Threatscape of the US Election

Discussing Threats and Risk Posed to US Election Infrastructure

Gage Mele
Security Analyst, Anomali
AGENDA

• Current State and Belief of Election Cybersecurity
• Political Views on Cybersecurity
• Likely Targets: Who and What?
• Disinformation
• Conclusion
• Questions
CURRENT STATE AND BELIEF OF ELECTION CYBERSECURITY

- Post 2016 presidential election
  - Wikileaks
  - APT28, APT29
  - “Value” of disinformation

- Designation of US election infrastructure as Critical Infrastructure (January 2017)
  - 17 Critical Infrastructure sectors designated by Department of Homeland Security
CURRENT STATE AND BELIEF OF ELECTION CYBERSECURITY

• Contention by National Association of Secretaries of State (NASS)
  • State vs local
• Election Assistance Commission (EAC)
  • Funding
  • Push for online voter registration
• More targets

https://www.nass.org/about-nass
https://www.eac.gov/
POLITICAL VIEWS ON CYBERSECURITY

• Sen. Ron Wyden writes a letter (April, 2017)
  • Basic cybersecurity practices
  • Two-factor authentication

• House Democrats write letter to Speaker Paul Ryan (December 2017)
  • 18 of 21 states targeted during 2016 election
  • Special Counsel indicts 12 Russians
  • Request assistance from DHS and FBI
  • Cite DEF CON report and vulnerable voting machines
POLITICAL VIEWS ON CYBERSECURITY

- Sen. Amy Klobuchar, James Lankford propose Bill (December 2017)
  - Secure Elections Act (SEA)
  - Paper vs Digital, audits
- Pres. Donald Trump signs Consolidated Appropriations Act (March 2018)
  - $380 million in grants to Help America Vote Act (October 2002)
  - $3-$34 million per state for election security
LIKELY TARGETS: WHO?

• Campaign officials, candidates, candidate family and friends, websites, voters
• Tactics, Techniques, and Procedures (TTPs)
  • Distributed Denial-of-Service (DDoS), timing of attacks
  • Phishing and spear phishing
  • Typosquatting (.democrat, .republican)
• PhishPoint
  • Utilizing legitimate software to bypass security measures
• CVEs
LIKELY TARGETS: WHAT?

- Voter databases
  - Democratic National Committee (August 2018)
  - Data leak, Deep Root Analytics (June 2017)
  - Personally Identifiable Information (PII)
- Voting security and voting machines
  - DEF CON 26, Voting Machine Hacking Village (August 2018)
  - Letter to Election Systems and Software (ES&S) (August 2018)
DISINFORMATION

- Internet Research Agency (IRA)
  - Bots, trolls
  - Small-town media
  - Impersonation, Chicago Daily News
  - Patience, long-term
- Social media organizations
  - Reddit – removed 1,000 accounts (April, 2018)
  - Facebook – removed 32 pages (July, 2018)
- Political organizations
  - Democratic Congressional Campaign Committee (DCCC)
  - National Republican Congressional Committee (NRCC)
  - New software, social media platforms
CONCLUSION

• Current State and Belief of Election Cybersecurity
  • Complex by nature
  • Individual voting systems
  • Critical infrastructure designation

• Political Views on Cybersecurity
  • Employing “basic” security, multi-factor authentication
  • Funding for election security

• Likely Targets: Who & What
  • Campaign officials, candidates, family and friends
  • Voter databases, voting machines, websites

• Disinformation
  • IRA
  • Forums, social media, media outlets
  • DCCC, NRCC
ADDITIONAL RESOURCES

Whitepaper
Threatscape of the US Election from Anomali Labs

Whitepaper
United States of America: Anomali Labs Cybersecurity Profile

Whitepaper
CSO Online: The Changing Landscape of U.S. Election Security