บทเรียนจากปัญหา
การโจมตีเครื่องฝาก-ถอนเงินสดอัตโนมัติ (ATM) ด้วยมัลแวร์และการเตรียมรับมือในอนาคต

Lessons Learned from ATM Malware Attacks

The lessons learnt from the recent problems of ATM machines being attacked with malware, and the preparation of future protective measures.

นายปริญญา หอมเอนก
Mr. Prinya Hormanek,
ACIS Professional Center Co., Ltd. and Cybertron Co., Ltd.

เครื่องฝากถอน-เงินสดอัตโนมัติหรือที่รู้จักกันดีในนาม "เครื่องเอทีเอ็ม" เข้ามามีบทบาทในชีวิตประจำวันของเราตั้งแต่วันที่ 27 มิถุนายน พ.ศ. 2510 (ก่อนผู้เขียนจะเกิดเสียอีก) โดยเครื่องเอทีเอ็มเครื่องแรกตั้งอยู่ที่มหานครลอนดอน เป็นของธนาคาร Barclays จากนั้นก็เริ่มนิยมกันอย่างแพร่หลายทั่วโลก จากความนิยมการใช้งานเครื่องเอทีเอ็มที่เพิ่มขึ้น การโจมตีสถาบันการเงินที่มุ่งการโจมตีไปที่เครื่องเอทีเอ็มก็กำลังเพิ่มขึ้นทั่วโลกเช่นกัน การถอนเงินจากเครื่องเอทีเอ็มอย่างผิดกฎหมายของกลุ่มแฮกเกอร์ได้สร้างความเดือดร้อนต่อธนาคารและลูกค้าของธนาคารต่างๆทั่วโลกในเวลานี้

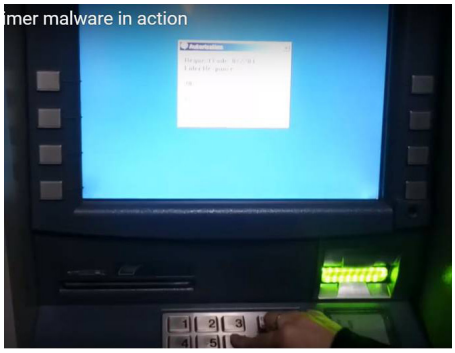
มาทำความเข้าใจองค์ประกอบของเครื่องเอทีเอ็มกันก่อน

องค์ประกอบของเครื่องเอทีเอ็มทุกเครื่องในโลกนี้ประกอบด้วยส่วนของ Hardware และ Software ที่ต่อเชื่อมกับระบบเครือข่ายภายในของธนาคาร เริ่มจากส่วนของ Hardware ของผู้ผลิตแต่ละรายจะมีลักษณะที่แตกต่างกัน ยี่ห้อยอดนิยมที่เราเห็นกันบ่อยๆ ได้แก่ Diebold, Wincor Nixdorf และ NCR แต่ละยี่ห้อมีการออกแบบที่ไม่เหมือนกัน การทำงานภายในเครื่องก็มีความแตกต่างกันในแต่ละยี่ห้อ ภายในเครื่องเอทีเอ็มประกอบไปด้วยส่วนของเครื่องคอมพิวเตอร์ที่ส่วนใหญ่ทำงานด้วยระบบปฏิบัติการ Windows และส่วนของเครื่องเซฟที่ใช้เก็บเงินที่มีความมั่นคงปลอดภัยสูงกว่าตัวเครื่องคอมพิวเตอร์ที่ภายในเครื่องเอทีเอ็ม

จุดอ่อนของระบบที่พบเป็นประจำได้แก่ ช่องโหว่ของระบบปฏิบัติการ Windows ที่เกิดขึ้นในเครื่องคอมพิวเตอร์ตามสำนักงานหรือตามบ้านทั่วไปก็ไม่ต่างกับกับช่องโหว่ของระบบปฏิบัติการ Windows ของเครื่องคอมพิวเตอร์ที่อยู่ในเครื่องเอทีเอ็ม ดังนั้นเครื่องเอทีเอ็มก็มีโอกาสในการติดไวรัสคอมพิวเตอร์หรือถูกโจมตีด้วยมัลแวร์เช่นกัน เพียงแต่ที่เครื่องเอทีเอ็มไม่ค่อยมีปัญหานี้มาก่อน เนื่องจากเครื่องเอทีเอ็มอยู่ในเครือข่ายปิดของธนาคารมาโดยตลอด จนเมื่อปี ค.ศ.2010 แฮกเกอร์หนุ่มชาวนิวซีแลนด์ Mr. Barnaby Jack ได้แสดงการเจาะระบบเครื่องเอทีเอ็มบนเวทีงาน Black Hat Computer security Conference 2010 ที่ลาสเวกัส การเจาะระบบในครั้งนั้นเป็นที่โด่งดังไปทั่วโลกในหัวข้อการบรรยายที่รู้จักกันทั่วไปในชื่อ "ATM Jackpotting" (ดูรูปที่ 1) ทำให้ชาวโลกได้เรียนรู้ว่าเครื่องเอทีเอ็มไม่ปลอดภัยจากแฮกเกอร์อีกต่อไป (ปัจจุบัน Mr. Barnaby Jack ได้เสียชีวิตไปแล้ว ณ กรุงซานฟรานซิสโก เมื่อปี ค.ศ. 2013)

No.1 "ATM Jackpotting" Hacking Show in Las Vegas, 2010

เหตุการณ์มัลแวร์ที่เกิดขึ้นกับเครื่องเอทีเอ็มเป็นครั้งแรกของโลก เกิดขึ้นในปี 2009 โดยได้รับชื่อว่า "Skimer" โดยมัลแวร์ "Skimer" มีการแพร่ในช่วงปี ค.ศ. 2010-2013 แฮกเกอร์ชาวรัสเซียได้นำมัลแวร์ "Skimer" กลับมาใช้อีกครั้งหนึ่ง ซึ่งถูกตรวจพบโดย Kaspersky LAB เป็นเวอร์ชั่นใหม่ของมัลแวร์ Skimer ที่เข้าถึงเครื่องเอทีเอ็มโดยการเปิดเครื่องโดยตรง และเข้าถึงโดยผ่านทางเครือข่ายปิดภายในธนาคาร จากนั้นก็สั่งให้เครื่องเอทีเอ็มจ่ายเงินออกมา แต่ต่างกันที่มัลแวร์ Skimer แอบดักข้อมูล Credit Card ของลูกค้าธนาคารอย่างเงียบๆ (หน้าตาจอของมัลแวร์ Skimer ดูได้ในรูปที่ 2) มัลแวร์สั่งให้เครื่องเอทีเอ็มจ่ายธนบัตรออกมาครั้งละ 40 ฉบับ และยังเก็บข้อมูลใน CHIP และ PIN ของลูกค้าที่มาใช้เครื่องเอทีเอ็มอีกด้วย ข้อมูลเหล่านี้ถูกนำไปสร้างบัตรเครดิตปลอมไปกดเงินต่อได้อีก จะเห็นได้ว่า มัลแวร์ Skimer สามารถ Skim หรือดักข้อมูลลูกค้าของธนาคารได้โดยไม่ต้องติดตั้ง Hardware Skimmer แต่อย่างใด และมีการแพร่หลายไปยังผู้ผลิตเครื่องเอทีเอ็ม



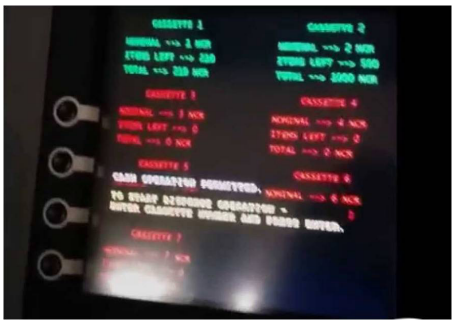
No.2 Skimer ATM Malware Gets Updated, Turns ATMs into Skimming Machines

หลายๆ ยี่ห้อทั่วโลก โดยพบที่ UAE, France, USA, Russia, Macao, China, Philippines, Spain, Germany, Georgia, Poland, Brazil และ Czech Republic

จากเหตุการณ์มัลแวร์ Skimer ช่วงปี ค.ศ. 2013-2014 ตามต่อมาด้วยการค้นพบมัลแวร์อีกตัวที่โจมตีเครื่องเอทีเอ็มเช่นกัน มัลแวร์ตัวนี้มีชื่อว่า Tyupkin ถูกค้นพบโดย Kaspersky LAB ในปี 2014 ในเครื่องเอทีเอ็มแถบยุโรปตะวันออก และยังแพร่ไปยังสหรัฐอเมริกา, อินเดีย และจีน อีกด้วย (ดูรูปที่ 3) มัลแวร์จะทำงานบนระบบปฏิบัติการ Windows 32 บิท ในช่วงเวลากลางคืนเท่านั้น พบว่าแฮกเกอร์ใช้กุญแจผีไขเครื่องเอทีเอ็มและนำ CD-ROM ไปบู๊ตเครื่องคอมพิวเตอร์ในเครื่อง โดยมัลแวร์จะทำให้เครื่องเอทีเอ็มจ่ายเงินออกมาเป็นธนบัตรครั้งละ 40 ฉบับ เช่นกัน มัลแวร์ Tyupkin เป็นต้นแบบของการโจมตีเครื่องเอทีเอ็มโดยไม่จำเป็นต้องโจมตีเครือข่ายของธนาคารหรือดักข้อมูลของลูกค้า แต่โจมตีไปที่ตัวเครื่องเอทีเอ็มโดยตรงเลย จากช่องโหว่ทางกายภาพของตัวเครื่อง และช่องโหว่ทางด้านระบบปฏิบัติการและการป้องกันการเข้าถึงเครื่องคอมพิวเตอร์ภายในเครื่อง

เมื่อเดือนกรกฎาคม ค.ศ. 2016 ที่ผ่านมา เครื่องเอทีเอ็มในประเทศไต้หวันเพิ่งถูกแฮกค์ไปทั่วประเทศเช่นกันโดยมีความสูญเสียถึง2.5ล้านเหรียญสหรัฐ พบว่าเป็นฝีมือของแฮกเกอร์ชาวยุโรปตะวันออกและรัสเซีย ซึ่งเป็นครั้งแรกในประเทศไต้หวันที่มีเหตุการณ์โจมตีเครื่องเอทีเอ็มทั่วประเทศในลักษณะแบบนี้ ทำให้ธนาคารต้องหยุดให้บริการเอทีเอ็มกว่า 1,000 เครื่อง สืบเนื่องกับเหตุการณ์ที่เกิดขึ้นในประเทศญี่ปุ่น ก็มีการโจมตีเครื่องเอทีเอ็มเช่นกัน แถมยังใช้เวลาแค่เพียง 3 ชั่วโมงแต่สร้างความเสียหายสูงถึง1.4พันล้านเยน(12.7ล้านเหรียญสหรัฐ) เกิดขึ้นกับเครื่องเอทีเอ็มตามร้านสะดวกซื้อ 1,400 เครื่องเมื่อวันที่ 15 พฤษภาคม ค.ศ. 2016 เวลา 05.00 AM — 08.00 AM เพียง 3 ชั่วโมงเท่านั้น โดยมีการโจมตีด้วยวิธี Hardware Skimming รวมทั้งการปล่อยมัลแวร์เข้าโจมตีเครื่องเอทีเอ็มและยังนำบัตรเครดิตปลอมที่แฮกค์ได้จากแอฟริกาใต้มากดเงินอีกด้วย โดยจำนวนอาชญากรมีถึง100 คนร่วมกันถอนเงินครั้งใหญ่ ถือว่าเป็นครั้งแรกในญี่ปุ่นเช่นกันที่มีเหตุการณ์แบบนี้เกิดขึ้น

4. เฝ้าระวังการทำงานของเครื่องเอทีเอ็มผ่านเครือข่ายภายในของธนาคารแบบ 24 X 7 เพื่อที่จะสามารถตรวจสอบความผิดปกติทางเครือข่ายภายในได้ตลอดเวลา
5. ทำการ Harden ปิดช่องโหว่ เครื่องคอมพิวเตอร์ที่อยู่ในเครื่องเอทีเอ็มทุกเครื่องโดยทำตามมาตรฐานความมั่นคงปลอดภัยขั้นต่ำที่เป็นมาตรฐาน หรือ ทำตาม PCI DSS Security Guidelines
6. เครื่องเอทีเอ็มควรอยู่ในที่สว่าง มีกล้อง CCTV คอยบันทึกภาพตลอดเวลา เจ้าหน้าที่ธนาคารหมั่นตรวจสอบความผิดปกติของเครื่องอยู่เป็นระยะๆ
7. ธนาคารควรตรวจสอบเงินสดในเครื่องเอทีเอ็มควบคู่กับการทำ Reconcile กระทบยอดทุกวัน
8. ธนาคารควรทำ Security Audit ด้วยการทำ Penetration Testing ระบบเอทีเอ็มครั้งใหญ่อีกครั้ง เพื่อให้มั่นใจในความมั่นคงปลอดภัยของเครือข่ายภายในธนาคารทั้งนี้เป็นการสร้างความมั่นใจให้ลูกค้าของธนาคารอีกด้วย



No. 3 Tyupkin Malware

2009	2010	2013	2014
Skimer 1st Gen	ATM Jackpotting	Plotus/Padin	SUCEFUL
2014	2015	2016	2016
Tyupkin	GreenDispenser	Skimer 2nd Gen	RIPPER

No. 4 Timeline ATM Malware from 2009-2016

นอกจากนี้ยังมีการค้นพบมัลแวร์ ชื่อ PLOUTUS และ PADIN ค้นพบโดย Symantec แพร่ในประเทศเม็กซิโก และ ในโซนเอเชียของเราก็มีการตรวจพบมัลแวร์ในประเทศมาเลเซียถูกโจมตีไปมีมูลค่าความเสียหายกว่า 3 ล้านริงกิต โดยมัลแวร์ PADIN เช่นกัน และยังตรวจพบอีกว่า คู่มือของเครื่องเอทีเอ็มชื่อดังรวมถึง เครื่อง point-of-sales และ เครื่อง self-service kiosk ถูกนำมาโพสต์ในเว็บไซต์ที่บริษัท Baidu เป็นเจ้าของการโจมตีในลักษณะนี้ ทำให้ธนาคารต้องให้ความสำคัญกับความปลอดภัยทางกายภาพ (Physical Security) ของเครื่องเอทีเอ็มมากขึ้น

8 แนวทางในการลดความเสี่ยงของธนาคารจากการถูกโจมตีเครื่องเอทีเอ็มในอนาคต

1. ต้องตรวจสอบความปลอดภัยทางกายภาพ (Physical Security) ของเครื่องเอทีเอ็มทุกเครื่องที่ธนาคารเปิดให้บริการอยู่ว่ามีความปลอดภัยเพียงพอหรือไม่ต่อการถูกโจมตีที่ตัวเครื่องเอทีเอ็มโดยตรง
2. ควรเปลี่ยนกุญแจเครื่องเอทีเอ็ม โดยไม่ใช้ Master Key ที่เตรียมให้โดยบริษัทผู้ผลิตเครื่องเอทีเอ็ม
3. ควรติดตั้งระบบเตือนภัยที่เครื่องเอทีเอ็มให้แจ้งเตือนการบุกรุกโดยอัตโนมัติ

กล่าวโดยสรุปจะเห็นว่าในปัจจุบันและอนาคตทิศทางในการเจาะและโจมตีเครื่องเอทีเอ็มของธนาคารนับวันจะเริ่มแพร่หลาย และมีความสลับซับซ้อนมากขึ้น ทำให้ธนาคารทุกธนาคารต้องอยู่ในสภาวะเตรียมพร้อม ควรมี Security Operation Center และ Incident Response Plan/ Incident Response Drill ให้พร้อมต่อการโจมตีอยู่เสมอ เพื่อสร้างความมั่นใจให้กับลูกค้าในที่สุด

Automatic teller machines, or widely-known as ATM's, have played a major and ever- increasing role in our everyday lives ever since 27 June, 1967 (even before the author of this article was born!), when the first ever ATM was installed and made available in London by the UK's Barclays Bank. Thereafter, they became popular and widely used everywhere throughout the world. With the ever-increasing popularity and widespread use of ATMs, cyber attacks on financial organizations have focused on hacking into their ATMs, and have become correspondingly widespread globally as well – such as, illegal cash withdrawals from ATMs by various groups of hackers that have recently caused much headache and problems for many banks around the world.

Let's look at and understanding the components of an ATM first

The key components of all ATMs are its Hardware and Software, which is used to connect the ATM to the respective internal banking network. Firstly, the Hardware: the characteristics and features of this key component will differ for the various respective makes of ATMs. The most widely seen and used makes of ATMs are: Diebold, Wincor Nixdorf and NCR, each with their respective differing designs and external appearances. However, the internal computer of all ATMs will be based on a Windows Operating System; while the internal safe (for storage of the cash) will have more security features and be well-protected than the internal computer in an ATM.

It is often found that the weakest feature of an ATM is the vulnerability to be affected by 'bugs' in its Windows Operating System that often occurs – which is no different for those PCs' being used in many homes or offices. Therefore, ATMs also have the opportunity to be affected by computer bugs or be attacked by malware. However, this vulnerability was not evident before and until recently, since ATMs have always been a part of a bank's 'closed' network. That is, up till 2010, when a young New Zealand hacker, named Barnaby Jack was able to demonstrate, publically on stage the Black Hat Computer Security Conference 2010 held in Las Vegas, that he was able to hack into an ATM. That demonstration in hacking into an ATM was widely seen globally and is known as "ATM Jackpotting" (Please see photo No.1), resulting in the general public becoming aware that ATMs are no longer as safe and secure from hackers as previously believed. (At present, Mr. Barnaby Jack has passed away in San Francisco since 2013,)

The very first incident of a malware attack on ATMs that occurred in 2009, which was referred to as an attack using a 'skimmer' malware. Such 'skimmer' attacks became more widespread during 2010 – 2013, when a Russian hacker again used such a 'skimmer' malware to attack ATMs, which was discovered by the Kaspersky LAB to be a new version of the 'skimmer' malware. This new version can access ATMs directly as well as through the bank's closed network, which then authorizes the ATM to dispense cash; whereby the difference is that this new 'skimmer' can also access and steal confidential data from credit cards of the bank's customers. (Please see a view of the 'skimmer' malware in Photo 2). This new malware authorizes the ATM to dispense 40 bank notes at a time, as well as store confidential data on a CHIP together with the confidential PIN code of a bank's customers who use the ATM. Such confidential customer information is used to create fake credit cards that are then used for making further cash withdrawals. It can be seen that this 'skimmer' malware is able to skim or access and steal confidential bank customers' information without the need to insert and install any Hardware Skimmer. It has also seen increased and widespread usage with many various makes of ATMs across the world - as has been found in the UAE, France, USA, Russia, Macao, China, Philippines, Spain, Germany, Georgia, Poland, Brazil and the Czech Republic.

From the many 'skimmer' malware attacks during 2013 – 2014, another type of malware was also discovered by the Kaspersky LAB in 2014 and called the 'Tyupkin' malware, and found to be used in attacking ATMs in Europe as well as on a widespread basis in the US, India, and China (please see Photo 3). This malware is used only at night time, through the Windows 32 bit Operating System. It was found that a hacker made use of a fake copy of a key to access the ATM and stole the CD-Rom that was then used to boot up the internal computer system, which also resulted in the malware authorizing the ATM to dispense 40 bank notes at a time. This 'Tyupkin' malware was the origin of many ATM attacks without the need to access the bank's network or skimming and stealing the customer's confidential data. Instead, it directly attacks the ATM itself, through using a weakness in the physical make up of the machine together with a vulnerable feature of its Operating System and a faulty security feature in preventing access to its internal computer system.

Additionally, other malwares – named PLOUTUS and PADIN – were discovered by Symantec, to be used on a widespread basis in Mexico. In our Asia region, the same PANDIN malware was found to be used in Malaysia where damages and losses of over 3 million Malaysia Ringit were incurred. It was also discovered that the operating handbooks of a well-known make of ATM as well as of point of sales devices and a self-service kiosk were posted on a website owned by Baidu. These malware attacks resulted in banks giving added attention to the physical security aspects of ATMs.

In July 2016, ATMs throughout Taiwan also began to be attacked by hackers with total damages and losses amounting to as much as US$ 2.5 million. It was found that the hackers were from Eastern Europe and Russia. It was also the very first time that such ATM attacks occurred in Taiwan in a similar manner throughout the country, which resulted in banks there having to stop providing their services through a total of 1,000 ATMs that was subsequent to a similar situation in Japan where such attacks on ATMs also occurred. Moreover, it only took 3 hours for the resulting overall damages and losses to total as much as Yen 1.4 billion (or equal to US$ 12.7 million), with over 1,400 ATMs located in convenience stores becoming affected by the attacks over only a brief period of 3 hours between 05:00 am to 8:00 am on 15 November, 2016. As such, the attacks were made by means of hardware 'skimming' together with making use of malware attacks on the ATMs. Also, hackers from Africa used fake credit cards to withdraw cash, with more than 100 perpetrators working together to withdraw massive amounts of cash. It was the first time ever that such an incident occurred in Japan.

8 Guidelines for Banks in reducing the risks of having their ATMs being attacked in the future.

1. Undertaking regular inspection of the physical security features of ATMs used in providing banking services to customers, so as to make sure whether or not their security and safety features are adequate to protect the ATMs from being attacked directly.
2. Keys for the ATMs should be changed from the master key as supplied by the ATM manufacturer.
3. An alarm system should be installed in the ATM, so as to automatically alert the bank of any irregular access or attack to the ATMs.
4. Be vigilant and always fully informed, on a 24 x 7 basis, of the actual operations of bank's ATM network via the bank's own internal system, so as to be always be able to assess any irregular incidents that may occur at all times.
5. Harden any potential weak points or vulnerabilities of the computer system being used within the ATMs at all times, through following and implementing the recommended basic security/safety features and operating standards, or through following the PCI DSS Security Guidelines.
6. ATMs should be installed in a well-lit location together with a CCTV system that can then always record their usage. Bank offi9cials should also always assess and check out any irregular incidents or situations on a regular basis.
7. Banks should check and verify the amount of cash in the ATM together with reconciling this with the daily transactions made.
8. Banks should undertake a Security Audit through a repeat major Penetration Testing of their ATM operations system, so as to be fully confident of the internal security and safety systems of the bank, which, in turn, will also enhance the confidence of its customers.

In summary, it can be seen that the current and future trends in stealthily accessing and attacking a bank's ATMs will both become increasingly widespread as well as more sophisticated and complex. As such, this will result in banks having to become much better prepared. Banks should establish their respective Security Operation Center and Incident Response Plan/Incident Response Drill, so as to always be well-prepared to face and deal with any possible attacks, as well as to ultimately establish increased confidence on the part of their customers.