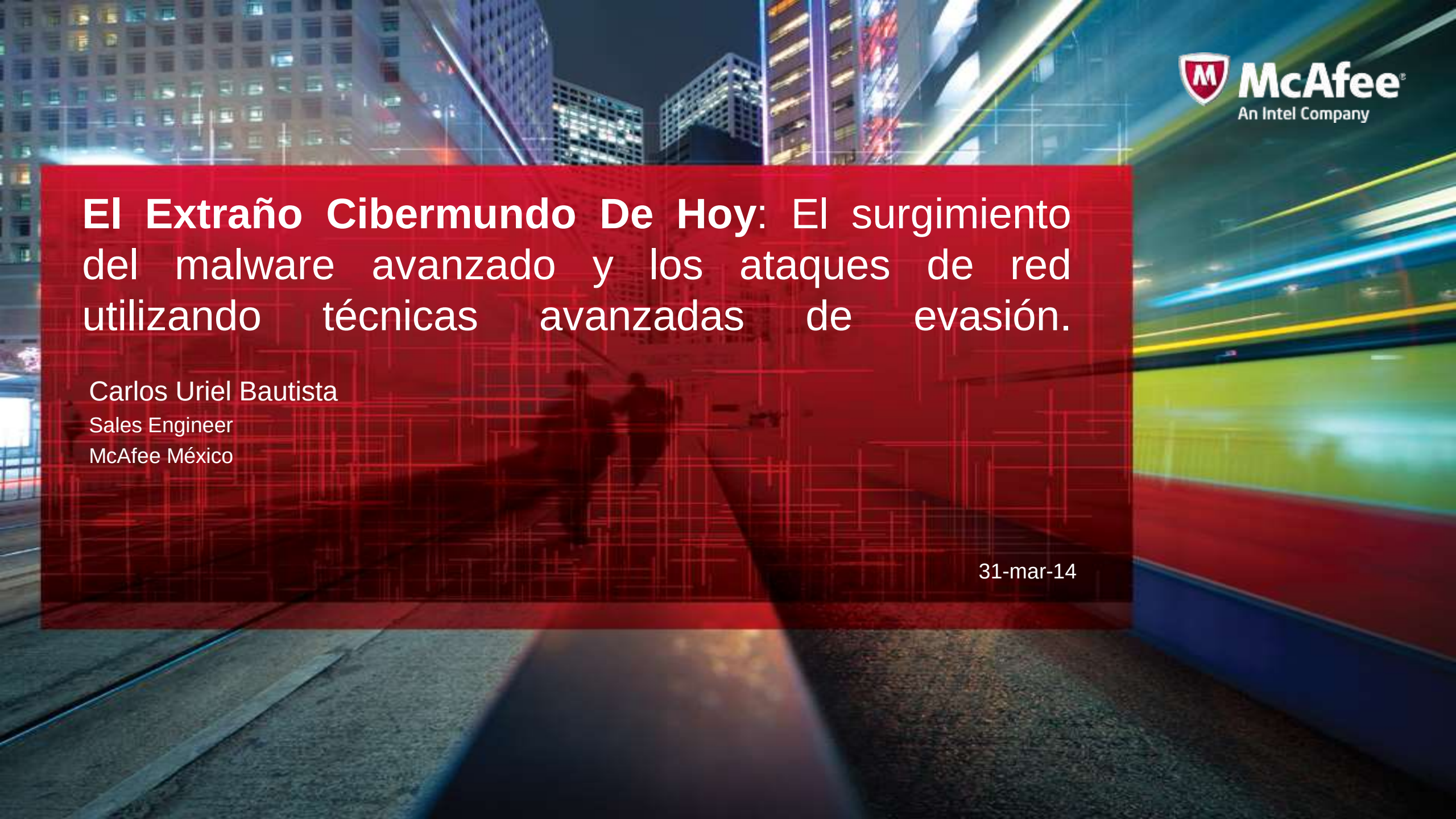


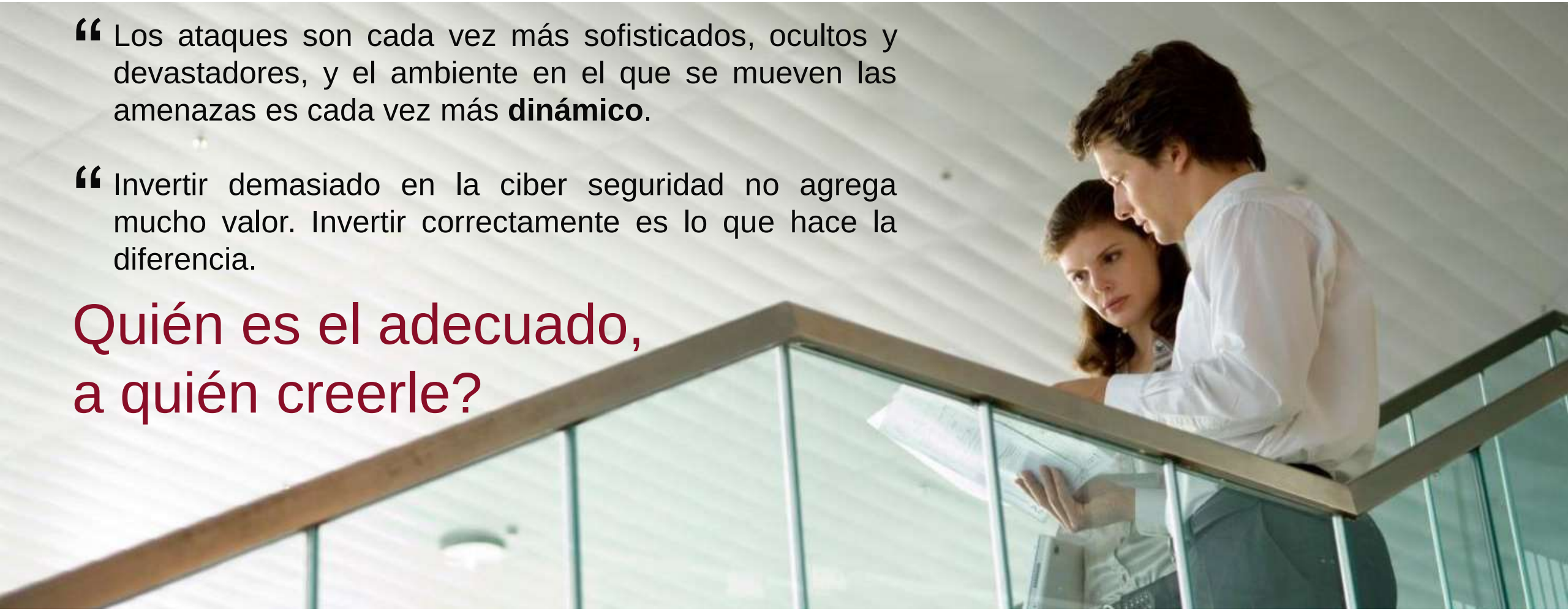
El Extraño Cibermundo De Hoy: El surgimiento del malware avanzado y los ataques de red utilizando técnicas avanzadas de evasión.

Carlos Uriel Bautista
Sales Engineer
McAfee México

31-mar-14

Un Día Normal para un CISO y Su Equipo a Cargo de la Seguridad de la Red

McAfee
An Intel Company



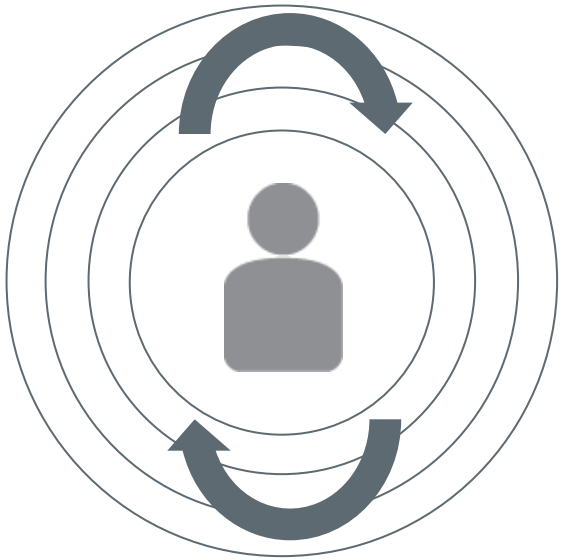
- Los ataques son cada vez más sofisticados, ocultos y devastadores, y el ambiente en el que se mueven las amenazas es cada vez más **dinámico**.

- Invertir demasiado en la ciber seguridad no agrega mucho valor. Invertir correctamente es lo que hace la diferencia.

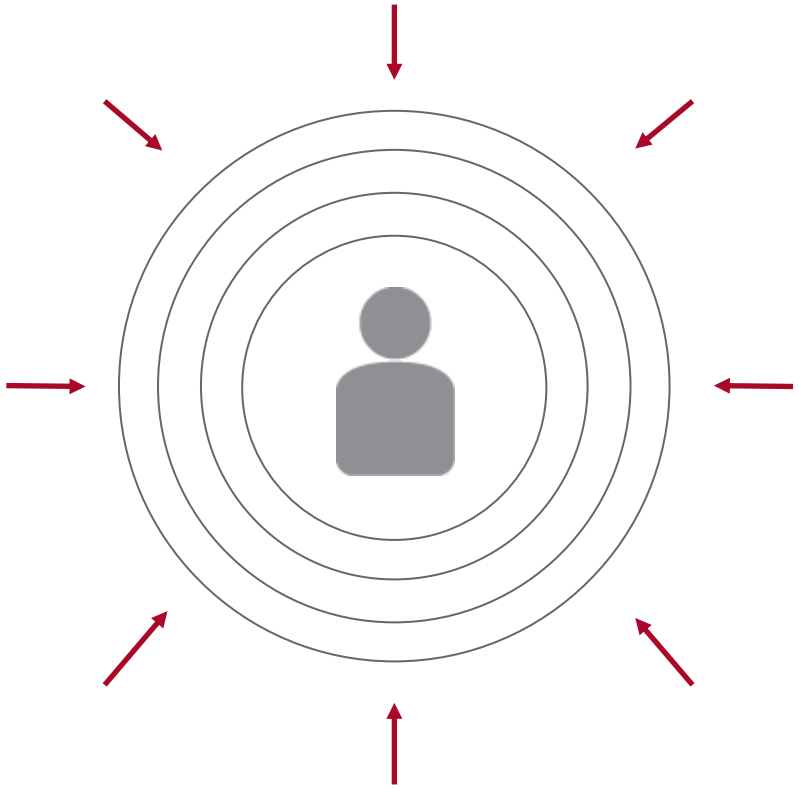
Quién es el adecuado, a quién creerle?

Prólogo

- La ley de la seguridad de red



TODO esta conectado digitalmente, con direcciones IP en la red…



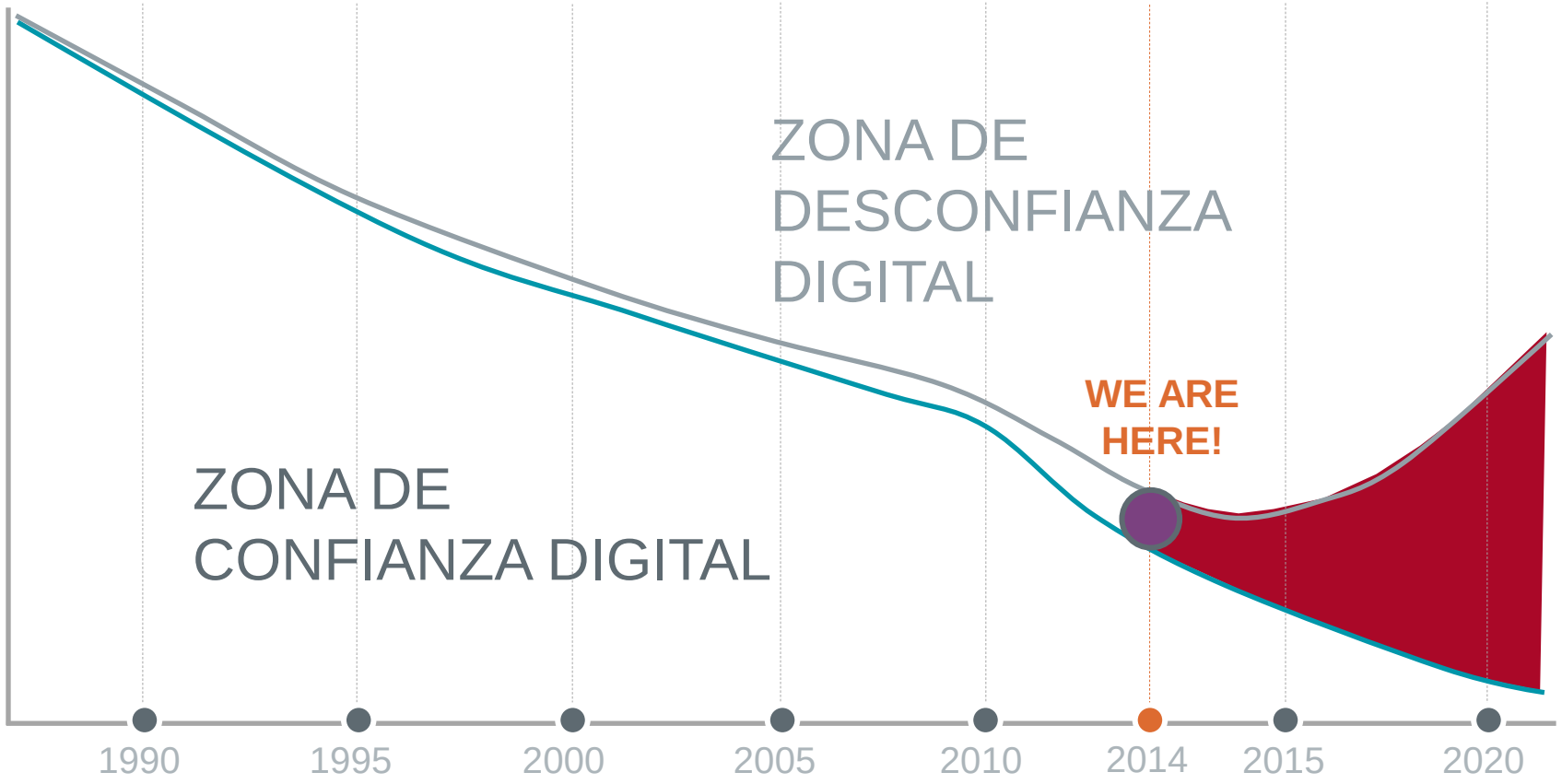
..Y **TODO** lo conectado en la red se encuentra vulnerable.

Por lo tanto **TODO** puede ser hackeado!

El extraño Ciber Mundo de hoy

El surgimiento de ciber ataques **AVANZADOS** y **EVASIVOS**.

Estamos llegando al punto de inflexión



DIGITALIZACION, MOBILIDAD Y EL RESTO EN INTERNET

Los Cibercriminales hacen más dinero hoy día

McAfee
An Intel Company

que el PIB del la economía #28 mundial

Que es Seguridad? Modelo-Realidad-Sentimiento

70-80%

…de los ciber ataques son reportados por terceros.

EN PROMEDIO ESTOS ATAQUES SUCEDEN

12

meses atrás

LA CIBER SEGURIDAD ES AUN..

UNA **IDEA** TARDÍA

…al tomar decisiones de negocio.

Es Responsabilidad de Todos!

- El Flujo del Ciber Sufrimiento

CYBER SHOCK

USUARIO(S)
Baja Productividad

ADMINS
Extra Trabajo, Presión en el tiempo

GESTIÓN DE LA RED Y LA SEGURIDAD
- Trabajo de Gestión
- Presión Profesional
- Necesidad de Cambio

CEO
Valor de las Acciones

VENTAS & MARKETING
Confianza del Cliente

CFO
Impacto Económico

CIO
Falla en Habilitar el negocio y la estrategia

Existen dos Tipos de Víctimas:

- AQUELLOS CON ALGO DE VALOR
- AQUELLOS QUE SON VICTIMAS OBVIAS.

Por lo Tanto…

El Surgimiento de Ciber Ataques Avanzados y Evasivos

Definiciones

APT

ADVANCED PERSISTENT THREAT

"**Un atacante altamente motivado** implementando un ataque enfocado. Utiliza múltiples metodos de hacking y malware avanzado con el objetivo de penetrar y mantenerse oculto por un periodo largo de tiempo. Con frecuencia utiliza AETs para mejorar su porcentaje de éxito al intentar penetrar la red."

Malware Avanzado y Evasivo

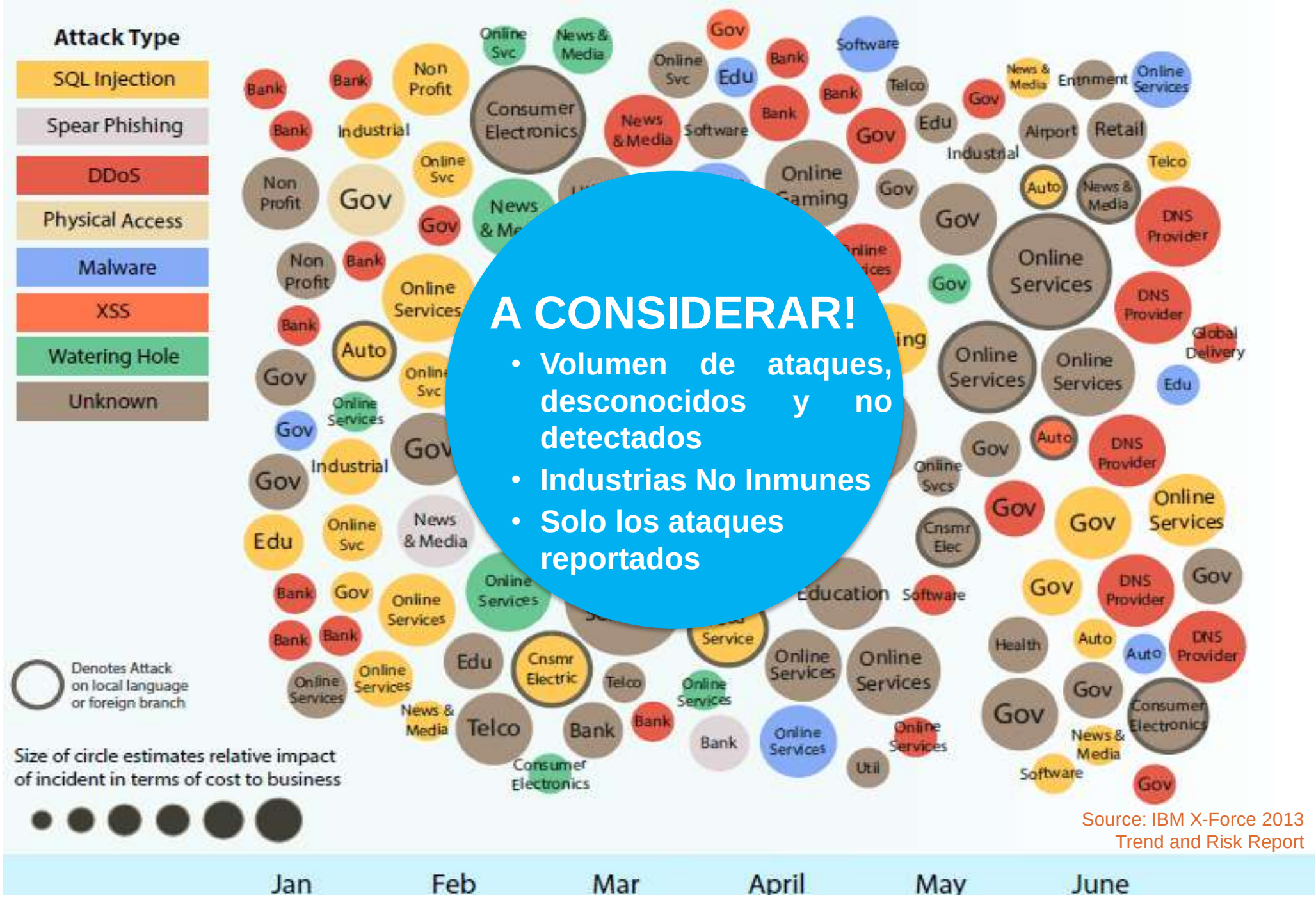
MALWARE AVANZADO Y EVASIVO PARA ATAQUES BASADOS EN HOST

"**Cualquier tipo de malware** diseñado y desarrollado para operar y no poder ser detectado mientras penetra en puntos de acceso y hosts objetivo."

AET

TECNICAS AVANZADAS DE EVASION EN AMBIENTES DE RED

"**Son Técnicas especificas de hacking** que han sido desarrolladas para burlar los dispositivos de seguridad y entregar código malicioso o un exploit a un objetivo sin ser detectado. Los AETs pueden ser utilizados para entregar exploits y contenido malicioso conocido y no tan conocido..



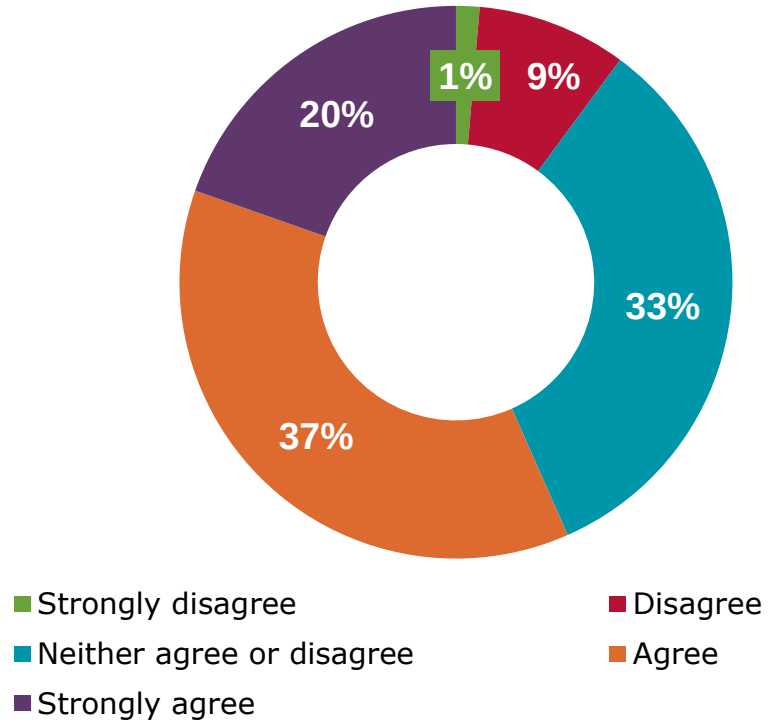
Source: IBM X-Force 2013 Trend and Risk Report

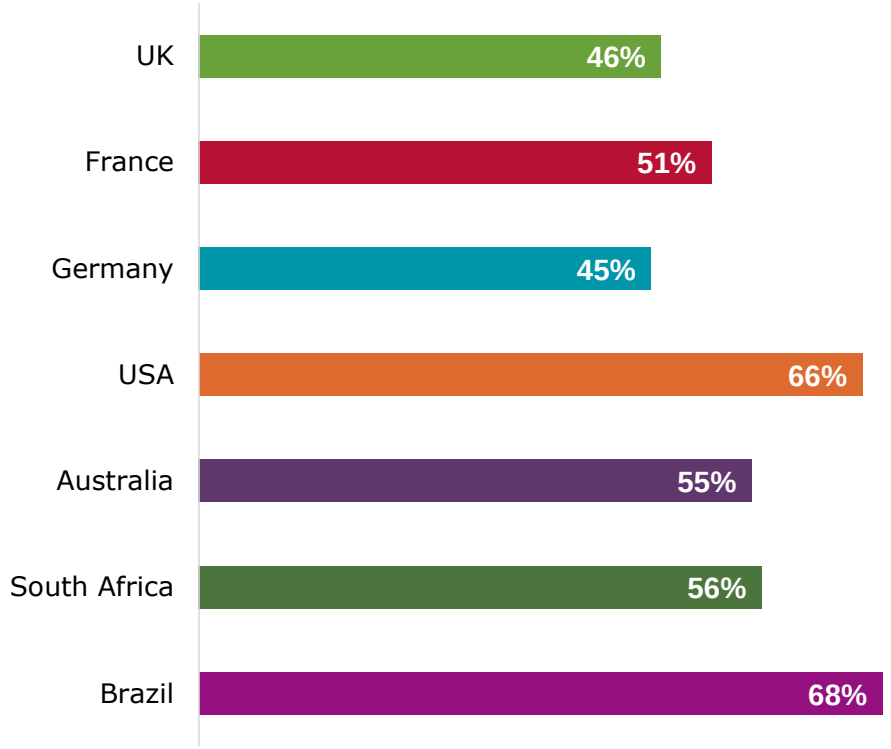
El Nacimiento de lo “Desconocido”

Una clara evidencia de los métodos avanzados y evasivos

Observando el Nacimiento

de lasTécnicas Avanzadas de Evasión



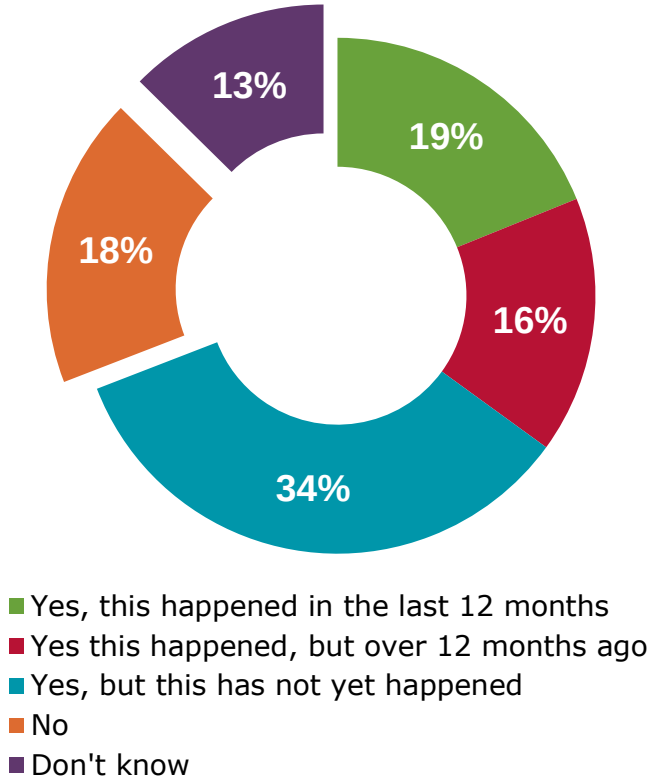


"Por favor indique que tan de acuerdo está con lo siguiente" AETs representan una amenaza inmediata a mi negocio de una muestra de empresas corporativas (800)

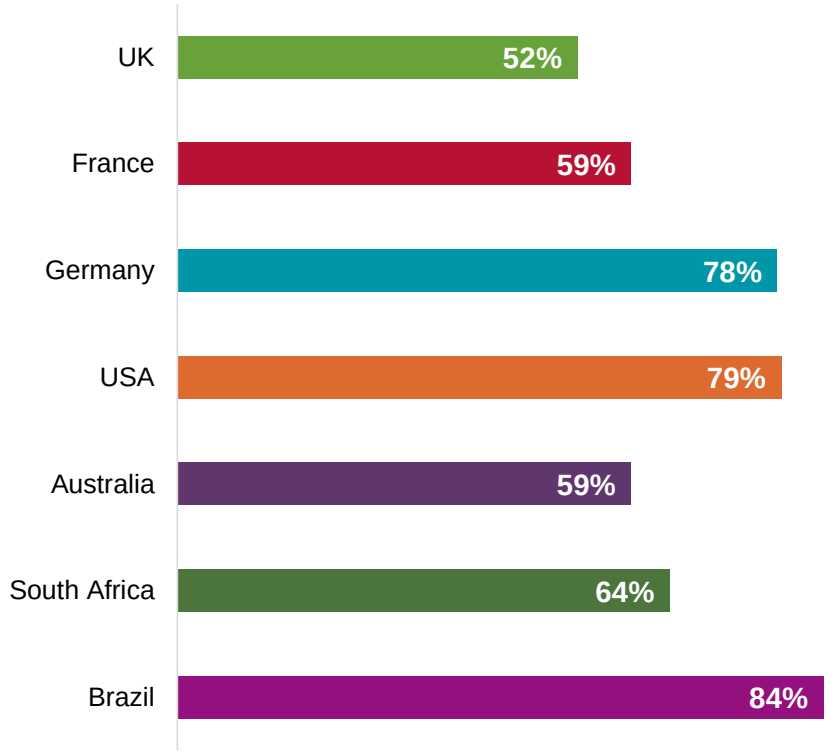
Análisis de aquellos que estuvieron de acuerdo que las AETs representan una amenaza actualmente – por país de una muestra de empresas corporativas (800)

El Mundo Real

de las Técnicas Avanzadas de Evasión



"Los AETs han permitido redescubrir y explotar vulnerabilidades conocidas en su ambiente actual?"
De una muestra corporativa (800)



Análsis de las organizaciones que piensan que las AETs pueden redescubrir vulnerabilidades conocidas en sus ambientes
De una muestra corporativa (800)

AETs Apoyan el Caso de Negocio de los Hackers

Cuando los hackers compran y desarrollan nuevos exploits pueden mejorar su ROI sustancialmente al usar AETs. Inclusive pueden reciclar los datos maliciosos existentes al usar AETs.

Al utilizar AETs los hackers pueden Ingresar al lugar más profundo en la red.

…y puede ser realizado sin ser detectado, con sigilo.

Como Combatir las Técnicas Avanzadas de Evasión

Como defendernos y combatirlos?

Porque preocuparnos HOY?

- Que tal les va a los AETs en contra de los productos líderes de nueva generación?

7 CASO DE PRUEBA (Conficker worm)	ATAQUES DE AET EXITOSOS (NO detectados)
Divide exploit in IP fragments	70%
Divide exploit in TCP segments	90%
Using grey areas of protocols to hide the exploit	90%
Change byte encoding methods	40%
TCP segmentation and re-ordering	80%
TCP segmentation and re-ordering + urgent data	90%
Sending TCP payload with old timestamps (PAWS)	80%

CISCO

TippingPoint

paloalto NETWORKS

JUNIPER NETWORKS

Check Point SOFTWARE TECHNOLOGIES LTD.

SOURCEfire®

FORTINET

McAfee NGFW Ha sido Probado Exitosamente

NOTE: The NSS Labs evasion test consists of approx. 60 static, recorded AETs that can be easily fingerprinted.

Lo mínimo Antimalware y para Ataques de Evasión

…que su NGFW y las tecnologías de seguridad de red tengan la capacidad de **detectar, detener y generar reportes** de **Técnicas Avanzadas de Evasión**.

…adquiera únicamente capacidad real de Anti-Evasion.

…y verifique el estatus de protección contra AET.
No confie solo en la palabra de su fabricante.


McAfee®
An Intel Company