DDoS va Botnetlar haqida @MarshSecurity tomonidan article … maqola quyi qismini o’qishni unutmang

BOTNET & DDOS

DDoS (Distributed Denial of Service) hujumlarining maqsadi, maqsadlangan tizim yoki tarmoqni hamjihat qilish uchun katta miqdordagi trafikni yaratib, uning ishini to'xtatishdir. Bu seranganlar adolatsiz odamlar yoki guruhlar tomonidan amalga oshiriladi.

Botnet, "botmaster" yoki "bot herder" deb ataluvchi biror shaxs yoki guruhning nazoratida bo'lgan tarmoqdir. Bu tarmoqda "botlar" yoki "zombilar" deyiladi. Botnetning asosiy maqsadi, kompyuterlarni infeksiyalaydigan zararli dasturlar yordamida, zararkunandalar tomonidan nazorat qilinadigan kompyuterlarni birlashtirishdir.

Botnetning asosiy vazifasi botlarni birlashtirish va birlashtirishdan so'ng uni hamjihat qilishdir. Botlar, kompyuterlarga yuborilgan bot-malware orqali infeksiyalanadi. Infeksiyalangan kompyuterlarni nazorat qilish uchun "botmaster"ga aloqa o'rnatiladi. Bu botmasterga infeksiyalangan kompyuterlar ustidan so'rovlar yuborilishi mumkin.

Botnetlarda DDoS hujumlarini amalga oshirish uchun bir nechta botlardan foydalaniladi. Bir nechta botlar biriktirilganda, maqsadlangan tizim yoki tarmoqga yo'l qo'yish uchun katta miqdordagi trafik yaratish mumkin. Bu trafik yaratilganda, maqsadlangan tizim yoki tarmoq foydalanuvchilar uchun erkinlikni ta'minlash uchun yetersiz qoladi.

DDoS seranganlarda quyidagi xususiyatlardan foydalaniladi:

- UDP shovqi: Katta miqdordagi UDP paketlarini maqsadlangan tizimga yo'l qo'yish orqali tarmoq bandvidini sarflash.

- TCP SYN shovqi: Katta miqdordagi SYN so'rovlarni maqsadlangan tizimga yo'l qo'yib, uning resurslarini sarflash.

- HTTP shovqi: Katta miqdordagi HTTP so'rovlarni yuborish orqali veb-sayt yoki dastur qo'llaniladigan tizimni yo'l qo'yish.

- DNS amplifikatsiyasi: DNS serverlarni iste'mol qilib, katta miqdordagi trafikni maqsadlangan tizimga yo'l qo'yish.

Botnetlar nazoratga olinishni va bartaraf etishni qiyinlashtirish uchun turli usullardan foydalanishadi. Bu usullar orasida domen generatsiya algoritmlarini (DGA) ishlatish, IP manzillarini o'zgartirish, shifrlash va noaniqlashtirishni kiritish, markaziy server yordamida emas, balki Peer-to-Peer (P2P) kommunikatsiyasidan foydalanish kiritiladi.

DDoS va Botnetlar katta ta'sirga ega bo'lishi mumkin. Ular xizmatlar yo'q qilinadi, tashkilotning reputatsiyasiga zarar yetkazishi mumkin va moliyaviy izchilliklarni olib kelishi mumkin. DDoS hujumlarga qarshi kurashish uchun tarmoqni monitoring qilish, trafikni analiz qilish, IP manzillarini cheklash, DDoS himoyasini ta'minlash va kuchli xavfsizlik qoidalarni amalga oshirish kabi turli muhofaza usullaridan foydalaniladi.

Botnetlar va DDoS da yoki hujumlarga ishtirok etish qonuniy holatlarda jinoyat hisoblanadi. Bu ma'lumotlar faqat o'qish maqsadida taqdim etilgan.