Zásek do živýho

Honza „Klokánek“ Šípek

Jaké je české digitální podsvětí? Kdo jsou hackeři? Zbojníci či vandalové? Co dovedou? Proč dělají své odvážné kousky? Jací jsou policisté, kteří je pronásledují? Firmy, vlády, velké společnosti, špionážní služby, státní správa, banky, komunikační satelity – je vůbec něco v bezpečí?

DISCLAIMER

Tento text jsem napsal na gymplu v roce 1999 pro jakousi středoškolskou odbornou činnost. Plánoval jsem „jednou" ji rozšířit do podoby knihy, ale jak tomu bývá, to „jednou" jsem odkládal tak dlouho, až nikdy nepřišlo. Neboť po webu kolujou různé verze tohoto textu, a navíc se zdá, že o hackerské scéně v daném období toho dneska už moc dohledat nejde, zveřejňuju ji aspoň v nejucelenější dobové podobě, i když je možné, že se věci staly jinak, než píšu, a že bych se dneska za text už styděl, nebo se nad ním minimálně pousklíbal.

As is, no warranty, own risk, atd.

V roce 2012 byl text připraven k webovému vydání a doplněny některé Pajkusovy poznámky s odstupem let.

H. Š.

Děkuji především (v abecedním pořadí): 91,9 FM, Astonovi, Blackymu, Detvan, Dextrovi, Drsoňovi, Jirkanovi, Olze Machovcové, Pajkovi, Sanovi, Shaddackovi, Zuzaně Paulinové, bez nichž by tato kniha nikdy nevznikla.

Proklínám všechny, kteří se systematicky snažili o opak.

Zvláštní poděkování patří tvůrcům interního policejního informačního systému, kteří mé jméno a příjmení uvádějí jako příklad uživatelského jména v instrukcích pro přihlášení do systému a vytvořili mi tak mezi znalými pověst hackera z největších :-).

Autor není zodpovědný za jakékoliv škody způsobené nevhodným použitím tohoto dokumentu.

Tato kniha studuje historii, nikoliv techniky digitálního undergroundu. Pokud jsou některé techniky z ilustračních důvodů přesto popsány, autor důrazně varuje, že jejích použitím můžete ohrozit cizí vlastnictví a/nebo porušit zákon. Autor též upozorňuje všechny policejní složky, že nezná totožnost osob, které jsou uvedeny pod přezdívkami či pseudonymy. Setkal se s nimi buď v anonymním prostředí českých a slovenských hospod nebo s nimi komunikoval pomocí emailu.

Kontakt:

---

klokanek@eldar.cz

digitální verze této knihy:
`http://eldar.cz/kangaroo/zasek_do_zivyho`

Motto: „Každý má právo vyjadřovat své názory slovem, písmem, tiskem, obrazem nebo jiným způsobem, jakož i svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice státu.“

Listina základních práv a svobod, článek 17

Obsah

Kapitola 1

Janošíkové, šprýmaři, zločinci a cyberpunkeři

Lidé, které bychom nazvali *hackery,* žili a bavili se ještě před rozšířením prvních počítačových systémů. Pro začátek jim stačily dálkové hovory na cizí účet, škodolibé pozměňování elektronických mechanismů či odposlech policejního vysílání.

Když se pak objevily první sálové počítače, seskupili se kolem lidé, kteří systémům zcela propadli. Fascinovaly je, viděli v nich neuvěřitelnou budoucnost lidstva. Do hloubky počítače prozkoumali, naučili se je používat a vylepšovat, stavěli své vlastní, stali se skutečnými odborníky. Problémy pro ně představovaly výzvu, do jejich řešení se pouštěli s vervou a nadšením. Celé noci nespali, v řeči se nedokázali zbavit počítačových termínů, stlali si pod stoly v laboratořích a kontrolovali obrazovky terminálů. Měli většinou svůj vlastní nonkonformní styl vystupování i práce, který jim raději nikdo nebral. V té době slovo *hacker* znamenalo cosi jako „všeznalý počítačový odborník" a vyvolávalo úctu.

Venku už ovšem čekala druhá generace *hackerů.* Neměli přístup k prvním počítačům v armádě, na univerzitách a ve vědeckých laboratořích, ale také se chtěli učit, poznávat systém. Nechápali, proč by přístup neměli mít. A tak si ho opatřili.

Pronikali do systémů a zevnitř je prozkoumávali. Stali se v jistých ohledech lepšími, než jejich učitelé a lidé, kteří se o velké systémy starali. Většinou nic nepoškozovali, jen se dívali, občas si něco vyzkoušeli, získávali přístup dál. Ne pouhá zvědavost, ale přímo živelná touha po poznání, je hnala hlouběji. Zdálo se jim absurdní, že systémy, které v sobě mají potenciál ulehčit život celému lidstvu, zmírnit humanitární

problémy, zrychlit běh byrokratických záležitostí a odstranit rozdíly mezi lidmi, jsou používány maximálně na řízení armády.

Hackeři druhé generace si začali mezi sebou vyměňovat zkušenosti, setkávali se kdesi mezi dráty v hromadných telekonferencích na vyhrazených telefonních linkách. Vznikaly první hackerské časopisy, které ukazovaly stále další a další metody průniku.

Objevily se osobní počítače. Teenageři kolem patnácti let seděli ve svých dětských pokojích a pronikali do počítačových sítí americké armády. Zjistili, že i na jejich počítači může běžet systém BBS[1], díky kterému se k nim mohou po telefonu připojovat ostatní hackeři a diskutovat s nimi, vyměňovat si soubory, posílat si elektronickou poštu. BBS, zvané častěji boardy, se staly prvními skutečnými elektronickými komunitami, jejichž členové se většinou znali jen pod přezdívkami a ve skutečnosti se nikdy neviděli.

Hackeři získali přístup do armádních systémů, sítí telefonních společností, komerčních organizací. Většinou věděli o zabezpečení systému více, než sami lidé, kteří ho zabezpečili. Většina hackerů podnikala své průniky pouze pro vlastní potěšení a zábavu, z obyčejné zvědavosti, či pro pocit geniality při přelstění důmyslného ochranného mechanismu.

Nejlepší hackeři nikdy nezískávali peníze přes počítač a nezabývali se podvody s kreditními kartami. Byli však i lidé, kteří likvidovali celé systémy ve jménu boje proti počítačovému monopolu vlády a velkých společností. A samozřejmě se přidali i zloději, kteří na počítačových podvodech vydělávali desetitisíce dolarů, nebo prodávali informace získané z nabouraných počítačů. To se však většině hackerů příčilo. Hacking se stal pro mnohé bojem za vlastní právo na informace.

Když na počátku devadesátých let došlo k zhroucení půlky americké telekomunikační sítě AT&T vlivem softwarové chyby a tento čin byl připsán na vrub hackerům, rozpoutaly federální úřady spolu s telekomunikačními společnostmi obrovský zátah na hackery. Byly při něm zatčeny desítky lidí, kterým média udělala image geniálních zločinců mezinárodního formátu.

Pro slovo hacker byl najednou synonymem zločinec.

Teenageři inspirovaní filmy jako Válečné hry a četbou kyberpunkové sci-fi najednou chtěli být také hackery. Většinu z nich to rychle přestalo bavit, ale někteří vytrvali.

Jak se osobní počítače stále více rozšiřovaly, začal růst jejich výkon a klesat jejich cena. Rozšířil se Internet a byl přístupnější stále

[1] ***B**uletin **B**oard **S**ystem, „elektronická vývěska“, board*

většímu počtu lidí.

Výkonné počítače i informace – to, o co hackeři tolik bojovali – byly najednou dostupné každému.

Hackeři však nezmizeli, právě naopak – Internet se pro ně stal živnou půdou. Za lokální telefonní poplatky (ne že by na tom záleželo) se mohli dostat do jakéhokoliv počítače kdekoliv na světě. Najednou všude kolem bylo tolik počítačů (=cílů)! A každý z hackerů může provozovat vlastní internetový server.

Útoky neztratily na své divokosti, technické mazanosti a těžce recesním rázu.

Ale bezpečnostní hlediska už nejsou dnes tak podceňována jako v osmdesátých letech. Bezpečnost systémů se mnohem zvýšila ve strachu před útoky hackerů.

Jeden z Murphyho zákonů však praví, že každý program obsahuje alespoň jednu chybu. Hackeři tyto chyby hledají, využívají je k útokům, ale zároveň na ně často i upozorňují a umožňují tak jejich opravu.

Zdá se, že jde o nekonečný koloběh. Čím dokonalejší budou systémy, tím mazanější budou hackeři. Nezastaví se a co víc, díky svému aktivnímu přístupu k bezpečnosti budou vždycky o krok vpředu před správci systémů.

I v Čechách a na Slovensku vznikla komunita hackerů. Dlouho fungovala skrytě, věděli o ní jen samotní hackeři a správci postižených serverů, kteří se raději, z důvodů, které poznáme později, příliš neozývali.

Až se v listopadu 1996 na titulní stránce oficiálního webového serveru Armády České republiky *(http://www.army.cz)* objevil titulek: *„Lidi, spěte klidně, nad vámi bdí Armáda České republiky“*. Prohlášení, pod nímž byl podepsán voják Švejk, hrdě hlásalo: *„www.czert.army.cz poskytuje uživatelům snažší přístup k vybraným Intranet-adresám a informacím v oboru dezinformačních paskvilů. Poskytuje minimální množinu servrů, standartů a norem z oblasti bezpečnosti (?!), včetně důležitých článků, statí či publikací – to vše v čínském originále i české provenience. Zvláštní sránky jsou věnovány virové problematice a jejich tvorbě. Zdroje zde najdou i vývojoví programátoři a hackeři. Zvláštní část je věnována česko-německé otázce, dětské pornografii, výrobě plastických trhavin a vysoce návykových drog. Můžete také navštívit domovskou stránku Ministerstva obrany Čínské republiky, kde získáte informace o Armádě Čínské respubliky, její struktuře, aktivitách, vojenském školství, špionážních akcích, úplatkářských afé-*

rách apod. Autoři se obracejí na všechny, kdo se chtějí aktivně zúčastnit, se žádostí o poskytnutí dalších podnětů, resp. materiálů – CzERT pozn. : jsme tady a umístili jsme zde pár námětů pro reportáž. Škoda jen, že se nám nepodařilo zastihnout Radka Johna s jeho ‚Na vlastní oči'.“[2]

Následovaly odkazy na stránky o drogách a prostituci. Česká veřejnost se poprvé přímo setkala s útokem hackerů. „CzERT“, podepsaný pod útokem, se stal démonem českého Internetu. Změnil a zparodoval stránky Ministerstva zdravotnictví, Ministerstva životního prostředí, i známých komerčních serverů jako Cesnet, MAmedia (později Mageo), Seznam, stránky banky Union dokonce třikrát. Hrozivá animace nestvůry s červeným obličejem a ostrými zuby budila ze sna nejednoho správce serveru či sítě, policisty a novináře.

O všem, co předcházelo a následovalo, je tahle knížka.

[2]hacknuté stránky Armády ČR, elektronicky, `http://hysteria.sk/hacked`

Kapitola 2

Kolébka hackingu: Spojené státy

Nadšení hackerů a zděšení státních orgánů, grandiózní průniky i odhalení, první velké procesy, hackování jako politická záležitost

První hackeři se objevovali tam, kde byly první počítače. Právě ve Spojených státech musíme hledat skutečné kořeny dnešních hackerů. Vznikli zde jako živočiný druh, žili, vyvíjeli se i umírali. Prodělali i své konflikty se zákonem, společnost k nim dokázala zaujmout postoj. Již na konci osmdesátých a na začátku devadesátých let zde proběhly změny v zákonech a precedentní soudní spory, které naši zemi teprve čekají.

V této kapitole se podíváme na počátky i současnost amerického digitálního undergroundu či, chcete-li, počítačového podsvětí a jeho pozadí. Samozřejmě není možné na tak malém prostoru dosáhnout úplnosti, která ani není naším cílem. Ale abychom skutečně poznali, kdo hackeři jsou, musíme i my vyjít z těchto končin.

--=:o0o:=--

Vše začalo telefonními podvody. Jako každá telefonní síť měla i ta americká své díry, které se daly zneužít k telefonování zadarmo,

přesměrovávání telefonních hovorů, odposlechům a podobně. Jednou z metod k tomu účelu používaných bylo zneužití tónu o frekvenci 2600 Hz, který otevíral operátorský režim práce s telefonní ústřednou. Na vysílání tohoto tónu vyrobil technický mág s přezdívkou „Al Gilbertson“ malé zařízení nazývané „Blue Box“, které způsobilo technikům telekomunikačních společností mnoho vrásek. „Blue Box“ nebylo příliš obtížné postavit a proto se velmi rychle šířilo. Svou kariéru na jeho výrobě odstartovali dokonce i Steve Wozniak a Steven Jobs, pozdější zakladatelé společnosti Apple.[1] Zatímco jako *hackeři* jsou dnes označováni počítačoví kouzelníci pronikající do počítačových systémů, *phreakeři* se říká lidem zneužívajícím telefony a telefonní ústředny.

Anarchistické a odbojné organizace ospravedlňovaly své telefonní podvody bojem proti velkým korporacím a státnímu establishmentu. „Yippies“, příslušníci *Youth International Party,* anarchistického proudu hippies, Abbie Hoffman a člověk známý jako „Al Bell“ začali v květnu 1971 vydávat časopis *Youth International Party Line* (YIPL), který přímo vyzýval ke zneužívání telefonů a poskytoval pro to praktické návody. Hoffman byl navíc ještě autorem knihy s názvem „Ukradni tuto knihu“, manuálu k tomu, jak bez peněz přežít ve městě a narušit při tom zkostnatělý systém státní byrokracie.

Když se „Al Bell“ rozešel s Yippies, změnil název časopisu na TAP, čili *Technical Assistance Program* (je to dvojsmysl, protože „tap“ současně v angličtině znamená i odposlech), soustředil výhradně na technické záležitosti elektronického okrádání a politické nechával stranou. Koncem sedmdesátých let předal „Al Bell“ vydávání TAPu nadšenci přezdívanému „Tom Edison“. Když „Edisonovi“ v roce 1983 žháři vypálili dům a navíc ještě ukradli počítač, způsobilo to konec časopisu. Ovšem jen dočasný, po sedmi letech neexistence TAP oživil počítačový desperát „Predat0r“ z Kentucky.

−−=:○0○:=−−

Koncem sedmdesátých a začátkem osmdesátých let přišel ten pravý rozmach osobních počítačů. Byly malé, relativně levné a přestože toho nedokázaly moc, stačilo to k tomu, aby si získávaly víc a víc příznivců především mezi teenagery, kteří byli novou technikou doslova okouzleni.

[1] Zdroje všech těchto informací jsou uvedeny v příloze „Časová osa amerického digitálního undergroundu“ na straně 67

K důležitému (ačkoliv mírně kolumbovskému) objevu došlo v únoru 1978, kdy Ward Christensen a Randy Suess rozjeli v Chicagu první Buletin Board System (BBS), častěji nazývaný jako board[2]. Princip byl v tom, že každý, kdo měl osobní počítač a modem[3], mohl zpřístupnit po telefonní lince svá data úplně každému. A nejen to. Většina boardů navíc měla určitý systém, který umožňoval přihlašování uživatelů pod jménem či přezdívkou. To už umožňovalo určit, kdo jaký soubor na board „přinesl“[4], či jaký si „odnesl“[5]. Protože uživatelé navštěvovali svůj oblíbený board pravidelně nebo alespoň častěji, měli i možnost psát do diskusních skupin k určitým tématům a vyměňovat si s ostatními uživateli elektronickou poštu. Pokud měl board více telefonních linek (a více modemů), mohli spolu jeho návštěvníci diskutovat naživo, v reálném čase – chatovat.

Tehdejší přenosová rychlost modemů byla v porovnání s dneškem velmi malá a ještě ji snižovaly nekvalitní analogové linky. Provozovatelé boardů byli většinou nadšenci, kteří dávali veřejnosti k dispozici svůj osobní počítač, jehož hardware nebyl obvykle nic moc. Některé boardy se mohly pochlubit i „obrovskými“ čtyřicetimegovými disky. Přes všechna omezení se tyto osamělé ostrůvky v moři papírových informací staly prvními skutečnými digitálními komunitami.

−−=:○0○:=−−

Lidé na boardy přicházeli ze všech směrů, ze všech částí regionu i celých Států, ale vlastně nezáleželo na tom odkud. Komunikovali s ostatními pouze pomocí klávesnice a monitoru, vystupovali pod svou přezdívkou.

Nikdo nemůže tušit, kdo jste. Nemůže vědět, že jste destiletý klouček, který musí sedět na třech polštářích, aby dosáhl na klávesnici tatínkova počítače. Nebo že jste Rom či černoch, šišláte, máte metr dvacet, obličej posetý tisíci uhrů, nebo že vám chybí pravá ruka. V digitálním světě se projevuje pouze vaše osobnost. Můžete být přesně tím kým chcete být. Můžete si dokonce vytvořit více virtuálních identit a „být“ zároveň několika lidmi najednou.

[2]V češtině se používá anglické slovo *board* nebo *bíbíeska,* fonetický přepis zkratky BBS. Doslovný překlad „nástěnka“ se neujal.

[3]*modem* – zkatka z modulátor-demodulátor zařízení pro přenos počítačových dat po telefonních linkách

[4]Většinou se používá anglický termín *upload,* česky překládaný jako natáhnout či poslat soubor.

[5]anglicky *download,* česky se zažily výrazy *stáhnout* či *sosat*

Na boardech se začaly utvářet mezilidské vztahy pravých komunit. Všichni se znali a přestože nevěděli, jak se jmenují ostatní, odkud jsou a jak vypadají, věděli kdo jsou možná ještě přesněji než lidé, kteří s nimi byli v denodenním kontaktu. Nabízí se námitka, že člověk může virtuálně vše jen předstírat. Samozřejmě že může! A s omezenými kanály kontaktu je to ještě mnohem jednodušší, než v „realitě“, kde máme k dispozici spoustu dalších informací o člověku (gesta, mimika, tón hlasu a podobně) a dokážeme mnohem lépe odhalit lež či nekalé úmysly. Ale při delším používání jedné identity se v ní vaše skutečná osobnost dřív nebo později projeví. A mimo to – kolikrát o sobě v „reálném“ světě vytváříme různé iluze a přetvářky? Téměř neustále nosíme nějaké masky.

Když uděláte ve své virtuální komunitě nějaký průšvih, můžete docela jednoduše zmizet a vytvořit si novou identitu pod novým jménem. Zvládnete to za pár minut. Ale daleko zajímavější je pokusit se své problémy řešit, což vás vlastně nestojí zas o tolik víc času a úderů do kláves.

Virtuální komunity (stejně jako boardy) existují dodnes. Internet jim dal ještě mnohem větší rozměr a přístupnost z celého světa za místní telefonní poplatky je učinila ještě atraktivnějšími. Příslušníků velké české komunity Mageo (`http://www.mageo.cz`), dříve MAmedia, je v době vzniku této knihy přes 15 000 a jejich počet stále roste. A ještě více lidí dnes chatuje v systémech jako je Xchat.

`--=:o0o:=--`

Není divu, že se *boardy* na začátku osmdesátých let začaly množit jako houby po dešti. Firmy si je začaly zakládat, aby mohly elektronicky šířit ceníky a informace o svých produktech. Jednotlivci je vytvářeli, aby mohli ukázat celému světu něco ze svých nápadů, programů či textů, nebo chtěli vytvořit místní digitální komunitu. Některé z nich se začaly specializovat. Existovaly boardy knihoven, škol, radioamatérů, unixáků, programátorů, hippíků, skateboardistů, punkerů, pozorovatelů UFO, distributorů shareware… a samozřejmě i boardy digitálního undergroundu. Prvním takovým byl pravděpodobně systém s názvem 8BBS, otevřený v březnu 1980. O dva roky později byl zabaven policií, což bylo zdůvodněno používáním modemu, darovaného jedním z vděčných uživatelů, který byl zakoupen na ukradenou kreditní kartu. Avšak to nemohlo underground zastavit. Každý, kdo měl počítač, mohl mít doma board. Na začátku 90. let se množství boardů v

USA odhadovalo asi na čtyři tisíce. Jen malá část z nich patřila undergroundu, ale přesto byla nekontrolovatelná a necenzurovatelná státní mocí.

Na undergroundových boardech se dají dodnes najít návody na šizení telefonů, na pronikání do systémů od VMS[6] až po Linux, ale i plány na výrobu výbušnin, či „deset způsobů jak zabít člověka holýma rukama“. Mezi stovkami souborů HOW-TO (Jak na...?), které jsem stahoval z jedné hackerské BBSky, byl i soubor HOW-TO Rape. Než jsem si uvědomil, co znamená anglické sloveso *to rape* a stiskl tlačítko Stop, načetlo se několik kilobytů toho nechutného textu. Jsou tyto návody nebezpečné?

Před několika lety vysílala TV Nova v pořadu Na vlastní oči dramatickou reportáž, o tom, že na boardu SPT Telecom je umístěn návod na výrobu jaderné bomby a každý si ho odtud může stáhnout. Měl jsem ho už několik týdnů předtím z jiného boardu.

K jeho sepsání stačily prakticky jen středoškolské znalosti chemie a fyziky. Pojednával zhruba o tom, že vezmete dvě podkritická množství plutonia a spojíte je dohromady a ono to udělá bum. Následoval návod jak získat plutonium z vyhořelého jaderného paliva, dokonce i postup, jak palivo dostat z kontejnerů.

Výroba plutonia ve sklepě by vám trvala podle autora návodu několik tisíc let. Kdyby návod byl použitelný, nemyslíte, že by měl každý průměrný studentík ve sklepě atomovou bombu? A přesto velké množství počítačových nadšenců vlastní tento návod a pyšní se jím před svými kamarády. Mají kousek zakázaných vědomostí. Vědí.

Na Internetu jsou ke stažení návody na výrobu čehokoliv od střelného prachu po falešný napalm. Drtivá většina lidí, kteří tyto návody čtou a stahují, nikdy nic podobného nezkusí vyrobit. Stačí jim, že vědí.

Ano, máte pravdu, existují lidé, kteří bomby skutečně podle návodů z Internetu postavili. (Což byl údajně i případ bombového útoku na olympiádě v Atlantě). Ale ti by se jistě snažili pekelné stroje produkovat i bez Internetu či undergroundového boardu. Jen by více experimentovali. Avšak ani návody z boardů nejsou dokonalé. Často jsou pouhou fikcí, fantazií svého tvůrce, nesplněným snem z klukovských let (což se může krýt se současností) a jejich realizace může být i docela hazardem se životem.

Hacking se stal bojem o svobodu informací.

Avšak u návodů na šizení telefonních společností a pronikání do

[6]VMS (Virtual Memory System) – operační systém pro počítače VAX společnosti Digital Equipement Corp.

počítačů nestačilo pouhé vlastnictví informace, vědění. Bylo totiž co poznávat dál. Bylo co hledat. Bylo co a koho přelstívat.

Když vyrábíte bombu nikoho nemůžete přelstít a navíc jste vystaveni rizku, že vám vybouchne pod rukama.

Hackeři si na boardech vyměňují a doplňují své zakázané informace.

Pokud stáhnete HOW-TO, máte trochu odvahy a technické mazanosti, může se vám podařit někam proniknout.

Vznikají hackerské skupiny. Lidé, kteří se v životě neviděli, se setkávají na stejných nabouraných megapočítačích. Někdy podnikají průniky jen kvůli pocitu překonání technických překážek, někdy získají pro své operace a experimenty silný sálový počítač, jindy zase přístup do další sítě. Uvnitř většinou nic nepoškodí, jen se dívají. Neškodná činnost, že? Pokud se nedívají zrovna... do vaší pošty.

−−=:o0o:=−−

V roce 1982 pronikla do Sloan-Ketteringova centra pro rakovinu a do vojenských počítačů v Los Alamos (základna, v jejíchž laboratořích vznikla první jaderná bomba) skupina hackerů s názvem 414 Gang. Vyvolala tím velikou mediální reakci, zvláště když vědci začali mluvit o tom, že v centru pro rakovinu mohli hackeři ohrozit něčí život. Jak se zdá, přestává končit legrace.

O rok později je do kin uveden film *War Games* (Válečné hry), pojednávající o teenagerovi, který se snažil nabourat do boardu jedné herní společnosti a získat tak dosud neuveřejněnou hru a omylem se proboutá do armádního superpočítače, kde si pustí simulaci („hru“) „termonukleární válka“, zvolí si za stranu Sovětský svaz a odpálí jadernou raketu na své rodné městečko. Reálné Spojené státy se chystají k protiúderu.

War Games se staly skutečně populárním filmem a jak píše Bruce Sterling ve své knize *The Hacker Crackdown*, „Zdá se, že každý americký kluk chtěl dostat k Vánocům modem.“ Většina z nich modem po půl roce odložila do skříně, ale byli i kluci, kteří na boardech poprvé přičichli k digitálnímu životu a stali se hackery, nebo alespoň příslušníky digitální komunity.

Kevin Poulsen, sedmnáctiletý Texasan, hackoval už dávno předtím. Odmalička pronikal do telefonních systémů a zkoušel, co s nimi dovede. V srpnu 1983 však pronikl s kamarádem Ronem Austinem do

počítačů Výzkumných laboratoří námořnictva v San Diegu. Ron Austin byl v listopadu zatčen a propuštěn na kauci, avšak Kevin ještě nebyl právně zodpovědný a zůstal tedy na svobodě.

O několik měsíců později, v roce 1984 začíná člověk, který si říká „Emanuel Goldstein" (podle postavy fiktivního disidenta v Orwellově románu „1984") vydávat časopis „2600: Hackerský čtvrtletník". Rozdíl oproti TAPu byl v tom, že „2600" byl registovaným periodikem, měl ISBN, vydavatele, předplatné[7] i distribuci a byl tedy chráněn dodatkem americké ústavy o svobodě tisku. Ve stejném roce založil Lex Luthor (svou přezdívku přijal podle hlavního záporáka comixu Superman) undergroundový board *Legion of Doom* (Legie zkázy, LoD). Kolem tohoto boardu se utvořila skupina hackerů, kteří si začali říkat jeho jménem. Jejich počet se neustále měnil a nebylo ho nikdy možné odhadnout, nicméně o nejvýraznějších postavách *Legion of Doom* (LoD) ještě uslyšíme.

V následujícím roce „Taran King" („Král tarantulí") a „Knight Lightning" („Rytířský blesk") začínají vydávat elektronický hackerský občasník Phrack (spojení slov phreak a hack), který se začíná šířit po všech undergroundových boardech. Patří ke stavovské cti, mít na svém boardu všechna čísla Phracku.

Vzniká WELL „Whole Earth 'Lectronic Link" (dnes `http://www.well.com`), board Point Foundation, zřejmě nejrozsáhlejší a nejsofitikovanější elektronická komunita té doby. Well nebyl hackerský či undergroundový board, ale otázky etiky hackingu se na něm často probíraly a diskusních fór na Wellu se účastnily i skutečné celebrity.

Policie si uvědomuje skutečnou nebezpečnost undergroundových boardů, ale zároveň je vidí i jako prostředek ke stíhání hackerů. Boardy jsou buď důkazy o trestné činnosti, nebo jejími nástroji. FBI například zabavuje board časopisu 2600 a část jeho softwaru označuje za „lupičský nástroj ve formě počítačového programu".

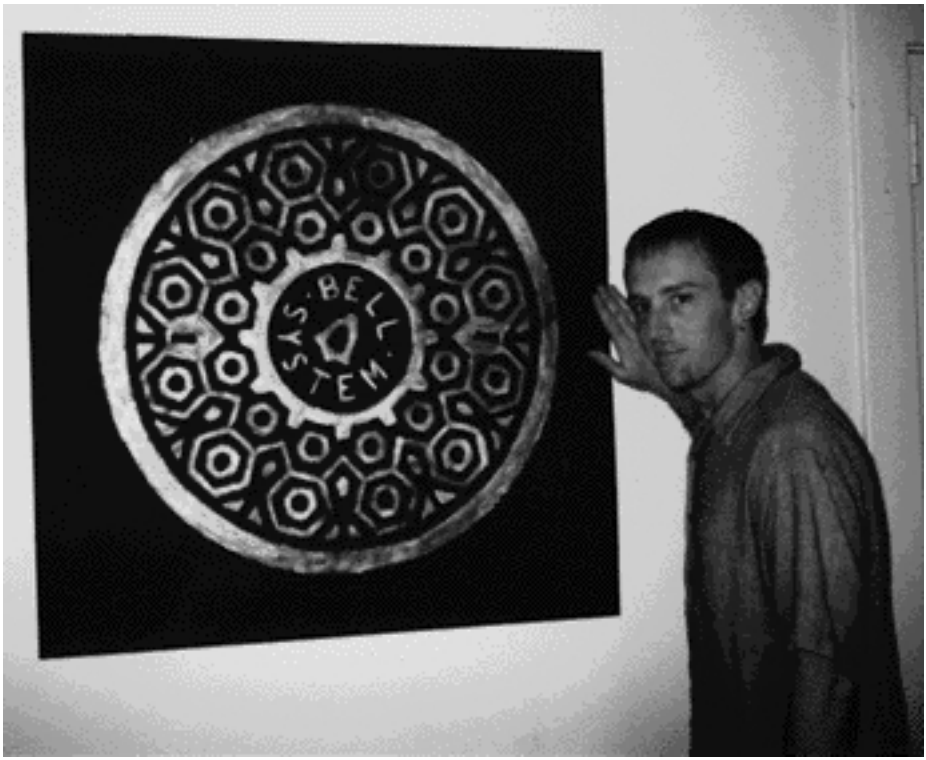
Policejním složkám už nestačí jen to, že pronikají do undergroundu, vydávaje se za hackery. Zakládají vlastní boardy, které se tváří jako „hackerské". Brzo si policejní počítače jako „Underground Tunnel" či „The Phone Company" získávají své příznivce a hackeři na nich šíří ilegální vědomosti jedna radost. Dokud ovšem nejsou zatčeni a nezjistí, že důvěryhodní správci boardů jsou ve skutečnosti policisty.

Stíhání hackerů a skutečnou ilegalitu jejich činů umožňuje Zákon o soukromí v elektronické komunikaci, schválený v roce 1986. V témže roce je již zmiňovaný hacker Kevin Poulsen zaměstnán v Institutu pro

[7] za 260 USD dnes můžete dostat doživotní předplatné 2600 včetně všech čísel vyšlých od roku 1984 a dvou triček

Kevin Poulsen se jako operátor účastnil i simulace termonukleární války. Cosi na způsob War Games.

Zdroj: http://www.kevinpoulsen.com



Dnes má Kevin Poulsen na zdi svého bytu alespoň poklop od telefonního rozvodu společnosti Bell.
Zdroj: `http://www.kevinpoulsen.com`

řízení dat (SRI), který vyvíjí armádní software pro velení vojskům a vedení války. Včetně války termonukleární.

16. července absolvuje Kevin na základně americké atomové útočné síly a raket dlouhého doletu v letecké základně Offut v Omaze jedno z vojenských cvičení NATO, simulaci operace „Globální štít“. Je to vlastně zkouška jaderné války. Podobná cvičení absolvuje jako operátor systému ještě několikrát. Někdy startují skutečná letadla a jsou v akci skuteční vojáci, jindy se vše odehrává jen v cyberspace, kdesi na linkách mezi počítači.

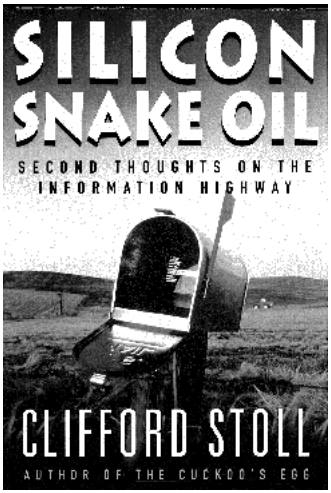
V srpnu vypršely peníze z grantu astronomu Cliffu Stollovi z *Lawrence Berkeley Laboratory*, části Kalifornské university. Nadřízení ho přeřadili do počítačového oddělení LBL. Jako nováček mezi počítačovými mágy dostal podivný a na první pohled banální úkol. Vysvětlit příčinu shodku ve výši 75 centů v systému plateb za strojový čas. Několik dní se problémem zabýval až dospěl k podivnému závěru – musela to být stopa po hackerovi. Přilepil se hackerovi na paty a v průběhu mnoha měsíců sledoval každý jeho krok. Zjistil, že se přes LBL dostává do Milnetu, americké armádní sítě. Dlouhou dobu se mu nedařilo zburcovat pozornost státních orgánů, FBI ho odmítala, stejně jako Tajná služba USA. Měl problémy i s tím, aby ho jeho šéf vůbec nechal na sledování hackera pracovat. Zlom přišel, když Cliff měl v ruce důkazy o tom, že hacker stahoval informace o jaderné strategii státu, rozmístění důležitých a tajných základen a podobně. Najednou měl plnou podporu všech bezpečnostních složek. Se svou přítelkyní zpracoval hromadu smyšlených dokumentů o Strategické obrané iniciativě (SDI), známé též jako Projekt Hvězdné války, jejichž stahování mělo hackera zdržet, aby mohl být vystopován.

Mezi tím se Kevin Poulsen s falešnou přístupovou kartou v noci vloupává do hlavní budovy společnosti Pacific Bell. Dostane se až do bezpečnostního oddělení, které je prakticky soukromou armádou pro boj proti hackerům, a odnáší si odsud spoustu suvenýrů.

„Cliffův“ hacker se chytil na falešné dokumenty. Bleskové sledování po několika linkách telefonních a jedné satelitní přes oceán nachází hackera až v Německu. 29. června 1987 vtrhává německá policie do bytu Marcuse Hesse a zabavuje mu počítač, asi stovku disket a dokumentaci k jeho hackerským kouskům. Vyšetřování později ukáže, že Hess prodával informace z Milnetu sovětské špionážní službě KGB.

25. července 1988 jsou němečtí hackeři „Hunter“ (Marcus Hess), „Hagbard“ (Karl Koch), „Pengo“ a „Bresinsky“ oficiálně obviněni ze spolupráce s KGB.

V září pronikají hackeři z *Legion of Doom* do telefonního systému



Cliff Stoll nakonec o svém honu na hackera napsal knihu Kukaččí vejce. Toto je titulní stránka jeho další knihy o informační superdálnici Silicon Snake Oil. Zdroj: `http://www.OCF.Berkeley.EDU/~stoll`

společnosti Bell South a přeprogramovávají telefonní ústředny podle své potřeby. Pokud se dostanete do systému ústředny, můžete si například zrušit telefonní poplatky, ukrást nepoužitou linku, přesměrovat hovory z jednoho čísla na druhé, vytvářet telekonference a podobně.

Americká státní správa konečně přestává podceňovat nebezpečí přicházející od hackerů. V Chicagu vzniká například Chicagská operační skupina proti počítačové zpronevěře a zneužití počítačů *(Chicago Computer Fraud and Abuse Task Force)*. Federální autority ustanovují i organizaci CERT – *Computer Emergency Response Team*, která má shromažďovat a distribuovat jednak informace o útocích na bezpečnost počítačových systémů a také informace o konkrétních chybách v systémech a návody jak chyby odstranit. Zatímco na pirátských boardech se lidé dozvídali, jak na systémy útočit, CERT nabízí informace o tom, jak se před útoky chránit.

Na podzim roku 1988 proniká hacker s přezdívkou „Prophet“ („Prorok“) – jeden ze tří členů atlantské větve *Legion of Doom* (LoD) – do centrálního systému pro automatické řízení společnosti BellSouth „AIMSX“ a odnáší si jako suvenýr dokument o struktuře práce služby 911. Číslo 911 je telefonní číslo tísňového volání v celých Spojených státech.

Hacker najednou vlastnil dokument popisující strukturu této

služby. „Prophet“ nechtěl dokument zneužít, či službu 911 nabourat. Vlastnil ho pouze jako technickou kuriozitu. Zazálohoval si ho na několik boardů. Jeden ze sysopů však dokument našel a poslal ho svému kolegovi. Zdál se jim podezřelý... Mezitím „Prophet“ posílá „dokument 911“ *Taran Kingovi* a *Knight Ligtningovi*, kteří z něj vymazávají „citlivější“ pasáže a zveřejňují jej ve svém Phracku.

Druhého listopadu 1988 v 20 hodin vypouští postgraduální student Cornellovy university Robert Tappan Morris do sítě první internetový virus nazvaný Internet Worm (Internetový červ). Virus se má s využitím bezpečnostní chyby neškodně šířit od jednoho stroje se systémem Unix k druhému, avšak kvůli „programátorské chybě“ dramaticky sníží výkon každého počítače, do kterého se dostane.

Ve 21:24 se virus dostává do počítačů Rand Corporation v Santa Monice. Rand Corp. má na starosti státní obranné zakázky. Virus se dostává i do vstupní brány sítě Kalifornské university v Berkeley a Livermoru, kde pracuje Cliff Stoll. Cliff varuje další státní organizace, které jsou k síti připojeny. Virus proniká do Státních laboratoří v Los Alamos. Napadá i Výzkumné středisko NASA, které je do půlnoci vyřazeno z provozu.

„Morrisův červ“ za dobu svého fungování zhroutil na 6 000 počítačů, přibližně 10% počítačů připojených k tehdejšímu Internetu.

Kevin Poulsen, který už delší dobu operuje v systému Cosmos, umožňujícím práci s telefonními ústřednami, a o víkendových nocích se obvykle vloupává do telefonních ústředen, nachází několik zvláštních linek. Nakonec zjistí, že se jedná o odposlechy telefonů Jihoafrického, Čínského a Izraelského konzulátu a několika soukromých osob. Podle platných zákonů musí být odposlechy povoleny soudem. Odposlechy konzulátů však evidentně odsouhlaseny nebyly.

Třináctého června 1989 provedl phreaker „Fry Guy“ velmi drzý a provokující kousek. Přesměroval všechny hovory do úřadu kurátora Palm Beach County v Delray Beach na Floridě na pornografickou horkou linku ve státě New York. Každý, kdo zavolal do tohoto úřadu, byl spojen s pracovnicí „Tinou“ na druhém konci Spojených států. „Legrace?“ ptaly se státní úřady. „A co když jednoho dne bude s pracovnicí ‚Tinou‘ spojen umírající účastník autonehody, který vytočil číslo 911?!“ Tajná služba Spojených států se chystala na silný protiúder.

Další zajímavou červnovou událostí byl akt skupiny *NuPrometheus League*, která ukradla kus copyrightovaného počítačového kódu společnosti Apple Computer a s odůvodněním, že vynikající softwarové kódy by měly patřit celému světu, rozeslala dvanáct kopií konkurenčním společnostem po celých Státech. NuPrometheus byli pravděpo-

dobně propuštění zaměstnanci Applu, ale veřejné vlastnictví informací, jakýsi informační komunismus či anarchie byly rysy, které byly v americkém digitálním undergroundu vždy patrné.

--=:o0o:=--

22. července byla Tajná služba připravena na velký zátah. Na linky hackerů Leftista, Urvila a Propheta, členů LoD, takzvané Atlantské trojky, nainstalovala zařízení DNR, tedy záznamníky, které zapisovaly všechna telefonní čísla vytočená na lince. A nejen to. Leftista toho dne zadržela a provedla u něj domovní prohlídku.

Prohlídky Tajné služby u lidí podezřelých ze zneužití počítačů byly vždy velmi rázné a nekompromisní. Většinou jako „důkaz" zabavila veškeré technické vybavení shromažďované celé roky, včetně telefonů, tiskáren, všech disket včetně disket s licencovaným softwarem, soukromou korespondencí, rozepsanými odbornými pracemi; včetně většiny literatury (manuály, sci-fi knihy, herní příručky pro hry AD&D či Gurps) a všech osobních záznamů. I přestože „oběti" prohlídky nebyly často z ničeho obviněny, nikdy jim nebyl žádný trestný čin dokázán, své vybavení zpátky nedostaly, bylo prostě zabaveno jako „důkaz".

Nicméně „Leftist" byl hacker a člen „Atlantské trojky" k tomu. Další dva jeho kamarádi „Prophet" a „Urvile" byli zadrženi téhož dne, stejně jako „Fry Guy", pachatel přesměrování z Delray Beach. Zadržením „Atlantské trojky" si Tajná služba splnila svůj tajný sen. „Fry Guy", který ke „trojce" nepatřil, se ke všemu přiznal a dokázány mu byly podvody s telefony a kreditními kartami.

Přiznání hackerů a phreakerů je vůbec zajímavý fenomén. V genech tohoto druhu je prý zakódována chvástavost hned za genialitou a technickou mazaností. Většina zadržených pachatelů se policistům přímo chlubila, co dokázala. Stávalo se, že nejdrzejší phreakeři na svobodě dokonce policistům sami telefonovali a vychloubali se svými kousky a svou nepolapitelností.

Druhého října 1989 Senát Spojených států jednomyslně schvaluje Zákon o počítačové zpronevěře a zneužití počítače. To dává policii další možnosti ve stíhání počítačového zločinu. Bude je potřebovat.

--=:o0o:=--

15. ledna 1990 se ze záhadných důvodů zhroutila polovina telefonní sítě AT&T pro dálkové hovory. Druhá polovina sítě nezvládala mocný nápor nevyřízených hovorů. Šedesát tisíc lidí najednou zůstalo bez spojení, přerušeno bylo přibližně sedmdesát miliónů hovorů.

Bylo to něco zcela bezprecedentního. Něco, co se ještě nikdy v minulosti nestalo. Technici AT&T okamžitě zjistili, že zhroucení bylo způsobeno softwarem. Agentům Tajné služby a bezpečákům telefonních společností se zježily chlupy na zátylku. Zcela jistě to musel být útok anarchistických hackerů!

Po nějaké době se sice ukázalo, že pád systému vyvolal chybný řádek zdrojového kódu softwaru ústředen, ale mezitím stihly všechny policejní složky rozjet obrovský zátah na hackery.

Devět dní po kolapsu sítě uskutečnila Tajná služba razii u hackerů Phiber Optika, Acid Phreaka a Scorpiona. První dva byli rovnou obviněni ze způsobení kolapsu.

Šest dní nato, 24. ledna, zastavuje Mentor, autor kultovního textu „Svědomí hackera“ (viz přílohy, na straně 81) z obav před policejní razií svůj ambiciózní hackerský board *Project Phoenix*.

V únoru jsou v Německu „hannoverští hackeři“ shledáni vinnými a odsouzeni. Peter Carl na dva roky, Dirk Brzezinsky na čtrnáct měsíců a Marcus Hess na dvacet měsíců odnětí svobody. Trest jim byl podmínečně odložen.

21. února zabavila Tajná služba veškeré počítačové vybavení za asi 20 000 dolarů včetně necelého gigabytu dat počítačovému expertovi Robertu Izenbergovi, který byl podezřelý ze spolčení s hackerem *Terminem*. Toto podezření nikdy nebylo prokázáno, Izenberg nikdy nebyl oficiálně obviněn ani zatčen, avšak své vybavení ani data zpátky nedostal.

Přestože Project Phoenix již neběžel, Tajná služba provedla ráno 1. března 1990 domovní prohlídku u „Erika Bloodaxea“, jeho spolusprávce. Také jemu zabavila veškeré vybavení včetně telefonu a ani on nebyl nikdy obviněn.

Ve stejnou dobu navštívila tatáž organizace i samotného Mentora. Agenti mu jako „důkaz“ zabavili jeho klon IBM PC-AT, laserovou tiskárnu Hewlett Packard LaserJet II., naprosto legální a velice drahý operační systém SCO-Xenix 286, programy PageMaker a Microsoft Word včetně instalačních disket a dokumentace, odnesli i telefon. Mentorova manželka přišla o svou nedokončenou diplomovou práci...

Mentor byl zaměstnán u společnosti Steven Jackson Games (SJG), která se zabývala přípravou her Gurps, které jsou u nás známy jako „Hry na hrdiny“, tedy cosi na způsob Dračího doupěte či AD&D. Právě k Mentorovu zaměstnavateli se agenti vydali na další razii.

Bruce Sterling o ní v knize The Hacker Crackdown píše: *„Agenti nenechali nikoho jiného vstoupit dovnitř. Povolení k prohlídce, které posléze předložili, nebylo podepsáno. Zjevně snídali v místním stánku s občerstvením, protože uvnitř byly později nalezeny papírové obaly od hamburgerů. Důkladně také okusili gumové medvídky ze sáčku jednoho ze zaměstnanců SJG. Nálepka ‚Dukakis for President‘ byla stržena ze zdi. (...) Jacksonova společnost přišla o tři počítače, několik pevných disků, stovku disket, dva monitory, tři modemy, laserovou tiskárnu, různé elektrické šňůry, kabely a adaptéry (a kupodivu i o malý pytlík šroubků, matiček a podobných drobností). Zabavení BBS Illuminati připravilo SJG o všechny programy, textové soubory a soukromou elektronickou poštu na boardu. Ztráta dalších dvou strojů byla pro firmu stejně závažná, protože na nich byly elektronicky zaznamenané smlouvy, finanční rozbory, seznamy a adresáře odběratelů, údaje o zaměstnancích, obchodní korespondence a neméně důležité koncepty nových her a herních knih. Nikdo ze Steve Jackson Games nebyl zatčen. Nikdo nebyl obžalován z žádného zločinu. Nebylo vzneseno vůbec žádné obvinění. Všechny odnesené věci byly oficiálně zadrženy jako ‚důkaz‘ zločinů, které nebyly nikdy specifikovány.“*

Následujícího dne se vydal Steve Jackson, majitel SJG, v doprovodu svého právníka na místní služebnu Tajné služby, aby získal zpět rukopis již k tisku připravené nové herní knihy „GURPS Cyberpunk“. Agent Tajné služby to odmítl s tím, že tato sci-fi kniha je „příručkou pro počítačové zločince“.

Tento postup byl zcela neopodstatněný a zjevně i velmi nedemokratický. Vláda si jasně koledovala o velký problém. Opoziční síly se začínaly formovat.

O pět týdnů později, 9. května, vydává úřad státního zástupce v Phoenixu v Arizoně tiskovou zprávu, která informuje o celostátním policejním zátahu s názvem „Operace Sundevil“ proti „ilegálním aktivitám počítačových hackerů“. Akce proběhla 7. května a bylo do ní nasazeno 150 policistů ve „dvanácti“ městech po celých Spojených státech (různé zprávy místního tisku uváděly „třináct“, „čtrnáct“ a „šestnáct“ měst). Proběhlo sedmadvacet domovních prohlídek, zabaveno bylo asi 40 počítačů a přibližně 23 000 disket obsahující také legálně koupené počítačové hry, legální software, soukromou elektronickou poštu, obchodní záznamy a osobní korespondenci. Vyřazeno z provozu bylo na

25 boardů, z nichž některé jako board Dr. Ripco ovšem svou činnost vzápětí obnovily. Pouze tři lidé byli zatčeni.

--=:o0o:=--

Reakce na podobný postup vlády již nešly déle udržet. Hackeři sice vládli znalostmi počítačů a telefonních systémů, ale často to byli lidé zalezlí ve svých doupatech, nervózní bez svých počítačů a nedokázali příliš ovlivňovat veřejné mínění. Ke slovu přišli obránci lidských práv. Není přeci možné připustit nedemokratické praktiky a teror státních orgánů!

V červnu se textař kapely Grateful Death John Perry Barlow a Mitchell Kapor, zakladatel Lotus Development, rozhodují založit Nadaci elektronického pohraničí (*Electronic Frontier Foundation, EFF*). Cílem nadace je „financovat, uskutečňovat a podporovat snahy, které by právní cestou demonstrovaly, že Tajná služba USA uskutečňovala preventivní cenzuru publikací, omezovala svobodu slova, neoprávněně zabavovala vybavení a data, užívala nepřiměřenou sílu a všeobecně postupovala arogantně, despoticky a protiústavně“. Rozsáhlou finanční pomoc nabízejí kromě Kapora ještě Steve Wozniak (spoluzakladatel Apple) a John Gilmore (spoluzakladatel Sun Microsystems) .

Podle slov zakladatelů by EFF neměla být fondem na podporu hackerů, jejím účelem je spíše obhajoba lidských práv a svobody informací.

24. července čeká EFF první důležitý a vlastně i precedentní soudní spor. Vzpomníváte si na „dokument 911“, který byl zveřejněn v Phracku? Knight Lightning, jeden ze dvou vydavatelů tohoto časopisu, je souzen za jeho zveřejnění a podíl na jeho krádeži. BellSouth tvrdí, že dokument má hodnotu 80 000 dolarů a s jeho použitím mohl kdokoliv ohrozit životy lidí v nebezpečí.

Hackského novináře zastupuje EFF, která nakonec vyrukuje s překvapujícím faktem, že dokument je šířen samotnou BellCore (vývojové laboratoře Bellu) za 13 dolarů a je k dispozici ve větších technických knihovnách.

Soud je díky tomu nakonec odložen na neurčito a již nikdy nebyl obnoven. Pro EFF a pro svobodu projevu ve Spojených státech to znamenalo významné vítězství a jak se zdá, vzalo to poslední síly velkému zátahu na hackery.

V září 1991 uznal soudce Bua žádost o výmaz a zabezpečení záznamů o Knight Lightningovi. Tajná služba USA dostala příkaz vy-

jmout a zničit všechny záznamy o jeho případu.

„Fry Guy“, pachatel přesměrování z Delray Beach, je 14. září podmínečně odsouzen na 44 měsíců a 300 hodin veřejně prospěšných prací.

--=:o0o:=--

Podívejme se nyní opět na Kevina Poulsena. Na začátku září 1990 běží v televizní stanici NBC upoutávky na televizní dramatizaci Kevinových zločinů s názvem „Temný Dante“. Na natáčení mají být jako vždy přítomni agenti FBI a diváci mají možnost telefonovat přímo do studia. Připraven je také štáb, který je schopen okamžitě vyjet na místo, kde by mohly být zjištěny nějaké další údaje o případu. Kevin dopisem varuje producenta pořadu, aby zvážil některá obvinění a formulace v pořadu. Dodává, že například přezdívku „Temný Dante“ použil naposledy jako dítě.

Producent nijak nereagoval a skladbu pořadu nezměnil.

Na začátku živého vysílání pořadu odpojuje Kevin všech 40 linek, které vedou do televizního studia a sleduje pořad z přenosné televize ve svém sportovním autě.

Kevin už dávno ví, že ho zatknou, čeká jen kdy a snaží se ten okamžik co nejvíce oddálit.

V únoru 1991 byl zadržen hacker *Phiber Optik*. Obviněn však mohl být jen ze zneužití triku s předvolbou 900 k bezplatnému volání. Byl shledán vinným a odsouzen k 35 hodinám veřejných prací.

Kevin Poulsen je zatčen 10. dubna 1991 v samoobsluze, při výběru rybí polévky v konzervě. Koncem června je zatčen i jeho spolupracovník, Eric Heinz, který je však později propuštěn jako špicl FBI. Pomáhá při zatčení Kevinova kamaráda Rona Austina.

Kevin je souzen 10. dubna 1995, po čtyřech letech odkladů. Dostává trest 51 měsíců vězení. Většinu vězení má už tou dobou za sebou.

--=:o0o:=--

Bohužel, pád sítě z 15. ledna 1990 nebyl poslední. 17. září 1991 zkolabovala část telefonní sítě v New Yorku. Bez spojení byla i tři letiště, která musela zrušit více než 500 letů a dalších asi 500 letů mělo zpoždění. Problémy se spojením mělo tedy přibližně 85 000 lidí. Po

trapné události s domělým útokem na telefonní síť již AT&T nemohla ukázat na temné zlé hackery a poštvat Tajnou službu a policii na lov. Kolaps z 15. ledna byl jednou z dalších neopakovatelných záležitostí, které jsme při své procházce americkým digitálním undergroundem prozkoumali.

--=:o0o:=--

Útoky na státní instituce a armádu nikdy neustaly. Ministerstvo obrany Spojených států například přiznává, že v roce 1995 se podařilo ve více než 162 500 případech proniknout do sítě Pentagonu. Celkově je prý pokusů o útok na čtvrt milionu ročně, avšak úspěšných je asi jen 64% hackerů. A pouze asi každý sto padesátý z nich je stíhán a odhalen.

17. března 1998 Pentagon přiznává, že hackeři ze skupiny MOD pronikli v říjnu 1997 k programu, který kontroluje vojenské satelity.

V únoru 1999 list The Sunday Business s odvoláním na bezpečnostní zdroje uvádí, že hackeři přebírají kontrolu nad britským vojenským komunikačním satelitem a požadují výkupné. Podle zdrojů listu hackeři v první polovině února změnili dráhu jednoho ze čtyř britských vojenských komunikačních satelitů a zastavení manipulací podmiňují složením výkupného. „Je to naše noční můra," vyjádřil své pocity jeden ze zaměstnanců tajné služby. Vojenští stratégové tvrdí, že při jakémkoliv (i jaderném) útoku na Británii jsou případnému agresorovi největším trnem v oku právě komunikační systémy. „Nejedná se o nějaké počítačové nadšence, kteří jen tak naslepo zkoušejí, co se dá. Je to velmi vážné a vyhrožování to dělá ještě vážnějším," cituje agentura Reuters bezpečnostní zdroj. Policie se odmítá ke kauze vyjádřit, protože vyšetřování je prý ve velmi citlivé fázi. Nevyjadřuje se ani britské ministerstvo obrany.

V této souvislosti se nabízí mnoho otázek – skutečně se všechny tyto průniky uskutečnily? Když má každá větší společnost hardwarově oddělenou vnitřní síť od vnější, proč tak neučinila armáda Spojených států či britská armáda? Jestliže hackeři mají skutečně přístup k družicím, proč nezveřejňují například satelitní snímky? A jestliže mají přístup k družicím, které žádný novinář nemůže zkontrolovat, nemají také přístup k mnohem prozaičtějším datům? A není to vše jen lobby, která má oběma armádám zaručit více peněz na zabezpečení?

--=:o0o:=--

Kapitola 3

S.irup E.mergency R.eaction T.eam

SERT, předchůdci CzERTu. Mazali servery s ilegálním softwarem, hackovali na Slovensku, v Čechách, v Maďarsku a v Polsku. Vydali o sobě i oficiální agenturní zprávu.

Jak už víme, americké federální autority ustanovily v roce 1988 organizaci CERT, která měla pomoci s řešením počítačové bezpečnosti ve státní správě i v soukromém sektoru. CERT dostal za úkol shromažďovat a rozšiřovat všechny informace o útocích na počítačové systémy a informace o chybách (angl. *bug*) v bezpečnosti. Organizace vydala od té doby stovky zpráv (advisory) o bezpečnostních chybách, které každý zodpovědný správce serveru pravidelně prochází a chyby ze svého systému odstraňuje[1]. 25. března 1996 napsal Pajkus, slovenský hacker a pravidelný čtenář advisories CERTu, parodii na jedno takovéto oznámení. Ve svém lehce laděném textíku popisuje žargonem počítačové bezpečnosti závažnou chybu (*bug*) v bezpečnostním systému jahodového sirupu. Plastovou láhev s jahodovým sirupem můžeme totiž otevřít tak, aby „bezpečnostní pásek“, normálně při otevření lahve odtržený od zátky, zůstal se zátkou v jednom celku. Dosáhneme toho tak,

[1]Tyto zprávy můžete dostávat i vy elektronickou poštou, stačí poslat email na adresu cert-advisory-request@cert.org a do předmětu zprávy (subject) zadat text SUBSCRIBE vaše-emailová@adresa. Advisories CERTu by měly patřit k povinné četbě každého zodpovědného správce serveru.

že celou zátku i s páskem pevně uchopíme a otáčením lahev otevíráme. Pokud bezpečnostní pásek tiskneme k zátce dostatečně silně, v průběhu procesu se neoddělí. Do otevřeného systému nyní můžeme vložit cizí objekty, nazývané občas viry či trojské koně, jako jsou žížaly, kamínky, slimáci a podobně a celý systém znovu uzavřít, takže se tváří jako neporušený. (originální text *Sirup bug SERT Advisory* najdete v příloze na straně 87).

Pajkus text ukázal svým kamarádům Dzajrovi, Dzimimu a Bebetovi, kterým se zalíbil, stejně jako myšlenka jeho použití jako hlavního motta hackerské skupiny. Zbýval už jen název. Rozhodovali se mezi Sirupem a SERTem, druhý návrh nakonec vyhrál.

Hackeři se pustili do svých útoků, převážně na systémy Unix a zvlášť Linux.

Linux je unixový operační systém, vyvinutý studentem Linusem Torvaldsem a zcela volně šiřitelný na základě Obecné veřejné licence (GNU GPL)[2]. Jeho oblíbenost a vysoká efektivita a stabilita je dána především tím, že zdrojové kódy celého operačního systému jsou volně k dispozici a proto si je může upravovat podle svého a samozřejmě i zefektivňovat každý, kdo se alespoň trochu vyzná v jazyce C. Na jeho vývoji spolupracují zcela volně nezávislí vývojáři z celého světa. Linux je typickým operačním systémem nejen studentských a školních serverů, ale i některých komerčních společností. V době psaní této knihy je Linuxu přikládán stále větší význam právě i v komerční sféře. Pro svou velkou dostupnost stal také jedinečným způsobem, jak poznat systémy typu Unix a není se co divit, že na něm pracuje většina hackerů. Linuxy jsou totiž velmi stabilní a jejich volné pojetí je velice vzdáleno strategii Microsoftu, který velké množství hackerů upřímně nenávidí.[3] Avšak stejně jako Linux sám o sobě není synonymem bezpečnosti, neznamená to, že hackeři útočí pouze na linuxové stroje či na všechny Linuxy.

Protože Internet na Slovensku se tehdy skládal z relativně malého množství serverů, pracovali hackeři ze SERTu většinou v zahraničí – v Maďarsku, Polsku a Čechách. Tyto tři státy si vybrali, protože byly blízko a spojení s nimi bylo tedy rychlé, ale nebyly zase tak blízko, aby je to ohrozilo. Vždycky je lepší pracovat někde dál od domova, tvrdí s úsměvem Pajkus.

Pro útoky v Maďarsku používal Dzajro docela klasickou metodu – slovník neboli wordlist. Ta je založená na faktu, že většina lidí používá všeobecně známá a uhodnutelná hesla. Existuje slovník nejčastějších

[2] viz např. `http://www.gnu.cz`

[3] další informace o Linuxu naleznete na adrese `http://www.linux.cz`

Když se správce serveru místo obvyklé výzvy k zadání hesla zjevilo toto logo složené z ASCII znaků, věděl, že je zle...

hesel, které na daném serveru a pro určitého uživatele zkouší speciálním programem tak dlouho, než heslo uhodne. Když hacker tímto způsobem získá nějaký přístup do stroje, může získat soubor s dalšími hesly, rozšifrovat je a přihlásit se jako správce systému.

Obecně je několik možností průniku. Ta první je již naznačená – hacker uhodne heslo běžného uživatele. Pokud je systém skutečně na úrovni a bez bezpečnostních chyb, může z takto získaného stroje podnikat jen další výpady. Pokud jsou v systému bezpečnostní chyby, dají se zneužít k získání operátorského přístupu *(root shell)*, a to ze získaného konta normálního uživatele či přímo z venčí.

Když má hacker *root shell*, chce po sobě samozřejmě co nejdříve zamazat stopy. V tom si pomůže automatickou úpravou záznamů o činnosti systému (logů) a upravenými systémovými programy, které nezobrazují jeho přítomnost v systému. Server je získán, plně pod hackerovou kontrolou. Většinou z něj podniká výpady dál, uchovává si na něm své hackerské utility nebo jej používá k přesměrování útoku (většina útoků je přesměrována přes 3-6 strojů, takže útočník je jen těžko zjistitelný). Může na něm také nainstalovat utilitu zvanou sniffer, která zachytává vše, co přeběhne po TCP portu, tedy i hesla do dalších a dalších strojů, ke kterým putují pakety přes nabouraný server.

Kromě Polska a Maďarska si SERTi oblíbili ještě dvě země – Finsko a Taiwan. Hlavně kvůli jejich rychlým linkám a velkému počtu špatně zabezpečených linuxových serverů. Některé znich byly dokonce umístěny v domácnostech, s rychlým připojením a slabým dohledem. *„V tychto dvoch krajinach sme mali casto stroje, ktore sme volali ‚stargate', alebo ‚redirektory', z nich sme utocili na cielove masiny (vo Vychodnej Europe),"* vzpomíná s odstupem let Pajkus. *„Tiez sme z nich*

```
  .:::::::..,::::::  ::::::::..  ::::::::::::
;;;`    `;;;;''''  ;;;;``;;;;;;;;;;;;;''''
'[==/[[[[,[[cccc    [[[,/[[['       [[
  '''     $$$""""   $$$$$$c         $$
 88b     dP888oo,__ 888b "88bo,     88,
 "YMmMY" """"YUMMMMMMMM   "W"      MMM
```

Sirup Emergency Response Team

Další „SERTovská“ ukázka takzvaných ASCII Art – log a obrázků poskládaných z různých znaků ASCII (American Standard Code for Information Interchange). Pozkládat obrázky z písmenek je dávný způsob, jak zobrazovat „grafiku“ na čistě textových konzolích. Jednou bude patřit do učebnic folkloristiky.
zdroj: SERT

. . . a toto je hlavní stan (tzv. server) celé mocné organizace SERT.
zdroj: `http://hysteria.sk/sert`

spustali skenovacie roboty (jednoduche skripty, casto pisane len v bashi nad nmap-om, ktore hladali zranitelne masiny). V Taiwane a Finsku sme na hacknutych masinach prevadzkovali aj vlastne BBS, niekedy dokonca pod vlastnou domenou tretej urovne, ked sme hackli nejaky DNS server.

Okrem Internetu bola vtedy stale silna scena BBSiek po telefonnych linkach. Na tie sme chodili z hacknutych masin, ktore boli pripojene na Internet, ale ktore mali v sebe aj modem. Jeden taky casto pouzivany sme mali na Madarskej Akademii Vied v Budapesti. Telefonovali sme odtial na BBSky po celom svete.“

−−=:o0o:=−−

SERT je dnes velmi známý kauzou kolem českých serverů s tzv. warezem. „Warez“ je v internetovém slangu nelegální software a na Internetu jsou celé servery, kde si počítačoví piráti warez zadarmo stahují. Tato praktika je samozřejmě ilegální a o to horší je, když zálibu ve warezu mají správci školních serverů, zakoupených za nějakým bohulibým účelem například z grantu. Archív ilegálního software na stroji znamená nejen úbytek diskového prostoru na úkor běžných uživatelů, ale i snížení přenosové kapacity z důvodu neustálého stahování programů lidmi zvnějšku. Správce takového systému většinou nejprve omezí diskový prostor pro běžné uživatele (sníží kvóty) a kvůli přenosové rychlosti zakáže například stahování více souborů najednou. Sebemenší přestupky pak razantně trestá.

SERTi při svém „běhu po mašinách“ občas narazili na školní server plný warezu. To byl případ například serverů diana.troja.mff.cuni.cz a kmotr.pf.jcu.cz.

Správcům obou serverů poslali v dubnu 1996 email tohoto znění:

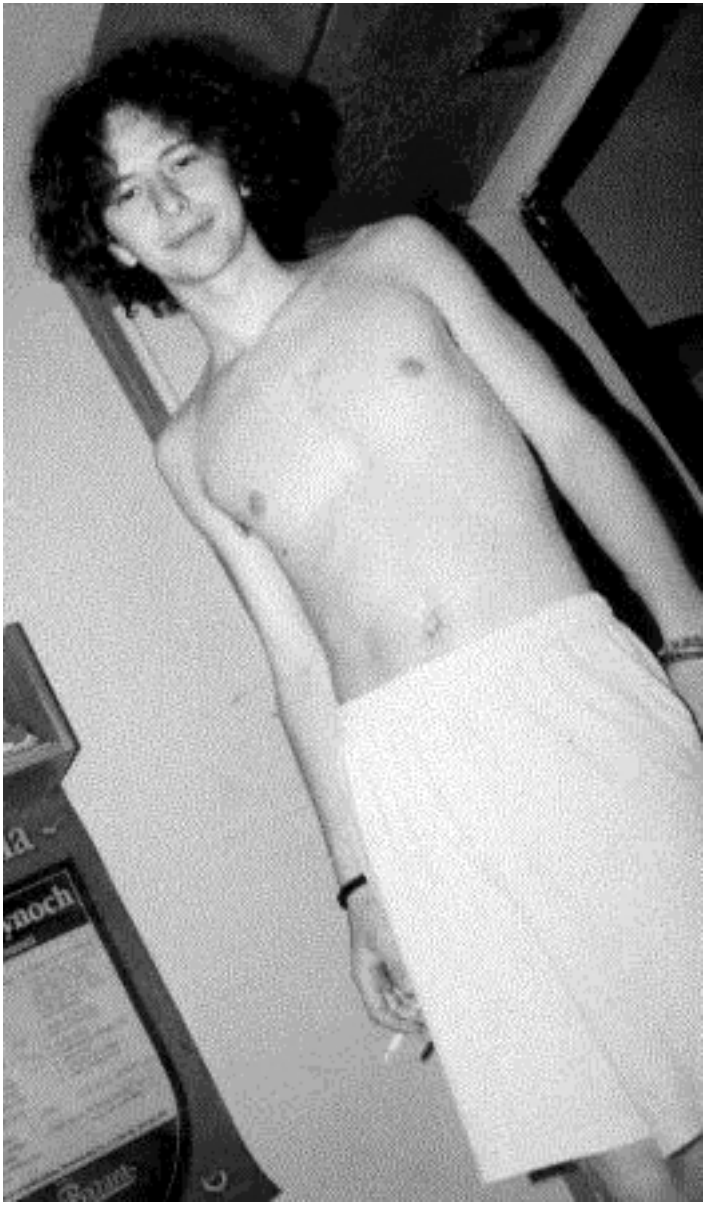
„Cau ty zasrany warezak,

Ludia ako ty su mi odporni... Za statne peniaze si na skolskych servroch budujete warez sajty a userom prikazujete prisne quoty. Polka tvojej masiny je posrany winblows warez. Rooti ako ty spinia vzduch, kazia linky a zasravaju hard disky warezom.

Mas tam peknu masinu, slusny hardware, pekne nakonfigurovany.. tak preco namiesto normalnej prace furt warezujes ? Chod do pice a zer Sirup bratku,

S pozdravom,

m0dus



Saso by prý nemohl být zachycen jinak než s cigaretou.

zdroj: http://hysteria.sk/sert

PS: nie si prvy ani posledny“[4]

Hackeři smazali archívy ilegálního software a upozornili správce, že v případě jeho obnovení smažou celý stroj. Uživatelé, kteří se k systému připojili, dostali následující hlášení: *„Vazeni uzivatelia, Na tomto servri bol doteraz velky archiv s nelegalnym licencnym softwarom, co je v rozpore so zakonom. Tento archiv bol odstraneny. Je mozne ze bude tento server nejaku dobu mimo prevadzky z dovodu vysetrenia priciny zmiznutia tohoto nelegalneho softwaru. Za tento vypadok sa ospravedlnujeme, S pozdravom, Modus“*

To bylo něco u nás zcela bezprecedentního. Hackeři vzali „spravedlnost do svých rukou“, stali se jakýmisi Janošíky digitálního věku. Root „Kmotra“ jménem Ludvík Friebel se omlouval tím, že ve školství nejsou peníze, někde software brát musí. Archív obnovil. Hackeři oponovali tvrzením, že má na serveru i spoustu her a v srpnu 1996 ze SERT party v Košicích „Kmotra“ veřejně přes satelitní linku smazali.

Není pochyb o tom, že na smazání cizího serveru neměli hackeři nejmenší právo. Ani o tom, že správci školních (ale ani žádných jiných) serverů už vůbec nemají žádné právo umísťovat na univerzitní počítače ilegální programy. Představa, že někdo kontroluje legalitu vašeho software tak, že vám sám a hezky natvrdo smaže všechen ilegální, je trošku drsná.

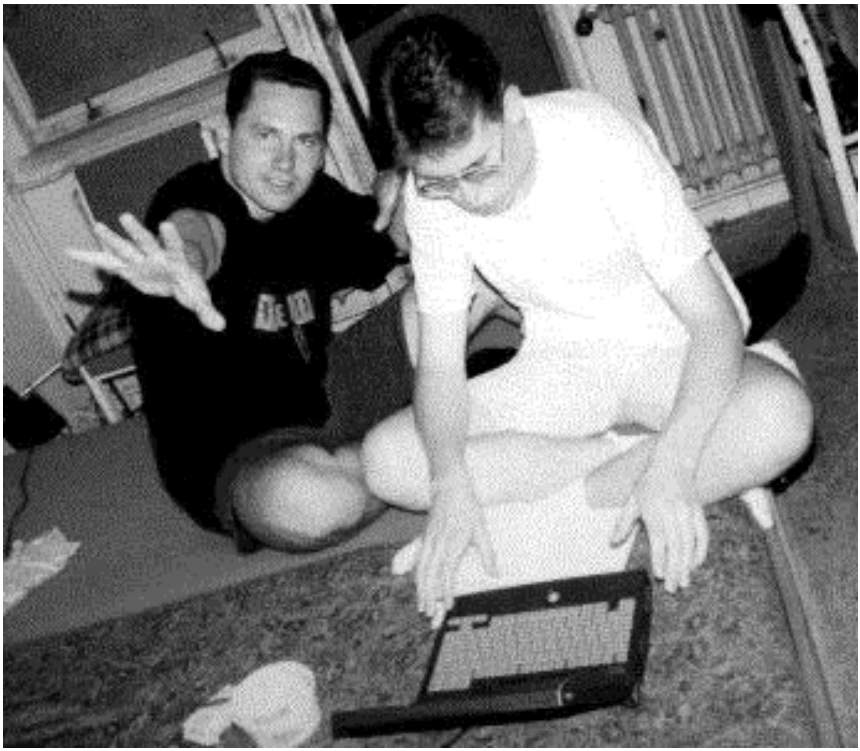
Pajkus však popírá, že by se se svou skupinou stavěl do pozice nějakých moralistů či ochránců autorských práv. Sám přiznává, že také používal warez, když měl MS Windows a dodnes si sem tam něco ilegálního stáhne. Na Linuxu ale nejčastěji ani žádný ilegální software není zapotřebí, protože jsou k dispozici (kvalitnější) volné programy.

SERT se prý na warez servery nespecializoval, ale když se nějaký naskytl...

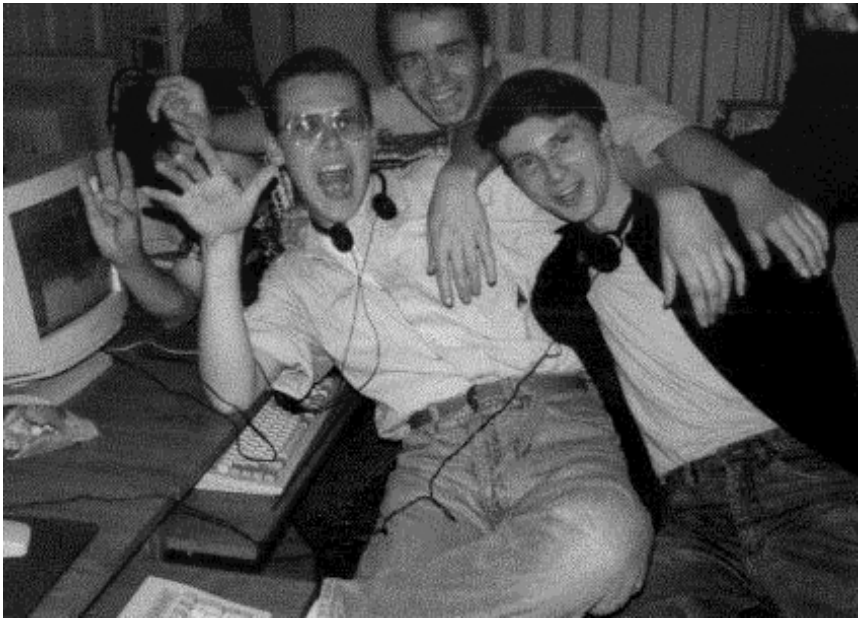
Tato kauza vyvolala na Internetu celkem zajímavý poprask, ale veřejně se ke smazaný serverům raději nikdo příliš nehlásil. SERTi mezitím seděli na nabouraných serverech a pozorovali korespondenci správců dumajících společně o tom, jak se nejspíš hackeři do jejich systémů dostali a o tom, kam schovali své utility a jak je asi používají. Jen občas hackeři připsali ironický komentář do soukromé korespondence, aby se na ně nezapomnělo.

−−=:o0o:=−−

[4] poskytl Pajkus



Pajkus (aka m0dus, vlevo) a Dzajro (aka Debo, vpravo) hackují z internátu v Mlynskej doline v Bratislavě (léto 1996)..
zdroj: `http://hysteria.sk/sert`



Noční akce v sídle Zdennyho zaměstnavatele v Košicích.
zdroj: `http://hysteria.sk/sert`

Rodinné foto SERTu z výletu do Košic.
zdroj: `http://hysteria.sk/sert`

18. září 1996 se objevila na webové stránce Tiskové agentury Slovenské republiky (TASR, `http://www.tasr.sk`) tato zpráva o slovenských hackerech ze SERTu:

„Niekolko slovenskych pocitacov a serverov napojenych na sieti Internet bolo tento tyzden tercom utokov skupiny hackerov, nazyvanych Syrup Emergency Reaction Team (SERT). Dovodom ich utoku bolo upozornit na rozmach zneuzivania Internetu na rozsirovanie kradnuteho licencneho softwaru. Medzi napadnutymi pocitacmi boli aj servery firiem zaoberajucimi sa poskytovanim sluzieb suvisiacichs pripojenim k sieti Internet, ako napriklad Slovak Academic Network (SANET), alebo Netlab s.r.o., ale aj mnoho skolskych servrov, o ktorych je zname ze su zneuzivane na distribuciu nelegalneho softwaru. Na napadnutych serveroch bol vymazany vsetok najdeny nelegalny software a boli na nich instalovane propagacne stranky povzbudzujuce k boju proti sireniu kradnuteho softwaru.“ Text se tvářil jako zcela normální agenturní zpráva, podepsán pod ním byl redaktor Roman Kebisek a některé noviny jej také přejaly. Teprve když Pavol Mederly (o kterém

ještě uslyšíme později) z výpočetního centra Komenského University v Bratislavě zavolal do „oddělení slovního zpravodajství“ TASR, zjistil, že pan Kebisek ma tou dobou dovolenou. Zjistil také, že server TASR běží na relativně staré (a tedy i nepříliš bezpečné) verzi Linuxu. Když Mederly na článek agenturu upozornil, byl z Internetu stažen.

Ano, je to tak, hackeři ze serveru zfalšovali dokonce i zpravodajství oficiální tiskové agentury svého státu!

−−=:o0o:=−−

Tou dobou provedli Pajkus, Dzimi, Dzajro a Bebeto a další jejich přátelé mnoho útoků a změn stránek například slovenského poskytovatele Internetu NetLab; Slovak Academic Network (SANET), či deníku SME (na jeho titulní stranu umístli nápis „Boli SME, ale už NIE sme“). Pořádali SERT Parties, odkud podnikali další výpady, scházeli se tajně po nocích v prezentačním středisku Zdennyho zaměstnavatele v Košicích...

Jejich konec se však neodvratně blížil.

−−=:o0o:=−−

V červnu 1996 už byly aktivity skupiny tak rozsáhlé, že to nemohlo zůstat bez povšimnutí, tím méně ze strany výpočetního centra University Komenského v Bratislavě. Na události, které bezprostředně vedly k pádu SERTu vzpomíná dnes Pajkus takto: *„SERT vtedy sniffoval kompletne UK v blave a okrem ineho mal pristup aj na novell siet na MFF UK. mali administratorske heslo na novell, tak si debo a bebeto dali na novell napevno doom... riadna somarina.. vsetci o tom vedeli.. a dmin na to prisiel a zacal vysetrovat.. zistil ze utoky pochadzaju z masiny cicero.fmph.uniba.sk ktory administroval ruuto, dalsia spriaznena dusa. cicero.fmph.uniba.sk bol vtedy nieco ako hlavny stan SERT... takze prisli do kancelarie Mederly este s niekym, odpojili cicero zo zasuvky (nedali ani shutdown), schytili ho pod pazuchu a odniesli si ho do vypoctaku asi na tyzden a tam ho studovali.. odtial mali tolke dokazy..“*

Hackeři známí jako Dzajro a Dzimi dostali děkanskou podmínku, neboli byli podmínečně vyloučeni. Ve skutečnosti dostala zřejmě (neoficiální) podmínku Univerzita Komenského od Sanetu, přes který byla

připojená k Internetu. Buď vyhodí hackery, nebo Sanet prostě odstříhne dráty. Tak velké riziko si nemohl Sanet dovolit. Dzajro a Dzimi vyletěli od první zkoušky, ke které přišli.

„Raději vás necháme vyhodit, než abychom riskovali, že ztratíme připojení," řekl jeden z univerzitních pedagogů hackerům.

--=:o0o:=--

Po této ráně pokračoval SERT stylem „od deseti k pěti".

Dzajro šel na elektrofakultu a po nějaké době přestoupil na Matfyz.

Dzimi chodil s „nějakou podivnou holkou," jak říká Pajkus, která ho stěží pouštěla s kamarády do hospody a ještě méně mu byla ochotná tolerovat noční hackerské eskapády.

Bebeto si našel práci v počítačové společnosti, ze školy mířil rovnou do práce, vracel se večer.

„Byl do toho strašně nadšenej," říká se smíchem Pajkus, když si vzpomene na okouzlení svého kamaráda nad tím, jak snadno si může v komerčním sektoru vydělat peníze. Bebeto sám byl expertem hlavně na Windows 95, které dokázal geniálně zneužívat a elegantně po nich „běhat".

Zdenny šel na vojnu.

Pajkus osaměl.

V každém případě se SERT zapsal do československé počítačové historie jistým průkopnictvím. Vytvořil jedny z prvních místních hackerských nástrojů – české a slovenské slovníky nejčastěji používaných hesel pro tzv. wordlisty, vydával vlastní rootkity, tj. modifikované části Linuxu určené k vytváření „zadních vrátek" do serverů a skrývání hackerů, kteří v nakažených strojích operovali. Mezi tyto nástroje patřily i „skenery" a skripty na automatické vyhledávání strojů s bezpečnostními dírami.

Kapitola 4

Démon českého a slovenského Internetu

Kdo byl CzERT? Co ho vedlo k jeho kouskům? Jak pracoval? Kam se dostal? Byl dopaden? A jak vlastně skončil?

V listopadu 1996 člověk či skupina s označením CzERT nabourala internetový server Armády ČR a upravila jeho titulní stránku. Hackerská „moc“ se v České republice poprvé ukázala široké veřejnosti. Neviditelný pes, internetový deník Ondřeje Neffa o tom přinesl nadšené zpravodajství a modifikovanou verzi stránek uložil do „psího hackerského archívu“. Jak upravené stránky vypadaly, se můžete přesvědčit z grabu na následující straně.

Noviny se poprvé chytly případu hackingu. Hackera označily za „démona českého Internetu“. Armáda rezolutně popírala, že by došlo k úniku tajných informací. Už to pro normálního člověka vypadá podezřele. Avšak pokud hackeři změní stránky například nějaké banky na Internetu, neznamená to, že pronikli do jejich sítě. Znamená to pouze, že se dostali do webového serveru, který je většinou oddělen od vnitřní sítě, či je vůbec fyzicky umístěn někde úplně jinde, například u firmy, která stránky na zakázku vytvářela. Navíc podle výkladů některých odborníků na bezpečnost k žádným únikům ani dojít nemohlo, protože prý armáda shraňuje všechny informace v obřích kovových registračkách a nikoliv na počítačových sítích.

CzERT v krátkém časovém období změnil i stránky Ministerstva zdravotnictví ČR (v CzERTově podání Ministerstvo smrti Čínské re-

Pajkus tak, jak se dříve ukazoval na své domovské stránce a na serveru MAmedia...
zdroj:http://hysteria.sk/pajkus

publiky) a společnosti Hollywood Classic Entertainment. Poté poskytl vůbec první rozhovor Ondřeji Neffovi (najdete jej v příloze na straně 91) ve kterém se zmiňuje o své motivaci, stylu práce a filosofii. Jakékoliv detailnější informace ale nechce sdělit, přestože tvrdí, že na anonymitu moc nedá.

Několik dní nato se ozval správce onoho nabouraného serveru, který říká, že i tak dalo dost práce své nadřízené přesvědčit o nutnosti webových stránek a že po útoků musel být server uzavřen a jeho další osud není jistý

--=:o0o:=--

Možná se ptáte, má-li CzERT něco společného se SERTem.

Má. Hlavní postavu SERTu, Pajka (který si ovšem v té době říkal spíš m0dus). Myslím, že je právě nejvhodnější čas, povědět si o Pajkovi něco bližšího.

K hackování se tento slovenský hacker dostal na Texaské Universitě v Austinu, kde studoval. V sedmnácti letech se tam seznámil s o čtyři roky starším Italem, také studentem.

. . . a tohle je vše, co na svých stránkách ukazuje dnes.
zdroj:http://hysteria.sk/pajkus

Dnes má firmu na zabezpečení počítačových systémů. Ptáte se, jak může hacker zabezpečovat servery? Já jsem se zeptal také.

„Docela normálně," říká Pajkus, „tím že hackuješ, máš mnohem větší informace o bezpečnosti, než normální správce, který tak maximálně sedí za serverem a klepe se, aby ho někdo nenapadl. Tím, že aktivně pronikáš do systémů, znáš je dokonale, víš co zalepit." Navíc zcela vážně tvrdí, že nikdy nesměšuje práci a zábavu. Není těžké si představit jeho motivaci. Jednou je prostě jeho cílem proniknout do systému, jindy ho zcela ochránit. Nicméně říká, že jeho firma ho v současné době neživí a funguje jen zřídka.

Proč proniká do systémů?

Prý pro zábavu. V jeho akcích není žádná hlubší filosofie, prostě jenom zábava, výzva k překonání problému. Chce také upozornit na závažná opomentutí v bezpečnosti systémů. Většina útoků je podle něj možná jen díky tomu, že správci jsou často lehkomyslní lajdáci.

„Každá firma chce být honem na Internetu, vytáhnou server z krabice, z cédéčka nainstalují systém a radují se a halekají. O bezpečnosti nemají někdy ani tušení," říká.

Odhalení se příliš nebojí. Policie mu prý nemá co dokázat a správci napadených serverů to berou spíše jako reklamu a recesi.

--=:o0o:=--

Když se rozpadl SERT, zůstal Pajka sám. Po nějakém čase se zkontaktoval s Genericem, studentem medicíny z Moravy. Generic se domníval, že SERT znamená Slovak Emergency Response Team (ve skutečnosti Sirup Emergency..., jak už víme) a odvodil od něj název CzERT, jako Czech Emergency Response Team, což se většinou vyslovuje jako „Čert".

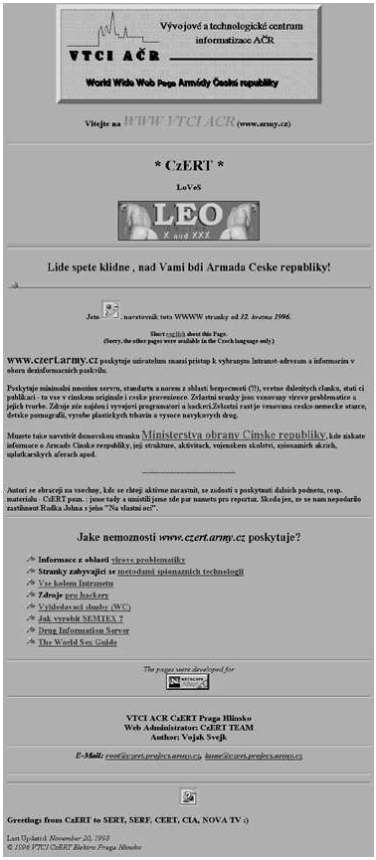
Podle Pajkových slov byl Generic začátečník, což občas přinášelo problémy. Jednou prý požádal Pajka, aby mu dal přístup do nějakého stroje, aby si mohl hackování také vyzkoušet. Dostal tedy backdoor (zadní vrátka) do Nitranské university s varováním, ať po sobě smaže stopy z logů. Generic údajně poběhal po mašině a aby smazal záznamy o sobě z logu, otevřel mnohamegabytový soubor v textovém editoru. Slabý počítač se z toho zhroutil. Na čištění logů hackeři totiž hackeři obvykle nepoužívají textový editor, ale speciální prográmky. Mimochodem armádou používaná ochrana proti zpětné úpravě logů je prý jejich průběžný tisk. Také řešení, i když u serverů s hustším provozem asi finančně neúnosné.

Poté, co kdosi podepsaný „-rwsr-xr-x" (což je popis práv k souboru v systému Unix) hacknul Mendelovu universitu v Brně (a změnil ji na Lesbickou universitu v Brně, údajně to byla odplata za vyhazov ze školy), vyzval Pajkus útočníka, aby se mu ozval. Přihlásili se dva kamarádi Seteuid, linuxový hacker, a Dusheen, programátor v jazyce C. Ti se k CzERTu přidali a společně podnikali průniky. Ovšem v oficiálních prohlášeních o sobě kolektivní identita CzERTu mlžila výroky o tom, že „není jasné, kolik nás přesně je."

„Nejsme organizace, spíše nás spojuje podobná filosofie," říká Pajkus.

--=:o0o:=--

Dalším velmi sledovaným a mírně kontroverzním útokem byl průnik do již několikrát zmiňovaného serveru MAmedia. I na této sofistikované internetové komunitě se samozřejmě objevoval hacking a warez. Warez – to bylo téma dalšího CzERTovského útoku z 15. února 1997. Pajkus věděl, že Milan Votava, správce MAmédií, nemá server u sebe doma či v kanceláři a musí ho spravovat dálkově po Internetu.



Upravená stránka Armády ČR
zdroj: `http://www.army.cz`

Rozfázovaná animace démona od Mika Stricka.
zdroj: `http://www.geocities.com/SoHo/2223`

Heslo nakonec zachytil Seteuid, který už v té době sniffoval provoz téměř celé sítě Cesnet. Po zhruba pěti dnech příprav se Pajkus mohl v sobotu večer přihlásit jako správce (root). Kolem 20:00 odhlásil Votavu, právě spravujícího server, a zakázal mu heslo. Během pěti minut přebarvil stránky načerno a umístil na ně animaci rudého démona s ostrými zuby, kterou někdo poslal do auditoria. Na stránkách zveřejnil i seznam častých návštěvníků auditoria warez na MAmediích, včetně jejich skutečných jmen, adres a telefonů. Votava se však za pár minut vrátil přes zadní vrátka ve WWW a shodil celý stroj (včetně Pajka) a předělal všechny stránky do původní podoby. Pajkus se ovšem kolem 21:00 opět dostal dovnitř, shodil celý stroj a kompletně zablokoval přístup, protože věděl, že stroj je fyzicky u Cesnetu a kdyby ho chtěl Votava získat zpátky, musel by sednout do auta a jet nabootovat ze systémové diskety. Votava pak Pajka kontaktoval na MA, navázali spolu hovor a dohodli se, že Votava dostane zpátky přístup a nechá Pajkovi stránky do pondělí na serveru. Pajka také na měsíc dostal správcovský přístup a mohl zasahovat do běhu MAmédií.

„Zajímavé na tom bylo, jak jsme si psali," říká Pajkus „Měl jsem totiž tna MAmedii nainstalovaný upravený telnet daemon, kteý mi umožňoval psát mu přímo na obrazovku. Vlezl jsem mu na obrazovku, pustil textový editor a tam jsme si psali."

Milan Votava v rozhovoru pro časopis Internet později uvedl, že hacknutí stránek serveru pro něj bylo vlastně dobrou reklamou a že CzERT se nejspíš stane čímsi jako jeho bezpečnostním konzultantem. Krátce po změně stránek hackerem zkontaktoval ČTK, která o tom vydala zprávu.

Pajka se svým správcovským (root) přístupem „zpříjemňoval" warezákům život. Nejen že zveřejnil na titulní stránce onen seznam včetně jejich plných jmen, získaný skupinou -rwsr-xr-x, ale zasahoval i do jejich auditoria. Nainstaloval do něj například skript, který ze všech slov „software" v příspěvcích udělal „warez", z „Microsoftu" „Mickeysoft", z „Windows" „Winblowz" a podobně.

Povídal si také s jedním Slovákem žijícím ve Francii o tom, jak nejlépe auditorium o ilegálním softwaru „pojmenovat". Jeho rada byla „staré prádlo". Zajímavou prý pointou je, že ono označení se mezi samotnými šiřiteli ilegálního software ujalo.

„Tuhle jsem seděl v hospodě a sedeli tam nějací dva kluci a bavili se nějak jako: ‚Nemáš nějaké nové staré prádlo?' ‚Ne, nemám, potřeboval bych nějaké staré prádlo vypálit!' a podobně," říká Pajkus.

––=:o0o:=––

O necelý týden později, v pátek a v sobotu, došlo k útoku na Seznam, pravděpodobně nejnavštěvovanější český server. Zajímavostí je, že na titulní stránce byl odkaz, ukazující přímo na volný terminálový přístup do serveru. Ani zde však hackeři nesmazali žádná data.

V neděli měli hackeři na programu Banku Union, ze které udělali „Ruin Banku“. Stránky Unionu byly změněny několikrát za sebou a když už šílivší správce serveru smazal http daemon, program obsluhující webové stránky, Pajkus mu jej znovu nainstaloval.

--=:o0o:=--

18. 2. 1997 nebyl den jako každý jiný. Žádný den není stejný. V den, který nebyl jako každý jiný, zvlášť ne pro internetovou komunitu se na Neviditelném psu (`http://pes.eunet.cz`) objevila zprávička, že server www.mobil.cz o mobilních telefonech byl hacknut cZertem. Vzápětí bylo na Neviditelném psu zveřejněno toto oznámení od správce Mobilu, Petra Mitošinky: „Rád bych uvedl na pravou míru zprávu o hacknutí serveru www.mobil.cz, která byla uveřejněna v Neviditelném psovi dne 18.2. Zmínka na jedné ze stran tohoto serveru, která byla pochopena jako hacknutá stránka, je míněna pouze jako poděkování spřátelenému hackerovi za jeho ‚malou službu‘. Rozhodně tím nikdy nebyl míněn žádný žert vůči hackerům. Petr Mitošinka peta@mobil.cz“ Jak vidno, ne každý správce je „čistý“. Spřátelení hackeři poskytují službičky, a hacknutí serveru udělá často serveru větší reklamu než bombastické reklamní proužky na jiných serverech.

Vzápětí udělali vtípek cZerti a server skutečně hackli a změnili titulní stránku.

Potom se však stalo něco, co veřejnost zaregistrovala poprvé – smazání celého serveru. V případě WareZu se správci ani moc nemohli ozývat, sami měli černé ruce, ale protože šlo o tak dokonalý a propracovaný server, udržovaný několika nadšenci, zdvihla se na českém Internetu vlna nevole. Internauté byli otřeseni. Ondřej Neff, vydavatel Psa zareagoval bleskově: *„Anonymní parchante, ať jsi kdo jsi, zničil jsi práci slušných lidí. Vyvolal jsi zbytečný spor mezi lidmi, kteří by jinak k sobě měli blízko. Vím, že to můžeš udělat znovu. Můžeš smazat mobil znovu, můžeš smazat Psa na serveru nebo na mém počítači – není chráněný, nesedím za firewallem, jsem na fuckin´n pětadevadesátkách. Můžeš se mi i vysrat na schody. Můžeš vzít kladivo a rozbít mi glášsajbu limousiny. Uříznout ocas Bartovi nemůžeš, protože a) ho*

nemá, b) by tě kousnul do prdele. Jinak můžeš všechno, ze skrytu, zbaběle a zákeřně. Jsi ze stejného rodu, jako fašisté, kteří pořezali ksicht Pavlovi Dostálovi. Patříš ke špíně světa. Jsi živé hovno. Smrdíš a nestojí ti pták. Že tebou pohrdám doufám že jsi už vytušil." Ano, takhle reagoval TEN, Ondřej Neff, který na svém deníku vedl archív hacknutých stránek, který překládal proslulý *The Hacker Crackdown* a který ještě před nedávnem dělal s CzERTy rozhovory. Následující den pak bylo zveřejněno jen toto strohé oznámení: *„Jako odpověď na podlý útok na stránku http://www.mobil.cz jsem smazal celý adresář hackers se všemi archivovanými hacknutými stránkami včetně překladu Sterlingova Hackers Crackdown, navíc v červnu skončí v Telnetu jeho vydávání na pokračování a navíc ho nevydám knižně, třebaže jsem za něj zaplatil autorská práva. Nadále se nehodlám hackerskými kousky zabývat. Náhled možná změním, pokud dostanu na talíři virtuálně uříznutou hlavu fuckera, který zničil nezištnou a užitečnou práci kamarádů ze serveru mobil, ale jisté to není. Pro ty, kdo nevědí, oč jde, doporučuji přečíst víkendového Psa. Aston"* Jak vidíme, neznámý hacker dokonale ťal do živého. Většina lidí si myslela, že „hackeři jsou děsný bozi, který občas změní stránky na nějakém zbytečném serveru, ale jinak neškodný".

Podle Pajka však bylo všechno jinak. Nyní si poslechněme jeho verzi. *„ten mobil.cz som robil ja... kratko nad ranom – asi okolo 5 am sme diskutovali so seteuidom na cZert chat robotovi. seteuid cital vtedy cerstve vydanie neviditelneho psa, a tam neff robil narazku na to ze www.mobil.cz asi hackol cZert, pri tom to nebola pravda. dokonca bola kopia www.mobil.cz umiestnena na archive hacknutych stranok. tak sme si povedali ze by vznikla velmi vtipna a absurdna situacia ked ten server www.mobil.cz naozaj hackneme.*

*www.mobil.cz sa nachadzal na sieti inet provajdera ‚netforce', ktory seteuid velmi dobre poznal... cela siet *.netforce.cz bola totiz uz niekolko mesiacov domovom viacerych hackerov, aj ja som par krat zneuzil ich masiny na presmerovanie IP packetov (tzv. redirektormi). seteuid bezal na netforce sniffer (program zachytavajuci hesla na lokalnom ethernete), takze mal zoznam viacerych login/hesiel na pocitace v netforce. tie mi dal a isiel spat :)*

ja som potom skocil do Nitry na pocitac sai.uniag.sk a z neho som zautocil na mobil.cz. nebolo mozne sa dostat na www.mobil.cz cez telnet, myslim ze tam mali hosts.deny ktory povoloval pristup iba z niektorych vybranych masin. FTP vsak mali pristupne odvsadial, takze som pouzil dost stary trik ze som uploadol cez FTP subor .forward a program na otvorenie shellu na specifikovanom porte, ktory sa spustal

prave cez .forward. potom som poslal postu na server mobilu a otvoril sa mi shell na vysokom porte, takze som mohol interaktivne pracovat na www.mobil.cz. ked uz som tam bol lognuty tak to bolo dost jednoduche... ziskal som prava httpd a zmenil html stranky, to bolo asi o 6:45 am a potom som isiel hned spat. ked som sa zobudil poobede, bola uz na inete velka fama o tom ze czert vymazal www.mobil.cz...

kontaktoval som neffa a spravcov z mobil.cz ohladne tej veci a napisal som im ze som to ja nebol... spravcovia mobil.cz mi dali za pravdu podla informacii o mojom utoku ktore som im poskytol. vedel som ze na netforce bol v tej dobe doslova hackersky kabaret... hackovalo tam viacej ludi – videli sme ich stopy. nevedeli sme vsak kto to bol. musel to byt nejaky hacker ktoreho zavist voci cZertu priviedla k tomu aby vymazal cely server www.mobil.cz, kedze jeho utok bol taky rychly a pohotovy (musel byt niekedy medzi 7am – 9am), bol to jeden z ludi ktori mali pod palcom celu netforce siet...

kto to bol to dodnes neviem, v kazdom pripade ma sokovala reakcia adminov mobilu ktori vysvetlovali novinarom ze sme im to vymazali my, napriek tomu ze som s nimi bol v e-mail kontakte, spolu sme sa zhodli na tom ze som to ja nebol na zaklade dokazov, a navrhol som im moju pomoc pri patrani, k comu sa vobec nevyjadrili. ludia z mobil.cz potom chodili rumazgat a vyplakavat na mamediu a k novinarom, pricom zaujimave je ze za par hodin po utoku mali cely server naspat online so vsetkymi datami. tvrdia ze nemali backup, ako je potom mozne ze bol cely server zniceny a aj tak ho mali za par hodin po utoku zdravy a zivy naspat on-line ? obcas mam pochyby o tom, ci vlastne bol ten server vymazany...

utok na mobil.cz bol iba otazkou casu a bol zapricineny neprofesionalitou a nizkou urovnou znalosti administratorov siete netforce.cz. na ich serveroch sa vdaka ich blbosti rozputala hackerska diskoteka, a toto bol vysledok – myslim si ze aj tak vsetko dopadlo relativne dobre. hocikto s hackerov co operovali na netforce.cz mohol totiz napriklad zhodit vsetky ich servre kompletne z vlny, cim by vyradil prevadzku tohoto Inet providera podla mojho odhadu tak minimalne na 2-3 dni. to uz by boli naozaj seriozne skody... takto si to odniesol iba ich blby www servrik o mobilnych telefonoch...“

Správce Mobilu, Petr Mitošinka zálohu skutečně neměl, ale podařilo se mu soubory podle jeho vytáhnout z proxy cache. Hackeři však prý zanechali na serveru stopy. Pajkus se jen pousmál. *„som rad ze to vsetko relativne dobre dopadlo, lebo si velmi vazim pracu chalanov z mobil.cz, maju fakt zaujimavy server. je stastie ze sa im to podarilo vcelku lahko nahodit z tej proxyny,“* řekl několik týdnů po útoku.

Dnes je však stále přesvědčen, že server nikdy nebyl smazán, protože v proxy cache se nemohlo zachytit všechno. A co se týče stop? *„tie stopy by som rad videl. totiz – stopy boli zachovane z toho mojho ranneho utoku – upload .forward cez ftp, nasledne 2,3 mejly a potom telnet na vysoky port, cele to bolo robene z pocitaca na Nitrianskej Univerzite. Pokial existuju nejake stopy po 8:00 am ohladne toho zmazania – rad by som ich videl.“* Správci serveru prý nebudou na Netforce podávat ani žalobu ani z toho nevyvodí žádné důsledky. Obě strany se shodují na tom, že to mohl být někdo jiný. Podezření je však stále na cZertech. Dnes, po více než dvou letech těžko někdo zjistí, kdo útok provedl. Stopy jsou dávno zaváté.

Pajkus slíbil, že se po hackerech poohlédne, ale tvrdí, že na tuto jeho nabídku Mobil nijak nereagoval, takže to nechal plavat. Petr Mitošinka naproti tomu tvrdí, že nabídku od cZertů dostal a čeká, co hackeři objeví. Takže chyba komunikace? A není to směšné ve věku, kdy se komunikace stává snadnější a efektivnější než kdykoliv předtím?

--=:o0o:=--

Komerční i neziskové servery (převážně však ty prvé) hackovali CzERTi docela běžně, na Slovensku se vložili i do politických událostí. V průběhu politické krize a universitních stávek na Slovensku odeslali asi 125 000 hromadných emailů s politickým textem. Jeden z nich najdete v příloze na straně 99. CzERTi uskutečnili i SMS-flood, neboli hromadné rozeslání vzkazů na mobilní telefony. To vše přesto, že se v životě neviděli. Setkávají se až v červnu 1997 v Praze na „cZert Session“. „Drasťákoidně melodaramatický příběh“ o průběhu tohoto setkání najdete na straně 53. Podobná „session“, tentokrát hojně propagovaná a otevřená veřejosti, je naplánována na 17. leden 1998.

--=:o0o:=--

17. října 1997 na tiskové konferenci v Brně náš starý známý Jiří Dastych říká, že policisté jsou již na stopě počítačovému démonovi, který vystupuje pod jménem CzERT a že s každým dalším průnikem se hacker přibližuje odhalení. Zpráva ČTK doslova uvádí: *„Policisté jsou na stopě počítačovému démonovi, který vystupuje pod jménem CzERT a v uplynulých měsících se ‚naboural‘ na Internetu do stránek ministerstva zdravotnictví, české pobočky americké firmy Hollywod*

Classic Entertainment, společnosti MaMedia a dalších. Řekl to dnes v rozhovoru pro ČTK Jiří Dastych z policejního prezídia, který se touto problematikou intenzívně zabývá. CzERT si z uvedených institucí udělal ‚dobrý den' tím, že přepsal jejich stránky nebo je svérázně upravil." Ondřej Neff v Invexovém Neviditelném psu tuto zprávu komentuje: *„Skvělý úspěch! Czert byl dnes navštívit stánek Internet Servisu zde na Invexu, zdvořile jsme spolu pohovořili, pravda bez srdečnosti, on mě ujistil, že nezničil server Mobilu, já ho ujistil že to vím, nemám však důvod svůj odstup od hackerů revidovat a měnit. Žádných pánů v bouřinkách s lupou v ruce plazících se Czertovi v patách jsem si nevšiml, možná že byli maskovaní. Pokud by je napadlo mě opět macerovat, ujišťuji je, že jsem byl otočený, Czerta jsem neviděl, nevím jak vypadá, nelegitimoval se mi a panáka jsem mu nenabídl, tudíž nemám otisk palce na skleničce."*

Krátce po Dastychově tiskovém prohlášní hackeři z CzERTu napadli i server Policie.cz, kde jeho slova řádně zparodovali.

−−=:o0o:=−−

Pajka: uh, ok takze czert session je napevno rozhodnuta – v sobotu 17.1. o 18.00 pri soche sv. vaclava...

dusheen: no jo, tak ja teda asi prijdu :)))

Pajka: OK, takze zatial sa mi ozvali tito ludia ze tam asi pridu : seteuid, xjpa, janina, dusheen, chaky, koles, xalex..

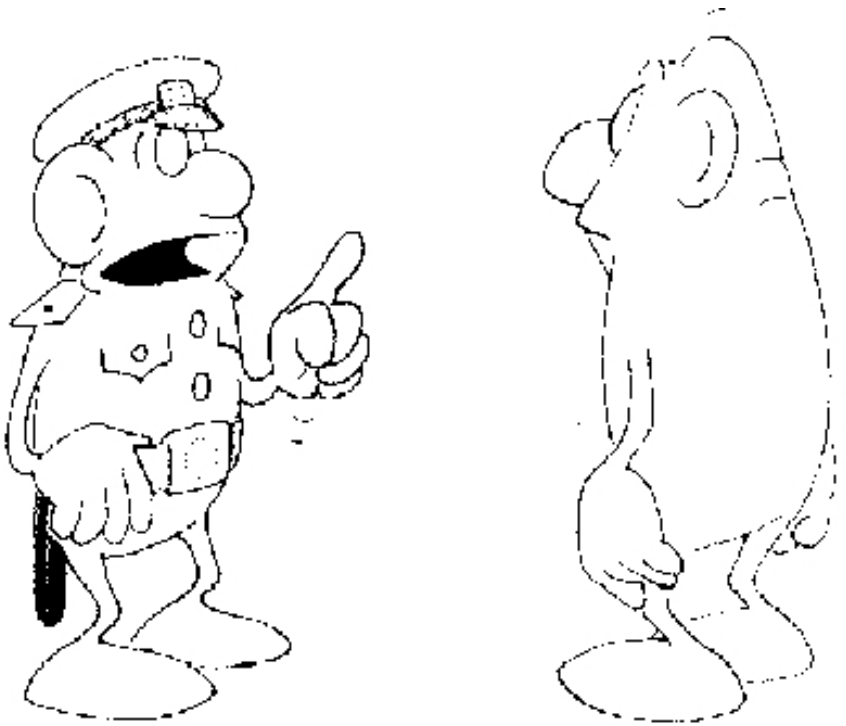
Ook: Ale tak ja taky pridu :-) Jenom nevim, jak se dostanu domu...

Boban: V jednote je sila. Doufam, ze prijdou vsichni !!!

Pajka: jo takze pripisal som ooka a designera a este kohosi kto mi pisal do mejlu do zoznamu tych co pridu asi na session... chaky pisal ze nemoze prist...

Kolem CzERT SESSION bylo na českém a slovenském Internetu docela živo. Na webu se válely velké reklamní bannery (některé umístěné i na hacknutých cizích stránkách), oznamující, že sraz je 17. ledna v 18 hodin u Václava na Václaváku v Praze, jel speciální server pro diskusi zúčastněných, výzvy k účasti byly rozlepeny všude...

Když jsem přišel ke koni, upoutala mě na první pohled skupina výstředně (kyberpunkově) oblečených lidí. Občas k nim někdo jim podobný přišel, podali si zvláštním způsobem ruce a debatovali v jakémsi subkulturním slangu. Měli všichni strašně divný boty. Byli mezi nima



Tento obrázek a následující text použili hackeři z CzERTu na modifikované stránce Policie: *„Zeptali sme se pana Dastychla z policejniho prezidia zda nam muze rict blizsi informace o dane stope na CzERTa. : ‚Ano, mohu Vam rict jakou konkretni stopu mame na hackera CzERTa: Zjistili sme konecne co je to ten Internet., co vo nem furt ten CzERT mluvi ze na nem je.‘“*
zdroj: http://www.policie.cz

i týpkové, kteří vypadali přesně jako zadržení hackeři z novin, dlouhé vlasy, plnovous, divoké oči, oblečení v černém. Pravá subkultura. Přicházeli mezi ně další a další a mě jen udivovalo, že je mezi nimi docela velké procento žen. Hackerky? Asi těžko, ale proč by hacker nemohl vzít na session – společenskou událost počítačového undergroundu – svou přítelkyni? Skupinka se stále rozrůstala a já, sedíce na lavičce, pozoroval jsem jedním okem je a druhým pár (!NENÁPADNÝCH!) fotografů a kameramanů, kteří se, *jen tak* procházeli kolem, foťáky otevřený, prsty na spoušti, červená světýlka kamer svítila do stále houstnoucí tmy.

Pár příslušníků této zvláštní subkultury se občas odtrhne a odejde kamsi – napřed. Obávám se, že vypadám málo výstředně.

O kus dál stojí skupinka několika naprosto *normálních* lidí, co když *to* jsou *oni.* Posouvám se mezi obě skupinky. Ze skupinky *cyberpunkerů* se ozývá slůvko *informace,* kdosi z *normálů* říká *ímejl.* To ale nic neznamená, mejl přece používá každej.

Jméno *Pajkus,* které zaslechnu od *normálů* mě přesvědčilo. Hackeři nevypadají jako *hackeři,* co je znáte z filmů. Nebavěj se ani moc o počítačích. Kyberkultura, vybásněná Gibsonem a Sterlingem, jako by se jich netýkala.

Přichází Pajkus.

Grupa se vydává po silnici dolů po Václaváku. Auta se vyhýbají skupině asi dvaceti největších hackerů z Čech a ze Slovenska.

Ptám se Pajka právě na kyberkulturu.

„Jediný, co se mě z kyberkultury týká, je IRC. Večer sednu k počítači, pokecám s kamarádama a potom někdy běhám po nějakých těch mašinách."

Hackeři doráží „na místo" – do restaurace Ve Zlaté, která se později zapsala do análů policie.

„Miro, bude přistavěný autobus do Bartolomějské?" vtipkuje kdosi.

„No jasně, původně jsme to chtěli udělat v té kavárně přímo naproti prezídiu, abychom si jenom popošli. . . "

Nad večeří se hackeři, dosud vesměs mlčící začínají rozpovídávat, diskuse se docela slušně rozbíhá. Kdyby dlouhý stůl obsazený košatým rodiným klanem obhlédl někdo nezasvěcený, tipnul by si, že si prostě pár studentíků zašlo na večeři a docela dobře se bavěj. Oblíbená barva hackerů je černá a většinou to i sedí (jen Pajkus má bílou košili).

Pajkus říká, že má nyní firmu, která se stará o bezpečnost počítačových sítí. Jako hacker ví, kde jsou v systému škvíry, ale zná i postupy na jejich zatmetlení. Je schopen zaručit maximální bezpečnost, simulovat hackerské útoky. . . Není to nemorální, používat vědomosti

získané jakýmsi *škoděním* k nějakému odobnímu prospěchu?

„Proč?“ směje se, „hackeři budou vždycky napřed před adminama. Admin jenom mžourá za serverem a když občas někdo zaútočí, ucpe sem tam nějakou díru. Ale když já běhám po mašinách, můžu na jeho stroj útočit celé týdny, zkoumat ho a hledat skulinku, vždycky jsem jako hacker napřed.“

„Má informace,“ doplňuje ho Ook, „tak je použije.“

Pajkus, Ook a MiRaGe se mi snaží vysvětlit, že hacking, tak jak je dělají cZerti není nic špatného.

Stále mě děsí to, že hacker, který profesionálně zabezpečuje sítě, si může někde nechat skulinku, backdoor.

„CzERT, ten folklór kolem toho a všechno to ostatní – to byla jenom studentská prča. Recese, tak jak to studenti dělávají. Nikdy nemíchám CzERT a business dohromady.“

Z Ooka se vyklubal filozof mezi hackery. Mluví v dlouhých, úhledně skládaných větách, klidně, snaží se mi vysvětlit filozofii toho, co je pro ostatní zločin.

V dnešní době může hackovat kdokoliv. K dispozici jsou příručky pro začátečníky i pokročilé, hackerské utility, popisy bugů… Ale CzERTi na svých stránkách nabízejí utlity, se kterými už musíte umět pracovat. Hřebíky, dřevo, železné součásti a titěvu, ze kterých si samostříl sice postavíte, ale musíte to umět.

„Pokud někdo zveřejní popis bugu, je to jedna věc. Když někdo zveřejní bug a způsob, jak ho zneužít, je to věc druhá. A když někdo zveřejní utilitu, kterou stačí jenom zkompilovat a shazuješ mašiny, je to taky něco jinýho. Jsou k dispozici programy, který akorát zkompiluješ a už to padá. *To* mě děsí. A *to* mi přijde nemorální, když někdo zveřejňuje takovýhle věci. Představ si třináctiletýho puberťáka, kterej si říká hacker…“

„Počkej,“ přeršuje ho Pajkus, „třinárct se mi zdá dost málo…“

„Jo, pár takovejch jsem viděl,“ nenechává se vyvést z rovnováhy, „víš, jak si přijde silnej? Je boss, stáhne si nějakýho Nuka a schodí mašinu.“

„No, vlastně jenom zresetuje…“

„Jo, jenže jak to nabůtuje, hodí to znova.“

„WinNuke je nejhorší,“ dodává MiRaGe, „je to normální windousovej Drag-n-Drop, Každej, kdo ví, co to je myš, s tím umí zacházet…“

Začínám sdílet jejich obavy. „Je možný shodit třeba celou doménu?“ ptám se.

„Ne, routery jsou stále ještě dobře chráněný. Ale tak před rokem, když se objevil jeden nový bug, to možný bylo. Zamindrákovanej pu-

berťák mohl shodit klidně celý český Internet.“

A co technické řešení. Jak je těžké hackovat?

„My cZerti jsme vlastně měli docela štěstí,“ prozrazuje Pajkus, „že jsme objevili jeden docela neznámý bug, jinak ty útoky byly na docela nízké technické úrovni.“

Rutina. Na hacknutý server (tak dva až tři denně) se umístí přesměrovávač paketů (redirector). Příkazy, které hackeři používají, jsou tak zdánlivě odesílány z tohoto stroje.

„Přes dva tři redirektory mě nemá nikdo šanci vystopovat,“ začíná se chlubit Pajka.

„Ale má,“ kroutí hlavou Ook.

„Jo, ale musel by bejt stejně dobrej jako já. Nebo lepší,“ usměje se.

„Jenže u nás není nikdo, kdo by tě sledoval. Jednou jsem něco hackul a asi za týden mi přišel mejl s takovým směšným obsahem jako HA, HA, DOSTAL JSEM TĚ! !!!BOOOOM!!!, PRASKLO TO – a podobně. Ten správce, místo aby si to spravil, mě tejden hledal na webu. A přitom o anonymitu nějak moc nedbám.“

Na řadu přicházejí historky o návštěvách agentů FBI na ČVUT a UK v Bratislavě – studenti se občas pokoušejí probourat do amerických vládních počítačů.

Dostáváme se tedy k otázce bezpečnosti hackování pro samotného hackera.

„Nebojíš se, že nějaký naštvaný správce po tobě bude pátrat a najde tě?“

„Najde, proč by nenašel. Ale nic se nestane. Co by mi udělal? Jel by za mnou až na Slovensko? To by se mu ani nevyplatilo. To jako, že by na mě poslal nějaké korby, aby mi daly nakládačku? Proč? Snažím se neškodit. Většinou nějaká změna stránek ještě udělá tomu serveru reklamu.“

Vyciťuji na jednu stranu jakousi symbiózu mezi správci serverů a hackery a na stranu druhou i nelítostný boj. Dost často je hacker admin a dobrý admin je někdy hacker. Ale nejde někdy souboj až na ostří nože?

„Slovensko je přeci jenom na východě, blíž Ukrajině. My si na takovéhle věci najímáme ukrajinské dělníky,“ říká s úsměvem na tváři, ale najednou zvážní. „Jednou jsem honil jednoho hackera. . . “

„Hacker honil hackera?“

„Jo, hledal jsem takového darebáka, schodil jistý místní uzel jednoho poskytovatele a týden tam potom nešlo spojení. Provajdr byl hezky naštvanej. Našel jsem ho a tam se to řešilo nějakou takovouhle cestou. Ukrajinci a tak. . . Ale o to jsem se už moc nezajímal.“

„Raději," ozývá se po jeho levici. Přikyvuje.

Týpkové, co vypadali, že někde na webu zahlýdli banner, čekali, že budou coby nováčkové nadšeně přijati a zasvěceni do všech tajemství počítačového zločinu, co chvíli pili kolu, pak koukali do zdi, už znechuceně odešli ke svým WinNukům.

Do klidné restaurace vráží pětičlenné policejní komando. Jeden z policistů zastupuje dveře.

„Hele, Dastych," ozývá se jízlivá narážka. Autobus do Bartolomějské přistaven?

„Nezlobte se, že vás rušíme..." sype ze sebe policista nadrilované fráze, „vím, že tady máte uzavřenou společnost," doufejme, že brzy ne ZAVŘENOU, „ale dostali jsme anonymní oznámení," tak už to bývá, všechno se svede na anonymní oznámení, „že tady sedí pachatel," (takže jeden?) – hackeři znervózňují a vrtí se na židlích, „loupežného přepadení!"

Stůl rozvětvené křemíkové famílie se dává do hurónského smíchu. Velitel zásahu je zjevně zmaten, snaží se pravděpodobně studentíky, kteří si vyšli na společnou večeři, uklidnit, ale moc se mu to nedaří. Nakonec je zapsáno rodné číslo, jméno, adresa a podobně všech v restauraci, policisté se omlouvají a zase odcházejí!

Kdo má mobil, vytáčí správce všech novinkových webserverů a oznamuje tu úžasně absurdní událost.

K Pajkovi se přitáčí člověk v černém a spiklenecky mu ukazuje fialový balíček, skrytý v dlani: „Dáme si do nosu?"

„Jo," šeptá Pajkus. Hackeři prý často končí na drogách. Ke svým nočním toulkách po vláknech pavučiny občas využívají amfetaminy, stimulátory, které jim umožňují být vzhůru velmi dlouho do noci...

Pokládá na stůl balíček s psychedelickým potiskem – *fialovou krávou*.

Nad čokoládou se řeč točí kolem modemů, infvestic do linek, warezu, školních sítí...

Taky o tom, jak média prezentují Internet jako nebezpečnou oblast *hackerů*, *dětské pornografie, návodů na bomby* a *nakupování* po síti pomocí kreditky, jejíž číslo vám ukradnou právě hackeři. Noviny se mají proč bát, že je Internet převálcuje.

−−=:○0○:=−−

Později se ukázalo, že humor kolem „loupežného přepadení" byl poněkud nevhodný. Policisté údajně později předvolali 6 – 7 hackerů ze

session, ostatní prý obcházeli a opatrně se vyptávali, zda nemají něco společného s počítači.

Hack serveru Policie byl pravděpodobně posledním útokem hackerů. CzERT is dead. Nebyli pozavíráni, osouzeni či postříleni ukrajinskou mafií.

„CzERT se prostě rozpadl," říká Pajkus. „Z 95% jsem to byl já a když jsem v červnu 97 odešel ze školy, skončil i CzERT."

Kapitola 5

Příležitost dělá zloděje

Proniknout do banky není zdaleka tak jednoduché, jak ukazují filmy.

„Čau, tady je Martin[1],“ ozvalo se v telefonu. „Čau Martine,“ odvětil jsem, aniž jsem tušil o koho jde.

Následovalo dlouhé ticho.

„Martine?“ přerušil jsem ho.

„Jo, jsem tady,“ odpověděl.

„Eh… Co potřebuješ?“

„Volám kvůli tý práci, jak jsem ti mejloval, vzpomínáš?“ ozval se na druhé straně cyberspace hlas nejspíš studentíka odněkud z koleje.

„Chceš dělat nějaký stránky?“ ptám se nejistě.

„Jaký stránky? Cože??? ‚Hledám někoho dobrýho na dobře placenou práci, čau, Martin,‘ posílal jsem ti to mejlem, vzpomínáš?“ říká tónem, jakým vysvětlujeme mentálně postiženému, jak se jí příborem.

Vydám zvuk ukazující na náhlé rozsvícení čehosi v mozku.

„Fajn, o co jde?“ ptám se.

„No, víš, nechce se mi o tom příliš mluvit po telefonu.“

„Já ho nemám napíchlej!“ zasměju se.

„Ale já možná jo!“

Usměju se. Dobrá paranoia!

„Můžeš aspoň něco naznačit? … Jedná se… ehm… o… bezpečnost počítačových systémů?“

„Jo,“ připouští váhavě, „dám hodně peněz,“ dodává.

Užuž mám na jazyku obvyklou hlášku, že o hackerech pouze píšu, a sám nehackuju, pak ale zaváhám a ještě chvilku mlčím.

Martin navrhuje schůzku.

[1] bylo to pochopitelně jiné jméno

„Už přijíždím," volá mi následujícího dne z mobilu. Vydávám se na dohodnuté místo – na náměstí jednoho malého středočeského městečka. Jsem nervózní. Prohlížím si podezřele všechna auta, ubezpečuju se, že ve velké bílé dodávce nesedí team policistů, připravených mě zatknout při prvním vyslovení slova „hacker". Každý člověk, procházející kolem, či jen tak postávající na rohu, jako by patřil k policii, každý pohyb jako by sledoval kapitán Dastych na svém monitoru…

Paranoidní studentík Martin má zpoždění.

Nervózně popocházím a stále přehlížím každý kousek prostoru. Dva muži, postávající uprostřed náměstí, které tipuju na zdejší mafiosy, udělají směrem ke mě několik nenápadných gest.

Přijdu blíž.

„Ty seš Honza?" ptá se mě jeden z mužů.

Přitakám.

„Já jsem Martin, tohle je Patrik," říká, zatímco mi oba mačkají pravici.

Usedáme na lavičku uprostřed náměstí. Kolem pomalu projede policejní Favorit.

Chvilku hovoříme o počítačích, o hackování, hackerech a jejich světě. Ptají se mimo jiné i na kapitána Dastycha, občas do něj rýpnou, tahají ze mě informace o jedniném softwarovém policistovi v zemi. Uvažuju, jestli nesedí za rohem a neposlouchá klepy o sobě, vysílané přímo od obou pánů. Nebo prostě underground chce vědět co nejvíc o svých protivnících?

„Budeme mluvit na rovinu," řekne najednou Martin. „Chceme udělat banku. Přes počítač. Potřebujeme vědět jestli to jde a jak to dokázat."

Docela mi vyrazí dech.

Neskrývají to, že jejich motivací není intelektuální požitek z přelstívání bankovnách systémů, zřejmě nejchráněnějších na světě, ale peníze. Kam jinam taky pro peníze než do banky.

Podruhé mě vyděsí částka, kterou chtějí ukrást.

„Tak těch tři sta melounů… Když už, tak už!" zašklebí se Martin.

Dá se do vysvětlování. Pokud ho budou soudit za krádež tří set milionů, tvrdí, dostane nejspíš stejnou sazbu, jako za krádež dvaceti tisíc.

„Když mě zavřou za dvacet tisíc na dva roky, jsem blbej. To se mi nevyplatí. Když mě zavřou na dva roky za třista melounů, zaplatím si ve vězení každýho a až mě pustí, nebudu do smrti pracovat," říká s

filosofickým výrazem v tváři. Rozohňuje se nad tím, jak může někdo zastřelit člověka kvůli pár tisícům a téměř ukřivděně upozorňuje na nedávný případ loupežného přepadení benzínové pumpy.

„Tady krade každej," říká, „kdo má ruce, krade, kradou všichni, krade se, krade se, krade se…" Nepatří mezi lidi, kteří by s tím chtěli něco dělat. Nepatří prý ani mezi hlupáky, kteří nekradou, či alespoň krást nechtějí.

Mluví o tom, že chtějí obrat velkou společnost. „ČEZ, pojišťovnu nebo Telecom, ten nás obírá všechny," dodává Patrik.

„Ani si toho nevšimnou. Ty maj peněz, že nevěděj co s nima," přesvědčuje mě zas Martin. „Vím v Praze aspoň o deseti lidech, který maj miliardu."

„A další miliardu na zdech," připomíná Patrik. Martin se rozmluví o malířích. Zálibu má prý v Picassovi, ale žádného nevlastní. Zatím.

„Brečels, když to potápěli v Titanicu, viď," šťouchne do něj jeho společník.

Řada je na mě. Vysvětluju to málo, co vím o bezpečnosti bank, o práci hackerů, jejich mechanismech na zamazávání stop. Občas pro ilustraci ukážu na některou z budov bank – na náměstíčku jsou tři.

„Víme aspoň o dvou třech skupinách, které se o něco podobného pokoušejí," říká Martin.

Pro hackera, který by pro oba společníky pracoval, nabízejí široké zázemí. Falešné doklady, „levý" byt v Praze, telefonní linku na cizí jméno, komunikační techniku na odposlechy, počítač tak výkonný, jak si jen hacker bude přát. Není prý problém během několika hodin vše zabalit a přestěhovat se jinam, střídat byty po celé Praze. A po „akci" samozřejmě tučný podíl. Chtějí ale skutečně elitního hackera.

Slibuju, že předám jejich nabídku několika přátelům. Snad to není trestné.

−−=:○0○:=−−

„Průnik teoreticky možný je, ale dřív nebo později se na to přijde," začíná povídání o bezpečnosti bankovních systémů Petr Hasan, systémový programátor systému VMS[2], dnes zaměstnanec velkého bankovního domu. „Byly tady samozřejmě už pokusy, ale vždycky se na

[2] *Virtual Memory System* – operační systém pro počítače VAX od Digital Equipement Corporation

to přišlo," řekne a sedne si na velký stůl ve své prostorné kanceláři správce sítě. Dal by se tu klidně hrát basketball, kdyby tu byl mimo počítačů, tiskáren a dalšího technického vybavení ještě koš se síťkou, napadá mě.

„A kdyby se na to nepřišlo, samozřejmě o tom nevíš," vybíhám lehce k soupeřovu koši.

Usměje se a začne popisovat strukutru kontrol a kontrol kontrol.

Každá akce v systému se zaznamenává.

„Každý hacker po sobě maže stopy," opáčím nenechaje si vzít míč a přiblížím se pod koš.

„Všechno, co kdokoliv udělá, se zaznamenává třikrát. Nejprve do nějakého textového souboru, jako seznam provedených akcí. Všechny operace ještě se zaznamenávají do databáze. Pravidelně se navíc tisknou sestavy provedených operací, které se uschovávají do archívu na mnoho let," obehrává mě s profesionální přehledem o míč a nechá ho prošumět imaginárním košem.

Průnik zvenčí považuje Petr za téměř vyloučený. Veškeré transakce jsou sice vedeny počítačově a šířeny po celobankovní počítačové síti, ale neexistuje žádná linka, kterou by se mohl účastník dostat dovnitř. Data posílaná po linkách, jimiž jsou spojeny jednotlivé pobočky, jsou šifrovaná. I kdyby hacker dokázal napíchnout vyhrazenou bankovní linku a data velmi rychle odšifrovat (běžně dostupné systémy by tuto operaci v reálném čase nezvládly), nemohl by je změnit, jelikož je s nimi posílán i kontrolní součet.

Internetový server pro homebanking[3] je do vnitřní sítě banky neprůchodný, odebírají se z něj pouze jednoduché řetězce konkrétních operací, ale nic jiného dovnitř proniknout nemůže. „Hacker by se musel dostat do banky a operace provést z terminálu v budově. Jenže jak by se dostal k terminálu?" ptá se expert. „Leda že by se sem v noci vloupal," říká s úsměvem.

Kdyby se nějaký hypotetický hacker do pobočky banky vloupal (a nezašel by rovnou do trezoru), zasednul k terminálu, zastaví se u hesla. Naivní jsou představy tvůrců filmů, kteří si dávají jako hesla do systému jména svých dětí, psů, manželek a milenek a myslí si, že to dělá každý, zvláště pracovníci bank. Zkuste si někdy naslepo zkoušet uhodnout nějaké heslo, které má třeba jen pět znaků! Hesla bývají často dlouhé řetězce (25 znaků není vyjímkou) v nichž se vyskytují čísla, písmena i pomlčky, hvězdičky, pluska, procenta a další nealfanumerické znaky. Uhodnout heslo prostě nemáte šanci.

[3] uskutečňování bankových operací po telefonu nebo po Internetu

A kdyby se nějaký zaměstnanec zachoval k bance neloajálně, pustil našeho hackera ke svému terminálu, dokonce mu prozradil své heslo a nikdo z kolegů by si jich stále ještě nevšiml (což se u nudících se úředníků nedá čekat :-)?

„Nedostal by se dál, než na co má daný zaměstnanec práva," vysvětluje Petr a dává mi další koš. Už je ani nepočítám. „Nedokázal by změnit systémové záznamy. Nedají se změnit. Jen na to, aby je člověk mohl prohlížet, musí mít zvláštní přístupová práva. Ta mají zaměstnanci, kteří mají na starosti kontrolu. A o tom, že záznamy někdo prohlížel, se uchovává záznam, prohlížený někým na vyšší úrovni."

I kdyby zůstal v systému záznam, mohli by přeci oba vzít svou hromádku peněz a druhý den být za kopečky? Chápu se opět míče.

Petr klidně stojí uprostřed své kanceláře/téměř-tělocvičny a ani se nesnaží dostat míč zpátky.

„Jo." Dávám koš. Připadá mi, že to byl ten nejjednodušší trik od dob, kdy američtí indiáni provozovali svůj sport s kaučukovým míčem. „To riziko je tady vždycky, stejně jako když bankovní úředníci manipulují se skutečnými penězi. Můžou si strčit svazeček bankovek do kapsy. Ale přijde se na to, a přijde se na to kdo to udělal."

Navíc se situace naší dvojce hacker, úředník situace ještě komplikuje. Peníze sice převedli na své konto, ale co s nimi udělají? Při opravdu dobrém postavení hvězd by se na to nemuselo přijít celý týden.

Převedou si peníze na zahraniční konto?

„Převody do zahraničí nejsou tak jednoduché, jak ukazují akční filmy. Rozhodně to není hned, nějakou dobu to trvá."

Vyberou si je?

„Ve většině poboček znají své klienty. Výběry větší hotovosti se navíc musí hlásit dopředu."

Vzpomínáme na případ, kdy si zaměstnanec jedné banky převedl na svůj účet něco kolem 3 milionů korun a potom si je šel vybrat. Poznala ho kolegyně u přepážky, které bylo trcohu divné, že si její kolega programátor najedou vybírá z účtu astronomickou částku.

Ani mezibankovní převody podle Petra Hasana nejsou tak jednoduché, všechny cestují přez cleeringové centrum ČNB, což stojí také čas. Mimoto jdou vrátit, poslat zpátky, nebo zmrazit na cestě.

„I kdyby se jim tohle všechno ‚povedlo', co by s těmi penězmi dělali?" ptá se Petr. „Nakupovali? Za deset milionů v supermarketu? K čemu jim ty věci budou, když budou sedět ve vězení?"

Začínám házet míč do vlastního koše. Petr nechápe, jak může mít takový podvodník dojem nepolapitelnosti. Přijde se na to. Všechny ope-

race se několikrát kontrolují. Podplatit kontrolu? Stal se prý případ, kdy kontrolovaný zaměstnanec a kontrolor byli příbuzní a domluvili se na úniku. Jenže se na to také přišlo. Peníze se nemůžou nikde ztratit.

Běžný zaměstnanec tedy nemá šanci, ale co systémový programátor?

Vzpomene si ještě na jeden případ. Systémový programátor si v době vysokých úroků převedl větší částky z termínovaných vkladů klientů na svůj účet a potom je zase „vrátil“. Na jeho účtu mu naskákaly úroky. Nedokázal smazat záznamy, ale dokázal upravit program tak, že do záznamu nezapisoval. Jenže zapisoval do dalších dvou.

Trojrozměrné tvary jeho spořiče obrazovky divoce zavíří.

„Navíc každý systémák má jenom taková práva, která potřebuje. V rámci své pobočky. Zvrchu je samozřejmě kontrolován a jsou věci se kterými nepohne. Další ochrana je v tom, že každý zná jenom kousek celého systému. Nikdo nedokáže pracovat s celým systémem.“

Jsou ve VMS chyby? ptám se. Je možné do něj proniknout?

Petr se přizná, že to zkoušel ještě v době, kdy pracoval pro drážní zásobování. Průnik je možný, ale velice zdlouhavý a složitý a hlavě jsou k němu potřeba systémová práva, která chce průnikem získat.

„Průnik je možný, ale dřív nebo později se na to přijde,“ zopakuje Petr ještě jednou, ukáže mi pár fotek ze svých oblíbených her a mezi dveřmi ještě popřeje štěstí této knize. Pak si jde píchnout odchod. Jestli ovšem v bance mají píchačky.

Časová osa

Chronologie amerického digitálního undergroundu

květen 1971 Abbie Hoffman a „Al Bell“ začínají vydávat časopis Youth International Party Line (YIPL), propagující a distribuující metody šizení telefonů. Později se časopis přejmenoval na Technical Assistance Program (TAP). *(Zdroj: Sterling)*[4]

21. únor 1978 Ward Christensen s Randym Suessem vytvářejí v Chicagu první BBS čili board. *(Zdroj: Sterling)*

březen 1980 Zahajuje provoz 8BBS, zřejmě první undergroundový board. *(Zdroj: Sterling)*

1982 Systém 8BBS je zabaven policií protože mu jeden z vděčných uživatelů daroval modem zakoupený na cizí kreditní kartu. *(Zdroj: Sterling)*

1982 Skupina „414 Gang“ proniká do Sloan-Ketteringova centra pro rakovinu a vojenských počítačů v Los Alamos a vyvolává tak novinářskou senzaci. *(Zdroj: Sterling)*

1983 Žháři zapálili „Tomu Edisonovi“, současnému vydavateli TAPu dům a ukradli jeho počítač. To znamenalo smrtelnou ránu pro TAP. *(Zdroj: Sterling)*

1983 Do kin je uveden film War Games (Válečné hry). *„Zdá se, že každý americký kluk chtěl dostat k Vánocům modem,“* píše Bruce

[4] *Bruce Sterling: The Hacker Crackdown* (česky neoficiálně jako *Zátah na hackery,* překlad Václav Bárta, elektronicky, http://hysteria.sk/zatah)

Sterling v knize The Hacker Crackdown (Zátah na hackery). *(Zdroj: Sterling)*

srpen 1983 Sedmnáctiletý Kevin Polusen se dostává do počítačů Výzkumných laboratoří námořnictva v San Diegu. *(zdroj: Littman)*[5]

2. listopad 1983 Je zatčen hacker Ron Austin, kamarád Kevina Poulsena. Později je propuštěn na kauci. *(zdroj: Littman)*

1984 Lex Luthor otevírá svůj board Legion of Doom (LoD). *(zdroj: Sterling)*

1984 Člověk, který si říká Emanuel Goldstein začíná vydávat tištěný časopis „2600: Hackerský čtvrtletník". *(zdroj: Sterling)*

1985 Vzniká WELL „Whole Earth 'Lectronic Link", board Point Foundation, svého času nejživější a nejsofistikovanější elektronická komunita. *(zdroj: Sterling)*

17. listopad 1985 Taran King a Knight Lightning začínají vydávat elektronický hackerský časopis Phrack.[6]

1985 Policie nastražuje na hackery návnady – „pirátské" boardy *„Underground Tunnel"* a „The Phone Company". *(zdroj: Sterling)*

1985 FBI zabavuje board časopisu 2600 a část jejího softwaru formálně prohlašuje za „lupičský nástroj ve formě počítačového programu". *(zdroj: Sterling)*

1986 Je přijat Zákon o soukromí v elektronické komunikaci. *(zdroj: Sterling)*

16. červenec 1986 Hacker Kevin Poulsen jako zaměstnanec SRI (Institut pro řízení dat) absolvuje na základně atomové útočné síly a raket dlouhého doletu v letecké základně Offut v Omaze jedno z vojenských cvičení NATO, simulaci operace „Globální štít". *(zdroj: Littman)*

---

[5] *Jonathan Littman: Hacker – Podivuhodný život a zločiny počítačového génia Kevina Poulsena,* Práh, Praha, 1997

[6] *Taran King: Introduction...* in *Phrack* svazek 1, číslo 1, soubor 1, 17. listopad 1985, elektronicky

srpen 1986 Astronom Cliff Stoll odhaluje v síti Lawrence Berkeley Laboratory shodek ve výši 75 centů. Přestože tomu nikdo zpočátku nevěří, jedná se o stopy po hackerovi. Jak Cliff později zjistil, hacker se z Německa probourával do amerických armádních sítí a kopíroval z nich tajná data. *(zdroj: Stoll)* [7]

15. únor 1987 Kevin Poulsen se vloupává do hlavní budovy společnosti Pacific Bell. Z bezpečnostního oddělení si odnáší velké množství suvenýrů. *(zdroj: Littman)*

29. červen 1987 Německá policie vpadla do Hessova bytu a zabavila asi stovku disket, počítač a dokumentaci k jeho hackerským kouskům. *(zdroj: Stoll)*

1987 Vznikla *Chicago Computer Fraud and Abuse Task Force* (Chicagská operační skupina proti počítačové zpronevěře a zneužití počítačů). *(zdroj: Sterling)*

září 1987 Hackeři z LoD pronikají do telefonního systému BellSouth a přeprogramovávají ústředny. *(zdroj: Sterling)*

1988 Americké federální autority ustanovují organizaci CERT(R) – *Computer Emergency Response Team,* která má shromažďovat a distribuovat všechny informace o útocích na bezpečnost systémů a chybách počítačových sítí, tedy jakási skupina pro pomoc počítačům v nouzi.[8]

podzim 1988 „Prophet“ proniká do centrálního systému pro automatické řízení společnosti BellSouth „AIMSX“ a odnáší si s sebou dokument o struktuře práce služby 911 (tísňové volání v USA). *(zdroj: Sterling)*

2. listopadu 1988 Ve 20:00 vypouští postgraduální student Cornellovy university Robert Tappan Morris do sítě první internetový virus s názvem Internet Worm. Ve 21:24 se virus dostává do počítačů Rand Corporation v Santa Monice, která zajišťuje státní obranné zakázky. V důsledku údajné programátorské chyby v se Internet worm nejen šíří, ale i dramaticky sníží výkon každého počítače, na kterém běží. Dostane se i do vstupní brány sítě Kalifornské university v Berkeley a Livermoru a do Státních laboratoří v Los Alamos. Do půlnoci je vyřazeno z provozu Výzkumné

[7] *Cliff Stoll: Kukaččí vejce, Jota*

[8] *internetové stránky CERT,* elektronicky, http://www.cert.org

středisko NASA. Virus zhroutil přibližně 6000 počítačů na vznikajícím Internetu (zdorj: Littman, Sterling)

1987-1988 Kevin Poulsen odhaluje ilegální odposlechy Jihoafrického, Čínského a Izraelského konzulátu a několika soukromých osob. (zdroj: Littman)

25. července 1988 Němečtí hackeři Hunter (Marcus Hess), Hagbard (Karl Koch), Pengo a Bresinsky jsou obviněni ze spolupráce s KGB, pro kterou podnikali výpady do amerických armádních systémů. (zdroj: Stoll)

13. června 1989 Každý, kdo volal do úřadu kurátora Palm Beach County v Delray Beach na Floridě byl automaticky přesměrován na pornografickou horkou linku ve státě New York. (Zdroj: Sterling)

červen 1989 Skupina *NuPrometheus League* krade kus copyrightovaného počítačového kódu firmy Apple Computer a ve dvanácti kopiích je rozílá počítačovým společnostem po celých USA. (Zdroj: Sterling)

22. července 1989 Tajná služba nainstalovala Atlantské trojce (Leftist, Prophet, Urvile) na jejich telefonní linky záznamníky vytáčených čísel (DNR). (Zdroj: Sterling)

22. července 1989 Tajná služba zadržela Leftista a provedla v jeho domě domovní prohlídku, krátce poté byli zadrženi i Prophet a Urvile. (Zdroj: Sterling)

22. července 1989 Pachatel přesměrování z Delray Beach, známý pod přezdívkou „Fry Guy“ byl dopaden a přiznal se. Dokázány mu byly podvody s telefony a kreditními kartami. (Zdroj: Sterling)

2. října 1989 Senát Spojených států jednomyslně přijal Zákon o počítačové zpronevěře a zneužití počítače. (Zdroj: Sterling)

1990 „Predat0r“, nadšený hacker z Kentucky, obnovuje vydávání časopisu TAP. (Zdroj: Sterling)

1990 Podle odhadů je v USA kolem 4000 boardů. (Zdroj: Sterling)

15. ledna 1990 Vlivem softwarové chyby se zhroutila síť AT&T pro telefonní dálkové hovory. Šedesát tisíc lidí zůstalo bez spojení. (Zdroj: Sterling)

24. ledna 1990 Tajná služba USA uskutečňuje razii u hackera Phiber Optika, Acid Phreaka a Scorpiona. Dva první byli obviněni ze způsobení kolapsu z 15. ledna. (Zdroj: Sterling)

30. ledna 1990 Z obav před policejní razií Mentor zastavil svůj board Project Phoenix. (Zdroj: Sterling)

únor 1990 Po vleklém procesu byli hannoverští hackeři shledáni vinnými a odsouzeni. Peter Carl na dva roky, Dirk Brzezinsky na čtrnáct měsíců a Marcus Hess na dvacet měsíců odnětí svobody. Trest jim byl podmínečně odložen. (Zdroj: Stoll)

21. února 1990 Tajnou službou Spojených států bylo zabaveno veškeré počítačové vybavení za asi 20 000 dolarů včetně necelého gigabytu dat počítačovému expertovi Robertu Izenbergovi, který byl podezřelý ze spolčení s hackerem Terminem. Toto podezření nikdy nebylo prokázáno, Izenberg nikdy nebyl oficiálně obviněn ani zatčen, své vybavení ani data však zpátky nedostal. (Zdroj: Sterling)

1. března 1990 ráno Tajná služba USA provedla domovní prohlídku u co-sysopa[9] Projectu Phoenix „Erika Bloodaxea“ a zabavila mu veškeré vybavení včetně telefonu. Také on nebyl nikdy obviněn. (Zdroj: Sterling)

1. března 1990 ráno Tajná služba USA provedla prohlídku i u Mentora. Agenti mu zabavili jako „důkaz“ jeho klon IBM PC-AT, laserovou tiskárnu Hewlett Packard LaserJet II., naprosto legální a velice drahý operační systém SCO-Xenix 286, programy PageMaker a Microsoft Word včetně instalačních disket a dokumentace, odnesli dokonce i telefon. Mentorova manželka přišla o svou nedokončenou diplomovou práci. (Zdroj: Sterling)

1. března 1990 Tajná služba USA provedla razii i u Mentorova zaměstnavatele Steve Jackson Games. Bruce Sterling o ní píše: *„Detaily dalšího průběhu operace jsou nejasné. Agenti nenechali nikoho jiného vstoupit dovnitř. Povolení k prohlídce, které posléze předložili, nebylo podepsáno. Zjevně snídali v místním stánku s občerstvením, protože uvnitř byly později nalezeny papírové obaly od hamburgerů. Důkladně také okusili gumové medvídky*

[9] „spolu-správce“ boardu, SysOp je zkratkta pro systémového operátora, neboli správce boardu

ze sáčku jednoho ze zaměstnanců SJG. Nálepka ‚Dukakis for President' byla stržena ze zdi. (...) Jacksonova společnost přišla o tři počítače, několik pevných disků, stovku disket, dva monitory, tři modemy, laserovou tiskárnu, různé elektrické šňůry, kabely a adaptéry (a kupodivu i o malý pytlík šroubků, matiček a podobných drobností). Zabavení BBS Illuminati připravilo SJG o všechny programy, textové soubory a soukromou elektronickou poštu na boardu. Ztráta dalších dvou strojů byla pro firmu stejně závažná, protože na nich byly elektronicky zaznamenané smlouvy, finanční rozbory, seznamy a adresáře odběratelů, údaje o zaměstnancích, obchodní korespondence a neméně důležité koncepty nových her a herních knih. Nikdo ze Steve Jackson Games nebyl zatčen. Nikdo nebyl obžalován z žádného zločinu. Nebylo vzneseno vůbec žádné obvinění. Všechny odnesené věci byly oficiálně zadrženy jako ‚důkaz' zločinů, které nebyly nikdy specifikovány." (Zdroj: Sterling)

2. března 1990 Steve Jackson navštívil Tajnou službu v doprovodu svého právníka, protože chtěl získat zpět rukopis herní knihy „GURPS Cyberpunk". Agent Tajné služby to odmítl s tím, že scifi kniha je „příručkou pro počítačové zločince". (Zdroj: Sterling)

7. května 1990 V rámci „Operace Sundevil" proběhlo sedmadvacet domovních prohlídek, tři lidé byly zatčeni. V akci bylo nasazeno 150 policistů ve „dvanácti" městech po celých Spojených státech (Různé zprávy místního tisku uváděly „třináct", „čtrnáct" a „šestnáct" měst). Zabaveno bylo asi 40 počítačů a přibližně 23 000 disket obsahující také legálně koupené počítačové hry, legální software, soukromou elektronickou poštu, obchodní záznamy a osobní korespondenci. Vyřazeno z provozu bylo na 25 boardů. (Zdroj: Sterling)

1990 V Chicagu je v rámci Operace Sundevil zabaven Tajnou službou board Dr. Ripco, ale vzápětí obnovuje svůj provoz s novými stroji. (Zdroj: Sterling)

9. května 1990 Úřad státního zástupce v Phoenixu v Arizoně vydal tiskovou zprávu, oznamující celostátní policejní zátah proti „ilegálním aktivitám počítačových hackerů". Jeho oficiální název byl „Operace Sundevil". (Zdroj: Sterling)

červen 1990 Textař Grateful Death John Perry Barlow a zakladatel Lotus Development Mitchell Kapor se rozhodují založit Nadaci elektronického pohraničí (Electronic Frontier Foundation,

EFF). Cílem nadace je „financovat, uskutečňovat a podporovat snahy, které by právní cestou demonstrovaly, že Tajná služba USA uskutečňovala preventivní cenzuru publikací, omezovala svobodu slova, neoprávněně zabavovala vybavení a data, užívala nepřiměřenou sílu a všeobecně postupovala arogantně, despoticky a protiústavně.“ Rozsáhlou finanční pomoc nabízejí kromě Kapora ještě Steve Wozniak (spoluzakladatel Apple) a John Gilmore (spoluzakladatel Sun Microsystems). (Zdroj: Sterling)

24. - 27. července 1990 Probíhá proces s Knight Lightningem (vlastním jménem Craig Neidorf), jedním z vydavatelů Phracku. Obviněn byl z šíření Dokumentu 911 v časopise Phrack. Díky EFF a faktu, že údajně nebezpečný dokument v údajné hodnotě 80 000 dolarů je veřejně šířen samotnou Bellcore[10] za 13 dolarů, byl nakonec soud odložen na neurčito. (Zdroj: Sterling)

5. září 1990 Kevin Poulsen odesílá dopis televiznímu producentovi, který o něm připravuje televizní dramatizaci, ve kterém ho žádá, aby zvážil některé pasáže a formulace v pořadu. (zdroj: Littman)

14. září 1990 „Fry Guy“ je podmínečně odsouzen na 44 měsíců a 300 hodin veřejně prospěšných prací. (Zdroj: Sterling)

10. října 1990 Kevin Poulsen odpojuje všech 40 linek do živého televizního pořadu stanice NBC o jeho zločinech s názvem „Temný Dante“. (zdroj: Littman)

únor 1991 Hacker Phiber Optik byl zatčen a obviněn ze zneužití triku s předvolbou 900 k bezplatnému volání. Byl shledán vinným a odsouzen k 35 hodinám veřejných prací. (Zdroj: Sterling)

10. dubna 1991 V samoobsluze, při výběru rybí polévky v konzervě, je zatčen hacker Kevin Poulsen. (zdroj: Littman)

21. června 1991 Je zatčen hacker Eric Heinz, spolupracovník Kevina Poulsena. (zdroj: Littman)

1. a července 1991 Selhání softwaru telefonních ústředen způsobuje výpadek spojení ve Washingtonu, Pittsburgu, Los Angeles a San Francisku – důsledky pocítilo okolo 12 000 000 lidí. (Zdroj: Sterling)

[10] BellCoRe – Bell Communication Research – vývojové laboratoře Bellu

9. září 1991 Soudce Bua uznává žádost o výmaz a zabezpečení záznamů o Knight Lightningově obžalobě. Tajná služba USA dostala příkaz vyjmout a zničit všechny záznamy o jeho případu. (Zdroj: Sterling)

17. září 1991 Dochází ke kolapsu části telefonní sítě v New Yorku. Přerušeno bylo spojení se třemi letišti, zrušeno bylo více než 500 letů a dalších asi 500 letů mělo zpoždění, takže problémy se spojením mělo asi 85 000 pasažérů. (Zdroj: Sterling)

10. dubna 1995 Po čtyřech letech odkladů je Kevin Poulsen souzen a odsouzen na 51 měsíců vězení. Většinu trestu má tou dobou za sebou. (zdroj: Littman)

1995 V tomto roce se podle ministerstva obrany podařilo ve 162 500 případech proniknout do sítě Pentagonu. Odhalen a stíhán je prý pouze jeden ze 150 hackerů.[11]

listopad 1996 Hackeři pronikají do systému dublinského nahrávacího studia a kradou zde a na Internetu zveřejňují dvě dosud nevydané skladby U2 Discotheque a Wake up Dead Man. Skladby začali též v Irsku a Británii šířit na kompaktech po deseti dolarech.[12]

1997 Pentagon oznámil, že jeho veřejnosti nepřístupné počítače připojené na Internet jsou čtvrtmilionkrát do roka cílem hackerských útoků – ze 64 procent úspěšných.[13]

17. března 1998 Pentagon přiznává, že hackeři ze skupiny MOD pronikli loni v říjnu k programu, který kontroluje vojenské satelity, „nervovou soustavu“ americké armády. Avšak zatímco mluvčí ministerstva obrany USA Susan Hansenová tvrdí, že nedošlo k úniku tajných informací, hackeři už nabízejí k prodeji program, s jehož pomocí prý vojáci navádějí přes satelity na cíl rakety a využívá se také k navigaci civilních letadel.[14]

únor 1999 Hackeři přebírají kontrolu nad britským vojenským komunikačním satelitem a požadují výkupné. Uvádí to list The Sunday Business s odvoláním na bezpečnostní zdroje. Podle

[11] *Armáda odolává počítačovým pirátům, in* Mladá Fronta DNES, 10. června 1996

[12] Hackers release two upcoming U2 songs on Internet, tiskový servis Associated Press, 18. 11. 1996

[13] Počítačoví piráti se dostali k satelitům, in Mladá Fronta DNES, 23.4.1998

[14] Počítačoví piráti se dostali k satelitům, in Mladá Fronta DNES, 23.4.1998

zdrojů listu hackeři v první polovině února změnili dráhu jednoho ze čtyř britských vojenských komunikačních satelitů a zastavení manipulací podmiňují složením výkupného. „Je to naše noční můra," vyjádřil své pocity jeden ze zaměstnanců tajné služby. Vojenští stratégové tvrdí, že při jakémkoliv (i jaderném) útoku na Británii jsou případnému agresorovi největším trnem v oku právě komunikační systémy. „Nejedná se o nějaké počítačové nadšence, kteří jen tak naslepo zkoušejí, co se dá. Je to velmi vážné a vyhrožování to dělá ještě vážnějším," cituje agentura Reuters bezpečnostní zdroj. Policie se odmítá ke kauze vyjádřit, protože vyšetřování je prý ve velmi citlivé fázi. Nevyjadřuje se ani britské ministerstvo obrany.[15]

[15]Satellite seizure, blackmail reported, servis Reuters Limited, 28. 2. 1999

Hacking v České a Slovenské republice v datech

25. března 1996 Z recese vzniká dokument „Jahodový sirup Security Advisory“ na jehož popud vzniká spontánně skupina SERT.[16]

duben 1996 Skupina SERT maže archívy ilegálního software na serverech diana.troja.mff.cuni.cz a kmotr.pf.jcu.cz a upozorňuje správce, aby je neobnovovali či znovu nezakládali, jinak budou jejich servery smazány.

srpen 1996 Poté co správce serveru Ludvik Friebel obnovil warez ftp na „kmotrovi“, byl tento server znovu smazán.

18. září 1996 Skupina SERT vyřadila z provozu LIANE BBS (buteo.kin.vslib.cz).

18. září 1996 Skupina SERT změnila stránky TASR (Tisková agentura Slovenské republiky) a přidala tam následující článek, který se tvářil, jako skutečné zpravodajství: *„Niekolko slovenskych pocitacov a serverov napojenych na sieti Internet bolo tento tyzden tercom utokov skupiny hackerov, nazyvanych Syrup Emergency Reaction Team (SERT). Dovodom ich utoku bolo upozornit na rozmach zneuzivania Internetu na rozsirovanie kradnuteho licencneho softwaru. Medzi napadnutymi pocitacmi boli aj servery firiem zaoberajucimi sa poskytovanim sluzieb suvisiacichs pripojenim k sieti Internet, ako napriklad Slovak Academic Network (SANET), alebo Netlab s.r.o., ale aj mnoho skolskych ser-*

[16] Jahodový sirup Security Advisory, elektronicky, http://hysteria.sk/arxiv/folklor

vrov, o ktorych je zname ze su zneuzivane na distribuciu nelegalneho softwaru. Na napadnutych serveroch bol vymazany vsetok najdeny nelegalny software a boli na nich instalovane propagacne stranky povzbudzujuce k boju proti sireniu kradnuteho softwaru.“

15. února 1997 CzERT změnil titulní stránku serveru MAmedia a zveřejnil na ní pravá jména, adresy a telefony účastníků konference o ilegálním softwaru.[17]

18. února 1997 Na Neviditelném psu se objevuje zprávička o hacknutí serveru Mobil.cz.

22. února 1997 CzERT změnil titulní stránku nejnavštěvovanějšího českého serveru Seznam.[18]

23. února 1997 CzERT třikrát změnil titulní stránku banky Union[19].

24. dubna 1997 CzERT odeslal massmail s politickým textem asi na 25 000 adres na Slovensku. V průběhu politické krize a univerzitních stávek odeslal cZert celkem asi 125 000 emailů.

červen 1997 Všichni CzERTi se poprvé scházejí v Praze.

17. října 1997 Jiří Dastych pro ČTK říká, že policisté jsou na stopě počítačovému démonovi, který vystupuje pod jménem CzERT a že s každým dalším průnikem se hacker přibližuje odhalení.[20] Ondřej Neff v deníku Neviditelný pes píše, že ho dnes CzERT navštívil ve stánku Internet Servisu na Invexu v Brně, zdvořile spolu pohovořili a že žádné stopující policisty hackerovi v patách neviděl.[21]

17. leden 1998 V Praze se koná další CzERT session. Tentokrát na ni vtrhne Policie ČR a legitimuje všechny účastníky

[17] hacknutý server MAmedia, elektronicky, *http://www.mamedia.cz,* dnes *http://www.mageo.cz*

[18] hacknutý server Seznam, elektronicky, http://www.seznam.cz

[19] 38 hacknutý server Union Banky, elektronicky, http://www.union.cz, auditorium „HACKING, aneb proč žádat roota o konto“ MaMedií (http://www.mamedia.cz) ze dne 23. 2. 1997

[20] zpráva ČTK ze 17. 10. 1997, elektronicky

[21] *Neviditelný pes, 17. 10. 1997,* elektronicky, http://pes.eunet.cz

Folklór

Mentorův manifest

Tento manifest by se dal označit za kultovní. Poprvé se objevil v Phracku v říjnu 1986 a od té doby se s ním ztotožňují hackeři i počítačoví nadšenci z celého světa. Naleznete jej také na většině hackerských stránek na Internetu.

=-

Následující text jsem napsal krátce po mém zatčení...

\/\Svědomí hackera/\/

napsal

+++ The Mentor +++

Napsáno 8. ledna 1986

=-

Dneska byl zase zatčen nějaký další hacker, jsou toho plné noviny. „Teenager zatčen pro počítačový zločin“, zatkli hackera za průnik do banky.

Zatracené děti. Všechny jsou stejné.

Ale pokusili jste se svou jasnou psychologií a trojkusým technomozkem padesátých let někdy nahlédnout do mysli hackera? Položili jste si někdy otázku, jaká síla ho zformovala, co vytvarovalo jeho osobnost?

Já jsem hacker, vstupte do mého světa...

Můj svět začíná školou... Jsem chytřejší než většina ostatních dětí, ty hovadiny, co nás učí, mě nudí...

Zatracený neschopa. Jsou všichni stejní.

Jsem na gymplu, nebo na střední škole. Padesátkrát jsem už slyšel jak zkrátit zlomek. Chápu to. „Ne, slečno Smithová, nenapsal jsem postup. Udělal jsem to z hlavy...“

Zatracené dítě. Asi to někde opsal. Jsou všichni stejní.

Dneska jsem udělal objev. Našel jsem počítač. Počkejte momentík, je to perfektní. Dělá to co chci. A když to udělá něco špatně, je to proto, že já jsem udělal chybu. Ne proto, že mě nemá rád...

Nebo se mnou cítí ohrožený...

Nebo si myslí, že jsem vychcanej parchant...

Nebo nemá rád učení a měl by odsud vypadnout...

Zatracený děti. Jenom si pořád hrajou. Jsou všechny stejný.

A pak se to stalo... dveře do světa se otevřely... vyslaný elektronický signál se řítí telefonní linkou jako heroin žílou narkomana a hledá úkryt před ubíjející každodenností... nalézá board.

„To je to místo... sem patřím..."

Znám tu každého, i když jsem se s nimi nikdy nepotkal, nikdy s nimi nemluvil, možná o nich už nikdy neuslyším... Znám vás všechny...

Zatracený děti. Pořád jenom obsazujou telefon. Jsou všechny stejné...

Válíte si zadky a my jsme všichni stejní... krmili jste nás kojeneckou výživou ve škole, když jsme chtěli steak... sousta masa, která jste nechali proklouznout byla předžvýkaná a bez chuti. Byli jsme ovládáni sadisty, nebo ignorováni apatiky. Ta trocha, která nás měla něco naučit a udělala z nás dobrovolné žáčky byla jako pár kapek vody v poušti.

Toto je náš svět... svět elektronů a ústředen, svět krásného baudu.

Používáme již existující služby a neplatíme za to, co by mohlo být směšně laciné, kdyby to nebylo majetkem chamtivých nenažranců, a jsme pro vás zločinci. Zkoumáme, a jsme pro vás zločinci. Chceme se učit, a jsme pro vás zločinci. Jsme bez rozdílu barvy, národnosti, bez náboženských předsudků... a jsme pro vás zločinci. Vy stavíte atomové bomby, vedete války, vraždíte, podvádíte a lžete nám a chcete, abychom uvěřili, že je to pro naše vlastní dobro, ale my jsme pro vás zločinci.

Ano, jsem zločinec. Páchám zločin zvědavosti. Páchám zločin posuzování lidí podle toho, co říkají a co si myslí, ne podle toho, jak vypadají. Páchám ten zločin, že jsem chytřejší než vy, a to mi nikdy neodpustíte.

Já jsem hacker a tohle je moje vyznání. Můžete zastavit jednotlivce, ale nemůžete zastavit nás všechny... jsme přece všichni stejní.

+++ The Mentor +++[22]

[22]in Phrack svazek 1, číslo 7, soubor 3, 25. říjen 1986, elektronicky, překlad autor

Hacking jako boj proti monopolům

$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$

Technologická revoluce

napsal

Doctor Crash

$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$

Hacking. Záliba polykající všechen čas, zabírající nespočetné množství hodin týdně učením, experimentováním a provozováním umění pronikání do mnohouživatelských systémů. Proč hackeři tráví největší část svého času hackováním? Někdo může říct, že z vědeckého zájmu, jiný, že to znamená mentální stimulaci. Ale skutečné kořeny hackerovy motivace jsou mnohem hlouběji. V tomto souboru popíšu základní motivy hackerů, vysvětlím vám spojení mezi hackingem, phreakingem, cardingem a anarchií, a představím „technologickou revoluci", která je zaseta v mozku každého hackera.

Abychom plně pochopili skutečné motivy stojící za hackingem, musíme nejdříve nahlédnout do historie. V šedesátých letech skupina studentů MIT postavila první moderní počítačový systém. Tato divoká, rebeliózní skupina mladých lidí nesla jako první označení „hackeři". Vyvinuli své systémy se záměrem řešit celosvětové problémy a pomoci celému lidstvu.

Ale jak vidíme, nestalo se to. Počítače se dostaly pouze do rukou velkých společností a vlády. Úžasná zařízení, která měla obohatit život lidí se stala nástrojem k jejich odlidšťování. Pro vládu a velké společnosti nejsou lidé více než místo na disku a vláda nepoužívá počítače,

aby poskytla pomoc potřebným, ale aby ovládala smrtící nukleární zbraně. Průměrný Američan může získat přístup pouze k malému mikropočítači, jehož hodnota je jen zlomkem toho, co za něj zaplatí. Korporace drží skutečně dobré vybavení za nepřekonatelnou hradbou neuvěřitelně vysokých cen a byrokracie. Kvůli takovýmhle věcem vznikl hacking.

Hackeři si uvědomují, že velké komerční organizace nejsou jako jediné oprávněny k používání moderních technologií. Vloupávají se do online systémů a používají je pro své vlastní účely. Samozřejmě vláda nechce, aby byl technologický monopol zrušen a tak postavila hacking mimo zákon a uvězní každého, koho chytí. Ale ještě horší než vláda, jsou bezpečnostní oddělení velkých společností. Vystupují jako „soukromé armády" jejichž nemilosrdnou taktiku vláda přehlíží, protože slouží také jejím potřebám.

Hacking je hlavní fasetou v boji proti monopolům na počítače. Jeden z prostředků, kterými hackeři dosahují svých cílů, se vyvinul do samostatného umění: telefonní phreakování. Je normální, že každý hacker je zároveň phreakerem, protože ovládnutí technologie telefonních společností potřebuje k přístupu do počítače daleko od místa, kde žije. Telefonní společnost je další příklad zneužívané technologie, nepřístupné lidem kvůli vysokým cenám.

Hackeři často zjistí, že jejich současné vybavení kvůli monopolní taktice počítačových společností nedostačuje pro jejich účely. Pro více než přehnané ceny není možné legálně si koupit potřebné vybavení. Tato potřeba dala vzniknout další části boje: cardingu. Carding je způsob získání nezbytných věcí bez placení. Carding je tak jednoduchý opět kvůli hlouposti komerčních společností a ukazuje, že světový obchod je v rukou lidí, kteří mají mnohem menší přehled v technologiích než my, hackeři.

A je tu poslední způsob vedení války proti zneužívání počítačů. Je méně důvtipný, méně elektronický, ale mnohem přímější a dává vše jasně najevo. Mluvím o tom, co je nazýváno anarchií. Anarchií nemyslím význam, který je s tímto slovem obvykle spojován, ale proces fyzické likvidace budov korporací a státní správy. Je to velmi drastická a přesto zásadní část „technologické revoluce".

Hacking musí pokračovat. Musíme naučit nováčky umění průniku. Musíme také zlepšit bourání počítačů (crashing). Vím, že zbourání systému vypadá jako odporná činnost, ale není žádný jiný způsob, jak ukázat společnostem, že jejich praktiky musí skončit.

Jak jsem už napsal, toto jsou pouze motivy. Pokud potřebujete návod, jak provést nějakou z popsaných praktik, přečtěte si o tom nějaký soubor. A cokoliv uděláte, pokračujte v boji. Ať to víte nebo ne, pokud jste hackeři, účastníte se na revoluci. Nedělejte si starosti, jste na správné straně[23].

- -

Pokud máte otázky nebo připomínky k tomuto souboru či k „technologické revoluci“, nechte mi email na Metal Shop AE (314)256-7284, nebo na jakékoliv jiné BBS, kde bych se vyskytl.

$$

[23] in Phrack, svazek 1, číslo 6, soubor 3, 1986, elektronicky, překlad autor

Sirup bug

Tento soubor stál u zrodu skupiny SERT (více v textu na straně 30). Napsal ho Pajkus 25. března 1996.

JAHODOVY SIRUP SECURITY ADVISORY - 25 March 1996
Sirup Emergency Reaction Team (sert@sert.org)
Mon, 25 Mar 1996 00:51:21 -0700
Message-Id: <9603172340.AA02237@sert.org>
X-Sender: 6886@jahoda.sert.org
X-Mailer: Windows Eudora Pro Version 2.1.2 for Syrup Experts
Mime-Version: 1.0
To: (Recipient list suppressed)
From: Sirup-Security-Expert-Team
Subject: BoS: JAHODOVY SIRUP SECURITY ADVISORY - 25 March 1996
Sender: owner-best-of-sirup-security@suburbia.net
Content-Type: text/plain; charset="us-ascii"
Content-Length: 55291
Status: RO

=== SIRUP ADVISORY: 25 Marec 1996 ===

Volna Distribucia tohoto Sirup Security Advisory je povolena.

Toto upozornenie #14 je archivovane SERT teamom na :
ftp.sert.org:/pub/security/sirup/Sirup-Advisory.#14.25-Mar-1996

Toto Upozornenie tykajuce sa bezpecnosti Sirupov bolo poslane na nasledovne mailing listy a newsgroupy:

SIRUPTRAQ (siruptraq@crimelab.com)
SERT (Sirup Emergency Response Team, sert@sert.org)
food.security.sirup (newsgroup)
food.administration.sirup (newsgroup)

==========

Jahodovy sirup Bug & Exploit
==========

SYNOPSIA: Tento bug umozni uzivatelom ziskat neziaduce privilegia a poskodit system jahodoveho sirupu pred jeho zakupenim a uzivanim.

VERZIE SYSTEMOV: O tychto systemoch je zname ze su napadnutelne spomenutym
bugom:

- Jahodovy sirup, v.1.00-litrove balenie s obrazkom Rumcajza pod Jedlickou od vyrobcu Karpatia a.s., Prievidza.
- Jahodovy sirup, v.0.70-litrove balenie s obrazkom Rumcajza pod Jedlickou od vyrobcu Karpatia a.s., Prievidza.

Nevylucuje sa moznost napadnutelnosti inych verzii a systemov ale toto su v sucastnosti jedine overene verzie. Nas bezpecnostny team v sucasnej dobe skuma moznost napadnutelnosti inych verzii a prichuti sirupov.

EXPLOIT: Z bezpecnostnych dovodov bude presny postup na exploit tohoto bugu
zverejneny az dva tyzdne po vypracovani dokladneho patch-u na vyssie spomenute dve verzie jahodoveho sirupu.

DESCRIPTION: Tieto dve verzie jahodoveho sirupu su distribuovane so suid vrchnakom. Pri pozornom studiu jahodoveho sirupu si vsimnete ze sirupova flasa ma pri uzaveri bezpecnostnu ochranu z plastikoveho obalu. Vsimnite si ze tento plastikovy obal pokryva cely vrchnak a taktiez uzavieraci system sirupovej flase. Pozornemu uzivatelovi sirupu urcite neujde dolezity fakt, ze na to aby tento plastikovy obal pokryvajuci vrchnak flase bol funkcny, musi byt odstraneny jedine pri prvom otvarani a pouziti jahodoveho sirupu. Avsak nas team sirup-expertov zistil, ze ak uzivatel pevne uchopi cely vrchnak flase aj s plastikovym obalom do ruky a opatrne ho odkruti, je mozne dosiahnut otvorenie sirupovej flase bez porusenia ochranneho plastikoveho obalu. Tym bude mat uzivatel kompletne cely otvaraci mechanizmus sirupu v ruke a tym aj kontrolu nad celym sladkym sirupovym systemom.

Po takto ziskanych sirupovych-systemovych privilegiach moze uzivatel vlozit do sirupu ihle, spendliky a ine predmety odborne zvane "trojske kone", alebo cerviky, dazdovky a ine organizmy nazyvane "virusy". Potom moze naspat bezpecne uzavriet vrchnak jahodoveho sirupu bez porusenia jeho plastikoveho obalu. Vynaliezavost takych podvratnych individui ako sirupovych hackerov je zial znama z viacerych pripadov v minulosti, kedy doslo k infiltracii sirupov.

Budeme Vas priebezne informovat o postupe naseho vyskumu v oblasti

bezpecnosti jahodoveho sirupu s obrazkom Rumcajza pod Jedlickou.

S pozdravom: "Sirup - Zaklad racionalnej vyzivy !!" sa luci,

SERT Team

Koniec Sirup Security Advisory #14, 25. Marec 1996.[24]

[24] poskytl Pajkus, elektronicky, ke stažení na http://hysteria.sk/arxiv/folklor

Rozhovor Ondřeje Neffa s CzERTem

Nejdříve něco o sobě: jsi sám nebo vás je víc? Asi muž... kolik je ti let?

Jsem CzERT a to musí stačit, více by byly detaily, do kterých nechci zbytečně zabíhat, proto taky budu psát v jednotném čísle.

Ano, jsem chlap.

A k mému věku asi tolik. CzERTu (jako osobě) bude zřejmě něco mezi 20-30 let. Žádný stařík, žádný mladík, prostě nejlepší věk. K čemukoliv.

Jake vzdelani je treba mit, aby ses stal hackerem schopnym nabourat ministerske a vojenske web servery?

Pokud dobre vim, jedinec se stava hackerem od doby, kdy se nauci psat na klavesnici az do veku nad hrobem. Zalezi na informacich , schopnostech a mnohdy i na nahode. Vzdelani je uzitecne, ne vsak nutne. Hacker muze byt vyuceny kuchar nebo vysokoskolsky profesor informatiky.

Podle jakeho klice si vybiras svoje cile?

Zasadne podle zadneho klice, proste se jen tak brouzdam po siti, prohlizim servery, a pokud naleznu v systemu skulinku a dany stroj stoji za povsimnuti, je casto navstevovan, ci vicemene oficialni, byla by skoda toho nevyuzit.

pozn.: www.army.cz byl vybran, protoze v jejich systemu byla obrovska lochna, ktera umoznovala komukoliv ziskat absolutni pristup do systemu a k datum. Pro root-a na www.army.cz : heslo KLEOPATR (pro system je dulezitych prvnich 8 znaku hesla, zbytek je ignorovan) je unsecure, to by mel zkuseny administrator jiste vedet. Takze jsem na tento problem upozornil sveraznym zpusobem. Podle meho by bylo lepsi to udelat takhle, nez nechat tam diru a umoznit potencialnim narusitelum s jiste nekalymi umysly udelat neco strasneho.

Predchazely nejake pripravy a pokud ano, jake?

Pripravy pred bitvou, v jako kazde valce :)

Co sledujes svou cinnosti – chapu recesi z vojaku a ministerstva zdravotnictvi, proc Hollywood? Je to jen zabava, prekonani technickeho problemu?

Zabava na prvnim miste, nekdo sbira znamky, ja servery. A mam z toho poteseni, samozrejme. Dale tim chci upozornit na soucasnou situaci, kdy mnoho ceskych firem v prekotnem snazeni o pripojeni se k Internetu zapomina na zakladni bezpecnostni principy, neuvedomuje si, do jakeho nebezpeci se tim dostava, a u nami hacknutych serveru to plati dvojnasob. Obzvlaste vladni instituce, by si mely uvedomit, ze pracuji s privatnimi daty vsech obcanu, ktere se touhle cestou mohou dostat do nepovolanych rukou.

Nebo je vyber dany proste bezpecnostnimi opatrenimi?

Nerek bych.

Jsou dva druhy serveru. Prvni, ktere si o to vyslovene rikaji, a ty druhe, ktere me zajimaji at z toho ci jineho duvodu.

Proc uderis vzdycky v patek – je to proto, ze technici maji volno a nehlidaji servery?

To je jeden z duvodu. A pak taky ten,ze po temer probdele noci v sobotu nemusim vstavat, pres vikend maji vsichni volno a kazdy ho vyuzije jinak.

Jaky mas pocit, kdyz se ti to povede?

Prijemny.

Uz se nekdy stalo, ze se ti nepodarilo do serveru vniknout?

Ne vsechny servery jsou na tom z hlediska bezpecnosti spatne.

Zatim – pokud vim – jsi vzdycky jenom pozmenil homepage. Citis pokuseni – dejme tomu – znicit datovy obsah serveru?

Obcas me to napadne, ale slusne vychovani je silnejsi.

Jsi pripraven na eventualitu, ze budes odhalen?

Uz mam slusnou zasobu buchet.

Bojis se trestu, nebo si takovou moznost nepripoustis?

Bojim, ale pokuseni je silnejsi.

Pral by sis, aby lidi jako jsi ty, zabyvajicich se podobnou cinnosti, bylo vic?

Pral bych si svetovy mir, ale k veci: konkurence je zdrava, ale v podstate je mi to jedno.

Jsi v kontaktu se zahranicnimi (myslim tim hlavne americkymi) hackery?

Rekneme ze v primem kontaktu ne, ale obcas se hodi par jejich informaci.

** CzERT-man **

PS: vyridte pratelum z MP at jsou radi, ze to dopadlo takhle, a venuji se radeji jinym, dulezitejsim pripadum.[25]

[25] in Neviditelný Pes, 2. 12, 1997, elektronicky, http://pes.eunet.cz

Hacker je nejdarwinističtější tvor

Tento text ukazuje rysy svým způsobem pro hackery charakteristické. Hacker ho zveřejnil na upravených stránkách Lanprojectu.

to nam to zase ubehlo, co? co nevidiet budem sediet vo vlaku na ceste na prazdniny u babicky (alebo take cosi) a tesit sa ako budem nahanat dievcata po zahumienkoch. totiz poviem vam, dievcata miluju hackerov, a to neplacam iba do vetra, ale mam to podlozenou darwinovou teoriou. v minulosti slo o to mat schopnost zabit medveda jednym uderom tomahawku a priniest zene medvedie labky na nedelny obed a kozusinu do obyvacky na stenu, avsak tieto vlastnosti sa stavaju coraz menej dolezitymi. prichadzajuca era informacnej revolucie nam prinasa tri jasne rozdielne smery evolucie homo sapiens:

prvy evolucny typ su hackeri – expertni znalci pocitacov a informacnych sieti. tento typ homo sapiens sa postupne prepracuje na veduce miesta nasej spolocnosti a bude vladnut svetu. (vynimkou su unix administratori a tech support, oni su odsudeni na zivot v tupej nevedomosti.. fakt nekecam.. mrknite sa na .bash_history miestneho admina a zasmejte sa spolu so mnou)

druhy typ su bezni pocitacovi (l)useri, to je ten typ ludi co sa tvari ze ovlada ms excel ale pritom potajme maju v sufliku pracovneho stola kalkulacku a vzdy si radsej vsetko rucne prepocitaju. Je to aj ten typ co sedi s pootvorenymi ustami nad novou verziou dooma, neovlada cheat kody a bedzucho klika cely den do tlacitka ctlr. tento evolucny typ postupne vyhynie na svoju vlastnu blbost. k tomu typu patris s najsamvacsou pravdepodobnostou aj ty. a poviem vam jednu vec - ja vas nemam rad a ste mi ukradnuti. vymyslate o mne chabrusoviny,

kritizujete moje aktivity z moralnej stranky, z technickej stranky, z moralno-technickej a technicko-moralnej, ale viete co ? ja vas mam fest na haku !

pri behani po serveroch mi islo o to aby sa admini poklopkali po cele a uvedomili si ze praca na internete vyzaduje ovela viacej ako vytiahnut server z krabice a zapnut ho do zasuvky. vas evolucny typ homo sapiens postupne vyhynie na vlastnu blbost. pokial som vam hackol v minulosti server, tak patrite prave do tejto kategorie a veru si to aj zasluzite takyto potupny koniec - totiz to ze som vam hackol server a trapne prerobil html fajly znamena ze ste pre svojich uzivatelov a klientov nevytvorili dostatocne bezpecne prostredie. to by prave malo byt vasim zakladnym poslanim. juj ale to uz som sa rozohnil certovskym pekelnym plamenom.. takze podme radsej este naspat k tym evolucnym typom..

finalne tu je tretia vyvojova kategoria homo-sapiens ludia nepouzivajuci pocitace. Tym postupne narastie srst a chvost a budu umiestneni do ZOO kam sa na nich budeme chodit pozerat a krmit ich bananmi. (do tejto kategorie urcite patria redaktori Mladeho Sveta, ktori bez akejkolvek znalosti pisali o mne defektoskopiny, pozliepali odpovede, napisali ze unix je programovaci jazyk.. a tak.. ten clanok bol fakt shit :)

poviete si – no dobre, dobre.. prestan uz kecat somariny, aj tak to nikto necita. nuz hej, ale na predoslych hacknutych CzERT www strankach boli iba suche a trapne obrazky, vulgarnosti a oplzlosti. ja viem, preto mam co dohanat ohladne ukecanosti :) no podme naspat k zenam a k prazdninam.. tak co si myslite, ktory evolucny typ si vyberie zena ? no jasne ze ten najdarwinistickejsi (nie je to bomba vyraz ?) - cize si vyberie *hackera* s potencialom stat sa svetovym vladcom. no a hackeri su fakt dobri milenci.. hovoril mi to kolega seteuid a stale sa s tym chvasta... ja sice zovseobecnujem na zaklade jednej malej statistiky, ale uznajte ze aj tak je to doteraz moj najsilnejsi a najrozumnejsi argument.

no a zoberte si ozonovu vrtsvu. pravda, kedysi boli v mode opaleni svalovci v ciernych plavkach ktori obletovali dievcata na mestskom kupalisku. ale vazeni, pri dnesnom stave ozonovej vrtvsy budu tito opaleni svalovci uskvareni zaziva ako spekacky a umru v pekelnych mukach. Ti co neumru (lebo pouzivaju Nivea opalovaci krem s fakto-

rom 10) budu v klietkach v ZOO a my sa na nich budeme chodit smiat. preto zeny miluju muzov ktori sa zatvaraju na 24 hodin denne doma pri pocitaci.

Henry Kissinger napisal ze moc je ten najsilnejsi afrodiziak. A Bill Clinton povedal ze mudrost je najsilnejsia moc. z toho logicky vyplyva, podla prehlasenia vlady Spojenych Statov, ze mudrost je nasilnejsi afrodiziak. pre tych co by chceli proti tomuto argumentovat - pozrite sa ja som iba zasrany binarny schizofrenik - ale toto tvrdi vlada usa, tak to sakra akceptujte. nezabudnite ze vlada usa ma pod kontrolou distribuciu a dane na cigarety, alkohol a drogy - takze maju velmi dobre skusenosti ohladne uspokojovania zien.

hacker je proste sexualny idol informacneho veku a hovorte si co chcete. ja planujem stravit toto leto niekde zasity daleko prec od pocitacov a osvedcit si tuto teoriu v praxi, hehe. pre tych co ma poznaju - majte sa tu krasne a dufam ze sa uvidime pocas leta na sessionoch.. zdravim ricolu za jeho super pristup k veci, ilpha lebo aj tak mucha tse-tse to sklo prerazi, kuceraveho eskimaka lebo mi nadava ze som bashovy dialupista, seteuida lebo je najlepsi milenec.. *wink*.. deba pozdravujem iba zo sucitu, lebo ma zdravotne problemy, generica lebo moze deba vyliecit, xxa lebo ma nema rad, a vy ostatny bezte do pekla, ale nezabudnite - czert owns ya !

Zdroj: Hacknuté stránky Lanprojectu [26]

[26] hacknutá verze, elektronicky, http://hysteria.sk/hacked

Politický massmail CzERTu odeslaný na přibližně 25 000 adres

Date: Thu, 24 Apr 1997 03:28:38 +0200
From: Maco Mliec <root@nms.lanprojekt.cz>
Subject: Anna Remiasova: Ludia, prosim, zobudte sa!

Motto:
"Drviva vacsina studentov na
Slovensku podporuje HZDS."

Predseda HZDS na mitingu hnutia v sportovej
hale na Pasienkoch.

MINISTERSTVO VNUTRA je na to, aby dbalo na dodrziavanie zakonov. Ja nemozem ministra napominat' za to, pokial' sa nepreukaze, ze prekrocil kompetencie, ze chrani statne organy. Ja nemozem uznat' vylucne pravo opozicie vedenej Carnogurskym a spol. na porusovanie zakonov tohoto statu. Ked' toto zlo by v spolocnosti prevladlo, tak potom toto zlo sa bude sirit' ako lavina vsade. Tomuto zlu nesmieme dat' moznost' sa rozrast'. Toto je nieco od coho musime prec. Co treba zastavit' kym je to este male ale nemoze to narast'.

Predseda vlady pre masmedia 12.3. vo svojej reakcii na brutalny
zasah policie v priestoroch Ministerstva Kultury . . .

++

ROBERT KOTIAN

Rozhodnutie vlady SR, ktorym sa uklada MINISTROVI VNUTRA nedorucovat' obciam hlasovacie listky s otazkou c. 4 dovtedy, pokial Ustavny sud SR vo veci nerozhodne, t.j., ci je otazka c. 4 (o priamej volbe prezidenta) v sulade s Ustavou SR, resp. ci mozno menit referendom ustavu SR, nema ziadnu oporu v zakone. Podla $ 15 ods. 3 zakona 564/1992 o sposobe vykonania referenda totiz Ministerstvo vnutra zabezpeci, aby sa hlasovacie listky vytlacili a v potrebnom mnozstve dorucili obci. O nedorucovani hlasovacich listkov (hoci aj do rozhodnutia ustavneho sudu) sa v zakone nic nehovori, nehovoriac o tom, ze vlada uz v tomto case nema nic spolocne s organizovanim referenda, ktore je cele zalezitostou ustrednej referendovej komisie, okresnych a okrskovych komisii. Toto neznamena nic viac ako to, ze vlada SR, ktora "moze konat iba na zaklade ustavy, v jej medziach a v rozsahu a sposobom, ktory ustanovi zakon", kona PROTIZAKONNE.

IVAN SIMKO

Mozno postup vlady hodnotit ako marenie referenda, ktore je trestnym
cinom?

Kazdy, kto by ucinnym sposobom maril vykonanie referenda, dopustal by sa trestneho cinu podla $177 Tr. zakona."

NIHIL NOVE SUB SOLVE ... uz sme si zvykli.(?)(!)

Prezident sa pyta, preco prokuratura v 26 konkretnych pripadoch nedbala na dodrziavanie zakonnosti
14-04-1997, 1. strana
BRATISLAVA (SME - bog, jo, pan) - Prezident Michal Kovac zaslal v uplynulych dnoch ustavnym cinitelom a predstavitelom politickych stran 13-strankovy material o nevyriesenych podozreniach zo spachania zavaznych trestnych cinov na Slovensku. Poukazuje v nom na zodpovednost organov prokuratury, najma vsak generalneho prokuratora SR JUDr. M. Vala. "Pachatelia zavaznych trestnych cinov (vrazd, unosov, vybuchov aut) zostavaju nepotrestani. Beztrestne sa na nasom uzemi rozsiruje aj ekonomicka moc roznych mafii, pricom sa uz neboja ani za bieleho dna vyrovnat si ucty vrazdou. Verejnosti nie je zname, ze by bol niekto odhaleny a trestne postihnuty za umyselne pouzitie vybusniny proti zivotom a majetku obcanov. Su dovodne podozrenia o prepojeni mafianskych klanov s procesom privatizacie a ich spojenia s politickymi kruhmi. Beztrestni zostavaju ti, ktori v rozpore so zakonmi sprivatizovali milionove hodnoty," uvadza prezident. Podla

neho to u obcanov vyvolava pocit bezmocnosti, deziluzie a rozkladne to posobi na zakonnost a principy pravneho statu. Obcania si podla M. Kovaca kladu otazky, preco organy cinne v trestnom konani, najma prokuratura, nekonaju aktivnejsie alebo preco nekonaju vobec vo veciach, ktore su obcanom zname a u ktorych aj neodbornik predpoklada podo- zrenie z porusovania ustavy a zakonov. Hlava statu preto v materiali kladie otazky suvisiace s 26 konkretnymi pripadmi, ktore sa za posledne tri roky udiali.
>>>
Prvy sa tyka necinnosti prokuratury vo veci protipravneho podpisu dohody medzi kandidatmi HZDS na zvolenie do NR SR o tom, ze sa vzdaju mandatu a uhradia volebne naklady, ak prestanu byt clenmi HZDS. Dalej poukazuje na trestny cin poskodzovania cudzich prav - zaslanie obalky o tzv. vzdani sa mandatu F. Gauliedera do NR SR, pricom okresny prokurator zistil, ze obalku listu Gaulieder nepisal a k jej odoslaniu doslo proti jeho voli. Dalsie pripady sa tykaju nezakonneho policajneho preverovania peticnych harkov DU a ulozenia pripadu falsovania harkov ZRS napriek konstatovaniu, ze doslo k spachaniu trestneho cinu marenia pripravy a priebehu volieb. Dalej dokument uvadza podozrenie, ze prislusnici SIS zinscenovali diskreditaciu predsedu Konferencie biskupov Slovenska R. Balaza v pripade predaja triptychu Klananie troch kralov - trestne stihanie sice bolo zastavene ako nezakonne, ale organy prokuratury dosial nevydali pokyn na preverenie podozrenia z trestneho cinu zneuzivania pravomoci verejneho cinitela a nezrusili nariadenie vysetrovatelky o vrateni veci. Ine pripady suvisia so zavlecenim M. Kovaca ml. do cudziny, nekonanie organov pri podozreniach z trestneho cinu zneuzivania pravomoci verejneho cinitela riaditelom SIS I. Lexom a jeho podriadenymi, ako aj sefom sekcie vysetrovania MV SR J. Kostovom. Spominaju sa aj krive obvinenia vysetrovatelov Lexom, ulozenie pripadu telefonickeho rozhovoru Lexa - Hudek, pouzivanie informacnotechnickych prostriedkov SIS-kou bez suhlasu sudov, nekonanie organov proti generalnemu prokuratorovi za zneuzitie pravomoci verejneho cinitela, ked nerealizoval milosti udelene prezidentom. Hlava statu kladie v materiali otazky aj o privatizacnych rozhodnutiach. V pripade Nafta Gbely nadobudatel Druha obchodna, s. r. o., poskodila stat o najmenej 2,5 mld Sk odkupeni akcii pod trhovu cenu. Dalej material menuje Skloobal Nemsovu, kde privatizujuca spolocnost nebola ani zapisana v Obchodnom registri, Bardejovske kupele, Piestanske kupele ci pridelenie bytov FNM ministrom a vysokym statnym uradnikom. Premier podla materialu porusil tajomstvo prepravovanych sprav, ked na mitingu HZDS zverejnil list papeza urceny mons. R.

Balazovi. V texte sa spomina aj prijimanie prislusnikov StB do SIS, napriek vtedy platnemu lustracnemu zakonu, monitorovanie oslav narodenin J. Langosa, prislusnikmi SIS atd. Prezident v zavere vyzyva NR SR a politicke strany, aby sa zasadili o napravu tohto stavu a dodrziavanie zakonnosti v SR.

JURAJ SULIK,
predseda Koordinacneho centra strajkovych vyborov vysokych skol:
"Dnes o 13.00 startujeme pred VSMU na Venturskej druhy pochod na parlament, na ktorom sa zucastnia v podobe papierovych hlav aj nasi najvyssi statni predstavitelia. Pred zasadnutim Vyboru NR SR pre vzdelanie, vedu, kulturu a sport chceme protestovat proti vzniku dvoch novych vysokych skol v Banskej Bystrici a Trencine, ktore nemaju svoje opodstatnenie. Ministerstvu skolstva chyba 680 milionov korun a tieto skoly budu stat dalsie stovky milionov. O tyzden, v utorok 29. aprila, sme sa rozhodli pripojit k pochodu na pamiatku vyrocia smrti Roberta Remiasa, lebo v tomto pripade nejde o zaujmy politickych stran, ale o problem vztahu medzi obcanmi a mocou. Pred rokom tu zahynul mlady clovek a dnes je uz dokazane, ze nasilnou smrtou. Vec treba konecne jednoznacne pomenovat a vyriesit! A pokial ide o referendum - studenti sa budu tiez podielat na pochode Slovensko do Europy od 6. do 20. maja. Tam sa budu rozdavat aj materialy, vysvetlujuce, preco je EU pre nas dolezita, preco sa treba zucastnit referenda a vstupit do NATO. Ved podla agentury FOCUS 80 percent mladych chce do Europskej unie, to je nas jasny motiv."

29. aprila bude DU spolu s ostatnymi stranami organizovat miting a svieckovy pochod k uradu vlady SR (zaciatok o 17. hodine na Namesti SNP). Zaroven sa uskutocni v Kosiciach akcia tamojsieho Liberalneho klubu, na ktorej prislubili ucast predstavitelia DU, osobnosti spomedzi otvoreneho fora Zachranme kulturu. Pozvanie prijala aj matka R. Remiasa. Akcia sa uskutocni 29. 4. o 17. hodine v priestoroch zasadacej miestnosti kosickeho magistratu.

==========

Co si myslis Monika, preco ta dali rodicia do Detskeho domova?

<PRETOZE IM SRDCE STVRDLO NA ROZUM>

(baculate dievcatko sa zarazi v modrych ockach sa jej na chvilu mihne tien nepochopitelnej hrozy ...)

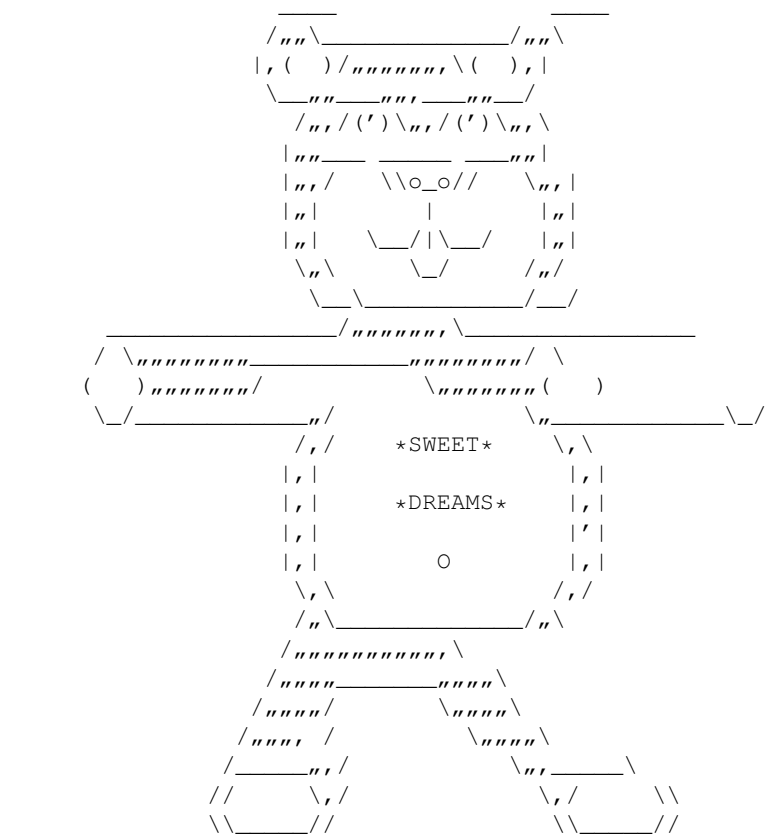
Kupili mi medvedika ... aha ... pozrite!

A mas ho rada?

<NEMAM>

Mam ...

<MAS PRAVDU ...>



cZert

CzERT session - drasťákoidní melodramatický popis

Vramci vseobecnej prazdninovej nudy som sa pokusil napisat taky drastakoidny melodramaticky popis nedavnej cZert session v Prahe.. je to stylovo niekde medzi MAMEho Drastakom a medzi zapisnikom 14-rocneho pubertaka co cita iba Dicka Francisa a Raymonda Chandlera.. heh tu to je :)

Hodinky sa ledva prevliekli cez pol dvanastu. Sedel som hore pri soche na Vaclavskom namesti a dlhu chvilu som si kratil sledovanim mladych turistov z Germanska, ich maly synator priserne vrieskal a kopal do akehosi svojho hybridu z Lega. Cakal som na dvanastu hodinu... uz iba za 30 minut sa odohra historicke stretnutie vsetkych cZertov.. vyznamne som si zapalil barborku lajtku..

..Cestou na cZert session meskal moj let Airbusom A340 spolocnosti Ceske Aerolinie cele 3 hodiny. Kapitan nam vysvetlil ze inzinieri sa snazia rebootnut software na kontrolu letu. Nebola to bohvieako povzbudzujuca sprava, zaspal som oprety o operadlo sedadla s myslienkou co by sa tak asi stalo keby im bol ten software zlyhal pocas letu...

Vysoky, ulizany steward s povysunutou dolnou sankou ma zobudil silnym trmacanim za plece, s pozvankou do pilotnej kabiny.

Kapitan lietadla ma hned spoznal podla velkej cervenej hlavy, vysklabeneho usmevu a zarasteneho chvosta. Hned ako sa zavreli dvere pilotnej kabiny, pochopil som ze nieco nie je v poriadku. Kapitan sa pozrel na mna cez jeho tmave Ray-Ban-ky a na hlase mu bolo poznat

uzkost v hrdle: "Dekuji Bohu ze ste na palube, CzERTe. Ste jediny kto nas v tehle chvili muze zachranit - podivejte se." Obrazovka palubneho pocitaca bola bez znamky zivota, riadiace kable sa ledabolo pohojdavali vo vzduchu a kontrolky automatickeho pilota boli vyhasnute. Vsetky video-obrazovky v kabine boli prazdne okrem napisu 'Abort? Retry? Fail?'

"Vsechny systemy jsou mimo provozu. Rychle stracime vysku. Jenom hacker vaseho kalibru dokaze ziskat kontrolu nad palubnim pocitacem pred tim ako se zroutime na zem." Skusal som protestovat, drziac hore pravu ruku s mozolnatymi prstami vydratymi od SUN Workstationovej infra-cervenej myse a drsnej klavesnice a nervozne som sa skrabal medzi rohy: "Sakra, toto je chabrus, ja som uplne mimo formy... od cias prveho hacknutia serveru Armady Ceskej Republiky lietam iba na UNIXoch, uz 3 roky som nemal v rukach nic vacsie ako je MS Natural Keyboard !" Kapitanovi sa po mojich slovach zjavili na cele chmary. "To je velice zle CzERTe, vypada to tak ze dnes tady zemre spousta lidi." "Frantisku nemame tady na palube jeste nekoho kto by dokazal nabehnout palubni server ?" dodal a obratil sa pri tom na toho vysokeho ulizaneho stewarda s povysunutou dolnou sankou. Ten sa chvilu prehrabaval v zozname cestujucich. "Neni to sice zadny expert jako CzERT, ale mame tady aspon neco... na sedadle 46C sedi pan William H. Gates, mam ho jit sem zavolat pane kapitane ?"

Bill Gates ! Moj odveky nepriatel, ako zvycajne najlacnejsie sedadlo v economy triede. Chvilu som sa pohraval s myslienkou nechat ho nech sa potrapi s palubnym pocitacom a nech potom vysvetluje na tlacovke v Seattle vypustenie novej bug-free verzie Fligh Control for Windows 95. Moja smrt by bola vlastne zanedbatelna malickost pri predstave ze by so mnou zomrel aj Gates.

Potom som sa ale obzrel cez ulicku dozadu na tie desiatky nevinnych nic-netusiacich tvari, pochrumkavajucich oriesky a veselo hladiacich von z okna na oblaciky plavajuce oblohou. Stvrdli mi crty tvare a vyhrnul som si vyznamne rukavy. "Uhnite sakra, preberam vedenie lietadlan !" Ignorujuc stiplavu bolest prenikajucu z mojich mozolnatych prstov, zacal som sa bleskurychlo pohybovat po klavesnici palubneho pocitaca. Pred ocami sa mi mihali statistiky procesov, zatazenie kernela, vysledky fsck.ext2... Sledoval som kutikom oka, ako dolna sanka ulizaneho stewarda od obdivu klesla o dalsich 5 centimetrov, pripominajuc zivanie vodneho byvola.

Moje prsty sa este zrychlili, teraz uz nebolo mozne rozoznat jednotlive udery do klavesnice. Prstove operacie sa zmenili do celoliatej masy premyslenych postupov. Ticho v kabine a bzukot klavesnice prerusil moj diabolsky smiech.

"Sakra-Chabrus-Cecky-Certi-Motorky, mam to !!" Natukal som na konzolu pocitaca, teraz uz pomaly a dorazne, par finalnych prikazov:

```
cZert[13:41][742]/usr/local/bin$ ./exploit.sh
krach...
seteuid()
Cracking.. please wait..
root[13:42][743]/usr/local/bin# whoami
root
root[13:42][744]/usr/local/bin# id
uid=0(root) gid=0(chabrus)
root[13:42][744]/usr/local/bin# shutdown -r now
```

Pocitac sa rebootol a zo zadu sa ozval zvuk styroch motorov Rolls Royce pomaly stupajucich do crescenda. "Priputajte sa prosim", precedil som cez zatate zuby, "teraz nas to bude triast". V zrkadlovom odraze predneho skla Airbusu A340 som zbadal kvapky potu kotulajuce sa po mojom cervenom cele. Cez okno bolo vidiet v dialke dispecersku vezu Ruzinskeho letiska....

Pohlad na velku postavu kracajucu smerom ku vchodu do Metra ma prebral z myslienok. Vaclavske namestie, 11:45. Maly German stale ziapal na vedlajsej lavicke. Vedel som ze postava kraca ku mne, vtedy som vsak este nevedel ze je to sam velky MARAT, ochranca kanala #marat-ltd.

Postava podisla ku mne a energicky ohlasila: "Irc.stealth.net 11:45 Mode -o neologic on #marat-ltd by Marat." Nerozumel som sice ani slovo, ale predpokladal som ze je to jeden z povestnych prazskych dialektov, preto napriek Meciarovmu novemu zakonu o Slovenskom statnom jazyku som sa pokusil dohovorit sa lamanou cestinou. "Prominte, ja nemluvit jazykem vaseho kmene, vy mluvite slovensky ?" spytal som sa opatrne. "Irc.stealth.net 11:46 Mode +nti on #marat-ltd by Marat" bola odpoved, ktoru som vsak nestacil zaregistrovat. V tom okamihu totiz nastal na Vaclavskom namesti nepopisatelny zmatok, rovnajuci sa soku zo zmetrasenia.. ludia padali na zem, potkynali sa o seba, krkolomo utekali prec z namestia, sprintovali do bocnych uliciek

a do podchodov... kym som si uvedomil co sa deje, cele namestie bolo ludoprazdne. Vtedy som pochopil.

MARAT je IRC RoBot ! Eggdrop ! V sekunde zlomku som sa vrhol k zemi a pevne som sa chytil rukami lavicky. Ale uz bolo po vsetkom, videl som z Vodickovej ulice pribiehat usmiateho SETEUIDa, GENERICa a DUSHEENa. CzERTi su tu !

SETEUID mi od dialky krical "Che che, to bol ale massdeop a masskick, co ?!" a vzapati mi dal opa. Vedla neho stala _JANINA_ a podavala mi ruku. Omraceny jej krasou nemohol som vyjachtat ani slovka, tak som cakal co mi povie. "Cestovni listky prosim." zasvitorila tichym hlasom. Nechapajuc som sa na nu pozrel. Zmurkla velkymi ocami a ja som v tej chvili chcel verit ze to zmurkla na mna. "Cestovni listky prosim !" povedala mi znova. Od prekvapenia som otvoril oci.

Nachadzal som sa v medzinarodnom rychliku Strela na trase Praha - Bratislava. Zbytky sna sa rozplynuli ked som par krat prekvapene zablikal ocami a odovzdal sprievodkyni cestovny listok. Mimovolne som sa obzrel von z okna smerom na zapad, tam kde este pred par hodinami bola historicka cZert session. Rozliate cervene slnko sa pohupovalo kusok nad obzorom.

Vonku za oknom sa odlomila vetvicka z jablone a clupla do vody.

Pajkus

zdroj: auditorium **cZert** na serveru MAmedia[27]

[27] 18.6.97 - 18:27, elektronicky, http://www.mamedia.cz

Hacker, lamer a luser

Ako som zistil, vacsina pouzivatelov pocitacov by sa dala zaradit do troch kategorii: Hacker, Lamer a Luser (volne prelozene Makac, Trapos a Uboziak). Nie kazdy vie, do ktorej kategorie patri (okrem hackerov) a tak vznikaju rozne paradoxy, napr.:

1) Kazdy si o sebe mysli, ze je Hacker.
2) Lamer si mysli, ze *LEN ON* je Hacker
3) Luser si mysli ze Hacker je Lamer.

Ako sa tito traja muzici spravaju v realnom zivote, ake su ich zvyky a navyky, vidiet v nasledujucich situaciach.

- Ake ma heslo na pocitaci:
La: tazke, napr. #3;2Gu=0 , kazdy tyzden ho zabudne
H : lahke, napr. zuzana, je mu to jedno, ci ho niekto hackne
Lu: lahke, napr. zuzana, odkial by niekto vedel, ze jeho zena sa vola Zuzana?

- Ked ma vysoky telefonny ucet:
H : hackne telefonnu ustrednu, za 3 roky ho chytia policajti
La: hackne susedovu linku, za 2 mesiace ho chytia policajti
Lu: preda modem, ide okopavat zahradku

- Zisti, ze stratil kluce od domu:
H : odomkne si dratikom
La: vykopne dvere, zisti, ze sa pomylil o jeden vchod (poschodie)
Lu: zazvoni

- Musi ist na pisomku z matiky: (podobnost z existujucimi osobami nahodna)

Lu: uci sa 2 tyzdne, vie to aj po rumunsky odzadu, 2
H : uci sa 5 min, 3 hodiny sa hra na pocitaci, 1
La: hra sa 3 hodiny aj 5 minut, nakoniec odpise od Hackera, 3

- Najde na sieti navod na vyrobu trhavin:
Lu: zavola na policiu a na ministerstvo, ziada svetovu vojnu
La: vyrobi si trinitritoluen, ukaze ho vsetkym priatelom, vsetci mrtvi
H : zacuduje sa, ako rychlo sa siria jeho recepty

- Pokazi sa mu na ceste auto:
H : okamzite odhali defektne tiahlo c) hriadela W12, nahradi ho zuvackou a zapalkou a odfrci
La: kopne do auta, skusi vymenit koleso, potom sviecky, a ked nic tak zavola do servisu
Lu: rozplace sa, odtlaci auto do servisu

- Ked musi ist do opery:
H : sadne si a zaspi este pred zaciatkom, na konci zatlieska
Lu: sedi so zavretymi ocami, poklepkava si prstami do rytmu, obcas sa rozplace
La: zbali uvadzacku, navstivi bufet, pluje z balkonu ludom na hlavy

- Pokazia sa mu hodinky:
Lu: umyje ich mydlom, pomikrovlnkuje a odnesie k hodinarovi
H : rozoberie ich a opravi, ostane mu polovica suciastok na dalsie pouzitie
La: rozoberie ich a perfektne zlozi, chvilu idu dozadu a potom navzdy zastanu

- Vlastni domace zviera:
La: buldoga, vola ho Hrdlorez
H : len pocitacovu mys (nemusi ju aspon krmit), kanarik, co trci z klietky zomrel pred dvoma rokmi
Lu: sliepky v panelaku

- Posledne slova pred smrtou:
Lu: (pise testament)
La: Dobry, Hrdlorez, dobry psicek, nehryz pana farara do nozicky!
H : logout

- Oblubeny film:
H : Apollo 13, Siet, Tron

La: Angelika I-VII
Lu: Beverly Hills, Baywatch, Dallas

- Oblubena kniha:
H : manualy k SunOSu, zdrojaky ku vsetkemu, aj Kucharska kniha
La: sci-fi
Lu: Chram Matky Bozej v Parizi

- Zivotny ciel:
Lu: zarobit vela penazi
H : hacknut ich vsetkych
La: stat sa hackerom

- Cita v novinach:
H : sport
La: predpoved televizie
Lu: horoskopy pre seba, zenu, vsetky deti, kolegov, sefa, vodica trolejbusu

- Otazka: Kolko je hodin?
Lu : za 10 min dvanast
La : 96/01/06 23:50:10 Sat
H : 7236289 (sekundy od 1.1.1970)

Slovníček

aka *„also known as“,* zkratka pro přezdívku

cracker člověk znalý strojového kódu, který různým způsobem odstraňuje ochranu proti kopírování v programech, hledá v nich hesla, či je jinak pozměňuje

crack pokud pomineme pojmenování drogy, jedná se o malý prográmek, po jehož spuštění dojde k úpravě jiného programu například k aktualizaci z omezené verze na verzi plnou. Výrobou cracků se zabývají především crackeři.

cyberpunk literární proud ve science fiction, založený v roce 1981 povídkou Johnny Mnemonic (česky Ikarie 1991/11) Williama Gibsona. Ukazuje temnou budoucnost lidstva ve světě megakorporací, dokonakých počítačových technologií a Matrix, globální počítačové sítě vizualizované v 3D modelu. Literární proud časem přešel v samostatné hnutí se svou vlastní subkulturou, kterou přijali za svou i mnozí hackeři.

echelon globální špionážní systém provozovaný a sdílený pětici velmocí — Spojenými státy, velkou Británií, Kanadou, Austrálií a Novým Zélandem

infopsychologie (původně exopsychologie) teorie Timothy Learyho, podle které lidé postupně přesídlí do virtuálního světa

kyberpunk viz **cyberpunk**

nekonečná smyčka viz **smyčka nekonečná**

smyčka nekonečná viz **nekonečná smyčka**

trójský kůň bájná finta Řeků při dobývání tróje, v počítačovém jazyce znamená program, který skryt v systému působí nějakou činnost (zachytává hesla, maže soubory, zpřístupňuje počítač útočníkům), avšak nedokáže se narozdíl od viru šířit na jiné systémy

hacker osoba, která se zabývá pronikáním do chráněných počítačových sítí nebo systémů

phreaker zabývá se nabouráváním telefonních sítí a zařízení, někdy jen k pouhému telefonování zadarmo, jindy k využívání operátorských služeb, odposlechu telefonů a datových přenosů a podobně. V době počítačového pravěku musel být většinou hacker i phreaker

virus, vir malý kousek počítačového kódu, který se dokáže replikovat (množit). Podobně jako skutečné biologické viry se může sám vložit do jiného souboru, pomocí kterého se dostane k jinému systému. Některé viry se jen šíří, jiné způsobují i různé destruktivní akce (mazání souborů, formátování pevných disků, psychický teror na uživatelích a podobně)

Zdroje

BookmarX- kam si to namířit na webu?

http://hysteria.sk vlajková loď českých a slovenských hackerů

http://eldar.cz/publiczone Public Zone – další články o hackerech

http://hysteria.sk/zatah překlad úryvků ze Sterlingovy knihy *The Hacker Crackdown*

http://hysteria.sk/prielom slovenský hackerský časopis *Prielom*

http://neworder.box.sk vyhledávací server na texty a nástroje k hackingu

http://underground.cz český časopis o digitálním undergroundě a věcech kolem

http://netmag.cz český časopis o počítačové bezpečnosti

http://underground.org „oficiální“ stránky světového počítačového podsvětí

http://www.2600.com hackerský čtvrtletník *2600*

http://www.phrack.com elektronický hackerský časopis *Phrack*

http://www.cert.org souhrn chyb v bezpečnosti systémů a návody na jejich opravu

http://www.rootshell.com databáze programů a návodů na zneužívání chyb v bezpečnosti systémů

http://www.kevinpoulsen.com Switchroom – domovská stránka hackera Kevina Poulsena

http://www.kevinmitnick.com Domovská stránka hackera Kavina Mitnicka

http://www.eff.org Electronic Frontier Foundation – Nadace elektronického pohraničí

http://earthspace.net/esr/faqs/hacker-howto.html jak se stát hackerem – hlavně snadno a rychle

http://www.OCF.Berkeley.edu/~stoll domovská stránka Cliffa Stolla, člověka, který odhalil průnik německých hackerů do amerických armádních sítí

http://berlin.ccc.de Chaos Computer Club Berlín

Doporučené čtení

Bruce Sterling: The Hacker Crackdown, elektronicky

česky zatím nevyšlo, ale nejdůležitější pasáže v češtině (překlad Václav Bárta) najdete na adrese `http://eldar.cz/publiczone/crackdown.html`. Český překlad k vydání připravoval Ondřej Neff, avšak po smazání serveru Mobil od tohoto záměru upustil

Gundolf S. Freyermuth: Cyberland – Průvodce hi-tech undergroundem, Jota, Brno, 1997

základní informace o digitálním undergroundu, hnutí cyberpunk

William Gibson: Neuromancer, Laser, Plzeň, 1998

kultovní sci-fi román, nejznámější dílo proudu cyberpunk

Jonathan Littman: Hacker – Podivný život a zločiny počítačového génia Kevina Poulsena, Práh, 1998

další informace o životě hackera, se kterým jsme se setkali v 1. kapitole

Cliff Stoll: Kukaččí vejce, Mladá fronta, Praha, 1997

příběh honu na hackery najaté KGB, aby pronikali do amerických armádních počítačů. Knížku sepsal sám člověk, který hackery v systémech objevil a pátrání po nich vyprovokoval.

Timothy Leary: Chaos a kyberkultura, Maťa, DharmaGaia, Praha, 1997

Timothy Leary prováděl v 60. letech na Harvardu oficiální experimenty s LSD, médii byl označován za „LSD gurua“, v 90. letech se pak věnoval virtualitě a počítačům, jako prostředkům rozšíření vědomí a individuality. V knize

jsou nejen Learyho teze a články, ale také rozhovory s významnými představiteli kontrakultur a kyberkultury.

Použitá literatura a zdroje

Většina informací o českém digitálním undergroundu byla získána z osobních rozhovorů či soukromé korespondence autora s jednotlivými postavami. Autor nezná žádné další údaje, které by mohly vést k identifikaci pachatelů případných trestných činů.

Ostatní bibliografické informace jsou uvedeny v poznámkách pod čarou.