

---

Threat **STOP**™

## Cloud Network Defense

**Tom Byrnes**

Founder & CEO

760.542.1550 x4242

[tomb@threatstop.com](mailto:tomb@threatstop.com)

[www.threatstop.com](http://www.threatstop.com)

- RANUM: “the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents.”

# The “Fire”Wall



# Issues:

- Time to detection.
- Preservation and non repudiation of record.
- Certainty of Actor.
- Volume of data.
- Often long after event.
- Often not admissible in court (rw storage, chain of custody).
- What machine had that IP AT THAT TIME?
- Who was logged on?
- Most irrelevant, alerts, etc.

# Threat List Management

# Threat **STOP**<sup>TM</sup>

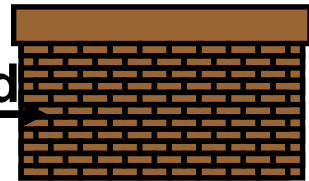
Cloud Network Defense

## Sensors



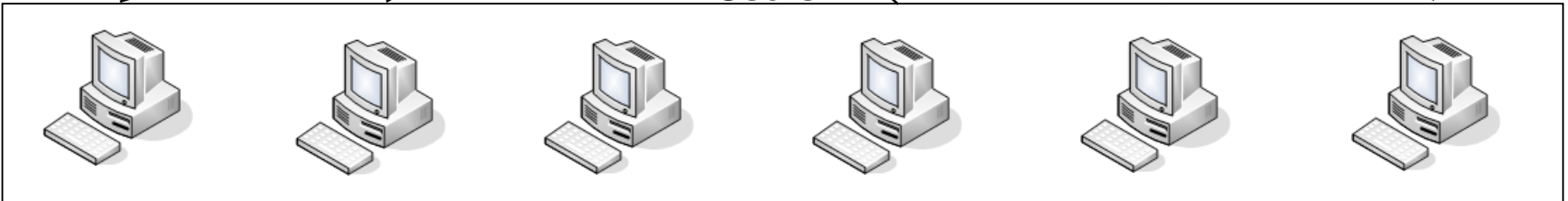
Threat **STOP**<sup>TM</sup>

Standard  
DNS



Firewall

## Users



**Lists Updated Every 2 Hours  
For Real Time Protection**



### Filter, correlate, alert, in real time.

The best event is one that didn't happen.  
Block, alert, remediate.  
At the very least, alert.  
“We make your firewall better.”

### Firewall Report - Stopped Outbound Connections for All devices

Please select the device and dates you would like to view. The report only shows connections to and from addresses that are in our block lists.

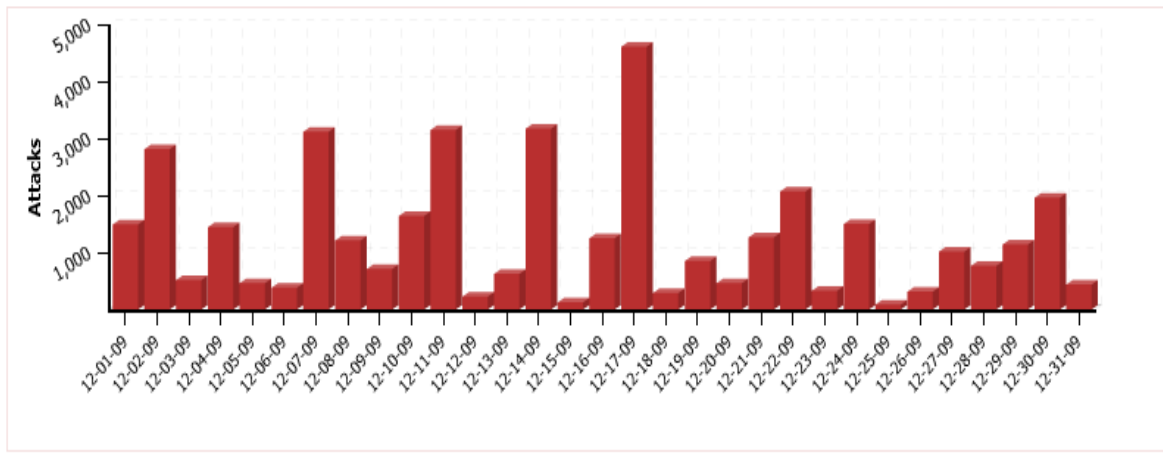
To export all the data, [please click here.](#)

From:   To:  

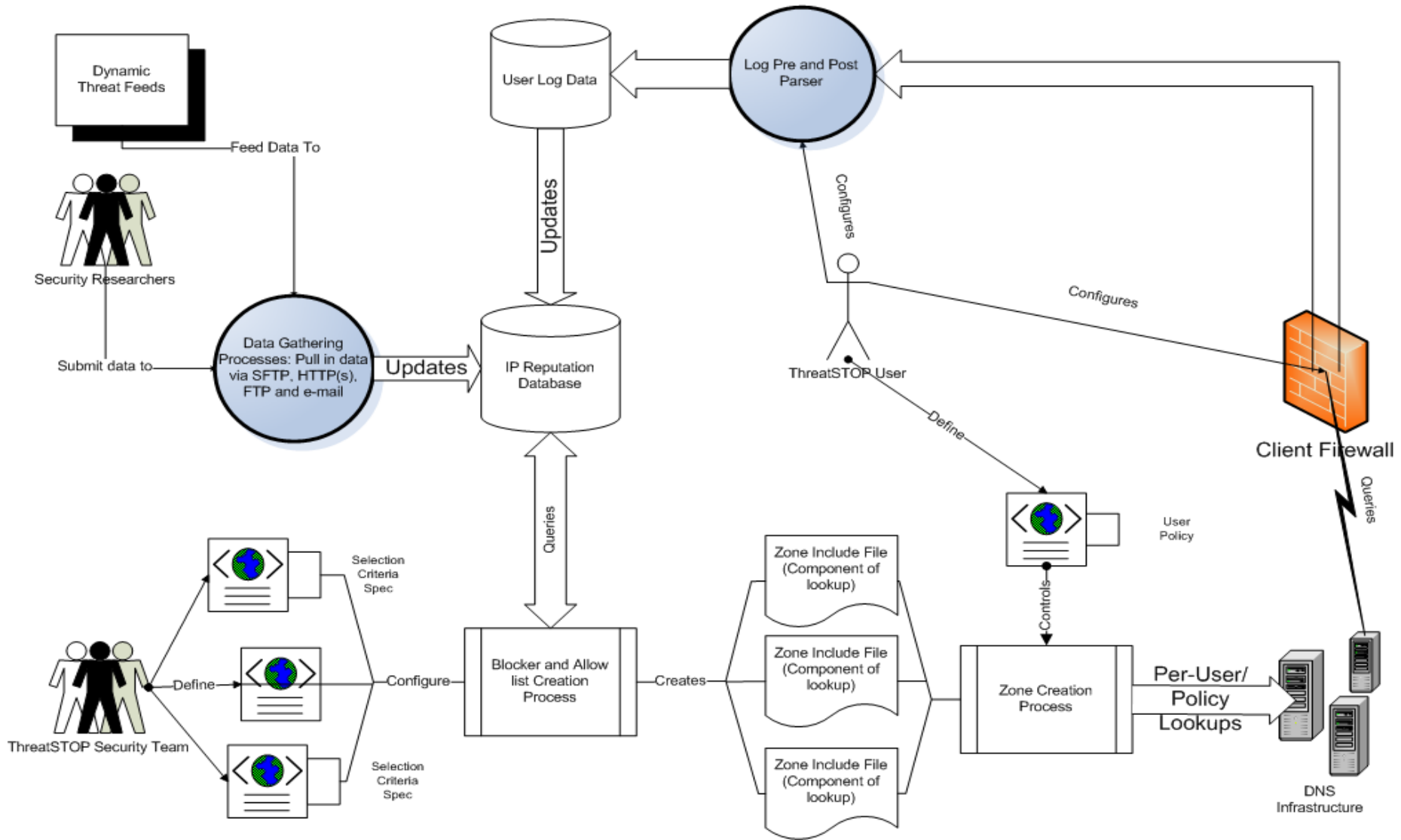
Devices:  Report:

Number of attacks : 39454  
Number of attackers : 1086

Attack Frequency : 1273 per day  
Last log file processed on:  
09/14/2010



# How it works



## Check Your Logs

The ThreatSTOP log analyzer has examined your log and discovered that the following IP addresses have had contact with your system. Please note that, unless the only hit is from a Geographic IP address list, these IP addresses are either known for their criminal activity or a trojaned host.

IPs Checked	Known	Unknown
5	5	0

Bot or Trojan IPs	Number of Connections	First Identified	Last Seen	Feed
91.213.121.176	1	2009-12-23 13:36:58 2010-01-06 17:00:46	2010-02-09 17:00:01 2010-09-13 18:01:12	Parasites, Hijackers and Spyware Domains Spamhaus Don't Route or Peer
88.198.88.123	1	2009-12-23 13:36:21	2010-07-15 01:30:06	Parasites, Hijackers and Spyware Domains
8.12.43.252	1	2008-11-10 12:00:03	2010-06-02 05:00:05	Parasites, Hijackers and Spyware Domains
64.136.44.21	1	2008-07-03 10:27:28	2010-09-13 18:00:18	Parasites, Hijackers and Spyware Domains
207.46.179.247	1	2008-07-03 10:28:37	2010-09-13 18:00:18	Parasites, Hijackers and Spyware Domains

[Check a new log](#)

---

# Threat **STOP**™

## Cloud Network Defense

**Tom Byrnes**

Founder & CEO

760.542.1550 x4242

[tomb@threatstop.com](mailto:tomb@threatstop.com)

[www.threatstop.com](http://www.threatstop.com)