



3.4.2006



Lägesrapport 1/2006

I slutet av kvartalet blev hotnivån högre på grund av sårbarheter som upptäcktes i webbläsarprogramvaror. Sårbarheterna utnyttjades också effektivt genom att till exempel installera skadliga botnet-program i hemdatorer. En modern webbläsarprogramvara utgör en mycket komplicerad och omfattande helhet som redan på grund av storleken på dess programkod är utsatt för programmeringsfel. Som vanligaste enstaka användargränssnittet för tillämpningar är webbläsare föremål för aktiv sårbarhetsundersökning och utveckling av skadliga program.

Serien av phishing-bedrägerier som riktade sig mot Nordeas nätbankskunder fortsatte även i januari, men efter den har några motsvarande försök inte rapporterats. Globalt sett är phishing-bedrägerier ett fenomen som fortfarande utvecklas.

Under kvartalet publicerades tre betydande uppdateringar för Apples Mac OS X-operativsystem för att förbättra dess informationssäkerhet. Första exempel på skadliga program som utnyttjar sårbarheterna i Apple-miljön har redan rapporterats. Upprätthållande av informationssäkerheten för Mac OS X-operativsystemet kräver kontinuerlig uppdatering i likhet med andra operativsystem.

Sårbarheter i programvaror

En egenskap hos Windows Metafile-bildformatets (WMF) behandling som kan utnyttjas skadligt aktiverade skrivare av skadliga program vid årsskiftet. De första skadliga programmen som utnyttjade sårbarheten spreds innan programtillverkaren hade hunnit publicera en programkorrigering. Sårbarheten gällde alla versioner av Windows-operativsystemet. Nya skadliga program som är avsedda för att utnyttja WMF-sårbarheten skrivs fortfarande även om det har funnits en programkorrigering tillgå sedan början av året. Uppenbarligen finns det fortfarande ett stort antal ouppdaterade och därmed sårbara operativsystem kopplade till nätverket Internet.

En webbläsarprogramvara är det vanligaste användargränssnittet för Internet-tjänster. Ofta används samma webbläsarprogramvara också som användargränssnittet för ett företags interna tjänster. Speciellt skadliga är sådana sårbarheter i en webbläsarprogramvara som gör det möjligt för attackeraren att köra sin egen programkod. Typiskt räcker det att man besöker en webbplats, som har skapats med syfte att skada, med en sårbar webbläsarprogramvara för att sårbarheten utnyttjas. I slutet av mars upptäcktes fyra sårbarheter i Internet Explorer-webbläsaren. En av dessa utnyttjades omedelbart genom att placera skadlig programkod på hundratals webbplatser. Vid publiceringen av denna rapport hade en korrigeringsuppdatering för sårbarheterna ännu inte kommit ut.

Apple publicerade tre betydande uppdateringar för Mac OS X-operativsystemet för att förbättra dess informationssäkerhet. I Apples webbläsarprogramvara Safari och e-postprogramvara Mail upptäcktes sårbarheter som var lätta att utnyttja. Uppenbarligen håller Apple som datasystemmiljö på att visa sig vara intressantare för dem som skriver skadliga program och undersöker sårbarheter än tidigare.



3.4.2006

CERT-FI

Phishing-bedrägerier

Med phishing avses inhämtande av elektroniska identiteter (användaridentifikationer, personuppgifter) som hör till användare av nättjänster. Attackerna genomförs vanligen genom att vädja till användarens godtrogenhet och hjälpsamhet. Genom att kapa en annan persons elektroniska identitet försöker attackerare få ekonomisk nytta.

Phishing-bedrägerier som riktade sig mot Nordeas nätbankskunder fortsatte i januari. Denna serie av bedrägerier var hittills den största serien som har riktat sig mot finländska Internettjänster som behandlar ekonomiska uppgifter. Internationellt sett expanderar phishing-verksamhet fortfarande kraftigt. Den internationella gruppen som undersöker phishing-fenomenet, Anti-Phishing Working Group (APWG), rapporterade att enligt den senaste statistiken från januari [1] har antalet falska webbplatser ökat avsevärt, upp till över 30 %. Till APWG rapporterades 9715 olika falska webbplatser i januari.

Phishing-fenomenet gäller inte bara banker. Phishing-bedragare är intresserade av alla elektroniska identiteter för olika system. I Förenta Staterna har antalet phishing-attacker i synnerhet mot skattemyndigheters nättjänster och andra offentliga kundtjänster tydligt ökat.

En phishing-attackmetod som enligt APWGs uppgifter håller på att bli vanligare är att kapa och vidareförmedla text som skrivs på en dators tangentbord med hjälp av ett s.k. skadligt keylogger-program.

Skadliga botnet-program

Numera kan användning av datornätverk som är infekterade av skadliga program i stor utsträckning betraktas som professionell verksamhet. Största delen av de infekterade datorerna används t.ex. för att installera reklamprogram i en infekterad dator, för s.k. pay-per-click-bedrägerier, för phishing-bedrägerier eller för att avpressa med denial-of-service-attacker. Att stjäla information håller på att bli ett viktigt användningsändamål. Strukturen på de skadliga programmen har också blivit avsevärt komplexare. För att försvåra analyseringen använder de som skriver skadliga program allt oftare en krypterad kommandokanal för att kommendera nätverket för skadliga program. Bot-nätverket upprätthålls med modifierade och skyddade serverprogramvaror. Även kodstrukturen på själva det skadliga programmet skyddas allt oftare med olika krypteringsmetoder och s.k. logiska bomber.

Attackerare vill ha kontroll över datorn som är infekterad av ett skadligt program längre än tidigare. För att främja det här syftet hämtar det skadliga programmet allt oftare en rootkit-programvara och installerar den i den infekterade datorn för att attackeraren kan dölja det skadliga programmet och spår av dess verksamhet i systemet. Med en rootkit-programvara kan attackeraren också gömma önskade processer så att säkerhetsprogrammen och användaren inte upptäcker dem. Med hjälp av rootkit är det också möjligt att använda datorns nätförbindelse utan att användaren eller brandväggen som möjligen har installerats i datorn upptäcker trafiken.

Riktade attacker

Internet-domännamnssystemet (DNS) erbjuder en global decentraliserad adressdatabas för omvandlingar mellan domännamn och adresser. Namnservrar som är kopplade till systemet och har definierats för öppet kan användas för att producera skadlig trafik avsedd för denial-of-



3.4.2006

CERT-FI

service-attacker. En förfrågning som är försedd med en falsk källadress och riktad mot en data-post utformad på ett visst sätt producerar en svarsmeddelande som är avsevärt större än förfrågningsmeddelandet. Genom att skicka förfrågningen till ett stort antal namnservrar som tillåter rekursiv förfrågningstrafik orsakas en avsevärd mängd oönskad svarsmeddelandetrafik till den falska adressen. De som upprätthåller systemet borde därför se till att namnservrar inte svarar på rekursiva förfrågningar som kommer utanför det egna serviceområdet. Detta togs upp för första gången i CERT/CC:s rapport år 2000.[2]

Nättjänster som är skrivna i skriptspråket PHP är populära föremål för attacker mot informationssäkerhet. Orsakerna för populariteten är att attacksvärktyg är lätta att använda och webb-läsare som utgör föremålet för attackerna har en relativt stor nätkapacitet. De upptäckta sårbarheterna har vanligen inte berott på att själva PHP-språket skulle ha varit sårbart. Orsakerna bakom problemen har oftast varit programmeringsfel i PHP-tillämpningar eller i de bibliotek för bifogade programvaror som används av de PHP-baserade tillämpningarna. I början av året angreps flera finländska PHPbb-chattforum genom att förvandla framsidan till religiös propaganda. Angreppen har ett samband med karikatyrincidenten i Danmark. Det finns ingenting som skulle syfta på att attackerna speciellt hade riktat sig mot finländska chattforum. I samband med angreppen smutsades tusentals webbplatser för PHPbb-nätnyttsservrar överallt i världen.

Den vanligaste metoden för attacker som riktar sig mot Unix-liknande datasystem är att försöka knäcka huvudanvändarens användaridentifikation-lösenord genom att använda en SSH-skyddad terminalförbindelse och en omfattande lista över vanligaste lösenord. Knäckningsförsök kan ofta fortsätta länge om upprätthållaren av datasystemet som attackerar inte aktivt kontrollerar ovanliga inloggningsförsök i systemets loggfiler.

Fel och störningar

Under början av året uppstod några betydande felsituationer i IP-stamnäten som påverkade fungeringen av de kommunikationstjänster som baserar sig på dessa nät. Förutom uppstod det en allvarlig felsituation i början av februari som gällde en e-posttjänst och påverkade ett stort antal finländska e-postkunder. När tjänstproduktion centraliseras bör man ägna speciell uppmärksamhet åt att försäkra tillgänglighet genom att t.ex. decentralisera kritiska tjänster.

Framtidsutsikter

De som undersöker sårbarheter och skriver skadliga program kommer att fokusera på webbläsarprogramvaror även i framtiden. Speciellt utmanande är situationer där programvaratillverkaren inte får veta om sårbarheten först och konfidentiellt för att kunna utarbeta en lämplig programkorrigerings. Uppenbarligen säljs information om sårbarheter och till och med metoder för att utnyttja sårbarheter allt oftare som handelsvaror.

Det att skadliga program effektivt gömmer sig genom att t.ex. använda rootkit-tekniker är ett fenomen som tydligt blir starkare. Egenskaperna hos rootkit-programvaror utvecklas vidare.

[1] http://www.antiphishing.org/reports/apwg_report_jan_2006.pdf

[2] http://www.cert.org/incident_notes/IN-2000-04.html