Univerzitet u Kragujevcu
Fakultet inženjerskih nauka

Seminarski rad
Kriptografija

Tema:
Uticaj koji sajber napadi na web i mobilne platforme imaju na preduzeća i javne ustanove

Student:

Jovana Stefanović 622/2020

Predmetni profesor:

Doc. dr Milan Čabarkapa

Kragujevac 2024.

Sadržaj rada

1. Uvod

U poslednjih nekoliko decenija, društveni i ekonomski razvoj uslovljen je razvojem informacionih tehnologija. Ta uslovljenost nosi pretnju, jer paralelno sa razvojem tehnologije i njenom dostupnošću širokom krugu korisnika raste i mogućnost zloupotrebe.

Sa sajber kriminalom problem imaju, kako nerazvijene zemlje i zemlje u tranziciji, tako i zemlje sa razvijenim ekonomijama.

U digitalnom dobu, preduzeća i javne ustanove, uključujući vladine agencije, zdravstvene organizacije, obrazovne institucije i opštinske službe, sve više se oslanjaju na web i mobilne platforme za svoje poslovne operacije, komunikaciju i interakciju s klijentima i građanima. Ove platforme su postale ključne za pristup tržištima, pružanje usluga i povećanje efikasnosti. Međutim, s rastućom digitalizacijom dolazi i povećana izloženost sajber pretnjama. Sajber napadi na web i mobilne platforme predstavljaju ozbiljan rizik, ugrožavajući ne samo podatke i privatnost korisnika, već i integritet i reputaciju preduzeća i javnih ustanova. Ovi napadi mogu imati dalekosežne posledice, ne samo po same institucije, već i po građane koji zavise od njihovih usluga.

Kompanija ,,Kasperski" je tokom 2023. godine analizirala broj sajber napada na mobilne telefone koji je dostigao skoro 33,8 miliona širom sveta, što je više od 50 odsto u odnosu na prethodnu godinu, dok je broj nezabeleženih napada sigurno mnogo veći.

Najnoviji podaci otkrivaju porast napada koji eksploatišu korisnike linux-a. Linux se sve više koristi kao operativni sistem na desktop računarima. U periodu januar-mart 2024. broj napada na linux korisnike je skočio za više od 130 odsto.

2. Pretnje u sajber prostoru

Vera Tasić i Ivan Bauer u Rečniku kompjuterskih termina, sajber prostor definišu kao ,'okruženje virtuelne realnosti (kao što je Internet) u kome osobe komuniciraju pomoću povezanih (umreženih) računara''. [Tasić, Bauer, 2003]

Napadač je osoba koja koristi svoje znanje o informaciono-komunikacionim tehnologijama (IKT) da bi ugrozila bezbednost računarskih sistema. Napadi su slučajevi potencijalnog oštećenja računarskog sistema koje upravlja napadač. Svaka akcija koja narušava bezbednost računarskog sistema smatra se napadom, a napadi mogu biti realizovani od strane korisnika sistema (unutrašnji) ili lica van sistema (spoljašnji). Skup povezanih napada čini incident.

Napadači se mogu podeliti u nekoliko grupa na osnovu njihovog etičkog ponašanja i ciljeva:

1. White Hat hakeri: Ovi hakeri pronalaze bezbednosne propuste iz nesebičnih ili dobronamernih razloga. Koriste iste tehnike i alate kao i potencijalni napadači, ali za razliku od njih, ne oštećuju sistem i ne kradu informacije. Njihov cilj je proceniti bezbednost sistema i obavestiti vlasnika o propustima i načinima njihovog otklanjanja.

2. Black Hat hakeri: Ovi hakeri narušavaju bezbednost sistema bez odobrenja i poznati su kao krekeri (crackers). Često kreiraju zlonamerne programe (računarski virusi, crvi, trojanci) sa ciljem krađe podataka ili oštećenja računarskih sistema.

3. Grey Hat hakeri: Ovi hakeri poseduju veliko znanje o računarima, ali imaju dvostruka etička načela. Oni su mešavina između White Hat i Black Hat hakera. Iako najčešće nemaju zle namere i ne rade radi materijalne koristi, ponekad učestvuju u nezakonitim aktivnostima tokom iskorištavanja bezbednosnih propusta. Njihovi proboji se smatraju manje destruktivnim jer ne uzrokuju štetu, a cilj im je ispitivanje i nadgledanje sistema.

4. Blue Hat hakeri: Velike kompanije ih angažuju da pronađu bezbednosne propuste pre nego što izdaju programske pakete. Na primer, Microsoft organizuje Blue Hat Microsoft Hacker Conference, gde njihovi inženjeri razmenjuju znanja sa Blue Hat hakerima kako bi poboljšali bezbednost svojih proizvoda.

Haktivisti su posebna kategorija hakera, političko-ideološki motivisana, čije je delovanje usmereno protiv informacionih sistema i tehnologija neprijateljskih zemalja i organizacija. Haking se ovde javlja kao sredstvo za skretanje pažnje javnosti na određeni politički ili društveni problem, neka vrsta gerilskog ratovanja u sajber prostoru, pri čemu se generalno šteta ne nanosi neutralnim korisnicima mreže (npr. na određenu web stranicu postave se sadržaji vrednosno kontrastni onima koje promoviše sajt, ili on biva blokiran). Tokom agresije NATO-a na SRJ 1999. godine srpski haktivisti (tačnije među njima najaktivnije grupe: "Crna ruka" i "Srpski anđeli") su napali elektronske baze podataka američkih, britanskih i albanskih vojnih, državnih i obaveštajnih službi i prisvajali i modifikovali određene informacije, u čemu su kasnije su dobili podršku ruskih, a potom i kineskih hakera. Posledica ovih napada bila je višenedeljna

onesposobljenost američkih vojnih informacionih sistema, nakon čega je Federalni istražni biro otpočeo sa hapšenjima američkih hakera da bi se ponovo uspostavila i obezbedila zaštita računarskih sistema, što je pak dovelo do pobune američkih hakerskih grupa.

Svaki računarski sistem ima određene ranjivosti, što predstavlja izazov za njegovu bezbednost. Nedostaci u računarskom sistemu ili njegovim komponentama (zbog grešaka u izradi, instalaciji, implementaciji itd.) otežavaju zaštitu sistema i povećavaju verovatnoću da potencijalne pretnje budu ostvarene. Napadači koriste određene alate i tehnike za iskorišćavanje poznatih ranjivosti. Ranjivosti su tačke slabosti u sistemu, kao što su greške u aplikacijama ili slabosti korisnika, koje mogu dovesti do ugrožavanja poverljivosti, integriteta ili dostupnosti podataka.

2.1 Napad uskraćivanjem usluga

Napad uskraćivanjem usluga (DoS) je vrsta napada koja ima za cilj sprečavanje legitimnih korisnika pristupa mrežnim uslugama putem preopterećenja mrežnih servisa ili stvaranja prekomjerne konekcije, što rezultira padom konekcije ili servisa. Ova vrsta napada se ostvaruje preplavljivanjem ciljanog servera velikim brojem zahteva kako bi se iscrpeli njegovi resursi, čime se onemogućava normalno funkcionisanje. Distributed Denial of Service (DDoS) je naprednija forma ovog napada, gde se koristi snaga više posrednih korisnika za isti cilj.

DDoS napadi su postali posebno ozbiljni od 2000. godine, kada su popularni sajtovi poput Amazona, CNN-a,GitHub-a, eBay-a i Yahoa bili onesposobljeni. Ovi napadi koriste veliki broj računara inficiranih računarskim crvima ili trojancima kako bi istovremeno napali ciljni sistem u veoma kratkom vremenskom periodu. Identifikacija i sprečavanje DoS i DDoS napada su izuzetno teški zadaci.

Simptomi DoS napada uključuju usporavanje mrežnih performansi, nemogućnost pristupa određenim web sajtovima i nagli porast primljenih spam poruka. Najefikasniji način zaštite od ovih napada često uključuje promenu konfiguracije rutera kod pružalaca internet usluga.

- 2007. godine, estonski sajtovi vlade, banaka i medija su bili cilj napada uskraćivanjem usluga, što je rezultiralo njihovim blokiranjem tokom nekoliko nedelja. Ruski hakeri su optuženi za ovaj napad, što je pokrenulo široke rasprave o bezbednosti u cyber prostoru na međunarodnom nivou.
- prema izveštaju Njujork Tajmsa, grupa ruskih hakera je uspela da pristupi preko milijardu lozinki velikih svetskih kompanija, uglavnom američkih, kao i internet portalima. Takođe, američka kompanija Nasdak bila je meta hakerskog napada koji je mogao ozbiljno narušiti funkcionisanje američkog ekonomskog sistema i privrede. Identitet napadača još nije utvrđen, iako FBI sumnja da bi iza toga mogla stajati grupa hakera podržana od ruske vlade. Hakerski napadi mogu imati ozbiljne posledice, kako na berze, kao što je slučaj sa američkim ekonomskim sistemom, tako i na nuklearna postrojenja, kao što se desilo 2009. godine kada su amerikanci ubacili virus koji je uništio rad sistema u iranskim nuklearnim

postrojenjima. Takođe, hakeri iz Severne Koreje su uspešno napali nekoliko južnokorejskih banaka i medija.
- Na Twitter nalogu nekadašnjeg ruskog premijera Dmitrija Medvedeva, osvanula je tada lažna poruka o njegovoj ostavci, nakon čega je press služba vlade reagovala demantom i brisanjem poruka koje su postavili hakeri.
- Nakon nestanka malezijskog aviona MH370, kineski hakeri su, nezadovoljni radom zvaničnika koji su radili na rasvetljavanju slučaja, poslali e-mailove službama vlade Malezije sa lažnim naslovom da je avion pronađen. Ovi e-mailovi su sadržavali viruse koji su prosleđivali bitne podatke sa zaraženih računara u Kinu. Napad je otkriven od strane Agencije za tehnologiju i inovacije tek nakon što je pogođeno preko 30 računara u Odeljenjima za civilno vazduhoplovstvo i nacionalnu bezbednost.
- U oktobru 2016. godine, DNS provajder Dyn je bio žrtva velikog DDoS napada. Ovaj napad je uticao na popularne internet platforme poput Twittera, Netflix-a, Reddit-a i drugih, što je rezultiralo privremenim prekidima u pristupu ovim uslugama.

2.2 Botnet

Botovi su programi instalirani na računare s ciljem automatskog izvršavanja određenih funkcija i omogućavanja neovlašćenim korisnicima daljinsku kontrolu putem komunikacionog kanala. Zaraženi računari koji su pod kontrolom botova nazivaju se zombiji ili botovi, i mogu biti raspoređeni širom sveta. Oni čine skrivenu mrežu računara koja se koristi za slanje spama, izvođenje DoS napada, fišing, distribuciju adware-a i slične aktivnosti.

Botovi nikada ne deluju samostalno, već su deo veće mreže zaraženih računara koji su opremljeni "zadnjim vratima" za izvršavanje komandi. Ovi botnetovi mogu uključivati stotine ili hiljade računara ili čak mobilnih uređaja, svi zaraženi istim malicioznim programom. Njihova moć, koja se daljinski kontroliše, može biti iskorišćena za širok spektar aktivnosti, od slanja spama do napada na kritične informacione infrastrukture.

Botnetovi se koriste za napade na države i kritične informacione infrastrukture, kao što je bio slučaj u maju 2007. godine u Estoniji, kada je DDoS napad izveden uz pomoć 560 računarskih mreža iz preko 50 zemalja. Najčešća upotreba botnetova je emisija spama i distribucija malicioznih programa, što predstavlja izazov za donosioce odluka i provajdere internet usluga širom sveta koji se trude da spreče štetne sadržaje.

Mirai Botnet: Mirai je botnet koji je postao poznat po napadima na IoT (Internet of Things) uređaje poput pametnih kamera, rutera i digitalnih video rekordera. Koristeći ove zaražene uređaje, Mirai botnet je izveo velike DDoS napade koji su izazvali prekide u radu popularnih internet servisa.

Zeus Botnet: Zeus je botnet koji je bio fokusiran na krađu finansijskih podataka. Koristeći tehnike kao što su phishing, keylogging i spremanje podataka o karticama, Zeus je inficirao veliki broj računara širom sveta radi krađe bankovnih informacija.

Gameover Zeus Botnet: Ovo je varijanta Zeus botneta koja je posebno ciljala korisnike online igara. Gameover Zeus je koristio zaražene računare za krađu korisničkih podataka, kao i za izvršavanje DDoS napada na gejming servere.

Kelihos Botnet: Kelihos je botnet koji je bio poznat po svojoj sposobnosti za širenje spam poruka, distribuciju malvera i krađu informacija. Koristeći zaražene računare širom sveta, Kelihos je bio jedan od najaktivnijih botnetova tokom nekoliko godina.

Jedan od poznatih primera napada korišćenjem botneta je "WannaCry" ransomware napad iz 2017. godine. Ovaj napad koristio je botnet zvani "EternalBlue", koji je iskorišćavao ranjivost u Microsoft Windows operativnom sistemu kako bi se proširio na računare širom sveta. "WannaCry" ransomware je enkriptovao podatke na zaraženim računarima i tražio otkup za njihovo otključavanje. Napad je posebno pogodio preduzeća i javne ustanove, uključujući bolnice, obrazovne ustanove i druge organizacije koje su zavisile od pouzdane i sigurne obrade podataka. Ovaj napad je izazvao ozbiljne posledice, uključujući prekid rada sistema, gubitak podataka i finansijske štete. Iako su mnogi korisnici i organizacije brzo reagovali i preduzeli korake da se zaštite od WannaCry ransomware-a, napad je naglasio ranjivosti u internet bezbednosti i potrebu za jačanjem odbrambenih sistema i procedura.

2.3 Fišing

Fišing je oblik napada na internetu gde napadači koriste postojeće internet servise da prevari korisnike i namame ih da otkriju osetljive informacije poput korisničkih imena, lozinki ili podataka sa kreditnih kartica, koje se potom mogu iskoristiti u kriminalne svrhe.

Napadači, poznati kao fišeri, često izvode fišing napade putem lažnih e-mail adresa koje izgledaju kao da dolaze od poznatih institucija s kojima žrtva ima kontakt, kao što su banke, osiguravajuće kuće i slično. U ovim e-mailovima, žrtvi se obično sugeriše da ažurira svoje lične informacije kako bi izbegla blokadu računa, uz priloženi link ka lažnom veb sajtu koji izgleda kao verodostojna kopija institucije. Na ovaj način, potencijalna žrtva je preusmerena na lažni veb sajt gde se od nje traži da unese broj računa i lozinku, koji se kasnije mogu zloupotrebiti, uglavnom u finansijske svrhe.

Pored elektronske pošte, fišeri koriste različite internet servise kao što su Windows Messenger, Skype, Google Talk, kao i društvene mreže poput Facebook-a, Twitter-a i MySpace-a.

Fišing napadi se oslanjaju na socijalni inženjering i tehničke metode. Spam je glavni alat koji fišeri koriste da bi postigli veliki broj potencijalnih žrtava, koristeći baze podataka e-mail adresa kako bi poslali elektronsku poštu koja izgleda što je moguće više autentično. Takođe, fišeri koriste botnetove za istovremeno izvođenje velikog broja fišing napada.

Jedan od primera fišing napada dogodio se 2016. godine kada su kriminalci ciljali kompaniju "Seagate", jednog od najvećih proizvođača hard diskova na svetu. U ovom napadu, napadači su slali fišing e-mailove zaposlenima u Seagate-u, predstavljajući se kao legitimni partneri ili kolege unutar kompanije. U tim e-mailovima su tražili zaposlene da ažuriraju svoje korisničke informacije ili da potvrde svoje identitete klikom na linkove koji su vodili do lažnih veb sajtova dizajniranih da izgledaju kao Seagate-ovi interni sistem za prijavu. Kao rezultat toga, mnogi

zaposleni su nehotice otkrili svoje korisničke informacije, uključujući korisnička imena i lozinke, napadačima. Ove informacije su zatim iskorišćene za neovlašćen pristup Seagate-ovim sistemima i pokušaje krađe podataka. Iako Seagate nije detaljno izneo sve pojedinosti ovog napada, incident je naglasio ranjivost i opasnost koju fišing napadi predstavljaju za preduzeća, te potrebu za jačim sistemima zaštite i obukom zaposlenih o cyber bezbednosti.

2.4 Spam

Spem, ili neželjena elektronska pošta, je vrsta pošte koju korisnik nije tražio niti je dao saglasnost pošiljaocu da šalje takve poruke na njegovu adresu. Najčešće su to reklamne poruke ili ponude, ali mogu biti i poruke sa ciljem ubacivanja malicioznog softvera u željeni računar. Ova vrsta elektronske pošte često pokušava da sakrije e-mail adresu pošiljaoca kako bi otežala praćenje ili se koristi obmanjivanjem prilikom ispisa u polje "predmet", u nameri da natera primaoca da otvori primljenu poštu.

Spameri, ili pošiljaoci spema, često svoju infrastrukturu smeštaju u zemlje koje nemaju stroge zakone protiv slanja neželjene pošte. E-mail adrese se prikupljaju na različite načine, uključujući četove, web stranice, news grupe ili kroz zaražene računare putem malicioznog softvera. Najčešći način prikupljanja e-mail adresa je korišćenje robotskih sakupljača (harvestera) - botova koji pretražuju internet u potrazi za e-mail adresama. Spameri takođe međusobno razmenjuju baze prikupljenih e-mail adresa.

Spem predstavlja izazov koji delom proističe iz prirode interneta kao distribuiranog sistema bez centralne kontrole. Postaje sve ozbiljniji problem na internetu jer može zagušiti poštanske sandučiće korisnika i otežati razlikovanje legitimne pošte od neželjene.

Zaštita od spema se ostvaruje kroz primenu softvera za filtriranje, skrivanje e-mail adrese kako ne bi bila javno dostupna, edukaciju korisnika, primenu anti-spam regulativa i drugih mera. Ovo je bitno kako za obične korisnike, tako i za provajdere internet usluga koji moraju povećati svoje kapacitete kako bi se nosili sa velikim količinama neželjene pošte.

"Nigerijska prevara" ili "419 prevara" - u ovim porukama, korisnici su obaveštavani o navodnom nasledstvu, nagradi ili poslovnoj prilici iz Nigerije ili drugih afričkih zemalja. Da bi dobili "nagradu", primalac bi trebalo da uplati određenu sumu novca, ali u stvarnosti, nema nikakve nagrade.

Spameri često ciljaju korisnike e-pošte sa ponudama za "prilike života" kao što su poslovni poduhvati, investicije ili "lak način za zaradu novca". Ove poruke su često previše obećavajuće i rizične, i često su povezane sa prevarom ili piramidalnim šemama.

2.5 Socijalni inženjering

Socijalni inženjering je metod manipulacije ljudima putem uveravanja, obmanjivanja ili lažnog predstavljanja kako bi se dobile poverljive informacije ili pristupile zaštićenim sistemima.

Korišćenjem ljudskih slabosti, napadači zaobilaze tehnološke mehanizme zaštite radi izvršenja krađe, prevare, špijunaže, krađe identiteta ili izazivanja prekida u radu sistema.

Napadi socijalnog inženjeringa često se fokusiraju na veće organizacije poput sistema odbrane, finansijskih institucija, velikih korporacija, bolnica ili vladinih agencija. Napadači se služe različitim taktikama kako bi postigli svoje ciljeve, a jedan od najčešćih načina je korišćenje telefonskih poziva. Na primer, mogu se lažno predstaviti kao članovi IT podrške ili administratori i zatražiti lozinke ili druge poverljive informacije od zaposlenih.

Na primer, jedan incident socijalnog inženjeringa dogodio se 2014. godine kada je firma StubHub, platforma za prodaju i kupovinu karata za događaje, postala meta napada. U ovom slučaju, napadači su koristili socijalni inženjering kako bi pristupili korisničkim nalozima na StubHub-u i izvršili prevaru. Napadači su koristili ukradene informacije o korisnicima, uključujući korisnička imena i lozinke, kako bi pristupili njihovim nalozima na StubHub-u. Pretpostavlja se da su ove informacije bile ukradene putem phishing e-mailova ili drugih taktika socijalnog inženjeringa. Nakon pristupa nalozima, napadači su kupovali karte za različite događaje i prodavali ih putem drugih platformi, ostvarujući značajnu finansijsku dobit.

Ovakvi primeri ilustruju kako napadači koriste socijalni inženjering kako bi iskoristili ljudsku nepažnju ili naivnost i ostvarili pristup zaštićenim sistemima ili poverljivim informacijama u organizacijama. Osnovna zaštita od ovakvih napada leži u edukaciji zaposlenih o sigurnosnim rizicima i sprovođenju stroge politike zaštite informacija i sistema.

2.6 Sniffing

Njuškala su alati, kako hardverski tako i softverski, koji omogućavaju nadgledanje mrežnog saobraćaja i prikupljanje podataka koji se prenose putem računarske mreže, bilo zakonito ili nezakonito. Oni mogu čitati sve aktivnosti koje se dešavaju na mrežnom sloju i koriste se kako bi se izolovali problemi na mreži, iako istovremeno mogu usporiti mrežne performanse.

Koristeći njuškala, napadači mogu neovlašćeno prikupljati poverljive informacije koje se prenose putem mreže, poput lozinki, ličnih podataka ili poslovno osetljivih informacija. Na primer, napadač može postaviti njuškalo na mreži unutar neke kompanije i uhvatiti podatke koji se prenose između korisničkih računara i servera, prikupljajući osetljive informacije koje mogu biti zloupotrebljene.

Poznati softverski alati za njuškanje uključuju Ethereal, tcpdump i slične, koji omogućavaju detaljnu analizu mrežnog saobraćaja. Napadi pomoću njuškala često su teško otkriveni, jer se izvode neprimetno, te je potrebno uložiti napore u zaštitu mreže od ovakvih pretnji, uključujući upotrebu enkripcije podataka i strogu kontrolu pristupa mrežnim resursima.

2013. godine je američki trgovinski lanac Target postao žrtva velikog hakovanja podataka. Napadači su koristili njuškala kako bi neovlašćeno prikupili poverljive podatke o kreditnim karticama korisnika tokom procesa plaćanja. Napadači su postavili njuškala na mreži unutar sistema za obradu plaćanja u više od 1.800 Targetovih prodavnica širom Sjedinjenih Američkih Država. Ova njuškala su tajno snimala podatke o kreditnim karticama svaki put kada su korisnici

vršili transakcije. Prikupljeni podaci uključivali su brojeve kartica, datume isteka i sigurnosne kodove. Ovaj napad rezultirao je krađom podataka o više od 40 miliona kreditnih kartica korisnika Targeta, što je imalo ozbiljne posledice po poverenje korisnika i finansijske gubitke za kompaniju.

2.7 Spoofing

Spufing (spoofing) je obmana tj. prevara kojom se stvara utisak da prenos vrši ovlašćeni korisnik. To je prefinjena tehnika provere autentičnosti jedne mašine prema drugoj, falsifikovanjem paketa iz adrese izvora kojoj se veruje. Autentičnost koja se javlja u trenutku konekcije se potpuno bazira na IP adresi izvora. IP adrese (i mnoga polja IP zaglavlja) se mogu falsifikovati. Ovo je najlakši mehanizam zloupotrebe IP rutiranja izvora. IP spufing je jedan od oblika spufinga i tada se falsifikuje izvorna adresa IP paketa. Postoje i druge tehnike (ARP, DNS i TCP spoofing). Address Resolution Protocol (ARP) spoofing – falsifikovanje Media Access Control (MAC) adrese Ethernet frejmova. Domain Name System (DNS) spoofing – falsifikovanjem podataka u DNS paketima.

2008. godine "Kožni incident" (The Conficker Worm). U ovom napadu, zlonamerni softver nazvan Conficker Worm iskorišćavao je spufing tehnike kako bi se proširio kroz računarske mreže. Conficker Worm je koristio spufing kako bi falsifikovao izvorne adrese IP paketa, čime je maskirao svoj pravi izvor i stvorio utisak da dolazi sa legitimnih izvora unutar mreže. Ovaj zlonamerni softver se brzo širio kroz računarske mreže, iskorišćavajući ranjivosti u operativnim sistemima i mrežnim protokolima. Jednom kada bi se inficirao računar unutar mreže, Conficker bi koristio spufing tehnike kako bi se maskirao kao legitimni mrežni promet, čime bi izbegao detekciju i sprečio njegovo uklanjanje. Conficker Worm imao je globalni domet. Inficirani računari su identifikovani širom sveta, uključujući Severnu Ameriku, Evropu, Aziju, Australiju i druge regione, imao je ozbiljan uticaj na računarske mreže i sisteme širom sveta.

2.8 Maliciozni programi

Razvojem Interneta i različitih servisa pojavljuje se mnoštvo malicioznih programa, poznatih kao malware, koji se brzo šire mrežom zbog ranjivosti sistema, grešaka u softveru, neopreznosti korisnika i drugih faktora. Malware predstavlja softver koji nanosi štetu ciljanom računarskom sistemu, a razlikuje se po svojim aktivnostima, načinu umnožavanja i izvršavanja.

Računarski virusi su maliciozni programi koji se samorepliciraju tako što ubacuju kopije sebe u druge izvršne kodove ili dokumente, inficirajući datoteke i programe na ciljanom računaru. Oni mogu naneti štetu brisanjem ili menjanjem fajlova na disku, ili oštećenjem softvera na ciljanom sistemu. Virus se pokreće kada korisnik pokrene zaraženi program.

ILOVEYOU virus (2000): Možda jedan od najpoznatijih virusa u istoriji, ILOVEYOU je bio masivni email virus koji se širio putem elektronske pošte. Korisnici su dobijali poruke sa naslovom "ILOVEYOU" i pričvršćenom datotekom "LOVE-LETTER-FOR-YOU.txt.vbs". Kada

bi korisnik otvorio prilog, virus bi se aktivirao i počeo da se kopira na druge datoteke na računaru, braneći sebe i šireći se na kontakte u korisnikovoj adresar.

Stuxnet je bio sofisticiran maliciozni program koji je ciljao industrijske sisteme, posebno nuklearne postrojenja u Iranu. Napad je bio izuzetno složen i ciljao je da ošteti centrifuge za obogaćivanje uranijuma. Stuxnet je koristio različite ranjivosti u Windows operativnom sistemu i napredne tehnike infekcije kako bi se širio i izbegao otkrivanje.

Računarski crvi(worm) su samostalni programi koji se šire putem računarskih mreža, umnožavajući se automatski sa jednog računara na drugi. Oni koriste mrežu da bi se preneli na druge sisteme, brzo se šireći bez intervencije korisnika. Crvi mogu zauzeti protok mreže i naneti štetu sistemu.

Morris crv (1988): jedan od prvih poznatih računarskih crva. Kreirao ga je Robert Tappan Morris, a cilj mu je bio da istraži razmere Interneta. Međutim, zbog greške u kodu, crv se brzo širio i izazvao preopterećenje sistema na zaraženim računarima. Ovaj incident označava prvi veliki napad na Internetu i dovelo je do razvoja većih bezbednosnih mera.

Slammer crv (2003): je bio izuzetno brz računarski crv koji je ciljao SQL Server baze podataka. Napad je bio izuzetno destruktivan i izazvao je prekid u radu mnogih kompanija i institucija širom sveta. Slammer je uspeo da se širi tako brzo zbog ranjivosti u SQL Server softveru koju je exploatovala.

WannaCry (2017): Iako se WannaCry često opisuje kao ransomware, zapravo je kombinacija ransomware-a i računarskog crva. Ovaj napad je bio izuzetno razoran, inficirajući računare širom sveta putem ranjivosti u Windows operativnom sistemu. Nakon infekcije, WannaCry je šifrovao fajlove na zaraženim računarima i zahtevao otkupninu za njihovo dešifrovanje.

Trojanski konji su zlonamerni programi koji se prerušavaju u legitimne programe ili aplikacije kako bi korisnik bio prevaren da ih pokrene. Oni obično izgledaju kao bezopasni programi, ali zapravo imaju zlonamerne funkcije, poput brisanja fajlova ili krađe informacija.

1. Zeus: Zeus je jedan od najpoznatijih trojanskih konja koji je korišćen za krađu finansijskih informacija. Napad je obično započinjao tako što bi se trojanski konj infiltrirao na računar putem zaraženih e-mailova ili preuzimanjem zlonamernih fajlova sa Interneta. Nakon toga, Zeus bi presreo informacije o bankovnim računima, korisničkim imenima i lozinkama prilikom online transakcija.
2. Emotet: Emotet je trojanski konj koji se prvobitno koristio za krađu informacija, ali je kasnije postao poznat i po distribuciji drugog malicioznog softvera, uključujući ransomware. Napad Emotetom bi često započinjao putem zlonamernih e-mailova ili lažnih web stranica, gde bi se korisnici nagovarali da preuzmu zaražene priloge ili kliknu na zlonamerne linkove.
3. Keyloggers: Trojanski konji koji deluju kao keyloggers prate i beleže aktivnosti korisnika na računaru, uključujući sve što korisnik kuća na tastaturi. Ovi trojanci mogu biti

korišćeni za krađu osetljivih informacija poput korisničkih imena, lozinki, brojeva kreditnih kartica i drugih ličnih podataka.

4. DarkComet: DarkComet je trojanski konj koji je poznat po svojim špijunskim i daljinskim kontrolnim mogućnostima. Napadači su mogli da koriste DarkComet da prate aktivnosti na zaraženom računaru, snimaju ekran, upravljaju fajlovima i pretraživačem, pa čak i da aktiviraju kameru i mikrofon.

Sony Pictures Entertainment(U novembru 2014. godine), postao je žrtva ozbiljnog napada trojanskim konjem koji je izazvao ozbiljne štete kompaniji. Napadači su uspeli da prodru u mrežu Sony Picturesa i preuzmu kontrolu nad hiljadama računara. Ovaj trojanski konj je uništio i šifrirao ogromnu količinu podataka, uključujući i osetljive informacije o zaposlenima, finansijske podatke i komercijalne tajne kompanije.

U decembru 2015. godine, Ukrajinska elektroprivreda postala je žrtva napada trojanskim konjem koji je izazvao masovni prekid napajanja električnom energijom u nekoliko regiona zemlje. Napadači su uspeli da preuzmu kontrolu nad sistemima za upravljanje elektroenergetskom mrežom i daljinski isključe napajanje u više od 230.000 domova. Ovaj napad je izazvao velike poteškoće i ekonomske gubitke za Ukrajinu.

Logičke bombe su programi koji se aktiviraju kada se ispune određeni uslovi ili u određenom vremenskom periodu, nanoseći štetu računarskom sistemu. One mogu zauzeti resurse računara ili izazvati druge štetne efekte. Mogu biti upotrebljene kao sredstvo osvete ili sabotaže protiv organizacija i ustanova. Logičke bombe mogu izazvati ozbiljne probleme u funkcionisanju sistema i prouzrokovati značajne gubitke za organizacije. Zbog prirode ovih napada, često se ne objavljuju detalji o njima u javnosti ili se čak ne otkriju.

Vremenska bomba je maliciozni program koji se aktivira u određenom, unapred isprogramiranom, trenutku, a ne delovanjem korisnika. Kao i logička bomba, dovodi do toga da se nekontrolisanom samoreprodukcijom, zauzimaju resursi računara.

Špijunski programi(spyware) prikupljaju informacije o korišćenju računara, poput posećenih sajtova ili ličnih informacija, i prenose ih bez znanja korisnika.

Carbanak je bio napad koji je ciljao finansijske institucije širom sveta. Napadači su koristili phishing poruke kako bi inficirali računare zaposlenih u bankama, a zatim su koristili spyware za krađu finansijskih podataka i izvršili prevaru u vrednosti od više miliona dolara.

Rootkit je program dizajniran da sakrije dokaze o ugroženosti računarskog sistema i preuzme kontrolu nad njim, izbegavajući detekciju od strane antivirusnih programa.

"Sony BMG rootkit incident" iz 2005. godine. U ovom incidentu, muzička izdavačka kuća Sony BMG je distribuirala CD-ove sa audio sadržajem koji su bili zaštićeni digitalnim pravima (DRM). Međutim, kako bi ograničila neovlašćenu reprodukciju, Sony BMG je uključila rootkit tehnologiju u softver za upravljanje digitalnim pravima (DRM) koji se automatski instalirao na računarima korisnika kada bi CD bio ubačen u računar. Rootkit je bio dizajniran da sakrije prisustvo DRM softvera na računaru, čime bi onemogućio korisnicima da primete njegovo postojanje ili da ga uklone. Međutim, ovaj rootkit je imao ozbiljne posledice po bezbednost računara, jer je otvorio vrata za druge zlonamerne aktivnosti i potencijalne napade hakera. Kada je otkriveno da Sony BMG koristi rootkit tehnologiju na svojim CD-ovima, izbio je veliki skandal i Sony BMG je bio primoran da izda zakrpe za uklanjanje rootkita i preduzme korake kako bi se ispravila situacija. Ovaj incident je naglasio rizike povezane sa upotrebom rootkita u komercijalne svrhe i izazvao raspravu o etičnosti i bezbednosti takvih praksi.

Otkrivanje rootkit programa moguće je ‘’cross-view’’ tehnikom, metodama zasnovanim na proveri integriteta podataka i memorije. S obzirom na permanentnu pojavu novih rootkit programa, nužno je koristiti veći broj komercijalnih (UnHackMe, Proces Master, Vipre…) i alata otvorenog koda (GMER, Sophos Anti-Rootkit, RootkitRevealer, RootKit Hook Analyzer…)

Oglašavački programi su malware koji prikazuju oglase korisnicima bez njihovog znanja ili dozvole, često ometajući normalno korišćenje računara.

2015. godine kompanija Lenovo je predinstalirala softver Superfish na svoje laptop računare kako bi prikazivala ciljane oglase korisnicima prilikom pretraživanja interneta. Međutim, Superfish je koristio tzv. "man-in-the-middle" tehniku, što znači da je omogućavao pristup internet saobraćaju korisnika, čime se narušavala privatnost i sigurnost korisnika. Ovaj incident je izazvao veliku zabrinutost među korisnicima jer su bili zabrinuti za svoju privatnost i sigurnost podataka. Lenovo je kasnije izdao uputstva za uklanjanje Superfish softvera i izvinio se korisnicima zbog neovlašćene instalacije ovog programa.

Pokazatelji prisustva malicioznog programa na računaru mogu biti sledeći: usporavanje rada na računaru, sporije učitavanje programa česti iskakajući (pop-up) prozori neobične promene u radu računara.

Ovi maliciozni programi mogu naneti ozbiljnu štetu korisnicima i organizacijama, uzrokujući gubitak podataka, oštećenje sistema i krađu ličnih informacija. Važno je redovno ažurirati antivirusne programe i preduzeti ostale mere zaštite kako bi se sprečila infekcija računara ovakvim malware-om.

Operacija "Shady RAT" je naziv koji se odnosi na napade na računarske mreže koje su izvele cyber-kriminalne grupe podržane od strane država. Ovaj napad je prvi put javno obznanjen 2011. godine kada je kompanija McAfee objavila izveštaj o otkriću velikog broja napada na računarske sisteme širom sveta. Napadi su bili usmereni ka različitim organizacijama, uključujući vlade, međunarodne organizacije, privatne kompanije i nevladine organizacije, trajali su 5 godina i došlo je do krađe intelektualnog vlasništva više od 70 državnih agencija, multinacionalnih korporacija i drugih organizacija iz 14 zemalja.

Grupa hakera iza "Shady RAT" operacije koristila je različite tehnike, uključujući phishing, spyware i exploit kits, kako bi prodrli u računarske mreže ciljanih organizacija.

. McAfee je podatke izvukao iz upravljačkog servera botnet mreže koji je prikupljao logove sa podacima(od 2006.godine). Ovakva pretnja nazivana je Advanced Persistent Threat zbog svoje sofisticiranosti. Joe Stewart iz kompanije Dell SecureWorks, otkrio je da su napadači za prikrivanje svojih lokacija koristili 10 godina star kineski alat HTran. Ovaj incident je ukazao na ozbiljnost pretnje od cyber-kriminala podržanog od strane država.

Ne tako davno su bili brojni hakerski napadi grupe Anonimusi. Ovu grupu čine hakeri širim sveta i smatra se najbrojnijim hakerskim grupom. Njihova najpoznatija serija pada počela je napadom na Sajentološku crkvu, a potom na vlade Egipta i Irana, a zatim na kompanije u vlasništvu konzervativnih aktivista i miliona Čarlsa Koha i Dejvida. U znak odmazde za saradnju sa FBI-jem u identifikaciji članova grupe, Anonimusi su takođe napali HBGary Federal. U jeku kampanju koje su američke vlasti vodile protiv Wikileaks-a, Anonimusi su pokrenuli uzvratnu operaciju umerenu protiv kompanije PayPal, Visa i MasterCard, koje su, pod privatnom zahtevom američkih vlasti, prekinule sa prenosa finansija na račun Wikileaks. Grupa je preuzela odgovornost za napad na nekoliko Sony veb lokacija koji je usledio nakon krivičnog gonjenja nekoliko PlayStation 3 hakera. Anonimusi su osporili Sonyjeve optužbe o naknadnom napadu na PlayStation Networks i Sony Online Entertainment i upad u bazu podataka za koji je kompanija optužila grupu, priznajući samo učešće u početnim DDoS napadima. Hakerska grupa Anonimous je u julu 2011. hakovala kompjutersku mrežu NATO vojne alijanse i došla do oko gigabajta poverljivih podataka, da bi u oktobru 2011. godine preuzeli odgovornost za napad na više od 40 tajnih web sajtova sa dečjom pornografijom i objavljivanje imena više od 1.500 članova jednog od hakovanih pornografskih sajtova.

3. Zaključak

Sajber napadi predstavljaju ozbiljnu pretnju kako za preduzeća tako i za javne ustanove širom sveta. Ovi napadi mogu izazvati ozbiljne ekonomske i reputacione posledice, uključujući gubitak finansijskih sredstava, oštećenje reputacije organizacije i gubitak poverenja korisnika. Analizom stvarnih primera kao što su WannaCry napad na NHS, Target breach, Equifax breach, Yahoo breach i drugi, možemo videti da su ekonomske posledice ovih napada izuzetno velike i mogu imati dugoročne efekte na finansije kompanija.

Ključno je razumeti da su sajber napadi postali sve sofisticiraniji i češći, te da je neophodno preduzeti odgovarajuće korake kako bi se ublažili ovi rizici. To uključuje implementaciju naprednih sigurnosnih sistema i tehnologija, redovno obučavanje osoblja o sajber bezbednosti, uspostavljanje efikasnih procesa nadzora i reagovanja na incidente, kao i saradnju sa stručnjacima za sajber bezbednost.

Ublažavanje ekonomskih posledica sajber napada zahteva pažljivo planiranje i upravljanje rizicima. Kompanije bi trebalo da procene svoje ranjivosti, identifikuju ključne tačke napada i razviju strategije zaštite kako bi se smanjili potencijalni gubici. Takođe, neophodno je imati planove oporavka od napada kako bi se brzo reagovalo u slučaju incidenta i minimizirali štetni efekti.

Naposletku, važno je naglasiti da sajber bezbednost nije samo tehničko pitanje, već i pitanje upravljanja rizicima i organizacione kulture. Kompanije i javne ustanove moraju imati holistički pristup sajber bezbednosti koji uključuje sve nivoe organizacije i kontinuirano ulaganje u unapređenje sigurnosti. Samo tako mogu se adekvatno zaštititi od sajber pretnji i očuvati svoju reputaciju i finansijsku stabilnost.

4. Literatura

Nenad Putnik, Sajber prostor i bezbednosni izazovi, Fakultet bezbednosti Univerziteta u Beogradu, 2009., str. 123, 124, 86

Dragan Simeunović, Terorizam, Pravni fakultet Univerziteta u Beogradu, 2009., str. 28

Ljubomir Stajić, Osnovi sistema bezbednosti sa osnovama istraživanja bezbednosnih pojava, Pravni fakultet Univerziteta u Novom Sadu, Novi Sad, 2008., str. 211

Allison A., Cyber "hostilities" and the war powers resolution, Military Law Review, Vol. 217, 2013, p. 186-187.

https://www.politika.rs/scc/clanak/614416/Sajber-napadi-ne-posustaju

https://www.politika.rs/scc/clanak/601664/Vise-od-33-miliona-sajber-napada-na-mobilne-uredaje

https://www.it-klinika.rs/blog/ukradi-zakljucaj-uceni-ransomware-izvestaj-za-2023

https://www.symantec.broadcom.com/hubfs/Symantec_Ransomware_Threat_Landscape_2024.pdf?hsCtaTracking=767be7a3-c8a1-4cd1-8387-7ec8ac770b3c%7Ce27274de-c76f-4496-ac64-e943054afaa8

Vuletić, D., (2012a). Bezbednost u sajber prostoru, Medija centar ‘’Odbrana’’, Beograd.

Vuletić, D., (2012b). Napadi na računarske sisteme, Vojnotehnički glasnik br. 1, Medija centar ‘’Odbrana’’, Beograd

Vuletić, D., (2015a). Smernice za izradu strategije obezbeđenja sajber prostora, Vojno delo broj 5, Medija centar ‘’Odbrana’’, Beograd

Vuletić, D., (2015b). Sajber terorizam (separat monografije) Grupa autora, Savremeni terorizam, JP ‘’Službeni glasnik’’ i Institut za međunarodnu politiku i privredu, Beograd