Načini hakovanja računara i primjeri *cyber* kriminala

Da li se internet pretrage preusmjeravaju na web lokacije koje nemaju veze s onim što se želi pronaći? Da li je antivirusni softver na neobjašnjiv način onemogućen ili je brzina računara mnogo manja? Ovi i drugi simptomi mogu značiti da se desilo hakovanje. Još gore nego samo neugodan virus, napad na sistem u režiji hakera može biti mnogo štetniji i skuplji.

Mnogi korisnici smatraju da su neinteresantna meta da bi ih hakeri napali. Ranije su se *cyber*-kriminalci možda slagali sa tom procjenom, ali to se brzo mijenja. Danas, hakeri vide podatke pojedinca izrazito primamljivim. Bez potrebe da se prođu sofisticirani *firewall*-i ili zaobiđu složene sigurnosni protokoli, ideja o prodiranju u gotovo nepostojeću odbranu ličnog računara postala je vrlo atraktivna.

Jednom kada hakeri dobiju pristup sistemu, mogu se dogoditi brojni neugodni scenariji. Pomoću sofisticiranih i dobro isplaniranih metoda, znali su da ucjenjuju podacima, bave se krađom identiteta i čak koriste ‘preuzete’ računare za pokretanje napada na druge mreže. Najbolji način borbe protiv *cyber*-kriminalaca je razumijevanje kako izvode napade.

Kako hakeri dobijaju pristup podacima

Vjerovatno su svi čuli za prevare putem lažnih mejlova, poruka i drugih oblika društvenog inženjeringa koje hakeri koriste. Osnovno poznavanje sigurnosti računara i malo zdravog razuma u svakodnevnim mrežnim aktivnostima, generalno su dovoljni da se izbjegnu posledice. Međutim, ove obmane nisu jedini trikovi modernih hakera.

Evo nekoliko drugih visokotehnoloških načina kojima može biti izložen računar:

1. Trojanci

Trojanac je maliciozni softver prerušen u naizgled bezopastan softver, nazvan po drvenom konju kojeg su stari Grci koristili za ulazak u grad Troju. Namjera hakera je da se ubijedi korisnik da ga instalira tako što vjeruje da je to sigurno. Jednom instaliran na računaru, trojanac može učiniti

bilo šta, od bilježenja pritisnutih tipki, do otvaranja pozadine i davanja hakerima pristupu datom sistemu.

Postoji nekoliko načina na koji Trojanac može zaraziti lični računar. Najčešće hakeri koriste neki metod da prevare korisnika da klikne na određenu datoteku ili *attachment* e-pošte. Često se ti *attachment*-i mogu poslati od nekog prijatelja čiji je računar već inficiran, zbog čega se obično ne sumnja u u sadržaj mejla. Takođe, haker će možda pokušati da uplaši korsinika kako bi otvorio prilog mejla, tako što izgleda da je to službeno obavještenje policije, univerziteta, banke i sl.

E-pošta je možda popularno sredstvo za ubacanje Trojanaca u računar, ali nije jedino. Klikom na maliciozni link na Facebook-u ili drugim web lokacijama društvenih medija može se omogućiti hakeru da ubaci Trojanca u dati računar. Iako ovi web sajtovi sigurnost shvataju ozbiljno, bilo je slučajeva da su Trojanci na ovaj način zarazili korisnike.

2. *Drive-By Downloads*

U *drive-by download* napadu ne mora se kliknuti na nešto da bi se pokrenulo preuzimanje i instalacija malicioznog softvera – već samo posjećivanje kompromitovane web stranice dovoljno je da se računa zarazi. Prilično star, ali dobar primjer toga bio je zaraženi sajt poznat kao LyricsDomain.com. Prema Spyware Warrioru, 2004. godine korisnici interneta koji su posjetili LyricsDomain.com imali su na njihovim sistemima instaliran neželjeni softver - kolekciju osam reklamnih programa koji su, osim što uzrokuju druge probleme, 'preoteli' njihovu početnu web stranicu i *search bar* pretraživača te postavili reklame u folderu „Favorites" korisnika.

Drive-by download koristi nedostatke sigurnosti u web pretraživaču, operativnom sistemu ili drugom softveru koji nije ažuriran ili zakrpljen. Nažalost, preuzimanje i instaliranje zlonamjernog softvera žrtvi je obično nevidljivo. Takođe, ne postoji način da se zaključi da li je neka web lokacija zaražena samo gledanjem.

Ako postoji sumnja da neka web lokacija predstavlja moguću prijetnju računaru, treba provjeriti crnu listu malicioznih web stranica. BlackListAlert.org pruža besplatnu uslugu koja može upozoriti korisnike koji su sajtovi postavljeni na crnu listu.

Nevidljivost i efikasnost *drive-by download* čine ga jednom od najboljih metoda u hakerskom arsenalu danas. Kao rezultat, ovaj oblik napada je u porastu i nastaviće se pogoršavati samo ako korisnici računara ne preduzmu odgovarajuće mjere opreza. Ažuriranje softvera i korišćenje najnovije verzije omiljenog web pretraživača je dobar početak, jer će zatvoriti sve novootkrivene sigurnosne rupe koje ove zaražene web lokacije mogu iskoristiti.

3. *Rootkits*

Rootkit nije baš zlonamjerni softver poput virusa ili trojanca. To je nešto još gore: zlonamjerni segment koda umetnut u kompjuterski sistem, osmišljen da sakrije bilo kakvu neovlašćenu aktivnost. Budući da rootkits napadaču daju administrativnu kontrolu, računar se može koristiti bez ograničenja i bez znanja vlasnika.

Rootkit može napasti i zamijeniti važne datoteke operativnog sistema, dopuštajući mu da sakrije ili prikriva sebe i druge zlonamjerne programe. Nakon što se rootkit infiltrira duboko u sistem, može prikriti tragove uljeza (mijenjanjem sistemskih zapisa), prikriti dokaze zlonamjernih procesa koji se izvode u pozadini, sakriti datoteke svih vrsta i otvoriti port za stvaranje *backdoor*-a.

Neki rootkiti osmišljeni su da inficiraju BIOS (*basic input/output system*) računara (osnovni sistem ulaza/izlaza), što je vrsta firmvera koji inicijalizira hardver kada je računar uključen. Kada rootkiti napadnu ovaj dio sistema, čini da čak i ponovna instalacija operativnog sistema ili zamjena diska bude nedjelotvorna strategija za neutralizaciju infekcije rootkita.

Mnoge od najgorih, najrazornijih vrsta zlonamjernog softvera koriste rootkit tehnologiju. Budući da rootkiti mogu zaraziti različita područja i različite datoteke, čak je i iskusnim korisnicima teško izaći na kraj sa njima. Nažalost, korisnik neće znati da li ima ovu vrstu zlonamjernog softvera, jer je dizajniran tako da se skriva vrlo efikasno. Zato je izbjegavanje sumnjivih web stranica, ažuriranje antivirusnog softvera, izbjegavanje sumnjivih priloga e-pošte i generalno zaštita sistema dobar način da se izbjegnu ove vrste genijalno zlonamjerne infekcije.

Šta hakeri rade nakon što dobiju pristup računaru?

Navedene tehnike i tehnologije neki su od najefikasnijih alata koji moderni hakeri imaju na raspolaganju. Međutim, današnji korisnik računara koji je svjestan sigurnosti mogao bi imati koristi od napomena na jedan dodatni podatak: hakerska logika.

Čak i neobrazovani, polutehnički haker ne pokušava biti samo smetnja. Velika većina su kriminalci s jednim ciljem: stvaranje profita. Evo nekoliko stvari koje haker može učiniti kada dobije pristup računalu.

Transformisanje računara u zombije

Zombi ili "bot" je računar pod kontrolom hakera, bez znanja korisnika računara. Zlonamjerni softver koji se zarazi naziva se bot programom, a razne kombinacije i tehnike mogu se koristiti za njegovo postavljanje na ciljni sistem. Dosta često se isporučuje kao trojanski, aktivira se klikom na zlonamjerni prilog e-pošte ili link, a od korisnika ostaje skriven jer ima ugrađenu rootkit tehnologiju. Glavni cilj hakera u ovoj vrsti napada je da kompromitirani računarski dio postane robotska mreža ili botnet.

Hakeri koji su zaduženi za botnet ponekad se nazivaju i bot herder-i. Novoinstalirani bot program otvara *backdoor* u sistemu i izvještava nazad bot herder-u. To se vrši preko command-and-control (C&C) servera. Koristeći ove C&C servere, bot herder kontroliše cijeli botnet, s tim da svi zombi računari djeluju kao jedna cjelina. Botnetovi imaju ogromnu količinu procesorske snage s ponekad do stotine hiljada zombija širom svijeta.

Uvlačenje računara u Botnet

Jednom kada računar postane dio botneta, bot herder ga može ga koristiti na brojne načine. Može se koristiti za slanje neželjene pošte i virusa, krađu ličnih podataka ili se može upotrijebiti u prevari klikova kako bi se lažno povećao web promet. Neki bot herder-i čak iznajmljuju procesorsku moć svojih botneta drugim hakerima.

Ova vrsta *cyber*-kriminala predstavlja veliki problem u mnogim dijelovima svijeta. Međutim, institucije uzvraćaju najbolje što mogu. U 2014. godini, uklanjanje ogromnog botneta pod nazivom Gameover Zeus usporilo je širenje sofisticiranog oblika ransomware-a poznatog kao CryptoLocker.

Iznuđivanje enkripcijom

Zamisao da hakeri mogu da ‘otmu’ računar i iznude gotovinsko plaćanje od korisnika nije mašta. Nažalost, scenario je sasvim moguć i odvija se vrlo uspješno već godinama. Sigurnosna prijetnja klasifikovana je kao ransomware i izuzetno je isplativa za *cyber* kriminalce.

Insertovanjem u sistem putem automatskog preuzimanja ili slične metode, ransomware obično radi jednu od dvije stvari: ili zaključava računar, ili šifruje sve lične datoteke. U oba slučaja prikazuje se poruka u kojoj se navodi da se mora platiti otkupnina ili više neće postojati pristup datotekama. Otkupnina za zlonamjerni program poput CryptoLocker-a može se kretati od 300 pa čak do 2000 dolara. Nažalost, prema Microsoftovom centru za zaštitu od zlonamjernog softvera, ne postoji garancija da će se plaćanjem otkupnine ponovo dobiti pristup računaru ili datotekama.

Realni primjeri

Evo nekoliko najozloglašenijih primjera zaraze zlonamjernim softverom, uz metode i tehnike koje hakeri koriste kako bi prodrli u sisteme. Ova kršenja sigurnosti koštala su korisnike računara neprocjenjivo mnogo vremena, frustracije i novca.

Koobface

Anagram Facebook-a, Koobface je bio hibridni ili kombinovani, zlonamjerni softver. Koristio je lukav aspekt trojanca i autonomno replicirajuću prirodu kompjuterskog crva - vrste samostalnog virusa koji se ne mora vezati za drugi program za širenje zaraze. Koobface je ušao u sisteme nesumnjičavih korisnika Facebooka, prevarivši ih da vjeruju da su kliknu na video. Kao i u drugim prevarama, hakeri su koristili kompromitovani nalog Facebook-ovog prijatelja slanjem privatne poruke putem Facebook.

Korisnik, vjerujući da je riječ o istinskoj poruci poznanika, uzeo bi 'mamac' i kliknuo na video. Nakon toga bi se korisnici preusmjerili na web sajt tvrdeći da je potrebno nadograditi njihov Adobe Flash Player softver. Lažna stranica bi im tada pružila link za preuzimanje ažuriranja. Preuzimanje je zapravo Koobface, a nakon što se instaliran, napadaču pruža potpuni pristup ličnim podacima žrtve, uključujući lozinke i bankarske podatke.

Budući da je virus Koobface neutralizovan samo nekoliko godina nakon što se prvi put pojavio 2008. godine, teško je procijeniti puni obim štete koju je uzrokovao. Prema podacima Kaspersky laboratorije, virus Koobface je tokom 2010. godine inficirao između 400.000 i 800.000 računara.

Mac Flashback

Mac Flashback napadi su se gotovo uvijek događali bez znanja žrtve, kao što su korisnici Apple Mac saznali početkom 2012. god. Mac Flashback je *drive-by download* napad, genijalno osmišljen i izveden instaliranjem preuzimanja na računar žrtve. Nakon što bi se ovaj uređaj za preuzimanje u potpunosti instalirao, počeo je s preuzimanjem i instaliranjem drugih vrsta zlonamjernog softvera na ciljni sistem.

Originalnu metodu zaraze započeli su hakeri upotrebom lažnog *plug-in* dodatka, oglašenog kao podesan alat za WordPress blogere. Hiljade blogera uključilo ga je u stvaranje svojih blogova, stvarajući tako gotovo 100.000 zaraženih blogovskih web stranica. Kada bi korisnici Maca posjetili bilo koju od ovih web lokacija, njihov računar bi se odmah zarazio. U tom trenutku se na računaru žrtve može preuzeti i instalirati sve, od pretraživača sa zlonamjernim softverom do softvera za evidentiranje lozinke.

Popravak infekcije stigao je prilično brzo. Za nekoliko mjeseci, Apple je objavio ažuriranje za Mac koji je riješio sigurnosni problem i eliminisao prijetnju Mac Flashback-a. Međutim, ovo nije došlo na vrijeme kako bi se pomoglo Mac korisnicima koji su već zaraženi, a čiji je broj premašio premašio 600.000.

ZeroAccess

Rootkit ZeroAccess pojavio se prvi put 2011. godine, zarazivši više od 9 miliona računarskih sistema širom svijeta. Glavna svrha ZeroAccess-a bila je pretvaranje zaraženog računara u zombija koji se kontroliše na daljinu. Budući da je razvijen kao rootkit koji je u stanju da se prikrije i pokrije tragove hakera, mnoge žrtve nisu znale da su njihovi sistemi zaraženi dok nije bilo prekasno.

Jednom kada bi haker imao kontrolu, zombi bi se uključio u botnet. Od svih zaraženih računarskih sistema, oko 20% je uspješno asimilovano u ovu malicioznu mrežu. Zbog toga je procijenjena veličina botneta ZeroAccess bila odgovorna za stvaranje na 1,9 milona računara do 2013. god.

Ogromnu moć procesiranja botneta koriste *cyber*-kriminalci da bi se uključili u ilegalne aktivnosti poput distribuiranih *denial-of-service* napada. To je slučaj kada se više računara, pod kontrolom hakera, usmjerava da poplave mrežu podacima kako bi je stavili van funkcije. Grupa pod vođstvom Microsofta pokušala je 2013. god. ugasiti botnet kreiran od ZeroAccess, ali pokušaj nije bio potpuno uspješan. Neke komponente botneta, uključujući nekoliko servera naredbi i kontrole, ostavljene su u funckiji.

CryptoLocker

Jedan od najuspješnijih primjera ransomware-a je ozloglašeni trojanac zvan CryptoLocker. Na scenu se pojavio u septembru 2013. godine. CryptoLocker je zarazio desetine hiljada računara širom svijeta i za samo nekoliko mjeseci donio milione *cyber* kriminalu. Ovaj izuzetno uspješan niz ransomware-a koristi enkripciju kako bi se lične datoteke učinile nečitljivim i kriptuje sve, od datoteka sa slikama u digitalnom foto albumu, do dokumenata koji se koriste za rad.

Zaista izvanredna stvar ove vrste *cyber*-kriminala je broj žrtava koji na kraju plaćaju otkupninu. Istraživanje koje je objavilo Istraživačko središte za *cyber* sigurnost Univerziteta u Kentu, pokazalo je da je 40% žrtava CryptoLockera odlučilo platiti otkupninu za obnovu svojih dosijea.

Danas CryptoLocker nije prijetnja kakva je nekad bila. Kada su agencije za sprovođenje zakona u SAD-u i Evropi neutraliziovale botnet zvan Gameover Zeus, to je spriječilo širenje CryptoLockera. *Cyber*-kriminalci koji upravljaju Zeusom programirali su ga da postavi CryptoLocker na svaki sistem s kojim bi stupio u kontakt.

Takođe, brojne kompanije za *cyber* sigurnost, od kojih se mnoge mogu naći putem kataloga koji je stvorio Cybersecurity Ventures, nude žrtvama uslugu dešifrovanja datoteka, poništavajući štetu koju je CryptoLocker prouzročio. Međutim, još uvijek postoje druge varijante i vrste ransomware-a, poput Cryptowall-a, koji su jednako opasni i još uvijek nisu obuhvaćeni spomenutom opcijom.

Da li se desilo hakovanje?

- **Antivirusni softver je onemogućen.** Ako je antivirusni softver onemogućen a nije isključen - ili se ne može ponovo uključiti - možda postoji problem. Ostali programi za provjeru istog simptoma su Windows Task Manager i Registry Editor.
- **Instaliran je nepoznati softver.** Pažnja na nepoznate *toolbars*-e, *plugins*-e ili bilo koje druge softvere koji su se nedavno pojavili.
- **Random Pop-Ups**. Ako nastave i nakon što se završi sesija pregledanja web stranica, možda postoji problem. Lažne antivirusne poruke su najopasnije. Nikada ne klikati na njih.
- **Internetske pretrage su preusmjerene.** Ako se na primjer traži recept za jelo a pretraživač prikazuje oglas za kliniku za obnavljanje kose - krivac je možda naizgled 'nevini' *toolbar* koji je haker mogao postaviti na sistem.
- **Lozinke su promijenjene.** Ako je korisnik odlogovan sa društvenih mreža ili e-pošte, a uoči da su mu prijatelji dobijali neželjene mejlove i poruke, koje izgledaju kao da dolaze od njega, vjerovatno postoji problem.
- **Kursor se kreće sam.** Obično ako se to dogodi, to je manji ili privremeni propust u računaru. Međutim, kada se kreće neslučajno, otvaranjem mapa i pokretanjem aplikacija, haker udaljeno kontroliše sistem.

Kako se zaštititi?

Nema šanse da se lični računar učini potpuno neprobojnim za *cyber*-napad. Čak ni korporativne kompanije, sa timom za računarsku sigurnost, koji ne radi puno radno vrijeme, ne mogu to da garantuju. Srećom, što je hakerima teže ući u sistem, manja je vjerovatnoća da će posvetiti vrijeme i trud tome. U nastavku slijede koraci koji se mogu preduzeti da bi sistem bio zaštićen od gotovo svih sigurnosnih prijetnji.

1. **Instaliranje ili ažuriranje antivirus softvera.** Ako ima mogućnosti za omogućavanje sigurnog surfovanja internetom ili zaštitu identiteta na mreži, treba uključiti ove opcije. Proizvodi Norton, McAfee i sl. su u redu, ali postoje i besplatane verzije, Avast i Malwarebytes...
2. **Osigurati kućnu mrežu.** Provjeriti da li je zaštićena lozinkom i svakako postaviti firewall kako bi se spriječili uljezi. Mnogi ruteri dolaze s unaprijed instaliranim firewall-ima.
3. ***Update*-ovati Softver**. Time se popravljaju poznate sigurnosne rupe. Operativni sistem i web pretraživač treba ažurirati što je češće moguće.
4. **Download-ovati samo sa provjerenih izvora**. Čak i ako je administrator web sajta pouzdan, bez odgovarajućih sigurnosnih mjera web sajt može biti kompromitovan.
5. **Opreznost sa prilozima e-pošte.** Oni su omiljeni hakerima. Paziti na šta se klika, čak i ako u poruci piše da je to od npr. vlade ili banke.
6. **Nikada ne posjećivati sumnjive stranice.** Ako postoji sumnja da li je web lokacija sigurna, prvo je provjeriti servisima za provjeru internet stranica poput Norton Safe Web.
7. **Održavati Password-e**. Kreirati lozinke koje je teško pogoditi, redovno ih mijenjati i nikad ih ne koristiti za više web sajtova. 1Password je popularni sistem za upravljanje lozinkama koji se može koristiti.
8. **Izbjegavati upotrebu besplatnog WiFi.** Kada se koristi WiFi veza u nekom lokalu, uvijek pretpostaviti da neko prisluškuje vezu i preduzeti odgovarajuće mjere.
9. **Isključiti računar**. Kada se ne koristi duži vremenski period, treba isključiti računar. Ovo je siguran način zaštite sistema od bilo kakvih upada.