Mesečni bilten za podizanje svesti o bezbednosti informacija

Zaštitite se od malvera

Uvod

Sigurno ste već u pričama o sajber bezbednosti čuli za termine kao što su virus, trojanac, ransomver ili rutkit. Sve su to različiti tipovi malicioznih programa poznatih kao malver, koje sajber kriminalci koriste da bi zarazili računare i uređaje. Kada se instaliraju na vašem uređaju, ovi programi mogu da urade sve što želi onaj ko ih je kreirao. U ovom tekstu saznaćete šta je malver, do kakvih opasnosti dovodi, kao i ono najvažnije, šta možete da uradite da biste se od njega zaštitili.

Šta je malver?

Jednostavno rečeno, malver je softver, računarski program, koji se koristi za izvršavanje malicioznih aktivnosti. Reč malver je složenica reči maliciozan i softver. Sajber kriminalci instaliraju malver na vašim računarima i uređajima sa ciljem da uspostave kontrolu nad njima. Po uspešnoj instalaciji, malver može da omogući kriminalcima nadgledanje vaših aktivnosti na internetu, krađu vaših lozinki ili fajlova, ili da korišćenjem vašeg sistema napadnu druge. Malver čak može da uskrati pristup vašim podacima, tražeći da platite otkupninu da biste ga vratili. Mnogi ljudi veruju da malver predstavlja pretnju samo za Windows računare. Nažalost, malver može zaraziti bilo koji uređaj, od Mac računara i pametnih telefona do digitalnih video i bezbednosnih kamera. Što više računara i uređaja sajber kriminalci zaraze, njihova zarada će biti veća. Zato smo svi, pa i vi sami, potencijalna meta.

Zaštitite se – zaustavite malver

Možda vam se čini da je dovoljno da instalirate bezbednosni program poput antivirusnog softvera da biste bili zaštićeni od malvera. Nažalost, antivirus ne može da zaustavi sav malver. Sajber kriminalci neprestano razvijaju novi i sve napredniji malver koji ima osobinu da ostane neprimećen. S druge strane, proizvođači antivirusnog softvera stalno ažuriraju svoje proizvode novim funkcionalnostima za otkrivanje malvera. Na mnogo načina to sve više liči na nekakvu trku u naoružavanju, u kojoj su loši momci obično za korak ispred. Pošto se ne možete osloniti samo na antivirus, evo dodatnih koraka koje treba da preduzmete da biste se zaštitili:

Sajber kriminalci često iskorišćavaju ranjivosti u vašem softveru da zaraze računare ili uređaje. Što je vaš softver ažurniji, to su vaši sistemi manje ranjivi i sajber kriminalcima je teže da ih zaraze. Potrudite se da vaši operativni sistemi, aplikacije, veb pregledači (eng. Web browser) i dodaci za pregledače budu uvek ažurirani i aktuelni. Najlakši način da to postignete je da, kad god je to moguće, uključite njihovo automatsko ažuriranje.

Uobičajen način koji sajber kriminalci koriste da zaraze računare ili mobilne uređaje je kreiranje lažnih računarskih ili mobilnih aplikacija i njihovo objavljivanje na internetu, nakon čega ostaje samo da vas prevare da ih preuzmete i instalirate. Zato je najbolje da softver ili aplikacije preuzimate i instalirate samo iz pouzdanih onlajn prodavnica. Takođe, izbegavajte mobilne aplikacije koje su potpuno nove, imaju malo pozitivnih ocena, retko se ažuriraju ili ih je preuzeo mali broj ljudi. Ukoliko ste prestali ste da koristite neki softver ili mobilnu aplikaciju, deinstalirajte ga.

Dešava se često i da sajber kriminalci, služeći se prevarom, instaliraju malver u ime drugih. Na primer, oni vam mogu poslati mejl poruku koja izgleda legitimno i sadrži neki prilog ili link. Može se čak desiti i da poruka izgleda kao da je šalje vaša banka ili prijatelj. Međutim, ako biste otvorili priloženi fajl ili kliknuli na link, aktivirali biste maliciozni kod koji instalira malver na vašem sistemu. Ako poruka stvara snažan osećaj hitnosti ili izgleda previše dobro da bi bila istinita, to ukazuje na potencijalni napad. Budite sumnjičavi, zdrav razum je često vaša najbolja odbrana.

Redovno kreirajte rezervne kopije vašeg sistema i podataka korišćenjem Cloud rešenja za bekap ili eksternih diskova koje ćete čuvati oflajn, odnosno fizički odvojene. Time ćete zaštititi vaše bekape u slučaju da malver pokuša da ih šifruje ili obriše. Rezervne kopije su veoma važne jer su često jedini način da se oporavite od štete koju vam je malver naneo.

Ponovimo na kraju, najbolji način da se odbranite od malvera je da redovno ažurirate sav softver i uređaje, instalirate pouzdan antivirusni softver kad god je to moguće i uvek budete na oprezu kako vas neko ne bi prevario da zarazite sopstveni sistem. Kada sve ostalo padne u vodu, bekap je često jedini način za oporavak vaših podataka.

Verzija na srpskom

Telekom Srbija kao društveno odgovorna telekomunikaciona kompanija pomaže prevođenje i distribuciju ovog biltena kako bi se unapredila svest korisnika informaciono-komunikacionih tehnologija o bezbednosti informacija.

Gost urednik

Leni Zelcer *ima veliko iskustvo u borbi protiv malvera. Bavi se kreiranjem endpoint bezbednosnih rešenja u kompaniji Minerva Labs i predaje na SANS Institutu. Leni je aktivan na Tviteru kao* @lennyzeltser *i autor je bloga o sajber bezbednosti* zeltser.com.

Dodatni materijal

Ransomver:	https://www.sans.org/u/EdI
Rezervne kopije i oporavak:	https://www.sans.org/u/EdN
Ne dajte se upecati:	https://www.sans.org/u/EdS

OUCH! bilten objavljuje SANS Security Awareness program i distribuira se pod Creative Commons BY-NC-ND 4.0 licencom. Biltene je dozvoljeno *distribuirati ili koristiti za svoj program unapređenja svesti o bezbednosti informacija pod uslovom da se sadržaj ne modifikuje. Za pitanja u vezi prevoda ili za dodatne informacije, kontaktirajte* www.sans.org/security-awareness/ouch-newsletter. *Redakcija: Walt Scrivens, Phil Hoffman, Кэти Клик, Cheryl Conley | Preveli: Dragan Ristić i Gordana Živanović*

© SANS Institute 2018