Mesečni bilten bezbednosnih saveta za korisnike računara

OUCH!

U OVOM IZDANJU...

„Hakovani“ ste, šta sada?

Uvod

Ubeđeni smo da vodite računa o bezbednosti svojih računara i mobilnih uređaja i da preduzimate sve potrebne mere u cilju njihove zaštite. Međutim, bez obzira na to koliko vešto koristite tehnologiju, pre ili kasnije može vam se desiti da budete „hakovani“ ili „kompromitovani“. U ovom izdanju objasnićemo kako da ustanovite da li je vaš računar ili mobilni uređaj „hakovan“, i ako jeste, šta je potrebno da uradite u vezi sa tim. U krajnjoj liniji, što ranije otkrijete da nešto nije u redu i brže reagujete, veća je verovatnoća de ćete umanjiti štetu koju sajber napad može da izazove.

Gost urednik

Samantha Davison (**@sam_e_davison**) je menadžer za bezbednost informacija - edukaciju i trening, u kompaniji Uber i odgovorna je za edukaciju svih zaposlenih u preko 350 gradova širom sveta.

Kako da znate da ste hakovani?

Obzirom da ne postoji jedinstveni način da se to utvrdi, često može biti veoma teško da utvrdite da li ste hakovani. Umesto toga, hakeri često za sobom ostavljaju više naznaka/tragova, često nazvanih indikatorima, koji mogu tome da posluže. Ukoliko neki od vaših uređaja pokazuje simptome slične navedenim indikatorima, velika je verovatnoća da je „hakovan“ ili „kompromitovan“.

- Antivirusni program je aktivirao obaveštenje da je vaš sistem inficiran, posebno ako poruka kaže da nije u stanju da ukloni ili premesti u karantin zaražene fajlove.
- „Homepage“, početna stranica vašeg Internet pretraživača je neočekivano promenjena ili vaš Internet pretraživač otvara Internet stranicu koju niste želeli da posetite.
- Na vašem uređaju se pojavio novi korisnički nalog koji vi niste kreirali, ili nova aplikacija koju vi niste instalirali.
- Uređaj ili aplikacije se same od sebe isključuju, pojavile su se ikonice od vama nepoznatih aplikacije ili čudna obaveštenja operativnog sistema.
- Aplikacija zahteva vašu autorizaciju da izvrši promene na sistemu, iako ne instalirate ili ne ažurirate ni jednu od vaših aplikacija.

„Hakovani“ ste, šta sada?

- Vaša lozinka vise ne funkcioniše kada pokušate da se prijavite na vaš uređaj ili on-line nalog, iako ste potpuno sigurni da lozinka ispravna.
- Prijatelji vas pitaju zašto im šaljete spam el. poštu za koju ste potpuno sigurni da niste poslali.
- Račun vašeg mobilnog telefona je drastično uvećan usled troškova poziva ili slanja SMS poruka na vama nepoznate brojeve telefona.
- Vaš mobilni telefon je odjednom počeo da drastično više troši bateriju.

Pre ili kasnije neki od vaših uređaja može biti kompromitova, što brže detektujete i odgovorite na takav incident, to je po vas bolje.

Kako da reagujete

Ako verujete da je vaš uređaj hakovan, što pre reagujete, to je bolje. Ako se radi o uređaju vašeg poslodavca ili ga koristite u poslovne svrhe, ne pokušavajte da sami otklonite problem. Tako ne samo da možete da prouzrokujete više štete nego koristi, nego možete i da uništite vredne dokaze koji mogu da pomognu istragu. Umesto toga, odmah prijavite incident nadležnima u vašoj organizaciji, obično je to služba za podršku, tim za bezbednost ili nadređeni. Ako iz nekog razloga ne možete da kontaktirate svoju organizaciju, ili ste zabrinuti zbog kašnjenja, isključite uređaj sa mreže i onda ga potpuno isključite, suspendujte ili prebacite u avionski mod. Čak iako niste sigurni da ste hakovani, uvek je, za svaki slučaj, bolje da slučaj prijavite nadležnima. Ako se radi o vašem uređaju koji koristite u privatne svrhe, pratite sledeće savete:

- **Promena lozinke**. Ovo ne podrazumeva samo promenu lozinke za vaše računare i mobilne uređaje, nego i sve vaše on-line naloge. Vodite računa da kada menjate lozinke ne koristite hakovan uređaj. Umesto toga koristite neki drugi uređaj za koji ste sigurni da je bezbedan.
- **Antivirsni program**. Ako ste od vašeg antivirusnog programa dobili obaveštenje da ste inficirani, pratite preporuke koje vam on predlaže, što obično podrazumeva, premeštanje fajla u karantin, čišćenje ili brisanje fajla. Većina antivirusnih program će vam predočiti reference gde se detaljno možete upoznati sa određenim infekcijama i kako da ih prevaziđete. Ako ste u dilemi, premestite fajl u karantin. Ako to nije moguće, obrišite ga.
- **Reinstalacija uređaja**. Ako ne možete da otklonite infekciju ili želite da budete potpuno sigurni da je vaš sistem siguran, možda se odlučite da reinstalirate uređaj. Ako se radi o računaru, pratite instrukcije proizvođača. U većini slučajeva to će podrazumevati reinstalaciju operativnog sistema. Nemojte reinstalirati operativni sistem iz

„Hakovani“ ste, šta sada?

rezervnih kopija pošto se može desiti da uključuju iste propuste koje su i dovele do hakovanja vašeg sistema. Rezervne kopije je potrebo samo koristiti za oporavak vaših podataka. Ako se radi o mobilnim uređajima, sledite uputstva proizvođača ili provajdera, što je verovatno dostupno na njihovim Internet stranicama. U većini slučajeva to je veoma jednostavno, slično vraćanju uređaja na fabrička podešavanja. Ako niste sigurni u svoje sposobnosti, možete potražiti pomoć profesionalaca. U slučaju da je vaš uređaj star, možda je jednostavnije da nabavite novi, i u tom slučaju vodite računa da je potpuno ažuriran i da je automatsko ažuriranje uključeno kad god je to moguće.

- **Rezervne kopije (backup)**. Jedna od najvažnijih stvari koju je potrebno da preduzmete unapred u cilju svoje zaštite je da redovno pravite rezervne kopije podataka. Što češće pravite rezervne kopije to je bolje. Neka rešenja će automatski pravite rezervne kopije novih i promenjenih fajlova na svakih sat vremena. Bez obzira kako pravite svoje rezervne kopije periodično proverite da li je moguće da iz njih povratite svoje fajlove. Vrlo često je oporavak podataka iz rezervnih kopija jedini način da se oporavite u slučaju da ste hakovani.
- **Policija ili nadležni državni organi**. Ako se na bilo koji način osećate ozbiljno ugroženi, prijavite incident lokalnoj policiji ili nadležnim državnim organima.

Saznaj Više

Prijavi se na OUCH! mesečni bilten bezbednosnih saveta za korisnike računara, pristupi prethodnim OUCH! izdanjima i saznaj više o SANS rešenjima u vezi svesnosti bezbednosti informacija na našoj internet prezentaciji http://www.securingthehuman.org.

Dodatne informacije

Rezervne kopije i oporavak:	http://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_se.pdf
Propusne fraze:	http://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_se.pdf
Šta je malver:	http://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_se.pdf
Bezbednost vašeg novog tableta:	http://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201601_se.pdf

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Preveo: Nenad Varinac