Česká policie používá malware

Co ukazuje případ Hacking Team

Italská firma Hacking Team se nechává najímat na „špinavou práci“ – hackování počítačů, telefonů, odposlechy, kradení hesel. Začátkem července však někdo hacknul její servery a data zveřejnil. Svět je rozhořčen, že firma pracovala i pro autoritářské režimy. Pro nás je zajímavé, že jedním z klientů je i česká policie.

HONZA ŠÍPEK

Hacking Team je IT firma jako spousta jiných. Má portfolio produktů, linku uživatelské podpory, cenovou politiku, obchodní zástupce. To, co prodává, ji ovšem zařadilo na Seznam nepřátel internetu od mezinárodní neziskovky Reportéři bez hranic. Hlavním produktem firmy je trojský kůň RCS (Remote Control System). Když jím infikujete počítač, program neviditelně běží a sbírá data – zadávaná hesla, seznamy otevřených webových stránek, snímky obrazovky, soubory z disku. Pokud je počítač vybaven mikrofonem, umí nahrávat zvuk, pokud má kameru, natáčí obraz a pořizuje fotografie. Umí zaznamenávat hovory skrze Skype a soukromá data zachytává ještě předtím, než je zašifrujeme a vyšleme do sítě. Může s počítačem dělat skoro cokoliv – nahrát na něj soubor, nainstalovat jiný program nebo sám sebe smazat.

Ještě děsivější je varianta pro mobily, jež se nabízí ve variantách pro iPhone, Android či Symbian. Trojský kůň umí nahrávat zvuk v okolí telefonu, hovory, zaznamenávat SMS, pořizovat fotky, natáčet video, hlásit polohu. Je možné ho naprogramovat jen na určitý čas a místo, umí šetřit baterií a místem na kartě. Nainstaluje se pomocí skryté či konfigurační SMS či krátkým připojením USB kabelu. Data se v obou variantách posílají „domů“, na řídicí server umístěný u zákazníka.

Způsoby infekce

E-maily, které zveřejnil server Wikileaks, poskytují fascinující vhled do „uživatelské podpory“ hackovací služby – uživatelé softwaru žádají o radu, ale také například chtějí vytvořit malware přímo na míru. Mezi zákazníky patří i česká policie a armáda, které zastupuje firma Bull, dodavatel proslulého „systému pro monitoring internetu“. Richard Hiller z Útvaru zvláštních činností české policie objednává například malware upravený pro doménu ParlamentniListy.cz, Seznam.cz, web Komerční banky či prodejce túji. Seznam „zasažených“ adres je mnohastránkový.

Odborný server Lupa.cz vznesl oficiální otázky na Policii ČR, odpovědí však byla jen krátká tisková zpráva o tom, že všechno probíhá v režimu utajení, v souladu se zákonem o veřejných zakázkách, čímž policie spolupráci nepřímo potvrdila. Definitivního potvrzení se pak dostalo parlamentní komisi pro kontrolu odposlechů.

Bývalý Klausův mluvčí Petr Hájek se rozčiluje, že policie hackovala Parlamentní listy, ale to je mylné pochopení techniky útoku. Malware se podle všeho instaloval tak, že si policie nechala vyrobit trojského koně na míru oběti. Kdosi pak dostal odkaz na článek *Protikorupční policie obvinila člena předsednictva ČSSD Duška*, uveřejněný na Parlamentních listech, z e-mailové adresy někoho, komu důvěřoval (odesílatele e-mailu lze podvrhnout velmi snadno). Klikl tedy na odkaz, ten však byl zamaskovaným odkazem jinam a přesměroval uživatele na servery Hacking Teamu, odkud se začal instalovat zlotřilý software, načež byl uživatel rychle přesměrován na původní adresu a pravděpodobně si ničeho nevšiml. Další metodou útoku je skrytí malwaru do přílohy e-mailu, wordovského dokumentu, prezentace PowerPoint nebo souboru PDF (třeba „zadost o rozhovor.zip“). Software se pak instaluje po rozbalení a otevření souboru v Microsoft Office nebo Adobe Acrobat. Tato technika se nazývá „phishing“ a běžně ji používají počítačoví bandité k tomu, aby se dostali k vašemu elektronickému bankovnictví. Weby Komerční banky či Raiffeisenbank na „policejním seznamu“ jsou výmluvné.

Nejzáludnější metodou instalace je pak Network Injection. To se koupí škatule zvaná NIA. Ta se zapojí mezi uživatele a internet. Uživatel surfuje webem a všechna komunikace prochází přes škatuli. Když si stáhne jakýkoli použitelný soubor odkudkoliv, škatule do něj vsune malware. Netřeba ani posílat e-mail, ani na nic klikat. Nejčastěji se využívá zranitelnosti přehrávače Flash. V seznamu webů, které je software schopen nakazit, je YouTube a hromada pornoserverů. „Tak to to porno asi oželím,“ glosuje to jeden z diskutujících na internetu. Česká policie takovou škatuli podle zveřejněných e-mailů získala. „Pošleme vám NIA příští týden,“ píše Massimiliano Luppi v lednu 2013. Pokud se takové zařízení umístí na některou z páteřních linek, může být počet potenciálních cílů skutečně veliký.

Zdá se, že námezdní hackeři se trochu vytahovali. O tom ostatně svědčí i fakt, že se sami nechali hacknout

Policie, Bull a ČVUT

Mezi stovky uživatelů internetu, kteří si data Hacking Teamu stáhli, patří i výzkumníci z pražského hackerspace Brmlab. Ti se pustili do analýzy, jejíž výsledky průběžně zveřejňují. Nejčastěji s Hacking Teamem komunikuje Richard Hiller z Útvaru zvláštních činností Policie ČR a Tomáš Hlavsa ze společnosti Bull. Když něco nefunguje, přibalují do přílohy záznamy o provozu, které mají pomoci odhalit chybu. Z nich se čeští výzkumníci dozvídají seznamy podvržených stránek, telefonní čísla útočníků i obětí. Při hledání jednoho z telefonních čísel na internetu nacházejí diskuse o Land Roverech, inzerát na nákup zbraně či prodej kombajnu. Dlouho si nejsou jistí, zda jde o sledovaného mafiána, nebo policistu. Teprve twitterový profil prozradí policistu Marka Bartoše. Některé z požadavků na uživatelskou podporu jsou úsměvné. Policista si například stěžuje, že ovládací SMS malwaru se oběti zobrazují na displeji telefonu. „Z technického hlediska je ten jejich malware dost bída,“ říká český výzkumník. Zdá se, že námezdní hackeři se trochu vytahovali. O tom ostatně svědčí i fakt, že se sami nechali hacknout.

Pozoruhodná je série e-mailů ze září 2012, v nichž Bull domlouvá s italskou firmou dodání podkladů od „akademického partnera“, s nímž spolupracuje při hledání zranitelností. V srpnu 2013 pak tajemného partnera představuje: má jím být Tomáš Zahradnický, vedoucí Katedry počítačových systémů na Fakultě informačních technologií ČVUT. Ten podle e-mailu vede tým, jenž hledá zranitelnosti softwaru a vyvíjí exploity. Je tedy možné, že veřejná vysoká škola dodávala informace o zranitelnosti softwaru soukromé firmě, která je pak prodávala zpět českému státu? Na mé otázky Zahradnický odpověděl: „Soukromě jsem se společností Hacking Team neměl a nemám nic co do činění. Co se týče vztahu mezi Fakultou informačních technologií a firmou Bull, ten byl smluvní a obsahoval závazek mlčenlivosti. Nemohu ho proto jakkoliv dále komentovat.“ Podle informačního systému vědy a výzkumu zpracoval Zahradnický v roce 2013 pro Bull „Speciální softwarový balíček“ za 50 tisíc korun, který je však předmětem obchodního tajemství. Zmiňuje se zde projekt „Janus“, ke kterému odkazují i uniklé e-maily.

Co řeknou soudci?

Než výzkumníci zanalyzují 400 gigabytů dat, bude to ještě chvíli trvat. Už teď ale analýza vede k závažným otázkám. Jak je možné, že policie spolupracuje na odposleších se soukromou firmou a sdílí s ní citlivé údaje? A jak je možné, že citlivé údaje putují do rukou zahraniční firmy s nepříliš dobrou pověstí? Podle spekulací na internetu mohl malware RCS obsahovat zadní vrátka a mohl tak Hacking Teamu dávat přístup k přístrojům obětí. Navíc byla „služba“ nastavena tak, aby každý jednotlivý požadavek na infekci musel projít italskou firmou. Zařízení na záznam odposlechů se podle všeho instalovalo do vnitřní sítě policie a je možné, že Hacking Team má zadní vrátka i tam. To je závažné bezpečnostní riziko.

A hlavně – je nakažení počítače či telefonu vůbec legální? Policie sice ubezpečuje, že software instaluje pouze na základě povolení soudce a na dobu nejdéle šesti měsíců. Malware však umožňuje nahrát do počítače oběti soubor. Tuto možnost podle všeho měl kromě policie i Hacking Team samotný. Zdrojové kódy softwaru uvádějí jako příklady názvů souboru „childporn.avi“ či „bomb_blueprints.pdf“. Bude tohle vědět soudce? A bude soubor nalezený v zabaveném počítači soudním znalcem považován za soubor nahraný uživatelem malwaru? Další otázkou je, kdo zaručí, že budou zasaženi jen uživatelé, které označil soud. Zejména v situaci, kdy v zadávacích požadavcích Bull požaduje, aby bylo vlastnictví systému utajeno, „dokonce ani soud (soudce) o tom nebude vědět“? Ta část provozních dat, která unikla, prozradila některé oběti. A veřejnost se nyní může ptát třeba majitele Vinotéky u Lípy, zda je proti němu vedeno trestní řízení.

Než se vše objasní, nezbývá nám než se vyvarovat na webu Flash Playeru, používat bezpečnější systém než Windows (Linux není dokonalý, ale je rozhodně bezpečnější) a bezpečnější programy než Microsoft Office a Adobe Acrobat Reader. Být obezřetní při otevírání příloh a odkazů v e-mailu. Na telefonování používat něco, co umí jen telefonovat a esemeskovat, anebo z chytrého telefonu vytahovat baterku. A počkat si, který antivirus jako první začne malware RCS odhalovat. V reklamních dokumentech se Hacking Team chlubí tím, že to žádný neumí.

Autor je dokumentarista.