VRSTE SAJBER NAPADA

CIRT.ME

Sajber napad je pokušaj otkrivanja, izmjene, onemogućavanja, uništavanja, krađe ili neovlašćenog pristupa računarskom sistemu, infrastrukturi, mreži ili bilo kom drugom pametnom uređaju.

Sajber kriminalci koriste razne metode za pokretanje napada, među kojima su najčešće fišing, ransomver, distribuirano uskraćivanje usluga (DDoS) i razne vrste malvera.

1 FIŠING (eng. phishing)

Fišing je vrsta napada metodama socijalnog inženjeringa koja ima za cilj da prevarom dođe do korisnikovih podataka koji služe za potvrdu identiteta, kao što su lozinke, brojevi kreditnih kartica, podaci o bankovnim računima i slično.

Smišing (eng. smishing) predstavlja vrstu fišing napada koji se vrši putem SMS-a na mobilnim telefonima.

Višing (eng. vishing) predstavlja vrstu fišing napada koja se vrši putem telefonskih poziva ili VoIP servisa.

2 MALVER (eng. malware)

Malver je zlonamjerni softver koji je napisan u maliciozne svrhe, odnosno koji ima cilj da nanese štetu računarskim sistemima ili mrežama.

Najčešće vrste malvera su:

- virusi,
- crvi,
- trojanci,
- botovi,
- ransomver (ransomware),
- bekdor (backdoor),
- spajver (spyware),
- i adver (adware).

3 RANSOMVER (eng. ransomware)

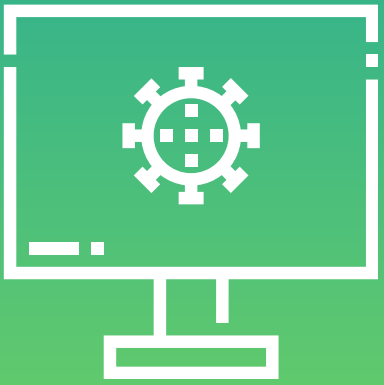
Ransomver je vrsta zlonamjernog softvera koji zaključava korisničke datoteke ili neprestano blokira pristup istim. Koristi tehniku šifrovanja podataka, čineći ih nedostupnim i zahtijeva plaćanje otkupnine u zamjenu za omogućavanje pristupa podacima.

Ransomver se širi na različite načine uključujući fišing poruke elektronske pošte ili otvaranje zaraženih internet stranica.

4 VIRUSI

Virusi su najčešći zlonamjerni softveri koji se šire sa jednog računara na drugi. Šire se tako što se virus priključi na izvršnu datoteku, što znači da može postojati na sistemu, ali neće biti aktivan i neće se širiti dok korisnik ne pokrene ili otvori zlonamjernu host datoteku ili program.

Mogu se prenositi sa jednog računara na drugi koristeći mrežu, disk, dijeljenjem datoteka ili putem zaraženog priloga u elektronskoj pošti.



5 CRVI

Crvi su slični virusima po tome što umnožavaju sami sebe ali za razliku od virusa, ne inficiraju druge programe.

Nije im neophodna ljudska interakcija za širenje, već za to koristi različite ranjivosti u programima i operativnim sistemima.

Crv koji se aktivirao u sistemu može da izazove mnogo neprijatnosti: može da izbriše datoteke, umanji performanse sistema ili deaktivira programe.

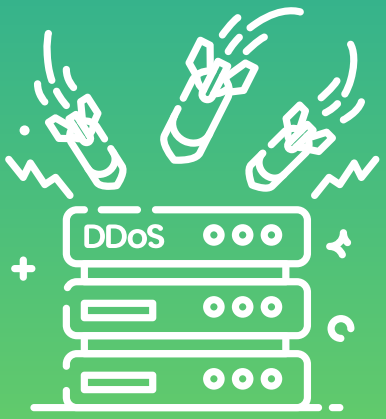
6

TROJANCI

Trojanac je vrsta zlonamjernog softvera koji izgleda legitimno ali u pozadini otvara mogućnost zlonamjernim korisnicima da pristupe sistemu. Za razliku od virusa i crva, trojanci se ne razmnožavaju inficiranjem drugih datoteka niti se samostalno umnožavaju. Trojanci se najčešće šire preko priloga elektronske pošte ili preuzimanjem i pokretanjem datoteka sa interneta sa neprovjerenih izvora.

7

DDoS NAPADI



DDoS (Distributed Denial of Service) napad je vrsta sajber napada koja ima za cilj da onesposobi online servis, mrežu ili veb stranicu tako što će opteretiti ciljani sistem ogromnim brojem zahtjeva. Napadači koriste mrežu računara ili uređaja koji su zaraženi zlonamjernim softverom (botnet) kako bi sinhronizovano poslali veliki broj zahtjeva ka ciljanoj mreži, preopterećujući je i čineći je nedostupnom za legitimne korisnike.

8

KRAĐA IDENTITETA

Krađa identiteta se definiše kao proces korišćenja tuđih podataka sa ciljem ostvarivanja direktne koristi, radi dobijanja finansijskih zarada i drugih pogodnosti na osnovu zloupotrijebljenog identiteta. Najčešći primjeri krađe identiteta su putem elektronske pošte, zlonamjernih softvera i slično... Sve što je povezano sa internetom može biti iskorišćeno za napad na korisnika, bilo da je u pitanju veb stranica, e-mail nalog, baza podataka i slično.

OPŠTE PREPORUKE ZA ZAŠTITU OD SAJBER NAPADA

- **REDOVNO AŽURIRAJTE OPERATIVNI SISTEM I ANTIVIRUSNI SOFTVER**
- **REDOVNO KREIRAJTE REZERVNE KOPIJE**
- **KREIRAJTE KOMPLEKSNE LOZINKE**
- **KORISTITE DVOFAKTORSKU AUTENTIFIKACIJU**
- **AKTIVIRAJTE ANTIVIRUS I KOMPLETNO SKENIRANJE UREĐAJA**

CIRT.ME