

Pennsylvania courts say no ransom was paid in cyberattack, and attackers never sent a demand

February 15 2024, by Marc Levy



The exterior of the Pennsylvania Judicial Center, home to the Commonwealth Court in Harrisburg, Pa., Feb. 21, 2023. A weekend cyberattack on the website of Pennsylvania's state courts agency disabled some online systems but did not appear to compromise any data and didn't stop the courts from opening Monday, Feb. 5, 2024, officials said. Credit: AP Photo/Matt Rourke, File

Pennsylvania's state courts agency said Thursday that it never received a ransom demand as part of a cyberattack that briefly shut down some of its online services earlier this month and prompted a federal investigation.

The attack, called a "denial of services" attack, on the website of the Administrative Office of Pennsylvania Courts disabled some online portals and systems that were all fully restored this week, officials said.

The attack didn't compromise any data or stop the courts from operating on a normal schedule, officials said.

A courts agency spokesperson said officials there never received a ransom demand from the attackers, never had any communication with the attackers and never paid anything to meet any sort of demand.

The state Supreme Court's chief justice, Debra Todd, said a federal investigation was continuing.

Neither the courts nor the FBI or the federal government's lead cybersecurity agency, the U.S. Cybersecurity and Infrastructure Security Agency, have identified the attacker. There have been no apparent claims of responsibility.

In a statement, Todd said the "significant and serious" attack was "orchestrated by a faceless and nameless virtual opponent who was intent on attacking our infrastructure and orchestrating a shutdown of our state judicial system."

"These anonymous actors attempted to undermine our mission to make justice accessible and to shutter the operation of the statewide court system," Todd said.

A "denial of service" cyberattack is common and happens when attackers flood the targeted host website or network with traffic or requests until the site is overwhelmed or crashes.

The attack comes after Kansas' judicial branch was the victim of what it called a "sophisticated cyberattack" late last year from which it took months and millions of dollars to recover. That attack was blamed on a Russia-based group.

Major tech companies Google Cloud, Microsoft and Amazon Web Services have been hit by such attacks in recent years, as have financial institutions. In 2022, some U.S. airport sites were hit. Some of the biggest attacks have been attributed to Russian or Chinese hackers.

Cybersecurity experts say denial-of-service hackers are often state-backed actors seeking money and can use tactics to try to hide their identity. Such attacks also can be used to mask an underlying attack, such as a ransomware attack, experts say.

Networking experts can defuse the attacks by diverting the flood of internet traffic.

© 2024 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed without permission.

Citation: Pennsylvania courts say no ransom was paid in cyberattack, and attackers never sent a demand (2024, February 15) retrieved 11 May 2024 from <https://techxplore.com/news/2024-02-pennsylvania-courts-didnt-pay-ransom.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.
