Bezpečnost bankomatů

Bezpečnost bankomatů není příliš medializovaným tématem. Znamená to však, že jsou bankomaty bezpečné? Náš tým expertů má za sebou penetrační testy různých typů bankomatů, takže může tuto problematiku objektivně zhodnotit. Závěry vás možná překvapí.

S bankomatem se v každodenním životě potkává většina z nás. V okamžiku naplnění (tzv. dotace) obsahuje více než jeden milion korun, což z něj činí atraktivní cíl pro kriminální živly a zároveň klade nemalé nároky na bezpečnost. Počet útoků na terminálové služby a bankomaty ve světě stále narůstá. Podle statistik EAST (European Association for Secure Transactions) byl celkový počet fyzických útoků na bankomaty v období 2016 až 2017 zvýšen o 21 %. Útoky využívající malware vzrostly dokonce o 231 %. [1] Bližší údaje jsou uvedeny v tab. 1. Většina laické veřejnosti považuje bankomaty za vysoce zabezpečená zařízení. Jak to tedy s jejich bezpečností v dnešní době je?

Řadu let byly největší hrozbou pro zákazníky a vlastníky bankomatů skimmery – speciální zařízení připojená za účelem krádeže dat z bankovních karet. Útoky se však s postupem času stávaly stále propracovanější. Rok 2014 se nesl ve znamení malwaru s názvem Tyupkin [2], který se stal jedním z prvních známých příkladů malwaru, jehož cílem byly právě

Statistika kriminality – evropské platební terminály/bankomaty						
Útoky na terminály	2013	2014	2015	2016	2017	Δ 2016/17
Celkem hlášených incidentů	21 346	15 702	18 738	23 588	20 971	-11 %
Celková výše škod (v €)	248 mil.	280 mil.	327 mil.	332 mil.	353 mil.	+6 %
Fyzické útoky na bankomaty	2013	2014	2015	2016	2017	Δ 2016/17
Celkem hlášených incidentů	2 102	1 980	2 657	2 974	3 584	+21 %
Celková výše škod (v €)	23 mil.	27 mil.	49 mil.	49 mil.	31 mil.	-37 %
ATM malware a logické útoky	2013	2014	2015	2016	2017	Δ 2016/17
Celkem hlášených incidentů	0	51	15	58	192	+231 %
Celková výše škod (v €)	0	1,2 mil.	0,74 mil.	0,46 mil.	1,52 mil.	+230 %

Tab. 1: Počty útoků na terminálové služby a bankomaty [1]

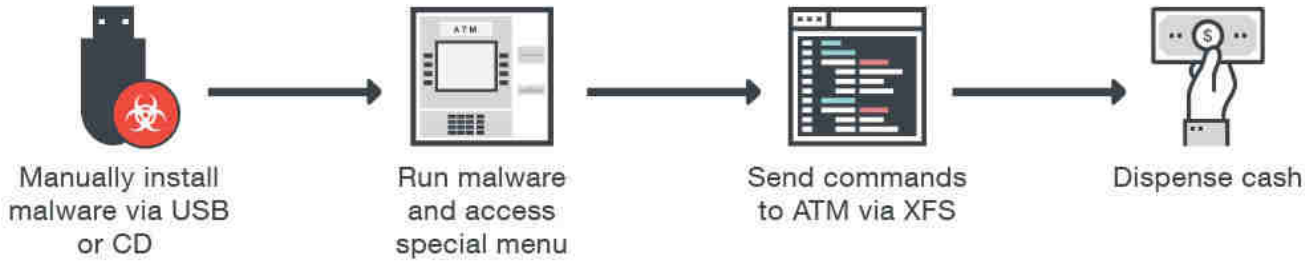
bankomaty. Za vznikem pravděpodobně stála ruská hackerská skupina a dopad byl nejcitelnější právě pro bankomaty ruské federace.

V roce 2015 byl odhalen gang Carbanak [3], který byl schopen provést kompletní vybrání veškeré hotovosti z bankomatů v důsledku kompromitace bankovní infrastruktury a chyb v její implementaci. Oba zmíněné příklady útoků byly možné díky zneužití několika slabých míst v technologii zabezpečení bankomatů a jejich infrastruktuře. Tento typ útoku se stal později známým pod pojmem Money Jackpotting, kdy útočník infikoval bankomat malwarem, který postupně zcela vyprázdnil trezor bankomatu a vydal útočníkovi veškerou hotovost bez jakékoli autentizace.

Tato nová hrozba byla pro banky více než dostatečnou motivací, aby se začaly bezpečností svých bankomatů seriózně zabývat. V průběhu posledních let jsme v AEC spolu s kolegy provedli několik penetračních testů bankomatů pro banky v České i Slovenské republice. Vycházíme tedy z přímé zkušenosti z těchto testů. Jedním z hlavních cílů bylo prověření odolnosti bankomatů vůči výše popsanému útoku Money Jackpotting. Výsledkem bylo zjištění, že ani jeden z testovaných typů bankomatů nebyl proti tomuto útoku odolný.

Na jakém principu to vlastně funguje?

Je nutné si uvědomit, že bankomat není nic jiného než klasický počítač. Co ho však od klasického počítače odlišuje, jsou periferní zařízení (typicky připojená přes USB), kterými bývá např. šifrovaný PIN pad, kamera a hlavně dispenser. Dispenser je část bankomatu, která vám po ověření vydá požadovanou hotovost. Jako každý počítač má i bankomat svůj operační systém. U bankomatu se však nejedná o žádný nadstandardně zabezpečený Linux či speciálně upravenou verzi Windows.



Obr. 1: Postup fyzického útoku malware na ATM [5]

Bankomaty jsou provozovány na klasických desktopových verzích Windows, nikoli však na těch nejnovějších. Výrazná část bankomatů je stále provozována s operačním systémem Windows XP, který byl vydán v roce 2001. Netřeba připomínat, že Microsoft již ukončil veškerou podporu tohoto systému. V dnešní době se tento poměr naštěstí pozvolna mění ve prospěch operačního systému Windows 7, nicméně zastoupení Windows XP je stále výrazné. Použití zastaralých systémů určených spíše pro domácí použití než pro provoz kritických aplikací bezpečnosti bankomatu příliš nepřidává.

Jak tedy na Money Jackpotting?

Pojďme se nyní podívat trochu hlouběji na podstatu útoku. Malware pro bankomaty téměř vždy komunikuje prostřednictvím XFS vrstvy (eXtension for Financial Services). [4] Veřejně dostupný a popsaný standard XFS umožňuje, aby počítač umístěný uvnitř bankomatu komunikoval s bankovní infrastrukturou a hardwarovými jednotkami zpracovávajícími hotovostní a kreditní operace. Zároveň zajišťuje nezávislost na použitém technickém vybavení od různých společností jako Wincor nebo Diebold Nixdorf (čtečka karet, speciální tiskárny, PIN pad, dispenser apod.).

Zásadním problémem je, že XFS v nejrozšířenějších verzích používaných bankomaty v dnešní době nevyžaduje žádné oprávnění/autorizaci pro zpracovávané příkazy. Tedy každá aplikace nainstalovaná nebo spuštěná v bankomatu může vydávat příkazy k libovolným hardwarovým jednotkám bankomatu (rovněž označovaným jako ATM), a to včetně čtečky karet nebo dispečeru (viz obr. 1).

Pokud malware úspěšně infikuje ATM, získává téměř neomezené možnosti ovládání:

- Může přeměnit PIN pad včetně čtečky karet na „nativní“ skimmer a zachytávat údaje o platebních kartách.
- Může dispenseru „poručit“ výdej veškeré hotovosti z trezoru bankomatu.

Právě druhá uvedená možnost je podstatou již zmíněného útoku Money Jackpotting, kdy útočník zcela obejde nutnost vložení karty do bankomatu, autentizaci PINem či ověření zůstatku na účtu. Přímo na nejnižší vrstvě vydá příkaz pro výdej veškeré hotovosti. Tento útok se pravidelně daří realizovat a demonstrovat při námi prováděných penetračních testech.

Fyzická bezpečnost

V řadě známých a zmapovaných případů z nedávné doby zločinci vůbec nemusejí používat malware k infikování bankomatů přes síť banky, do které je bankomat připojen. Za vše může nedostatečné fyzické zabezpečení samotných bankomatů, které útoky výrazně usnadňuje. Bankomaty jsou často umístěny a instalovány tak, že třetí osoba snadno získá fyzický přístup k počítači uvnitř bankomatu nebo k síťovému kabelu, který zařízení připojuje do sítě.

Získáním částečného či úplného fyzického přístupu k bankomatu mohou potenciální útočníci docílit především:

- instalací vlastního hardwarového zařízení uvnitř bankomatu, které umožní útočníkům vzdálený přístup a realizaci zmíněného Money Jackpotting útoku; k tomuto účelu jsou vhodné malé jednodeskové počítače o velikosti platební karty, např. Arduino, Raspberry PI [6],

- přepojením bankomatu na podvrhnuté procesní centrum pod kontrolou útočníka starající se o zpracování příkazů pro jednotlivé hardwarové jednotky s cílem podvrhovat a posílat libovolné příkazy.

Přestože lze teoreticky zajistit ochranu spojení mezi bankomaty a zpracovatelským centrem, opatření jako šifrování SSL/TLS nebývají v praxi často implementována nebo jsou nesprávně nakonfigurována. Mluvíme-li o fyzické bezpečnosti, nelze opominout útoky „hrubou silou“, kdy útočník násilím odcizí celý bankomat či trezor. Obranou proti tomuto útoku bývá použití kapslí s ochranným barvivem, nicméně ne všechny bankomaty bezpečnostní kapsle používají.

Jak se bránit?

Smutnou realitou zůstává, že i přes současnou snahu dodavatelů vyvíjet bankomaty s vylepšenými bezpečnostními prvky, mnohé banky stále používají starší nezabezpečené modely, což je činí ideálními cíli pro útočníky, kteří aktivně napadají bezpečnost těchto zařízení.

Přestože bezpečnostní problémy s největší pravděpodobností ovlivňují mnoho bankomatů po celém světě, neznamená to, že situaci nelze výrazně zlepšit. Dodavatelé bankomatů a samotné banky mohou snížit riziko útoku na hotovostní stroje použitím následujících opatření:

- vyřazení všech bankomatů s nepodporovaným operačním systémem (Windows XP),
- implementace novější verze vrstvy XFS, která vyžaduje autentizaci pro volání kritických operací (zásadní obrana proti Jackpotting útoku),
- implementace šifrování komunikace a kontrola integrity dat přenášených mezi jednotlivými hardwarovými jednotkami a počítačem uvnitř bankomatu.

Pravidelné bezpečnostní testy bankomatů a stále narůstající počet útoků, které jsou rok od roku propracovanější, přispívají společně k řešení otázek bezpečnosti. V běžné praxi však bývá implementace nových ochranných opatření časově i finančně náročným procesem, zvláště když je síť bankomatů provozovatele rozsáhlá. V oblasti zabezpečení bankomatů nicméně začíná svítat na lepší zítřky, avšak ještě několik let potrvá, než budeme moci konstatovat, že bankomaty jsou opravdu nadstandardně zabezpečenými zařízeními.

Lukáš Antal
Lukas.Antal@aec.cz

Stanislav Klubal
Stanislav.Klubal@aec.cz

Ing. Lukáš Antal

Ing. Stanislav Klubal

Autoři působí ve společnosti AEC a.s. na pozicích Cyber Security Specialist. V týmu etických hackerů se řadu let věnují testování prostředí bankovních společností. Mají za sebou desítky úspěšně realizovaných projektů nejen po celé Evropě, ale také na asijském kontinentu.

POUŽITÉ ZDROJE

[1] European Association for Secure Transactions. ATM Malware attacks hit Europe. E.A.S.T [online]. 2018-04-10. Dostupné z https://www.association-secure-transactions.eu/tag/payment-terminal-fraud/)
[2] Kaspersky. Tyupkin Virus (Malware) | ATM Security. Kaspersky Lab [online]. 2014. Dostupné z https://www.kaspersky.com/resource-center/threats/tyupkin-malware-atm-security-malware)
[3] Kaspersky. Carbanak APT. Kaspersky Lab [online]. 2015. Dostupné z https://www.kaspersky.com/resource-center/threats/carbanak-apt)
[4] CEN. CEN Workshop on eXtensions for Financial Services (WS/XFS). European Committee for Standardization [online]. Dostupné z https://www.cen.eu/work/areas/ICT/eBusiness/Pages/WS-XFS.aspx)
[5] Trend Micro. A Shift in the ATM Malware Landscape: From Physical to Network-based Attacks. Trend Micro [online]. Dostupné z https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/shift-in-atm-malware-landscape-to-network-based-attacks)
[6] Raspberry Pi [online]. Dostupné z https://www.raspberrypi.org/)