C2-Frameworks:
Wie Angreifer Systeme kontrollieren

8COM
CYBER SECURITY

1
Grundlagen C2-Frameworks

2
Demo

3
Verteidigung in der Tiefe

8COM
CYBER SECURITY

Fighting Cybercrime

C2-Frameworks:
Wie Angreifer Systeme kontrollieren

8COM
CYBER SECURITY

1 Grundlagen C2-Frameworks

Fighting Cybercrime

Grundlagen C2-Frameworks

Was ist ein C2-Framework

Ein C2-Framework ist Schadsoftware, welche es einem Angreifer ermöglicht Systeme zu kontrollieren und weitere Aktionen auszuführen. Der Fokus liegt dabei auf OPSEC (Operational Security).

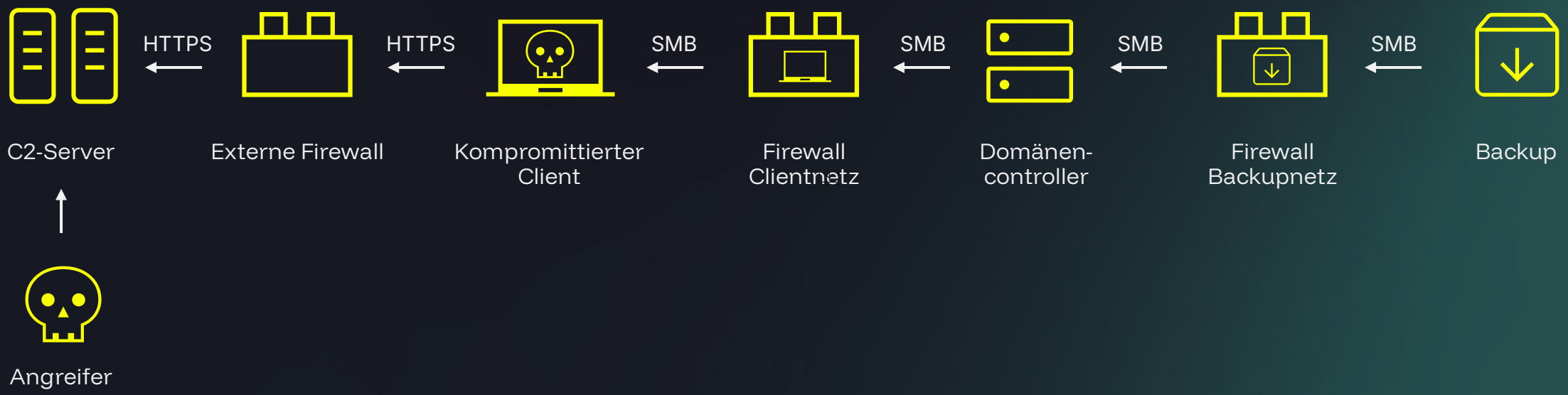
- C2-Server: Hauptkomponente
- C2-Client: Kommunikation der Angreifer mit dem Server und Agents
- C2-Agent (Beacon): Kommunikation der kompromittierten Systeme mit dem Server

Grundlagen C2-Frameworks

Wie funktionieren C2-Frameworks

- Ausgehende Verbindung über HTTPS oder DNS
- Angreifer hinterlegen Aufgaben (Tasks) für Agents auf C2-Server
- Beacon Verbinden sich regelmäßig mit dem C2-Server
- Agents beziehen neue Tasks vom Server und geben Information zurück

Grundlagen C2-Frameworks



Grundlagen C2-Frameworks

Warum verwenden Angreifer C2-Frameworks

- OPSEC
- Funktionalität
- Erweiterbarkeit (BOFs, execute-assembly)
- Skalierbarkeit (mehrere Clients/Operatoren)

C2-Frameworks: Wie Angreifer Systeme kontrollieren

8COM CYBER SECURITY

2 Demo

Fighting Cybercrime

C2-Frameworks: Wie Angreifer Systeme kontrollieren

8COM CYBER SECURITY

3 Verteidigung in der Tiefe

Fighting Cybercrime

Verteidigung in der Tiefe

Sicherheitsstrategie bei der mehrere Verteidigungsmaßnahmen eingesetzt werden, um Angriffe zu verhindern bzw. zu verlangsamen.

- Erhöhte Ausfallsicherheit
- Erhöhte Sichtbarkeit
- Erhöhte Sicherheit

Verteidigung in der Tiefe

- Technisch
  - EDR/XDR, SIEM, IDS
- Administrativ
  - Prozesse, Tiering Model, Zero Trust
- Physisch
  - Zutrittskontrolle, Kameras, Sicherheitszonen
- Präventiv
  - Regelmäßige Pentests, Patch-Management, Netzwerksegmentierung

Sie haben noch Fragen?

Sprechen Sie mich gerne an!

8COM
CYBER SECURITY

Robin Meier
Penetration Tester

robin.meier@8com.de
www.8com.de

8com.de/newsletter