Background

The 2016 U.S. presidential election has sparked a wave of politically-fueled hacktivism, leading to cyber assaults on candidates, political parties and governmental IT networks due to political and social affiliations. As protests transition from the streets to cyber channels, those with political influence have become the target of cyber-attacks and should have mitigation plans in place to protect both personal and business holdings. For example, earlier this year Donald Trump became the target of hackers attempting to damage his reputation and business operations.

These politically-fueled cyber assaults often result in prolonged, continuous campaigns, and it is likely these attacks will persist as the U.S. Election Day nears, with potential peaks during major events such as the Republican and Democratic National Conventions in July. Various forms of cyber-attacks should be expected, including physical and digital break-ins, data dumps and denial of service attacks that prevents the flow of real-time data. Apart from cyber assaults, these events pose the risk of hackers entering the venues and using the WLAN to access confidential data.

Hackers could disrupt the U.S. election process in November. A denial of service attack could target voting machines if they're unprotected and connected to the internet, or assault streaming data for those external to the process relying on live updates regarding the results, such as media and voters. Another method would be to target confidential information such as a voter's database, as happened in the Philippines earlier this year. This information could be valuable to an opponent or sold on the Darknet.

Examples of Election-Related Cyber Assaults

- **Philippines** – COMELEC[i] – This year hackers compromised the Philippines election commission and leaked a voter database containing the information of 55 million voters.

- **Bulgaria** – Commissions Website[ii] - In October 2015, hackers launched a denial of service attack against the website of the Bulgarian Commission in an attempt to disrupt local and national elections.

- **Russia** – Kremlin[iii] - In September 2015, hackers launched a denial of service attack against the Kremlin's defense system and presidential website. This attack was in response to the process involved in the current elections in Russia

- **Ukraine** – Election Website[iv] - In October 2014, hackers launched a denial of service attack targeting the website of the Ukraine's election commission in an attempt to disrupt the current election

U.S. Presendential Candidate Hacks

- **Trump**[v] – Donald Trump has been a constant target of denial of service attacks and data dumps.
- **Clinton**[vi] – Hillary Clinton's private email server was hacked and indexed on WikiLeaks.
- **Sanders**[vii] – Bernie Sanders' staffers accessed Clinton's voter data after a vulnerability was discovered in the voter data software.

Primary Risks to Consider

The modern election is becoming increasingly connected. With new technology comes new risk. Currently, the biggest risk posed to the election process is the loss of connectivity, and therefore, visibility. Without both, the electoral system could be undermined and voters could lose trust in the process. This is why DDoS attacks during the election process are focused at commission, voting and statistical websites. When voters no longer trust the system, panic can take hold, often times to the satisfaction of the hackers.

Smart Venue Security Considerations

Smart and connected venues are becoming increasingly popular as organizations attempt to recapture today's digital voter. These locations are becoming increasingly sophisticated, offering a wide variety of digital amenities for attendees. These same amenities provide potential threats that can jeopardize the mobile devices of anyone connected to a WLAN network, resulting in stolen data, a mobile botnet, or worse (see Figures 1 & 2).

RNC – The Republican National Convention (RNC) will be held at the Quicken Loans Arena[viii] in Cleveland. This stadium features 461 antennas, 235 DAS and 230 Wi-Fi access points that provide access to those attending events inside the stadium. The DAS system is built by Verizon Wireless and provides 4G LTE speeds.

DNC – The Democratic National Convention (DNC) will be held at the Wells Fargo Center[ix] in Philadelphia. This stadium features 3501 Wi-Fi access point and 700 Bluetooth beacons. The system is powered by Cisco's latest generation, connected stadium solution that provides users with a 1Gbps connection.

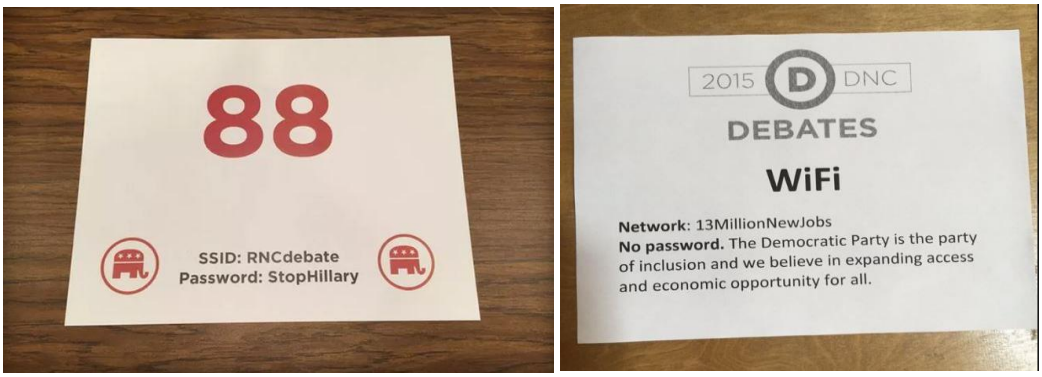

Figure 1 & 2: Password Politics, Nov 2015

What to Expect at the RNC/DNC

Could a hacker attack one of the conventions this year? Possibly, but it's more likely that they will directly target politicians or their websites. It is possible that Trump's and/or Clinton's websites could be attacked if they are announced as their party's nominee. If a hacker does target one of the conventions, it will likely be in the form of a SQL injection or a denial of service attack. The attackers would be aiming to disrupt the flow of real-time data or steal attendee and donor information.

How to Prepare

Technology can provide a more immersive and rewarding experience for voters, but also create security risks for those managing large scale, connected events. Here are suggestions for both attendees and stadium management/wireless network providers supporting political events.

Attendees/Users:

- Ensure your phone is updated with the latest operating system
- Disable Bluetooth when not in use
- Disable Wi-Fi when not in use
- Use the stadium's Wi-Fi when device is in use
- Use VPN
- Have RFID shields to protect RFID cards

- Exercise caution when presented with pop-ups while browsing

Stadium Operators:

- Ensure hardware is updated
- Regularly patch devices in the stadium
- Conduct audits of the network between games
- Access Control List (ACL) – Filtering network traffic
- Use load balancing for traffic distribution
- Have network and application protection to detect, mitigate and alert in real time.

Organizations Under Attack Should Consider

Protection against DDoS attacks:

- A hybrid solution combining on-premise detection and mitigation with cloud-based protection for volumetric attacks. It facilitates quick detection, immediate mitigation and internet pipe saturation.
- The solution must distinguish between legitimate and attack traffic, blocking it to protect SLAs.
- An integrated, synchronized solution that can protect from multi-vector attacks by combining DDoS with web-based exploits such as website scraping, Brute Force and HTTP floods.
- A cyber-security emergency response plan that includes a dedicated emergency team of experts.

Protection from data leakage and web application vulnerabilities:

- Shortest time from deployment to a full coverage of OWASP Top-10.
- Automatic and real time generation of policies to protect from zero-day, unknown attacks.
- IP-agnostic device fingerprinting: having the ability to detect attacks beyond source-IP using by developing a device fingerprint that enables precise activity tracking over time.

Radware's hybrid attack mitigation solution provides a set of patented and integrated technologies designed to detect, mitigate and report todays most advanced threats. Dedicated hardware and cloud solutions protect against attacks in real time and help ensure service availability.

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button".

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

---

[i] https://www.hackread.com/anonymous-philippines-hacks-leaks-voters-data/
[ii] http://www.novinite.com/articles/171533/Huge+Hack+Attack+on+Bulgaria+Election+Authorities+'Not+to+Affect+Vote+Count'
[iii] http://www.wnd.com/2015/09/russia-reports-very-powerful-hack-of-kremlin/
[iv] http://www.securityweek.com/hackers-target-ukraines-election-website
[v] https://security.radware.com/ddos-experts-insider/ddos-practices-guidelines/optrump2016/
[vi] https://wikileaks.org/clinton-emails/
[vii] http://www.nbcnews.com/politics/2016-election/bernie-sanders-campaign-penalized-dnc-after-improperly-accessing-clinton-voter-n482341?cid=sm_tw&hootPostID=8dd4d976784c2eaab53d61349039311e
[viii] http://www.nba.com/cavaliers/releases/q-wireless-130411
[ix] http://www.wellsfargocenterphilly.com/arena-info