Hornetsecurity Advanced Threat Protection

Detectar y evitar ataques inteligentes y de gran complejidad de forma efectiva y en tiempo real.

Proteja con Hornetsecurity ATP a su compañía frente a ataques dirigidos e individuales desde el primer mensaje de correo electrónico malicioso. Motores de análisis forense altamente innovadores se encargan de evitar los ataques de forma inmediata. Al mismo tiempo la solución ofrece información detallada acerca de los ataques a la compañía.

Protección frente al ransomware

Desde comienzos de 2016 el ransomware está en auge: Aquí se trata de virus que bloquean la terminal o una red informática por completo mediante el cifrado de los archivos almacenados a nivel local. Solo mediante el pago de un rescate, de ahí su nombre, los usuarios podrán volver a tener acceso a sus datos. Locky, Tesla, Petya y compañía son virus polimórficos muy difíciles de detectar. Hornetsecurity ATP utiliza para ello, entre otros, un motor para el aislamiento de procesos con el fin de analizar el comportamiento de los archivos adjuntos al abrirlos y filtrar los mensajes de correo electrónico en caso de que el resultado del análisis sea positivo. Además de esto, Hornetsecurity "congela" los mensajes de correo electrónico sospechosos para volver a escanearlos una vez transcurridos unos pocos minutos, cuando haya actualizado la signatura del filtro.

Protección frente a Blended Attacks

Los Blended Attacks combinan diferentes formas de ataque para tener éxito. El correo electrónico puede contener, por ejemplo, un archivo adjunto en el cual se ocultan, a su vez, un enlace que dirige a una página web de descarga con malware. Hornetsecurity ATP combate este tipo de ataques mediante el escaneo y la reescritura de las URL, pero, además de esto, aquí también entra en acción el aislamiento de procesos y la "congelación".

Protección frente a ataques dirigidos

Con frecuencia, los empleados de alto rango de la compañía son el objetivo de ataques individuales, los conocidos como Spearphishing, Whaling o también fraude del CEO. Los atacantes intentan aquí acceder a contraseñas o datos de tarjetas de crédito, o lograr que los empleados efectúen una transferencia a una cuenta específica. Es prácticamente imposible detectar estos ataques por medios convencionales. Con Hornetsecurity ATP, la comunicación interna entre personas específicas de la compañía se comprueba de forma dirigida en busca de este tipo de ataques y, de esta forma, se impide el uso indebido por falsificación de la identidad.

Protección frente al espionaje digital

Según una encuesta de la organización profesional de informática Bitkom, más de la mitad de las empresas alemanas han sido objeto del robo de datos, sabotaje o espionaje. El Sistema Forense Spy-Out de Hornetsecurity reconoce patrones de piratería informática tanto conocidos como completamente nuevos. El sistema reacciona instantáneamente y alarma al empleado antes de que la información digna de ser protegida salga de la empresa.

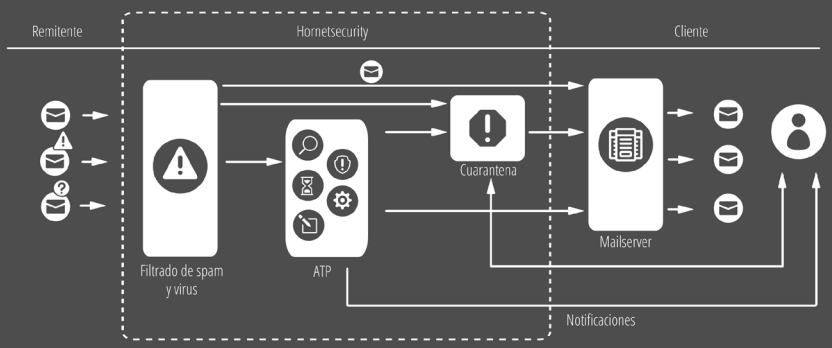
Notificación en caso de ataques

Las alertas en tiempo real de Hornetsecurity notifican en tiempo real los ataques agudos sobre la empresa y posibilitan la pronta adopción de medidas internas adicionales y de procedimientos jurídicos. Para ello, el sistema de notificación ofrece resultados detallados del análisis. Asimismo, el equipo de seguridad del cliente puede concienciar a los empleados para que puedan reconocer otras vías de ataque como, por ejemplo, telefónicas. Si se reconocen con posterioridad correos electrónicos ya recibidos como potencialmente maliciosos, la alarma Ex-Post posibilita al equipo de seguridad técnica la comprobación de las cuentas o sistemas afectados.

Integración de Hornetsecurity ATP en la Gestión de Seguridad del Correo electrónico.

Hornetsecurity ATP se integra perfectamente en los filtros antispam y antivirus. Los mensajes de correo electrónico que hayan superado esta primera comprobación, serán sometidos a análisis posteriores por parte de Hornetsecurity ATP. Aquí, el sistema ejecuta archivos adjuntos, entre otros, y observa detalladamente su comportamiento.

Fig.: proceso del filtro antispam y antivirus con Hornetsecurity ATP



HORNETSECURITY®

Hornetsecurity Advanced Threat Protection - Real Time Alert

The Hornetsecurity Advanced Threat Protection Service has just detected the following email attack:

Classification:

User:	accounting@hornetsecurity.com
Date:	08/19/2016 06:38 PM CEST
Sender:	phisher@hackeddomain.com, phisher@hackeddomain.com
Server Address:	123.123.123.123, relay42.hackerserver.com
Reason:	Hornet-ATP02
URL:	http://bit.ly/axJoQXLn

Notificaciones en tiempo real

Tan pronto como Hornetsecurity ATP detecta un ataque, se envía una notificación al equipo de seguridad técnica de la compañía para informarle inmediatamente acerca de una posible amenaza. Aquí, la persona encargada recibe diferentes detalles acerca del tipo y el objetivo del ataque, del remitente y de la causa por la que se interceptó dicho mensaje de correo electrónico.

Fig.: notificación en tiempo real de Hornesecurity

Motores de Hornetsecurity ATP	Funcionamiento y ventajas
Motor del entorno de aislamiento de procesos	Los archivos adjuntos se ejecutan en una multitud de entornos de sistema diferentes y se analiza su comportamiento. Si se determina que se trata de un malware, el cliente será notificado al respecto. Esto ofrece protección frente a ransomware y Blended Attacks.
Reescritura de las URL	El motor de reescritura de URL asegura todos los accesos a Internet desde los mensajes de correo electrónico a través del filtro web de Hornetsecurity. Aquí el motor del entorno de aislamiento de procesos también analiza las descargas.
Escaneo de las URL	En un documento adjunto en un mensaje de correo electrónico (p. ej., un PDF o un documento de Microsoft Office) puede haber enlaces. Estos no pueden sustituirse, pues dicha acción podría dañar la integridad del documento. El motor de escaneo de URL de Hornetsecurity conserva el documento en su forma original y comprueba, a continuación, el destino de estos enlaces.
Congelación	Los mensajes de correo electrónico que no puedan clasificarse inmediatamente de forma inequívoca, pero que sean sospechosos, quedan bloqueados mediante la "congelación" durante un breve periodo de tiempo. A continuación, tiene lugar una comprobación adicional con signaturas actualizadas. Esto ofrece protección frente a ransomware, Blended Attacks y ataques de Phishing.
Alarma Ex-Post (todavía no está disponible)	Si se determinase a posteriori que un mensaje de correo electrónico previamente entregado debe clasificarse como malicioso, el equipo de seguridad técnica de la compañía recibirá inmediatamente una notificación acerca de la magnitud y las posibles contramedidas. Esto permite una rápida contención de una situación potencialmente peligrosa.
Targeted Fraud Forensics	El Targeted Fraud Forensics detecta los ataques dirigidos y personalizados sin malware o enlaces. Para ello se utilizan aquí los siguientes mecanismos de detección: • Intention Recognition System: alarma en caso de patrones de contenido que indiquen una intencionalidad maliciosa • Fraud Attempt Analysis: comprueba la autenticidad y la integridad de los metadatos y de los contenidos de los mensajes de correo • Identity Spoofing Recognition: reconocimiento y bloqueo de remitentes con identidades falsificadas • Spy-Out Detection: contraespionaje para ataques que intenten obtener información valiosa • Feign Facts Identification: análisis del contenido de los mensajes en base a la pretensión de hechos falsos • Targeted Attack Detection: reconoce los ataques dirigidos a personas individuales