SIM2K
Adapting Technology to Your Business Needs

CYLANCE

Cylance® Case Study: Education

INDUSTRY

Education

ENVIRONMENT

- 7,500 enrolled students
- 1,500 endpoints

CHALLENGES

Reduce the amount of malware introduced to the network from infected student endpoints

Prevent the exploitation of the University's assets and protect students' personally identifiable information

Safeguard student computers with minimal impact

SOLUTIONS

Deploy CylancePROTECT® to students faculty and University endpoints

Retain Cylance® Consulting's ThreatZERO™ Services to handle alerts generated by student actions

Engage Cylance Consulting to perform a full Compromise Assessment to identify if the University's security was previously breached

The Customer

A traditional northeastern university with over 7,500 enrolled students (both undergraduates and postgraduates).

The Situation

The University's financial aid office was the victim of a CryptoLocker variant. CryptoLocker is a ransomware Trojan that attacks computers running Microsoft Windows®. It is propagated via infected email attachments and botnets, and when activated, encrypts certain file types on local and network drives. The encrypted files can only be opened with a private key stored on the malicious actor's command and control server.

The victim received a message offering to decrypt the data only if payment was received through Bitcoin or a pre-paid cash voucher by a stated deadline. The message threatened that if payment was not made by the deadline, the private key would be deleted or a higher ransom would be demanded.

Understanding that traditional signature-based antivirus was not capable of protecting their infrastructure from advanced malware like this CryptoLocker variant, the University reached out to Cylance and initiated a Proof of Concept (POC) for CylancePROTECT, a next-generation antivirus product.

The Process

Over the course of four weeks, Cylance deployed and monitored CylancePROTECT on 57 systems inside the University. Out of the 57 monitored hosts, Cylance was able to identify and block malware that had gone undetected by traditional antivirus solutions on 33.

In total, Cylance was able to immediately quarantine 183 pieces of unique malware already present and 107 additional potentially unwanted programs. Of those malware samples, 35 were completely missed by every other antivirus engine.

During the POC, multiple variants of CryptoLocker were identified, blocked and prevented from executing without disrupting any of the University's normal operations.

SIM2K®
Technology Consultants

6330 E. 75th St., Suite 336
Indianapolis, Indiana 46250

317.251.7920
800.746.4356
www.sim2k.com
sales@sim2k.com

SIM2K

Adapting Technology to Your Business Needs

CYLANCE™

The Results

Following the POC, the University purchased a full site license for CylancePROTECT and deployed it throughout the University, replacing Microsoft Security Essentials in less than eight hours with no impact on the end-users.

Consultation

Want to see how CylancePROTECT and SIM2K will empower your organization in the fight against cyberattacks? Contact us today for a free consultation at (317-251-7920), or SIM2K.com/Cylance.

CylancePROTECT worked quickly to identify and block nearly 200 threats that traditional antivirus software flat out missed. With a large number of faculty and student endpoints to protect, we are confident Cylance is securing our systems.

-University's IT Manager

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.

SIM2K®
Technology Consultants

6330 E. 75th St., Suite 336
Indianapolis, Indiana 46250

317.251.7920
800.746.4356
www.sim2k.com
sales@sim2k.com