TEHNIČKA ŠKOLA RUĐERA BOŠKOVIĆA

SEMINARSKI RAD IZ RAČUNALNIH MREŽA

BLACK HAT HAKERI: TAMNA STRANA HAKIRANJA I NJIHOV UTJECAJ NA DIGITALNI SVIJET

Niko Marinović, 3.G

Zagreb, svibanj, 2025.

SADRŽAJ

1. Uvod

Kibernetička sigurnost postala je ključni element modernog društva, budući da je sve veći broj svakodnevnih aktivnosti prebačen u digitalni prostor. Od bankarskih transakcija do komunikacije, privatnih i poslovnih podataka – gotovo sve se danas odvija online. U tom kontekstu, pojam "hakiranje" zauzima centralno mjesto, a razni oblici hakiranja nose različite konotacije i posljedice. Posebno su zabrinjavajući tzv. *black hat* hakeri – pojedinci ili grupe koji koriste svoje vještine za zlonamjerne i ilegalne svrhe.

Black hat hakeri predstavljaju značajnu prijetnju ne samo pojedincima, već i državama, korporacijama te globalnoj infrastrukturi. Njihove aktivnosti obuhvaćaju krađu podataka, ucjenjivanje, špijunažu, sabotažu i stvaranje kaosa. Cilj ovog rada je istražiti tko su zapravo black hat hakeri, što ih motivira, koje metode koriste, koji su poznati primjeri njihove aktivnosti i kako se svijet bori protiv njih.

2. Tko su black hat hakeri?

2.1 Definicija pojma "black hat" haker

Pojam "black hat" haker odnosi se na osobu koja koristi svoje računalne vještine za nelegalne i štetne aktivnosti. Ime potječe iz starih western filmova, gdje su negativci nosili crne šešire. Black hat hakeri provaljuju u sustave bez dopuštenja, kradu informacije, ometaju usluge i često nanose veliku financijsku i reputacijsku štetu svojim žrtvama.

2.2 Povijesni pregled pojave hakera

Hakeri su se prvi put pojavili sredinom 20. stoljeća kao entuzijasti koji su eksperimentirali s računalima i pokušavali unaprijediti tehnologiju. Tijekom vremena razvila se razlika među hakerima – na one koji djeluju etički i oni koji djeluju zlonamjerno. Podjela na *white hat* (etičke), *grey hat* (neutralne) i *black hat* (zlonamjerne) hakere postala je standard.

2.3 Razlika između black hat i white hat hakera

White hat hakeri djeluju u skladu sa zakonom i etikom. Oni pomažu organizacijama da otkriju ranjivosti u svojim sustavima i spriječe napade. Suprotno tome, black hat hakeri koriste te ranjivosti za vlastitu korist ili kako bi naštetili drugima. White hat hakeri često surađuju s tvrtkama, vladama i sigurnosnim agencijama, dok su black hat hakeri uglavnom u sukobu sa zakonom.

3. Motivacije black hat hakera

3.1 Financijska dobit

Jedan od najčešćih motiva black hat hakera je financijska korist. Kroz krađu podataka, krađu identiteta, ucjene pomoću ransomwarea ili ilegalnu prodaju informacija na dark webu, ovi hakeri ostvaruju značajne zarade.

3.2 Ideološki ili politički razlozi (hacktivizam)

Neki black hat hakeri djeluju vođeni ideološkim ili političkim uvjerenjima. Njihove akcije često su usmjerene na vlade, korporacije ili organizacije koje smatraju nepravednima. Grupa Anonymous poznata je po takvim napadima.

3.3 Moć, slava i izazov

Pojedinci se uključuju u hakerske aktivnosti iz želje za dokazivanjem, stjecanjem ugleda unutar hakerske zajednice ili radi adrenalina koji pruža izazov probijanja sigurnosnih sustava.

3.4 Industrijska i državna špijunaža

Države i korporacije ponekad unajmljuju ili sponzoriraju hakere da bi došli do povjerljivih informacija konkurenata ili stranih vlada. Ovakva špijunaža može imati dalekosežne posljedice na geopolitiku i tržišta.

3.5 Psihološki faktori

Neki hakeri imaju osobne razloge – osjećaj neprihvaćenosti, frustracije, antisocijalna ponašanja ili čak psihopatološke osobine. Motivacija može biti i unutarnji bijes prema sustavu ili društvu.

4. Najčešće metode i alati black hat hakera

4.1 Phishing i socijalni inženjering

Ova metoda podrazumijeva manipulaciju korisnika kako bi dobrovoljno otkrili osjetljive podatke. Phishing napadi često dolaze u obliku lažnih e-mailova koji izgledaju kao da dolaze iz pouzdanog izvora.

4.2 Malware
Zlonamjerni softver uključuje viruse, trojance, spyware i ransomware. Malware omogućuje hakerima da preuzmu kontrolu nad računalima, prikupljaju podatke ili blokiraju pristup dok se ne isplati otkupnina.

4.3 DDoS napadi
Distribuirani napadi uskraćivanja usluge (DDoS) koriste velik broj zaraženih uređaja kako bi preopteretili servere ciljanih sustava i učinili ih nedostupnima korisnicima.

4.4 Eksploatacija ranjivosti
Zero-day exploit odnosi se na ranjivosti koje još nisu poznate proizvođačima softvera. Black hat hakeri koriste ove slabosti prije nego što ih se uspije zakrpati.

4.5 Dark web i prodaja ukradenih podataka
Na dark webu se često trguje ukradenim informacijama – brojevima kreditnih kartica, osobnim podacima, lozinkama i slično. To je važno tržište za mnoge hakere.

4.6 Primjeri popularnih alata
Alati poput Metasploit, Wireshark, John the Ripper, i Hydra koriste se za testiranje i probijanje sigurnosnih sustava, ali i u zlonamjerne svrhe.

5. Poznati primjeri black hat hakera

5.1 Kevin Mitnick
Jedan od najpoznatijih hakera 20. stoljeća. Uhićen je zbog krađe softvera i hakiranja velikih korporacija poput Nokia i IBM. Danas radi kao konzultant za sigurnost.

5.2 Anonymous
Decentralizirana hakerska grupa poznata po napadima na vladine institucije, crkve, korporacije. Djeluju iz ideoloških razloga.

5.3 WannaCry ransomware napad
Napad iz 2017. zahvatio je stotine tisuća računala u preko 150 zemalja. Uzrokovao je ogromne štete, osobito u britanskom NHS-u (zdravstvenom sustavu).

5.4 Sony Pictures hack
U 2014. godini, Sony Pictures je pretrpio težak napad koji je rezultirao curenjem osjetljivih podataka i filmova. Napad je navodno povezan sa Sjevernom Korejom.

6. Posljedice napada black hat hakera

6.1 Financijske štete
Tvrtke i pojedinci mogu izgubiti milijune dolara zbog gubitka podataka, prekida poslovanja i reputacijskih šteta.

6.2 Krađa osobnih podataka
Ukradeni osobni podaci često završe na dark webu i mogu se koristiti za krađu identiteta, prijevare i ucjene.

6.3 Utjecaj na sigurnost država
Napadi na vladine agencije, elektrane, bolnice i slične infrastrukture mogu imati razorne posljedice po nacionalnu sigurnost.

6.4 Psihološki i društveni utjecaji
Ljudi koji su žrtve hakiranja mogu razviti strah, nepovjerenje prema tehnologiji i stresne poremećaje.

7. Zaštita i borba protiv black hat hakera

7.1 Sigurnosne mjere
Firewall, antivirusni programi, enkripcija podataka, dvofaktorska autentifikacija i redovno ažuriranje sustava osnovni su koraci zaštite.

7.2 Uloga etičkih hakera
White hat hakeri provode penetracijsko testiranje i savjetuju organizacije kako se zaštititi. Oni su ključni saveznik u borbi protiv prijetnji.

7.3 Policija i sigurnosne agencije

Organizacije poput FBI-a, Europola i INTERPOL-a imaju specijalizirane jedinice za kibernetički kriminal i

često surađuju međunarodno.

7.4 Zakonodavstvo i kazne

Mnoge zemlje su donijele stroge zakone protiv kibernetičkog kriminala. Hakeri se mogu suočiti s višegodišnjim zatvorskim kaznama.

7.5 Edukacija korisnika

Edukacija korisnika o prepoznavanju phishing napada, važnosti sigurnih lozinki i digitalne higijene je jedan od najvažnijih alata u borbi protiv hakera.

8. Zaključak

Black hat hakeri predstavljaju jednu od najozbiljnijih prijetnji digitalnom svijetu. Njihove metode su sofisticirane, motivacije raznolike, a posljedice razorne. Ključno je razumjeti kako oni djeluju, zašto to rade i kako ih možemo spriječiti.

Budućnost kibernetičke sigurnosti leži u tehnološkom razvoju, međunarodnoj suradnji i edukaciji korisnika. Svi sudionici digitalnog društva – od pojedinaca do vlada – imaju odgovornost u zaštiti svojih podataka i sustava.

Samo kroz informiranost, prevenciju i odlučnu borbu možemo osigurati sigurniji digitalni prostor za sve.