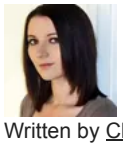
Capcom quietly discloses cyberattack impacting email, file servers

zdnet.com/article/capcom-quietly-discloses-cyberattack-impacting-email-file-servers/

Home Innovation Security

Updated: The attack forced Capcom to temporarily pull services to stop the attack from spreading.



Written by Charlie Osborne, Contributor on Nov. 5, 2020

-
-
-
-
-

Update 14.46pm GMT: ZDNet has learned that the security incident may be due to a Ragnar Locker ransomware infection.

Capcom has disclosed a cyberattack that impacted the company's operations over the weekend.

Security

- My Instagram account was hacked, and two-factor authentication didn't help
- The 5 best browsers for privacy: Secure web browsing
- Stop doing these 10 things that let hackers in, says FBI and NSA
- What is a cybersecurity degree?
- How to delete yourself from search results and hide your identity online

The Osaka, Japan-based video game developer said in a notice dated November 4 that two days prior, beginning in the early morning, "some of the Capcom Group networks experienced issues that affected access to certain systems" due to a cyberattack.

Email and file servers were impacted.

See also: Marriott fined £18.4 million by UK watchdog over customer data breach

Capcom has described the attack as "unauthorized access" conducted by a third-party. As the security incident took place, the company stopped some operations on its internal networks, likely to prevent the cyberattack from spreading further and potentially compromising additional corporate resources.

Capcom claims that there is "no indication" that customer information has been accessed or compromised; at least, at this stage.

"This incident has not affected connections for playing the company's games online or access to its various websites," the company said. "Capcom expressed its deepest regret for any inconvenience this may cause to its various stakeholders."

CNET: Election still too close to call: How to spot misinformation while you wait for results

At the time of writing, Capcom says it is "unable to reply to inquiries and/or to fulfill requests for documents" made through the investor relations contact form.

The game developer is currently working toward restoring its systems and has reported the cyberattack to law enforcement.

TechRepublic: It's an urgent plea this Election Day: Don't click on ransomware disguised as political ads

Capcom has not revealed any further details relating to the attack, but the company is not the only game developer targeted this year. In October, Ubisoft and Crytek were the victims of the Egregor ransomware gang, which attempted to extort a ransomware payment from the firms on the threat of the public release of proprietary data stolen during attacks.

Egregor is an active ransomware group believed to be responsible for cyberattacks against GEFCO and Barnes & Noble. Researchers from Malwarebytes suspect that past affiliates of the Maze ransomware group -- now retired from the scene -- are now turning to Egregor as an alternative.

Update 14.46pm GMT: ZDNet has learned that the security incident may be due to a Ragnar Locker ransomware infection. Ragnar Locker, associated with an attack on energy company EDP in July, is a ransomware variant of which some operators deploy in virtual machines (VMs) to avoid detection. The ransomware is generally used against corporate targets.

ZDNet

ZDNet has sent Capcom a request for comment and will update if we hear back.

Previous and related coverage

Have a tip? Get in touch securely via WhatsApp | Signal at +447713 025 499, or over at Keybase: charlie0