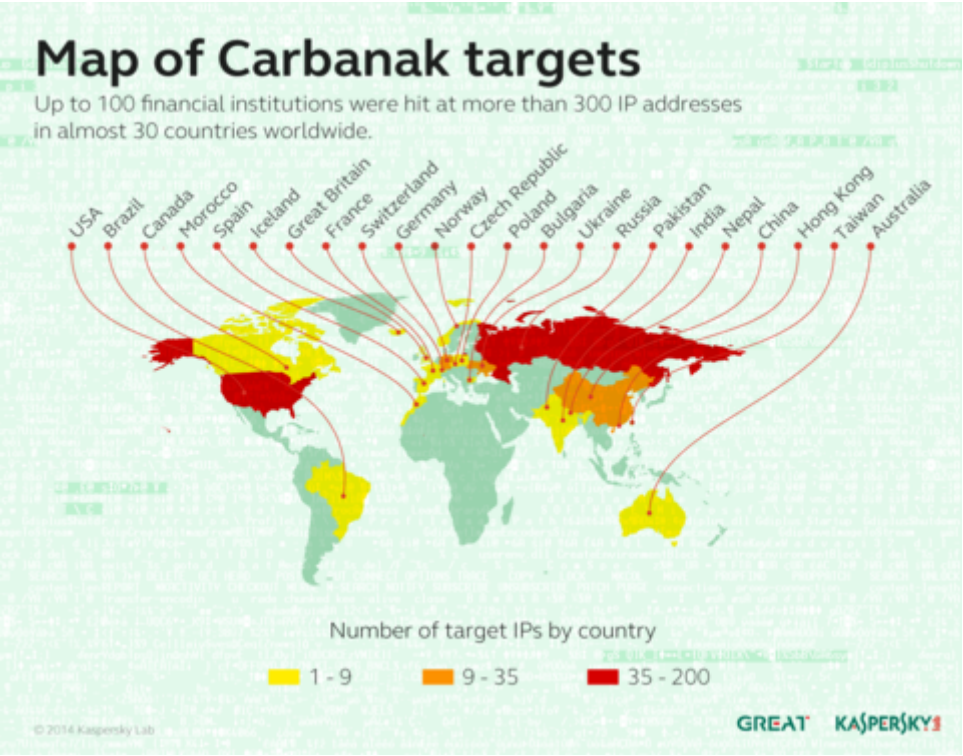
Miljard dollarit läinud - küberkurjategijad tühjendasid finantsasutusi

10 aastat tagasi - 18.02.2015 Autor: AM



Tänapäeva pangaröövlid ei pea nagu Bonnie & Clyde automaatidega pangahoonesse sööstma, et oma saak kätte saada. Kaspersky Labi, Europoli ja Interpoli ühise uurimise käigus avastati pretsedenditu küberkuritegevuslik operatsioon, mille käigus varastasid ründajad miljard USA dollarit.

Kübervargus kestis kaks aastat ja hõlmas umbes 100 finantsasutust üle maailma. Eksperdid oletavad, et selle suurvarguse taga on rahvusvaheline kuritegelik grupeering, millesse kuulub küberkurjategijaid Venemaalt, Ukrainast ja mitmest Euroopa riigist, aga ka Hiinast.

Kriminaalne rühmitus, mis sai nimeks Carbanak, kasutas suunatud rünnakutele iseloomulikke meetodeid. Erinevalt paljudest teistest juhtumitest tähistab see rööv siiski küberkuritegevuse uut etappi: nüüd on küberkurjategijad võimelised varastama juba otse pankadest, mitte ainult kasutajatelt.

Kübermaffia Carbanaki tegevus puudutas umbes 100 panka, maksesüsteemi ja muud finantsasutust ligi 30 riigis, sealhulgas USA, Venemaa, Saksamaa, Hiina,

Ukraina, Kanada, Hong Kong, Taivan, Rumeenia, Prantsusmaa, Hispaania, Norra, India, UK, Poola, Pakistan, Nepal, Maroko, Island, Iirimaa, Tšehhi, Šveits, Brasiilia, Bulgaaria ja Austraalia. Eestist ei näpatud seekord midagi.

Eksperdid selgitasid välja, et kõige suuremad summad varastati pangavõrku tehtud sissetungi käigus: iga sellise reidiga omastasid küberkurjategijad 10 miljonit dollarit. Keskmiselt kestis üks pangaröövv – alates ettevõtte võrgu esimese arvuti nakatamisest kuni raha varastamise ja tegevuse kokkutõmbamiseni – kaks kuni neli kuud.

Kuritegelik skeem algas andmepüügitehnika kaudu ettevõtte ühe töötaja arvutisse sisenemisest. Pärast arvuti pahavaraga nakatamist pääsesid kurjategijad ligi panga sisevõrgule, leidsid rahatehingute süsteemi administraatorite arvutid ja rakendasid nende ekraanidele videovalve. Sel viisil teadis Carbanaki rühmitus iga detaili pangatöötajate töös ja suutis imiteerida töötajate tavalisi tegevusi raha ülekandmisel petukontodele.

„Need pangaröövid erinevad ülejäänutest selle poolest, et küberkurjategijad kasutasid meetodeid, mis andsid neile sõltumatuse pangas kasutatavast tarkvarast, isegi kui see oli ainulaadne. Häkkerid ei pidanud isegi pangateenuseid lahti muukima. Nad sisenesid lihtsalt korporatsiooni võrku ja õppisid kuritegelikke tegevusi legaalseteks maskeerima. See on tõesti väga professionaalne rööv,” selgitab Kaspersky Labi juhtiv viirusetõrjeekspert Sergey Golovanov.

„Rünnakud on järjekordne kinnitus sellele, et ründajad kasutavad ära iga vähegi haavatava koha mis tahes süsteemis. Sellises olukorras ei saa üheski valdkonnas end täiesti turvaliselt tunda ja seetõttu tuleks kaitseküsimustele jätkuvalt tähelepanu pöörata.

Kuidas Carbanaki rühmitus raha varastas

1. Kui jõuti nii kaugele, et oli aeg raha välja võtta, kandsid küberkurjategijad internetipanga või maksesüsteemide kaudu raha panga kontodelt oma kontodele. Petukontod avati Hiina ja Ameerika pankades, aga eksperdid ei välista varastatud raha hoidmist ka muude riikide pankades.

2. Mõnel juhul tungisid ründajad raamatupidamissüsteemi ja suurendasid petutehingu abil konto saldot. Näiteks, kui kurjategijad said teada, et kontol hoiti tuhandet USA dollarit,

suurendasid nad saldot kümne tuhandeni ja kandsid seejärel üheksa tuhat oma kontole. Konto omanik ei kahtlustanud midagi, sest algselt kontol olnud tuhat dollarit oli seal ikka alles.

3. Küberkurjategijad said lisaks oma kontrolli alla sularahaautomaadid ja aktiveerisid määratud ajal sularaha väljavõtmise käske. Seejärel läks mõni rühmituse liige sularahaautomaadi juurde ja korjas raha kokku.

Kõik finantsasutused peaksid oma võrku tähelepanelikult Carbanaki pahavara suhtes skannima, soovitavad küberturvalisuse organisatsioonid. Pahavara avastamise korral on kõige parem pöörduda kohe õiguskaitseorganite poole.

- Uudised
- Turvalisus