Domoljubni radio

Portal domoljubnog radija

UPOZORENJE: U tijeku je velika kampanja s ciljem krađe osobnih podataka putem e-pošte

Mario Strinavić · Thursday, January 9th, 2020

VAŽNO! U tijeku je velika phishing kampanja usmjerena na korisnike interneta u Hrvatskoj. Korisnicima se savjetuje da takve poruke brišu iz pristigle pošte, ne slijede i ne otvaraju poveznice i ostale kolege upozore na aktualnu phishing kampanju. Piše cert

Detalji se nalaze u nastavku uz priloženi primjer poruke elektroničke pošte:

——

Pošiljatelj: Dostava Eracuna <dostava@moj-eracun.hr> – lažirano “From:” polje
Mail server: tucity.vservers.es [91.142.213.216]
Naziv maila: **Popis neplaćenih računa za prosinac 2019. godine**

FTP server: ftp[.]dalitecnoimagen[.]cl [208.85.243.132]

Tekst poruke:

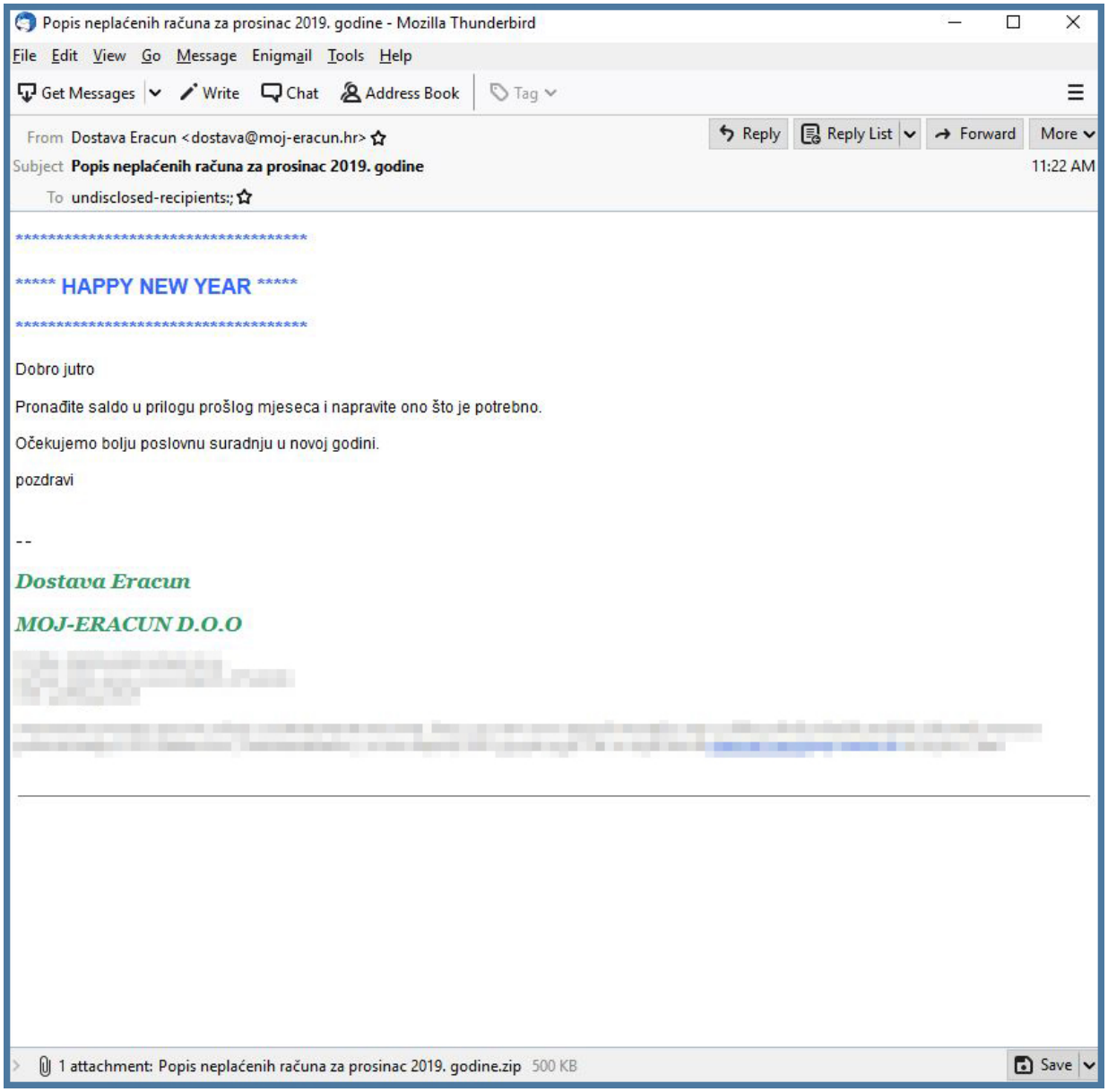
Dobro jutro

Pronađite saldo u prilogu prošlog mjeseca i napravite ono što je potrebno.

Očekujemo bolju poslovnu suradnju u novoj godini.

pozdravi

Naziv priloga: **Popis neplaćenih računa za prosinac 2019. godine.zip**



Analiza:

U zip datoteci se nalazi .exe izvršna datoteka s ikonom mape i nazivom “Popis neplaćenih računa za prosinac 2019. godine.exe.” Iza te izvršne datoteke se nalazi zlonamjerni sadržaj nazvan “Agent Tesla” čija je svrha krađa podataka sa zaraženog korisnikovog računa.

HASH: MD5 68D6A8DA98B575E5350F0FC3AF2C2DC0
SHA1 D32BAF9C79CD1BA6A584AEBA70C10DED7F2A98FE
S H A 2 5 6
B93D23BD04DB6E6D790BF947E80981058805570177 7D95D488FF738D14E8FF96SS
DEEP

Poslane su prijave pružatelju usluge udomljavanja internetskog sadržaja na čijem se serveru nalazi FTP poslužitelj za spremanje ukradenih podataka i izvoru phishing poruka elektroničke pošte. U porukama se nalaze i adrese nadležnih CERT-ova tih država. U trenutku pisanja upozorenja nismo zaprimili odgovore o statusu rješavanja istih.

Što je Phishing ?

Phishing (varijanta engleske riječi za pecanje, fishing) je vrsta socijalnog inženjeringa koja se odnosi na prijevare, kojima se služe zlonamjerni korisnici šaljući lažne poruke koristeći pritom postojeće internet servise. Riječ je o kriminalnoj aktivnosti. Koristeći razne načine manipulacije, kriminalci od korisnika pokušavaju prikupiti povjerljive podatke (korisnička imena, lozinke, podaci s kreditnih kartica i sl.) kako bi ostvarili financijsku korist. U pravilu, phishing poruke prenose se putem elektroničke pošte koja navodi korisnika da klikne na određeni link koji ga dalje vodi na stranice zloćudnog web poslužitelja. Takve zloćudne Web stranice obično se lažno predstavljaju kao Web stranice banaka, servisa za elektroničko plaćanje (PayPal i dr.) i sl. krivotvoreći, odnosno imitirajući njihov izgled. U svrhu phishing-a, osim elektroničke pošte, mogu poslužiti i drugi servisi poput foruma, servisa za izravnu komunikaciju (Windows Messenger, ICQ, Skype, Google Talk i dr.) te društvene mreže (Facebook, MySpace). Društvene mreže posebno su opasne jer podaci prikupljeni sa njih mogu poslužiti za krađu identiteta, ali i zbog činjenice da poruke dobivene od prijatelja, kojima su kompromitirani (oteti) računi, imaju određeni kredibilitet.

Foto: Ilustracija

Mario Strinavić

This entry was posted on Thursday, January 9th, 2020 at 7:50 pm and is filed under Nekategorizirano You can follow any responses to this entry through the Comments (RSS) feed. Responses are currently closed, but you can trackback from your own site.