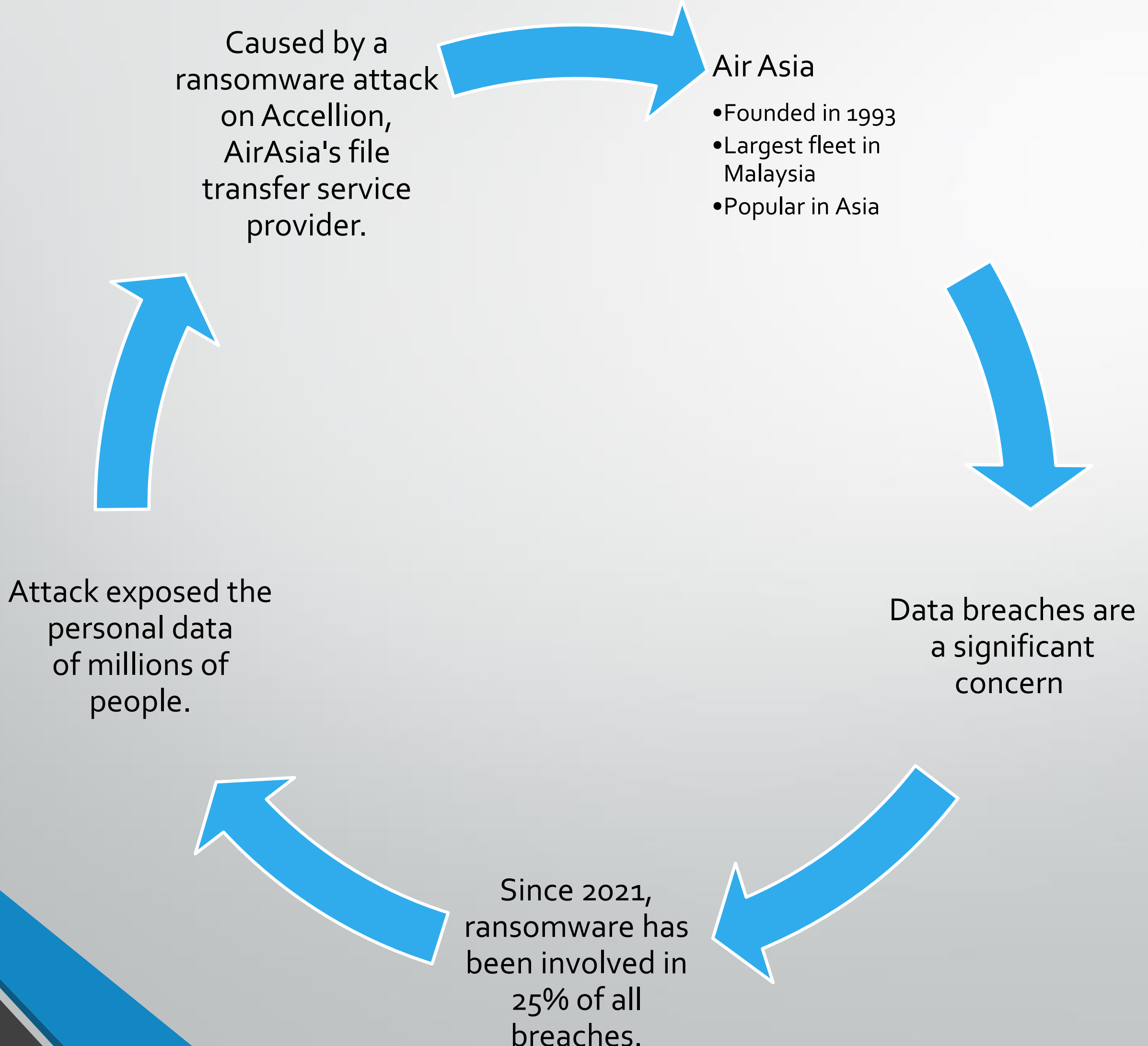
AirAsia Data Breach

- **LIS5775 – Organizational Information Security**
- **Instructor: Dr. Bill Hunkapiller**
- **Date: April 23, 2023**
- **Group: Team C**
- **Students:** Adam MacDougall, Thomas Matejek, Madhu Nepal, Mehmet Ozmen, Chris Panczak, Chandra Rawat, Shavaughn Robinson

Overview

- Analyze the recent ransomware attack on Air Asia.
- Attack
- Financial Cost Analysis
- Detection and Prevention
- Solutions

Introduction



Air Asia

- Founded in 1993
- Largest fleet in Malaysia
- Popular in Asia

Data breaches are a significant concern

Since 2021, ransomware has been involved in 25% of all breaches.

Attack exposed the personal data of millions of people.

Caused by a ransomware attack on Accellion, AirAsia's file transfer service provider.

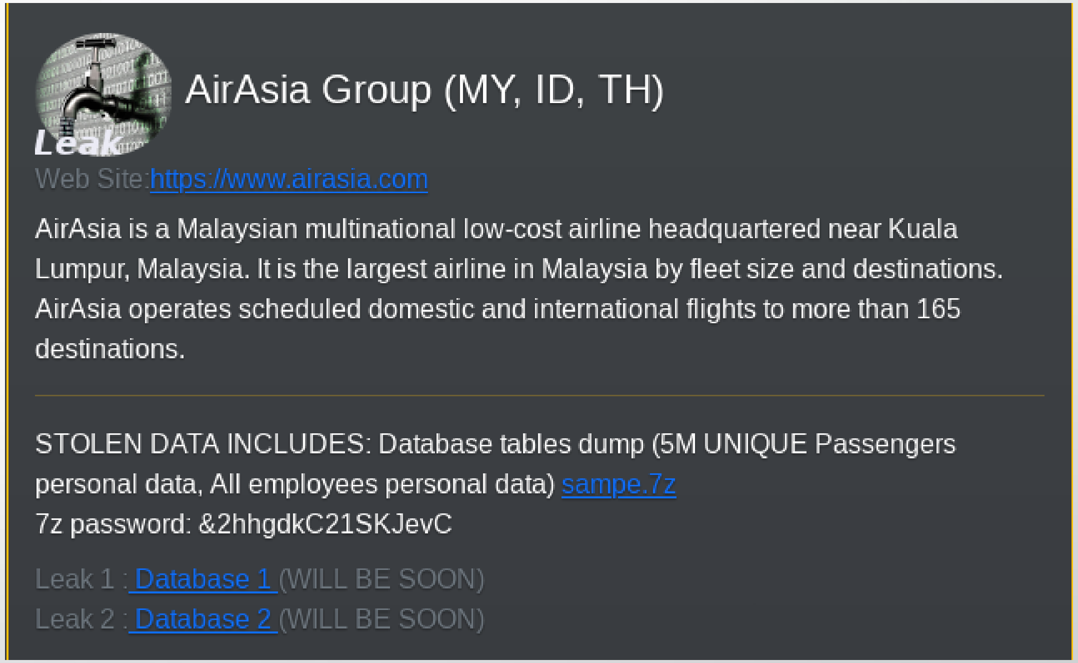
Attacks

Daixin Team gained unauthorized access to the AirAsia's VPN servers via spear phishing and VPN vulnerabilities.

After gaining access, attackers resetted passwords of privileged accounts and dumped credentials to obtain account logins.

Attackers then used reverse proxy tool called "Ngrok" to extort data from the VMware ESXi servers.

After retrieval of unauthorized data of confidential information of the companies' customer and employees, attackers installed a ransomware similar to "Babuk Locker" to their VMware ESXi servers inflicting all the machines in the network to be locked.



AirAsia Group (MY, ID, TH)

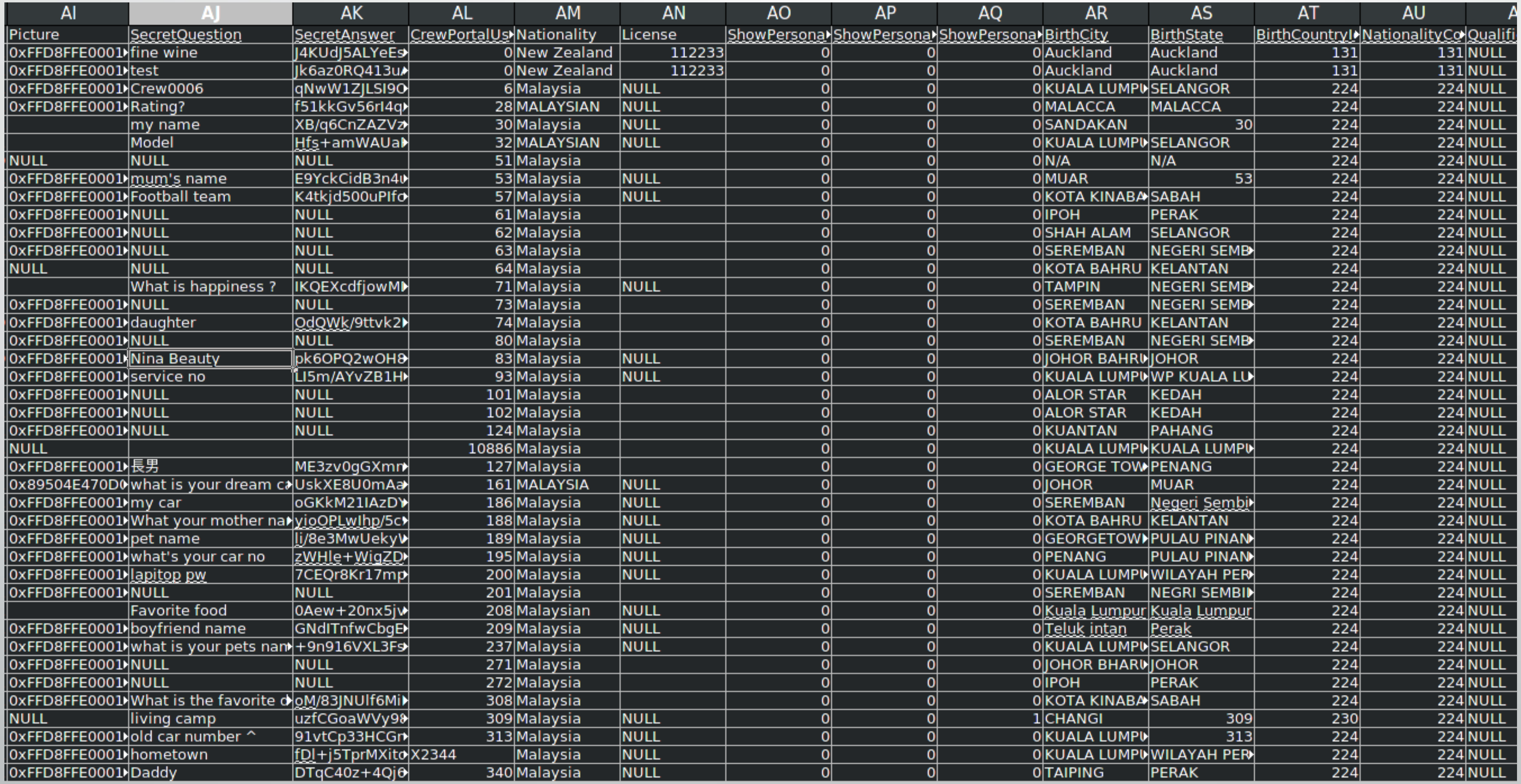
Web Site:https://www.airasia.com

AirAsia is a Malaysian multinational low-cost airline headquartered near Kuala Lumpur, Malaysia. It is the largest airline in Malaysia by fleet size and destinations. AirAsia operates scheduled domestic and international flights to more than 165 destinations.

STOLEN DATA INCLUDES: Database tables dump (5M UNIQUE Passengers personal data, All employees personal data) sampe.7z
7z password: &2hhgdkC21SKJevC

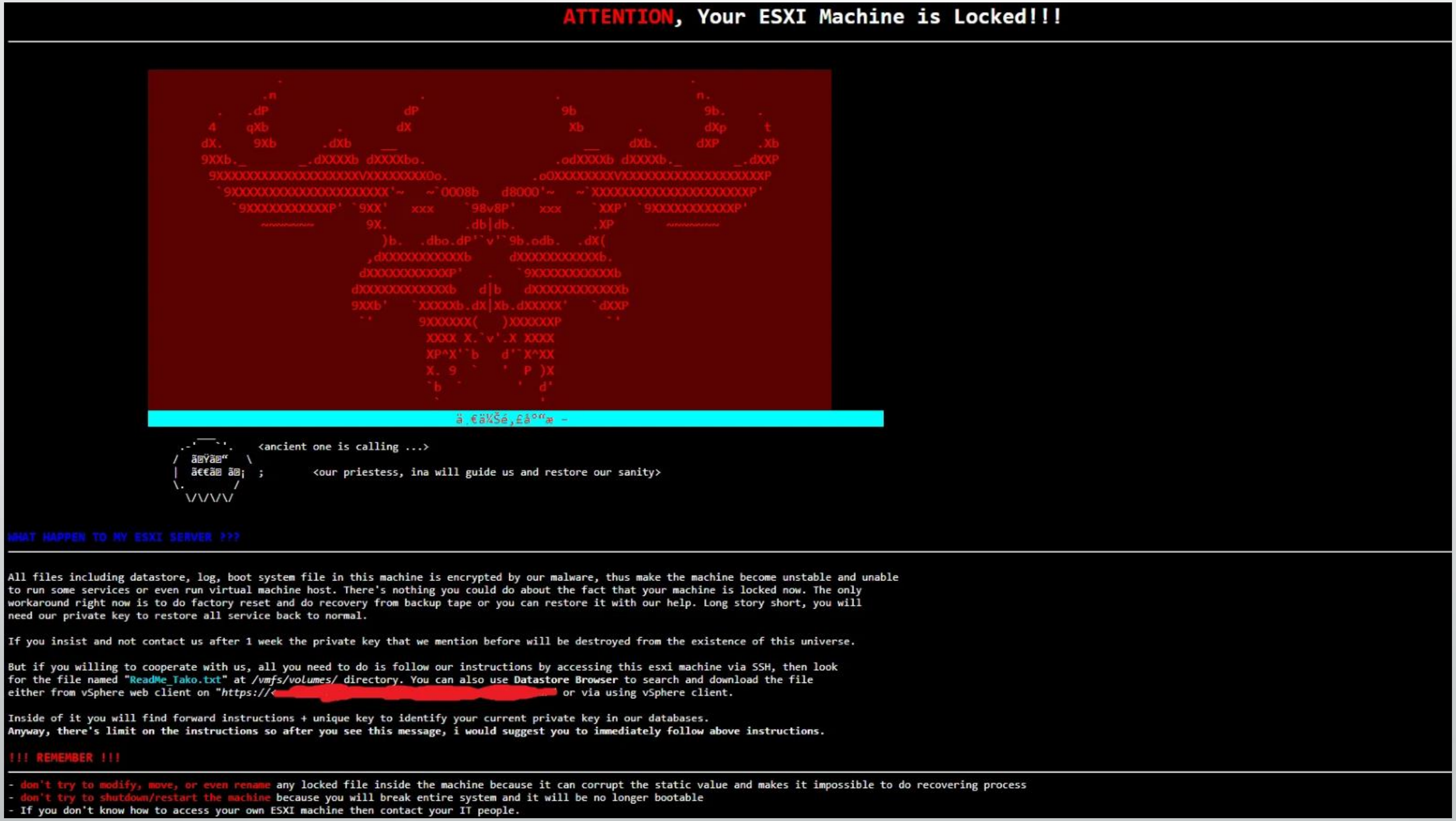
Leak 1 : Database 1 (WILL BE SOON)
Leak 2 : Database 2 (WILL BE SOON)

A .csv file with personal and work-related information



AI	AJ	AK	AL	AM	AN	AO	AP	AQ	AR	AS	AT	AU	A
Picture	SecretQuestion	SecretAnswer	CrewPortalUs	Nationality	License	ShowPersona	ShowPersona	ShowPersona	BirthCity	BirthState	BirthCountryI	NationalityCo	Qualifi
0xFFD8FFE0001	fine wine	J4KUdJ5ALYeEs	0	New Zealand	112233	0	0	0	Auckland	Auckland	131	131	NULL
0xFFD8FFE0001	test	Jk6az0RQ413u	0	New Zealand	112233	0	0	0	Auckland	Auckland	131	131	NULL
0xFFD8FFE0001	Crew0006	qNwW1ZJLSI9O	6	Malaysia	NULL	0	0	0	KUALA LUMPU	SELANGOR	224	224	NULL
0xFFD8FFE0001	Rating?	f51kkGv56rI4q	28	MALAYSIAN	NULL	0	0	0	MALACCA	MALACCA	224	224	NULL
	my name	XB/q6CnZAZVz	30	Malaysia	NULL	0	0	0	SANDAKAN	30	224	224	NULL
	Model	Hfs+amWAUa	32	MALAYSIAN	NULL	0	0	0	KUALA LUMPU	SELANGOR	224	224	NULL
NULL	NULL	NULL	51	Malaysia		0	0	0	N/A	N/A	224	224	NULL
0xFFD8FFE0001	mum's name	E9YckCidB3n4u	53	Malaysia	NULL	0	0	0	MUAR	53	224	224	NULL
0xFFD8FFE0001	Football team	K4tkjd500uPIfo	57	Malaysia	NULL	0	0	0	KOTA KINABA	SABAH	224	224	NULL
0xFFD8FFE0001	NULL	NULL	61	Malaysia		0	0	0	IPOH	PERAK	224	224	NULL
0xFFD8FFE0001	NULL	NULL	62	Malaysia		0	0	0	SHAH ALAM	SELANGOR	224	224	NULL
0xFFD8FFE0001	NULL	NULL	63	Malaysia		0	0	0	SEREMBAN	NEGERI SEMB	224	224	NULL
NULL	NULL	NULL	64	Malaysia		0	0	0	KOTA BAHRU	KELANTAN	224	224	NULL
	What is happiness ?	IKQEXcdfjowM	71	Malaysia	NULL	0	0	0	TAMPIN	NEGERI SEMB	224	224	NULL
0xFFD8FFE0001	NULL	NULL	73	Malaysia		0	0	0	SEREMBAN	NEGERI SEMB	224	224	NULL
0xFFD8FFE0001	daughter	OdQWk/9ttvk2	74	Malaysia		0	0	0	KOTA BAHRU	KELANTAN	224	224	NULL
0xFFD8FFE0001	NULL	NULL	80	Malaysia		0	0	0	SEREMBAN	NEGERI SEMB	224	224	NULL
0xFFD8FFE0001	Nina Beauty	pk6OPQ2wOH8	83	Malaysia	NULL	0	0	0	JOHOR BAHRU	JOHOR	224	224	NULL
0xFFD8FFE0001	service no	LI5m/AYvZB1H	93	Malaysia	NULL	0	0	0	KUALA LUMPU	WP KUALA LU	224	224	NULL
0xFFD8FFE0001	NULL	NULL	101	Malaysia		0	0	0	ALOR STAR	KEDAH	224	224	NULL
0xFFD8FFE0001	NULL	NULL	102	Malaysia		0	0	0	ALOR STAR	KEDAH	224	224	NULL
0xFFD8FFE0001	NULL	NULL	124	Malaysia		0	0	0	KUANTAN	PAHANG	224	224	NULL
NULL			10886	Malaysia		0	0	0	KUALA LUMPU	KUALA LUMPU	224	224	NULL
0xFFD8FFE0001	長男	ME3zv0gGXmn	127	Malaysia		0	0	0	GEORGE TOW	PENANG	224	224	NULL
0x89504E470D0	what is your dream ca	UskXE8U0mAa	161	MALAYSIA	NULL	0	0	0	JOHOR	MUAR	224	224	NULL
0xFFD8FFE0001	my car	oGKkM21IAzDY	186	Malaysia	NULL	0	0	0	SEREMBAN	Negeri Sembi	224	224	NULL
0xFFD8FFE0001	What your mother na	yioOPLwlhp/5c	188	Malaysia	NULL	0	0	0	KOTA BAHRU	KELANTAN	224	224	NULL
0xFFD8FFE0001	pet name	lj/8e3MwUekyV	189	Malaysia	NULL	0	0	0	GEORGETOW	PULAU PINAN	224	224	NULL
0xFFD8FFE0001	what's your car no	zWHle+WigZD	195	Malaysia	NULL	0	0	0	PENANG	PULAU PINAN	224	224	NULL
0xFFD8FFE0001	lapitop pw	7CEQr8Kr17mp	200	Malaysia	NULL	0	0	0	KUALA LUMPU	WILAYAH PER	224	224	NULL
0xFFD8FFE0001	NULL	NULL	201	Malaysia		0	0	0	SEREMBAN	NEGRI SEMBI	224	224	NULL
	Favorite food	0Aew+20nx5jv	208	Malaysian	NULL	0	0	0	Kuala Lumpur	Kuala Lumpur	224	224	NULL
0xFFD8FFE0001	boyfriend name	GNdITnfwCbgE	209	Malaysia	NULL	0	0	0	Teluk intan	Perak	224	224	NULL
0xFFD8FFE0001	what is your pets nam	+9n916VXL3Fs	237	Malaysia	NULL	0	0	0	KUALA LUMPU	SELANGOR	224	224	NULL
0xFFD8FFE0001	NULL	NULL	271	Malaysia		0	0	0	JOHOR BHARU	JOHOR	224	224	NULL
0xFFD8FFE0001	NULL	NULL	272	Malaysia		0	0	0	IPOH	PERAK	224	224	NULL
0xFFD8FFE0001	What is the favorite d	oM/83JNUlf6Mi	308	Malaysia		0	0	0	KOTA KINABA	SABAH	224	224	NULL
NULL	living camp	uzfCGoaWVy98	309	Malaysia	NULL	0	0	1	CHANGI	309	230	224	NULL
0xFFD8FFE0001	old car number ^	91vtCp33HCGn	313	Malaysia	NULL	0	0	0	KUALA LUMPU	313	224	224	NULL
0xFFD8FFE0001	hometown	fDl+j5TprMXito	X2344	Malaysia	NULL	0	0	0	KUALA LUMPU	WILAYAH PER	224	224	NULL
0xFFD8FFE0001	Daddy	DTqC40z+4Qj6	340	Malaysia	NULL	0	0	0	TAIPING	PERAK	224	224	NULL

An example screenshot of a ransomware affecting VMware ESXi machine



ATTENTION, Your ESXI Machine is Locked!!!

```
<ancient one is calling ...>

<our priestess, ina will guide us and restore our sanity>
```

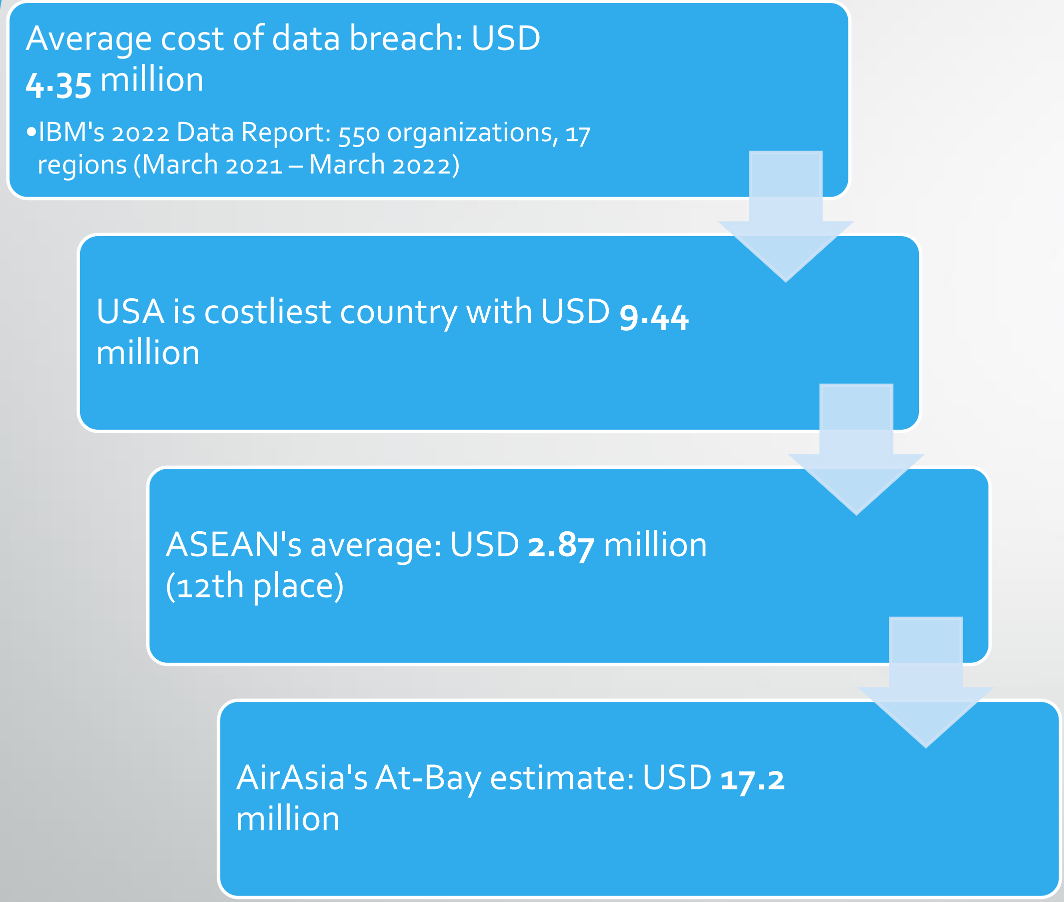
WHAT HAPPEN TO MY ESXI SERVER ???

```
All files including datastore, log, boot system file in this machine is encrypted by our malware, thus make the machine become unstable and unable
to run some services or even run virtual machine host. There's nothing you could do about the fact that your machine is locked now. The only
workaround right now is to do factory reset and do recovery from backup tape or you can restore it with our help. Long story short, you will
need our private key to restore all service back to normal.

If you insist and not contact us after 1 week the private key that we mention before will be destroyed from the existence of this universe.

But if you willing to cooperate with us, all you need to do is follow our instructions by accessing this esxi machine via SSH, then look
for the file named "ReadMe_Tako.txt" at /vmfs/volumes/ directory. You can also use Datastore Browser to search and download the file
either from vSphere web client on "https://[redacted] or via using vSphere client.

Inside of it you will find forward instructions + unique key to identify your current private key in our databases.
Anyway, there's limit on the instructions so after you see this message, i would suggest you to immediately follow above instructions.
```

!!! REMEMBER !!!

```
- don't try to modify, move, or even rename any locked file inside the machine because it can corrupt the static value and makes it impossible to do recovering process
- don't try to shutdown/restart the machine because you will break entire system and it will be no longer bootable
- If you don't know how to access your own ESXI machine then contact your IT people.
```

Financial Analysis



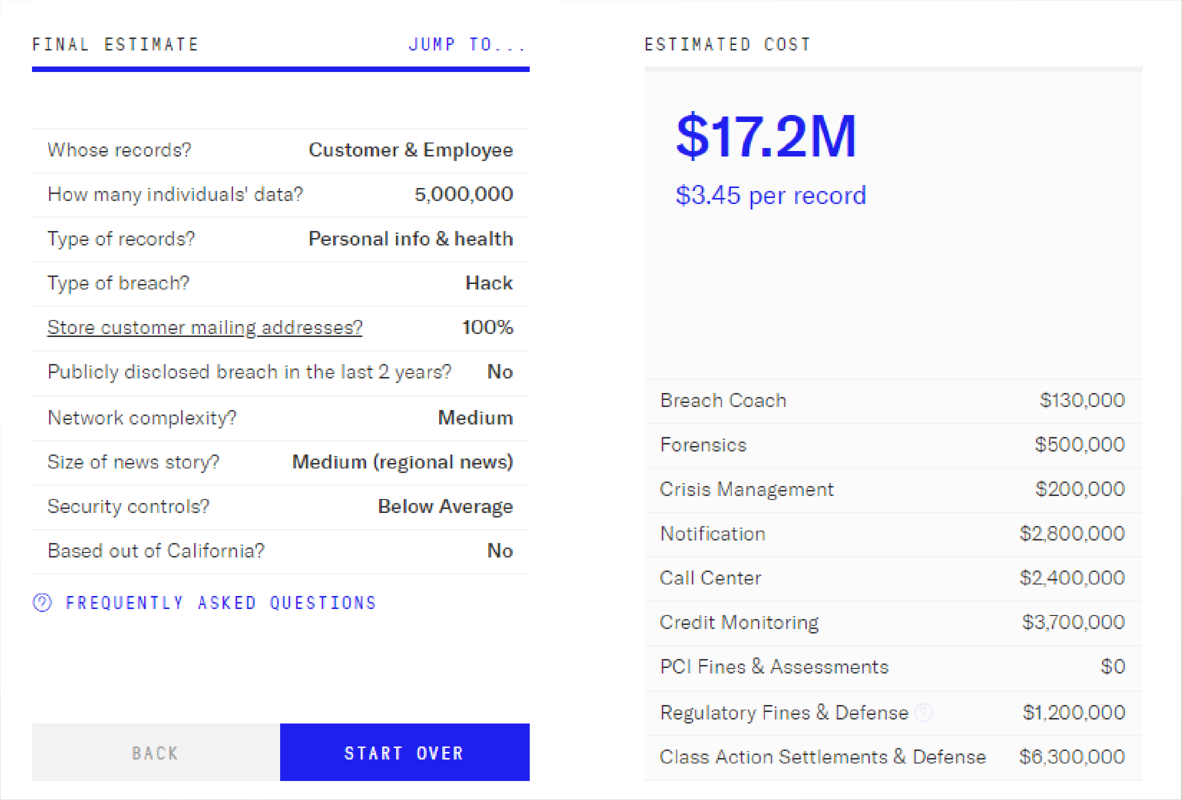
Average cost of data breach: USD **4.35** million

- IBM's 2022 Data Report: 550 organizations, 17 regions (March 2021 – March 2022)

USA is costliest country with USD **9.44** million

ASEAN's average: USD **2.87** million (12th place)

AirAsia's At-Bay estimate: USD **17.2** million



Whose records?	**Customer & Employee**
How many individuals' data?	5,000,000
Type of records?	**Personal info & health**
Type of breach?	**Hack**
Store customer mailing addresses?	100%
Publicly disclosed breach in the last 2 years?	**No**
Network complexity?	**Medium**
Size of news story?	**Medium (regional news)**
Security controls?	**Below Average**
Based out of California?	**No**

$17.2M

$3.45 per record

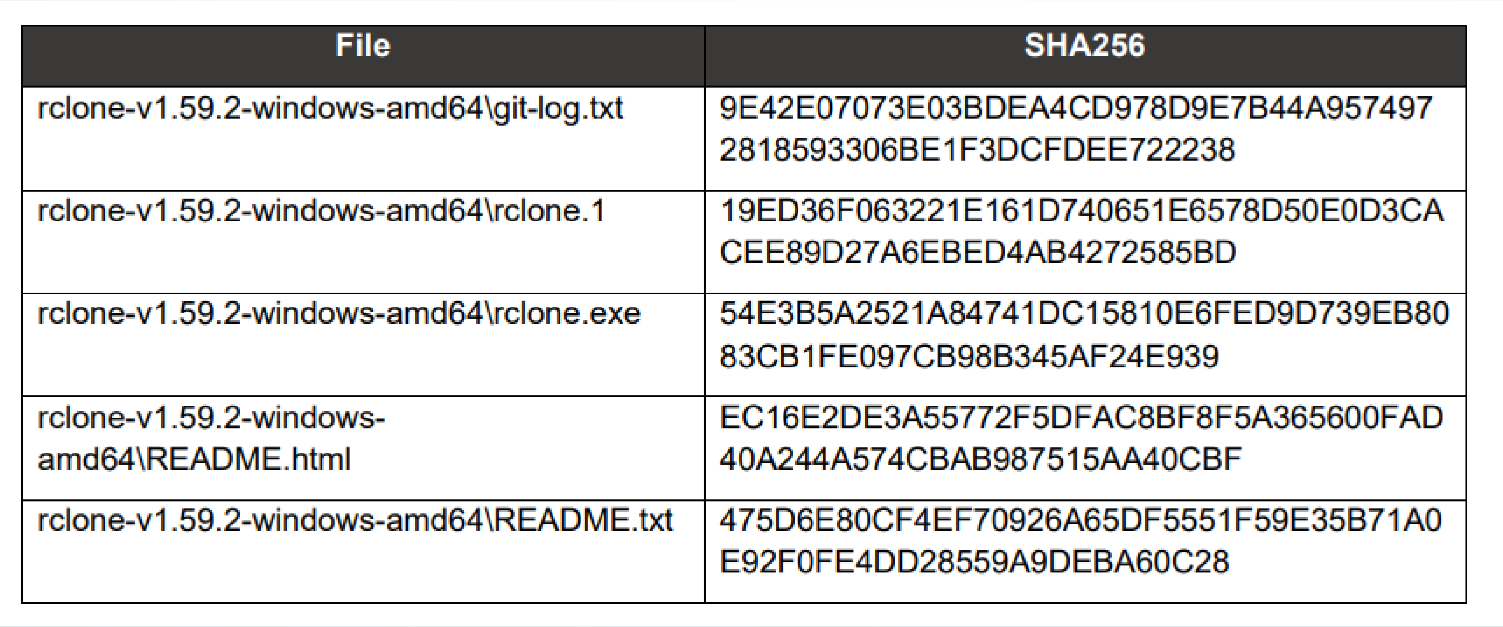
Breach Coach	$130,000
Forensics	$500,000
Crisis Management	$200,000
Notification	$2,800,000
Call Center	$2,400,000
Credit Monitoring	$3,700,000
PCI Fines & Assessments	$0
Regulatory Fines & Defense	$1,200,000
Class Action Settlements & Defense	$6,300,000

Detection and Prevention

- The CISA has the following recommendations:
  - Maintaining offline backups of data.
  - Creating and exercising an incident response plan.
  - Training employees to identifying phishing attacks.
- Updating software to the latest version helps patch vulnerabilities that threat actors can exploit.
  - Ex: Accellion FTA software deployed several patches following the first detected breach.
  - This includes ensuring that any software isn't at its end-of-life.

Detection and Prevention

- Cyberattacks can be detected by indicators of compromise (IoC).
  - The CISA released indicators of compromise connected to Daixin attacks.
  - Helps prevent or mitigate attacks early.



File	SHA256
rclone-v1.59.2-windows-amd64\git-log.txt	9E42E07073E03BDEA4CD978D9E7B44A9574972818593306BE1F3DCFDEE722238
rclone-v1.59.2-windows-amd64\rclone.1	19ED36F063221E161D740651E6578D50E0D3CACEE89D27A6EBED4AB4272585BD
rclone-v1.59.2-windows-amd64\rclone.exe	54E3B5A2521A84741DC15810E6FED9D739EB8083CB1FE097CB98B345AF24E939
rclone-v1.59.2-windows-amd64\README.html	EC16E2DE3A55772F5DFAC8BF8F5A365600FAD40A244A574CBAB987515AA40CBF
rclone-v1.59.2-windows-amd64\README.txt	475D6E80CF4EF70926A65DF5551F59E35B71A0E92F0FE4DD28559A9DEBA60C28

IoCs related to Daixin team attacks, available in a CISA/FBI cybersecurity advisory.

Countermeasures and solutions

- **Zero Trust approach:**
- **Patch Management:**
- **Regular vulnerability assessments:**
- **Employee training :**
- **Implement multi-factor authentication (MFA):**
- **Data encryption:**
- **Third-party risk management**
- **Incident response planning:**

Thank you

- Adam MacDougall,
- Thomas Matejek
- Madhu Nepal
- Mehmet Ozmen
- Chris Panczak
- Chandra Rawat
- Shavaughn Robinson