El infame botnet Glupteba ha adquirido un nuevo y astuto poder: un bootkit UEFI nunca antes visto. Esta característica esconde el malware en las entrañas del sistema, haciéndolo casi imposible de detectar y eliminar.

Los expertos en seguridad alertan que esto impulsa las capacidades de persistencia y evasión de Glupteba. Este botnet ya se dedicaba al robo de información, la minería de criptomonedas y la distribución de malware. Ahora, gracias al bootkit, puede ocultarse aún mejor.

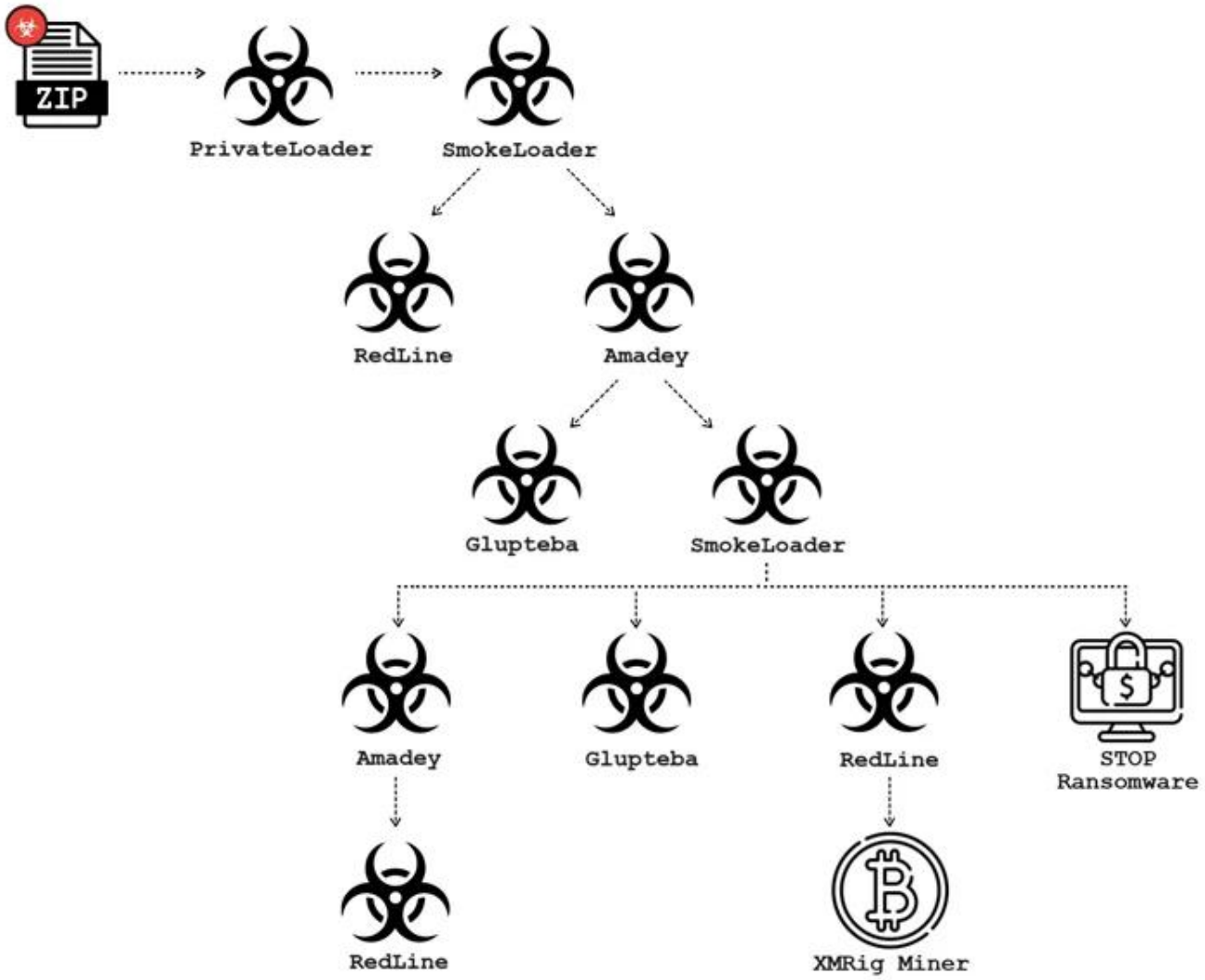
Lo que debes saber:

- El bootkit de Glupteba manipula el proceso de arranque del sistema, volviéndose invisible para las herramientas de seguridad tradicionales.
- Esto añade otra capa de defensa a este malware ya versátil, famoso por sustraer datos, minar criptomonedas y desplegar otros programas maliciosos.
- Glupteba también es conocido por utilizar la blockchain de Bitcoin como sistema de comunicación de respaldo, lo que lo hace resistente a los intentos de eliminación.

Esta nueva artimaña pone de relieve la constante evolución de las amenazas cibernéticas. Los atacantes no se detienen en su innovación, y las soluciones de seguridad deben seguir el ritmo.

Puntos adicionales a tener en cuenta:

- El uso de servicios de pago por instalación como Ruzki para distribuir Glupteba indica un cambio hacia métodos de distribución más elaborados.
- La cadena de infección de múltiples etapas empleada por Glupteba demuestra cómo los atacantes encadenan diferentes herramientas para burlar las defensas.
- Este incidente subraya la importancia de mantener la vigilancia y usar soluciones de seguridad completas que puedan detectar y eliminar incluso las amenazas más avanzadas.



> Los investigadores explican que *«los actores maliciosos suelen distribuir Glupteba como parte de una cadena de infección compleja que propaga varias familias de malware simultáneamente. «Esta cadena de infección suele comenzar con una infección de PrivateLoader o SmokeLoader que carga otras familias de malware, y luego carga Glupteba».*

Como señal de que el malware se mantiene activamente, Glupteba viene equipado con un

bootkit UEFI que incorpora una versión modificada de un proyecto de código abierto llamado EfiGuard, capaz de deshabilitar PatchGuard y Driver Signature Enforcement (DSE) durante el arranque.

> Cabe destacar que se descubrió que versiones anteriores del malware *«instalaban un controlador del núcleo que el bot utilizaba como rootkit, y realizaban otros cambios que debilitaban la seguridad del host infectado».*
>
> *«El malware Glupteba sigue siendo un ejemplo notable de la complejidad y adaptabilidad que muestran los ciberdelincuentes modernos. La identificación de una técnica de evasión UEFI no documentada en Glupteba subraya la capacidad de innovación y evasión de este malware. Además, con su papel en la distribución de Glupteba, el ecosistema PPI pone de manifiesto las estrategias de colaboración y monetización empleadas por los ciberdelincuentes en sus intentos de infección masiva»,* afirmaron los investigadores.