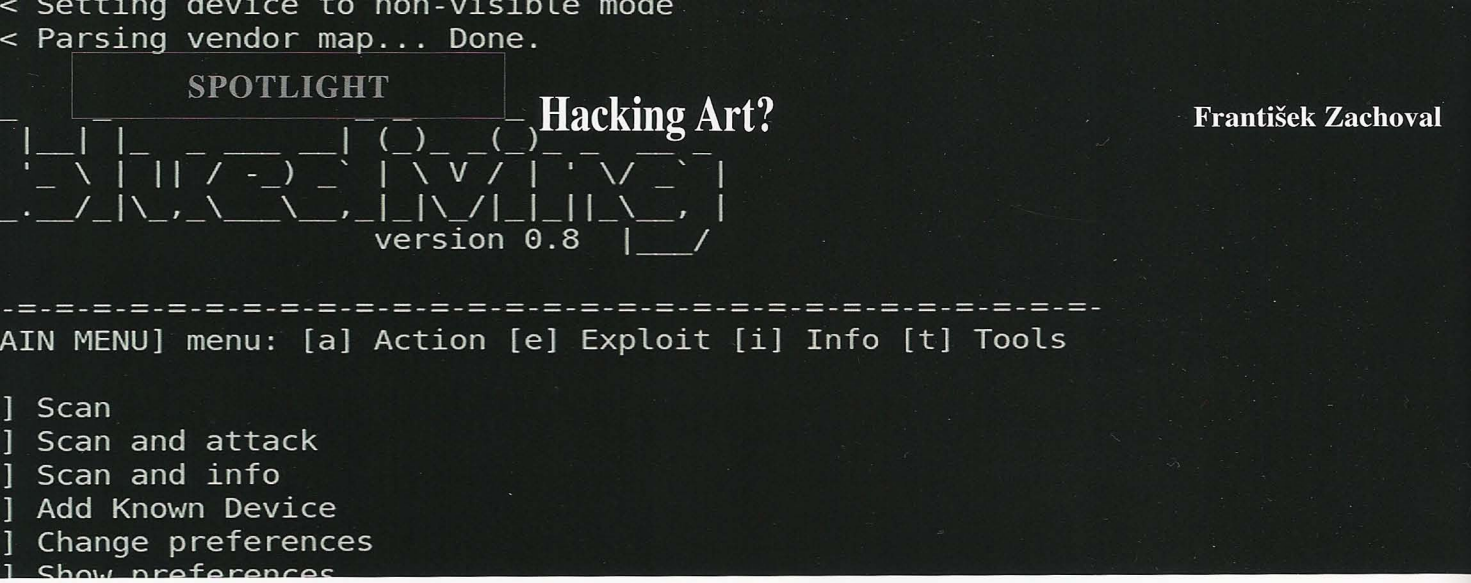

SPOTLIGHT

Hacking Art?

František Zachoval

První domácí hackerské skupiny začaly vznikat těsně po rozpadu republiky, když skupina SERT[1] jánošíkovským způsobem mazala pravidelně warez[2] na českých a slovenských univerzitách.[3] Po jejím rozpadu část členů přešla pod značku CzERT,[4] která je spojována hlavně s rokem 1997, kdy proběhly její mediálně kontroverzní akce, a od té doby jsou hackerské výstupy vnímány velice negativně. Téhož roku se zformovala volná skupina lidí okolo informačního portálu *hysteria.sk*[5] a té se částečně podařilo zvrátit naakumulovanou antipatii, zejména vydáváním on-line magazínu *prielom* a chytrou koexistencí s komunitním portálem *kyberia.sk*, kde logicky samotní uživatelé svou přítomností legitimizují projekty a činnost *hysterie*.

ČÍM VÍC TOHO DOKÁŽEŠ, TÍM MÉNĚ ZNEUŽÍVÁŠ

Petr koexistuje v prostoru *hysteria*, je přispěvatelem ezinu *prielom* a současně studuje informatiku MFF UK v Praze. „Čím víc rozumíš kódu a mechanizmům společnosti, tím míň toho zneužíváš", přibližuje mi svůj postoj, zatímco scanuje všechny bluetooth zařízení v jedné zapadlé kavárně pomocí aplikace, na jejímž vývoji se podílel. Svým přístupem jen potvrzuje to, že nepatří k zákeřným zlodějům a škůdcům, ale do skupiny hackerů softwarové bezpečnosti a síťových spojení, tedy do komunity, která určuje aktuální respektovanou bezpečnost konkrétních projektů. Tito hackeři obvykle působí jako penetrační testeři u velkých firem. Při své práci se často pohybují na hraně zákona. Neprovokují lacině okolí nabourávání se do html stránek, žijí v anonymitě. Když jsme pozdě k večeru vyměnili kavárnu za vernisáž v MeetFactory, tak se Petr podivoval nad nesrozumitelností vystavených děl.
Začal jako všichni v komunitě zkoušením věcí, ke kterým našel návody, ale záhy se vydal cestou experimentování, kde již žádné texty, publikace a postupy neexistovaly. Podílí se na vývoji *Bluedivingu*[6] a *CAPTCHA*[7] technologií, na nichž s kolegou testují systém založený na neuronových sítích, který tuto ochranu obchází. Vyvíjí vlastní keyloggery – zařízení, která zaznamenávají stisky jednotlivých kláves a absurdně se dostal až k lock pickingu, což je otvírání zámků pomocí planžet.

MOBILNÍ ČIP

Motivace jeho účasti na projektu *Bluedivingu* souvisí s novou technologií bluetooth. „*Bluediving* je můj další smysl, senzor. S ním vidíš svět pestřeji." V duchu přemítám, jestli Petr není deviant, který si kompenzuje hodiny kódování snahou dozvědět se víc než ostatní. „Projdeš-li se Prahou, potkáš tisícovku mobilních čipů, které na tebe vysílají. Usmívám se na Lenku, Marušku, Pavla... Zhruba nad jedním procentem mám absolutní kontrolu. Na dálku držím jejich mobil v ruce a zkoumám, co je zač. Poodejdu-li na víc než dvacet metrů, ztrácím spojení. K samotnému scanneru aktivuji čtecí zařízení, které reprodukuje vyskakující informace z konzole programu a signál je poslán do sluchátek. A ještě k tomu se před měsícem objevil na trhu mobil, jehož základ je v otevřeném systému, kam mohu migrovat celou aplikaci, a notebook v batohu je historií."
Bluediving je prezentován jako nástroj na doladění bezpečnosti bluetooth zařízení, a právě toto tvrzení je diskutabilní. Středně zdatný uživatel operačního systému linux si stáhne připravené balíčky na svůj notebook, dle potřeby je zkompiluje a scanování za jakýmkoli účelem může začít. Všeobecně je známo, že v úplných začátcích bylo bluetooth zařízení abnormálně děravé. Majetnější uživatelé jako manageři a politici byli pak prvními, kteří nevědomě sdíleli své intimní informace.
Petr dál říká, že ze získaných dat lze vizualizovat malou komunikační architekturu: „Společnost je organizmus, který má nějaké vazby, a ty lze sledovat." Nakonec jednoduše poznamená, že zveřejnění je z právního hlediska problematické.

HACKING ART?

S nástupem e-mailové komunikace všichni stále více uploadujeme vlastní život na nějaké servery, zároveň bojujeme proti implantátům, které si vlastně dobrovolně kupujeme v podobě mobilů, a ještě si platíme jejich provoz. *Hacking Art* není novotvarem - v různých souvislostech se objevuje v posledních letech, třeba jako ve výstavě *Open_Source_Art_Hack* v roce 2002 v New Museum v New Yorku, kde kurátor výstavy Steve Dietz poznamenává: „Jsme vystaveni neustálému dozoru ze strany státu a jeho bezpečnostních složek. Na tuto problematiku a hrozící nebezpečí mohou adekvátním způsobem reagovat pouze hackerské komunity."
Záleží také na tom, jakým způsobem se definuje samotná osobní filozofie hackera a jaké důsledky mají jeho činy. Obecně platí, že dopady aktivit většiny spektra aktérů mají plošný charakter – vytvářejí společné duševní vlastnictví: jsou sice vázány na konkrétní místa a události, ale mají globální následky. Pokládají si konkrétní otázky a navrhují konkrétní řešení slabin a dilemat digitálního světa, proto se s jakýmkoliv uměleckým provozem nekonfrontuje žádný z těch, kteří v této oblasti pracují. Je také důležité nepominout široce vzrůstající zájem o filozofii Open source software, která ve spojení s hackerským aktivismem představuje důležitou polohu institucionální kritiky. Tu lze samozřejmě dále modifikovat akademickým způsobem, jak to dělají umělecké skupiny Rafani, Pode Bal, Guma Guar..., ale také kontroverzní formou, jakou používají lidé okolo volného sdružení *hysteria.sk*.

František Zachoval je specialista na nová média, pracuje v Digilabu na AVU v Praze.

1. SERT / Sirup Emergency Response Team, SERT volné sdružení hackerů Komenského university v Bratislavě. Většinou se zaměřoval na boj s nelegálním softwarem warez. Skupina se rozpadla zásahem vedení university, z níž hackeři útočili. Tři studenti byli vyloučeni. prielom #2, 26.2.98, http://hysteria.sk/prielom/
2. Termín počítačového slangu označující autorská díla, se kterými je nakládáno v rozporu s autorským právem. http://cs.wikipedia.org/wiki/Warez
3. Nejznámější školní warez server se byl „kmotr.zf.jcu.cz" na Jihočeské univerzitě v Českých Budějovicích
4. Czech Emergency Response Team, společná značka zhruba deseti hackerů.
5. Zkušenosti zakládajících členů z praktik českých a slovenských providerů a freemailových služeb vedly k zakoupení vlastního serveru, který hlavně sloužil jako dočasná autonomní zóna, kde měli uživatelé své soukromí pod vlastní kontrolou.
6. Bluediving je napsán v programovacím jazyce C a Perl, licencován pod GPL a je ovládán přes terminál. Celý projekt byl odstartován v roce 2004 Bastianem Ballmanem. Na vývoji se dále podílel Marcel Holtmann, Martin Herford a Collin Mulliner z trifinite.group, dále Pierre Betouin, Ollie Whitehouse, Martin Karger, John Cartwright, ^_^ a Petr.
7. CAPTCHA je Turingův test, který se na webu používá ve snaze automaticky odlišit skutečné uživatele od robotů. cs.wikipedia.org/wiki/CAPTCHA

Nahoře: menu Bluedivingu.