Computer giant Acer hit by $50 million ransomware attack

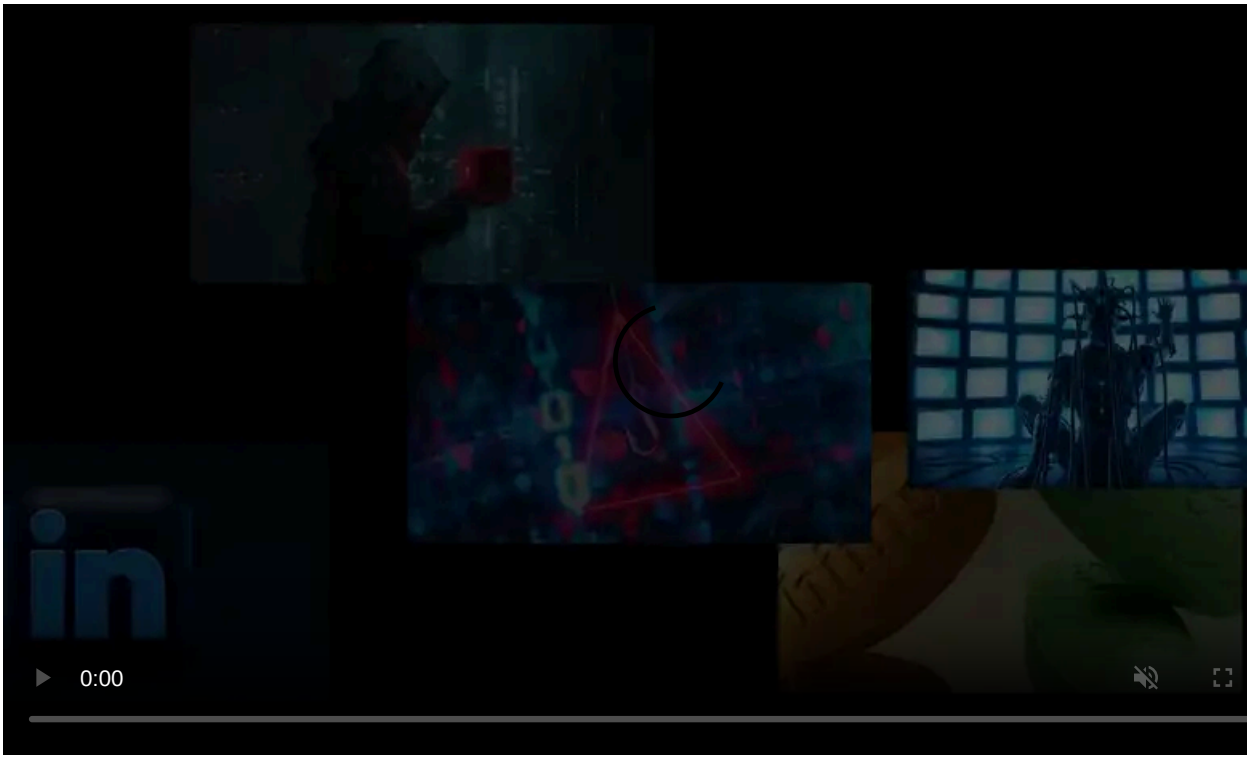
By Lawrence Abrams

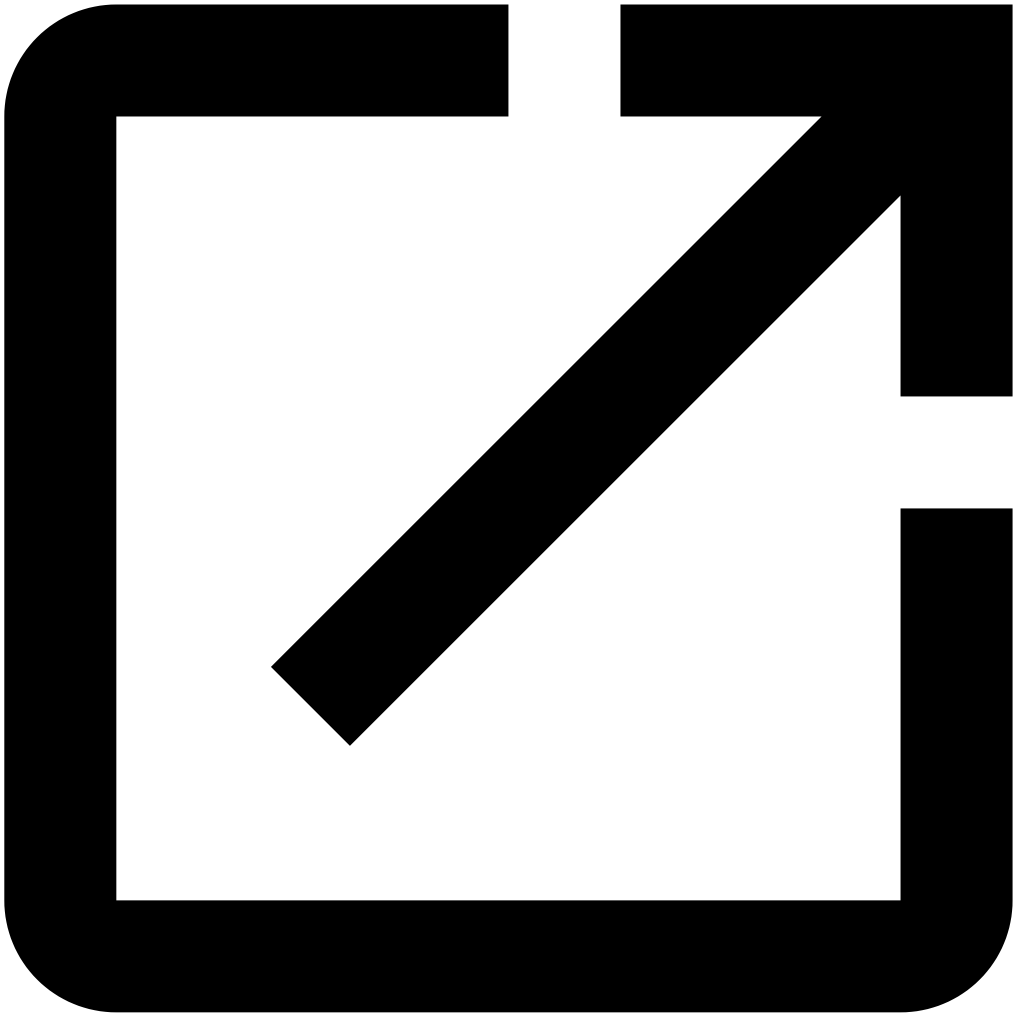
Published: 2021-03-19 · Archived: 2026-04-05 15:43:36 UTC

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

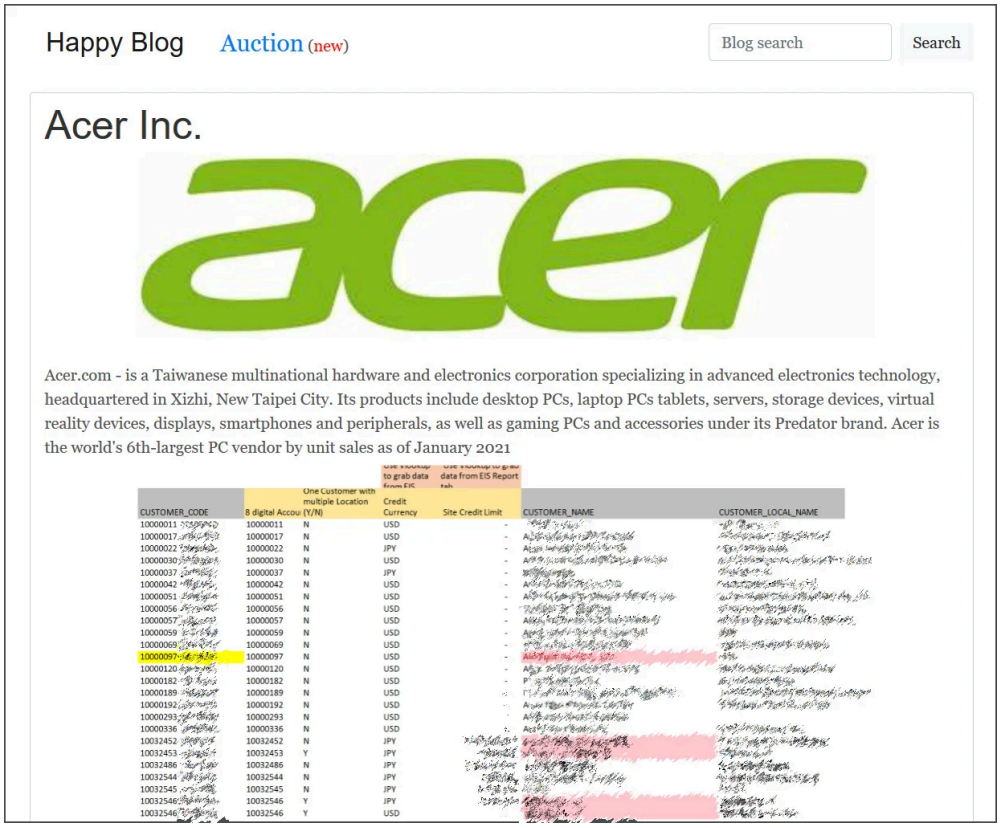
Acer is a Taiwanese electronics and computer maker well-known for laptops, desktops, and monitors. Acer employs approximately 7,000 employees and earned $7.8 billion in 2019.

Yesterday, the ransomware gang announced on their data leak site that they had breached Acer and shared some images of allegedly stolen files as proof.


0:00



These leaked images are for documents that include financial spreadsheets, bank balances, and bank communications.



Acer data leak on REvil ransomware site

In response to BleepingComputer's inquiries, Acer did not provide a clear answer regarding whether they suffered a REvil ransomware attack, saying instead that they "reported recent abnormal situations" to relevant LEAs and DPAs.

You can read their complete response below:

> "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 cyber security disciplines and best practices, and be vigilant to any network activity abnormalities." - Acer.

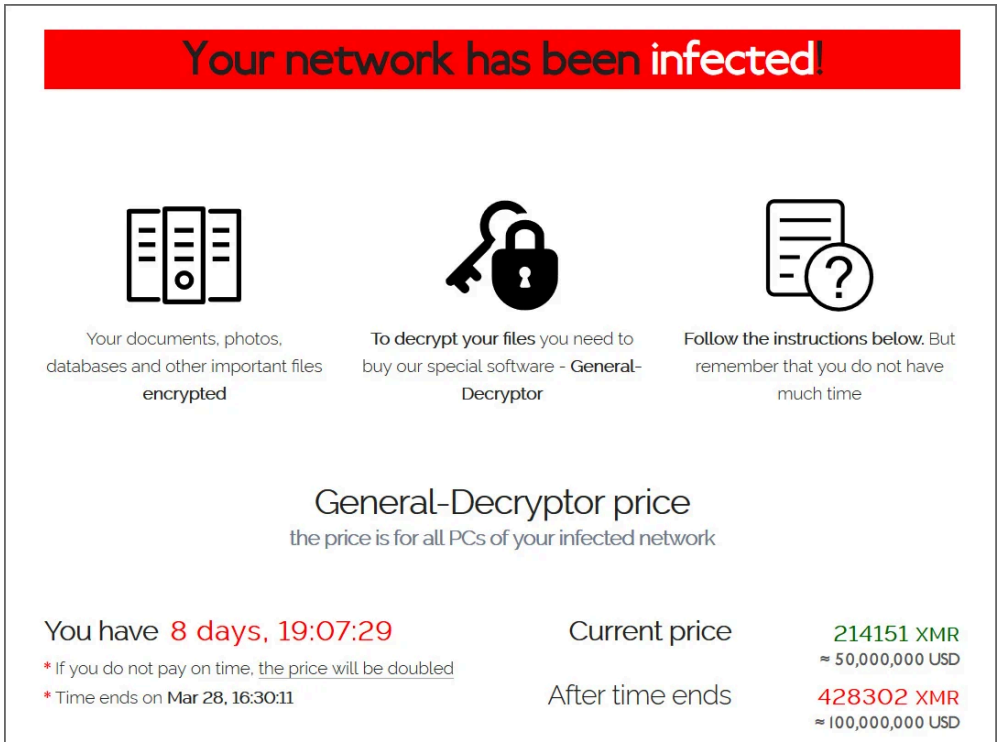
In requests for further details, Acer said "there is an ongoing investigation and for the sake of security, we are unable to comment on details."

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731 or on Wire at @lawrenceabrams-bc.

Highest known ransom demand

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

Soon after, BleepingComputer found the sample and can confirm that based on the ransom note and the victim's conversation with the attackers, the sample is from the cyberattack on Acer.



Acer ransom demand on Tor payment site

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.

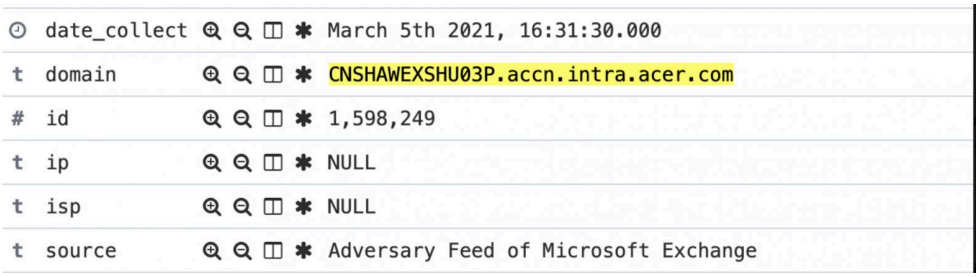
At one point, the REvil operation offered a cryptic warning to Acer "to not repeat the fate of the SolarWind."

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.

Possible Microsoft Exchange exploitation

Vitali Kremez told BleepingComputer that Advanced Intel's Andariel cyberintelligence platform detected that the Revil gang recently targeted a Microsoft Exchange server on Acer's domain.

"Advanced Intel's Andariel cyberintelligence system detected that one particular REvil affiliate pursued Microsoft Exchange weaponization," Kremez told BleepingComputer.



Andariel feed showing targeting of Acer Exchange Server

The threat actors behind the DearCry ransomware have already used the ProxyLogon vulnerability to deploy their ransomware but they are a smaller operation with fewer victims.

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.

Update 3/19/21 2:45PM: Updated with information from discovered Acer ransomware sample.

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