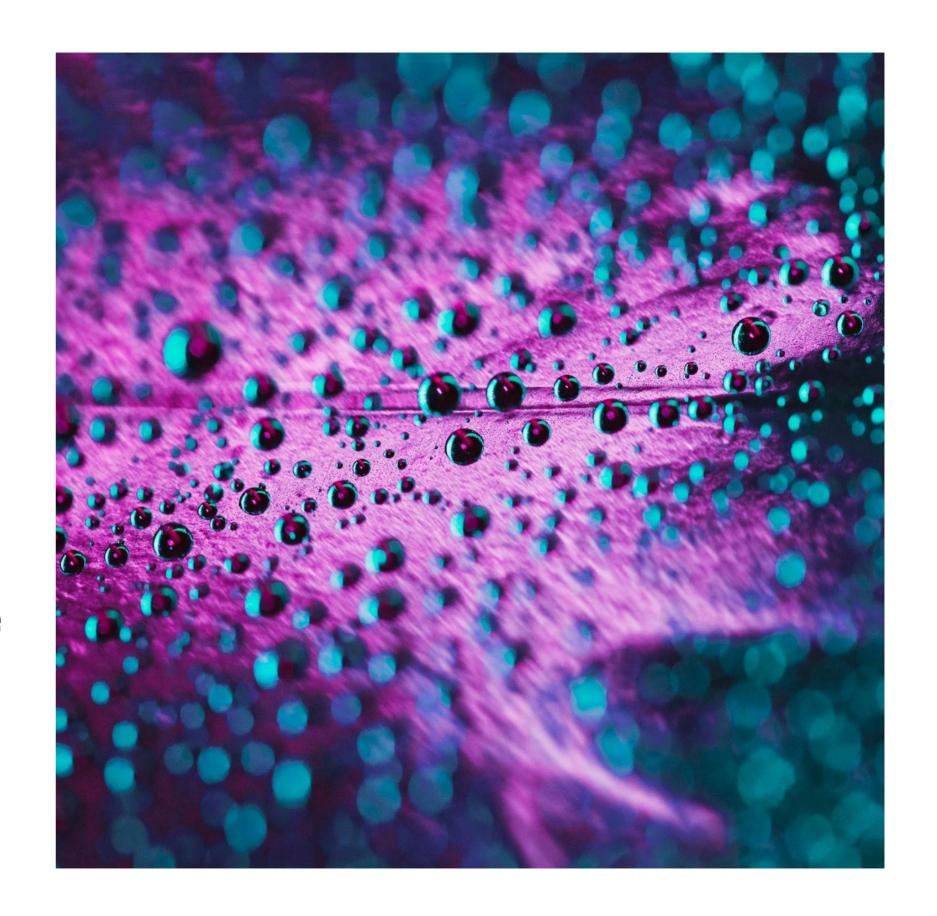


Ataques DDoS: BotNets en Acción

Introducción

En la sociedad actual, casi todos poseen dispositivos electrónicos que facilitan el trabajo y la comunicación, pero también conllevan riesgos como los **ataques DDoS**.

Este trabajo analiza estos ataques, su funcionamiento y tipos, destacando la importancia de entenderlos para configurar servidores y firewalls que minimicen los daños.



Objetivos

El objetivo principal es comprender y mitigar los riesgos de los ataques DDoS, mejorando la seguridad y continuidad de sistemas y servicios.



¿Qué es un Ataque DDoS?

Un ataque de denegación de servicio distribuido (DDoS) es un intento de hacer que un recurso en línea sea inaccesible para sus usuarios. Los atacantes utilizan BotNets para coordinar los ataques y sobrecargar los servidores.



Funcionamiento de una BotNet

Una **BotNet** es una red de dispositivos infectados controlados por un atacante. Estos dispositivos, conocidos como *bots*, actúan en conjunto para lanzar ataques coordinados, aprovechando su poder de cómputo combinado.



Técnicas de Ataque DDoS

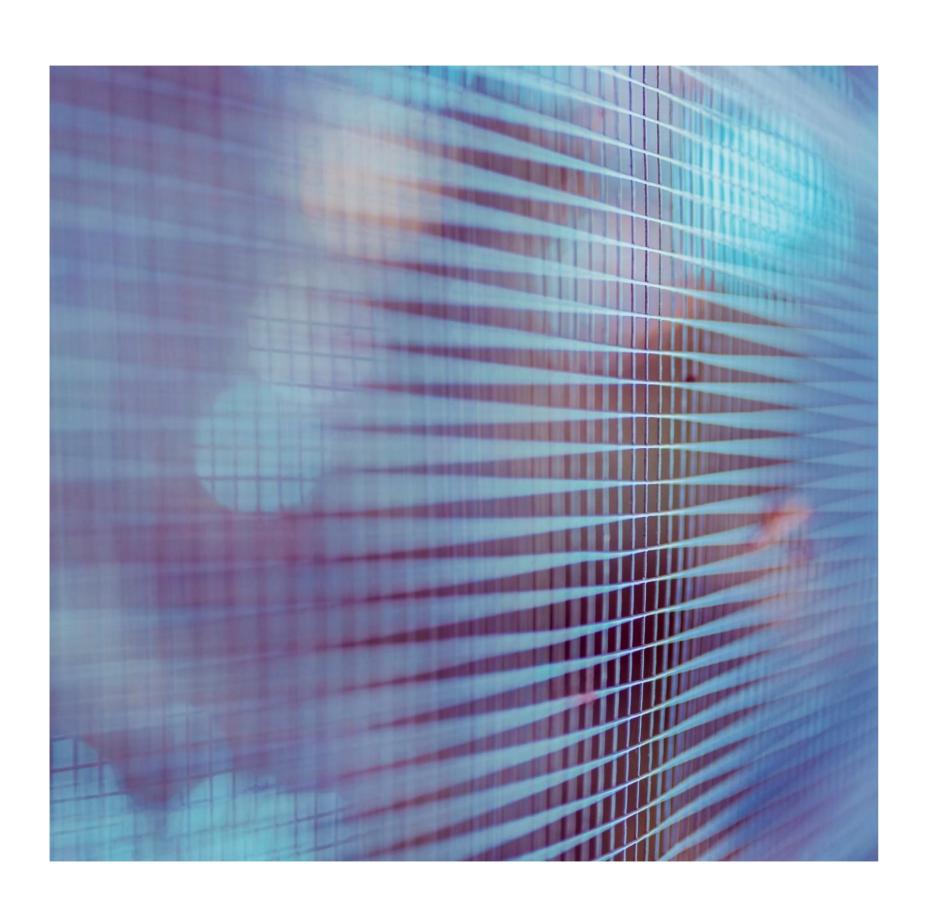
Los atacantes utilizan diversas técnicas, como el ataque de inundación UDP, el ataque SYN Flood y el ataque de solicitud HTTP falsa, para saturar los recursos del servidor y causar la denegación de servicio.



Medidas de Defensa

La defensa contra los **ataques DDoS** implica la implementación de **firewalls**, la **limitación de tráfico sospechoso** y el uso de servicios de **mitigación de DDoS**. La detección temprana y la respuesta rápida son fundamentales.





Conclusión

En conclusión, comprender la **los ataques DDoS** y el papel de las *BotNets* es crucial para proteger los recursos en línea. La prevención, detección y respuesta efectivas son fundamentales para mitigar el impacto de estos ataques.

Thanks!

Do you have any questions?