Indicadores IOC 2024-12-16 #2

Globe Sistemas - Av. Libertador Jardin America

Resumen de la actividad

Se analizará un artefacto utilizando VirusTotal y capturará detalles sobre sus indicadores de compromiso relacionados utilizando la Pirámide del Dolor.

La Pirámide del Dolor, que se utiliza para comprender los diferentes tipos de indicadores de compromiso (IoC). Un IoC es una prueba observable que sugiere indicios de un posible incidente de seguridad.

La Pirámide del Dolor describe la relación entre los IoC y el nivel de dificultad que experimentan los actores maliciosos cuando los IoC son bloqueados por los equipos de seguridad.

VirusTotal es una de las muchas herramientas que los analistas de seguridad utilizamos para identificar y responder a los incidentes de seguridad. VirusTotal es un servicio que permite analizar archivos, dominios, URL y direcciones IP sospechosos en busca de contenido malicioso.

A través del crowdsourcing, VirusTotal recopila e informa sobre la inteligencia de amenazas de la comunidad global de ciberseguridad. Esto nos ayuda a determinar qué IoC han sido reportados como maliciosos.

Escenario

Como analista del centro de operaciones de seguridad (SOC) de nivel uno se ha recibido una alerta sobre la descarga de un archivo sospechoso en el ordenador de un empleado.

Se ha investigado esta alerta y se descubrio que el empleado recibió un correo electrónico que contenía un archivo adjunto.

El archivo adjunto era una hoja de cálculo protegida por contraseña. La contraseña de la hoja de cálculo se facilitaba en el correo electrónico. El empleado descargó el archivo e introdujo la contraseña para abrirlo. Cuando el empleado abrió el archivo, se ejecutó una carga maliciosa en su ordenador.

Se recuperó el archivo malicioso y se creó un hash SHA256 del archivo. El hash es un método criptográfico utilizado para identificar de forma única el malware, actuando como la huella dactilar única del archivo. Se utilizará VirusTotal para descubrir otros IoC asociados al archivo.

Revisión de los detalles de alerta

La siguiente información contiene detalles sobre la alerta. Los detalles incluyen un hash del archivo y una cronología del suceso.

**Hash de archivo SHA256**: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Más de 50 proveedores han informado de que el hash del archivo es malicioso.

Tras una investigación más exhaustiva, se ha descubierto que este hash del archivo es el malware Flagpro, que ha sido utilizado habitualmente por el actor de amenazas avanzadas BlackTech.

He aquí una cronología de los acontecimientos que condujeron a esta alerta:

09:30:14 AM: Un empleado recibe un correo electrónico que contiene un archivo adjunto.

09:33:18 AM: El empleado descarga y abre correctamente el archivo.

09:34:01 AM: Se crean varios archivos ejecutables no autorizados en el ordenador del empleado.

09:35:22 AM: Un sistema de detección de intrusos detecta los archivos ejecutables y envía una alerta al SOC.

Indicadores de Compromiso IOC (Indicator of Compromise)

Después de haber explorado las secciones del informe de VirusTotal, se descubrió otros IoC que están asociados al archivo según el informe de VirusTotal.

**Valor hash:** 287d612e29b71c90aa54947313810a25 es un hash MD5 asociado a este malware según la pestaña Detalles del informe de VirusTotal.

**Dirección IP**: La dirección IP 104.115.151.81 es con la que se contactó este malware, aparece como una de las muchas direcciones IP en la pestaña Relaciones del informe de VirusTotal. Esta dirección IP también está asociada con el dominio org.misecure.com tal y como aparece en la sección Resoluciones DNS bajo la pestaña Comportamiento del informe de la caja de arena Zenbox.

**Nombre de dominio:** org.misecure.com ( *http://org.misecure.com/index.html* ) se reporta como un dominio malicioso contactado en la pestaña Relaciones del Informe de VirusTotal.

**Artefacto de red/artefacto de host**: Los artefactos relacionados con la red que se han observado en este software malicioso son peticiones HTTP (HTTP Requests) realizadas al dominio org.misecure.com. Esto aparece en la sección de Comunicaciones de red en la pestaña de Comportamiento de los informes de Venus Eye Espacio aislado y Rising MOVES sandbox.

**Herramientas**: La captura de entradas (Input Capture) aparece en la sección Recopilación de la pestaña Comportamiento del informe de la caja de arena Zenbox. Los actores maliciosos utilizan la captura de entradas para robar datos de los usuarios, como contraseñas, números de tarjetas de crédito y otras informaciones confidenciales.

**Tácticas, técnicas y procedimientos (TTP)**: Las TTP describen el comportamiento de un atacante. Comando y control aparece como una táctica en la pestaña Comportamiento del Informe de la caja de arena Zenbox. Los actores maliciosos utilizan el Comando y control para establecer canales de comunicación entre un sistema infectado y su propio sistema.

Se adjunta un gráfico llamado La Pirámide del Dolor explicando la importancia de cada IoC (grado de importancia de cada indicador de compromiso de acuerdo su posición en la pirámide).