HORNETSECURITY

FACT SHEET

ADVANCED THREAT PROTECTION

Contrarrestar las amenazas modernas con los mecanismos de defensa más avanzados

El riesgo de un ataque cibernético de secuestro de datos, fraude del CEO y troyanos aumenta cada vez más. Protege tu empresa de los devastadores ataques de malware con IAdvanced Threat Protection (ATP).

protección contra:

- **Ransomware**
- **Blended Attacks**
- **Targeted Attacks**
- **espionaje digital**

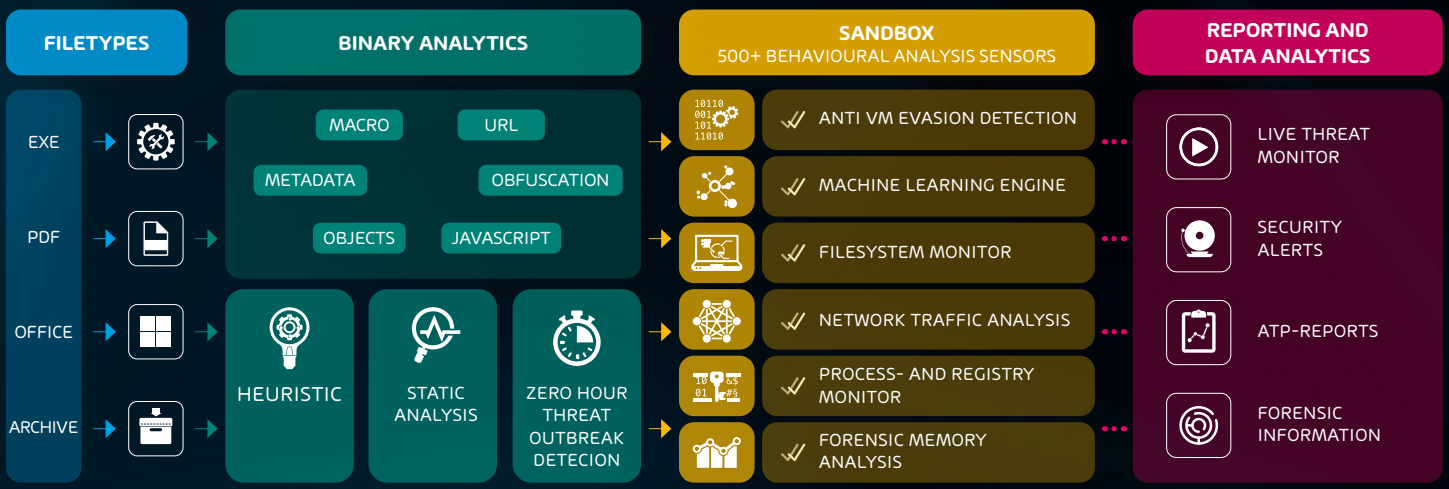
Mecanismos de protección contra el fraude

- Análisis de los correos electrónicos fraudulentos en cuando **a contenido y a nivel meta**
- Análisis de los **datos de transporte SMTP** en el contexto de la estructura de gestión de una empresa
- Las solicitudes de fondos/información crítica sólo se permiten de fuentes internas de la empresa
- Los correos electrónicos externos con remitentes que se hacen pasar por gerentes se bloquean.

Mecanismos de protección contra el secuestro de datos

- **ATP Sandbox** utiliza las bases de datos de Threat Intelligence para analizar los archivos adjuntos de los correos electrónicos
- Los **Indicators of Compromise (IoC)** almacenados se clasifican utilizando más de 50 motores antivirus disponibles en el mercado
- Enriquecimiento de los análisis con información sobre sumas de hash ya conocidas (por ejemplo, de adjuntos defectuosos o direcciones IP que están en contexto con entidades maliciosas)
- **En 2018, sólo alrededor del 5 % de los IoCs para nuevas campañas de secuestro de datos se evaluaron negativamente por los motores antivirus convencionales en la primera aparición de un secuestro de datos.**
- **Alarma en tiempo real: Notificación en tiempo real a los equipos de seguridad informática sobre los ataques graves a la empresa. Contiene información detallada sobre el tipo y el alcance del ataque.**

Imagen: Advanced Threat Protection Sandbox vs. Ransomware y virus polimórficos



HORNETSECURITY

FACT SHEET

ATP-Engines	Funcionalidad y ventajas
Sandbox Engine	Los archivos adjuntos de los correos electrónicos se analizan en busca de posibles códigos maliciosos ejecutando el archivo sospechoso en un entorno de prueba virtual e identificando los efectos potencialmente peligrosos. Si se descubre que el documento enviado con el correo electrónico es malware, el correo se traslada directamente a la cuarentena.
URL Rewriting	Asegura todas las visitas de internet de los correos electrónicos a través del filtro web. El „análisis del tiempo de clic" asegura toda la sesión del usuario que sale del enlace en el correo electrónico en vivo.
URL Scanning	Deja el documento adjunto a un correo electrónico en su forma original y sólo comprueba el destino de los enlaces contenidos en él.
Freezing	Los correos que no se pueden clasificar claramente de inmediato, pero los que son sospechosos, se retienen durante un corto período de tiempo. El correo electrónico corporativo se somete a una nueva revisión con firmas actualizadas.
Malicious Document Decryption	Los archivos adjuntos codificados de los correos electrónicos se descifran mediante módulos de texto adecuados dentro de un correo electrónico. Por último, el documento desencriptado se somete a un análisis de virus más profundo.
Targeted Fraud Forensics	El análisis forense de fraudes selectivos se identifican los ataques personalizados sin malware ni enlaces. Se utilizan los siguientes mecanismos de detección: **Intention Recognition System:** Alerta sobre patrones de contenido que indican una intención maliciosa. **Fraud Attempt Analysis:** Comprueba la autenticidad e integridad de los metadatos y el contenido del correo. **Identity Spoofing Recognition:** Detección y bloqueo de identidades falsas de remitentes. **Spy-Out Detection:** Defensa contra ataques de espionaje de información confidencial. **Feign Facts Identification:** Análisis del contenido del mensaje independientemente de la identidad, para identificar datos ficticios **Targeted Attack Detection:** Detección de ataques dirigidos a personas particularmente vulnerables.