S21sec

Comprometidos con la seguridad

Lookwise Device Manager for ATM

v 2.2.0

Autor: S21sec
Fecha: 20 febrero 2015

lookwise | DEVICE MANAGER DM

Índice

- Seguridad **ATM** – Escenario Global
- Lookwise Device Manager (*LDM*) for **ATM**
  - ***LDM* – Solución ATM**
  - ***LDM* – Contramedidas ATM**

S21sec

// Seguridad ATM

Algunas características de las redes de ATMs

- Mercado global ATM de +- 3 MM Cajeros
  Redes desde unos pocos cientos hasta varias decenas de miles
- Hardware Legacy - escasez de recursos
  Impacto en rendimiento
- Sistemas Operativos Legacy - fuera del periodo de soporte de Microsoft (XP)
  Propensos a vulnerabilidades
- Objetivo - ejecución del Aplicativo del ATM
  El resto (S.O. + red) es overhead y fuente de vulnerabilidades
- HW específico - dependiente del modelo y fabricante
  Falta de estandarización
- Entorno estático - poco cambiante
  Actuaciones en remoto -> lentas y con alto coste

S21sec

ATMs: Objetivo de Ataques

- **Los ATMs son objetivos muy atractivos para los atacantes:**
  - Siempre disponen de **dinero en metálico**, se rellenan periódicamente
  - Manejan información sensible: **Tarjetas de Crédito/Débito y PINs**
  - Poco vigilados o atendidos
  - Escasas medidas de seguridad lógica

- **Múltiples vectores de ataque:**
  - Ataques **Físicos**
  - Ataques **Lógicos**
    (Malware)
  - Ataques **Lógico-Físicos**
    (Malware + Acceso Físico al ATM)

- **Alto componente regional en los ataques**

S21sec

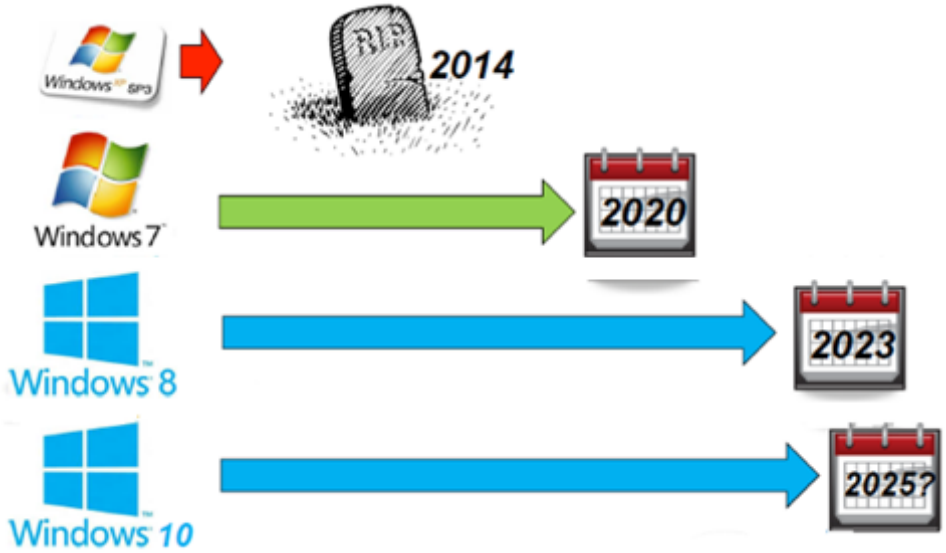
ATMs: Sistemas Vulnerables

SISTEMAS OPERATIVOS LEGACY

- S.O. en End of Support
- S.O. sin parchear
- Extended Support (*Pay-Per-Patch*)
- Ingeniería Inversa (*XP/W7 Patches*)

COEXISTENCIA DE MÚLTIPLES VERSIONES:

- Proceso de Migración Costoso:
  - Tiempo
  - Dinero
- Alta dependencia aplicativo ATM
- Limitaciones por HW obsoleto

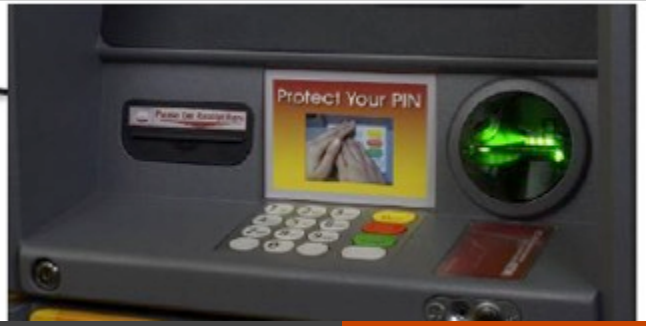


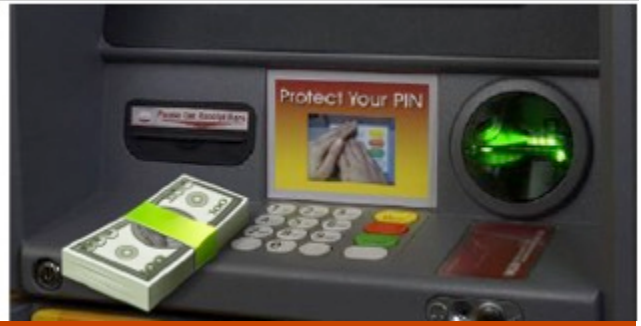
S21sec

ATMs: Ataques Lógico-Físicos

- Acceso al Top-Box del ATM
- Boot desde dispositivo externo
- Desactivar SW de seguridad
- Infectar con Malware
- ReBoot del ATM

- Control ilegítimo del ATM:
  - PINPAD
  - SMS
  - Keyboard
- Activación del Malware por código
- Cash-Out





S21sec

Lookwise Device Manager for ATM

Lookwise Device Manager for ATM

Lookwise Device Manager for ATM permite gestionar la seguridad de su red de cajeros de manera centralizada mediante la **monitorización, protección** y **control** de sus ATMs.

- **Application Whitelisting**
- **Protección del Hardware**
- **Full Disk Encryption**
- **Integridad del File System**
- **Detección de Malware**
- **Control Remoto del ATM**
- **Consumo de recursos muy limitado**

Lookwise Device Manager está especialmente adaptado a las necesidades de los entornos de redes ATM

S21sec

lookwise | DEVICE MANAGER DM

MONITORIZACIÓN

Conozca lo que está sucediendo en sus equipos

PROTECCIÓN

Bloquee el acceso a recursos no autorizados en sus equipos

CONTROL

Ejecute acciones de manera remota sobre sus equipos

S21sec

Lookwise Device Manager
Solución Integral de Seguridad ATM

- **Soluciones de Fabricante:**
  - NCR, Diebold, Wincor-Nixdorf, Fujitsu, Hyosung, EDGE…
  - Redes ATM multi-fabricante
  - Soluciones de Seguridad mono-fabricante (OEMs)

- **LDM – Solución Integral:**
  - **Independiente del fabricante del ATM**
  - Solución de Seguridad unificada
  - Gestión central del parque de ATMs
  - Políticas de Seguridad por Fabricante/ Modelo
  - Integración con sistemas SIEM

S21sec

// Lookwise Device Manager for ATM

LDM - Contramedidas de Seguridad para ATMs

- **APPLICATION WHITELISTING**
  - Evita la ejecución de Malware o SW fraudulento
  - Ejecución limitada a procesos autorizados
  - Control de librerías y parámetros de los procesos (ej. Java)
  - La mejor contramedida en equipos con sistemas operativos obsoletos y vulnerables
- **PROTECCIÓN DE HARDWARE**
  - Evita la conexión de HW fraudulento
  - Acceso limitado a Hardware autorizado
  - Barreras de Protección:
    - Nivel 1: periféricos de almacenamiento
    - Nivel 2: Hardware ID (make/model/version)
    - Nivel 3: Hardware Instance ID

S21sec

LDM - Contramedidas de Seguridad para ATMs

- **FULL DISK ENCRYPTION**
  - Evita acceso al disco fuera del S.O.
  - Integración con SW Diskcryptor
  - Reinicio desatendido del ATM
  - Gestión remota del cifrado

- **INTEGRIDAD DEL FILE SYSTEM**
  - Evita manipulaciones fraudulentas del File System
  - Monitorización de cambios en ficheros
  - Monitorización de cambios en directorios
  - Protección de escritura de ficheros

S21sec

LDM - Contramedidas de Seguridad para ATMs

- **DETECCIÓN DE MALWARE**
  - Detecta evidencias de presencia de Malware
  - Procesos, drivers y ficheros ocultos
  - Hooks

    (*sólo Windows XP*)

- **CONTROL REMOTO DEL ATM**
  - Permite controlar el ATM de manera remota
  - Reinicio remoto
  - Cambio de contraseña en remoto
  - Recuperación de ficheros en remoto
  - Ejecución de Acciones Remotas (configuración, forense, cifrado de disco, limpieza de malware…)

S21sec

GRACIAS

SPAIN • MEXICO •BRASIL •UK •USA

www.s21sec.com

S21sec

Comprometidos con la seguridad