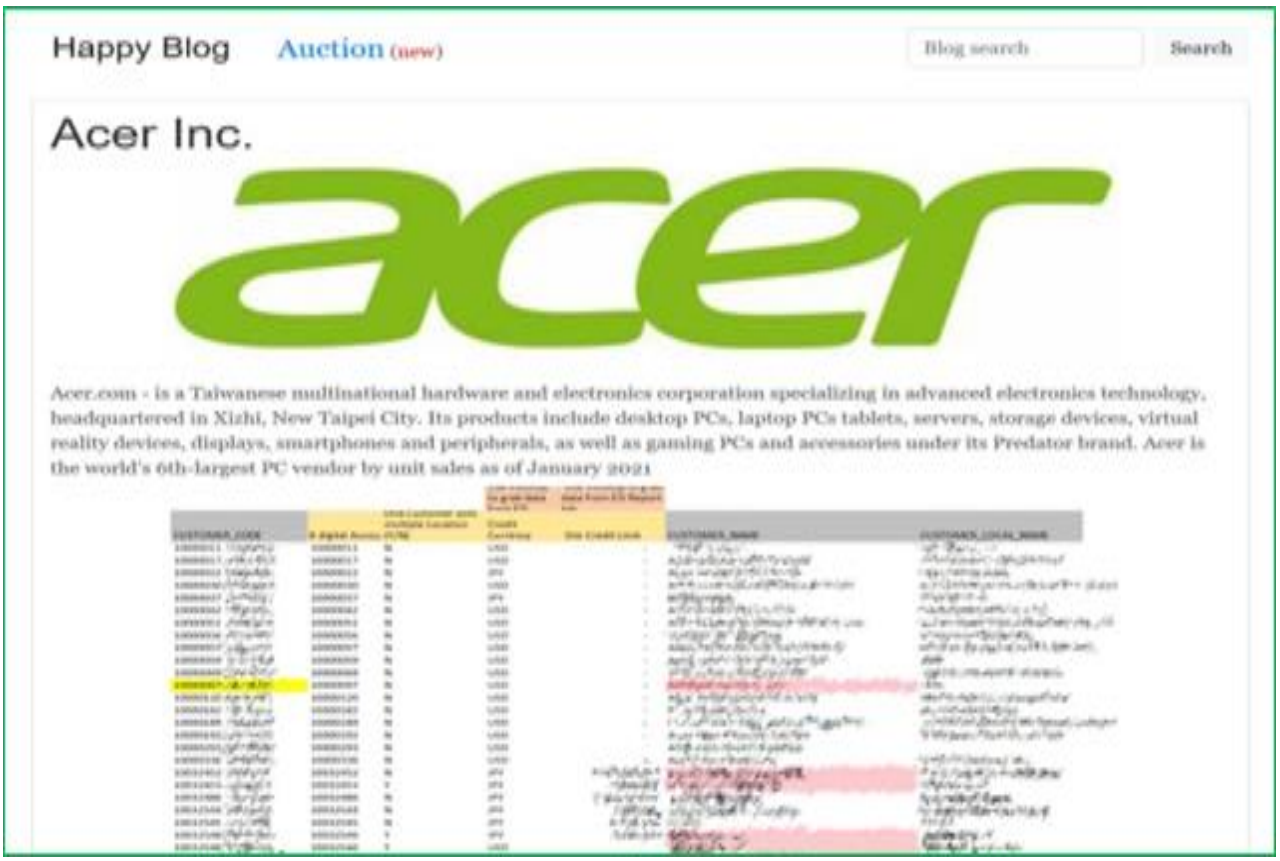
Tech Giant Acer Hit by a REvil Ransomware – Attackers Demanding $50,000,000 Ransom



Taiwanese computer manufacturer Acer has been hit by a REvil ransomware attack where the threat actors are demanding the largest known ransom to date, $50,000,000.

Acer is the world's 6th-largest PC vendor by unit sales as of January 2021 and well-known for laptops, desktops, and monitors.

Who is REvil?

A Computer Weekly report calls REvil "one of the most active and dangerous ransomware threats in the wild." REvil is also known as Sodinokibi, was first discovered in 2019 by Cisco Talos.

McAfee's Advanced Threat Research (ATR) team shared insights into the affiliates' methods using REvil, including distributing the ransomware through spear-phishing and weaponized documents.

These documents – batch files that download payloads from Pastebin to processes on the target OS – compromises remote desktop protocols (RDPs) and uses script files and password cracking tools to distribute them over the target network.

REvil usually demands ransoms between 0.44 and 0.45 bitcoin, which is approximately $4,000.

The ransomware gang announced on their data leak site that they had breached Acer and shared some images of allegedly stolen files as proof.The leaked images are for documents that include financial spreadsheets, bank balances, and bank communications.

Acer's Response

In response to BleepingComputer's inquiries, Acer's response as follows:

"Acer routinely monitors its IT systems, and most cyberattacks are well defensed. Companies like us are constantly under attack, and we have reported recent abnormal situations observed to the relevant law enforcement and data protection authorities in multiple countries."

"We have been continuously enhancing our cybersecurity infrastructure to protect business continuity and our information integrity. We urge all companies and organizations to adhere to cybersecurity disciplines and best practices and be vigilant to any network activity abnormalities." – Acer.

Acer also said, "there is an ongoing investigation and for the sake of security, we are unable to comment on details."

Acer Ransome Demand

Valery Marchive of LegMagIT discovered the REvil ransomware sample used in the Acer attack that demanded a whopping $50 million ransom.

In conversations between the victim and REvil, which started on March 14th, the Acer representative showed shock at the massive $50 million demand. Later in the chat, the REvil representative shared a link to the Acer data leak page, which was secret at the time.

The attackers also offered a 20% discount if payment was made by this past Wednesday. In return, the ransomware gang would provide a decryptor, a vulnerability report, and the deletion of stolen files.

At one point, the REvil operation offered a cryptic warning to Acer "to not repeat the fate of the SolarWind." REvil's 50 million demand is the largest known ransom to date, with the previous being the $30 million ransom from the Dairy Farm cyberattack, also by REvil.

Probable Microsoft Exchange exploitation

"Advanced Intel's Andariel cyber intelligence system detected that one particular REvil affiliate pursued Microsoft Exchange weaponization", says Vitali Kremez.

If REvil did exploit the recent Microsoft Exchange vulnerabilities to steal data or encrypt devices, it would be the first time one of the big game-hunting ransomware operations used this attack vector.

References:

https://cybersecuritynews.com/acer-hit-by-revil-ransomware/

https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/

https://www.thequint.com/tech-and-auto/acer-hit-by-a-50dollar-million-ransomware-demand-should-you-worry#read-more