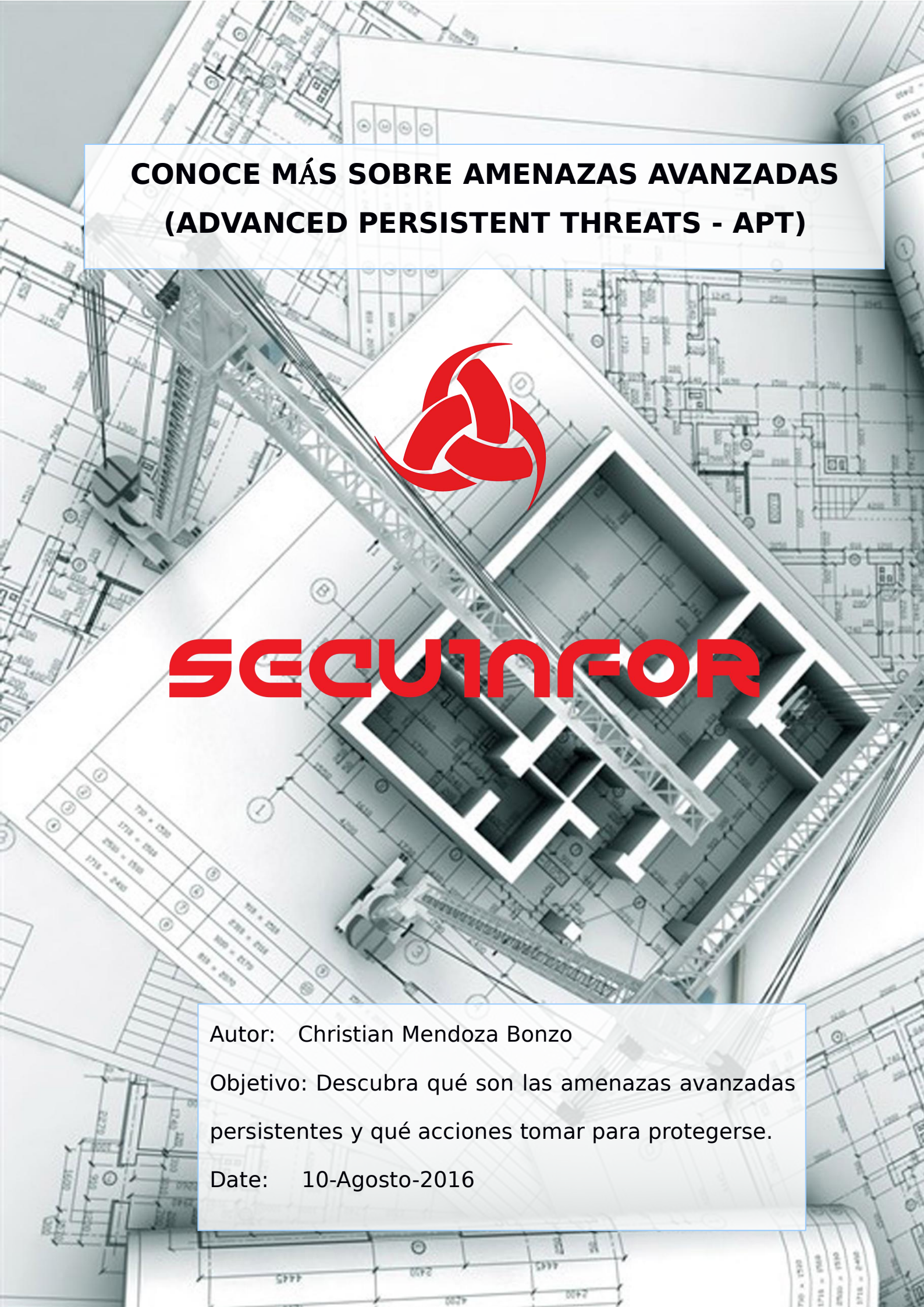
CONOCE MÁS SOBRE AMENAZAS AVANZADAS (ADVANCED PERSISTENT THREATS - APT)



SECUINFOR

Autor: Christian Mendoza Bonzo

Objetivo: Descubra qué son las amenazas avanzadas persistentes y qué acciones tomar para protegerse.

Date: 10-Agosto-2016

Una amenaza avanzada persistente (Advanced Persistent Threat-APT), es un ataque muy elaborado, digirido a la infraestructura tecnológica de una organización, en el cual una persona sin autorización obtiene acceso a los sistemas tecnológicos y permanece por un periodo largo de tiempo sin ser detectado.

El propósito de un atacante de APT, es tomar ventaja o robar información en lugar de causar daño o afectación sobre los sistemas informáticos de la organización. Estos ataques de APT se dirigen a organizaciones en sectores estratégicos o con información de alto valor económico para el atacante, tales como: defensa nacional, sistemas financieros, industrias farmacéuticas, empresas de marketing, entre otros.

En los ataques tradicionales, un intruso intenta entrar y salir tan rápido como le sea posible con el fin de evitar ser detectado por algún sistema de seguridad informática; sin embargo, en un ataque de APT el objetivo no es entrar y salir, sino por el contrario permanecer de forma indetectable, valiéndose de las debilidades en los sistemas en conjunto con herramientas y varias técnicas avanzadas.

Para permanecer el mayor tiempo posible sin ser detectados y obtener información valiosa los atacantes utilizan una combinación de técnicas o herramientas como las siguientes:

√ **Spear Phishing:** Es una nueva sub-categoría del phishing, en otras palabras, es una suplantación de identidad dirigida a un grupo u organización específicos.

√ **Malware:** Es el nombre genérico que se le da a un programa informático malicioso, antes de ser catalogado según sus características como virus, troyano, gusano, etc. El atacante usualmente utiliza dos piezas de software malicioso, una para evadir los mecanismos de control y otra para mantener los accesos y filtrar información.

√ **DoS o DDoS:** Son el acrónimo para Denegación de servicio (Denial of Service) o Denegación de Servicio Distribuida (Distributed Denial of Service), estos ataques provocan daño o afectación sobre la infraestructura de una organización, los atacantes ofrecen estos ataques como servicio a las empresas que desean captar nuevos clientes de forma no ética o como mecanismo de distracción para efectuar otros ataques.

√ **Ingeniería Social:** Es una de las herramientas más poderosas de los hacker o hacktivistas, consiste en obtener datos que al procesarlos o unirlos se convierten en información de mucho valor, un ejemplo de esto puede ser cuando se encuentra en reunión y uno de sus colegas le pregunta cuántos caracteres tiene su clave y si usted usa letras y números; a pesar de no preguntar la contraseña, con esos simples datos es posible deducir su

contraseña.

QUÉ HACER PARA PROTERGERNOS

Cuando se habla de seguridad, en realidad se mencionan varias cosas que las personas no comprenden, esto se debe a que tienen en su mente una solución sencilla, rápida que aspiran funcione para todos los casos, sin embargo esto está lejos de la realidad, la seguridad o protección de la información nunca será absoluta, es decir que siempre existirá algo que no está protegido o nos falta por proteger, de ahí se puede mencionar que la seguridad es un proceso continuo de mejora en los mecanismos de protección, en donde intervienen estrategias, políticas, herramientas.

Entonces ¿qué podemos hacer? Se estará preguntado ¿por dónde podemos iniciar? Vamos a listar una serie de iniciativas que le permitirán tomar acciones sobre las amenazas avanzadas:

- √ **Crear una política de seguridad:** esto le permitirá gestionar y administrar adecuadamente la inversión necesaria en seguridad.
- √ **Cree una estrategia de seguridad:** le permitirá conocer qué hacer ante ciertos ataques.
- √ **Efectúe monitoreo continuo:** conozca el comportamiento y tendencias de su infraestructura.
- √ **Efectúe aseguramiento:** sobre su infraestructura o sistemas críticos exigiendo que le mencionen contra qué tipos de ataques lo están protegiendo.
- √ **Cree campañas de concientización:** a nivel organizacional, sus colaboradores conocerán más de seguridad y serán menos propensos a fraudes.
- √ **Implemente o sub-contrate mecanismos de protección:** seguridad perimetral, prevención de intrusos, anti-virus, anti-malware, navegación segura, prevención de fuga de información, entre otros.
- √ **Saque provecho a sus herramientas de seguridad:** Añada inteligencia o correlación, le permitirá estar una paso adelante de los atacantes.

Si desea conocer cómo podemos ayudarlo a proteger su información confidencial contáctenos a:

Email: info@secuinfor.com
PBX: +593-4-3726620
Website: http://www.secuinfor.com