NORTH Dakota | Information Technology

Be Legendary.™

NORTH DAKOTA CYBERSECURITY PROGRAM

Re: Assessment of Election Information

Contents

CyOps Analysis Report

Introduction

This report is regarding your request for the NDIT Cyber Operations Team to assess data posted on the thebiglie.frankspeech.com website. Allegations made on this site suggest that specific IP addresses are associated with the voting system in North Dakota and that IP addresses belonging to North Dakota counties were purportedly visited by out-of-state and international IP addresses.

Initial background of Elections Infrastructure:

- The voting system in North Dakota is an air-gapped system and is not connected to the Internet. The voting system is physically isolated, with no Internet connections either directly, indirectly, or wirelessly.
- An Election Security Operations Task Force was formed leading up to the 2020 election cycle. This multi-disciplinary advisory team consisted of members from the NDIT Cyber Operations Center, Secretary of State, North Dakota National Guard, ND Department of Emergency Services - Homeland Security, along with representatives from numerous other state agencies.
- Under the guidance of the Election Security Operations Task Force, an Election Security Operations Center (ESOC) was stood-up and tasked with the mission to identify, protect, detect, respond, and recover to/from threats and/or attacks aimed at disrupting and/or impacting the State of North Dakota's elections, election infrastructure, and/or election results.
- The ESOC actively monitored the election infrastructure in conjunction with the federal Election Infrastructure Information and Sharing Center (EI-ISAC) leading up to, during, and after both, the primary and general election in 2020.

Initial observations of data posted to "frankspeech" site:

- The information provided on the site, "frankspeech," appears to be constructed from uncorrelated data. The longitude and latitude is mismatched and calls into question the validity of the data. PCAP files show TCP/IP traffic and not physical location of assets.
- The data posted to the "frankspeech" site implies that certain source IP addresses communicated with target IP addresses at specific dates and times and that those communications had an impact on election results.
- The data gives no indication as to whether the traffic was blocked, what protocol was used, what port was traversed, or what action, if any, was taken on the alleged systems.
- The data gives no indication if the target IPs were determined to be related to elections infrastructure and, in some cases, does not provide a target IP at all.

Despite concerns with the data, the NDIT Cyber Operations Team agreed to perform an assessment and provide additional context.

Analysis

Analysis by the Cyber Operations Team included the "Source" domains and IP addresses in question with the following findings:

- Some host names indicate that the IP addresses are used for DSL, cable, service providers, or other broadband Internet services that would typically be seen in Internet traffic.

- The existence of such connections originating from foreign countries is not unexpected nor unusual. International IPs are normal on public-facing systems such as websites that are publicly available.

The Cyber Operations Team also reviewed the "destination" domains and IP addresses in question. The results are as follows:

- None of the IP addresses are associated with the North Dakota election infrastructure or the Secretary of State maintained Election Night Reporting (ENR) website.
- Most county websites are hosted out-of-state by third party web hosting and cloud computing companies, despite latitude and longitude numbers indicating otherwise. Again, these items are not typically formatted this way in log files or PCAPs.
- Third party web hosting/cloud providers would not show a location such as Bismarck or Ward County.

Summary

There is no validity to the information regarding North Dakota as it is incomplete. At no time during or after the 2020 election cycle, was any cyber security incident identified that could have affected the confidentiality, integrity, or availability of the North Dakota election infrastructure, information systems, data, or services related to the election process.

Please let us know if you'd like to have further discussions regarding this analysis or if other information is needed.