

Electrical contracting firm short-circuits malware threats

Briggs Electric uses Malwarebytes to remediate CryptoLocker and prevent malware from shocking its systems

INDUSTRY

Construction

BUSINESS CHALLENGE

Add a layer of protection against damaging exploits

IT ENVIRONMENT

Data center with Trend Micro antivirus on desktops and file encryption

SOLUTION


Malwarebytes Endpoint Security, which includes Anti-Malware, Anti-Exploit, and the Management Console

RESULTS

- Remediated CryptoLocker attack
- Prevents new exploits
- Protects servers by blocking attempts at entry by malicious actors

Business profile

Briggs Electric, Inc. provides electrical contracting services for commercial construction, tenant improvement, and renewable energy projects across a wide range of vertical markets. Locations in Tustin, California, and Carson City, Nevada, experienced malware issues, but the IT team turned to Malwarebytes and pulled the plug on malicious threats.



Since deployment, we have not detected any additional exploits—especially CryptoLocker. Now I can sleep at night.

—Larry Reed, IT Manager, Briggs Electric, Inc.

Business challenge

Prevent malware from overpowering users

Approximately 50 office staff and 100 field electricians keep Briggs Electric powering ahead on a wide range of projects for large healthcare, government, financial services, retail, and education clients. Laptops and desktop systems keep everyone connected in the office and in the field, but the machines were increasingly vulnerable to malware. Although Briggs had deployed a Trend Micro antivirus solution on its endpoints, the software left a lot to be desired because it routinely missed significant threats. Unfortunately, in 2015 the company was hit with CryptoLocker ransomware.

“We first realized that we had been attacked when a user couldn’t open a file as usual,” said Larry Reed, IT Manager at Briggs Electric. As Reed reviewed network activity, he was able to quickly narrow the search to a specific machine, remove it from the network, and identify the problem. However, he also had to ascertain how much damage the malware did. CryptoLocker had encrypted Microsoft Word and Excel files and .pdf documents before Reed was able to stop it. It took a week to recover files and clean up the machines.



The solution

Malwarebytes Endpoint Security

“We needed another layer of protection,” said Reed. “I trusted Malwarebytes because it had always enabled us to detect and remediate malware in the past. We chose Malwarebytes Endpoint Security to provide robust, comprehensive prevention and defense against malware and dangerous exploits.”

Malwarebytes Endpoint Security provides a powerful multi-layered defense engineered to defeat the latest, most dangerous malware, including ransomware. It includes Malwarebytes Anti-Malware, Anti-Exploit, and the Management Console in one comprehensive solution. Malwarebytes Anti-Malware detects and eliminates zero-hour malware, Trojans, worms, rootkits, adware, and spyware in real time. It stops threats in their tracks and saves Reed from having to manually remove malware from endpoints. Malwarebytes Anti-Exploit adds even more defenses against malware. Four layers of protection work together to block exploits and prevent malicious payloads from being delivered.

Reed deployed Malwarebytes on each machine to ensure that all were now clean and protected. Once installed on all machines, the software found a significant amount of malware, especially toolbars and malicious code that had been installed with other software packages downloaded from the Internet.

Fast, efficient remediation

Now as Reed monitors Internet traffic and browsing patterns, when he sees suspicious behavior he contacts the end user and has the user perform a Malwarebytes scan on the machine. If the machine is clean, the user notifies Reed. If malware is found, the user easily removes it and notifies Reed what was found. Reed plans to deploy

the Malwarebytes Management Console, which will simplify management even further and deliver additional visibility into endpoints and malware.

Protecting servers

Briggs also deployed Malwarebytes on its servers, which enabled the company’s Exchange servers to successfully block threats trying to gain entry through email.

“Why not put it on servers? It works and it enables us to keep bring-your-own-device endpoints from introducing malware onto our network,” said Reed. “We’re refreshing our data center and I will certainly deploy Malwarebytes on the new machines.”

Peace of mind


“We have not detected any additional exploits,” said Reed. “The primary reason I chose Malwarebytes was for peace of mind. Now we know that we can address threats successfully if necessary, and I can sleep at night.”


With Malwarebytes, Briggs Electric gained strong endpoint protection while reducing the risk of malware gaining entry through its servers. Shocking, isn’t it?


| About

Malwarebytes is the next-gen cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company’s flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. More than 10,000 businesses worldwide use, trust, and recommend Malwarebytes. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia, and a global team of threat researchers and security experts.

 Santa Clara, CA

 malwarebytes.com

 corporate-sales@malwarebytes.com

 1.800.520.2796