CASE STUDY

HIGHLIGHTS

Company: Orange Communications

Industry: Telecommunications

Location: Israel

About the Customer

Orange, the brand name for Partner Communications Company Ltd., is a leading Israeli communications operator, providing communications services, including mobile telephony, fixed telephony, international telephony, Internet services, transmission, data and Primary Rate Interface (PRI). The company has two primary security imperatives. First, the company wants to protect customer and business data and uphold privacy. Second, the company needs ensure the quality and uptime of its operations so that its customers will remain loyal. Preventing a data breach resulting in theft or damage contributes towards those goals.

The Need

Like most enterprises, Orange was concerned about the escalating volume and magnitude of targeted data breaches, and was looking for a solution to detect active breaches on their network. To protect against a data breach, they had previously relied heavily upon an Intrusion Detection System (IDS) and a Security Information and Event Management (SIEM) system, combined with a well-trained security operations team.

Arieh Shalem, Chief Information Security Officer, recognized that the IDS provided preventative measures against intrusion attempts, but could not reliably or efficiently detect an active intruder at work inside the network. At the same time, the IDS was producing some 800 alerts per day, a staggering number for the team of six security operators. These alerts were largely false-positives that required a large amount of triage and investigation before ascertaining whether or not remediation or response was needed. The SIEM was generally not used for any breach detection but primarily used as a centralized management tool and for reporting and analysis of all security incidents after the fact.

Shalem understood that they needed to add resources to address a potential breach, supposing that some attacker might get beyond the company's overall perimeter security and circumvent its preventative measures.

> **"The visibility was so good that we immediately completed our evaluation and dropped the other POCs that were in process."**
>
> - Arieh Shalem, CISO, Orange

Why LightCyber Magna

In 2014, the Orange security team wanted to have capabilities directly focused on finding an active data breach efficiently and accurately. At the time there were very few mature solutions available on the market, so they considered a variety of Advanced Persistent Threat (APT) solutions but realized that APT protection is just another form of malware detection – not a breach detection system. While Orange continued to look for an APT solution, it wanted something that would look for the behaviors an intruder would have to use inside an unfamiliar network if and when they were able to successfully penetrate their network.

LIGHTCYBER

CLOSING THE BREACH DETECTION GAP

Key Challenges

- Effeciently stop the escalating volume and magnitude of targeted data breaches.
- Reduce the high volume of false alerts.
- Streamline and reduce resources focused on security breaches.

Key Results

- High, accurate visiblility into network anomalies.
- Accurate and effecient detection of active breaches.
- Ease of installation and increased staff productivity.

About LightCyber

LightCyber is a leading provider of Active Breach Detection solutions that accurately detect active cyber attacks that have circumvented traditional threat prevention systems. The LightCyber Magna platform is the first security product to simultaneously profile both network traffic and endpoint state in order to accurately detect compromised user accounts and devices early in the attack lifecycle, and to enable security operators to remediate breaches and stop attacks before real damage is done. Founded in 2011 and led by world-class cyber security experts, the company's products have been successfully deployed by top-tier customers around the world in the financial, legal, telecom, government, media and technology sectors.

LIGHTCYBER, 5050 El Camino, Suite 226,
Los Altos, CA 94022 Ph: (844) 560-7976
www.lightcyber.com

"When we discovered the LightCyber Magna™ platform, it seemed too good to be true," admitted Shalem. "In evaluating it we could see that it looked for an active data breach very differently than other malware-focused threat prevention systems." Magna looks for the operational activities an attacker must use—namely the reconnaissance and lateral movement needed to understand the network and identify valuable target assets. By passively applying Deep Packet Inspection (DPI) to all network traffic, Magna can profile all users and devices to understand anomalies using sophisticated machine learning. Intelligence from its agentless endpoint technology refines the understanding and provides automated investigated data that increases accuracy and operational efficiency.

Results

The first thing the team noticed was the level of accurate visibility into network anomalies they could get the LightCyber Magna platform. "The visibility was so good that we immediately completed our evaluation and dropped the other POCs that were in process," said Shalem. During the evaluation, they found the so-called Lenovo SuperFish virus through various command and control (C&C) breach indicators fired by Magna. Later they uncovered the clandestine use of a Remote Access Tool (RAT) that was believed part of an attempted breach.

The other remarkable result was the ease of use and installation. "This was the first ever solution in my 20-year career that you plug it and it immediately starts working," said Shalem. After a short soak period, the Magna platform was fully productive. It is also easy to use and greatly contributes to the security team's productivity. "You don't have to be a master of security to use LightCyber," said Shalem. "It just works."

Products Deployed

One Magna Detector D-500 and Pathfinder agentless endpoint software subscription service.

LIGHTCYBER
CLOSING THE BREACH DETECTION GAP