Mesečni bilten bezbednosnih saveta za korisnike računara

OUCH!

U OVOM IZDANJU...

Šta je malver

Uvod

Verovatno ste bili u prilici da tokom nekog razgovora u vezi sajber bezbednosti čujete za termine kao što su virus, trojanac, ransomver (ransomware) ili rutkit (rootkit). Svi ovi pojmovi imaju zajedničku karakteristiku, to su računarski programi koje koriste sajber kriminalci da inficiraju računarske uređaje. Zajednički termin ili naziv koji opisuje sve ove različite programe je reč malver (malware). U ovom izdanju objasnićemo šta je malver, ko ga kreira i zašto, i što je i najvažnije, šta možete da učinite da bi ste se zaštitili.

Gost urednik

Lenny Zeltser je zadužen za bezbednost IT poslovanja klijenata u NCR korporaciji i podučava borbu sa malverom pri SANS institutu. Lenny je aktivan na Twitter-u kao **@lennyzeltser** i na blogu **zeltser.com**.

Šta je malver?

Jednostavno, malver je softver, računarski program, koji se koristi u štetne (maliciozne) svrhe. U stvari malver (malware) je kombinacije dve engleske reči, malicious (štetan) i software (računarski program). Sajber kriminalci instaliraju malver na računarima ili drugim uređajima svojih žrtvi u cilju preuzimanja kontrole ili pristupa sadržaju tih uređaja. Kada je malver instaliran, napadači ga koristi za različite kriminalne aktivnosti, praćenje on-line aktivnosti žrtve, krađu lozinki ili fajlova, ili korišćenje inficiranog računara za napade na druge sisteme ili osobe. Malver čak može da vam onemogući pristup sopstvenim fajlovima, i da pri tome zahteva da platite otkup napadaču da bi ste ih povratili, baš kao kod otmice.

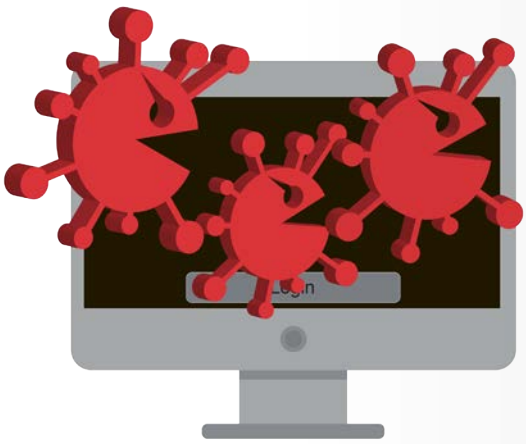
Nemali broj ljudi ima pogrešno shvatanje da je malver problem vezan samo za Windows računare. Nema sumnje da je Windows zbog svoje rasprostranjenosti najveća meta, ali malver može da inficira i druge platforme, uključujući Mac računare, pametne telefone ili tablete. Kriminalci znaju da što više računara ili drugih uređaja inficiraju, to više novca mogu da zarade. Stoga, niko nije bezbedan i svako od nas je potencijalna meta.

Ko kreira malver?

Malver više ne kreiraju samo znatiželjni entuzijasti ili hakeri amateri, već i sofisticirani sajber kriminalci. Oni za cilj imaju da inficiranjem tuđih računarskih uređaja zarade novac, prodajom ukradenih podataka, slanjem neželjene (spam) el. pošte ili

Šta je malver

iznudom. Tip ljudi koji kreiraju, distribuiraju i imaju koristi od malvera je raznolik, mogu da budu pojedinci koji samostalno deluju, pripadnici dobro organizovanih kriminalnih grupa ili čak organizacije pod okriljem država. Ljudi koji kreiraju najnoviji sofisticirani malver su često potpuno posvećeni toj delatnosti, kreiranje malvera je njihov primarni i jedini posao. Osim toga, kada jednom razviju svoj malver, često ga prodaju drugim pojedincima ili organizacijama, čak im pružaju i redovno ažuriranje i podršku.



Zaštitite se od malvera tako što ćete biti skeptični u vezi sumnjivih el. poruka, redovnim ažuriranjem svih svojih uređaja i korišćenjem aktuelnog antivirusnog softvera, kad kog je to moguće.

Kako da se zaštitite?

Prva stvar koju je potrebno uraditi je svakako instalacija pouzdanog antivirusnog softvera renomiranog proizvođača. Takvi alati, često nazvani i antimalver softver, su posebno dizajnirani da detektuju i zaustave malver. Ipak, takav softver ne može da zaustavi i ukloni sve maliciozne programe. Sajber kriminalci permanentno smišljaju i kreiraju novi, sofisticiraniji i složeniji malver koji može da izbegne detekciju. Sa druge strane, proizvođači antivirus softvera konstantno ažuriraju svoje proizvode novim mogućnostima detekcije malvera. Na mnogo načina, sve podseća na trku u naoružanju, u kojoj obe strane pokušavaju da nadmudre onu drugu. Nažalost, loši momci su obično korak ispred. Usled toga jasno je da se ne možete samo osloniti na antivirusni softver, već je potrebo da se pridržavate i sledećih saveta:

- Da bi inficirali računarske uređaje sajber kriminalci često koriste slabosti softvera koji je instaliran na samim tim uređajima. Što je novija verzija nekog softvera, to je manje poznatih slabosti i teže za sajber kriminalce da inficiraju računar. Prema tome, budite sigurni da su operativni sistemi i sve aplikacije na vašim uređajima podešeni da se automatski ažuriraju.
- Uobičajen način na koji sajber kriminalci inficiraju mobilne uređaje je da kreiraju lažne aplikacije, postave ih negde na Internetu, i onda prevare ljude da ih preuzmu i instaliraju. Usled toga, preuzimajte i instalirajte aplikacije samo iz pouzdanih i proverenih on-line prodavnica. Osim toga, preuzimajte i instalirajte samo aplikacije koje nisu skoro postavljene, koje su preuzete od velikog broja korisnika i kod kojih prevladavaju pozitivni komentari.
- Na računarima umesto Administrator-skog ili „root“ naloga, koristite standardni nalog sa limitiranim privilegijama. Takvim pristupom osiguraćete dodatnu zaštitu pošto ćete limitiranim privilegijama onemogućiti određene tipove malvera da budi instalirani.

Šta je malver

- Sajber kriminalci često prevare ljude da sami instaliraju malver, na primer tako što im pošalju el. poštu koja izgleda legitimno i sadrži prilog ili „web-link“. El. pošta može da izgleda kao da dolazi od vaše banke ili prijatelja. Međutim, kada otvorite prilog ili kliknete na „web-link“ aktivira se maliciozni kod, koji instalira malver na vašem uređaju. Ako je poruka koje ste primili zbunjujuća, previše dobra da bi bila istinita, stvara osećaj hitnosti i pritiska, moguće je da se radi o napadu. Budite sumnjičavi, često je zdrav razum vaša najbolja zaštita.
- Redovno kreirajte rezervne kopije svojih sistema i fajlova po mogućstvu korišćenjem pouzdanih servisa baziranih na računarskom oblaku, ili eksternih diskova. Na takav način moći ćete da povratite svoje uređaje ili fajlove ako malver uspe da ih enkriptuje ili obriše. Rezervne kopije su nekada jedini način da se sistemi i fajlovi oporave od malver infekcije.

Konačno, najbolji način da se zaštitite od malvera je da redovno ažurirate svoj softver, koristite pouzdani antivirusni softver renomiranog proizvođača, da stalno budete na oprezu i koristite zdrav razum.

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

Sajber pecanje: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201512_se.pdf

Društveni inženjering: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201411_se.pdf

Bezbedno korišćenje aplikacija na mobilnim uređajima:
https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201501_se.pdf

Bezbednost vašeg novog tableta: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201601_se.pdf

Rezervne kopije i oporavak: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_se.pdf

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