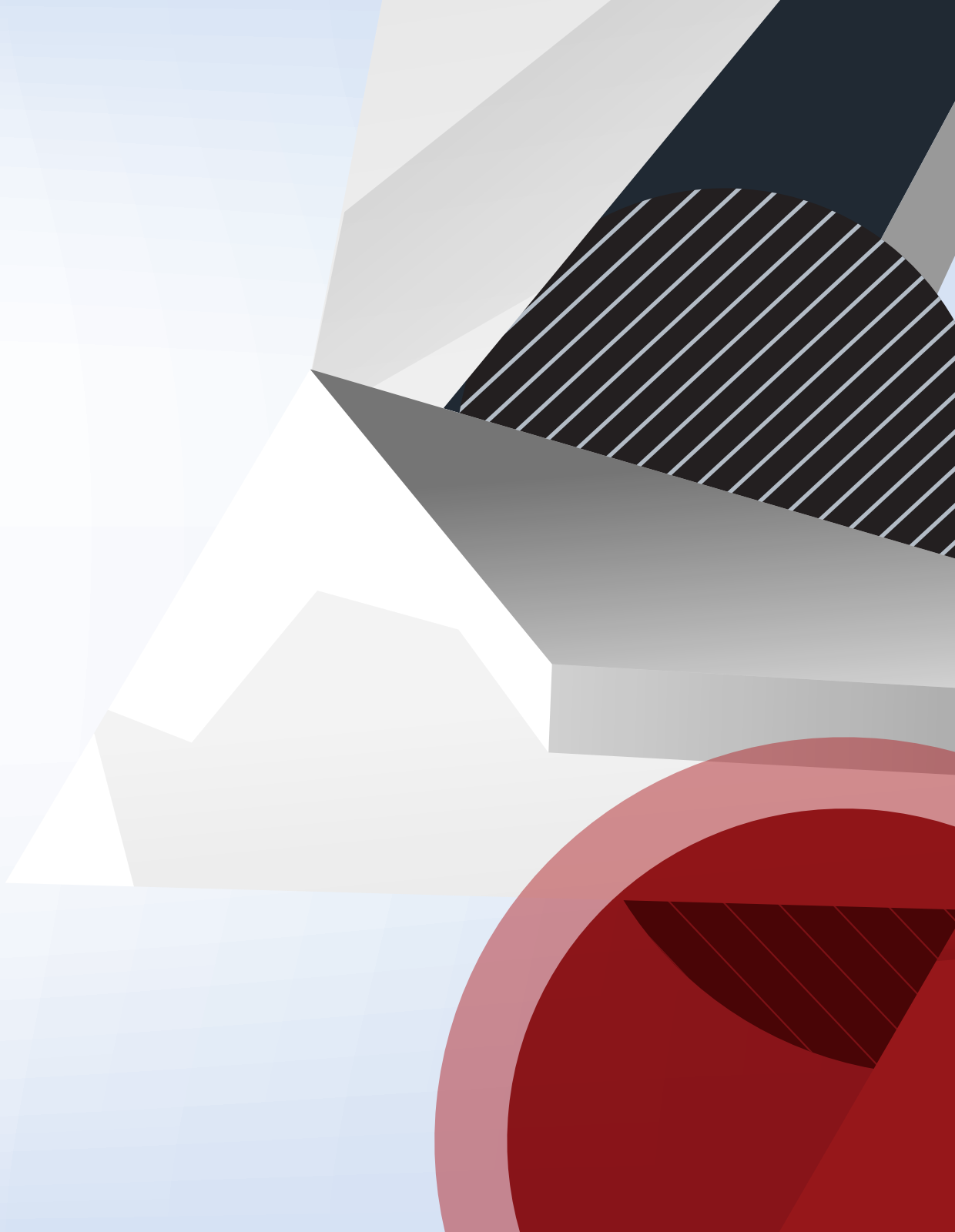
FIREEYE™

CYBER THREAT ACTIVITY TARGETING ELECTIONS



Introduction

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

Based on this data, FireEye experts have noted several items of interest.

Highlights of Analyses

FireEye Threat Intelligence continues to observe that 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 FireEye data observed to date, threat actors have focused on carrying out intrusions that target election administrators, political parties and other organizations and assets with comparatively larger attack surfaces than core election systems.

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

FireEye Threat Intelligence anticipates future threat scenarios could include disruptive threats such as ransomware attacks, impacting electoral processes and related organizations.

Targets of Threat Activity

We assess with high confidence that cyber threat actors with various motivations and 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. With comparatively larger attack surfaces than the core election systems, much of the threat activity FireEye has observed around elections has impacted the latter two categories.

ELECTION SYSTEMS

Observed Activity:

No observed successful compromises of voting machines; limited indications of targeting of election systems manufacturers

VOTING MACHINES

SOFTWARE & HARDWARE MANUFACTURERS

ELECTION MANAGEMENT SYSTEMS

ELECTION ADMINISTRATORS

Observed Activity:

Targeting of election commission websites

Theft of data from electronic voter databases and pollbooks

ELECTION COMMISSIONS

ELECTORAL REGISTERS

STATE & LOCAL OFFICIALS

ELECTION CAMPAIGNS

Observed Activity:

Compromises of political parties and campaigns

Propaganda distribution through social media platforms

NEWS ORGANIZATIONS

POLITICAL PARTIES & CAMPAIGNS

SOCIAL MEDIA PLATFORMS

PACS & DONOR GROUPS

Types of Threats

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

SPREADING OF DISINFORMATION ON SOCIAL MEDIA PLATFORMS AND MESSAGING SERVICES

DISINFORMATION CAMPAIGNS USING STOLEN DATA, FABRICATED CONTENT, OR COMPROMISED ACCESS

CYBER ESPIONAGE, SPEARPHISHING AND SOCIAL ENGINEERING OF POLITICAL CAMPAIGNS, ELECTION ADMINISTRATORS AND OTHERS INFLUENCERS

ATTACKS ON CRITICAL ELECTION INFRASTRUCTURE TO TAMPER WITH OR ALTER VOTES

Future threat scenarios could predominantly include disruptive attacks that use ransomware to target election administrators. Such attacks could provide threat actors a deniable means to affect public perception around the security of these election administrators—without having to impact core electoral systems.

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.

Examples of Election-Related Threat Activity (continued)

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.
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.

For more information, visit **www.fireeye.com/elections** or contact **elections@fireeye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.