STONESOFT

Lehdistötiedote

Ensimmäiset tekniset kuvaukset Stonesoftin löytämistä evaasiotekniikoista

Tietoturvavalmistajilla ollut puoli vuotta aikaa päivittää järjestelmänsä 23 kehittynyttä evaasiotekniikkaa vastaan

Helsinki, 16. joulukuuta 2010 - Tietoturvayhtiö Stonesoft julkisti eilen tekniset kuvaukset ensimmäisistä kehittyneistä evaasiotekniikoista (Advanced Evasion Techniques, AE-tekniikat). Nauhoitukset 23 evaasiomenetelmästä kuvauksineen toimitettiin CERT-FI:lle toukokuussa, syyskuussa ja lokakuussa 2010. Prosessin mukaisesti tietoturvavalmistajilla on ollut kuusi kuukautta aikaa päivittää järjestelmänsä. Tekniset kuvaukset kaikista 23 evaasiotekniikasta ovat nähtävillä osoitteessa http://www.antievasion.com/principles/principles/part-3 **.**

Annettuaan tietoturvayhtiöille kuusi kuukautta aikaa reagoida löydettyihin uusiin uhkiin, CERT-FI julkaisi aiheesta uuden haavoittuvuustiedotteen eilen. Tiedotteen mukaan vain muutama yhtiö on toistaiseksi antanut CERT-FI:lle vastauksen aiheesta.

“Toivoimme tietysti, että valmistajat olisivat reagoineet aiheeseen laajemmin. Jos heidän ratkaisunsa eivät tarjoa suojaa kehittyneitä evaasioita vastaan, heidän olisi prosessin mukaan pitänyt raportoida, miten ja millä aikataululla he päivittävät ne”, Stonesoftin operatiivinen johtaja **Juha Kivikoski** sanoo.

“Näyttää siltä, että useimmissa tapauksissa tarjottu “korjaus” on vain tapa estää epäilyttävältä vaikuttava liikenne tiettyjen näytteistä löytyneiden,evaasioiden käyttöön viittaavien parametrien perusteella. Tämä ei kuitenkaan tarjoa todellista suojaa muuttuvia evaasioita vastaan,” Stonesoftin tekninen johtaja **Mika Jalava** tarkentaa. ”Oikea tapa olisi protokollan tulkitseminen ja normalisointi ennen sen tarkistamista. Pelkästään evaasioiden etsiminen verkkoliikenteestä ei riitä, koska niitä on helppo muokata yksinkertaisen tunnistamisen välttämiseksi. Tällainen havainnointi aiheuttaa myös helposti virheellisiä löydöksiä, koska monet evaasioina käytettävät tekniikat ovat nykystandardien mukaan sallittuja verkkoliikenteen ominaisuuksia. Pelkkä evaasioiden havaitseminen ja niitä sisältävän liikenteen estäminen ei riitä myöskään sen vuoksi, että tällöin ei saada tietoa varsinaisista hyökkäyksistä.”

Estääkseen kehittyneiden evaasiotekniikoiden avulla piilotetut hyökkäykset, tietoturvajärjestelmien olisi ymmärrettävä ja osattava lukea verkkoprotokollia samalla tavalla kuin niitä käyttävät tietokoneet. Kun evaasiot kehittyvät, myös tietoturvaratkaisujen on kehityttävä. Pitkällä tähtäimellä Stonesoft suosittelee ohjelmoijia, suunnittelijoita ja Internetin standardoinnista vastaavia tahoja vähentämään verkkoprotokollien monitulkinnallisuutta. Nykyiset verkko-ongelmat liittyvät yhä useammin tietoturvaan sen sijaan, että ongelmana olisi yhteensopimattomuus vanhentuneiden järjestelmien kanssa. Erityisesti evaasioihin liittyvät haasteet ovat usein lähtöisin protokollien vääränlaisesta toteutuksesta. Tietoturvan tulisikin olla osa protokollasuunnittelua ja standardoimista sen sijaan, että se lisätään jälkikäteen muuten jo valmiiksi rakennettuun järjestelmään.

Uusia kehittyneitä evaasiotekniikoita löydetty

Stonesoft jatkaa kehittyneiden evaasiotekniikoiden tutkimista yhteistyössä CERT-Fi:n kanssa. Aiemmin julkaistujen 23 esimerkin lisäksi näytteitä on löydetty jo lisää ja ne ovat toiminnoiltaan yhä monipuolisempia. Osa uusista evaasioista perustuu useiden tekniikoiden yhdistämiseen.

Stonesoft olettaa haavoittuvuuskoordinoinnin uusien löydösten osalta kestävän pidempään kuin aiemmin niiden monimutkaisuudesta johtuen. Uusia näytteitä ei ole vielä testattu yhdelläkään julkisesti saatavilla olevilla testityökalulla, eikä niitä siten ole myöskään lisätty tämän hetkisiin testauskriteereihin.

“Jatkamme edelleen tutkimustyötämme säilyttääksemme etumatkan verkkorikollisiin ja auttaaksemme organisaatioita suojelemaan tietopääomaansa evaasioita vastaan”, Kivikoski sanoo. ”Kehittyneet evaasiotekniikat ovat todistettavasti uusi haaste tunkeutumisen havainnointi- ja estolaitteille, eikä tietoturva-alalla ole enää varaa vaieta niistä.”

CERT-FI haavoittuvuustiedote:
http://www.cert.fi/haavoittuvuudet/2010/haavoittuvuus-2010-153.html

Tekniset kuvaukset 23 evaasiotekniikasta löytyvät osoitteesta
http://www.antievasion.com/principles/principles/part-3.

Lisätietoja:
Stonesoft Oyj
Juha Kivikoski, operatiivinen johtaja
Puh. 040 518 0999
Sähköposti: juha.kivikoski(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/.