TechXplore

US Marshals computer system hit by ransomware attack

March 1 2023, by Lindsay Whitehurst

Credit: CC0 Public Domain

In a major breach of a U.S. Marshals Service computer system this month with ransomware, hackers stole sensitive and personally identifiable data about agency employees and targets of investigations, an agency spokesman said Tuesday.

The hacked system was disconnected from the network shortly after the breach and stolen data were discovered Feb. 17. The Justice Department determined it was a major incident and opened an investigation as the Marshals work "swiftly and effectively," to tamp down any risks associated with the breach, agency spokesman Drew Wade said Tuesday.

The hack was first reported by NBC News.

The incident was the latest example of cybercriminals targeting a government agency in a ransomware plot and raises questions about the Justice Department's cybersecurity protocols.

Feb. 17 was also when CNN reported that an FBI computer system had been breached. It quoted unnamed sources as saying the system was at the FBI's New York field office. Asked about the intrusion, the bureau provided a statement that called the intrusion "an isolated incident that has been contained." It declined further comment, including when the intrusion occurred and whether ransomware was involved.

Ransomware attacks have become the world's most serious cybersecurity concern. They have crippled everything from Britain's postal service to Ireland's national health network to Costa Rica's government. Schools, hospitals and local governments are routinely targeted.

The FBI and international law enforcement officials scored a win last month when they disrupted, at least temporarily, a prolific ransomware gang, saving a potential $130 million in ransom payments.

In ransomware attacks, organized gangs break into computer networks and sow malware that paralyzes them by encrypting data. But before activating the ransomware they steal data. The criminals can then hold the data hostage even if the target quickly restores the affected network with backup data.

The hacked U.S. Marshals system contains sensitive law enforcement information and personally identifiable information about subjects of investigations and certain U.S. Marshals employees, the agency said. It is tasked with tracking down fugitives, transporting federal prisoners, protecting witnesses and providing court security.

In May 2021, hackers targeted largest fuel pipeline in the U.S., causing the operators to briefly shut it down and make a multimillion-dollar ransom payment, which the federal government later largely recovered.

A hacker claimed in December to have breached an FBI-run outreach program that shares sensitive information on national security and cybersecurity threats with public and private officials who run U.S. critical infrastructure.

Citation: US Marshals computer system hit by ransomware attack (2023, March 1) retrieved 23 April 2024 from https://techxplore.com/news/2023-03-marshals-ransomware.html