Was ist ein Smurf-Angriff?

Smurf-Angriffe sind eine Unterkategorie der DDoS-Angriffe. Sie basieren auf der Smurf-Malware - von wo auch der Name erschien. Smurf- Angriffe sind laut [1] Verstärkungsvektoren, die das Schadenspotenzial erhöhen, indem sie die Schwäche eines Rundfunknetzes ausnutzen. Es ist leicht, die Smurf-Malware aus infizierten Quellen zu versehen, so wie ein Smurf-Trojaner. Die Malware ist ausgeblendet, bis sie von einem Remote-Benutzer aktiviert wird. Da es "schläft"(inaktiv ist), kann es ein Bündel Rootkits enthalten, die es dem Hacker ermöglichen, Hintertüren im infizierten System zu öffnen. Manchmal ein Smurf-Angriff, wenn es erfolgreich ist, lähmt das System von Stunden bis Tage und kann unheimliche Szenarien abdecken, in welchen Dateien und Informationen gestohlen werden.

In [1] wird ein Szenario eines Smurf-Angriffs beschrieben:

Smurf-Malware wird verwendet, um eine gefälschte Echo-Anforderung zu generieren, die eine gefälschte Quell-IP enthält, die eigentlich die Zielserveradresse ist.

Die Anfrage wird an ein zwischengeschaltetes IP-Broadcast-Netzwerk gesendet.

Die Anforderung wird an alle Netzwerkhosts im Netzwerk übertragen.

Jeder Host sendet eine ICMP-Antwort an die gefälschte Quelladresse.

Wenn genügend ICMP-Antworten weitergeleitet wurden, wird der Zielserver heruntergefahren.

Es ist wichtig zu wissen, dass der Angriff umso stärker ist, je mehr Hosts vorhanden sind, da der Verstärkungsfaktor mit der Anzahl der Hosts korreliert ist [1].

Eine andere Quelle [3] definiert, dass ein Smurf-Angriff in zwei Kategorien unterteilt werden kann:

Der grundlegende Angriff: Wo sich das Opfer in der Mitte des ICMP-Anforderungspakets befindet. Wenn sich die Pakete korrekt verteilen, antwortet jedes Gerät, das eine Verbindung zum Netzwerk herstellt, auf die ICMP-Anforderung. Dies führt dazu, dass die Bandbreite "aufgebraucht" wird, was zu einer Menge Verkehr führt und letztendlich das System zerstört.

Ein anderer Typ ist der erweiterte Angriff: Er beginnt wie der grundlegende Angriff, sendet jedoch die Antworten an einem drietter Opfer. Dies bedeutet, dass die Hacker einen größeren Teil des Netzwerks verlangsamen, als das, was sie mit nur einem Opfer erreichen würden.

Wie bekämpft man einen Smurf-Angriff?

Eine Möglichkeit besteht darin, die IP-Broadcast-Adresse auf dem Netzwerkrouter zu deaktivieren. Diese Funktion wird selten verwendet und wenn sie deaktiviert ist, kann der Hacker das Netzwerk nicht überfordern. Wie bei anderen DDoS-Angriffen ist eine robuste Präventionsmethode erforderlich, um Anomalien zu überwachen und zu erkennen.

Der Smurf-Angriff klingt wie ein Kinder-Cartoon, stellt jedoch eine echte Bedrohung dar: der Server und Netzwerke werden überlastet. Die wichtigsten Schutzmaßnahmen laut [2] sind sicherzustellen, dass der gerichtete Broadcast-Verkehr blockiert wird, und die Hosts und Router müssen so konfiguriert werden, dass sie nicht auf ICMP-Echoanforderungen reagieren.