AKAMAI CASE STUDY

# Large Manufacturing Company Improves its Security Posture with Enterprise Threat Protector

## Requirements

- Add another layer of defense to a pre-existing security suite
- Cause minimal network disruption
- Be self-serviceable and require minimal support

## The Situation

A leading manufacturer in Europe was interested in improving its overall security posture against evolving cyber threats. It did not have specific ideas of what additional security layers were needed when it first met with Akamai's team, but instead asked Akamai to work with it to identify potential gaps in security. Enterprise Threat Protector appealed to the manufacturer because the product addressed an existing security vulnerability, was easy to use, and required minimal support after deployment. The manufacturer signed up for a product trial soon after meeting with Akamai.

## The Trial Program

Over only a few weeks, the manufacturing company noticed that more than 7,000 DNS requests had been flagged by Akamai's security list, indicating potential threats on their network. Further analysis by Akamai's team uncovered that these command and control (CnC) requests were related to Conficker.B malware. Conficker — also known as Downup, Downadup, and Kido — is a computer worm targeting Windows operating systems. It uses flaws in Windows OS software and dictionary attacks on administrator passwords to form a botnet, and has been unusually difficult to counter because of its combined use of many advanced malware techniques.

Enterprise Threat Protector also detected DNS requests to legitimate websites that had been known to be used to distribute Cryptolocker and Locky ransomware. Once installed on an enterprise's network, this malware moves across the network and encrypts files on endpoint devices and servers. Ransomware now poses a significant threat to enterprises, and there have been a number of high-profile cases in the past 12 months.

These discoveries were more than enough to create a compelling business case for the manufacturer to purchase Enterprise Threat Protector, shifting a general desire for a new security layer into a targeted way to proactively protect the enterprise.

## Why Akamai?

After successfully running the trial, the company knew that Enterprise Threat Protector was a necessary addition to its current suite of security products. Not only did it integrate seamlessly with the security products the customer already had in place (endpoint anti-virus and Dell firewalls), but it also offered a proactive approach to protecting against future attacks with real-time intelligence updates regarding new, emerging threats.

Now, all of the manufacturing company's external recursive DNS traffic is directed to Enterprise Threat Protector, and requested domains are checked against Akamai's real-time domain risk scoring threat intelligence, so the company can proactively block users and devices from accessing malicious domains and services. As this validation happens before the IP connection is made, threats can be stopped earlier in the security kill chain, i.e., farther away from their perimeter. Enterprise Threat Protector has been simple for the customer to use, required no major network changes, and allowed company-wide, uniform enforcement of policy