Zaštita računala od napada s mreže

Iako konzument niže obrađenih tema treba biti krajnji korisnik računala, članak je pisan za vas – moju braću i sestre sistemce. Radi se, naime, o **predlošku uputa za korisnike računala**, glede zaštite od provala s računalno-komunikacijskih mreža.

Važno je uočiti da u ovom članku termin „računalo“ rabim kao generički pojam za razne vrste umreženih digitalnih uređaja za osobnu uporabu: PC desktop, PC prijenosnik, pametni telefon, tablet.... bogme i pametni televizor. Uskoro ćemo pojmom „umreženo računalo“ uskoro morati obuhvatiti i automobile, te gledati kako da ih zaštitimo od provala s mreže, jao!

Nedvojbeno je da koncept BYOD, te raznovrsnost spomenutih uređaja – time i operativnih sustava koji ih pogone, dakako – nama sistemcima izrazito kompliciraju praksu zaštite informatičkih sustava za koje smo odgovorni. Nećemo sada dublje ulaziti u to trusno područje, zadržavamo se na edukaciji korisnika za sigurnosno pravilnu uporabu umreženog računala.

Primijetit ćete izostanak opisivanja kako nešto napraviti, uzrok tomu je raznorodnost operativnih sustava i, posljedično, procedura. Škrtarimo i s tehnikalijama, težište je na savjetima i što poduzeti, s pratećim ilustracijama.... ukratko, didaktički, metodički i lingvistički nastojimo biti što uviđavniji prema targetiranoj publici.

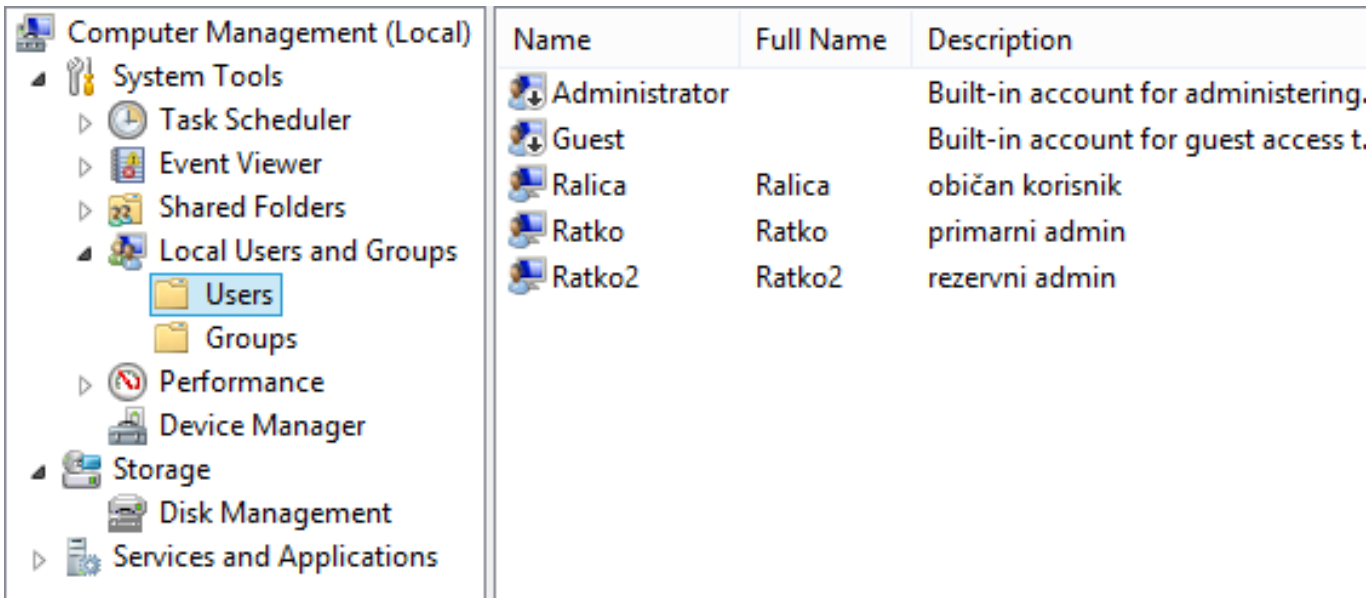
Ovisno o specifičnostima korisničkog skupa vaše IT unije, niže izloženo gradivo ćete prilagoditi, npr. ako se kod vas dominantno rabe Android smartfoni i tableti, jasno je da ćete upute uskladiti sa tom činjenicom. Samo nemojte pretjerati s tehnikalijama, naime, nije nam interes odbiti čitatelja kad smo već uložili poveći trud u materijal namijenjen njemu, zar ne?!

Sigurnosne upute za korisnike

1. Svakako postavite neku autentikaciju (pristupni kod, vjerodajnica) kao preduvjet za uporabu računala, bez obzira rabi li se interaktivni ili udaljeni način pristupa. Ako Vaš uređaj omogućuje stvaranje lokalne baze računa, za svoje potrebe kreirajte:
- jedan običan korisnički račun, sa minimalnim privilegijama – njega je preporučljivo rabiti kad ste na Internetu;
- dva računa sa administrativnim privilegijama – jedan je rezervni, njega ćete rabiti samo ako maliciozni softver ošteti ili modificira profil kojega operativni sustav kreira za Vaš glavni administrativni račun.

Svim računima dodijelite ekstradugačku kompleksnu zaporku, znači, minimalne duljine 12 (dvanaest) znakova. Naizgled je taj minimum od 12 znakova pretjeran, ali vodite računa da su vjerodajnice tipa „ime/zaporka“ dokazano najneotpornije na probijanje i krađu.

Baza lokalnih korisničkih računa trebala bi izgledati kao na nižoj slici; uočite da je deaktiviran originalni Administrator operativnog sustava.



2. Na računalo instalirajte samo neophodan softver. Prije instalacije bilo kojeg softvera informirajte se, ne samo o njegovim funkcionalnim već i o sigurnosnim značajkama. Dodatno, uvjerite se da se taj softver održava i unaprijeđuje.

Kad s Interneta skidate besplatni softver, birajte servise sa ugledom. Time značajno umanjujete mogućnost instaliranja softvera inficiranog nekim zlоćudnim kodom. Nižom slikom ilustriramo rečeno: postoje Web servisi – u tu kategoriju spadaju i on-line dućani Applea, Googlea, Microsofta... - koji vode „zdravstveni karton“ za softver u svojoj ponudi, bio on komercijalan ili besplatan. Time oni, štiteći svoj ugled i poslovanje, štite i korisnika.

We've got big news to share: we're proud to inform our users that **Softonic has become the most secure free software download site in the world**, thanks to the development and implementation of the Security Seal service.

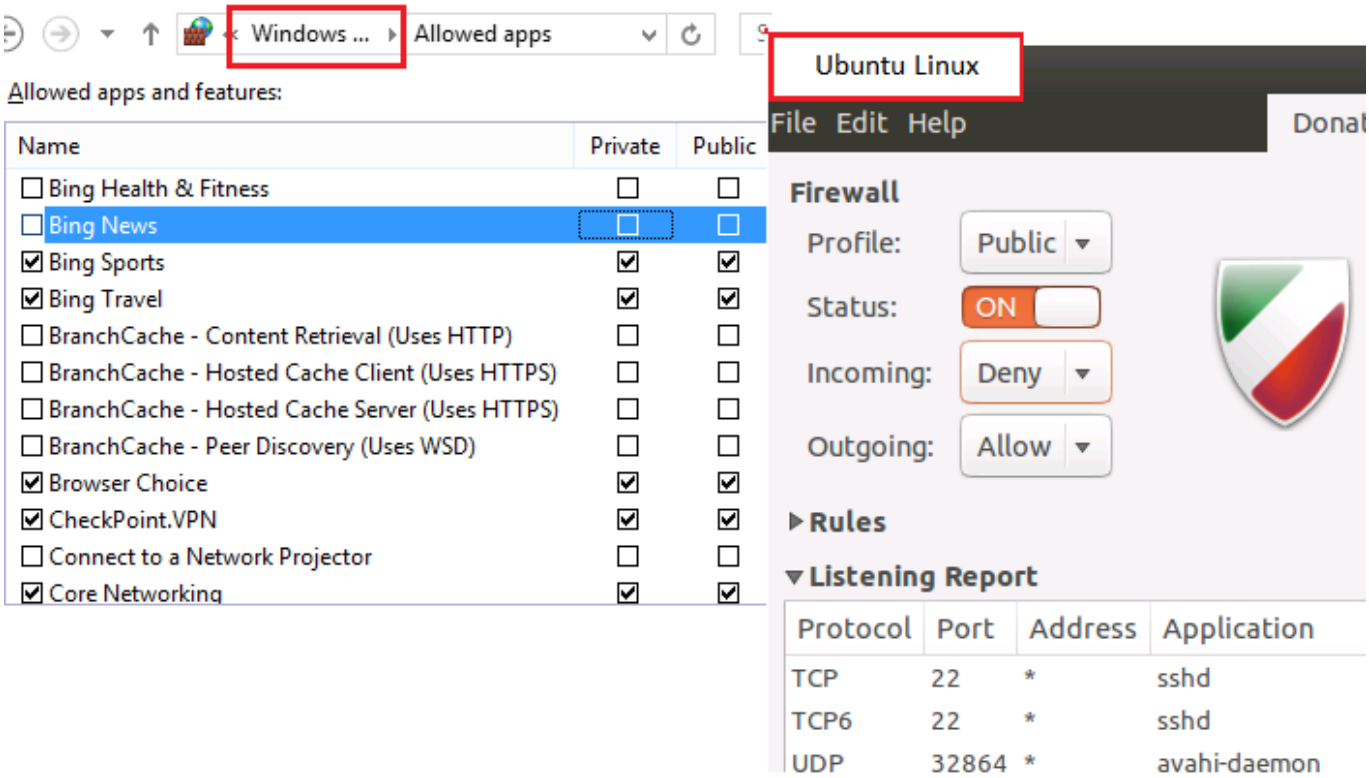
Softonic is aware of our users' growing demand for security; that's why we've invested so much effort in developing this service. **Its features mean that all software on our portal is scanned using thirty different antivirus programs, which will guarantee that these programs are not infected.** The list of these thirty antivirus programs includes the biggest ones on the market, such as Avast, Kaspersky, and Norton.

After the analysis, which is carried out on a regular basis, **users can see the security level of the programs they want to download**. If there's no risk of viruses or Trojans, there will be an option to securely download via the Security Seal service. We also give our users the opportunity to look at the analysis in detail and offer secure alternatives for downloading similar programs.

3. Uključite lokalni vatrozid (firewall). Pravilno konfiguriran vatrozid odbija sve konekcije ili transakcije koje nije iniciralo Vaše računalo. Potom je moguće, po raznim kriterijima, primijeniti iznimke, ali neka tih iznimaka bude što manje. Povremeno, posebno nakon instalacije aplikacija, prekontrolirajte stanje i konfiguraciju vatrozida.

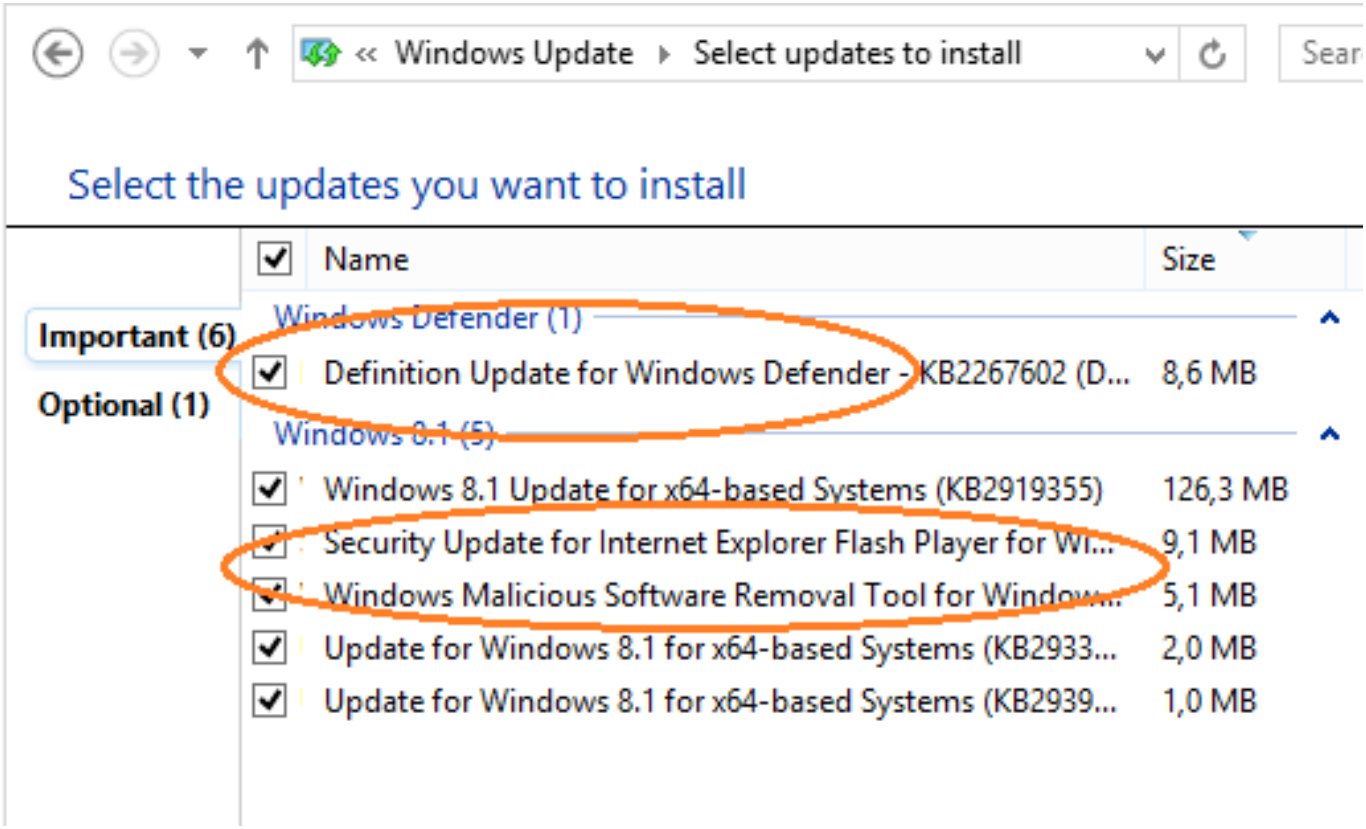
Na nižoj slici dva su vatrozida – lijevo je Windows Firewall, desno je na Linuxu popularni Uncomplicated Firewall. UFW je podešen tako da bez oglašavanja odbaci sav dolazni promet kojega

računalo nije iniciralo. Windows Firewall upravo rekonfiguriramo utoliko što onemogućavamo komunikaciju sa Microsoftovim Bing servisom. Jasno, Microsoft je podesio vatrozid tako da njegov Windows operativni sustav može komunicirati sa njegovim Bing servisom ali mi smo zaključili da nam to ne treba.



4. Redovito primjenjujte sigurnosna ažuriranja, od razine pogonskih programa (drivera) preko operativnog sustava do aplikacija. Vodite računa da se softver različitih proizvođača ne može ažurirati („pokrpati“) sa samo jednog mjesta, na primjer, na računalu s nekim Windows OS-om nećemo moći, rabeći samo Windows Update servis, ažurirati razne ne-Microsoft aplikacije, a takve sigurno imamo na računalu. Isto pravilo važi i za druge operativne sustave.

Na nižoj slici, sa Windowsa 8.1 pristupili smo Windows Update servisu. Možemo primijetiti da je Microsoft pripremio važna sigurnosna ažuriranja za našu verziju Windowsa.



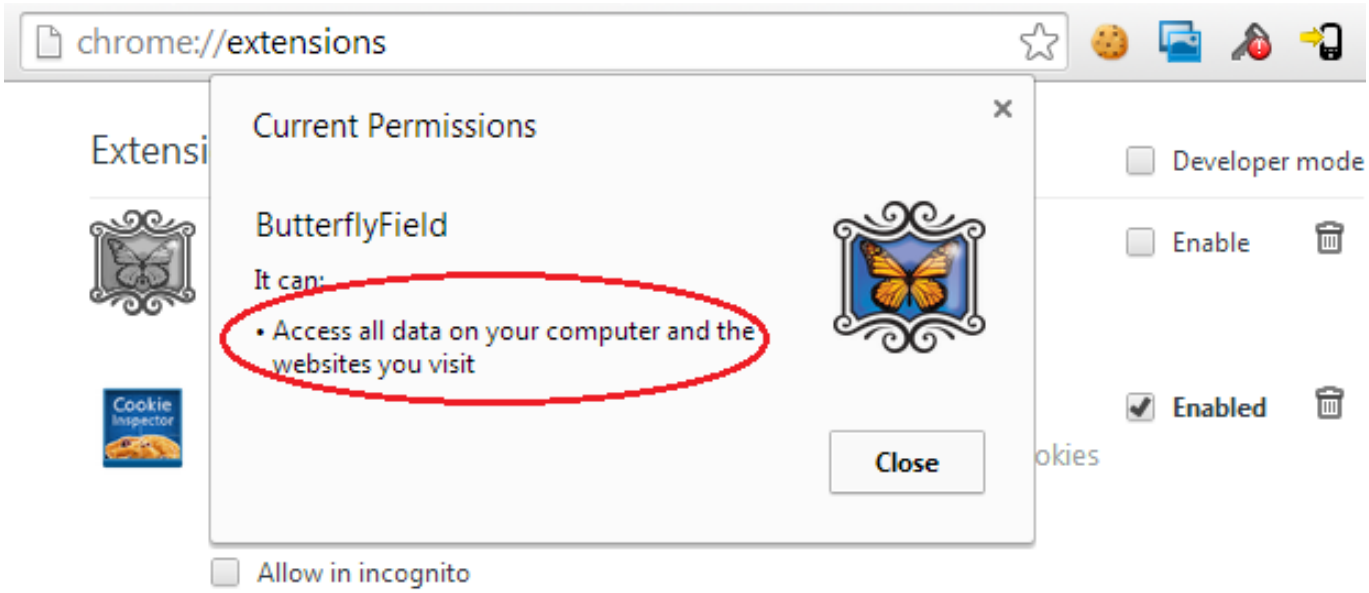
* Redovita primjena sigurnosnih ažuriranja na sav sofver računala najefikasniji je način zaštite!

5. Instalirajte i održavajte softver za otkrivanje, neutraliziranje i uklanjanje malicioznog softvera. Budući da ne postoji zaštitni softver ove vrste koji jednako kvalitetno brani računalo od raznih vrsta malicioznog koda (virusi, crvi, trojanci, špijuni.... itd.), mudro je instalirati na računalo jedan „glavni“ detektor/eliminator malicioznog koda - taj je ujedno zadužen za nadgledanje računala u stvarnom vremenu – te par pomoćnih detektora/eliminatora. Povremeno ćemo se maknuti s računalne mreže, opozvati glavni a pokrenuti pomoćne programe u full-scan načinu rada.

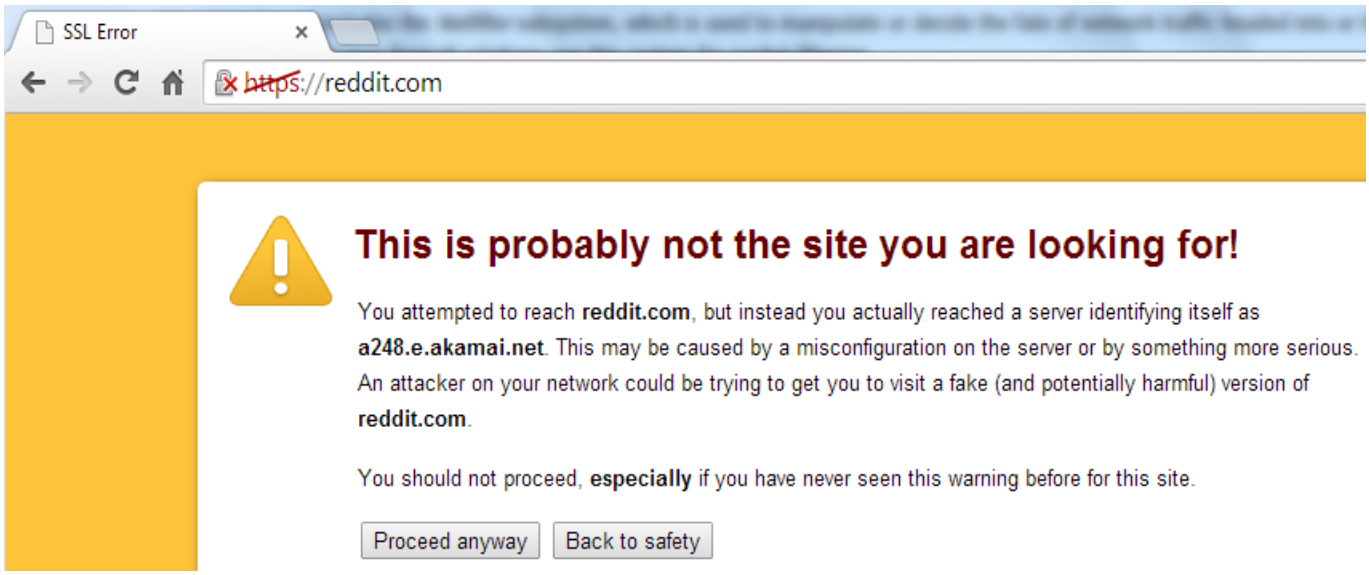
Na gornjoj slici u 4. točki možete primijetiti da Microsoft, proizvođač Windowsa, primjenjuje upravo opisani način zaštite, naime, sa servisa Windows Update skidamo ažuriranja za Windows Defender i Windows Malicious Software Removal Tool. Besplatni a vrlo kvalitetni alati te namjene dostupni su na Webu, samo slijedite sugestije iz 2. točke.

6. Uključite sigurnosne funkcije Internet preglednika a isključite sve nepotrebne dodatke i ekstenzije (poznate i kao add-ons, plug-ins i sl.). Upravo kroz Internet preglednik mi stupamo u interakciju sa raznim Web sadržajima, stoga se cyber kriminalci fokusiraju na sigurnosne propuste Internet preglednika. Ali računaju oni i na nesmotrenost korisnika tog preglednika! Zato ne isključujte zaštitne funkcije preglednika „jer samo smetaju“, naime, ono što je korisniku „smetnja“, napasniku onemogućava ili barem otežava provalu u računalo!

Na nižoj slici smo onemogućili jednu ekstenziju (možemo ju i ukloniti) Chrome preglednika kad smo vidjeli kakva su joj prava na našem računalu.

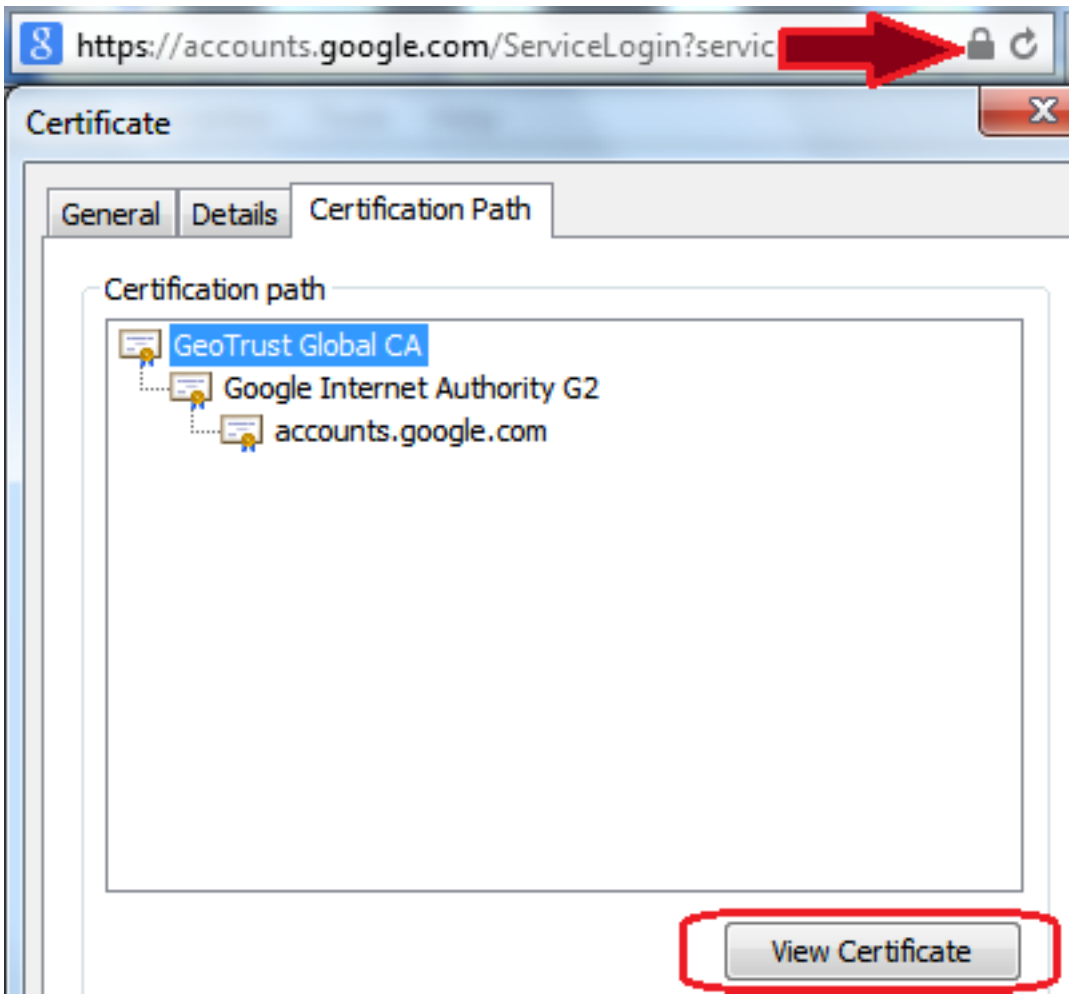


7. Favorizirajte one Web usluge koje nude ili nameću https: tip konekcije, jer tada nam naš Internet preglednik može pomoći u izbjegavanju zamki. Niže je prikazana ta situacija. Nastavit ćemo dalje samo ako smo sigurni da je riječ o lažnoj uzbuni.



Jednom uspostavljena, *https* veza je vrlo siguran komunikacijski kanal. Ali postoje napadi poznati kao ***man-in-the-middle*** i ***SSLstrip*** - oni se izvode tijekom (početkom) uspostave *https* konekcije tako da se korisnika preusmjeri na kopiju ciljne Web usluge koja je pod kontrolom hackera. Dakle, čak i kada pristupimo nekoj Web usluzi bez prethodnih upozorenja browsera, a moramo odraditi neke osjetljive poslove – recimo, financijsku transakciju – dobro je provjeriti autentičnost tog Web mjesta. To radimo uvidom u certifikate kojima se to Web mjesto predstavlja. Najvažniji je Certification Path – on se proteže od certifikata usluge do vršnog (root) izdavatelja certifikata i mora biti konzistentan, neprekinut.

Niža slika pokazuje kontinuirani Certification Path za Google uslugu Gmail. Vidimo da je server kojemu smo pristupili, i koji od nas traži unos vjerodajnica ime/zaporka, dobio certifkat od Google Internet Authority. Taj nam je autoritet nepoznat ali, srećom, izdavatelj njegovog certifikata je poznati PKI autoritet GeoTrust, dakle, možemo zaključiti da je sve u redu i da smo zaista na originalnom Google servisu Gmail.



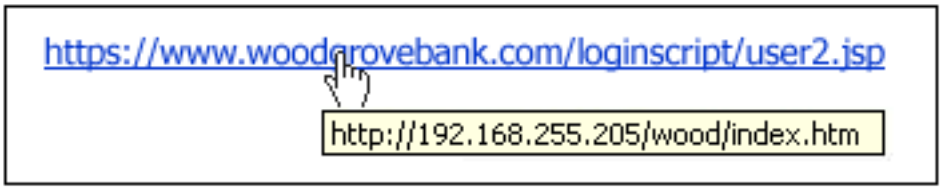
* U konfiguracijskim postavkama Internet pregledniku podesite verzije SSL/TLS sigurnosnih protokola (bez njih se ne mogu kreirati HTTPS konekcije): SSL 2.0 i TLS v.1.0 moraju biti isključeni jer su dokazano i nepopravljivo ranjivi.

8. Ako smo se na neki Internet resurs spojili http: protokolom, uređaj i podaci koji se u njemu nalaze izrazito su izloženi raznim vrstama napada, stoga, u ovoj se situaciji korisnik treba zaista odgovorno ponašati. Osnovne mjere (samo)zaštite su:

- prije spajanja pokrenuti Internet preglednik s pravima običnog korisnika računala (a ne administratora);
- izbjegavati „skitaranja“ po Internetu i „istraživanja“ Web sjedišta;
- ne kliketati brzopleto mišem po dijaloškim okvirima, linkovima i sličnim elementima web stranice;
- ne rabiti olako svoje vjerodajnice;
- ako posumnjamo da smo izloženi napadu: namjestiti glavni anti-malware program na skeniranje cijelog računala tijekom boot sekvence; isključiti računalo i nakon par minuta ga uključiti.

9. Promišljeno rabite e-poštu – dovoljan je jedan lakomisleni klik mišem na naizgled bezazlenom linku unutar pristigle poruke kako bi se pokrenuo napad na uređaj, time i na Vas, korisnika tog uređaja. Mudro je imati barem dvije mail adrese: jednu „privatnu“ – nju ćemo rabiti samo za prepisku sa poslovnim partnerima i osobama od povjerenja, te jednu „javnu“, koju ćemo rabiti u slobodnijoj komunikaciji. Razumljivo, opreznije ćemo postupati s porukama pristiglim na našu javnu mail adresu. Sigurnosno gledano, poruke od nepoznatih osoba najbolje je niti ne otvarati.

Niža slika otkriva ne samo zamku koju su nam hakeri ugnijezdili u poruku nego i način kako tu zamku pravovremeno uočiti: nadnesemo pokazivač miša nad link i usporedimo pravi link (na slici to je onaj donji, uokviren) sa onim prikazanim u poruci.

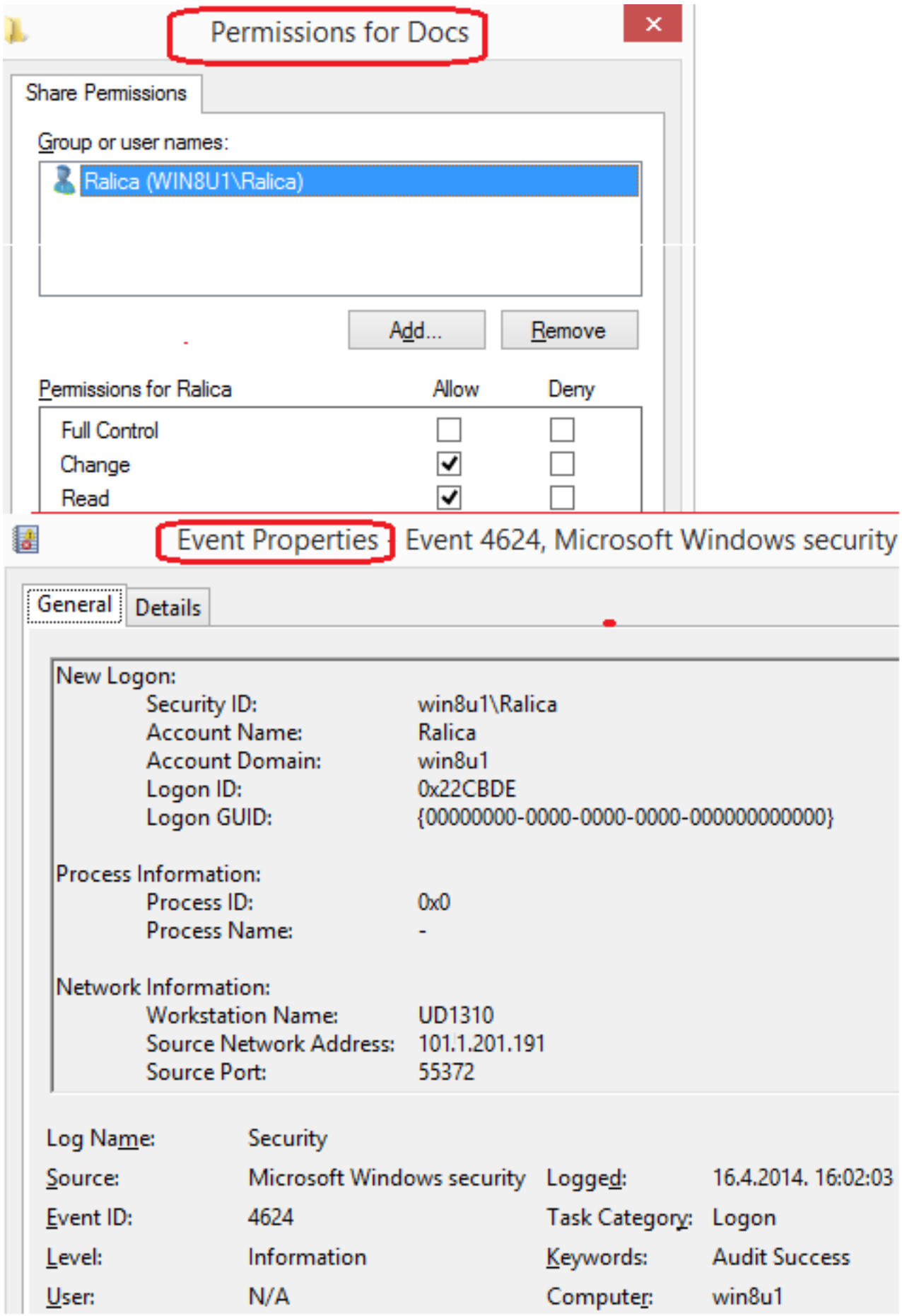


* Znate li da dvoklikom mišem na dokumentu tipa .doc ili .pdf, priloženom uz e-poruku, možete pokrenuti inficiranje računala zloćudnim kodom? Rečeno vrijedi i za druge tipove datoteka, uključujući slikovne!

10. Kad dijelite lokalne mape (direktorije, foldere) za pristup s mreže, vodite računa o sljedećem:

- nitko se ne smije moći spojiti na dijeljeni direktorij bez prethodne autentikacije – ovime omogućujete identificiranje eventualnog napadača jer će operativni sustav zapisati razne podatke o autenticiranom korisniku;
- nikome ne dodjeljujte pravo Full Control; preferirajte dodjelu prava Read – omogućuje samo čitanje i skidanje dokumenata. Već pravo Change može se zlorabiti. To pravo omogućuje zapisivanje u mapu ili dokument te brisanje dokumenata. Dakle, zlonamjerna osoba može izbrisati dokumente, štoviše, može zapuniti spremišni prostor vašeg računala što, posljedično, dovodi do nestabilnosti sustava kao funkcionalne cjeline.

Niža slika govori nam sljedeće: na računalu Win8u1 smo dodijelili pravo zapisivanja u direktorij Docs lokalnom računu Ralica. Kasnije u Event Vieweru vidimo da se je s mreže, sa Ubuntu računala Ud1310, na računalo Win8u1 spojila osoba rabeći račun Ralica. Evidentirano je i točno vrijeme te akcije, te IP adresa Ubuntu stanice. U slučaju potrebe, dovoljno podataka za istraživanje i utvrđivanje činjeničnog stanja.

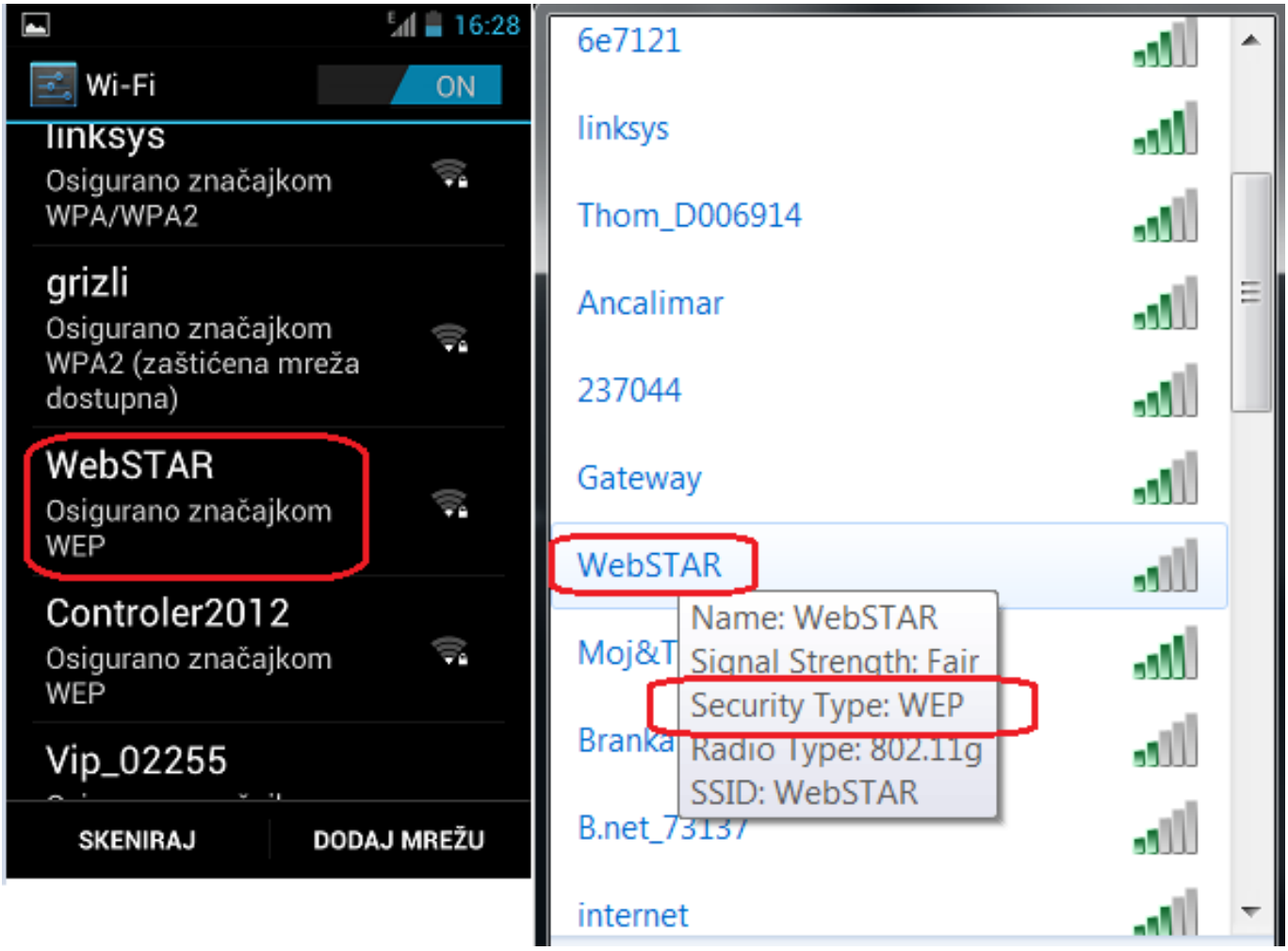


11. Tijekom spajanja svojim računalom na nepoznatu Wi-Fi (bežičnu) mrežu, uvjerite se da je zaštićena WPA2 protokolom. Ne pristupajte nepoznatoj a otvorenoj Wi-Fi mreži jer je vrlo vjerojatno

mamac. Na takvim ste mrežama, kao i na onima koje rabe samo WEP protokol, neizbježno izloženi napadu eavesdropping (prisluškivanje, uhođenje). Posljedično, ako baš morate raditi na nepoznatoj, ili poznatoj ali slabo zaštićenoj Wi-Fi mreži, prakticirajte sljedeće:

- primijeniti najrestriktivniju politiku na lokalnom vatrozidu Wi-Fi kartice;
- spajati se samo na servise koji se umiju predstaviti ispravnim certifikatom;
- rabiti VPN konekcije jer omogućuju tzv. tuneliranje kroz nesigurne mreže (obuhvaća enkripciju prometa i obostranu identifikaciju u komunikaciju involviranih strana).

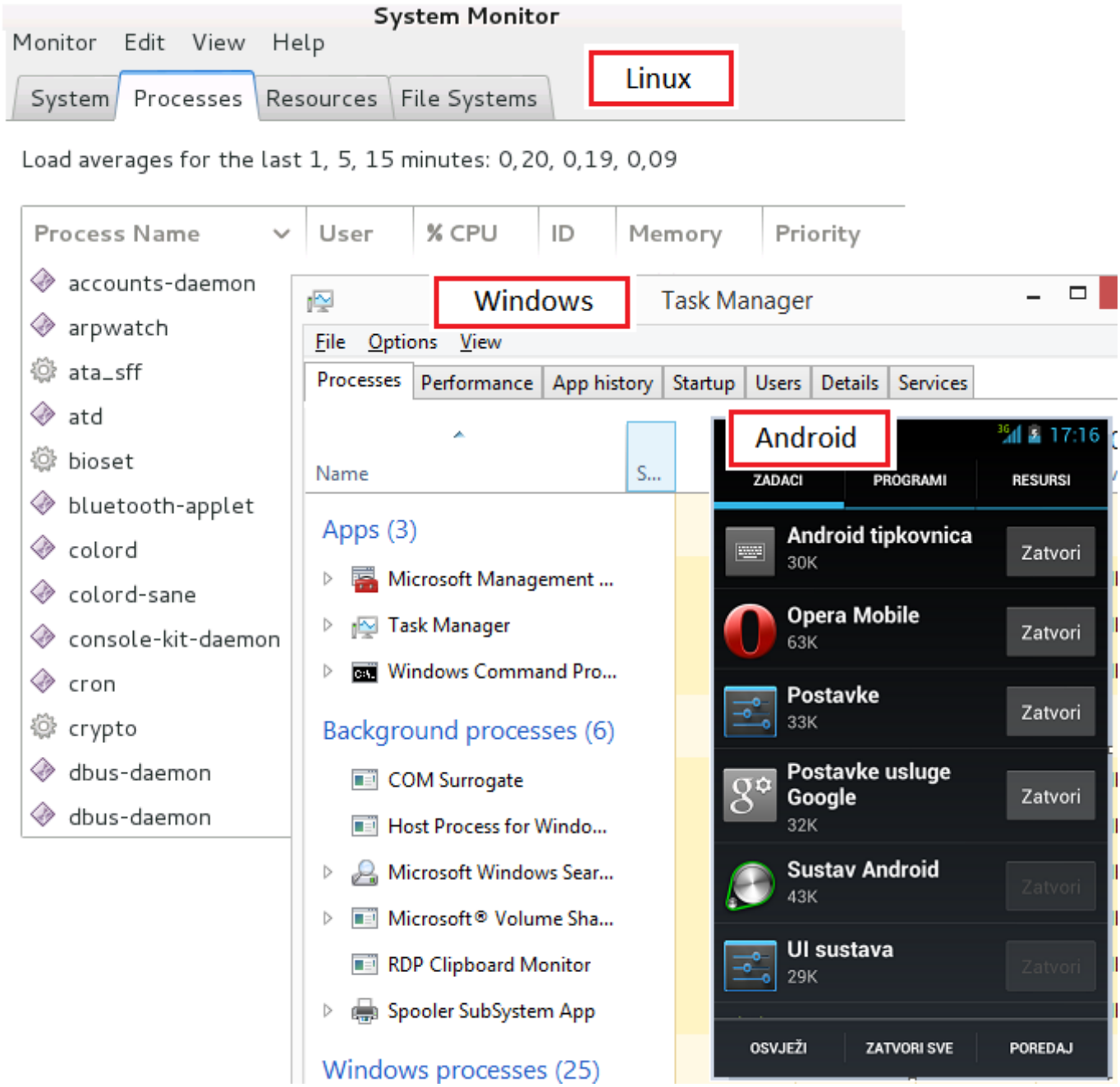
Na nižoj slici su uređaji smartphone (OS je Android) i PC prijenosnik (OS je Windows) detektirali iste Wi-Fi mreže. Neke od njih su, poput označene WebSTAR, nesigurne jer su „osigurane“ dokazano nesigurnim WEP protokolom. Ako se spojimo na takvu mrežu, izloženi smo spomenutom napadu uhođenja.



* Kad ne rabite Wi-Fi, Bluetooth i slične bežične tehnologije, isključite ih! Treba, naime, imati na umu da postoje, i konstantno se razvijaju, softver i metode za ilegalni pristup računalu na kojem je aktivna bežična logika.

12. Periodično - posebice nakon instaliranja aplikacija ili pristupanja nepoznatim Web mjestima – provjerite da li je došlo do izmjena u konfiguraciji računala, naročito lokalnog vatrozida. Također, pratite rad svog računala. Ako niste radili nikakve promjene a uređaj je postao usporen, dolazi do povećanja uporabe ključnih hardverskih resursa (radna memorija, mrežna kartica, procesor, skladišta podataka), pojavili su se nepoznati procesi, zastajkuje ili se ruši aplikacija koja je dobro radila, u Internet pregledniku pojavila se nova ekstenzija, sistemski logovi se pune neuobičajenim porukama.... simptomi su računala zaraženog malicioznim kodom.

Većina računala raspolaže nekim predinstaliranim preglednikom i/ili upraviteljem procesa, aplikacija, zapisa o događajima i sličnim, za ovu temu zaštite, relevantnim alatima. Besplatne a vrlo kvalitetne alate te namjene možemo skinuti s Weba (vidi točku 2).



POZOR!

Educirajte se za primjenu naprednih metoda zaštite svog računala jer sve što je do sada navedeno spada u osnovne mjere i postupke zaštite. Samopomoć ponekad nije dovoljna, stoga, ne ustručavajte se obratiti svojem informatičaru.

Uprava svakog poduzeća/ustanove očekuje od zaposlenih odgovornu uporabu računala pa, ukoliko se Vaše računalo detektira kao izvorište zaraze drugih računala i/ili kanal istjecanja poslovno senzitivnih podataka, nitko neće pokazati previše razumijevanja prema Vama.

Štiteći svoje računalo, mi u stvari štitimo sebe – svoju osobnost, svoj privatni, javni i poslovni integritet!

sri, 2014-04-23 06:50 - Ratko Žižek**Kategorije:** Sigurnost [1]
Vote: 5

Vaša ocjena: Nema Average: 5 (2 votes)

Source URL: https://sysportal.carnet.hr/node/1386

Links
[1] https://sysportal.carnet.hr/taxonomy/term/30