COMPUTERWORLD

Hackernes historie del 3, og dermed også computeren og internettets historie

Det var så forløbig del 3. Læs Tom Madsens artikler i Alt om Data. Det er hans oprindelige materiale der har inspireret disse 3 artikler.

Skrevet den **03. Feb 2009** af **bufferzone** I kategorien **Generelt IT / Andet** | ★★★☆☆

Hacking, hackerne og dermed computerens og Internettets historie, Del 3

Del 1: http://www.eksperten.dk/artikler/558.
Del 2: http://www.eksperten.dk/artikler/559.
Del 3: http://www.eksperten.dk/artikler/579.

Fargo-4A and Knights of Shadow.
Fargo 4A er også en af de grupper man bør kende. Gruppen levede ikke ret længe, man da den var en af de første i miljøet og talte medlemmer som f.eks. Quasi Moto (se Legion of Doom). Gruppen lavede bl.a. en del social engineering med telefonselskaberne og selv om gruppen relativt hurtigt opløstes, er flere af medlemmerne stadig aktive. Foruden Quasi Moto kan nævnes Bioc Agent 003, TUC, Big Brother, Video Warhead, and the Wizard of Arpanet

Lige som Fargo 4A er Knights of Shadow en af de hacker grupper hvis navn man finder over alt på mailinglister og BBS dokumenter. Gruppen står også som forfattere til en del at de første og grundlæggende arktikler om hvad hacking er og hvad det vil sige at hacke. Blandt medlemmerne finder vi flere gengangere, f.eks. Lex luthor LOD, Lord Digital LOD og Apple Mafia samt Elric of Imrryr. Lex Luthor startede faktisk i KOS, man da flere af de folk han foreslog som medlemmer ikke blev optaget, startede han sin egen gruppe, der jo blev til LOD,

http://os-infiltraitors.freehomepage.com/tutorials.html
http://www.palmcoder.net/files/Archives/hacking/hack_em.txt

Cult of the Dead Cow.
http://www.cultdeadcow.com/
Cult of the Dead Cow er en meget berømt/berygtet, meget gammel hacker gruppe, og selvom den har eksisteret længe, er det meste af gruppens offentlige berømmelse af nyere dato. Den mest kendte af gruppens meritter er udgivelsen af bagdørs programmet Back Orifice, oprindeligt i 1988, og back Orifice 2000 (der faktisk udkom i 1999). Back Orifice er en klar reference tilbage til Massachusetts Institute of Technology og Tech Model railroad club og de oprindelige hackers. Selv om programmet er gammelt, florere det faktisk stadig. Jeg fandt det selv på en maskine så sent som december 2004.
cDc er politisk aktiv i miljøet, uden de kan siges at tilhører den ene eller anden politiske fløj. De er/var en del at en international koalition af hacker grupper der talte imod en online cyber warfare kampagne der var rettet imod Irak og Kinas regering og sener dannede cDc gruppen Hacktivismo (http://hacktivismo.com), der arbejder med anti-censorship technologi og for menneskerettigheder på Internettet.
Udover Hacktivismo har cDc også startet en hacker konference kaldet HoHoCon. Den afholdes normalt i Houston Texas og en af de ledende figure er Drunkfux, eller dFx som hans handel også skrives. HoHoCon er den første hacker konference hvor både journalister og lovens repræsentanter er inviteret med. Der har i alt været afholdt 5 HoHoCon's.
cDc lavede den (næsten) uhackelige web server. Den bestod af Eprommer (Erasable Programmable Read-

Only Memory) og CD-ROM drev med hjemmebrændte skiver. Serveren havde ingen harddisk og alle websiderne var brændt ned på CD-Rommerne så de ikke kunne ændres. Det eneste man kunne var at lave Denial of service og så lave ting der blev skrevet til serverens hukommelse.

The T-Files
The T-files er en reference til en del af de bærende formater på Internettet og en hel del at de formater linux anvender. F.eks.:
.tab, .tar, .tex, .tb, .tfw, .tga, .tgr, .th, .tif, .tiff, .tlb, ,tmd, .tmp, .ttf og . txt

cDc siger selv "We're not into t-files for the groupies and money." Deres formulerede mål er "Global Domination Through Media Saturation,". I modsætning til de fleste andre hacker grupper er åbenhed nærmest et mål i sig selv. De stiller gladelig op til interviews, TV programmer, som forelæsere og andre offentlige ting. "Nothing can compare to the money-throwing, stage-diving, crotch-grabbing, guitar-wailing, inter-species sex-depicting, computer-smashing & panty-wetting experience that is a live cDc performance."
Der er mange rygter om cDc. At de skulle have forstyrret kommunikation ved at repositionere satellitter, At de ligger i åben krig med "Church" of Scientology; at det var cDc der gav Ronald Reagan Alzheimers disease, at Slobodan Milosevic forsøgte at inddrage cDc under hans krigsretssag, at de afholder møder I en underjordisk bunker under en forladt militærbase I Nevadas ørken.
Alt dette er sandt, siger cDc, men der er meget meget mere.

L0pht.
(http://en.wikipedia.org/wiki/L0pht)
Medlemmerne i L0pht (udtales "loft) er automatisk også medlemmer af cDc og omvendt og 2 af de ledende figure var blandt dem der startede cDc tilbage i 1984.
L0pht startede som en ganske almindelig hackergruppe, med alt hvad dette indebar. Ret hurtigt udviklede L0pht sig dog til en halv kommerciel tænketank med navnet L0pht Heavy Industries, der udgav security advisories, beskrev exploits og også lavede den meget berømte password cracker L0phtCrack (som du kan læse om i en af mine andre artikler).
I 1998 afgav medlemmer fra L0pht vidneforklaring foran den amerikanske kongres, hvor de påstod at de kunne lamme hele Internettet på 30 minutter. En påstand der nok ikke skal tages direkte for pålydende, men tjener til at understrege at Internettet er bygget uden sikkerhed og at et samfund baseret på Internettet, på godt og ondt er afhængig af dette.
I 2000 fusionerede L0pht Heavy Industries med @stake, der var et nystartet firma og cementerede dermed transitionen fra undergrunds gruppe til et legitimt ("white hat") computer security firma. I september måned 2004 annoncerede Symantec Corp. at man havde underskrevet aftaler om overtagelse/fusionering af/med @stake, Inc.

Ghetto Hackers.
The Ghetto Hackere er en Seattle baseret hacker gruppe der har vundet berømmelse og anseelse på især to områder. De er bl.a kendt fra Kevin Mitnick sagen, eller rettere fra de debatter Kevin Mitnick efterfølgende har deltaget i, hvor bl.a. Ira Winkler, der er chief security strategist for Hewlett-Packard har talt imod ansættelse af tidligere dømte hackere i IT sikkerhedsbranchen, på trods af at han faktisk selv har ansat fork fra bl.a. Ghetto Hackers.
Det som The Ghetto Hackers er mest kendt for i miljøet er deres Capture the Flag hacking konkurrence også kaldet "Root Fu" der er gennemført på de tre seneste DefCon hacker konferencer. The Ghetto Hackers planlægger en endnu større version af konkurrencen, der skal gennemføres over Internettet The "Mega Root Fu" forvendtes at kunne tiltrække tusinder af Hackere. Konkurrencen er i 2005 begrænset til Teams fra USA, den lanceres som en slags East Coast Vs West Coast og man kan registrere sig indtil februar 2005 (http://mega.rootfu.org/).
Der har været en del diskussioner omkring det etiske i afholdelse af en sådan konkurrence over det offentlige Internet og nogle er bange for at denne hacking skal sprede sig ud til systemer, der ikke er med i konkurrencen. The Ghetto Hackers har ideer om at anvende VPN til at holde konkurrencen afskærmet fra

det resterende net

414" hackers.
The 414 Hackers er også en af de berømte oprindelige hacker grupper. 414 er en reference til områdenummeret for det område i Milwaukee hvor gruppens medlemmer boede. Gruppens berømmelse skyldes til dels at nogle af deres kendteste hacks blev afsløret i 1983, lige efter filmen War Games havde haft premiere. Gruppens bedst publicerede eskapader er indbrud i Sloan-Kettering Cancer Center og Los Alamos militære forsknings center og en medvirkende faktor til at gruppen fik så meget opmærksomhed som de gjorde, var at de ved en fejl fik slettet nogle filer, der ikke skulle have været slettet og på den måde, gjorde opmærksom på, hvad der faktisk kunne ske, når man ikke tog sikkerheden alvorligt.
Gruppens foretrukne metode var faktisk latterlig enkel. De fleste af deres indbrud skete med en almindelig Telnet klient, der jo findes som default på stort set alle computere, og brug af default passwords. Selv den dag i dag, er den metode ganske (man fristes til at sige skræmmende) gangbar da mange glemmer at ændre default passwords i routers, Firewalls, database administrationsmoduler, web løsninger og andet. Har du husket det ?? ellers var det måske en ide kontrollere det nu.

The Realm.
Amerikanerne har haft deres rigelige andel af hackergrupper, Tyskerne kom på landkortet med CCC. Sidst i 1980'erne var turen så kommet til Australien, hvor hacker gruppen The Realm begyndte at sætte elektroniske spor i forskellige logfiler rundt omkring. The Realm holdte til i Melbourne området, og de to mest kendte figurer var Electron og Phoenix. Disse to hackere stjal en liste med sikkerheds data og brugde denne liste som springbræt til at bryde ind i nogle af verdens, indtil da, tilsyneladende mest sikre systemer. Deres angreb var så hurtigt og så udbredt at man i første omgang var sikker på at der var tale om et automatiseret/scriptet angreb, men Phoenix kunne ikke holde tæt, og ringede til New York Times for at prale. Efter ganske kort tid var både US Secret Service og FBI på sporet af dem, og det Australske federale politi havde ransaget deres hjem.
Mens phoenix og Electron var aktive, var et at de ønsker der stod højest på deres, og de fleste andre hackeres ønskeliste, Deszip og Zardoz.
Deszip er et password cracker værktøj der hørte sammen med den oprindelige DES (Data Encryption Standard) algoritme. Dette værktøj var hot news i miljøet og alle de kendte hackere var på jagt for at få fingre i det. Forskellige af hackernes samlingssteder, som f.eks. Altos i tyskland, blev brugt til at koordinere indsatsen for at få fingrende i dette værktøj. Man forsøgte at trænge ind på forskellige netværk, f.eks. på universiteterne og på at hacke kendte personer i IT sikkerheds branchen, f.eks. Eugene Spafford, fordi man forventede at kunne finde Deszip der.
Zardoz var en verdensomspændende mailingsliste, lidt ligesom Bugtraq i dag. Enkelte mails cirkulerede i hackerkredse, men hele arkiver blev betragtet som en guldgruppe da det indeholde samtlige opdage huller i de fleste systemer i brug på Internettet samt "de professionelles" diskussion om disse hulder. Med adgang til Zadoz ville hackere af phoenix og Electron's kaliber kunne bevæge sig frit ind og ud af alle de systemer de lystede. Zardoz var omgæret am megen bekymring fra de professionelles side, på den ene side var det en uundværlig ressource men på den anden side var man utrolig bange for at den skulle falde i de forkerte hænder.

http://www.abc.net.au/tv/documentaries/stories/s853348.htm

Det var så del 3. Om der kommer en del 4 hvor jeg lige binder hackingens historie op til i dag, samt samler et par af de historier der mangler, har jeg ikke besluttet endnu, vi må se hvad tiden siger. Skulle du have nogle ønsker eller ligge inde med nogle navne på folk der fortjener behandling, så lad mig endelig det vide

Skulle du have spørgsmål, kommentarer eller rettelsen (herunder især stavefejl) er du velkommen til at kontakte mig på kim@bufferzone.dk, ligesom jeg ofte er at finde på Eksperten.

Kommentar af punnishment d. 17. Oct 2005 | 1

genialt

Kommentar af burzum d. 08. Jan 2005 | 2

Kommentar af ttj d. 09. Jan 2005 | 3

Fin artikel..

Kommentar af eneq d. 10. Jan 2005 | 4

Kommentar af the_ghost d. 06. Feb 2005 | 5

Kommentar af mikze d. 09. Jan 2005 | 6

Kunne godt lide det der med at du nævne 404 (mine ynlings hackere) :D

Kommentar af da9el d. 12. Feb 2005 | 7

Kommentar af m-smith d. 08. Jan 2005 | 8

Kommentar af morteeart d. 09. Jan 2005 | 9

Denne form for historier undervisning er meget sjovere end den i skolen :D , lol hvad sker der for folk ? medmindre man giver 100% god til en artikel, SKAL man skrive en kommentar.

Kommentar af talrinys d. 16. Jan 2005 | 10

Sjove artikler, bliver næsten helt fristet

Kommentar af nemesis_123 d. 28. Apr 2005 | 11

Kommentar af sjatten d. 09. Jan 2005 | 12

Kommentar af rlau d. 23. Apr 2006 | 13

Meget spændende artikel, syntes dog du mangler at nævne gruppen milw0rm.

Kommentar af kamiga d. 14. Jun 2006 | 14

God artikel - som altid ;b

Kommentar af fks d. 06. Feb 2008 | 15