



STORMSHIELD



PROTECCIÓN DE SERVIDORES, PUESTOS Y TERMINALES

SEGURIDAD ENDPOINT

NETWORK SECURITY | ENDPOINT SECURITY | DATA SECURITY

UNA CONSTATACIÓN: LOS PUESTOS DE TRABAJO Y LOS SERVIDORES ESTÁN TODAVÍA EN RIESGO

HERRAMIENTAS TRADICIONALES INSUFICIENTES

A pesar de los millones invertidos, las empresas se enfrentan al **fracaso de las herramientas de defensa tradicionales** en la lucha contra los ataques dirigidos o sofisticados.

Las herramientas de tipo antivirus o HIPS proponen, en efecto, un enfoque reactivo y no proactivo para detectar los programas y los comportamientos maliciosos. Utilizan una base de firmas que se limita a las amenazas conocidas y suelen verse impotentes contra los ataques completamente nuevos.

Además, los hackers ponen en práctica mecanismos de camuflaje avanzados para disimular sus movimientos y, de ese modo, saltarse esas protecciones basadas en firmas.

ATAQUES CADA VEZ MÁS AVANZADOS Y DIRIGIDOS

Se considera que un ataque es sofisticado cuando es capaz de eludir los mecanismos de seguridad tradicionales.

Esta sofisticación se obtiene gracias a la combinación de múltiples métodos de ataque avanzados como, por ejemplo, la explotación de una vulnerabilidad de aplicaciones (servidor web, lector de archivos PDF) y después la propagación de un software malicioso a través de la red de la empresa o obtención de la acceso a de los activos sensibles mediante la elevación de privilegios.

EL IMPACTO DE LAS AMENAZAS EN CIFRAS

14 mil millones de €

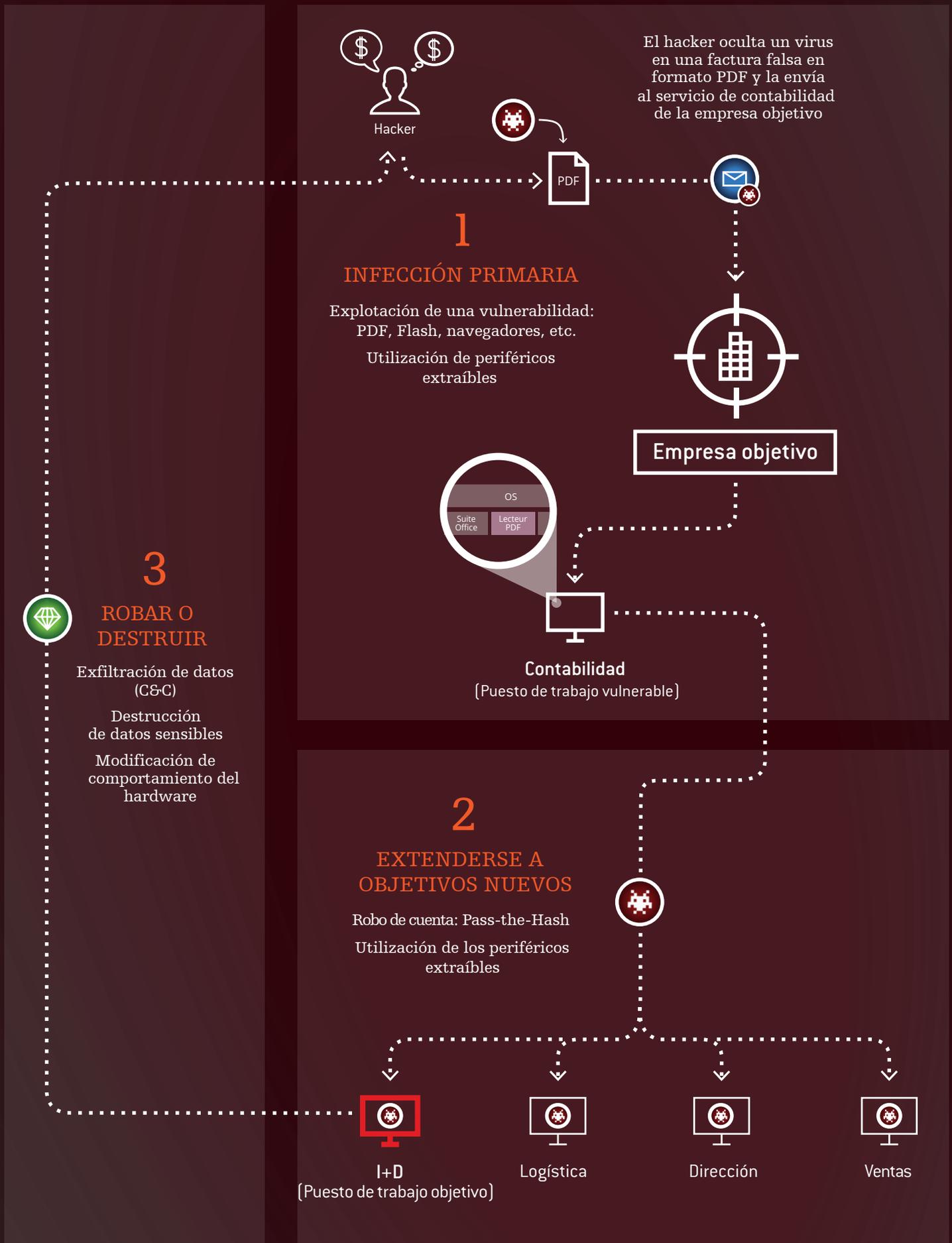
Coste de las inversiones en herramientas tradicionales de seguridad en 2014

53 %

Aumento del coste financiero de las intrusiones en 1 año

(Fuente: Global State of Information Security Survey)

Funcionamiento de los Ataques Avanzados Dirigidos (Advanced Targeted Attacks – ATA)



Stormshield Endpoint Security le protege contra los Ataques Avanzados Dirigidos (ATA)



Hacker



El hacker oculta un virus en una factura falsa en formato PDF y la envía al servicio de contabilidad de la empresa



1

PROTEGER CONTRA LOS ATAQUES DESCONOCIDOS

Nuestra protección única bloquea los ataques desconocidos de manera proactiva, por ejemplo, detectando la explotación de una vulnerabilidad.



Empresa objetivo



Contabilidad

3

PROTEGER Y PRESERVAR LOS DATOS

Stormshield Endpoint Security integra una amplia gama de protecciones, tanto de base de firmas como de análisis de comportamientos, encaminados a detectar las transferencias de datos o las manipulaciones indeseables.



2

BLOQUEAR LA PROPAGACIÓN DE LA AMENAZA

Stormshield Endpoint Security le permite evitar el robo de datos de cuenta mediante un control meticuloso de las operaciones realizadas en el disco duro, en las memorias USB, en el registro o incluso en los procesos del sistema operativo.



I+D



Logística



Dirección



Ventas

SÉCURIÉ

La protección total y probada de los servidores y los terminales

Stormshield Endpoint Security 2 productos



FULL PROTECT

El producto Full Protect se caracteriza por tener una tecnología proactiva única, sin firmas, que brinda una protección eficaz contra los ataques desconocidos y sofisticados.

PROTECCIÓN CONTRA LAS AMENAZAS DESCONOCIDAS

- Protección contra la explotación de vulnerabilidades del sistema operativo
- Protección contra la explotación de vulnerabilidades de las aplicaciones de terceros
- Control de la integridad de la memoria del sistema

PROTECCIÓN DEL PUESTO DE TRABAJO

- Detección de programas maliciosos mediante el análisis de comportamiento
- Endurecimiento del sistema operativo
- Control aplicativo (mediante listas blancas y listas negras)
- Control meticuloso de los derechos de usuario
- Control meticuloso de la exfiltración de datos sensibles

PREVENCIÓN DE INTRUSIONES

- Cortafuegos
- Detección de intrusiones en la red



FULL CONTROL

El producto Full Control permite definir, de manera detallada, la protección de los puestos de trabajo dentro de un marco de utilización conforme a la política de seguridad de la empresa.

CONTROL Y AUDITORÍA DE LOS PERIFÉRICOS

- Autorización o bloqueo de un periférico por su tipo o número de serie
- Bloqueo o restricción de diferentes operaciones de utilización del periférico
- Protección contra infecciones de periféricos externos (por ejemplo, una memoria USB infectada)
- Seguimiento de los archivos cargados en un periférico específico y/o por un usuario específico
- Evaluación de transferencias de archivos (apropiadas o no)

CONTROL DE LAS COMUNICACIONES

- Cortafuegos
- Puesta en cuarentena de los ordenadores infectados
- Autorización de las zonas sensibles WI-FI públicas únicamente si el Cliente VPN corporativo está activo
- Lista blanca de los puntos de acceso WI-FI de la empresa
- Imposición de las normas de seguridad WPA/WPA2
- Prohibición de WI-FI en modo ad hoc

Los dos productos pueden estar activados en la misma consola de gestión y en el mismo agente.

OPCIONES ADICIONALES DISPONIBLES

ANTIVIRUS

ANTIVIRUS A BASE DE FIRMAS

- Análisis de archivos en tiempo real o por solicitud
- Análisis de los mensajes de correo electrónico antes que lleguen a los buzones
- Análisis del tráfico de Internet
- Gestión del módulo con total transparencia desde la consola de gestión

ENCRIPCIÓN

CIFRADO DE DATOS

- Cifrado del disco con autenticación pre-boot
- Autenticación única (SSO) con la sesión Windows
- Administración centralizada, segregación de los roles
- Eliminación segura de los archivos

MONITORIZACIÓN DE SEGURIDAD

OFERTA DE SERVICIO DE VIGILANCIA AVANZADA

- Análisis de las vulnerabilidades que afectan los sistemas operativos o las aplicaciones
- Envío periódico de un informe de análisis certificando el nivel de protección efectivo
- Suministro de recomendaciones para lidiar con los eventuales riesgos residuales
- Respuesta eficaz para los sistemas operativos que ya no son compatibles



STORMSHIELD



Stormshield ofrece soluciones innovadoras de seguridad de extremo a extremo en todo el mundo para proteger las redes (Stormshield Network Security), los puestos de trabajo (Stormshield Endpoint Security) y los datos (Stormshield Data Security).

WWW.STORMSHIELD.EU

Version 2.2 - Copyright Stormshield 2016