Dr. sc. Siniša Franjić, dipl. iur,
Internacionalni univerzitet Brčko distrikt Bosne i Hercegovine
sinisa.franjic@gmail.com

Stručan rad
UDK:050(045:343.5)497.6
https://doi.org/10.59417/nir.2023.22.33

HACKING NA KONKRETNOM PRIMJERU

Sažetak:

Hackeri, kao osobe koje se bave najrazličitijim oblicima računalnog kriminaliteta, daju si toliku slobodu pa ljudima šalju e-mailove ucjenjivačkog karaktera. To je jedan od najčešćih oblika računalnog kriminaliteta kojega treba organizirano sprječavati. U današnjem modernom, virtualnom svijetu, nezamislivo je da se događaju situacije u kojima hackeri protupravno dolaze do tuđih podataka na način da provaljuju u tuđa računala i računalne sustave. Za svaki takav slučaj potrebno je izvršiti kriminalističko istraživanje, pronaći počinitelja i primjereno ga kazniti.

Ključne riječi: Internet, Računalni kriminalitet, E-mail, Kazneno djelo, Modus operandi

1. Uvodna razmatranja

Ljudski talent, inteligencija i obrazovanje dolaze do izražaja kroz komunikaciju s drugim ljudima (Šimundić i Franjić, 2009). Ta je komunikacija počela napredovati od sredine XV. stoljeća uporabom raznovrsnih i sve savršenijih tehničkih pomagala koji se smatraju temeljem svjetske informacijske revolucije. Za razliku od informacijske, informatička revolucija obuhvaća ona tehnološka rješenja koja se ostvaruju korištenjem modernih informatičkih i komunikacijskih postrojenja, strojeva, različitih uređaja i mreža kojima se unose, obrađuju i pohranjuju podaci, prenose slike, glas, zvuk i signali u digitalnom obliku.

Problematika računalnog kriminaliteta jest problematika čija je pojavnost sve učestalija u modernom društvu. Računalni kriminalitet nastaje i razvija se na isti način u svim dijelovima svijeta. O njemu se javno piše i govori, a rezultati njegova sprječavanja praktički su zanemarivi. Danas to više nije tako jer je sve više država koje u vlastitim nacionalnim zakonodavstvima imaju opisana kaznena djela kaznena djela koja proizlaze iz uporabe modernih informacijsko-računalnih tehnologija.

2. Internet

Internet je globalni informacijsko-komunikacijski sustav koji povezuje i spaja mreže pojedinih zemalja i organizacija te tako omogućava korisnicima računala diljem svijeta da putem svojih lokalnih mreža i telefonskih veza komuniciraju, razmjenjuju informacije i koriste druge usluge (Dragičević, 2004). Razvoj interneta počinje 1969. godine kada je pokrenut projekt Arpanet s ciljem stvaranja pouzdane mreže koja će moći funkcionirati i kada jedan njezin dio nije u funkciji zbog napada ili tehničke neispravnosti (Šimundić i Franjić, 2009). U tu svrhu započet je razvoj mrežnog protokola koji bi omogućio da se komunikacija preko mreže automatski preusmjerava mimoilazeći mjesto gdje je problem nastao i tako spriječi dobivanje informacija bez obzira na novonastale probleme. Internet je omogućio razmjenu i dostupnost informacija lakšom nego ikada prije, a vremenom je profilirao pet osnovnih funkcija:

- prikupljanje, pohranjivanje i obradu informacija, jednostavniju i bržu razmjenu podataka i programa
- veliki prostor oglašavanja
- rasprostranjen e-mail
- interaktivna neposredna komunikacija između korisnika, telekonferencija i internet telefonija
- obavljanje najrazličitijih poslovnih aktivnosti

Prvotna namjena interneta nije bila komercijalna niti je bila usmjerena prema onome što danas predstavlja. Nije se usmjeravala dovoljna pozornost prema sigurnosti pa su protokoli bili, uglavnom, usmjereni prema djelotvornosti, fleksibilnosti i otvorenosti sustava.

Razvoj interneta prati rast broja i učestalosti napada (Franjić, 2015.). Točan, ali i približan broj napada ne može se utvrditi. Kada su u pitanju veliki informacijski sustavi, tendencija je prešućivanje napada zbog tajnosti podataka ili straha od gubitka korisnika. Današnje procjene kažu da se štete nastale računalnim kriminalitetom nalaze odmah iza šteta nastalih trgovinom drogom i trgovinom oružjem. Razvojem interneta raste i broj potencijalnih počinitelja. Sve veće tehničko znanje i sve sofisticiranija oprema omogućuju stvaranje naprednih softverskih alata namijenjenih lakšem i bržem napadanju. Najčešći razlog tomu jest dostpunost izvornih kodova programa koji počiniteljima omogućavaju uvid u samu strukturu programa i njegove slabosti koje se mogu iskoristiti. Do napada dolazi usljed:

- neovlaštenog pristupa
- neovlaštenog mijenjanja podataka
- neovlaštenog brisanja podataka
- presnimavanja malicioznih programa (virusa, crva itd.)
- uporabe tuđeg računala za pristup drugom sustavu
- stvaranja uvjeta za nastanak štete na sustavu
- krađe, oštećenja, uništenja hardverske osnovice, medija itd.

Sve ovo bi bilo besmisleno kada se počinitelj ne bi mogao povući, ne ostavljajući nikakve dokaze o svome neovlaštenom pristupu. Anonimnost je jedan od temelja računalnog kriminaliteta i osnovni razlog zašto ga je teško sprječavati i suzbijati. Napadači će nastojati ukloniti podatke o svom pristupu, a u kojoj će im mjeri to biti moguće, ovisit će o njihovim vlastitim sposobnostima, ali i sposobnostima sustava koji je bio meta njihova napada.

3. Modus operandi

Neki napadači su toliko sigurni u svoje informatičko znanje pa čak žrtvi priznaju koja su kaznena djela počinili kako bi joj naštetili. Autor ovog rada je od sredine listopada 2019. do sredine travnja 2020. godine bio meta potencijalnom hackeru. Uputio mu je šest e-mailova prijetećeg sadržaja koji su imali za cilj ucjenu autora i na taj način stjecanje protupravne imovinske koristi. Autor ovdje navodi sadržaje svih e-mailova uz napomenu da je peti i šesti e-mail dobio istog dana. Zbog potreba kriminalističkog istraživanja je potrebno navesti sadržaje svih e-mailova kako bi istražitelji dobili što precizniju sliku o napadaču. Prvi e-mail je poslan s nepoznate adrese, a ostali s autorove tako da ova situacija u konačnici izgleda ovako: autor je sam sebi poslao sporne e-mailove.

3.1. E-mail 1[1]

Zdravo!
Ja sam haker koji ima pristup vašem operativnom sustavu.
Također imam puni pristup vašem računu.
Promatram te već nekoliko mjeseci.
Činjenica je da ste bili zaraženi zlonamjernim softverom putem web mjesta za odrasle koje ste posjetili.

[1] Ovaj e-mail je „primljen“ 17. 10. 2019.

Ako niste upoznati s tim, objasnit ću vam.

Trojanski virus pruža mi potpuni pristup i kontrolu nad računarom ili drugim uređajem.

To znači da mogu vidjeti sve na vašem zaslonu, uključiti kameru i mikrofon, ali vi ne znate za to.

Također imam pristup svim vašim kontaktima i svu vašu prepisku.

Zašto vaš antivirus nije otkrio zlonamjerni softver?

Odgovor: Moj zlonamjerni softver koristi upravljački program, ažuriram njegove potpise svaka 4 sata kako bi antivirus bio tih.

Napravio sam video koji prikazuje kako se zadovoljavate u lijevoj polovini ekrana, a u desnoj polovici vidite video koji ste gledali.

Jednim klikom miša mogu poslati ovaj video na sve vaše e-poruke i kontakte na društvenim mrežama.

Također mogu objaviti pristup svim vašim e-mail prepiskama i glasnicima koje koristite.

Ali ne brinite se previše, tu je način na koji možemo riješiti problem privatnosti. Trebamo samo uplatnicu u Bitcoinu u iznosu od £6,960.00 GBP, što mislim da je s obzirom na okolnosti fer cijena.

Bitcoin adresa za plaćanje je: 123DhE3VHRqUjAtcbsXwyA2LZqLh2bzg7K

NAPOMENA: SPOMENITE SE DA PONOVO POTVRDITE BITCOIN ADRESU S NAMA PRIJE UPLATE DA IZBJEGNITE PLAĆANJE dva puta.

Ako ne razumijete bitcoin, idite na YouTube i pretražite "kako kupiti bitcoin" ili google za "lokalne bitcoine", to je prilično jednostavno.

Nakon primitka uplate, izbrisat ću videozapis i više nas nikada nećete čuti.

Dajem vam 48 sati da platite. Obavijestila sam da čitam ovo pismo i timer će raditi kad vidite ovo pismo.

Podnošenje žalbe negdje nema smisla, jer se ova e-pošta ne može pratiti kao moja bitcoin adresa.

Ne pravim nikakve greške.

Ako ustanovim da ste ovu poruku podijelili s nekim drugim, video će se odmah distribuirati.

Odgovorite samo da potvrdite Bitcoin adresu za plaćanje ili imate pitanja u vezi s plaćanjem, a zatim kliknite odgovor. Ne pokušavajte uspostaviti kontakt sa mnom jer koristim e-poštu žrtve koja je bila hakirana i izložena.

3. 2. E-mail 2 [2]

Pozdrav!

Kao što ste možda primijetili, poslao sam vam e-poruku s vašeg računa.

To znači da imam puni pristup vašem računu.

Promatram te već nekoliko mjeseci.

Činjenica je da ste bili zaraženi zlonamjernim softverom putem web mjesta za odrasle koje ste posjetili.

Ako niste upoznati s tim, objasnit ću vam.

Trojanski virus pruža mi potpuni pristup i kontrolu nad vašim računalom ili bilo kojim drugim uređajem.

To znači da mogu vidjeti sve na vašem zaslonu, uključiti kameru i mikrofon, ali vi ne znate za to.

Također imam pristup svim vašim kontaktima i svu vašu prepisku.

Zašto vaš antivirus nije otkrio zlonamjerni softver?

Odgovor: Moj zlonamjerni softver koristi upravljački program, ažuriram njegove potpise svaka 4 sata kako bi antivirus bio tih.

Napravio sam video koji prikazuje kako masturbirate u lijevoj polovini ekrana, a u desnoj polovici vidite video koji ste gledali.

Jednim klikom miša mogu poslati ovaj video na sve vaše e-poruke i kontakte na društvenim mrežama.

Jesam također mogu objaviti pristup svim vašim e-mail prepiskama i glasnicima koje koristite.

Ako to želite spriječiti, prenesite iznos od 950€ na moju bitcoin adresu (ako ne znate kako to učiniti, napišite Googleu: "Kupi bitcoin").

Moja bitcoin adresa (BTC novčanik) je: 15WFuB2rBPDpzBbjaT26zKfqwXtssJv7FS

Nakon primitka uplate, izbrisat ću videozapis i više me nikada nećete čuti.

Dajem vam 48 sati da platite.

Imam obavijest o čitanju, i timer će raditi kad vidite ovo pismo.

Podnošenje žalbe negdje nema smisla, jer se ova e-pošta ne može pratiti poput moje bitcoin adrese.

Ne pravim nikakve greške.

Ako ustanovim da ste ovu poruku podijelili s nekim drugim, video će se odmah distribuirati.

Srdačan pozdrav!

[2] Ovaj e-mail je „primljen“ 22. 01. 2020.

3. 3. E-mail 3 [3]

Pozdrav!

Imam jako loše vijesti za tebe.

08.01.2020. - na ovaj dan provalio sam u vaš operativni sustav i dobio puni pristup vašem računu s adrese@domain.com.

Naravno možete promijeniti lozinku .. Ali moj zlonamjerni softver presreće ga svaki put kad ga promijenite.

Kako sam to učinio:

Došlo je do ranjivosti u softveru usmjerivača putem kojeg ste stupili na mrežu.

Upravo sam hakirao ovaj usmjerivač i na njega stavio svoj zlonamjerni kod.

Kad ste otišli na mrežu, moj trojanski program instaliran je na OS vašeg uređaja.

Nakon toga napravila sam cijelu kopiju vašeg diska (imam cijeli vaš adresar, povijest pregledavanja , sve datoteke, telefonske brojeve i adrese svih vaših kontakata).

Prije mjesec dana htio sam zaključati vaš uređaj i zamoliti malu količinu u bitcoinima za otključavanje.

Ali pogledao sam web mjesta koja redovito posjećujete i bio sam šokiran onim što sam vidio !!!

Mislim na web mjesta za odrasle.

Želim reći - veliki ste perverznjak. Vaše maštarije nemaju nikakve veze s normalnom percepcijom obične osobe.

I imao sam ideju ...

Snimila sam snimku zaslona sa web mjesta za odrasle, gdje se zabavljate (znate o čemu se radi, zar ne?).

Nakon toga snimio sam snimke zaslona kako masturbirate (pomoću kamere vašeg uređaja) i kombinirao ih.

S lijeve strane masturbirate, a s desne strane - objekt vašeg uzbuđenja.

Ispalo je nevjerojatno! To će zadiviti svakoga, posebno vaše rodbina i prijatelji!

Znam da im ne biste htjeli pokazati ove snimke zaslona.

Mislim da je 970€ izuzetno mali iznos za moju šutnju.

Uz to sam vas tako dugo špijunirao, trošeći puno vremena!

Platite SAMO u Bitcoinima!

Moj BTC novčanik: 14R1gsh6YxyUXksPHWemavJTAPPDEtn7Qa

Ne znate kako koristiti bitcoin?

[3] Ovaj e-mail je „primljen“ 16. 03. 2020.

U bilo koju tražilicu (na primjer Google) unesite upit: "Kako napuniti BTC novčanik."
Vrlo je lako.
Na ovo vam dajem dva dana (48 sati) od trenutka otvaranja ovog pisma.
Napominjemo da će čim otvorite ovo pismo, tajmer raditi i vrijeme će proći.
Nakon uplate moj virus i sve snimke zaslona vaše masturbacije automatski uništavaju bit će automatski uništene.
Ako od vas ne primim naznačeni iznos, tada će vaš uređaj biti blokiran, a svi vaši kontakti dobit će snimke zaslona vaše vulgarne užitke.
Nadam se da razumijete svoju situaciju.
- Nemojte pokušavati pronaći i uništiti moj virus! (Svi vaši podaci, datoteke i snimke zaslona već su preneseni na udaljeni poslužitelj).
- Nemojte me pokušavati kontaktirati (to nije moguće, jer sam vam poslao poštu s vašeg hakiranog računa).
- razne sigurnosne usluge neće vam pomoći; formatiranje pogona ili uništavanje uređaja neće pomoći jer su vaši podaci već na udaljenom poslužitelju.
P.S. Nisi mi jedina žrtva. I garantiram vam da vas više neću gnjaviti nakon uplate!
Ovo je hakerski kodeks časti
Molim vas i da ubuduće redovito ažurirate svoje antivirusne programe. Na ovaj način više nećete biti u sličnoj situaciji.
Ne ljuti se na mene. Svatko svoj posao.
Sretno.

3. 4. E-mail 4 [4]

Pozdrav!
Kao što ste možda primijetili, poslao sam vam e-poruku s vašeg računa.
To znači da imam puni pristup vašem računu.
Promatram te već nekoliko mjeseci.
Činjenica je da ste bili zaraženi zlonamjernim softverom putem web mjesta za odrasle koje ste posjetili.
Ako niste upoznati s tim, objasnit ću vam.

[4] Ovaj e-mail je „primljen“ 01. 04. 2020.

Trojanski virus pruža mi potpuni pristup i kontrolu nad vašim računalom ili bilo kojim drugim uređajem.
To znači da mogu vidjeti sve na vašem zaslonu, uključiti kameru i mikrofon, ali vi ne znate za to.
Također imam pristup svim vašim kontaktima i svu vašu prepisku.
Zašto vaš antivirus nije otkrio zlonamjerni softver?
Odgovor: Moj zlonamjerni softver koristi upravljački program, ažuriram njegove potpise svaka 4 sata kako bi antivirus bio tih.
Napravio sam video koji prikazuje kako masturbirate u lijevoj polovini ekrana, a u desnoj polovici vidite video koji ste gledali.
Jednim klikom miša mogu poslati ovaj video na sve vaše e-poruke i kontakte na društvenim mrežama.
Jesam također mogu objaviti pristup svim vašim e-mail prepiskama i glasnicima koje koristite.
Ako to želite spriječiti, prenesite iznos od 950€ na moju bitcoin adresu (ako ne znate kako to učiniti, napišite Googleu: "Kupi bitcoin").
Moja bitcoin adresa (BTC novčanik) je: 1PDGXxvBGxLHk3zwxHgtDdY3Qirn5USUwY
Nakon primitka uplate, izbrisat ću videozapis i više me nikada nećete čuti.
Dajem vam 48 sati da platite.
Imam obavijest o čitanju, i timer će raditi kad vidite ovo pismo.
Podnošenje žalbe negdje nema smisla, jer se ova e-pošta ne može pratiti poput moje bitcoin adrese.
Ne pravim nikakve greške.
Ako ustanovim da ste ovu poruku podijelili s nekim drugim, video će se odmah distribuirati.
Srdačan pozdrav!

3. 5. E-mail 5 [5]

Pozdrav!
Imam jako loše vijesti za tebe.
17/01/2020. - na ovaj dan provalio sam u vaš operativni sustav i dobio puni pristup vašem računu s adrese@domain.com.

[5] Ovaj e-mail je „primljen“ 17. 04. 2020. u dva navrata s razmakom od deset minuta

Naravno možete promijeniti lozinku .. Ali moj zlonamjerni softver presreće ga svaki put kad ga promijenite.

Kako sam to učinio:

Došlo je do ranjivosti u softveru usmjerivača putem kojeg ste stupili na mrežu.

Upravo sam hakirao ovaj usmjerivač i na njega stavio svoj zlonamjerni kod.

Kad ste otišli na mrežu, moj trojanski program instaliran je na OS vašeg uređaja.

Nakon toga napravila sam cijelu kopiju vašeg diska (imam cijeli vaš adresar, povijest pregledavanja , sve datoteke, telefonske brojeve i adrese svih vaših kontakata).

Prije mjesec dana htio sam zaključati vaš uređaj i zamoliti malu količinu u bitcoinima za otključavanje.

Ali pogledao sam web mjesta koja redovito posjećujete i bio sam šokiran onim što sam vidio !!!

Mislim na web mjesta za odrasle.

Želim reći - veliki ste perverznjak. Vaše maštarije nemaju nikakve veze s normalnom percepcijom obične osobe.

I imao sam ideju ...

Snimila sam snimku zaslona sa web mjesta za odrasle, gdje se zabavljate (znate o čemu se radi, zar ne?).

Nakon toga snimio sam snimke zaslona kako masturbirate (pomoću kamere vašeg uređaja) i kombinirao ih.

S lijeve strane masturbirate, a s desne strane - objekt vašeg uzbuđenja.

Ispalo je nevjerojatno! To će zadiviti svakoga, posebno vaše rodbina i prijatelji!

Znam da im ne biste htjeli pokazati ove snimke zaslona.

Mislim da je 1250€ izuzetno mali iznos za moju šutnju.

Uz to sam vas tako dugo špijunirao, trošeći puno vremena!

Platite SAMO u Bitcoinima!

Moj BTC novčanik: 1GanNLCVpeZ93bfG5yRdTXZ5MvudE2qkt8

Ne znate kako koristiti bitcoin?

U bilo koju tražilicu (na primjer Google) unesite upit: "Kako napuniti BTC novčanik."

Vrlo je lako.

Na ovo vam dajem dva dana (48 sati) od trenutka otvaranja ovog pisma.

Napominjemo da će čim otvorite ovo pismo, tajmer raditi i vrijeme će proći.

Nakon uplate moj virus i sve snimke zaslona vaše masturbacije automatski uništavaju bit će automatski uništene.

Ako od vas ne primim naznačeni iznos, tada će vaš uređaj biti blokiran, a svi vaši kontakti dobit će snimke zaslona vaše vulgarne užitke.
Nadam se da razumijete svoju situaciju.
- Nemojte pokušavati pronaći i uništiti moj virus! (Svi vaši podaci, datoteke i snimke zaslona već su preneseni na udaljeni poslužitelj).
- Nemojte me pokušavati kontaktirati (to nije moguće, jer sam vam poslao poštu s vašeg hakiranog računa).
- razne sigurnosne usluge neće vam pomoći; formatiranje pogona ili uništavanje uređaja neće pomoći jer su vaši podaci već na udaljenom poslužitelju.
P.S. Nisi mi jedina žrtva. I garantiram vam da vas više neću gnjaviti nakon uplate!
Ovo je hakerski kodeks časti
Molim vas i da ubuduće redovito ažurirate svoje antivirusne programe. Na ovaj način više nećete biti u sličnoj situaciji.
Ne ljuti se na mene. Svatko svoj posao.
Sretno.

4. Kaznena djela

4. 1. Hacking

Neovlašteni pristup računalnom sustavu su radnje kojima je cilj zaobilaženje provjere pristupa sustavu i omogućavanje počinitelju da se pod krinkom ovlaštenog služi uslugama i resursima sustava (Šimundić i Franjić, 2009). Posljedica napada je povreda tajnosti, dostupnosti podataka i programa, ali i dostupnosti usluga.

Počinitelji su osobe kojima je omogućen pristup sustavu pri čemu se koriste terminalima drugih zaposlenika ili su to osobe koje putem modema pristupaju sustavu. Dijele se na unutarnje i vanjske počinitelje.

Unutarnji počinitelji pristup ostvaruju, uglavnom, nepažnjom drugih zaposlenika dok se vanjski počinitelji koriste raznim metodama kako bi došli do lozinki za pristup sustavu.

Počinitelji vode računa da djela koja počine putem tuđih računalnih sustava ili uporabom kloniranih mobitela ostanu neotkrivena kako bi zameli svoj trag i onemogućili druge koji tragaju za njima.

4. 2. Računalna prijevara

Računalna prijevara obuhvaća razne vrste manipulacija na podacima, najčešće financijskim, s namjerom da se sebi ili drugome nezakonito pribavi protupravna imovinska korist (Pavišić, Modly i Veić, 2012). Do takvih manipulacija može doći tijekom unosa, obrade, pohranjivanja, distribucije podataka i informacija, kao i pri razmjeni podataka unutar računalne mreže ili putem telefonskih i drugih komunikacijskih kanala. Pri tome se podaci mogu nalaziti na bilo kojem digitalnom mediju. Noviji razvoj računalnih mreža i telekomunikacija u velikoj mjeri je pridonio njihovom širenju i pojavi novih oblika prijevara. Razvoj bankomata i njihovo sve šire uvođenje u redovito poslovanje banaka otvorilo je nove mogućnosti manipulacija s računalno pohranjenim podacima na karticama ili unutar sustava. Daljnjim razvojem računalnih mreža te širenjem elektroničkog poslovanja i digitalnog novca, ovakve manipulacije zbog lakoće izvođenja i relativno teškog otkrivanja postaju jedan od najčešćih oblika računalnog kriminala. U tu svrhu počinitelji se sve češće koriste tuđim podacima i otuđenim programski dobivenim brojevima kreditnih kartica kako bi sebi ili drugome pribavili neku korist (kao što je kupovina raznih proizvoda, plaćanje nekakve usluge i sl.).

4. 3. Iznuda

Počinitelj kaznenog djela može biti svaka osoba (Pavišić, Modly i Veić, 2012). Iznudom počinitelj primjenjuje silu ili ozbiljnu prijetnju te prisiljava drugog da nešto učini ili ne učini na štetu svoje ili tuđe imovine s ciljem da sebi ili drugom pribavi protupravnu imovinsku korist. Iznuda sadrži posebni oblik kaznenog djela prisile kao i razbojništvo i razbojnička krađa. Prisila, međutim, kod iznude nije sredstvo oduzimanja ili zadržavanja stvari, nego je usmjerena na volju drugoga da sam nešto učini ili ne učini.

Kvalificirani oblik djela postoji ako je osnovnim kaznenim djelom pribavljena znatna imovinska korist ili je uporabljeno kakvo oružje ili opasno oruđe, ili je uzrokovana smrt osobe.

5. Pretraga

Pretraga pokretnih stvari obuhvaća i pretragu računala i s njim povezanih uređaja, drugih uređaja koji služe prikupljanju, pohranjivanju i prijenosu podataka, telefonskim, računalnim i drugim komunikacijama i nositelja podataka (Pavišić, 2013). Na zahtjev tijela koje poduzima pretragu, osoba koja se koristi računalom ili ima pristup računalu ili drugom uređaju ili nositelju podataka, te davatelj telekomunikacijskih usluga, dužni su omogućiti pristup računalu, uređaju

ili nositelju podataka, te dati potrebne obavijesti za nesmetanu uporabu i ostvarenje ciljeva pretrage.

6. Dokazi

Elektronički dokaz je za postupak značajan prije svega za kaznena djela računalnog kriminaliteta, zatim za druga kaznena djela počinjena računalnim sustavom, kao i za prikupljanja elektroničkih dokaza općenito (Pavišić, 2013). Baš ta posljednja zadaća je vrlo važna imajući u vidu da je računalna tehnologija u svim porama društvenog života.

Posebni oblici radnji kojima se prikupljaju elektronički dokazi su hitna zaštita pohranjenih računalnih podataka, nalog za proizvodnju, pretraga i oduzimanje pohranjenih računalnih podataka i prikupljanje računalnih podataka u realnom vremenu.

7. Tjeralica

Tjeralica je akt suda ili kaznene ustanove kojim se pokreće potražna djelatnost za određenom osobom (Pavišić, 2013). Uvjete za raspisivanje tjeralice propisuju postupovni propisi. Ona može biti raspisana za okrivljenikom protiv kojeg je pokrenut postupak zbog kaznenog djela za koje se progoni po službenoj dužnosti i za koje se može izreći kazna zatvora od tri godine ili teža kazna, a nalazi se u bijegu, ili ako je osuđenik pobjegao s izdržavanja kazne ili zavodske mjere. Prema području na kojem se vodi potražna djelatnost, tjeralice mogu biti raspisane za područje cijele države ili mogu biti međunarodne. Kad raspisuje tjeralicu na području države, sud koji vodi postupak obraća se nalogom određenoj policijskoj upravi mjesno nadležnoj za određeni sud. Policijska uprava raspisuje tjeralicu putem računalnog sustava, tako da je cjelokupnom području države u svakom trenutku dostupna lista potraživanih osoba.

Međunarodnu tjeralicu raspisuje sud putem Centralnog nacionalnog biroa Interpola. U sklopu Interpola od 1987. godine djeluje računalni sustav kriminalističkih informacija (CIS). Baze podataka tog sustava sadrže i podatke: a) traže li se određene osobe ili su osumnjičene za određena kaznena djela, b) terete li određene osobe obavijesti temeljem kojih se zahtijeva uhićenje ili postoji nalog ili opis određenog modus operandi; c) smatraju li se pojedine osobe međunarodno značajnim i postoji li opasnost da će počiniti nova kaznena djela.

8. Zaključak

Kaznena djela iz područja računalnog kriminaliteta događaju se gotovo svakodnevno i njih treba sprječavati na način da se počinitelji što prije uhvate i kazne. Naravno, uz hvatanje i kažnjavanje počinitelja, potrebno je puno ulagati u softverske alate koji će onemogućavati kaznene aktivnosti iz područja računalnog kriminaliteta bez obzira gdje se počinitelj nalazio. Ako je žrtva iz jedne države, a počinitelj iz druge, postoje mehanizmi kaznenog sankcioniranja počinitelja i njih je potrebno primjenjivati u praksi. Prema njima, kazneno sankcioniranje kaznenih djela iz područja računalnog kriminaliteta, trebalo bi se, uz ustupanje predmeta, provoditi u državi iz koje je počinitelj i to tek onda kada se utvrde sve relevantne činjenice u kriminalističkom istraživanju. Ako se mehanizmi kaznenog sankcioniranja počinitelja kaznenih djela računalnog kriminaliteta ne budu primjenjivali u praksi, onda njihovo postojanje gubi svaki smisao. Počinitelje kaznenih djela, bez obzira na vrstu, potrebno je sankcionirati kako se ista ne bi događala. Iz toga bi počinitelji svakako trebali nešto naučiti.

Literatura:

1. Dragičević, Dražen, Kompjutorski kriminalitet i informacijski sustavi, IBS, Zagreb, 2004, str. 28
2. Franjić, Siniša, Geneza računalnog kriminaliteta, Fakultet za kriminalistiku, kriminologiju i sigurnosne studije, Sarajevo, 2015, str. 53 - 70
3. Pavišić, Berislav, Komentar Zakona o kaznenom postupku, Drugo izdanje, Dušević & Kršovnik, Rijeka, 2013, 611; 344 – 345; 1103
4. Pavišić, Berislav; Modly, Duško i Veić, Petar, Kriminalistika – Knjiga 2, Dušević & Kršovnik, Rijeka, 2012, str. 621; 247 – 248
5. Šimundić, Slavko; Franjić, Siniša, Računalni kriminalitet, Sveučilište u Splitu – Pravni fakultet, Split, 2009, str. 17 – 21; 37

Siniša Franjić, Ph.D.
International University Brčko District BiH
sinisa.franjic@gmail.com

HACKING ON A CONCRETE EXAMPLE

Abstract:
Hackers, as individuals dealing with various forms of computer criminality, give themselves so much freedom and send people e-mails of blackmail. It is one of the most common forms of computer criminality which must be organize prevented. In today's modern, virtual world, it is unthinkable that there are situations where hackers unlawfully access someone else's data by hacking into someone else's computers and computer systems. In each such case, a criminal investigation must be carried out, the perpetrator should be found and punished accordingly.

Keywords: Iternet, Computer criminality, E-mail, Criminal act, Modus operandi