
Threat

STOP™

Internet.Security.Community

Tom Byrnes

Founder & CEO

760.402.3999

tomb@threatstop.com

"In God we trust, all others bring data."

W. Edwards Deming

Manual Processes

ENFORCEMENT TOOLS

Host System Security



Auditing



Router Security



Firewalls



Intrusion Detection System



Incident Response System



Threat **STOP**TM
Adaptive Real-Time Security

ThreatSTOP Automates Process Like Anti-Virus Auto-Update, but in Real-Time

GOOD GUYS WITH THREAT INFO

Internet Storm Center - DShield

Shadowserver

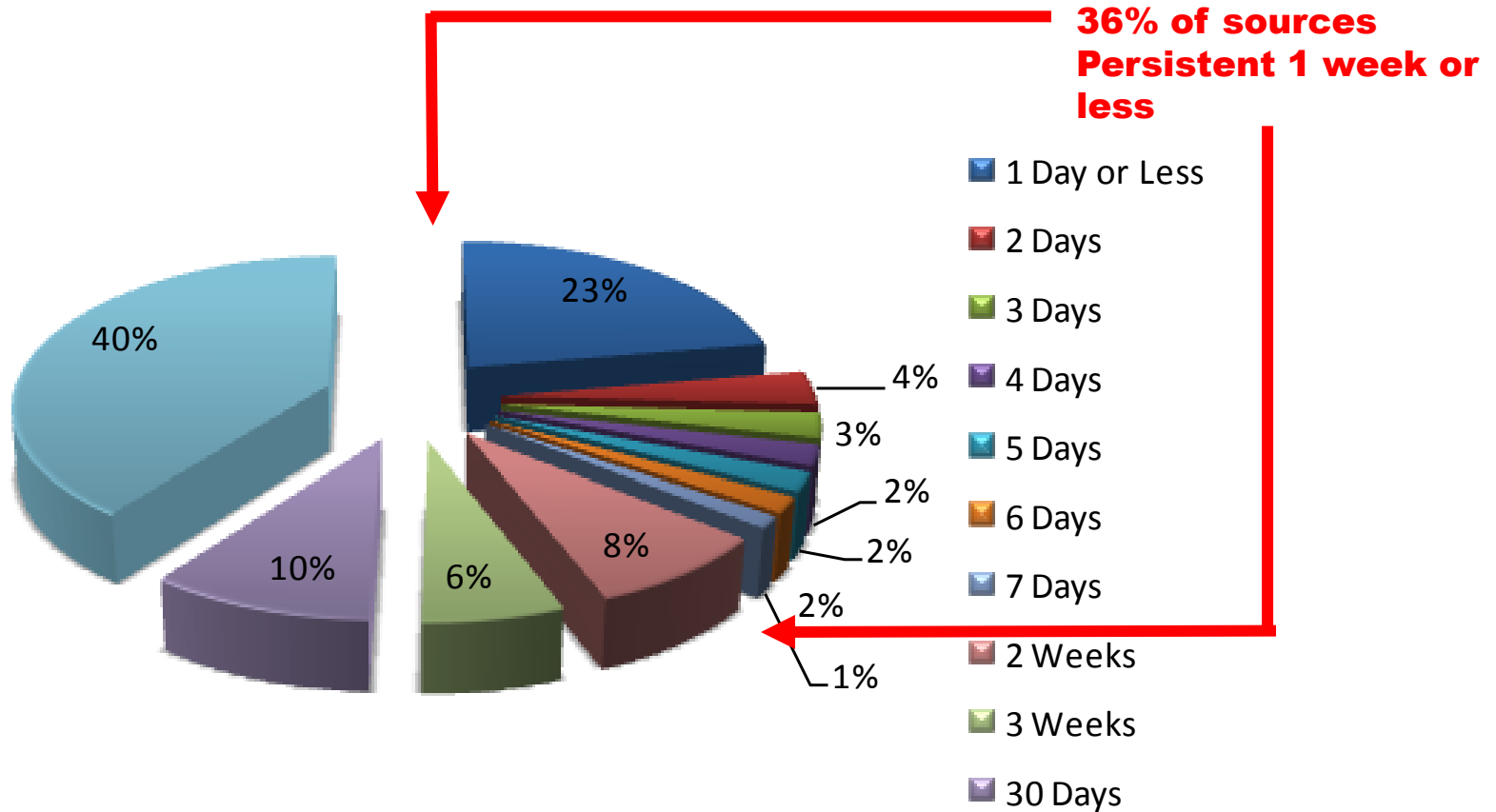
SRI MTC

Cymru Bogons

PhishTank

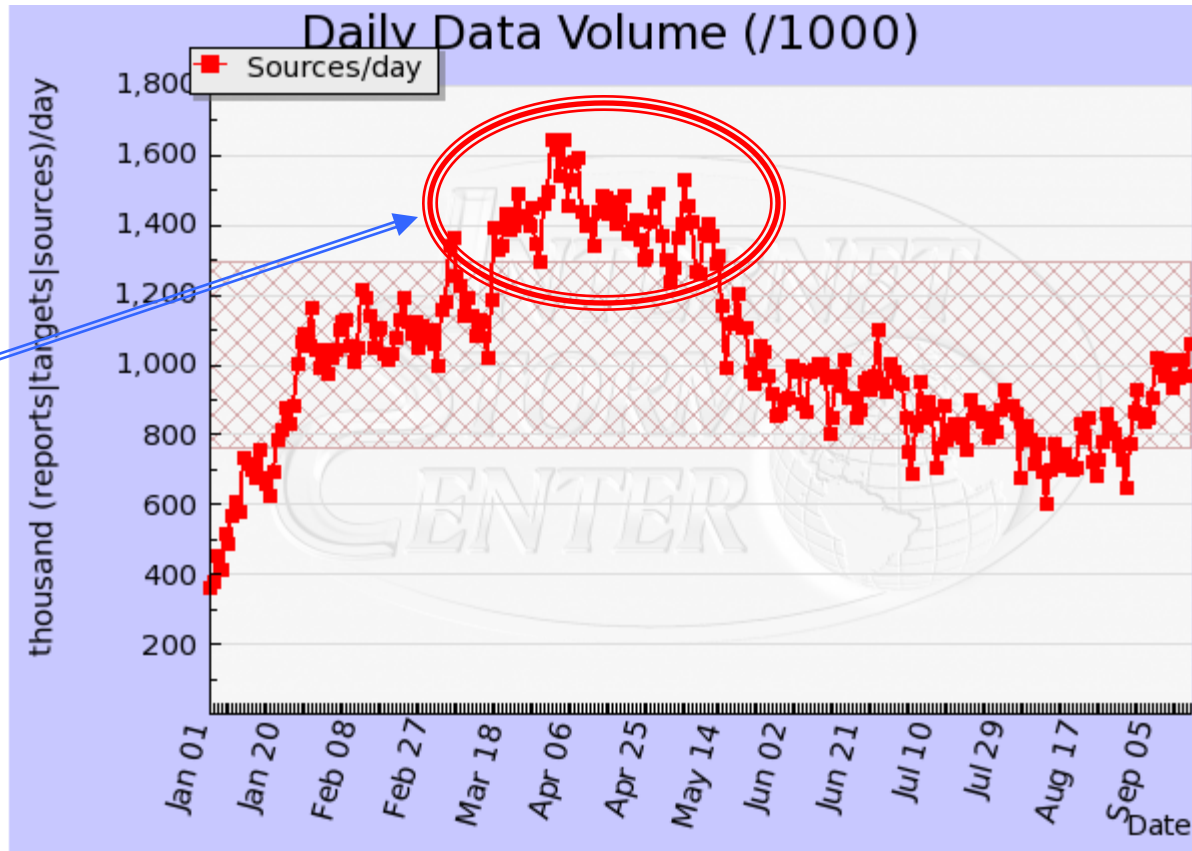
DROP Advisory Null List

Threats Change Rapidly



Source: SANS - Internet Storm Center, DShield top 10,000 sources, 9/17/2009

2009 Attack Events



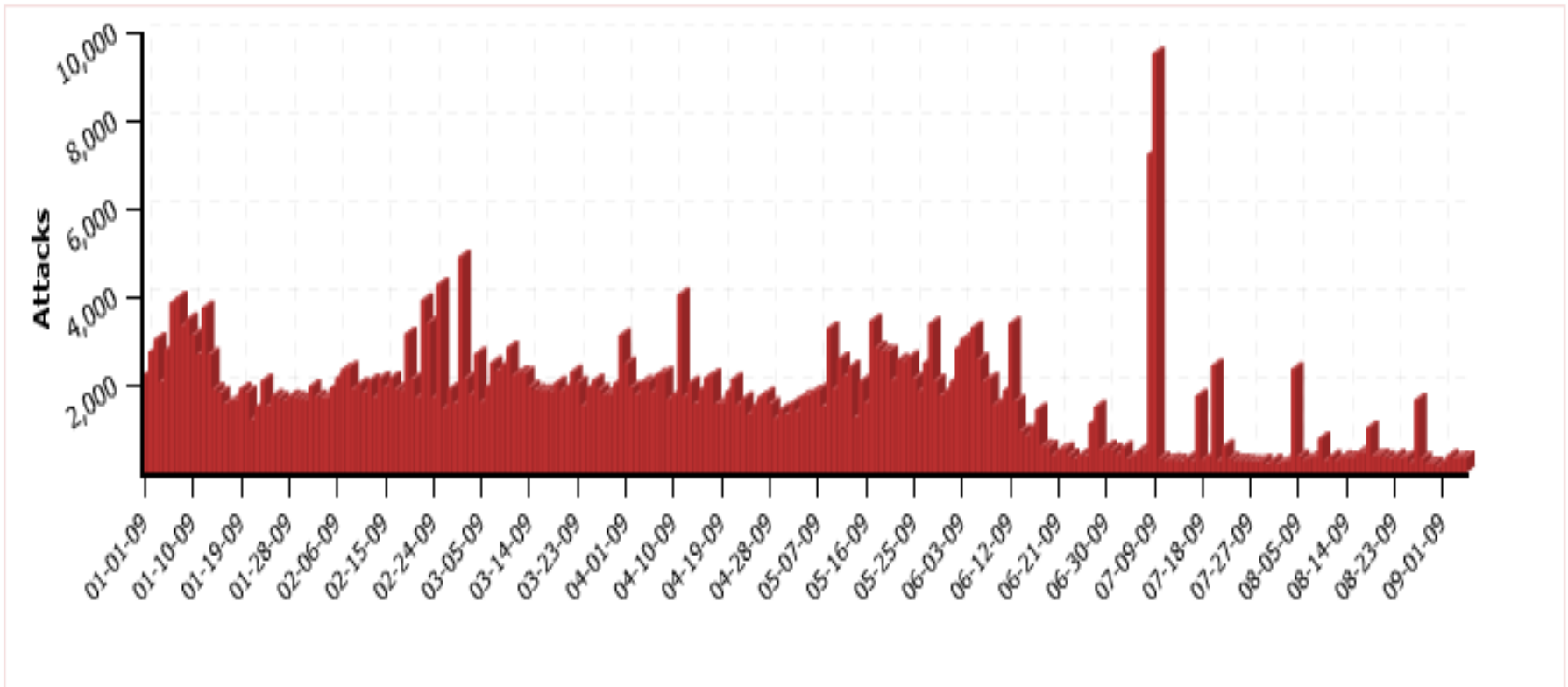
Internet storm center Jan-Sep 2009

Trends this year

Number of attacks : 413057

Number of attackers : 9747









Attack Frequency : 1666 per day



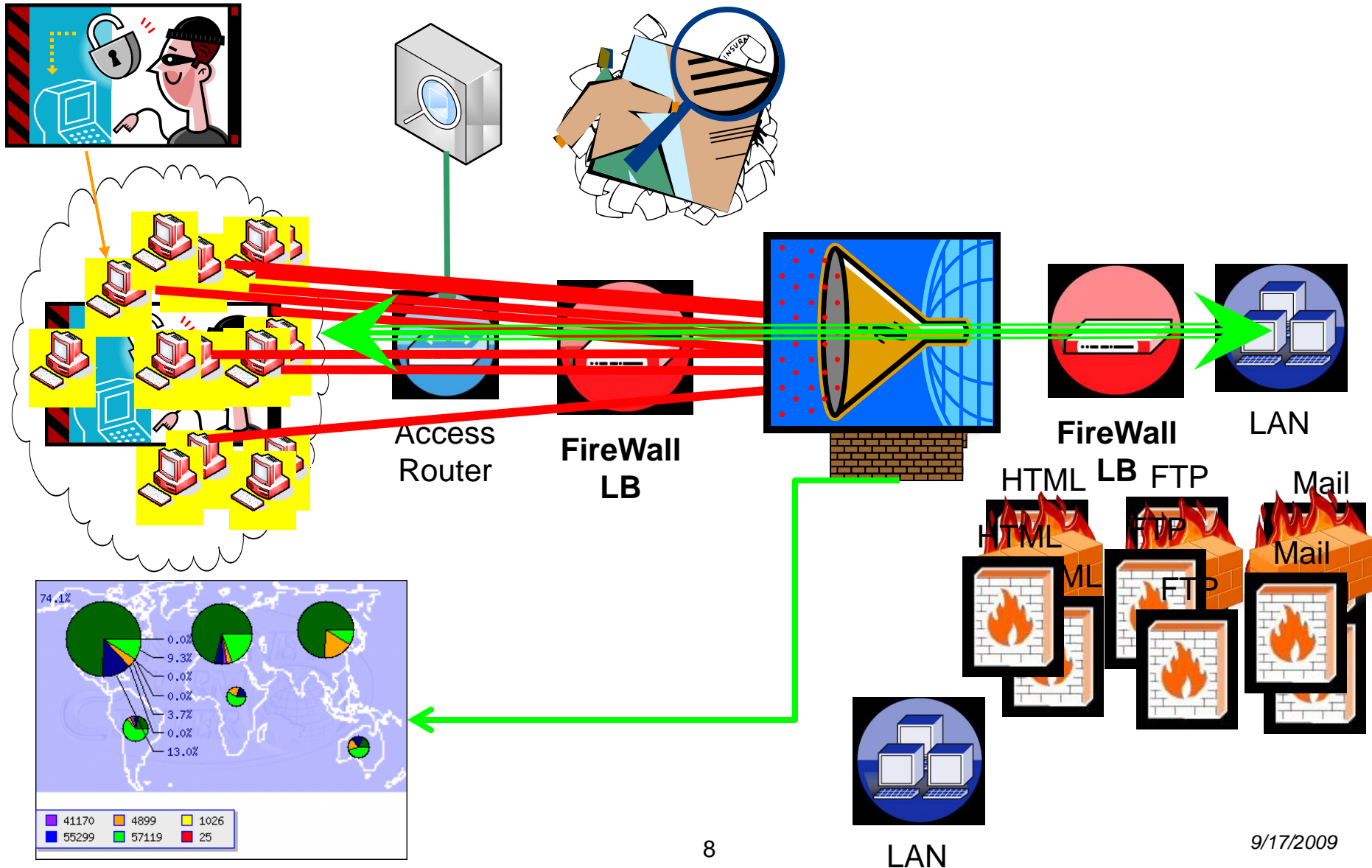
Most Aggressive Malware Attack Source and Filters

Fri Sep 18 08:35:58 2009

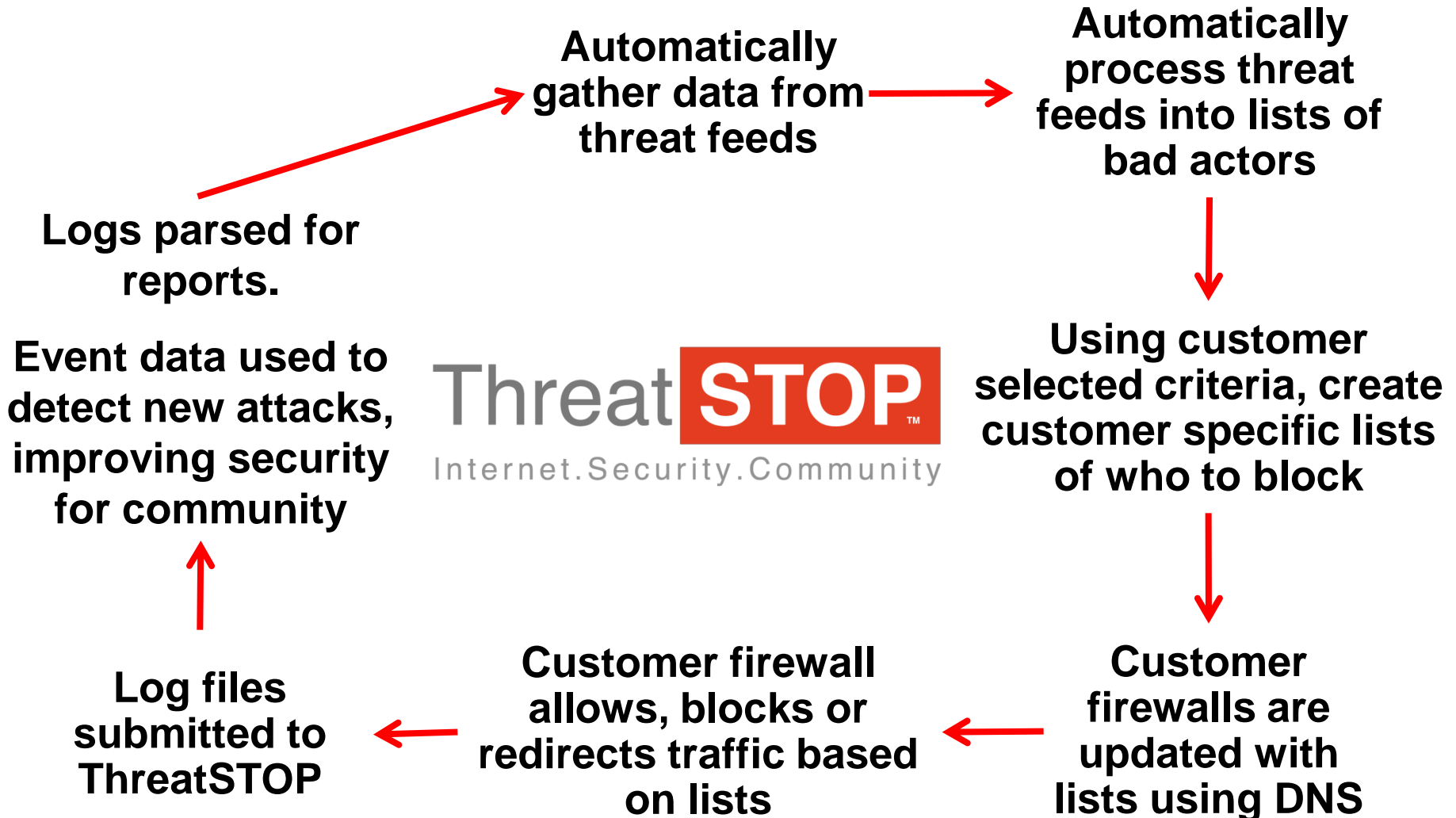
rank = 30-day importance ranking (1 to 100) of most aggressive infection sources

rank	hits	first	last	domain	country	filter
53	5	08/23	09/12	cox.net		deny ip host 24.234.68.126 any log
53	5	08/19	09/16	verizon.net		deny ip host 72.66.8.36 any log
52	4	09/04	09/16	metrocast.net		deny ip host 74.214.47.11 any log
50	4	09/01	09/14	-		deny ip host 118.87.20.81 any log
35	3	09/03	09/14	rr.com		deny ip host 67.10.91.238 any log
33	3	09/03	09/15	-		deny ip host 96.50.173.224 any log
32	3	09/03	09/14	-		deny ip host 72.21.131.167 any log
32	2	09/15	09/15	net.kpnqwest.pt		deny ip host 193.126.203.208 any log
31	2	09/14	09/17	panevo.ro		deny ip host 86.105.216.12 any log
31	2	09/14	09/16	pldt.net		deny ip host 58.71.45.90 any log

Escalating Net-Warfare

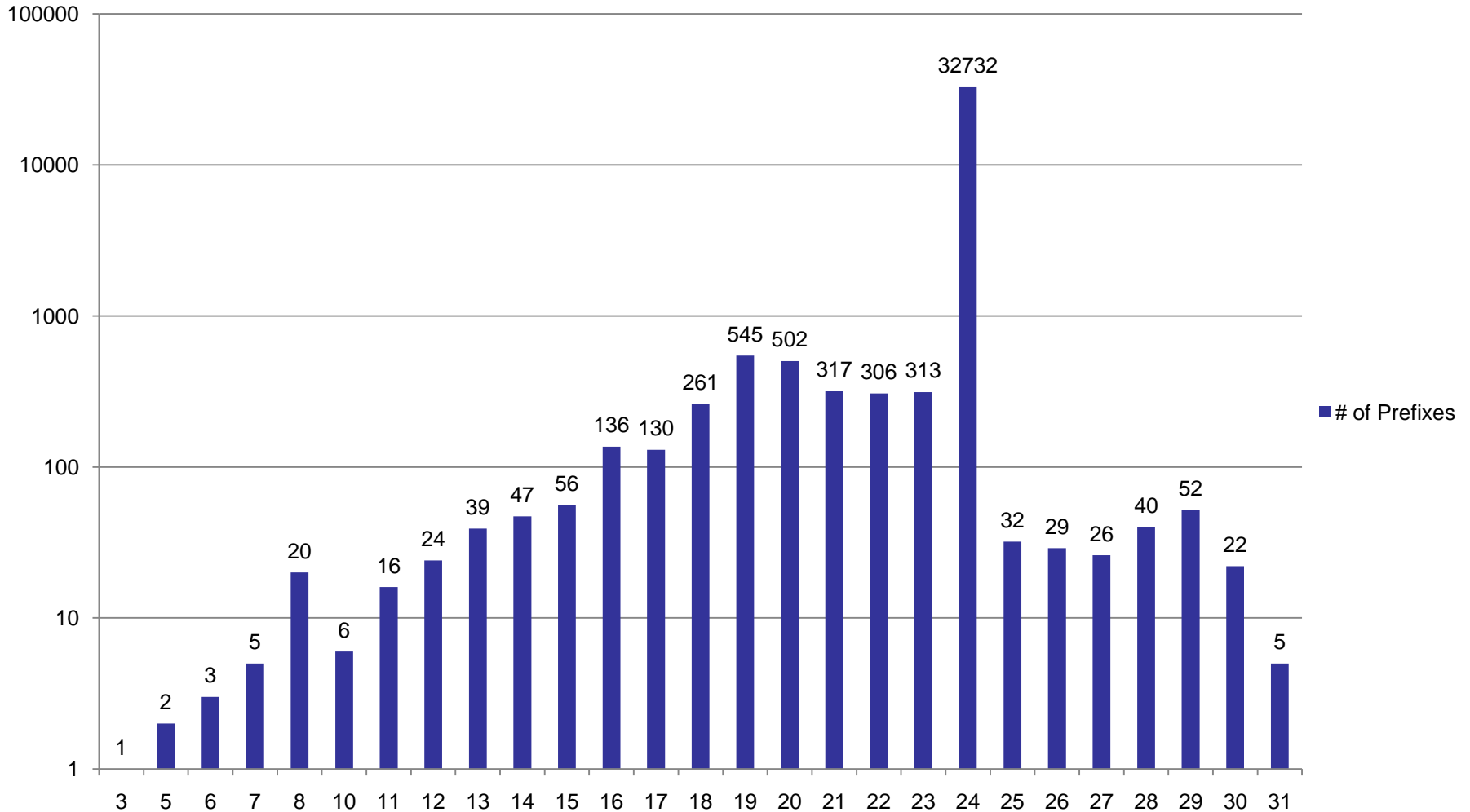


Community ↑ Security



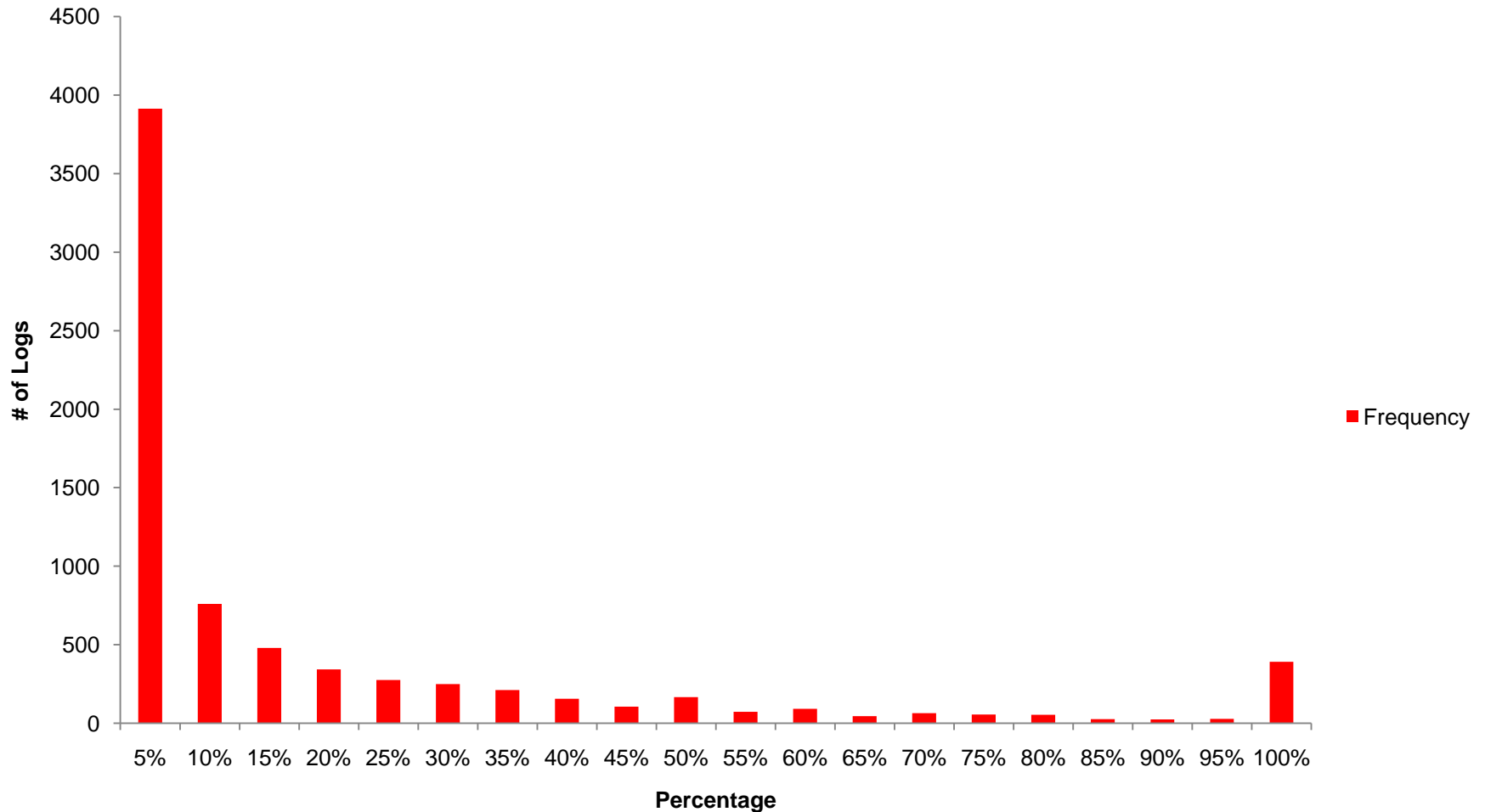
Distribution of “Bad” Nets

of Prefixes



Distribution of log entry Sources in IP Rep DB

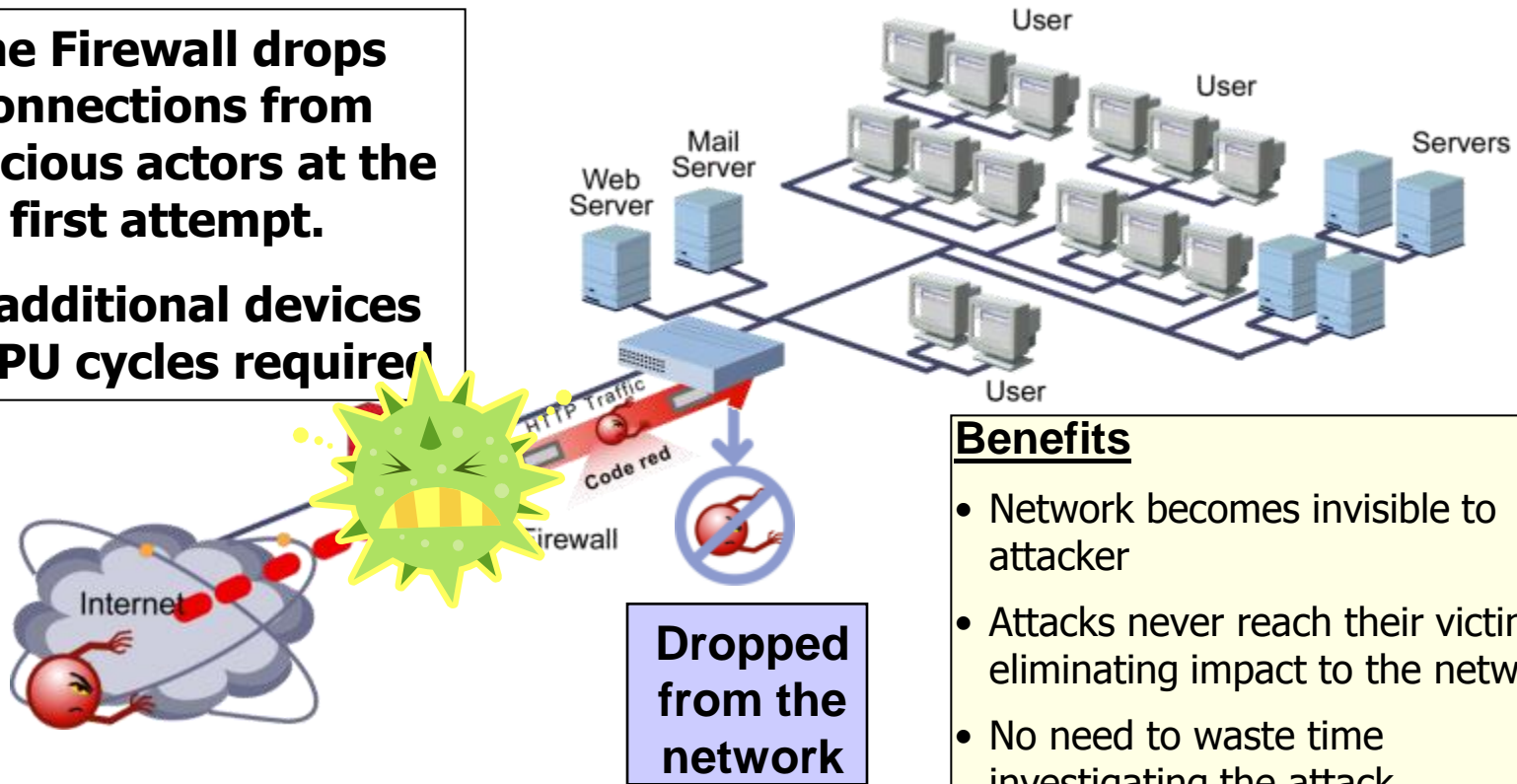
% Connections in Database



Drop At first SYN

The Firewall drops connections from malicious actors at the first attempt.

No additional devices or CPU cycles required

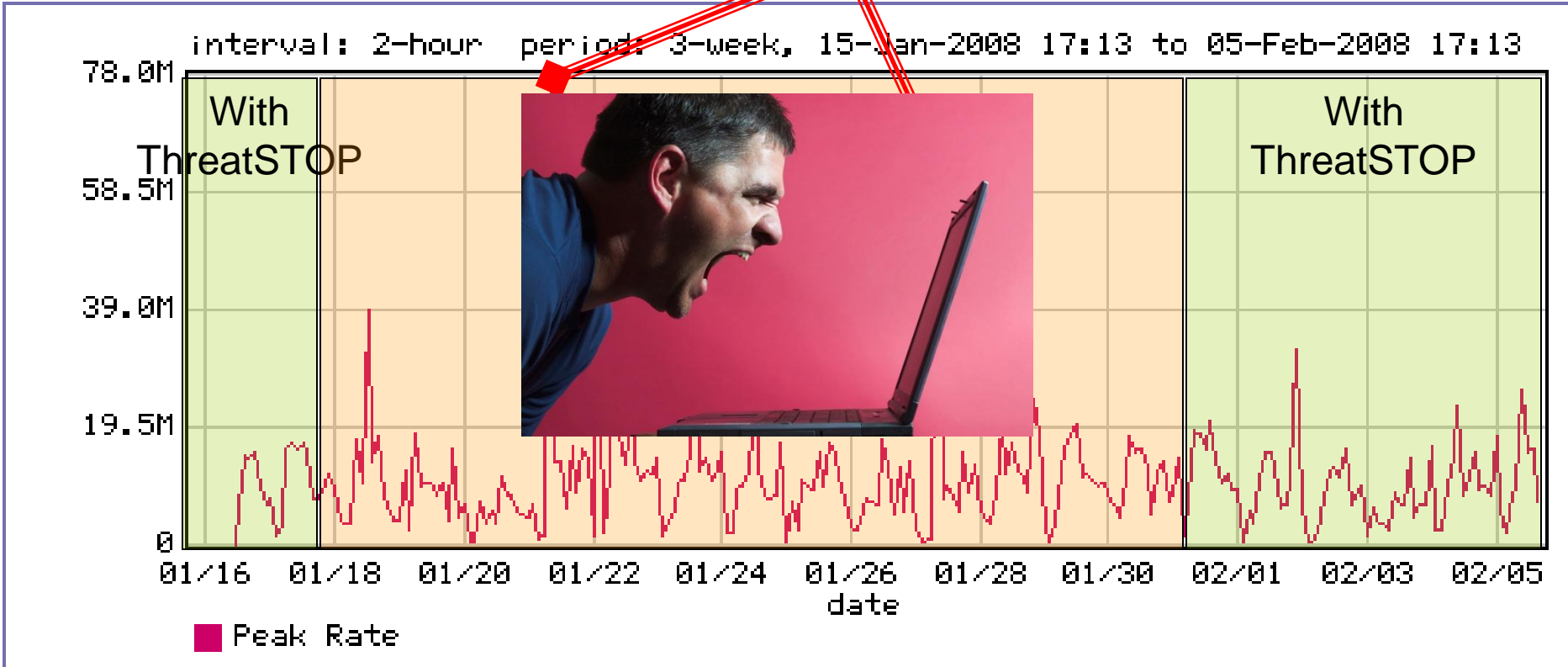


Benefits



- Network becomes invisible to attacker
- Attacks never reach their victim, eliminating impact to the network
- No need to waste time investigating the attack
- Works for all traffic (IP, TCP, UDP, etc.)
- Drops only traffic from known bad actors

SMTP Traffic Test

Bandwidth saturated by SMTP



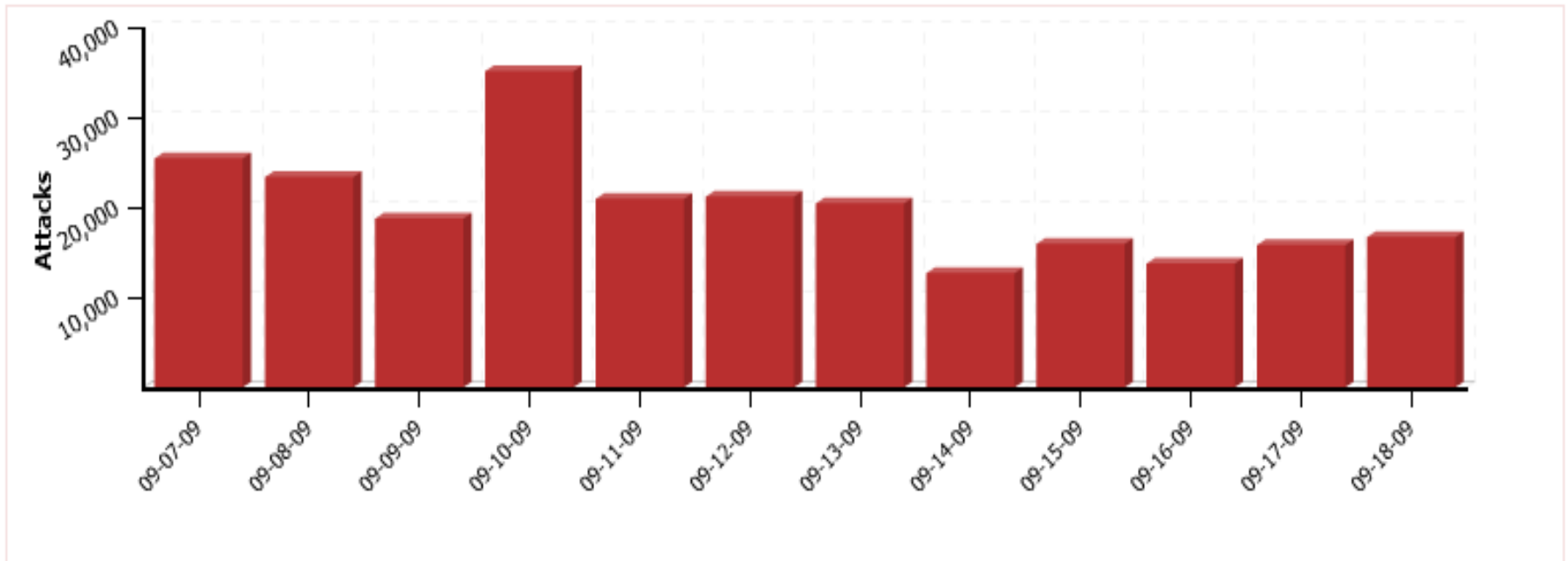
A Day in the Life

From:  To: 

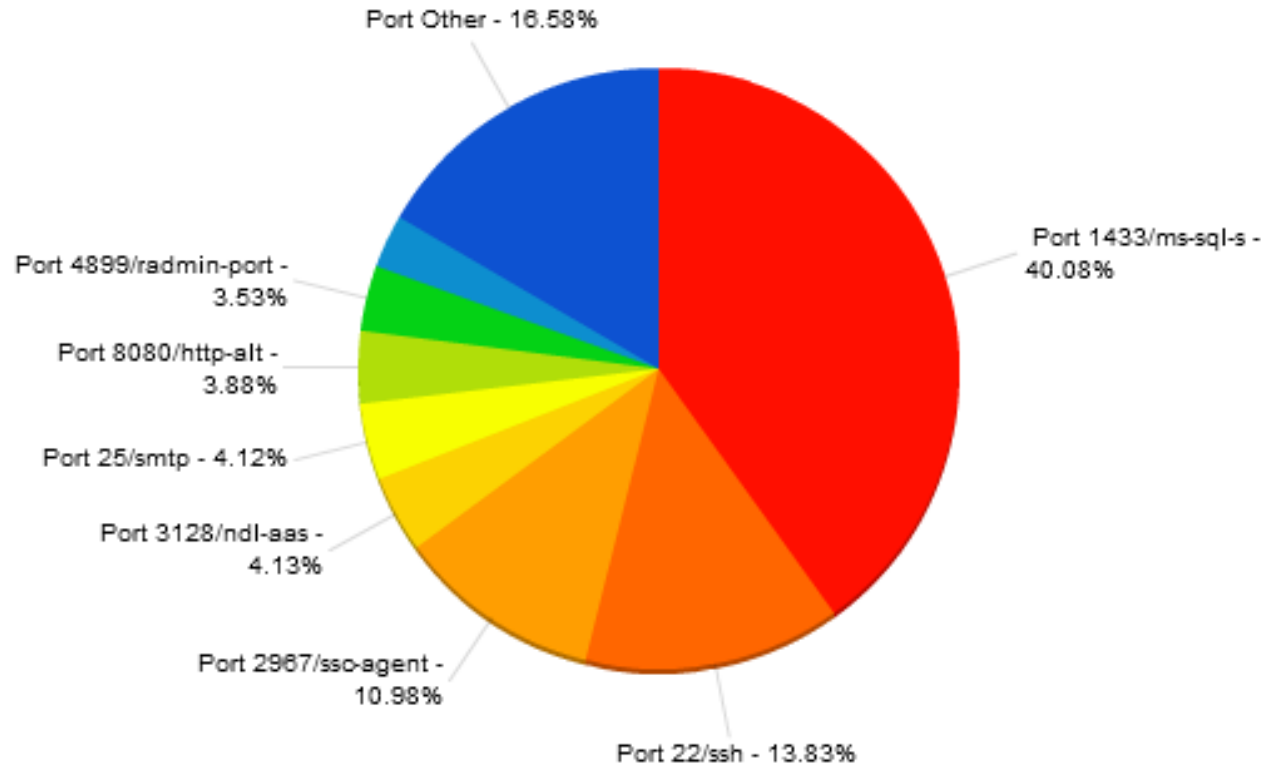
Devices: Report:

Number of attacks : 240248
Number of attackers : 443

Attack Frequency : 20021 per day
Last log file processed on:
09/19/2009



What's being attacked



Who is doing it

Source IP	Destination IP	Destination Port	Number of Attacks
61.191.190.71	203.25.171.38	1433 / ms-sql-s	878
125.89.77.214	203.25.171.38	1433 / ms-sql-s	828
60.190.216.150	203.25.171.38	1433 / ms-sql-s	322
222.35.78.251	203.25.171.38	1433 / ms-sql-s	253
221.8.126.131	203.25.171.38	1433 / ms-sql-s	89
202.98.234.103	203.25.171.38	1433 / ms-sql-s	72
210.32.205.40	202.177.223.252	2967 / ssc-agent	55
210.32.205.40	202.177.223.254	2967 / ssc-agent	55
125.89.77.214	203.14.211.0	1433 / ms-sql-s	48
125.89.77.214	203.14.211.2	1433 / ms-sql-s	48
125.89.77.214	203.14.211.3	1433 / ms-sql-s	48
125.89.77.214	203.14.211.4	1433 / ms-sql-s	48
125.89.77.214	203.14.211.5	1433 / ms-sql-s	48
125.89.77.214	203.14.211.7	1433 / ms-sql-s	48
125.89.77.214	203.14.211.8	1433 / ms-sql-s	48
125.89.77.214	203.14.211.9	1433 / ms-sql-s	48
125.89.77.214	203.14.211.10	1433 / ms-sql-s	48
125.89.77.214	203.14.211.11	1433 / ms-sql-s	48
125.89.77.214	203.14.211.12	1433 / ms-sql-s	48
125.89.77.214	203.14.211.13	1433 / ms-sql-s	48
125.89.77.214	203.14.211.14	1433 / ms-sql-s	48
125.89.77.214	203.14.211.15	1433 / ms-sql-s	48
125.89.77.214	203.14.211.16	1433 / ms-sql-s	48
125.89.77.214	203.14.211.17	1433 / ms-sql-s	48
125.89.77.214	203.14.211.18	1433 / ms-sql-s	48
125.89.77.214	203.14.211.19	1433 / ms-sql-s	48
125.89.77.214	203.14.211.20	1433 / ms-sql-s	48
125.89.77.214	203.14.211.21	1433 / ms-sql-s	48
125.89.77.214	203.14.211.22	1433 / ms-sql-s	48
125.89.77.214	203.14.211.23	1433 / ms-sql-s	48
125.89.77.214	203.14.211.24	1433 / ms-sql-s	48
125.89.77.214	203.14.211.25	1433 / ms-sql-s	48
125.89.77.214	203.14.211.26	1433 / ms-sql-s	48
125.89.77.214	203.14.211.27	1433 / ms-sql-s	48
125.89.77.214	203.14.211.28	1433 / ms-sql-s	48
125.89.77.214	203.14.211.29	1433 / ms-sql-s	48
125.89.77.214	203.14.211.30	1433 / ms-sql-s	48
125.89.77.214	203.14.211.33	1433 / ms-sql-s	48
125.89.77.214	203.14.211.34	1433 / ms-sql-s	48
125.89.77.214	203.14.211.35	1433 / ms-sql-s	48
125.89.77.214	203.14.211.36	1433 / ms-sql-s	48
125.89.77.214	203.14.211.37	1433 / ms-sql-s	48
125.89.77.214	203.14.211.38	1433 / ms-sql-s	48
125.89.77.214	203.14.211.39	1433 / ms-sql-s	48
125.89.77.214	203.14.211.40	1433 / ms-sql-s	48
125.89.77.214	203.14.211.41	1433 / ms-sql-s	48
125.89.77.214	203.14.211.42	1433 / ms-sql-s	48
125.89.77.214	203.14.211.43	1433 / ms-sql-s	48
125.89.77.214	203.14.211.44	1433 / ms-sql-s	48
125.89.77.214	203.14.211.45	1433 / ms-sql-s	48

1 | 2 | 3 | 4 | 5 > [1710]

Who Are We?

- **Tom Byrnes - Founder & CEO**
- Security experience spans 25+ years of civilian & military
 - Radware, iPivot, Zero Gravity, ADN, Datatech, U.S. Army
- **VP Engineering – Boris Veksler (Betria Consulting)**
 - 15+ years experience in project management & engineering
 - Tradebeam, Struxicon, Johnson Controls, Neiman Marcus, Tyco
 - MBA from Anderson School at UCLA; MS in Structural Analysis & Mathematics/Computer Science from St. Petersburg Technical Univ.
- **VP Customer Experience (QA & Operations) – David Daugherty**
 - Operations in e-commerce platforms: Virtual Dreams, ArtistDirect
 - Test and QA: iPivot, Intel and ADN
- **Paul Mockapetris – Advisor & Member BOD**
 - Inventor of the Domain Name System (DNS)
 - Currently the Chief Scientist and Chairman of Nominum, Inc.
- **Marcus H. Sachs, P.E. – Advisor**
 - Verizon Exec. Dir. of Gov. Affairs for National Security Policy
 - First head of Cybersecurity @ DHS
 - Director of the SANS Internet Storm Center
- **Johannes Ullrich - Advisor**
 - Chief Research Officer for the SANS Institute
 - Founded DShield.org

What's Been Done

- Feed parsing and IP reputation database
- Threat Feed aggregation and datamart
- Log parsing
- Log correlation with Threat Feeds
- Log Reporting
- Log Forensics

What remains to be done

- More Blocking
 - HPBLs (SRI/ISC predictive block lists per node)
 - More Data feeds.
 - Additional types of data feeds:
 - Web Honeynet (Dshield).
 - IDS: OISF/Sidreporter
- Data warehousing and sharing
- More real-world experimentation
 - Run two firewalls side by side on same traffic stream and compare.
 - This your brain on ThreatSTOP, this is your brain Off ThreatSTOP.
- Additional device type support

Subscribe/Contact

- www.threatstop.com
- info@threatstop.com
- +1-858-412-7334
- Tom Byrnes: tomb@threatstop.com