A bankautomaták biztonsági áttekintése

An overview of ATM Security

BAKOS Tamás[1], Dr. COLEȘA Adrian[2], Dr. SEBESTYEN Gheorghe[3]

Számítástechnikai Tanszék, Kolozsvári Műszaki Egyetem,
George Bariţiu utca, 26-28 szám, Kolozsvár, Románia
[1]tamas.bakos@student.utcluj.ro,
[2]adrian.colesa@cs.utcluj.ro,
[3]gheorghe.sebestyen@cs.utcluj.ro

Abstract

Automated Teller Machines became popular among bank customers for the fast access to cash withdrawal from their bank accounts, and also among criminals for the large amount of money they contain, far away from the bank vaults' security. The way the latter access the money in an unauthorized manner from the ATM ranges from physical attacks, like forcing the safe open, sniffing magnetic data from bank cards, to software attacks that interact with the cash dispenser, allowing them to retrieve currency without having to damage the safe. This paper is intended as a warning about attack methods and a guide about defenses for ATM manufacturers,and financial institutions to help them in securing their products and assets. We focus on analyzing existing attacks and countermeasures based on known techniques, and proposing defensive mechanisms from multiple perspectives, most importantly a protection against ATM malware.

Keywords: ATM Security, ATM Attacks, XFS, Jackpotting, Blackbox attack, Lock Bypass, Cash Dispenser

Kivonat

A bankautomaták népszerűvé váltak a banki ügyfelek körében a gyors készpénzfelvétel lehetőségének eredményeképp, és a bűnözők körében is a bennük tárolt nagy összeg miatt, mert ezek nem részesülnek a banki páncélszekrények biztonságában. A módszerek, ahogyan az utóbbi személyek jogosulatlanul hozzá próbálnak férni ehhez a pénzhez változatosak: léteznek fizikai támadások, például a széf felfeszítése vagy a bankkártyák mágneses adatainak lehallgatása, és szoftvertámadások melyek folyamán egy rosszindulatú program rákapcsolódik a készpénzadagolóra, ami lehetővé téve számukra a pénz kiadását bankkártya nélkül és anélkül, hogy károsítanák a széfet. Cikkünk célja, hogy figyelmeztetésként szolgáljon a támadási módszerekre és útmutatóként a bankautomata-gyártók és pénzügyi intézmények számára, ezáltal segítve eszközeik biztosítását. A létező támadások és védekezési intézkedések elemzésére koncentrálunk, ismert technikák alapján bemutatva a lehetséges támadásokat, és biztonsági mechanizmusokat javaslunk, főképp bankautomatát célzó számítógépes vírusok ellen.

Kulcsszavak: bankautomata biztonság, bankautomata elleni támadások, XFS, Jackpotting, fekete doboz támadás, zár megkerülése, készpénzadagoló

BEVEZETŐ

A bankautomaták (angolul ATM, vagyis Automated Teller Machine) felkeltették a bűnözők figyelmét már 1967-ben, amikor széles körben elterjedtek, de négy évtizeden keresztül csak fizikailag támadták ezeket az eszközöket, elsősorban a készpénzt tartalmazó széfet a bankjegyek kinyerésére, a kártyaolvasót pedig a bankkártyák klónozása céljából.

A támadási módszerek változóak, a kezdetlegesektől, például robbanóanyagok vagy elektromos szerszámok használata a széf feltöréséhez, a bonyolultabb módszerekig, mint például a széf kombinációjának kitalálása, és a külső mágneses kártyalehallgató csatolása a kártyaolvasóhoz, a kliensek bankkártyáinak leolvasása, majd lemásolása érdekében. Ezek maradtak az egyedüli ismert módszerek, amellyel jogosulatlan módon pénzt szereztek a bankautomatákból, egész 2008-ig, amikor először észlelték az első, Skimer néven ismert, bankautomatára írt számítógépes vírust.

Sajnálatos módon a bankautomaták számos aspektusát, mind hardver, mind szoftver szinten, nem a biztonság szem előtt tartásával tervezték. Ezzel a problémával foglalkozunk a pénzügyi biztonságot fenyegető veszélyek csökkentése érdekében, mivel e terület tanulmányozása és jobb megértése elősegíti a banki szolgáltatások biztonságosabbá tételét. A biztonsági hibák kivizsgálásával, valamint a már meglévő fenyegetések és védelmi módszerek megismerésével új sebezhetőségeket fedeztünk fel, amelyekre a jelenleg rendelkezésre álló védekezési mechanizmusok még nem terjednek ki. A fenyegetettségi és támadási felület fejlődik, mivel a bűnözők folyamatosan újabb módszereket találnak ki az illegális pénzügyi haszon elérésére, ezért fontos, hogy lépést tartsunk velük a bankautomaták biztonságának területén, és továbbra is ellensúlyozzuk előrehaladásukat innovatív védelmi megoldásokkal. Ebben a cikkben az említett eszközök hardver és szoftverének tervezési és felépítési módosításait fogjuk javasolni, amelyek segíthetnek a meglévő biztonsági problémák megoldásában.

Tanulmányunk következőképpen épül fel: a 2. részben a kapcsolódó munkákat, a 3. részben a bankautomaták és biztonságuk elméleti hátterét mutatjuk be, a 4. részben a fenyegetéseket és a védekezési intézkedéseket, majd ezeknek az intézkedéseknek a problémáit és sérülékenységeit mutatjuk be, a bankautomaták biztonsági felmérésében szerzett tapasztalataink alapján. Ugyanebben a részben megoldásokat vetünk fel a biztonság további javítása érdekében. Az 5. részben e megoldások hatékonyságát értékeljük kísérletek által, majd a 6. részben következtetéseket vonunk le.

KAPCSOLÓDÓ MUNKÁK

Braeuer et al.[1] a linz-i Johannes Kepler Egyetemről és a KEBA AG-tól kockázatértékelést végeztek, leírják a bankautomaták elleni szoftvertámadások által jelentett kockázatokat, és megoldásokat ajánlanak a kockázatok csökkentésére. Munkájuk eredménye a bankautomaták klasszikus sebezhetőségei okainak azonosítása volt. Három kategóriába sorolják az ATM-eket fenyegető veszélyeket: kártya- és valutacsalás, fizikai támadások és logikai támadások, és elemzik az iparágban alkalmazott ellenintézkedések megfelelőségét mind technikai, mind kockázatkezelési szempontból. Ellenintézkedésekként a változásvezérlő rendszert, az alkalmazások engedélyezési listáját, a gazdagép-alapú tűzfal bevezetését, a teljes merevlemez-titkosítást és a frissítések kezelését említik.

Ezzel ellentétben Rasiah [2] kizárólag nem technikai szempontból tárgyalja az ATM rendszerek kockázatkezelését, hanem statisztikákat vizsgál a bankautomatákkal kapcsolatos csalásokról, a mechanikai hibákon vagy a hibás üzleti logikán alapuló géphibákról, a kockázatok azonosításáról és az esetleges veszteségek csökkentéséről. Végül leírja a szervezeti ellenőrzéseket és az üzleti folyamatok ellenőrzését a kockázatok mérséklése érdekében.

Az előző tanulmányokhoz hasonlóan Kasanda et al.[3] is a Zambiai Egyetemről az említett rendszerek kockázatelemzésével foglalkoztak munkájuk során, de további támadástípusokat is leírnak, például zsarolóvírus (ransomware), közbeékelődéses (man-in-the-middle - MitM) és fekete doboz támadásokat. Esettanulmányuk végén felsorolják a követendő biztonsági eljárások listáját is.

A Payment Card Industry Data Security Standard (PCI DSS) [4] egy a Payment Card Industry Security Standards Council (PCI SSC) által kezelt információbiztonsági szabvány, amelyet a fizetőkártyákat kezelő szervezetek számára hoztak létre a kártyacsalások csökkentése céljából. A tanács szabványokat is megállapított a PIN Transaction Security (PTS) névre keresztelt interakciós fizetőeszközök (Point of Interaction - POI) gyártói számára, amely kiterjed az összes PIN hitelesítéssel működő eszközre. Ezeknek a szabványoknak a kiegészítése dokumentálja az ATM biztonsági gyakorlatait, a PCI PTS POI ATM néven. A munka négy szakaszban tartalmaz biztonsági irányelveket, amelyek mindegyike felsorolja különböző szempontok biztonsági célkitűzéseit, és párosítja azokat a legjobb gyakorlatokra vonatkozó irányelvekkel.

ELMÉLETI HÁTTÉR

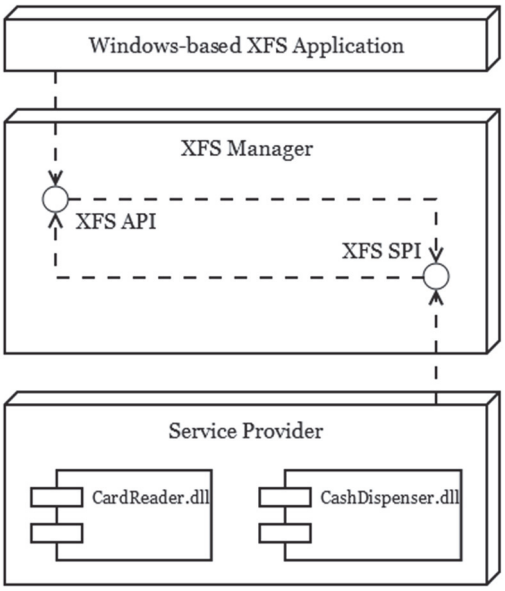
3.1. Hardver felépítés

Az első bankautomaták mikrovezérlőkön és specifikus integrált áramkörökön alapultak, de lassan eltávolodtak ettől az architektúrától, amikor az egyre komplexebb banki szoftverek felvetették a nagyobb számítási teljesítmény, a hálózati kapcsolat és számos periféria egyszerű integrálásának igényét. Ezek most a személyi számítógép (Personal Computer - PC) modellre épülnek, amely a korábbi konstrukciókkal összehasonlítva kihasználja a PC-k gyors számítási sebességét, nagyobb memóriakapacitását, valamint a perifériás csatlakozások, pl. a hálózati interfész vezérlő (Network Interface Controller - NIC) és az univerzális soros busz (Universal Serial Bus - USB) vezérlő interoperabilitását az elterjedt operációs rendszerekkel, főleg a Microsoft Windows rendszerrel. Két fő működési módjuk van: kioszk mód, amelyben az ügyfél csak a bankautomata szoftverét kezelheti, és el van határolva az operációs rendszer többi részétől; és rendszergazdai mód, amelyben a fejlesztők és karbantartók normál felhasználóként jelentkezhetnek be az operációs rendszerbe, szoftverfrissítések, diagnosztika elvégzése és beállítások módosítása céljából.

A modern bankautomaták perifériás eszközei az eszköz két fő rekeszében vannak elhelyezve: a szekrényben (amely tartalmazza a számítógépet, a kijelzőt, a nyugtanyomtatót, a kártyaolvasót és az azonosító számkód (Personal Identification Number - PIN) billentyűzetet), és a széfben (amely megvédi a készpénzadagolót és esetenként a készpénzbefogadót). Az ebben a két rekeszben tárolt eszközök között a tervezők fontosságbeli különbségeket feltételeznek, és emiatt ezek különböző mértékben védettek: a szekrény vékony fém burkolata csak egy egyszerű zárószerkezettel és egy egyszerű kulccsal van rögzítve, míg a széf megerősített falakkal és ajtókkal van felszerelve, kombinációs zárral, PIN-kóddal, komplex kulccsal vagy a fentiek mindegyikével van megvédve. Cikkünkben azzal érvelünk, hogy ez tervezési hiba, mivel a szekrény biztonsága majdnem olyan fontos lett, mint a széf biztonsága.

3.2. Szoftver keretrendszer

Mivel a bankautomaták perifériás eszközeit több különböző szolgáltató tervezti és gyártja, egy egységes felületre volt szükség a velük történő szoftveres kommunikációhoz. Ennek érdekében a Microsoft 1995-ben kifejlesztett és kiadott egy szabványt, a Windows Open Services Architecture (WOSA) alatt eXtensions for Financial Services (XFS) néven, amely rövidítve WOSA/XFS néven vált ismertté; ezt az Európai Szabványügyi Bizottság (CEN) 1998-ban nemzetközi szabványnak fogadta el, így a neve CEN/XFS lett.



1. ábra. *XFS Architektúra*

Amint az 1. ábrán látható, az XFS keretrendszer egy rétegzett szoftverarchitektúrának felel meg, amely két interfészt határoz meg annak érdekében, hogy absztrakciót biztosítson a különböző eszközökkel való interakcióhoz. A bankautomata szoftver, amely egy Windows-on futó XFS-alapú alkalmazás, a szabványosított XFS alkalmazásprogramozási felületet (Application Programming Interface - API) használja a különböző perifériás eszközökkel való kommunikációhoz, ami az eszköz gyártójától független. Az XFS Menedzser ezeket szolgáltatói interfész (Service Provider Interface - SPI) függvényhívásokká alakítja le, amely függvényeket az eszközgyártók valósítják meg, és amelyek kompatibilitást biztosítanak az XFS és az általuk fejlesztett perifériás eszközök között. A Szolgáltató (Service Provider) réteg ezután maga kezeli az eszközök közvetlen elérését és irányítását. Ez az architektúra rugalmasságot biztosít az ATM szoftverfejlesztők számára, akiknek csak az XFS API-t kell használniuk az egyes gyártók interfésze helyett, és elméletileg lehetővé teszi az univerzális bankautomata szoftverek írását is.

A könnyen használható XFS bevezetése jelentősen megkönnyítette az ATM szoftverek fejlesztését, de ugyanakkor lehetővé és egyszerűvé tette a támadók számára, hogy új támadási módszereket fejlesszenek ki. Ez a keretrendszer a bankautomaták biztonságának új korszakát vezette be, ahol pénzt lehet kinyerni az ATM szoftver vagy a hálózat manipulálásával, és a gyártóknak és pénzintézeteknek ennek megfelelően kell alkalmazkodniuk a pénzkezelő gépeik megvédése érdekében.

TÁMADÁSI ÉS BIZTONSÁGI MÓDSZEREK

4.1. Fizikai megközelítés

A bankautomata elsődleges fizikai védelmi mechanizmusa a széf, amelyben megtalálható a bankjegyeket tartalmazó készpénzadagoló. A legprimitívebb módszer ezen védelmi vonal leküzdésére a fúrógépek, marógépek vagy robbanóanyagok használata. Előfordulnak olyan esetek is, amikor a támadók építőipari nehézgépeket használtak fel a védőfalak és az akadályok lebontására, valamint az egész bankautomata kiemelésére, elvitelére annak érdekében, hogy egy félreeső helyen fel tudják nyitni. A kifinomultabb támadások közé tartozik a kártya vagy a bankjegyek beszorítása, ami úgy történik, hogy egy speciális eszközt helyeznek a kártyaolvasóba vagy a pénzkiadó nyílásba, amely azt eredményezi, hogy az áldozat felhasználójának kártyája vagy pénze elakad a gépben a nyílás előtt, ami lehetővé teszi, hogy a csaló, aki a csapda mechanizmusát felszerelte, ellophassa a beszorult értékeket, hogyha a felhasználó otthagyja a bankautomatát miután észreveszi az üzemzavart.

E támadások észlelésére, ellensúlyozására és elrettentésére különböző módszereket fejlesztettek ki: léteznek rezgésérzékelők a fúrás vagy vágás észlelésére, gázérzékelő a gépbe fecskendezett robbanó gáz érzékelésére, mozgásérzékelők a gép elmozdításának észlelésére, érintkezésérzékelők, amik figyelik, hogy kinyitják-e a szekrény ajtaját [5], és idegen tárgyak érzékelői a kártyaolvasóhoz és a készpénzadagolóhoz. Mindezeket az érzékelőket egy tartalék akkumulátor támogatja, hogy működésben tartsák azokat áramszünet vagy a támadó általi árammegszakítás esetén. Ha ezeket az érzékelőket egy tervezett karbantartási műveleten kívül aktiválják, a biztonsági cég vagy a rendőrség automatikusan értesítést kap az incidensről, vagy a legsúlyosabb esetben a bankjegy megsemmisítő rendszer, a festékcsomagok lépnek működésbe.

Az általánosan használt fizikai támadások másik fontos kategóriája a skimming támadások, amelyek révén a bűnözők apró, észrevehetetlen elektronikus eszközöket rögzítenek az automaták kártyaolvasóira, amelyek lehallgatják és tárolják a behelyezett kártya mágneses sávjának adatait. Az ilyen támadásokat általában a PIN-kód megszerzése végett egy kis kamera rögzítése kíséri. Ezzel a módszerrel a támadók klónozhatják a kártyát, és pénzt vehetnek fel vele.

Mivel a kártyalehallgatás a bankautomata támadásokból származó veszteségek 95%-át teszi ki [6], a gyártók bevezettek olyan védelmi megoldásokat, amelyek véletlenszerű elektromágneses zajt vagy zavaró jeleket bocsátanak ki a kártyaolvasó közelében, ami megakadályozza, hogy a skimmer eszközök pontosan leolvassák a kártyaadatokat [7]. A kártyák klónozásának további ellensúlyozása és a biztonságosabb fizetési mód kialakítása érdekében a bankkártyagyártók és szolgáltatók egyre inkább az intelligens kártyák és az Europay, a Mastercard és a Visa (EMV) által közösen kifejlesztett és az általuk elnevezett szabványok felé kezdtek elmozdulni. Így a kártyás fizetés biztonságosabb tranzakció-engedélyezési módra váltott a bankkártya-chipek használatával, ami megbízhatóbb a mágnescsíkos adatok használatánál, mivel az utóbbiak titkosítatlan formátumban vannak tárolva és könnyen olvashatók, így nem biztonságosak.

A bankautomata szekrény legszembetűnőbb fizikai sebezhetősége korábban az volt, hogy a gyártók minden gépükre ugyanazokat a zárakat telepítették, amelyeket ugyanolyan szabványos kulccsal lehetett kinyitni, és amilyet az interneten is meg lehet vásárolni. Ez megváltozott az újabb modellekben, mivel a gyártók minden géphez különböző zárakat kezdtek használni. Azonban mivel sok régi ATM-modell még mindig működésben van, különösen a fejlődő országokban, ez a tervezési hiba a mai napig komoly problémákat okozhat.

A biztonsági felmérés fizikai része kulcsfontosságú amikor hardveres rendszerekről van szó, ezért munkánk során elkezdtük elemezni több bankautomata burkolatát. Alapos vizsgálat után arra a következtetésre jutottunk, hogy a széf biztonságával ellentétben az ATM-szekrények zármechanizmusai nincsenek teljesen biztonságosra tervezve, gyakran kulcs nélkül is kinyithatóak, megkerülve a zárat. Ez jelentős előnyt jelenthet egy támadó számára, mivel nem hagy nyomot a fizikai manipulációról, ellentétben a szekrényajtó felfeszítésének vagy fúrásának történő széles körben elterjedt módszerével, illetve gyorsabban elvégezhető, mint egy tolvajkulccsal megpróbált zárfeltörés.

A bankautomata számítógépét védő mechanizmusok a szekrényen rugós zárszerkezeteken alapulnak: egy rögzített és egy mozgó elemből vannak kialakítva, amelyek közül az egyik egy lakatszem vagy forgóretesz, a másik pedig az ebbe beakadó horogzár. A mozgó részhez rugó van rögzítve, és a rugó feszültsége az alapértelmezett helyzetben tartja azt, ami a bezárt állapotnak felel meg. Miközben a kulcsot a zárban elforgatjuk, ennek a mozgó alkatrésznek a helyzete a rugó húzóerejével ellentétes irányba változik, így kinyitja a mechanizmust. Ennek a kialakításnak a hibája az, hogy a mozgó részt csak a rugó tartja a helyén, a zár egyhelyben maradása nem korlátozza a mozgását.

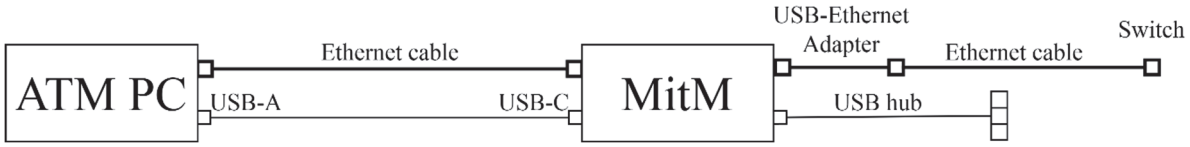
A zár kikerülésének elve mindkét esetben az, hogy a zárral és kulccsal működtetett mozgatható rész a zártól függetlenül is elmozdítható. Általában elegendő hely marad a bankautomata szekrény ajtaja és a fala között, így megfelelő alakú feszítőszerszámot lehet behelyezni annak érdekében, hogy elérje és erőt gyakoroljon a mozgó részre, hogy azt nyitott helyzetbe tolja, mivel ezt csak a rugó tartja helyben. Ezzel a módszerrel számos bankautomata szekrényét ki lehet nyitni kulcs vagy tolvajkulcs nélkül, egy vékony szerszámot használva.

A szekrényajtó zárva tartásának megfelelő módszere egy rugó nélküli zár, például holtcsavar használata lenne, amely a mechanizmus mozgó részének elmozdulását kizárólag a zár kulcs általi forgatásával együtt teszi lehetővé, és nem engedi, hogy önállóan mozogjon. Ily módon nem lehetne megváltoztatni a mozgó alkatrész helyzetét úgy, hogy közvetlenül gyakorlunk rá erőt egy szerszám segítségével.

Ahhoz, hogy valakinek elég tapasztalata legyen arról, hogyan kell pontosan kezelni, illetve kulcs vagy felfeszítés nélkül kinyitni a záró mechanizmust, alapos tanulmányozást és sok gyakorlást igényel. Ennek ellenére a szervezett bűnözői csoportok rendelkezhetnek elegendő erőforrással ahhoz, hogy megvásárolhassanak egy bankautomatát és gyakorolják a rendhagyó kinyitás módszerét.

A szekrény kinyitása után a támadó hozzáférhet az automata számítógépéhez, valamint a hálózati és a perifériás eszközökhöz csatlakozó kábelekhez. Ettől a ponttól kezdve a támadók telepíthetik saját hardverüket közbeékelődéses vagy fekete doboz támadás végrehajtására; vagy feltölthetik saját végrehajtható fájljaikat, illetve számítógépes vírusokat a rendszerbe egy USB tároló segítségével. Előfordultak olyan esetek is, amikor a bűnözők kinyitották a bankautomata szekrényét annak érdekében, hogy ellophassák a számítógépet vagy annak merevlemez-meghajtóját (HDD), hogy elemezni tudják a banki szoftvert, és kártékony programokat tudjanak létrehozni ezen ismeretek alapján.

Hardver csatlakoztatása a rendszerhez megoldható kevés feltűnéssel, vagyis, ha a számítógép és a támadó eszköz között hosszú USB és Ethernet kábeleket használunk, és az eszközt a szekrény hátuljában, a számítógép mögött helyezzük el, ahonnan tovább fut a számítógép eredeti hálózati kábele a hálózat többi része felé, ahogy a 3. ábrán látható. Megfelelő jelölt erre a feladatra egy Raspberry Pi, mivel kis méretű, könnyen beszerezhető és konfigurálható. Hogy ezt a felállást még tovább vigyük, a bankautomata számítógépének összes USB portjába álkábeleket csatlakoztathatunk, miközben előtérben hagyunk egy a Rasperry Pi-hoz csatlakozó USB elosztót (USB hub), ezzel késztetve a technikusokat, hogy karbantartás esetén a támadó mini-számítógépen keresztül csatlakoztassák a billentyűzetüket.



2. ábra. *Közbeékelés USB és Ethernet kábelre*

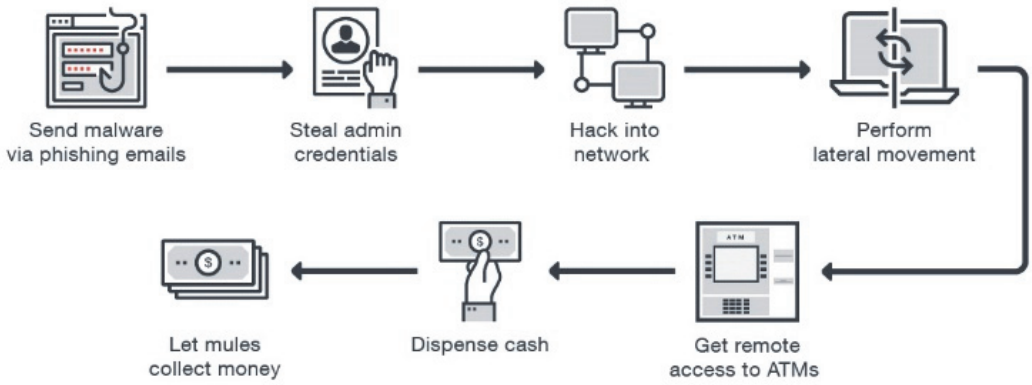
Mivel az ilyen hardver elhelyezést egy gyanútlan vagy gyakorlatlan szemnek nehéz észrevenni, azt javasoljuk, hogy az ATM karbantartásáért felelős vezetők egy új szakaszt foglaljanak bele a technikusok módszertanába, nevezetesen, hogy minden alkalommal, amikor kinyitják az automata szekrényét, alaposan ellenőrizzék, hogy nincs-e idegen hardver beépítve, különösen minden alkalommal, amikor riasztás érkezik, hogy a szekrényajtót a tervezett karbantartási időn kívül nyitották ki. Ezekben a helyzetekben kulcsfontosságú, hogy a technikusok tudatában legyenek annak, hogy ilyen szembe nem tűnő támadások előfordulhatnak.

Természetesen ezeket a fizikai támadási kockázatokat sokszor mérsékli a gépre telepített kamerák, a zártláncú kamerarendszer (CCTV) és a biztonsági személyzet alkalmazása, de mivel ezek nem mindig vannak jelen, az említett fizikai biztonsági problémákkal alaposan foglalkozni kell.

4.2. Hálózat

A fentebb leírt hardver elhelyezés lehetséges eredménye, hogy közbeékelt támadó hardver kerül az hálózati csatlakozásra. Hálózati közbeékelődés esetén fennáll a veszélye, hogy a támadó hardver lehallgatja a bankautomata és a szerver közti kommunikációt, és parancsokat, illetve esetenként módosítja azokat a támadó javára. Egy példa erre az lenne, hogy pénzváltó bankautomaták esetén megváltoztatják a szervertől kapott információt a valutaváltó árfolyamról, sokszorosítva azt, aminek eredményeképp, aki épp pénzt vált, az a várt valuta sokszorosát kapja. Emellett ez a módszer hasznos lehet a nyomok eltűntetésére is, például hálózaton küldött riasztások megállítása/ejtése.

A fizikai támadások mellett egy másik módszer arra, hogy a bűnözők számítógépes vírusokat telepítsenek bankautomatákra, a bank hálózatába való beszivárgás. Ez egy nehezebben kivitelezhető megközelítés, mivel létfontosságú infrastruktúrájuk miatt a pénzintézetek hálózata ideális esetben jól védett a külső támadásokkal szemben. A fő belső hálózat és az ATM-ek alhálózata el vannak különítve, ami azt jelenti, hogy a támadónak még a pénzügyi intézmény hálózatába való beépülés után, de még a célgépek elérése előtt is további akadályai vannak, például tűzfalak vagy virtuális magánhálózat (VPN) átlépése. Ennek ellenére még azokban az esetekben is, amikor hálózati szegregációt alkalmaztak, előfordultak olyan esetek, amikor a bűnözők sikeresen telepítettek rosszindulatú kódot bankautomatákra ezt a módszert alkalmazva.



3. ábra. *Bankautomaták hálózaton keresztüli megtámadása*

Az ilyen típusú támadások rutinszerű módszere, amint azt a 3. ábra szemlélteti, azzal kezdődik, hogy egy banki alkalmazottat céloznak meg adathalász (phishing) módszerekkel. Miután megszerzi az alkalmazott jelszavát, a támadó beléphet és oldalirányban mozoghat a hálózatban további számítógépeket

megfertőzve, közben további felhasználóneveket és jelszavakat gyűjtve, amelyek felhasználhatók a bankautomaták hálózatához való hozzáférésre VPN kapcsolaton keresztül, ha szükséges, majd Remote Desktop Protocol-lal (RDP) a bankautomaták számítógépéhez való csatlakozásra. Létezik olyan módszer is, ami a szoftverfrissítések szerverének feltörése által meghamisított, és rosszindulatú frissítést küld az ATMeknek. A Ripper kampány volt az első, amely rosszindulatú támadást hajtott végre anélkül, hogy fizikailag meg kellett volna nyitnia az automatákat [8].

4.3. Periférikus eszközök

Gyakori támadó módszer a betelepített hardver esetében a fekete doboz támadás, ami azt jelenti, hogy leválasztjuk a készpénzadagoló USB kábelét a számítógépről, és csatlakoztatjuk a támadó mini-számítógéphez, a „fekete dobozhoz", amely ezután közvetlenül a készpénzadagolónak ad parancsokat. Ez a lehetséges sebezhetőség az ATM szoftver és a készpénzadagoló közötti kölcsönös hitelesítés esetleges hiányának eredménye.

Az ATM számítógép és a készpénzadagoló kölcsönös hitelesítésén alapuló ellenintézkedést a gyártók a széfben található perifériás eszközhöz való hozzáférés igazolásával ellenőrzik. Egy ilyen kézfogás az eszközök között az ATM szoftverből elindítva fizikai műveletet kér az adagolón, ami vagy egy gomb megnyomásával, vagy egy pénzkazetta eltávolításával és visszahelyezésével teljesíthető [9]. Ennek eredményeként az adagoló megjegyzi az számítógépet, mint egyetlen eszközt, amellyel a következő kölcsönös hitelesítésig kommunikálni fog, valamint egy titkosított kulcscserét is végrehajt a további biztosított kommunikáció érdekében, amelyre szükség van a fekete dobozos vagy a közbeékelődéses (man-in-the-middle - MitM) támadások leküzdéséhez, amit ebben és a következő alfejezetben tárgyalunk.

Az USB csatlakozások közbeékelése is hasznos lehet egy támadó számára. Az első és legfontosabb előnye a billentyűleütések befecskendezése, vagyis a hardver a billentyűk lenyomását utánozva parancsokat futtathat a bankautomata számítógépén. Ez a technika kiterjeszthető, hogyha egy technikus a közbeékelt USB csatlakozáson keresztül írja be a jelszót a bankautomata operációs rendszerébe, akkor a támadó hardver ezeket a billentyűleütéseket továbbítja a számítógép felé, hogy ne legyen feltűnő, és egyszerre fel is jegyzi a begépelt jelszót, hogy később annak segítségével jelentkezzen be a billentyűk emulálásával. Ezt a technikát BadUSB 2.0 néven mutatták be [10].

A billentyűzetemuláció fontos felhasználási területe az a tény, hogy a parancssoron keresztül fájlokat lehet feltölteni, különösen abban az esetben, ha a tárolóeszközök csatlakoztatása le van tiltva. Ez úgy történik, hogy egy szkript segítségével a feltöltendő fájlt darabokra osztjuk, a darabokat base64 formátumba kódoljuk, és a kimeneti átirányítással párosított *echo* parancs segítségével kódolt formájukat fájlba írjuk. Végül, amikor a feltöltés befejeződött, a fájlok dekódolhatók vagy a CertUtil segédprogrammal Windows rendszeren, vagy a base64 paranccsal Linux rendszereken. Ez a fájl feltöltési módszer viszonylag lassú, de nehéz ellenintézkedéseket felállítani ellene, mivel karbantartási célból minden rendszerrel kapcsolatba kell tudni lépni, és ennek elsődleges módja a billentyűzet használata.

Ezzel a technikával párosítva egy USB tárolóeszközt, vagy annak emulálását fel lehet használni arra is, hogy automatizáltan egy másik operációs rendszert, például Linuxot indítsunk el a bankautomata számítógépén, ami által hozzáférést nyerhetünk a fájlrendszerhez, és így egyenesen meg tudjuk változtatni a Windows operációs rendszer jelszavait, vagy számítógépes vírust tudunk telepíteni. Ezen kívül ilyen esetekben a támadók létrehozhatnak egy hátsó ajtót (backdoor) a bejelentkezési képernyőn elérhető végrehajtható fájlok (pl. Nagyító, Képernyő-billentyűzet) cmd.exe-re való cseréjével, hitelesítő adatok hozzáadásával vagy megváltoztatásával, sőt kikapcsolhatják a védelmi rendszereket, mint például az antivírusokat.

A billentyűzetemuláció részben kiküszöbölhető a perifériás eszközök hitelesítésével, amik a hardverazonosítóik vagy típusaik alapján engedélyezhetők. Annak ellenére, hogy megakadályozhatjuk az ismeretlen eszközökkel való kapcsolatot, amelyeknek rögzített a hardverazonosítója, ennek megkerülése az USB eszköz-emulációval megvalósítható, ahol a gyártó- és termékazonosítók dinamikusan beállíthatók. Így a támadó képes végigpróbálni az azonosítókat, amíg valamelyiket az operációs rendszer el nem fogadja, és a kapcsolat létrejön. Jelenleg az elterjedt végpontvédelmi megoldások nem észlelik ezt a viselkedést.

4.4. Titkosítás és jelszavak

Figyelemre méltóak a szokásos biztonsági javaslatok a komplex jelszavak beállításáról a BIOS menü, a rendszerindító menü (boot menu) és a Windows rendszerbe való belépéshez, hogy ezáltal megakadályozzák az idegen operációs rendszerek indítását vagy az aktuálishoz való hozzáférést. A BIOS és a rendszerindító menü jelszavának gyári beállításra való visszaállítása továbbra is lehetséges lehet a támadó számára, aki fizikai hozzáféréssel rendelkezik a számítógéphez, bizonyos eszközök esetében, de egy ilyen művelet magába foglalja vagy az alaplap csatlakozóinak elérését, vagy a CMOS akkumulátor eltávolítását és pár perc várakozást, ami időigényes és nehezen megvalósítható, mivel jelentősen növeli a támadás felfedezésének esélyeit.

Amint fentebb említettük, a gép fizikai kinyitása után rosszindulatú programok telepítése lehetséges egy másik operációs rendszer indításával egy USB tárolóról, így teljes mértékben irányítva a gépet, és különösen annak fájlrendszerét. Az ilyen típusú támadások leghatékonyabb ellenintézkedése a merevlemez-titkosítás, például a BitLocker telepítése és elindítása, amely a Microsoft Windows újabb verzióiba bele van építve. Ez megakadályozza az előbb leírt támadások végrehajtását. Ezenkívül a HDD ellopása esetén a titkosítás elérhetetlenné és használhatatlanná teszi a meghajtón lévő adatokat.

Hálózati közbeékelődéses (MitM) támadások esetében [11] esetében pedig, kulcsfontosságú a hálózati kommunikáció védelme a TLS (Transport Layer Security) megvalósításával a kliens-szerver interakcióban, vagy VPN-kapcsolat használatával az adatátvitel védelme érdekében.

Egy másik szempont arra vonatkozóan, hogy miért nem szabad implicit módon megbízni a vezetékeken történő adatátvitelben, az a tény, hogy a támadók közbeékelődéses támadásokat hajthatnak végre az ATM szoftver és a készpénzadagoló között is, ha a kommunikáció nincs titkosítva. Ebben az esetben módosíthatják vagy újrajátszhatják a pénzkiadási parancsokat, amelyek az operációs rendszer szintű védelmi mechanizmusok számára nem láthatóak. Szerencsére a gyártók egyre inkább tudatában vannak ennek a problémának, és folyamatosan frissítik a banki szoftvereket és a perifériás firmware-t annak érdekében, hogy kölcsönös hitelesítésük eredményeképpen biztosítsák a köztük lévő információk és parancsok titkosított továbbítását [12].

A TLS használatát fentebb bemutattuk a közbeékelődéses támadások elleni védekezésként, ez meglehetősen elterjedt a modern rendszerekben. Az egyetlen módja annak, hogy a támadó megkerülje ezt a védelmet, ha hozzáfér a titkosítatlan Windows fájlrendszerhez egy másik operációs rendszer indítása után, vagy a rendszergazdai fiók jelszavához. Mindkét módszer használható a billentyűzet-emulátor segítségével egy a támadó által generált tanúsító hatóság (Certificate Authority - CA) gyökértanúsítvány (root certificate) telepítéséhez az operációs rendszerbe, amely alapján a közbeékelt gép egy a rendszer által megbízhatónak nyilvánított TLS-tanúsítványt tud generálni minden olyan szerver megszemélyesítésére, amelyhez az ATM szoftver csatlakozik. Ez alapján lehetséges a TLS forgalom titkosításának feloldása a közbeékelt eszközökön, illetve annak módosítása.

Míg a végpontvédelmi megoldásoknak figyelmeztető jelzéseket kellene indítaniuk amikor új gyökértanúsítványt telepítenek a rendszerbe, ez nem mindegyik történik így, és ezek a termékek egyébként is kikapcsolhatóak, ha a támadó a fent említett módok valamelyikével hozzáfér a rendszerhez. Annak érdekében, hogy megbizonyosodjon arról, hogy a szerverkapcsolat titkosítása nem sérült-e, az ATM-szoftvereknek ajánlott végrehajtaniuk a tanúsítvány rögzítését (certificate pinning), vagyis azt, hogy figyelmen kívül hagyják a rendszer tanúsító hatóságait, és csak egy előre meghatározott tanúsítványban, vagy egy bizonyos megbízható tanúsító hatóság által aláírt tanúsítványban bízzanak a szerverrel való kommunikációban.

4.5. Operációs rendszer és alkalmazás

A bankautomaták széfjei elleni támadási módszerek kifinomultabbak lettek, és ahelyett, hogy a rablók fizikailag törjék fel, rosszindulatú programok fejlesztésébe és felhasználásába kezdtek, hogy azok segítségével a készpénzadagolón keresztül nyerjék ki a pénzt, bankkártya használata nélkül. Ezt a módszert Jackpotting támadásnak nevezik.

Az első ismert bankautomatára tervezett számítógépes vírus, a Skimer, a Diebold nevű gyártó saját szoftverével kommunikálva működött, és fő célja az ügyfelek tranzakciós adatainak lehallgatása volt. A legújabb vírusok viszont már az XFS keretrendszert használják a perifériás eszközök, például a készpénzadagoló, a PIN-kód billentyűzet vagy a nyugtanyomtató irányítására a gyártótól függetlenül, és ezen keresztül főleg a pénz kiadására.

Más ismert rosszindulatú programcsaládok, mint például Padpin-Tyupkin, Ploutus, GreenDispenser, Alice és Ripper, hogy csak néhányat említsünk, elsősorban a készpénz kinyerésére összpontosítanak, az XFS-en keresztül az említett perifériás eszközre való csatlakozás és a pénzkiadási parancsok közvetlen küldése révén. Néhányuk olyan funkciókat is tartalmaz, amelyek lehetővé teszik a PIN-kód billentyűzetével történő vírusvezérlést, vagy egy előre meghatározott mágneses sávú kártya behelyezésével történő aktiválást. Egyikük, a Ploutus, kiemelkedik ilyen szempontból, mivel a támadók bizonyos esetekben fizikailag egy mobiltelefont telepítettek az ATM szekrényébe, amely SMS-en keresztül kapott parancsokat, és USB csatlakozás segítségével továbbította őket a számítógépre telepített rosszindulatú programnak [13].

Figyelemre méltó jellemző, hogy ezeknek a rosszindulatú programoknak egy része, nevezetesen a Padpin-Tyupkin, a Ploutus, a Cutlet és a GreenDispenser változatai olyan aktiválási vagy dekódolási kulcsokat igényelnek, amelyek csak a vírus-fejlesztőtől szerezhetők be a pénzkiadás végrehajtásához. Ez annak a ténynek köszönhető, hogy ezeket a verziókat Malware-as-a-service (MaaS) modell keretében értékesítették az online feketepiacon [14].

Gyakori a bankautomata vírusok körében az, hogy az „msxfs.dll” nevű, dinamikusan összekapcsolt könyvtárban (Dynamic Link Library - DLL) rendelkezésre bocsátott függvényeken keresztül kommunikálnak az XFS keretrendszerrel, ezzel szemben azonban kevés olyan rosszindulatú alkalmazás ismert, amelyek függvényeket térítenek el a function hooking módszerrel. Köztük van a Skimer, a Suceful és a Prilex, amelyek közül csak a második téríti el az XFS függvényhívásokat.

Annak érdekében, hogy bebizonyítsuk az ilyen típusú támadások megvalósíthatóságát, kifejlesztettünk egy koncepció-igazoló programot (POC), amely kódot fecskendez a bankautomata szoftver folyamataiba, eltéríti az XFS API függvényeket, és így nyomon követhettük a banki szoftver által végrehajtott összes művelet, és ezzel együtt a gépet kezelő banki ügyfél műveleteit. A felhasználási esetek közé tartozik a kiosztott pénz megsokszorozása egy jogos tranzakció módosításával, parancsok visszajátszása, önálló pénzkiadási parancs indítása, a kinyomtatott nyugták tartalmának megváltoztatása, hogy elfedje a hamisítást és a kártyaadatok rögzítése. A rosszindulatú kód futtatása a jogos ATM folyamatok címteréből nem okoz feltűnést, mivel az XFS parancsok a megszokott folyamatból származnak.

A pénzügyi intézmények által alkalmazott megszokott védelmi mechanizmusok, nevezetesen a vírusírtó megoldások különböző mértékben hatékonyak, mivel sokszor a rosszindulatú futtatható fájlok profiljának vagy bájtmintájának egyezésén alapulnak. Mind a saját fejlesztésű támadó program, ami egy klasszikus végrehajtható fájl, amely közvetlenül kommunikál az XFS-szel, mind a fent említett kódbefecskendezést használó program, le tudott futni a tesztelt ATM gépeken annak ellenére, hogy jelen voltak vírusírtó szoftverek. Ennek két oka lehet: a végrehajtható fájljainkat nem azonosították korábban rosszindulatú programként, és/vagy nem tartalmaztak vírus kódrészleteket és klasszikus rosszindulatú programok jellemzőit. Ebből arra a következtetésre jutottunk, hogy a viselkedésalapú védelmi megközelítés jobban működik az XFS-szel kommunikáló rosszindulatú programok elleni védelemben. Az Endpoint Detection and Response (EDR) termékek hasznosak ehhez, ezek összesítik a rendszerben történt eseményeket, összehasonlítják azokat bizonyos előre felállított észlelési szabályokkal, és a talált viselkedési minták alapján észlelik a rosszindulatú tevékenységeket.

Az bankautomata vírusok ellen a következő viselkedési szabályokat javasoljuk:

- Csak engedélyezett DLL-ek betöltése az ATM-specifikus folyamatokba: ha egy bankautomata szoftver folyamat egy nem engedélyezett DLL-t tölt be, az azt jelenti, hogy be lett fecskendezve
- Ne engedélyezze az "msxfs.dll" függvények eltérítését: figyelje az XFS DLLben a függvények első bájtjait és az exportcímtár bejegyzéseit; ha valamelyik megváltozik, az azt jelenti, hogy a függvényeket megpróbálják eltéríteni
- Ne engedélyezze a bankautomata szoftveren kívüli folyamatok számára az XFS használatát: ha az "msxfs.dll" betöltődik az egyik ilyen folyamatba, akkor valószínűleg rosszindulatú programról van szó.
    - Mivel egyes kibúvási technikák között szerepel a DLL-fájl másolása, átnevezése és néhány bájt módosítása betöltés előtt, ezért az adott DLL-fájl észlelése a memóriában az exportkönyvtár elemzésén és az exportált függvénynevek ellenőrzésén kell alapuljon

Jó eredmények érhetők el a folyamatok engedélylistázási megoldásaival is, amelyek csak bizonyos végrehajtható fájlokat engednek futtatni, és blokkolnak minden olyan bináris fájlt, szkriptet és parancsot, amelyek nem jogosultak végrehajtásra.

Mint minden rendszer biztonsága esetében, erősen ajánlott a javítócsomagok automatikus kezelése annak biztosítására, hogy a legújabb operációs rendszer, szoftver és firmware frissítések telepítésre kerüljenek, amint a gyártók kiadják azokat. Ez segít elkerülni számos lehetséges támadást, mivel sok közülük azon alapul, hogy a célrendszerek elavultak, és ismert és közzétett, de nem javított biztonsági réseik vannak.

Sajnos tapasztalataink alapján az ATM-rendszerek általában nem követik a legkisebb jogosultság elvét, mivel mind a kioszk mód, mind a karbantartási mód felhasználói adminisztrátorként szerepelnek a futó szolgáltatások egyszerű kezelése érdekében. Miután a támadó hozzáfér egy ATM rendszerhez, nem kell bajlódnia a jogosultságok növelésével, hogy meg tudja változtatni a rendszer és a biztonsági szoftver beállításait. Ezért erősen ajánlott alacsonyabb jogosultságú felhasználók bevezetése mind a kioszk üzemmódba, ahol a szolgáltatások automatikusan elindíthatók, mind a bankautomatába való bejelentkezéshez karbantartás céljából, ahol a technikusok adminisztratív jogokat kérhetnek a Windows karbantartási felhasználói fióknak, amikor minden magasabb kiváltságokra van szükség.

KÍSÉRLETEK

A javasolt hardver-ellenőrzés, amelyet el kellene végezni a riasztások alkalmával, hatékony, de tudatosítást igényel. Társadalomtechnikai kísérletet végeztünk azzal, hogy megkérdeztük az ATM szakembereket, hogy látnak-e valami szokatlant a gépen, miután elültettük benne a közbeékelt hardvert, és első pillantásra semmi gyanúsat nem észleltek.

A védelmi viselkedési szabályok, beváltak az ismert ATM víruscsaládok ellen. Ezt teszteltük mind valódi vírus-minták futtatásával egy virtualizált bankautomatán, mind pedig azzal, hogy kipróbáltuk saját XFS alapú rosszindulatú programjaink ellen egy igazi bankautomatán; az eredmények ugyanazok voltak, a rosszindulatú program nem tudott megfelelően lefutni, mivel az XFS keretrendszerrel való jogosulatlan kommunikációt leállították a viselkedési szabályok.

KÖVETKEZTETÉS

A támadók és védők információbiztonsági versenye macska-egér játék, mindkét oldal folyamatosan új módszerekkel áll elő a másik ellen. Amint ebben a cikkben láthattuk, sokféle támadás elkerülhető csupán alapvető biztonsági intézkedések végrehajtásával, mint például a merevlemez-titkosítás, az eszközhitelesítés, eszköz és folyamat engedélyezési lista, valamint erős jelszavak beállítása a BIOS menü, a rendszerindító menü és a Windows felhasználók számára, de a biztonsági felmérési tapasztalatok alapján a bankautomata-üzemeltetők hajlamosak figyelmen kívül hagyni néhány ilyen fontos lépést. Rendkívül fontos mindet megvalósítani, mivel a biztosítási erőfeszítések csak ezek alapján vezetnek alaposan védett rendszerhez; akár az egyik hiánya is biztonsági rést teremthet, amelyet a bűnözők kihasználhatnak.

HIVATKOZÁSOK

[1] Bräuer, J and Gmeiner, B and Sametinger, J.: *A Risk Assessment of Logical Attacks on a CEN/XFS-based ATM Platform*. International Journal on Advances in Security, 2016.

[2] Rasiah, D.: *ATM risk management and controls*. European Journal of Economics, Finance and Administrative Sciences, 2010.

[3] Kasanda, E and Phiri, J.: *ATM Security: A case study of Emerging Threats*. International Journal of Advanced Studies in Computer Science and Engineering, 2019.

[4] PCI Security Standards Council: *ATM Security Guidelines*. Payment Card Industry Data Security Standards, 2013.

[5] Terrier Security Services: *Terrier Smart ATM Solution*. https://www.terrier.co.in/atm-security-solution/

[6] NCR: *ATM Security - Explaining Attack Vectors, Defense Strategies and Solutions*. NCR Whitepaper, https://www.ncr.com/content/dam/ncrcom/content-type/brochures/ATM_Security_white-paper-attack-vectors-and-solutions.pdf , 2017.

[7] NCR: *I am the NCR Skimming Protection Solution*. NCR Patent Pending, https://www.ncr.com/content/dam/ncrcom/content-type/datasheets/skimming-protection-solution-ds.pdf , 2014.

[8] Schwartz, M.: *ATM Hackers Double Down on Remote Malware Attacks*. Bank Info Security, https://www.bankinfosecurity.com/atm-hackers-double-down-on-remote-malware-attacks-a-10338 , 2017.

[9] NCR: *Dispenser Security Solution*. NCR Secure Whitepaper, https://www.ncr.com/content/dam/ncrcom/content-type/documents/NCR_Secure_white_paper-Dispenser_Security_Solution_September_2018.pdf , 2018.

[10] Kierznowski D.: *BadUSB 2.0 : USB man in the middle attacks*. 2016.

[11] NCR: *Man in the Middle Network Attacks*. NCR Security Update, https://www.ncr.com/content/dam/ncrcom/content-type/documents/NCR-Security-Alert-2015-01-Man-in-the-Middle-Attack-in-Mexico.pdf , 2015.

[12] NCR: *Critical Platform Component Update for S1 and S2 Currency Dispenser*. NCR Security Update, https://www.ncr.com/content/dam/ncrcom/content-type/documents/NCR_Security_Alert-2018-10-S1_and_S2_Critical_Update.pdf , 2018.

[13] Sancho, D. and Huq, N. and Michenz, M.: *Cashing in on ATM Malware - A Comprehensive Look at Various Attack Types*. Trend Micro - Europol Joint Reports, https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf , 2017.

[14] Zykov K.: *ATM malware is being sold on Darknet market*. Kaspersky Securelist, 2017.