CASE STUDY | **PUBLIC AFFAIRS CONSULTANCY**

CRYPTONITE NXT

Sophisticated threat actors continue to actively infiltrate, monitor, and compromise key corporate data and financial assets.

The Challenge

No industry is immune to the continued barrage of cyberattacks. Even one of the largest cybersecurity consultancies in the world, despite their considerable capability, fell prey to an advanced and targeted attack in late 2017, which breached both customer data and intellectual property. Sophisticated threat actors continue to actively infiltrate, monitor, and compromise key corporate data and financial assets.

Public affairs consultancies are also at substantial risk. These businesses deal with highly sensitive and confidential information. Their goal is to use this information to optimize and deliver impactful communications to targeted organizations and groups, including broad segments of the population, as in political campaigns and issue advocacy, as well as corporate, trade, and international partnerships. Specialized internal groups such as opposition research provide consulting services which center around the collecting information on political opponents and business adversaries. This information is often used for strategy and planning and, in some cases, can be used to directly discredit the opposition.

The information gathered for opposition research can include financial, educational, legal, criminal, social media, and biographical information and can come from open sources, special inquiry (freedom of information act), or specific human intelligence gather activity from a broad variety of disparate sources. Significant computing resources are used for data mining and analysis, and new content from social media has added considerably to the data stores and analysis required to support these activities.

Our Case Study

Our case study focuses on the selection and installation of CryptoniteNXT Moving Target Cyber Defense (MTD) and network segmentation by one of the leading public affairs and opposition research consultancies in the United States. This contractor

provides essential consulting and support services to associations, trade groups, politically aligned groups and parties, and global business enterprises.

The security of their networks and information technology resources is of paramount concern. Given the current environment, they regularly review cybersecurity with both clients and prospective customers.

While headquartered in the United States, our client must support a distributed and global organization. They have a centralized team managing their physical security and their security operations center to protect their information technology resources with active on-site surveillance and management. Their facility is physically secured using state-of-the-art protection and requires multi-factor based authentication for access.

In some cases, their employees and contractors travel to security-challenged environments, such as mainland China. During these trips, they remain concerned about targeted attacks which could compromise their information resources and client data. Upon return, all laptops and mobile devices are scanned for possible intrusions, memory dumps are analyzed for hidden threats, and in some cases all of the software is completely removed and reloaded.

Their Chief Operating Officer had considerable interest in segmentation strategies based upon guidance from NIST and recommendations from ex-government consultants with deep experience protecting classified intelligence assets and resources. They also reviewed, in detail, the red team analysis data provided by Rapid7 (Metasploit) during and after penetration testing against a network protected by CryptoniteNXT. They evaluated alternate approaches and ultimately selected CryptoniteNXT due to the advantages of combining moving target cyber defense (MTD) with the proven capabilities of micro-segmentation, recommended by NIST.

Their team ran the CryptoniteNXT platform through a comprehensive evaluation of functionality, and documented, in detail, that the proposed capabilities functioned as expected. They found high value in the integration of authenticated mobile users with micro-segmentation protected domains and believed this would contain any attacks to perhaps just the endpoint impacted. The appliance was integrated quickly into their network environment and continues to operate without failure or degradation.

"Moving Target Cyber Defense (MTD) enables us to deploy a Zero Trust network. Zero Trust mitigates the weaknesses in our network without changing how authorized users interact with resources and applications. In the event of any intrusion past our perimeter, the CryptoniteNXT micro-segmentation limits lateral movement to the minimum possible, and the moving target defense completely stops all reconnaissance. If cyberattackers cannot see our information resources, and cannot find them, then they cannot attack them. Most important, the CryptoniteNXT system provides a rapid, highly automated and active response to the threat"

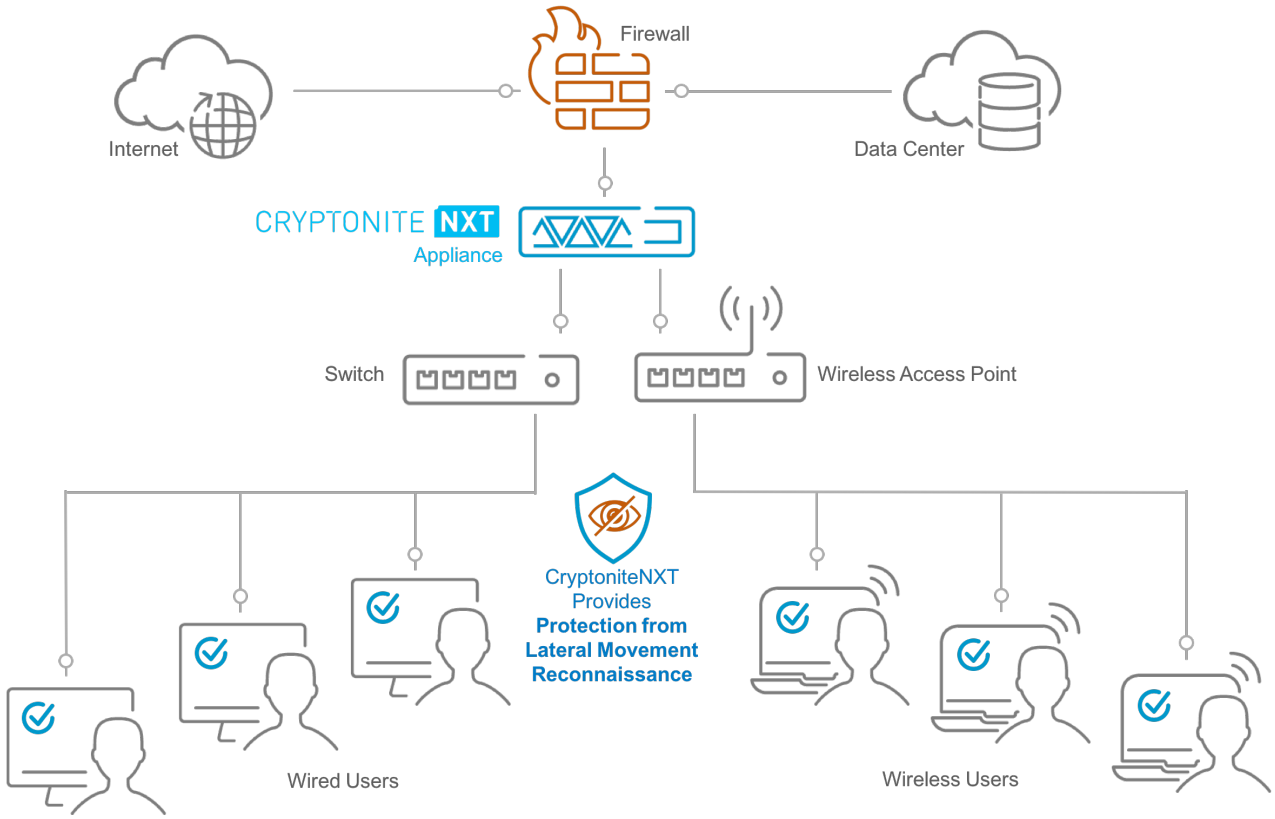
— Chief Operating Officer

The Results

The CryptoniteNXT appliance was selected to protect the top opposition research team members globally. It has become an essential part of their defensive techniques, tactics, and procedures to secure their data and intellectual property assets against any form of cyberattack.

Attackers that seek to compromise the network are identified and immediately shut down and stopped. Attacker or insider threat lateral movement out of policy is logged and generates an alert and, at the same time, it is restricted and shut down by CryptoniteNXT automation. This fast response automation benefits the security operations team and shortens both the time to detection and the time to remediation.

The CryptoniteNXT platform was then selected for permanent internal use. The production use of MTD technology has gone well, and a company-wide deployment of CryptoniteNXT was completed in the fourth quarter of 2017.



CryptoniteNXT Architecture

About Cryptonite, LLC

Cryptonite is a leader in moving target cyber defense. CryptoniteNXT enables any network to actively shield itself from cyberattacks by preventing all attacker reconnaissance and lateral movement. Patent pending moving target cyber defense and micro-segmentation technologies protect enterprise networks from an advanced cyberattacker, insider threats, and ransomware. The Cryptonite customer base includes leading commercial and government customers around the world. Learn more at **www.cryptonitenxt.com.**