Unai Gorrotxategi

Giltzarrapoak behar direnean

Antibirusa hiltzera kondenatuta omen dago. Hori diote Symantec enpresaren arduradunek. Norton antibirusa garatzen duten enpresan argi dute. Ziber erasoek etengabeko bilakaera izan dute azken urteotan, eta, Symantec etxearen arabera, gaur egun antibirusak erasoen %45 geldiarazteko gai besterik ez dira. Hala ere, ezin da esan antibirusaren beharrik ez dagoenik. Windows sistemetan adibidez, gomendagarriak baino, beharrezkoak izaten dira.

Nork daki antibirusekin zer gertatuko den etorkizunean. Segurtasun enpresetan argi dagoen gauza bakarra da ezin direla geldirik geratu. Aste honetan adibidez, McAfee antibirusaren sortzaileak mezulari zerbitzu berri baten berri eman du. Telegram edo Whatsapp bezalako aplikazioen antzeko funtzioak izango lituzke. McAfee etxearen arabera, zerbitzu berri hau guztiz segurua da. Chadder zerbitzuaren bitartez idatzitako mezuak igorleek eta hartzaileek soilik irakur ditzakete, komunikazio segurua bermatuz.

Laster urtebete beteko da Edward Snowden AEBetako NSA Segurtasun Nazionalerako Agentziaren espioitza metodoak filtratzen hasi zenetik, eta orduz geroztik segurtasun informatikoa indartzen duten zerbitzu eta tresnak biderkatu egin dira. Alde batetik, hacktibista eta hacker komunitateek behar-beharrezkoa ikusi dutelako tresna eta zerbitzu berriak sortzea, Interneteko erabiltzaileon askatasunak bermatuta izan daitezen. Bestetik, kapitalak ere, NSArekin espioitza hitzarmen askotan kolaboratu duen arren, jendearen segurtasun nahia asetzeko ahaleginetan diru kopuru handiak inbertitu dituelako. Aurrera begira ere, gainera, kapitalak segurtasunean inbertitzen jarraitzeko asmoa duela dirudi.

Software libreaz hitz egiten dugunean, askotan nabarmentzen dugun ezaugarrietako bat da segurtasuna. Ez da seguruagoa garatzaileak azkarragoak direlako, softwarea bera edonork ikuskatu ahal duelako baizik. Erabiltzaile eta garatzaile komunitateen ikuskaritza eta hobekuntzei esker bilakatzen dira seguruagoak erabiltzen ditugun aplikazio, zerbitzu eta programak. Hacktibista eta hacker komunitateak ez dira software librea egiten duten bakarrak. Enpresa asko dira software librea garatuz edo software librearekin zerikusia duten zerbitzuak eskainiz dirua irabazten dutenak. Baina gaur egun erabiltzen diren zerbitzu fidagarrienak hacker komunitateek aurrera ateratakoak dira.

Snowden berak ere tresna eta zerbitzu hauek erabili zituen. Eskuartean zuen informazioaz jabetuta, Snowdenek bazekien ezin zituela egunero erabiltzen ditugun zerbitzuak erabili. Google, Microsoft, Yahoo, Apple... bezalako Interneteko zerbitzu emaile handienek espioitza hitzarmenak dituzte NSArekin. Bere ekintzak jarrai zitzaten saihesteko, ohikoak ez diren tresnak erabili zituen. Tails sistema eragileari esker, bere ordenagailuan ez zuen utzi berak egindako ekintzen arrastorik. USB bidez kargatzen den Linux banaketa horri esker, ordenagailuan egindako ekintza guztien arrastoak ordenagailua itzaltzearekin batera ezabatzen dira. Tor browser bezalako nabigatzaileekin ere, Interneten barrena anonimotasunez nabigatu ahal izan zuen. GPG bitartez bere filtrazioen fitxategiak zifratu ahal izan zituen. Posta erabiltzeko garaian ez nuen, noski, Gmail bezalako zerbitzurik erabili. Kontutan izan behar dugu Google berak aitortu duela bere zerbitzuaren bidez jaso eta bidaltzen ditugun mezuak irakurtzen dituela. Horren ordez, Lavabit zerbitzua erabili zuen. Auzia aireratu zenean Lavabit posta zerbitzua itxi behar izan zuten, FBI agentziarekin kolaboratzeko agindu judiziala jaso baitzuten.

Internet leku seguruago bat izan dadin zerbitzu eta tresna berriak hobetzen eta sortzen ari dira. Ekainaren 5erako, adibidez, Reset The Net ekimena aurkeztu dute. Snowdenen filtrazioen lehen urteurrenean pribatutasuna eta segurtasuna indartzeko ekintzak egitera deitu dute. Internet seguruago bat posible da eta behar-beharrezkoa dugu. •

Internet seguruago bat posible da eta behar-beharrezkoa dugu. GAUR8

3 BEGIRADA: osasuna /geltokiak / komunikazioa