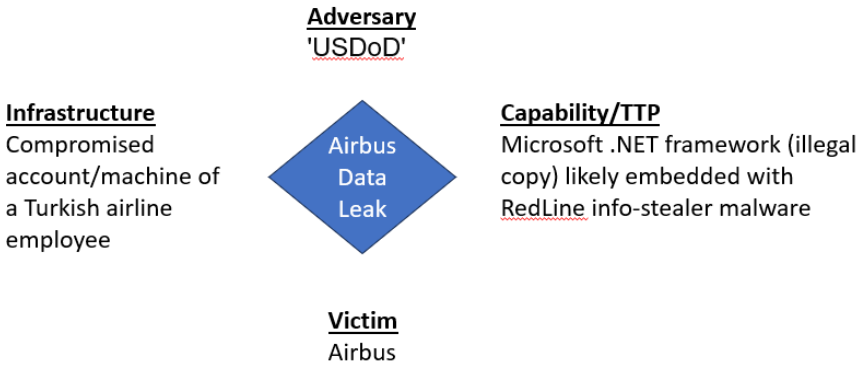
Summary Report



Date	September 2023
Incident	Data Breach
Actor	"USDoD"; could be linked to "Ransomed" ransomware group
Motivation	Possibly financial gain or desire for notoriety
Attack Vector	An employee of a Turkish airline downloaded an illegal copy of Microsoft .NET framework, resulting in the spread of the RedLine info-stealer malware. Credential(s) obtained from infected system(s) was used as initial attack vector into Airbus website.
Impact	Compromise of personal data of 3,200 individuals associated with **Airbus vendors (E.g. Thales and Rockwell Collins)** such as names, phone numbers, and email addresses, addresses and job titles
Lesson to be learnt	**It is recommended for organisations to restrict unauthorised software downloads by their employees and prohibit the use of pirated software in organisational assets.** **It is recommended for internet facing web application to have multi-factor authentication (MFA) to make it difficult for adversary to gain access even with stolen credentials.**
Associated Threats	- **Increased in threat actor interests in using information stealing malware often observed distributed via downloads masquerading as cracked or legitimate software installers** - **Information-stealing malware typically gathers huge number of credentials from infected machines, and malware operator may sell the credentials to other threat actors** - **RedLine info-stealer malware has been advertised for sale on underground forums** - **Leaked personal data can be leveraged for malicious activities such as business email compromise (BEC) and phishing**
Other Information	- "USDoD" previously sold FBI's InfraGard database on a forum called "Breached" in December 2022, leading to the seizure of the forum by law enforcement. The new forum where the Airbus data breach is posted is "breachforums[.]is". - "USDoD" announced in the forum their intention to target Lockheed Martin and Raytheon in future attacks - "Ransomed" is a relatively new ransomware group that is rapidly gaining prominence, proudly claiming on Twitter to have targeted a number of companies with ransomware attacks in September 2023
References	- https://cybersecuritynews.com/airbus-cyber-attack/

	- https://www.hudsonrock.com/blog/an-avoidable-breach-fbi-hacker-leaks-sensitive-airbus-data - https://thecyberexpress.com/airbus-cyber-attack-usdod-turkish-airlines/ - Close source intel