

Smart Protection Network

Christoph Brecht
Major Account Manager
Trend Micro

10 September 2009



Agenda

- Definition of Smart Protection Network
- Why do we need it
- A closer look at Cloud Client File Reputation in more detail
- FAQ

Threat Landscape and the need for the Smart Protection Network

Every 2 seconds,
new malware is
released

205 per hour

1.800 per hour

4920 per day

43.200 per day

34440 per week

302.400 per week

1790880 per year

15.724.800 per year

Traditional Endpoint Security **Cannot Keep Up**



Signature file updates take too long

- Delay protection across all clients and servers
- Leave a critical security gap
- Require multiple updates a day to keep up with threats, complicating signature management

Signature files are becoming too big

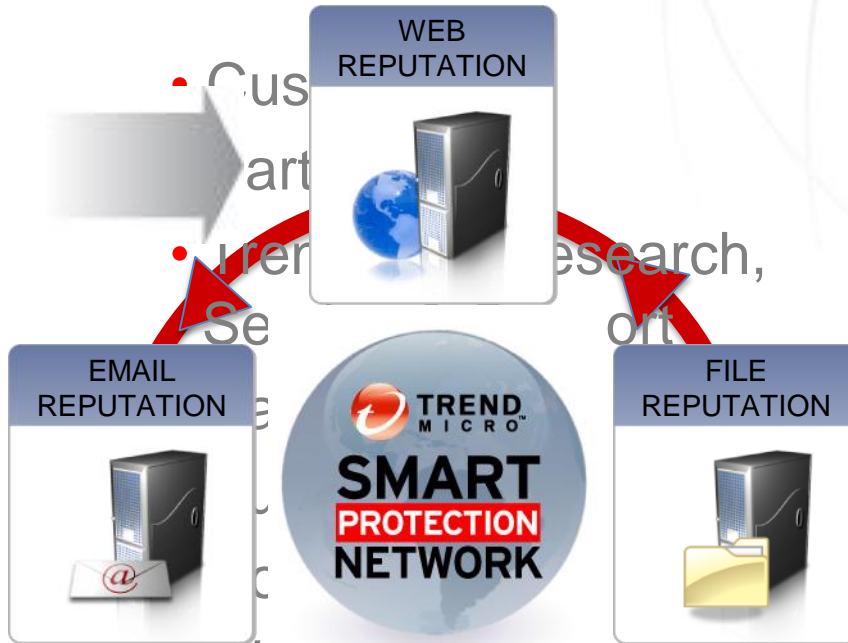
- Increase endpoint memory footprint
- Increase impact on endpoint performance
- Increase bandwidth utilization
- Unpredictable increase of client size



Unique threat samples **PER HOUR** *

* Source: TrendLabs

Correlation of threat vectors



• Customer
• Search, research,
• Software

• Web
• Feedback Loops

• Behavioral Analysis
Spam sources, embedded links,
dangerous files, and
websites with malicious content



How Smart Protection Network Works

Securing Your Web World



Fallece uno de los Grandes Joaquin Lopez Doriga

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

From: Esmas Noticias
Date: Sunday, October 26, 2008 7:49 PM
To: [Redacted]
Subject: Fallece uno de los Grandes Joaquin Lopez Doriga

Canal de las Estrellas
Fallece uno de los Grandes
Canal 2

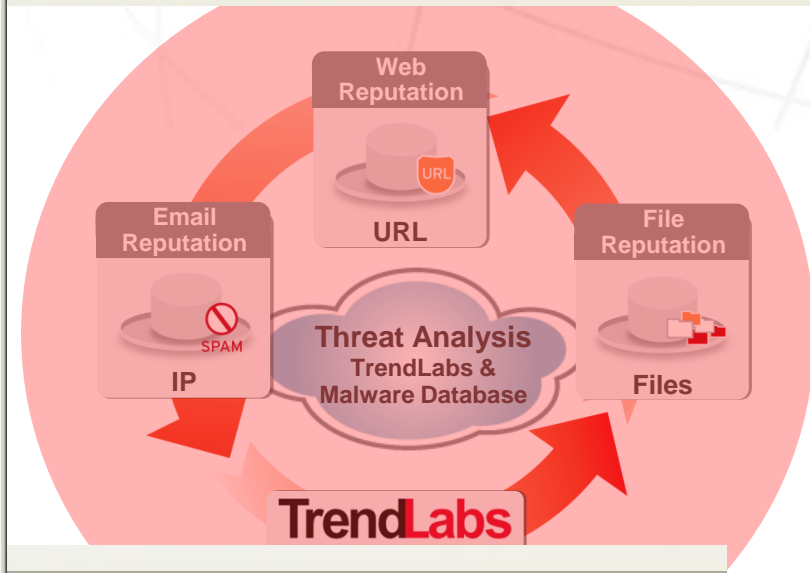
TREND MICRO™
SMART PROTECTION NETWORK

La Secretaria de Seguridad Publica (SSP) Federal informo que en el kilómetro 503 de la citada autopista, el periodista falleció por un accidente en el que estuvo involucrado un autobús de la línea ADO impactando de frente contra el automóvil del periodista en el que iba acompañado de su familia.

Puedes descargar el video desde [Aqui](#).

http://www.esmas-canal2-nota408405.mex.tc/

/components/com_admin/videoDoriga.exe



08405.mex.tc/videoDoriga.exe

The new bit: Cloud-Client File Reputation

Cloud-Client File Reputation (CCFR)



- CCFR is a Blacklisting File Reputation Technology to combat the problem of having large pattern files on every endpoint by placing Anti-malware definitions in the cloud
- CCFR reduces the bulk of pattern updates that would otherwise be downloaded to the client.
- CCFR is being introduced into all Trend Micro Endpoint Technology



Local Scan Server

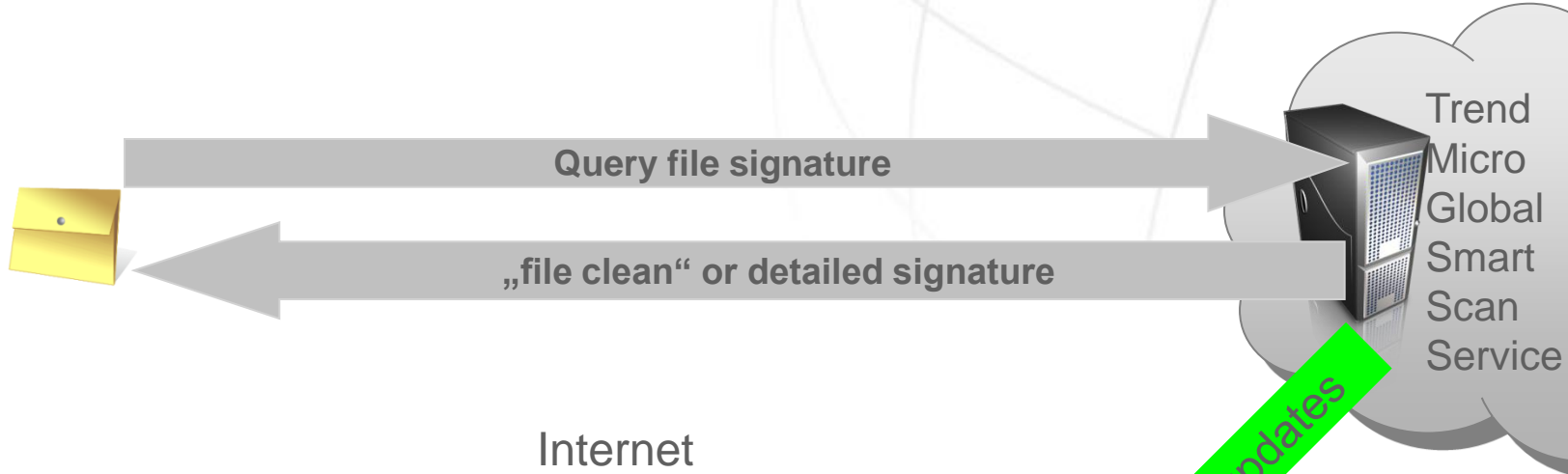
More effective protection
Less impact on performance

80% pattern file

20% pattern file



Cloud Client File Reputation



Internet

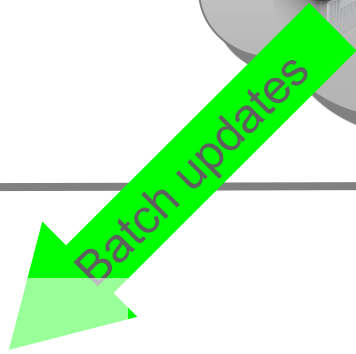
Corporate Network



Smart Scan Agent Pattern combined with the Smart Filter



Local Scan Server



Smart Scan Agent Pattern –Less Protection?



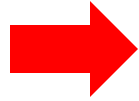
- Each client has the ‘Smart Scan Agent Pattern File
- Smart Filter is designed to prevent the Smart Client from querying the Scan Server for every single file that needs to be scanned.
- Smart Filter leverages complex mathematical models to determine—with a high degree of accuracy—whether the file scanned can be found in the actual pattern file

Scenario



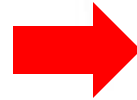
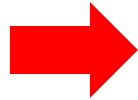
- A robbery has taken place and the Police have set up numerous roadblocks
- They have descriptions of the two robbers, who are poorly dressed, unshaven and are driving a 1990 Black VW Golf
- The Head of Police has instructed his offices at the roadblocks to stop all Black VW Golfs and then call the Police Station to verify some details.

An Analogy of how the smart filter works with the scan server



The Police office checks his notes confirms that this vehicle was not involved and passes through the roadblock

An Analogy of how the smart filter works with the scan server



Policeman checks his notes and is suspicious about this car. So he calls the Police Station for more information. The people are well dressed and cleanly shaven. Car can continue



An Analogy of how the smart filter works with the scan server



Policeman checks his notes and is suspicious about this car. So he calls the Police Station for more information. Detailed information is passed back to the Policeman and he confirms that these are the 2 robbers and they are arrested.



FAQ and Common Misconceptions

The background is a vibrant red color. It features a pattern of white dots of varying sizes, some of which are arranged in a circular or starburst pattern. On the right side, there are several overlapping, curved white shapes that resemble stylized waves or abstract geometric forms.

Other Vendors have reputation services what so special about yours?



● 3 Correlated Reputation services

- File, Web and Email

- Everyone benefits from all 3 services even if they are only running desktop

What is the Reduction in Memory Usage with CCFR?



- There is a misconception that File Reputation will reduce the memory footprint TODAY
- The key value of CCFR technology with regards to client side memory reduction is that we are reducing the growth rate of the client side memory usage over time. This is the essence of immunizing our customers against the Threat of Volume.

Are offline workers protected?



● Yes

- Each machine has the Smart Agent Pattern File and the Smart Filter
- If a file cannot be fully checked because the machine is offline and cannot connect to the Scan Server, file is placed in a deferred scan until it reconnects.
- A Machine connected to the internet will use the Global Scan Server

Will Word and Excel get scanned every time it runs?



- Within the Smart Filter, there is a Cache. Which helps to reduce the need to access the network to verify a given file's reputation.

I don't want Trend Micro knowing what files we are running



- Data sent to and from the Scan Server is encrypted
- There is never any personally identifiable or sensitive information in these transactions, only hashes

Questions?

