PASSTEAL kradljivac lozinki

Iz kompanije TrendMicro došlo je još jedno upozorenje o opasnom malveru koji prijeti pri korištenju web stranica za razmjenu datoteka. Radi se o malveru nazvanom PASSTEAL. To je alat koji se može naći prerušen u generatore ključeva za komercijalne programe ili neke popularne e-knjige. Kao što mu samo ime govori koristi različite tehnike kako bi se dočepao lozinki koje su sačuvane u web preglednicima.

Otkriveno je nekoliko varijanti PASSTEALA koje koriste taktike društvenog inženjeringa kao što je maskiranje malvera u generatore ključeva za komercijalne programe ili dolaze u paketu sa krivotvorenim instalerima komercijalnih aplikacija. Računa se na korisnike koji za preuzimanje i dijeljenje datoteka koriste BitTorrent ili posjećuju sajtove za djeljenje datoteka u potrazi za ilegalnim softverom.

Jedna od varijanti TSPY_PASSTEAL.B, koristi alate za oporavak lozinke „WebBrowserPassView“ i „PasswordFox“ za krađu lozinki iz web preglednika kao što su Google Chrome, Safari, IE i drugi.

PASSTEAL nije jedini razlog zbog kojeg bi trebalo biti oprezan pri preuzimanju datoteka sa stranica za dijeljenje datoteka, također on nije jedini takav softver. Jedan od sličniH malvera je ZACCESS koji se također nudi kao generator ključeva za aktiviranje ilegalnog softvera, igrica i slično. Takve malvere je vrlo teško ukloniti sa zaraženih sustava, a ZACCESS je jedan od vodećih po broju infekcija u ovoj godini.

Mnogi korisici vjeruju da će jedna lozika biti dovoljna za sve ako je dovoljno jaka i složenog karaktera. Takvo razmišljanje apsolutno nije dobro, te napominjem da svakako treba imati nekoliko lozinki za pristup različitim aplikacijama. Ista lozinka za pristup različitim web sajtovima ili aplikacijama lako se pamtli, ali istovremeno predstavlja golem sigurnosni rizik. Provaljivanjem te lozinke postajemo ranjivi na svim mjestima gdje ju koristimo, a to nikako ne želimo. Uz to, korisnici su često lijeni pa pristaju da im preglednici zapamte lozinke, kako ih ne bi morali utipkavati, što također olakšava krađu identiteta.

Izvorno priopćenje kompanije TrendMicro možete pročitati ovdje [1].

pon, 2012-11-26 07:48 - Ivan Sokač**Vijesti:** Sigurnost [2]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1147

Links
[1] http://blog.trendmicro.com/trendlabs-security-intelligence/passteal-sneaks-into-users-systems-via-file-sharing-sites/
[2] https://sysportal.carnet.hr/taxonomy/term/13