

# Cyberattack on Tennessee election website preceded outage

May 11 2018, by Adrian Sainz

---

An intentional cyberattack and suspicious activity by foreign computers preceded the crash of a website that was reporting results in a Tennessee county's primary elections, a cyber-security firm said Friday.

The Knox County elections website suffered the attack, and "a suspiciously large number of foreign countries" accessed the site on May 1, according to the report by Sword & Shield Enterprise Security. The firm hired by the county said those actions were among the likely causes of the crash, which also included a large increase in errors and in overall traffic.

Officials have said no voting data was affected, but the site was down for an hour after the polls closed—causing confusion among voters—before technicians fixed the problem.

The report notes that no compromise of official election data could have happened. Physical access would have been the only way to manipulate official data, and access to the results was closely guarded.

Investigators said there were multiple attempts to attack a vulnerable part of the site, but it's not clear where the so-called "denial of service" attack originated from.

"The effect was clearly a loss of service, but it is unclear, with the information provided, if the outage was an intended event or a side effect of the events," the report said.

David Ball, the county's deputy director of information technology, said the vulnerability issue identified by Sword & Shield has been fixed. Additional safeguards also have been put into place.

The report said the website received requests for access from about 100 countries. The most foreign requests came from Canada, Great Britain and Chile. Source addresses from Ukraine and Great Britain tried to exploit a vulnerability in the website, the report said.

Dan Wallach, a computer science professor at Rice University, notes that the internet is a "messy place" with a lot of background traffic.

"It is often quite difficult to understand what is an attack, and what is just random traffic," Wallach said.

However, if it is a specific attack, then it would be difficult to find its origin because attackers are very good at hiding their location, Wallach said.

"What attackers will do is they'll break into other computers and then launch their attacks from there," he said.

Joyce McCants, a spokeswoman for the FBI in Knoxville, said Knox County has not reached out to the FBI in relation to the website crash.

© 2018 The Associated Press. All rights reserved.

Citation: Cyberattack on Tennessee election website preceded outage (2018, May 11) retrieved 26 April 2024 from <https://phys.org/news/2018-05-cyberattack-tennessee-election-website-outage.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.