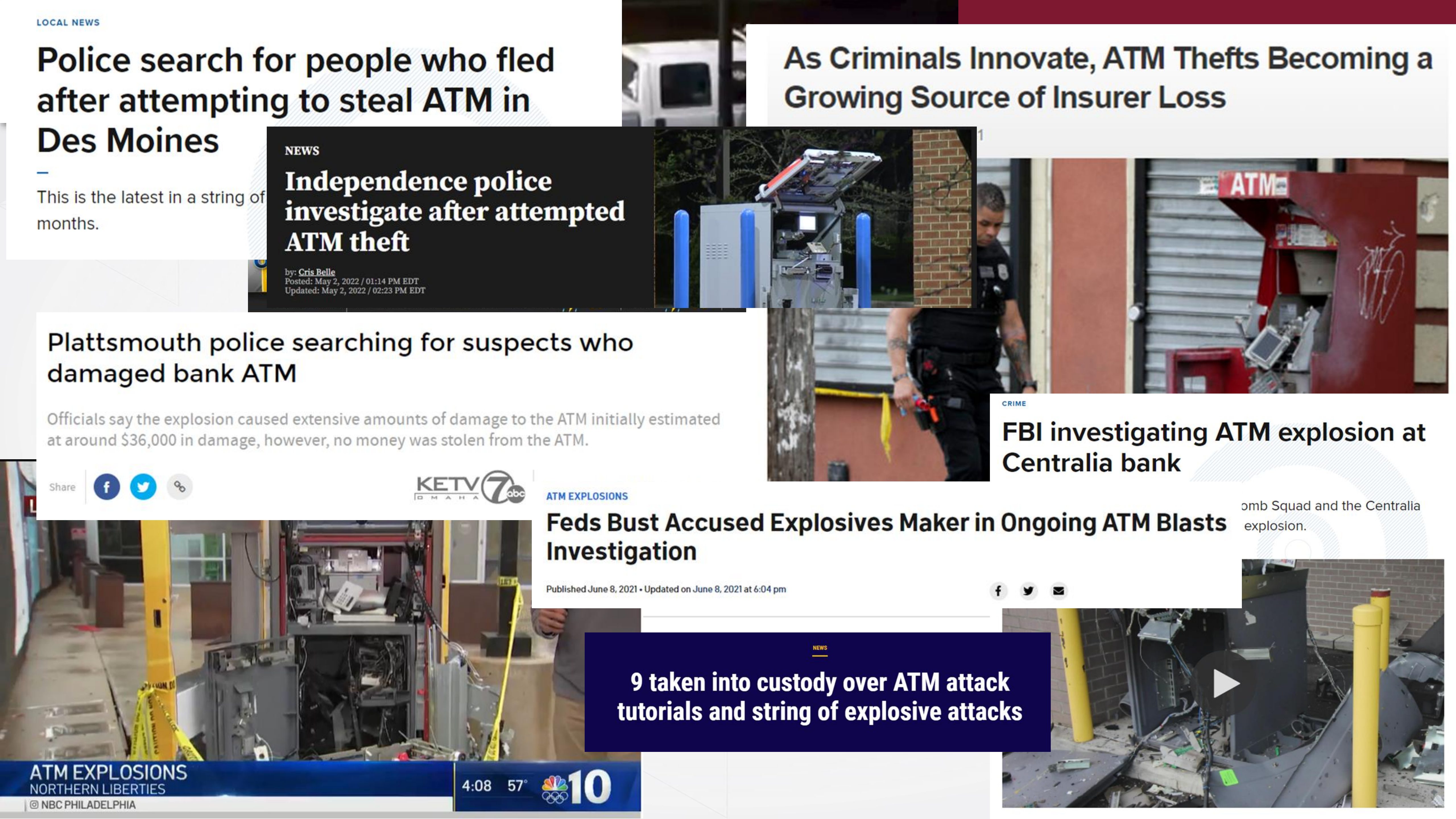
DBE
Data Business Equipment, Inc.

Cyber and Physical Security Threats

Paul Cowley – VP Technical Support and Logistics, DBE



LOCAL NEWS

Police search for people who fled after attempting to steal ATM in Des Moines

This is the latest in a string of
months.

As Criminals Innovate, ATM Thefts Becoming a Growing Source of Insurer Loss

NEWS

Independence police investigate after attempted ATM theft

by: Cris Belle
Posted: May 2, 2022 / 01:14 PM EDT
Updated: May 2, 2022 / 02:23 PM EDT

Plattsmouth police searching for suspects who damaged bank ATM

Officials say the explosion caused extensive amounts of damage to the ATM initially estimated at around $36,000 in damage, however, no money was stolen from the ATM.

Share

KETV 7 OMAHA abc

CRIME

FBI investigating ATM explosion at Centralia bank

omb Squad and the Centralia
explosion.

ATM EXPLOSIONS

Feds Bust Accused Explosives Maker in Ongoing ATM Blasts Investigation

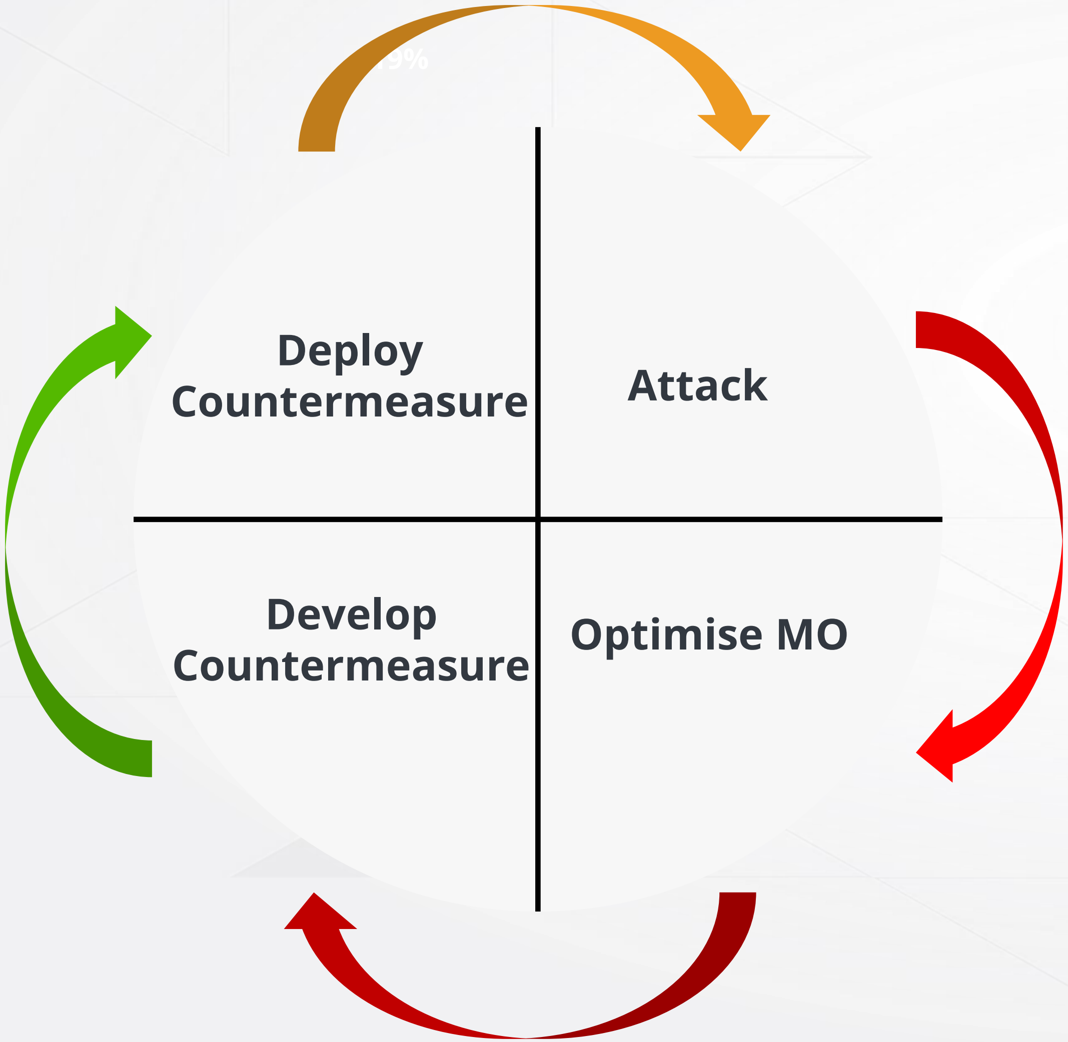
Published June 8, 2021 • Updated on June 8, 2021 at 6:04 pm

NEWS

9 taken into custody over ATM attack tutorials and string of explosive attacks

ATM EXPLOSIONS
NORTHERN LIBERTIES
4:08 57°
10
© NBC PHILADELPHIA

ATM Crime - Modus Operandi Evolution Cycle



Deploy Countermeasure

Attack

Develop Countermeasure

Optimise MO

4 phases of 'Attack / Countermeasure' cycle

- **1st and 2nd** phases – an attack vector may see many iterations until MO is optimised by the criminals – nearly limitless testing and no budget resource pressures as seen in industry
- **3rd Phase** – OEMs, Partners, and FIs developing protection
- **4th Phase** – deployment of countermeasure

- **Cycle begins again with a new attack vector**

DBE
Data Business Equipment, Inc.

ATM Attack Categories

Logical / Data Attacks

- Skimming
- Host Spoofing
- Eavesdropping
- Black Box
- Malware
- Data Loss/Compromise

Physical Attacks

- In-situ Tools
- Ram-Raid/Pull-Out
- Hook and Chain
- Jaws of Life
- Explosives
  - Gas
  - Solid

Jackpotting Malware

First observed in Mexico in early 2023

- ATM vendor-agnostic, referred to as FiXS
- Currently a known, active exploit against older Diebold machines

New iteration of previous malware, but works with the same MO as Ploutus (first observed in 2013)

- Typically introduced by physical access (e.g. USB stick or remove/replace HDD)
- Evolved to make the malware harder to reverse engineer and defeat

Logical Attacks – Jackpotting/Cash-out Malware

- Countermeasures include:
  - Harden the Operating System (OS)
  - Ensure monthly OS security updates are applied regularly
  - Lock down BIOS and machine configuration menus
  - Replace ATMs that have exceeded OEM support lifecycle
  - Upgrade software that has exceeded OEM support lifecycle
  - Ensure platform software is patched and updated regularly
  - Control physical access through monitored alarms
  - Deploy hard disk encryption and anti-malware solutions

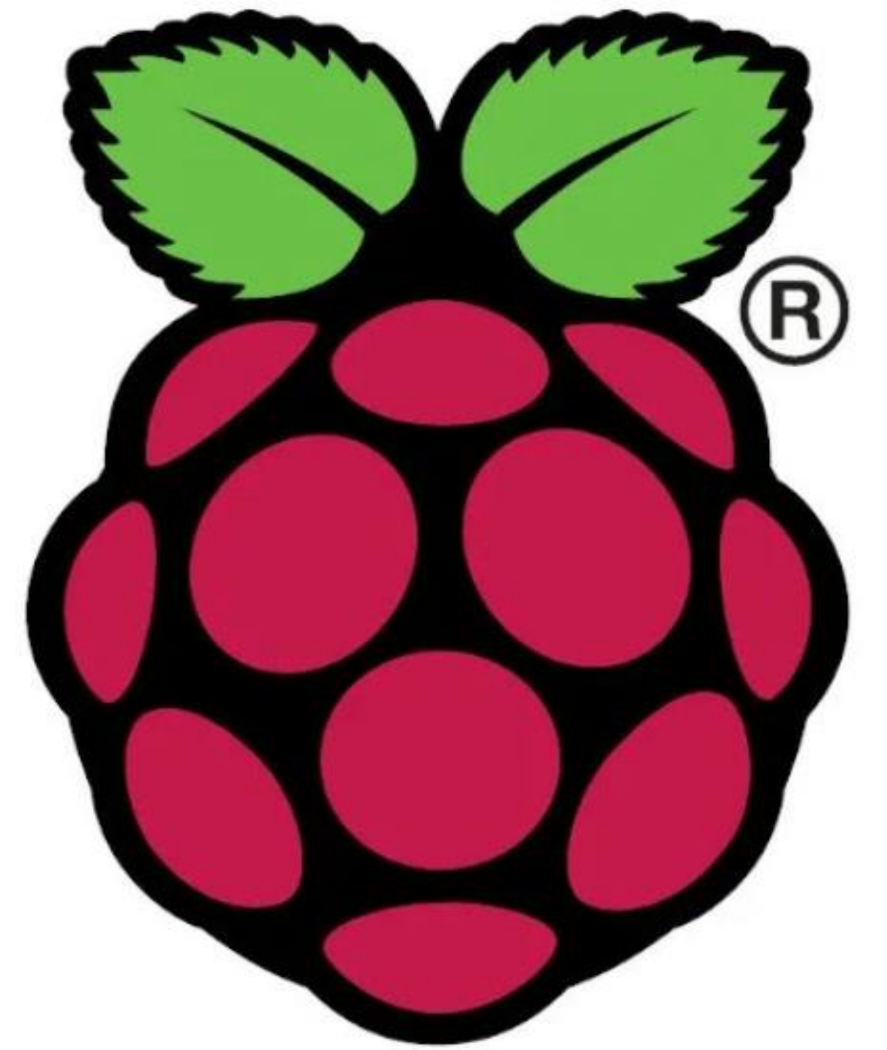
Host Spoofing / ‘Man-in-the-Middle’ (MITM)

Rapidly emerging threat since Q3 2023

- Currently targeting machines using NDC Host messaging
- First attacks observed in Texas mid-year 2023
- Known attacks confirmed across the US
- Results in a complete ‘cash-out’ of the ATM over 60-90 minutes

Access to the ATM ‘top box’ is obtained and the network cable is removed. A RaspberryPi SBC with custom software is connected in place of the network cable

- Frequently targeting smaller FIs
- Belief is that the bad actors assume a less-robust investment in security countermeasures by smaller FIs



Logical Attacks – Host Spoofing/’MITM’

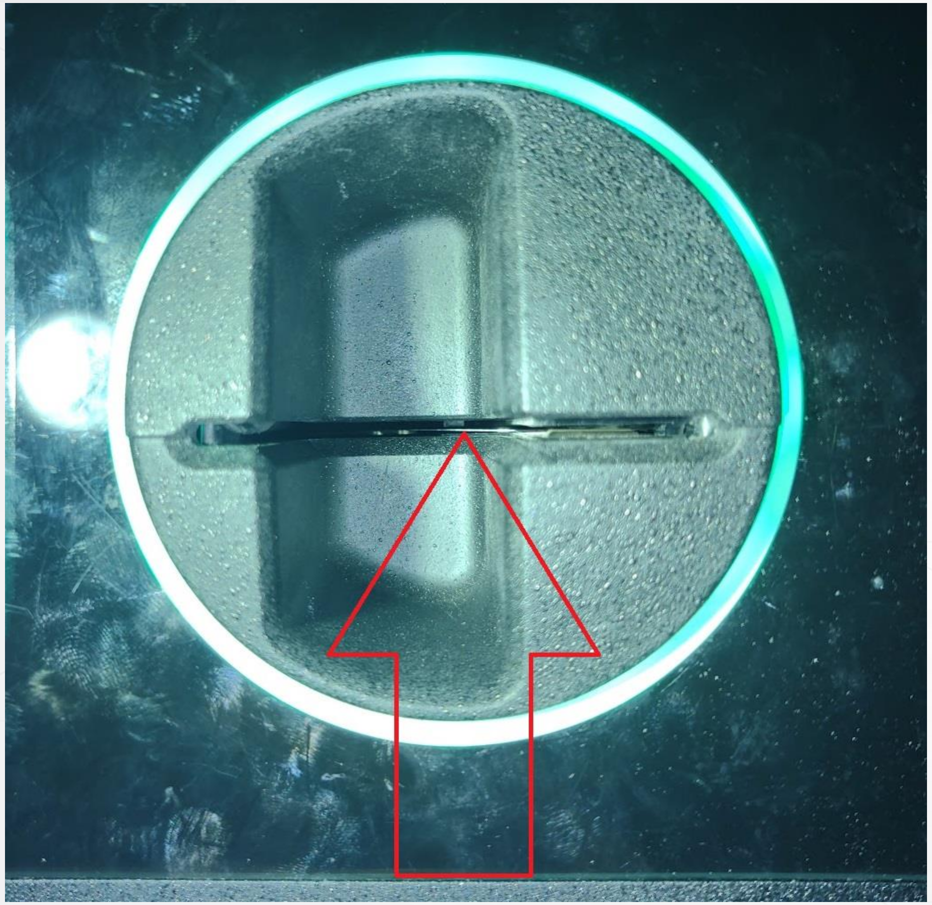
- Countermeasures include:
  - Enable end-to-end encryption on Host communications using TLS1.2
  - Control physical access to the ‘top box’ of the machine
    - Monitored alarms
    - Custom keying solutions
  - Protect network configuration menus with passwords
  - Utilize SHA-256/TR-34 and TR-31 protocols for encryption keys
  - Ensure monthly OS security updates are applied regularly
  - Ensure platform software is patched and updated regularly
  - Deploy hard disk encryption and anti-malware solutions

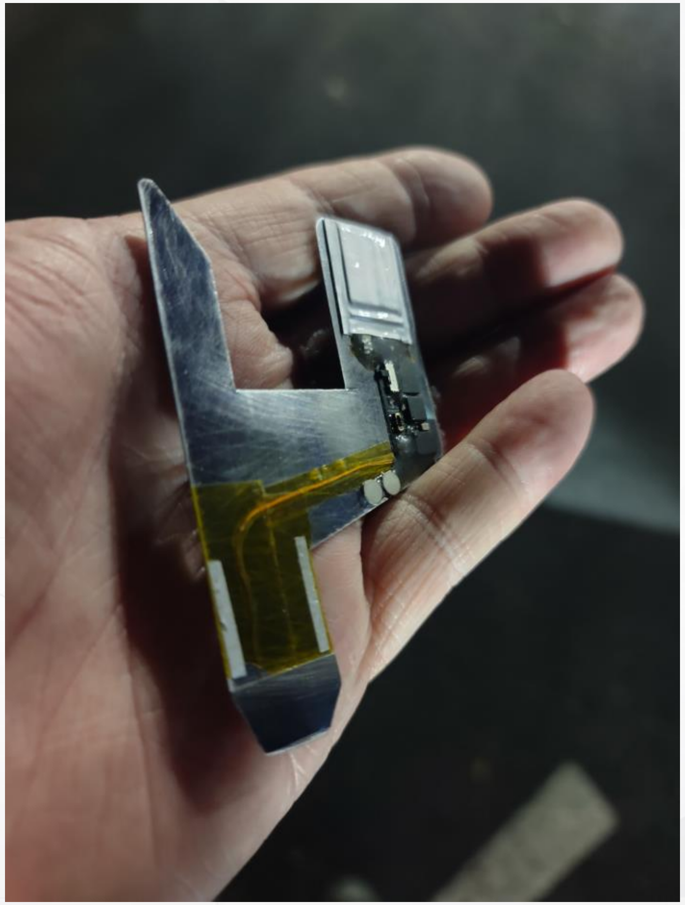
Logical/Data Attacks – Black Box

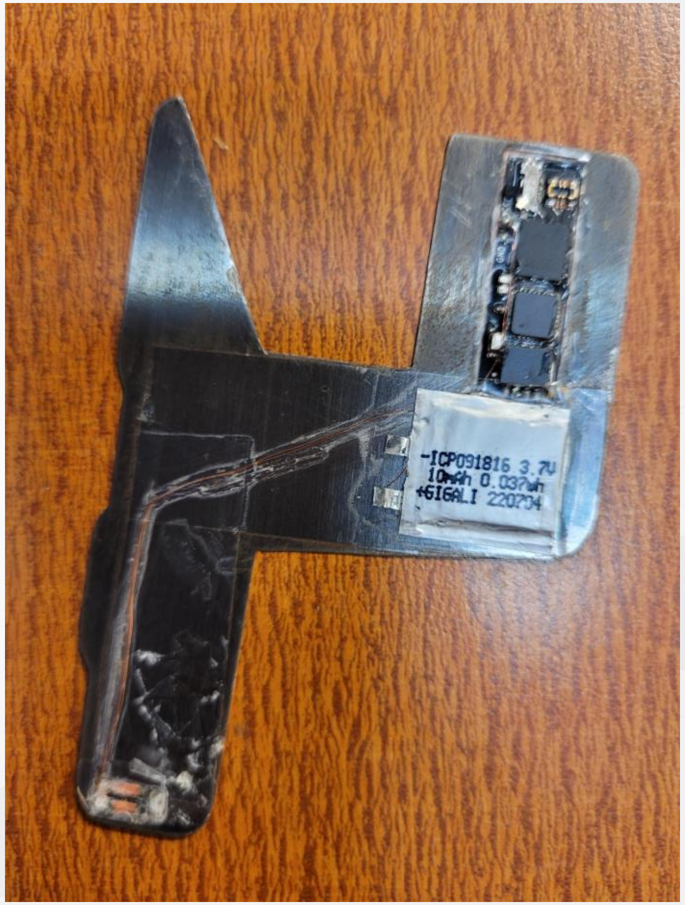
- Standalone electronic device that sends dispense commands directly to the cash dispenser

- Countermeasures include:
  - Replace ATMs that have exceeded OEM support lifecycle
  - Ensure platform software is current and patched/updated regularly
  - Ensure OEM dispenser authentication recommendations are being followed
  - Control physical access through monitored alarms

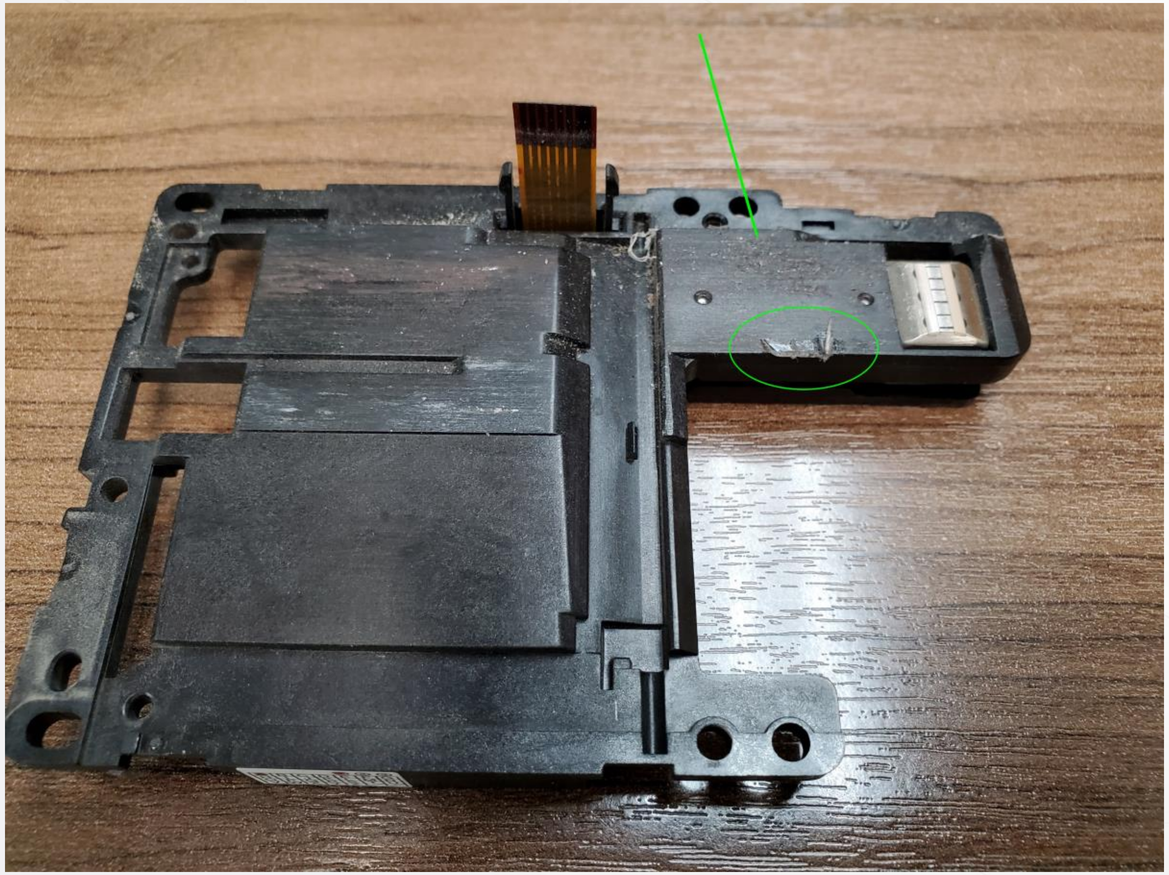
Ultra-thin Deep-insert Skimming Attacks

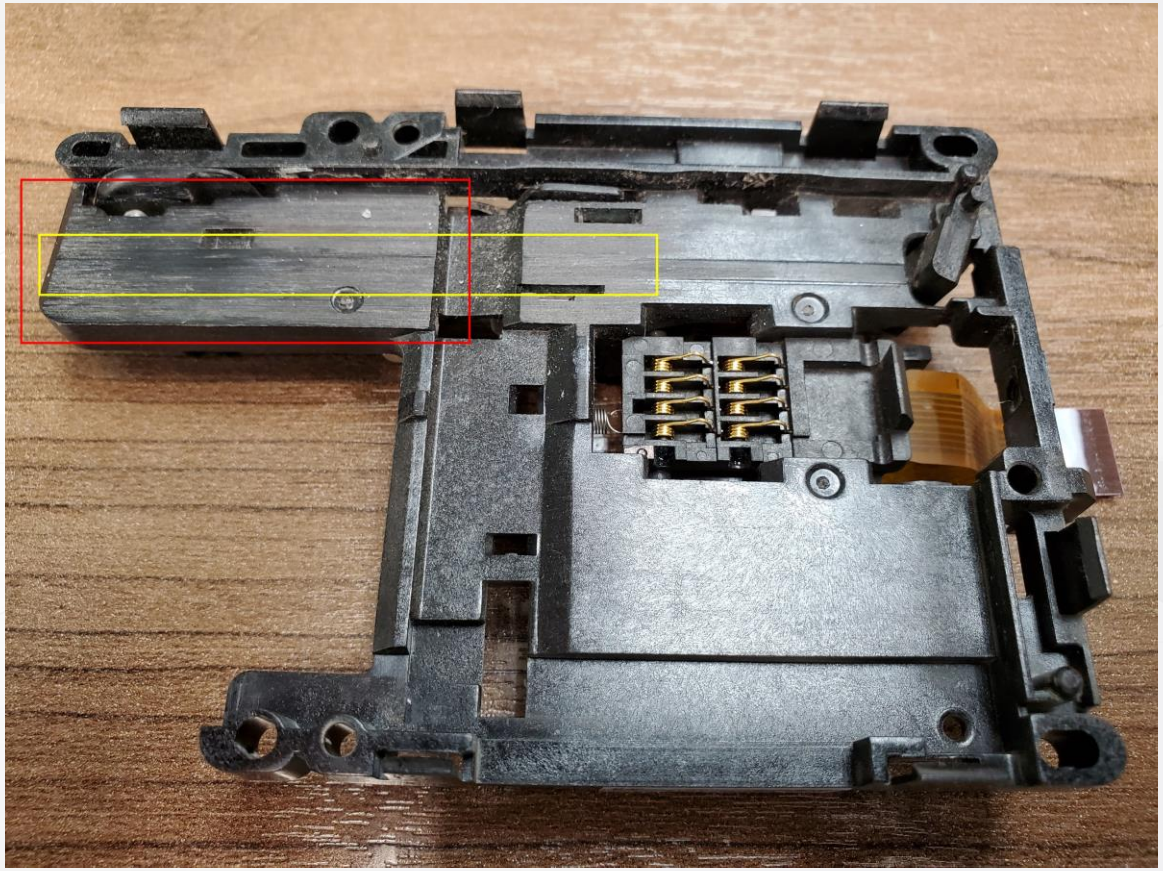




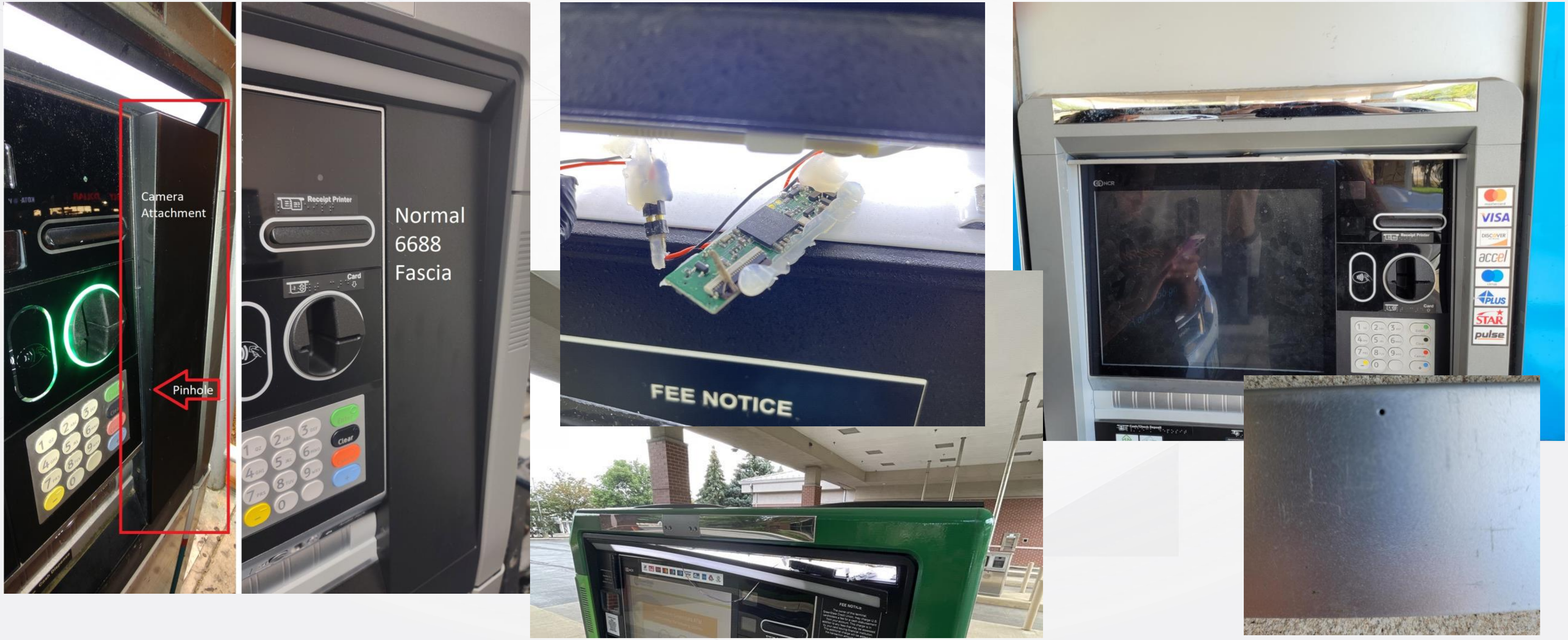


Ultra-thin Deep-insert Skimming Attacks





Ultra-thin Deep-insert Skimming Attacks



Tools to Stop the Skimming “Arms Race”

Card skimming remains a problem because it is too easy for a criminal to capture and reuse the static Track 2 data found on magnetic stripe cards

- Contactless EMV / NFC
  - Educate users about increased security offered by contactless transactions
  - Contactless EMV uses unique cryptograms in each transaction which cannot be reused if captured
  - The elimination of card insertion eliminates the opportunity for fascia AND deep-insert skimming
  - Disable EMV fallback transactions
- Tamper Detecting Card Reader (TDCR)
  - Devices as thin as 0.5mm so passive space restriction is no longer an effective countermeasure
  - TDCR is available as an in-place upgrade to all currently-supported NCR ATMs
  - Now a standard feature on all DBE-supplied ATMs manufactured after 8/1/2023
  - Software integration for TDCR detection capability requires Activate Enterprise 3.8 software
- Skimming Protection Solution (SPS)
  - Still the best-available option for preventing ‘overlay’ skimming

Physical Attacks

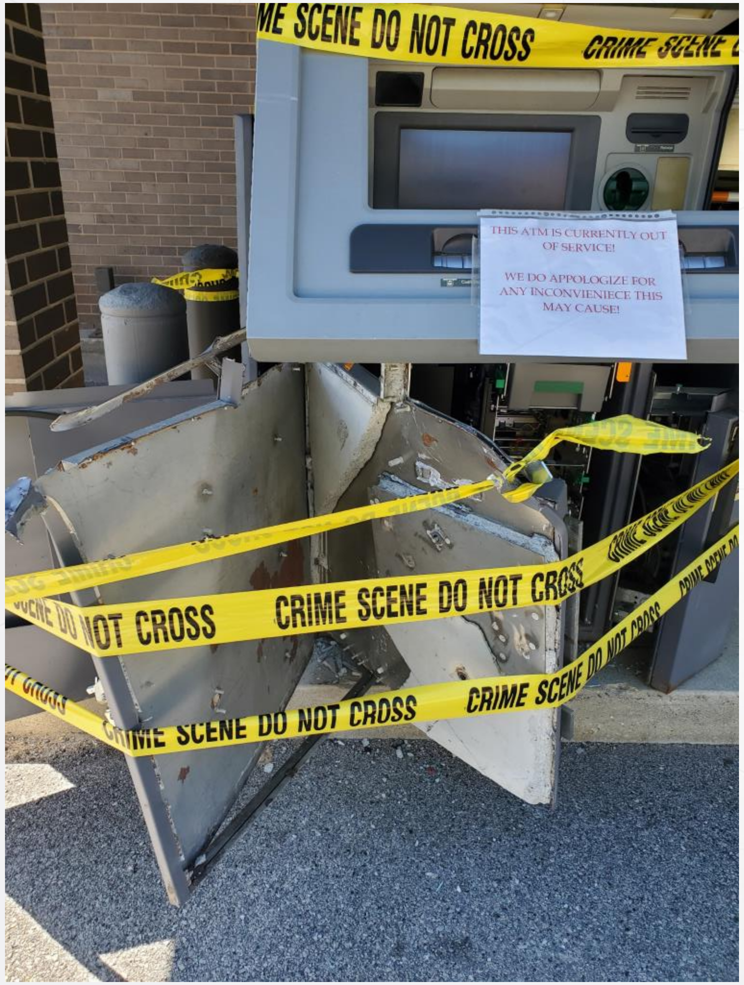
Physical Attacks

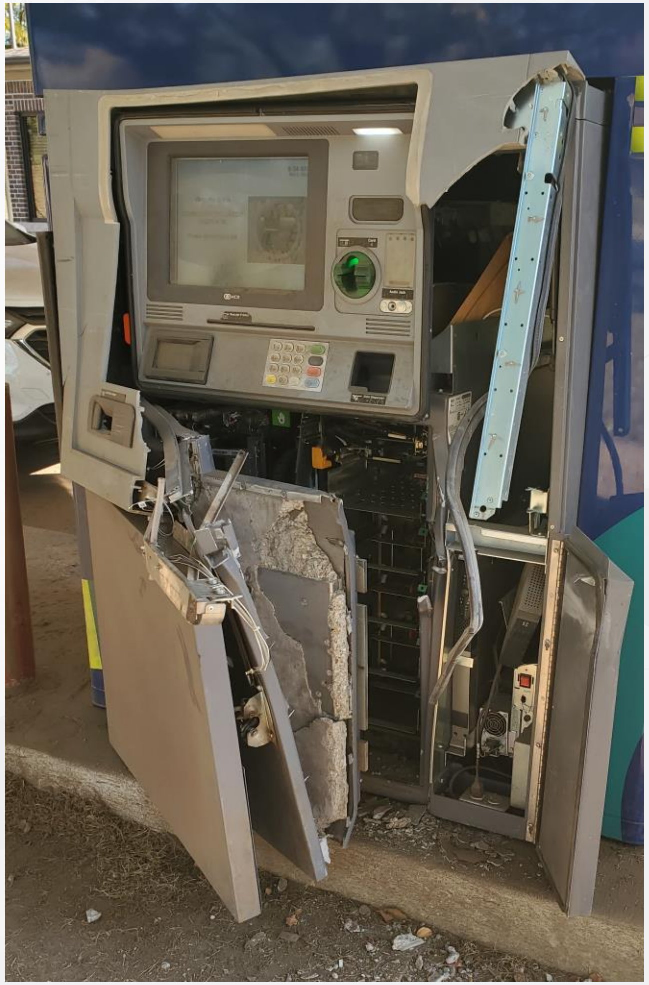
- In-situ Tools
- Ram-Raid/Pull-Out
- Hook and Chain
- Jaws of Life
- Explosives
  - Gas
  - Solid

‘Hook and Chain’ Attacks

- Brute-force attack STILL being widely employed across the US
  - Begins with the theft of a vehicle (typically medium-duty truck)
  - Typically targets older-generation island ATM/ITMs with sufficient site access
  - Utilizes heavy chain or cable to forcibly remove the safe door
  - Successful attacks against ALL makes, including Hyosung, NCR, and Diebold Nixdorf machines
- Average loss per incident is estimated at approximately $120k
  - Equipment, Safe Contents, and Site Damage

‘Hook and Chain’ Attacks

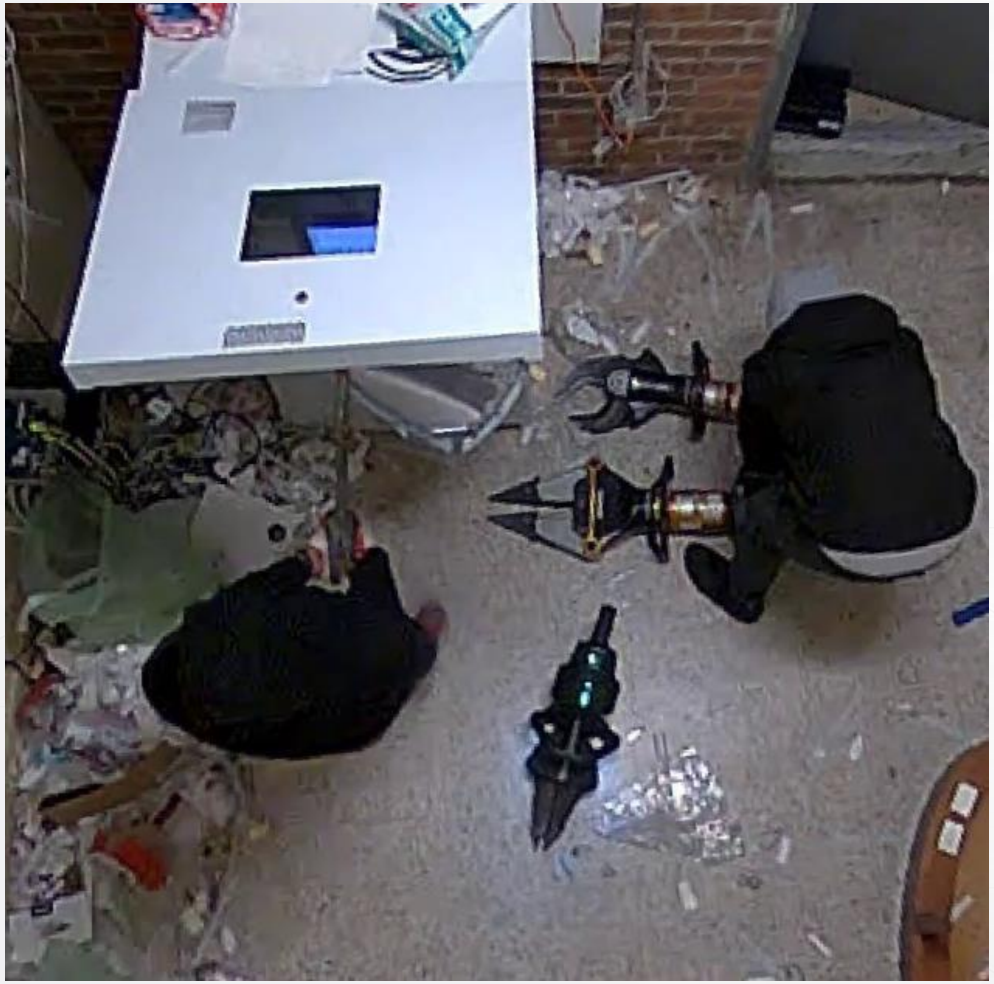

CRIME SCENE DO NOT CROSS
THIS ATM IS CURRENTLY OUT OF SERVICE!
WE DO APPOLOGIZE FOR ANY INCONVIENIECE THIS MAY CAUSE!

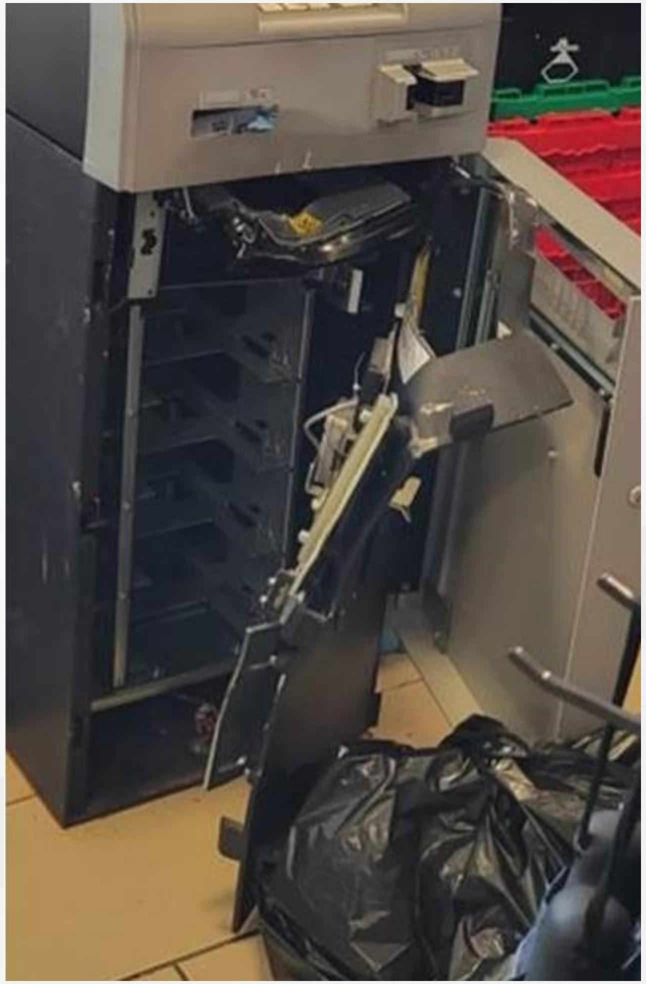


‘Jaws of Life’ Attacks

- Emerging attack being reported across the US
  - Begins with theft of hydraulically-powered public safety rescue equipment
  - VERY effective attack on UL Level 1 and Business-Hours rated security enclosures
  - Given enough time, even CEN-I rated vaults have been compromised

‘Jaws of Life’ Attacks



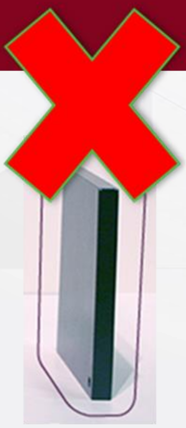


Physical Attack Countermeasures

- Deploy new machines with higher security ratings

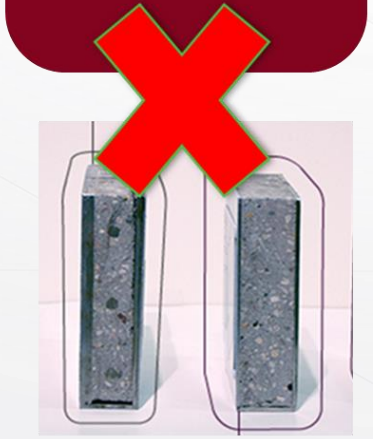
UL291 Level 1 (24 hour)

- Tested for door attack only
- 15mins (common mechanical tools)
- Lower grades uses "hand tools" only for attack testing
- Construction requirements defined in spec must be met
- High tensile steel walls
- Discontinued in favor of CEN safes



CEN L

- Steel door skin and steel outer shell filled with concrete composite mix
- Superior safe door with more resistance to thermal attacks
- Discontinued in favor of CEN I safes

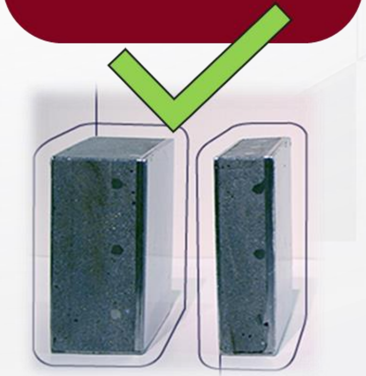


CEN I

- Body is the same strength as the door (CEN L standard allows a weaker body)
- Offers 66% more resistance to full access attacks and 50% more resistance in attacks to remove cassettes on the CEN I body
- Steel door skin and steel outer shell filled with concrete composite mix
- Body 40mm thick
- Relockers used in case of breach of lock to secure door
- One lock required and tested as part of the EN 1143-1:2019 standard
- Not designed to withstand explosive attacks
- Weight 478 kg
- Discontinued on island drive up units in favor of CEN III GAS-EX

CEN III GAS-EX

- Sheet steel outer and inner skin, with concrete in between.
- Additional grid-like reinforcement welded within inner body
- Concrete composite includes hardened particles
- Additional top and bottom bolts
- Additional hooking bolts to contain explosions but allow energy to expel
- Additional reinforcement of corners
- Offers 2 ½ more resistance to cutting attacks than CEN I
- Body 40mm thick
- Weight – 603 kg
- Same footprint as CEN I



Other Physical Security Considerations

- Adopt a layered and preventative approach to addressing physical attacks – BEFORE they happen
- Evaluate ATM locations and risk environments regularly
- Consider security impacts of site design whenever possible
- Install and maintain remotely-monitored alarms on both the ATM top box AND vault/security enclosure
  - Additional alarm zone on kiosk or building if ATM is through-the-wall
- Employ UL437-rated locks on cabinet doors
- Utilize high-security electronic locks for access to ATM safe
- Consider deploying IBNS (Intelligent Banknote Neutralization System) functionality

Q & A

Email: pcowley@dbeinc.com