Malwarebytes

CASE STUDY

Waverley Christian College creates a malware-free curriculum

Malwarebytes delivers fast response and remediation for "invisible" malware

Business profile

Waverley Christian College provides 1900 students in Victoria, Australia, with a quality Christian education experience. Programs from kindergarten through secondary school prepare students to achieve outstanding results, whether they plan to attend university or pursue immediate employment. A fileless malspam attack made it clear that the existing antivirus solution wasn't up to the test, so the College turned to Malwarebytes.

Business challenge

Making the invisible, visible

With 2100 endpoints across two campuses, the six-person Waverley Christian College ICT team has an extensive cyberattack surface to defend. All was going well until a previously unknown malware payload was deployed on several staff systems, which caused the machines to exhibit intermittent problems.

"I saw the spam email arrive and alerted my staff," recounted Alan Oh, ICT Manager for Waverley Christian College. "However, several College staff members had already responded to the email and unknowingly installed the malicious payload."

Although the Kaspersky antivirus detected a malicious email payload, it couldn't identify or clean it up. The ICT team removed systems from the network to prevent the threat from moving laterally to other systems. They activated Microsoft AppLocker as an extra control to stop unapproved applications and scripts from being executed. But the malware remained invisible.

Mr. Oh and his team searched the Internet to learn more about the malware. During their search, they came across Malwarebytes Endpoint Protection with Multi-Vector Protection and integrated remediation capabilities.

OVERVIEW

INDUSTRY
Education

BUSINESS CHALLENGE
Detect and prevent malware from being deployed on College systems

IT ENVIRONMENT
Microsoft environment

SOLUTION
Malwarebytes Endpoint Protection using education licensing

RESULTS
Identified and remediated new, previously unknown fileless malware within a few hours

Rapidly deployed advanced, multi-vector protection

Gained protection across all systems—online and offline

> MALWAREBYTES' RESPONSE WAS PHENOMENAL. THAT, COMBINED WITH THE ABILITY TO SITE-LICENSE THE PRODUCT FOR OUR TWO CAMPUSES, MADE OUR DECISION EASY. WE REPLACED KASPERSKY WITH MALWAREBYTES ENDPOINT PROTECTION.
>
> ALAN OH, ICT MANAGER,
> WAVERLEY CHRISTIAN COLLEGE

"We conducted a comprehensive search, looking for solutions that could detect and stop malicious payloads before they deploy," said Mr. Oh. "We immediately contacted Malwarebytes and launched a trial, which delivered unexpected benefits for everyone."

The solution

Malwarebytes Endpoint Protection

The Malwarebytes team first scanned the affected systems and found…nothing. That meant the threat was a type of fileless malware, so they retrieved Farbar Recovery Scan Tool (FRST) logs and registry information from the affected Windows systems. This data revealed a new, unknown variant of EMOTET, a banking trojan, which leveraged a fileless PowerShell script and DLL library to hide in the system registry. Unchecked, EMOTET can steal passwords and administrator credentials, emailing itself to address book contacts, and copying itself across the network via shared folders.

Now the Malwarebytes Research team had what they needed to quickly create and publish a new detection rule that addressed this zero-day threat. Within hours, Waverley Christian College and Malwarebytes customers worldwide could surgically target and clean this EMOTET trojan infection.

"Malwarebytes' response was phenomenal," said Mr. Oh. "That, combined with the ability to site-license the product for our two campuses, made our decision easy. We replaced Kaspersky with Malwarebytes Endpoint Protection."

Fast speed-to-protection

In 12 days, Waverley Christian College had tried, chosen, and deployed Malwarebytes across its two campuses. The ICT team used Microsoft System Center Management to push out Malwarebytes to its endpoint systems. The software was deployed and protecting users within three hours.

Better protection performance

Since adopting Malwarebytes, the College has protected users and systems against a wide range of PUPs, malware, malicious websites, and malspam. The College considered Microsoft ATP to defend Office 365 email, but chose Malwarebytes for broader protection. Malwarebytes defends against threats that are activated when malicious links and file attachments are launched, as well as threats arriving from non-Microsoft email domains such Gmail and HotMail.

"Malwarebytes enables us to protect systems, even when they are offline," said Mr. Oh. "Whether it's a Windows system, Mac, or iOS device, we can be sure that they defend against malware with the most current protection, even when not connected to our network. It's a huge relief."

At-a-glance visibility

Malwarebytes makes it easy for the ICT team to stay apprised of potential threats. The Malwarebytes Endpoint Protection cloud console provides an instant overview of College systems and their cyber-health status. The easy-to-use console enables anyone on the team to gain visibility into specific threats, and alerts notify the team of anything requiring immediate attention.

"We needed 24x7 protection for our users, and we got it with Malwarebytes," said Mr. Oh. "Malwarebytes' teamwork, fast response, and effective protection against previously unknown threat variants are second to none."

malwarebytes.com/business corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware and exploits that escape detection by traditional antivirus solutions. Malwarebytes completely replaces antivirus with artificial intelligence-powered technology that stops cyberattacks before they can compromise home computers and business endpoints. Learn more at www.malwarebytes.com.