Se descubrió una nueva pieza de malware sigiloso de Linux llamado Shikitega, que adopta una cadena de infección de varias etapas para comprometer los puntos finales y los dispositivos IoT y depositar cargas útiles adicionales.

> *«Un atacante puede obtener el control total del sistema, además del minero de criptomonedas que se ejecutará y configurará para persistir»*, dijo AT&T Alien Labs en un informe.

Los hallazgos se suman a una lista creciente de malware de Linux que se encontró en la naturaleza en los últimos meses, incluyendo BPFDoor, Symbiote, Syslogk, OrBit y Lightning Framework.

Una vez implementada en un host objetivo, la cadena de ataque descarga y ejecuta el metasploit Mettle para maximizar el control, explota vulnerabilidades para elevar sus privilegios, agrega persistencia en el host por medio de crontab, y en última instancia, lanza un minero de criptomonedas en dispositivos infectados.

Aún se desconoce el método exacto por el cual se logra el compromiso inicial, pero lo que hace que Shikitega sea evasivo es su capacidad para descargar cargas útiles de próxima etapa desde un servidor de comando y control (C2) y ejecutarlas directamente en la memoria.

La escalada de privilegios se logra mediante la explotación de CVE-2021-4034 (también conocido como PwnKit) y CVE-2021-3493, lo que permite al adversario abusar de los permisos elevados para obtener y ejecutar los scripts de shell de etapa final con privilegios de raíz para establecer la persistencia e implementar el minero de criptomonedas Monero.

En otro intento de pasar desapercibido, los operadores de malware emplean un codificador polimórfico «*Shikata ga nai*» para que sea más difícil de detectar por los motores antivirus y abusan de los servicios de nube legítimos para funciones C2.

> *«Los actores de amenazas siguen buscando formas de entregar malware de nuevas maneras para permanecer bajo el radar y evitar la detección»,* dijo el investigador de AT&T Alien Labs, Ofer Caspi.

> *«El malware Shiketega se entrega de forma sofisticada, utiliza un decodificador polimórfico y entrega gradualmente su carga útil donde cada paso revela solo una parte de la carga útil total».*