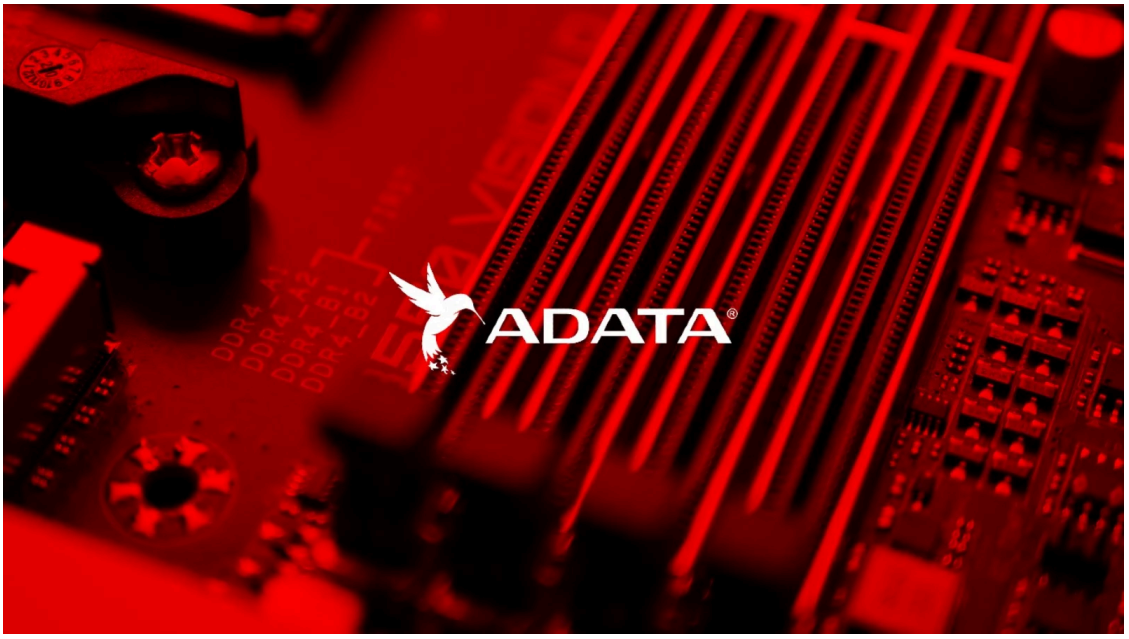
Computer memory maker ADATA hit by Ragnar Locker ransomware

By Sergiu Gatlan

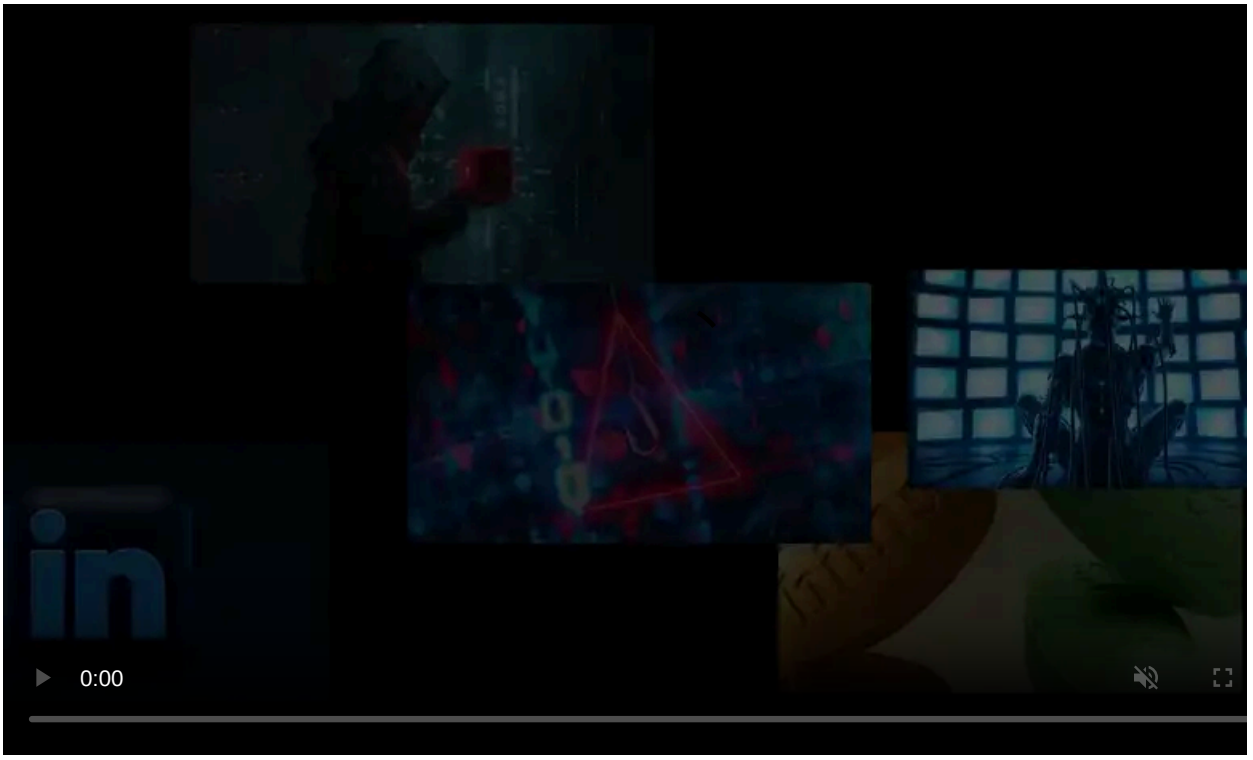
Published: 2021-06-08 · Archived: 2026-04-05 17:43:47 UTC

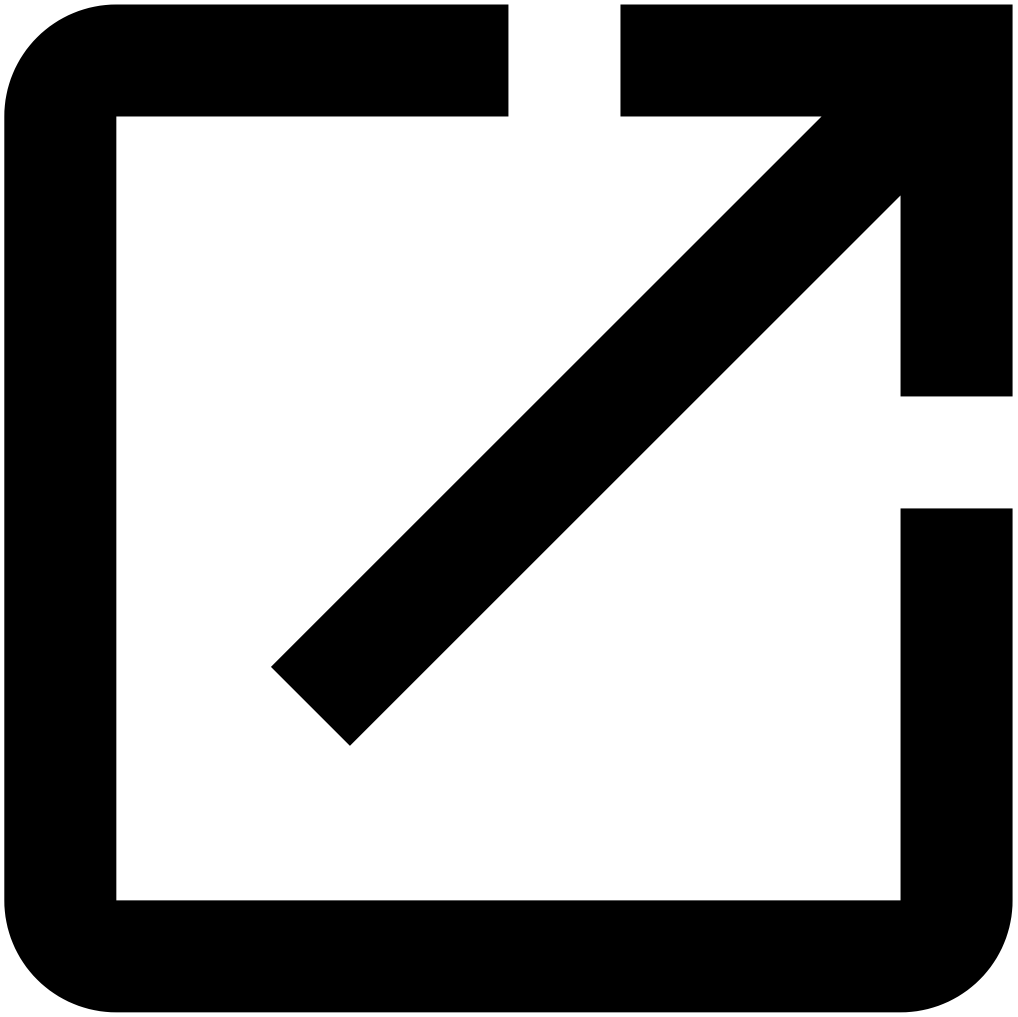


Taiwan-based leading memory and storage manufacturer ADATA says that a ransomware attack forced it to take systems offline after hitting its network in late May.

ADATA manufactures high-performance DRAM memory modules, NAND Flash memory cards, and other products, including mobile accessories, gaming products, electric power trains, and industrial solutions.

The company was ranked as the second-largest DRAM memory and solid-state drives (SSD) maker in 2018.


0:00



ADATA confirms May ransomware attack

The Taiwanese memory manufacturer took down all impacted systems after detecting the attack and notified all relevant international authorities of the incident to help track down the attackers.

"ADATA was hit by a ransomware attack on May 23rd, 2021," the company told BleepingComputer in an email statement today.

ADATA's business operations are no longer disrupted according to the memory maker, with affected devices being restored and services closing regular performance.

"The company successfully suspended the affected systems as soon as the attack was detected, and all following necessary efforts have been made to recover and upgrade the related IT security systems," ADATA added.

"Gladly things are being moved toward the normal track, and business operations are not disrupted for corresponding contingency practices are effective.

"We are determined to devote ourselves making the system protected than ever, and yes, this will be our endless practice while the company is moving forward to its future growth and achievements."

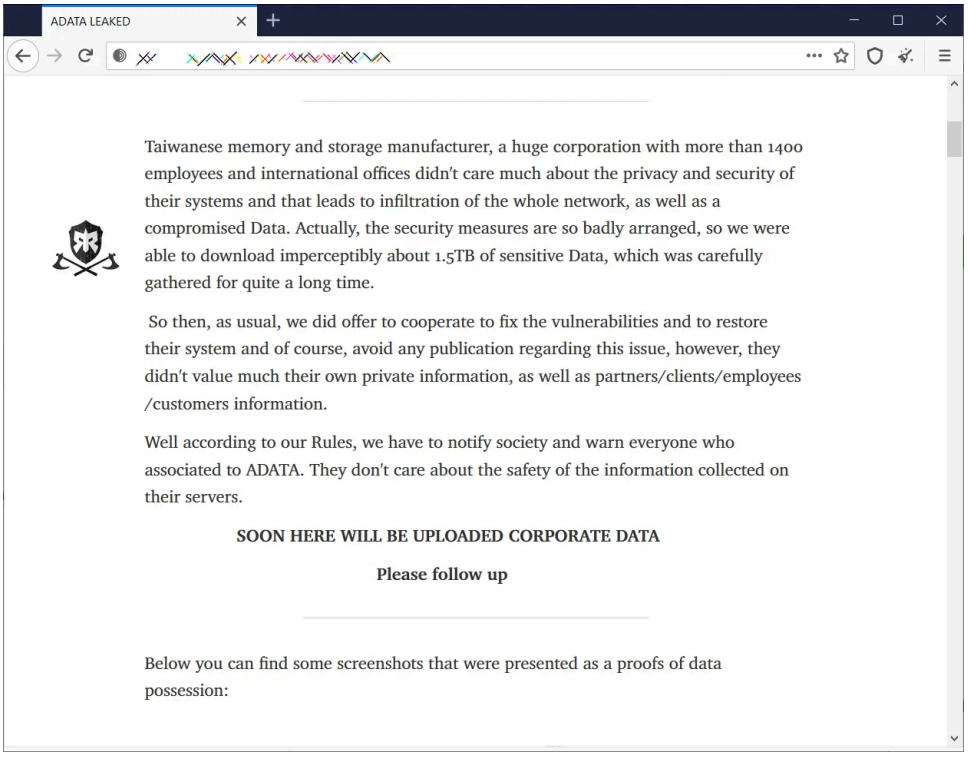
Ragnar Locker ransomware claims the attack

ADATA did not provide information on the ransomware operation behind the incident or any ransom demands. However, the attack has already been claimed over the weekend by the Ragnar Locker ransomware gang.

Ragnar Locker says that they have allegedly stolen 1.5TB of sensitive data from ADATA's network before deploying the ransomware payloads.

So far, the ransomware gang has only posted screenshots of stolen files and folders as proof of their claims, but they are threatening to leak the rest of the data if the memory manufacturer doesn't pay the ransom.

According to the screenshots already posted by Ragnar Locker on their dark web leak site, the attackers could collect and exfiltrate proprietary business information, confidential files, schematics, financial data, Gitlab and SVN source code, legal documents, employee info, NDAs, and work folders.



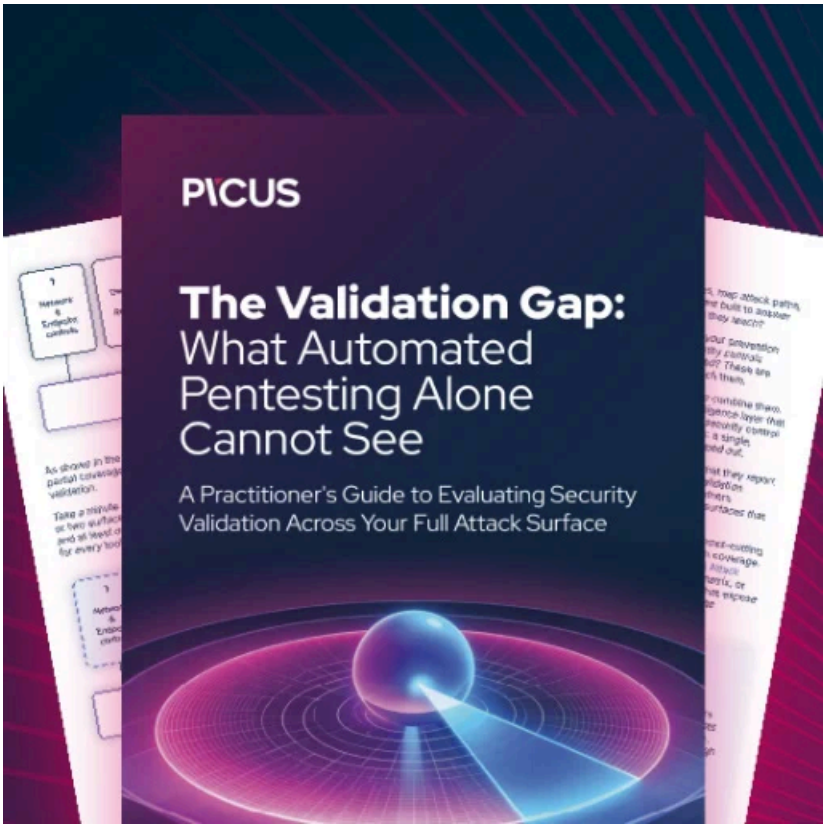
Ragnar Locker ransomware activity was first observed being deployed in attacks against several targets in late December 2019.

On compromised enterprise endpoints, Ragnar Locker operators terminate remote management software (such as ConnectWise and Kaseya) used by managed service providers (MSPs) to manage clients' systems remotely.

This allows the attackers to evade detection and ensure that admins logged in remotely do not block the payload deployment process.

The FBI warned private industry partners of increased Ragnar Locker ransomware activity after an April 2020 attack that impacted the network of multinational energy giant Energias de Portugal (EDP).

As seen by BleepingComputer, Ragnar Locker ransom demands range from $200,000 to roughly $600,000. However, Ragnar Locker demanded a ransom of 1580 bitcoins (the equivalent of over $10 million) in EDP's case.



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.
