Hromadná doprava jako oblíbený cíl hackerů

Martin Klubal

V posledním listopadovém týdnu si obyvatelé kalifornského města San Francisco mohli vedle lákavých slev tzv. černého pátku vychutnávat i městskou hromadnou dopravu zadarmo. Důvodem ovšem nebyl zmíněný komerční svátek, nýbrž páteční útok hackerů, který postihl vnitřní síť tamního dopravního podniku. Útočníkům se podařilo infikovat systémy MHD pomocí tzv. ransomwaru, neboli škodlivého softwaru šifrujícího všechna data na lokálních i síťových discích, přičemž za jejich dešifrování útočníci požadovali výkupné. V tomto případě se jednalo o rovných 100 bitcoinů, což v přepočtu z virtuální měny na tu tradiční představuje bezmála dva miliony korun. Správci ovšem na podmínky útočníků nepřistoupili, obnovili zašifrovaná data ze zálohy a na sklonku neděle vrátili síť i preventivně odpojené kiosky do původního stavu. Jak se útočníkům podařilo do sítě nabourat a zda je chyba již opravena, podnik ve svém prohlášení nesdělil.

Ransomware je nejrozšířenějším druhem malwaru posledních let, neboť generuje jejich tvůrcům nemalé zisky. Nemusíte být ani zdatným útočníkem, abyste se stali rentiérem tohoto nekalého byznysu, dnes je totiž možné si ransomware pronajmout na černém trhu i jako službu. Názory na placení, respektive neplacení požadovaného výkupného se liší. Zatímco obecně se uhrazení leckdy nemalé částky nedoporučuje, předpokládá se, že velká část korporací, ale i obyčejných uživatelů, vyjde útočníkům vstříc. Přitom jako efektivní obrana stačí dodržovat základní pravidla bezpečného chování na internetu, pravidelně aktualizovat aplikační vybavení a zálohovat svá data, tedy nic, co by nebylo do nekonečna omílanou mantrou všech bezpečnostních analytiků za poslední dvě dekády. O zveřejnění dešifrovacích nástrojů zdarma ze strany antivirových a jiných bezpečnostních společností pro mnohé varianty ransomwaru ani nemluvě.

Podobné útoky se nevyhýbají ani tuzemským dopravním podnikům. V roce 2013 byla zveřejněna metoda útoku na plzeňský dopravní podnik, při které bylo možné prostřednictvím informačních a dobíjecích kiosků PMDP získat vedle přístupových hesel do databáze a aktualizačního FTP serveru i seznam všech držitelů Plzeňské karty. Ve stejném roce pak bylo prolomeno i šifrování pražské karty OpenCard. Ta je založena na zastaralé technologii Mifare DESFire, kterou lze prolomit v řádu několika hodin. Následně je možné díky znalosti soukromého klíče data upravovat a jezdit městskou hromadnou dopravou, ale i využívat parkovacích míst zdarma. Přesto na tom nejsme ještě tak špatně, jako například v Ruské federaci. Tam je městská hromadná doprava řešena vedle klasických žetonů pomocí nešifrovaných karet Mifare Ultralight, jezdit zdarma tak lze i bez potřeby prolamovat jakékoliv šifrování. Jelikož je ale MHD v Moskvě velmi levná, jedná se ze strany hackerů spíše o projev vzdoru vůči systému než o snahu ušetřit náklady za dopravu.

Útok na dopravní infrastrukturu jsme zaznamenali i letos, kdy neznámí útočníci nabourali nešifrovanou komunikaci mezi úsekovými kamerami na D1 a obecními úřady v Rosicích a Šlapanicích, které následně rozesílaly pokuty. Na vtipně upravených fotografiích se změněnými registračními značkami se tak přestupku dopustil mj. i maskot největšího elektronického obchodu u nás.

Stoupající trend podobných útoků je nekompromisní, budeme se s nimi setkávat stále častěji a ne vždy to pro nás bude znamenat městskou hromadnou dopravu zdarma nebo neprůkazné fotografie z rychlostních kamer. Již dnes jsme svědky úspěšných útoků na železniční přejezdy nebo informační cedule na dálničních tazích, které mohou vést v lepším případě k dopravnímu kolapsu, v horším ke ztrátám na lidských životech. S rozšiřující se sítí pro internet věcí (IoT), ruku v ruce s často fatální absencí jakéhokoliv zabezpečení ze strany výrobců aktivních prvků pro tuto síť, jsou navíc vyhlídky bezpečnostních analytiků v této oblasti spíše pesimistické. ■

Ing. Martin Klubal

Autor článku je Senior IT Security Consultant ve společnosti AEC.