

ZAŠTITA BREND A I RAČUNARSKA PREVARA

Jovan Krstić, zamenik Republičkog javnog tužioca
jkrstic@EUnet.yu

Rezime: *Pravna zaštita prava intelektualne svojine ima veliku važnost za moderne države i sastoji se iz međunarodne (globalne) i nacionalne komponente. Globalni ekonomski aspekti zaštite prava intelektualne svojine podrazumevaju ispunjenje svih osnovnih principa multilateralnih konvencija i njihovo uključivanje u nacionalno zakonodavstvo. Novi Zakonik o krivičnom postupku donosi nove zadatke, funkcije, a takođe i povećava paletu aktivnosti i performansi javnog tužilaštva time što mu daje novu poziciju. Usled promena u modernoj ekonomiji i strategiji poslovanja došlo je do primene novih pravnih sredstava zaštite. Nove kiber metode istrage sada stoje na raspolaganju tužiocima. Danas se susrećemo sa digitalnim izazovom na polju zaštite od kriminala. Narodna skupština Srbije, kako bi obezbedila priključivanje i učešće u radu međunarodnih organizacija, je usvojila novi Krivični zakonik Srbije u koji su uneta nova krivična dela.*

Ključne reči: *brend firme - računarska prevara – kiber metode istrage*

BRAND PROTECTION AND COMPUTER FRAUD

Abstract: *Legal protection of the IPR has the significant importance for modern states and it has both global and national components. Global economic aspects of the IPR protection includes fulfillment of all basic principles of the multilateral conventions and adoption in the national legislation. The new Criminal Procedure Act (CPA) brings new assignments, new functions, as well as increased scope of activity and performance by changing the position of public prosecutor compared to the situation we had before. Due to the changes in modern economy and business strategy, the new legal tools of protection were introduced. The new cyber methods of investigation are now available to prosecutors. We are facing with the digital challenge on the field of the protection from crime. In order to join and participate in international organizations National Parliament of Serbia adopted the new Penal Code by introducing new criminal offenses.*

Key words: Brand Name – Computer Fraud – Cyber Methods of Investigation

Pravna zaštita prava intelektualne svojine ima veliku važnost za moderne države i sastoji se iz međunarodne (globalne) i nacionalne komponente. Globalni ekonomski aspekti zaštite prava intelektualne svojine podrazumevaju ispunjenje svih osnovnih principa multilateralnih konvencija i njihovo uključivanje u nacionalno zakonodavstvo. Novi Zakonik o krivičnom postupku donosi nove zadatke, funkcije, a takođe i povećava paletu aktivnosti i performansi javnog tužilaštva time što mu daje novu poziciju. Usled promena u modernoj ekonomiji i strategiji poslovanja došlo je do primene novih pravnih sredstava zaštite. Nove kiber metode istrage sada stoje na raspolaganju tužiocima. Danas se susrećemo sa digitalnim izazovom na polju zaštite od kriminala. Narodna skupština Srbije, kako bi obezbedila priključivanje i učešće u radu međunarodnih organizacija, je usvojila novi Krivični zakonik Srbije u koji su uneta nova krivična dela kao što je neovlašćena upotrebe tuđeg autorskog i drugog srodnog prava čl. 199 i dr.

Krivični zakonik sankcioniše sve osnovne vrste napada u oblasti visokotehnološkog kriminala:

- Čl. 298. sankcioniše oštećenje računarskih baza i programa;
- Čl. 299. sankcioniše sabotazu;
- Čl. 300. sankcioniše pravljenje i unošenje računarskih virusa;
- Čl. 301. sankcioniše računarsku prevaru;
- Čl. 302. sankcioniše neovlašćen pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka;
- Čl. 303. sprečavanje i ograničavanje pristupa javnoj računarskoj mreži;
- Čl. 304. sankcioniše neovlašćeno korišćenje računara i računarske mreže.

Kad je reč o zaštiti brenda, stoji nam na raspolaganju odredba čl. 233. KZ kojom se sankcioniše neovlašćenu upotrebu tuđe firma. Za ovo krivično delo neophodno je da ga izvršilac vrši u nameri da obmane kupce ili korisnike usluga i da se pri tome posluži tuđom firmom, tuđom geografskom oznakom porekla, tuđim žigom ili zaštitnim znakom ili tuđom posebnom oznakom robe ili unese pojedina obeležja ovih oznaka u svoju firmu, svoj žig ili zaštitni znak ili u svoju posebnu oznaku robe. U posebnoj glavi KZ-a „Krivična dela protiv intelektualne svojine“, kod krivičnog dela povreda moralnih prava autora i interpretatora iz čl. 198. KZ, sankcioniše se objavljivanje tuđeg dela pod svojim imenom. Kod neovlašćenog uklanjanja ili menjanja elektronske informacije o autorskom i srodnim pravima iz čl. 200. KZ. Sankcioniše se objavljivanje dela bez navođenja autora. Kod povrede pronalazačkog prava iz čl. 201. KZ, te kod neovlašćenog korišćenja tuđeg dizajna iz čl. 202. KZ, sankcioniše se neovlašćena upotreba ovih intelektualnih dobara. Sve ove radnje često se preduzimaju radi obmane korisnika usluga na Internetu. Zbog subtilnosti postupanja od strane izvršilaca i poslovične anonimnosti na Internetu i nedostataka antropomorfnih karakteristika izvršilaca na internetu, principi istrage koje treba da primeni budući Posebni tužilac za visokotehnološki kriminal su daleko od klasičnih.

Za uspešnu zaštitu od visokotehnološkog kriminala neophodno je da se u MUP RS osnuju odgovarajuća odeljenja za borbu protiv kompjuterskog kriminala, za zaštitu prava intelektualne svojine i za borbu protiv privrednog kriminala uz odgovarajuće prilagođavanje u odeljenju za borbu protiv organizovanog kriminala i u obaveštajnim agencijama. U Okružnom sudu u Beogradu je u toku formiranje posebnog odeljenja za postupanje za krivična dela visokotehnološkog kriminala, a u Okružnom javnom tužilaštvu u Beogradu se priprema tim koji će sačinjavati Posebno tužilaštvo za borbu protiv visokotehnološkog kriminala. U tom cilju vrši se i stručno usavršavanje zamenika javnog tužioca uz pomoć univerziteta, nevladinih organizacija CLDP, UNDP, OSCE i dr.

Zaštita računarskih podataka i proizvoda intelektualne svojine na Internetu podrazumeva primenu novih instituta krivičnog procesnog prava koji se nazivaju

specijalnim istražnim metodama, taktikama i postupanja, kao što su: presretanje, praćenje, prisluškivanje, nadgledanje, snimanje, kontrolisane isporuke, simulovani ugovori, ubacivanje svedoka saradnika, pretres, zaplena i dr. Pri tome treba imati u vidu da je opšti uslov validnosti dokaza da se na zakonit način pribave tzv. nezavisno potvrđeni dokazi. Dokazi prikupljeni istragom na Internetu moraju biti takvog kvaliteta da ih mogu potvrditi nezavisni izvori (ekspertne ustanove, službeno vođeni dnevници događanja, izveštaji firmi čiji je brend zloupotrebljen, provajderi čiji serveri su registrovali pristup osumnjičenog i sl.).

Nezavisno potvrđivanje dokaza može biti faktičko potvrđivanje ili dokumentalno potvrđivanje. Faktičko potvrđivanje obuhvata snimanje i konverziju poruka (sačuvanih u arhivu i poslatih u pravnom saobraćaju) ili izdate poruke od strane provajdera na zahtev javnog tužioca, a po odobrenju istražnog sudije. Dokumentalno potvrđivanje se vrši dokumentima pribavljenim postupkom tzv. Registracione zamke ili monitoringom i traganjem na Internetu ili pribavljanjem dokumenata putem pravne pomoći od država izdavanja dokumenta, država prijema dokumenta ili država tranzita dokumenta.

Postavljaju se sledeća osnovna pitanja za istragu na Internetu: Koju vrstu podataka tražimo? Koja procesna sredstva stoje na raspolaganju tužiocima? Koja je osnovna koncepcija istrage?

Prvo: Koju vrstu podataka tražimo? Osnovno je razlikovati sadržajne podatke od nesadržajnih podataka. Nesadržajni podaci su podaci o prometu, informacije o podnosiocu, o ceni usluga itd. i lako ih je pribaviti, ali imaju manju snagu, sa manjim stepenom upuštanja suda u raspravu i u provere. Sadržajni podaci su bitniji i ostavljaju veći utisak na sud, jer imaju odgovarajući intelektualni sadržaj.

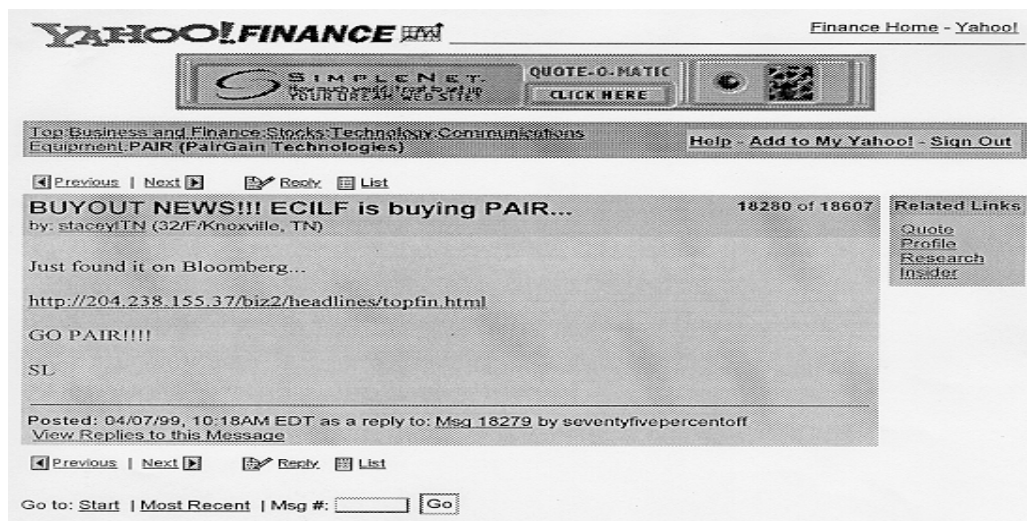
Kad je reč o vremenu stvaranja dokumenata, potrebno je razlikovati Real-time podatke od istorijskih podataka. Istorijska podatke je lako pribaviti jer su oni pouzdano sadržani u odgovarajućim dnevnicima događanja na serveru provajdera ili arhivi baze podataka u informacionom sistemu. Podaci dobijeni u realnom vremenu su mnogo značajniji, ali se teško pribavljaju putem pretresanjem sadržaja poruka ili putem monitoringa nad saobraćajem poruka. Ova vrsta podataka zahteva viši nivo dokazivanja, jer se sud više upušta u njihovo razmatranje i proveru.

Osnovno znanje koje mora imati javni tužilac i istražni sudija je poznata tehnologija komunikacije na Internetu (uprošćeno: računari imaju ličnu kartu - IP adresu - kombinaciju od četiri ili šest serija brojeva, uloga mrežnih računara – rutera, da emisio-ni računari seckaju poruke u paketiće, a odredišni računari sklapaju poruke, da postoje protokoli emitovanja i sporazumevanja – po TCP protokolu – se seckaju i pakuju poruke po slučajnom redosledu, a po IP – protokolu se obrađuju datagrami i dodeljuju adrese).

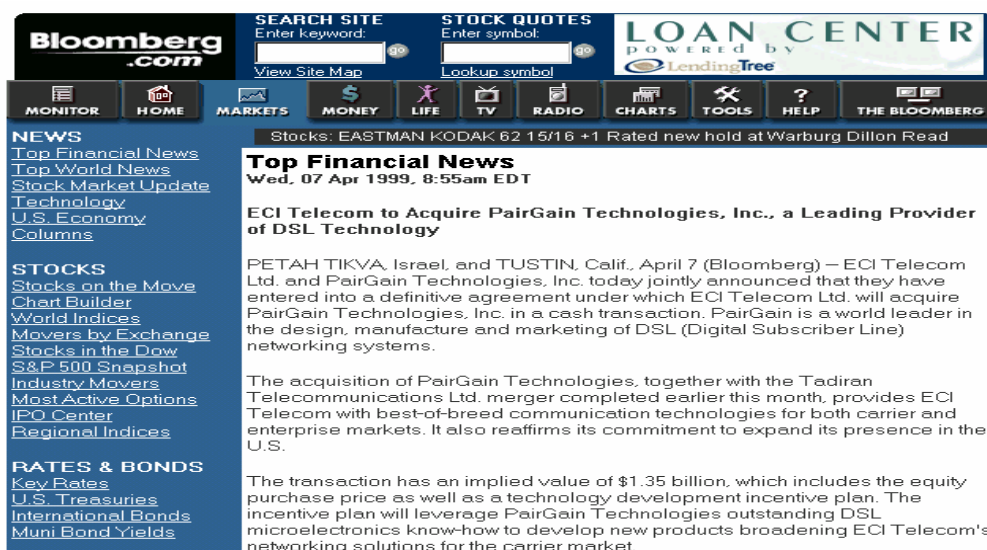
Na primeru istrage slučaja zloupotrebe brenda firme Pair Gain Technologies¹ u svrhu prevare investitora ilustrovana je osnovna koncepcija pristupanja u otkrivanju izvršilaca krivičnih dela putem Internet tehnologije (www - World Wide Web – Svetska mreža).

Kako to obično biva, izvršioci krivičnih dela na Internetu prvo učine verovatnim najavu svojih prevarnih poruka na svetskom pretraživaču kao što je na primer Yahoo.com. Najava služi da usmeri samo ozbiljno zainteresovane i odnosi se na posebnu grupu imućnih lica koja prate finansijsko stanje poznatih firmi i nastoje da što pre jeftino kupe akcije kompanija koje će kasnije ostvariti najveći profit na tržištu i kojima će vrednost akcija skočiti. To je za investiranje isto tako neodoljivo kao kada bi ponudili da vam, na primer, prodaju delove za „folsvagen“ upola jeftinije od drugih i to na čvorištu koje garantuje da ga je sama fabrika stvorila? Tekst najave u konkretnom slučaju je jednostavan: „Upravo sam našao nešto (interesantno) na Blumbergu...“

¹ Jason Gull, Attorney at Law, US Department of Justice, Case Presentation



Tekst prevarne poruke je, kada su zainteresovani proveravali, zaista bio objavljen na Finance message board – u koji predstavlja Blumbergov portal na kome učesnici objavljuju razne finansijske vesti i ponude. Dakle, i sam brend portala je zloupotrebljen, tako da se istraga već u prvim danima mora uveriti da li je portal originalan ili „hakovan“.



Sadržinski gledano ovaj dokument sadrži neistinitu poruku koja se oglašava kao vrhunska finansijska vest o tome da su firme ECI Telecom i Pair Grain Technologies sklopile sporazum o primeni najsavremenije komunikacione tehnologije i proširenju svog prisustva na američkom tržištu zbog čega se očekuje znatno povećanje vrednosti njihovih akcija. Međutim, nakon izvesnog vremena i prijave investitora, ispostavilo se da je ova priča lažna. U dnevnoj štampi je objavljeno upozorenje da zajednički posao nije nikada ugovoren, a investitori se suočavaju sa potencijalnom prevaram na Internetu.

Internet Hoax Sends O.C. Tech Stock Up 31%

■ **Cyberspace:** False, detailed report that PairGain was being acquired illustrates growing potential for Net fraud.

By JONATHAN GAW
TIMES STAFF WRITER

In one of the biggest and most elaborate Internet stock frauds yet, an unknown perpetrator constructed a bogus announcement that an Orange County-based technology company was being acquired for \$1.35 billion, driving the company's stock up 31% Wednesday morning.

The hoax underscores mounting concerns about stock manipulation and other fraud on the Internet. The instant and free flow of information over the Net, a soaring stock market and a booming online trading industry are providing fertile ground for such scams.

The hoax involving Tustin-based PairGain Technologies was unusual in its detail and precision. It used a free Web page service owned by Lycos Inc. to create a site that looked and behaved almost identical to that of Bloomberg News, the financial information

wire service. The false report was then spread on Yahoo Inc.'s finance message boards, causing investors to bid up PairGain's shares, making it one of the day's most actively traded stocks.

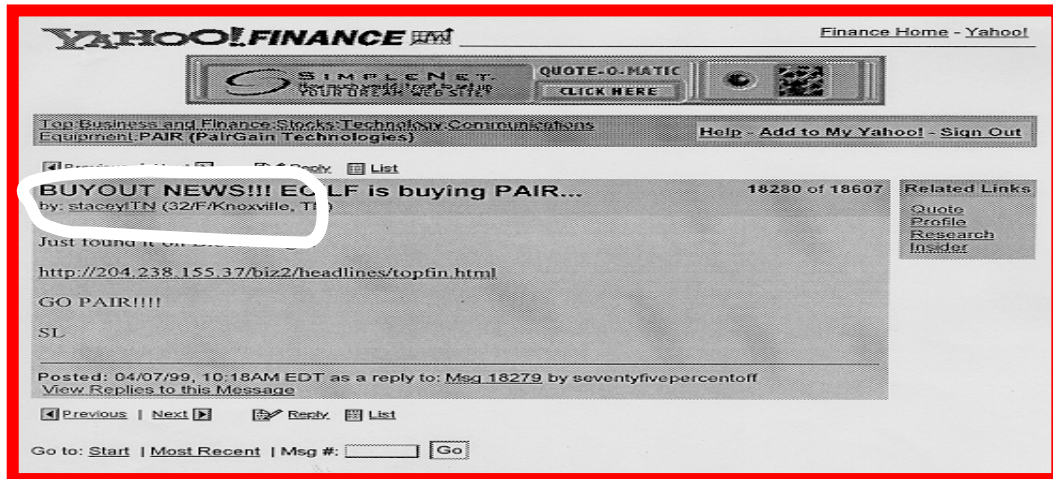
The perpetrator's goal, conceivably, was to boost the stock price in order to unload shares at a better price.

Most cases of online stock fraud involve small companies whose stocks are thinly traded. The PairGain case is significant because the company's stock is worth more than \$650 million. There are 52.8 million shares in public hands, and nearly 2 million of those are traded every day.

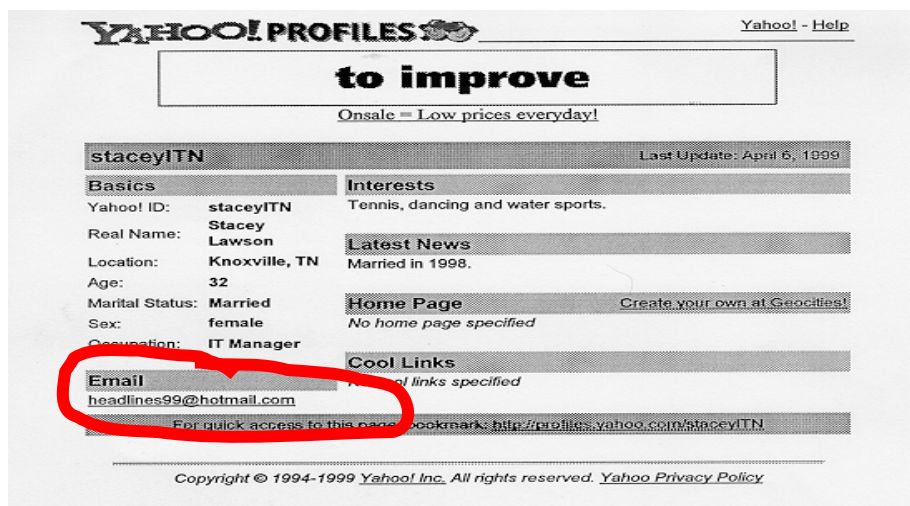
PairGain has long been the subject of acquisition rumors, and the alleged acquiring company named in the hoax, ECI Telecom Ltd. of Israel, is often mentioned as a potential suitor, making the ruse all the more believable. Officials at both companies said they had no

Please see HOAX, A10

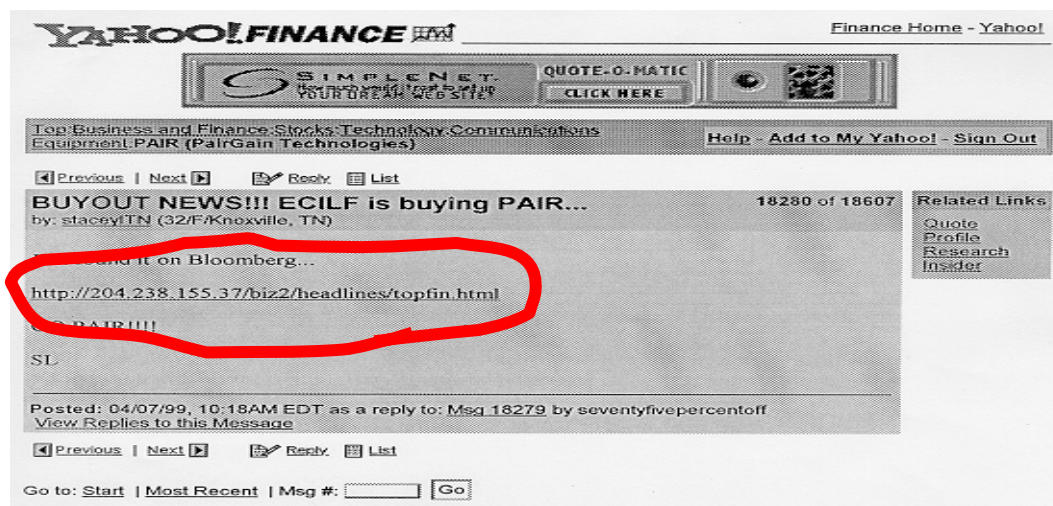
Tradicionalne istražne metode u ovakvim slučajevima ne pomažu. Ako pratimo kretanje novca, ako uočavamo neobične komercijalne poslove, ako tražimo lica koja imaju koristoljubive motive i ako sarađujemo sa Upravom za sprečavanje pranja novca, to još nije dovoljno da identifikujemo izvršioca. Internet je sam po sebi mozaik intelektualnih svojina, a lica koja se pojavljuju na internetu nemaju antropomorfne karakteristike po kojima bi bila identifikovana. Uobičajenim istražnim radnjama je nemoguće otkriti izvršioca. Cyber-metode istrage su mnogo delotvornije...



Cyber-metode istrage podrazumevaju ispravne polazne tačke za započinjanje istrage. Prvo je neophodno iskoristiti listing javne baze podataka na svetskom pretraživaču „Yahoo.com“. Pošto je pristup ovoj bazi podataka slobodan, u svakom trenutku se može utvrditi ko je nominalno korisnik usluga bilo kog provajdera. U ovom slučaju domen provajdera je poznat. Međutim, ovaj identitet je često lažan, kao u ovom slučaju. „Stacey ITN“ je korisničko ime lažne gospođe Lawson.



Pravila syber-metode nalažu da se na osnovu datih podataka i adresa izvrše provere koje podrazumvaju upotrebu javno dostupnih alata za proveru IP adresa (na primer na: ARIN, www.samspace.org, geektools.org) kako bi se proverila IP adresa "204.238.155.137". U ovom slučaju ona pripada slobodnom web hosting servisu pod nazivom „Angelfire”. Tako se utvrđuje zemlja domicila servisa sa koga se putem pravne pomoći ili u mreži za saradnju tužilaca traže podaci o korisniku. Tada otkrivamo da je niz prevarnih poruka poslat preko više servisa čiji se imidž pouzdanosti i ozbiljnosti praktično zloupotrebljava.



Prva dilema koju mora da reši svaki istražni tim je da odredi da li je cela firma (u ovom slučaju Pair Gain Technologies) umešana u prevaru i koristi svoje ime za potrebe neosnovanog reklamiranja ili je eventualno neko u toj firmi izvršilac ili je izvršilac lice van firme. Postavlja se pitanje šta se u stvari može saznati o firmi Pair Gain Technologies i o zaposlenim licima?

Podaci o klijentima Web host Angelfire customers servisa otkrivaju neke lažne informacije (na primet: ime i adresa su po pravilu lažni), ali je e-mail adresa ista kao i alternativna adresa „StaceyITN”. Tako dolazimo do efektne primene Cyber-metoda

istrage kod provajdera. „Angelfire“ koji čuva listu korisnika koji edituju ili kreiraju web page. Ove liste se dobijaju na zahtev suda u međunarodnoj pravnoj pomoći ili na zahtev policije u međunarodnoj policijskoj saradnji. Ove liste otkrivaju veze između IP adresa koje poseduju Mindspring i Pair Gain.



Liste korisnika beleže pristup Lreynolds54 i StaceyITN i otkrivaju da pripadaju

Izvesnom Gary Dale Hoke, Jr. zaposlenom u firmi PairGain Technologies. Međutim, kada se u istrazi i dođe do nekog konkretnog fizičkog lica, to još uvek ne znači da je to lice automatski osumnjičeno lice. Osnovno je da se razlikje krivična odgovornost pravnog lica od odgovornosti personalne substance tog lica. Ovaj princip nameće pitanje: Ko šalje poruke za PairGain Technologies? Ono što se obično utvrđuje je da link očigledno pripada toj firmi, što uvek pobuđuje sumnju da je firma pribegla prevarnom načinu sticanja dodatnog kapitala. Pribavljeni dnevници monitoringa po nalogu suda su čvrst dokaz o umešanosti firme. Posmatrane su aktivnosti u poslovanju i na mreži i svi pristupi su beleženi po vremenu i IP adresama. Ovi dnevници pokazuju da račun kojim je plaćeno čvorište „ghoke“ pripada Gary Hoke-u, inače zaposlenom u firmi čiji se brend koristi.

U ovoj fazi istrage se tek postavljaju prava pitanja. Prvo pitanje: da li je „ghoke“ račun „hakovan“? Odgovore na ovo pitanje daju pregledi pristupa (radius log entries) koji snimaju prispele informacije o identitetu (ID) pozivara na serveru Internet servis provajdera (ISP). Svaki NN korisnik pa i korinik zvani „ghoke“, ostavlja trag TT linije pa i servis „Mindspring-a“ otkriva da je poziv na servr došao iz kuće osumnjičenog. Samo prisluškiivanje, praćenje ili pretres kuće definitivno razrešava identifikaciju svakog izvršio-oca ovih krivičnih dela na Internetu. I u međunarodnoj pravnoj pomoći može se zatražiti pretres stana osumnjičenog lica kada je posledica krivičnog dela nastala na teritoriji više država.

U epilogu konkretnog slučaja pretres stana na određenoj adresi u mestu Raleigh, N.C. je rezultirao zaplenom laptop računara kao sredstva za izvršenje dela sa nacrtima lažnog novinskog članka objavljenog na Blumbergovim vestima, u toku pretre- sa osumnjičeni je, kao što to biva, pokušao da obriše ove podatke, a profit od korišće- nja lažnih podataka o firmi u kojoj je zaposlen nameravao je da skine sa računa na koja su sredstva uplaćena i pobegne.

Ilustrovani slučaj je jednostavan i zato je poslužio kao ilustracija metodologije, ali se sada u praksi, u toku traganja na Internetu i u pogledu upotrebljenih alata radi o brojnim dodatnim merama koje istražni organi moraju da primene da bi ušli u trag izvršiocima koji vrše razne skokove sa servera na server po Internetu i koji koriste razne slabosti sporazumevanja po postojećim protokolima. To dovodi istragu do neverovatno komplikovanih vrsta monitoringa uz upotrebu alata koji su dizajnirani da se upuštaju u sadržaj i analizu sadržaja informacija.

http://www.telekom.yu/SiteTelekom/Default.htm - Microsoft Internet Explorer

Datei Bearbeiten Ansicht Favoriten Extras ?

Zurück Suchen Favoriten Medien

Adresse http://www.telekom.yu/SiteTelekom/Default.htm

Telekom Srbija Serbian Search

Home Telephone directory Site map Contact

Telephone directory White pages Yellow pages

Network group: Beograd - 011 Town: Beograd (Beograd)

Phone number: 2882711

Surname: Street:

Name: Number:

Number of items: 10

Search Reset

Instruction

Phone No.	Surname	Name	Street	No.	Apt.No.	Town
2882711	Stajić	Golubica	27 Marta	16		Beograd

Result: 1 subscriber(s)
Page 1

About us

Services and products

- Fixed telephony
 - Types of equipment
 - Value added services
 - How to become a subscriber
 - HALO payphones and cards
 - Important telephone numbers
 - National area codes
 - International area codes
 - Telephone book
 - Tariff system
- ISDN
- Mobile telephony
- Paging
- Data transmission
- Internet
- Complete solutions
- Frequently asked

[illegible]

CORNER
Bank Card Center





Corner Banca SA
Via Canova 16
6901 Lugano
Tel: 091 800 41 41
www.cornercard.ch