ESET

Nasveti za neposredno sporočanje

..Sredi novembra je računalniški črv razvijalce pri Microsoftu prisilil, da so v programu Live Messenger 2009 začasno ukinili vse aktivne povezave. Neposredno sporočanje je zelo učinkovit način za širjenje nevarnih programov..

»Računalniški črvi, ki se širijo s programi za neposredno sporočanje, kot so Skype, Yahoo! Messenger in Microsoft Live Messenger, niso novost, zato je nedavna ukinitev aktivnih povezav v programu Live Messenger 2009 s strani Microsofta presenetljiva. Eden odtakšnih črvov, ki je bil med nevarnejšimi - AimVen, je bil odkrit že v letu 2003, ciljal pa je na uporabnike plaftorme za sporočanje America Online Instant Messenger," je dejal Pierre-Marc Bureau, raziskovalec pri programski hiši ESET, ki je na zadnji konferenci organizacije Virus Bulletin prejel nagrado za najboljšega novinca v protivirusni industiji.

"Princip širjenja takšnih računalniških črvov je preprost. Žrtev od svojih kontaktov najprej prejme sporočilo, ki vključuje povezavo. Ko uporabnik to povezavo odpre, se njegov računalnik okuži," je še dodal Bureau. Nekateri računalniški črvi obvladajo tudi zemljepisno lociranje in tako svoje žrtve nagovarjajo v domačem jeziku ali pa ga skušajo prepričati z navajanjem novic in dogodkov iz njegove bližine. Takšne napredne tehnike lahko ukanijo tudi najprevidnejše uporabnike.

Strokovnjaki iz ESETa nam ponujajo sedem zlatih pravil za varnejše neposredno sporočanje:

1. Nikoli ne odpirajte slik, ne prenašajte datotek in ne klikajte na povezave, ki jih prejmete od nekoga, ki ga ne poznate. Pred odpiranjem sumljivih datotek in povezav, ki jih prejmete od znancev, poskusite preveriti verodostojnost le-teh pri pošiljatelju.
2. Ne odgovarjajte na sporočila, ki jih ne pričakujete in prihajajo od oseb, ki jih ne poznate. Zavrnite vse zahteve in pozive, da bi med svoje kontakte dodali osebe, ki jih ne poznate.
3. Blokirajte vsa neželena sporočila, ki prihajajo od neznancev. Takšno filtriranje neželenih sporočil je veliko enostavnejše, kot se sliši, saj večina programov za neposredno sporočanje omogoča ustvarjanje takšnih seznamov.
4. V programih za neposredno sporočanje nikoli ne pošiljajte občutljivih informacij in osebnih podatkov. Izogibajte se izmenjavi podatkov o kreditnih karticah, različnih geslih ali osebnih podatkih, kot so telefonske številke, naslovi ali uporabniška imena v programih za neposredno sporočanje ter elektronski naslovi.
5. Geslo za dostop do vašega računa v programu za neposredno sporočanje naj bo kompleksno. Za dostop do različnih spletnih storitev – spletno bančništvo, spletne igre, forumi, e-pošta itn. – uporabljajte različna gesla. Kolikor uporabljate tudi javne računalnike ali spletne kavarne, ne pozabite onemogočiti možnosti samodejne prijave.
6. Ne dogovarjajte se za srečanja z neznanci, ki ste jih spoznali pri klepetanju s programi za neposredno sporočanje. Kolikor se za to odločite, na srečanje pripeljite še nekoga.
7. Takrat, ko spletne kamere na svojem računalniku ne uporabljate, jo onemogočite. Nekateri škodljivi programi kiberkriminalcem omogočajo snemanje video vsebine ali zajemanje slik.

Dejstvo je, da kiberkriminalci svoje tehnike za pretentanje uporabnikov v programih za neposredno sporočanje neprestano nadgrajujejo in izboljšujejo, zato ostanite previdni in nezaupljivi.

(P.R.)