Ransomware gang leaks data from Stanford, Maryland universities

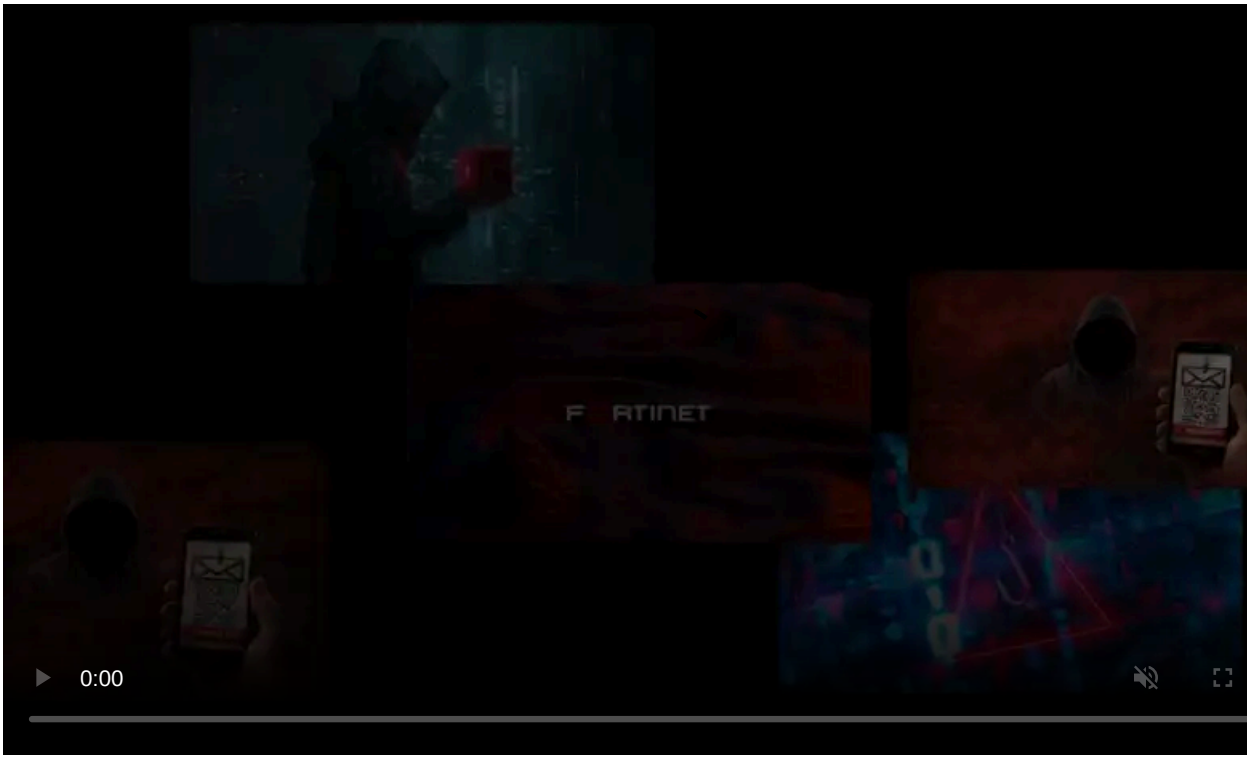
By Sergiu Gatlan

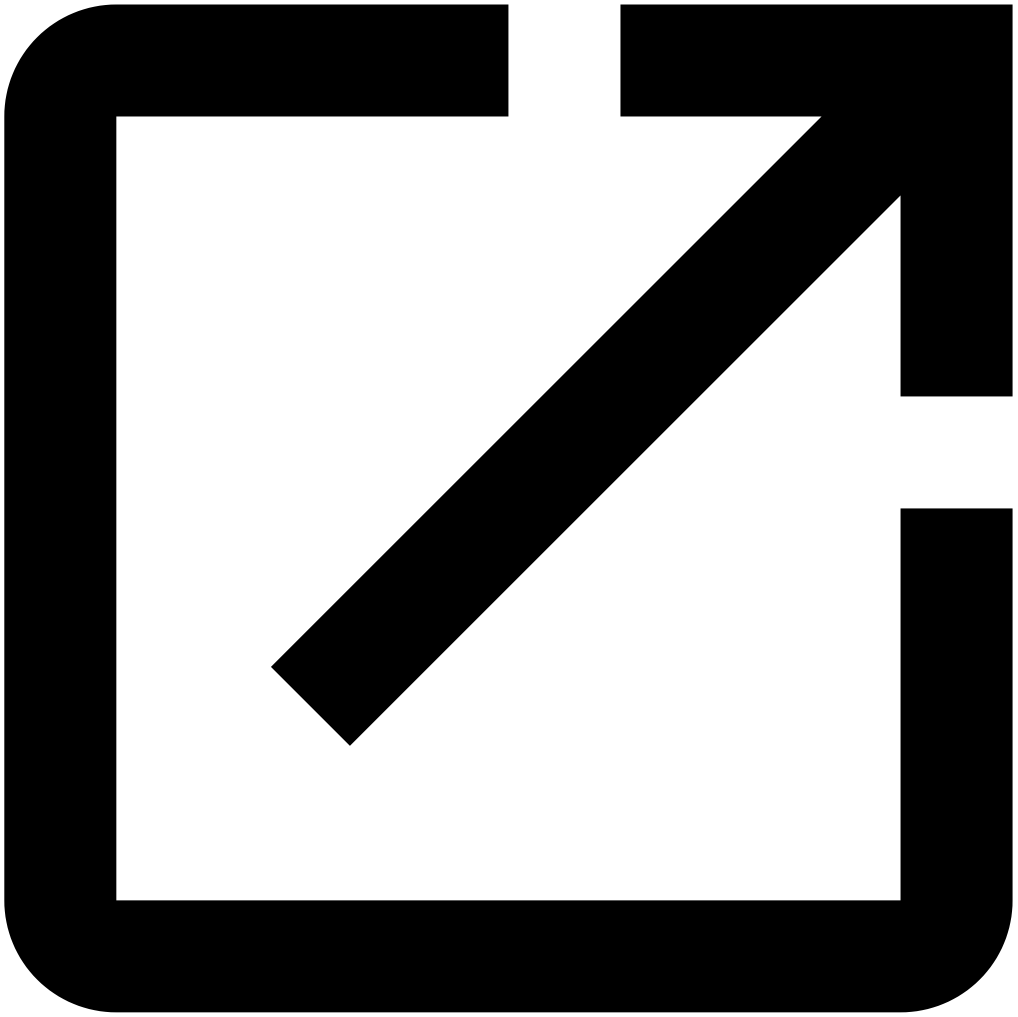
Published: 2021-04-03 · Archived: 2026-04-05 20:42:30 UTC

Image: Dom Fou

Personal and financial information stolen from Stanford Medicine, University of Maryland Baltimore (UMB), and the University of California was leaked online by the Clop ransomware group.

The threat actors obtained the documents after hacking the universities' Accellion File Transfer Appliance (FTA) software used to share and store sensitive information.


F RTINET
0:00



Data stolen in the attack targeting Stanford Medicine's Accellion server includes names, addresses, email addresses, Social Security numbers, and financial information, reported the Stanford Daily.

"We discovered the breach earlier this week when the hackers posted evidence that they had accessed a limited number of files in our system containing some personally identifiable information," UMB also told DataBreaches.net.

"UC has learned that it, along with other universities, government agencies, and private companies throughout the country, was recently subject to a cybersecurity attack," a statement issued by the UC Office of the President reads.

"The attack involves the use of Accellion, a vendor used by many organizations for secure file transfer, in which an unauthorized individual appears to have copied and transferred UC files by exploiting a vulnerability in Accellion's file-transfer service."

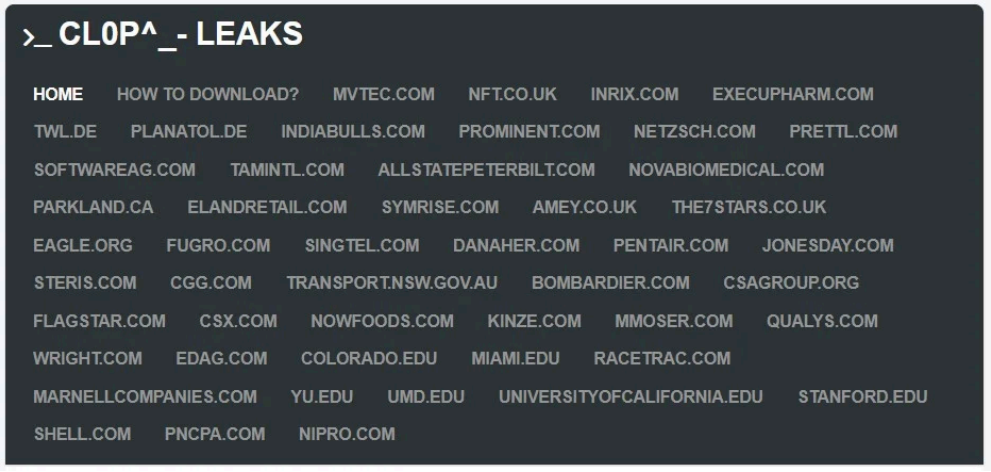
Colorado and Miami universities also hit

Since February, the ransomware operation has been leaking files stolen after compromising vulnerable Accellion FTA file-sharing servers.

The ransomware gang started leaking the universities' data during late March, attempting to coerce them to pay ransoms to have the stolen data deleted and the leaks stopped.

Last month, the Clop ransomware gang leaked other data sets allegedly stolen from the University of Colorado and the University of Miami.

The attackers haven't gained access to universities' internal networks, with the incident only impacting their Accellion servers.



Clop leak site

While still unclear if Clop is behind these Accellion attacks or they're collaborating with another group, a joint statement from Mandiant and Accellion shed more light on these attacks also linking them to a second operation, the FIN11 cybercrime group.

BleepingComputer has reported multiple data breaches affecting companies and organizations after these threat actors successfully compromised their Accellion FTA servers and exfiltrated sensitive information.

Starting with January, we reported attacks on energy giant Shell, cybersecurity firm Qualys, supermarket giant Kroger, the Reserve Bank of New Zealand, Singtel, the Australian Securities and Investments Commission (ASIC), the Office of the Washington State Auditor ("SAO"), as well as multiple universities and other organizations.

Five Eyes members also issued a joint security advisory in February about ongoing attacks and extortion attempts targeting orgs that use vulnerable Accellion File Transfer Appliance (FTA) versions.

In related news, Brown University, a private Ivy League research university, is still working on bringing systems online after it had to disable them following a cyberattack on Tuesday.

Source: https://www.bleepingcomputer.com/news/security/ransomware-gang-leaks-data-from-stanford-maryland-universities/