Mandiant

EBOOK

Cyber Threat Activity Targeting Elections

Introduction

Cyber threats to democracy are a growing global challenge for government agencies, elected officials and election campaigns. The election process involves the protection of many attacker-targeted technologies. The need for protection of election campaigns, election administration and election systems must include third-party and supply chain compromise assessment and mitigation strategies to adequately defend democracies and elections from influence, disruption and compromise.

Mandiant gathers and analyzes considerable amounts of proprietary data from victim, adversary and machine intelligence worldwide, as well as managed detection and response, incident response and other consulting engagements.

Highlights of Analyses

Mandiant Threat Intelligence continues to observe the state-sponsored and other threat actors routinely seek to target national elections for the purposes of collecting intelligence and influencing, delegitimizing or causing disruption to the electoral process, and we assess with high confidence that actors will continue to target entities associated with elections.

Based on Mandiant data observed to date, threat actors have focused on carrying out intrusions that target election administrators, political parties and other organizations with comparatively larger attack surfaces than core election systems.

Mandiant Threat Intelligence has not observed compromises of core election systems leading to the alteration or manipulation of votes, although this part of the ecosystem remains the most opaque.

Mandiant Threat Intelligence anticipates future threat scenarios could include disruptive threats such as ransomware attacks that impact electoral processes and related organizations.

Threats of Threat Activity

We assess with high confidence that cyber threat actors with various motivations and state sponsorship will continue to target entities associated with elections and referendums worldwide for the foreseeable future. Historically, that activity has been directed against three categories of targets: core election systems, election administrators and entities associated with election campaigns. Much of the threat activity Mandiant has observed around elections has impacted election administrators or election campaigns because they have comparatively larger attack surfaces.

Election Campaigns

News Organizations

PACs & Donor Groups

Political Parties & Campagins

Social Media Platforms

Observed activity

- Compromises of political parties and campaigns
- Propaganda distribution through social media platforms

Election Administrators

Election Commissions

Electoral Registers

State & Local Officials

Observed activity

- Targeting election commission websites
- Theft of data from electronic voter databases and pollbooks

Election Systems

Voting Machines

Software & Hardware Manufacturers

Election Managment Systems

Observed activity

- No observed successful compromises of voting machines
- Limited indications of targeting of election systems manufacturers

Types of Threats

With respect to election security, Mandiant has observed threat activity that include:

Spreading of disinformation on social media platforms and messaging services

Cyber espionage, spearphishing and social engineering of political campaigns, election administrators and other influencers

Disinformation campaigns using stolen data, fabricated content, or compromised access

Attacks on critical election infrastructure to tamper with or alter votes

Mandiant anticipates that future threat scenarios will focus on attacking voter confidence in the system itself and destructive attacks masquerading as ransomware.

To attack voter confidence, threat actors will attempt to exploit verified platforms such as government websites or social media sites to create voter confusion and distrust in the system. This tactic has been successful in the past; it is difficult for a government or agency to counter statements on these platforms.

We expect attacks will continue to align with global conflicts, such as activities observed surrounding Russia's invasion of Ukraine that attempt to influence the shifting geopolitical landscape. While these operations have presented an outsized threat to Ukraine, they have also threatened the U.S. and other Western countries.

As a result, we anticipate that such operations, including those involving cyber threat activity and potentially other disruptive and destructive attacks, will continue as the conflict progresses.

Examples of Election-Related Threat Activity

2016 March	Philippines	Anonymous Philippines defaces the Philippines Commission on Elections (COMELEC) website and leaks 340 GB of genuine data.
2016 June	United States	Russia-affiliated actors APT28 and APT29 compromise a Democratic National Committee (DNC) server in mid- 2015 and maintain that access until at least June 2016. Russian threat actor Sandworm Team is suspected of having targeted several states' election infrastructure. Separately, we observed a broad network of social media accounts use material from the DNC leaks as springboards to promote a variety of false or misleading narratives. These activities are consistent with known tactics, techniques, and procedures (TTPs) associated with the Russian Internet Research Agency (IRA).
2017 May	France	Suspected Sandworm Team activity targets the French political party, "En-Marche!".
2017 August	Kenya	Discovery of several news websites created to mimic legitimate Kenyan and international news websites--a subset of which appear to have been created in coordination with each other to damage the reputation of an opposition party candidate.
2017 November	Russia	Observations of numerous concerted anti-opposition messages in various IRA-linked YouTube videos, the Russian social media platform VK, and on Russian blogs.
2017 December	Catalonia	As part of the #OpCatalunya campaign, a Spanish hacktivist group publishes a blog post claiming to have gained unauthorized access to "iPARTICIPA," a cloud-hosted system belonging to the administrator of the electronic voting system used in the Catalonian elections.
2018 January	Honduras	Anonymous-affiliated hacktivists launch the #OpHonduras campaign in protest of the recent inauguration of Honduran President Juan Orlando Hernández.
2018 June	Cambodia	APT40 compromises the website of Cambodia's National Election Commission using AIRBREAK malware.
2018 March	Malaysia	Suspected Chinese threat actors leverage a series of lure documents related to the Malaysian election against multiple government agencies.

Examples of Election-Related Threat Activity (continued)

2018 July	Mexico	Multiple websites and Facebook groups observed disseminating fabricated content in support of and against presidential candidates.
2018 October	Hong Kong	Chinese cyber espionage actors leverage EVILNEST malware in a campaign targeting Hong Kong entities in October 2018.
2018 November	Taiwan	Suspected Chinese threat actors target Taiwanese government entities with election-themed lures, utilizing TAIDOOR malware.
2018 November	United States	Discovery of multiple Twitter accounts appearing to impersonate U.S. Republican congressional candidates as part a network of English-language social media accounts that appeared to be tied to actors supporting Iranian interests.
2019	Unnamed European Country	Spearphishing of an election administrator and a media organization by unknown threat actors.
2020	United States	Iranian information operations campaign impersonating the 'Proud Boys' organization conducts mass email campaign threatening U.S. voters

With the combination of Mandiant services, expertise and Mandiant Advantage SaaS solutions, we can empower organizations to continually evolve as elections threats continually change. Mandiant has helped many organizations to be better informed, protected and responsive to the latest election cyber threats with ongoing and holistic election security program.