**Subject: Fraudsters using heat signatures of fingertips on keypads to crack passwords/PINs.**

## Threat Summary

A new attack technique is being used by fraudsters of cracking passwords/PINs (ATMs, POS machine, Smart doors with keypad locks, etc.) by examining heat signatures that fingertips leave on keyboards/screens while entering passwords, such frauds use combination of thermal imaging and Artificial Intelligence (AI).


*Fig. 01 – Sample normal image*

AI algorithms are used to accurately guess the passwords as per the snapped heat signatures. The brighter the area appears on the thermal image, the more recently it would have been touched. Using such correlations PINs/passwords are being cracked.

## Modus Operandi

- Fraudsters generally target ATMs which are unguarded and not surveilled properly with video cameras.
- Fraudsters wait for their victims to avail desired services (such as withdraw, submit or sending money). As soon as the victim vacates the ATM, the fraudster takes pictures/videos by using a thermal-imaging camera to record the heat signature of the keys touched to enter the PIN.

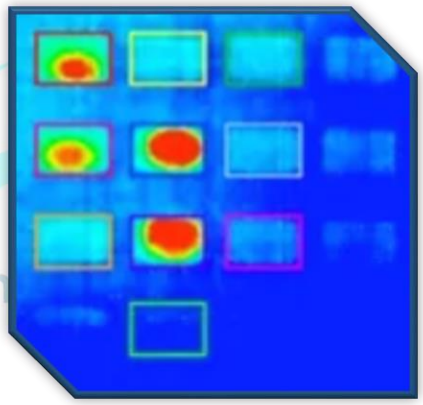

*Fig. 02 – Sample thermal image*

- Sometimes a camera is also placed inside an ATM for real-time capturing of heat signatures.
- The warmer the heat signal of an area (of a key) is, the more recently it was touched, which allows fraudsters to determine the possible PIN combinations.
- Smart doors using keypad locks and POS machines being used at various shops/restaurants are also vulnerable to such methods.

- Aforesaid method is generally used along with card skimming, hacking unsecured Wi-Fi networks (being used for payments/subscriptions), malware, phishing links, or data breaches, etc. by fraudsters for perpetrating such frauds.

## Suggestions

- Avoid using ATMs which are unguarded and not surveilled properly with video cameras.
- Always examine the ATMs for any suspicious attachments (in ATM rooms walls or the machine). Hide the keypad area while entering the PIN.
- Press multiple random number keys (buttons) before leaving the ATM machine/POS machine/Smart Locks to generate non meaningful heat signature.
- Properly check the SMSs and emails sent by your bank regarding any transactions properly, contact your bank instantly if a suspicious transaction is spotted.
- Report any such incidents on the *cybercrime.gov.in* portal and follow *@CyberDost* on Twitter, YouTube, Facebook, Instagram, Public, Koo and LinkedIn to know more about safety tips.

Regards,

Indian Cyber Crime Coordination Centre
CIS Division, MHA
011-23438207