Threat STOP

ThreatSTOP | Customer Story | U.S. Public School District

How a Tennessee Public School District Taught Advanced Threats a Lesson

CUSTOMER OVERVIEW

The Public School District comprises over a dozen campuses with 6,000 students and 750 teachers and administrators. Its 1,500 computers and 50 servers connect to the Internet via one exit point at the district office, through a router and firewall. Before ThreatSTOP, the network was protected by the Firewall's built-in features, an M86 content filter administered by the State, and a free DNS forwarding content filter administered by the State.

SOLUTION IMPACT

Full Visibility
into the network

Over 140K
of attacks blocked
per week

Remediation
capabilities to
quarantine infections

INDUSTRY

Education

SECURITY CHALLENGES

The PSD's network and critical data were inadequately protected, and they had already been breached by malware and botnets.

WHY THEY CHOSE THREATSTOP

The school district's team selected ThreatSTOP because the cloud-based solution delivered reliable inbound and outbound threat prevention, over both IP and DNS communications, without requiring skilled people to manage it or any new hardware.

> *"I had no idea my network printers are talking to China!"*
>
> *- Network Administrator, TN Public School District*

THE PROBLEM

When the School District first signed up for a ThreatSTOP trial, they had no perceived problem in mind, but what they found using ThreatSTOP was eye-opening. “I had no idea my network printers are talking to China”, their Network Administrator exclaimed. It quickly became clear that their network’s data security was inadequate, leaving them extremely vulnerable to data breaches and attacks. “I didn’t know what I didn’t know,” the Admin continued, and his 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 and malware already inside those customers’ networks 100% of the time, just as it did for the PSD.

THE SOLUTION

ThreatSTOP's cloud service on the firewall is the first line of defense against malware threats like ransomware, botnets and phishing, and provides the best next-stage protection against outbound data theft. By implementing ThreatSTOP , the customer saw an immediate change, with a weekly average of over 140K attacks blocked. These are typical results for a small to medium school district; larger ones, and post-secondary schools see much greater attack volumes due to larger user and device populations or more open internet access policies.

A sample of the outbound blocks in the customer's network shows various cybercriminal syndicates attempting to breach their network. As discovered by our bad IP lists, they are on: Russian Business Network, SpamHAUS DROP, Cymru bogons, DSHIELD, including IPs from Ukraine, Latvia and China. These are certainly IP addresses that no one associated with the school district should be talking to.

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

RESULTS - *Effective Protection and Peace of Mind*

The ThreatSTOP platform is a proven, easy and cost-effective cloud service that stops the pervasive botnet and malware problem at the gateway before damage is done. Automatically aggregating over 900 threat intelligence sources, it protects against all cyberthreats and data theft without the cost, time and complexity of a forklift upgrade that most other solutions require. ThreatSTOP's web-based reports provide a simple and effective diagnostic as well as remediation tool for IT and security professionals to protect their networks.