

Using Behavior Analysis to Block Threats

Postini provides proven, patented threat identification data

WHAT IS PTIN?

The Postini Threat Identification Network™ (PTIN) is a comprehensive, real-time information service that identifies malicious computers that have recently launched email attacks such as viruses, phishing, spam, and directory harvests. PTIN has been designed to be embedded in network equipment to provide network layer security, accessed by ISPs that want to stop spammers from hijacking their networks, and accessed by email accreditors and certification agencies that want clear, objective data about their clients.

Subscribers use PTIN data to make better decisions about which computers to accept messages from, and which to block, when, and for how long. The result is fewer viruses, less spam, and greatly reduced bandwidth consumption. PTIN has numerous advantages over other technologies that are supposed to block bad computers, like “sender reputation” systems and real-time blackhole lists (RBLs).

Based on Actual Behavior

PTIN data is updated several times per minute by Postini’s proprietary Traffic Monitor process, so PTIN’s repository of malicious computers, identified and tracked by their IP addresses, is always up to date. At any given time, PTIN contains threat information for approximately 40,000 suspicious computers. Computers listed in PTIN have been observed sending unwanted

email in the past few hours. PTIN data is based on the 500 million SMTP connections that Postini processes every day for its 30,000 managed service customers. Unlike reputation systems, senders cannot self-certify their “good” reputation, thus bypassing defenses.

Completely Objective

PTIN is based on a completely objective evaluation of the behavior of sending computers, tracking and evaluating more than 20 aspects of every SMTP connection processed by Postini. This means that PTIN has none of the manual submission and subjective human review that plagues RBLs.

Truly Real-Time

PTIN is a real-time process, with data updated by Postini every few seconds. In comparison, unlike RBLs whose manual submission process can take hours or days to block an offending computer, and weeks or months to unblock. In a world where most unwanted email comes from “spam zombies” (PCs that have been compromised by viruses), this kind of latency is unacceptable. A PC can go from well-behaved, to malicious, and back to well-behaved again in a matter of minutes, so any system designed to track offending computers must be similarly dynamic in its data collection and updating. The average half-life of an IP address in PTIN is just 2.5 hours, incredibly responsive compared with reputation and RBL systems. This response allows for immediate action

against senders as attacks occur, rather than after the fact. This ability to identify and eliminate threats at the connection level is crucial as a first line of defense.

Flexible

PTIN’s database contains detailed offense scores, rather than the simplistic deny/allow entries found in RBLs. This feature allows customers to set their own thresholds for handling offending computers. Granular scoring lets customers choose different actions — drop, block, redirect, throttle, blackhole, quarantine or deliver—based on their preferences.

THREE WAYS TO USE PTIN

PTIN Access

PTIN Access is designed to be embedded in network devices like routers and mail transfer agents, or in security software and appliances. PTIN Access can be integrated by the original equipment manufacturer, or by the customer. The source IP address of inbound traffic can be immediately checked against PTIN to determine if the packets should be routed or dropped. PTIN data can be accessed three ways:

- **BGP:** PTIN data can be distributed to network devices over BGP (border gateway protocol), and offending source IPs routed to null routes.

- **DNS:** Network devices can make real-time queries of PTIN using DNS (Domain Name System) calls.
- **Text files:** PTIN data can be periodically downloaded as flat file lists of IP addresses and scores.

PTIN Monitor

PTIN Monitor is aimed at ISPs that want to know if they have offending computers on their networks sending junk email. ISPs periodically receive updates from Postini regarding offending IP addresses that belong to the ISP. This allows ISPs to actively identify problems such as spammers on their networks, or subscriber PCs that have been converted into spam zombies by viruses.

- **DNS:** Network devices can make real-time queries of PTIN using DNS calls.
- **Text files:** PTIN data can be periodically downloaded as flat file lists of IP addresses and scores.

PTIN Query

PTIN Query is designed for email accreditors and certification agencies that want to verify the legitimacy of their clients, by establishing that the client has never been listed in PTIN as having offending computers. Client IP addresses

are entered into a web interface for immediate feedback on their prior history.

LEARN MORE ABOUT PTIN

To find out more about PTIN services, contact Postini Business Development at 1-650-486-8249, or email ptin@postini.com. You can also learn more about PTIN online at www.postini.com/postini_ptin.



ABOUT POSTINI

As the leader in Integrated Message Management, Postini managed services protect businesses from a wide range of IM and email threats, provide message archiving and encryption, and enable the management and enforcement of enterprise policies to meet regulatory compliance requirements.

Corporate Headquarters

San Carlos, CA USA
Toll-free: 1-866-767-8461
Email: info@postini.com
www.postini.com

EMEA Headquarters

London, UK
Tel: +44 (0)20 7082 2000
Email: info_emea@postini.com

Asia Pacific Headquarters

Tokyo, Japan
Tel: +81 80 3089 7470
Email: info_apac@postini.com