VISA Payment Fraud Disruption Technical Analysis

AUGUST 2016

ATM JACKPOTTING MALWARE ALERT

Distribution: Visa Issuers, ATM ISOs, Processors, Third-Party Servicers and Acquirers

Summary: Since July 2016, Visa has received reports of an ATM "Jackpotting" incident targeting ATMs in the Asia-Pacific region. To date, according to public reporting surrounding the incident investigation, four malware file names and three file hashes associated with the malware have been identified. Visa continues to analyze these indicators of compromise (IOCs) associated with this recent incident. While these IOCs are specifically associated with an investigation involving ATMs in the Asia-Pacific region, Visa notes that the methods employed by the criminals in this incident represent a broader criminal threat to ATM manufacturers/models worldwide and their deployers.

> *ATM "Jackpotting" refers to the use of malware, launched via an executable file in order to target an ATM, that allows the attacker to empty the ATM cash cassettes via direct or remote manipulation by using the malware to submit commands to the ATM.*

1. Indicators of Compromise associated with Asia-Pacific Incident

In the July 2016 incident, investigators identified at least four different files associated with the malware used to conduct the attack:

File	MD5 Hash	Description
cnginfo.exe	658B0502B53F718BD0611A638DFD5969	to "read" and display information of the ATM operating system
cnginfo_new.exe	Unidentified	similar to cngdisp.exe, but potentially contains more robust capabilities than cngdisp.exe
cngdisp.exe	C0105ADA8686DC537A64919C73A18DB7	to execute the function of dispensing bills
sdelete.exe	C74673589D5DD38B6443DA6054B8DD7A	to delete the other two programs above. "sdelete" deletes the implanted files after the cash has been withdrawn
cleanup.bat	Unidentified	this batch file is used to command sdelete.exe to delete the executable files

The criminals included actions in their operation to delete traces of the attack, in order to prevent the bank from detecting irregularities in the ATM behavior.

It is important to note that the files employed as part of this incident could change (file name or file hash); thus it is just as critical to review the criminal methodology observed in this incident.

2. Criminal methodology associated with the Asia-Pacific Incident

According to reporting of the ATM Jackpotting incident in the Asia-Pacific region, Visa identified the following criminal methodology associated with this incident. While this methodology was associated with this incident, it could be employed to potentially target and compromise multiple manufacturers and ATM models worldwide. Further, although this attack targeted a Financial Institution, this attack vector could be launched from a processor or Third Party Servicer of ATMs.

1. The criminals initially compromised a vulnerable "telephone recording" system used by the targeted financial institution in order to establish network access. Details regarding the telephone recording system and its configuration are not available at this time.
2. The criminals used this network access to move laterally within the targeted bank's network, mapping out the network topology, and subsequently gaining access to a push update service utilized to deliver software updates across the network.
3. Criminals then use the update service to send malware to the target ATMs. The malware masquerades as a software update.
4. The criminals open and utilize the Telnet service to remotely command the infected ATMs and issue commands to empty the cash-carrying cassettes. Telnet is a both a network protocol and an application that uses that protocol. Most often, telnet is used to connect to remote computers and issue commands on those computers.
5. The malware was controlled during illegitimate withdrawals via the bank's network. There was no action required at the ATM except the collection of the money
6. In the final phase of the attack, the criminals delete (sdelete.exe) components of the malware employed in the attack.

Further, based on the methodology employed by the criminals in the Asia-Pacific incident, the criminals demonstrated a sophisticated approach to ATM Jackpotting.

- The targeting of a bank's network enabled the criminals to compromise multiple ATMs in a single attack. In more general jackpotting incidents, criminals target ATMs individually onsite in order to execute malware.

The incident in July 2016 demonstrated a sophisticated attack, in which criminals possessed a deep understanding and knowledge of the targeted bank's ATM operations. This was evident by the speed at which they traversed the network and implemented the malware.

- The criminals quickly deployed malware to multiple ATMs, in a targeted manner.
- The targeted bank ceased operations of all of its ATMs. This demonstrated that the criminals had access to the whole ATM network.

3. Visa recommends that Visa Issuers, ATM ISOs, Processors, Third-Party Servicers and Acquirers take the following actions:

1. **Check local networks for IOCs provided in this report.**
2. **Target System Environment and PCI DSS Requirements:** The malware likely operated within the Windows XP or Windows NT operating systems on the targeted ATMs.
    a. On 8 April 2014 Microsoft discontinued public patching for the Windows XP operating system.
    b. For all the merchants and ATM deployers currently using a POS/ATM system on Windows XP, not being able to apply security patches presents a serious threat to their overall security posture. Without security patches, these organizations are vulnerable to malware attacks.

c. It should be noted that PCI DSS requires that all system components and software are protected from known vulnerabilities by installing security patches, therefore the inability to receive and install security patches for Windows XP may jeopardize an organization's PCI DSS compliance. Visit the PCI SSC website for more information.
   i. Windows XP Support is ending
   ii. PCI FAQ 1130: Are operating systems that are no longer supported by the vendor non-compliant with the PCI DSS?
   iii. PCI Data Security Standard Quick Reference Guide
   iv. PCI Data Security Standard Requirements and Testing Procedures v3.2
   v. PCI ATM Security Guidelines

3. **Implement real-time monitoring of software activity on ATMs to ensure that suspicious activities or processes are identified.**
   a. Investigate suspicious activities like deviating or non-consistent transaction or event patterns which are caused by unauthorized system usage.
   b. Ensure real-time monitoring of security relevant hardware and software events.
   c. Introduce real-time checks in monitoring and application to detect tampering of the ATM
   d. Investigate suspicious patterns that can be identified remotely via monitoring such as unsolicited shutdown and restart of the ATM.

4. **Ensure that Intrusion Detection Systems (IDS) are updated to monitor for the methodology provided in this alert.**
   a. In addition, implemented IDS should allow for the identification of any deviating ATM system behavior from normal operations.
   b. Implement hard disc encryption and strong authentication (multi-factor authentication or integrity check controls) mechanisms to protect the ATM from software modifications initiated by external boot attacks (offline attacks).
   c. Lock down remote access and remote software update capability to ATMs to only authorized processes. Monitor and log when software updates are performed to ensure it is authorized and appropriate.
   d. Deploy an ATM specific solution to protect the software stack during runtime.
   e. Configure network firewalls to block Telnet services and ensure proper network segmentation between the ATM, bank network, and the Internet. IDS should also be used to monitor Telnet and other prohibited services as well.

5. **Follow network and information security best practices.**
   a. Ensure the security of ATMs and that ATM software is patched and up-to-date.
   b. Work with your ATM vendor to have the ATM vendor assist with deploying or recommended solutions to address overall ATM security and to ensure your ATMs are operating with the latest version of software
   c. For more information on controls and PCI DSS compliance, please refer to the PCI Security Standards, Data Security Standard version 3.2, reference guide
   d. Keep your software stack and your configuration up to date.
   e. Implement secure ATM installation and software delivery processes
   f. Follow network security best practices

For information please contact, **paymentintelligence@visa.com**