Protect Your ATMs against Black Box attacks

vortex™
Helping banks reach out

Automated Teller Machines (ATMs) being the foremost point of contact for the customers with their banks, are vulnerable to a gamut of malware and logical attacks. "Black Box" is the most prevalent and sophisticated logical attack executed by the cyber-criminals to cash-out or jackpot the ATMs.

Attack Methodology

'Black Box' is a cash jackpotting attack on ATMs, executed with the help of an unauthorized device connected to the ATM which will replace the active core and act as the proxy core sending commands to the cash dispenser to dispense the cash.

1. Get access to top enclosure
2. Replace the core with an unauthorised device - Blackbox
3. Execute program and cash out the ATM
4. Replace the unauthorized device with the actual core

According to the survey conducted by the European Association for Secure Transactions (EAST), the number of black box attacks on the ATMs witnessed a significant increase of 269% in the first half of 2020 over the same period in 2019. Loss of one million euros reported to the banking community and this has a potential to increase to more alarming levels if left unchecked. Cyber-criminals are more active in executing numerous logical attacks on the ATMs. 'Black box' attacks must be considered as a very serious threat and security systems in place must be to the highest level.

EUROPEAN PAYMENT TERMINAL CRIME STATISTICS - SUMMARY

Terminal Related Fraud Attacks	H1 2016	H1 2017	H1 2018	H1 2019	H1 2020	% +/- 19/20
Total reported Incidents	10,820	11,934	6,760	10,723	3,631	-66 %
Total reported losses	€174m	€124m	€107m	€124m	€109m	-12 %

ATM related Physical Attacks	H1 2016	H1 2017	H1 2018	H1 2019	H1 2020	% +/- 19/20
Total reported Incidents	1,604	1,696	2,046	2,376	1,829	-23 %
Total reported losses	€27m	€12.2m	€15.1m	€11.4	€12.6	+11 %

ATM Malware & Logical Attacks	**H1 2016**	**H1 2017**	**H1 2018**	**H1 2019**	**H1 2020**	**% +/- 19/20**
Total reported Incidents	**28**	**114**	**61**	**35**	**129**	**+269 %**
Total reported losses	**€0.41m**	**€1.51m**	**€0.25m**	**€0.00m**	**€1.00m**	**N/A**

SOURCE: EUROPEAN ASSOSICIATION FOR SECURE TRANSACTIONS (EAST)

Protection against Black box attack – Dispenser Host Pairing and Encryption

ATMs can be protected from black box attacks through effective host pairing and encrypted communication between the ATM's core and the cash dispenser. Ecoteller® ATMs are equipped with a robust host pairing mechanism between the core and the cash dispenser. As a result of this, the Vortex cash dispenser will accept commands only from the core it has been paired with. In addition to this, the communication between the core and the cash dispenser is encrypted such that it is not possible to reverse engineer the communication between the core and the cash dispenser. Dispenser host pairing and encryption is a security module available with Vortex's Terminal Security Solution. As we witness an upsurge in the black box attacks on the ATMs, it will be a prudent measure to safeguard the interest of the banking community by deploying the highest level of security features in the ATMs.

CONNECT WITH US TODAY FOR A SECURE BANKING TOMORROW

Email: info@vortexindia.co.in