

Kehv seis veebimaastikul: Eestis on 43 Wordpressi lehte 50st haavatavad

8 aastat tagasi Autor: [Oliver Sild](#)



Peale juulis toimunud rünnakute lainet panime tähele, et suuremat osa veebilehtedest, mis rünnaku alla sattusid, ühendas üks kindel sarnasus. Kõik veebilehed kasutasid Wordpressi sisuhaldussüsteemi.

Otsustasime olukorra tõsisust ise testida ning panime augusti alguses käiku kampaania, mille käigus tegime 50 Eesti Wordpressi platvormil ehitatud kodulehele täiesti tasuta auditi.

Auditi eesmärgiks oli näidata veebilehede omanikele infot nende kodulehe kohta, mida näeb potentsiaalne ründaja ning seda ilma igasuguse ligipääsuta (ehk siis auditi läbiviimiseks piisas vaid avalikust veebilehest).

Mida me avastasime

43 veebilehel 50-st esinesid turvariskid, mida on võimalik avalike ründevektorite (*public-exploitide*) kasutamisel rünnata. 45 veebilehel oli võimalik kätte saada haldusliidese kasutaja nimed ning ID'd ning 22 veebilehel oli jäänud haldusliidesele alles admin nimeline kasutaja. Antud infot on võimalik ära kasutada *Brute-Force* tüüpi rünnakute läbi viimiseks, kuna 45 veebilehel 50st puudus ka töötav tulemüür, mis takistaks logimiste arvu või üldse antud andmete lekkimist.

Keskmiselt oli igal veebilehel 3 aegunud lisamoodulit (pluginat) ning 2 erinevat haavatavust, mida on võimalik häkkeritel rünnakute läbi viimiseks ära kasutada.

Enim populaarsed aegunud moodulid olid järgmised:

- [contact-form-7](#)
- [WPML](#)
- [Yoast-SEO](#)

Enim populaarsed haavatavused:

- [Contact Form 7 <= 3.5.2 – File Upload Remote Code Execution](#)
- [WPML <= 3.1.7.2 – Multiple Vulnerabilities \(Including SQLi\)](#)

Mida me sellest järeldame?

Pea iga veebileht, mis on arendatud Wordpress platvormile, võib olla järgmine ohver näostamisele ning võib levitada nii pahavara, kui spämmi. Kuna rünnakud on poolautomaatsed ning haavatavused tekivad kodulehele praktiliselt iseenesest, siis on vaid aja küsimus, millal sinu veebilehel istuva aegunud tarkvara kord kätte jõuab.

Mis rünnaku tulemusel juhtub?

Oleme näinud olukordi, kus veebilehe omanik on pidanud varunduste puudumise pärast arendama peale rünnakut täiesti uue kodulehe. Kui rünnak avastatakse hiljem, (tihti peale võib nii minna, kui esileht jäetakse puutumata) võib veebileht sattuda musta nimekirja ning rikutakse ka veebilehe SEO, nagu näha alloleval pildil.

HACKED BY D3str0y3r S3c -

www. [redacted] hacked(1).html ▼ Tõlgi see leht

HACKED BY D3str0y3r S3c. ~Comunism With Fail~. Exploited By D3str0y3r S3c. Your Web Site Has Been Exploited ! (:::An0nyGh05t:::<

Olete seda lehte külastanud 2 korda. Viimati külastasite: 6.09.16

Otsingumootorisse jääb ründaja mäрге maha ka peale rünnaku parandamist.

Kui veebilehele on lisatud pahavara ja spämmiroboteid, võid ühel hommikul avastada, et sinu veebileht on veebimajutuse poolt hoopis suletud ning lehe saad taasavada vaid juhul, kui veebilehel on haavatavused parandatud ning pahavara eemaldatud.

Miks on veebilehe tulemüür niivõrd tähtis?

Tarkvara aegub pea igapäevaselt. Uuendused Wordpressi platvormile tulevad välja üsna tihedalt ning Wordpress pakub enda uuendusi ka üsna agressiivselt. Kodulehte arendades aga kasutatakse pea alati ka erinevaid lisamooduleid (pluginaid), mis annavad veebilehele juurde mõne spetsiifilise funktsiooni. Antud lisamoodulid aga aeguvad märksa kiiremini ning mõnda neist edasi ei arendatagi ning isegi, kui plugin on haavatav, ei ole uuendusi tulemas. Teistpidi jällegi on mooduleid, mis väljastavad uuendusi iga nädal ning kogu selle uuenduste protsessiga tegelemiseks oleks vaja juba eraldi inimest.

Tulemüüri eesmärk on ära tunda pahatahtlikud külastajad ning isegi, kui veebilehel on aegunud mooduleid ning nendega seotud haavatavusi, hoiab tulemüür olukorda kontrolli all. Automaatseid rünnakuid proovitakse läbi viia kogu aeg ning Tulemüür teab, kus on veebilehe nõrgad kohad ning kuhu probleemi tekitajaid ligi ei lasta.

WebARX

Sinu litsents kehtib kuni 26.Juuni 2017

Veebileht on rünnakute eest kaitstud!

Brute-Force kaitse



Veebilehe tulemüür



Automaatne pahavara skänner



Viimane skanneerimine toimus

Tue Sep 06 2016 18:30:30 GMT+0300 (EEST)



WebARX on blokeerinud 3357 rünnakut.

[Näita logisid...](#)

26.Juunist alates on ka meie veebilehel proovitud läbi viia üle 3000 rünnaku.

Pakume endiselt (piiratud aja jooksul) Wordpressi omanikele tasuta mini-auditeid ning kui tahad teada, mida potentsiaalne ründaja sinu veebilehe tarkvara kohta leiab, siis [kirjuta](#) oma soovist.

OLIVER SILD

Tegevjuht, Eesti veebiturvalisuse agentuur ESEC

- [Uudised](#)
- [Lahendused](#)

- [Tarkvara](#)
- [Turvalisus](#)