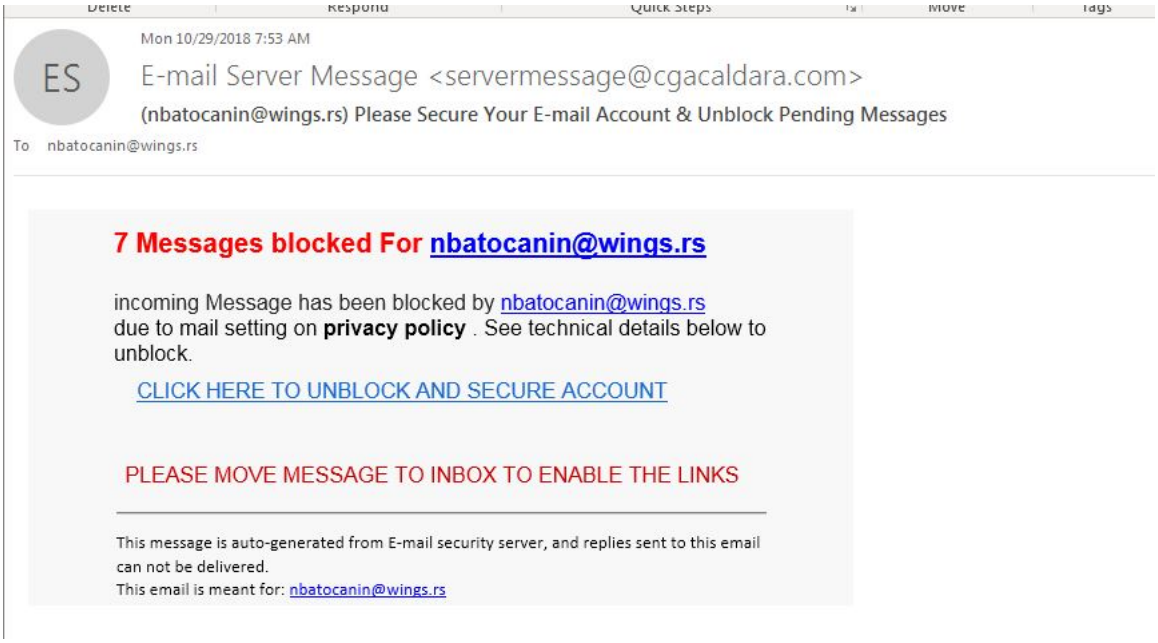
Kako da znate da li mail sadrži virus?

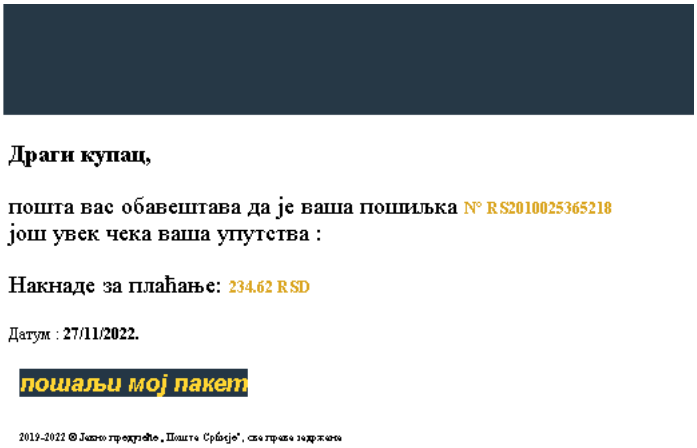
Najveći broj virusa se danas dobija preko mejla. Na primer, možete dobiti mejl od nekog poznanika ili poslovnog partnera u kome vas poziva da kliknete na neki interesantan link ili da vidite neku sliku ili video. Takođe vam može stići upozorenje od provajdera da vam je mejl nalog blokiran i da treba da kliknete kako biste rešili probleme. Sada su sve češći mejlovi koji vas obaveštavaju da je stigla e-faktura, pošiljka, da vam ukidaju mail nalog... Spisak je ogroman i svaki dan se proširuje. Postavlja se pitanje kako da prepoznate mail koji sadrži virus?

Prvo treba da shvatite kako sistem funkcioniše: autori virusa prvo upadnu na neki računar i sa njega ukradu sve mejlove. Ako ste se bilo kada dopisivali sa tom osobom, tako dolaze do vaše mail adrese. Takođe tako dobijaju i mejlove koje vam je ta osoba slala. Sada oni generišu lažni mail, ali ga maskiraju kao da dolazi od te osobe i u njega umeću program kao fajl ili link koji služi da preuzme kontrolu nad vašim računarom. Klikom aktivirate virus koji vam može potpuno blokirati računar i uništiti sve podatke. Zato oprez: **pazite na šta klikćete u mejlovima**!

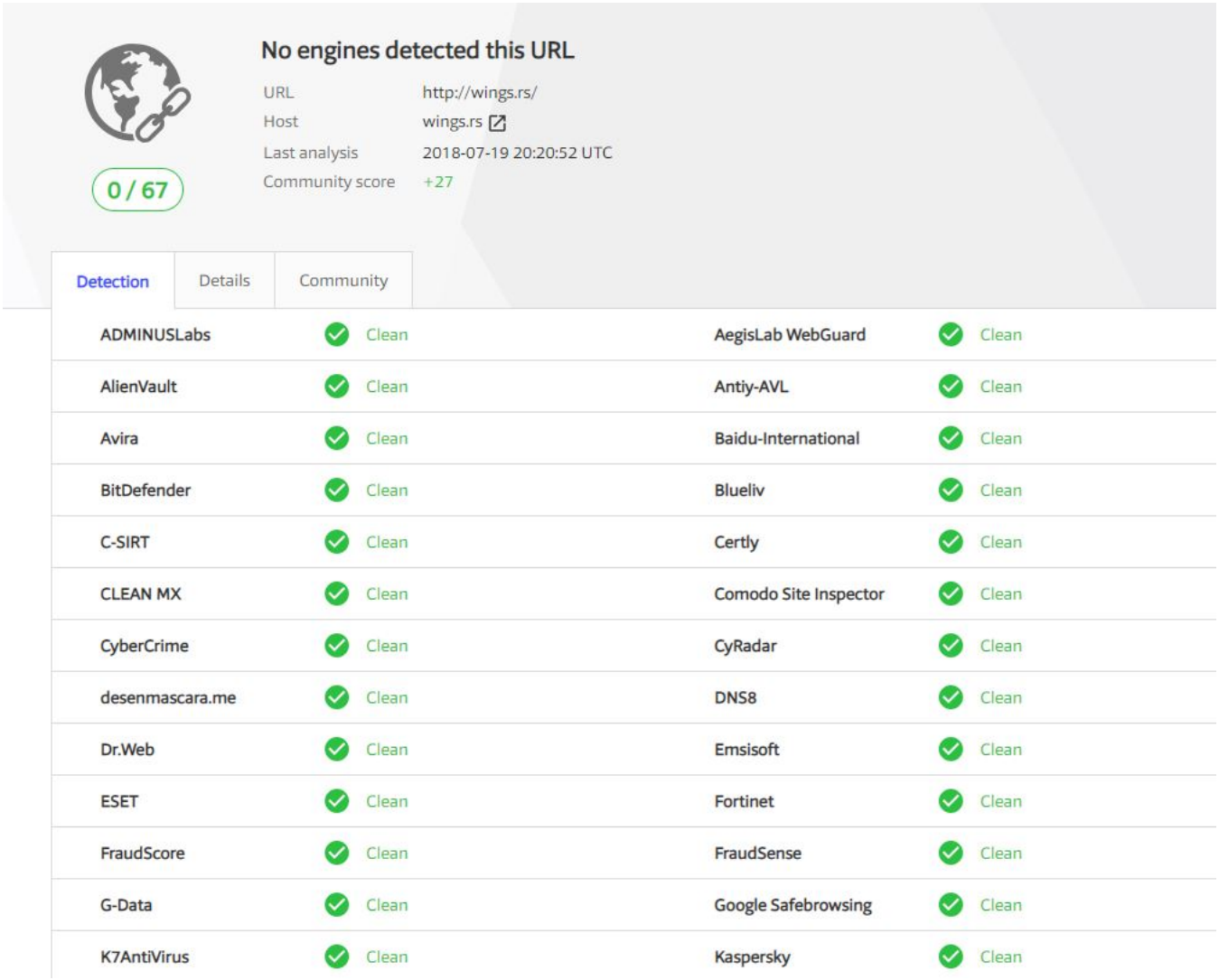
Kako da prepoznate ove mailove? To nije tako jednostavno, jer se autori trude da što vernije imitiraju originalni izgled i maskiraju virus. Obratite pažnju na sledeće:

- ako vam poznanik šalje samo link, bez dodatnog objašnjenja, verovatno je u pitanju virus.
- poznanik vam se obraća na engleskom jeziku
- bilo kakvo odstupanje od standardnog izgleda može značiti da je u pitanju virus.
- ako ste dobili mejl od nekog servisa koji inače koristite (na primer, PayPal), nemojte kliknuti na ponuđeni link, nego idite na sajt tog servisa – ako zaista postoji neki problem, sve možete završiti na sajtu.

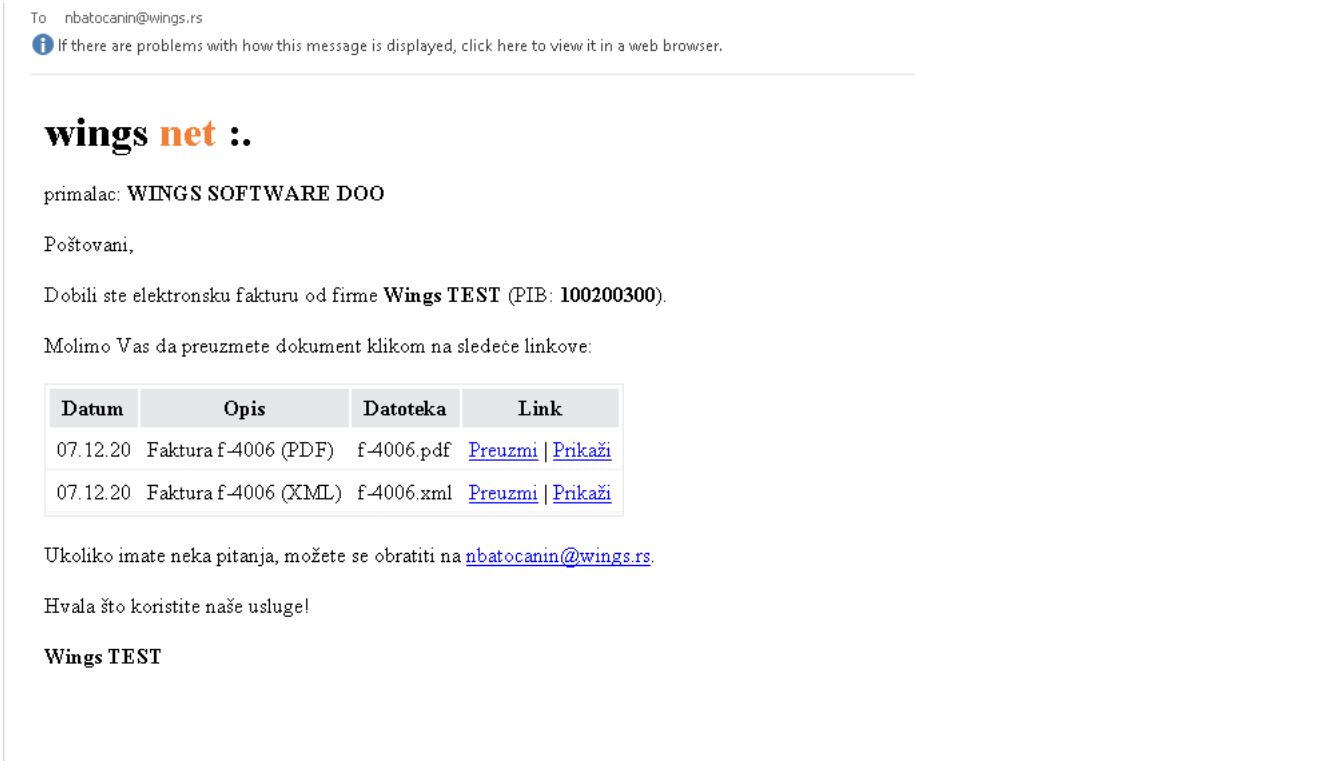




- ako ste dobili mejl sa sumnjivim linkom ili fajlom, možete ga proveriti koristeći sledeći servis https://www.virustotal.com. Na njemu možete zadati sumnjiv link ili fajl i on će biti proveren sa većim brojem različitih AV programa.



- Proverite link koji vam se nudi. Primera radi, kada dobijate fakturu preko WingsNeta, dobijate ovakav mail:



Pomerite kursor na link “Preuzmi” (ali nikako nemojte kliknuti na njega!) i većina programa će vam ispisati adresu na koju vodi link. U slučaju WingsNeta početak linka treba da bude **https://net.wings.rs** – ako vidite da link vodi na neki nepoznati sajt, nikako ga nemojte aktivirati.

Nažalost, prikaz linka se može lažirati, pa ni to nije 100% pouzdan način da se proveri. Ukoliko sumnjate, koristite prethodno opisani sajt za proveru. Prvo, stanite na link i kliknite **desnim** tasterom miša. Iz ponuđenog menija izaberite “Copy link address” ili “Copy hyperlink”. Zatim idite na sajt:

https://www.virustotal.com

Izaberite opciju URL i komandom Ctrl-V iskopirajte link koji ste malopre dobili u ponuđeno polje. Tako dobijate izveštaj od više vrhunskih programa za testiranje da li je vaš link siguran.

- Da li očekujete mail od određene ustanove? Ako dobijete mail od recimo pošte, a ne očekujete pošiljku, obavezno pažljivo proverite šta piše.
- Nemojte kliknuti na mejl koji ste “dobili” od Microsofta ili tako neke poznate firme gde vas upozoravaju na neki virus – vrlo je verovatno da upravo ta poruka sadrži virus!

Ukoliko ste dobili sumnjiv mail, najbolje je da ga izbrišete i konsultujete nekog stručnog da proveri da li je u pitanju virus.