Visa Security Alert

AUGUST 2016

ATM CASHOUT MALWARE COMPROMISE IN SOUTHEAST ASIA

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

Summary: In late August 2016, Visa became aware of a recent ATM malware compromise in Southeast Asia and is providing indicators of compromise (IOCs) in order to enable security and incident response teams of financial institutions and ATM manufacturers to check and secure network environments. While these IOCs are specifically associated with an investigation involving ATMs in the Southeast Asia incident, 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.

Visa previously published a technical analysis on malware, including filenames, malware hashes, and criminal methodology involved in a separate ATM Jackpotting incident in the Asia-Pacific region. While there are similarities between the two events, this notification serves to highlight key differentiators – including malware and methodologies - pertaining to the incident in Southeast Asia.

1. Indicators of Compromise (IOC) Associated with the Southeast Asia Incident

On 26 August 2016, FireEye published IOCs and details associated with a new ATM malware they have named, "RIPPER". Based on FireEye's initial review and subsequent analysis and correlation of information performed by Visa, it has been determined that RIPPER was in fact the malware involved in the Southeast Asia incident. The following IOC, detailed by FireEye, is associated with RIPPER:

File	MD5 Hash	Description
RIPPER	15632224b7e5ca0ccb0a042daf2adc13	Primary RIPPER ATM malware file, reportedly uploaded to Virus Total on 10 July 2016

Visa is also aware of other versions of RIPPER, identified previously as dbackup.exe. and is providing the associated IOCs below:

File	MD5 Hash	Description
Dbackup.exe	af8fcec7d9817ddc68e3d66fb9f1a540	Other version of RIPPER, identified as dbackup.exe
Dbackup.exe	b428c8af87e85522dc847f054f4d1e5f	Other version of RIPPER, identified as dbackup.exe
Dbackup.exe	c092bf1244c88b6e7e112e3614db79dc	Other version of RIPPER, identified as dbackup.exe

FireEye details how RIPPER will kill the dbackup.exe process – a process specific to a single ATM vendor, and replace the original executable binary under c:\\Windows\system32\ (if present on the system) with a copy of RIPPER. Visa believes that during the course of the incident in Southeast Asia, dbackup.exe was replaced by the newer version of the malware, RIPPER.

In addition to the primary file hash, it is important to highlight two general, distinct features of the malware:

- RIPPER is capable of specifically targeting multiple ATM vendors.
- Once RIPPER is installed on the ATM, it monitors the card insertions on the ATM looking for a specific card used by the cybercriminals. Once the criminal's card is detected, RIPPER will intercept the normal process, and instead of the ATM performing normal authentication with the host, the authentication process is bypassed entirely. RIPPER launches a menu feature with functions for the criminal to execute. This is a key difference from the previous incident in Asia-Pacific.

For additional details regarding RIPPER, refer to FireEye's 26 August 2016 analysis.

It is important to note that the malware employed as part of this incident could change (file name or file hash); thus it is just as critical to review Visa's recommendations in section three (3).

2. Criminal Methodology Represents Broader Cybercrime Threat

The cybercriminals used multiple attack methods to carry out this compromise.

- First, the criminals compromised an offsite ATM. The malware was loaded onto the ATM and a Software Distribution and Management Systems (SDMS) software was also installed on the initial offline machine to use as a jumping off point to propagate the malware.
- The malware propagated to other ATMs and the attacks were carried out using a spoofed SDMS server using an ATM client IP address and a Debian Linux system with a version of the same SDMS software.

According to media reports, the perpetrators allegedly exploited vulnerabilities in the ATMs' software by installing malware (dbackup.exe, RIPPER), which enabled them to withdraw the cash held by the machines. While the incident was a targeted attack, the malware could be duplicated and employed elsewhere to potentially target and compromise multiple manufacturers and ATM models worldwide. As discussed in the FireEye report, the RIPPER malware incorporated similar techniques previously observed in other ATM malware, specifically Padpin (Tyupkin), SUCEFUL, and GreenDispenser, suggesting that cybercriminals could effectively adopt similar malware capabilities.

The incident also demonstrates a sophisticated attack methodology, in which criminals possessed access and knowledge of the targeted ATMs, their operating systems, and general operations.

- The criminals deployed malware specific to the ATM vendor associated with the targeted bank.
- RIPPER requires an ATM card used by the criminals as a method of authentication.
- Finally, the criminals demonstrated a sophisticated approach to compromise multiple ATMs in a single compromise.

3. Mitigation Recommendations:

Visa recommends Issuers, ATM ISOs, Processors, Third Party Agents and Acquirers take the following actions to mitigate against these threats:

- **Check local networks for IOCs provided in this report.**
- **Verify the implementation of required security patches:** PCI DSS requires that all system components and software are protected from known vulnerabilities by installing security patches. Visit the PCI SSC website for more information.

- **Refer to Visa's *What to do if Compromised (WTDIC)* document, published August 2016:**
  - https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf

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

- **Ensure that Intrusion Detection Systems (IDS) are updated to monitor for the methodology provided in this alert.**
  - IDS should identify any unusual ATM system behavior that differs from normal operations.
  - 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).
  - 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.
  - Deploy an ATM specific solution to protect the software stack during runtime.
  - 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.

- **Follow network and information security best practices.**
  - Ensure the security of ATMs and that ATM software is patched and up-to-date.
  - Ensure ATMs are operating with the latest version of software
  - Work with the ATM vendors to address overall ATM security
  - Visit the PCI SSC website for more information on security requirements and best practices:
    - PCI FAQ 1130: Are operating systems that are no longer supported by the vendor non-compliant with the PCI DSS?
    - PCI Data Security Standard Quick Reference Guide
    - PCI Data Security Standard Requirements and Testing Procedures v3.2
    - PCI ATM Security Guidelines
  - Keep the software stack and configurations up to date.
  - Implement secure ATM installation and software delivery processes
  - Follow network security best practices

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

To report a data breach, contact Visa Fraud Control:

- Europe: Datacompromise@visa.com
- Asia Pacific Region, Central Europe/Middle East/Africa Region: VIFraudControl@visa.com
- U.S. and Canada: USFraudControl@visa.com
- LAC: LACFraudInvestigations@visa.com