

Stop Botnets Stealing from You!

ThreatSTOP Botnet Defense Cloud is a cloud service based on IP reputation that enables your existing firewalls to block botnet and malware traffic to and from your network. The service prevents data theft, increases network “goodput”, reduces network load, attack surface, help desk calls and reportable events. It is deployable within an hour without the expense, complexity and delay of hardware upgrades, network reconfigurations, retraining or manual updates.

ThreatSTOP is the most effective botnet/malware protection solution with the lowest TCO. It is superior to the prevailing signature-based products in the market today with much higher catch rates and accuracy, earlier detection and faster updates.



The Botnet Problem

Botnets and active malware are the most serious network security problems today

- 100% of networks have active malware
- Signature-based products—the majority in the market—are ineffective
- Do you know what’s inside your network? Are you “botted” **already**?
- Breach is expensive: financial, brand, non-compliance, productivity cost

Key Benefits

- Stop data theft by blocking “call homes” to command and control hosts
- Cut inbound attacks and network attack surface
- Minimize 0-day attacks
- Increase network “goodput” by 10-25%
- Reduce network load and capacity upgrade cost
- Reduce help desk calls and reportable events
- Install and use in <1 hour
- Immediate protection

Block. Protect. Save Money.

“ThreatSTOP works great. We are attacked every day and it stops them. It gives me the “warm and fuzzies” that I am protected. It’s well worth every penny.”

*Richard Gaustad
VP—CIO, Earth Systems*

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

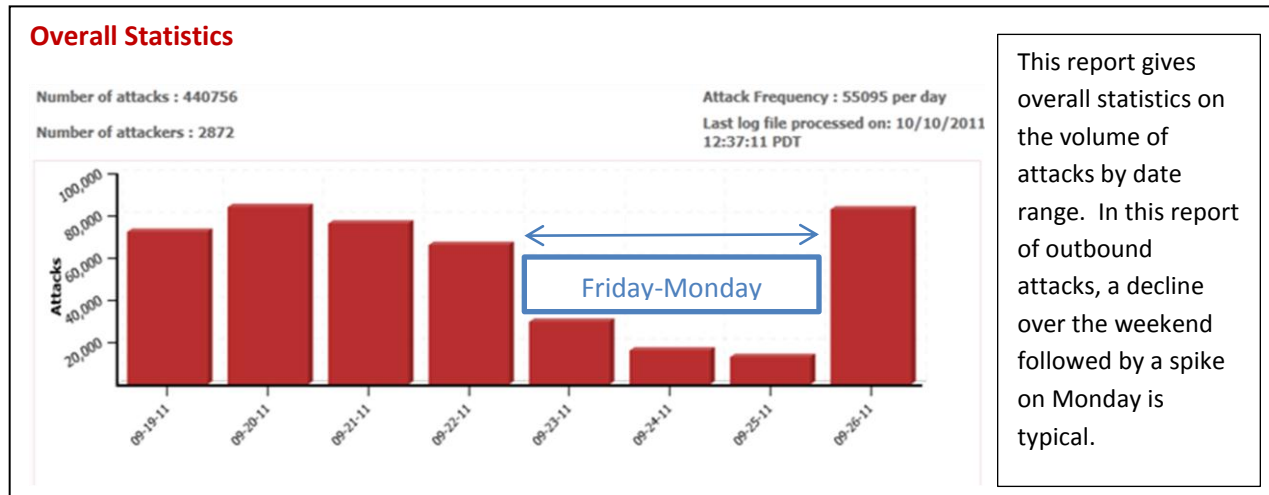
*Gary Woodward
Network Administrator
West Memphis School District*

“ThreatSTOP saved us \$200,000 on email server upgrades that we put into classrooms instead.”

*Steve Gorham
CIO
Hillsborough Community College*

Web-based Reports

Web-based reports included in the service are great malware discovery, analysis, monitoring and remediation tools. To get them, you need to submit your firewall logfiles to be parsed by our log parsers. There are three reports:



Analysis and Remediation

This report provides deeper research into blocked IP addresses from ThreatSTOP and other sources such as DShield and SANS. By exporting the data to a csv file, users can find the infected machines and take remedial action.

Export to CSV (max 2500 records)

Source IP	Destination IP	Destination Port	Number of Attacks
Research	212.7.196.67	80 / http	10743
Research	212.7.196.76	80 / http	10444
Domains	212.117.184.169	53 / domain	5035
McAfee	212.117.184.149	53 / domain	5014
Dshield	194.236.96.8	53 / domain	4924
Recursive Whois	212.95.63.29	53 / domain	4816
SANS Drilldown	212.95.63.30	53 / domain	4812
Project Honeypot	212.117.184.149	53 / domain	4798

Forensics Drill Down

For each IP address, a “rap sheet” is available for forensics analysis and action. Data includes: dates first and last seen, reporting sources, Google DNS and Whois information.

Research IP 193.232.130.14

First Identified	Most Recently active	Present in the following feeds:	Present in the following blockers:
0.14	2010-12-06 10:00:09	Russian Business Network	ADVANCED
0.14	2011-06-06 19:50:49	Geographic IP Russia	RUSSIA
			RUSSIA
			Eastern Europe
			Modified ITAR

Google DNS

```

3.6-P1-RedHat-9.3.6-16.P1.e15 <<> @8.8.4.4 -x 193.232.130.14
(amd)
Ions: printcmd
:
<- opcode: QUERY, status: NOERROR, id: 11947
rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
    
```

Easy to Deploy on Major Firewalls

- <1 hour to install simple script
- A few rules on each firewall
- Set custom white/black lists
- No more manual updates
- Major firewalls supported (Cisco ASA, Juniper SRX, Checkpoint, Vyatta, IP Tables-based)

Turnkey Cloud Service

- 30 public, private and proprietary sources
- Heuristics engine produces predictive blacklist
- Updated in real-time
- Distribution of list automatically via DNS to firewalls (patent-pending)
- Customer logfiles become part of ThreatSTOP intelligence network

Start your 30-day FREE TRIAL and get protected immediately!

www.threatstop.com

sales@threatstop.com

US: 760-542-1550

EU: +44-1223-970-150