Los investigadores han revelado una versión actualizada de un malware para macOS de Apple llamado Rustbucket que presenta mejoras en sus capacidades para establecer persistencia y evitar ser detectado por software de seguridad.

> *«Esta variante de Rustbucket, una familia de malware que se dirige a sistemas macOS, incorpora capacidades de persistencia que no se habían observado previamente . Se está utilizando una metodología de infraestructura de red dinámica para el comando y control»*, señalaron los investigadores de Elastic Security Labs en un informe publicado esta semana

RustBucket es obra de un actor de amenazas norcoreano conocido como BlueNoroff, el cual forma parte de un conjunto de intrusiones más amplio conocido como Lazarus Group, una unidad de piratería de élite supervisada por el Reconnaissance General Bureau (RGB), la principal agencia de inteligencia del país.

El malware salió a la luz en abril de 2023, cuando Jamf Threat Labs lo describió como una puerta trasera basada en AppleScript capaz de obtener una carga secundaria desde un servidor remoto. Elastic está monitoreando la actividad bajo el nombre de REF9135.

El malware de segunda etapa, compilado en Swift, está diseñado para descargar desde el servidor de comando y control (C2) el malware principal, un archivo binario basado en Rust con funciones para recopilar información extensa, así como para obtener y ejecutar binarios Mach-O adicionales o scripts de shell en el sistema comprometido.

Esta es la primera vez que el malware de BlueNoroff se dirige específicamente a usuarios de macOS, aunque desde entonces ha aparecido una versión en.NET de RustBucket en la naturaleza con un conjunto similar de características.

> *«Esta reciente actividad de Bluenoroff ilustra cómo los conjuntos de intrusiones recurren a lenguajes multiplataforma en sus esfuerzos de desarrollo de malware,*

> *ampliando aún más sus capacidades y muy probablemente expandiendo su alcance de víctimas»,* mencionó la empresa francesa de ciberseguridad Sekoia en un análisis de la campaña RustBucket a finales de mayo de 2023.

La cadena de infección consiste en un archivo instalador de macOS que instala un lector de PDF modificado pero funcional. Un aspecto importante de los ataques es que la actividad maliciosa solo se activa cuando se abre un archivo PDF manipulado utilizando el lector de PDF falso. Los vectores iniciales de intrusión incluyen correos electrónicos de phishing, así como el uso de perfiles falsos en redes sociales como LinkedIn.

Los ataques observados tienen un enfoque altamente selectivo y se centran en instituciones relacionadas con finanzas en Asia, Europa y Estados Unidos, lo que sugiere que la actividad está dirigida a generar ingresos ilícitos para evadir sanciones.

Lo que destaca en la versión recién identificada es su mecanismo de persistencia inusual y el uso de un dominio de DNS dinámico (docsend.linkpc[.]net) para el comando y control, además de incorporar medidas orientadas a pasar desapercibido.

> *«En el caso de esta muestra actualizada de RUSTBUCKET, establece su propia persistencia mediante la adición de un archivo plist en la siguiente ruta: /Users//Library/LaunchAgents/com.apple.systemupdate.plist, y copia el binario del malware en la siguiente ruta: /Users//Library/Metadata/System Update»,* afirmaron los investigadores.