

INFORMATIONSSÄKERHETSÖVERSIKT 2/2007

Blockeringsattacker som upptäcktes under årets första kvartal fortsatte också under slutet av våren. Attacker mot statliga tjänster i Estland och Rundradions tjänster i Finland fick stora rubriker i maj. Metoder och mål för de undersökta blockeringsattackerna avvek från varandra och på basis av tillgängliga uppgifter fanns det inte något direkt samband mellan händelserna.

Under andra kvartalet publicerade CERT-FI 39 meddelanden om sårbarheter i mjukvara och 35 artiklar under Tietoturva nyt! (Informationssäkerhet nu!). Några varningar publicerades inte.

Det skadliga programmet Allapple, som fungerar och sprider sig självständigt, har redan ett års tid infekterat datorer och orsakat störningar i trafiken i en finländsk www-server. Attackens inverknings avvärs nu med ett program som levereras i samband med Windows-uppdateringarna.

Attacker mot statliga och bankers system i Estland

Blockeringsattackerna väckte stora rubriker när attackerarna försökte lamslå estländska myndigheters webbtjänster, särskilt www-sidor. Dessutom utsattes bankernas och nyhetstjänsternas servrar för attacker. Attackerna, som pågick i flera veckor, började i slutet av april vid ett bråk kring en bronsstaty som föreställer en rysk soldat.

I Estland avvärsdes attackerna först genom att begränsa all inkommande trafik från länder utanför Estland, vilket blockerade majoriteten av den belastande trafiken. Senare användes filtrering på basis av IP-adresser och innehållet i förbindelserna.

Synliga blockeringsattacker även i Finland

I maj blev CERT-FI också informerad om blockeringsattacker mot finländska tjänster. Måndagen den 14 maj blev Rundradions www-server utsatt för en riktad blockeringsattack som upprepades samma kväll. Attacken fortsatte följande dag vilket gjorde att www.yle.fi-sidorna fungerade långsamt eller inte alls. Attacken avvärsdes först genom att blockera tillträdet till tjänsten från utomlands. Senare började man analysera innehållet i inkommande paket och på basis av denna information avskiljde man störande trafik från normala förbindelser. I attacken mot Rundradion styrdes begäran om förbindelser från mer än hundra tusen olika IP-adresser för att belasta servern. Begäran gällde P2P-fildelningsprogram.

Måndagen den 14 maj informerades även om en attack mot Eniros suomi24.fi-sidor; attacken syntes i form av avbrott i och långsammare funktion av tjänsten. Enligt den information som CERT-FI fick genomfördes attacken på ett annat sätt än mot Rundradion. Servrar som var mål för attacken finns i Sverige. Attacken upprepades måndagen den 21 maj.

Syftet med blockeringsattacker är att servern som är målet för attacken överbelastas så att normal användning inte är möjlig. Attackerna utförs oftast antingen med skadliga program som sprider sig och fungerar självständigt eller med hjälp av botnät. Attacken mot Rundradion utnyttjade dock brister i säkerheten hos fildelningsprogram som fungerar i ett P2P-nätverk.

3.7.2007

CERT-FI

Publicitet medförde onödiga anmälningar

Nyheter om samtidiga blockeringsattacker ledde till fel slutsatser även när det gällde vanliga avbrott, eftersom tjänsterna och deras funktion var under exceptionellt noggrann tillsyn. CERT-FI fick inte veta om särskild många händelser som kan klassificeras som blockeringsattacker.

I slutet av maj publicerades två meddelanden om blockeringsattacker och hur man förbereder sig för dem. Dessutom höll CERT-FI en presskonferens om blockeringsattacker den 22 maj och publicerade en extra informations säkerhetsöversikt 1B/2007.

Ett steg framåt vid avvärjande av Allaple

Sedan juli 2006 har ett skadligt program Allaple spridit sig i informationsnäten. Programmets enda syfte är att hindra vissa webbtjänsters funktion. Ett av målen befinner sig i ett finländskt nät. Efter att Allaple har släppts ut försöker det drabba nya datorer och stör sina mål självständigt utan någon kommando- eller styrförbindelse. Att kommandoförbindelsen saknas betyder också att trafik som den spridande masken orsakar inte längre kan stoppas. Problemet elimineras först när alla infekterade datorer har kopplats bort från nätet och programmet slutar sprida sig.

För att lindra de skadliga effekterna av programmet har Microsoft tillagt Allaples kännetecken i verktyget som tar bort skadlig programvara. Windows-verktyget Malicious Software Removal Tool, som känner igen och tar bort Allaple, distribueras vid automatiska uppdateringar. CERT-FI följer effekterna av åtgärderna - hittills har störande trafik inte minskat avsevärt.

Spionprogram känner till flera tusen nätbanker

Användarna av bankernas webbtjänster utsätts ibland för bedrägeriförsök där kundens dator smittas av ett spionprogram. Spionprogrammet kan ta över användarnamn, lösenord och andra uppgifter. Det finns även program som kan ta över användarens nätbanksförbindelse så att attackeraren matar in uppgifter i tjänsten utan att användaren upptäcker det.

Antalet banktjänster som skadliga program känner till ökar hela tiden. De allmänna spionprogrammen fungerar med flera tusen olika nätbankstjänster, bland dem finns också finländska banker. Enligt CERT-FI:s uppgifter har finländska bankers tjänster inte varit utsatta för sådana missbruk som skulle kräva att användarna utöver normal försiktighet måste vidta vidare åtgärder.

Spionprogram sprids systematiskt antingen som filbilagor till spam eller som länkar till www-sidor som innehåller ett skadligt program. Datorn smittas av ett skadligt program i allmänhet när användaren klickar på länken med webbläsaren. Skadliga program kan även utnyttja sådana okorrigerade sårbarheter i operativsystemet eller tillämpningar som möjliggör att datorn drabbas utan några åtgärder från användarens sida.

På sistone har man fått veta om ett särskilt program som är avsett för spridning av skadliga program och saluförs via internet. Med MPack är det lätt att utnyttja många olika sårbarheter för spridningen av skadliga program genom www-sidor som syns vara harmlösa. Den som sprider det skadliga programmet installerar programmet på en angripen www-server och det startas när man bläddrar i sidorna. Programmet försöker smitta användarens dator genom att utnyttja flera olika sårbarheter. Datorn kan bli infekterad på grund av en enda sårbarhet som inte har korrigerats.

3.7.2007

CERT-FI

Antalet sårbarheter lika stort som vanligt

De flesta sårbarheterna i programvara gällde program som används i arbetsstationer. I slutet av mars offentliggjordes en Windows-sårbarhet som hänför sig till hantering av animerade markörer (musens pekare). Någon korrigeringskod var inte tillgänglig omedelbart. Sårbarheten gällde flera Windows-versioner, även den nya Windows Vista, och det var lätt att utnyttja den genom en webbsida eller ett e-postmeddelande. Microsoft publicerade en korrigeringskod snabbare än normalt genast i början av april. Flera andra sårbarheter i Windows och Office korrigerades också.

Det upptäcktes många sårbarheter i informationssäkerhetsrelaterade produkter, såsom antivirusprogram och brandväggar. Korrigeringskod publicerades även i fråga om Mozilla Seamonkey, Firefox och Thunderbird.

CERT-FI fick veta om flera www-sidor som hade blivit angripna på grund av sårbarheter i PHP-programmeringsspråket.

Fel och störningar

Under påsktiden den 6 - 8 april 2007 var det ett avbrott i TeliaSoneras e-posttjänst; avbrottet berodde på ett tekniskt fel. Som störst inverkade felet på 400 000 e-postkunder, och 200 000 kunders förbindelser var utsatta för hela den tid som felsituationen pågick.

Det förekom några fel i stamnätets transmissionssystem vilka orsakade kortvariga avbrott i bredbandstjänster, fasta telefontjänster och mobiltjänster. I stamnätet orsakade jordbyggnadsarbeten några kabelavbrott som på vissa områden hindrade telefon- och datatrafik.

På vissa regioner har det förekommit avbrott i det markbundna digitala tv-nätets och analoga tv-nätets sändningar. Avbrotten har orsakats av störningar i tv-sändare. Den största störningen hände i Joutseno den 26 - 27 maj 2007. Det gällde ett sändarfel som förorsakades av ett blixtnedslag i sändarmasten.

Framtidsutsikter

Elektroniska tjänster för uträttande av ärenden har visat sig vara lätta mål för attacker, och det är sannolikt att blockeringsattacker eller intrångsförsök i system förekommer även i fortsättningen. Fel i tjänster som tillhandahålls via internet är under ständig och noggrann tillsyn även i media, vilket gör att de är mycket lockande mål när man vill få publicitet.

I Finland har man hittat inte bara angripna datorer eller datorer som kan göra attack utan också kommandoservrar som används för styrning av botnät i attackerna. Det verkar som om förberedelserna för attack i Finland inte hittills har gjorts professionellt utan det handlar om unga människor som har en hel del angripna datorer till sitt förfogande och som vill få publicitet. Botnät kan dock i brottsligt agerande användas systematiskt för att få ekonomisk nytta eller för att sprida propaganda.