Hackers informáticos patrocinados por el estado iraní, desplegaron una nueva variedad de malware de borrado de datos en la red de Bapco, la compañía petrolera nacional de Bahrein.

Este incidente ocurrió el pasado 29 de diciembre, pero no tuvo el efecto duradero que los piratas informáticos hubieran querido, ya que solo una parte de la flota de computadoras de Bapco se vio afectada, y la compañía siguió operando luego de la detonación del malware.

La Autoridad Nacional de Ciberseguridad de Arabia Saudita emitió una alerta de seguridad que se publicó la semana pasada. Los funcionarios sauditas enviaron dicha alerta a las compañías locales activas en el mercado de la energía, en un intento por advertir sobre ataques inminentes, e instaron a las compañías a asegurar sus redes.

El incidente de Bapco salió a la luz en medio de las crecientes tensiones políticas entre Estados Unidos e Irán, luego de que el ejército estadounidense ejecutara a un general militar iraní en un ataque con aviones no tripulados la semana pasada.

Aunque el ataque a Bapco parece no estar relacionado con las tensiones políticas actuales, sí muestra las capacidades técnicas avanzadas de Irán para desarrollar ataques cibernéticos a gran escala, un tema sobre el que el Departamento de Seguridad Nacional de Estados Unidos advirtió en una alerta publicada el fin de semana.

Dustman

En el ataque de Bapco se encontró una nueva variedad de malware denominada Dustman. Según un análisis realizado por la agencia de seguridad cibernética de Arabia Saudita, Dustman es un limpiador de datos, es decir, malware diseñado para eliminar datos en computadoras infectadas.

Dustman representa el tercer malware diferente de borrado de datos vinculado al régimen de Teherán. Los hackers respaldados por el estado iraní ya tienen una larga historia de desarrollo de malware que elimina datos.

La incursión de Irán en el malware de eliminación de datos se remonta a 2012, cuando desarrollaron Shamoon, también conocido como Disttrack, una pieza de malware responsable del borrado de datos en más de 32 mil computadoras en la compañía petrolera Saudi Aramco, en Arabia Saudita.

Se descubrieron dos versiones más de Shamoon en los siguientes años, Shamoon V2, utilizada en 2016 y 2017, y Shamoon V3, utilizada en 2018 y 2019.

Según un informe publicado por IBM X-Force, los piratas informáticos iraníes también están vinculados a ataques de borrado de datos con una segunda cepa de malware diferente llamada ZeroCleare, descubierta por primera vez en la naturaleza en septiembre de 2019.

Los funcionarios sauditas de la CNA afirman que Dustman parece ser una versión mejorada y más avanzada del limpiador ZeroCleare, que se descubrió en el otoño pasado, que a su vez, tenía muchas similitudes de código con el Shamoon original.

EL principal componente compartido entre las tres cepas es EldoS RawDisk, un kit de herramientas de software legítimo para interactuar con archivos, discos y particiones. Las tres cepas de malware utilizan distintos exploits y técnicas para elevar el acceso inicial al nivel de administrador, desde donde desempaquetan y lanzan la utilidad EldoS RawDisk para eliminar datos en hosts infectados.

Debido a que Dustman se considera una versión evolucionada de ZeroCleare, la mayor parte del código es el mismo, pero los funcionarios sauditas de la CNA que analizaron el malware aseguran que Dustman cuenta con dos diferencias importantes:

- La capacidad destructiva de Dustman y todos los controladores y cargadores necesarios se entregan en un archivo ejecutable en lugar de dos archivos, como fue el caso de ZeroCleare.
- Dustman sobrescribe el volumen, mientras que ZeroCleare borra un volumen sobre escribiéndolo con datos basura (Ox55).

Según ZDNet, la focalización de Bapco con Dustman encaja en el modus operandi regular de conocidos piratas informáticos patrocinados por el estado iraní.

Históricamente, antes del despliegue de Dustman el 29 de diciembre, los hackers iraníes utilizaban Shamoon y ZeroCleare exclusivamente contra empresas en el campo petrolero y de gas.

Los objetivos anteriores incluían compañías con vínculos con el régimen saudita y Saudi Aramco, la compañía petrolera nacional de Arabia Saudita. Irán y Arabia Saudita ya han tenido relaciones tensas desde la década de 1970, debido a las diferencias en la interpretación del Islam, y debido a su competencia en el mercado de exportación de petróleo.

Bapco es una compañía propiedad del régimen de Bahrein, un país que tiene muchas relaciones políticas tensas con el régimen de Teherán, y que es conocido como socio comercial de Saudi Aramco.

Hasta el momento, Bapco parece ser la única víctima de un ataque con el malware Dustman, aunque esto no significa que el malware no se haya implementado en la red de otros objetivos.

Según el informe de la CNA, los atacantes no parecen haber planeado desplegar Dustman en el momento en que lo hicieron, pero parece que desencadenaron el proceso de borrado de datos como un último esfuerzo para ocultar evidencia forense luego de cometer una serie de errores.

Los funcionarios sauditas de la CNA, y fuentes exclusivas de ZDNet, confirmaron que el punto de entrada eran los servidores VPN de la compañía. El informe de la CNA cita *«vulnerabilidades de ejecución remota en un dispositivo VPN que se reveló en julio de 2019″* como el punto de entrada de los atacantes en la red de Bapco.

Aunque los funcionarios no culparon a ningún dispositivo específico, lo más probable es que

se refieran a un informe Devcore, publicado durante el verano, que reveló errores de ejecución remota en una gran cantidad de servidores VPN de nivel empresaria, como los de Fortinet, Pulse Secure y Palo Alto Networks.

Al realizar una búsqueda con el motor BinaryEdge, se encontró que una parte de la red vpn.bapco.net, se ejecuta en dispositivos Fortinet VPN. Sin embargo, también es posible que Bapco haya ejecutado servidores Pulse Secure en el pasado.

El texto siguiente es un extracto del informe:

> *«El actor de la amenaza obtuvo cuentas de administrador y servicio de dominio en la red de la víctima, que se utilizó para ejecutar el malware «Dustman» en todos los sistemas de la víctima. El atacante usó la cuenta de servicio de la consola de administración de antivirus para distribuir el malware por medio de la red.*
>
> *El actor accedió a la red de la víctima y copió el malware y la herramienta de ejecución remota «PSEXEC» en el servidor de la consola de gestión de antivirus que estaba conectado a todas las máquinas dentro de la red de la víctima debido a la naturaleza de su funcionalidad. Pocos minutos después, el atacante accedió al servidor de almacenamiento de las víctimas y eliminó todos los volúmenes de forma manual.*
>
> *Después, los atacantes ejecutaron un conjunto de comandos en el control de gestión antivirus para distribuir el malware a todas las máquinas conectadas, y por medio de (PSEXEC) el malware ejecutó y soltó tres archivos adicionales, dos controladores y el limpiador. La mayoría de las máquinas conectadas fueron borradas».*

Los ataques cibernéticos exitosos dieron como resultado que todos los sistemas eliminados

mostraran un mensaje de pantalla azul de la muerte (BSOD).

Según los funcionarios sauditas, existía una sensación de urgencia en las acciones del atacante. Se desconoce el motivo de la urgencia.

> *«El malware DUSTMAN se compiló, posiblemente en la infraestructura del actor de la amenaza, unos minutos antes de desplegarlo en la red de la víctima. Esto es inconsistente con los ataques destructivos conocidos, ya que generalmente se prueban antes de desplegarse»,* dijeron funcionarios de la CNA.

Sin embargo, la prisa y falta de pruebas provocaron que la operación de borrado no fuera exitosa y el malware no se ejecutó correctamente en algunos sistemas.

Los funcionarios sauditas creen que los hackers también notaron las acciones fallidas, ya que intentaron eliminar los rastros de Dustman de los sistemas, y luego borraron los registros de acceso en el servidor VPN antes de abandonar la red.

Los funcionarios de Bapco se enteraron del ataque al siguiente día, el 30 de diciembre, cuando los empleados llegaron a trabajar. Ellos lograron rastrear el ataque y lo identificaron como Dustman porque algunas estaciones de trabajo estaban en modo de suspensión en el momento del ataque.

Cuando se iniciaron estos sistemas, intentaron ejecutar el malware, pero el antivirus, que estaba desactivado en el momento del ataque original, detectó y evitó el ataque.