

SENSITIVE GOVERNMENT AGENCY

SUBSTANTIVE REVISION: Network Defense Notice: Publicly Available U.S. Voter Registration Information for Six U.S. States Downloaded from Commercial Websites by PRC CNE Actor in January 2022; Same Actor Attempts to Download Ohio Voter Registration Application;

[REDACTED]

[REDACTED] This is a revised copy. The State of Oklahoma has been added. In addition, the websites hosting the voter registration records are commercial websites, and that fact has been clarified in the report. Please remove the original report from all manual and computer files.

[REDACTED] Publicly available U.S. voter registration information for six states was downloaded by a PRC, [REDACTED], CNE actor on 14 January 2022. The CNE actor [REDACTED] Colorado, Connecticut, Florida, Michigan, Oklahoma, and Rhode Island voter registration information from U.S. commercial websites and a U.S. IP address. In addition, an Ohio voter registration application was also of interest to the CNE actor, but failed to download.

[REDACTED] Voter registration information from at least 2013 through 2021 is publicly available for download from the commercial websites and it appears the PRC CNE actor downloaded the full repositories. This activity represents newly-identified interest by this PRC CNE actor in U.S. elections, and the PII information obtained - to include names, party affiliations, email addresses, physical addresses, and phone numbers - could, in theory, be leveraged to carry out anything from future CNE operations to election influence operations, although the actual motivations for collecting this information is unknown.

[REDACTED] The victim information was passed to the appropriate agencies for CND response actions. [REDACTED]

[REDACTED] Colorado, Connecticut, Florida, Michigan, Oklahoma, and Rhode Island States' historical U.S. voter registration information from 2013 to 2021 was downloaded by a PRC CNE actor on 14 January 2022 from U.S. commercial websites, and a U.S. IP address hosting, among other things, U.S. state voter registration information. (T1594) [REDACTED] On the same day, an Ohio voter registration application was also of interest to the PRC CNE actor, but failed to download from the U.S. State Government's website .

[REDACTED] While the PRC government has historically demonstrated interest in U.S. elections, this is a newly-identified interest for this individual actor. The U.S. voter registration information is available for public download, with 2021 voter registration information available for some states. The PRC actors could, in theory, leverage the PII information obtained - to include names, party affiliations, email addresses, physical

1. [REDACTED] CISA and the NCJTF CYWATCH have established a Victim Notification process that provides a systematic way to contact organizations during cyber incidents. Before anyone outside of the Federal Cybersecurity Centers contacts a U.S. victim, the notification should be deconflicted through CISA and NCJTF CYWATCH, using the contact information below:

2. [REDACTED] According to the MITRE ATT&CK framework, T1594 describes how adversaries may search websites owned by potential victims for information that can be used during targeting. Victim-owned websites may contain a variety of details, including names of departments/divisions, physical locations, and data about key employees such as names, roles, and contact info. These sites may also have details highlighting business operations and relationships.

addresses, and phone numbers - for anything from future CNE operations to election influence operations, although the actual motivations for collecting this information is unknown.

[REDACTED]

[REDACTED] Election security organizations should be aware that U.S. State voter registration information may be hosted on websites outside the control of government agencies, and that APT actors may harvest voter registration information outside the monitoring of election security organizations.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

