Monetization of Financial Institution Attacks:

ATM Cashouts
ATM Jackpotting
Other Fraud

Murugesh Krishnan, Sr. Director, Franchise Risk Mgmt & Investigations

Penny Lane, VP, Payment Fraud Disruption

Continued Threat

ATM Cash-Out Fraud

- Accounts targeted can be debit, credit, prepaid
- Successful incident can result in significant losses
- Criminals are typically resident on targeted network for several months prior to fraud event
- Cashouts in all regions
- Groups consistent in their targeting methodology – learn the TTPs

Common Methods of Monetizing Bank Compromise

- Unauthorized Account Manipulation
- Payment Switch Compromise
- ATM Jackpotting
- Fraudulent SWIFT Transactions

Bank Account Administration Compromise

- Malware targets bank administrators
- Attackers use administrative access to manipulate fraud levels and withdrawal limits
- Allows dispensing large amounts of cash by using counterfeit cards with valid data

Anatomy of ATM Cash-out Attack

Limits increased

Payment Switch App Server Compromise

- Malware is targeted at financial institution's payment switch application server
- Malware intercepts transaction messages and approves all transactions for a given account range
- Allows for dispensing cash using counterfeit cards that lack valid or complete data

ATM cash-outs

x 1,400

x 120

US$19M loss

Source: Bank Info Security, "Lessons from ATM Cash-Out Scheme in Japan," May 25, 2016

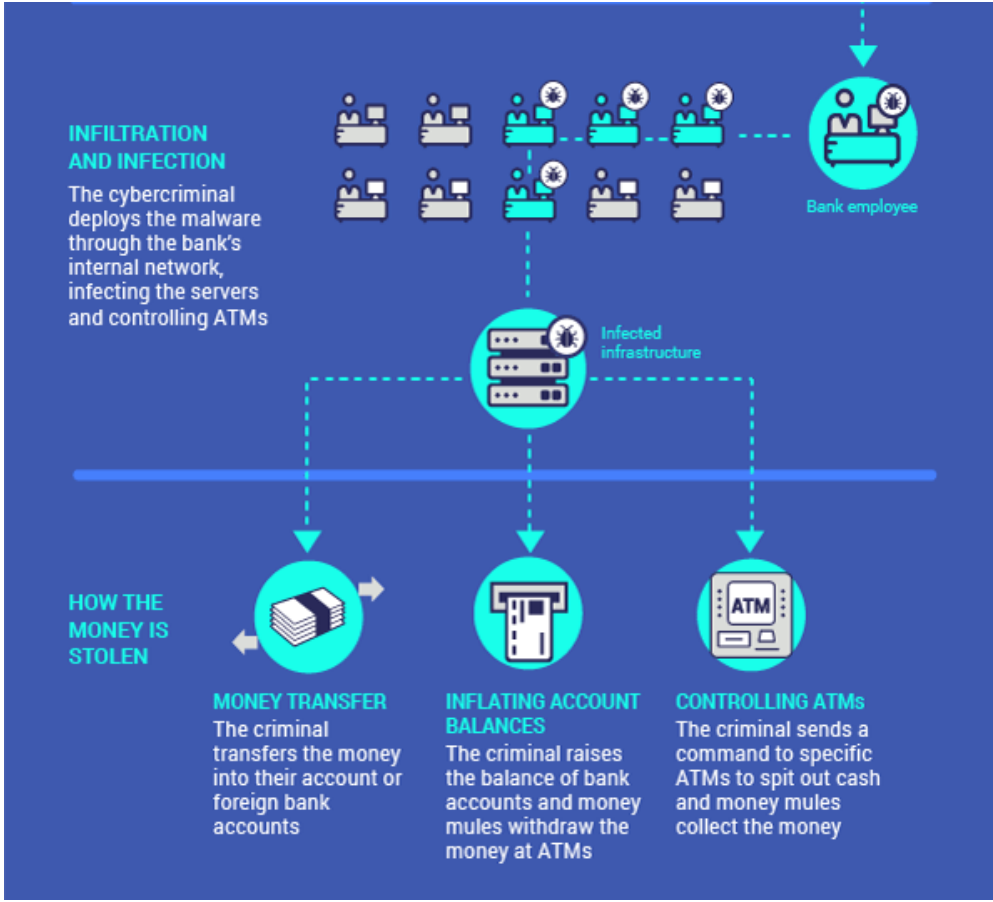
VISA

ATM Jackpotting

- Malware targets ATMs
- Initial intrusion can be the financial institution or directly at the ATM
- Allows direct control over the ATM
- Attackers can dispense cash without stolen card data

Cash-out Options

- A single infection can be leveraged for multiple cash-out methods
- The Carbanak / Cobalt group is known for using a variety of cash-out methods



Source: EUROPOL, "Carbanak / Cobalt", www.Europol.Europa.eu

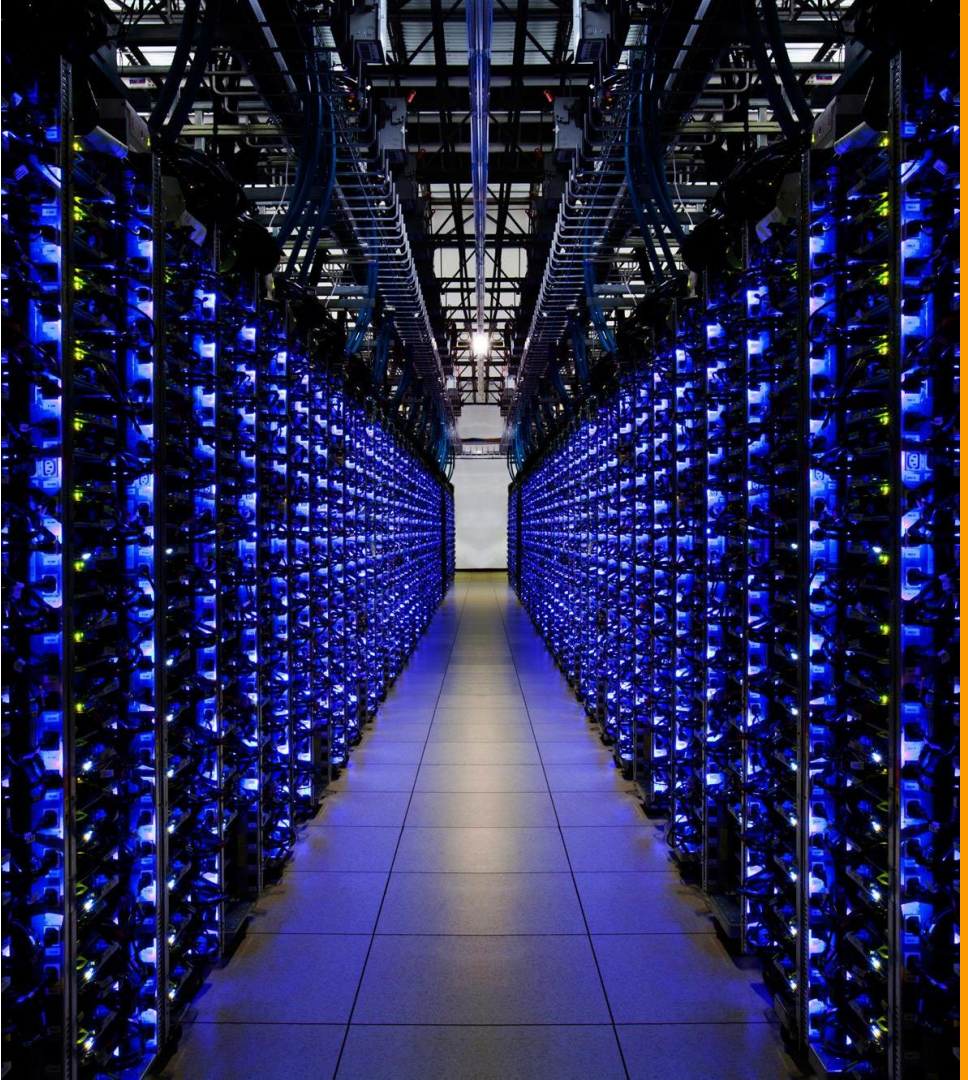
Unauthorized SWIFT Transactions

- Sometimes happens after an ATM cash-out is performed
- Typically very large dollar amounts per transaction
- Money is immediately transferred electronically

Disrupting Compromises

Protect and Defend

- Employee Phishing Training
- Strictly adhere to the PCI DSS
- Verify the implementation of required security patches
- Install and properly configure file integrity monitoring software
- Implement and practice incident response procedures **off hours**
  - A quick response and escalation when suspicious activity is identified can save millions of dollar. Every minute counts.
- Report suspicious activity immediately



How Visa Can Help

Visa monitors for and counters ATM cashout attempts for all VisaNet clients by employing sophisticated technical and analytical capabilities

Vital Signs Capability

- Real-time, global service
- Concise alerting and automated notification
- Ability to temporarily halt ongoing fraudulent withdrawals
- Continued optimization

Vital Signs Importance for Clients

- Independent complement of client defenses
- Reduces financial exposure associated with fraudulent cashout attempts
- Current 24x7 contact info in Client Directory is critical

Intelligence Alerting

- Visa Payment Fraud Disruption publishes intelligence alerts warning of ongoing threats to the payment ecosystem
- Alerts containing Indicators of Compromise (IOCs) to assist clients in identifying threats to their networks
- If any IOCs are identified on your network, refer to Visa's What to do if Compromised (WTDIC) document and take immediate actions to contact a possible infection
  - Reset passwords for users with access to critical payment systems
  - Initiate imaging of critical payment systems to preserve evidence for investigators

How Visa's intelligence and visibility helps stop attackers

- Capability to correlate ATM Cashout attack activity at all phases of malicious operations and immediately notify clients worldwide
- Intelligence alerts proactively enabled clients to identify phishing, malware, and criminal activity on networks to mitigate attacks
- Visa's insight into operations provide clients with the earliest insight into attacks, full understanding of the malware, and the ability to mitigate
- Vital signs automated alerting to stop ATM cashout attempts
- Global law enforcement engagement enables Visa to quickly share key details of malicious operations for law enforcement to target criminal operators

Why do Intelligence Alerts matter?

- Timely intelligence - issued within 24-48 hours of activity being discovered
- Provide actionable intelligence and technical recommendations on how to identify and mitigate malicious activity
- Relevant ATM cash-out attacks often follow alerts
- Visa Online is 24x7 repository of latest Alerts; search "Intelligence"
- Facilitate process of ensuring intelligence reports are communicated to the right personnel e.g., Network Security
- Feedback always appreciated paymentintelligence@visa.com

Communication is Critical

Verify and update 24x7 contact information for your financial institution

- Contact information must be submitted in the “Client Directory” section of Visa On-Line (VOL)
- It is critical that Visa be able to quickly contact issuer staff of suspicious activity

Q&A

Securing the ecosystem by working together

Visit us on Visa Online
Search for “Payment Systems Intelligence”