Update on IT Security Incident at UCSF

ucsf.edu/news/2020/06/417911/update-it-security-incident-ucsf

- Campus News
- June 26, 2020

As we disclosed on June 3, UCSF IT staff detected a security incident that occurred in a limited part of the UCSF School of Medicine's IT environment on June 1.

We quarantined several IT systems within the School of Medicine as a safety measure, and we successfully isolated the incident from the core UCSF network. Importantly, this incident did not affect our patient care delivery operations, overall campus network, or COVID-19 work.

While we stopped the attack as it was occurring, the actors launched malware that encrypted a limited number of servers within the School of Medicine, making them temporarily inaccessible. Since that time, we have been working with a leading cyber-security consultant and other outside experts to investigate the incident and reinforce our IT systems' defenses. We expect to fully restore the affected servers soon.

Our investigation is ongoing but, at this time, we believe that the malware encrypted our servers opportunistically, with no particular area being targeted. The attackers obtained some data as proof of their action, to use in their demand for a ransom payment. We are continuing our investigation, but we do not currently believe patient medical records were exposed. As additional facts become known, we will provide further updates.

The data that was encrypted is important to some of the academic work we pursue as a university serving the public good. We therefore made the difficult decision to pay some portion of the ransom, approximately $1.14 million, to the individuals behind the malware attack in exchange for a tool to unlock the encrypted data and the return of the data they obtained.

This incident reflects the growing use of malware by cyber-criminals around the world seeking monetary gain, including several recent attacks on institutions of higher education. We continue to cooperate with law enforcement, and we appreciate everyone's understanding that we are limited in what we can share while we continue with our investigation.