ciab FEBRABAN 2016

Symantec FEBRABAN

Proteção para Auto-Atendimento

Vladimir Amarante
Director, LAMC Pre-Sales and Consulting
CISSP
@VladAmarante

PLOUTUS

March 2014

Embedded phone interacts with Windows Open Service Architecture (WOSA) eXtensions for Financial Services (XFS)

TYUPKIN

March 2014

TARGET	MALWARE	FUNCTIONALITY
ATM's with no alarm, limited physical security.	Attacker inserts a bootable CD. Malware disables security software.	Only runs Sunday & Monday Nights. Disables Network. Dispenses Cash.

When attacker enters valid command during valid times, malware prompts attacker for correct key, which varies for each session, & must be generated from a seed which the malware presents by knowing the algorithm.

After entering correct key, malware shows money in each cassette, allowing attacker to withdraw 40 notes from a cassette. It self-deletes on command.

FUNCTION4 ALSO KNOWN AS GREENDISPENSER

Mid-September 2015

TARGET	MALWARE	FUNCTIONALITY
2 specific ATM vendors	Attacker connects to peripheral port, installs malware, removes peripheral	Dispense Money Delete Itself Confirm Deletion Pause Execution

ATM device shows out of service message to deter use.

Attacker inputs commands via device pin pad.

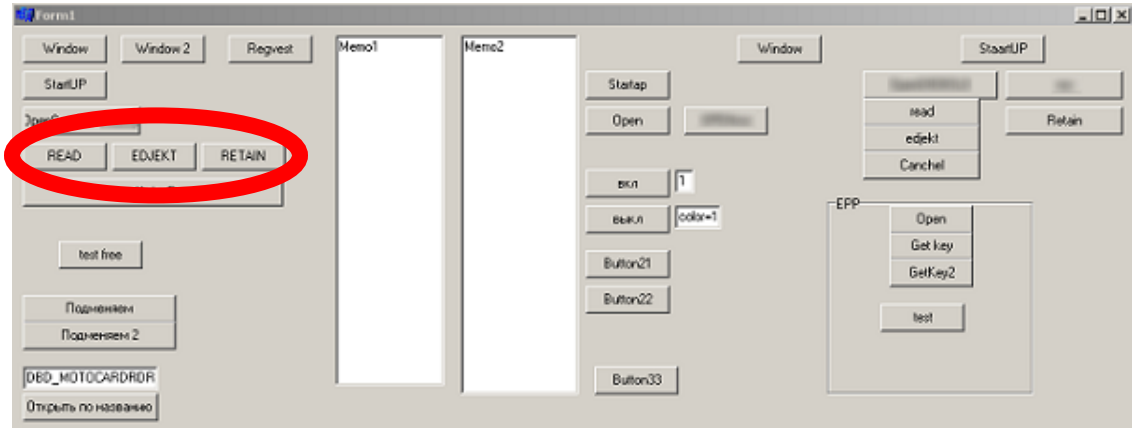
Function4 uses both a hardcoded (static) PIN plus a dynamic PIN.

Dynamic PIN is unique for each run of the malware, and may be generated from QR code displayed on compromised ATM after entering static pin.

Actor removes cash, malware removes itself.

SUCEFUL

Mid-September 2015



FUNCTIONALITY

- Retain/Eject Cards
- Read Card Data
- Read PIN pad entry
- Interact with ATM's Sensors & Indicators Unit (SIU)

WHY DATA INSTEAD OF CASH?

Card numbers & PIN, once captured, can be used on any ATM.

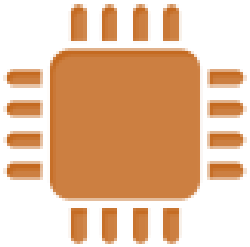
This can extract more cash than a single ATM.

SIU Suppression

Door sensors, Seismic, Facial light, Audible alarm, heat, and more

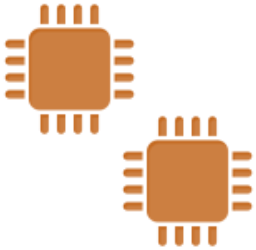
ATM SECURITY

- Underutilized countermeasures



HOST-BASED LOCKDOWN
Sandboxing, behavioral control, enforce “principle of least privilege.”

CODE SIGNING, SECURE BOOT, ENCRYPTION
Ensure all code is authorized to run. Ensure the OS loads correctly… Encrypt disk and traffic



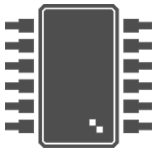
DEVICE AUTHENTICATION
Never trust unauthenticated peripherals.

LONG TERM USER AUTHENTICATION
Evolve beyond magnetic stripe, then evolve further.

LOCKDOWN

- Preventing UNKNOWN Code Execution Inhibits Malicious Activity





HARDENING	BEHAVIOUR	MEMORY	INTEGRITY	PERIPHERALS
SYSTEM CONTROL POLICIES	APPLICATION SANDBOXING & WHITELISTING	MEMORY CONTROL POLICIES	REAL-TIME INTEGRITY MONITORING	APPLICATION CONTROL
Apply least privilege principles to the device Secure connections and encrypted storage	Restrict program execution and behavior to only necessary actions	Defend against malicious code being inserted or executed from memory	Continuously monitor file and registry settings	Allow only white listed applications access to keypad. Control use of USB & other peripheral ports

LONG TERM USER AUTHENTICATION

- MAKING ADDITIONAL FACTORS SEAMLESSLY TRANSPARENT

ATM, CARD, & PIN, as today.

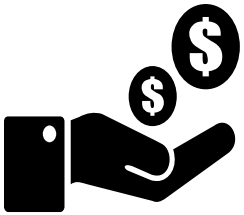
Is the cardholder's mobile device physically near the ATM?

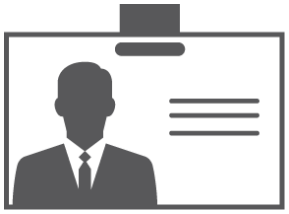
If suspicious, ask the cardholder on their mobile device, "Do you authorize this?"

For highest risk transactions, leverage biometrics built into the mobile device. Fingerprint, plus both facial and iris recognition with liveness detection.

TARGETING THE ATM

- More Threats, More Complexity, More Than Money





CASH	DATA	REPUTATION
ATM's are often targeted for physical cash inside.	Card numbers and PIN, once captured, can be used on any ATM. This can extract more cash than a single ATM.	Brand damage often drives 6% churn immediately, plus longer lasting damage.

ciab FEBRABAN 2016

FEBRABAN

Obrigado!

Vladimir Amarante
Director, LAMC Pre-Sales and Consulting
CISSP
@VladAmarante