Ce este atacul calul troian?

Printre amenințările cele mai grave și periculoase cand vine vorba de atacuri cibernetice, trebuie sa mentionam calul troian. Acesta este reprezentat de un fișier executabil în sistemul de operare Windows care detine diferite caracteristici specifice.

Dintre toate tipurile de atacuri, calul troian este cea mai populară și mai folosită formă de atac asupra computerelor. Chiar si numele sugerează faptul că are capacitatea de a înșela utilizatorul în a gândi că programul folosit rulează o acțiune autorizată de el atunci când, de fapt, este menit să manipuleze sistemul.

În funcție de acțiunea dăunătoare care e menit sa o intreprinda, troianul poate fi clasificat în cinci categorii:

1. Remote access Trojan: oferă atacatorului acces nelimitat la sistem, permițându-i să acceseze, să modifice, să distrugă și să fure date private, informații personale de identificare, precum și proprietate intelectuală.

2. Data sending Trojan: este conceput pentru a trimite date delicate, cum ar fi informații financiare, date de log-in in diferite conturi, detalii despre contul bancar și multe altele către hacker.

3. Destructive Trojan: este creat cu intenția de a distruge anumite fișiere din system, de asemenea nu poate fi detectat de aplicații anti-virus.

4. Security software disabler Trojan: are scopul de a face sistemul vulnerabil prin dezactivarea tuturor serviciilor de securitate, cum ar fi firewall-uri și antivirusuri.

5. Denial-of-Service attack Trojan: este menit să mențină sistemul ocupat astfel încât să nu poată fi efectuate nici o cerere de utilizator.

Cum detectam un asemenea atac?

Cea mai obișnuită modalitate de a detecta un software periculos este utilizarea de aplicații antivirus, însă aceștia s-au dovedit a fi ineficienți atunci când este vorba de detectarea cailor troieni datorită proprietății polimorfismice a acestuia.

Deoarece aceste fișiere sunt făcute pentru a înșela, este dificil să se facă diferența între fișierele răuvoitoare și cele legitime. De asemenea, colectarea semnăturilor tuturor cailor troieni și menținerea lor la zi într-o baza de date, este nu numai dificil de gestionat, ci datorită faptului că fisiere noi sunt scriptizate în fiecare zi, este cu totul imposibil.

Este important de observat că acele fișiere executabile dăunătoare posedă anumite proprietăți care ne permit să le distingem de cele legitime.

În loc să utilizeze semnături, o modalitate mai eficientă de detectare a fișierelor infectate este de a izola procesele și programele suspecte pe baza proprietăților și a comportamentului acestora.

Programe precum "Wireshark" pot fi utilizate pentru a monitoriza activitățile și procesele din sistem și a ne informa de fiecare dată când are loc o activitate sau un proces necunoscut.

Masuri de precautie