Se ha observado a un actor de amenazas motivado financieramente implementando un rootkit previamente desconocido dirigido a los sistemas Oracle Solaris, con el objetivo de comprometer las redes de conmutación de cajeros automáticos (ATM) y realizar retiros de efectivo no autorizados en distintos bancos utilizando tarjetas fraudulentas.

La compañía de inteligencia de amenazas y respuesta a incidentes Mandiant, está rastreando el grupo bajo el nombre de UNC2891, con algunas de las tácticas, técnicas y procedimientos del grupo que comparten superposiciones con las de otro grupo denominado UNC1945.

Las intrusiones organizadas por el actor involucran *«un alto grado de OPSEC y aprovechan el malware, las utilidades y los scripts públicos y privados para eliminar evidencia y obstaculizar los esfuerzos de respuesta»,* dijeron los investigadores de Mandiant.

Más preocupante todavía es que los ataques duraron varios años en algunos casos, durante los cuales, el actor permaneció sin ser detectado aprovechando un rootkit llamado CAKETAP, que está diseñado para ocultar conexiones de red, procesos y archivos.

Mandiant, que pudo recuperar datos forenses de la memoria de uno de los servidores conmutadores de cajeros automáticos víctimas, dijo que una variante del rootkit del kernel venía con funciones especializadas que le permitirían interceptar mensajes de verificación de tarjetas y PIN, además de utilizar los datos robados para realizar transacciones fraudulentas de retiro de efectivo de cajeros automáticos.

También se utilizan dos puertas traseras conocidas como SLAPSTICK y TINYSHELL, ambas atribuidas a UNC1945 y se utilizan para obtener acceso remoto persistente a sistemas de misión crítica, así como para la ejecución de shell y transferencias de archivos a través de rlogin, telnet o SSH.

> *«De acuerdo con la familiaridad del grupo con los sistemas basados en Unix y Linux, UNC2891 a menudo nombró y configuró sus puertas traseras TINYSHELL con valores que se hicieron pasar por servicios legítimos que los investigadores podrían pasar por alto, como systemd (SYSTEMD), daemon de caché de servicios de nombres (NCSD) y Linux at daemon (ATD)»,* dijeron los investigadores.

Además, las cadenas de ataque emplearon una variedad de malware y utilidades disponibles de forma pública, que incluyen:

- STEELHOUND: Una variante del cuentagotas en memoria STEELCORGI, que se utiliza para descifrar una carga incrustada y cifrar nuevos archivos binarios.
- WINGHOOK: Un registrador de teclas para sistemas operativos basados en Linux y Unix que captura los datos en un formato codificado.
- WINGCRACK: Una utilidad que se utiliza para analizar el contenido codificado generado por WINGHOOK.
- WIPERIGHT: Una utilidad ELF que borra las entradas de registro pertenecientes a un usuario específico en sistemas basados en Linux y Unix.
- MIGLOGCLEANER: Una utilidad ELF que borra registros o elimina ciertas cadenas de registros en sistemas basados en Linux y Unix.

> *«UNC2891 utiliza su habilidad y experiencia para aprovechar al máximo la distribución de la visibilidad y las medidas de seguridad que suelen estar presentes en los entornos Unix y Linux. Si bien algunas de las superposiciones entre UNC2891 y UNC1945 son notables, no es lo suficientemente concluyente como para atribuir las intrusiones a un solo grupo de amenazas»,* dijeron los investigadores.