CYLANCE

Retail **CASE STUDY**

INDUSTRY

Retail

ENVIRONMENT

- 200 locations worldwide
- 5,000 endpoints
- 10 million annual customers

CHALLENGES

Protect point of sale (POS) and digital signage systems from being exploited by Eastern European cybercriminals

Combat malware previously undetected by traditional antivirus

Protect private customer data

Safeguard millions of credit card numbers from motivated and skilled attackers

SOLUTIONS

Deploy CylancePROTECT® to 5,000 endpoints, replacing Symantec™ and Bit9™

Cylance® Compromise Assessment to identify breach activity and artifacts within days instead of months

The Company

An international retailer with hundreds of locations worldwide.

The Situation

The company suffered a compromise that resulted in the theft of millions of credit card numbers. They were notified about the breach by the United States Secret Service after the agency purchased a large batch of stolen credit cards from Russian hackers, with all cards tracing back to the retailer.

The Process

The company engaged Cylance Consulting to identify the origin of the breach and remediate.

Within hours, Cylance deployed a Compromise Assessment Tool on over 5,000 nodes across the enterprise. The Cylance Consulting team quickly identified the initial source of the breach, an employee's laptop infected with malware from the ZeroAccess family which served as a pivot point for the attackers.

Once on the network, the attackers were able to search and locate an IT administration script that contained a hard-coded password, giving them the ability to drop a BlackPOS variant on a series of Radiant Aloha POS settlement servers, scraping millions of credit card numbers over a series of weeks.

Unlike many breached corporations, this retailer tried to secure their infrastructure with full deployments of Symantec and Bit9. Unfortunately, Bit9 gives no contextual awareness as to the intent or possible risk a malicious executable can pose, so the malware the attacker deployed on the POS settlement servers was inadvertently whitelisted, allowing the malware to run without detection or alert from Bit9 or Symantec.

The Results

In the days following the investigation, CylancePROTECT was deployed enterprise-wide, replacing Symantec and Bit9 in order to permanently block not only the variants of malware discovered during incident response, but also to protect the endpoints from all malware threats moving forward.

Free Consultation

Want to see how CylancePROTECT and Cylance Consulting will empower your organization in the fight against cyberattacks? Contact us today for a free consultation!

Cylance Privacy Commitment
Cylance is committed to protecting your organization against advanced threats, which includes privacy disclosure. We do not publish the names of our case study partners for this reason.

"Despite deploying two well-known, traditional antivirus products, it was only CylancePROTECT that located and contained the malware that was the source of a breach. We have since made PROTECT and their HealthChecks a permanent part of our security process to ensure threats are identified before they execute."

-IT Manager
Retail Company

+1 (877) 97DEFEND
proservices@cylance.com
www.cylance.com
18201 Von Karman, Ste. 700 Irvine, CA 92612

R1_20160428