Insurer AXA hit by ransomware after dropping support for ransom payments

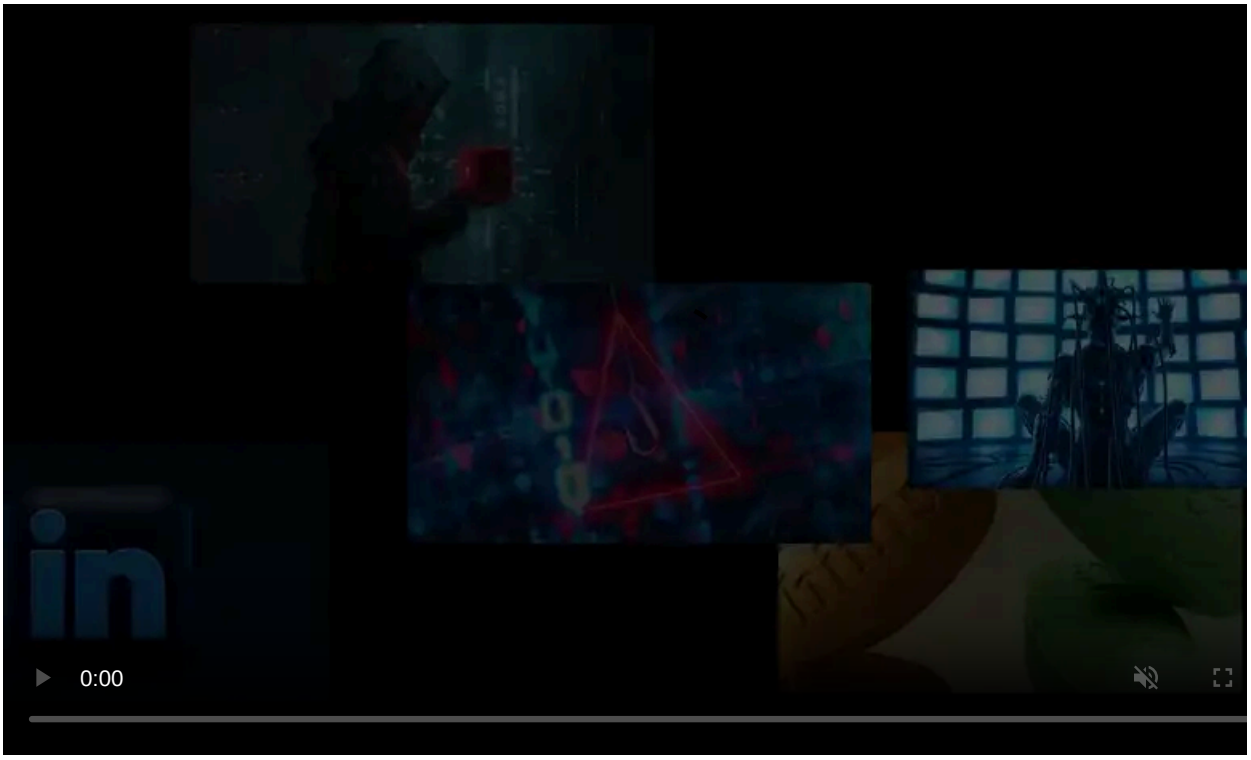
By Ax Sharma

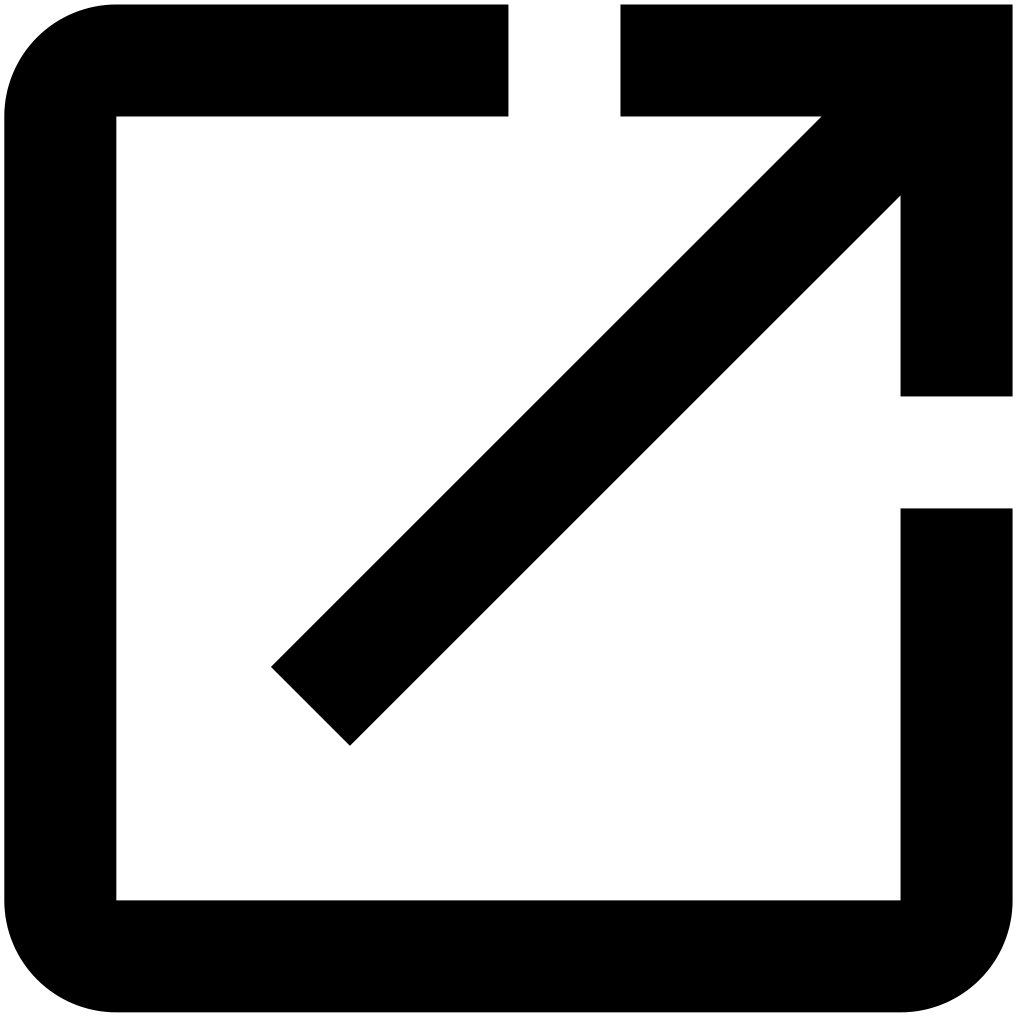
Published: 2021-05-16 · Archived: 2026-04-05 18:10:56 UTC

Branches of insurance giant AXA based in Thailand, Malaysia, Hong Kong, and the Philippines have been struck by a ransomware cyber attack.

As seen by BleepingComputer yesterday, the Avaddon ransomware group claimed on their leak site that they had stolen 3 TB of sensitive data from AXA's Asian operations.

Additionally, BleepingComputer observed an ongoing Distributed Denial of Service (DDoS) against AXA's global websites making them inaccessible for some time yesterday.


0:00



The compromised data obtained by Avaddon, according to the group, includes customer medical reports (exposing their sexual health diagnosis), copies of ID cards, bank account statements, claim forms, payment records, contracts, and more.

The announcement from the group comes roughly a week after AXA stated that they would be dropping reimbursement for ransomware extortion payments when underwriting cyber-insurance policies in France.

Ransomware group hits AXA's Asian offices

Yesterday, the Avaddon ransomware group claimed responsibility for attacking Asia-based branches of insurance giant AXA.

Additionally, the group claimed that AXA's websites based in Thailand, Malaysia, Hong Kong, and the Philippines were subject to an active DDoS attack:

AXA's Asia-based websites were timing out yesterday when accessed by BleepingComputer

The Avaddon ransomware gang first announced in January 2021 that they will launch DDoS attacks to take down victims' sites or networks until they reach out and begin negotiating to pay the ransom.

BleepingComputer first reported about this new trend in October 2020, when ransomware groups began using DDoS attacks against their victims as an additional leverage point.

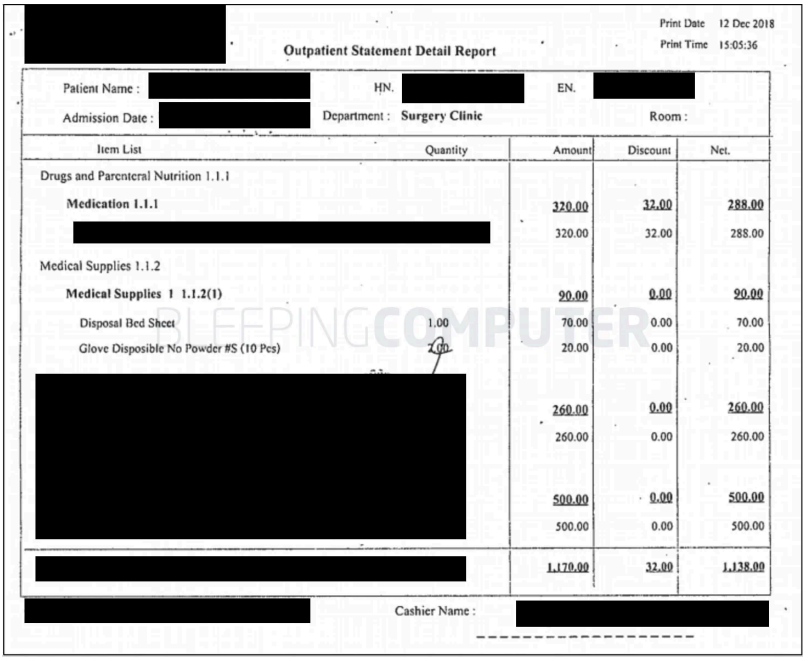
Avaddon's announcement of the attack on AXA's systems comes roughly a week after AXA had stated that their cyber-insurance policies written in France would no longer include reimbursement for ransomware extortion payouts.

Although the exact date of the attack is unknown, Avaddon began leaking some of the stolen data on their leak site yesterday, as seen by BleepingComputer.

Avaddon also threatened AXA that the insurance company had about ten days to communicate and cooperate with them, after which they would leak AXA's valuable documents.

The group claims to have obtained 3 TB of data belonging to AXA including:

- customer medical reports (including those containing sexual health diagnosis)
- customer claims
- payments to customers
- customers' bank account scanned documents
- material restricted to hospitals and doctors (private fraud investigations, agreements, denied reimbursements, contracts)
- Identification documents such as National ID cards, passports, etc.



[redacted]

Outpatient Statement Detail Report

Print Date 12 Dec 2018
Print Time 15:05:36

Patient Name : [redacted] HN. [redacted] EN. [redacted]
Admission Date : [redacted] Department : Surgery Clinic Room :

Item List	Quantity	Amount	Discount	Net.
Drugs and Parenteral Nutrition 1.1.1				
Medication 1.1.1		320.00	32.00	288.00
[redacted]		320.00	32.00	288.00
Medical Supplies 1.1.2				
Medical Supplies 1 1.1.2(1)		90.00	0.00	90.00
Disposal Bed Sheet	1.00	70.00	0.00	70.00
Glove Disposible No Powder #S (10 Pcs)	1.00	20.00	0.00	20.00
[redacted]		260.00	0.00	260.00
		260.00	0.00	260.00
		500.00	0.00	500.00
		500.00	0.00	500.00
[redacted]		1,170.00	32.00	1,138.00

[redacted] Cashier Name : [redacted]

Medical bill for a patient leaked by the group
Source: BleepingComputer

AXA: 'No evidence' data beyond a Thai partner accessed

When contacted by BleepingComputer, AXA said:

"Asia Assistance was recently the victim of a targeted ransomware attack which impacted its IT operations in Thailand, Malaysia, Hong Kong, and the Philippines."

"As a result, certain data processed by Inter Partners Assistance (IPA) in Thailand has been accessed."

"At present, there is no evidence that any further data was accessed beyond IPA in Thailand."

"A dedicated taskforce with external forensic experts is investigating the incident. Regulators and business partners have been informed. "

"AXA takes data privacy very seriously and if IPA's investigations confirms that sensitive data of any individuals have been affected, the necessary steps will be taken to notify and support all corporate clients and individuals impacted," an AXA spokesperson told BleepingComputer.

The timing around the incident is noteworthy considering, this week, the Federal Bureau of Investigation (FBI) and the Australian Cyber Security Centre (ACSC) had warned of ongoing Avaddon ransomware attacks targeting organizations from an extensive array of sectors in the US and worldwide.

Ransomware attacks on organizations continue to grow and cause disruptions for many with attackers demanding exorbitant ransom payments.

Recently, the DarkSide cybercrime group demanded $5 million to restore Colonial Pipeline system operations.

And, just this week, BleepingComputer reported on Ireland's Health Services hit with a $20 million ransomware demand.

AXA has not yet commented on the ransom amount demanded by Avaddon.

Source: https://www.bleepingcomputer.com/news/security/insurer-axa-hit-by-ransomware-after-dropping-support-for-ransom-payments/