Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°273	Fecha: 15-11-2023
		Página: 4 de 14

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Ddostf DDoS Malware Atacando Servidores MySQL En Entornos Windows		
Tipo de Ataque	Denegación distribuida de servicio DDoS	Abreviatura	DDoS
Medios de propagación	Red, Correo, Navegación de Internet		
Código de familia	F	Código de Sub familia	F01
Clasificación temática familia	Disponibilidad del Servicio		

Descripción

1. **ANTECEDENTES:**

   Los investigadores descubrieron que los servidores MySQL vulnerables se están implementando con el bot Ddostf DDoS, que es capaz de lanzar ataques de denegación de servicio distribuido (DDoS).

   Ddostf, que se identificó por primera vez alrededor de 2016, es conocido por admitir plataformas Windows y Linux y se cree que se creó en China.

   Análisis anteriores indican que las variantes de malware Gh0st RAT y AsyncRAT representan la mayoría de las cepas de malware dirigidas a servidores MySQL susceptibles.

2. **DETALLES:**

   AhnLab advierte que los atacantes maliciosos escanean Internet en busca de servidores MySQL de acceso público utilizando el puerto TCP 3306 y luego intentan comprometerlos utilizando credenciales débiles o explotando vulnerabilidades conocidas.

   Luego, los atacantes cargan una DLL maliciosa como una biblioteca UDF (función definida por el usuario), que les permite ejecutar comandos en el sistema infectado e implementar y ejecutar el malware Ddostf.

   Ddostf tiene un formato ELF que se puede utilizar en entornos Linux y un formato PE que se puede utilizar en entornos Windows.

   La inclusión de la cadena “ddos.tf” en el binario de Ddostf es una característica distintiva. Antes de registrarse como servicio, Ddostf se copia a sí mismo en el directorio %SystemRoot% con un nombre aleatorio cuando se ejecuta.

   Cuando se conecta por primera vez, recopila los datos más básicos del dispositivo comprometido y los transmite al servidor C&C.

   El servidor C&C responde con datos además de comandos cuando recibe información del sistema comprometido. Contiene la URL de descarga, por ejemplo, en el caso de métodos de ataque DDoS específicos o comandos de descarga.

   Los ataques SYN Flood, UDP Flood y HTTP GET/POST Flood son solo algunas de las técnicas utilizadas en los ataques DDoS internos.

   Además, Ddostf es único porque puede establecer una conexión a una dirección recién obtenida del servidor C&C y ejecutar comandos allí durante un cierto período de tiempo.

   Esto sugiere que el actor de amenazas Ddostf puede infectar una gran cantidad de sistemas y posteriormente vender ataques DDoS como un servicio.

3. **RECOMENDACIONES:**

   - Establecer contraseñas seguras para sus cuentas y restablecerlas periódicamente.
   - Aplicar las correcciones más recientes también ayudará a evitar ataques de vulnerabilidad.
   - Utilizar programas de seguridad, como firewalls, para servidores de bases de datos accesibles externamente.

Fuente de Información:	• hxxps://gbhackers.com/ddostf-ddos-malware/ • hxxps://www.securityweek.com/mysql-servers-docker-hosts-infected-with-ddos-malware/