

Regional Utility Company turns to FireEye to protect against advanced malware and targeted attacks to ensure flawless delivery of power to millions of subscribers

Summary

Company	Regional Utility Company
Industry	Energy and Utilities
Description	Among the nation's largest regional utility companies, the organization provides energy services to millions of electric and natural gas customers throughout its multi-thousand square-mile territory.
Challenge	Identify easy to deploy solution to combat the next generation of threats, including zero-day and targeted APT attacks, to supplement legacy security defenses across corporate infrastructure. Need to optimize efficiency of information security team and maximize accuracy of detection and blocking.
Solution	Implementation of FireEye Web Malware Protection System 7000 Series appliance, FireEye Central Management System and FireEye Malware Protection Cloud.
Benefits	Rapid deployment capabilities, centralized management and industry-leading levels of threat monitoring safeguard the integrity of the organization's extensive network and IT infrastructure. Exemplary false positive performance and highly detailed alert reporting enable the company's information security team to focus on remediating advanced malware.

Among the nation's largest publicly-owned utilities, providing energy to millions of electric and natural gas customers, the company understands the huge responsibility it has towards its own subscribers to ensure that its services are provided in a safe, reliable and responsible manner. To deliver on this commitment, there is a corporate-wide focus to lead the way to a secure energy future.

"One of the big attractions of the FireEye solution is that analysis is performed in a virtual execution engine to determine if a flagged piece of code actually is a threat. The detailed information that is generated allows us to pinpoint the optimal option for resolving an issue. It puts us in the position of knowing exactly how to react."

– Information Security Supervisor, Regional Utility Company

Reputation for Facilitating Remediation

In its quest to continually thwart the escalating plague of cyber-based attacks, the company explored the capabilities of the FireEye portfolio of malware protection appliances. The Utility's information security supervisor commented, "We were sufficiently impressed with the results of our research to implement a proof of concept using a FireEye Web Malware Protection System 7000 Series appliance."

The FireEye Web Malware Protection System (MPS) appliances can be deployed out-of-band or inline to monitor threats that legacy gateways allow to pass unimpeded. When used inline, unfamiliar code and suspicious web pages are stress tested using tightly controlled detonations to block polymorphic and zero-day malware and targeted APT attacks. The Utility's security team also evaluated the FireEye Central Management System (CMS) that functions as a security event repository and facilitates the centralized management and operational control of distributed FireEye appliances.

First Impressions are Lasting Ones

The information security supervisor stated, "The 7000 Series was exceptionally easy to install and we found the FireEye CMS interface to be very intuitive. The appliance immediately affirmed the bulk of our infrastructure was clean but did detect the presence of a certain malware in our network and allowed us

to zero in on a specific workstation for remediation. We ran the proof of concept for a few weeks and then purchased everything we were evaluating: It was an easy decision."

He added, "Since the very first day of deployment we have only ever seen one false positive! This has given us the confidence to aggressively pursue every threat alert in the knowledge that actual malicious potential has been detected."

The FireEye CMS and initial FireEye Web MPS 7000 Series were complemented by the purchase of additional 7000 Series appliances to provide comprehensive protection for the full network and infrastructure. To further enhance the effectiveness of the implementation, the team participates in the FireEye Malware Protection Cloud that connects FireEye appliances and FireEye research feeds into a real-time global exchange of data on confirmed, emerging threats.

The information security supervisor concluded, "Because of the business we're in, we have to be equipped to handle threats from anywhere across the globe. FireEye gives us visibility beyond that provided by other technologies."

Key Component

FireEye Web Malware Protection System 7000 Series appliance
FireEye Central Management System
FireEye Malware Protection Cloud

FireEye is the world leader in combating advanced malware, zero-day and targeted APT attacks that bypass traditional defenses, such as Firewalls, IPS, AV, and Web gateways!

© 2011 FireEye, Inc. All rights reserved. FireEye, Inc. and all FireEye, Inc. products are either trademarks or registered trademarks of FireEye, Inc. Other product and company names mentioned herein may be the trademarks of their respective owners. -- CS.WMPS052011