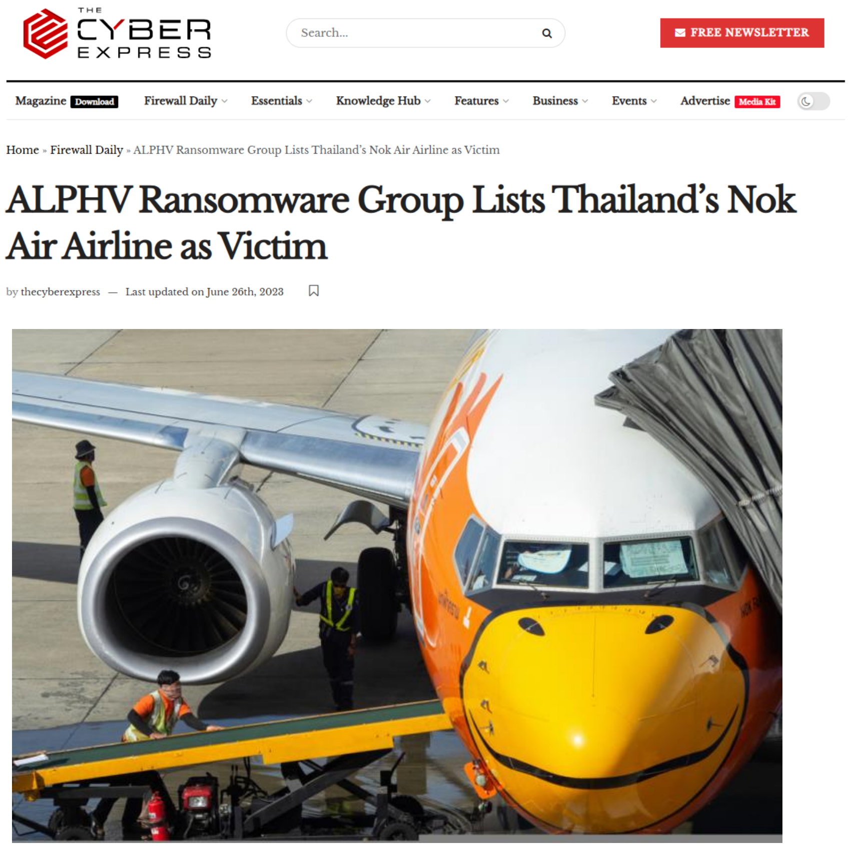
SANGFOR

DEEP INSIGHT INTO CYBER SECURITY

Apt attacks more successful why?

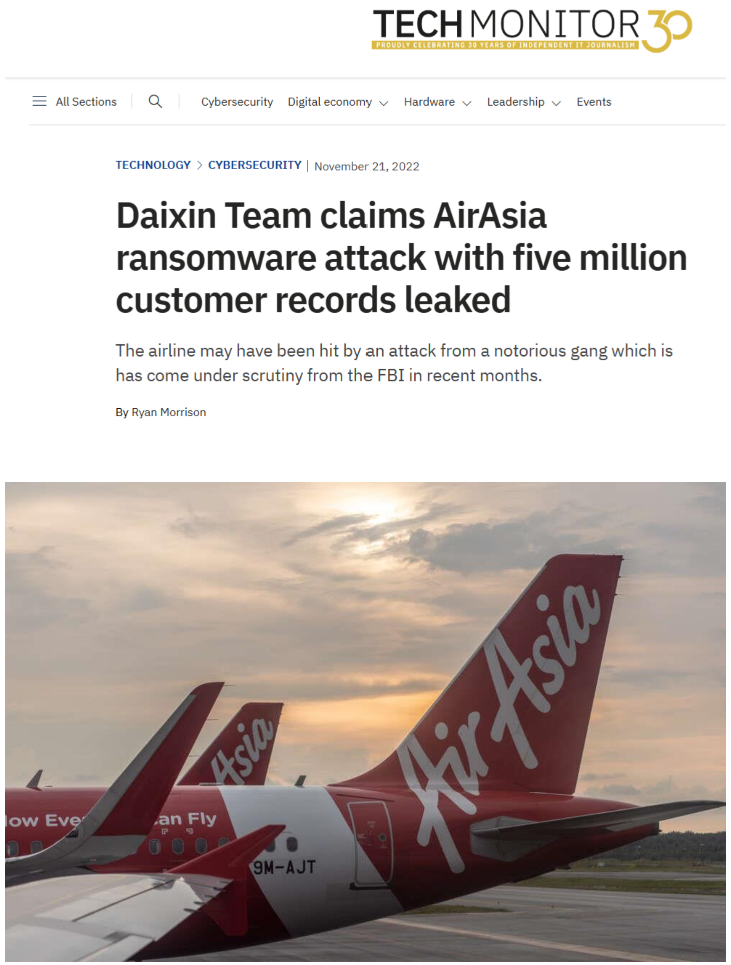


THE CYBER EXPRESS

Home » Firewall Daily » ALPHV Ransomware Group Lists Thailand's Nok Air Airline as Victim

ALPHV Ransomware Group Lists Thailand's Nok Air Airline as Victim

by thecyberexpress — Last updated on June 26th, 2023



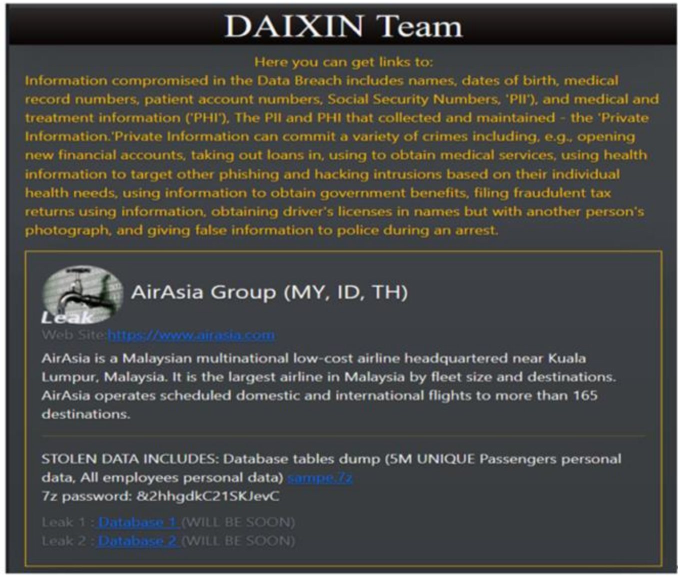
TECHMONITOR 30
PROUDLY CELEBRATING 30 YEARS OF INDEPENDENT IT JOURNALISM

TECHNOLOGY > CYBERSECURITY | November 21, 2022

Daixin Team claims AirAsia ransomware attack with five million customer records leaked

The airline may have been hit by an attack from a notorious gang which is has come under scrutiny from the FBI in recent months.

By Ryan Morrison



DAIXIN Team

Here you can get links to:

Information compromised in the Data Breach includes names, dates of birth, medical record numbers, patient account numbers, Social Security Numbers, 'PII'), and medical and treatment information ('PHI'), The PII and PHI that collected and maintained - the 'Private Information.'Private Information can commit a variety of crimes including, e.g., opening new financial accounts, taking out loans in, using to obtain medical services, using health information to target other phishing and hacking intrusions based on their individual health needs, using information to obtain government benefits, filing fraudulent tax returns using information, obtaining driver's licenses in names but with another person's photograph, and giving false information to police during an arrest.

Leak

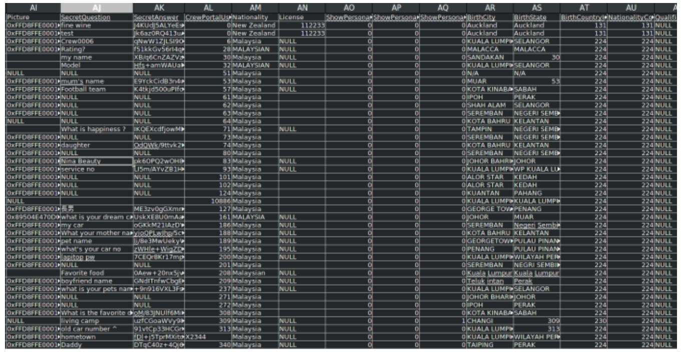
AirAsia Group (MY, ID, TH)

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)



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	BirthCountry	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 LUMP	SELANGOR	224	224	NULL
0xFFD8FFE0001	Rating?	f51kkGv56rl4q	28	MALAYSIAN	NULL	0	0	0	MALACCA	MALACCA	224	224	NULL
	my name	XB/q6CnZAZVa	30	Malaysia	NULL	0	0	0	SANDAKAN	30	224	224	NULL
	Model	Hfs+amWAUa	32	MALAYSIAN	NULL	0	0	0	KUALA LUMP	SELANGOR	224	224	NULL
NULL	NULL	NULL	51	Malaysia		0	0	0	N/A	N/A	224	224	NULL
0xFFD8FFE0001	mum's name	E9YckCidB3n4	53	Malaysia	NULL	0	0	0	MUAR	53	224	224	NULL
0xFFD8FFE0001	Football team	K4tkjd500uPlfo	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	pk6OPQ2wOH	83	Malaysia	NULL	0	0	0	JOHOR BAHRU	JOHOR	224	224	NULL
0xFFD8FFE0001	service no	Ll5m/AYvZB1H	93	Malaysia	NULL	0	0	0	KUALA LUMP	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 LUMP	KUALA LUMP	224	224	NULL
0xFFD8FFE0001	長男	ME3zv0gGXmn	127	Malaysia		0	0	0	GEORGE TOW	PENANG	224	224	NULL
0x89504E470D0	what is your dream c	UskXE8U0mAa	161	MALAYSIA	NULL	0	0	0	JOHOR	MUAR	224	224	NULL
0xFFD8FFE0001	my car	oGKkM21lAzD	186	Malaysia	NULL	0	0	0	SEREMBAN	Negeri Semb	224	224	NULL
0xFFD8FFE0001	What your mother na	yjoQPLwlhp/5c	188	Malaysia	NULL	0	0	0	KOTA BAHRU	KELANTAN	224	224	NULL
0xFFD8FFE0001	pet name	lj/8e3MwUeky	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 LUMP	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	GNdlTnfwCbgE	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 LUMP	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	uzfCGoaWVy9	309	Malaysia	NULL	0	0	1	CHANGI	309	230	224	NULL
0xFFD8FFE0001	old car number ^	91vtCp33HCGr	313	Malaysia	NULL	0	0	0	KUALA LUMP	313	224	224	NULL
0xFFD8FFE0001	hometown	fDl+j5TprMXit	X2344	Malaysia	NULL	0	0	0	KUALA LUMP	WILAYAH PER	224	224	NULL
0xFFD8FFE0001	Daddy	DTqC40z+4Qj	340	Malaysia	NULL	0	0	0	TAIPING	PERAK	224	224	NULL

Introduction

In 2023, generative artificial intelligence and various large models were rapidly applied in cyber attacks and defenses, bringing new attack and defense scenarios and security threats.

"As is often the case when we move rapidly towards new IT setups, security is an afterthought, Existing security tools were not designed with GPT in mind."

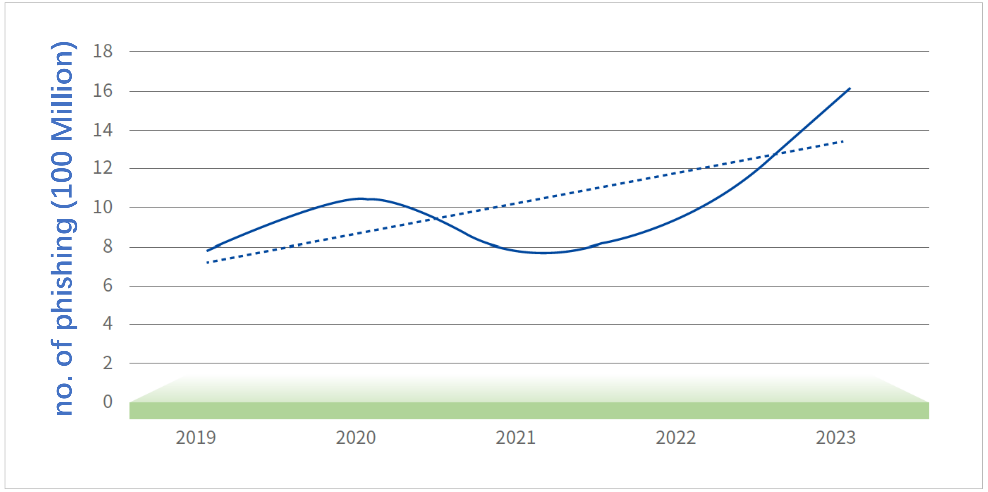
GPT Security Risk

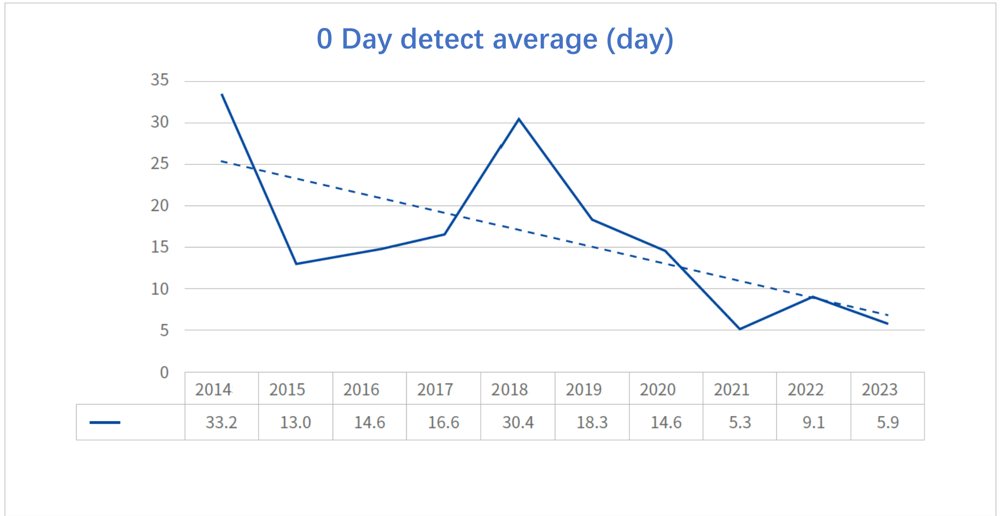
It is happening now

AI-Generated Phishing Scams

Duping ChatGPT into Writing Malicious Code

OpenAI

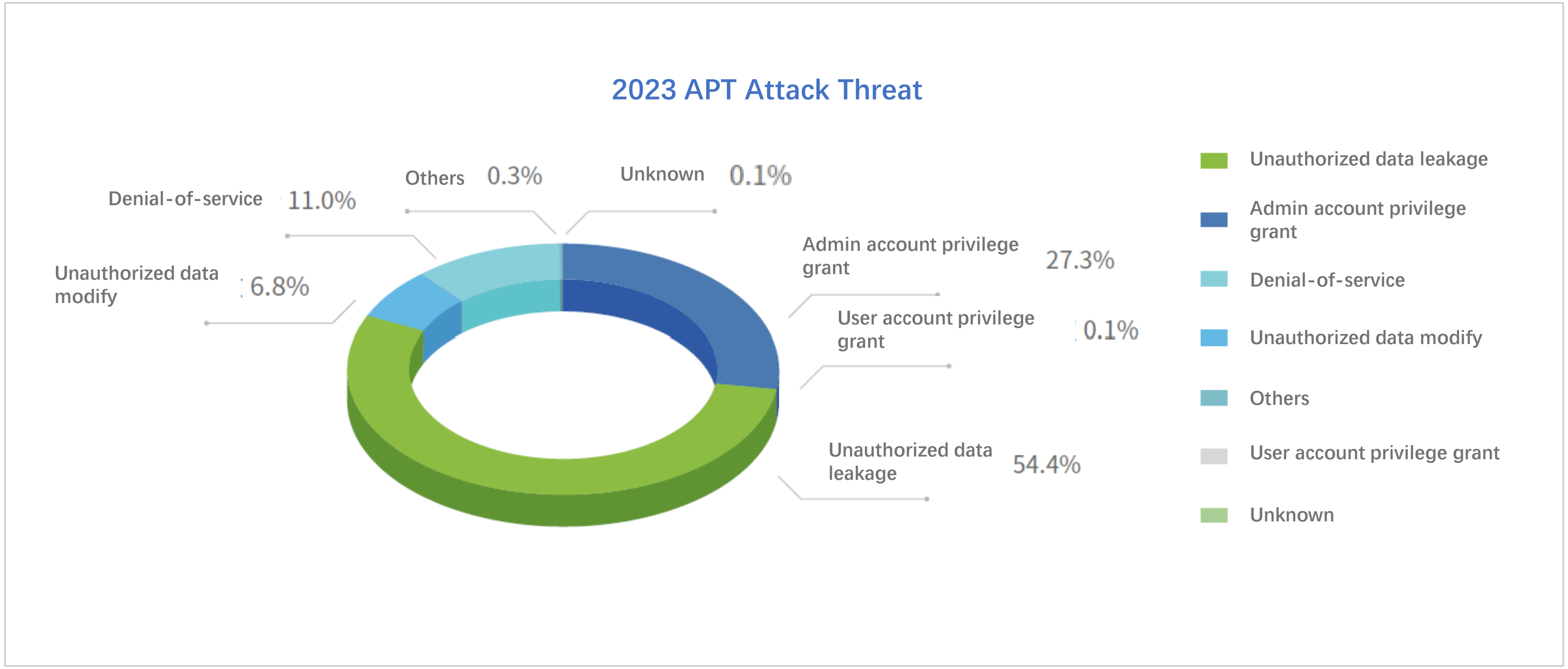




	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
—	33.2	13.0	14.6	16.6	30.4	18.3	14.6	5.3	9.1	5.9

APT Attack Trend

- The APT organization is becoming more sophisticated in social engineering of phishing attacks, and the bait they produce is becoming more deceptive.
- Supply chain attacks have become a popular way for APT organizations to gain initial permissions.
- Open source components are widely used in APT attacks to reduce attack costs and the effect of attack traceability.
- BYOVD technology is widely used in various major APT attack activities.



Advisory for against attack

Experienced Security Professionals

- Continuous analysis and identification
- Timely and relevant alerting
- Context-relevant advisory and guidance
- Actionable response drawing from experience
- Proven processes and procedures

State-of-the-art detection capabilities

- Powered by artificial intelligence
- Machine learning algorithms
- User and entity behavior analytics
- Global threat intelligence
- Intuitive security platform built and improved to delivery value

- Leverage advanced technology to detect different types of threats
- Inject professional “scepticism” and logic to better analyse and evaluate impact
- Provide practical, context-relevant response assistance for more effective remediation

SANGFOR

Thank you