HTC Global Services confirms cyberattack after data leaked online

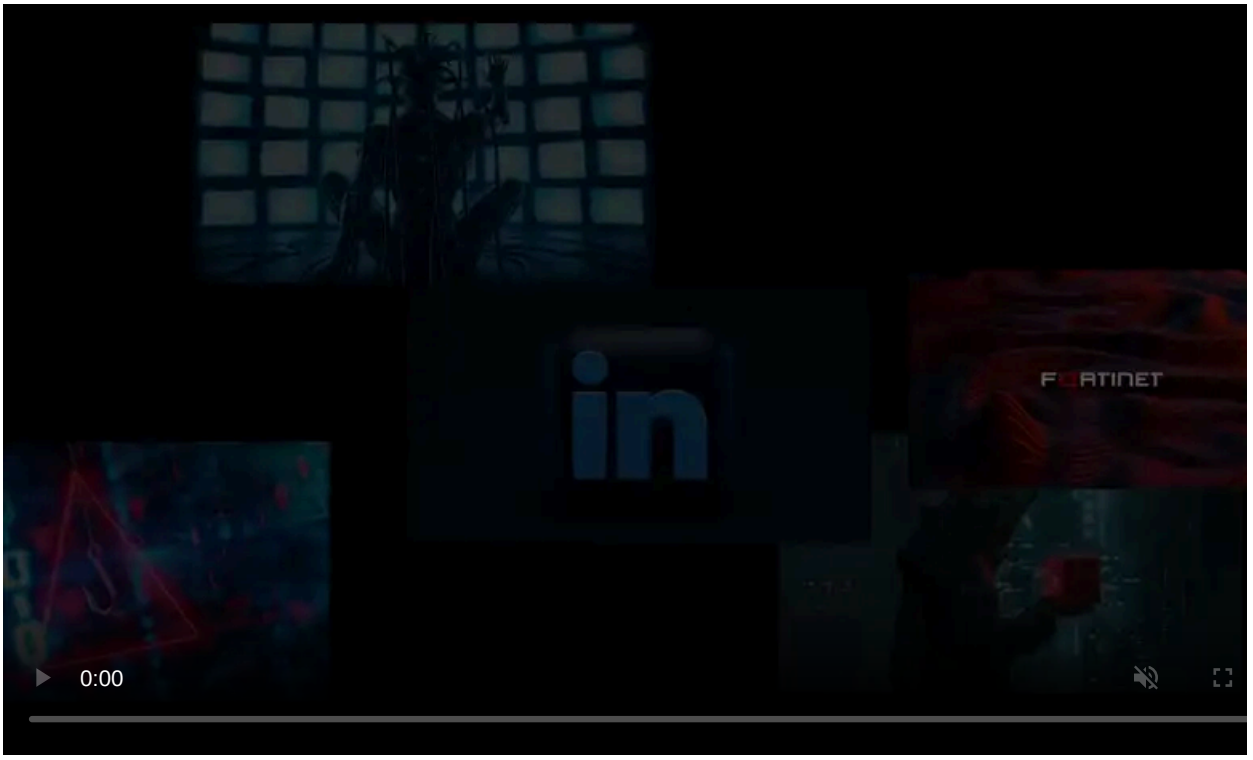
By Lawrence Abrams

Published: 2023-12-05 · Archived: 2026-04-05 19:39:10 UTC

IT services and business consulting company HTC Global Services has confirmed that they suffered a cyberattack after the ALPHV ransomware gang began leaking screenshots of stolen data.

HTC Global Services is a managed service provider offering technology and business services to the healthcare, automotive, manufacturing, and financial industries.

While HTC has not posted a statement to the company website, they issued a brief announcement last night on X confirming the attack.


0:00

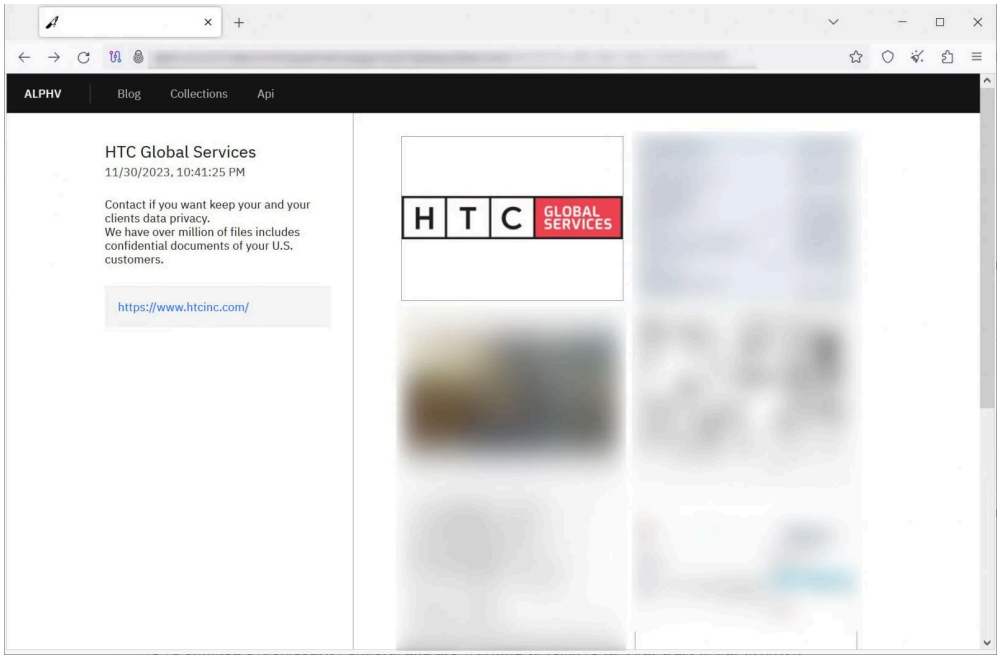
"HTC has experienced a cybersecurity incident," reads a tweet posted to HTC's X account last night.

"Our team has been actively investigating and addressing the situation to ensure the security and integrity of user data."

"We've enlisted cybersecurity experts and are working to resolve it. Your trust is our priority."

This announcement comes after the ALPHV (BlackCat) ransomware gang listed HTC on their data leak site, along with screenshots of allegedly stolen data.

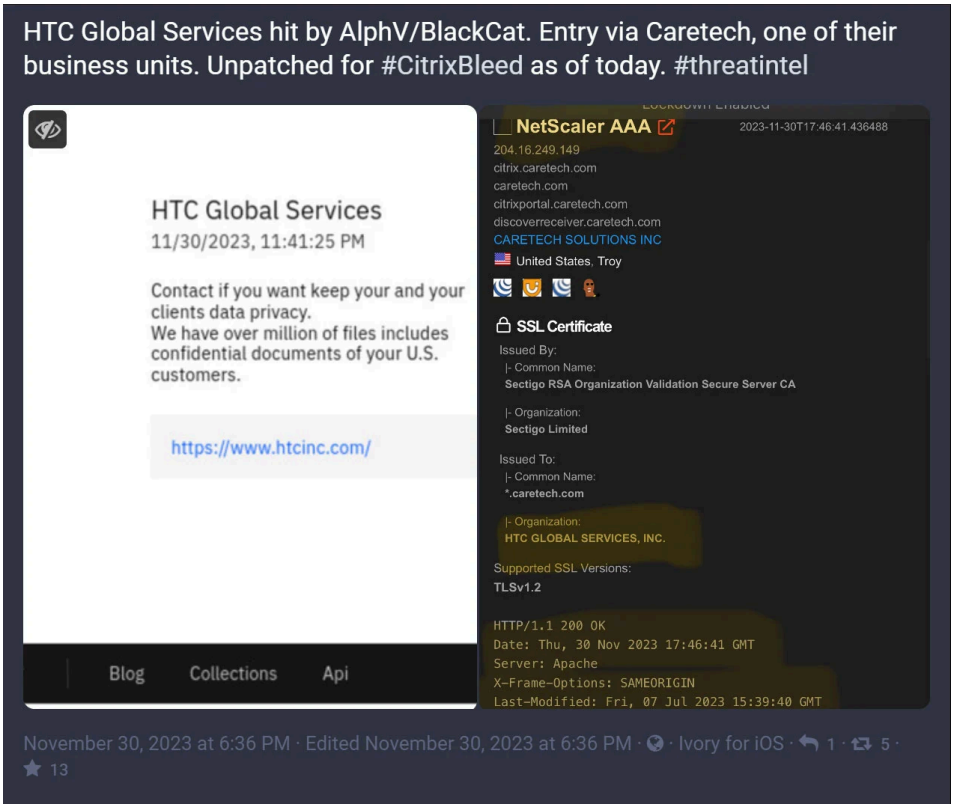
The leaked data includes passports, contact lists, emails, and confidential documents allegedly stolen during the attack.



HTC Global Services entry on the ALPHV data leak site

While little information about the attack on HTC is available, cybersecurity professional Kevin Beaumont believes the company was breached using the Citrix Bleed vulnerability.

According to Beaumont, one of HTC's business units, CareTech, operated a vulnerable Citrix Netscaler device, which was exploited for initial access to the company's network.



BleepingComputer has contacted HTC Global Services with questions about the attack and whether they were breached using Citrix Bleed, but a response was not immediately available.

ALPHV is amassing victims

The ALPHV/BlackCat ransomware operation launched in November 2021, is believed to be a rebrand of the DarkSide and BlackMatter ransomware operations.

As DarkSide, the group gained international attention after they breached Colonial Pipeline, leading to intense pressure from law enforcement agencies globally.

After rebranding again as BlackMatter in July 2021, their operations abruptly ceased in November 2021 when authorities seized their servers, and security firm Emsisoft created a decryptor exploiting a ransomware vulnerability.

This ransomware operation is known for consistently targeting global enterprises and continuously adapting and refining their tactics, and has seen a surge in attacks recently.

This evolution includes working with English-speaking threat actors, who utilize their encryptors and infrastructure to launch extortion attacks.

In a recent incident, a group of English-speaking affiliates tracked as Scattered Spider claimed responsibility for the attack on MGM Resorts, saying they encrypted over 100 ESXi hypervisors during the attack.

This week, one ALPHV affiliate claimed to have stolen data from Tipalti and said they have begun to extort impacted companies individually.

The threat actors have also recently attacked a publicly owned electricity provider and a hospital network, both classified as critical infrastructure in the United States.

The attacks on critical infrastructure may once again be the tipping point that leads to increased scrutiny by US law enforcement.
