ThreatSTOP

www.threatstop.com
sales@threatstop.com

US: 760.542.1550

ub
UNIVERSITY
OF BALTIMORE

University of Baltimore

Customer Story

Location

Baltimore, Maryland

Industry

Education

The Problem

- Significant manual resources used to blacklist IPs and clean up malware infections.
- Performance of hosts degraded by malware.
- Data breaches posed major security vulnerabilities for university's open environment.

The Solution/Benefits

- ThreatSTOP on the Juniper SRX immediately blocked malware and botnets.
- 90% drop in help desk tickets related to malware and eliminating manual IP blacklisting.
- Network performance improved significantly due to highly efficient inbound blocking by IP.

The University of Baltimore is part of the University System of Maryland with approximately 6,400 undergraduate and graduate students in law, business, public affairs, the applied liberal arts and sciences. Its law school is the nation's sixth largest public law school. Its network consists of several datacenters firewalled by Juniper Services Gateways and a Cisco router and switch network environment. The primary security product used before ThreatSTOP was Symantec antivirus.

The Problem

Like most universities, UB provides an open academic environment for learning and knowledge sharing, which makes information security a particularly tough challenge. It was expending significant security, network, and desktop resources to manually keep up with blacklisting IP addresses as well as cleaning malware infections that were getting through perimeter defenses. Despite ongoing user education efforts and other security controls in place, users would continue to respond to phishing and visit malicious websites which led to infected hosts.

> **"Our Help Desk team was overwhelmed. The whole malware problem was over utilizing vital resources"**
>
> **- Mike Connors**, Information Security Analyst

UB needed three things:

1. A way to limit users' ability to interact with phishing and exposure to bad sites while maintaining an open academic environment
2. Streamline and automate the process in which a bad IP could be blocked and updated, freeing staff for other tasks not associated with malware infection
3. Upgrade its old Juniper firewalls because they were an end-of-life product and could only support a very small number of IPs on a ThreatSTOP blocklist, which would of course limit the full capabilities of ThreatSTOP's service.

The Solution

After months of evaluation, UB selected Juniper SRX Services Gateways and ThreatSTOP Shield for its firewall upgrade project. Other products such as OpenDNS were evaluated but didn't satisfy UB's need. OpenDNS only blocks by domain names, which is not granular enough; UB receives a lot of malicious traffic via bad IPs. The selection criteria were:

1. For Juniper: the SRX firewall provided the functionality and capacity for future growth. Also, UB is familiar with Juniper's technology and environment, and the upgrade caused minimal disruption.

2. A major contributing factor to Juniper's selection is that ThreatSTOP integrates very easily with it and it can support ThreatSTOP's full functionality.

3. For ThreatSTOP: provided an automated IP updating and blocking service with a high malware catch rate and very low false-positives.

Benefits

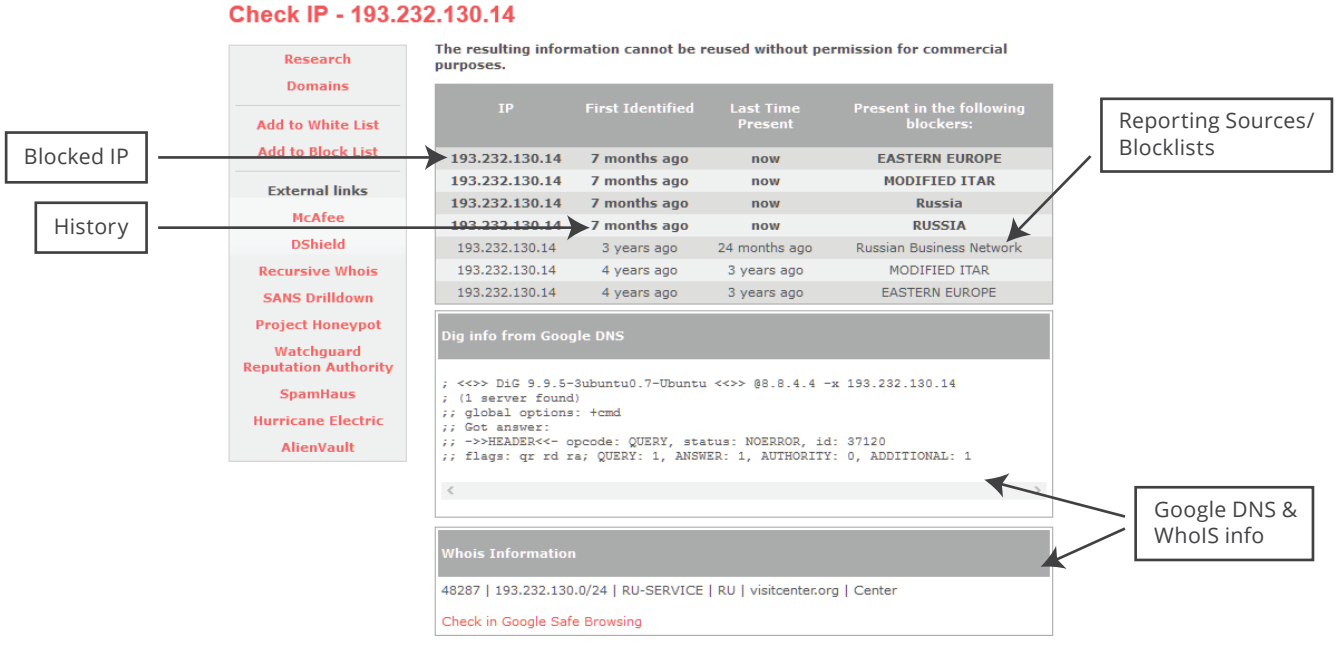
The ThreatSTOP firewall solution immediately provided benefits. In a typical one-week period in May, 2016, ThreatSTOP blocked the following malware traffic:

In the sample report, we can see that the attacks stopped were:

Inbound	**35,247,260**
Outbound	**185,138**

In one instance during their initial roll-out, a high-privileged user was discovered to be "botted." ThreatSTOP stopped the bot from "calling home" and activating a breach. This allowed UB's IT help desk to quarantine the machine before any damage was done.

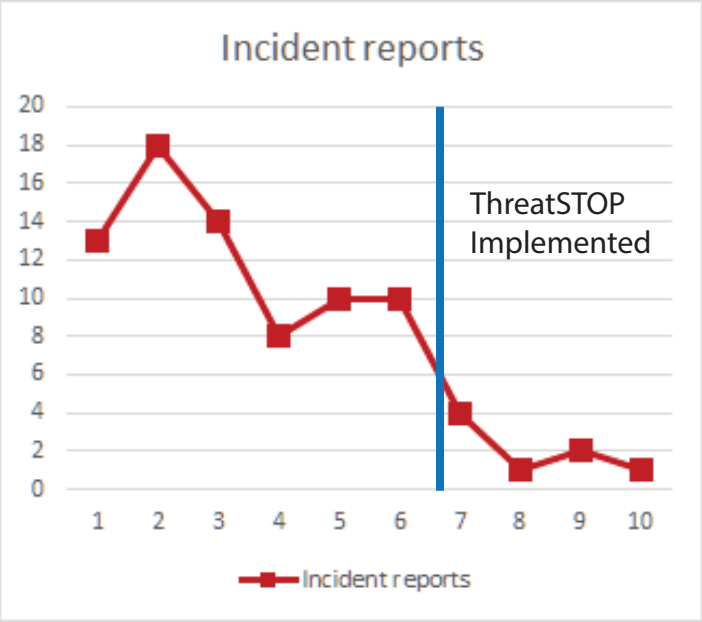
The ThreatSTOP service includes web-based reports parsed from customers' firewall logfiles that enable them to discover, analyze and remediate malware infestations. If necessary, they may also choose to prosecute the malware perpetrators using the information provided by these reports.



90% Drop in Help Desk Tickets Related to Malware Infections

The reduction in help desk tickets has also been immediate following ThreatSTOP deployment: from 10-18 per month before ThreatSTOP to the current 1-2/month, a 90% drop in malware tickets:

Help Desk Malware/Virus Incidents



"The decrease in malware/virus incidents has allowed our team to focus on other tasks."

- Dave Wells, Call Center Manager

Results—Protection, Reduce Cost and Peace of Mind

ThreatSTOP Shield is the most effective solution against malware with the highest catch rates and accuracy (low false positives), fastest updates and earliest detection rates. It enables customers' existing firewalls to solve the pervasive problem. Once installed via a simple script on a firewall, ThreatSTOP delivers a blocklist of known bad IP addresses to the firewall to enforce. The list is continually updated and automatically distributed to the firewall via DNS. It enhances the customers existing investment, and saves the customer the expense, hassle and delay of hardware upgrades, network reconfiguration, and retraining.