GSB – Cyber Incident

The case study – ATM Hack in 2016

บุญสน เจนชัยมหกุล

รองผู้อำนวยการธนาคารออมสินอาวุโส

กลุ่มเทคโนโลยีสารสนเทศ

- เหตุการณ์จริงซึ่งเกิดขึ้นในประเทศไทย ช่วงเดือน สิงหาคม 2559
- รายละเอียดที่ได้สัมผัส ทำให้แตกต่างอย่างสิ้นเชิงกับการอ่านกรณีศึกษาที่เกิดขึ้นในต่างประเทศ
- การออกแบบแผนกอบกู้วิกฤติ โดยไม่เคยศึกษาเหตุการณ์ที่เกิดขึ้น อาจได้แผนที่ไม่สามารถใช้งานได้อย่างสมบูรณ์
- ท่านเคยเห็น แผนอพยพหนีไฟ แต่ท่านเคยหนีไฟจริงๆ หรือไม่

ATM Fraud & Hacking techniques

Skimming

Jackpotting

Hackers Made Bank ATMs To Spit Cash

ตู้ NCR ธนาคารออมสิน ปี 2559

สรุปความเสียหาย

21 ตู้

12,291,000 ล้านบาท


ธนาคาร
ออมสินแจ้งปิด!
ตู้เอทีเอ็ม 3 พันจุด
คนร้ายส่ง Malware
แฮกเงิน 12 ล้าน


ออมสิน
ATM
24 hours
ขออภัย
เครื่องขัดข้อง
ภาพจาก : มติชน

สำนักงานตำรวจแห่งชาติ

รู้จักกับ ปอท


TCSD
TCSD
Technology Crime Suppression Division
กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี

Hacker

สรุปเหตุการณ์

วันที่	เหตุการณ์
3 สค. 2559	เงินขาด จำนวน 3 ตู้ ในพื้นที่ ภูเก็ต ชุมพร
4 สค. 2559	เงินขาด จำนวน 2 ตู้ ในพื้นที่ ภูเก็ต และสุราษฎร์ธานี - ถอด Harddisk เก็บ Log, CCTV เพื่อตรวจสอบ - ปิดตู้ในพื้นที่ทั้งหมดเพื่อตรวจสอบ
5 สค. 2559	เงินขาด จำนวน 2 ตู้ ในพื้นที่ จ. เพชรบุรี - เก็บ Log เพิ่มเติม - นำเงินออกและปิดให้บริการ NCR ATM นอกสถานที่ 3,343 ตู้ - ATM หน้าสาขา นำเงินออกและปิดบริการ 18:00- เช้าวันรุ่งขึ้น
	สรุปความเสียหายทั้งสิ้น 21 ตู้ 12,291,000 บาท

การวิเคราะห์

NCR :

- ธนาคารออมสิน ต้องทำการติดตั้งระบบการป้องกันที่ Update ที่สุด

ธนาคารออมสิน :

- การป้องกันตามที่ NCR แนะนำ ยังไม่สามารถอธิบาย Scenario ได้ครบถ้วน
- การติดตั้งระบบการป้องกัน 4,000 เครื่องทั่วประเทศ ต้องใช้งบประมาณ และแรงงานจากผู้ให้บริการ และ ธนาคารจำนวนมาก จึงไม่ควรทำหลายรอบ

กิจกรรม

- วิเคราะห์สาเหตุของปัญหาร่วมกับ NCR (ไม่สามารถมีใครที่จะสามารถวิเคราะห์ได้ดีกว่า เจ้าของผลิตภัณฑ์)

- ส่งข้อมูลต่างๆ ให้กับ ปอท. เพื่อวิเคราะห์
  - ปอท. มีความรู้เรื่อง พิสูจน์หลักฐาน
  - ทีมงาน ธนาคารมีความรู้เรื่องเนื้อหาการใช้งานของอุปกรณ์ ระบบงาน และการเชื่อมโยงเครือข่ายสื่อสารต่างๆ

ข้อมูลประกอบการวิเคราะห์

- เกิดขึ้นกับตู้ NCR นอกสถานที่
- ถอนจากเครื่องครั้งละ 40,000 บาท
- ไม่ปรากฏ ร่องรอยใดๆ ใน Log ภายในตู้
- ไม่มีความเสียหายต่อลูกค้าธนาคาร
- คาดว่า เป็นการดำเนินการในยามวิกาลเท่านั้น
- ATM ที่เกิดเหตุ ไล่เรียงจาก จ.ภูเก็ต ตามเส้นทางจนถึง จ.เพชรบุรี และสนามบินดอนเมือง
- มีภาพคนร้ายชัดเจน
- มีทะเบียนรถ (เช่าจากภูเก็ต ไม่มีหลักฐานผู้เช่า)

คาดเดาวิธีการ

- มีทีมงานที่เตรียมความพร้อมก่อน (ติดตั้งโปรแกรม เชื่อมโยงตู้เข้าสู่เครื่อง ATM ที่ภูเก็ต ซึ่งทำหน้าที่เป็น Server ปลอม)
- เข้าทำรายการ โดยบัตรหมายเลขพิเศษ
- ถอนต่อเนื่องครั้งละ 40,000 บาท (ปรกติลูกค้าถอนได้สูงสุดเพียง 20,000 บาทต่อครั้ง
- ลบข้อมูล
- เดินทางต่อ

ทำไมเฉพาะตู้ NCR ธนาคารออมสิน

- ธนาคารออมสินติดตั้ง 4,000 ตู้ จาก 7,000 ตู้ ส่วนใหญ่ นอกสถานที่
- ธนาคารไทยพาณิชย์ มี 2,000 ตู้ จาก 12,000 ตู้
- ธนาคารอื่น มีแต่ธนาคารขนาดเล็ก จำนวนตู้ไม่มาก

แนวทางในการป้องกัน

- NCR ยืนยันว่า ต้องทำการติดตั้งโปรแกรมล่าสุดอย่างครบถ้วน
- ผู้ให้บริการเครือข่าย ยืนยันว่ามีการป้องกันอย่างเต็มที่
- ธนาคารต้องการคำตอบที่ชัดเจนกว่านี้
  - หากสิ่งที่ระบุไว้ ป้องกันได้ เหตุการณ์ที่เกิดขึ้น สามารถอธิบายได้ครบถ้วนหรือไม่
- หาก NCR ไม่สามารถหาคำอธิบายได้ NCR คือผู้กระทำความผิด
  - บัตรทดสอบพิเศษ ซึ่งมีอยู่ใน ห้อง Lab เท่านั้น

ธนาคารอื่นๆ

- บางธนาคาร รีบดำเนินการปิดตู้ ATM NCR เมื่อทราบข่าวในทันที
- บางธนาคาร แจ้งผู้บริหารว่า ธนาคารออมสิน ไม่ได้ทำการป้องกันความปลอดภัยที่เพียงพอ
- ผู้บริหาร หน่วยงานกำกับ ผู้เชี่ยวชาญด้าน Cyber บางท่าน กล่าวโทษธนาคารออมสิน ถึงการป้องกันความปลอดภัยที่ไม่เพียงพอ (ไม่รู้ ชอบพูด กลัวตกขบวน)
  - ทีมงานตรวจสอบ ของ ธปท เข้าร่วมการวิเคราะห์สาหตุของธนาคารออมสินร่วมกับ NCR ในทุกประชุม และเก็บความลับ โดยแจ้งเฉพาะส่วนที่เกี่ยวข้องกับผู้บริหารที่เกี่ยวข้องเท่านั้น (Need to know basis)

สาเหตุหลัก

- คนร้ายสามารถเข้าถึง รหัสสูงสุดของ ระบบควบคุมเครื่องด้านการปรับปรุงโปรแกรมที่ตู้ (Software Distribution) ซึ่งทำการรับส่งข้อมูล
- GPRS (3G) Router ของทุกรายไม่มีการปิดช่องโหว่นี้ ทำให้สามารถเชื่อมโยงสู่ Server ปลอมได้ (ทุกธนาคารจะกำหนดให้มีการเชื่อมโยงกับระบบงานกลางได้เท่านั้น)
- เกิดได้กับทุกธนาคารที่ใช้ NCR และใช้การเชื่อมโยงเครือข่าย GPRS (3G) Router

ระบบงานลักษณะเดียวกันของ NCR มีราคาสูง จึงทำให้ NCR มีนโยบายซื้อโปรแกรมที่ทำงานในลักษณะเดียวกันนี้ จากประเทศมาเลเซีย และใช้กับลูกค้าใน Asia Pacific

NCR Security Awareness

DATE: August 29, 2016 **INCIDENT NO:** 2016-12 **REV:** #99

Malware attacks in Thailand

Summary

NCR is actively responding and investigating an attack on NCR ATMs associated with a single financial customer in Thailand.

Attackers are using network access points to connect to the bank's internal network and connect to ATMs locally.

This is a network attack. The attackers have breached the Financial Institutions internal network. Once inside the network, the attackers are spoofing the software distribution server as the means to deliver the malware to ATMs (Please note: In this case, the attack is performed on SDMS Version 2.3.0 from InfoMindz and at this time, we have no information regarding other versions of this software).

Network attacks are not new and are not unique to NCR ATM's, however this attack represents a newer variation of the network attack vector. Analysis of the malware indicates that it also targets other ATM vendors.

อื่นๆ

- สิทธิบัตรทางปัญญา
  - มีรายละเอียดอย่างครบถ้วนเพียงพอที่ Hacker ทำการศึกษา
- เครื่อง ATM สามารถขายให้กับใครก็ได้ (White-Label ATM)

บทเรียน : ทุก Incident มีความหมาย

- มีเหตุการณ์ในลักษณะเดียวกันเกิดขึ้นก่อนหน้านั้น จำนวน 1 ตู้ ที่จังหวัดพังงา ในเดือน มีนาคม 5 เดือนก่อนเกิดเหตุการณ์ ตั้งข้อสมมุติฐานว่าเป็นการลักลอบนำเงินออกจากตู้ โดยผู้ให้บริการ (ช่าง, เจ้าหน้าที่เติมเงิน)
- ไม่มีข้อมูลเพียงพอต่อการวิเคราะห์

Learning

- Cyber Drill
- Forensic need in depth knowledge
- Information Sharing is KEY
- Cyber Insurance