How the Russians penetrated Illinois election computers

SQL, an acronym for Structured Query Language, is a database programming language. An "SQL injection" is a common piece of cyber-trickery used to illegally gain access to government, financial, business and private computers. Experts estimate that 8 of every 10 data breaches occur as a result of SQL injection.

The favored tactic of hackers usually begins with certain commands typed on a public web form and ends with broad access to the site's server. In the case of Illinois, after hackers typed a specially-crafted code into the election database search box, records were stolen and the board had to shut down registration for ten days.

"Processor usage had spiked to 100% with no explanation" state investigators determined. "Analysis of server logs revealed that the heavy load was a result of rapidly repeated database queries on the application status page of the Paperless Online Voter Application (POVA) web site" they said.
DDoS Attack Hits Knox County, TN Results Reporting Site On Election Night

By Doug Chapin   May 7, 2018
North Carolina’s elections board provided this image to state lawmakers in a December 2017 presentation. - State Board of Elections and Ethics Enforcement
Ransomware

Six days after a ransomware cyberattack, Atlanta officials are filling out forms by hand

By Kimberly Hutcherson, CNN
Updated 3:00 PM ET, Wed March 28, 2018

City of Atlanta Needs $9.5 Million More for Ransomware Recovery

According to multiple sources, the City of Atlanta will need to find another $9.5 million to recover from the "SamSam" ransomware attack which brought their city government to a grinding halt. The number of applications and government services impacted by the attack has been revealed to be far greater than originally estimated, with the attack even affecting applications of the city police department and court system.
RANSOMWARE THUGS EXTORT INDIANA COUNTY FOR OVER $130,000 IN BITCOIN

Matt Masterson
February 12, 2020
A Cybersecurity Breach at Equifax Left Pretty Much Everyone's Financial Data Vulnerable

For Americans who want to protect their personal information, there is no way, in our current system, to do so.
Fed-up fatties kill aerobics instructor!

Thousands of gals want to marry Mr. Fuzzy-wuzzy!
Cybersecurity – Common Attacks

- Social Engineering
  - Spear-phishing
- Hacking
  - SQL Injection
  - Port scans
  - Man in the Middle (MITM) Attacks
- Distributed Denial of Service (DDoS)

- Information Operations
  - Leaking stolen information
  - Spreading false or misleading information
  - Amplifying divisive content
  - Interrupting service to public facing online resources
## Top Vulnerability Findings Across All Assessments

<table>
<thead>
<tr>
<th>Finding Description</th>
<th>EI Entities</th>
<th>SLTT Governments</th>
<th>Federal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spearphishing susceptibility</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Spearphishing weakness</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Patch management</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Administrator password reuse</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Insecure default configuration</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Clear text password disclosure</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Unsupported operating system or application</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Easily guessable credentials</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Weak password policy</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
This service tracks and reports the vulnerabilities identified for each system scanned and rates the most severe vulnerabilities identified as a “high” or “critical” severity level. While comparing the raw count of vulnerabilities, or vulnerabilities per sector, is statistically misleading, a comparison of the vulnerabilities, averaged per stakeholder group, provides a snapshot in time to compare across stakeholder groups.
The time it takes to mitigate vulnerabilities can be important information about the “health” of a network.

### Average time for entities to mitigate vulnerabilities (in days)

<table>
<thead>
<tr>
<th>Group</th>
<th>Time to Mitigate Critical</th>
<th>Time to Mitigate High</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>102.4</td>
<td>109.8</td>
</tr>
<tr>
<td>Federal</td>
<td>7.1</td>
<td>34</td>
</tr>
<tr>
<td>SLTT</td>
<td>185.4</td>
<td>205.3</td>
</tr>
<tr>
<td>EI</td>
<td>281.8</td>
<td>346.9</td>
</tr>
</tbody>
</table>

**Note:**

- **EI** stands for **Electronic Information**.
- The chart compares the average time it takes for entities to mitigate critical and high vulnerabilities.
- Federal entities have the shortest average time for both critical and high vulnerabilities.
- The Electronic Information (EI) category has the longest average time for both critical and high vulnerabilities.
Phishing remains one of the primary attack paths used by threat actors. As part of their assessment offerings, DHS provides focused PCAs. The amount of an organization’s users that click on the DHS phishing email—called user click rates—and the ratio of users that interact with a potentially malicious email can often indicate the success, or lack thereof, of an organization’s user training and awareness.

### Stakeholder Group

<table>
<thead>
<tr>
<th>Stakeholder Group</th>
<th>Median percentage of user click rates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Election Infrastructure entities</td>
<td>6.15%</td>
</tr>
<tr>
<td>SLTT Government entities</td>
<td>6.91%</td>
</tr>
<tr>
<td>Federal entities</td>
<td>6.05%</td>
</tr>
<tr>
<td><strong>Total user click rate across all assessments</strong></td>
<td><strong>6.71%</strong></td>
</tr>
</tbody>
</table>
With so many factors…

Things that matter

Things you can control

Where you should focus!
CISA Gears Up For 2020 Election Security

#PROTECT2020

cisa.gov
“Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”

16 Sectors: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials and Waste; Transportation Systems; and Water and Wastewater Systems.

  - See https://www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf
The 2017 designation of election infrastructure as critical infrastructure provides a basis for the Department of Homeland Security and other federal agencies to:

- Recognize the importance of these systems;
- Prioritize services and support to enhancing security for election infrastructure;
- Provide the elections community with the opportunity to work with each other, the Federal Government, and through the Coordinating Councils;
- Hold anyone who attacks these systems responsible for violating international norms.
My team’s mission: To ensure the Election Infrastructure Community has the necessary information to adequately assess risks and protect, detect, and recover from those risks.

- CISA can provide you free services and assessments for cyber and physical security
  - ncciccustomerservice@hq.dhs.gov

- We share tailored information through the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)
  - https://www.cisecurity.org/ei-isac/
CISA’s #PROTECT2020 Initiative

WHO WE SUPPORT

State and Local Election Authorities
Election Technology Providers
Campaigns and Political Infrastructure
Electorate

WHO WE PARTNER WITH

Federal, State, & Local Government Agencies
Academic Institutions and Think Tanks
Non-Governmental Organizations (NGOs)
Media, Tech, & Social Media Companies
Cybersecurity/Threat Assessment Firms

#PROTECT2020

1. Support the security efforts of the election community – elections officials and technology providers.
2. Advise and support the security of campaigns and political infrastructure.
3. Raise awareness of and build resilience against the threat of foreign influence operations.
4. Improve Warning and Response.
CISA’s Support to Election Community

- Increase engagement and support provided to local election officials
- Raise awareness regarding the need for regular investment in election infrastructure
- Further develop CISA’s understanding and conversations about risks to election infrastructure
- Improve communications and information sharing across the subsector
- CISA resources available to election officials and technology providers to #PROTECT2020
- Increase support to election system private sector
Vulnerability Scanning

- A scanning of internet-accessible systems for known vulnerabilities on a continual basis. As potential issues are identified, CISA notifies impacted customers so they may proactively mitigate risks to their systems prior to exploitation. Conducted remotely and fully automated.

Remote Penetration Testing

- Utilizes a dedicated remote team to assess and identify vulnerabilities and work with customers to eliminate exploitable pathways. The assessment simulates the tactics and techniques of malicious adversaries and tests centralized data repositories, externally accessible assets, and web applications.

Phishing Campaign Assessment

- Measures the susceptibility of an organization’s staff to social engineering attacks, specifically email phishing attacks. The assessment takes place during a six-week period. An assessment report is provided two weeks after its conclusion. The assessment report provides guidance, measures effectiveness, and justifies resources needed to defend against and increase staff training and awareness of generic phishing and spear-phishing attacks.

To request services email: NCCICcustomerservice@hq.dhs.gov
Physical Support Services

- Protective Security Advisors Serving 73 districts in 50 states and Puerto Rico
- Protective Security Advisors (PSAs) serve as the link to CISA infrastructure protection resources and the Federal Emergency Management Agency (FEMA).
  - Trained in the physical aspects of infrastructure protection, PSAs share information and conduct resilience surveys and vulnerability assessments
- PSAs assist facility owners and operators with resources, training, and access to other DHS products and services. For more information, or to reach your local PSA, contact nicc@hq.dhs.gov.
Join the EI-ISAC

• Provides cybersecurity support to SLTT governments.
• Furthers DHS efforts to secure cyberspace by distributing early warnings of cyber threats to SLTT governments.
• Shares security incident information and analysis.
• Runs a 24/7 watch and warning security operations center.
• Operates an election threat warning center, the Election Infrastructure-ISAC.
• Funded by DHS.

For more information, see https://www.cisecurity.org/ei-isac
Election Infrastructure: Information Sharing

Membership

- 50 State Election Offices
- Over 2000 Local Election Offices (49 states)
- 5 Territorial Election Offices
- 7 Election Official Associations
- 17 Election Vendors

Albert Sensor Coverage

- 50 State Election Sensors
- 24 Bottom-Up Local Election Sensors
- 78 State-Funded Local Election Sensors
- 2 Territorial Election Sensors
Ransomware is a type of malicious software designed to deny access to a computer systems or data until a ransom is paid.

If ransom demands are not met, the system or encrypted data remains unavailable, or data may be deleted.

In elections this could be used to deny access or delete Voter Registration and/or Vote Tabulation data.
Prepare for Ransomware

- Utilize CISA Services (NCCICcustomerservice@hq.dhs.gov)
  - Remote Penetration Testing (RPT)
  - Vulnerability Scanning

- Develop an Incident Response Plan

- Create Backups
  - Backup your data regularly
  - Have access to your software and source code in case you need to rebuild the system

- Test your plans and backups
Breaking Down Information Operations

INTERFERENCE IN ACTION: MAPPING INFORMATION OPERATIONS

GOAL: Strategic, Operational, Tactical?

RESEARCH/POSITIONING
What preparations were necessary to carry out this campaign?
In attacks of opportunity there may be none

KEY TAKEAWAYS
Lessons we can learn and apply across case studies

PRODUCTION
Content development includes:
- Images
- Articles
- Videos
- Websites
- E-mails
- Social media posts

COUNTERING INFORMATION OPERATIONS

PREVENT

RESPOND

MITIGATE

PUBLIC AND AMPLIFICATION
- How do they get their content out?
  - Event invites
  - Fake social media accounts
  - Bot accounts
  - Suspicious websites
  - Phone calls
  - Internet forums, including Darknet forums

Matt Masterson
February 12, 2020
Case Study: Louisiana Chemical Attack -- Russia

**Goal:** Undetermined. Breadth of techniques used on a limited scale could indicate testing in U.S.

**Research/Logistics**
- Access to cell phone numbers in local area
- Established social media accounts and bots
- Developed targeted media and key influencers list

**Production**
- Content developed includes:
  - Fake surveillance camera footage
  - Doctored images of flames engulfing plant
  - Fake YouTube video showing ISIS claiming responsibility
  - Wikipedia page content
  - Doctored CNN webpage showing disaster had made national news
  - Text messages and social media messaging

**Publication and Amplification**
- Text messages to local residents
- Hundreds of Twitter accounts posting about “disaster” using hashtag #ColumbianChemicals and doctored images/videos
- Tweets targeting reporters at local and national media – New Orleans Times-Picayune, CNN, and NYT
- Tweets targeting political commentators

Building Public Awareness

- War on Pineapple
  - Bring a non-divisive issue to the forefront to show how it could be used to sow discord
  - Raise awareness
  - Educate public on how they can mitigate the risk

**Disinformation Stops With You**
You have the power to stop foreign influence operations. Follow these steps:

- Talk to your circle
- Recognize the risk
- Question the source
- Investigate the issue
- Think before you link
Top Recommendations Provided Across All EI Assessments

1. Defend
   - Ensure all aspects of voting system are air gapped
   - Update all software patches
   - Review and update system configurations & access controls
   - Manage passwords & Implement multi-factor authentication

2. Detect
   - Join EI-ISAC: https://learn.cisecurity.org/ei-isac-registration
   - Have awareness and monitoring of your systems
   - Protect and detect malware - viruses, spyware, ransomware
   - Educate employees and pollworkers

3. Recover
   - Take regular backups & test them
   - Provisional ballot/backup ballot preparation
   - Auditable ballots & conduct audits
   - PLAN, PLAN, PLAN, PLAN

4. TAKE ADVANTAGE OF ALL AVAILABLE RESOURCE