STONESOFT

Lehdistötiedote

Näin suojaat kriittisen tietopääomasi uusilta, kehittyneiltä evaasiotekniikoilta

Helsinki, 24. maaliskuuta 2011 - Tietoturvatoimittaja Stonesoft havaitsi kehittyneet evaasiotekniikat (Advanced Evasions, AE-tekniikat) viime vuonna. Löydöksen jälkeen on vahvistunut, että AE-tekniikat ovat vakavasti otettava, kehittyvä ja dynaaminen uhka organisaatioiden kriittiselle tietopääomalle ja järjestelmille. Nyt Stonesoft neuvoo, kuinka organisaatiot voivat parhaiten suojautua tältä uhalta.

Stonesoftin löytämät kehittyneet evaasiotekniikat (AE-tekniikat) ovat täysin uudenlainen uhka, koska ne pystyvät ohittamaan suurimman osan organisaatioiden nykyisistä tietoturvajärjestelmistä. Heti löydettyään uhan viime vuonna, Stonesoft lähetti 23 ensimmäistä näytettä Suomen kansalliselle tietoturvaviranomaiselle CERT-FI:lle ja tiedotti aiheesta laajasti. Tämän jälkeen Stonesoft on löytänyt ja toimittanut CERT-FI:lle nauhoitukset 124 uudesta kehittyneestä evaasiotekniikasta. Nyt vaikuttaakin siltä, että kehittyneiden evaasiotekniikoiden määrälle ei näy loppua.

“Kaikilla palveluilla on huolto- tai päivitysajankohtansa, ja organisaatiot käyttävät tunkeutumisen havainnointi- ja esto- eli IPS-järjestelmiä suojaamaan liiketoimintansa kannalta kriittistä tietopääomaansa myös päivitysten välissä. Tämä koskee myös teollisuuden käytössä olevia ns. SCADA-verkkoja, joihin viime vuonna paljon huomiota herättänyt Stuxnet-mato iski. Kehittyneet evaasiotekniikat pystyvät ohittamaan IPS-suojauksen ja suorittamaan hyökkäyksen IPS-järjestelmän sitä havaitsematta. Tämä tarkoittaa sitä, että järjestelmä on haavoittuvainen koko ajan”, kertoo Stonesoftin kehitysjohtaja Klaus Majewski. ”Suojatakseen tietonsa AE-tekniikoilta, organisaatioiden tulee toimia ennakoivasti, kyseenalaistaa olemassa olevat tietoturvajärjestelmät ja harkita vaihtoehtoja uutta uhkaa vastaan. Verkkotietoturvan kenttä on muuttunut pysyvästi, eivätkä vanhat toimintatavat enää päde.”

Seuraavien kuuden vinkin avulla organisaatiot voivat parantaa tietoturvansa tasoa merkittävästi:

1. **Päivitä tietoturvaosaamisesi ja perehdy** kehittyneisiin evaasiotekniikoihin. Ne eroavat perinteisistä evaasioista monella tavalla. On tärkeää ymmärtää, että evaasiotekniikat eivät itsessään ole hyökkäyksiä, vaan tapoja viedä hyökkäys tai tietoturvauhka haavoittuvaan kohteeseen palomuurin tai tunkeutumisen havainnointi- ja estojärjestelmän sitä havaitsematta. Sataprosenttista suojaa kehittyneitä evaasiotekniikoita vastaan ei siis ole. Riskin minimoimiseksi yritysten tulisi käyttää verkkotietoturvaratkaisuja, jotka päivittyvät jatkuvasti ja kykenevät seuraamaan verkkoliikennettä kaikilla eri protokollatasoilla.

2. **Kartoita riskit.** Tarkasta organisaatiosi kriittinen infrastruktuuri ja järjestelmät ja analysoi, mitkä ovat merkittävimmät tietopääomat, miten ja mihin ne on tällä hetkellä varastoitu ja onko tiedoista varmuuskopiot. Priorisoi. Aloita varmistamalla, että kaikkein tärkeimmät tiedot ja julkiset palvelut on suojattu parhaiten.

STONESOFT

3. **Tarkista tietoturvapäivitykset.** Huolehtimalla siitä, että kaikki käytössä olevat järjestelmät on asianmukaisesti päivitetty, varmistat, että ne on myös suojattu parhaalla mahdollisella tavalla. Evaasiot voivat auttaa hyökkääjää läpäisemään tunkeutumisen havainnointi- ja estojärjestelmän tai palomuurin, mutta ne eivät auta hyökkääjää tunkeutumaan järjestelmään, jonka päivitykset ovat ajan tasalla. Järjestelmien päivittäminen ja paikkaaminen vie kuitenkin aikaa, joten asianmukaisesta tietoturvasta huolehtiminen on aina paras vaihtoehto.

4. **Arvioi tunkeutumisen havainnointi- ja estojärjestelmäsi uudelleen.** Arvioi tällä hetkellä käytössäsi olevan tunkeutumisen havainnointi- ja estojärjestelmän kyky suojata kehittyneiltä evaasiotekniikoilta. Ole kriittinen, proaktiivinen ja punnitse eri vaihtoehtoja. Kehittyneet evaasiotekniikat ovat muuttaneet tietoturvaa pysyvästi, joten tietoturvaratkaisu, joka ei osaa käsitellä evaasioita, on käytännössä hyödytön – riippumatta siitä, kuinka monta palkintoa se on saanut tai kuinka tehokas se on muilta ominaisuuksiltaan.

5. **Arvioi tietoturvasi hallinta uudelleen.** Keskitetty hallinta tuo merkittävää lisäarvoa tietoturvaan, erityisesti kehittyneitä evaasiotekniikoita vastaan puolustautuessa. Sen avulla voit automatisoida tärkeät päivitykset ja määritellä ohjelmistopäivitykset tietojärjestelmäsi laitteisiin nopeasti ja vaivattomasti. Näin varmistat, että järjestelmilläsi ja laitteillasi on aina paras mahdollinen suoja kehittyneitä evaasiotekniikoita vastaan.

6. **Kyseenalaista testitulokset.** Monet tietoturvavalmistajat tietävät kyllä miten puolustautua silloin, kun käytetään ennalta tunnettuja evaasioita testilaboratorioympäristössä. Samat uhat saattavat kuitenkin käyttäytyä hyvin eri tavoin oikeassa dynaamisessa ympäristössä, jolloin järjestelmät eivät enää tunnista niitä samalla tavalla. Kysy tietoturvavalmistajaltasi, miten voit testata itse omassa ympäristössäsi, että tärkeimmät tietosi on suojattu kehittyneiltä evaasiotekniikoilta.

Lisätietoja kehittyneistä evaasiotekniikoista sekä niiltä suojautumisesta löytyy osoitteesta www.antievasion.com.

Lisätietoja:
Klaus Majewski, kehitysjohtaja
Stonesoft Oyj
Puh. 358 40 824 7908
Sähköposti: klaus.majewski(AT)stonesoft.com

Stonesoft Oyj

Stonesoft Oyj (NASDAQ OMX: SFT1V) on innovatiivinen integroitujen verkkotietoturvaratkaisujen toimittaja, joka on keskittynyt hajautettujen organisaatioiden tiedonkulun turvaamiseen. Asiakkaidemme liiketoiminta edellyttää vaativaa verkkoturvallisuutta ja sovellusten luotettavaa saatavuutta.

STONESOFT

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