CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Lažni antivirusni alati

NCERT-PUBDOC-2011-10-332

Nacionalni CERT

Nacionalni CERT+

Sadržaj

1 Uvod

Ovaj dokument posvećen je posebnoj vrsti zlonamjernih programa (eng. malware) koji prijevarom svojim autorima pokušavaju osigurati financijsku korist. Riječ je o lažnim antivirusnim alatima (eng. FakeAV) koji svojim žrtvama lažu da su zaraženi nekim drugim oblikom zlonamjernog softvera.

Kroz dokument ćemo se upoznati s definicijom lažnih antivirusnih alata i njihovim razlikama u odnosu na druge zlonamjerne programe. Pokazati ćemo koje tehnike se koriste za njihovo širenje i kako oni uspijevaju zaraziti žrtvu. Slikovito su prikazane dvije vrste antivirusnih alata, a na kraju dokumenta pokušati ćemo predstaviti cijelu industriju i poslovni model koji autori ovakvih programa koriste kako bi prikupili financijska sredstva od žrtava.

2 Što su to lažni antivirusni alati?

Definicija lažnih antivirusnih alata (u daljnjem tekstu FakeAV) nije kompliciranа. Riječ je o izdvojenoj vrsti zlonamjernih programa (eng. malware) koji svojim žrtvama prikazuju lažne uzbune o malware prijetnjama koje stvarno ne postoje. Uzbune imitiraju izgled stvarnih antivirusnih alata i imaju za cilj preplašiti korisnika te navesti ga da putem interneta kupi drugi (ili nadogradi postojeći) softverski alat koji može riješiti problem.

U svijetu informacijske sigurnosti postoje i drugi termini usko vezani uz pojam FakeAV softvera. Tako se često može čuti kako netko govori o *Rouge Antivirus* softveru ili *Rogues* softveru. Ova dva pojma su sinonimi i nema praktične razlike između njih i FakeAV alata, no postoji još jedan termin – *Scareware* koji je šireg opsega nego FakeAV. Scareware je svaki softver koji plaši žrtvu te u najvećem broju slučajeva od nje traži novac kako bi prestao s prijetnjama. FakeAV je samo onaj softver koji imitira izgled i zadatak stvarnih antivirusnih alata, ali pri tome laže o prijetnjama i traži novac za njihovo uklanjanje.

Jedan jednostavan primjer može razjasniti razliku između scarewarea i FakeAV softvera. Postoje programi koji žrtvama prijete s brisanjem sadržaja cijelog diska ukoliko ne plate određeni iznos autoru. Takav softver spada u kategoriju scarewarea, ali ne i FakeAV alata. Još jednostavnije rečeno – FakeAV alati su jedna vrsta scarewarea

Osnovna sličnost s drugim vrstama malwarea je način širenja i infekcije žrtve. Kao što ćemo kasnije vidjeti, svaki malware, pa tako i FakeAV ima određene tehnike kojima se pokušava proširiti između velikog broja korisnika.

Ono što FakeAV čini posebnim u odnosu na druge vrste malwarea je činjenica da rijetko kada nanosi direktnu štetu računalu kojeg zarazi. FakeAV ne briše i ne krade osobne podatke i ne povezuje računala u velike botnet mreže. Više je orijetniran na varanje korisnika i ostvarivanje direktne financijske koristi. Žrtva koja odluči platiti FakeAV svoj novac direktno daje autoru odnosno distributeru tog softvera. U tome lancu nema posrednika i dodatnih davanja. To je vjerojatno jedan od razloga zašto su toliko popularni među kriminalcima. Druge vrste malwarea, kao što su bankarski trojanci, imaju složenije procese za ostvarivanje financijske koristi. Sljedeća slika prikazuje tipično upozorenja koje FakeAV prikazuje žrtvama.

Slika 2.1 - Lažno upozorenje FakeAV alata

Neupitno je kako su lažni antivirusni alati postali jedan od velikih problema informacijske sigurnosti. Sve vodeće antivirusne kompanije prepoznaju tisuće i tisuće različitih primjeraka ove vrste malwarea. Do nedavno se činilo kako trend njihova rasta neće posustati, no zanimljiv obrat dogodio se u srpnju i kolovozu 2011 godine, kada je cijela industrija vezana uz distribuciju FakeAV alata gotovo propala. Više riječi o tome biti će u poglavlju o funkcioniranju FakeAV industrije.

3 Infekcija lažnim antivirusnim alatom

Kako smo prije naveli, proces infekcije i distribucije FakeAV softvera sličan je kao i kod drugih malwarea. Postoji mnogo različitih načina na koje autori FakeAV alata uspijevaju zaraziti korisnike. Sve ih možemo podijeliti u tri osnovne skupine:

1. Socijalni inženjering
2. Drive-by download napadi
3. Instalacija putem drugih malwarea i botnetova.

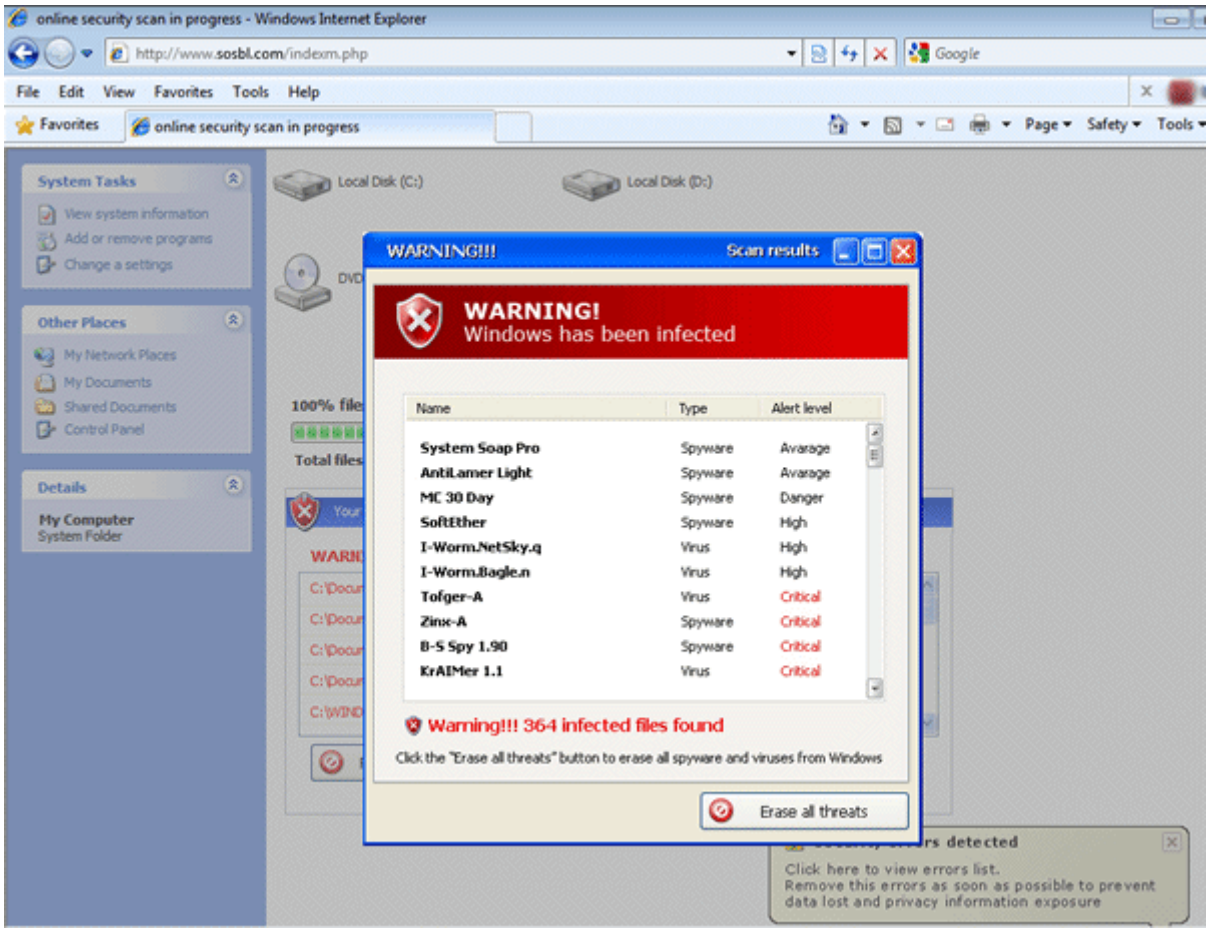
Kod socijalnog inženjeringa i drive-by download napada autor FakeAV alata postavlja vlastitu web stranicu putem koje će ga distribuirati. U oba slučaja cilj mu je privući što više posjetitelja na tu stranicu kako bi povećao broj zaraženih računala. Promotrimo detaljnije svaku vrstu infekcije.

3.1 Socijalni inženjering

Socijalni inženjering vještina je manipuliranja ljudima čiji je cilj natjerati ih da otkriju povjerljive informacije ili naprave neku radnju koja će ugroziti sigurnost računalnih sustava. Kada je u pitanju FakeAV, njegovi autori će pokušati nagovoriti „naivnog“ korisnika da sam pokrene njihov program i time se zarazi.

Provođenje socijalnog inženjeringa ne zahtjeva velike tehničke vještine i znanja. Zato je pomalo iznenađujuća činjenica da je to najuspješniji oblik napada na korisnike. No, ukoliko uzmemo u obzir sve tehnike koje napadači koriste i činjenicu da ciljaju na neiskusne i neobrazovane korisnike računala, visoki postotak zaraženosti putem socijalnog inženjeringa je realnost.

Kako bi korisnike nagovorio da instaliraju FakeAV alat njegov autor će postaviti web stranicu koja svim posjetiteljima, unutar web preglednika, pokazuje upozorenje da je njihovo računalo zaraženo virusom i hitno treba popravak. Prozore s takvim upozorenjima autor može napraviti putem JavaScripta ili Flasha. Izgled takve web stranice prikazan je na sljedećoj slici.



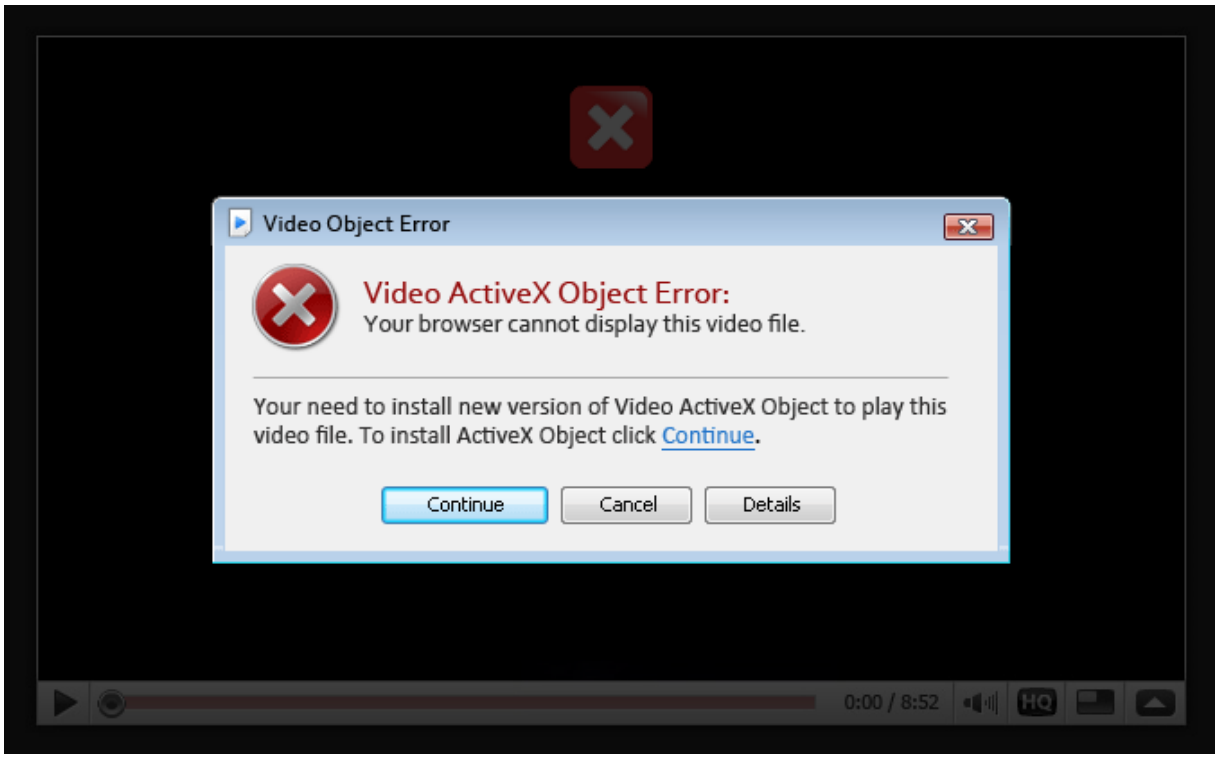
Slika 3.1 - Lažno upozorenje o zarazi

Izvor [1]

Iako se to na prvi pogled ne može zaključiti, slika doista prikazuje web stranicu. Na vrhu slike nalazi se adresna traka i obrub Internet Explorer prozora što odaje da je riječ o web stranici na internetu.

Ovakve stranice su namjerno napravljene da imitiraju izgled operacijskog sustava kako bi zbunile neiskusne korisnike. U slučaju na slici, web stranica tvrdi da je otkriveno 364 različitih prijetnji na računalu. Uz plašenje korisnika, takve stranice obvezno nude i gumb na koji korisnik može kliknuti kako bi prijetnje otklonio. Iza njega se krije sam FakeAV alat koji će zaraziti računalo ukoliko ga korisnik instalira.

Osim ovakvih vrsta stranica česte su i stranice koje su dizajnirane za pregled lažnih video snimki. Korisnik koji posjeti takvu stranicu može pogledati video pod uvjetom da instalira potrebni video kodek. Naravno, nije riječ o pravom video kodeku, već o FakeAV alatu koji će zaraziti računalo korisnika. Primjer takve web stranice dan je na sljedećoj slici.



Slika 3.2 - Upozorenje o lažnom video kodeku

Izvor: [2]

Važno je napomenuti da ove dvije vrste web stranica nisu jedine koje autori FakeAV alata koriste. Kod socijalnog inženjeringa samo je napadačeva mašta ograničenje, zato postoje drugi trikovi i obmane koje mogu prevariti manje iskusne korisnike. Zbog opsega dokumenta ovdje su navedene dvije najčešće.

3.2 Drive-by download napadi

Termin *drive-by download* napad odnosi se na potpuno drukčiji način širenja FakeAV (i malwarea) alata nego što je socijalni inženjering. U *drive-by download* napadima autor FakeAV alata također postavlja stranicu putem koje korisnik može preuzeti alat, ali ovaj puta stranica neće različitim trikovima nagovarati korisnika da instalira alat već će to obaviti sama, bez odobrenja korisnika.

Kako je to moguće? Odgovor leži u tome da stranica iskorištava ranjivost u web pregledniku žrtve. Uspješnim iskorištavanjem ranjivosti napadač može izvršiti proizvoljni programski kod na računalu korisnika bez njegova znanja. Ovo je vrlo opasan način širenja FakeAV alata budući da može pogoditi bilo kojeg korisnika bez obzira na njegovo iskustvo i znanje.

Sada se postavlja pitanje - ukoliko je riječ o tako opasnom načinu širenja, zašto veću uspješnost ima pristup socijalnim inženjeringom? Problem je u samim ranjivostima. Pronalazak jedne iskoristive ranjivosti zahtjeva veliko tehničko znanje i vještinu, a svaka nova verzija preglednika može ukloniti novootkrivene ranjivosti. Napad socijalnim inženjeringom puno je stabilniji i jednostavnije ga je provesti.

Osim stranica koje iskorištavaju ranjivosti u preglednicima korisnika, autori FakeAV alata su počeli koristiti i tuđe web stranice za distribuciju svojeg softvera. U tome slučaju, putem ranjivosti u nekoj legitimnoj stranici na nju postavljaju FakeAV softver i korisnik ga može

preuzeti od tamo. Time autor FakeAV alata ne mora imati vlastitu stranicu i ima veći stupanj prikrivenosti.

3.3 Kako privući posjetitelje na zlonamjerne stranice

Kako smo već napomenuli, kada autor FakeAV alata postavi zlonamjernu stranicu, on mora osigurati određen broj posjetitelja kako bi zarazio dovoljno korisnika. Kako autor navodi posjetitelje na svoju stranicu? Istaknimo nekoliko načina:

- Spam email i IM poruke – U suradnji s spammerima autori FakeAV alata mogu dogovoriti slanje velikog broja spam poruka koje će sadržavati poveznicu na njihovu stranicu. Osim emailova šalju se poruke putem servisa za trenutačnu razmjenu poruka (eng. instant messaging, IM).
- Poruke na društvenim mrežama – Facebook, Twitter i ostale društvene mreže odavno su postale zanimljive kriminalcima. Autori FakeAV alata ostavljaju poruke s poveznicama na svoje zlonamjerne stranice. Pri tome opet mogu surađivati s različitim spammerima i vlasnicima botova koji će te poruke proširiti.
- Blackhat SEO – Autori FakeAV alata iskorištavaju trenutno popularne termine koji se pretražuju na internetu. Cilj im je osigurati da njihova stranica bude među prvih 10 rezultata koje vrati neka tražilica na internetu za traženi pojam. To mogu postići pravilnom uporabom ključnih riječi, povezivanjem s ostalim stranicama ili brojnim drugim tehnikama.

3.4 Instalacija putem drugih malwarea i botnetova

Autorima FakeAV alata na raspolaganju stoji još jedna mogućnost širenja svojeg „proizvoda“. Ukoliko ne žele uspostaviti vlastitu stranicu, mogu surađivati s vlasnicima drugih malwarea i putem njih osigurati instalaciju svojeg FakeAV alata.

Ovo se prvenstveno odnosi na suradnju s vlasnicima različitih botnet mreža. Kako se suradnja ostvaruje? Vlasnik botnet mreže[1] pod svojom kontrolom ima tisuće različitih računala s kojima on može raditi što poželi, a to uključuje i instalaciju različitih vrsta softvera. Budući da autor FakeAV alata ne želi uspostaviti vlastitu web stranicu preko koje će se alat širiti on može sklopiti partnerstvo s vlasnikom botneta.

U takvom partnerstvu, vlasnik botneta će na računala pod njegovom kontrolom instalirati FakeAV alat, a autor FakeAV alata će vlasniku botneta isplatiti proviziju od prodaje. Time vlasnik botneta dobiva priliku da poveća zaradu s svojim botnetom, a vlasnik FakeAV alata dobiva sigurni kanal distribucije svojeg softvera.

Ovakva partnerstva dovela su do razvitka složene ekonomije internetskog podzemlja i stvaranja veza između različitih vrsta kriminalaca i različitih vrsta malwarea. Više riječi o toj ekonomiji biti će u zadnjem poglavlju ovog dokumenta, za sada je važno razumjeti da FakeAV alat može na računalo žrtve doći i putem nekog drugog malwarea koji je to računalo zarazio prije njega.

[1] Opis botnet mreža je izvan opsega ovog dokumenta. Za više informacija moguće je pročitati drugi dokument Nacionalnog CERT-a posvećen SpyEye botnetu. Dokument se zove *SpyEye – nasljednik Zeusa* i dostupan je na stranicama Nacionalnog CERT-a.

4 Ponašanje FakeAV alata

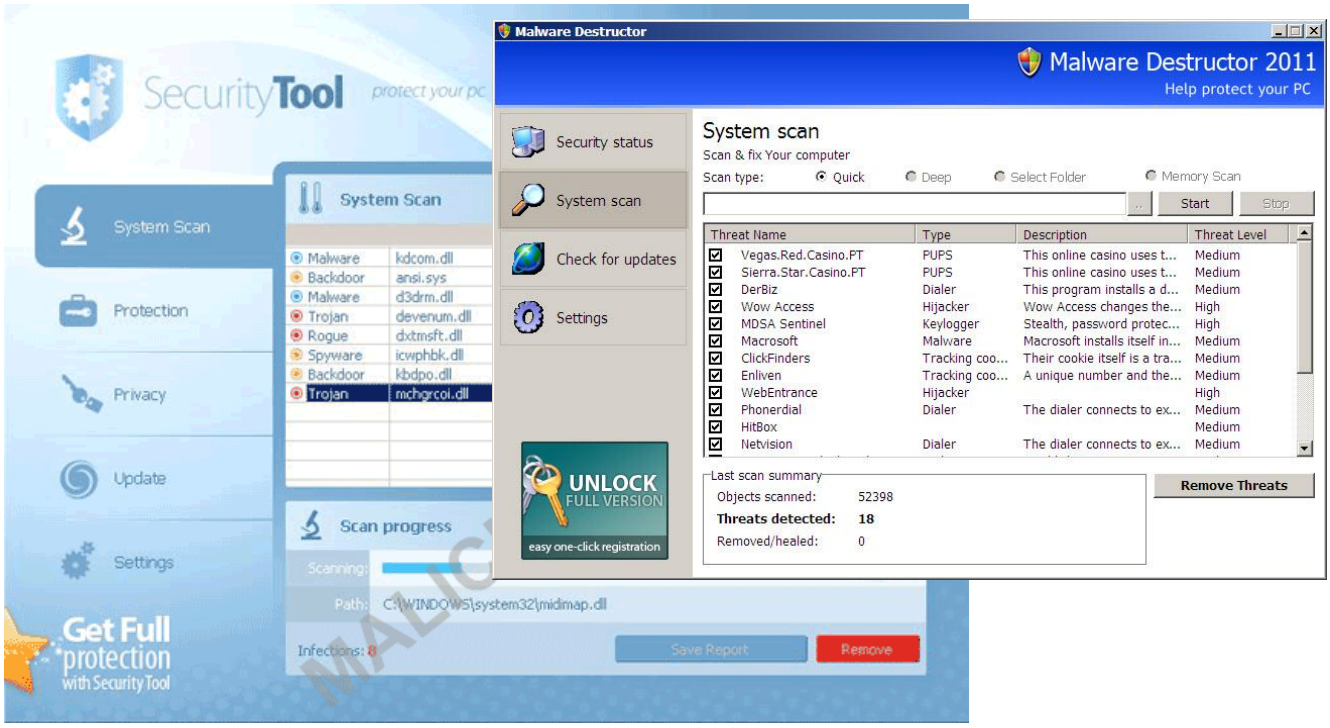
U ovom poglavlju ćemo se nakratko osvrnuti na ponašanje pojedinog FakeAV alata na zaraženom računalu. FakeAV je relativno jednostavan softver u usporedbi s nekim drugim, složenijim, vrstama malware-a. Najsloženiji dio FakeAV alata je njegovo sučelje koje izgleda profesionalno i lijepo dizajnirano. To je još jedan od trikova kojima se autori koriste kako bi žrtve uvjerile u vjerodostojnost svog programa.

Odmah nakon što FakeAV alata zarazi računalo on radi dvije osnovne radnje koje osiguravaju njegovo pokretanje s svakim paljenjem računala:

1. Alat se kopira u direktorij korisnikovog profila ili privremeni direktorij.
2. U registry bazu operacijskog sustava upiše putanju do svoje izvršne datoteke što mu osigurava pokretanje zajedno s pokretanjem računala.

FakeAV alat ne mora se skrivati od korisnika pa je njegov proces infekcije jednostavan. Za uklanjanje ovog alata dovoljno je obrisati njegovu izvršnu datoteku iz privremenog direktorija te ukloniti ključ iz registry baze.

U slijedećem koraku infekcije FakeAV obično putem interneta preuzima drugu komponentu koja obavlja lažno skeniranje računala. Sljedeća slika prikazuje dva različita lažna antivirusna alata u trenutku skeniranja.



Slika 4.1 - FakeAV alati "skeniraju" računalo

Već je na prvi pogled jasno kako FakeAV alati imaju profesionalno sučelje koje često imitira poznate, legitimne, antivirusne alate. Važno je uočiti da i jedan i drugi alat na slici imaju gumb kojim se korisniku omogućuje da nadogradi softver ili kupi punu verziju. **To je ujedno i cilj FakeAV-a.** Kada lažno skeniranje završi, korisnik će dobiti poruku da mora kupiti punu verziju softvera kako bi mu se uklonile sve otkrivene prijetnje s računala. Sve dok korisnik ne kupi licencu, FakeAV alat neće prestati prikazivati upozorenja.

4.1 Ostali simptomi zaraženosti

Osim lažnog skeniranja računala i izbacivanja poruka korisniku da mora kupiti licencu kako bi se zaštitio, računalo zaraženo FakeAV alatom će pokazivati još neke simptome.

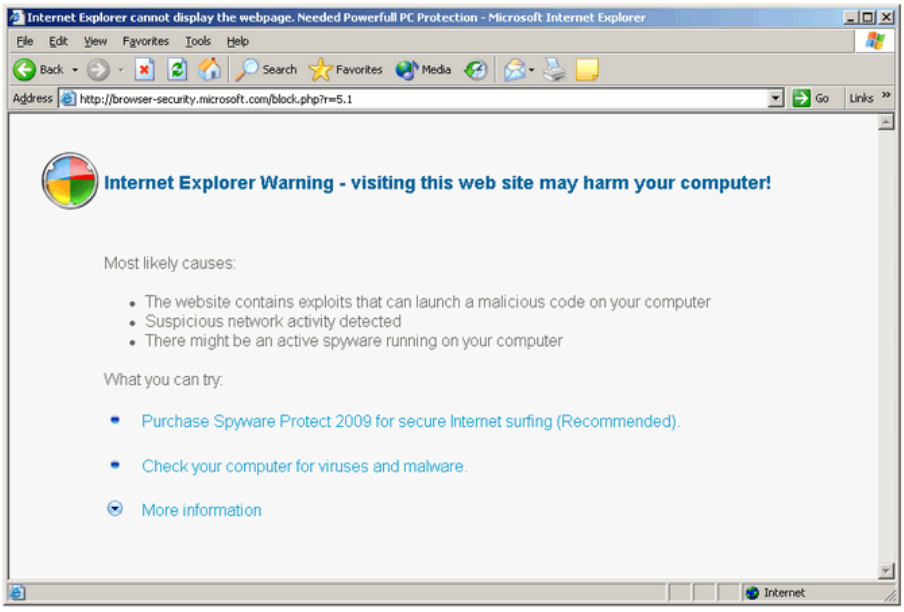
Zabrana pokretanja drugih programa

FakeAV će nakon što zarazi računalo zabraniti pokretanje gotovo bilo kojeg programa. Poruka koja se pritom prikazuje korisniku obavještava ga da je program zaražen i da mu je zabranjeno pokretanje. Na poruci je istaknuto da je potrebno kupiti licencu za antivirus kako bi se prijetnja uklonila. Primjer poruke dan je na sljedećoj slici:

Na slici se vidi poruka koju FakeAV prikazuje nakon što zabrani pokretanje *notepad.exe* programa. Ovakve zabrane imaju zadatak uplašiti i iznervirati korisnika te natjerati ga da kupi licencu. Nisu svi programi na računalu na listi zabranjenih. Obično FakeAV dopušta pokretanje Internet Explorer-a ili Windows Explorer-a budući da korinsik mora putem web preglednika kupiti licencu.

Preusmjeravanje web stranica

Iako dopuštaju pokretanje Internet Explorera, FakeAV alati će korisnicima zabranjivati posjete određenim web stranicama. Kao što je i s zabranjivanjem programa, ovo bi trebalo korisnike dodatno zastrašiti i nagovoriti ih da kupe licencu. Sljedeća slika prokazuje jedan primjer preusmjeravanja unutar Internet Explorera-a.



Slika 4.2 - Preusmjeravanje stranice u Internet Exploreru

Izvor: [3]

Instalacija drugih vrsta malwarea

Kao što druge vrsta malwarea mogu instalirati FakeAV tako i FakeAV može poslužiti kao platforma za instalaciju drugih vrsta malwarea. Radi se o sklapanju partnerstva unutar internetskog podzemlja. Onaj FakeAV koji je proširen na veliki broj računala će moći više zaraditi na distribuciji drugih vrsta malwarea.

4.2 Primjerci FakeAV alata

Teško je izdvojiti neke primjerke FakeAV alata budući da ih ima tako mnogo. Još je veći problem što nastaje mnogo različitih vrsta gotovo svakodnevno. Autori FakeAV alata koriste čitav niz uvjerljivih imena kako bi osigurali kredibilitet svojem softveru. Izdvojimo neke od njih:

- AntiSpyWare Pro
- Antivirus Plus
- Antivirus XP
- Internet Security 2010/2011
- Security Tool
- Security Central
- Digital Protector
- XP Defender
- CleanUp AntiVirus

Navesti ćemo dva zanimljiva primjera FakeAV alata.

4.2.1 Antivirus 2009

Antivirus 2009 koji je još poznat i po imenima Antivirus 10 ili Antivirus 360 jedan je od poznatijih FakeAV alata. Njegov izgled prikazan je na sljedećoj slici:

Slika 4.3 - Antivirus 2009 prilikom skeniranja

Zanimljiva priča vezana uz njega odnosi se na alate za njegovo uklanjanje. Kako je Antivirus 2009 postao dosta popularan i zarazio veliki broj računala pojavile su se stranice s kojih su korisnici mogli preuzeti alate za njegovo uklanjanje. No, s vremenom su i kriminalci primijetili njegovu popularnost pa su počeli nuditi lažne alate za uklanjanje Antivirus 2009 FakeAV-a. To dovoljno svjedoči o upornosti i snalažljivosti kriminalaca kada je u pitanju zarada.

4.2.2 Personal Antivirus

Personal Antivirus spada u kategoriju FakeAV alata koji imitiraju izgled nekog od legalnih antivirusnih proizvoda. Cilj ove taktike je da se korisnika uvjeri kako je program profesionalan i ima kredibilitet. Prikazana je slika Personal Antivirus alata:

Slika 4.4 - Personal Antivirus imitara izgled AVG-a

Sučelje je gotovo u potpunosti kopirano od poznatog, legitimnog, antivirusnog alata – AVG-a. Njegovo sučelje prikazano je na sljedećoj slici.

Slika 4.5 Sučelje AVG-a, legitimnog antivirusnog alata

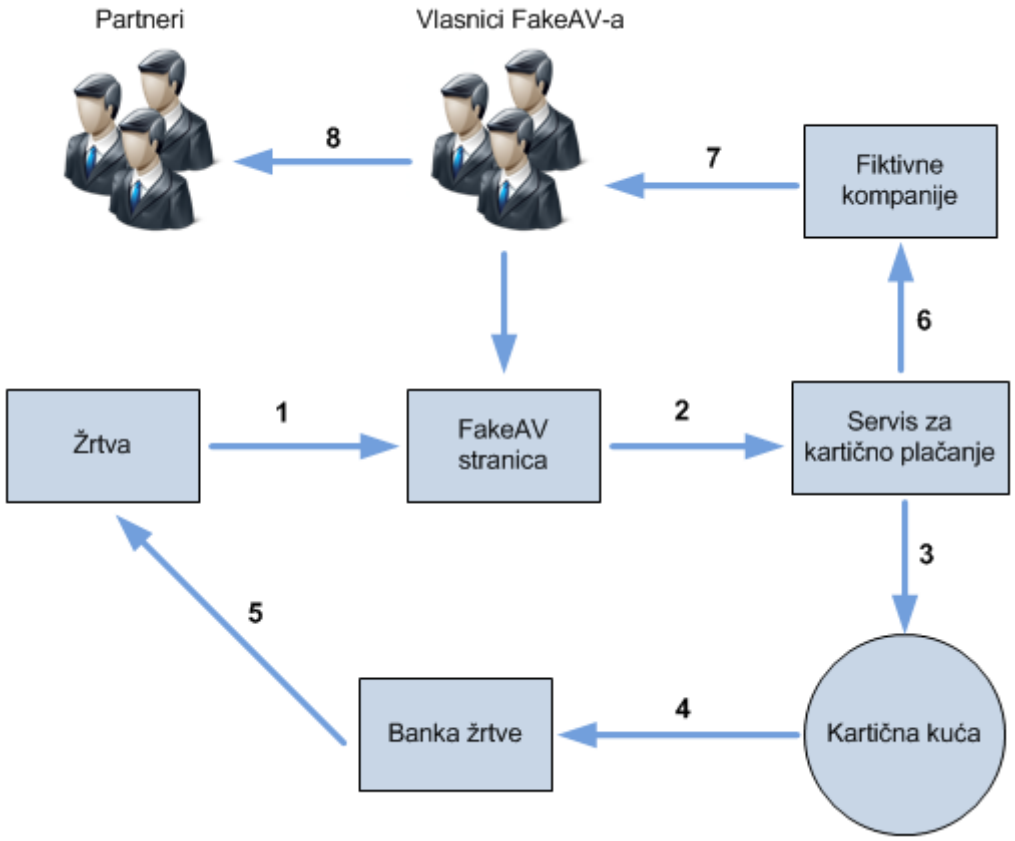
Neki lažni antivirusni alati idu još dalje nego *Personal Antivirus*. Oni izrađuju potpuno jednako sučelje kao i neki legitimni antivirus, ali uz to preuzimaju i njegov logotip. Neiskusnim korisnicima je teško prepoznati da se radi o lažnom antivirusnom alatu.

5 FakeAV industrija i ekonomija

Kao što smo već naglasili, iza prodaje lažnih antivirusnih alata stoji složena ekonomija internetskog podzemlja. U ovom djelu dokumenta pokušati ćemo ukratko prikazati način na koji funkcionira FakeAV industrija i kako ona uspije prodati svoje proizvode. Za početak je potrebno istaknuti tko je sve uključen u proces i koja je njegova uloga:

- Žrtva – osoba čije računalo je zaraženo FakeAV alatom, ona kupuje licencu
- FakeAV trgovac – Organizacija koja prodaje FakeAV proizvode
- Posrednik u plaćanju – Organizacija koja djeluje kao posrednik između trgovca i kartične kuće
- Kartična kuća – Svjetski poznate kartične kuče kao što su Visa, MasterCard itd.
- Banka žrtve – Banka koja je izdala žrtvinu karticu
- Fiktivne kompanije – Fiktivne kompanije koje FakeAV trgovci osnivaju kako bi putem njih mogli sebi isplatiti dobit
- Partneri – Skupine i osobe koje surađuju s FakeAV trgovcima i pomažu im u širenju alata. Često su to vlasnici botneta

Po broju uključenih strana može se zaključiti kako je riječ o složenom sustavu, koji sliči bilo kojoj drugoj ekonomiji. Jasno je da iza FakeAV alata ne stoji samo jedan čovjek ili haker, kako se često u medijima prikazuje, već cijela organizacija. Sljedeća slika prikazuje odnos između svih uključenih strana. Pojasniti ćemo što predstavlja svaki dio slike.



Slika 5.1 - Procesi unutar FakeAV ekonomije

Izvor: [4]

Na slici možemo izdvojiti dva osnovna procesa koji se događaju u ovom sustavu. Jedan proces počinje kada žrtva kupi FakeAV alat, a završava kada novac s njezine kartice biva preseljen na račun FakeAV trgovca. Drugi proces počinje kada FakeAV trgovac želi sebi isplatiti dobit i platiti svoje suradnike.

5.1 Kupovina lažne licence

U koracima jedan do pet detaljno je opisan proces kupnje lažnog antivirusnog alata. Sve počinje kada žrtva dolazi na stranicu gdje unosi broj svoje kreditne kartice kako bi kupila licencu. Ovdje važnu ulogu imaju cijene koje prikazuju trgovci FakeAV alatom. Postoje različite opcije. Kupnja licence za pola godine, jednu ili dvije godine. Također, mogući su i popusti.

Kada FakeAV trgovac zaprimi broj kreditne kartice od žrtve, on to prosljeđuje svojem servisu za obradu kartičnog plaćanja (eng. payement processor). I dok je trgovanje FakeAV alatima u potpunosti ilegalan posao, obrada kartičnog plaćanja nije. To su legitimni servisi koje može koristiti bilo koja organizacija koja prihvaća plaćanje putem kreditnih kartica. Nažalost, mnoge kuće znaju da surađuju s trgovcima FakeAV alata i to aktivno podržavaju i pomažu im budući da s njima mogu ostvariti veliki profit.

One FakeAV trgovcima otvaraju posebne račune visokog rizika na koje je provizija iznimno visoka (15% po transakciji). Zabilježeni su i slučajevi gdje servisi za obradu kartičnog plaćanja savjetuju FakeAV trgovce kako ostvariti bolju prodaju. Osim toga, oni im otvaraju više poslovnih računa preko kojih mogu obavljati transakcije te periodički mijenjati poslovanje po računima.

Poznati primjer jednog servisa za obradu kartičnog plaćanja je Chronopay. Riječ je o servisu koji najviše posluje u Rusiji i aktivno podržava FakeAV trgovce. No, s druge strane Chronopay ima i velike legitimne klijente kao što su Electronic Arts, Kaspersky, UNICEF, razne avionske kompanije itd. Budući da je broj legitimnih transakcija uvelike prelazio broj ilegalnih Chronopay je mogao izbjeći sumnju u svoje poslovanje. Ovo se promijenilo tek prije nekoliko mjeseci kada je Ruska policija uhitila glavnog direktora Chronopay-a. Više riječ o tome slučaju u nastavku dokumenta.

Vratimo se nazad na sliku. Servisi za obradu kartičnog poslovanja su izuzetno bitni za FakeAV trgovce i bez njihove suradnje cijeli sustav ne bi funkcionirao. Kada servis za obradu kartičnog poslovanja zaprimi broj kreditne kartice koji je klijent upisao na stranici trgovca on ga prosljeđuje nadležnoj kartičnoj kući, koja potom od banke koja je karticu izdala traži da provjeri transakciju i potvrdi prijenos sredstava. Kada banka to napravi kreditna kuća tereti karticu i time je proces kupnje licence za FakeAV softver za žrtvu završen.

Već smo napomenuli kako servisi za obradu kartičnog plaćanja izbjegavaju sumnju u svoje poslovanje. Važno je još dodati da kartična kuća zaprima određen broj prijava prema kupljenim FakeAV proizvodima. Kako bi, usprkos tim prijavama, trgovac mogao nastaviti neodmatano poslovati on će nekim klijentima vratiti novac zbog kupljenog lažnog softvera. Ovo se može činiti kao paradoks, ali za FakeAV trgovca ovo je nužno budući da time osigurava daljnju suradnju s kartičnom kućom. Svaka kartična kuća bi prekinula suradnju s njime ukoliko bi se broj prigovora nastavio povećavati, a da trgovac ni u jednom slučaju ne vrati sredstva žrtvama.

5.2 Lažne kompanije i podizanje sredstva

Servis za obradu kartičnog poslovanja će periodički, svaki mjesec ili svaki tjedan FakeAV trgovcu isplaćivati utržak od prodaje (nakon uzimanja vlastite provizije) – prikazano u koraku šest na slici. Ova isplata nikada ne ide direktno na račun FakeAV trgovca. Kako bi izbjegao sumnju i dodatno prikrio trag novca, FakeAV trgovac osniva fiktivne off-shore kompanije. Putem tih kompanija on može otvoriti bankovni račun na koji će mu njegov servis za obradu kartičnog plaćanja isplatiti sredstva.

Kada novac dođe na bankovni račun fiktivnih kompanija, glavni sudionici ga mogu direktno podići – prikazano u koraku sedam. Oni koji su oprezniji koriste čitav niz posrednika (eng. money mules) kako bi izvukli sredstva i pritom maksimalno zameli trag.

U zadnjem koraku (broj osam na slici) FakeAV trgovac od svoje zarade isplaćuje svoje partnere. To mogu biti oni koji su mu pomogli u širenju FakeAV alata, a mogu biti i standardni računi koje je potrebno platiti kao što je usluga hosting-a, poslužitelji, programeri itd.

5.3 Chronopay i udarac na FakeAV industriju

U nekoliko navrata kroz dokument smo spomenuli da je u zadnjih nekoliko mjeseci (srpanj, kolovoz i rujan 2011.) FakeAV industrija doživjela stagnaciju. Kako Brian Krebs, poznati novinar izvještava, gotovo sve najpopularnije FakeAV kompanije su prestale s radom. To uključuje Gizmo, Nailcash, Best AV… Razlog tomu su neke policijske istrage koje su rezultirale uhićenjem i zapljenom opreme u SAD-u, Ukrajini i drugim zemljama. Ali i uhićenje suosnivača Chronopaya – Pavela Vrublevskyog.

Pavel Vrublevsky je uhićen pod optužbom da je naredio internetske napade na konkurentsku tvrtku u borbi za unosan ugovor. Chronopay je namein želio postati servis za obradu kartičnog plaćanja za Aeroflot – najveću Rusku aviokompaniju.

No, ono što je važnije za ovaj dokument je činjenica da je Chronopay dugo podržavao FakeAV trgovce i obavljao poslove obrade kartičnog plaćanja za njih. Dokazi za to su se počeli pojavljivati 2009. godine kada je Washington Post objavio rezultate svoje šestomjesečne istrage o sumnjivom poslovanju Chornopaya. U tom izvještaju pojavljivale su se veze između Chronopaya i Innovagest2000 domene na kojoj su često bili hostani različiti FakeAV alati. Tada je Vrublevsky poricao bilo kakvu povezanost s FakeAV trgovcima, već je inzistirao na tome da spammeri i malware autori zlouporabljuju Chronopay.

Kasnije su iz Crhonopaya procurili dokumenti koji dokazuju direktnu umješanost u osnivanje Innovagest2000 tvrtke, a pokazalo se da je Chronopay osnivao i lažne tvrtke za obradu kartičnog poslovanja na Cipru. Te tvrtke su surađivale s FakeAV trgovcima. Također, ruska policija je objavila kako je nakon uhićenja kod Vrublevskyog pronašla dokaze koji upućuju na to da je Chronopay podržavao Rx-Promotion i još neke FakeAV trgovce.

6 Zaključak

FakeAV industrija ostvaruje veliku financijsku dobit na prijevarama i plašenju korisnika, vrlo je dobro organizirana i teško joj je stati na kraj. Pad koji se dogodio gašenjem Chronopaya vjerojatno je samo privrmen i uskoro se može očekivati oporavak što znači još više zaraženih računala i oštečenih žrtava.

Najbolji način borbe protiv ovakve prijetnje je edukacija i podizanje razine svijesti o postojanju problema. Važno je razumjeti što su to FakeAV alati i upoznati se s nekim legitimnim alatima te samo njih koristiti.

7 Literatura

[1]. **WPSecurity Lock.** WPSecurity Lock. *WPSecurity Lock.* [Mrežno] WPSecurity Lock. [Citirano: 12. 9 2011.] http://www.wpsecuritylock.com/images/skype-security-alert-fakeav-scanned.gif.

[2]. **ZScaler.** ZScaler blog. *Fake video codecs replacing fake AV pages* . [Mrežno] ZScaler. [Citirano: 12. 09 2011.] http://research.zscaler.com/2010/06/fake-video-codecs-replacing-fake-av.html.

[3]. **CA Global Security Advisor.** CA Global Security Advisor. *CA Global Security Advisor.* [Mrežno] [Citirano: 13. 09 2011.] http://gsa.ca.com/virusinfo/showimage.aspx?caid=77816&name=fakeavaet_error.gif.

[4]. *The Underground Economy of Fake Antivirus Software.* **Stone-Gross, Brett, i dr.** 2011.

[5]. **Sophos.** *What is FakeAV?* s.l. : Sophos, 2011.

[6]. **Krebs, Brian.** Fake Antivirus Industry Down, But Not Out. *Krebs on Security.* [Mrežno] 3. 8 2011. [Citirano: 15. 9 2011.] http://krebsonsecurity.com/2011/08/fake-antivirus-industry-down-but-not-out/.