DBE
Data Business Equipment, Inc.

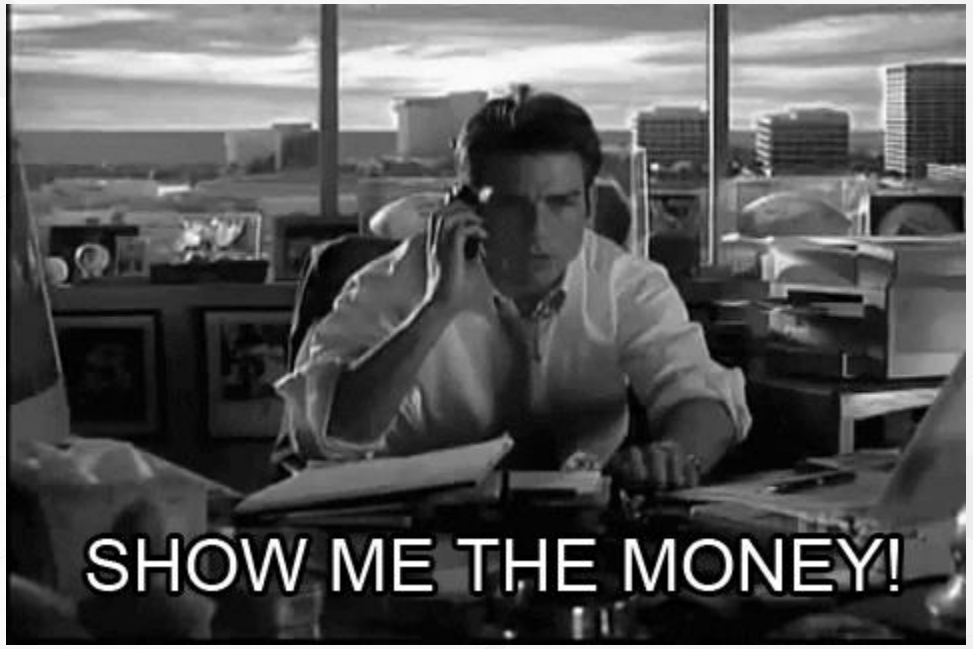
ENCOMPASS SECURE

WEBINAR HOSTED BY DBE

FEBRUARY 27, 2024 - JEFF IRWIN, VP OF TECHNOLOGY

Financial Industry Cyber Attacks

- United States is the number one target for cyber attacks
- 25% of all malware attacks hit banks and other financial industries, more than any other industry
- Financial Industry accounted for 3% of ransomware attacks



ATM Malware Landscape

- Criminals view compromising ATMs as a lucrative endeavor

- Physical attacks include:
  - Blowing up safes
  - Skimmers
  - Fake keypads
  - Infected USB drive or CD
  - Ink staining cassettes
  - SPS
  - Encrypted keypads
  - Locks / alarms

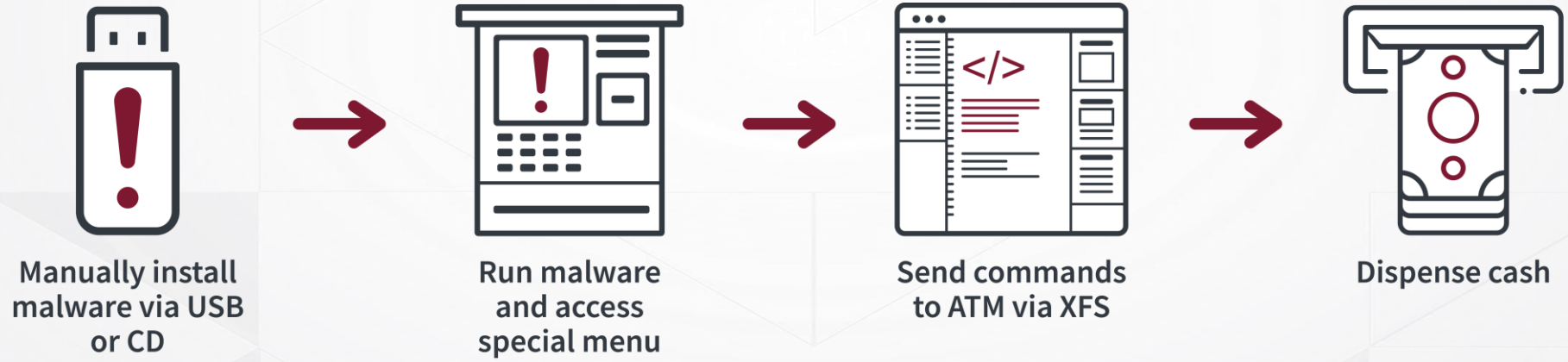
- Threat actors are now favoring Network-Based malware
  - Results in theft without evident tampering
  - Keeps actors remote

Threat Actors

- Nation-State Threats
  - Russia, China, North Korea, Iran
- State-Sponsored Threats
  - Lazarus Group, Cozy Bear, APT1, APT33
- Cyber Criminals
  - LockBit
  - BlackCat
  - Clop

Physical ATM/ITM Malware Attack

- A typical physical ATM / ITM malware attack process

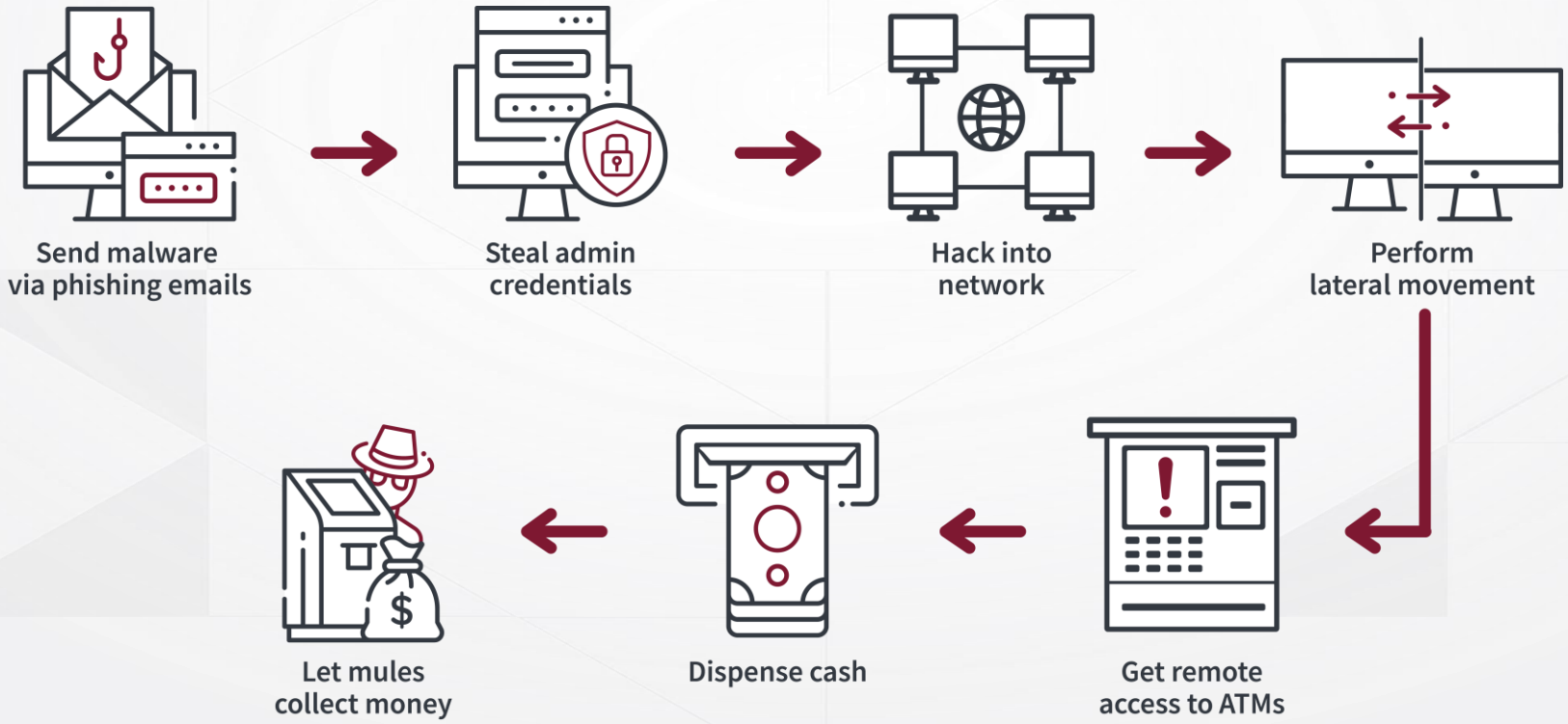


Physical ATM/ITM Malware Attack

- 2009 - Skimer
- 2013 - Ploutus
- 2014 – Ploutus.B
- 2014 - Padpin
- 2015 - GreenDispenser
- 2016 – Ploutus.C
- 2016 - Alice
- 2017 – Ploutus.D

Network ATM/ITM Malware Attack

- A typical Network ATM / ITM malware attack process



Network ATM/ITM Malware Attack

- 2014 – NeoPocket
- 2016 – Taiwan Network Attack
- 2016 – Cobalt Strike
- 2016 – Anunak/Carbanak
- 2016 - Ripper
- 2017 - ATMitch
- 2018 - Mimikatz
- 2022 – ZLoader

What is Secure?

- Partnered with best-in-class vendor, customized for financial endpoints
- Unified Prevention, Detection & Response Platform
- Attack Prevention
  - Prevention technologies and machine-learning models identify and stop attacks
  - We don’t just detect & respond after the fact
- Extended Detection and Response (XDR) as a Service

What does Secure do?

- Anti-ransomware
- Application Control
- Device control
- Encryption (requires TPM)
- Exploit Defense
- Fileless Attack Defense
- Machine Learning
- Network Attack Defense
- Sandbox Analyzer
- Security Incident Response

Operational Lifecycle

PREVENT

DETECT

RESPOND

REPORT

Prevent

- Secure agent hardens the endpoint
- Full drive encryption available (requires TPM chip)
- Policy definitions are housed locally (offline protection)
- Agent prevents unauthorized behaviors at the endpoint
- Updated policy sets keep the agent up-to-date
- Removal of agent requires unique key

Detect

- Continuous collection of host and network telemetry information
- Security analytics and automation enables proactive and responsive hunting, anomaly detection, and investigations
- Detections report back to our central server at regular intervals
- Files are quarantined to our cloud sandbox for analysis
- DBE approved patches are whitelisted during our patch QA

Respond

- Ensure effective incident response actions while minimizing the risk of business interruption
- Automated remediation actions also reduce attacker dwell time with pre-approved actions
- DBE's SOC responds to incidents during business hours
- Additional logging obtained via Encompass Remote Services

Report

- Monthly reports provide an overview of your service
- Post-mortem reports give you information to measure the impact on your business
- Prefer you setup a distribution group for reporting
- No client portal for Secure

Why Secure?

- Secure is a service managed by experts in the space
- QA process eliminates patching interruptions
- Self-managing is heavy lift on Security teams
- Recommend EPP on all ATM/ITMs

Next Steps

- Reach out to your DBE Account Rep
- DBE will provide Due Diligence package
  - Outlines communication parameters
  - Covers our XDR solution provider
  - Define impact levels and SLAs
- Identify deployment parameters and define success
- Agent is deployed to endpoints via Encompass Remote Services (required)