¿Puede cualquier empresa ser hackeada?

Joel Bo

Maximiliano Cittadini

EDSI Trend Argentina

TREND MICRO™

Securing Your Journey to the Cloud

Tom Kellermann, vice president of cyber security at Trend Micro, discusses the rising threat of cyber terrorism (Source: Bloomberg)

¿Puede?

"Si, y hay muchos como yo, incluso hay una cantidad enorme de "armamento" digital disponible en internet para quienes no poseen habilidades de programación pero desean perpetrar ataques contra otros individuos o empresas."

"Mas de 120 naciones poseen en la actualidad areas de cyber-seguridad, aunque por el momento suelen ser utilizadas para espionaje industrial"

"No debería sorprendernos. Lo que debería sorprendernos son las medidas anticuadas de seguridad que estaban colocadas. Es necesario dejar de enfocarse en detectar la bala y poder aplicar una defensa customizada."

Casos

The New York Times

Of the **45 different kind of malicious software** -- or malware -- the hackers used in their attack, Symantec **only detected one** of them.

The hackers who targeted The Times may have used a technique called "**spear phishing**", in which they send targeted emails that appear to be from a trusted source. When the victim opens a link or attachment, the hackers install malicious software -- known as malware -- onto their computer to steal documents, log keystrokes, or collect usernames and passwords.

Chinese hackers had gained entry into its computer network for **four months** in hopes of identifying a reporter's sources for an investigation into the business dealings of relatives of China's prime minister.

TREND MICRO

Casos

EVERNOTE

Evernote's Operations & Security team has discovered and
block e Evernote network that appears
to h empt to access secure areas of
te Service.

facebook

The investigation r, that the individual(s)
responsible w ss to Evernote user
information, which includes usernames, email addresses
associated with Evernote accou swords

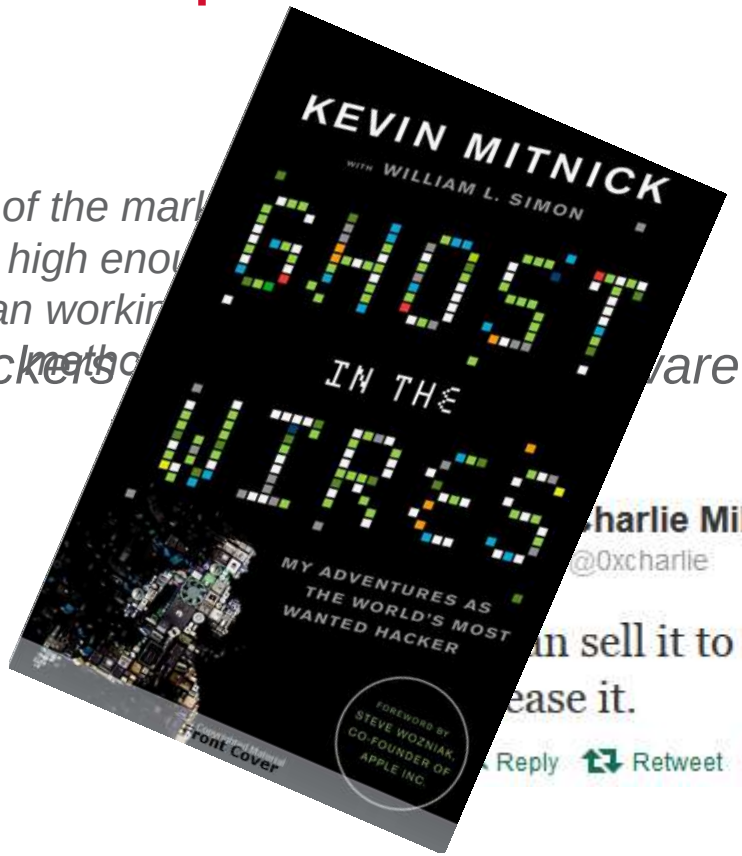
**vents with other large services have
, this type of activity is becoming more
common**

TREND MICRO

¿Qué podemos aprender?

"People with knowledge of the marl
the value of iOS bugs is high enou
much more attractive than workin

"today's hackers



are faster than

harlie Miller
@0xcharlie
Follow

n sell it to make $250k if you don't
ease it.

Reply Retweet Favorite More

- Métodos de ataque y prevención:
  - Ingeniería Social
  - Vulnerabilidades
  - Tecnología de Protección Anticuada

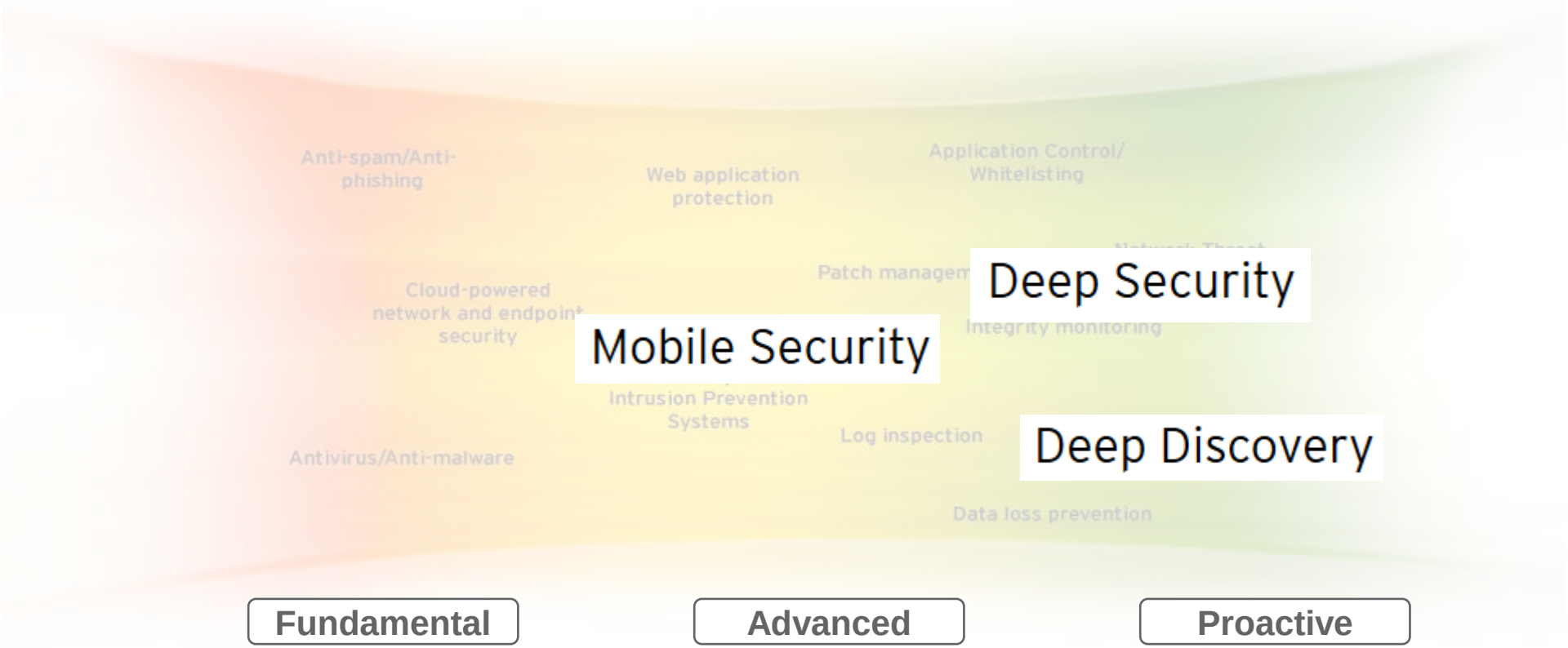
TREND MICRO

¿Que es seguridad customizada?

- Un nuevo paradigma de seguridad.

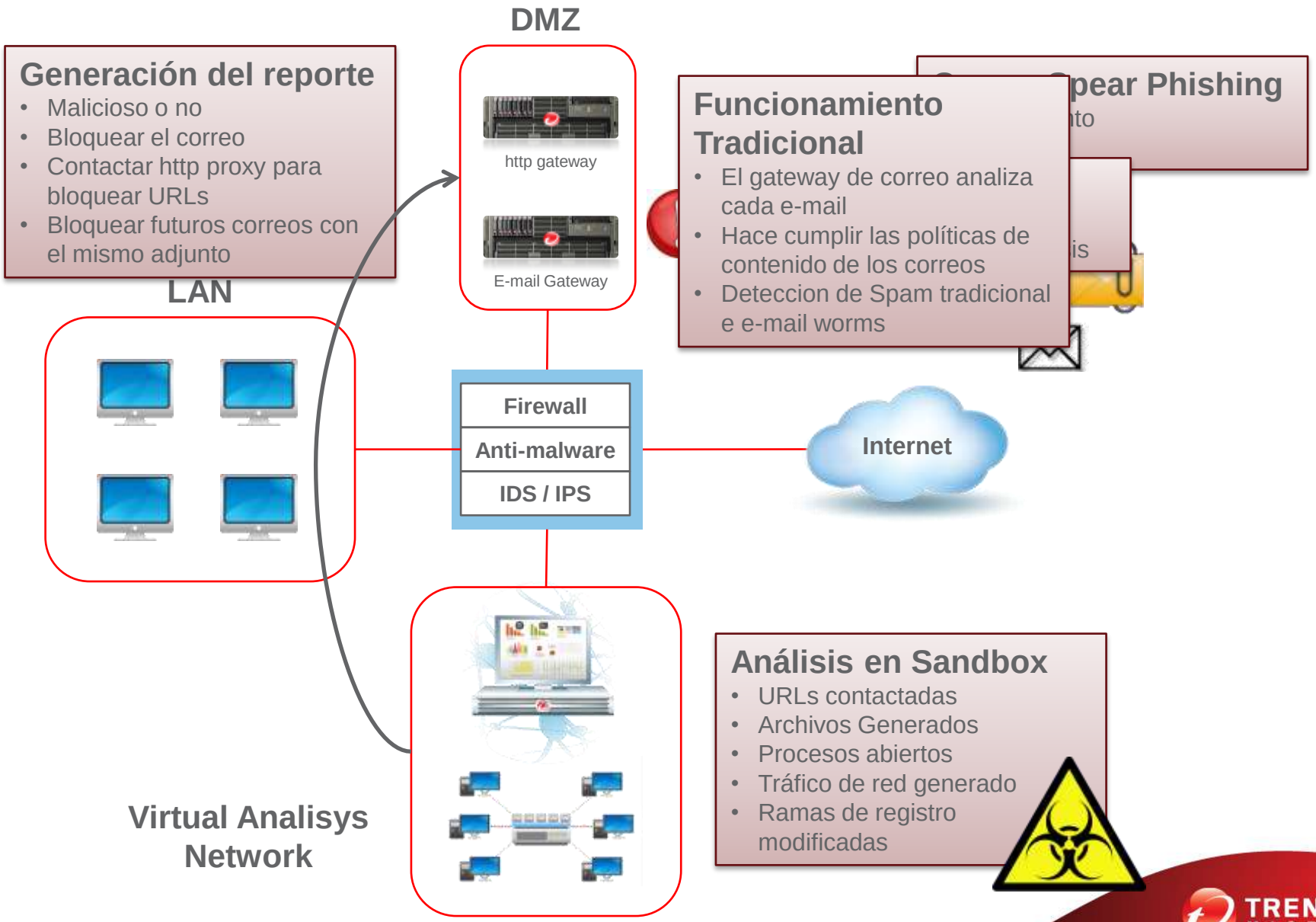
- Provee un estado de la situación de seguridad en tiempo real y adapta las defensas según corresponda.

Protection Options



Fundamental | **Advanced** | **Proactive**

Caso 1 – Spear Phishing



Caso 2 – Pendrive

Pendrive Infectado
- Nueva amenaza
- PC sin AV
- Lanza exploits a otros equipos para diseminar la amenaza
- (Conficker)

DMZ

Tráfico c&c
- Que debe hacer la amenaza
- Nuevas actualizaciones

Petición c&c

Bloquear URLs

LAN

Resetear Conexiones

Firewall

Anti-malware

IDS / IPS

Transferencia entre hosts
- Viaja copia vía SMB

Virtual Analisys Network

Análisis en Sandbox
- URLs contactadas
- Archivos Generados
- Procesos abiertos
- Tráfico de red generado
- Ramas de registro modificadas

TREND MICRO

Preguntas…

- ¿Realizo pen-test a mi infraestructura, de quienes gestionan mi red y la de mis principales proveedores?
- ¿Tengo la capacidad de aplicar parches virtuales ante vulnerabilidades de día cero?
- ¿Estoy usando file integrity monitor para detectar las huellas de los atacantes?
- ¿Cuento con herramientas de sandboxing para evaluar la carga que ingresa a mi red?

TREND MICRO

Securing Your Journey to the Cloud

Gracias