CYBER THREAT INTELLIGENCE INTEGRATION CENTER

14 September 2016

(b)(3) Possible State-Level Election Network Breaches and Related Intrusions

(U/(b)(3) Updates since 7 September 2016 in red.

State	Date of Reported Discovery	Details	Compromise Confirmed?	Data Exfiltrated? (Type)
Alabama	September 2016	(U/(b)(3) MS-ISAC identified IP address 185.104.9.39 targeting an unknown network. This is the same address linked to the compromise of the Illinois State Board of Election website.[1]	No	No
Alaska	September 2016	(U/(b)(3)) MS-ISAC identified 185.104.9.39 targeting an unknown network.[2]	No	No
Arizona	June 2016	(U//(b)(3) An unknown actor viewed a statewide voter registration database after obtaining a state employee's credentials through phishing and keystroke logging malware via 185.104.9.39, according to a private-sector DHS partner claiming secondhand access.[3] The actor used the credentials to access the database and was in a position to modify county, but not statewide, data.	Yes	No
California	September 2016	(U//(b)(3) MS-ISAC identified 185.104.9.39 targeting an unknown network.[4]	No	No

CYBER THREAT INTELLIGENCE INTEGRATION CENTER

14 September 2016

(b)(3)) Possible State-Level Election Network Breaches and Related Intrusions

(U//(b)(3) Updates since 7 September 2016 in red.

State	Date of Reported Discovery	Details	Compromise Confirmed?	Data Exfiltrated? (Type)
(b)(1), (b)(3)				
Colorado	September 2016	(U//(b)(3)) Colorado voters are receiving automated calls advising that their registration is incorrect and needs to be updated before they can receive a ballot for the November election, according to DHS information.[6]	Unknown	No
Connecticut	September 2016	(U//(b)(3)) MS-ISAC identified 185.104.9.39 targeting an election-related network.[7]	No	No
Delaware	September 2016	(U//(b)(3) MS-ISAC identified 185.104.9.39 targeting an election-related network.[8]	No	No
Florida	August 2016	(U//(b)(3)) MS-ISAC reported that the Florida State Board of Elections website communicated with 185.104.9.39, according to DHS information.[9] The actor attempted an SQL injection, but the traffic was blocked at the firewall, according to DHS information.[10]	No	No

CYBER THREAT INTELLIGENCE INTEGRATION CENTER

14 September 2016

(b)(3)) Possible State-Level Election Network Breaches and Related Intrusions

(U//(b)(3)) Updates since 7 September 2016 in red.

State	Date of Reported Discovery	Details	Compromise Confirmed?	Data Exfiltrated? (Type)
Florida	August 2016	(b)(3), (b)(7)(E)	Yes	(b)(3), (b)(7)(E)
Illinois	July 2016	(b)(3), (b)(7)(E)	Yes	(b)(3), (b)(7)(E)
Iowa	September 2016	(U//(b)(3)) MS-ISAC notified Iowa officials that a website associated with the Secretary of State was communicating with 185.104.9.39.[17]	No	No

CYBER THREAT INTELLIGENCE INTEGRATION CENTER

14 September 2016

(b)(3)) Possible State-Level Election Network Breaches and Related Intrusions

(U//(b)(3)) Updates since 7 September 2016 in red.

State	Date of Reported Discovery	Details	Compromise Confirmed?	Data Exfiltrated? (Type)
Maryland	August 2016	(U//(b)(3)) Maryland State Board of Elections officials discovered an IP address targeting their network via SQL injections after reviewing an MS-ISAC report regarding election compromises, according to DHS information.[18] The firewall may have been penetrated, but there is no evidence of a compromise.[19]	No	No
Minnesota	September 2016	(U//(b)(3) MS-ISAC identified 185.104.9.39 targeting an election-related network.[20]	No	No
New York	September 2016	(U//(b)(3)) Spear phishing attempt targeted Suffolk County, NY, elected officials.[21]	No	No
North Dakota	August 2016	(U//(b)(3) MS-ISAC notified NCCIC that state officials had identified malicious activity on voting infrastructure from 185.104.9.39; attempted SQL injection.	No	No
Ohio	August 2016	(U//(b)(3)) State election-related website communicated with 185.104.9.39.[22] MS-ISAC cannot determine the nature of the communications.	Unknown	Unknown

(b)(3) Possible State-Level Election Network Breaches and Related Intrusions

(U//(b)(3) Updates since 7 September 2016 in red.

State	Date of Reported Discovery	Details	Compromise Confirmed?	Data Exfiltrated? (Type)
Ohio	August 2016	(U//(b)(3) The MS-ISAC informed NCCIC of a potential compromise of the Ohio voter registration database.[23] (b)(3), (b)(7)(E) [redacted]	No	(b)(3), (b)(7)(E) [redacted]
Oklahoma	September 2016	(U//(b)(3)) MS-ISAC identified 185.104.9.39 targeting an election-related network.[24]	No	No
Oregon	September 2016	(U//(b)(3)) MS-ISAC identified 185.104.9.39 targeting an unknown network.[25]	No	No
Pennsylvania	March 2016	(U) An individual was attempting to sell on an Internet forum a database purportedly containing 600,000 Pennsylvania voter information records, according to a report from an information security firm.[26]	No	Possibly (Voter database)
Pennsylvania	September 2016	(U//(b)(3)) MS-ISAC identified 185.104.9.39 targeting an election-related network.[27]	No	No

(b)(3)) Possible State-Level Election Network Breaches and Related Intrusions

(U//(b)(3)) Updates since 7 September 2016 in red.

State	Date of Reported Discovery	Details	Compromise Confirmed?	Data Exfiltrated? (Type)
Tennessee	September 2016	(U//(b)(3)) Data extracted from a Tennessee charitable donation website via 185.104.9.39, according to DHS information.[28]	Yes	Yes (Names and Addresses; 4 to 5 GB)
Texas	September 2016	(U//(b)(3)) MS-ISAC identified 185.104.9.39 targeting an election-related network.[29]	No	No
Vermont	August 2016	(b)(3), (b)(7)(E)	Yes	(b)(3), (b)(7)(E)
Virginia	September 2016	(U//(b)(3)) MS-ISAC identified 185.104.9.39 targeting an election related network.[31]	No	No
Washington	September 2016	(U//(b)(3)) MS-ISAC identified 185.104.9.39 targeting an election-related network.[32]	No	No
Wisconsin	September 2016	(U//(b)(3)) MS-ISAC identified 185.104.9.39 targeting an unknown network.[33]	No	No

(b)(3)) Possible State-Level Election Network Breaches and Related Intrusions

(U/(b)(3)) Updates since 7 September 2016 in red.

State	Date of Reported Discovery	Details	Compromise Confirmed?	Data Exfiltrated? (Type)
Multiple States	August 2016	(U//(b)(3)) MS-ISAC reported to DHS that it observed voter registration information for Pennsylvania, Delaware, Rhode Island, and Washington available for sale on the dark web.[34] However, voter registration data for each of these states is made publicly available by state election authorities; thus, its presence on the dark web is unlikely the result of a breach.	No	Unlikely (Voter registration data)
Other—Election commission central server	October 2015	(U/(b)(3) A Russian-speaking cybercriminal offered to sell a database containing the personal information of approximately 190 million Americans from 49 states, according to DHS reporting.[35] The cybercriminal claimed the database had been copied from a "central server of the election commission"—the list of people who had voted in the election. However, an ongoing US Secret Service investigation revealed that the data is an aggregation of publicly available voter registration data which the criminal appeared to have obtained from a US company.[36]	No	No

(U) Sources

(b)(1), (b)(3), (b)(7)(E) [redacted]

CYBER THREAT INTELLIGENCE INTEGRATION CENTER

14 September 2016

(b)(1), (b)(3), (b)(7)(E) [redacted]