El primer ataque a Guardicore Global Sensors Network (GGSN) fue capturado el 24 de enero de 2020. Desde entonces, nuestros sensores han informado de un total de 92 ataques, lo que muestra un fuerte aumento en su número desde octubre.

Los ataques se originan en 11 direcciones IP diferentes, la mayoría de las cuales son de Irlanda y el Reino Unido. Lo que nos impulsó a seguir de cerca esta amenaza es el uso de doble extorsión, donde los datos robados se publican y se ofrecen a la venta como un medio para presionar a las víctimas a pagar el rescate.

Guardicore Labs observó dos variantes diferentes durante la vida útil de esta campaña. En el primero, que duró desde enero hasta finales de noviembre, los atacantes dejaron una nota de rescate con su dirección de billetera, la cantidad de Bitcoins a pagar y una dirección de correo
electrónico para soporte técnico.

No se utilizó la doble extorsión. Dado que las carteras de Bitcoin se especificaron explícitamente en las notas de rescate, pudimos explorar las carteras y la cantidad de BTC transferidas a cada una de ellas. Encontramos que un total de 1.2867640900000001 BTC equivalente a 24,906.00 USD se les había transferido a estas billeteras. Guardicore Sensors capturó 63 ataques de este tipo, provenientes de 4 direcciones IP diferentes.

La segunda fase comenzó el 3 de octubre y duró hasta finales de noviembre y marcó una evolución de la campaña. El pago ya no se realizó directamente a una billetera Bitcoin y no se necesitaron comunicaciones por correo electrónico. En cambio, los atacantes instalaron un sitio web en la red TOR donde se puede realizar el pago. Las víctimas se identifican mediante tokens alfanuméricos únicos que reciben en la nota de rescate.

El sitio web es un buen ejemplo de un mecanismo de doble extorsión: contiene todas las bases de datos filtradas por las que no se pagó el dinero. La lista web incluye 250k bases de

datos diferentes de 83k servidores MySQL, con 7 TB de datos robados. Hasta ahora, GGSN capturó 29 incidentes de esta variante, originados en 7 direcciones IP diferentes.

Cadena de Ataque

El ataque comienza con una contraseña de fuerza bruta en el servicio MySQL. Una vez que tiene éxito, el atacante ejecuta una secuencia de consultas en la base de datos, recopilando datos sobre las tablas y los usuarios existentes. Al final de la ejecución, los datos de la víctima se eliminan, se archivan en un archivo comprimido que se envía a los servidores de los atacantes y luego se eliminan de la base de datos.

Una nota de transferencia se deja en una tabla llamada ADVERTENCIA, exigiendo un pago de rescate de hasta 0.08 BTC.

Además, *abackdoorusermysqlbackups '@'% '* se agrega a la base de datos para su persistencia, proporcionando a los atacantes acceso futuro al servidor comprometido.

El dominio .onion –*hn4wg4o6s5nc7763.onion*-conduce a un tablero completo donde las víctimas pueden proporcionar su token y realizar el pago. El dominio de nivel superior .onion se utiliza para distinguir los servicios alojados en la red TOR. Dichos sitios web solo se pueden acceder desde el
navegador TOR, y garantizar que tanto sus operadores como los usuarios del lado del cliente permanezcan en el anonimato eligiendo utilizar un dominio .onion dificulta rastrear a los atacantes y dónde está alojada su infraestructura.

Todas las bases de datos robadas se ofrecen para una venta menor en el sitio web titulado Subasta, y todas tienen un precio uniforme de 0.03 Bitcoin. La tabla de esta página enumera todas las bases de datos robadas, junto con sus tamaños.

Al rastrear las páginas de la subasta, Guardicore Labs encontró casi 83 mil tokens únicos. La restauración de datos costará a una víctima 0.03 BTC, que equivale a alrededor de $520.00 USD.

Los Ataques de Ransomware Vienen en Diferentes Formas

Algunas campañas de ransomware son muy específicas; se planifican con anticipación durante meses y se ejecutan sin problemas. Esas campañas son amenazas avanzadas y persistentes (APT). Infringen la red, realizan movimientos laterales silenciosos y cuidadosos para infectar múltiples
activos, cifran datos valiosos y exigen un rescate para su restauración.

Otras campañas son de naturaleza oportunista. Estas campañas suelen ser automáticas, lo que significa que se ejecutan desde un script en lugar de un ser humano. La recopilación o el reconocimiento de inteligencia no son parte del proceso. Esta característica permite que estas campañas escalen significativamente y potencialmente infecten servidores importantes que están conectados por error a Internet.

Las campañas de ataque de este tipo son dirigidas voluntariamente. No tienen interés en la identidad o el tamaño de la víctima, y resultan en una escala mucho mayor que la disponible para los ataques dirigidos. Piense en ello como *«Ransomware de Fabrica»*: los atacantes ejecutan el ataque, ganando menos dinero por víctima, pero teniendo en cuenta el número de máquinas infectadas.

PLEASE_READ_ME es un gran ejemplo del último tipo:

1. Está dirigido: intenta infectar cualquiera de los 5 millones de servidores MySQL que están conectados a Internet.
2. Es transitorio: no pasa tiempo en la red además del requerido para el ataque real. Sin ningún movimiento lateral involucrado, el ataque comienza y termina dentro de la base de datos MySQL en sí y no intenta escapar de él.
3. Es simple: No hay cargas útiles binarias involucradas en la cadena de ataque, lo que hace que el ataque sea “sin malware”. Solo un simple script que irrumpe en la base de

datos, roba información y deja un mensaje.

Los operadores PLEASE_READ_ME están tratando de mejorar su juego usando doble extorsión en escala. Factorizar su operación hará que la campaña sea más escalable y rentable. Guardicore Labs proporciona un repositorio de anIOCs y seguirá monitoreando esta campaña para ayudar a las organizaciones a protegerse contra ella.

Mitigación

Como regla general, los servidores de bases de datos no deben estar orientados a Internet; deben ser internos a la red y accesibles solo por ciertos usuarios que utilizan clientes SQL específicos. Además, deben protegerse con contraseñas seguras.

Existen soluciones que le permiten identificar fácilmente los servicios expuestos a Internet y segmentarlos para proteger su centro de datos del ransomware y otras amenazas activas.

Autores: Ophir Harpaz, Omri Marom.