Investigacion de Incidente de Phishing 2024-12-18 #1

Globe Sistemas - Av. Libertador Jardin America

Resumen de la actividad

Se responderá a un incidente de phishing que implica un hash de archivo malicioso. Se trata del mismo Hash de archivo SHA256 que se investigó y verificó anteriormente como malicioso. Se seguirá las instrucciones del Phishing Playbook de la organización para investigar y resolver el ticket de alerta del incidente.

Los playbooks describen paso a paso las acciones necesarias para responder adecuadamente a un incidente de seguridad. Para los analistas de seguridad, los playbooks sirven de guía para apoyar eficazmente los esfuerzos de respuesta a incidentes de una organización.

Una acción coordinada, eficaz y rápida es fundamental durante la respuesta a un incidente y puede ayudar a los equipos de seguridad a minimizar el impacto de un incidente y reducir el tiempo de respuesta al mismo.

Escenario

Como analista de Tier1 del centro de operaciones de seguridad (SOC) en una empresa de servicios informáticos, IT, análisis y ciberseguridad, se recibió una alerta de phishing sobre la descarga de un archivo sospechoso en el ordenador de un empleado. Tras investigar el hash del archivo adjunto al correo electrónico, se ha comprobado que el archivo adjunto es malicioso.

Ahora que dispone de esta información, debe seguir el proceso de la organización para completar la investigación y resolver la alerta. Las políticas y procedimientos de seguridad de la organización describen cómo responder a alertas específicas, incluyendo qué hacer cuando recibe una alerta de phishing.

Al final de la investigación, se actualizará el ticket de alerta con las conclusiones sobre el incidente.

Actualizar el estado del ticket de alerta

En el ticket de alerta , se comienza la investigación actualizando de la lista desplegable Estado del ticket a Investigando.

Evaluación de alerta

A continuación, se evaluará el contenido del ticket de alerta, incluido el contenido de la sección Información adicional:

**Detalles del remitente**: Existe una inconsistencia entre la dirección de correo electrónico del remitente “76tguy6hh6tgftrt7tg.su’”, el nombre utilizado en el cuerpo del correo electrónico “Clyde West”, y el nombre del remitente, “Def Communications”.

**Cuerpo del mensaje**: El cuerpo del correo electrónico y la línea de asunto contenían errores gramaticales. El cuerpo del correo electrónico también contenía un archivo adjunto protegido con contraseña, “bfsvc.exe”, que se descargó y abrió en la máquina afectada.

**Archivos adjuntos o enlaces**: Después de haber investigado previamente el hash del archivo, se confirmó que se trata de un archivo malicioso conocido.

Attachment: filename="bfsvc.exe"

Investigación 5W

* ¿Quién causó el incidente?

La investigación a través VirusTotal indica que este archivo Hash es el malware Flagpro, que ha sido utilizado por el actor BlackTech.

* ¿Qué ha ocurrido?

La alerta del software IDS detectó y alertó al SOC de un archivo malicioso descargado de un correo electrónico de phishing.

* ¿Cuándo se produjo el incidente?

Jueves, 16 de Diciembre, 2024 09:30:14 AM. A continuación, 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 ejecutables y envía una alerta al SOC.

* ¿Dónde ocurrió el incidente?

centro de operaciones de seguridad (SOC) de globe sistemas, empresa de servicios informáticos, IT, análisis y ciberseguridad realizando servicios de ciberseguridad IDS para un tercero.

* ¿Por qué se produjo?

Porque un empleado descargó y abrió un archivo malicioso de un correo electrónico de phishing.

Investigación Exhaustiva

Una investigación crowdsourcing (cruce de información) más exhaustiva ha determinado que más de 50 proveedores han informado de que el hash del archivo es malicioso.

También se ha descubierto que este hash del archivo es el malware Flagpro, que ha sido utilizado habitualmente por el actor de amenazas avanzadas BlackTech.

**Valor hash:** 287d612e29b71c90aa54947313810a25 es también 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 Zenbox sandbox\*.

\*Sandbox, arenero o caja de arena = es un entorno de prueba aislado que se utiliza como medidas de ciberseguridad ofensiva / activa, que permite a los usuarios y empresas ejecutar programas o ejecutar archivos sin afectar la aplicación, el sistema o la plataforma en la que se ejecutan.)

**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 isolated spaces 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.

Determinar si la alerta debe escalarse y actualizar estado del ticket

**Escalamiento**: El ticket requiere una escalada, a un analista de SOC de Tier2 para que tome más medidas, debido a que el mail contiene/ia archivos adjuntos maliciosos conocidos y este fue abierto y ejecutado, según las instrucciones del playbook.

**Gravedad de la alerta**: Se eleva la gravedad de alerta a MEDIA.

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