


ACER computer manufacturer cyber attack.

In March of 2021, Acer was hit with a “ransomware” attack and asked to fork over \$50million dollars - this is the largest ransomware attack known to date according to the articles I read. On Security Magazine’s website


(<https://www.securitymagazine.com/articles/94870-acer-hit-with-up-to-50m-ransom>) they mention: “Acer's identity and data was posted on Sodinokibi's (aka REvil) data leakage site "Happy Blog" on March 18, 2021, and the data allegedly exposed included client lists, payment form applications, and financial documents. A leak of the ransom note revealed that Acer had until March 28, 2021, to pay a ransom of XMR 214,151 (Monero) (USD 50 million). If the ransom was not paid within the stipulated date, the ransom would double to USD 100 million.”

They continue to say: “...the attack may suggest that the REvil ransomware gang may have successfully weaponized the Microsoft Exchange ProxyLogon vulnerabilities to gain access to Acer.” It sounds like the hackers potentially exploited a weakness in Microsoft Exchange, but nobody seems to have a definitive answer on that.


Your network has been infected!



Your documents, photos, databases and other important files encrypted



To decrypt your files you need to buy our special software - **General-Decryptor**



Follow the instructions below. But remember that you do not have much time

General-Decryptor price

the price is for all PCs of your infected network

You have **8 days, 19:07:29**

* If you do not pay on time, the price will be doubled

* Time ends on **Mar 28, 16:30:11**

Current price

After time ends

214151 XMR
≈ 50,000,000 USD

428302 XMR
≈ 100,000,000 USD

I have not been able to find any other information as to what Acer has done to recover from the attack, and improve for the future. But REvil did offer a 20 percent reduction in ransom cost if they paid by the Wednesday prior to Sunday, March 28.