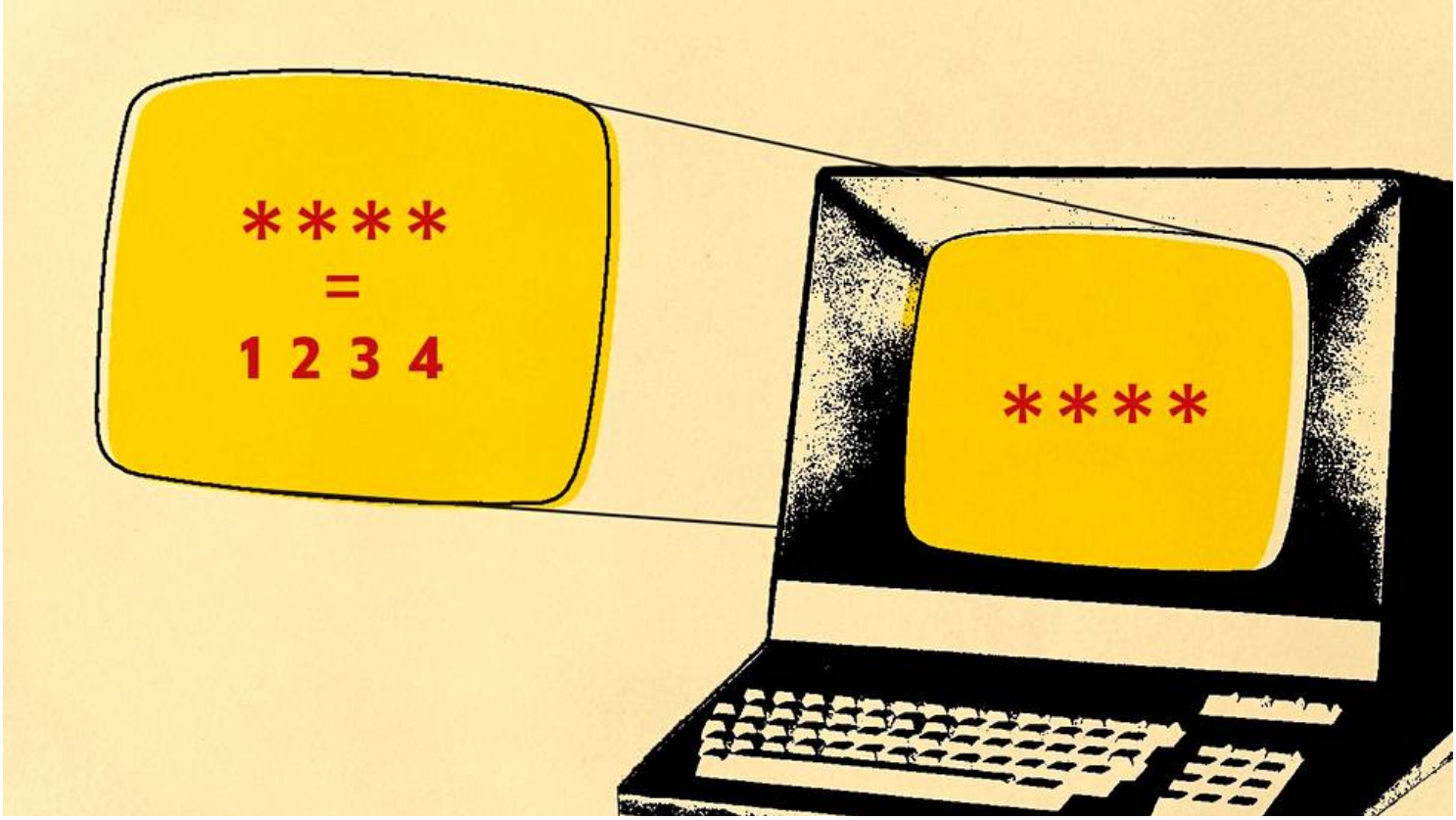
Teknologia

Näin salasanasi murretaan jopa muutamassa minuutissa – ja se on yllättävän helppoa, sanoo asiantuntija

Varastetut salasanalistat ovat nopeasti kauppatavaraa verkossa.



Verkkopalvelun salasanan on aina oltava pitkä, jotta se on vaikeasti murrettavissa. (KUVA: OLLI NURMINEN / HS)

Antti Tiainen HS

MIKÄ TAHANSA kahdeksan merkkiä pitkä tai sitä lyhyempi verkkopalvelun salasana on murrettavissa minuuteissa.

Se on tällä hetkellä tietoturva-alan yleinen totuus, koska nykytietokoneissa on niin valtavasti laskentatehoa.

Tässä artikkelissa kerrotaan, miten verkkopalveluiden salasanojen tekninen murtaminen käytännössä tapahtuu ja miksi pidemmät salasanat ovat niin paljon turvallisempia kuin lyhyemmät.

Juttua varten on haastateltu Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen tietoturva-asiantuntija **Perttu Halosta** sekä muita tietoturva-alan ammattilaisia.

Aiemmin HS on kertonut, miten salasanan sijaan voi luoda salalauseen, joka on nykyteknologialla käytännössä mahdoton murtaa.

MUTTA eikö salasanojen murtaminen vaadi sitä, että niitä pystyy kokeilemaan verkkopalveluiden kirjautumissivuilla rajattomasti?

Eihän sellainen onnistu, moni ihmettelee.

Paitsi että voi. Verkkopalveluissa on edelleen valitettavan usein kotikutoisia käyttöliittymiä ja tunnistustoteuksia, joissa moni salosanoja voi testata jopa rajattomasti, Halonen muistuttaa.

Mutta ihan tavallista se ei ole. Yleisemmin tilanne on se, että jos joku ulkopuolinen yrittää kirjautua käyttäjätilillesi ja syöttää salasanan useamman kerran väärin, verkkopalvelu rajoittaa kirjautumisyritysten määrää ja nopeutta tai lukitsee tilin.

Tällaisissa tapauksissa rikolliset yrittävät murtaa salasanoja suoraan verkkopalvelun kirjautumissivulla lähinnä silloin, kun he kokeilevat käyttäjän aiemmin nettiin vuotaneita salasanoja toisiin palveluihin.

Sen takia on tärkeää käyttää jokaisessa palvelussa eri salasanaa.

VARSINAINEN salasanojen tekninen murtaminen tapahtuu kuitenkin aivan toisella tavalla, niin sanottuna offline-hyökkäyksenä.

Se tapahtuu näin:

Kaikissa verkkopalveluissa, kuten sometileillä ja sähköpostiohjelmissa, salasanat on tallennettu palvelun tietokantaan.

Ennen salasanat oli tallennettu tietokantaan selväkielisinä. Jos salasana oli vaikkapa *Auto123*, se oli myös tietokannassa muodossa *Auto123*.

Silloin riitti, että rikolliset saivat tietokannan haltuunsa. Sen jälkeen he pystyivät kirjautumaan käyttäjätileille vaikka saman tien.

”Viimeisen kymmenen vuoden aikana verkkopalveluiden ohjelmointikirjastot ovat parantuneet niin, että ohjelmistokehittäjän ei yleensä tarvitse vaivata päätään sillä, miten käyttäjän tunnistaminen salasanalla ja salasanojen tallentaminen palveluun toteutetaan turvallisesti. Pikemminkin vaatii erityistä vaivannäköä toteuttaa ne jollakin kotikutoisella ja turvattomalla tavalla.”

Nykyään salasanat on siis tavallisesti salattu. Rikollisille ei silloin riitä pelkästään se, että he saavat salasanatietokannan haltuunsa. Sen jälkeen heidän pitää pystyä vielä murtamaan se.

Tosin esimerkiksi viime keväänä Liiketoimintasuunnitelma.com-verkkopalvelusta varastettiin laajassa tietomurrossa noin 130 000 käyttäjätunnusta ja salasanaa, jotka oli tallennettu selväkielisinä.

YMPÄRI nettiä tapahtuu jatkuvasti erikokoisia tietovuotoja, joissa rikolliset saavat verkkopalveluiden salasanoja haltuunsa.

”Se on helposti automatisoitavaa toimintaa. Rikolliset yrittävät käyttää tunnettuja ohjelmistohaavoittuvuuksia hyväkseen päästäkseen palveluiden tietokantoihin.”

Halosen mukaan alamaailma toimii verkossa kuin pienoisyhteiskunta. Sillä on suorastaan oma ekosysteeminsä.

”Ei luottokorttitietojen perässä oleva rikollinen todennäköisesti tee itse tietomurtoja salasanatietokantoihin, vaan palkaa toisen rikollisen tekemään sen. Tai ostaa murroissa saatuja tietoja pimeästä verkosta.”

KUN rikollisilla on salasanatietokanta kopioituna itselleen, ne voivat aloittaa salasanojen murtamisen.

”Silloin ei ole enää mitään rajoituksia millä tavalla voi yrittää erilaisia käyttäjätunnus ja salasana -yhdistelmiä.”

Nykyään salasanat on yleensä tallennettu niin sanottuina tiivisteinä. Niitä voi luoda monilla erilaisilla tiivistealgoritmeilla, jolloin sanasana käytännössä salakirjoitetaan uudelleen. Tiivisteinä olevia salasanoja ei pysty palauttamaan alkuperäiseen selväkieliseen muotoonsa.

”Salasanojen selvittämisen pystyy tekemään niin, että ottaa selväkielisen salasanan ja salaa sen samalla menetelmällä kuin tietokannan salasanat on salakirjoitettu. Sitten jos saa saman lopputuloksen, niin tietää, että kyseinen salasana kelpaa kyseiselle käyttäjätilille.”

KÄYTÄNNÖSSÄ tämä tarkoittaa, että rikollisten ohjelmistot raksuttavat läpi erilaisia vaihtoehtoja salasanoiksi siihen asti, kunnes tärppää.

Tämän takia myös kehitetään jatkuvasti uusia tiivistealgoritmeja, joissa tiivisteen laskeminen kuluttaa mahdollisimman paljon laskentatehoa tietokoneiden prosessoreilta ja muisteilta tai molemmilta.

”Aina kun jotain suojausta kehitetään, aina jollakulla on myös intressi kehittää työkalu, jolla siitä suojauksesta pääsee läpi. Täydellistä suojausta ei ole olemassakaan”, Halonen sanoo.

LISÄKSI tiivisteitä suojataan usein ”suolalla”. Kun tiivisteet on suolattu, tietokannasta voi paljastaa vain yhden salasanan kerrallaan.

Eli vaikka tilinomistaja A:lla ja tilinomistaja B:llä olisi molemmilla samassa verkkopalvelussa salasanana *2xKoira*, rikolliset eivät saa selville tiliomistaja B:n salasanaa, vaikka he olisivat saaneet jo selville A:n salasanan.

Tämä on mahdollista, koska ”suolauksessa” salasanan eteen lisätään sattumanvaraisia merkkejä ennen kuin siitä tehdään tiiviste.

”Kahdella eri käyttäjällä on silloin salasanoissaan eri tiivistearvo, vaikka itse salasanat olisivat samat. Tämä hidastaa merkittävästi hyökkääjien toimintaa, koska he eivät voi tehdä oikopolkuja murtamisessa.”

MAHDOLLISIMMAN suurta laskentatehoa rikolliset hankkivat tyypillisesti kolmella eri tavalla. Niitä

kaikkia käytetään myös kryptovaluuttojen louhimiseen.

1) Näytönohjaimet. Salasanatietokantojen murtaminen on äärimmäisen tehokasta nykyisillä näytönohjaimilla.

”Näytönohjaimilta vaaditaan korkeaa laskentatehoa ja niille pystytään tekemään ohjelmia, jotka kokeilevat parhaimmillaan valtavia määriä eri vaihtoehtoja sekunnissa.”

2) Pilvipalvelut. Laskentatehoa saa runsaasti myös pilvipalveluista, joita rikolliset voivat ostaa esimerkiksi varastetuilla luottokorttitiedoilla tai murtaumilla muiden käyttäjien pilvipalvelutileihin.

3) Bottiverkot. Rikolliset voivat hakea laskentatehoa myös bottiverkolla, jossa on yhdistetty toisiinsa useita kaapattuja tietokoneita.

”Kuka tahansa vähänkin enemmän tekniikasta ymmärtävä voi murtaa salasanoja hyvin helposti ja kustannustehokkaasti. Siihen ei tarvita tiedustelupalveluiden supertietokoneita tai muita agenttitarinoita”, tiivistää eräs pitkään alalla työskennellyt tietoturva-asiantuntija.

Usein käyttäjätunnukset ja salasanat päätyvät rikollisille kuitenkin tietojenkalastelun yhteydessä, jolloin käyttäjä itse tulee huijatuksi ja antaneensa vahingossa tietonsa.

Lue lisää: Sähköposti näytti aidolta, ja siksi niin moni suomalainen työntekijä menee lankaan – Näin tunnistat rikollisten kalasteluyritykset, joita tulee nyt jatkuvalla syötöllä

RIKOLLISTEN salasanojen murtamiseen käyttämät ohjelmistot perustuvat nykyään tavallisesti kahteen eri menetelmään ja niiden erilaisiin yhdistelmiin.

1) Sanakirjahyökkäys

SANAKIRJAHYÖKKÄYKSESSÄ automatiikka käy salasanojen tiivisteitä läpi hyödyntämällä esimerkiksi sanakirjoja, sanalistoja ja aiemmissa tietomurroissa selvinneiden kymmenien miljoonien erilaisten salasanojen listoja.

Sanakirjahyökkäyksessä automatiikka löytää perusmuodossa olevia sanoja ja niiden yhdistelmiä.

Lisäksi se kokeilee sanojen kanssa tyypillisesti esimerkiksi erilaisia numeroita ja osaa huomioida ihmisten yleisesti käyttämät kikat, kuten I-kirjaimen korvaamisen 1:llä ja A-kirjaimen numerolla 4.

Automatiikka voi tunnistaa myös valtavan kirjon tunnettuja sanontoja ja fraaseja tai kokeilla läpi vaikka tunnettujen kirjojen kaikki lauseet erilaisina yhdistelminä.

Sanakirjahyökkäyksiä kehitetään koko ajan monipuolisemmiksi. Ne ovat usein erittäin tehokkaita siksi, että ihmiset ovat huonoja keksimään aidosti sattumanvaraisia salasanoja, vaikka itse muuta kuvittelisivatkin.

2) Väsytysmenetelmä

VÄSYTYSMENETELMÄSSÄ eli brute-force-hyökkäyksessä salasanoja käydään läpi merkki merkiltä.

KAIKISTA tärkeintä on tehdä salasanasta pitkä.

Tästä artikkelista löytyy alempaa grafiikka, joka havainnollistaa asian. Se näyttää, kuinka paljon erilaisia salasanayhdistelmiä voi olla, kun salasana on 4, 8, 15 tai 20 merkkiä pitkä ja siihen on käytetty numeroita sekä latinalaisia aakkosia, jotka kaikki verkkopalvelut hyväksyvät salasanojen merkeiksi.

Latinalaisissa aakkosissa on 26 kirjainta (suomenkielisissä aakkosissa on lisäksi kirjaimet å, ä ja ö) eli yhteensä 52 erilaista merkkiä, kun käytössä ovat sekä isot että pienet kirjaimet.

Numeroista tulee kymmenen erilaista merkkiä (0–9). Alla olevassa grafiikassa käytetyissä esimerkeissä on siis kyse salasanoista, joissa voi olla yhteensä 62 erilaista merkkiä.

Määrän saisi vielä isommaksi käyttämällä myös erikoismerkkejä sekä kaikkia suomalaisten aakkosten kirjaimia.

Juttu jatkuu grafiikan jälkeen.

PALATAAN lopuksi jutun alussa mainittuun kahdeksan merkkiä pitkään salasanaan.

Sellainen voisi hyvin olla tallennettu esimerkiksi salasanatietokantaan, joka on suojattu MD5-tiivistealgoritmilla.

MD5-tiivistealgoritmi on laajasti käytössä salasanatietokantojen suojaamisessa.

Jos salasanan murtajat ovat hankkineet käyttöönsä vaikkapa Amazonin pilvipalvelusta ”yhden virtuaalikoneen” laskentatehoksi, he pystyvät oikeanlaisella ohjelmistolla murtamaan jopa noin 450 miljardia MD5-tiivistettä sekunnissa.

Eli automatiikka on käynyt läpi 8-merkkisen salasanan kaikki mahdolliset vaihtoehdot runsaassa 8

minuutissa. Samalla se tarkoittaa, että salasana murtuu keskimäärin vain runsaassa 4 minuutissa.

SEN SIJAAN 15-merkkisen salasanan kaikkien vaihtoehtojen läpi käymiseen samalla laskentateholla kuluisi teoriassa yli 50 miljoonaa vuotta.

”Näin pitkästä ja aidosti sattumanvaraisesta salasanasta tulee niin monimutkainen, ettei sitä saa missään järjellisessä ajassa käytyä lävitse.”

Eikä rikollisten tavoite yleensä olekaan yrittää murtaa kaikkia tietokannan salasanoja, Halonen uskoo.

”Isosta joukosta käyttäjätilejä löytyy aina heikkoja salasanoja. Se riittää rikollisille.”

Askarruttaako teknologia? Lähetä teknologia-aiheinen kysymys, ja HS:n teknologiatoimitus etsii siihen vastauksen. Se onnistuu alla olevalla lomakkeella tai sähköpostilla osoitteeseen teknologia@hs.fi.

Kysely

Mihin teknologia-aiheiseen kysymykseen haluais teknologiatoimitus etsii vastauksen? *

Kysymykset voivat liittyä esimerkiksi tietokoneisiin, internetiin, sovelluk

Lähetä kysymyksesi

Oikaisu 9.1. kello 14.48: Jutun grafiikassa oli alun perin tieto, että kun käytössä 62 erilaista merkkiä, niin 20 merkkiä pitkästä salasanasta voi muodostua hiukan yli 70 tuhatta kvintiljoonaa erilaista vaihtoehtoa. Vaihtoehtoja on hiukan yli 700 tuhatta kvintiljoonaa.