Los atacantes detrás de la red de bots de denegación de servicio distribuida (DDoS) Fodcha, resurgió con nuevas capacidades, según revelaciones de los investigadores de seguridad.

Esto incluye cambios en su protocolo de comunicación y la capacidad de extorsionar pagos en criptomonedas a cambio de detener el ataque DDoS contra un objetivo, dijo el Laboratorio de Investigación de Segurida de Redes de Qihoo 360 en un informe.

Fodcha salió a la luz por primera ve a inicios de abril, con el malware propagándose a través de vulnerabilidades conocidas en dispositivos Android e IoT, así como contraseñas débiles de Telnet o SSH.

La compañía de ciberseguridad dijo que Fodcha se convirtió en una botnet a gran escala con más de 60,000 nodos activos y 40 dominios de comando y control (C2) que pueden *«generar fácilmente más de 1 Tbps de tráfico».*

Se informa que la actividad máxima ocurrió el 11 de octubre de 2022, cuando el malware apuntó a 1396 dispositivos en un solo día.

Los principales países señalados por la botnet desde finales de junio de 2022 incluyen a China, Estados Unidos, Singapur, Japón, Rusia, Alemania, Francia, Reino Unido, Canadá y los Países Bajos.

Algunos de los objetivos destacados van desde organizaciones de atención médica y agencias de aplicación de la ley hasta un conocido proveedor de servicios en la nube que fue asaltado con un tráfico superior a 1 Tbps.

La evolución de Fodcha también ha ido acompañada de nuevas funciones ocultas que cifran las comunicaciones con el servidor C2 e incorporan demandas de rescate, lo que la convierte en una amenaza más potente.

> *«Fodcha reutiliza gran parte del código de ataque de Mirai y admite un total de 17*

> *métodos de ataque»*, dijo la compañía de ciberseguridad.

Los hallazgos surgen cuando una nueva investigación de Lumen Black Lotus Labs señaló el creciente abuso del Protocolo ligero de acceso a directorios sin conexión (CLDAP) para aumentar la escala de los ataques DDoS.

Para esto, se identificaron hasta 12,142 reflectores CLDAP abiertos, la mayoría distribuidos en Estados Unidos y Brasil, y en menor medida en Alemania, India y México.

En un caso, se observó que un servicio CLDAP asociado con un negocio minorista regional no identificado en América del Norte dirige *«cantidades problemáticas de tráfico»* hacia una amplia gama de objetivos durante más de nueve meses, emitiendo hasta 7.8 Gbps de tráfico CLDAP.