Lažni antivirusni programi

Lažni antivirusi sve se češće pojavljuju na računalima današnjih surfera. Radi se o malicioznom kodu kojeg najčešće pokupimo posjećujujući inficirane web stranice. Korisnik će u jednom trenutku dobiti poruku da je na njegovu računalu otkriven virus. Nakon što ga tako preplaši, lažnjak će mu ponuditi da za šaku dolara kupi antivirusni program koji će ga ubuduće zaštititi. Pri tom ga nastoji navesti da posjeti web stranicu gdje treba upisati osobne podatke i broj kreditne kartice. Naravno, radi se o prijevari: računalo nije zaraženo virusom, naivnom surferu koji da podatke novac će otići s računa, a kupljeni softver u najmanju ruku ne štiti od virusa. Radi ovakvog načina varanja korisnika, koje uključuje socijalni inženjering, lažne antiviruse često nazivaju i ***scareware***. Najčešća meta su Windows računala, ali u porastu su i napadi na Macove.

Ova je vrsta zloćudnih programa popularna među kriminalcima iz jednostavnog razloga, jer donosi znatan prihod. Kriminalci se često udružuju, pa partnerske grupe šire lažni antivirus, koji je zapravo i sam virus, da bi za to dobile dio zarade. Najčešće metode širenja su lažne dogradnje Windowsa, lažne Facebook aplikacije, web sjedišta tobožnjih antivirusnih tvrtki, web stranice s ubačenim Java Scriptom koji obavlja redirekciju, e-mailovi s linkovima ili prilogom, atraktivne slike koje ljudi često traže i zaraze se klikajući na njih. Jedan od načina širenja je i pomoću virusa tipa Trojan-Downloader, koji su u stanju spustiti i instalirati dodatni malware. U naprednije tehnike spada takozvani SEO, Search Engine Optimization poisoning. Pri tome koriste Google Trends [1], kako bi otkrili koje pojmove ljudi najčešće traže. Nudi se download popularnih sadržaja, na primjer filmova, a onda se ponudi (lažni) *codec* koji omogućava da ih se pogleda. Socijalni inženjering je u osnovi većine metoda, a oslanja se na naivnost i neukost korisnika, kojima je cijeli taj tehnički svijet isuviše složen i samo žele što prije riješiti problem. Popularni su spamovi u kojima se korisnika upozorava da mu je privremeno blokiran račun, ili mu je promijenjen password, a problem će riješiti klikom na priloženi programčić.

Tipično ponašanje po kojem možemo prepoznati lažni antivirus jest aktiviranje popup prozora u kojem obavještava korisnika da je otkriven virus, ili da je korisnikovo računalo izvor s kojeg se masovno šalju spamovi. Korisnika upozorava da mora poduzeti korake i navodi ga na web lažnog proizvođača zaštitnih programa.

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

Nakon što prevareni shvate o čemu se radi, na Internetu će se ubrzo pojaviti upozorenja i softver za uklanjanje napasti. Da bi izbjegli mogućnost da korisnici, prije nego nasjednu, jednostavnim guglanjem otkriju da se radi o prijevari, kriminalci često mijenjaju nazive svog malwarea. Pri tom biraju sugestivna imena, nalik na legalne proizvode, na primjer Internet Defender, Security Guardian, XP Protection, Mac Defender itd. Još jedna tehnika prikrivanja je polimorfizam, pri čemu serveri s kojih se skida malware povremeno nanovo zapakiraju izvršni kod, da se izbjegne prepoznavanje. Uostalom, lažni antivirus će nastojati blokirati korisnikov legalni AV program, a u tome mu pomažu korisnici koji rade s administratorskim ovlastima.

Sistemac bi trebao svoje korisnike educirati, objasniti im da je na njihova računala već instaliran legalni antivirusni klijent, pa nema potrebe za dodatnom zaštitom. Educirani korisnici morali bi odmah upozoriti sistemca na pojavu lažnog antivirusa. Osim deinstalacije malwarea i ponovnog aktiviranja legalno kupljenog antivirusa, trebalo bi upozoriti i ostale korisnike da ne nasjedaju na prijevaru.

Iz osobnog iskustva znam da će se lažni antivirusi pojavljivati uvijek kod istih korisnika. Ti recidivisti ne žele otkriti na koji su se način zarazili, koje su web stranice posjećivali, na što su klikali. Možemo samo nagađati iz kojeg razloga to skrivaju. S druge strane, mnogi kolege sistemci, opterećeni svakodnevnim obavezama, zadovolje se uklanjanjem virusa pa se i ne trude istražiti porijeklo zaraze. Organizacije koje shvaćaju vrijednost svojih podataka i ulažu u zaštitu informacijskih sustava zato zapošljavaju specijaliste za informacijsku sigurnost.

Za otkrivanje i prevenciju lažnih antivirusa bilo bi dragocjeno korištenje nekog naprednog vatrozida. Takozvani IPS-ovi (*Intrusion Prevention System*) ili *Next Generation Firewalli* ne samo da blokiraju većinu virusa, nego često ne dopuštaju posjet sumnjivim web stranicama, služeći se crnim listama koje održavaju njihovi proizvođači, ali i cijela internetska zajednica zainteresirana za sigurnost. Iz logova na takvom uređaju moći ćete izvući povijest ponašanja svojih rizičnih korisnika, prijaviti zloćudne siteove ili ih sami blokirati dodajući pravila filtriranja. Neki od tih uređaja čak omogućuju da oblikujete posebna pravila za svoje rizične korisnike.

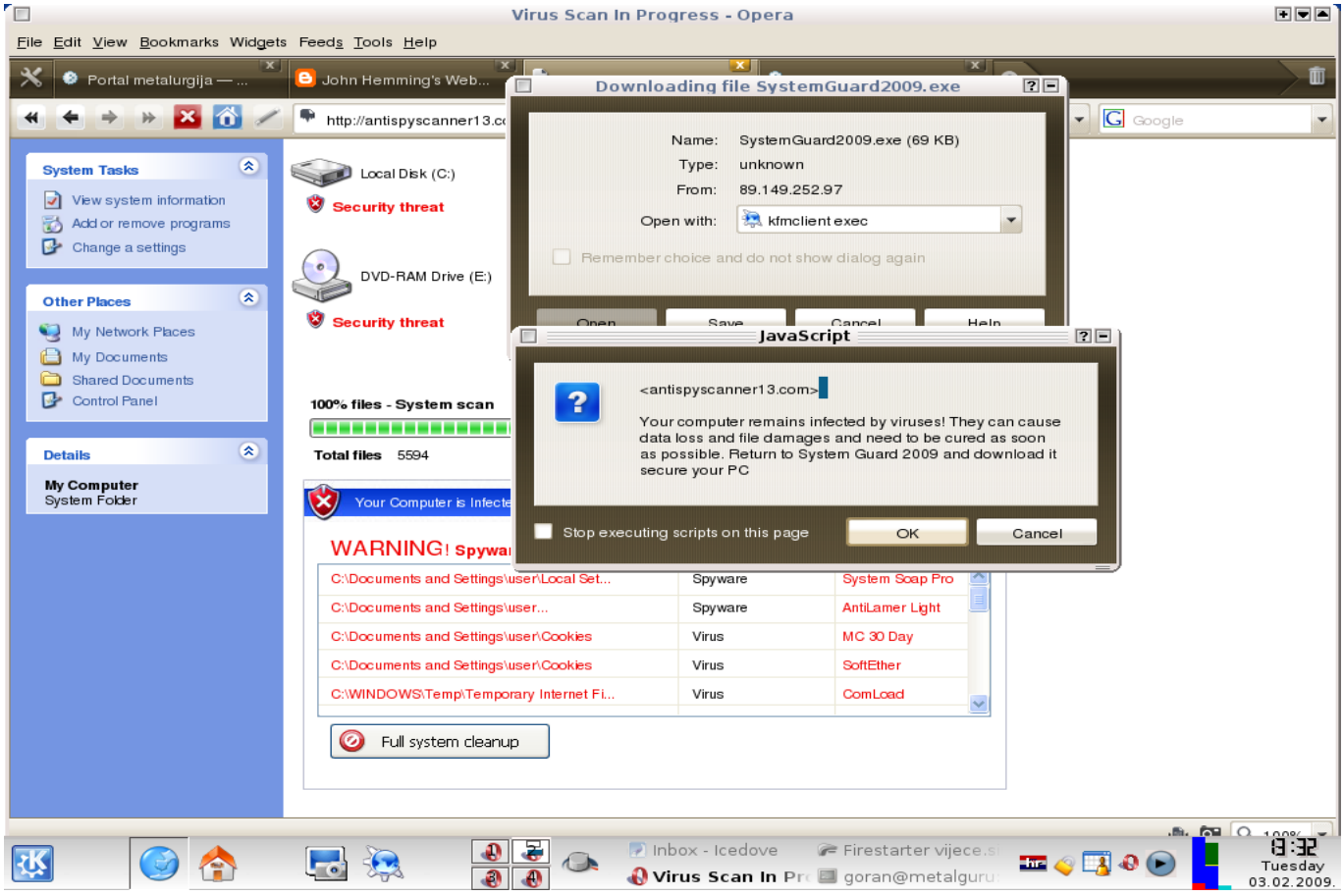
Obrana od ovako složenih napada ne može se prepustiti samo antivirusnim programima koji su instalirani na korisničkim računalima ili rade kao ulazni filtri na poslužiteljima elektroničke pošte.

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

Prije svega, uz viruse treba blokirati i spamove, jer oni ne predstavljaju samo gubljenje radnog vremena, nego su sredstvo za socijalni inženjering. Osim toga, obrana pomoću statičkih potpisa nije 100% uspješna protiv polimorfnih virusa. Zaštita treba uključivati i blokiranje sumnjivih IP adresa, ali i vatrozide koji su u stanju prepoznati sumnjivo ponašanje, te blokirati nove, nepoznate prijetnje. Obrana se postavlja i na liniju razdvajanja i na korisnička računala i na servere, a uz to se koriste još i specijalizirani uređaji, poput IPS-ova. Gotovo smo zaboravili spomenuti još jednu aktivnost, koja se na neki način podrazumijeva, a to je redovita instalacija zakrpa.

Proizvođaći antivirusnog softvera u svoje proizvode ugrađuju sve više sigurnosnih funkcija, pa je danas tipični antivirusni klijent ujedno i vatrozid. Neke implementacije blokirat će nepoznate programe i upozoriti administratora na konzoli, te zatražiti da se program stavi u crnu ili bijelu listu. Naravno, nestrpljivi korisnici će se buniti protiv svega što ih usporava u radu (ili zabavi), pa će nezaobilazan dio zaštite biti i pravilnici, sigurnosne politike, koje administratorima daju ovlasti kako bi mogli štiti svoje korisnike, kako od zločudnih programa tako i od njih samih.

Kolega Goran Šljivić poslao je slikicu iz svog iskustva, koja dobro ilustrira kako lažni antivirus straši korisnika:



čet, 2012-05-31 20:46 - Aco Dmitrović**Vijesti:** Sigurnost [2]
Kategorije: Antivirus [3]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

Source URL: https://sysportal.carnet.hr/node/1024?page=0

Links
[1] http://www.google.com/trends
[2] https://sysportal.carnet.hr/taxonomy/term/13
[3] https://sysportal.carnet.hr/taxonomy/term/31

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr