CROWDSTRIKE CASE STUDY

International Republican Institute

WANTED: INFORMATION ON U.S. FOREIGN POLICY

When most people think of organizations at risk from major cyber security attacks they usually cite events affecting retailers, banks and financial institutions, and a handful of other industries. But cyber threats facing the commercial sector are equally risky to international nonprofit organizations. In fact, while these organizations don't always contain petabytes of personally identifiable information, or potential access to billions of dollars of revenue from stolen credit card data, they are frequently targeted by global adversaries looking for specific information, such as intelligence about U.S. foreign policy, through secondary channels.

This is the situation that the International Republican Institute (IRI) is faced with as it promotes and sustains democracy around the world. Not only does the organization confront cyber attacks from politically motivated adversaries looking to disrupt its field operations, but its headquarters in Washington, D.C. are considered high-value targets by adversaries looking to gain insight into U.S. foreign policy strategy and other valuable national intelligence from data housed within the IRI's system.

Concerned with intensified threats against their operations both at home and in the field, IRI understood that they needed an industry-leading partner with a comprehensive understanding of advanced global adversary groups to best defend their systems and data against cyber attack.

THE FUTILITY OF WHITE LISTING

IRI is a mid-size organization whose primary security challenge is not so much its size, or the number of endpoints to be monitored, but the distribution of field offices around the world in remote locales, operating on local time. With its security team located centrally at the Washington, D.C. headquarters, the challenge was to find a comprehensive endpoint solution that was able to effectively support a globally distributed organization.

Quick Facts:

INTERNATIONAL REPUBLICAN INSTITUTE

BUSINESS OVERVIEW

Established in April 1983, International Republican Institute (IRI) is a nonprofit, nonpartisan organization committed to advancing freedom and democracy worldwide by helping political parties become more issue-based and responsive, assisting citizens to participate in government planning, and working to increase the role of marginalized groups in the political process – including women and youth. The IRI is headquartered in Washington, D.C. with field operations in Asia, Africa, Europe, Latin America, and the Middle East.

MISSION, VISION AND CORE VALUES:

The organization is tasked with encouraging democracy in places where it is absent, to help democracy become more effective where it is in danger, and share best practices where democracy is flourishing.

Website: www.iri.org

The Story:

CHALLENGE

International organizations such as IRI need to protect a complex array of endpoints and assets -- not just at headquarters, but around the world and often in inhospitable locations. Because they are repositories for governmental intelligence, classified information and other valuable data, such organizations need a high level of comprehensive cyber security protection.

Geoff Merck, Director of IT and Telecom at IRI, understood that with the organization's unique challenges, it would take an equally unique vendor to meet their needs. "When the time came to think about how to evolve our network defenses, we knew that we needed to move away from traditional cyber security postures and product vendors," Merck said. "We were finding ourselves in a situation where we had multiple vendors in place and were looking to add more vendor solutions on top of that. While it's a good strategy to have more than one vendor to provide a check-and-balance for monitoring and reporting, when your vendors become your primary focus and not what's happening on your network, it's time to re-evaluate."

As part of their evaluation process, Merck brought in the CrowdStrike team. Shortly after the deployment of the Falcon platform, a persistent attack on the IRI network was uncovered by CrowdStrike when an existing vendor's firewall failed and allowed traffic that had previously been blocked to communicate outside the network. The attack also was able to bypass the whitelisting-based solution IRI had in place. In fact, without CrowdStrike Falcon deployed in his environment, Merck and his team would have been unaware that anything was amiss.

"Whitelisting, while good in theory, is unable to provide any kind of reliable security for us in today's adversary-based environment," Merck said. "It's billed as a panacea, that once I have lists in place my organization will never get hit again. But with the way in which attacks are evolving, that's simply not true."

As a result of CrowdStrike Falcon's real-time endpoint visibility, and aided by guidance provided by the CrowdStrike Security Operations Center (CSOC), Merck terminated the adversary's access and communications, preventing the attempted exploitation of IRI's network to gain intelligence about their field office operations.

Merck also described another attack that happened shortly after the first detection. Falcon detected adversary activity from an intruder attempting to take control of IRI systems using a malware-free attack via webshell. Although the attackers had the password wrong, it was clear that they were intending to gain control of an IRI server. Thanks to CrowdStrike Falcon and the 24/7 CSOC resources, IRI was able to respond rapidly by taking the server offline before the attackers could succeed, Merck said

"From the moment the CrowdStrike solution was in place, I felt like I had a team experts working on my behalf," Merck continued. "I can't express how much I appreciate the CrowdStrike team. It didn't matter what time of day, or day of the week, if my team needed help or needed to know about something on our network, the CrowdStrike team was always there and always well prepared."

NEXT-GENERATION ENDPOINT PROTECTION

Taking the Relationship to the Cloud

Based on CrowdStrike Falcon's ability to detect both known and unknown attacks, the exceptional endpoint visibility that the platform provides, and timely support and advice from the CSOC team, the relationship between CrowdStrike and IRI is developing into a long-term partnership. Merck is currently in the process of

TASK:

IRI was at a critical juncture in developing its cyber security defenses. Recognizing the impact an attack could have on operations at headquarters and in the field, IRI needed a partner that not only provided visibility across all endpoints and next-generation protection against adversaries, but also a provider they could rely on for 24/7/365 monitoring and support — something IRI knew they themselves were unable to provide.

WHY IRI CHOSE CROWDSTRIKE

With CrowdStrike's Falcon providing comprehensive Cloud-based protection across all of IRI's endpoint systems, the IRI team can focus on their core jobs, knowing that attacks will be prevented and that they will be immediately alerted to trouble on their network — at headquarters or in a field office. CrowdStrike's next-generation endpoint protection, coupled with actionable threat intelligence, stops adversaries in their tracks and provides detail on the threat actor behind an attack.

Leveraging the power of the CrowdStrike Platform, the 24/7/365 CSOC team serves as an extension of IRI's own team, providing continuous coverage and alerts and allowing IRI to react to threats within minutes. IRI has been able to proactively react to multiple incidents since partnering with CrowdStrike.

incorporating IRI's field offices and endpoints into the Falcon platform, and he foresees a time when CrowdStrike will be the primary security vendor for the IRI. While it's essential to maintain some level of diversity in products and services to effectively quash adversaries, Merck said, "I'm looking forward to moving CrowdStrike front-and-center in our organization's cyber defenses. They can do so much more than other vendors and have made my team far more efficient and effective, allowing us to do our real jobs, rather than worrying about trying to anticipate the next attack."

Merck is particularly interested in the evolution of Cloud-based security solutions such as Falcon. "The power of the Cloud is more than hype, it's a huge benefit to an organization like mine, where our field offices have to act like they're stand-alone units rather than as part of the ecosystem of our headquarters. Security in the Cloud enables us to be more efficient in how we track and safeguard assets and endpoints and, in the end, partnering with CrowdStrike takes a whole lot of worry off my shoulders. When something happens — no matter where it happens — CrowdStrike has my back."

In addition, IRI has benefited from the cost savings inherent in CrowdStrike Falcon's Cloud-based architecture, which requires no hardware, and so eliminates the need for patching, updating and other maintenance requirements typical of traditional on-premise security solutions. "CrowdStrike, has made us far more cost-efficient, which always pleases management," Merck said.

CROWDSTRIKE HELPS ORGANIZATIONS PROTECT THEIR TEAMS AT HQ AND IN THE FIELD

In order for international organizations to carry out their missions in the areas where assistance is most needed, they need to have "boots on the ground," which in this day and age, includes the ability to operate a sophisticated and secure network that enables team members to communicate from remote and volatile regions back to headquarters. With many cyber attacks emanating from these regions to begin with, these networks are particularly vulnerable. This, combined with the sensitive nature of information that's being communicated — including policy goals, information from and in support of dissident groups, and names of local activists — heightens the value to politically motivated adversaries.

The needs of international not-for-profit organizations often are overlooked by cyber security companies that are built around the protection of commercial infrastructure and information. The adversary attribution capabilities of CrowdStrike's solutions, and the Cloud-based evolution of endpoint protection combined with exemplary service delivery, made Falcon the only choice for Merck. "International organizations need to realize that they are just as vulnerable and their data just as valuable to cyber attackers as healthcare records and credit card information. The work we do directly confronts these cyber attackers in their own back yards, and for that reason our presence, our networks, and our contacts are always vulnerable to attack," Merck said. "CrowdStrike has enabled my team to focus on our core jobs, which is to support our people as they promote democracy and democratic values around the world. Now that I know I'm going to be alerted to trouble on the network – at headquarters or in a field office – immediately, with recommendations that will stop an attack in its tracks and actionable intelligence on the adversary we're facing, my team is a lot more effective."

About CrowdStrike

CrowdStrike provides next-generation endpoint protection, threat intelligence, 24-hour monitoring and incident response services to many of the world's largest and most advanced companies and government agencies.

The 100% SaaS-based CrowdStrike Falcon Platform offers the most comprehensive endpoint protection technology available, enabling customers to detect, prevent, record and search in real time to stop targeted attacks before they can cause damage.

CrowdStrike's dedicated 24X7 Security operations Center, Threat Intelligence and Incident Response services use the Falcon platform to immediately detect — and often prevent — advanced malware and adversary activity on your endpoints while attacks are still in-progress, minimizing business impact and significantly speeding up incident response and recovery times.

To learn more about how CrowdStrike can help protect your organization, contact us today at sales@crowdstrike.com or visit www.crowdstrike.com/seedemo to request a demo.

CROWDSTRIKE

sales@crowdstrike.com | (888) 512-8906

www.crowdstrike.com