Domoljubni radio

Portal domoljubnog radija

Oprez: Hakerske Phishing kampanje iskorištavaju strah od epidemije COVID-19

Mario Strinavić · Thursday, March 19th, 2020

Nacionalni CERT izvijestio je da su počele *phishing* kampanje koje pokušavaju iskoristiti epidemiju koronavirusa da se lažno predstave kroz e-mail poruke i uvjere korisnika da pokrene maliciozni kod na svom računalu.

Jedna takva kampanja traje, a napadači se predstavljaju kao Svjetska zdravstvena organizacija (World Health Organization; skraćeno WHO), a najčešće teme koje se koriste u ovakvim vrstama poruka su:

- upozorenje iz zdravstvenih centara
- informacije o širenju virusa
- savjeti stručnjaka za zaštitu od zaraze
- analiza o utjecaju virusa na gospodarske sektore ili na druga područja
- ponude za ulaganja u "lijekove", cjepiva, čudotvordnu medicinu, proizvode za zaštitu
- "zanimljive" činjenice / snimke o bolesti
- "važne izjave" o "izvoru" virusa u kojima se ističe ljudska odgovornost iz određenih zemalja.

Konkretno, kod ove kampanje naslov e-pošte je *An important COVID-19 update for our community*, a pošiljatelj se lažno prikazuje ovisno o primatelju (WHO@domena-na-koju-se-šalje). Privitak se distribuira pod imenom je COVID-19.img.

Analizom je utvrđeno da se preuzimanjem gore spomenute .img datoteke na računalo s Windows operativnim sustavom sprema arhivirana zlonamjerna izvršna datoteka naziva "Chance.exe" koja pokreće podproces "RegAsm.exe" koji je "loader" za trojanski konj "Agent Tesla". Radi se o poznatoj vrsti trojanskog konja koji preuzima podatke iz računala i šalje ih napadaču.

Pozivamo vas na dodatan oprez kod otvaranja e-pošte od nepoznatih pošiljatelja, koristite antivirusne i anti-malware alate te molimo da prijavite policiji ako primijetite bilo kakve zlonamjerne on-line aktivnosti vezane uz COVID-19. Piše: koronavirus.hr

Detaljne informacije pročiajte na mup.gov.hr.
FOTO: ilustracija

This entry was posted on Thursday, March 19th, 2020 at 10:15 pm and is filed under Aktualno 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.