ELECTION INFRASTRUCTURE TRENDS REPORT

Election Infrastructure Report

Population: Election Infrastructure (EI) Subsector entities (EI entities).

Timeframe: Fiscal Year (FY) 2019.

Analysis: The report aggregates and analyzes non-attributable data gathered from EI entities that engaged in CISA's Cyber Hygiene (CyHy) persistent vulnerability scanning and Cybersecurity Assessments.

Note: Due to the limited sample size, the presented data should not be considered a rigorous statistical representation of the complex and varied EI entities that exist within the United States.

Eye on Elections: Looking More, Finding More

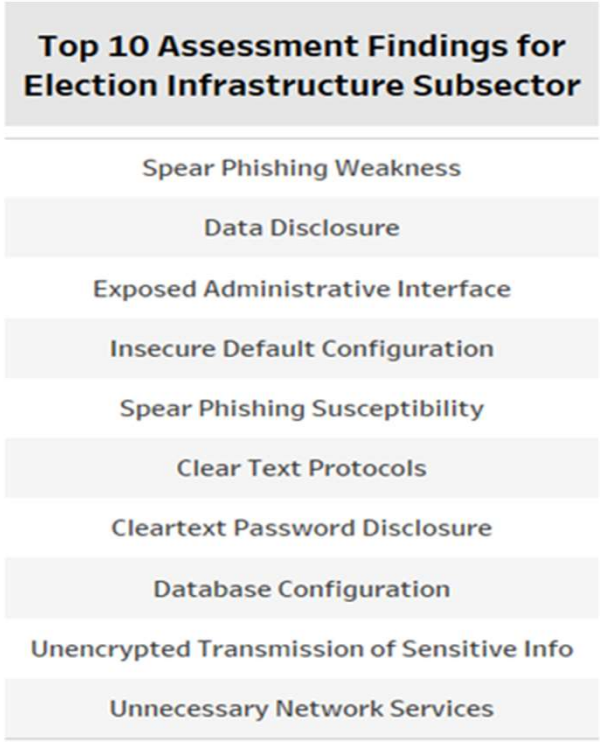
More sensors, more cyber firms, more eyes on elections have increased the awareness of cyber threats.

What we're seeing:

- Commodity malware – computer viruses available for purchase and use by nearly anyone
- Most are tools designed to target and hack various sectors
- On election networks, not necessarily targeting them but having an impact on election networks either directly or indirectly (see: Ransomware)
- Malware analysis, command and control indicators, and alerts being pushed by CISA through the EI-ISAC.

Significant Findings

- Assessments revealed that administrator credentials can be accessed.
- EI entities rely on a Microsoft domain architecture for a significant part of their user security.
- EI entities have a direct connection to other entities that support EI Subsector activities that could be used to access EI systems.
- Assessments revealed that in some cases assessors were allowed to access and modify election data.



* Presented in order of most commonly identified within the assessed population.

Top EI Critical and High Vulnerabilities

Top Critical Vulnerabilities

Vulnerability	EI Rank	EI %	Non-EI Rank	Non-EI %
PHP Unsupported Version Detection	1	21%	1	22%
Microsoft IIS 6.0 Unsupported Version Detection	2	12%	5	4%
MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)	3	11%	3	5%
Microsoft Windows Server 2003 Unsupported Installation Detection	4	7%	13	3%
Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	5	7%	6	4%
Microsoft Exchange Server Unsupported Version Detection (Uncredentialed)	6	4%	21	1%
Unix Operating System Unsupported Version Detection	7	4%	2	7%
OpenSSL Unsupported	8	3%	12	3%
PHP < 5.2.12 Multiple Vulnerabilities	9	3%	16	2%
Netatalk OpenSession Remote Code Execution	10	2%	17	1%

Top High Vulnerabilities

Vulnerability	EI Rank	EI %	Non-EI Rank	Non-EI %
SSL Version 2 and 3 Protocol Detection	1	52%	1	39%
Unsupported Web Server Detection	2	3%	3	3%
nginx 1.9.5 < 1.16.1 / 1.17.x < 1.17.3 Multiple Vulnerabilties	3	3%	2	7%
Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities	4	2%	4	3%
PHP 7.2.x < 7.2.16 Multiple vulnerabilities.	5	2%	14	1%
SSH Protocol Version 1 Session Key Retrieval	6	2%	5	2%
NTMail3 Arbitrary Mail Relay	7	1%	25	1%
PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution	8	1%	8	2%
Apple Mac OS X Find-By-Content .DS_Store Web Directory Listing	9	1%	21	1%
SNMP Agent Default Community Name (public)	10	1%	27	1%

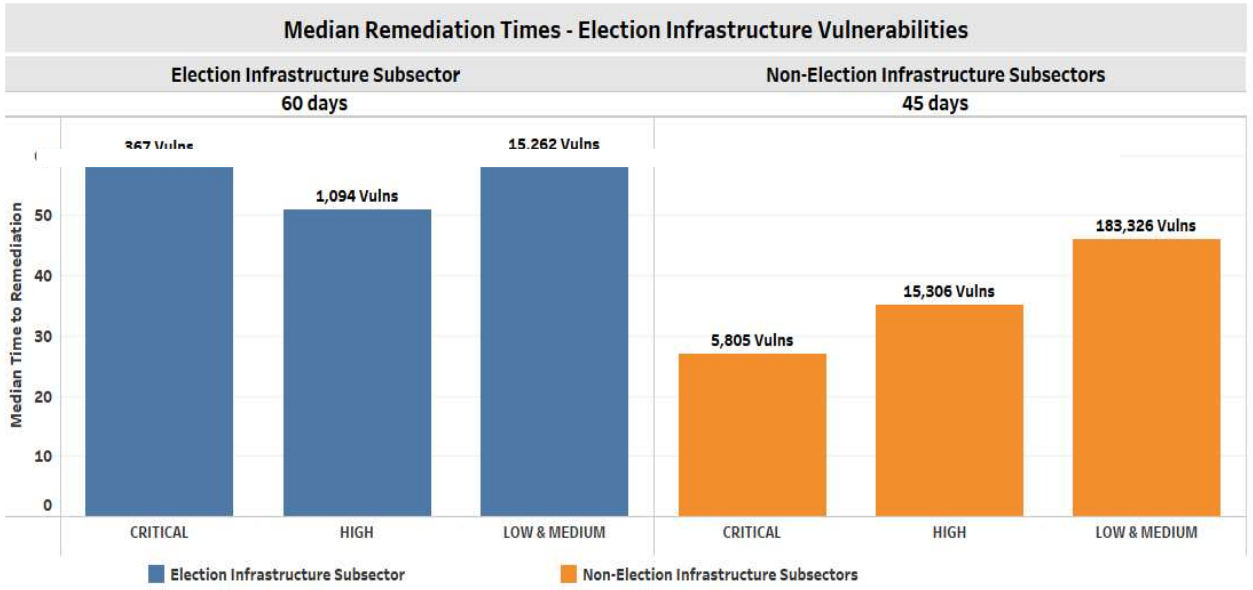
[+] Percentages reflect the assessed population found with a critical or high vulnerability.

Election Infrastructure Sector looks similar to other critical infrastructure sectors.

In FY19, EI and Non-EI sectors share many high and critical vulnerabilities findings

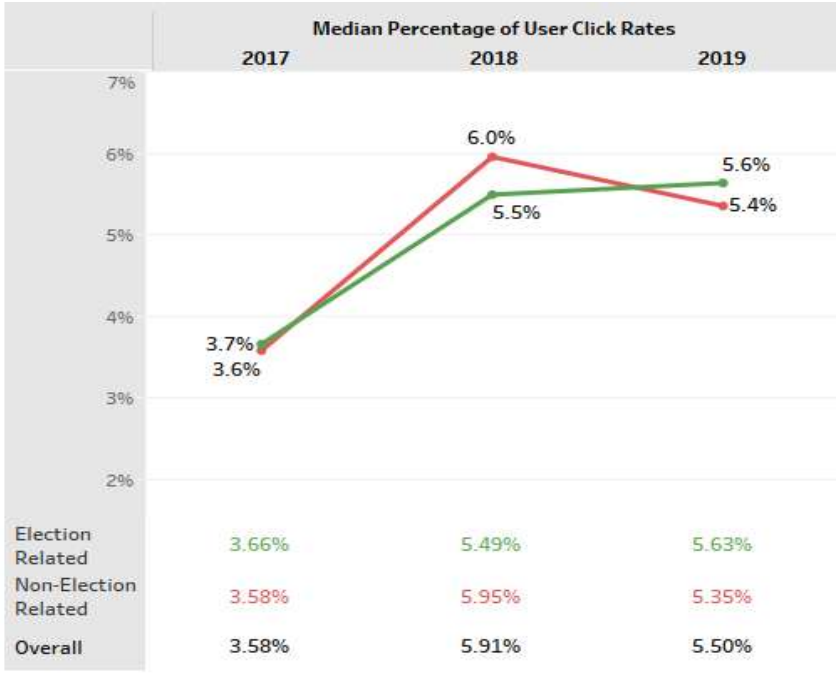
EI Vulnerability Remediation Time

- Assessed EI entities' median vulnerability remediation times:
  - Critical ~60 days
  - High ~50 days
  - Low and Medium ~60 days
- EI entities recorded a longer median time to remediation than Non-EI entities.



* Median remediation times reflect those within the assessed population, not the entire EI Subsector.

Phishing Campaign Click Rates

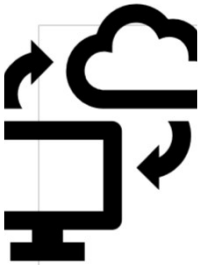


	2017	2018	2019
Election Related	3.66%	5.49%	5.63%
Non-Election Related	3.58%	5.95%	5.35%
Overall	3.58%	5.91%	5.50%

* Percentages reflect the assessed population, not the entire EI or Non-EI populations.

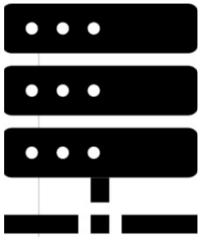
- A total of 8,078 email targets were sent out to EI entities in 2019. Of those targets, 5.63% unique users clicked the malicious email link or attachment.
- The median click time for EI users who clicked on an malicious email was 64 minutes after receiving the email.
- EI entities had a slightly higher click rate than Non-EI sector entities in 2019.

What to do?



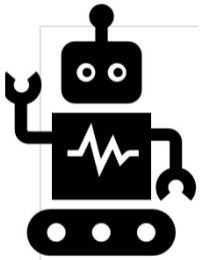
Continue

- Patching Vulnerabilities
- Receiving timely information from EI-ISAC
- Security Awareness Training/ Phishing Awareness
- Password management/ and Role based access controls



Implement

- Network Segmentation
- Multifactor Authentication
- Enable Unified Audit Log
- Disable legacy protocol authentication
- Consent to monitor banner



Consider

- Out-of-cycle Password and token reset
- Reporting suspicious behaviors

Network Segmentation

- **CISA has seen very flat networks that should be segmented to prevent attacks that could impact election infrastructure.**
- Segment more than just your voting infrastructure
  - Is the local county clerk's or registrar's office network segmented from any other parts of the county?
- Adversaries may not always be looking to attack what directly impacts the election, but rather another vulnerable part of the network then pivot over or impact it such as ransomware.
- Think about vectors of attack, if another part of the state or localities were to undergo an attack, would it impact anyone that could impact elections related work?

Credential Management

- **DHS CISA has observed instances where several people in election related offices have been sharing passwords over e-mail or default password are being used.**
- **DHS CISA has observed numerous phishing attacks where all it took is one user to give up their pw on a credential harvesting site and adversaries have taken control of e-mail accounts and can read all e-mails in that users in box.**
- Password Management
  - How are passwords to sensitive systems being stored? Are they being stored electronically?
  - Are they being shared among people within an office electronically?
- Multi-Factor Authentication
  - Having Multi-Factor Authentication turned on to access e-mail or any part of your environment is must.

What do these findings mean?

- Attack paths and vulnerabilities for Election Infrastructure enterprise network environments are comparable to those of other Critical Infrastructure sectors
- Election data to include voter registration data is at risk of being accessed and modified by attackers.
- Many of these risks can be mitigated by implementing basic cybersecurity best practices and cyber hygiene principles
  - MFA
  - Access Controls
  - Patching & Upgrades
- Empower your IT staff and support your locals!

Stay Informed of Critical Vulnerabilities

New Critical Vulnerabilities announced in July 2020

- SAP Netweaver AS Java
- F5 BIG-IP TMUI RCE
- Windows DNS Server

Locals need to patch these vulnerabilities

Enroll in EI-ISAC https://www.cisecurity.org/ei-isac/

Enroll in CISA CyHy Email: Central@cisa.dhs.gov

Share with your Locals Please!

Working Remotely

- Significant telework introduces additional cybersecurity and operational risks to be managed
- Greater reliance on virtual private networks and a shift in focus to the pandemic has presented opportunities for malicious cyber actors

DO:

- Use only approved collaboration tools (e.g. chat or conferencing software)
- Study and follow your organization's policies on telework and physical & information security
- Use only approved methods to share files
- Use only devices owned, managed, and protected by your organization whenever possible

DON'T:

- Use personal equipment for work purposes, and vice versa
- Leave devices unlocked and unattended
- Send sensitive content unencrypted
- Share devices that are used for work
- Forward work emails to personal accounts
- Connect to a network you don't own and control (e.g. public Wi-Fi)

How reporting helps protect everyone

- DHS CISA has seen an increase in phishing on a variety of topics, some with stealing passwords or account info, some downloading files leading to malware, however it is very hard for us to understand who else is seeing the same phishing attack if it is not being reported.
- The more information that is reported into CISA or the EI-ISAC helps everyone even if a phishing e-mail does not result in a compromise.
- If we identify patterns and or trends we can get them back to you in the community.

New Products

New:

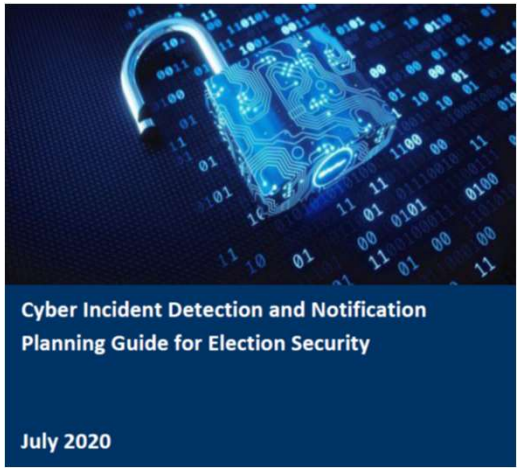
- Cyber Incident Detection and Notification: Incident Response Planning Templates

Coming Soon:

- *Guide to Vulnerability Disclosure for America's Election Administrators*
- COVID-19 Joint WG: Innovative Practices and New Solutions

Reminder:

- See all Covid-19 WG Products: cisa.gov/protect2020



Matt Masterson
Senior Cybersecurity Advisor
Matthew.Masterson@cisa.dhs.gov


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY