Page 01

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

~~-FOR OFFICIAL USE ONLY-~~

~~-Privileged Information/Pre-Decisonal and Deliberative-~~

Election Task Force Minutes

Wednesday, October 25, 2017

Conducted by (b)(6)

(b)(5); (b)(6)

Page 03

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 04

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 05

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 06

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 07

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 08

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 09

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 10

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 11

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 12

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 13

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 14

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 15

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 16

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 17

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 18

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act


NCCIC
NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

(b)(5); (b)(7)(E)

Page 20

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 21

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 22

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 23

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 24

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 25

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 26

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 27

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 28

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 29

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 30

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 31

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 32

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 33

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 34

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 35

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 36

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 37

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 38

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 39

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 40

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 41

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 42

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 43

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 44

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 45

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 46

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

TLP: GREEN
MS-ISAC CYBER ALERT

TO: All MS-ISAC Members, Fusion Centers, and IIC partners

DATE ISSUED: August 1, 2016

SUBJECT: Voter Registration Database Activity and RFI - TLP: GREEN

MS-ISAC is aware of three incidents that may or may not be linked - a cyber threat actor purportedly selling state voter registration databases on the darknet, open source reporting of a cybersecurity researcher who found an open database of U.S. voter records, and a compromised state's voter registration database records. At this time MS-ISAC is not aware of a link between any of the three events, but is providing the following information so that state's may query their Board of Election weblogs for suspicious activity and enable additional security precautions -- MS-ISAC would greatly appreciate the results (positive and negative) of the query.

- According to open source reporting, an actor calling himself "DataDirect" is purportedly selling U.S. voter registration databases on the darknet marketplace "The Real Deal" for 0.5 BTC (approximately $340.38) per state. The records are also offered at a discounted bulk rate of 12 bitcoin (approximately $7,800) for all 50 states. The listing was posted on or about July 16, 2016.
- In December 2015, according to open source reports, a cybersecurity researcher claimed to identify a public-facing database containing 191 million U.S. voter records. According to the security researcher that database was available on the Internet for an indeterminate period of time, at least several weeks, and included the voter's full names, home and mailing addresses, DOBs, email addresses, telephone numbers, party affiliations, and other voter-related information.
- In late June 2016, an unknown actor scanned a state's Board of Election website for vulnerabilities using Acunetix, and after identifying a Structured Query Language (SQL) injection (SQLi) vulnerability, used SQLmap to target the state website. The majority of the data exfiltration occurred in mid-July. There were 7 suspicious IPs and penetration testing tools Acunetix, SQLMap, and DirBuster used by the actor, detailed in the indicators section below.

Indicators associated with the Board of Elections intrusion:

- The use of Acunetix tool was confirmed when "GET /acunetix-wvs-test-for-some-inexistent-file – 443" and several requests with "wvstest=" appeared in the logs;
- The user agent for Acunetix was identified in the logs - "Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.21+(KHTML,+like+Gecko)+Chrome/41.0.2228.0+Safari/537.21";
- The use of SQLMap was confirmed after "GET /status.aspx DLIDNumber=1';DROP TABLE sqlmapoutput" appeared in the logs;

- The user agent for SQLMap is "Mozilla/5.0+(Macintosh;+U;+Intel+Mac+OS+X+10.7;+en-US;+rv:1.9.2.2)+Gecko/20100316+Firefox/3.6.2 200 0 0 421" (These are easily spoofed and not inclusive of all SQLMap activity);
- The user agent for the DirBuster program is "DirBuster-1.0-RC1+(http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)";
- 185.104.11.154
- 185.104.9.39
- 204.155.30.75
- 204.155.30.76
- 204.155.30.80
- 204.155.30.81
- 89.188.9.91

RECOMMENDATIONS:

MS-ISAC is requesting that states contact their Board of Elections and determine if any similar activity to the third event has been detected. This will help determine if this is a standalone incident or associated in some way to DataDirect' s files for sale on the darknet.

MS-ISAC is aware of additional interest in state Board of Election databases and we recommend all states take the following precautions:

- Conduct vulnerability scans on local government and law enforcement websites and promptly remediate any vulnerabilities (or contact your hosting provider to do so on your behalf). Particular attention should be paid to SQLi vulnerabilities. Website hosting providers should also pay attention to vulnerabilities on other websites on the same server, which may provide a back-door into the local government's website.
- Ensure all software and applications, especially content management software, are fully patched.
- Create custom, general error messages for the web application to generate, as malicious cyber actors can gain valuable information, such as table and column names and data types, through default error messages generated by the database during a SQLi attack.
- Validate user input prior to forwarding it to the database. Only accept expected user input and limit input length. This can be done by implementing a whitelist for input validation, which involves defining exactly what input is authorized.
- Implement the principle of least privilege for database accounts. Administrator rights should never be assigned to application accounts and any given user should have access to only the bare minimum set of resources required to perform business tasks. Access should only be given to the specific tables an account requires to function properly.
- The database management system itself should have minimal privileges on the operating system, and since many of these systems run with root or system level access by default, it should be changed to more limited permissions.
- Isolate the web application from the SQL instructions. Place all SQL instructions required by the application in stored procedures on the database server. The use of user-created stored procedures and prepared statements (or parameterized queries) makes it nearly impossible for a user's input to modify SQL statements because they are compiled prior

to adding the input. Also, have the application sanitize all user input to ensure the stored procedures are not susceptible to SQLi attacks.
- Use static queries. If dynamic queries are required, use prepared statements.
- Enable full logging on web servers and email servers to aid in forensic and legal responses if a breach does occur.

If you experience similar targeting, please do not hesitate to reach out to the MS-ISAC for assistance on this matter. We perform a variety of free incident response services including log analysis, malware analysis, computer forensics, and can assist with the development of a mitigation and recovery strategy.
Requests for these services can be obtained by calling 1-866-787-4722 or sending an email to SOC@msisac.org

Center for Internet Security (CIS)
Integrated Intelligence Center (IIC)
Multi-State Information Sharing and Analysis Center (MS-ISAC)
1-866-787-4722 (7×24 SOC)
Email: soc@cisecurity.org
www.cisecurity.org
Follow us @CISecurity

TLP: GREEN

(Go to www.us-cert.gov/tlp and copy the appropriate "How may it be shared?" description).
http://www.us-cert.gov/tlp/

Page 50

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 51

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 52

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 53

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 54

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 55

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 56

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 57

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 58

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 59

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 60

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 61

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 62

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 63

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

~~(U)~~ ELECTION INFRASTRUCTURE CYBER RISK CHARACTERIZATION

~~(U)~~ September 2016

NATIONAL PROTECTION AND PROGRAMS DIRECTORATE

OFFICE OF CYBER AND INFRASTRUCTURE ANALYSIS

/

Page 65

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 66

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 67

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 68

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 69

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 70

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 71

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 72

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 73

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 74

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 75

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 76

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 77

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 78

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 79

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 80

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

FROM: Office of Infrastructure Protection

TO: Critical Infrastructure Community Stakeholders

SUBJECT: *CRITICAL INFRASTRUCTURE STAKEHOLDER CONFERENCE CALL – FOLLOW UP TECHNICAL DISCUSSION OF THE JOINT ANALYSIS REPORT (JAR)*

Public and Private Sector Partners,

Following up on initial discussion of the recently released Joint Analysis Report (JAR), you are invited to participate in a Critical Infrastructure Stakeholder Conference Call, held by the Department of Homeland Security (DHS), Office of Infrastructure Protection. The purpose of the call is to provide a technical discussion of the JAR released by DHS and the FBI. Attendees are welcome from all sectors. The focus of the discussion will be on mitigating activities and addressing any technical questions from stakeholders.

The JAR provides information on the Russian intelligence services activities to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. government, political, and private sector entities. The JAR also includes recommended mitigations, and information on how to report such incidents to the U.S. government.

Attached you will find a copy of the JAR.

Date and Time: Friday, December 30, 2016, 11:30 a.m. EST

Point of Contact: NICC, (b)(6)

Conference Bridge: Dial-in: (b)(6) Participant Code: (b)(6)

Respectfully,

National Infrastructure Coordinating Center
National Protection and Programs Directorate
Office of Infrastructure Protection
Department of Homeland Security
(b)(6)

~~-FOR OFFICIAL USE ONLY-~~

~~Privileged Information/Pre-Decisonal and Deliberative~~

Election Task Force Minutes

Wednesday, October 11, 2017

Conducted by (b)(6)

(b)(5); (b)(6)

Page 83

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 84

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 85

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 86

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 87

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act

Page 88

Withheld pursuant to exemption

(b)(5) ; (b)(6)

of the Freedom of Information and Privacy Act