STONESOFT

Lehdistötiedote

Uusi uhka vaarantaa tietojärjestelmät maailmanlaajuisesti

Verkkoturvajärjestelmät voimattomia kehittyneiden evaasiotekniikoiden edessä

Helsinki 18. lokakuuta 2010 - Verkkotietoturvayhtiö Stonesoft on löytänyt uuden tietoturvauhkakategorian; kehittyneet evaasiotekniikat. Nämä uudenlaiset tekniikat pystyvät läpäisemään lähes kaikki olemassa olevat tietoturvajärjestelmät ennennäkemättömällä tavalla, ja muodostavat siten vakavan uhan yritysten tietojärjestelmille maailmanlaajuisesti. Stonesoft on raportoinut uudesta uhasta CERT-FI:lle haavoittuvuuskoordinoinnin käynnistämistä varten. Yhdysvaltalainen tutkimuslaboratorio ICSA Labs on vahvistanut löydöksen vakavuuden.

Stonesoftin tutkimat ja raportoimat uudet kehittyneet evaasiotekniikat (Advanced Evasion Techniques, AE-tekniikat) pystyvät läpäisemään nykyiset verkkoturvajärjestelmät jälkiä jättämättä. AE-tekniikat voivat kuljettaa järjestelmiin erilaisia hyökkäyksiä, kuten haitta- ja vakoiluohjelmia tai matoja ja viruksia, jotka yksin olisivat tietoturvajärjestelmien havaittavissa ja torjuttavissa. Tästä syystä AE-tekniikat antavat tietomurtoihin ja hakkerointiin erikoistuneille rikollisille tehokkaan ”yleisavaimen” , jonka avulla nämä voivat murtautua järjestelmiin ja tietoihin. Näkymättömyyden ansiosta evaasiotekniikoiden käyttö antaa myös enemmän aikaa ja mahdollisuuksia löytää toimiva hyökkäys kohdejärjestelmän haavoittuvuuteen, joten hyöty rikollisille on merkittävä.

Stonesoftin asiantuntijat havaitsivat uuden uhkakategorian tutkimuslaboratoriossaan Helsingissä, testatessaan yhtiön omaa verkon tietoturvaratkaisua verkkohyökkäyksiä vastaan. Myöhemmin testausta laajennettiin kattamaan myös muiden valmistajien johtavat ratkaisut. Näytteitä löydetyistä AE-tekniikoista lähetettiin edelleen tutkittaviksi Suomen CERT-FI:lle sekä yhdysvaltalaiselle ICSA Labsille, joka on maailman johtavien tietoturvatoimittajien tuotteiden riippumattomaan testaukseen ja sertifiointiin erikoistunut yritys. ICSA Labs on vahvistanut löydöksen merkittävyyden sekä sen, että AE-tekniikat ovat vakavasti otettava uhka. CERT-FI koordinoi haavoittuvuuksien korjausta tietoturvatuotteiden valmistajien kesken. CERT-FI julkaisi haavoittuvuuksista lausunnon 4.10. ja päivittää sitä tänään 18.10.

"Stonesoftin löytämät haavoittuvuudet vaikuttavat useisiin sisällöntarkistustekniikan toteutuksiin. Jatkuva yhteistyö CERT-FI:n, Stonesoftin ja muiden verkkolaitevalmistajien kesken on tärkeää, jotta löydetyt haavoittuvuudet saadaan korjattua. CERT-FI:n roolina on tukea tätä prosessia", CERT-FI:n haavoittuvuuskoordinoinnin vastuuhenkilö Jussi Eronen kertoo.

“Olemme testanneet Stonesoftin löydökset ja vahvistamme, että kyse on uudenlaisesta tavasta ohittaa olemassa olevat verkkotietoturvaratkaisut”, ICSA Labsin detection and prevention program manager **Jack Walsh** sanoo. ”Yritysten tietojärjestelmät ovat todella vaarassa, jos ohjelmistojen haavoittuvuuksia lähdetään hyödyntämään AE-tekniikoiden avulla.”

Testeistä saadut tulokset ja data osoittavat, että suurin osa nykyisistä verkkoturvaratkaisuista ei tunnista AE-tekniikkaa hyödyntäviä hyökkäyksiä ja epäonnistuu siksi niiden pysäyttämisessä. Tehokkain keino

suojautua tältä jatkuvasti kehittyvältä uhalta ovat joustavat ohjelmistopohjaiset järjestelmät, jotka ovat etäpäivitettäviä, keskitetysti hallittavissa ja joihin on päivitetty kyky tunnistaa ja torjua myös kehittyneet evaasiotekniikat. Suurin osa maailmalla tällä hetkellä käytetyistä järjestelmistä on kuitenkin staattisia ja laitepohjaisia, ja niiden päivittäminen AE-tekniikoita vastaan on erittäin hankalaa ja aikaavievää, tai jopa mahdotonta.

“Tämä on valitettavasti vasta alkua”, Stonesoftin operatiivinen johtaja Juha Kivikoski sanoo. ”Uskomme, että dynaamisen ja arvaamattoman muotonsa vuoksi AE-tekniikat tulevat mullistamaan koko verkon tietoturvan. Tietoturvatoimittajat käyvät jo nyt jatkuvaa kilpajuoksua yhä kehittyviä uhkia vastaan ja olemme vakuuttuneita, että tässä kisassa vain dynaamiset ohjelmistopohjaiset ratkaisut voivat selviytyä voittajina.”

StoneGate -verkkotietoturvaratkaisut tarjoavat tällä hetkellä kattavimman suojan uusia AE-tekniikoita vastaan. Keskitetyn hallinnan kautta ratkaisun kaikki komponentit ovat dynaamisesti ja automaattisesti päivitettävissä.

Lisätietoja kehittyneistä evaasiotekniikoista löytyy osoitteesta www.antievasion.com

CERTin lausunto AE-tekniikoista on luettavissa osoitteessa
http://www.cert.fi/haavoittuvuudet/2010/haavoittuvuus-2010-153.html

Lisää tietoa Stonesoftin StoneGate -verkkotietoturvaratkaisuista osoitteessa www.stonesoft.com

Seuraa aihetta: http://twitter.com/anti_evasion

Lisätietoja:
Stonesoft Oyj
Heli Harri, markkinointi- ja viestintäpäällikkö
Puh. 040 718 4799
Sähköposti: heli.harri@stonesoft.com

SEK Public Oy
Henrietta Malmari, viestintäkonsultti
Puh. 040 575 5646
Sähköposti: henrietta.malmari@sekpublic.fi

CERT-FI:n haavoittuvuuskoordinoinnin tavoittaa seuraavasti:

Sähköposti: vulncoord@ficora.fi
Mainitkaa otsikossa tapaustunniste [FICORA #385726]

Puh. 09 6966 510 Arkisin kello 8.00-16.00
Fax. 09 6966 515

Postiosoite:

Viestintävirasto/CERT-FI

CERT-FI
PL 313
00181 Helsinki

Lisätkää postiosoitteeseen sana haavoittuvuuskoordinointi.

CERT-FI suosittelee PGP- tai SMIME-salauksen käyttöä haavoittuvuuskoordinointiasioita käsiteltäessä. Avaimistomme löytyvät osoitteesta:
https://www.cert.fi/palvelut/yhteystiedot/rooliavaimet.html

CERT-FI:n haavoittuvuuskoordinoinnin periaatteet ovat luettavissa osoitteesta:
https://www.cert.fi/en/activities/Vulncoord/vulncoord-policy.html.

ICSA Labs:

Brianna Carroll Boyle, Public Relations Manager, Verizon and ICSA Labs
Puh. +1 703-859-4251
Sähköposti: brianna.boyle@verizon.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 ja http://stoneblog.stonesoft.com/.