

Copyright 2005-2006, Trend Micro, Inc.

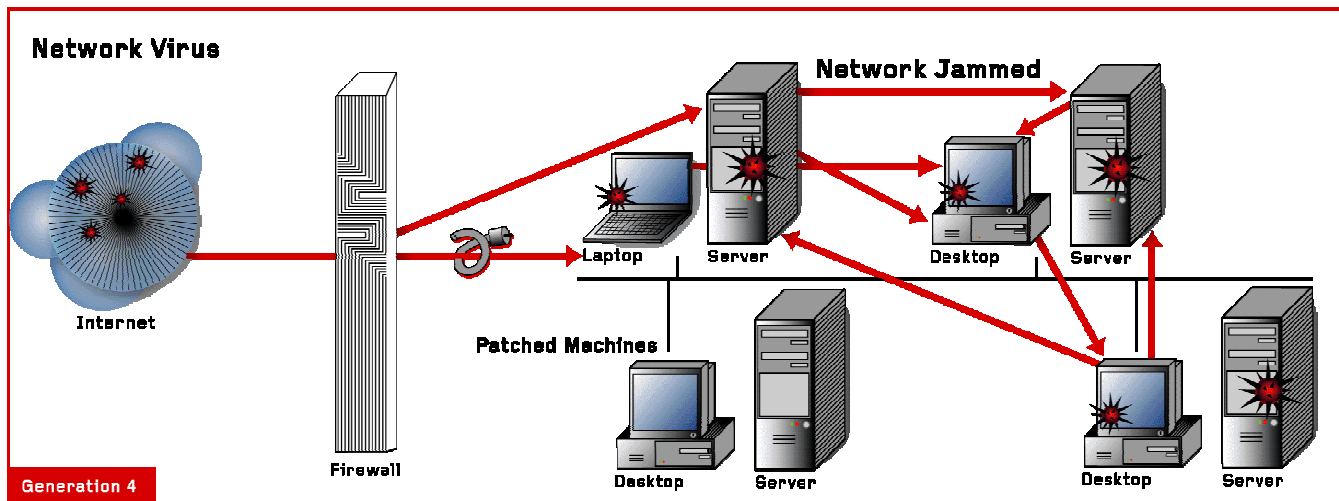
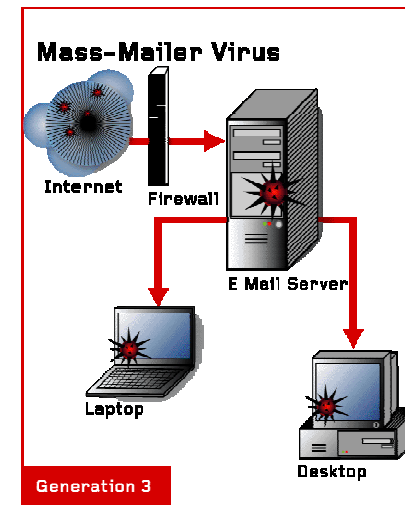
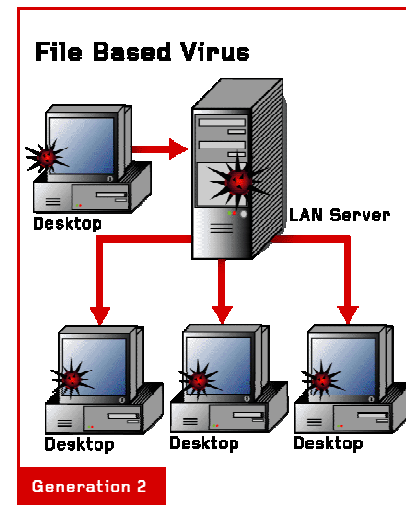
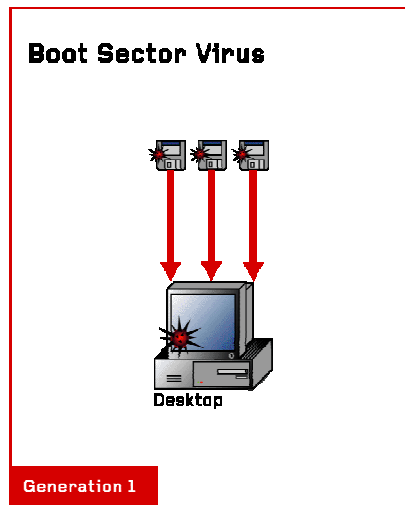
Strategie di prevenzione e difesa delle reti aziendali dalle “nuove” minacce

Patrick Gada
Senior Sales Engineer

18 ottobre 2005



Evoluzione dei Virus



Examples:

Worm_Sasser

Nachi

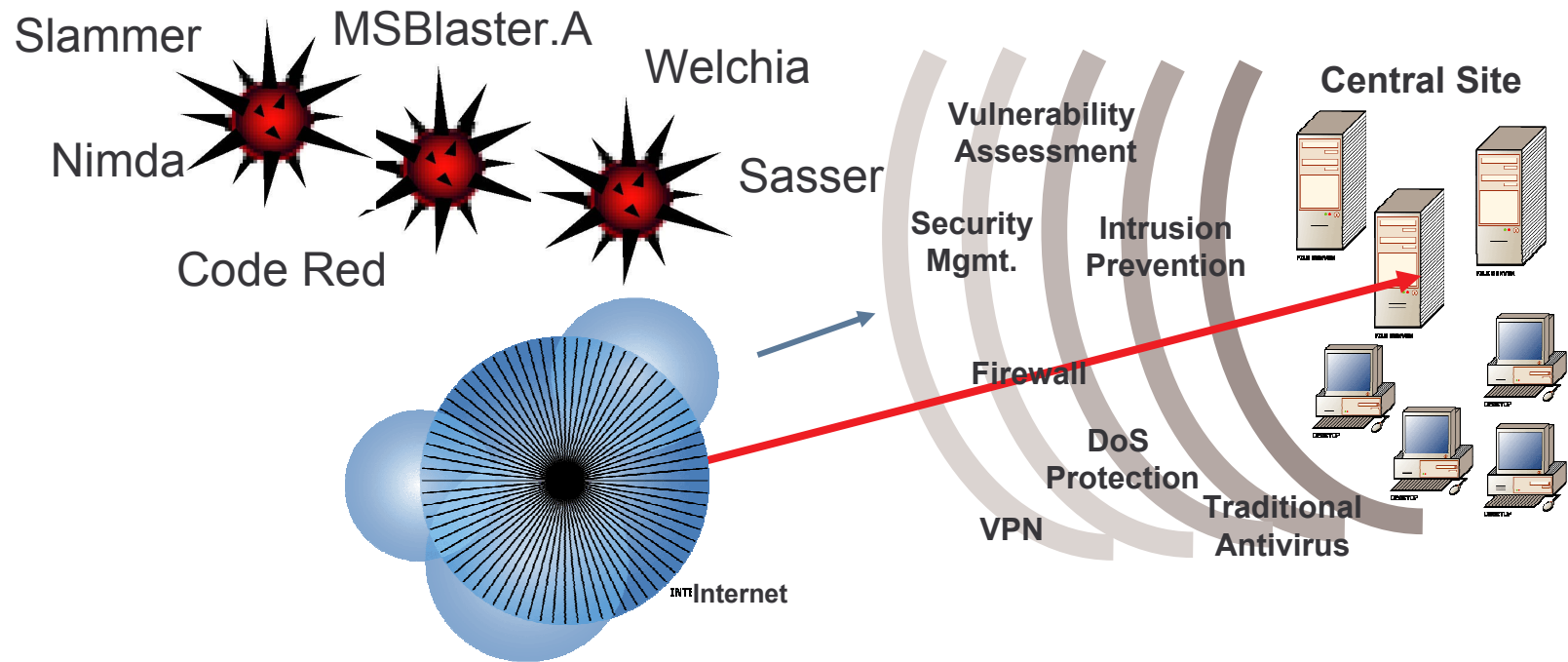
MSBlaster.A

Slammer

Code Red

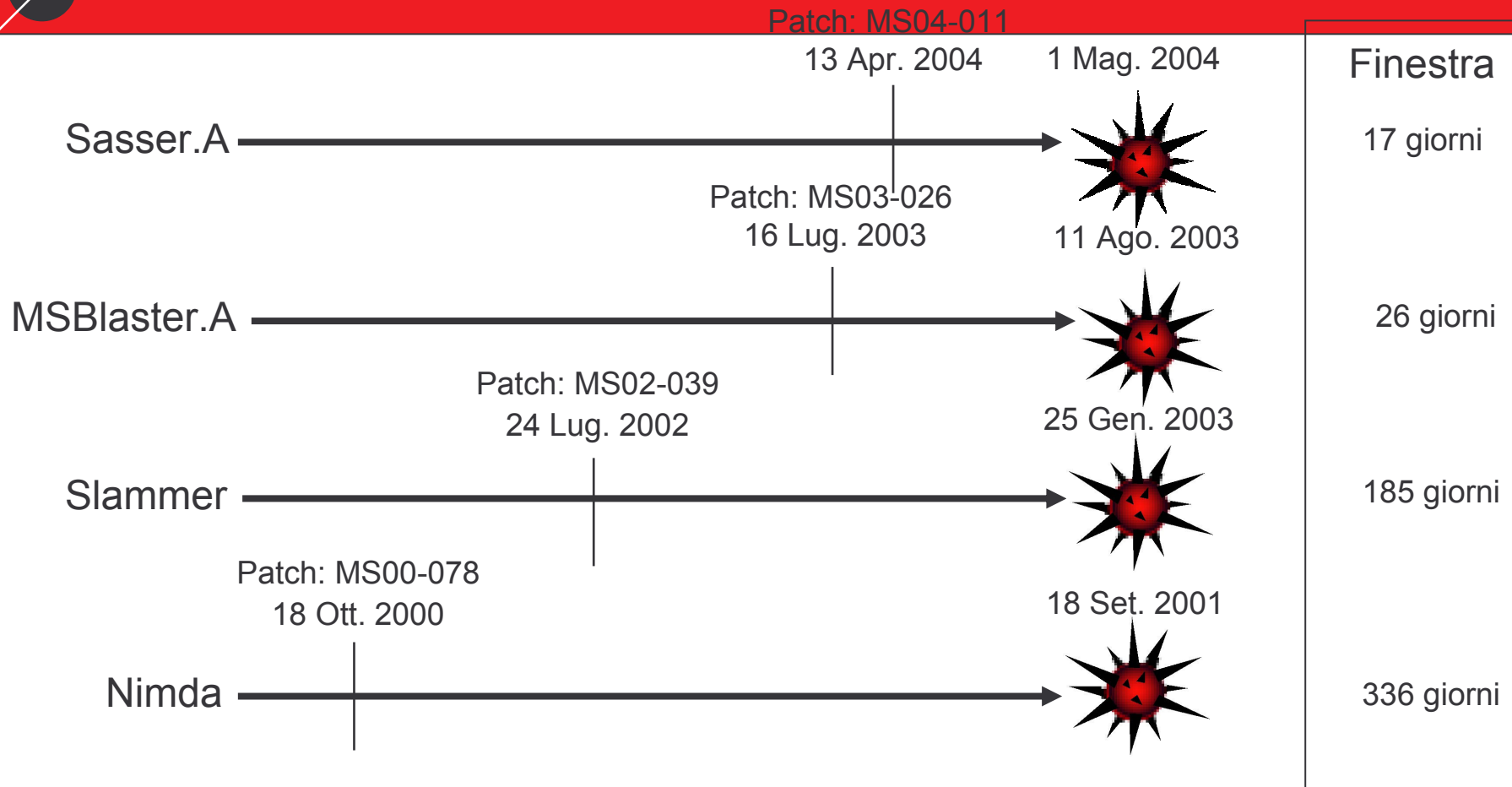
Nimda

Non è stato possibile bloccare i Network Viruses (Worms)



Nessuna soluzione ha bloccato o limitato la propagazione di questi virus
Molto spesso si è intervenuti in ritardo = \$2.15B di danni nel solo 2003

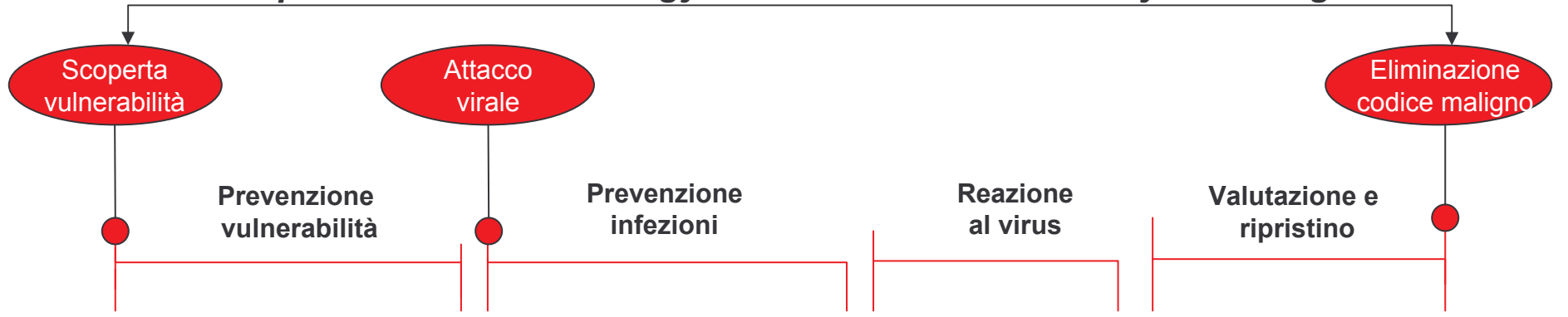
Sempre meno tempo per applicare le patch



La finestra temporale dalla disponibilità della patch all'infezione si sta riducendo
E' difficile dare priorità nell'applicazione delle patch ed isolare le macchine vulnerabili durante un infezione.

Enterprise Protection Strategy III

Enterprise Protection Strategy: Proactive Outbreak Lifecycle Management



Trend Micro™ Network VirusWall™



Trend Micro™ Network VirusWall™ è un dispositivo di prevenzione delle infezioni virali che, consente alle organizzazioni di neutralizzare i virus di rete (gli Internet Worm), bloccare le vulnerabilità ad alto rischio nel corso delle infezioni, mettere in quarantena e disinfettare le origini delle infezioni, compresi i dispositivi non protetti, nel momento stesso in cui accedono alla rete, grazie alle conoscenze specifiche distribuite da Trend Micro per ogni minaccia.

A differenza delle soluzioni di protezione che si limitano a monitorare le minacce e fornire informazioni.

Trend Micro™ Network VirusWall™



1. Vulnerability Assessment

**Vulnerability
Assessment**



3. Isolation & Remote Clean up



2. Network Worm Prevention –
No False Positives

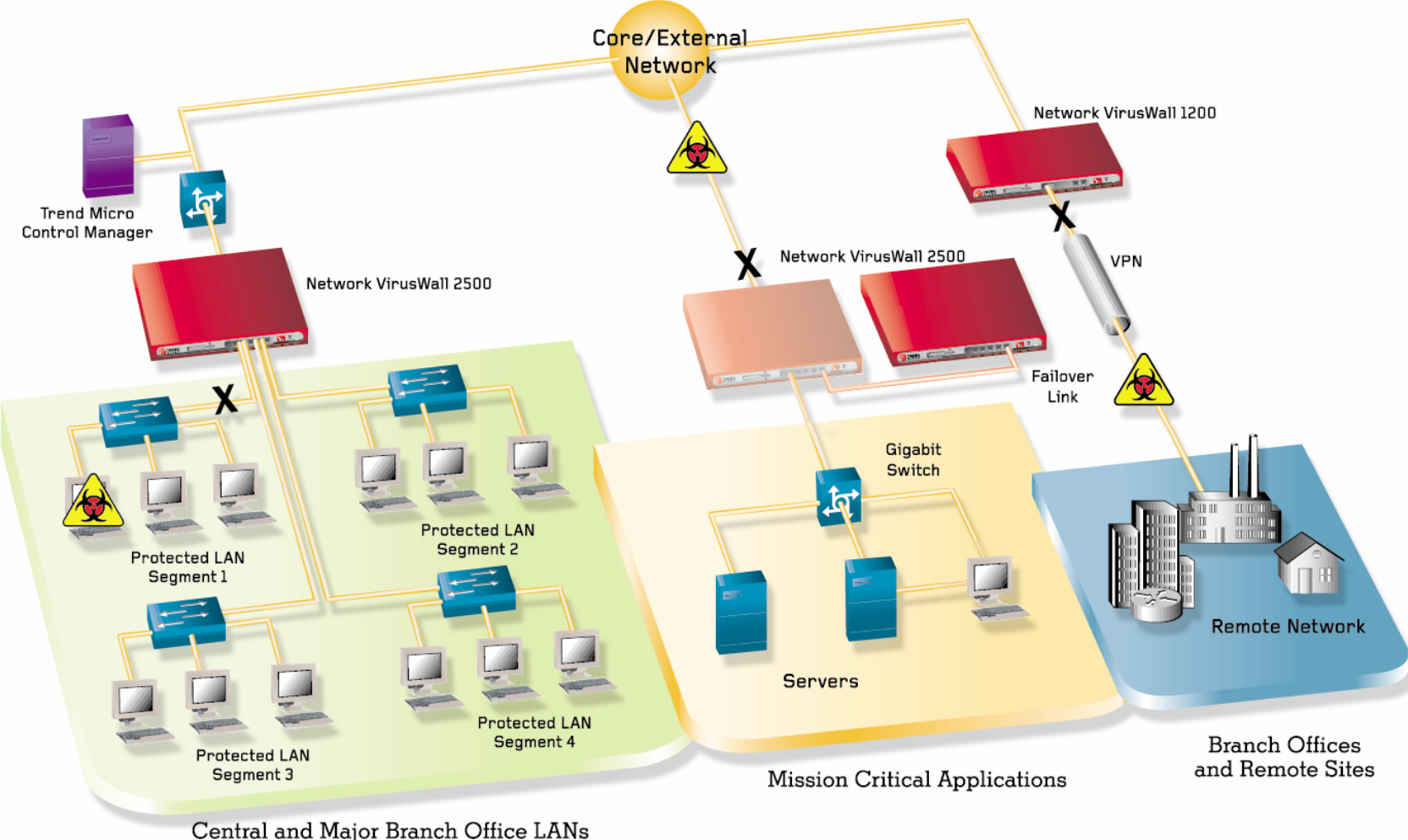


4. Security Policy Enforcement –
Agent-less



Trend Micro Control Manager

Come prevenire?



Phishing

Tecnica di attacco di ingegneria sociale utilizzata per carpire informazioni personali e riservate (numero di conto corrente, numero di carta di credito, password, ecc..) mediante l'utilizzo di messaggi di posta elettronica fasulli opportunamente creati per apparire autentici.

Pharming

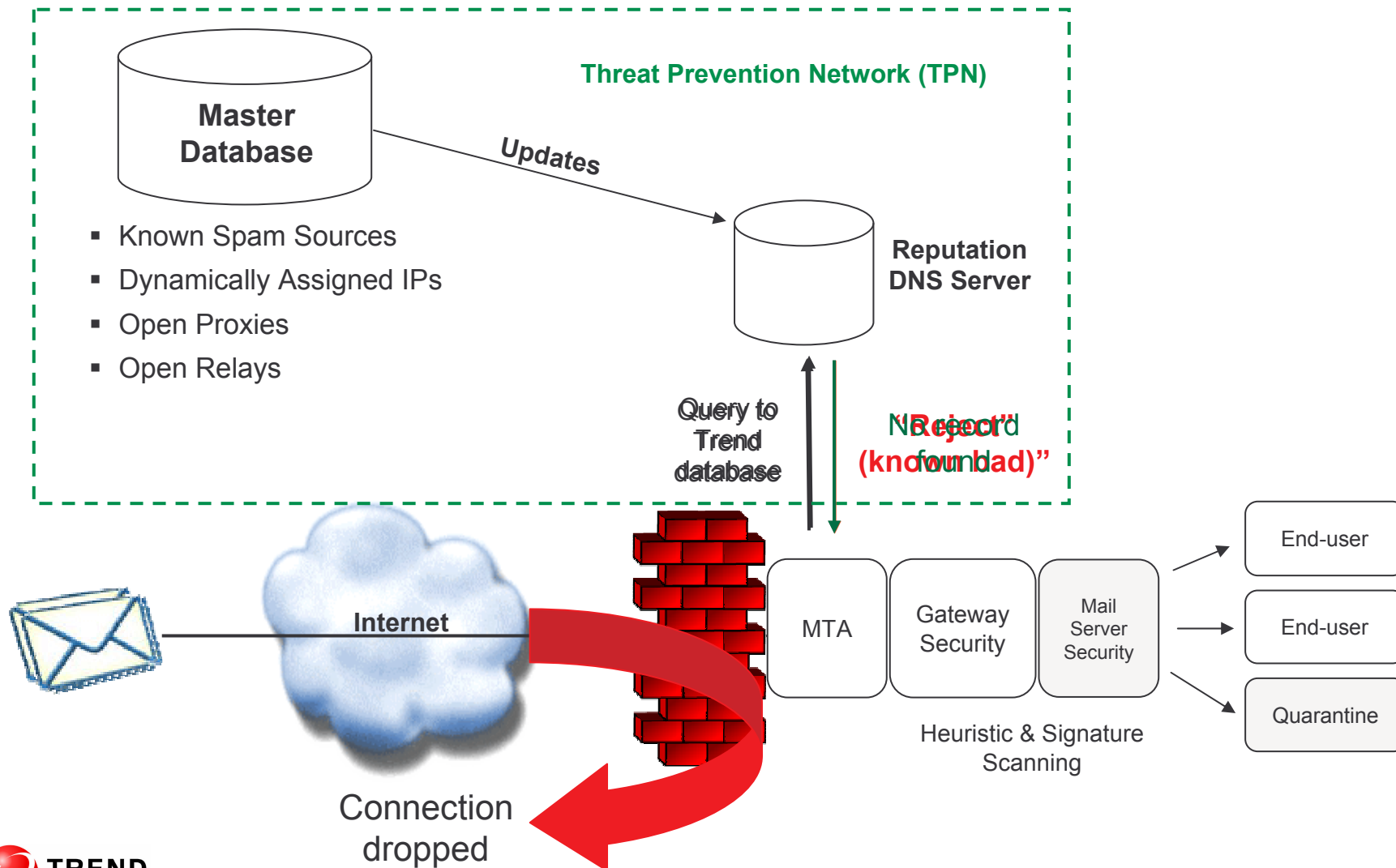
L'obiettivo è sempre quello di carpire informazioni personali e riservate (numero di conto corrente, numero di carta di credito, password, ecc..)

Tecnica di attacco che sfrutta le vulnerabilità del server DNS con l'obiettivo di alterare l'indirizzo IP di un sito web con quello di un sito trappola.

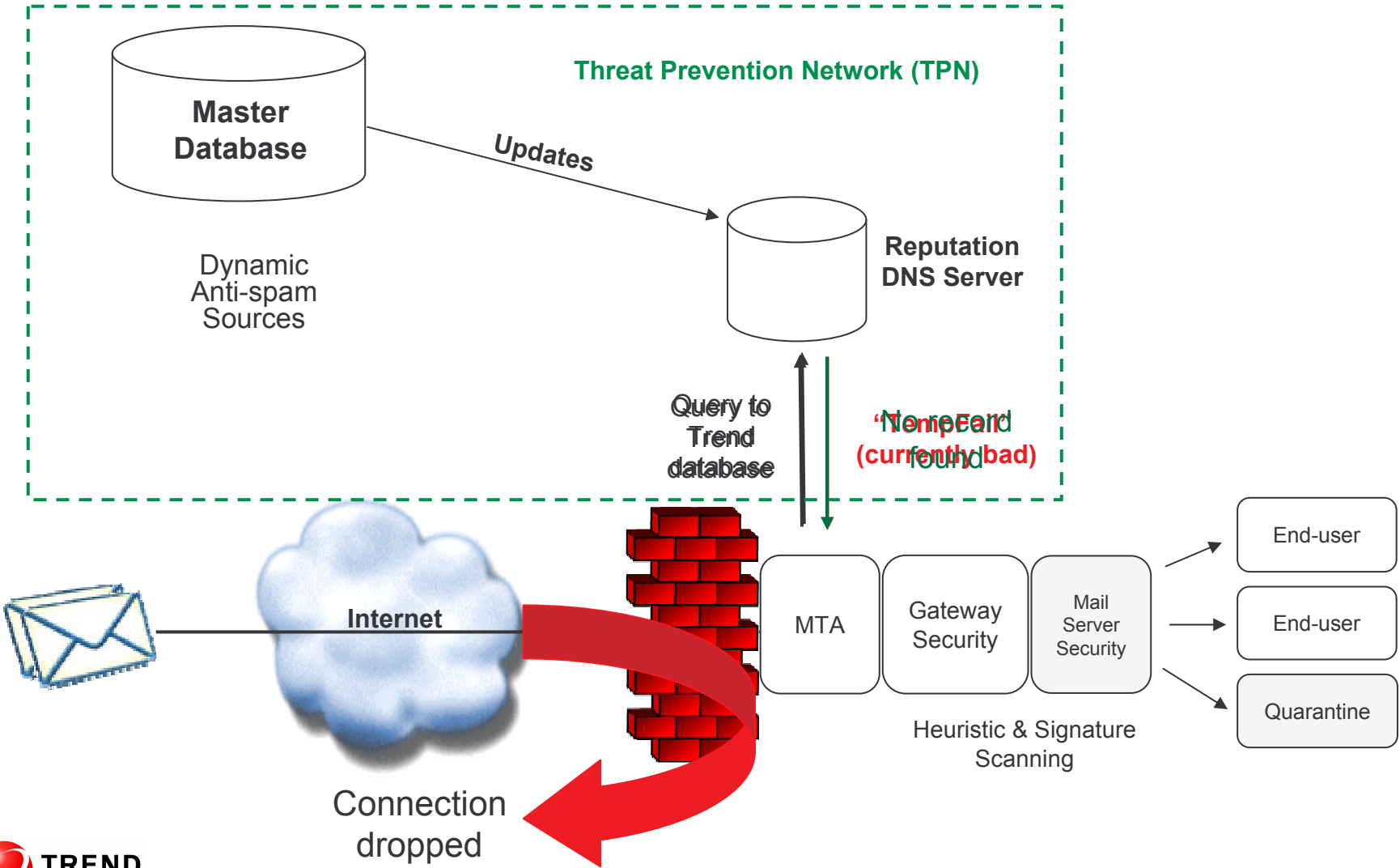
Network Reputation Services

- Trend Micro RBL+ Service
 - E' una collezione di indirizzi IP di sorgenti di spam conosciuti e comprende gli open relays e proxies
 - E' regolato dal team investigativo di Trend Micro
- Trend Micro Network Anti-Spam Service
 - Identifica nuove sorgenti Spam nel momento in cui si presentano in Internet (ad es. Zombies)
 - Utilizza tecnologie euristiche, algoritmi complessi e il monitoraggio in real-time.
 - Aggiornato dinamicamente e disponibile per effettuare delle query

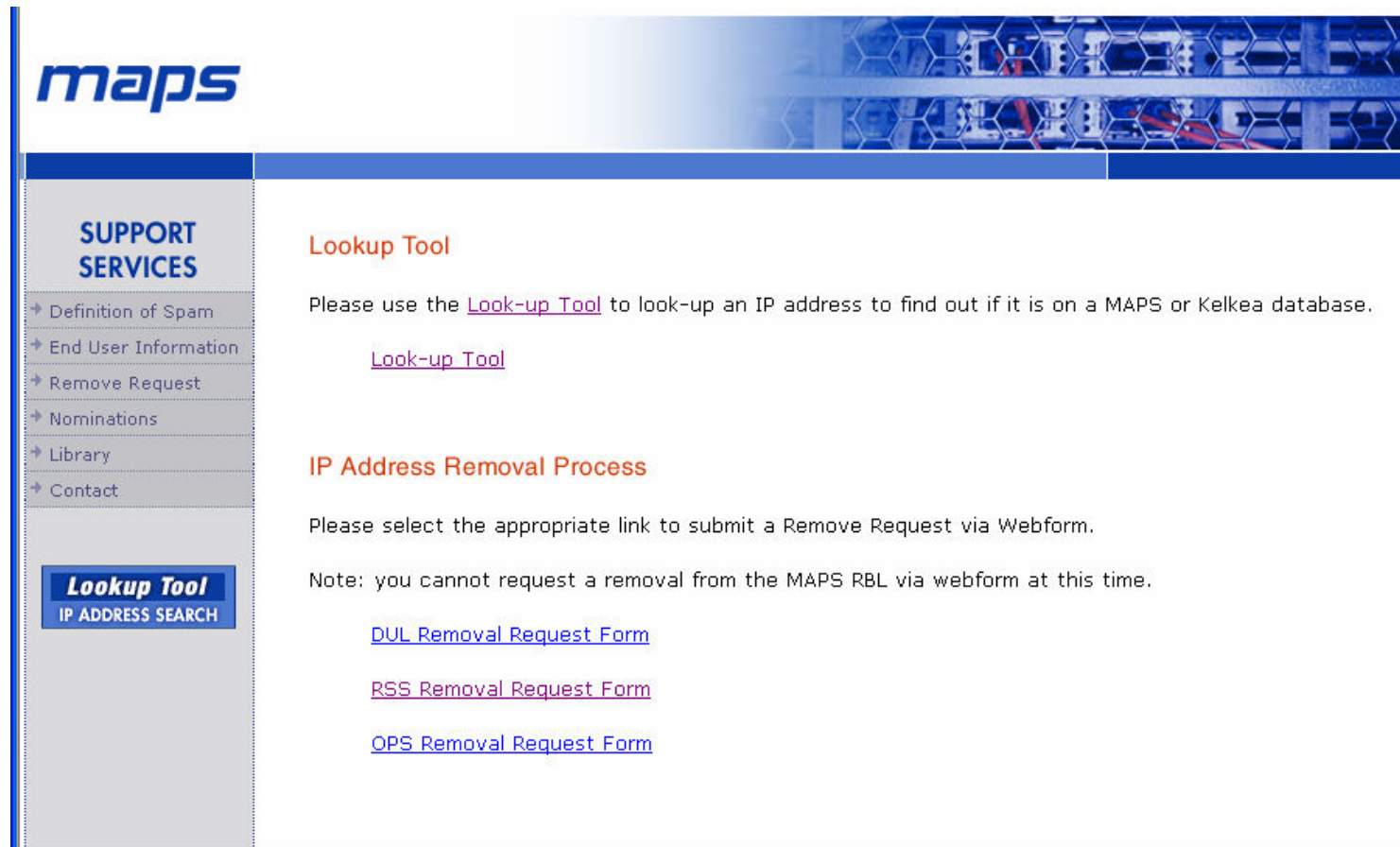
Nuovi servizi Antispam "RBL+" Service



Nuovi servizi Antispam "NAS" Service



Ricerca e rimozione di indirizzi IP bloccati



The screenshot shows the MAPS website interface. On the left is a navigation menu with the following items:

- SUPPORT SERVICES
 - Definition of Spam
 - End User Information
 - Remove Request
 - Nominations
 - Library
 - Contact

Below the menu is a button labeled "Lookup Tool IP ADDRESS SEARCH".

The main content area features a header image of server racks. Below it, the "Lookup Tool" section contains the text: "Please use the [Look-up Tool](#) to look-up an IP address to find out if it is on a MAPS or Kelkea database." followed by a link to the "Look-up Tool".

The "IP Address Removal Process" section contains the text: "Please select the appropriate link to submit a Remove Request via Webform." and a note: "Note: you cannot request a removal from the MAPS RBL via webform at this time." Below this are three links: "DUL Removal Request Form", "RSS Removal Request Form", and "OPS Removal Request Form".

<http://www.mail-abuse.com>