Ce este un atac smurf?

Atacurile Smurf sunt o subcategorie a atacurilor DDoS. Ele se bazează pe malware-ul smurf - de unde a apărut și numele. În conformitate cu [1] atacurile smurf sunt vectori de amplificare, care sporesc potențialul de distrugere prin abuzul slabiciuni unui sistem. Este ușor să înhați accidental malware-ul smurf, după [2] un virus troian, din surse infectate. Malware-ul este ascuns până când este activat de la distanță de un utilizator. Deoarece "doarme", poate avea un pachet de rootkituri, care permit hackerului să acceseze sistemul infectat fără ca victima sa observe. Uneori, un atac smurf, dacă a avut succes, oprește sistemul pentru ore sau zile la rând și poate acoperi mai multe scenarii sinistre unde fișiere și informații sunt furate.

În [1] este exemplificat un scenariu de atac smurf:

Smurf malware este folosit pentru a genera o cerere falsă de ecou conținând sursa IP falsă, care este de fapt adresa serverului țintă.

Cererea este trimisă la o rețea IP intermediară.

Cererea este transmisă tuturor host-urilor din rețea.

Fiecare host trimite un răspuns ICMP la adresa sursă falsificată

Odată cu trimiterea suficientelor răspunsuri ICMP, serverul țintă este redus.

Important de știut este că cu cât mai multe hosts există cu atât mai puternic este atacul, deoarece factorul de amplificare este corelat cu numărul de hosts [1].

O altă sursă, [3], definește faptul că un atac smurf poate fi împărțit în două categorii:

Atacul de bază: unde victima se află în mijlocul puhoiului de pachete de solicitare ICMP. Dacă pachetele se dispersează corect, atunci orice dispozitiv care se conectează la rețea va răspunde solicitării ICMP. Acest lucru conduce la folosirea memoriei aproape in totalitate, aceasta fiind "mâncată", rezultând un trafic mare de date și distrugerea sistemului în final.

Un alt tip este atacul avansat: începe precum atacul de bază, dar redirecționează răspunsurile la o noua victimă. Asta înseamnă că hackerii încetinesc o parte mai mare a rețelei, decât ceea ce ar reuși să realizeze cu o singură victimă.

Cum putem combate un atac smurf?

Una dintre modalitati este de a dezactiva adresa de difuzare IP pe routerul rețelei. Este o funcție rar utilizată, iar dacă este dezactivată este imposibil ca hackerul să dărâme rețeaua. La fel ca în cazul altor atacuri DDoS, este necesară o metodă robustă de prevenire pentru a monitoriza și detecta anomaliile.

Atacul smurf sună precum un desen animat pentru copii, dar reprezintă o adevărată amenințare dacă serverele / rețelele sunt atacate. Cele mai importante măsuri de protecție, în conformitate cu [2], sunt asigurarea faptului că traficul direct de rețea este blocat și iar configurarea host-ului/ routerelor este programata să nu răspundă la solicitările de ecou ICMP.