Ukraine computer involved in Tennessee elections attack

12 May 2018, by Adrian Sainz

Investigators found evidence of a "malicious intrusion" into a Tennessee county's elections website from a computer in Ukraine during a concerted cyberattack, which likely caused the site to crash just as it was reporting vote totals in this month's primary.

Cyber-security experts hired by Knox County to analyze the so-called "denial of service" cyberattack, said Friday that "a suspiciously large number of foreign countries" accessed the site as votes were being reported on May 1.

That intense activity was among the likely causes of the crash, according to the report by Sword & Shield Enterprise Security.

"Given the circumstantial evidence_especially the simultaneous proven malicious intrusion from a Ukraine IP address_I think it is reasonable to at least hypothesize that it was an intended event," David Ball, the county's deputy director of information technology, added in an email to The Associated Press.

County officials said no voting data was affected, but the site was down for an hour after the polls closed, causing confusion before technicians fixed the problem.

The vulnerability identified by Sword & Shield has been fixed and additional safeguards are now in place, said Ball.

The election results, to be officially certified later this month, left Glenn Jacobs, also known as the pro wrestler Kane, ahead by 17 votes in the Republican primary for Knox County's mayor.

Investigators said it's impossible to prove just where the so-called "denial of service" attack originated from, since the county can't store all the "packet data" needed to identify the source.

"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.

Ball said "the bottom line is that there was a proven malicious attack from a foreign source occurring simultaneously with an apparent deliberate DOS attack. Nothing was held back from Sword and Shield, and their assessment was well aligned with our initial assessment on election night."

Knox County uses Hart InterCivic's eSlate electronic voting machines, which do not create a paper record of the votes. Ball said Hart's equipment "is not networked in any way."

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.

Election security experts have raised concerns that foreign state actors could use such attacks to erode public confidence in the democratic process. Projects like Defend Digital Democracy at Harvard University have been urging elections officials across the country to prepare for exactly such scenarios.

Richard Moran, the county's information and technology senior director, has said that while heavy traffic came from overseas servers, it doesn't mean that the attacker was in a foreign country.

Dan Wallach, a computer science professor at Rice University, notes that the internet is a "messy place" with a lot of background traffic, and it would be difficult to find its origin because attackers are very good at hiding their location.

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

The report said the website received requests for access from about 100 countries, from all over the world.