STONESOFT

Lehdistötiedote

Stonesoft: Tietoturvauhat vuonna 2011

Helsinki, 12. tammikuuta 2011 - Alkuvuosi on aikaa, jolloin yritysjohto keskittyy kertaamaan edellisen vuoden tapahtumia ja ennustamaan, mitä tuleva vuosi tuo tullessaan. Tietoturva-ala ei ole tästä poikkeus. Moni tietoturvatoimittaja keskittyy listaamaan menneen vuoden merkittävimpiä uhkia. Verkkotietoturvayhtiö Stonesoft suuntaa katseensa tulevaisuuteen ja arvioi, minkälaisiin uhkiin yritysten tulisi vuonna 2011 varautua.

“Kuten kaikkina muinakin vuosina, tulemme varmasti näkemään monenlaisia odottamattomia yllätyksiä tietoturvan saralla”, Stonesoftin tietoturvapäällikkö **Joona Airamo** sanoo. ”Vuoden 2010 kantavia teemoja olivat ehdottomasti Stuxnet, sosiaalinen tiedustelu (engl. Social Engineering) sekä kehittyneet evaasiotekniikat, ja uskon, että tämän vuoden uhat tulevat pyörimään hyvin pitkälti näiden samojen teemojen ympärillä”, Airamo jatkaa.

Stonesoftilla on yli 20 vuoden kokemus tietoturvasta. Yhtiön näkemys alkaneen vuoden merkittävimmistä tietoturvauhista on seuraava.

1. Mitä laajemmalle Apple OS -käyttöjärjestelmä leviää, sitä todennäköisemmin tulemme näkemään madon tai viruksen, joka on kohdistettu juuri siihen.

2. Sosiaalisen median kuten Facebookin ja Twitterin kautta leviävien haittaohjelmien määrä tulee varmasti kasvamaan. Yksittäinen hyökkäys voi vaikuttaa tuhansiin tai jopa miljooniin ihmisiin. Hakkerit tulevat hyödyntämään haittaohjelmia, jotka kopioivat käyttäjän osoitekirjan tai ystävälistan ja lähettävät sitten saastuneen sähköpostin tai tiedoston kaikille osoitekirjasta löytyneille. Ja aivan kuten vanhoissa sähköpostimadoissa, saastunut tiedosto näyttää siltä kuin se olisi lähetetty aidolta lähettäjältä, joten vastaanottaja ei aavista tulevansa huijatuksi.

3. Näemme enemmän ohjelmistosodankäyntiin liittyviä hyökkäyksiä valtioita kohtaan. Hyökkäyksien motiivit ovat yhä useammin poliittisia, vaikka taloudelliset motiivit tulevatkin säilymään selkeästi hallitsevina.

4. Kohdistettu sosiaalinen tiedustelu (engl. targeted social engineering) yleistyy entisestään. Taitavat hakkerit tekevät yhä perusteellisempaa pohjatyötä kohdentaessaan hyökkäyksiä yritysverkkoon taloudellisen hyödyn saavuttamiseksi. Ihminen on aina ollut tietoturvan heikoin lenkki ja on toivottavaa, että yritykset alkaisivat panostaa yhä enemmän henkilöstön koulutukseen,

5. Myös Stuxnetin kaltaiset hyökkäykset lisääntyvät. Näiden kohteena ovat kriittiset infrastruktuurit kuten valtioiden tai puolustusvoimien järjestelmät. Hyökkäykset ovat silti edelleen melko harvinaisia, sillä tarvittavan mittakaavan viruksen rakentaminen vaatii hakkereilta paljon osaamista ja resursseja. Neljän ns.

STONESOFT

nollapäivähyökkäyksen lisäksi Stuxnet hyödynsi samaa tietoturva-aukkoa, jota Conficker-mato hyödynsi vuonna 2008. Viruksen monimutkaisuus ja kehityskustannukset viittaavat siihen, että sen suunnittelua on tukenut jokin valtiollinen taho.

6. Älypuhelimiin kohdistuvat hyökkäykset yleistyvät merkittävästi. Myytyjen älypuhelinten määrä vuonna 2011 tulee olemaan lähellä myytyjen PC-tietokoneiden määrää.

7. Hakkerit tulevat käyttämään yhä kattavampaa valikoimaa keinoja virusten levittämiseen. He pyrkivät parantamaan investointiensa tuottoa ja varmistamaan, ettei yksikään haavoittuvuus jää käyttämättä, hyödyntäen jokaisen päivittämättömien tietoturvaohjelmien tarjoaman mahdollisuuden.

8. Yksittäisten uusien haavoittuvuuksien määrä tuskin kasvaa vuonna 2011 merkittävästi, mutta keinot joilla hyökkäyksiä voidaan toteuttaa ja toimittaa kohteeseen kehittyvät ja tehostuvat. On rikollisille edullisempaa voida käyttää kaikkia olemassa olevia haavoittuvuuksia uudelleen, yhdistää niitä ja sitten toteuttaa hyökkäys menetelmällä, jota nykyinen tietoturvalaite ei tunnista eikä pysty estämään. Esimerkkinä tästä kehityksestä ovat Stonesoftin löytämät kehittyneet evaasiotekniikat (AET, Advanced Evasion Techniques). Uhkaavinta evaasioissa on se, että vaikka kohteessa olisi riittävä suoja yksittäisiä haittaohjelmia tai viruksia vastaan, se voidaan ohittaa uusien hyökkäysmenetelmien kuten kehittyneiden evaasiotekniikoiden avulla. . Evaasioita vastaan taistellessa olisikin ensiarvoisen tärkeää, että kaikki tunkeutumisen havainnointi- ja estolaitteiden valmistajat yhdistäisivät voimavaransa. Vain näin kyetään puolustautumaan näitä uusia hyökkäysmetodeja vastaan.

Lisätietoa suojautumisesta yllä mainittuja uhkia vastaan löytyy osoitteesta www.stonesoft.com tai ottamalla yhteyttä tietoturvatoimittajaasi.

Lisätietoja:
Joona Airamo
Tietoturvapäällikkö
Stonesoft Oyj
Puh. (09) 476 711
Sähköposti: joona.airamo(AT)stonesoft.com

Stonesoft Oyj

Stonesoft Oyj (NASDAQ OMX: SFTIV) on innovatiivinen integroitujen verkkotietoturvaratkaisujen toimittaja, joka on keskittynyt hajautettujen organisaatioiden tiedonkulun turvaamiseen. Asiakkaidemme liiketoiminta edellyttää vaativaa verkkoturvallisuutta ja sovellusten luotettavaa saatavuutta.

StoneGate(TM) on tietoturvaratkaisu, jossa yhdistyvät palomuuri, VPN, IPS (tunkeutumisen havainnointi- ja estojärjestelmä) sekä turvallisen etäkäytön mahdollistava SSL VPN. Ratkaisu yhdistää verkkotietoturvan, jatkuvan saatavuuden

sekä palkitun kuormantasausteknologian yhtenäiseksi, keskitetysti hallittavaksi järjestelmäksi. StoneGate-tietoturvaratkaisu tarjoaa alhaiset käyttökustannukset, erinomaisen suorituskyvyn ja tehostaa verkko-investointien tuottavuutta. Virtuaalinen StoneGate-tietoturvaratkaisu suojaa verkkoa ja takaa liiketoiminnan jatkuvuuden sekä virtuaali- että fyysisessä ympäristössä.

StoneGate Management Center -hallinnan avulla StoneGate-palomuuria, VPN-, IPS-, sekä SSL VPN -ratkaisua voidaan hallita keskitetysti. StoneGate-palomuuri ja hyökkäyksen havainnointi- ja estojärjestelmä toimivat saumattomasti yhdessä muodostaen koko yritysverkon kattavan kehittyneen kerroksellisen puolustuksen. StoneGate SSL VPN tarjoaa tehokkaan suojan mobiili- ja etäkäytön tarpeisiin.

Vuonna 1990 perustettu Stonesoft Oyj on maailmanlaajuisesti toimiva yhtiö, jonka pääkonttori on Helsingissä ja Amerikan alueen pääkonttori Atlantassa, Georgiassa. Lisätietoa osoitteesta www.stonesoft.com, www.antievasion.com ja http://stoneblog.stonesoft.com/.