PANDA CLOUD INTERNET PROTECTION

Simply... Evolution

AMENAZAS AVANZADAS Y PERSISTENTES

PANDA CLOUD OFFICE PROTECTION

PANDA CLOUD EMAIL PROTECTION

PANDA CLOUD INTERNET PROTECTION

PANDA SECURITY

INDICE

1

INTRODUCCIÓN 2
- CRONOLOGIA 2
- ATACANTES 2
- OBJETIVOS 2

FASES 2
- RECONOCIMIENTO 2
- ATAQUE INICIAL 2
- RECOPILACIÓN DE INFORMACIÓN 2
- ATAQUES POSTERIORES 2

¿CÓMO PROTEGE PANDA CLOUD INTERNET PROTECTION (PCIP) CONTRA LAS APTS? 3

CONTROLES PREVENTIVOS 3
- ANTIVIRUS/ANTI-SPYWARE 3
- INSPECCIÓN TOTAL DE CONTENIDOS 3

CONTROLES DE DETECCIÓN 3
- CONSOLIDACIÓN DE LOGS 3
- COMUNICACIONES SOSPECHOSAS 3
- ANÁLISIS FORENSE 3

SUITE PANDA CLOUD PROTECTION 4

INTRODUCCIÓN

Aunque no existe una definición universalmente aceptada de las Amenazas Avanzadas y Persistentes (APT, por sus siglas en inglés), tales ataques tienen las siguientes características:

- **Cronología:**
  Los ataques tienen lugar a lo largo de un período prolongado de tiempo. A menudo duran meses o incluso años y normalmente están precedidos de una fase importante de reconocimiento anterior a la infiltración en el sistema.

- **Atacantes:**
  Tienen altos conocimientos técnicos, están bien y organizados y disponen de fondos económicos. Se ven a menudo respaldados por organizaciones criminales o gobiernos extranjeros que apoyan sus actividades, por los que el acceso a los recursos que necesitan no supone un problema.

- **Objetivos:**
  Los usuarios domésticos son su objetivo, a menudo mediante ataques Web. La ingeniería social juega un papel importante en sus acciones, junto con una fase importante de reconocimiento. Esto se combina a menudo con exploits de carácter técnico que combinan vectores de ataque conocidos y desconocidos.

FASES

Las fases de los ataques dependen de la situación específica, pero en general son las siguientes:

- **Reconocimiento:**
  El objetivo de esta fase es recopilar información sobre los objetivos. Dicha información ayudará a diseñar los aspectos técnicos y sociales de los ataques iniciales y de cualquier otro ataque posterior. Puede incluir tanto información personal como profesional. Esta información puede ser obtenida mediante la monitorización pasiva de fuentes públicas o semi-públicas como las redes sociales. También podría implicar un reconocimiento activo mediante el ataque a otros objetivos o a través de técnicas de inteligencia.

- **Ataque inicial:**
  El objetivo del ataque inicial es penetrar en la organización atacada. Esto generalmente implica la instalación de un backdoor en la máquina de la víctima y de herramientas adicionales tales como keyloggers y otras utilidades. Esto permite la recogida de información así como la realización de nuevos ataques.

- **Recopilación de información:**
  El propósito real de una APT es normalmente obtener información confidencial con el objetivo de obtener un beneficio económico o político o llevar a cabo nuevos ataques. La información que se obtiene es enviada al exterior, normalmente al servidor de un tercero controlado por el atacante. La recogida de información continúa hasta que se alcanza el objetivo final, o indefinidamente obteniendo nueva información hasta que se identifica y elimina el ataque.

- **Ataques posteriores:**
  Desde el foco del ataque inicial es posible comprometer nodos adicionales como máquinas en la misma red local, oficinas remotas o redes de partners de confianza. máquina de la víctima y de herramientas adicionales tales como keyloggers y otras utilidades. Esto permite la recogida de información así como la realización de nuevos ataques.

¿CÓMO PROTEGE PANDA CLOUD INTERNET PROTECTION (PCIP) CONTRA LAS APTS?

No existe una solución infalible cuando se trata de proteger contra las APTs. Las empresas deben adoptar una estrategia de "defensa en profundidad" en la que diversas capas de protección protejan contra los diversos tipos de ataques. PCIP ofrece diversos controles preventivos y de detección contra todo tipo de amenazas, incluyendo las APTs.

CONTROLES PREVENTIVOS

En un caso reciente de APT, la Operación Aurora, se utilizó un exploit anteriormente desconocido contra un navegador vulnerable. PCIP permite a los clientes personalizar políticas que impidan a versiones vulnerables de sus navegadores o a plug-ins vulnerables de los mismos acceder a Internet. Una vez se hizo público el exploit, PCIP distribuyó identificadores a la nube para impedir la amenaza (que posteriormente se incluyó en Metasploit, una conocida plataforma de ataque). PCIP ofrece los siguientes tipos de protección para detectar y bloquear las amenazas de Internet:

- **Antivirus/Anti-spyware :**
  Análisis online de alta velocidad que impidlas infecciones causadas por variantes conocidas de malware.

- **Inspección total de contenidos:**
  Inspección SSL, completa y bidireccional de todo el contenido Web que identifica el contenido activo malicioso.

  - Ataques a exploradores
  - Controles ActiveX vulnerables
  - JavaScript malicioso
  - Cross-site scripting (XSS)

El espionaje o el robo de información secreta es uno de los factores habituales que motivan la aparición de amenazas avanzadas y persistentes. Existen varios ejemplos de este tipo de amenazas que han sido promovidas por distintos gobiernos, como Titan Rain. PCIP ofrece Protección contra la Fuga de Datos (DLP, por sus siglas en inglés), que bloquea la salida de cierto contenido al exterior y alerta a los clientes sobre el mismo.

Además, PCIP ofrece controles basados en políticas que permiten neutralizar las amenazas Web. Por ejemplo, un cliente puede bloquear las comunicaciones Web con ciertos países, así como ciertas IPs, URLs, o clasificar contenido relacionado con cierto enemigo o amenaza.

CONTROLES DE DETECCIÓN

- **Consolidación de logs:**
  PCIP ofrece a los clientes una visión completa de los logs Web de toda su empresa independientemente de la fuente del tráfico, incluyendo los portátiles de los clientes y los dispositivos que se conectan a Internet desde fuera de la red corporativa. PCIP ofrece una interfaz analítica que permite a los clientes hacer consultas, monitorizar tendencias y ver logs de interés, actividades críticas para la detección de incidencias continuadas.

- **Comunicaciones sospechosas:**
  Las amenazas avanzadas y persistentes incluyen malware que se conecta a servidores de control para la recepción de instrucciones adicionales, o para el envío de los documentos robados y pulsaciones del teclado. Estos patrones de tráficos son detectados en los logs de PCIP, que puede neutralizar así infecciones no identificadas previamente. Los investigadores de PCIP permanecen siempre en guardia para detectar amenazas dirigidas a sus bases de clientes.

- **Análisis forense:**
  Las herramientas de registro y utilidades analíticas de PCIP ofrecen a los clientes un histórico de todas las transacciones Web. En caso de que se detecte una incidencia, los clientes pueden analizar los logs y detectar las acciones realizadas por el host infectado así como detectar otras infecciones y amenazas potenciales.

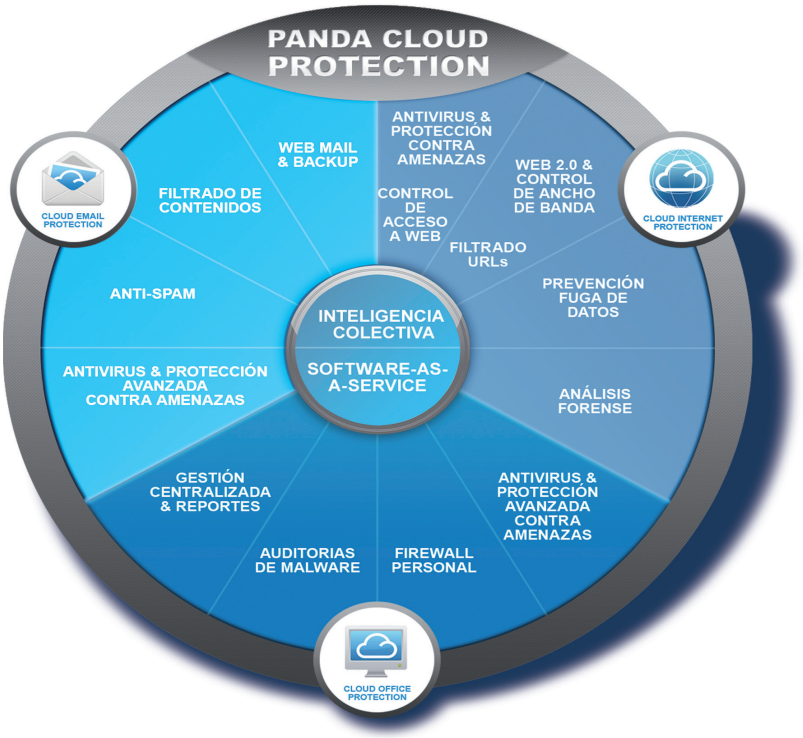
SUITE PANDA CLOUD PROTECTION

Panda Cloud Internet Protection es parte de la suite Panda Cloud Protection, una completa solución de seguridad SaaS que protege los principales puntos de entrada de amenazas -endpoints, correo electrónico y tráfico Web- contra el malware, spam, cross-site scripting y otros ataques avanzados de Web 2.0, mediante una solución ligera, segura y sencilla.

Esta suite de seguridad está basada en la nube, ofreciendo máxima protección, reduciendo el gasto y aumentando la productividad. La solución se despliega en cuestión de minutos y se gestiona de forma sencilla gracias a la intuitiva Consola de Administración en la Nube única de Panda.

La suite Panda Cloud Protection se beneficia de la gran capacidad de la Inteligencia Colectiva: un sistema basado en la nube que almacena 21 terabytes de conocimiento y experiencia obtenidos directamente de millones de usuarios. Panda Cloud Protection ofrece protección completa para el mundo real, no intrusiva e instantánea contra el malware conocido y desconocido.

Panda Cloud Protection explota el poder de la nube y proporciona protección en tiempo real contra las amenazas conocidas y desconocidas en cualquier momento y en cualquier lugar, gracias a su Consola de Administración en la Nube.



PANDA SECURITY

EUROPE
Ronda de Poniente, 17
28760 Tres Cantos. Madrid. SPAIN

Phone: +34 91 806 37 00

USA
230 N. Maryland, Suite 303
P.O. Box 10578. Glendale, CA 91209 - USA

Phone: +1 (818) 5436 901

www.pandasecurity.com

PANDA SECURITY