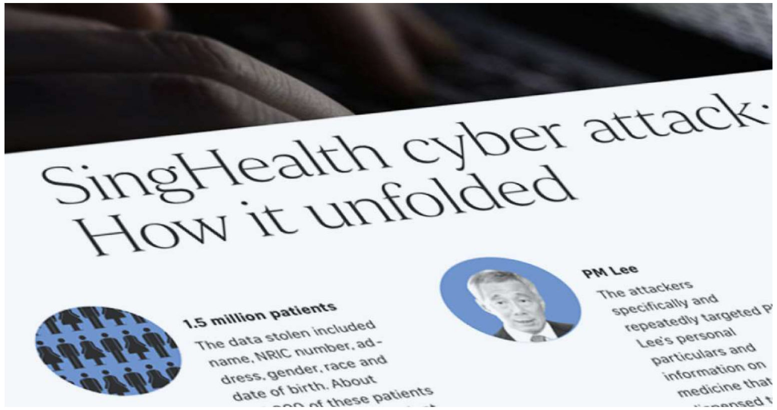
If in doubt, **check** with your local IT support

Cyber Risks



THE STRAITS TIMES

Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack



SingHealth cyber attack: How it unfolded

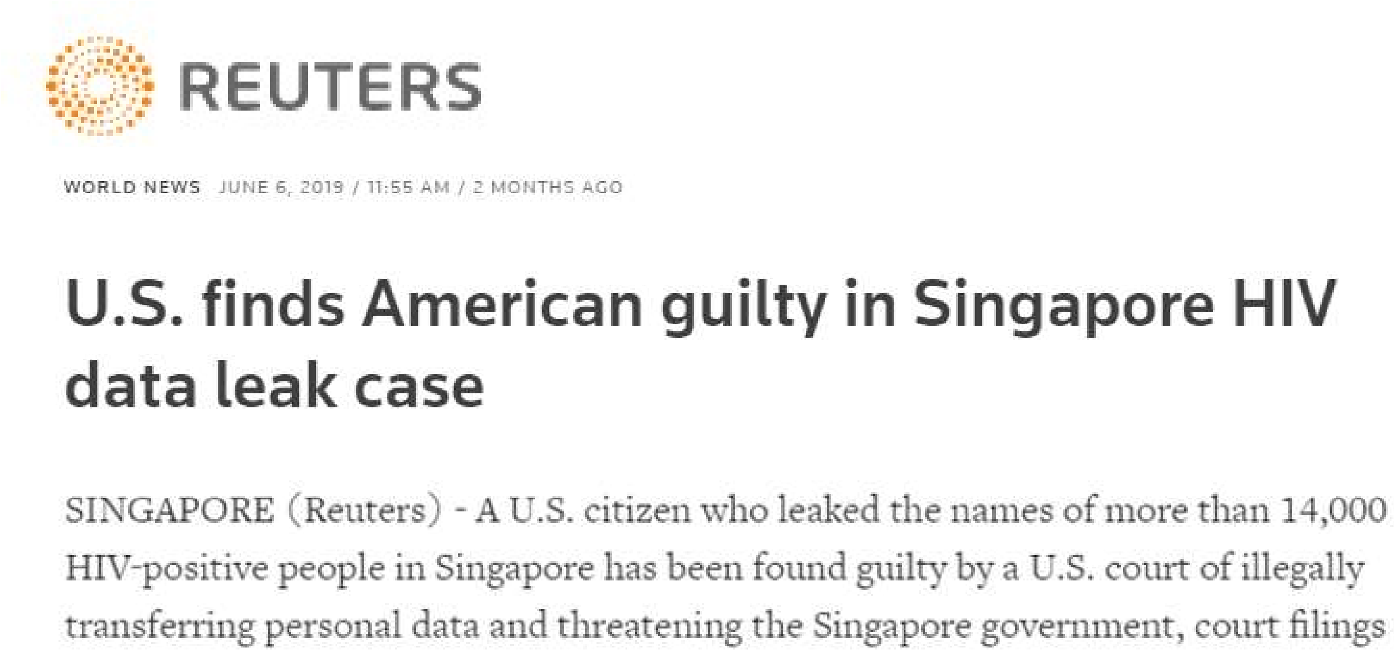
1.5 million patients

The data stolen included name, NRIC number, ad- dress, gender, race and date of birth. About

PM Lee

The attackers specifically and repeatedly targeted P Lee's personal particulars and information on medicine that

Technology Risks



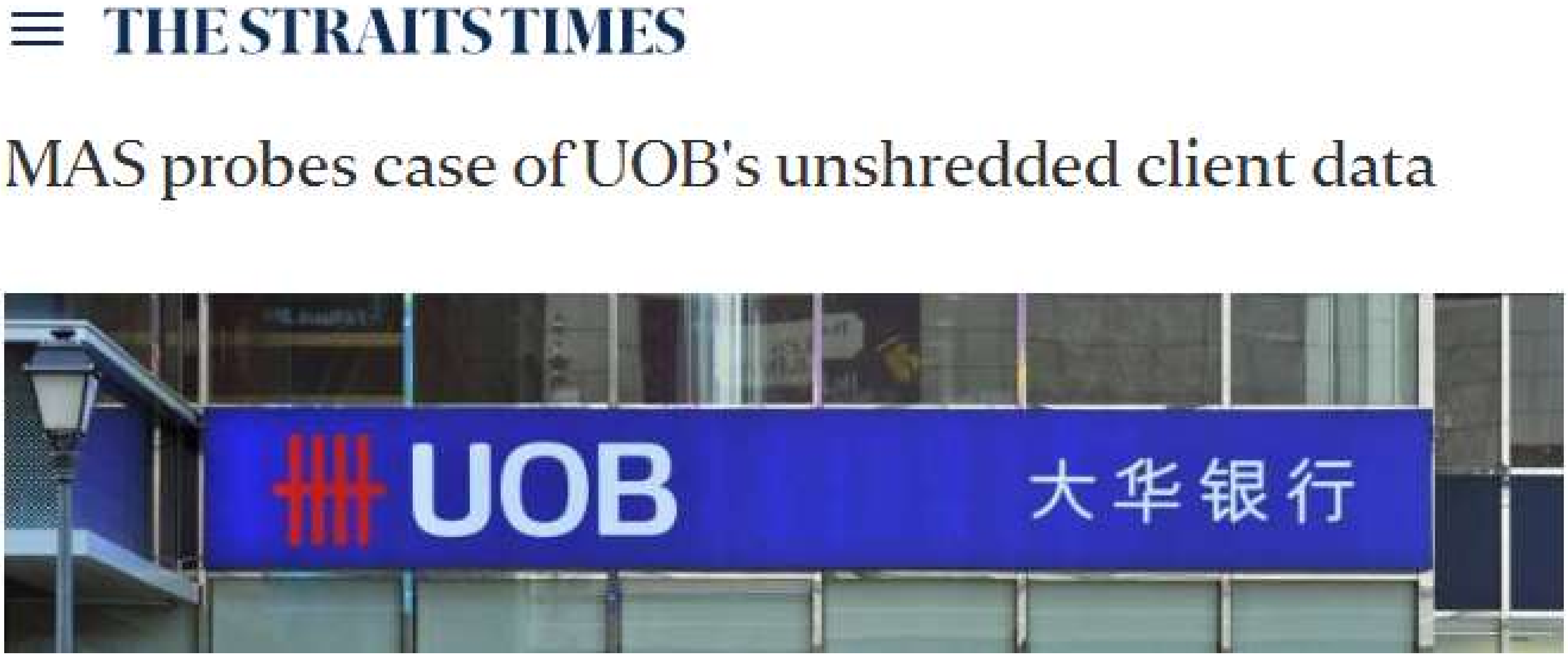
REUTERS

WORLD NEWS JUNE 6, 2019 / 11:55 AM / 2 MONTHS AGO

U.S. finds American guilty in Singapore HIV data leak case

SINGAPORE (Reuters) - A U.S. citizen who leaked the names of more than 14,000 HIV-positive people in Singapore has been found guilty by a U.S. court of illegally transferring personal data and threatening the Singapore government, court filings

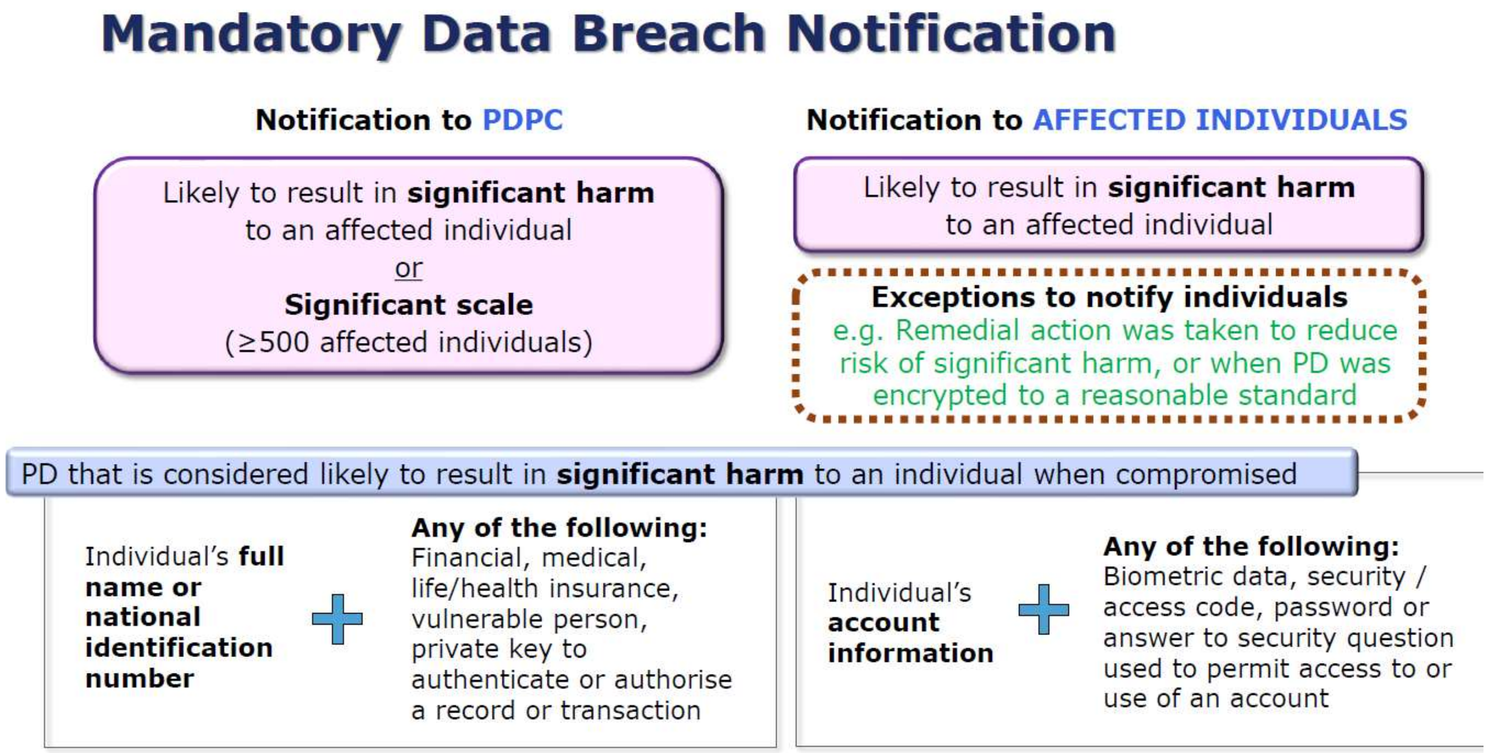
Information Risks



THE STRAITS TIMES

MAS probes case of UOB's unshredded client data

PDPA Updates



Mandatory Data Breach Notification

Notification to PDPC

Likely to result in **significant harm** to an affected individual

or

Significant scale

(≥500 affected individuals)

Notification to AFFECTED INDIVIDUALS

Likely to result in **significant harm** to an affected individual

Exceptions to notify individuals

e.g. Remedial action was taken to reduce risk of significant harm, or when PD was encrypted to a reasonable standard

PD that is considered likely to result in **significant harm** to an individual when compromised

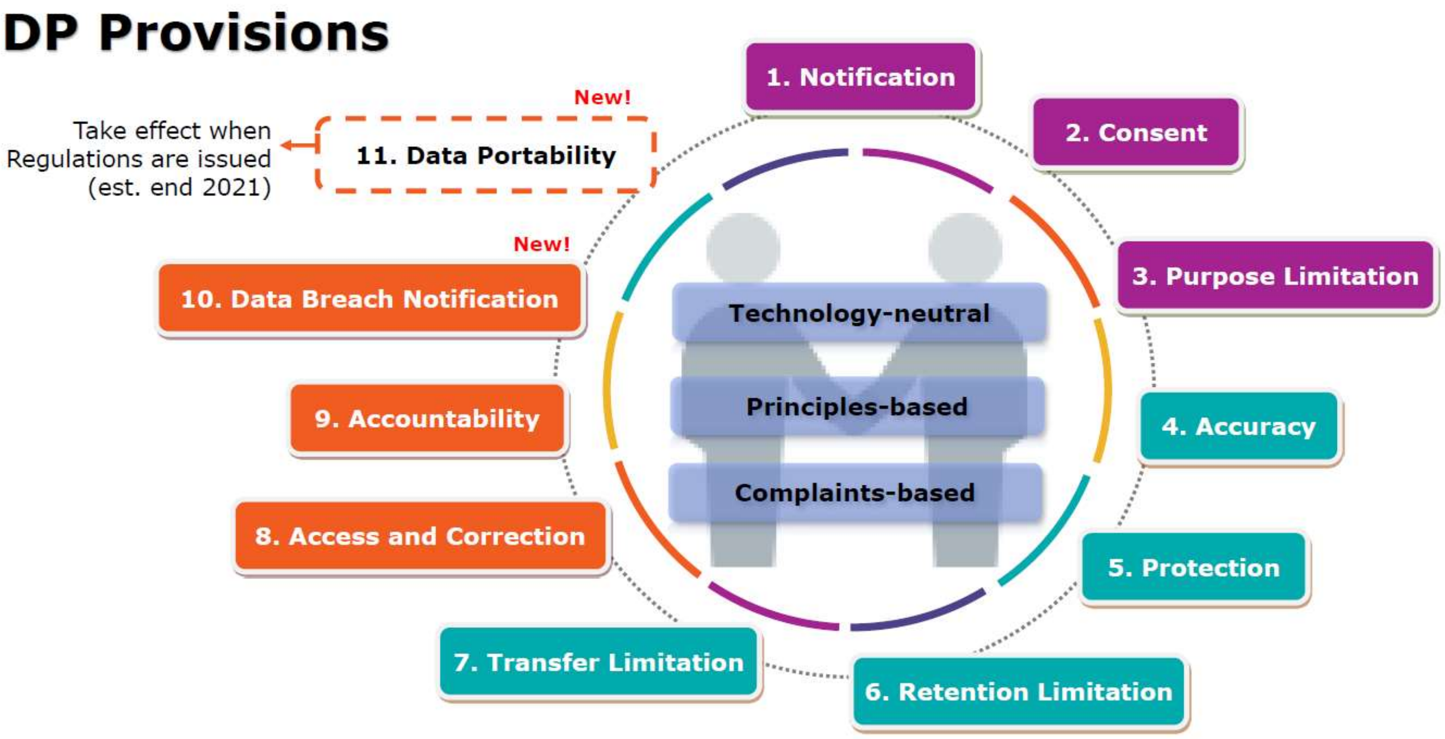
Individual's **full name or national identification number** + **Any of the following:** Financial, medical, life/health insurance, vulnerable person, private key to authenticate or authorise a record or transaction

Individual's **account information** + **Any of the following:** Biometric data, security / access code, password or answer to security question used to permit access to or use of an account

Stone Forest

PDPA Updates

PERSONAL DATA PROTECTION COMMISSION SINGAPORE



DP Provisions

Take effect when Regulations are issued (est. end 2021)

New!

11. Data Portability

New!

10. Data Breach Notification

9. Accountability

8. Access and Correction

7. Transfer Limitation

6. Retention Limitation

5. Protection

4. Accuracy

3. Purpose Limitation

2. Consent

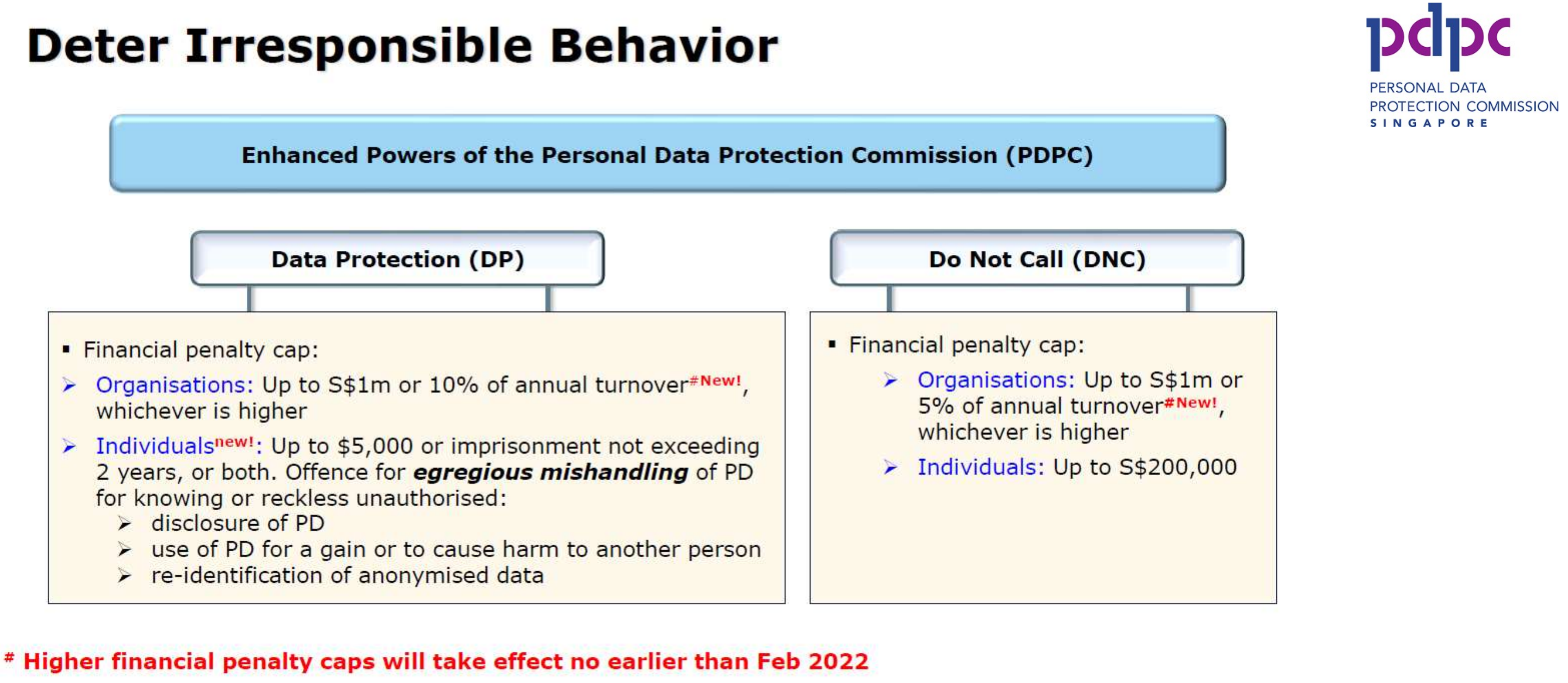
1. Notification

Technology-neutral

Principles-based

Complaints-based

PDPA Updates



Deter Irresponsible Behavior

PERSONAL DATA PROTECTION COMMISSION SINGAPORE

Enhanced Powers of the Personal Data Protection Commission (PDPC)

Data Protection (DP)

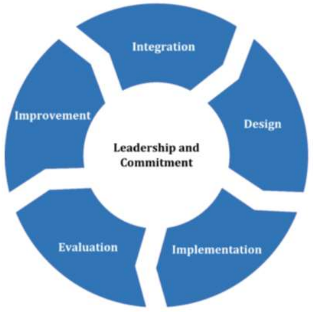
- Financial penalty cap:
  - Organisations: Up to S$1m or 10% of annual turnover#New!, whichever is higher
  - Individualsnew!: Up to $5,000 or imprisonment not exceeding 2 years, or both. Offence for ***egregious mishandling*** of PD for knowing or reckless unauthorised:
    - disclosure of PD
    - use of PD for a gain or to cause harm to another person
    - re-identification of anonymised data

Do Not Call (DNC)

- Financial penalty cap:
  - Organisations: Up to S$1m or 5% of annual turnover#New!, whichever is higher
  - Individuals: Up to S$200,000

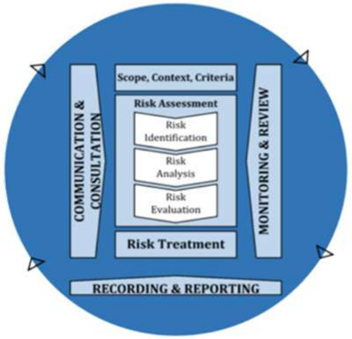
# Higher financial penalty caps will take effect no earlier than Feb 2022

Important Things to Note



Cyber resilience involves **continuously strengthening the risk management** process

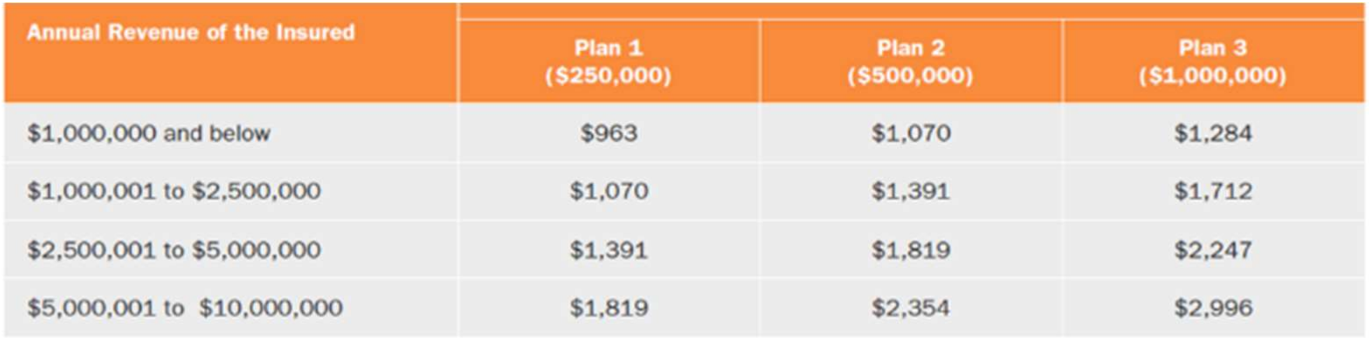
Constant education & awareness is required



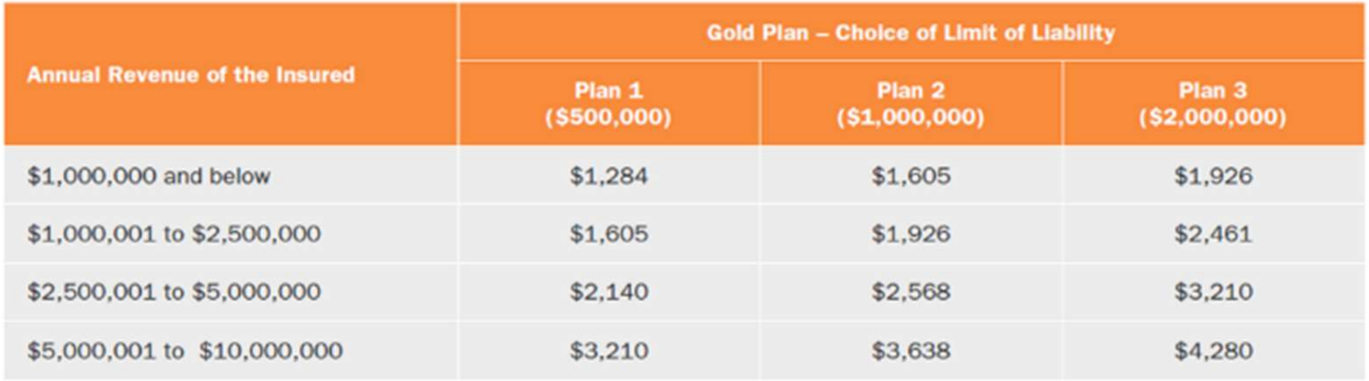
Leverage on **auditor's experiences**

Cyber Insurance

Are you protected with cyber insurance?

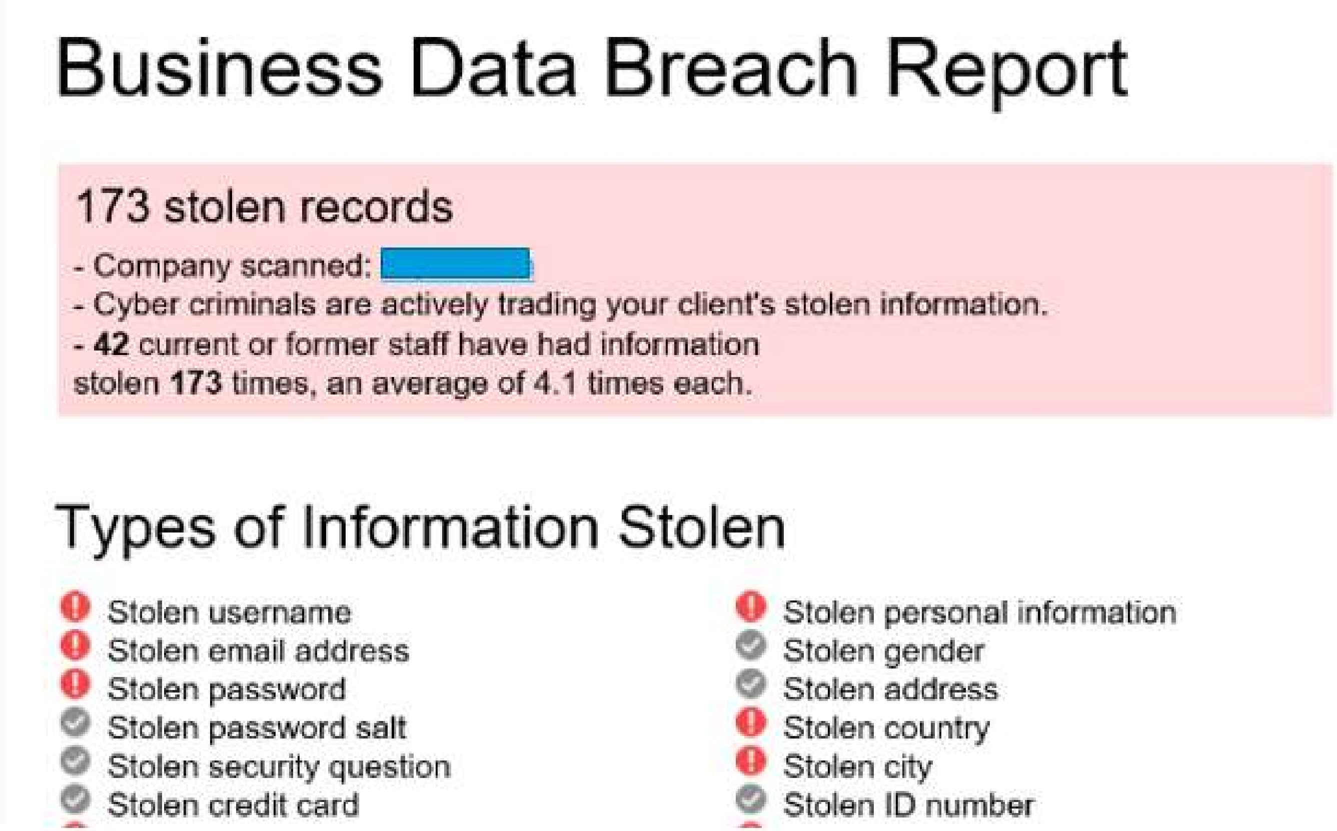


Annual Revenue of the Insured	Plan 1 ($250,000)	Plan 2 ($500,000)	Plan 3 ($1,000,000)
$1,000,000 and below	$963	$1,070	$1,284
$1,000,001 to $2,500,000	$1,070	$1,391	$1,712
$2,500,001 to $5,000,000	$1,391	$1,819	$2,247
$5,000,001 to $10,000,000	$1,819	$2,354	$2,996



Annual Revenue of the Insured	Gold Plan – Choice of Limit of Liability		
	Plan 1 ($500,000)	Plan 2 ($1,000,000)	Plan 3 ($2,000,000)
$1,000,000 and below	$1,284	$1,605	$1,926
$1,000,001 to $2,500,000	$1,605	$1,926	$2,461
$2,500,001 to $5,000,000	$2,140	$2,568	$3,210
$5,000,001 to $10,000,000	$3,210	$3,638	$4,280

Cyber Digital Footprint (Threat Intelligence/ Hunting)



Business Data Breach Report

173 stolen records

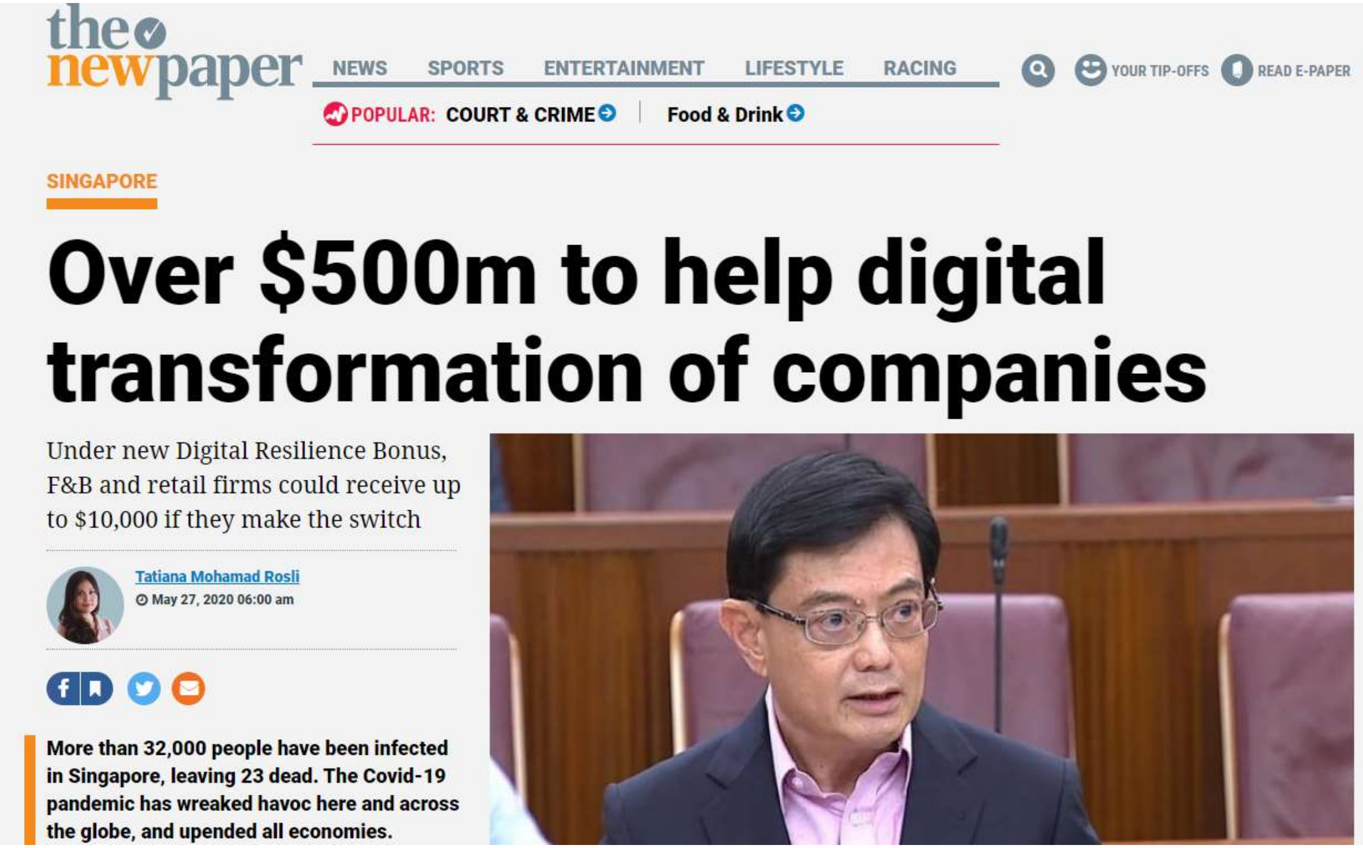
- Company scanned: [redacted]
- Cyber criminals are actively trading your client's stolen information.
- **42** current or former staff have had information stolen **173** times, an average of 4.1 times each.

Types of Information Stolen

❗ Stolen username
❗ Stolen email address
❗ Stolen password
✓ Stolen password salt
✓ Stolen security question
✓ Stolen credit card

❗ Stolen personal information
✓ Stolen gender
✓ Stolen address
❗ Stolen country
❗ Stolen city
✓ Stolen ID number

Singapore's Push for Digitalisation



the new paper NEWS SPORTS ENTERTAINMENT LIFESTYLE RACING YOUR TIP-OFFS READ E-PAPER

POPULAR: COURT & CRIME | Food & Drink

SINGAPORE

Over $500m to help digital transformation of companies

Under new Digital Resilience Bonus, F&B and retail firms could receive up to $10,000 if they make the switch

Tatiana Mohamad Rosli

May 27, 2020 06:00 am

More than 32,000 people have been infected in Singapore, leaving 23 dead. The Covid-19 pandemic has wreaked havoc here and across the globe, and upended all economies.

Stone Forest

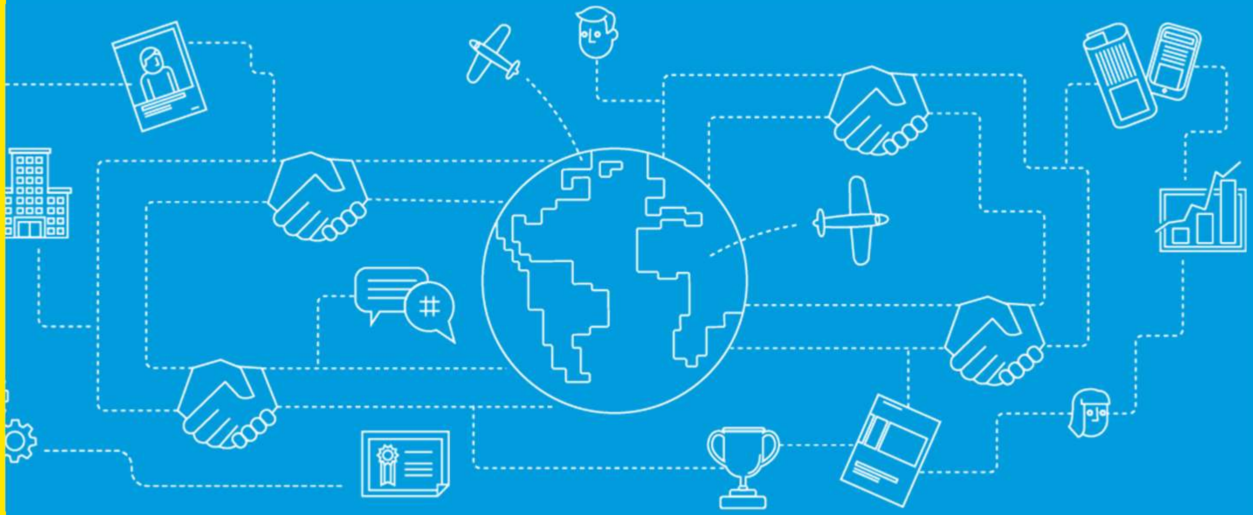
In Conclusion

1. Support from the Boards, Directors and management is very important

2. Technology risk should always be part of the organisation risk management framework

3. Boards, Directors and Management must always try to stay abreast with the latest technology news and risks

If not, you will become another cyber breach statistic!



Thank you

8 Wilkie Road, #03-08, Wilkie Edge, Singapore 228095
T +65 6533 7600 | **F** +65 6538 7600

Info@StoneForestIT.com.sg | www.StoneForest.com.sg

Stone Forest

Business Advisors to Growing Businesses