CASE STUDY

# Strategic Election Security Solutions in Action

## Government preparations for critical election protection

### GLOBAL GOVERNMENT SOLUTIONS

FireEye partners with international, federal, state, and local governments to deliver holistic cyber security capabilities through a partnership model in five areas:

- Single point of customer success and accountability
- Cyber security thought leadership and trusted advisor
- Operational program transformation
- Custom end-to-end solutions and mission support
- Simplified capacity building on a global scale

**The Challenge**

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, including voting machines, electronic poll books, voter registration systems, and campaign databases. Protection of election campaigns, election administration and election systems must also include third-party and supply chain compromise assessment and mitigation strategies to adequately defend democracies and elections from influence, disruption and compromise.

Political parties and their respective campaigns have recently been targeted by hacktivists and advanced persistent threat (APT) groups aiming to influence, propagate disinformation or obtain intelligence. A more strategic approach is needed to protect democracy from cyber threats.

**When Risks Outmatch Capabilities**

The Chief Information Security Officer (CISO) of a large North American city called on FireEye Mandiant during the 2016 presidential election. The city deemed itself a high-risk target and had deep concerns around election security based on the increasing threats and risks to election devices, election databases and advanced threat actor efforts to influence election outcomes. With support from the city's mayor, the CISO worked closely with Mandiant consultants to safeguard the upcoming presidential elections and improve overall election security.

Together, they quickly determined the election platform needed increased critical controls, threat visibility, and security expertise to combat advanced election attack threats. A comprehensive plan was developed to assess the agency's election risk posture, address critical gaps and prepare for future cyber security events.

**Root Cause Identification**
Over the course of a four-week integrated process engagement, FireEye Mandiant consultants conducted a **Compromise Assessment** to search for the presence of past and ongoing attacker activity. The assessment uncovered evidence of a China-based cyber espionage attack group that had achieved a foothold in the their environment via an email phishing attack. During the Compromise Assessment, experts also deployed FireEye **Digital Threat Monitoring** service which discovered active domain administrative credentials in use on the dark web. The Mandiant team helped quickly eradicate all system compromises from the environment and institute additional network security policies to prevent and mitigate similar future risks.

Next, due to the heightened risk associated with APT28, a Russian threat group known for targeting elections, Mandiant consultants performed a **Response Readiness Assessment** to baseline their posture and capabilities to protect, monitor and respond to cyber incidents. This engagement also included a crisis management **Tabletop Exercise** in collaboration with the city's cyber security leadership team. The workshop tested the team's incident response plan through roundtable scenario gameplay, which included challenges commonly seen by Mandiant experts in real-world election attacks. Mandiant consultants identified areas for increased response efficiencies and incident response experts created best practice domain playbooks to address denial of service, system compromise, social media poisoning, and insider threats for the city's security team to proactively implement moving forward.

The city saw immediate value from engaging a FireEye senior advisor to support cyber security capability and thought leadership. On election days and days leading up to them, Mandiant experts organized operational support for the city's leadership and staff, using a team of onsite trusted advisors and incident responders to secure the city's election process across vital stakeholders and facets of the security apparatus.

**Long-Term Improvements**
To improve and augment long-term detection, assessment, and response capabilities, Mandiant helped establish FireEye **Managed Defense** as the managed detection and response service for the city's digital environment. This provided the city with the capabilities of a 24x7x365 security operations center (SOC) for attacker monitoring and threat hunting at the highest capability of cyber defense.

Managed Defense relies on the FireEye technology stack, which includes **Network Security and Forensics, Email Security—Cloud Edition, Endpoint Security, and the FireEye Helix** solutions to continuously and effectively detect, investigate, and respond to cyber security events.

Within 30 days, Managed Defense blocked a new ransomware variant with FireEye Email Security after the ransomware bypassed the city's existing email security tool engineered by another vendor. Even today, the city continues to use FireEye Managed Defense as its primary service for continuous cyber defense coverage.

The city used **FireEye Threat Intelligence** to inform present and future security business decisions. FireEye Threat Intelligence provided frontline threat context that helped the city develop a strategic understanding of its threat landscape, gain specific insights into their organization's risks and align network defenses to thwart attackers.

**Continuous Digital Threat Monitoring** provided proactive defense services against risks to the city's brand, infrastructure, and valued partners. This service helps identify and anticipate threats that live outside the city perimeter and in the dark web so the city can take proactive steps to mitigate impending attacks.

Globally, FireEye observed cyber threat activity around elections in Europe, Ukraine, Asia, Africa, South America and the United States. FireEye published intelligence reports regarding Russian advanced persistent threats such as APT28 and the Sandworm Team, which have been tracked to intelligence operation activity and are suspected to be tied to the Internet Research Agency (IRA). FireEye also published reports on how China APT40 (Periscope) targeted the 2018 Cambodian elections as well as multiple election related entities in a spear-phishing campaign.

**Conclusion**

The goal of cyber threat actors against democracy is simple: collect intelligence, influence outcomes, and foster mistrust. To defend against these cyber threats, we must consider attacker motivation and understand how separate attack vectors are connected. To be effective, security teams need to be informed, ready, and able to defend against any type of attack.

FireEye recognizes the need for holistic strategic cyber security approaches to election protection. Our services and solutions secure government agencies that rely on multiple technologies and operations. Attempting to sync these technologies and operations on their own, or with multiple vendors might ultimately create greater security risks on a larger scale.

Our full suite of solutions, including FireEye Mandiant frontline incident response and expertise, Managed Defense, Threat Intelligence and additional FireEye technologies, offer the most comprehensive approach to cyber security in the industry.

The fastest and most effective defense against targeted attacks is to employ a single integrated team of industry recognized experts to protect an organization's critical assets and program processes. At FireEye, the global government solutions team offers program management of all FireEye services and technologies and acts as a single point of customer success and accountability. This is how FireEye strives to ensure free and fair elections across the globe.

To learn more about FireEye, visit: **www.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.

FIREEYE™