Alaska discloses ‘sophisticated’ nation-state cyberattack on health service

therecord.media/alaska-discloses-sophisticated-nation-state-cyberattack-on-health-service/

September 20, 2021

Image: Kayti Coonjohn

A nation-state cyber-espionage group has gained access to the IT network of the Alaska Department of Health and Social Service (DHSS), the agency said last week.

The attack, which is still being investigated, was discovered on May 2, earlier this year, by a security firm, which notified the agency.

While the DHSS made the incident public on May 18 and published two updates in June and August, the agency did not reveal any details about the intrusion until last week, when it officially dispelled the rumor that this was a ransomware attack.

Instead, the agency described the intruders as a “nation-state sponsored attacker” and “a highly sophisticated group known to conduct

complex cyberattacks against organizations that include state governments and health care entities.”

Attackers entered DHSS network via a vulnerable website

Citing an investigation conducted together with security firm Mandiant, DHSS officials said the attackers gained access to the department's internal network through a vulnerability in one of its websites and "spread from there."

Officials said they believe to have expelled the attacker from their network; however, there is still an investigation taking place into what the attackers might have accessed.

In a press release last week [PDF], the agency said it plans to notify all individuals who provided their personal information to the state agency.

"The breach involves an unknown number of individuals but potentially involves any data stored on the department's information technology infrastructure at the time of the cyberattack," officials said.

Data stored on the DHSS network, and which could have been collected by the nation-state group, includes the likes of:

- Full names
- Dates of birth
- Social Security numbers
- Addresses
- Telephone numbers
- Driver's license numbers
- Internal identifying numbers (case reports, protected service reports, Medicaid, etc.)
- Health information
- Financial information
- Historical information concerning individuals' interaction with DHSS

Notification emails will be sent to all affected individuals between September 27 and October 1, 2021, the DHSS said.

The agency has also published a FAQ page [PDF] with additional details about the nation-state attack.

"Regrettably, cyberattacks by nation-state-sponsored actors and transnational cybercriminals are becoming more common and are an inherent risk of conducting any type of business online," said DHSS Technology Officer Scott McCutcheon.

All systems breached by the intruders remain offline. This includes systems used to perform background checks and systems used to request birth, death, and marriage certificates, all of which are now processed and reviewed manually, in person or via the phone.

Tags

- Alaska

- APT
- cyberattack
- health department
- nation-state
- social security
- USA
- website vulnerability

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.