ESET je na web stranicama pronašao prijetnju i blokira pristup

Tema

ESET-ov program je na web stranici koja je pod vašom kontrolom detektirao prijetnju i onemogućio pristup.

Uvod

Vaš ESET ne štiti web stranice na serverima koji se nalaze kod nekog trećeg pružatelja usluga.

U slučaju prijetnji koje nisu razine “virusa”, nego su u kategoriji “nepoželjne datoteke” – ESET-ov program omogućuje da detekciju zanemarite i otvorite prethodno blokiranu stranicu (https://www.nod32.com.hr/podrska/kb8956).

U slučaju da je nađena ozbiljna prijetnja (virus, trojanski konj, …) ne možete izabrati da želite nastaviti s otvaranjem stranice i pristup je blokiran sve dok je ESET-ov program instaliran i aktivan.

Postupak – Kratko (tl;dr)

U oba slučaja vlasnik web stranica mora kvalitetnim antivirusnim programom skenirati datoteke na svom web serveru (posebno u slučaju da naš program javi točan naziv i lokaciju detektirane prijetnje) i ukloniti sve suvišne i inficirane datoteke.

Postupak – Detaljno

- provjerite s autorom stranica da se na serveru nalazi *samo* ono što je programirano i planirano i ništa više
- uklonite sve suvišne datoteke
  - ovo se posebno odnosi na Javascripte poput one koju je ESET detektirao (ako je vidljiva točna lokacija)
- poželjno je analizirati skriptu koju ESET detektirao kao prijetnju
  - moguće je da je netko namjerno ubacio ovu skriptu na web server
  - može biti da skripta nije pisana dovoljno dobro da bi spriječia zlonamjerne upade u sustav
- koristite isključivo pouzdane i/ili masovno korištene dodatke
- sve datoteke na serveru skenirajte kvalitetnim antivirusnim programom
  - pružatelji usluga, ISP, obično koriste besplatne antivirusne programe koji često nisu dovoljno dobri u ovim prilikama
- provjerite dopušta li web-server engine nasilnu promjenu sadržaja
  - sve nadogradnje za OS na kojemu je web server
  - sve nadogradnje za content engine
  - sve nadogradnje za proširenja (ekstenzije, add-ons, plug-ins)
- postoji i mogućnost da skripta ne sadrži u sebi maliciozni kôd ali sadrži upute za preuzmanje drugih datoteka s drugih servera, pa ih nakon pokretanja obriše
  - ESET detektira datoteke iz trećeg izvora
  - datoteke nisu prisutne svaki puta kad a skenirate

○ datoteke nisu prisutne ako ugasite web-server dok skenirate jer je izvorna skripta onda neaktivna i ne može preuzeti maliciozni dio
○ ovo je slučaj kada ESET sporadično detektira

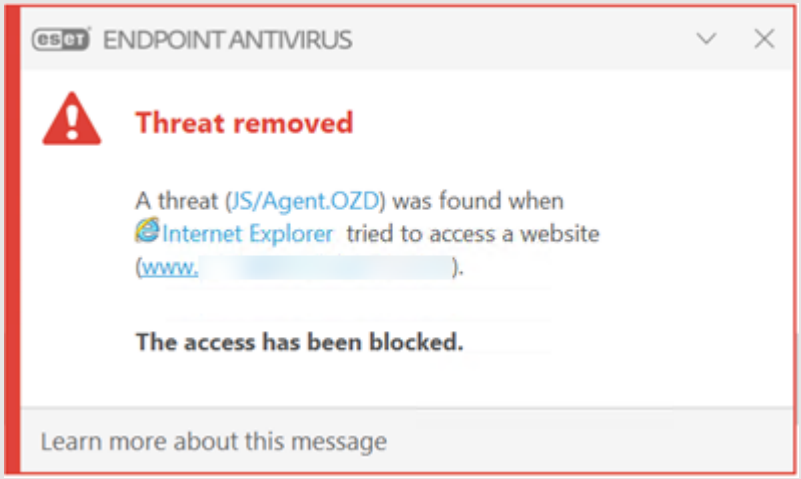
Nakon gornjih radnji nas obavijestite da je server “očišćen”, pa ćemo inicirati ponovno skeniranje dostupnih stranica na serveru i po potrebi ukloniti detekciju.

Razno

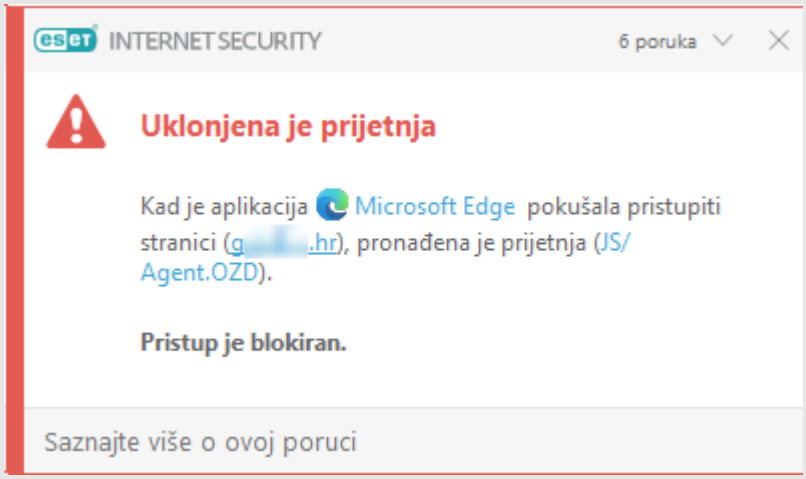
Gornje radnje treba provoditi redovito; nijedna od aktivnosti neće potpuno ukloniti mogućnost ponovne pojave prijetnje jer situacija ovisi o velikom broju faktora od kojih je mali broj njih pod Vašom kontrolom, ali se mogućnost može značajno smanjiti.

v. https://www.nod32.com.hr/podrska/kb8956

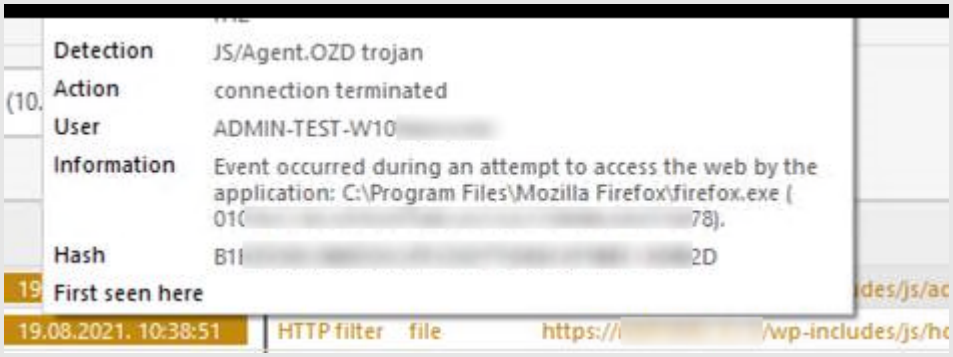
Slike



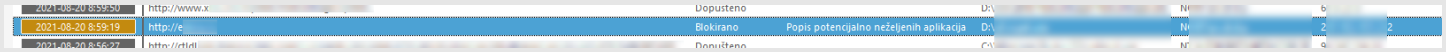
EIS Threat removed



EIS uklonjena je prijetnja



EES log



EIS log Filtrirane web stranice

Video

…

---

xprijetnjax prijetnja threat xthreatx xwwwx xwebx xblockx block xjsagentozdx xagentozdx xozdx xjsx xjavascriptx xscriptx pronađena je prijetnja