US aerospace services provider breached by Maze Ransomware

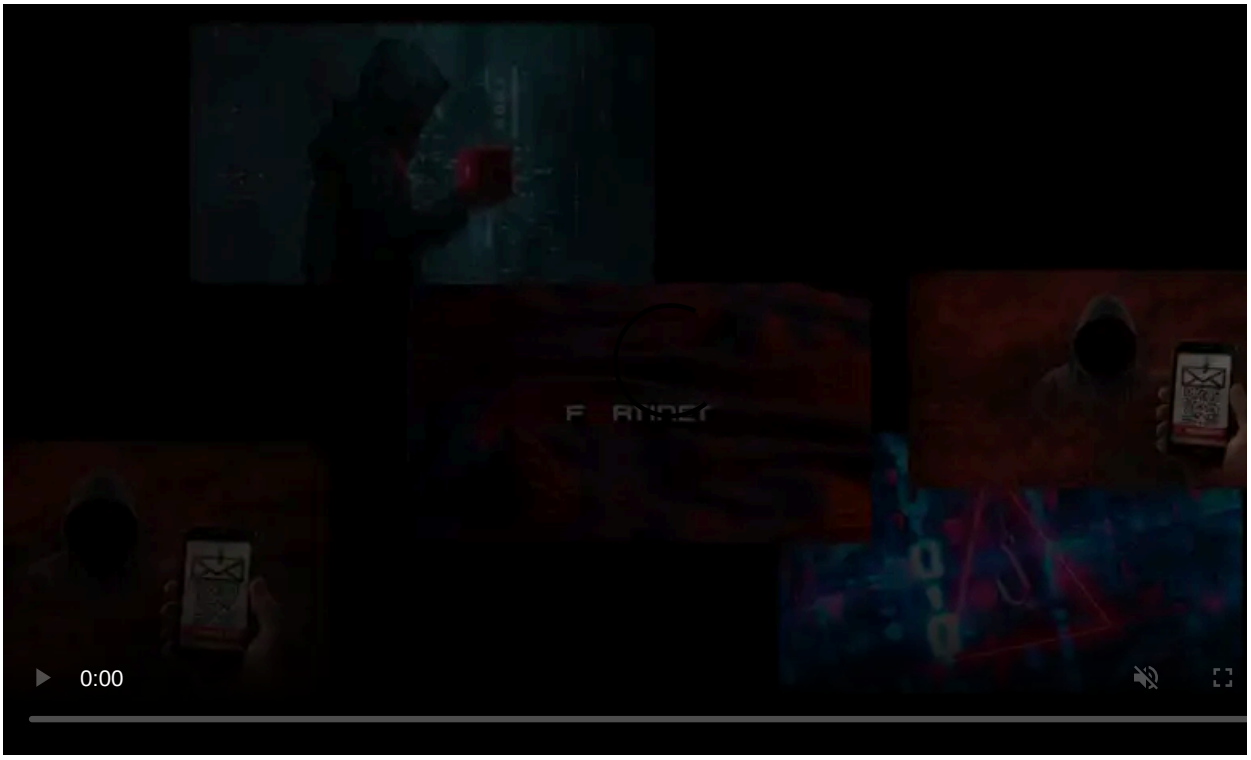
By Sergiu Gatlan

Published: 2020-06-05 · Archived: 2026-04-05 21:27:33 UTC

The Maze Ransomware gang breached and successfully encrypted the systems of VT San Antonio Aerospace, as well as stole and leaked unencrypted files from the company's compromised devices in April 2020.

VT San Antonio Aerospace (VT SAA) is a leading North American aircraft MRO (maintenance, repair, and overhaul) service provider specialized in airframe maintenance repair and overhaul, line maintenance, aircraft modifications, and aircraft engineering services.

VT SAA is a subsidiary of ST Engineering (part of ST Aerospace, its aerospace arm), one of the largest firms listed on the Singapore Exchange and an engineering group with customers in the defense, government, and commercial segments in over 100 countries, and roughly 23,000 people across Asia, Europe, Middle East, and the United States.

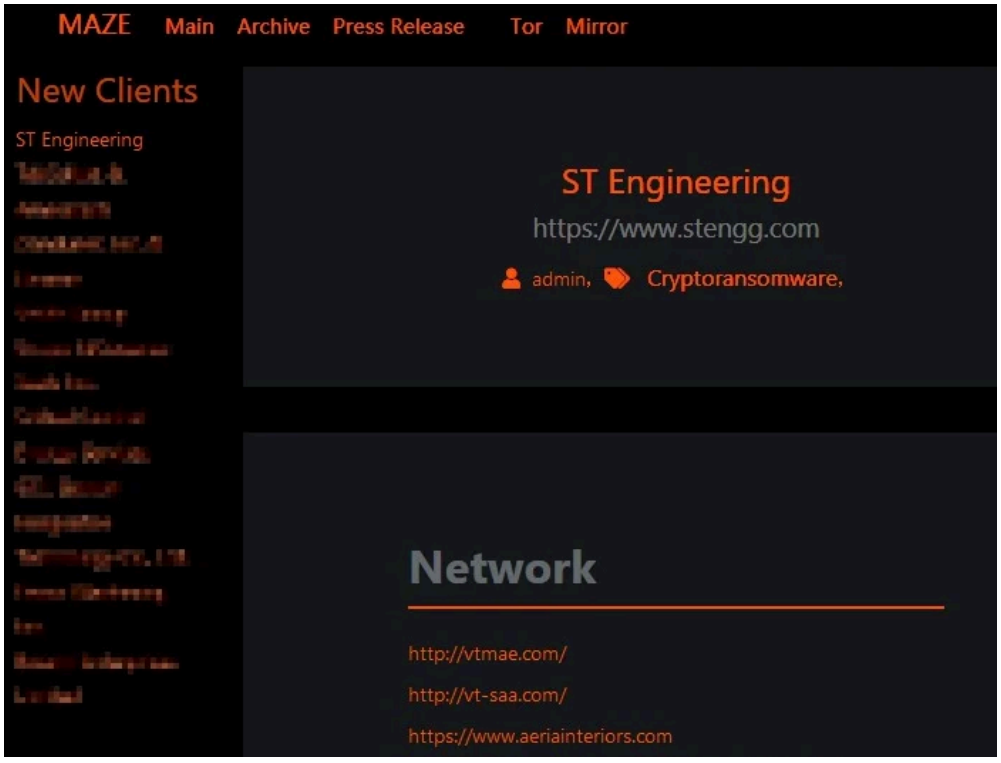

0:00

ST Aerospace provides repair and overhaul services for more than 25,000 mechanical and avionics component types fitted on various Airbus and Boeing aircraft and helicopters.

Maze encrypted VT SAA's network

The Maze Ransomware operators state in a new post on their data leak site that they breached the network of ST Engineering—actually that of VT SAA, one of the group's North American subsidiaries—stealing data and encrypting servers.

During the attack, before deploying the ransomware payload to encrypt the company's servers, Maze claims to have stolen 1.5 TB worth of unencrypted files to be used as leverage to pressure the ST Engineering subsidiary into paying their ransom.



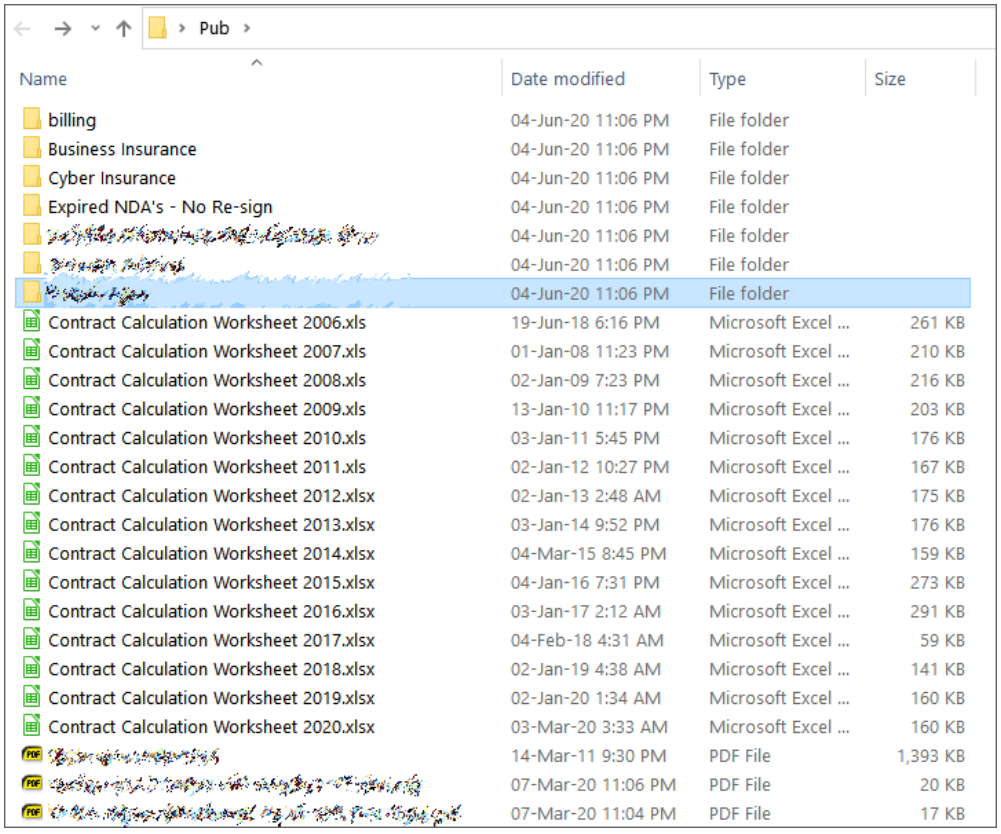
ST Engineering entry on Maze leak site

As 'proof' that they breached VT SAA's network, Maze has already leaked over 100 documents that consist of financial spreadsheets, cyber insurance contracts, proposals, and expired NDAs.

We were told that these files allegedly include financial information, "IT security systems" information, and how ST Engineering financially supports political groups in countries in Latin America and CIS. Maze did not provide any proof of these claims.

Stealing files from their victims' network before deploying the ransomware payload is a common procedure for the Maze Ransomware operators.

Other ransomware operators including but not limited to REvil, DoppelPaymer, Nemty, Netwalker, and CLOP have also adopted this extortion tactic.



Leaked files

BleepingComputer has also been told that VT SAA's cyber insurance contracts are with Chubb, who was also attacked by the Maze Ransomware operators and had its network encrypted in March 2020.

Bad Packets said at the time that Chubb had numerous Citrix ADC (Netscaler) servers unpatched against the CVE-2019-19871 vulnerability despite the insurance carrier's statement that its network was not compromised (this security flaw was exploited in the past as part of other ransomware attacks).

Details of Maze's attack

While Maze has not described details of their attack, they leaked the IT Manager's memorandum of the cyberattack memo which shows exactly how the attack occurred.

Maze first connected to one of VT SAA's servers via a remote desktop connection using a compromised Administrator account, then compromised the default Domain Administrator account and hit the company's domain controllers, intranet servers, and file servers on two domains.

The memo also says that all the encrypted systems were fully recovered within three days after VT SAA's systems were encrypted by Maze Ransomware on March 7, 2020.

Because of the number of files and the sensitive nature of the stolen data Maze has already posted on their leak site, ST Engineering Aerospace subsidiary will have to also disclose this incident as a data breach to all affected parties, including employees and clients.

System(S) and/or Data Affected:

- [redacted] DOMAIN
  - [redacted] – The only non-server infected computer
  - [redacted] – Domain Controller.
    - All User Profiles
    - SYSVOL
    - SCRIPTS
    - InetPub for CA Role
  - [redacted] – Intranet Server. No public hosting.
    - All user Profiles
    - All IIS Folders – InetPub, FTPRoot
  - [redacted] – Filer Server
    - All User Profiles
    - First five share folders. About 5% of over all datastore.
  - [redacted] – Backup Server
    - Arcserve Datastore share only. Server not directly compromised.
- [redacted] Domain
  - [redacted]: main file server
  - [redacted]: main domain controller

Affected systems and data

ST Engineering North America only partially affected by the attack

In a statement to BleepingComputer, VT San Antonio Aerospace Vice President and General Manager Ed Onwe said that the attack only affected a limited number of ST Engineering's U.S. commercial operations.

"VT San Antonio Aerospace discovered that a sophisticated group of cyber criminals, known as the Maze group, gained unauthorized access to our network and deployed a ransomware attack. At this point, our ongoing investigation indicates that the threat has been contained and we believe it to be isolated to a limited number of ST Engineering's U.S. commercial operations. Currently, our business continues to be operational," Onwe told BleepingComputer.

"Upon discovering the incident, the Company took immediate action, including disconnecting certain systems from the network, retaining leading third-party forensic advisors to help investigate and notifying appropriate law enforcement authorities.

"As part of this process, we are conducting a rigorous review of the incident and our systems to ensure that the data we are entrusted with remains safe and secure. This includes deploying advanced tools to remediate the intrusion and to restore systems. We are also taking steps to further strengthen the Company's overall cybersecurity architecture."

Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
