INTERNETOVÉ MAFII NA STOPĚ

Organizovaný zločin vstoupil do 21. století. Chip špicloval v mafiánských kruzích a odkrývá zločinecké metody. *Max Mustermann*

Octli jsme se uprostřed hackerského fóra Zloy. Zde se soustřeďuje ruská ilegalita – internetová mafie. Chvilku nám trvalo, než jsme se zorientovali, ale pak jsme našli, co jsme hledali: mezi azbukou jsme našli screenshoty, ceníky a ICQ kontakty. Tento on-line černý trh nabízí vše, co neseženete na eBay: trojské koně, boty, data účtů, čísla kreditních karet a samozřejmě hesla.

ILEGÁLNÍ NABÍDKY: Na některých fórech lze koupit cokoliv. Právě zde prodávají hackeři ukradené kreditní karty...

Infiltrace

Několik týdnů jsme pozorně sledovali část ruské internetové mafie, pozorovali jsme, jak obchod probíhá a jak jsou noví škůdci vytvářeni. Zvenčí zcela izolovaná a nedostupná scéna. Ale jakmile se našemu tajnému týmu podařilo do ní infiltrovat, vše už bylo jen pouhou dětskou hrou. Tento organizovaný zločin nabízí své služby zcela neskrývaně a otevřeně. Neobává se žádné vlády ani bezpečnostních společností. A ani nemusí. Tato scéna dokonce dokáže jednoduše skrýt případné neúspěchy, jako např. ten, který je datován k 11. září 2007, kdy německá „Public Prosecution Service“ zaznamenala největší úspěchy v boji proti mezinárodně organizovanému phishingovému gangu. Vyšetřování se táhlo osmnáct měsíců. Vyšetřovatelé sledovali tok peněz a pozorovali obžalované a nakonec bylo v Německu zadrženo osm osob (dvě ženy a šest mužů z Německa, Ukrajiny a Ruské federace), považovaných za hlavní aktéry stojící za nesčetnými phishingovými útoky. Pomocí padělaných e-mailů z Deutsche Telekom, eBay a dalších společností chytali tito lidé své oběti a způsobili škody v hodnotě několika desítek tisíců eur.

Tento zatím největší úspěch zmiňované organizace je pro internetovou mafii pouhým štípnutím. Jen o deset dní později totiž začala německé uživatele internetu zaplavovat další phishingová vlna. Trhlina, kterou dopadení gangu vytvořilo, byla ihned utěsněna: falešné maily zaplavily inboxy klientů bank.

ÚTOKY NA INTERNETU

Mafie se nebojí ničeho – ani na internetu. Útoky jsou nyní mnohem méně časté, zato podstatně více nebezpečné.

DDOS: Distributed Denial of Service

Samostatný počítač sotva udělá nějakou škodu. V sítích botů však internetová mafie kontroluje tisíce počítačů, které už leccos zvládnou. Stačí jeden příkaz, a vybraným obětem se začnou odesílat „žádosti". Ve finále je vytvořen takový objem žádostí, které příjemce nemůže zvládnout. Pokud je útok zaměřen na kořenový DNS server, zodpovědný za směrování IP adres po internetu, bývá dosahováno zátěže až 900 Mb/s.

Estonsko: 27. 4. 2007

Čtrnáctidenní „bombardování" Estonska.

Izrael: 17.5. 2006

Agresivní útok spammerů na společnost Blue Security.

USA: 21. 10. 2002

Útoky paralyzovaly kořenový DNS server. Pravděpodobně šlo o „test".

Irsko: 18. 1. 2002

Poskytovatel „Cloud Nine" ukončil činnost. Důvod nebyl nikdy zveřejněn.

Obchod na netu: jak podsvětí komunikuje?

Začali jsme špehovat v nejtemnějších koutech internetu, kde organizovaný zločin zpečeťuje své obchody. Pátrání po těch, kteří stojí v pozadí tohoto byznysu za miliardy, začíná na neškodně vypadajícím fóru. A to proto, že první „nástěnky" internetové mafie se nacházejí na volně dostupných webových stránkách, zvláště fórech. Tyto první adresy musí být známy, a teprve na nich se najdou „odkazy" na všechny ostatní. Celkem brzy tak zvídavý člověk narazí na stránky typu Cardez-Biz, Anti-Chat a Zloy. Zde se setkávají IT profesionálové patřící té„druhé straně", vyměňují si informace o bezpečnostních mezerách a nabízejí své produkty. Pár dnů sledujeme tato fóra bez jakýchkoliv výsledků, pak se ale konečně začíná něco dít. Jedno fórum přestane být dostupné, ale na dalších místech se objeví dvě nová – tajný tým Chipu musí být neustále ve střehu a snažit se neztratit stopu.

Brzy je to jasné: nezáleží na tom, kde právě jste – všude narazíte na stejná jména. Například na Infected Team, který nabízí svou síť botů pro spam a pro útoky. Je tak úspěšný, že má dokonce i své vlastní stránky. Ostatní se spokojí s příspěvky na fóru, stokrát opakovanými prostřednictvím Copy & Paste. Např. hacker Morozov, který nabízí nástroj Power Grabber na tvorbu trojských koní, svého škůdce specializovaného pro on-line bankovnictví propaguje pomocí screenshotu a krátkého popisu – a má kontakt na ICQ. Kdokoliv chce uzavřít obchod, získá veškeré detaily při virtuálním chatu.

Anonymní ICQ

Na této scéně je chatování velice populární – zvláště přes ICQ. ICQ protokol totiž umožňuje routing i přes proxy servery, což vám zaručí anonymitu. Tento fakt umožňuje rozkvět dvou nových obchodních odvětví. Návštěvníci fóra Nomerkov se specializovali

Nabízím nejlepší kousky. Za 300 dolarů jde o výhodnou nabídku...

Shaltan, dealer trojských koní

na získávání co nejkratších a lákavých ICQ čísel, protože stejně jako telefonní čísla i zde platí, že ICQ adresa se snadno zapamatuje. A tak hackeři jako „Komarik a Krokus" se snaží dostat se k heslům takovýchto ICQ kont pomocí nástrojů typu Malefic Brute. Za cenu od 7 do 70 dolarů za každý úspěšný hack je to skutečně velice výnosný obchod.

Nicméně i hackeři mají výlohy související s nebezpečím, protože jsou závislí na operátorech sítí botů a na zombie počítačů. Pro snížení rizika odhalení se používají pronajmuté proxy servery. The Fraud Crew např. nabízí balík proxy serverů za paušál 70 dolarů měsíčně. Za tuto cenu má zákazník přístup asi k 700 počítačům. A ICQ hacker to také potřebuje, jelikož stačí několik neúspěšných pokusů nalogovat se ze stejné IP adresy, a máte s ICQ utrum. Se sítí 700 proxy serverů jsou ataky typu Brute-Force snadno rozmístěny na různá konta a IP adresy, a zablokování ze strany ICQ tedy nehrozí…

Udělej si sám: trojský kůň ze stavebnice

Fakt, že se mafie schází na webu a vyměňuje si znalosti, má své opodstatnění. Nejvýznamnější je rozdělení práce. Místo pracného sestavování pracovního týmu a jeho organizace mafiáni preferují →

TAKTO ZÍSKÁVÁ MAFIE VAŠE PENÍZE Z PHISHINGU

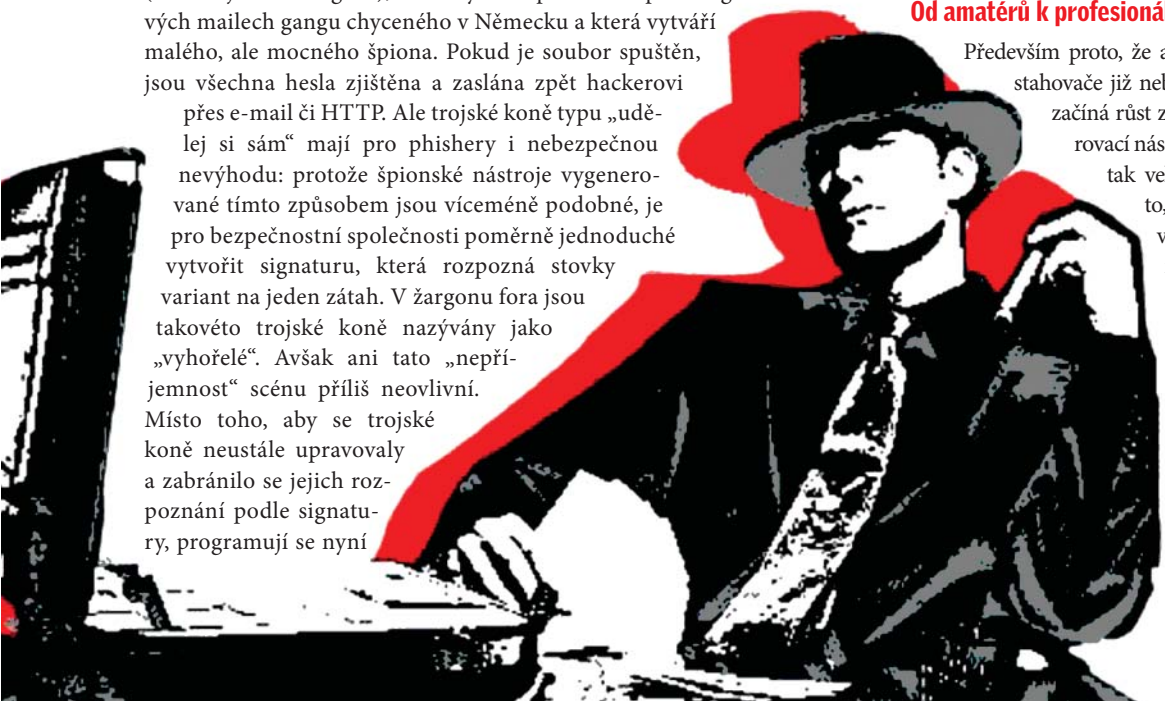
Prvním krokem phishingového gangu je „vyčmuchání" uživatelských dat (souvisejících s přístupem k bankovnímu účtu) a najmutí finančních „loutek". Ti pak přesunou peníze obětí phishingu na určené účty.

Komplicové
Další osoby se podílejí na finančních přesunech – největší částky putují na zahraniční konta. Část z peněz si ponechávají jako provizi.

Praní peněz
Peníze poté putují přes řadu zahraničních bank a internetových platebních systémů, ve finále jsou vyzvedávány v hotovosti.

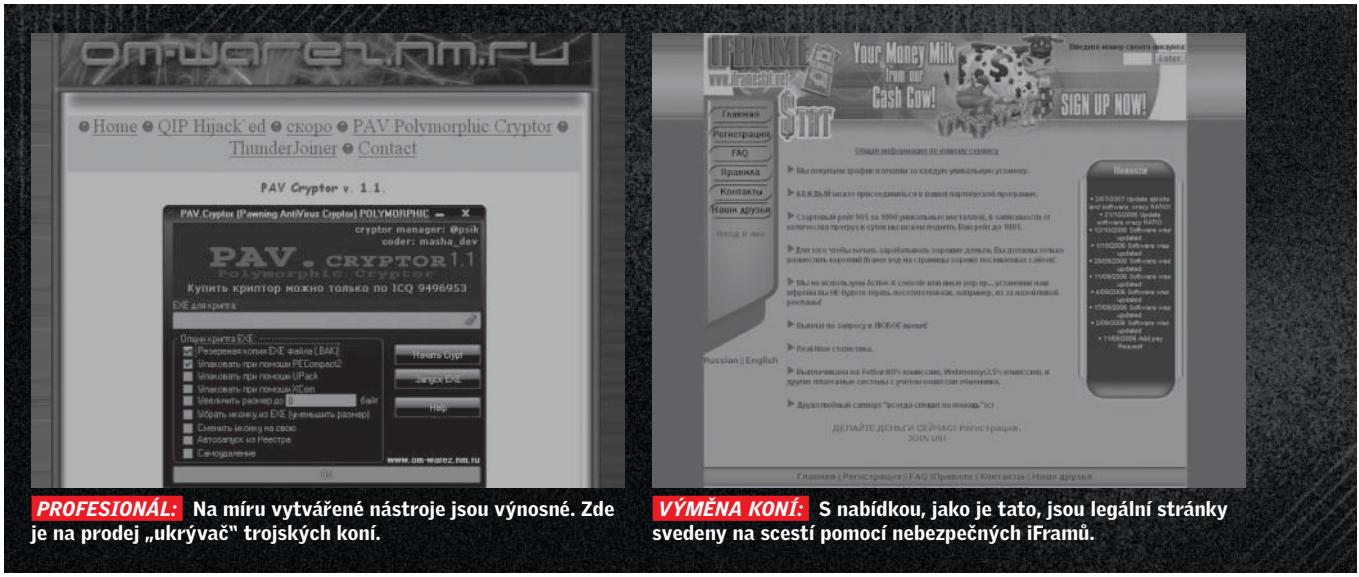
→ dobrovolníky. Na internetu snadno najdou specialisty na každou oblast – např. studenty informatiky. Ti si tak vydělají značně víc při příležitostné práci pro mafii než při jakýchkoliv stážích. Dokonce existují (neověřené) informace, že tito studenti jsou přetahováni přímo z univerzit jako programátoři trojských koní.

Mezitím náš tajný tým zjistil další zajímavou informaci: nejnovějším oblíbencem phisherů je takzvaný Pinch 3, stavebnice (tzv. Trojan-making set), která byla též použita ve phishingových mailech gangu chyceného v Německu a která vytváří malého, ale mocného špiona. Pokud je soubor spuštěn, jsou všechna hesla zjištěna a zaslána zpět hackerovi přes e-mail či HTTP. Ale trojské koně typu „udělej si sám" mají pro phishery i nebezpečnou nevýhodu: protože špionské nástroje vygenerované tímto způsobem jsou víceméně podobné, je pro bezpečnostní společnosti poměrně jednoduché vytvořit signaturu, která rozpozná stovky variant na jeden zátah. V žargonu fora jsou takovéto trojské koně nazývány jako „vyhořelé". Avšak ani tato „nepříjemnost" scénu příliš neovlivní. Místo toho, aby se trojské koně neustále upravovaly a zabránilo se jejich rozpoznání podle signatury, programují se nyní především stahovače (označované jako downloaders či droppers). Jedná se o skromné programy, jejichž hlavní prací je stáhnout aktuální malware.V současné době nejmenší varianta má pouze 474 bytů – to znamená, že je velká asi jako polovina prázdného dokumentu ve Wordu. K tomuto miniprogramu je často přidáno několik funkcí, které deaktivují bezpečnostní software (např. firewall a virové skenery).



Od amatérů k profesionálům

Především proto, že autoři chtějí mít jistotu, že stahovače již nebudou odhaleny, na fórech začíná růst zájem o komprimační a šifrovací nástroje. Hackery nezajímá ani tak velikost malwaru, jako spíše to, že komprimací a zašifrováním souborů se tak změní i jejich signatury. Metoda je natolik úspěšná, že se zdá, že bezpečnostní společnosti jsou nuceny udržovat odstup od metody otisků „Signature" a používat tak nové techniky, např. indentifikaci na základě chování. Pomocí této metody bezpečnostní program →



PROFESIONÁL: Na míru vytvářené nástroje jsou výnosné. Zde je na prodej „ukrývač" trojských koní.

VÝMĚNA KONÍ: S nabídkou, jako je tato, jsou legální stránky svedeny na scestí pomocí nebezpečných iFramů.

→ např. identifikuje stahovač při jeho pokusu deaktivovat firewall (jen o několik sekund později by došlo k nahrání druhého zákeřného programu z internetu). Nástroje, na které náš vyšetřovací tým narazil, mají jedno společné: jsou stále více profesionální. Dokonce i experti zjišťují, že je obtížné rozlišit mezi dobrými a špatnými aplikacemi. Nejjednodušší útočné nástroje jsou ale stále takzvané joiners. To jsou utility, které do neškodných programů – většinou obrázků a zábavního softwaru – zabalí trojské koně. Když uživatel tento „balík" otevře, na svůj počítač ihned obdrží záškodníka.

Máslo, rohlíky a dva trojské koně

Koupit trojského koně není vůbec obtížné, ale jak za tyto nebezpečné nástroje zaplatit? Abychom to zjistili, zkusili jsme uzavřít falešný obchod – pokusili jsme se koupit výše uvedeného trojského koně jménem Power Grabber. Podle popisu může tento software nepozorovaně vyčenichat všechna zajímavá hesla. A jak je to pro tuto scénu obvyklé, prodávajícího jsme našli přes ICQ. Je podezíravý a chce vědět, kde jsme získali adresu. Řekli jsme mu o fóru a vzápětí jsme obdrželi novou ICQ adresu. Tam jsme konečně mohli jít přímo k věci. Tento trojský kůň je už poněkud starší: hacker to ví a my také. Lámanou angličtinou smlouváme o ceně. Tu ovlivňuje i to, že jedinou novou věcí u tohoto trojského koně je změna signatury pomocí šifrovače. Tudíž hacker žádá 300 WBZ (čti dolarů). Zkratka WBZ skrývá e-Payment providera „Web money transfer", který je v podsvětí velice oblíben a který převádí svou měnu jedna ku jedné v dolarech. Náš tým vyšetřovatelů předstírá, že s obchodem souhlasí, a od WebMoney získává číslo bankovního konta. V této chvíli rušíme obchod. Po tom všem už nechceme hackerům házet další peníze. Kdybychom zaplatili a kdyby dealer dodržel slovo, pak bychom trojského koně obdrželi přes ruský download portál – podobný RapidSharu – v zašifrovaném RAR archivu.

KOLIK STOJÍ PHISHING?

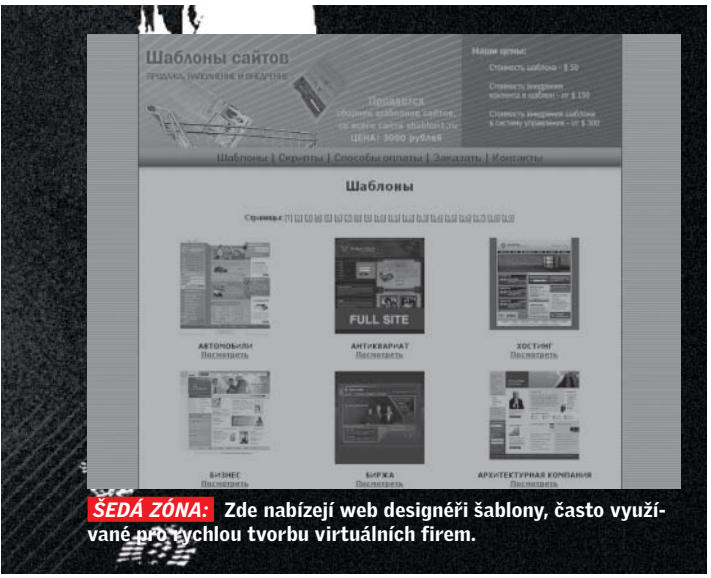
V některých fórech je možné sehnat vše potřebné pro phishingový útok. Například za 250 dolarů lze pořídit kompletní výbavu.

Trojský kůň	100 $
Šifrovač	50 $
Bot	5 $ za každých 100
Proxy server	70 $ za měsíc
ICQ adresa	20 $

Malwarové obchody: hacker zůstává v anonymitě

Bylo by možné najít hackera pomocí čísla jeho konta? Pravděpodobně ne. Konto u WebMoney se na první pohled nezdá tak anonymní. „Ale peníze nikdy nejsou převáděny přímo, místo toho tečou přes mnoho kanálů," vysvětluje bezpečnostní expert Eugene Kaspersky. Načrtává typický postup toku: aby se hackeři vyhnuli přímému spojení se zlomyslným programem, mají prostředníka. Ve spamové zprávě, kterou obdrží téměř každý, je jim přislíbena lukrativní práce na částečný úvazek. Jediným úkolem je zřídit konto a převádět doručené peníze na jiná konta. Za splnění tohoto úkolu prostředník dostane provizi. Běžné je jednociferné procento. Konto, na které jsou peníze převedeny, je vytvořeno hackerem pod falešným jménem v cizí zemi. Svůj zisk si nakonec vybere z automatu.

Téměř stejný manévr se používá při phishingových útocích. Jakmile phisher unikne s daty typu PIN, TAN a s čísly kont, pomocí on-line bankovnictví hned převede peníze na prostředníka. Ty jsou dále poslány dalšímu strawmanovi, či spíše dalším strawmanům. Ti pak znovu převedou peníze na další konta, která patří phisherům.



ŠEDÁ ZÓNA: Zde nabízejí web designéři šablony, často využívané pro rychlou tvorbu virtuálních firem.

Chobotnice

Skutečný rozsah ilegální činnosti je zřejmý, jakmile se nesoustředíte jen na příspěvky ve fórech, ale všímáte si i reklamy a přidružených linků. Jakmile je síť botů jednou vytvořena, může být použita nejenom k útokům na uživatele internetu a na jejich informace. Ve fórech totiž můžete často narazit i na reklamu od tzv. „traffic-dealers". Obvyklé jsou dvě varianty: Jedna nabízí „traffic". Pokud máte pocit, že vaši stránku navštíví málo návštěvníků a že legální optimalizační nástroje nejsou k ničemu, je to možnost pro vás. K dispozici je i mírně upravená varianta pro zlepšení výsledků na Googlu.

Peníze nejsou nikdy převáděny přímo, vždy tečou přes další kanály.

Eugene Kaspersky, Kaspersky Labs

Druhou variantou je nákup „trafficu". Na nesčetných webových stránkách typu iFrame.biz naši tajní surfaři narážejí na reklamy, inzerci phisherů. Nabídka je následující: pokud integrujete očividně neškodný iFrame na své stránky, dostanete za každého návštěvníka zaplaceno. Avšak tento obchod je nebezpečný a ne zas tak výnosný. Za 1000 návštěvníků denně obdrží vlastník stránky pouze 25 amerických centů. Webová stránka na iFrame však většinou obsahuje nebezpečné stahovače a jiný malware. To návštěvníky vaší stránky příliš nepotěší – většina surfařů totiž předpokládá, že nabídka je legální a zcela neškodná. Také někteří „operátoři" pornostránek, ztracení v bezbřehém internetu, se uchylují k mafii a její síti botů. Nabízejí platbu za to, že jejich oběti budou přesměrovány právě na jejich pornostránky. Oběti zamořené boty jsou nuceny zhlédnout pornoreklamy ihned po spuštění browseru nebo kdykoliv během surfování po jakýchkoliv webech. Tato nástraha se mnohým očividně vyplatí.

V mnoha případech tyto temné konexe už nikdy nebudou moci být dokázány. Existuje jen několik stop, které směřují k pochybným či zločineckým webovým stránkám. Navíc mnoho z těchto webových „prezentací" nemá kromě ICQ adresy žádný kontakt a mizerné anglické texty připomínají služby automatických překladů typu Babelfish.

Obžalovaný: kdo se skrývá za obchody

Zdaleka nejzajímavější otázkou je, kdo se za všemi těmito „obchody" na internetu skrývá. Ani sami experti, kteří se tím zabývají již několik let, nemohli našemu týmu poskytnout uspokojivou odpověď. Na výstavě o bezpečnosti nám jeden hacker řekl, že podezřívá klasickou ruskou mafii z toho, že si i zde našla svůj „kousek koláče". Jiní lidé věří konspirační teorii, že za vším jsou bývalí zaměstnanci zrušené sovětské tajné služby KGB. Dokonce ani specializované policejní útvary jednotlivých zemí si nejsou odpovědí příliš jisti. Když jsme několik z nich oslovili, řekli nám: „Opravdu nemůžeme vyvozovat žádné obecné závěry."

Co nás čeká

Posledním hřebíčkem do rakve našich nadějí jsou předpovědi na příští rok. Naše loňská předpověď se do posledního puntíku vyplnila: *„Počítačový zločin přerůstá v organizovaný zločin, v němž už není místo pro jednotlivé útočníky," řekl Jamz Yaneza, výzkumný analytik zabývající se hrozbami. „Náš výzkum ukázal, jak se hrozby postupně mění z rychlých a rozsáhlých epidemií na propracované útoky zasahující velmi specifické skupiny uživatelů.*

O to nepříjemnější jsou i naše předpovědi na příští rok:

★ Počet internetových hrozeb se v průměru zvýší o více než 100 procent.

★ Výrazně vzroste i počet botů. Odhadujeme průměrný měsíční nárůst 10 procent, což každý měsíc představuje přibližně 100 tisíc nových obětí.

★ Zcela zmizí „obyčejné viry", které jen škodí a svým tvůrcům nic nepřináší.

★ Zvýší se útoky na Windows Vista, která prozatím zůstávala ve stínu pozornosti mafie. ▬