Se ha observado que una nueva botnet llamada Dark Frost lanza ataques distribuidos de denegación de servicio (DDoS) contra la industria del juego.

> *«La botnet Dark Frost, inspirada en Gafgyt, QBot, Mirai y otras cepas de malware, se ha expandido para abarcar cientos de dispositivos comprometidos»,* dijo el investigador de seguridad de Akamai, Allen West.

Los objetivos incluyen empresas de juegos, alojamiento de servidores de juegos, proveedores, transmisores en línea e incluso otros miembros de la comunidad de juegos con los que el atacante ha interactuado directamente.

A partir de febrero de 2023, la botnet consta de 414 máquinas que ejecutan varias arquitecturas de conjunto de instrucciones, como ARMv4, x86, MIPSEL, MIPS y ARM7.

Las botnets suelen estar formadas por una amplia red de dispositivos comprometidos en todo el mundo. Los operadores tienden a usar los hosts esclavizados para extraer criptomonedas, robar datos confidenciales o aprovechar el ancho de banda colectivo de Internet de estos bots para derribar otros sitios web y servidores de Internet inundando los objetivos con tráfico basura.

Dark Frost representa la última iteración de una red de bots que parece haber sido ensamblada robando el código fuente de varias cepas de malware de redes de bots como Mirai, Gafgyt y QBot.

Akamai, que realizó ingeniería inversa de la botnet después de marcarla el 28 de febrero de 2023, fijó su potencial de ataque en aproximadamente 629.28 Gbps por medio de un ataque de inundación UDP. Se cree que el hacker está activo desde al menos mayo de 2022.

> *«Lo que hace que este caso en particular sea interesante, es que el actor detrás de los ataques ha publicado grabaciones en vivo de sus ataques para que todos los*

> *vean»,* dijo la compañía de infraestructura web.

> *«Se observó al actor alardeando de sus logros en las redes sociales, usando la botnet para pequeñas disputas en línea e incluso dejando firmas digitales en su archivo binario».*

El adversario ha establecido además un canal Discord para facilitar los ataques a cambio de dinero, indicando sus motivaciones financieras y planes para desarrollarlo como un servicio DDoS de alquiler.

Dark Frost constituye un ejemplo moderno de lo fácil que es para los cibercriminales novatos con habilidades de decodificación rudimentarias entrar en acción usando malware ya disponible para infligir daños significativos a las empresas.

> *«El alcance que pueden tener estos actores de amenazas es asombroso a pesar de la falta de novedad en sus técnicas. Aunque no es el adversario más avanzado o alucinante, la red de bots Dark Frost ha logrado acumular cientos de dispositivos comprometidos para cumplir sus órdenes»,* dijo West.