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

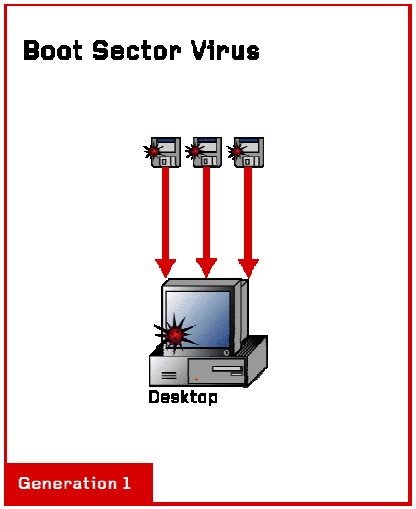
Patrick Gada

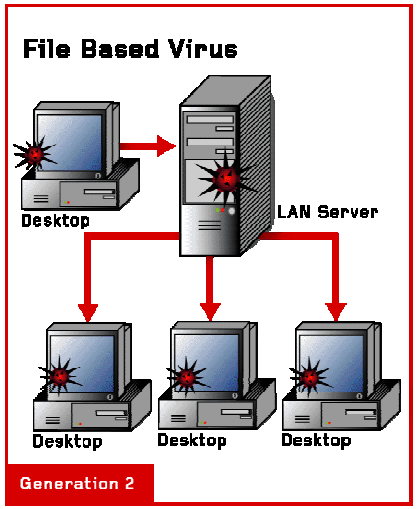
Senior Sales Engineer

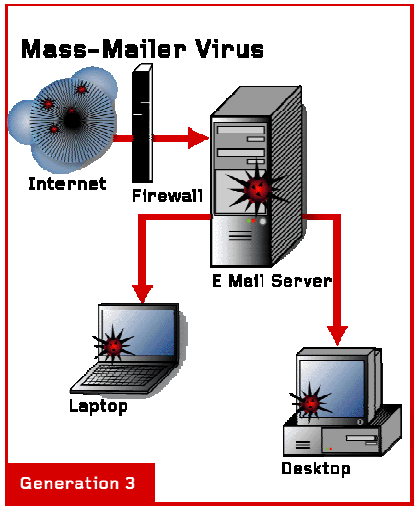
18 ottobre 2005

TREND MICRO

Evoluzione dei Virus

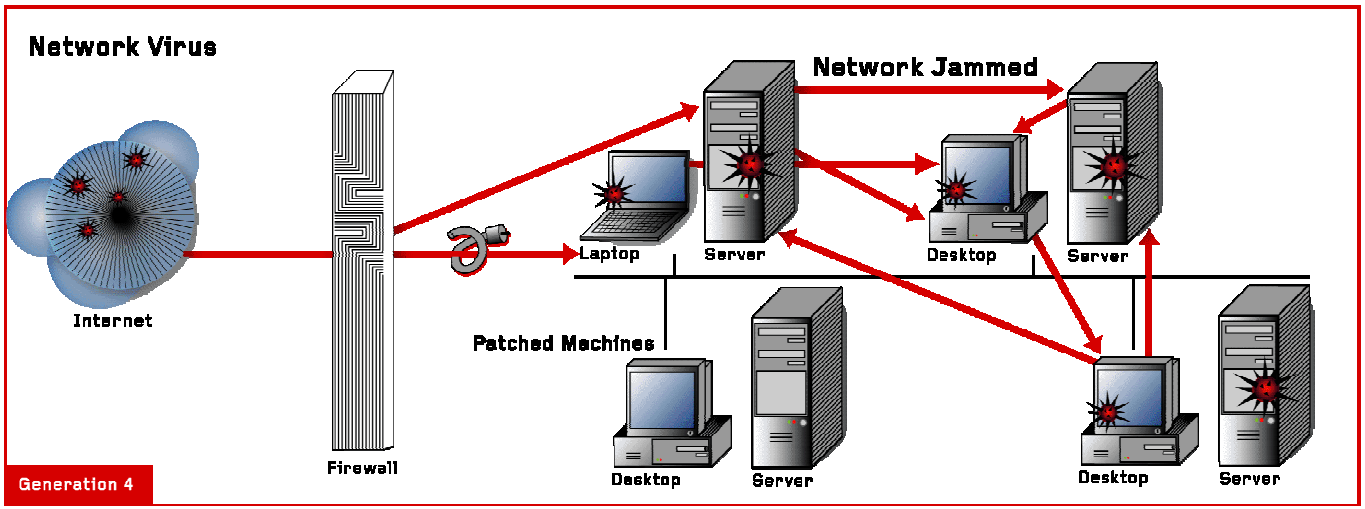






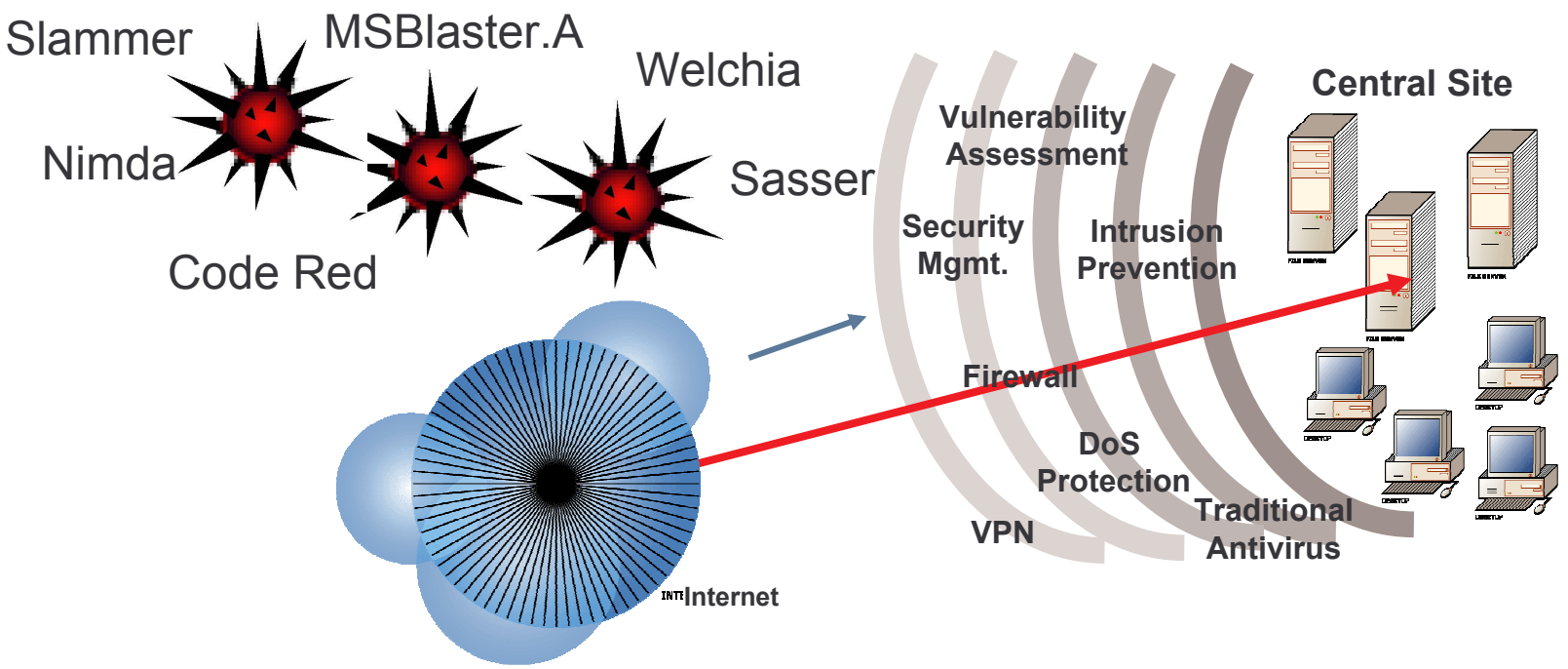
Examples:

- Worm_Sasser
- Nachi
- MSBlaster.A
- Slammer
- Code Red
- Nimda



TREND MICRO

Non è stato possibile bloccare i Network Viruses (Worms)



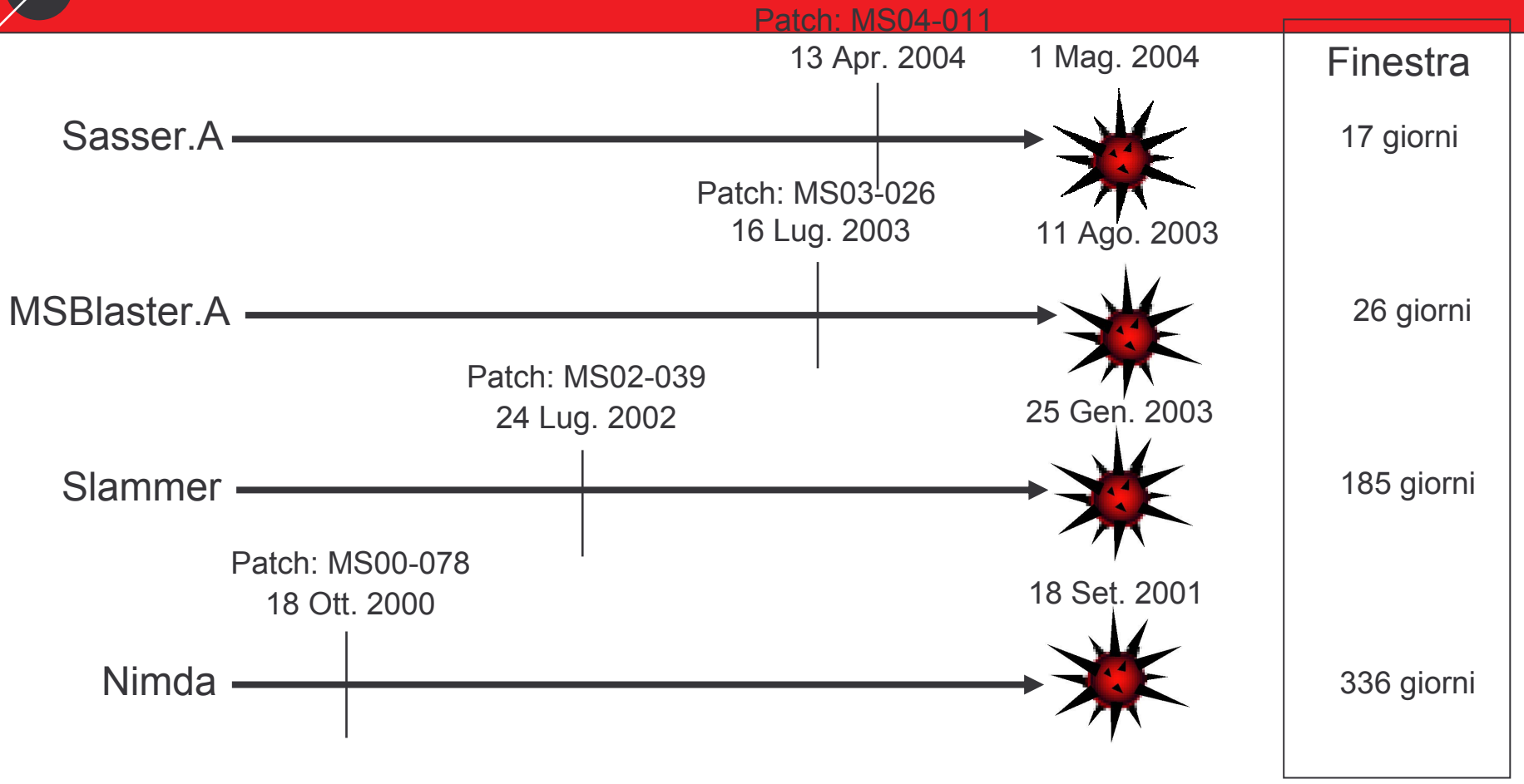
Nessuna soluzione ha bloccato o limitato la propagazione di questi virus

Molto spesso si è intervenuti in ritardo = $2.15B di danni nel solo 2003

TREND MICRO

Source: Trend Micro, Computer Economics

Sempre meno tempo per applicare le patch

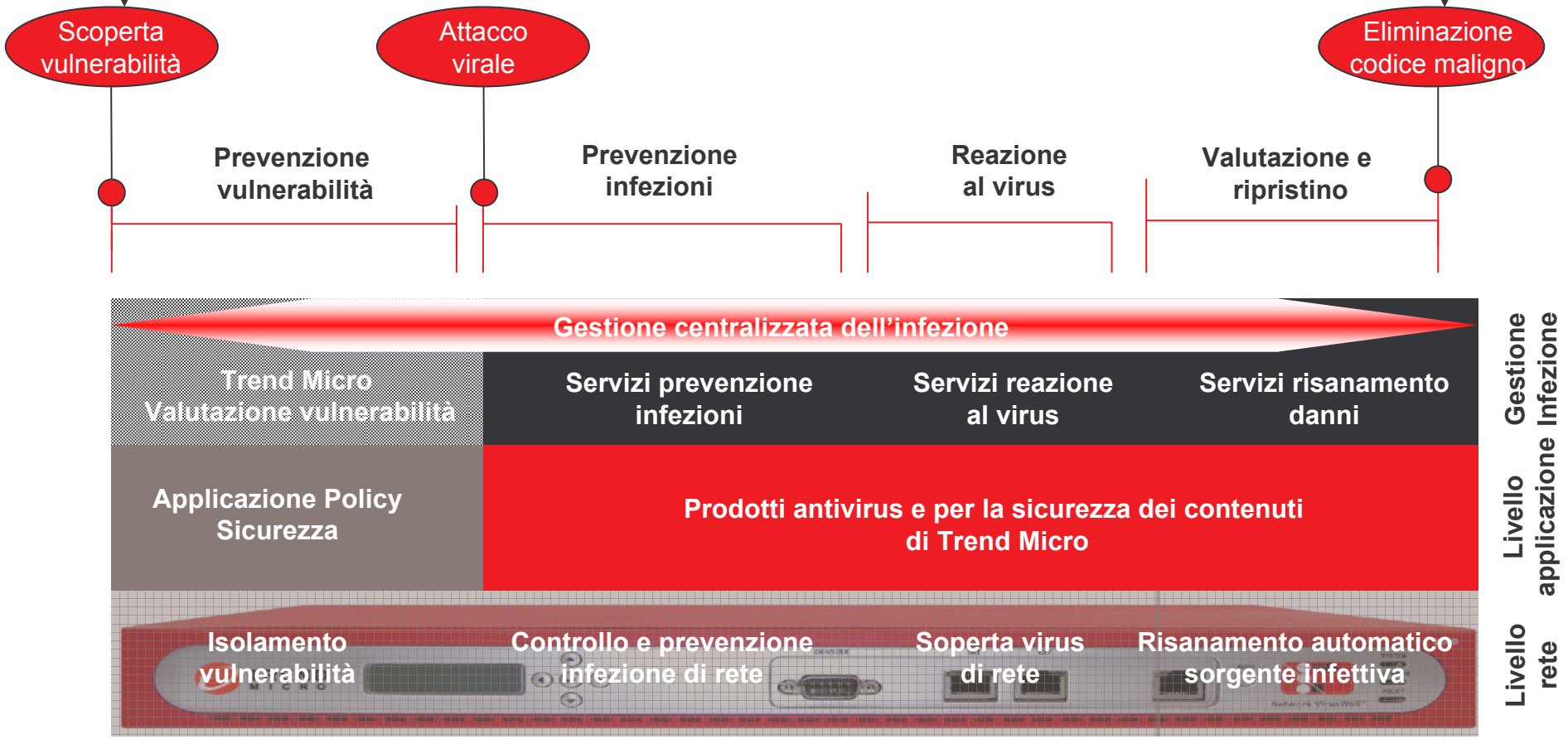


La finestra temporale dalla disponibilità della patch all'infezione si sta riducendo
E' difficile dare priorità nell'applicazione delle patch ed isolare le macchine vulnerabili durante un infezione.

Source: Trend Micro

Enterprise Protection Strategy III

Enterprise Protection Strategy: Proactive Outbreak Lifecycle Management



TREND MICRO

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

Trend Micro™ Network VirusWall™

1. Vulnerability Assessment

3. Isolation & Remote Clean up

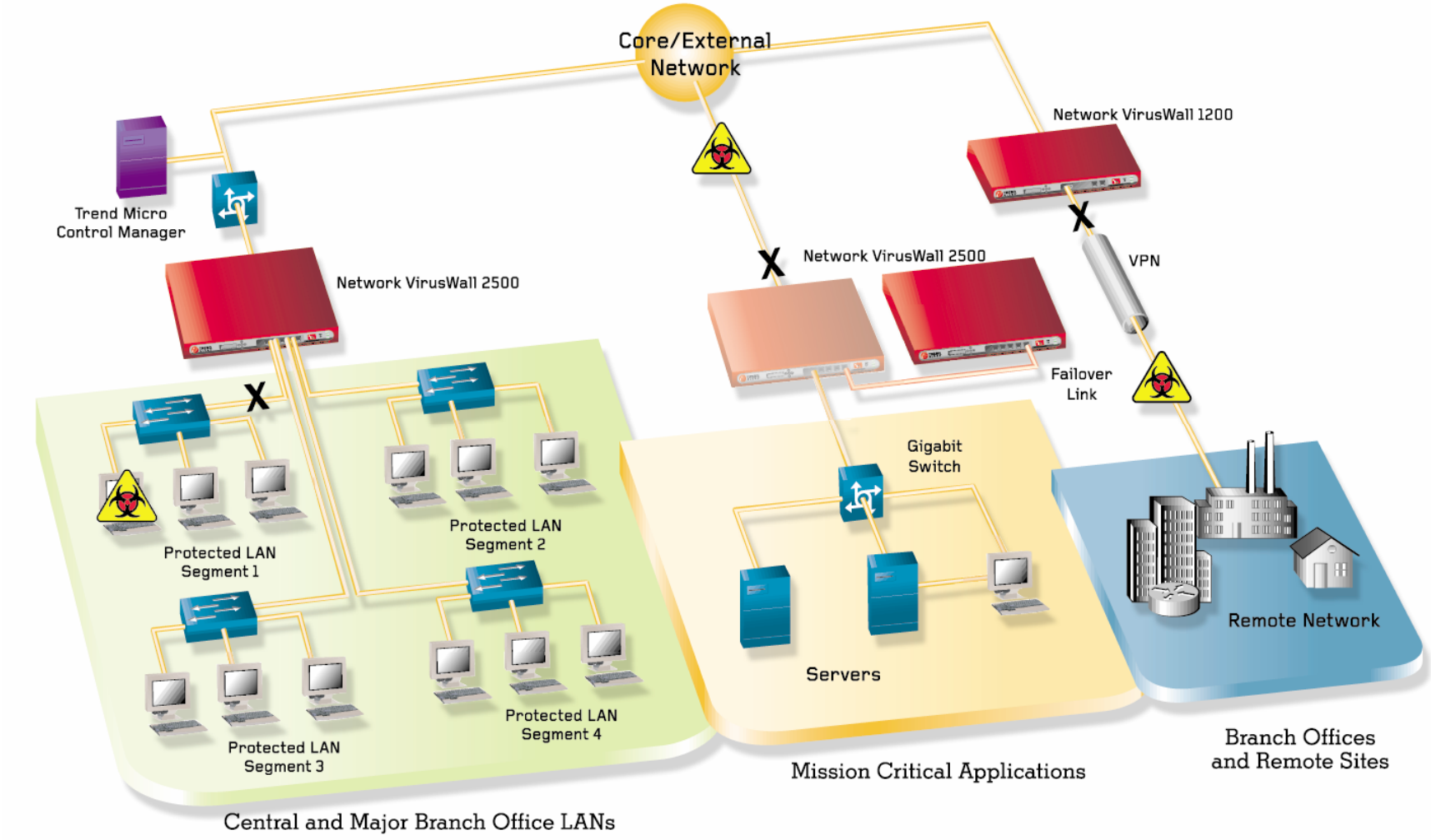
2. Network Worm Prevention – No False Positives

4. Security Policy Enforcement – Agent-less

Trend Micro Control Manager

TREND MICRO™

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, pawwsord, 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, pawwsord, ecc..)

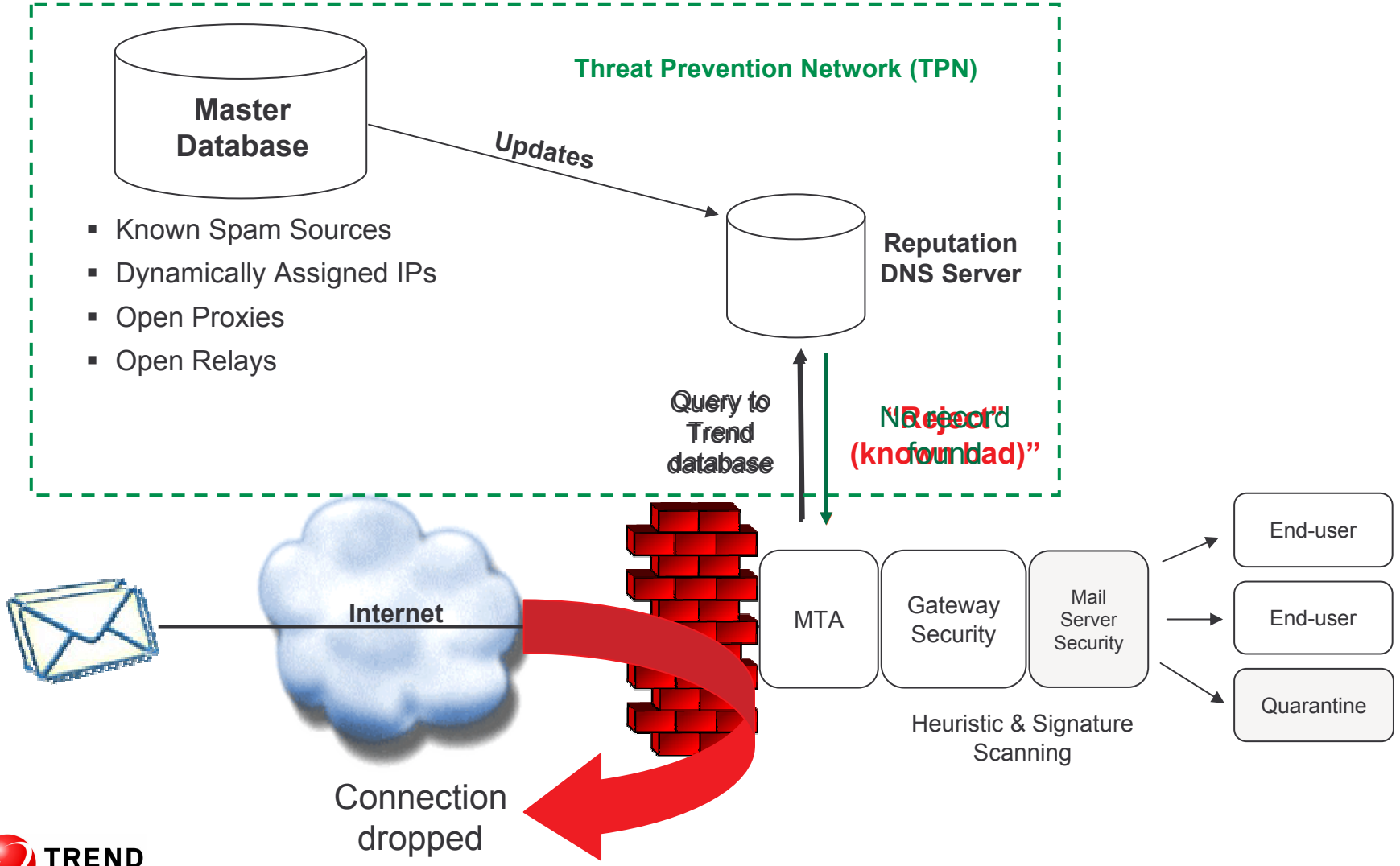
Tecnica di attacco che sfrutta le vulnerabilità del server DNS con l'obiettivo di alterare l'indirizzo IP di un sito web con quello di un sito trappola.

Network Reputation Services

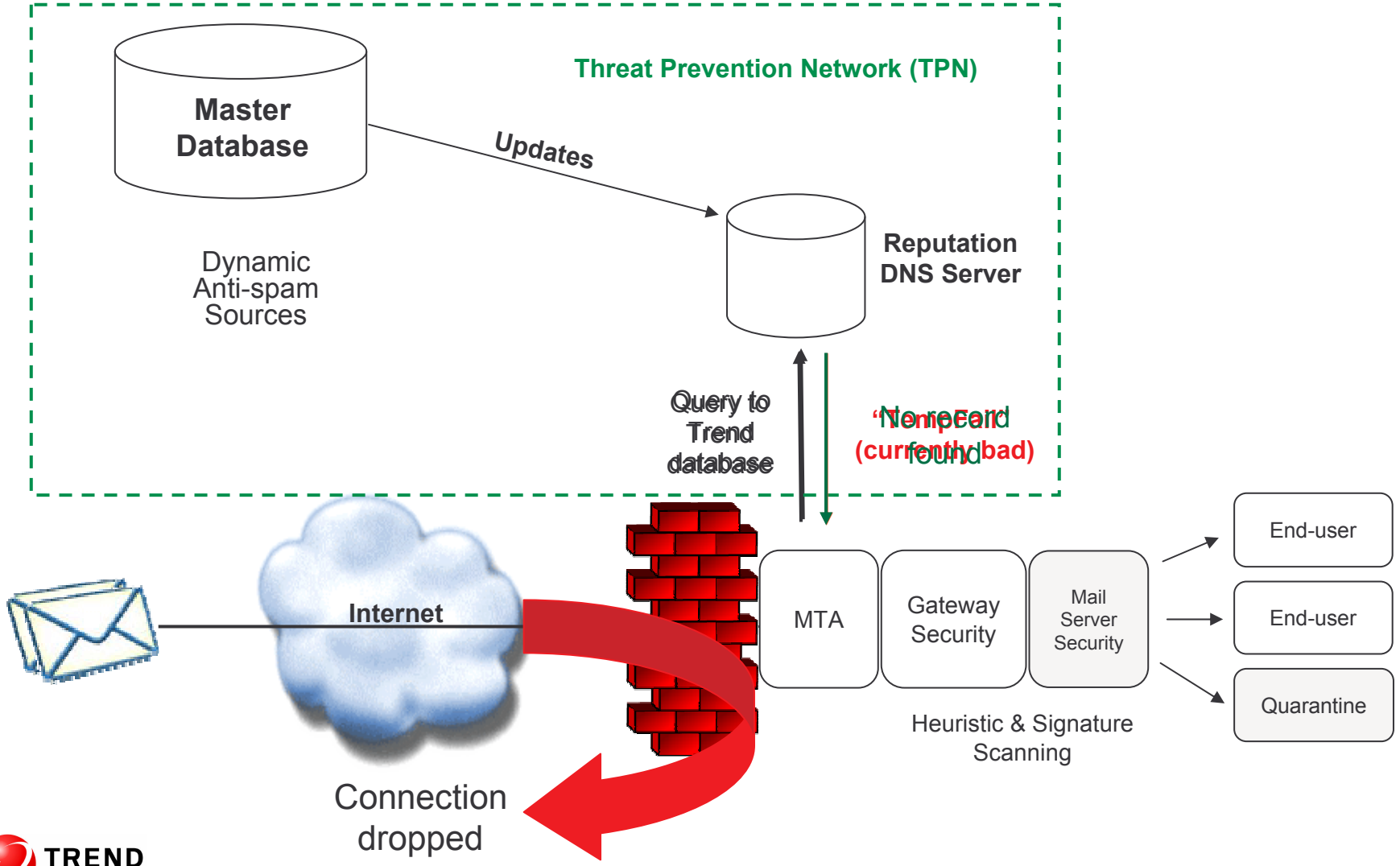
- Trend Micro RBL+ Service
  - E' una collezione di indirizzi IP di sorgenti di spam conosciuti e comprende gli open relays e proxies
  - E' regolato dal team investigativo di Trend Micro

- 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

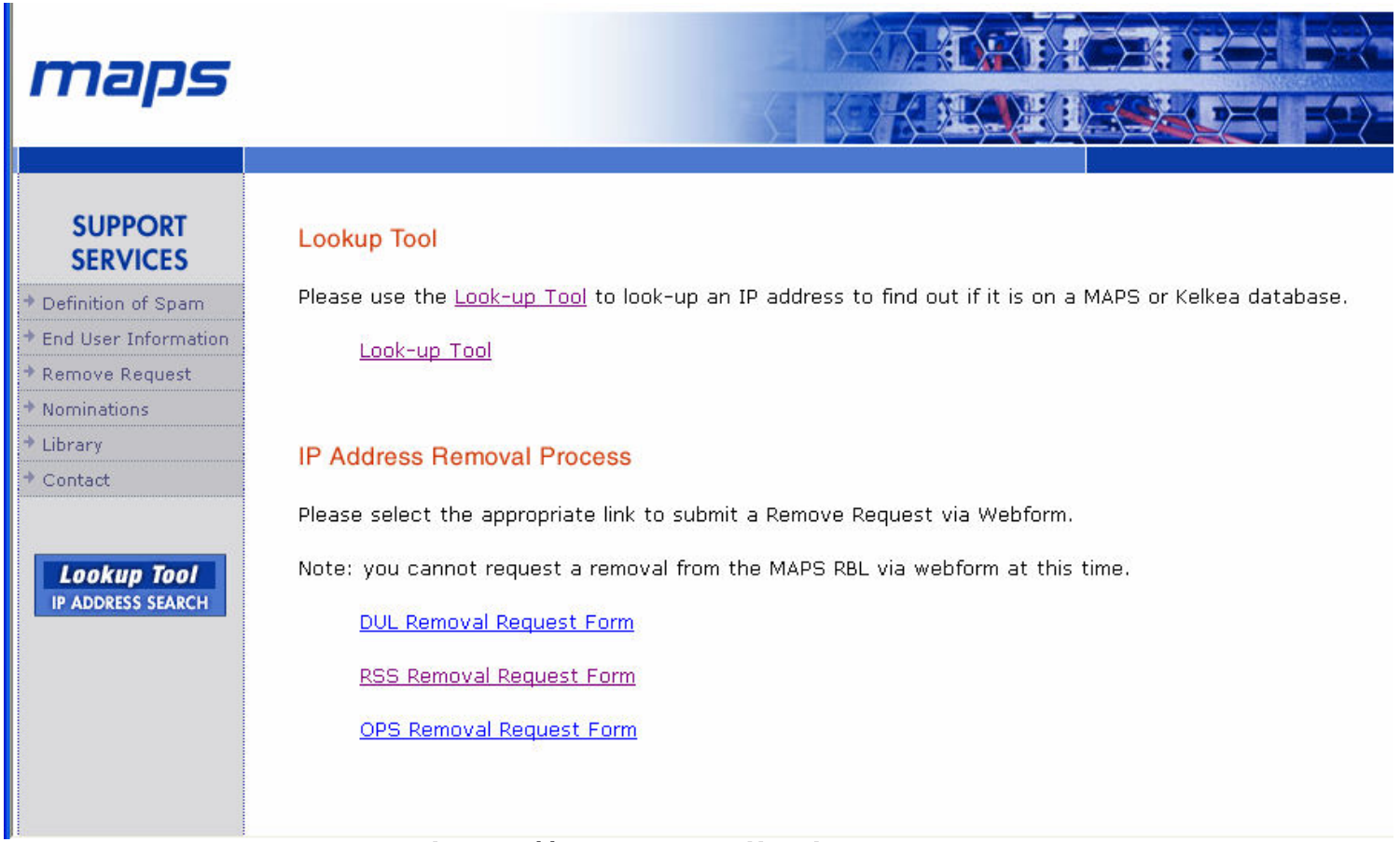


Nuovi servizi Antispam “NAS” Service



TREND MICRO

Ricerca e rimozione di indirizzi IP bloccati



http://www.mail-abuse.com

TREND MICRO