Ramazan KAHRAMAN

Denial-of-Service (DoS) / Trojan Malware

Abstract:

Denial-of-Service (DoS)-Angriffe sollen die Funktionalität eines Dienstes oder Systems reduzieren oder zerstören. Ein DoS-Angriff kann auch dazu dienen, die Kommunikation zwischen der Opfersite und ihren Benutzern/Clients zu behindern.

Klassifizierung: Paketvolumen und Anzahl der Angreifer

Verbreitungsweg/Angriffsvektor: Die normalen Datenverkehr eines anvisierten Servers, Dienstes oder Netzwerks zu stören

Technischer Infektionsvektor: Durch die schiere Menge an Verkehr erzielt, mit dem die Angreifer das Opfer überschwemmen

Schadfunktion/Ziel: Dienstes, Systems und Servers

DoS-Angriffe ist ein Angriff, die legitimen Benutzern die Verfügbarkeit von Ressourcen und Diensten durch absichtliche Handlungen verweigern, die die Leistung stark beeinträchtigen oder zu einem völligen Ausfall führen. Wir heben zwei Klassen von DoS-Angriffen hervor:

I. Eine Klasse nutzt latente Implementierungsfehler (Software-Schwachstellen) aus.

II. Eine zweite erschöpft Ressourcen (Bandbreite, CPU, Hauptspeicher, Festplatte), indem sie durch das Verkehrsaufkommen überflutet wird, oder indem feste Ressourcen verbraucht werden oder ressourcenintensive Operationen angefordert werden (z. B. Erzeugung asymmetrischer Schlüsselpaare).

Ein Flooding-Angriff kann sogar durch eine einzelne Angriffsmaschine möglich sein, die nur durch ihre CPU-Geschwindigkeit und Verbindungskapazität begrenzt ist und kontinuierlich Pakete an ein Ziel sendet. Solche Angriffe mit hoher Paketrate können Asymmetrien der Verbindungsgeschwindigkeit ausnutzen, d. h. Hosts mit Verbindungen mit hoher Bandbreite verwenden, um Ziele mit Verbindungen mit niedrigerer Bandbreite anzugreifen.

Ein Distributed Denial of Service (DDoS)-Flooding-Angriff ist ein Angriff, bei dem eine große Anzahl von Geräten über eine Vielzahl von Adressen hinweg verwendet wird (z. B. unter Verwendung eines Botnets).

Botnets sind kleine Programme, die auf verschiedenen Maschinen laufen und mit einer Kommandozentrale kommunizieren. Sie werden für viele böswillige Zwecke verwendet.Mitte Juni 2020 wehrte Amazon beispielsweise einen Rekordangriff auf seine Server ab. Mehr als drei Tage lang wurden die Webdienste von Amazon mit einem Datenstrom von 2,3 Terabyte pro Sekunde ins Visier genommen. Es braucht ein riesiges Botnet, um diese Art von Rechenleistung zu erhalten.

Die Computer, die Botnets erstellen, können als Zombie-Computer bezeichnet werden.Ein pulsierender Zombie wird verwendet, um intermittierende DoS-Angriffe auszuführen. Anstatt einen kontinuierlichen Strom von Angriffsdatenverkehr auszusenden, sendet ein pulsierender Zombie Angriffsdatenverkehr in unvorhersehbaren Bursts aus, die randomisiert sind, um das Erkennungsrisiko

zu verringern. Dies macht angreifende Maschinen schwerer zu verfolgen und kann verwendet werden, um die Fähigkeit zu demonstrieren, einen Angriff zum Zwecke der Erpressung zu starten.

Conclusion:

DoS-Angriffe sind per Definition leicht zu erkennen, vollständige Lösungen erscheinen jedoch unwahrscheinlich.

Quellen:

- David Harley, Ken Bechtel, Michael Blanchard, Henk K. Diemer, Andrew Lee, Igor Muttik, Bojan Zdrnja - AVIEN Malware Defense Guide for the Enterprise (2007, Syngress)

- Fahad Ali Sarwar - Python Ethical Hacking from Scratch Think like an ethical hacker, avoid detection, and successfully develop, deploy, detect, an (2021, Packt Publishing)

- Paul C. van Oorschot - Computer Security and the Internet - Tools and Jewels from Malware to Bitcoin-Springer (2021, Springer)

- Cyber Security Center - Bereich Prävention - Distributed Denial of Service (DDoS) Hintergründe, präventive Maßnahmen und Mitigationsmaßnahmen (2020, Digitalprintcenter des BMI)