Cyberint

Case Study

ROLE OF THREAT HUNTING FOR BUSINESS RESILIENCE

The retail business environment nowadays embraces digital transformation to maximize engagement with customers, increase customer touch points and extend trust zones. While increasing the digitization efforts, moving to the cloud or going for 3rd party solutions, companies require a strong cyber resilience enabling versatile, adjustable and scalable environments with effective tools to monitor and manage any asset or process.

RETAIL

#1 Industry for security compromises and data breaches in 2018

2019 Trustwave Global Security Report

Among top-5 industries with the longest mean time to identify and contain a breach

2019 Cost of a Data Breach Report. Ponemon Institute/IBM

CUSTOMER PROFILE

This case study is about a large US-based retailer providing services in North America, Europe and Asia. Operating both in the online and brick-and-mortar markets, the company is facing digital transformation and modern threats brought by sophisticated threat actors.

Before starting a full-scale cloud migration for the majority of its business operations out of the data center, the company was facing a challenge of improving agility of business processes and addressing any potential threats it may encounter.

CUSTOMER CHALLENGES

Assess if the current level of infrastructure is sufficient to enable resiliency

Ensure effective cyber resiliency to support and address cloud migration

THREAT HUNTING WITH CYBERINT

To address those challenges, Cyberint was invited to perform Threat Hunting engagement in an effort to ensure their cloud business infrastructure is secure.

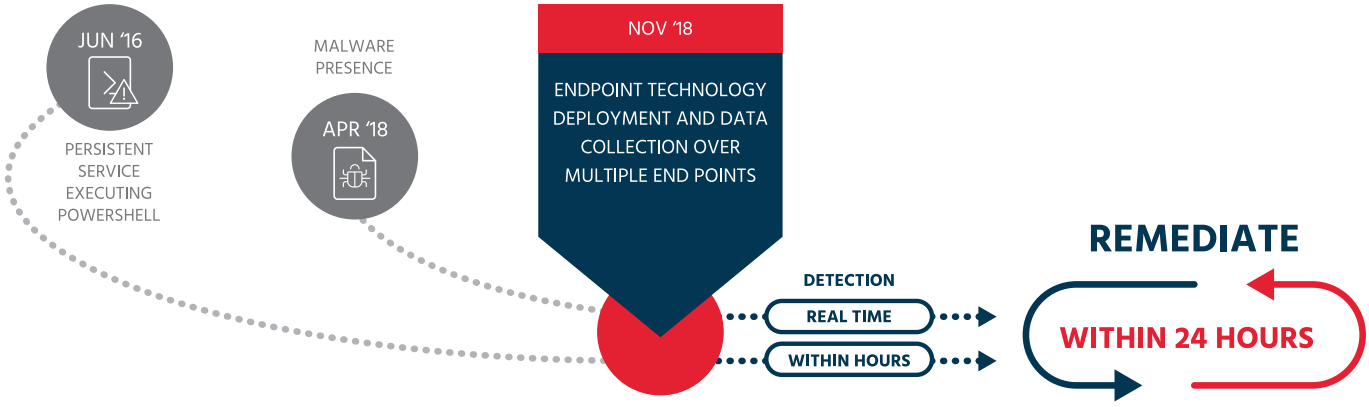
WHAT WAS DONE

- Deployed endpoint technology providing visibility into potentially suspicious and/or malicious activities
- Leveraged MITRE ATT&CK framework to construct hunting scenarios
- Collected and analyzed data

WHAT WAS DISCOVERED

CyberInt experts exposed two kinds of undetected malicious activities on the machines managing the POS configurations::

Persistent Service Executing Powershell	Malware Presence
Detected: Within hours | Dwell time: 2+ years	Detected: Real-time | Dwell time: 6 months
The service created by a user with domain admin privileges executing an encoded PowerShell script. After rapid triage it turned out to be an Invoke-Mimikatz script to dump credentials and exfiltrate them to a server under the attacker control.	Persistence mechanism allowed the malware to launch inside most of the processes that exists on the system. Investigation found evidence of anti-forensics in the form of time stomping. Keylogger enabled stealing user credentials while a user attempts to access shares across the network.



CybERInT ExPERTISE anD CaPabIlITIES allOWED TO:

- Detect malicious activities in the POS management environment, critical for business continuity
- Remediate threats within 24 hours of detection
- Ensure the company's environment was secure and ready for further cloud migration

ABOUT CYBERINT

We understand our customers need to have situational awareness and actionable insights to stay one step ahead, effectively responding to potential attacks and enabling their business mission. CyberInt's threat-centric approach to cybersecurity is more than just protection.

By endorsing real-time visibility across the entire business, digital risk protection solutions, integrated insights, proprietary threat hunting techniques leveraging MITRE ATT&CK™ framework, we transform cybersecurity into a business enabler that your organization values, and your customers trust.

CONTACT CYBERINT

Cyberint

www.cyberint.com

sales@cyberint.com

The Cyber Feed:
blog.cyberint.com

UNITED KINGDOM
Tel: +44-203-514-1515

USA
Tel: +1-646-568-7813

ISRAEL
Tel: +972-3-728677717

SINGAPORE
Tel: +65-316-357-6010

LATAM
Tel: +507-395-1553