Slanje sumnjive datoteke / e-poruke / web stranice na analizu

Tema

Kako poslati sumnjivu datoteku / e-poruku / web stranicu ii pogrešnu prijavu (*false positive*) na analizu.

Uvod

Naš program je detektirao nešto, a nije trebao ili nije detektirao, a čini Vam se da je trebao? Odmah nam pošaljite (na adresu "podrska@") uzorak na analizu kako bismo što prije mogli dodati detekciju ili ju ukloniti ako je bila pogrešna.

Postupak – Kratko (tl;dr)

• Spremite datoteku ili cijeli e-mail (kao .MSG ili .EML ili .TXT source) u komprimiranu arhivu, obavezno s lozinkom `infected` i pošaljite nam
• Za prijavu sumnjivih web stranica nam samo pošaljite njihov link
• U oba slučaja detaljno opišite situaciju

Postupak – Detaljno

Sumnjive datoteke

• spremite ih u neki od popularnijih oblika komprimirane arhive (ZIP, 7Zip, RAR, …)
• (ako ih ESET detektira, onda Vam neće dopustiti da kreirate arhivu; prvo napravite izuzetak: https://help.eset.com/eis/14/en-US/idh_performance_exclusion.html)
• obavezno stavite lozinku `infected` (ako nema lozinke, naš server će obrisati e-mail sa sumnjivim sadržajem)
• pošaljite nam poruku s detaljnim pojašnjenjem (naš program detektira datoteku kao prijetnju, a ne bi trebao ili ne detektira, a trebao bi, otkuda ste dobili datoteku / link, …)
• poruci priložite gornju arhivu s uzorkom
• ili arhivu stavite na neki svoj online-disk (One Drive, DropBox, …) i pošaljite nam poveznicu

Sumnjive e-poruke

Sumnjiva e-Poruka koju ćete nam poslati obavezno mora sadržati cijeli izvorni kôd (mail source code). Bez

uvida u puni sadržaj e-poruke, analiza često nije moguća. Spremite poruku kao datoteku u jedan od sljedećih oblika, ovisno o programu koji koristite.

• Outlook

Najjednostavnije je poruku “odvući” na Desktop – spremit će se kao .MSG datoteka.

• Thunderbird

Najjednostavnije je poruku “odvući” na Desktop – spremit će se kao .EML datoteka.

• Outlook.com

• u popisu poruka desnom tipkom miša kliknite na sumnjivu poruku
• odaberite “View”
• odaberite “View message source”
• označite kompletan tekst (Select all)
• kopirajte tekst
• otvorite Notepad i zalijepite tekst
• spremite u datoteku .TXT

(v. slike)

• GMail.com

• u popisu poruka desnom tipkom miša kliknite na sumnjivu poruku
• odaberite “Forward as attachment”

(v. slike)

• Ostali web-mail klijenti

Postupak je sličan ili jednak gore opisanima.

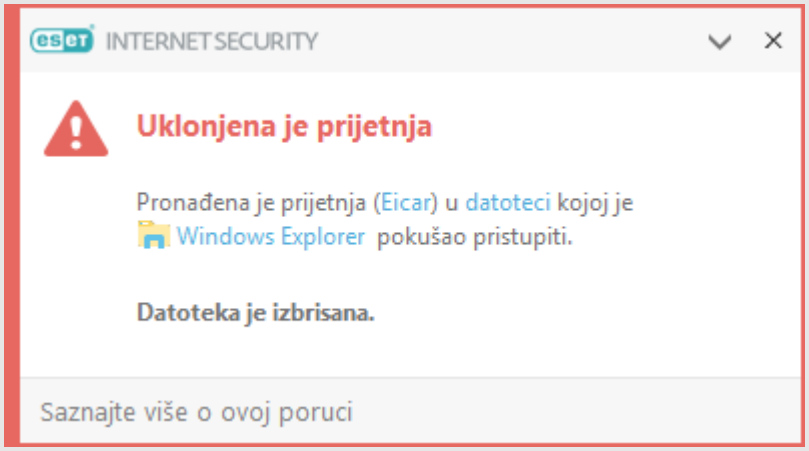
Sumnjive web stranice

Za prijavu je dovoljno da nam pošaljete e-mail u koji stavite link na stranicu koja je (pogrešno) kategorizirana ili detektirana.

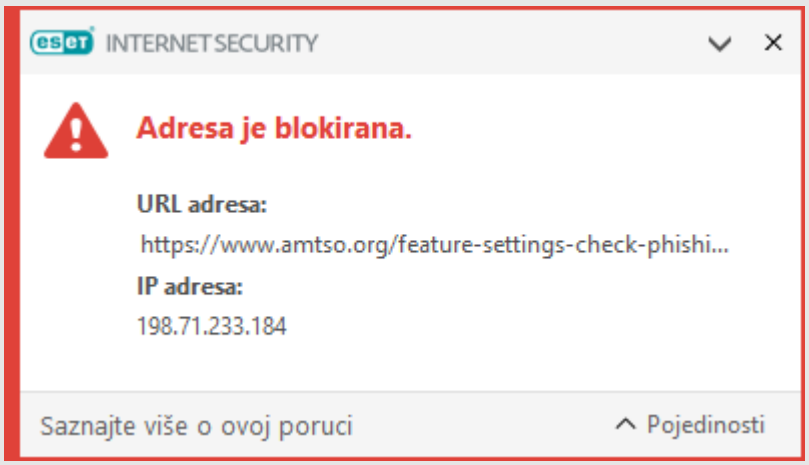
Razno

Po primitku datoteke / poruke analizirat ćemo ih, a po potrebi kontaktirati laboratorij u ESET-u i javiti Vam se s povratnom informacijom.

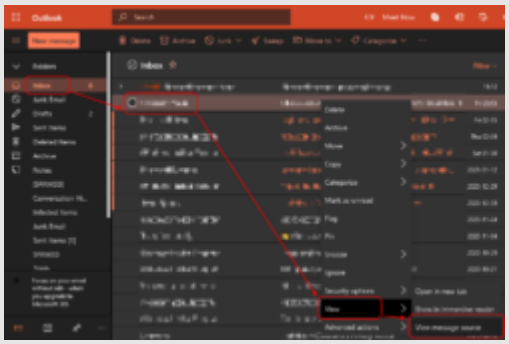
Slike



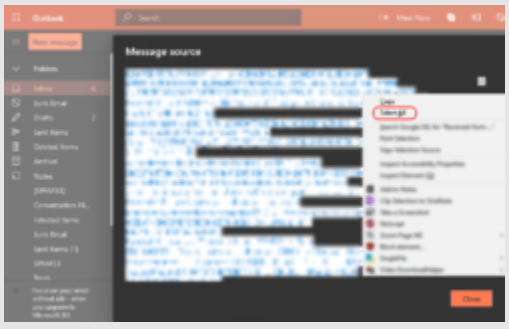
Prijava prijetnje



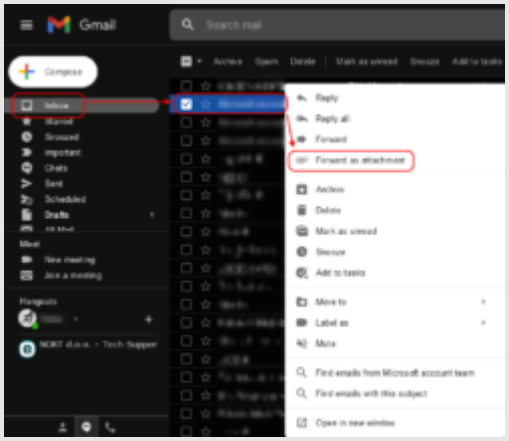
Prijetnja na web serveru



outlook.com 1



outlook.com 2



gmail.com

Video

(*nema*)

---

xsamplex xuzorakx xuzorcix xemlx xmsgx xfpx xfalsepositivex xprijetnjax xthreatx xvirusx