

West Memphis School District



Location

West Memphis, AR

Industry

Education

The Problem

- Network inadequately protected against malware by statewide content filter with free OpenDNS as backup.
- Network had malware and botnets **already inside**, “calling home” to China and other countries.
- Critical data vulnerable to breach from botnets.

The Solution

- ThreatSTOP immediately blocked malware and botnets bi-directionally on Vyatta router/firewall software.
- Gives network administrators clear view of what malware is inside network.
- Provides remediation tool for network administrator to clean/quarantine infected machines.

Customer Overview

The West Memphis School District comprises 12 campuses (one high school, 11 K-8) with 6,000 students and 600 teachers / administrators. Its 1,500 computers and 50 servers connect to the Internet via one egress point at the district office, through a 1-2 core Vyatta router/firewall software. Before ThreatSTOP, the network was protected by Vyatta’s NAT (network address translation), a M86 content filter administered statewide by the state, and a free OpenDNS as a backup.



The Problem

In the beginning, there was no perceived problem. Gary Woodward, WMSD’s network administrator, was intrigued by a description of ThreatSTOP on Vyatta’s customer forum, and decided to do a 30-day free trial. What ThreatSTOP found was eye opening. “I had no idea my network printers are talking to China”, Gary exclaimed! It was clear from then on that WMSD’s data security was inadequate, and it is very vulnerable to a breach.

“I didn’t know what I didn’t know,” Gary said. Gary’s experience is quite common. Signature-based products such as content filters, anti-virus software, IDS/IPS or firewall filters do not adequately catch botnets and advanced malware, or catch them in time. Customers of those products have a false sense of security. ThreatSTOP has found botnets **already inside** those customers’ networks 100% of the time, just as it did with WMSD.

“I had no idea my network printers are talking to China!”

--Gary Woodward

Network Administrator, WMSD

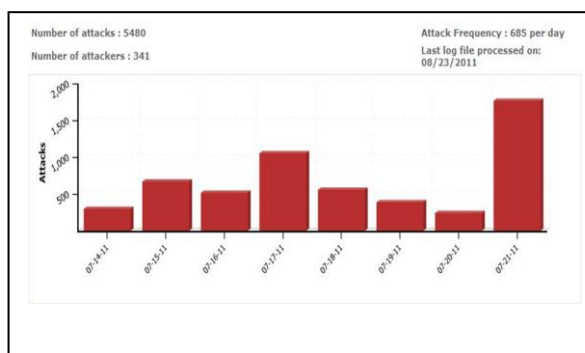
The Solution

With ThreatSTOP at the firewall, it provides the first line of defense and the best last hope against data theft. In a typical week in July, 2011, ThreatSTOP blocked the following:

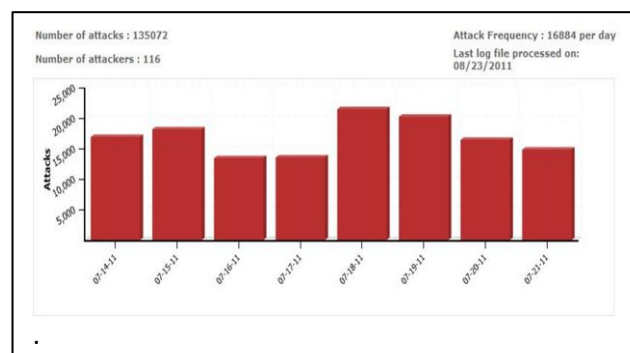
	Inbound	Outbound
# of Attacks	5,480	135,072
# of Attackers	341	116
Daily average	685	16,884

These are typical results for a small to medium organization; larger ones see attack volumes many times this. A sample of the outbound blocks shows a rogue gallery of the world's cybercriminal syndicates attempting to breach WMSD, as reflected in these bad IP lists they are on: Russian Business Network, SpamHAUS DROP, Cymru bogons, DSHIELD, and IPs from Ukraine, Latvia and China. These are certainly IP addresses that no one associated with WMSD should be talking to.

Inbound Blocks



Outbound Blocks



These Web-based reports, parsed from the firewall logfiles, are used to discover, diagnose and remediate WMSD's malware infestations daily. Gary has implemented a script that forces a blocked machine to request a work order so that it is operable again.

Results—Effective Protection and Peace of Mind

ThreatSTOP has proven to be an easy and very cost effective cloud service that solves the pervasive bonet and malware problem at the gateway. It protects against data theft without requiring the cost, time and complexity of a forklift upgrade that most other solutions require. Its web-based reports provide a simple and effective diagnostic as well as remediation tool for IT and security professionals to protect their networks.

“ThreatSTOP discovered the serious vulnerabilities in our network and provided the reports and tools to help me solve the problem on a daily basis.”

Gary Woodward

Network Administrator, WMSD