Píldora Informativa

GPIT

HONEYTOKEN

No. 004

Universidad Nacional Abierta y a Distancia

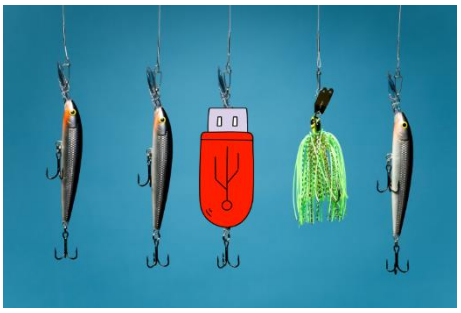
Fuente de autor:
https://cuadernosdeseguridad.com/2022/10/trucos-evitar-ataques-ingenieria-social/

UNAD

GRUPO FUNCIONAL DE SEGURIDAD INFORMATICA - GFSI

28/10/2022

HONEYTOKEN QUE ES Y PARA QUE SIRVE?



Fuente: https://www.redseguridad.com/actualidad/ciberc rimen/baiting-que-es-y-como-evitar-este-ataque-informatico-de-ingenieria-social_20210628.html

Se define como un señuelo para un intruso, tiene la función de detectar el uso indebido de datos lo cual significa tener un enfoque de prevención y no de disuasión.

Existe una variedad ilimitada de HONEYTOKEN y puede ser:

- Un archivo
- Una carpeta
- Un programa
- Hoja de cálculo Excel
- Presentación Power Point
- Documento de texto Microsoft
- Un enlace o un nombre de usuario
- Los datos de una tarjeta bancaria
- Cualquier otra entrada de una base de datos

HONEYTOKEN O CANARYTOKEN

Es un archivo, URL clave de API u otro recurso cuyo acceso se supervisa. Una vez que se ha accedido al recurso, se activa una alarma notificando dicho acceso al propietario del objeto, permite a los administradores identificar a quien se los robaron o como se filtraron. Todo lo creado por HONEYTOKEN no debe ser utilizado por ninguno de los usuarios legítimos, cualquier interacción con este señuelo constituye una actividad no autorizada o maliciosa. Esto convierte a los HONEYTOKEN la misma potencia y ventajas que los sistemas de detección tradicionales y amplia sus capacidades más allá de los ordenadores físicos.

ORIGEN

Se remonta a la utilización de canarios en sus jaulas en las minas a fin de detectar el peligro como medida de prevención para los mineros, esto gracias al sistema respiratorio de las aves que es más sensible que los de los humanos y podían detectar hasta la más mínima cantidad de gas tóxico. Cuando se desplazaban los mineros o trabajaban en la mina vigilaban el comportamiento de las aves, si se contonear o se caía, el trabajador salía a la superficie como medida de protección. En la actualidad la tecnología mediante los HONEYTOKEN permite detectar a los hackers en una fase temprana.

VENTAJAS DE LOS HONEYTOKEN

Como es bien sabido las cuentas de correo electrónico falsas han sido utilizadas para capturar o dar una alerta temprana a los Spammers. Muchas empresas crean cuentas de correo falsas y las dejan a la vista ya sea en el servidor de correo o colocándolas en lugares privados del servidor web. La idea es que la dirección web nunca se utilizará y por tanto no habrá razón para recibir spam. La recepción

de un mensaje no verificado en una dirección de correo señuelo significa que alguien ha accedido a la lista de correo interno de la empresa o ha pirateado el servidor web. Lo mismo puede hacerse con una estructura bancaria, estos Honeytoken serian números únicos, o datos bancarios, cuyo uso permitiría detectar un intruso. Las bases de datos pueden controlar los intentos de acceso a los registros y enviar una alerta de seguridad.

Los HONEYTOKEN recogen información sobre el atacante y permite averiguar, por ejemplo:

- La dirección IP de la persona que accedió al señuelo
- Fecha y hora del acceso no autorizado
- Ubicación (ciudad-país)
- Sistema operativo
- El dispositivo desde el cual se realizó el acceso
- Y otra información importante

Los HONEYTOKENS son una de las herramientas de ciberseguridad más sencillas, rentables y flexibles que existen. Puede ser utilizados por los usuarios ordinarios, para determinar si un ordenador ha sido comprometido no, así como por las organizaciones para advertir sobre una filtración en la base de datos.

HONEYPOT Y HONEYTOKEN

En ciberseguridad, la postura defensiva que adoptan las organizaciones se traduce en una forma de protegerse de los atacantes, participando en una persecución de alta tecnología para encontrar y atrapar a los ciberdelincuentes. Los HONEYTOKENS y HONEYPOTS representan una táctica claramente diferente. Las organizaciones las utilizan como herramientas para contratacar; persiguen a los ciberdelincuentes engañándolos para que se revelen a sí mismos y revelen información sobre sus métodos.

Los HONEYPOT es un sistema falso desplegado junto a sus activos digitales genuinos. Se hace para que parezca atractivo para los atacantes y permite que el criminal caiga en la trampa, no solo desperdicia sus recursos en un sistema inútil o en datos falsos, sino que permite revelar información crucial sobre la naturaleza de su estrategia de ataque.

Por otra parte, los HONEYTOKEN son una forma de identificar a sus atacantes, rastrea los actores maliciosos y permiten acceder a información crítica sobre su identidad y los métodos que utilizan para explotar un sistema.