**Indicadores de compromiso**

En esta lectura, se te presentará el concepto de la pirámide del dolor y explorarás ejemplos de los diferentes tipos de indicadores de compromiso. Entender y aplicar este concepto ayuda a las organizaciones a mejorar su defensa y reduce el daño que un incidente puede ocasionar.

**Indicadores de compromiso**

Los **indicadores de compromiso** (**IoC**) son evidencias observables que sugieren indicios de un posible incidente de seguridad. Los IoC trazan piezas específicas de evidencia que están vinculadas con un ataque, como un nombre de archivo asociado con un tipo de malware. Se puede pensar en un IoC como evidencia que apunta a algo que ya ha sucedido, como notar que un objeto de valor ha sido robado del interior de un automóvil.

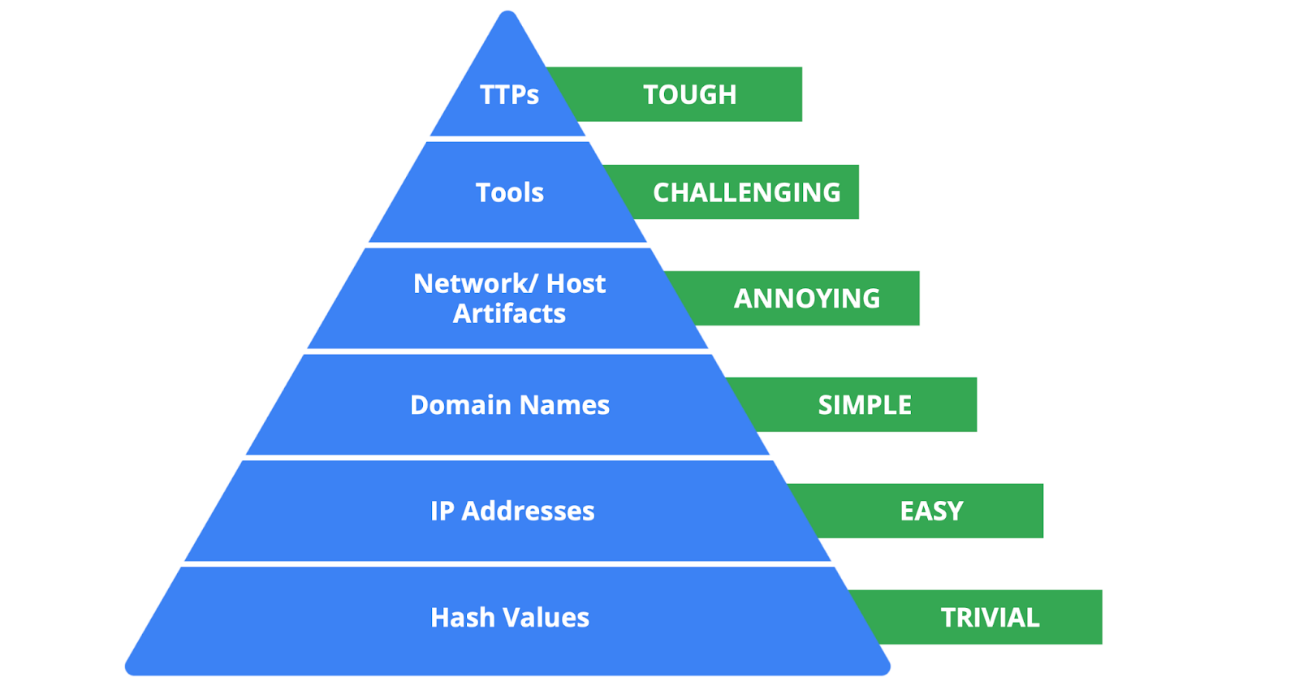
Los **indicadores de ataque** (**IoA**) son la serie de eventos observados que indican un incidente en tiempo real. Los IoA identifican el comportamiento de un atacante, incluidos sus métodos e intenciones.

Esencialmente, los IoC ayudan a identificar el *quién* y el *qué* de un ataque después de que haya tenido lugar, mientras que los IoA se centran en encontrar el *por qué* y el *cómo* de un ataque en curso o desconocido. Por ejemplo, observar un proceso que establece una conexión de red es un ejemplo de un IoA. El nombre de archivo del proceso y la dirección IP con la que se contactó el proceso son ejemplos de los IoC relacionados.

**Nota**: Los indicadores de compromiso no siempre son una confirmación de que ha ocurrido un incidente de seguridad. Los IoC pueden ser el resultado de errores humanos, mal funcionamiento del sistema y otras razones no relacionadas con la seguridad.

**Pirámide del dolor**

No todos los indicadores de compromiso son igual de importantes para los profesionales de seguridad y es clave que los conozcan en detalle, para poder detectarlos y responder a ellos de manera rápida y efectiva. Es por esto que el investigador de temas de seguridad David J. Bianco creó el concepto de la [pirámide del dolor](http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html), que tiene el objetivo de mejorar la forma en que se utilizan los indicadores de compromiso en la detección de incidentes.



La pirámide del dolor establece la relación entre los indicadores de compromiso y el nivel de dificultad que los agentes de amenaza deben enfrentar, cuando los indicadores de compromiso son bloqueados por los equipos de seguridad. De esta manera, enumera los diferentes tipos de indicadores de compromiso que los profesionales de seguridad utilizan para identificar actividades maliciosas.

Cada tipo de indicador de compromiso se clasifica en niveles de dificultad. Estos representan los niveles de “dolor” que enfrenta un atacante cuando los equipos de seguridad bloquean la actividad asociada con el indicador de compromiso. Por ejemplo, el bloqueo de una dirección IP asociada con un agente de amenaza se etiqueta como fácil porque estos pueden usar sin dificultad distintas direcciones IP para sortear esto y así continuar con su ataque. Si los equipos de seguridad logran bloquear los IoC ubicados en la parte superior de la pirámide, más difícil se vuelve para los atacantes continuar con su misión. A continuación, se presenta un desglose de los diferentes tipos de indicadores de compromiso que se encuentran en la pirámide del dolor.

1. **Valores hash**: Hashes que corresponden a archivos maliciosos conocidos. A menudo se utilizan para proporcionar referencias únicas respecto a muestras específicas de malware o archivos involucrados en una intrusión.
2. **Direcciones IP**: Una dirección de protocolo de Internet como 192.168.1.1
3. **Nombres de dominio**: Una dirección web como www.google.com
4. **Artefactos de red**: Evidencia observable creada por agentes de amenaza en una red. Por ejemplo, la información que se encuentra en los protocolos de red, como las cadenas del agente de usuario (User-Agent strings).
5. **Artefactos de host:** Evidencia observable creada por agentes de amenaza en un host. Un host es cualquier dispositivo que esté conectado en una red. Por ejemplo, el nombre de un archivo creado por malware.
6. **Herramientas**: Software que es utilizado por un agente de amenaza para lograr su objetivo. Por ejemplo, los atacantes pueden usar herramientas de descifrado de contraseñas (password cracking) como John the Ripper para realizar ataques de contraseña y obtener acceso a una cuenta.
7. **Tácticas, técnicas y procedimientos (TTP)**: Comportamiento de un agente de amenaza. Las tácticas tienen que ver con la visión general de alto nivel del comportamiento. Las técnicas proporcionan descripciones detalladas del comportamiento en relación a la táctica. Los procedimientos son descripciones muy detalladas de la técnica. Los TTP son los más difíciles de detectar.

**Conclusiones clave**

Los indicadores de compromiso y los indicadores de ataque son fuentes valiosas de información para los profesionales de seguridad, para detectar incidentes. La pirámide del dolor es un concepto que se puede utilizar para comprender los diferentes tipos de indicadores de compromiso y el valor que tienen a la hora de detectar y detener la actividad maliciosa.

Marcar como completo

Me gusta

No me gusta

Informar de un problema