# The Economics of Online Crime

Jakub Mareček

PV177 - Laboratoř pokročilých síťových technologií

4. května 2010

Původní text: Tyler Moore, Richard Clayton, Ross Anderson

# Dřívější přístup k hackingu

- amatérští hackeři
- spíš šlo o vychloubání se kdo bude lepší a první
- podvody s platebními kartami a účty byly individuální:
  - pracoval v obchodě, sestrojil čtečku a po nocích vybíral peníze z bankomatů
  - zaměstnanec call centra banky zneužíval hesla k účtům, které mu sdělili klienti

# Současná situace

- organizovanost
- díky internetu nemusí přijít zloději do styku s obětí
- obchodování se získanými údaji na černém trhu
- různé údaje mají různou cenu:
  - platební karta s PIN - $0,40 - $20 za údaj
  - přístupové údaje k bankovnímu účtu - $10 - $15 za kus
  - osobní údaje k získání úvěru - $1 - $15 za osobu
- lidé, kteří tyto údaje kradou je prodávají lidem, kteří teprve údaje zneužijí

# Převod ukradených peněz

- zloději peníze nekradou přímo :-)
- najímáni takzvaní "mezci na peníze"
  - přijímají peníze a přeposílají je dále
  - nabídky této "práce" se šíří pomocí spamu a lákají na práci z domu jako "sales executive" (vedoucí prodeje) či jako "transaction processor" (správce transakcí)
  - "zaměstnanci" si myslí, že jim chodí peníze za zboží a přerozdělují peníze, většinou je posílají pomocí služby Western Union
  - ve chvíli, kdy prostředník odešle peníze a je zjištěn podvod, má plnou zodpovědnost za peníze, které mu došly a má problém on, ne zloděj
- praní na online pokerových a aukčních serverech

# Sběr hesel a osobních údajů

- je organizovaný a velmi specializovaný
- vytvořena kopie pravé stránky banky, pomocí které jsou osobní údaje získány
- pomocí spamu rozesílány emaily, vypadající jakoby je poslala banka
- součástí emailů či podvržených stránek bývá i škodlivý software neboli *malware*
  - většinou funguje tiše a sbírá osobní data a bankovní hesla
  - často sdružuje počítače do tzv. *botnet* sítí
  - dříve psáván jednotlivci
  - dnes jej vyvíjejí specializované firmy, které poskytují aktualizace a záruku, že program nebude odhalen antivirem :-)
  - odhalena pouze malá část malware
  - nakažených počítačů - trvale kolem 5%, (10 000 000)

# Botnet sítě

- s rozmachem vznikla nová zaměstnanecká pozice - "botnet herder" (pasák botnetu)
  - spravuje počítače nakažené nějakým malware, které mohou být dálkově řízené a fungovat jako roboti
  - tyto sítě pronajímány pro rozesílání spamu a phishingové stránky
  - valná většina spamu je rozesílána přes botnety
  - sítě najímány na DNS útoky (mnoho počítačů k dispozici najednou)
- různé další zneužití internetu k podvodům a zločinu
  - neexistující loterie a charity
  - šíření dětského porna

# Přirovnání k běžnému zločinu

- ekonomické dopady online kriminality jsou velice podobné s dopady běžné kriminality
- analogie s dobou, kdy pachatelé začali používat auta
- rozdíly však mezi pachateli
  - běžné zločiny
    - okraj společnosti
    - opakovaně trestaní zločinci
    - závislost na alkoholu či drogách
  - online zločiny
    - schopní a vzdělaní lidé
    - často špatná možnost zaměstnání
    - špatná legislativa

# Problémy propojení s ekonomikou

- obtížné vyjádření ztrát a napojení na ekonomiku jednotlivých států
- různé organizace mají tendence nadhodnocovat či podhodnocovat
  - PhisTank zveřejnila informace o obrovském počtu phishing webů
    - způsobeno duplicitními servery se stejnou stránkou
  - APACS (britská bankovní asociace) poskytuje další příklad
    - nárůst phishingu o 726 % mezi lety 2005 a 2006
    - ale pouze 44% nárůst ztrát za stejné období
  - ISP zveřejňují záměrně nižší čísla
    - co nejmenší nebezpečný provoz od zákazníků
    - zachování dobrých vztahů mezi ISP (odpojení, sankce, ..)

# Zlehčování údajů bankami

- Britská vláda zavedla opatření, díky kterému jsou statistiky podvodů téměř nulové
  - podvod musí být nahlášen bance, policii už ne
  - velmi kritizováno britskou parlamentní komisí
- banky nezveřejňují ztráty z podvodů
- pouze Banque de France a APACS zveřejňují společně roční ztráty bank ve Francii a UK způsobené finančními podvody
- ostatní banky si vedou tyto údaje interně, nesdílí
- doporučeno národní sdílení těchto údajů všemi bankami

# Hlášení úniku dat

- 2002 - v Kalifornii přijat zákon o povinnosti hlásit úniky osobních dat
  - firmy i osoby, které spravují obchodně osobní informace musí jejich únik nahlásit
  - osobám má dát možnost lepšího zabezpečení jejich dat u obchodníků (45 milionů ukradených čísel platebních karet, ..)
  - motivace firem uchovávat data bezpečně
  - malý, ale důležitý pokles zločinů a úniků dat
  - podobný zákon přijat ve 34 členských státech, ovšem velmi se liší
- snížení podvodů s ukradenými osobními daty - sdílení dat a standardizace procesu

# Infiltrace spamu

- snaha prozkoumat principy fungování online zločinů přímo
- od roku 2006 některé skupiny monitorují kanály, na kterých podvodníci komunikují
- v roce 2008 infiltrován velký botnet rozesílající spam
- získána odpověď na důležitou otázku: **Kolik lidí reaguje na spam?**

# Infiltrace spamu

- snaha prozkoumat principy fungování online zločinů přímo
- od roku 2006 některé skupiny monitorují kanály, na kterých podvodníci komunikují
- v roce 2008 infiltrován velký botnet rozesílající spam
- získána odpověď na důležitou otázku: **Kolik lidí reaguje na spam?**
  - 28 dokončených prodejů léčiv prezentovaných ve spamu

# Infiltrace spamu

- snaha prozkoumat principy fungování online zločinů přímo
- od roku 2006 některé skupiny monitorují kanály, na kterých podvodníci komunikují
- v roce 2008 infiltrován velký botnet rozesílající spam
- získána odpověď na důležitou otázku: **Kolik lidí reaguje na spam?**
  - 28 dokončených prodejů léčiv prezentovaných ve spamu
  - spamů bylo 350 000 000 (conversion rate 0,00001 %)

# Legislativní problém infiltrace

- toto zjištění bylo velice přínosné
- ve většině zemí však mimo zákon, vykonávat smí pouze soudní orgán
  - často nedostatečné technické znalosti či vybavení
  - často ani nemají snahu něco vyšetřovat
- zákony spousty zemí od těchto výzkumů spíše odrazují
- žádná konkrétní čísla = žádná motivace vytvářet bezpečnější software
- zákazníci také odmítají platit více za kvalitu, kterou nemohou změřit

# Zodpovědnost a detekce

- umožnění připojení infikovaného počítače k Internetu - čí je to zodpovědnost?
  - uživatel, ISP, výrobce software, zákony
  - každý z nich chce aby zodpovědnost byla na někom jiném
  - nutnost řešit problém bezpečnosti komplexně
- ISP mají velmi dobrou možnost odhalení infikovaných počítačů
  - naopak zákazníci to často dlouho nemusí poznat
  - ISP mají možnost infikovaný počítač odpojit ze sítě
  - nejpoužívanější metoda - uzavřít do karantény, umožnit pouze vyčištění počítače
- u velkých poskytovatelů a firem je problém - moc velké sítě na odpojení

# Odstranění škodlivých webů

- útočníci registrují velké množství domén
  - platby prováděny přes ukradené kreditní karty
  - dříve názvy domén podobné bankám, nyní již rozdílné
  - velcí registrátoři vs. malí registrátoři - nutno aby měli stejné postupy
  - obecně se snižuje čas nutný k odhalení a zastavení domén s phishing weby
- podobná situace i ISP
  - liší se rychlost odpojení škodlivých webů
  - u nejlepších ISP kolem hodiny od nahlášení
  - někteří ISP klidně i několik týdnů
- navrhované řešení
  - sankce pro ISP při neodpojení do cca 3 hodin
  - vzor v letecké dopravě - primárně je zodpovědnost na aerolinkách

# Sdílení bezpečnostních informací

- mnoho bezpečnostních firem nezveřejňuje údaje o odhalených škodlivých webech
- sdílení údajů by však velmi pomohlo
- analogie s 80. a 90. léty minulého století
  - antivirové firmy nesdílely virové databáze
  - soutěžily o prvenství v počtu odhalených virů
  - od roku 1993 sdílí virové databáze
  - velký nárůst kvality zabezpečení
- anti-phishing společnosti toto nedělají
  - v roce 2008 analyzovány data z různých firem
  - o většině škodlivých webů věděla jiná organizace výrazně dříve než jiná
  - rozdíly v rychlosti odpojení v řádu desítek hodin (17 vs. 112)

# Výhody sdílení

- finanční - sdílení by mohlo ušetřit až $380 milionů ročně!
- eliminovalo by se soutěžení o co nejrozsáhlejší databázi
- snazší vstup na trh pro nové firmy
- firmy chtějí soutěžit - stále by mohly
  - v rychlosti odstranění, ceně, nástroje, technologie
  - banky by dostaly kvalitnější služby
- celkově sdílení přinese výhody jak uživatelům, bankám, tak bezpečnostním firmám

# Iniciativa a rychlost odpojení

- různé druhy *špatného* obsahu jsou odpojeny za různou dobu
- doba závisí na tom, kdo má iniciativu jej odstranit
  - phishingové weby jsou odstraněny nejrychleji - motivace bank
  - naproti tomu, online prodej léčiv nikdo neodstraňuje - nikoho nepoškozují
- banky však trápí pouze obsah, který je poškozuje přímo
  - banky neřeší *mule recruitment*
  - banky o peníze nepřijdou, přijde o ně klient a prostředník
  - nedá se zjistit, peníze které banky přes prostředníka potečou
  - phishing weby odstraněny mezi 4 až 96 hodinami
  - *mule recruitment* weby průměrně po 308 hodinách
  - v roce 2008 největší nárůst spamu - pravě *mule recruitment*

# Vliv technologií na rychlost odstranění

- technologie používané útočníky ovlivňují také rychlost odstranění
- nezkušení či *hloupí* útočníci hostují škodlivý obsah na:
  - free hosting
  - jednotlivé napadené webové servery
- je snadné je najít a odpojit
- profesionálové však využívají tzv. *fast-flux*
  - hůře vystopovatelné
  - web je dynamicky hostován na botnet síti
  - každých pár minut se přesouvá na další počítač
  - odstranění phishing webu - 100 hodin
  - odstranění léčiv - pokud vůbec - přes 2000 hodin

# Koordinace postupu

- na světě tisíce soudních orgánů
- mnohé z nich neinformovány o počítačové kriminalitě
- liší se stát od státu co je nelegální
- globální právní rámec přijat v USA, ale zatím ne ve většině zemí EU
- i po určení co je zločin stále málo pro společný postup policie
  - například z Ruska odejdou miliony spamů
  - pár desítek tisíc dorazí do Londýna
  - London's Metropolitan Police řekne FBI ať se tím zabývá a dál to neřeší
- policie je uzpůsobena k řešení velkých zločinů a vražd na jejich území
- neexistuje aparát, který by se zabýval tisíci malými zločiny

# Globální a lokální postup

- nejsledovanější online zločin je zobrazování dětské pornografie
- paradoxně nejpomalejší odstranění těchto webů
  - průměrně odstraněny po 719 hodinách
  - to je 150x více než phishing a 2x víc než *mule recruitment* !!
- v 90. letech dětská pornografie stanovena jako *zlo*, které by všechny země měly zakázat a stíhat
- ve 29 zemích existují linky pro nahlášení
- v Británii je dětská pornografie odstraněna do 48 hodin
- v Británii hostováno pouze 0,2 % těchto webů
- při nahlášení webů v jiných zemích, IWF tyto státy informuje, dál žádná akce

# Globální a lokální postup 2

- efektivnost a postup agentur po nahlášení se liší
- jen velice málo efektivních jako britská
- americká obdoba také reagovala rychle
  - mohla nařídit odpojení ale jen některým ISP
  - v listopadu 2008 zákon, že může zasáhnout do všech ISP
- další problém je legislativní
  - národní agentura $\rightarrow$ lokální soud $\rightarrow$ policie $\rightarrow$ ISP
  - velice pomalé a finančně náročné
  - řeší se jen to nejnutnější
- další problém - pouze policie může pátrat po dětské pornografii
  - soukromá firma či osoba, která stáhne fotky či udělá screenshot tímto porušuje zákon
  - existuje nepsaný předpis, že nebudou postihovány
  - což ale odrazuje od pátrání a hlášení

# Shrnutí

- od roku 2004 je online kriminalita organizovaná jako žádný jiný zločin (s možnou výjimkou obchodu s drogami)
- většina zločinů existuje v zákonech, ale je obtížné je postihovat kvůli globálnímu charakteru internetu
- online kriminalitu nejde zastavit úplně, způsobuje ztráty bankám, ISP a i běžným lidem
- zločin páchaný pomocí technologií se hodně vyvinul a změnil
- banky by se měly více zaměřit na praní peněz - globálně
- banky a bezpečnostní agentury by měly sdílet informace
- klíčem k ovládnutí online zločinu je jeho porozumění!

# Konec

- Díky za pozornost!

# Konec

- Díky za pozornost!
- Dotazy? Možná budou i odpovědi! :-)