What The Election Can Teach Us About Cybersecurity

Forbes Technology Council

Elite CIOs, CTOs & execs offer firsthand insights on tech & business.

Opinions expressed by Forbes Contributors are their own.

Post written by

Simon Crosby

Simon Crosby is Co–founder and CTO at Bromium.

It is rare for a U.S. president to face a major political stand-off before his own inauguration. But that was the history-making environment we saw playing out as president-elect Donald Trump, members of the U.S. intelligence community and Congress scuffled over the degree to which a Russian influence campaign, played out through cyber activity, shaped an election for the ages.

While U.S. political and diplomatic interests await reports and hearings, "election hacking" is already a global phenomenon, according to concerns out of Germany, Montenegro, France, the Netherlands and elsewhere. Despite alarming headlines, focused cyber operations against elections are in their relative infancy – meaning it's crucial for us in the security industry as well as those affected to define what's happened and marshal broad defenses.

Lowering The Bar For Information Warfare: Three Methods Of Interference

In the past, regimes wishing to upend elections had to do things like engineer strikes or military uprisings. Today the game has changed: Anyone can use the internet to destabilize elections in ways that are easily deniable -- and perhaps more effective.

Around the world, no two elections are conducted the same way. However, as more campaigns come under fire, we can now see common hallmarks of offensive interference.

Doxxing: *Gathering sensitive, confidential data and maliciously disclosing information in a calculated fashion to inflict setbacks in political momentum and unity.*

The best examples of this are the email leaks that plagued the offices of Hillary Clinton's presidential campaign and its allies in the Democratic National Committee (DNC) and Democratic Congressional Campaign Committee (DCCC) in 2016. The leaks arguably hobbled the campaign's response to news cycles and upended party unity when former DNC head, Debbie Wassermann Schultz was forced to step down in their wake.

Forget Watergate-style break-ins; today, doxxing is easy to accomplish with simple phishing e-mails introducing malicious software to email recipients. Many political organizations have relatively weak cybersecurity controls, despite relying on vast databases and email systems holding years' worth of confidential gossip and strategies. Expect many more cyber attackers to stage damaging data dumps around the globe, thanks to plentiful malware and public forums like WikiLeaks.

Digital Propaganda: *Inundating voters with misleading or inflammatory information masquerading as news and other trusted sources.*

Today it's easy to fabricate websites with seemingly innocuous domain names hosting digital propaganda and then use orchestrated, automated social bots and other methods to seed it across social media and other channels.

It's important to note that propaganda does not need to actually win over anyone to be effective in undercutting trust in informed, free and fair elections. A Pew Research Center study on this past election's fake news problem concluded "two-thirds believe the explosion of false information causes a 'great deal of confusion about the basic facts of current issues and events.'"

Hacking Election Machinery: *The most volatile attack scenario is compromising voting machines, agencies and other polling infrastructure.*

This is the hardest category to pull off, because remotely compromising a voting machine, for example, is more difficult than tricking election staffers into clicking on malicious email attachments (as stage one of a doxxing expedition). Yet, every newly-disclosed vulnerability rightfully worries election regulators. Even quick technical fixes applied after such disclosures may not reassure voters' perceptions.

Training their sights on election machinery is a high-stakes game for nation-state attackers, because a country could consider such intrusions attacks on their critical infrastructure systems, an act meeting the threshold for military retaliation and other dire responses in the physical world. The risk and sheer complexity of these attacks is likely why productivity-minded election adversaries spend most of their time on propaganda and email hacking.