

### Bibliotheek Rotterdam



#### Location

Rotterdam, Netherlands

#### Industry

Public Agency

#### The Problem

- Library was blacklisted and Internet access blocked by ISP due to botnets and malware on its Wi-Fi network.
- Library had to manually clean up network every day in order to have Internet service restored.
- Juniper SRX 240 gateway appliance with UTM services did not solve the problem as expected.

#### The Solution/Benefits

- ThreatSTOP Botnet Defense Cloud on the Juniper SRX 240 immediately blocked malware and botnets.
- Service stoppages and manual cleanups eliminated.
- Web-based reports provide great problem discovery, monitoring, analysis and remediation tool for network administrators.

#### Customer Overview

Bibliotheek Rotterdam is one of the largest libraries in the Netherlands with one central library and 23 branches serving over 3 million users each year. Its collection has over one million books, magazines and multimedia items including the Erasmus Collection. Initially, its network consisted of 450 office PCs, 450+ public PCs and Wi-Fi devices connected to the Internet via one egress point through a Cisco router. Security consisted of blacklisting on a SQUID proxy and the free version of OpenDNS as a backup.



#### The Problem

Every day about 1,000 visitors (mostly students) use the library's PCs as well as connecting to the library's free Wi-Fi network with their laptops. These users are always getting infected and, as a result, the library was constantly blacklisted by the ISP and its Internet access blocked due to the large amount of "botted" machines and active malware on the network despite the security in place.

After months of mounting frustration, the library bought a Juniper SRX 240H Gateway appliance with UTM services in April 2010. But the problem remained unsolved despite implementing this "best of breed" solution because the library had an **outbound** traffic problem while the SRX, like most firewalls and security products, was primarily configured to block **inbound** traffic. Outbound traffic was subjected to the security policy, but traffic on standard ports such as port 80 (HTTP) was passed through as normal traffic, even if the content of the traffic is a "botted" machine "calling home". The W-Fi network did not accept any inbound traffic; it was infected by all the users from the inside.

**"We had to delete data from the public PCs every night, clean it up, and start all over again every day!"**

*--Nikola Nikolic  
Services & Contracts Manager*

## The Solution

In July 2011, the library's managed service provider Avnet found ThreatSTOP through a recommendation from Juniper and signed up for a free trial. After a quick and successful trial, the library subscribed to the ThreatSTOP Botnet Defense Cloud service in September. The ThreatSTOP/Juniper combination worked immediately as expected.

In a typical two-week period in October, 2011, ThreatSTOP blocked the following outbound malware traffic:

# of Attacks	62,443
Daily average	4,163

The primary culprit here is the notorious Russian Business Network, which is constantly probing networks globally using many IP addresses under its control.

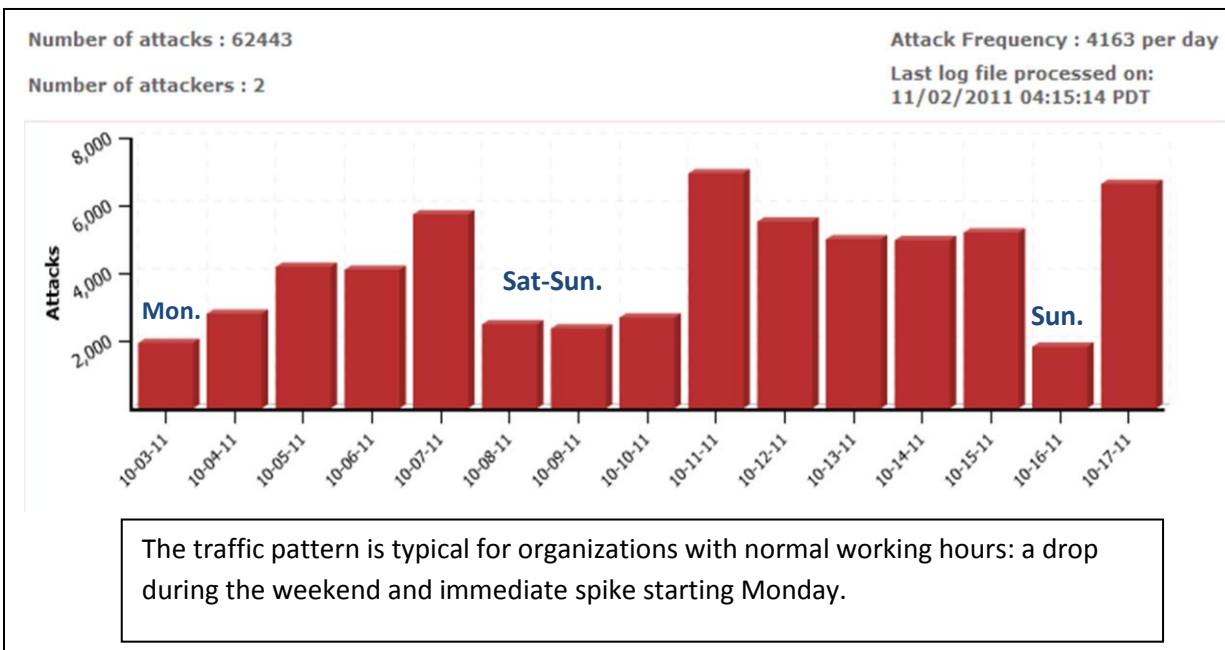
**"The ThreatSTOP service was very easy to install with a simple script and integrated with the SRX nicely as if it's part of the firewall. ThreatSTOP on the SRX 240 worked exactly as it should, and immediately blocked the botnets that have been plaguing the library for years."**

*--Dennie Spreeuwenberg  
Manager, Services Networking & Security  
Avnet Benelux*

## Reporting

ThreatSTOP also analyzes the log files uploaded from the SRX and presents a set of reports on what traffic was blocked with a simple way to drill down on individual events. With these Web-based reports included in the service, the library staff and its service providers can easily discover, monitor, analyze and remediate any malware problems.

### Outbound Blocks



## Results—Effective Protection and Peace of Mind

Firewalls on their own do not stop botnets/active malware effectively. Nor do traditional signature-based security products such as anti-virus, URL/content filters, email proxies, and IDS/IPSs.

ThreatSTOP enables customers' existing firewalls to solve what's considered by many as the biggest information security

problem today. Once installed via a simple script on a firewall, ThreatSTOP delivers a blocklist of known bad IP addresses to the firewall to enforce, automatically and continually updated via DNS. It leverages the customer's existing investment, and saves the customer the expense, complexity and delay of hardware upgrades, network reconfiguration, and retraining. ThreatSTOP provides immediate protection in a very cost effective way.

**“Now we have no service stoppages, no escalations with the ISP, and no manual cleanups. We just look at the reports and respond to any issues very quickly. ThreatSTOP has solved a very big headache for us.”**

*--Nikola Nikolic  
Services and Contracts Manager*