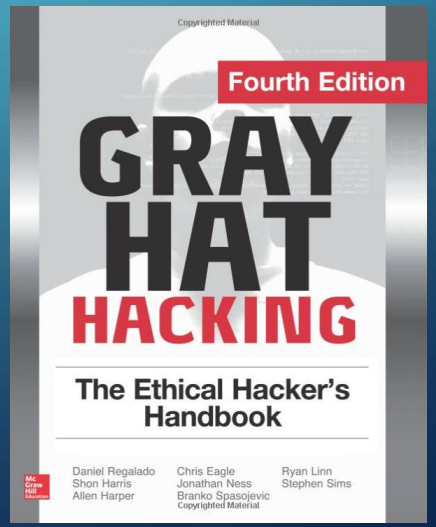
EL FIN DE PLOUTUS CON UN DISPENSADOR INTELIGENTE

DANIEL REGALADO AKA DANUX

@DANUXX

QUIEN SOY YO?

- Mexicano trabajando en Silicon Valley desde el 2008
  - Symantec, FireEye, Zingbox
- Reverse Engineer y Analista de Malware y Vulnerabilidades
- Speaker Bsides, Defcon/IoT Village – Las Vegas
- Lider descubridor de ATM Malware a nivel mundial
  - Ploutus, Padpin (Tyupkin), PanDeBono, Neabolsa, SUCEFUL, Alice, Ripper, Ploutus-D
- Autor Lider: Gray Hat Hacking Book 4th Edition



AGENDA

- Scope
- Cual es el Problema?
- Como instalan el Malware?
- Como interactuan con el Malware?
- Como vacian el cajero?
- Ataques vs Soluciones actuales
- Enfoque de proteccion fallido. Porque?
- Smart Dispenser Overview

ANTES DE COMENZAR

- Si crees en alguien por encima del ser humano, pidele por Mexico y si puedes donar, mucho mejor: http://levantaunacasa.org

SCOPE

- Hay 2 tipos de ATM Malware:
  - ✓Los que atacan al tarjetahabiente
  - ✓Los que atacan al Dispensador
- Esta platica se concentra en los virus que atacan al dispensador

Cual es el Problema?

PERDIDAS MILLONARIAS A NIVEL MUNDIAL

Country of Heist	Year	Infection vector	Net Loss (USD)	Mastermind Group	Members Nationality
Multiple	2012-2013	Bank Network Breach[1]	$45 Million	Unknown	Turkish
Mexico	2013-2017	ATM Malware[2]	$450 Million	Ploutus Team	Venezuelan
Russia	2015-2016	Spear Phishing[3]	$28 Million	Buhtrap	Russian
Japan	2016	Card Cloning[4]	$12.7 Million	Unknown	Japanese
Taiwan	2016	Bank Network Breach[5]	$2.5 Million	Unknown	Romanian, Moldovan

Como instalan el Malware?

COMO INSTALAN EL MALWARE?

- Directamente con accesso fisico al cajero
  - ✓Se abre la parte superior del cajero con la llave del fabricante
  - ✓Se instala el malware traves de puertos externos como USB, CD-ROM
- Instalando el malware desde la red bancaria (avanzado)
  - ✓Se necesita penetrar la red bancaria
  - ✓Se necesita encontrar una vulnerabilidad para cargar el malware en los cajeros
  - ✓Mas efectivo, pero mas dificil
  - ✓Caso ejemplo: First Bank en Taiwan
- Instalando el Malware desde la maquina del atacante
  - ✓Se monta el disco como unidad esclava
  - ✓El ladron se conecta a la Laptop de la mula via Wi-Fi dongle

Como interactuan con el Malware?

COMO INTERACTUAN CON EL MALWARE?

- A traves de teclado externo conectado al cajero
  - ✓Ploutus

- A traves del teclado del cajero (Pinpad)
  - ✓Padpin (Tyupkin)

- A traves de tarjeta de debito apocrifa
  - ✓Ripper

COMO INTERACTUAN CON EL MALWARE?

- A traves de mensajes de texto SMS
  - ✓Ploutus v2.0

- A traves de WiFi dongles
  - ✓Ploutus-D

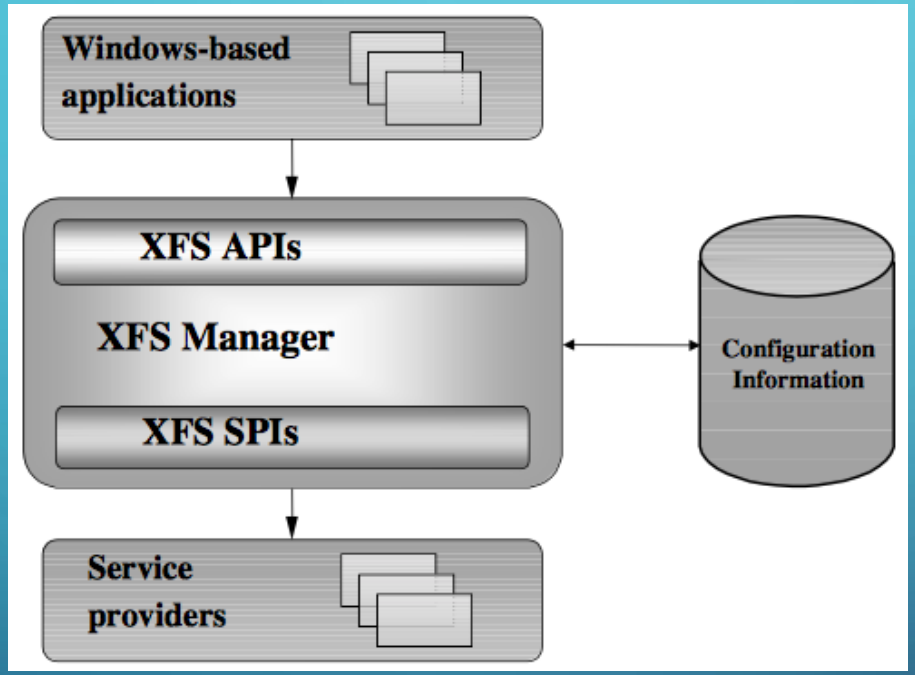
COMO INTERACTUAN CON EL MALWARE?

- A traves the touch screen
  - ✓Ploutus

Como vacian el Cajero?

COMO VACIAN EL CAJERO?

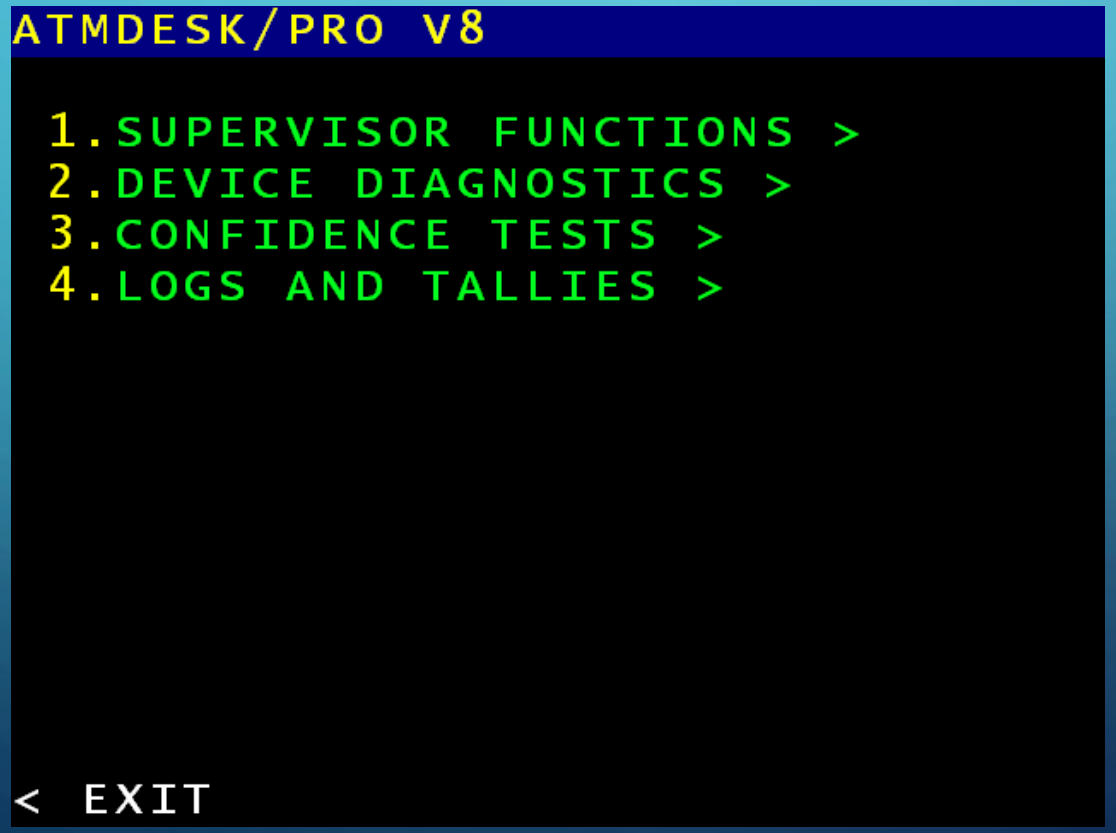
- Hay 2 tecnicas, tecnologia Ploutus y los demas
- Pero todos al final terminan interactuando con las mismas low-level APIS del XFS SDK



- Mensaje de KAL en relacion a Ploutus-D: “All XFS-compliant ATMs are at risk from this malware”
- El Dispensador entrega dinero a quien se lo pida ☹

VACIANDO EL CAJERO CON PLOUTUS V1.0

- Un cajero funciona en modo normal o supervisor (vendor mode)
- El modo supervisor permite configurar el cajero, es como ser root en Linux
  - ✓En este modo, todo el hardware esta a la orden del operador



PLOUTUS V1.0 – CAMBIANDO A VENDOR MODE

- Se crea clase XFSVendorModeClass() via NCR APTRA Middleware

```
PloutusService.MemoryData.XVMC = new XFSVendorModeClass();
PloutusService.MemoryData.XVMC.ActiveInterfaceChanged += new _IXFSVendorModeEven
PloutusService.MemoryData.XVMC.ActiveInterfaceSet += new _IXFSVendorModeEvents_A
PloutusService.MemoryData.XVMC.AvailabilityChanged += new _IXFSVendorModeEvents_
PloutusService.MemoryData.XVMC.Entered += new _IXFSVendorModeEvents_EnteredEventH
PloutusService.MemoryData.XVMC.EntryRequested += new _IXFSVendorModeEvents_EntryH
PloutusService.MemoryData.XVMC.Exited += new _IXFSVendorModeEvents_ExitedEventHa
PloutusService.MemoryData.XVMC.ExitRequested += new _IXFSVendorModeEvents_ExitRe
PloutusService.MemoryData.XVMC.UnableToSetActiveInterface += new _IXFSVendorModeI
PloutusService.MemoryData.XVMC.UnexpectedWOSAEvent += new _IXFSVendorModeEvents_
PloutusService.MemoryData.XVMC.XFSErrorEvent += new _IXFSVendorModeEvents_XFSErr
PloutusService.MemoryData.XVMC.Register();//Triggers the vdm_AvailabilityChanged
PloutusService.Utils.UpdateLog("VENDORLOAD OK");
PloutusService.Program.NCRV.UpdateText("Vendor Init OK");
PloutusService.MemoryData.VDMStatus = true;
return;
```

- Ploutus cambiando a modo ”Vendor mode”:

```
if (PloutusService.MemoryData.XVMC.SystemMode.ToString().Equals("VDM_NORMAL"))
{
    PloutusService.MemoryData.XVMC.RequestEntry();
    PloutusService.MemoryData.XVMC.AcknowledgeEntryRequest();
}
```

PLOUTUS V1.0 – CAMBIANDO A VENDOR MODE

- Una vez en Vendor mode y con esto, con el control del cajero, se empieza retirar el dinero

```
private static void vdm_Entered(System.DateTime timeStamp)
{
    PloutusService.Utils.UpdateLog(System.String.Concat("vdm_Entered:", timeStamp));
    PloutusService.MemoryData.VDMEntered = true;
    PloutusService.VdmManager.Command();
}
```

```
private static void Command()

{
    PloutusService.Utils.UpdateLog(System.String.Concat("Call Class:", PloutusService.MemoryData.CommandType));
    if (PloutusService.MemoryData.CommandType == 1)
    {
        (new System.Threading.Thread(new System.Threading.ThreadStart(PloutusService.VdmManager.DispenseThread))).Start();
        return;
    }
```

```
private static void DispenseThread()
{
    PloutusService.DispenceClass dispenceClass = new PloutusService.DispenceClass();
    dispenceClass.Start();
}
```

COMO LO VACIAN LOS DEMAS?

- Demas = Padpin (Tyupkin), Alice, Ripper, GreenDispenser, SUCEFUL
- Se aprovechan de un leak del manual de programacion de NCR

```
push    eax
push    1D4C0h              ; 12000
lea     eax, [ebp+var_3C]
push    eax
movzx   eax, word ptr [ebx]
push    12Eh                ; WFS_CMD_CDM_DISPENSE
push    eax
mov     [ebp+var_1F], 0
mov     [ebp+var_23], edi
mov     [ebp+var_36], 1
call    ds:WFSExecute
```

GreenDispenser

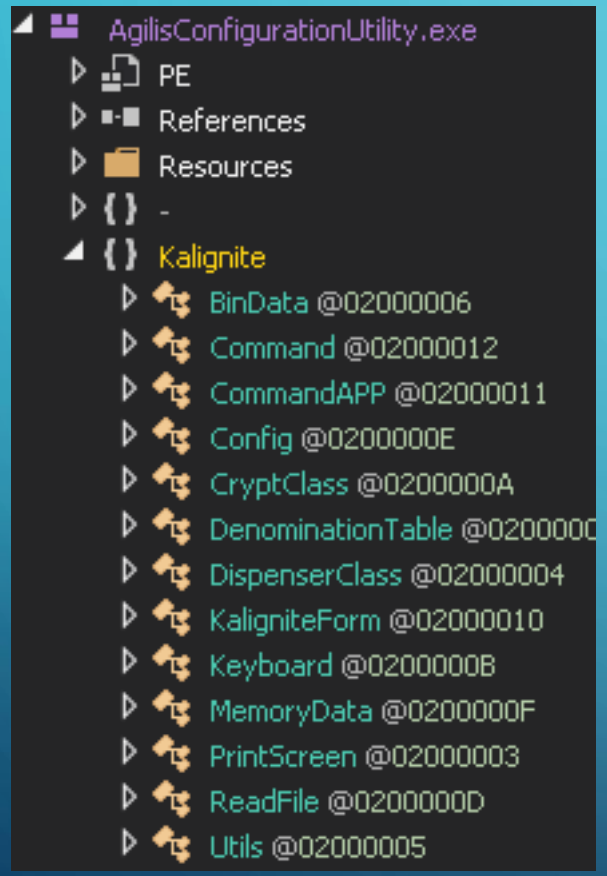
```
and     [esp+104h+var_F4], 0
xor     eax, eax                                        bills
inc     eax                                             bills
mov     word ptr [esp+104h+var_F8], ax                  bills
lea     eax, [esp+104h+var_F4]                          bill
push    eax
push    0
lea     eax, [esp+10Ch+var_F8]
push    eax
movzx   eax, word_44C86E
push    203                 ; WFS_CMD_IDC_EJECT_CARD
push    eax
call    ds:WFSExecute
jmp     short loc_401FA0
```

Ripper

```
hResult  =   WFSExecute( hService,
                         WFS_CMD_CDM_DISPENSE,
                         &tDispense,
                         TWO_MINUTES,
                         &lpResult
                       );
```

NUEVO PLOUTUS-D USA KALIGNITE

- Nueva catedra, conocimiento total del multi-vendor middleware



DispenserClass @02000004

```
1  using System;
2  using KXCashDispenserLib;
3
4  namespace Kalignite
5  {
6      // Token: 0x02000004 RID: 4
7      public class DispenserClass
8      {
9          // Token: 0x0600001B RID: 27 RVA: 0x00002867 File Offset:
10         static DispenserClass()
11         {
12             Class7.AoKcsMFzq0mvK();
13             DispenserClass.YkjoIvchS = new KXCashDispenserClass();
14             DispenserClass.int_0 = 0;
15             DispenserClass.bool_0 = false;
16             DispenserClass.string_0 = string.Empty;
17             DispenserClass.int_1 = 0;
18         }
```

Ataques vs Soluciones actuales

ATAQUE FISICO (INEVITABLE)

Vector de Ataque	Solucion Actual
Instalacion via USB/CD-ROM	Bloque de puertos
Desconexion de Disco Duro Desinstalacion de software de seguridad	NCR Secure Hard Disk Drive Encryption Terminal Security Hard Disk Encryption (Diebold) Expensive? Need to upgrade Hardware?
Malware running inside ATM	NCR/Diebold Products (App Whitelisting) AV/IPS
Infeccion de cajero desde la red bancaria - Ripper	Encryption – FAILED Whitelisting – Talvez funciona AV/IPS - FAILED
Replay Attack desde la red bancaria (transaccion “legitima”)	Encryption – FAILED Whitelisting – FAILED AV/IPS - FAILED
Offline Attack Desconexion del Casete (USB, RS232)	Encryption – FAILED Whitelisting – FAILED AV/IPS - FAILED
Offline Attack: Reemplazo de Disco Duro	Sin Secure Boot, ni Superman lo detiene

Enfoque de proteccion fallido Porque?

PORQUE NO ES SUFICIENTE?

- Que tienen en comun todos los virus de cajero que hemos visto?
  - ✓Controlan el Dispenser (ya que este controla los casetes con dinero)
- Que tienen en comun todas las soluciones que hemos visto?
  - ✓Nadie protege las transacciones con el Dispenser ☹
  - ✓Todas las soluciones estan en el Sistema Operativo
- Un Cajero se compone de Software y Hardware
  - ✓Por lo tanto, el Hardware tambien debe ser protegido

Smart Dispenser

“Un Firewall en la boveda de seguridad”

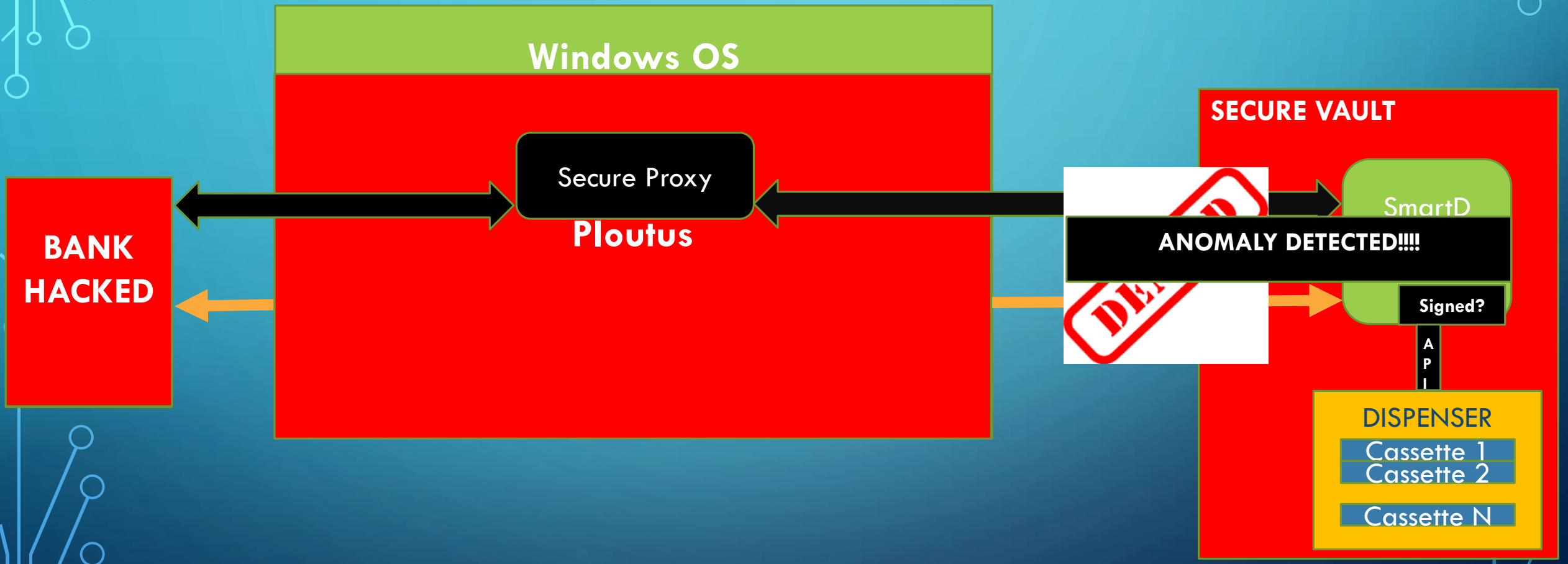
SMART DISPENSER OVERVIEW

(*PATENTE EN PROGRESO*)

- Solucion hibrida unica en el mercado
  - ✓Diebold propone tambien una solucion hibrida pero implementada de forma diferente
  - ✓Una sola tarea: Proteger el retiro de efectivo (no somos AV/IPS)
- **Secure Proxy**(software): Proxy entre SmartD y Banco
- **SmartD** (hardware): Caja magica en la boveda que vuelve al Dispensador inteligente
  - ✓Valida con el Banco las peticiones de retiro de dinero
  - ✓Detiene Replay Attacks
  - ✓Implementa politicas de seguridad del Banco:
    - Ejemplo: Rechaza retiros duplicados dentro de un lapso de 3 minutos
    - Rechaza arbitraria seleccion de casete para retiro
- La seguridad de SmartD depende de la seguridad de la boveda

SMART DISPENSER OVERVIEW

(*PATENTE EN PROGRESO*)



CONCLUSIONES

- Asumamos que el cajero sera infectado
  - ✓Y entonces protegamos al Dispensador
- Asumamos que la red bancaria sera comprometida
  - ✓Y entonces hagamos al Dispensador inteligente
- Forcemos de nuevo a los criminales a tener que abrir la boveda para llevarse el dinero

Preguntas?

@danuxx
Hackdef@hack-defender.mx

Gracias