A Journey To Protect Points Of Sale

Nir Valtman, CISSP
w: www.valtman.org
@: @ValtmaNir
Introduction
Zombies!!!
Defacement
OPEN SOURCE

AntiDef Secure TDD

Memory Scraper
Why Points Of Sale Targeted?
CC's are delivered like this:

IBAN | CVV/CVV2 | EXP DATE | NAME | ADDRESS | CITY | STATE (USA) | ZIP | COUNTRY | MMN | DOB
| SSN (USA) | PHONE | EMAIL |

USA CC Fullz + tutorial

Choose one or leave blank

- 5 Full info CC USA - $40 / 0.08BTC
- 10 Full info CC USA - $80 / 0.14BTC
- 20 Full info CC USA - $145 / 0.25BTC
- Dumps USA + PIN - $100 / 0.17BTC

Your Email (You will receive CC by email)

BUY (no javascript)
Deployment
Point Of Sale IS NOT Payment Application
Where Are My Credit Cards?

Rest

Transit

Memory

Store

Payment Processor’s Data Center

Rest

Transit

Memory

Where Are My Credit Cards?
Keys to the Kingdom

Matthew 16:19

The kingdom of heaven is like a treasure hidden in a field. When a man found it, he hid it again, and then in his joy went and sold all he had to buy that field. Matthew 16:19
Credit Cards

Mobile App

Presentation Server

Application & Payment Server

Payment Processor’s Data Center

Token Server
Retail Environment Assumptions

100% PCI Compliant
Retail Environment Assumptions
Retail
Environment
Assumptions
Retail Environment Assumptions

Not vulnerable
Retail Environment Assumptions
Retail Environment Assumptions

Cashier ≠ hacker
Retail Environment Assumptions

Big Brother
RATS

Achilles Tendon
Remote Administration Tools

Achilles Tendon
Routing

Achilles
Tendon
Threats
READ&WRITE
I AM BOB

ME TOO
Payment Stages - Authorization

Transmit Track 1/2

PA

POI

Route Track 1/2

Gateway

Processor

Issuer

Acquirer

Transmit Track 1/2

Difficult Exploitation
Payment Stages - Authorization
Payment Stages - Settlement

Store & Send PANs

Difficult Exploitation

PA Server
Payment Stages - Settlement
Memory Scraping Demo
Online VS Offline
Bypassed Solutions
SecureString Class Demo
Next Generation Firewall
ANTI ✯
Data loss
Correct Solutions
Cyber Intelligence
I have access to POS terminals in the US, what is the best malware I should use?
You need to infect the firmware of the terminal. By doing that, you can get full track 1 + 2, but the PIN will be hashed.
Selling malicious firmware for Verifone’s POS terminals.Leaks dumps + PINs through GPRS.
Price: Only 700$
Business Development Offer
Owner of a fake POS sells his terminal. Price: 50% from revenue sharing.
RFI: Change terminal configuration to require PIN for all cards. Cause: Get only 101 data, but wants PINs

Proposed Solution: Thermal Imager
Sandbox
Network-based Anomaly Detection
Operating System Anomaly Detection
Runtime Obfuscation
Not only products required!
Security Architecture

Denial of Service

Access Rights

Default Password

Mis-Configuration
Assembly Obfuscation
PROCESS ISOLATION
What Next
What Would You Steal?

BIP BIP
Memory Scraping
Cashier = hacker
Summary
Security by Obscurity
Simple Exploitation
Hard to Protect
You’re Insured
Thank You

Nir Valtman
w: www.valtman.org
_twitter: @ValtmaNir