

11.10.2007

CERT-FI

INFORMATIONSSÄKERHETSÖVERSIKT 3/2007

E-post har använts i avsevärd grad för att sprida skadliga program som används för att bilda botnet-nätverk. Storm Worm har blivit ett av de mest spridda skadliga programmen därför att det har spridits aktivt via skräppostmeddelanden.

CERT-FI har fått kännedom om riktade attacker mot företag där skadliga program som antivirusprogram inte känner igen har smittat datasystem i företagets interna nät. Skadliga program kan utnyttjas till exempel för att få uppgifter från systemen om företagets affärsverksamhet. Det är svårare att upptäcka riktade attacker än skadliga program som allmänt sprids i e-postmeddelanden.

Fortfarande hittades flera sårbarheter i mjukvara. Under tredje kvartalet publicerade CERT-FI 60 meddelanden om allvarliga sårbarheter i mjukvara och 26 artiklar under Tietoturva nyt! (Informationssäkerhet nu!). Några varningar publicerades inte.

Storm Worm sprids via e-post

Det skadliga programmet Storm Worm upptäcktes första gången i januari 2007 och det sprids via e-postbilagor och www-sidor. Under sommaren och hösten har det gått många skräppostmeddelanden som innehåller en länk till en webbplats som sprider Storm Worm. Storm Worm är för tillfället ett av de mest spridda skadliga programmen. CERT-FI har dock inte fått veta om något större antal smittade datorer i finländska nät.

Infekterade datorer blir en del av ett väldigt omfattande nätverk av Storm Worm-botnet. Nätverket, som de angripna datorerna bildar, får sina kommandon genom en effektivt decentraliserad mekanism som liknar peer-to-peer-nät, utan någon enskild och centraliserad kommandoserver. Enligt CERT-FI:s uppgifter används Storm Worm-botnet aktivt bl.a. för blockeringsattacker och skräppost.

Spridning av Storm Worm baserar sig främst på aktuella händelser på engelska eller frågor som annars väcker människors intresse och som det hänvisas till i e-postmeddelandena. Då kan det hända att läsarna följer givna länkar eller öppnar bilagor som innehåller det skadliga programmet. När Storm Worm smittar en dator installerar det samtidigt en rootkit-funktion som gör att det blir svårt att upptäcka det.

Storm Worm utnyttjar inte själv någon särskild sårbarhet i mjukvara utan de som läser meddelandena lockas att installera det på sina arbetsstationer genom att klicka på länkar som innehåller det skadliga programmet. Www-sidor som sprider det skadliga programmet försöker dock utnyttja kända sårbarheter i webbläsare. Då kan det skadliga programmet installeras i datorn utan att användaren märker det. Regelbundna uppdateringar av mjukvaran är viktiga när man vill minska sannolikheten för att datorn blir smittad omärkbart.

Malicious Software Removal Tool för Microsoft Windows är ett verktyg som känner igen Storm Worm och tar bort de flesta versionerna.

11.10.2007

CERT-FI

Riktade attacker mot företag

Blockeringsattacker mot olika företags www-sidor har fått mycket publicitet i media. Förutom blockeringsattacker kan även riktade attacker äventyra företagens informationssäkerhet. Riktade attacker försöker smitta skadliga program i företagets datasystem. Syftet med det kan vara till exempel att man vill skaffa uppgifter om företagets affärsverksamhet med hjälp av spionprogram. CERT-FI har fått veta om fall där finländska företag har varit mål för attacker.

Syftet med en riktad attack är att komma åt ett visst företags eller en organisations system. I attacken kan man använda ett skadligt program som har programmerats just för detta ändamål och som antivirusprogram inte känner igen. Sådana varianter av skadliga program kan även köpas via internet. I stället för att distribuera ett skadligt program via en stor mängd e-postmeddelanden som lätt kan kännas igen som skräppost, sänds meddelandena i liten grad till en noggrant utvald grupp av mottagare. Angriparen strävar efter att agerandet inte upptäcks och att några motåtgärder inte vidtas.

Skadliga program som används för attacken sänds oftast i ett dokument som bifogats till ett e-postmeddelande och som utnyttjar en känd sårbarhet i kontorsmjukvara. Till skillnad från massdistribuerade e-postmeddelanden har innehållet i meddelandet och adresserna valts omsorgsfullt så att även företagets egna medarbetare kan ha det svårt att upptäcka någonting dubiöst. Meddelandet kan gälla aktuella ärenden i företagets affärsverksamhet och det kan även vara sänt på företagets interna e-postlista.

Att upptäcka och avvärja riktade attacker kan vara utmanande, därför att automatiska antivirusprogram inte nödvändigtvis upptäcker dem. Både skadliga program och metoder som används för att smitta dem är i allmänhet skickligt valda. Risken för att datorn blir smittad blir mindre om man lagar kända sårbarheter och installerar tillverkarens uppdateringar i mjukvara. Elektronisk underskrift av meddelanden i företagets interna kommunikation skulle hjälpa att säkerställa sändarens identitet, men det används sällan.

Antalet sårbarheter i mjukvara fortfarande stort

Sårbarheter i mjukvara som hänför sig till operativsystemets komponenter, kontorsprogram och läsarprogram gäller en mängd användare av arbetsstationer. De utnyttjas oftast även för spridning av skadliga program och för kapning av datorer i syfte att få dem fungera som slavdatorer för botnet. Sårbarheter hittades också i snabbmeddelandetillämpningar och mediaspelare.

En del av sårbarheterna i webbläsare har samband med läsarnas plugin-utvidgningar. Då kan samma sårbarhet gälla flera olika mjukvaror.

För servrar är det värt att i synnerhet notera sårbarheterna i programmeringsspråket PHP och publikationssystem som genomförts med PHP, för de kan möjliggöra olovlig bearbetning av www-sidorna. Angripna www-servrar används generellt för spridning av skadliga program och för bluffsidorna utan att den som upprätthåller servern märker det. Sårbarheter hittades igen i flera informationssäkerhetsprodukter, t.ex. i antivirusprogram.

11.10.2007

CERT-FI

Åska orsakade störningar i kommunikationsnät

Den 22 augusti 2007 drog en åskfront över Finland och orsakade stora problem för kommunikationstjänster. På området som blev under åskfronten förekom en hel del störningar i funktionen av basstationer för mobiltelefoner. Åskan orsakade problem även för funktionen av det fasta telefnätet och bredbandsförbindelser. Avbrott i Radio Suomis sändningar i Nyland medförde även att möjligheten att sända myndighets- och nödmeddelanden i huvudstadsregionen avbröts för en stund. Störningarna avhjälpes dock ganska snabbt.

Skräppost överbelastade e-postservrar

Enligt CERT-FI:s uppgifter har finländska operatörers e-postservrar ibland varit överbelastade på grund av en stor mängd skräppost. Belastningen har tidvis fördröjt förmedlingen av meddelandena. Situationen har dock hållits under kontroll. Andra kortvariga problem i e-posttjänster har föränletts av fel i utrustning och ändringar i routning.

Omfattande störning i Skype

Skype är en mjukvara för internettelefoni som baserar sig på peer-to-peer-teknik. Användarna av Skype kan tala och kommunicera med varandra på internet utan samtalsavgift. Skype-tjänsten drabbades av en omfattande störning i mitten av augusti. Störningen började efter att Microsoft hade publicerat sina månatliga uppdateringar för mjukvara. Enligt Skype orsakades störningen av ett fel i mjukvara som ledde till att systemet blev överbelastat när talrika datorer försedda med Windows-operativsystemet försökte logga in igen efter en omstart. Störningar i att logga in i Skype pågick i flera dagar.

Blockeringsattack också mot CERT-FI:s www-server

Kommunikationsverkets www-sidor blev mål för en blockeringsattack under det sista veckoslutet i september. Därför var Kommunikationsverkets sidor, såsom www.cert.fi och www.ficora.fi inte tillgängliga för en stund.

Framtidsutsikter

Det är sannolikt att det blir flera blockeringsattacker som utnyttjar botnet. Dessutom ser det ut som om aktörer som förfogar över nätverk som används för attack också försvarar sig aktivt mot dem som undersöker deras verksamhet. Vissa attacker har drag som syftar till att attackerna är en hämnd mot dem som undersöker nätverkens funktion och struktur.

CERT-FI har bara fått veta om några få styrdatorer för botnet i finländska nät. Däremot har det hittats flera finländska användares datorer som angripits och anslutits till botnet. Sådana datorer har kopplats bort från nätet i samarbete med leverantörer av internetjänster.

Olika webbspel, till och med avgiftsbelagda spel, har ökat i popularitet och därför är det skäl att ta därtill relaterade sårbarheter och missbruk i beaktande. Oftast gäller det att skaffa användaridentifikation och lösenord till spelen.