Küberkurjategija välimääraja: 5 tüüpi, kes võivad sind netis rünnata

6 aastat tagasi - 17.02.2020 Autor: AM

Meie elu on kolinud suures osas Internetti ja sama on teinud ka kurjategijad. Väiksema mõjuga küberründed on muutunud juba nii igapäevasteks, et hakkavad uudisväärtust kaotama. IT haldus- ja juhtimisteenust pakkuva Iteraction OÜ IT teenuste juht Lauri Sinisaar toob välja viis küberkurjategija tüüpi ja avab, mis motiveerib neid uusi ründeskeeme välja mõtlema.

Eks peamine motivaator on muidugi raha. Tegemist on paljude jaoks tasuva ja õitsva äriga, mis võrreldes teiste kuritegevuse liikidega on üsna riskivaba. Bromiumi uuringute andmetel teenisid küberkurjategijad eelmisel aastal kokku üle 1,5 triljoni dollari aastas.

Tasub meelde tuletada, et triljon on miljon miljonit ehk 1 000 000 000 000 ehk 10^{12}. Personaalselt teenivad edukaimad 2 miljonit ja isegi juuniortaseme häkkerid üle 40 tuhande dollari aastas. Kui küberkuritegevus oleks riik, siis oleks see kõrgema sisemajanduse kogutoodanguga riikide seas 13. kohal.

Kuid vaatame nüüd erinevaid küberkurjategijate profiile lähemalt.

1. TÄNAVAKÜBERKURJATEGIJAD

Tänapäeva ründajad ei pruugi olla intelligentsed nohikud, kes end päevadeks keldrisse arvuti taha lukustavad. Nüüdisaegsete tehnoloogiate ja taristu abil on isegi piiratud oskustega kurjategija võimeline palju paha korda saatma. See tüüp panustab inimeste nõrkusele ja kasutab ära seda, mis on võimalikult väikese vaevaga saavutatav. Keegi õnnestub alati õnge otsa saada.

Näiteks 2019. aasta lõpus langes Eesti kodanik investeerimiskelmuse ohvriks. Ohvrit juhendati telefoni teel ning selle juhendamisega kandis ohver välismaisele kontole üle 500 000 euro.

Veel üks näide: postkasti saabub kiri Nigeeriast, milles teatatakse, et oled võitnud suure summa raha. Et see summa kätte saada, tuleb aga tasuda teenustasu X eurot asjaajamis- ja pangatasusid.

Kuid raha pole sugugi ainus ajend ja motivaator. Huvi pakuvad neile ka andmed, identiteedid ja juurdepääsud – kõik, mida saab müüa või vahetada muude teenuste vastu. Identiteedivargus on kasvav trend, kuna inimeste personaalsed andmed on digitaalsel kujul, need on kas avalikult kättesaadavad või kasutatakse andmeid ligipääsu saamiseks.

Sisselogimisinfo õngitsemine jõuab ohvrini enamasti e-kirjas olevate olevate veebilinkide kaudu, mis võivad välja näha väga tõetruud ja sarnased reaalsetele veebilehtedele (näiteks ohvri kodupank või Amazoni sisselogimisvorm). Levinud on ka e-kirjad justnagu Outlooki või Gmaili teenustelt sisuga, et teie postkasti maht on täis, palun vajutage siia, et juurdepääs säilitada vms. Identiteedivarguse puhul kasutatakse ohvri kohta kogutud teavet kas ohvri vastu näiteks raha välja petmiseks või edasistes rünnakutes.

Õngitsemine on väga levinud ka äris. Tuttava identiteediga postkasti potsatav kiri tundub usaldusväärne ja on suurem tõenäosus, et siis tehakse soovitud tegevus või klõpsatakse lingil või avatakse fail, mille õngitseja on saatnud. Lingi taga või failis aga peitub lunavara, pahavara või viirus. Näiteks kaaperdab ründaja kõigepealt raamatupidaja meilivestlused, seejärel varastab koostööpartneri identiteedi. Ühes kirjas palutakse juba raamatupidajal kohe maksta ära arve märkega, et koostööpartneri kontonumber on muutunud. Kiri ise näeb välja täpselt selline, nagu tavapäraselt ja saabub päev enne tavalist aega ja reaalset arvet.

Nüüd aga kujutage ette, et installite tarkvara ja äkki on kõik salvestatud failid krüptitud. See juhtub siis, kui teie arvuti on nakatunud lunavaraga. Oma andmed saate tagasi ainult lunaraha vastu, kui üldse.

Tervise- ja delikaatsete isikuandmete lekkeid toimub iga päev igal pool üle maailma. 2018. aastal krüpteeriti ühe Eesti perearstikeskuse infosüsteemid lunavaraga, mis häiris oluliselt patsientide vastuvõtmist. 2017. aasta mais aga nakatus "WannaCry" lunavaraviirusega rohkem kui 300 000 arvutit 150 riigis. Väljapressimistarkvara levis ainult tunni ajaga miljoneid kordi. Nakatunud olid muu hulgas ka näiteks Deutsche Bahni arvutid ja piletiautomaadid.

II AVALIKE TEENUSTE JA INSTITUTSIOONIDE RÜNDAJAD

Järgmine tase on organiseeritud ja ambitsioonikad kurjategijad, kes tegelevad ka tööstusspionaaži ja ulatuslike rünnakutega strateegilise infrastruktuuri, ettevõtete, valitsusasutuste, haiglate, pankade vastu. Nende eesmärk on tekitada (majanduslikku) kahju või luurata. Sellisel tasemel kurjategijate eesmärk on

varastada riikide ja kaubanduse tundlikku ning salastatud teavet, näiteks intellektuaalse omandiga seotud informatsiooni.

Näiteks 2010. aastal Iraani tuumarajatiste vastu loodud Stuxneti rünnak põhjustas Iraani tuumaprogrammi planeerimata häireid. Eksperdid arvavad, et Stuxneti sabotaažiprogrammi väljatöötamine läks maksma umbes 50 miljonit dollarit ja sellesse olid väga tõenäoliselt kaasatud ka riigiasutused.

III HAKTIVISTID

Haktivistid kasutavad arvutit protestivahendina poliitiliste või ideoloogiliste eesmärkide saavutamiseks. Nende rünnakud on suunatud kas valitsuse või ettevõtete vastu, kelle tegevus läheb vastuollu nende tõekspidamiste ja missiooniga. Haktivistid kasutavad oma eesmärkide saavutamiseks erinevaid tööriistu, nagu näiteks veebisaitide päringutega üleujutamist nii, et neid ei saa tundide või päevade jooksul külastada.

Näiteks on sellega tegelenud rahvusvaheline võrgustik *Anonymous*. Neil ei ole suuri juhte, kogukond tegutseb pigem ideede kui käskude järgi. 2014. aastal käivitas kogukond Islamiriigi ISISe vastu kübersõja, mille käigus avati, võeti üle või muudeti kasutamiskõlbmatuks hulk ISIS-e liikmete kontosid Twitteris ja Facebookis.

IV SISERINGI PAHALASED

Lohakad töötajad ei põhjusta ettevõttele meelega kahju, vaid on lihtsalt hooletud või ohtudest mitteteadlikud. Näiteks võivad töötajad kogemata kustutada faile või avada viirusega nakatunud faile. Kompromiteeritud töötajad on langenud ka näiteks õngitsuskirjade ohvriks.

Teadlikult pahatahtlikud siseringi pahalased võivad olla aga nii praegused kui endised töötajad või näiteks partnerid, kes võivad kuritarvitada oma juurdepääsu võrkudele, rakendustele ja andmebaasidele, et tahtlikult tekitada kahjustusi ja häireid ning tundlikke andmeid või intellektuaalomandit kustutada, muuta või varastada.

Näiteks 2015. aastal tuli avalikuks, et üks suure tervisekindlustust vahendava ettevõtte Anthem töötaja oli kuritarvitanud andmebaasi, mis sisaldas isiklikku teavet umbes 80 miljoni kliendi ja töötaja kohta.

V TEENUSEPAKKUJAST KÜBERKURJATEGIJA

Teenusepakkuja on kurjategija, kes ei ründa oma ohvrit otseselt, vaid pakub turule oma teadmisi, ressursse ja meetodeid, mille on teenusena välja töötanud: arendaja tuge, pahavara, rünnakute arvutusvõimsust (*Botnet*), anonüümseks muutmise ja hostimise teenuseid või kasutaja andmeid (krediitkaardiandmed, sisselogimisandmed, paroolid ja kehtivad e-posti aadressid).

Kasutades küberkuritegevust teenusena, võib ka IT maailmas kogenematu kurjategija ilma tehniliste oskusteta algatada keeruka rünnaku valitud sihtmärkide vastu.

Pilt

346252