

Computer giant Acer hit by \$50 million ransomware attack

By Lawrence Abrams

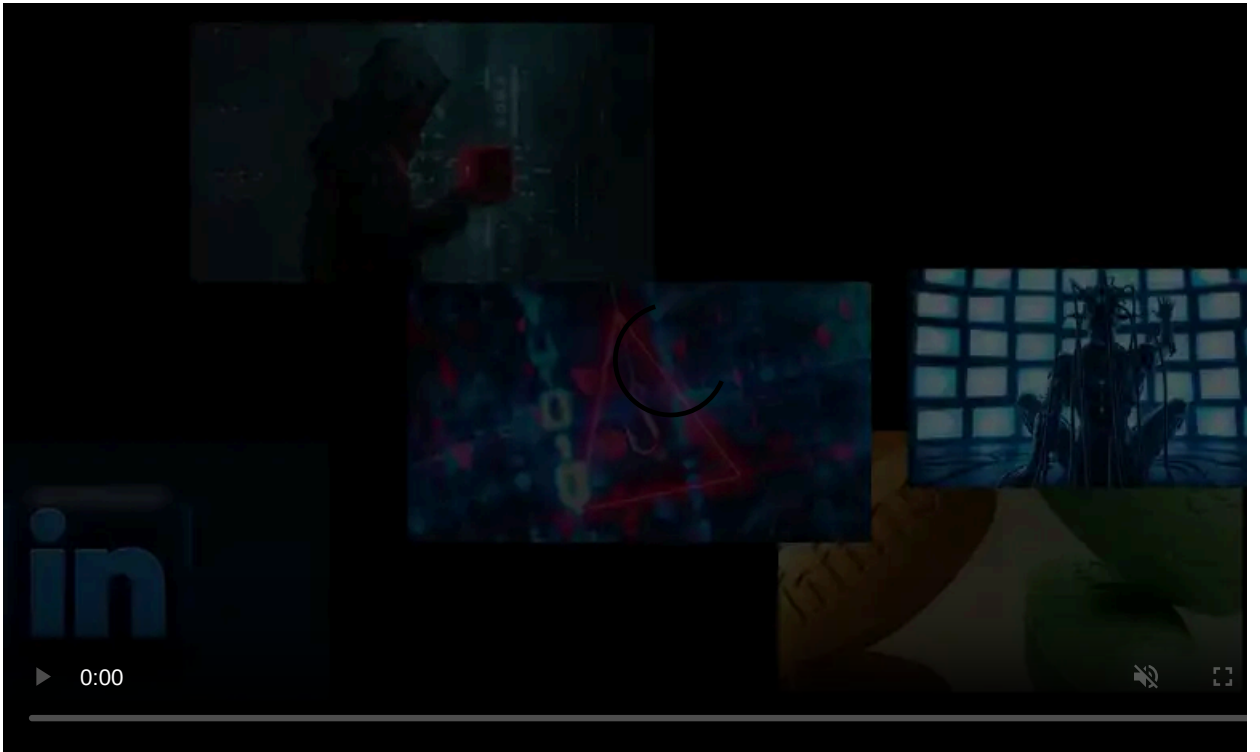
Published: 2021-03-19 · Archived: 2026-04-05 15:43:36 UTC



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.




Visit Advertiser website [GO TO PAGE](#)

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

Happy Blog Auction (new)

Acer Inc.



Acer.com - is a Taiwanese multinational hardware and electronics corporation specializing in advanced electronics technology, headquartered in Xizhi, New Taipei City. Its products include desktop PCs, laptop PCs tablets, servers, storage devices, virtual reality devices, displays, smartphones and peripherals, as well as gaming PCs and accessories under its Predator brand. Acer is the world's 6th-largest PC vendor by unit sales as of January 2021

CUSTOMER_CODE	8 digit Accou (Y/N)	One Customer with multiple Location	Credit Currency	Site Credit Limit	CUSTOMER_NAME	CUSTOMER_LOCAL_NAME
10000011	10000011	N	USD	-	-	-
10000017	10000017	N	USD	-	-	-
10000022	10000022	N	JPY	-	-	-
10000030	10000030	N	USD	-	-	-
10000037	10000037	N	JPY	-	-	-
10000042	10000042	N	USD	-	-	-
10000051	10000051	N	USD	-	-	-
10000056	10000056	N	USD	-	-	-
10000057	10000057	N	USD	-	-	-
10000059	10000059	N	USD	-	-	-
10000069	10000069	N	USD	-	-	-
10000097	10000097	N	USD	-	-	-
10000120	10000120	N	USD	-	-	-
10000182	10000182	N	USD	-	-	-
10000189	10000189	N	USD	-	-	-
10000192	10000192	N	USD	-	-	-
10000293	10000293	N	USD	-	-	-
10000336	10000336	N	USD	-	-	-
10032452	10032452	N	JPY	-	-	-
10032453	10032453	Y	JPY	-	-	-
10032486	10032486	N	JPY	-	-	-
10032544	10032544	N	JPY	-	-	-
10032545	10032545	N	JPY	-	-	-
10032546	10032546	Y	JPY	-	-	-
10032546	10032546	Y	USD	-	-	-

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 defended. 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](tel:+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.


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 214151 XMR
≈ 50,000,000 USD

After time ends 428302 XMR
≈ 100,000,000 USD

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.

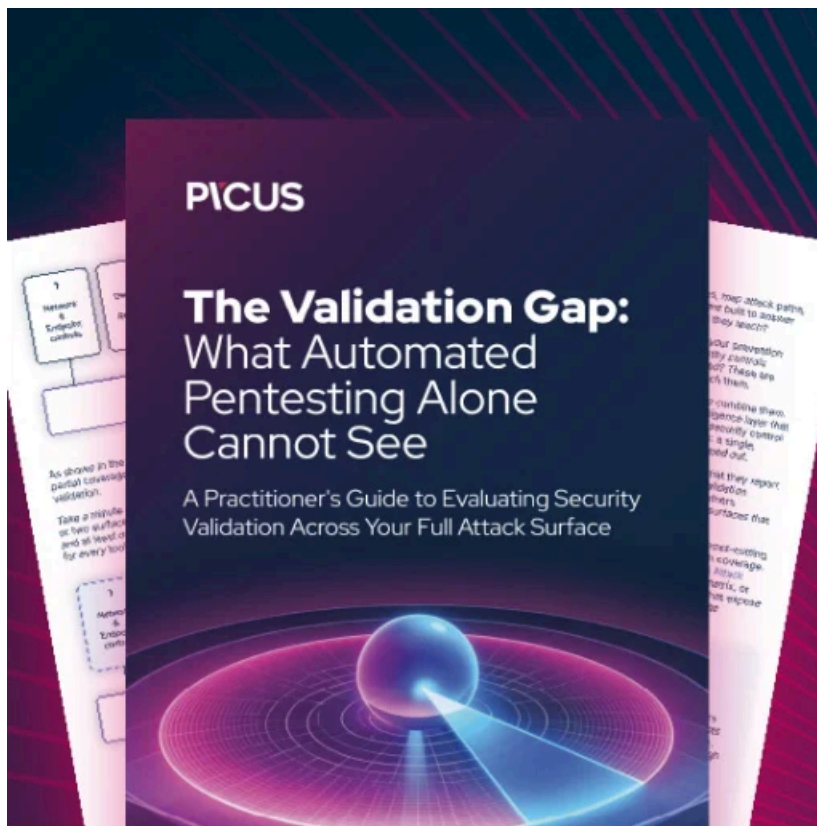
🕒 date_collect	🔍 📄 *	March 5th 2021, 16:31:30.000
t domain	🔍 📄 *	CNSHAWEXSHU03P.accn.intra.acer.com
# id	🔍 📄 *	1,598,249
t ip	🔍 📄 *	NULL
t isp	🔍 📄 *	NULL
t source	🔍 📄 *	Adversary Feed of Microsoft Exchange

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.



[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.

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