Seguridad Logica De Cajeros Automaticos

Liquidnexxus

- Lider global en formación en seguridad y riesgo de medios de pago

Colaboraciones Estratégicas

PCI Security Standards Council®

PCI GLOBAL TRAINING NETWORK (PGTN)™

ATEFI

REDES LATINOAMERICANAS DE MEDIOS DE PAGO

E.A.S.T

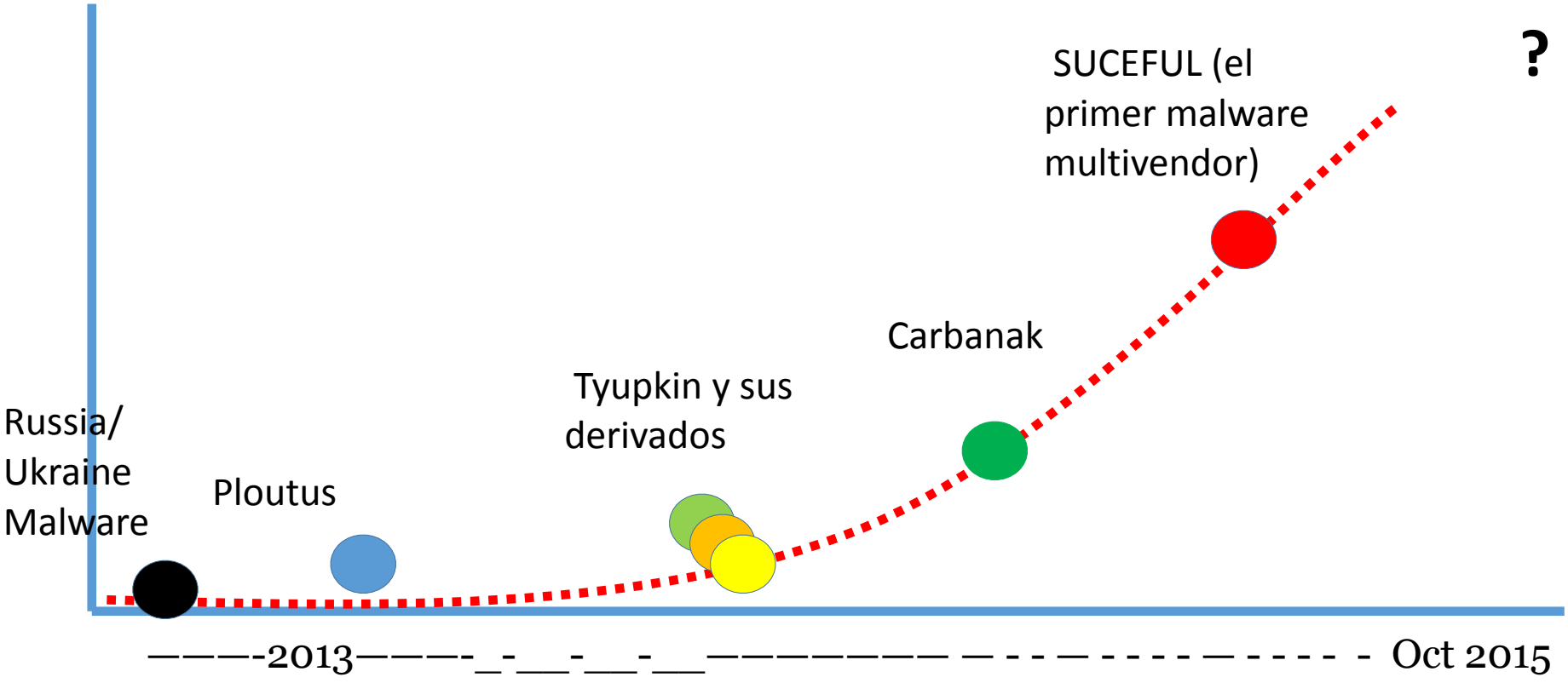
European ATM Security Team
Associate Member

Introductions & Agenda

- **Agenda**
  - Contexto Cibercrimen
  - Análisis de Malware
  - Recomendaciones

  - Por motivos de seguridad la distribución de la presentación completa esta restringida, si desea la presentación completa contáctenos en info@liquidnexxus.com

Evolucion Del Malware De Atms



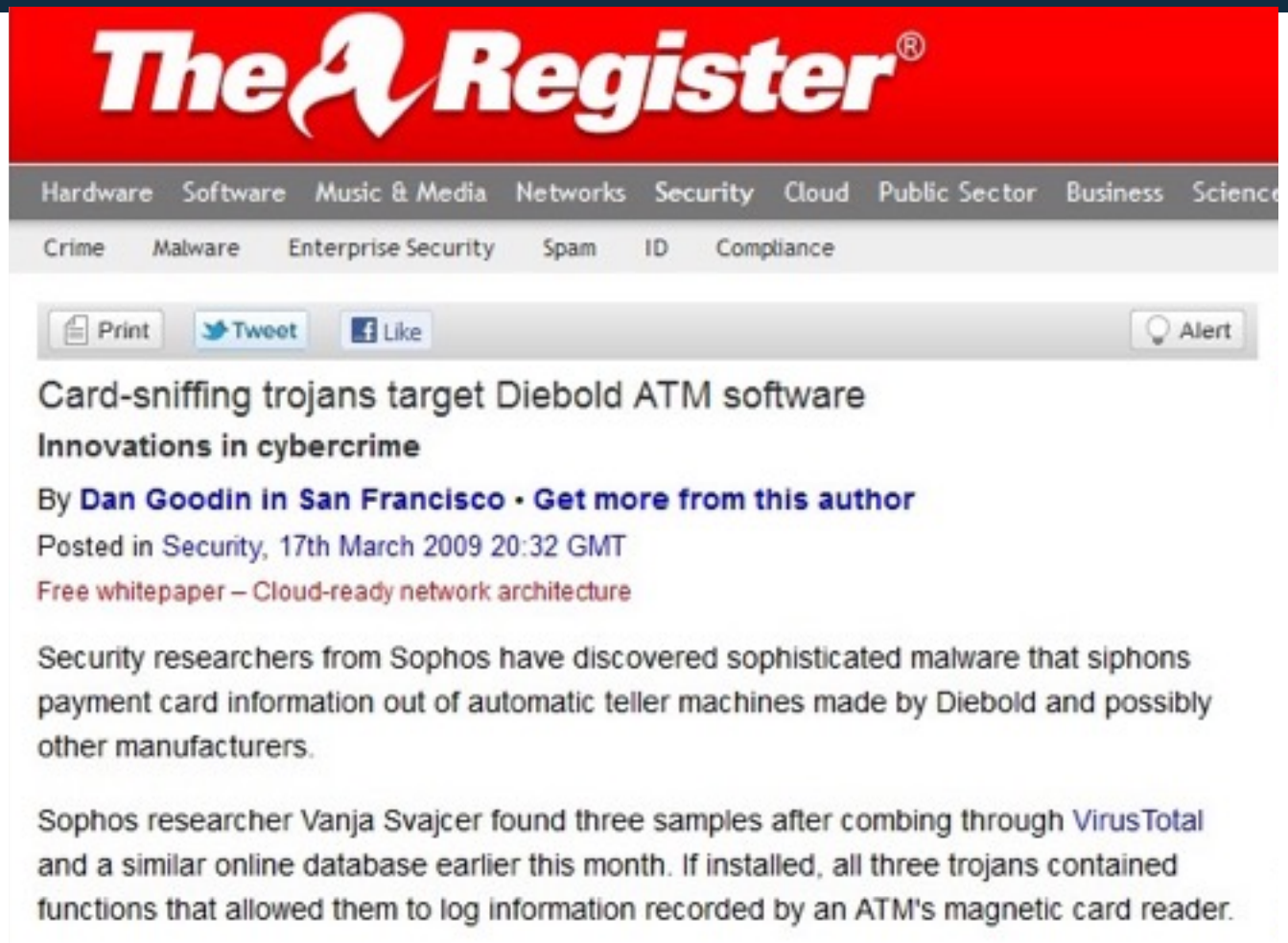
Jackpotted 2010: Barnaby Jack

Jack reprogrammed the ATM remotely over a network, without touching the machine;

- The Tranax hack was conducted using an authentication bypass vulnerability that Jack found in the system's remote monitoring feature, which can be accessed over the internet or dial-up, depending on how the owner configured the machine.
- an attacker would need to know an ATM's IP address
- War dialing

- Upload software or overwrite the entire firmware on the system.
- Installed a malicious program (Scrooge).
- Initiated in two ways:
  - touch-sequence entered on the ATM's keypad
  - inserting a special control card.

Eastern Europe Malware - April 2009



The Register®

Hardware Software Music & Media Networks Security Cloud Public Sector Business Science

Crime Malware Enterprise Security Spam ID Compliance

Print Tweet Like Alert

Card-sniffing trojans target Diebold ATM software

Innovations in cybercrime

By **Dan Goodin in San Francisco • Get more from this author**

Posted in Security, 17th March 2009 20:32 GMT

Free whitepaper – Cloud-ready network architecture

Security researchers from Sophos have discovered sophisticated malware that siphons payment card information out of automatic teller machines made by Diebold and possibly other manufacturers.

Sophos researcher Vanja Svajcer found three samples after combing through VirusTotal and a similar online database earlier this month. If installed, all three trojans contained functions that allowed them to log information recorded by an ATM's magnetic card reader.

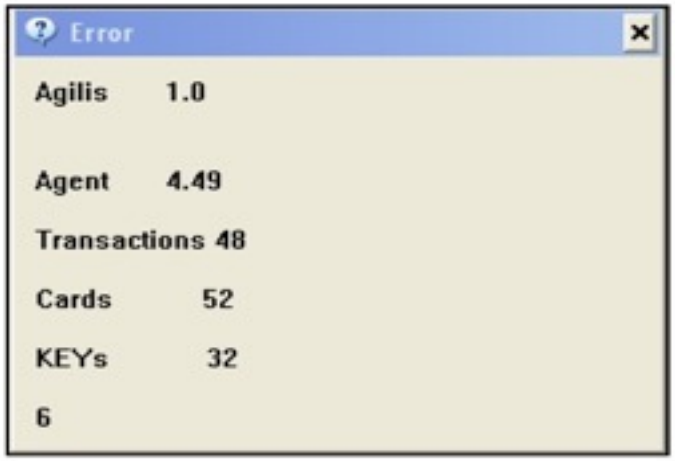
Eastern Europe Malware - April 2009

Trojan.Skimer.A – first trojan for ATMs

Main target – interception of Track2 and PIN data

Made in Russia or Ukraine

First infection – November 2008, first notification – January 2009

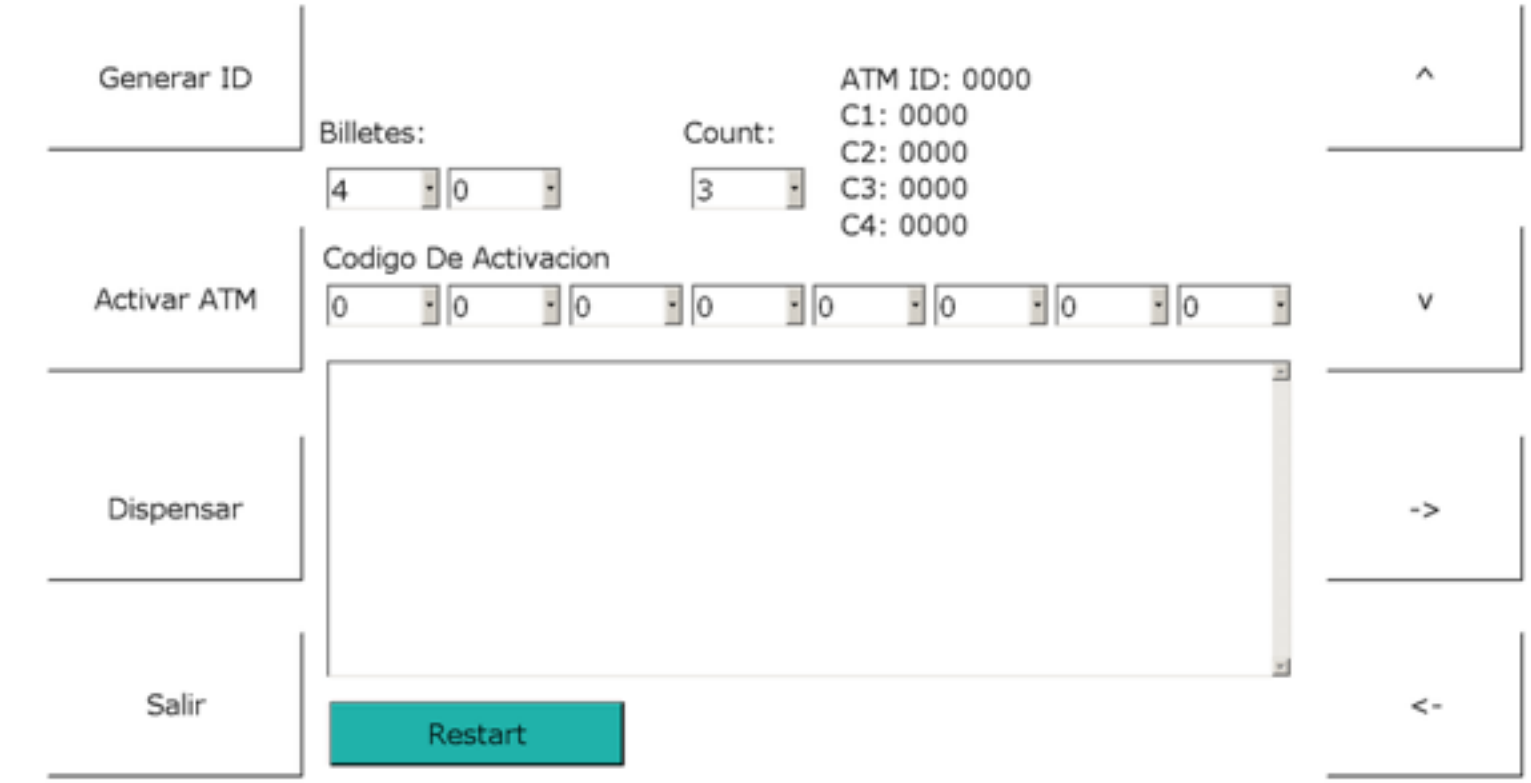


Ploutus – Mx

NCRDRVPS service

```
private void InitializeComponent()
{
    this.ServiceProcessInstallerP = new ServiceProcessInstaller();
    this.ServiceInstallerP = new ServiceInstaller();
    this.ServiceProcessInstallerP.Account = ServiceAccount.LocalSystem;
    this.ServiceProcessInstallerP.Password = null;
    this.ServiceProcessInstallerP.Username = null;
    this.ServiceInstallerP.ServiceName = "NCRDRVPS";
    this.ServiceInstallerP.StartType = ServiceStartMode.Automatic;
    base.Installers.AddRange(new Installer[] { this.ServiceProcessInstallerP, this.ServiceInstallerP });
}
```

Ploutus – Mx

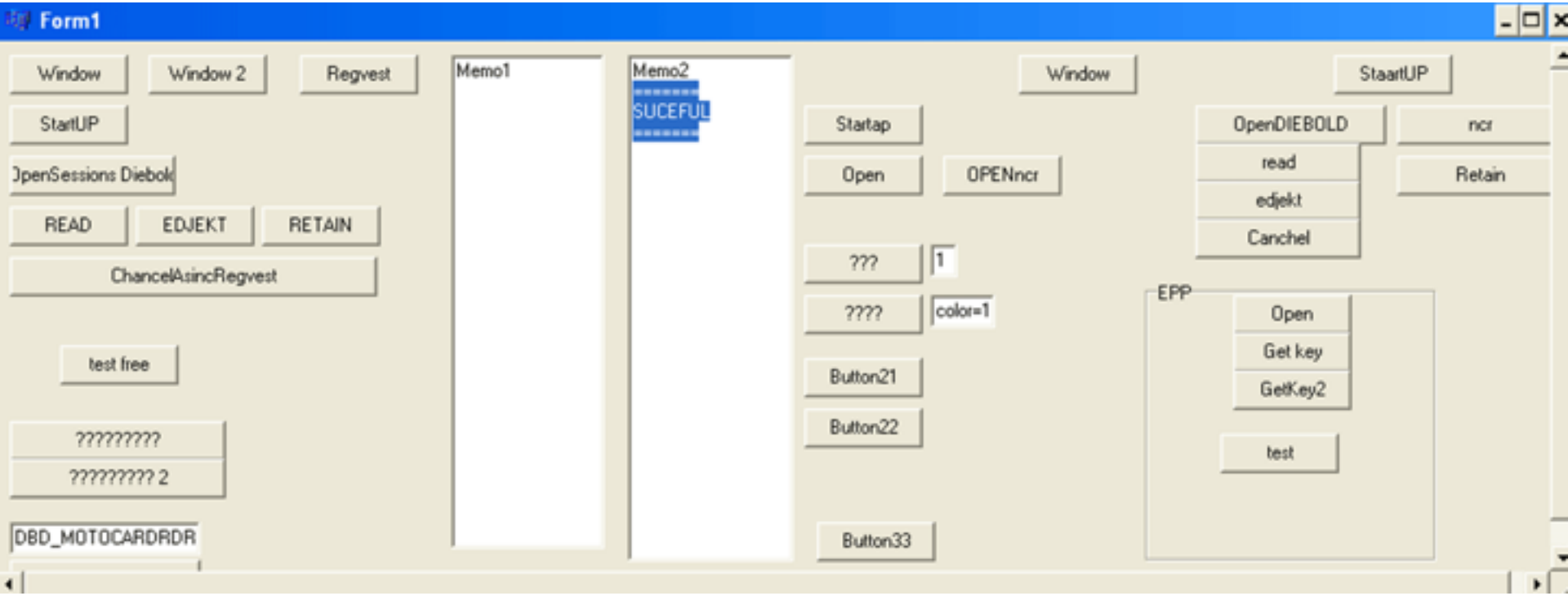

Generar ID
Billetes:
4
0
Count:
3
ATM ID: 0000
C1: 0000
C2: 0000
C3: 0000
C4: 0000
^
Activar ATM
Codigo De Activacion
0
0
0
0
0
0
0
0
v
Dispensar
->
Salir
Restart
<-

Suceful

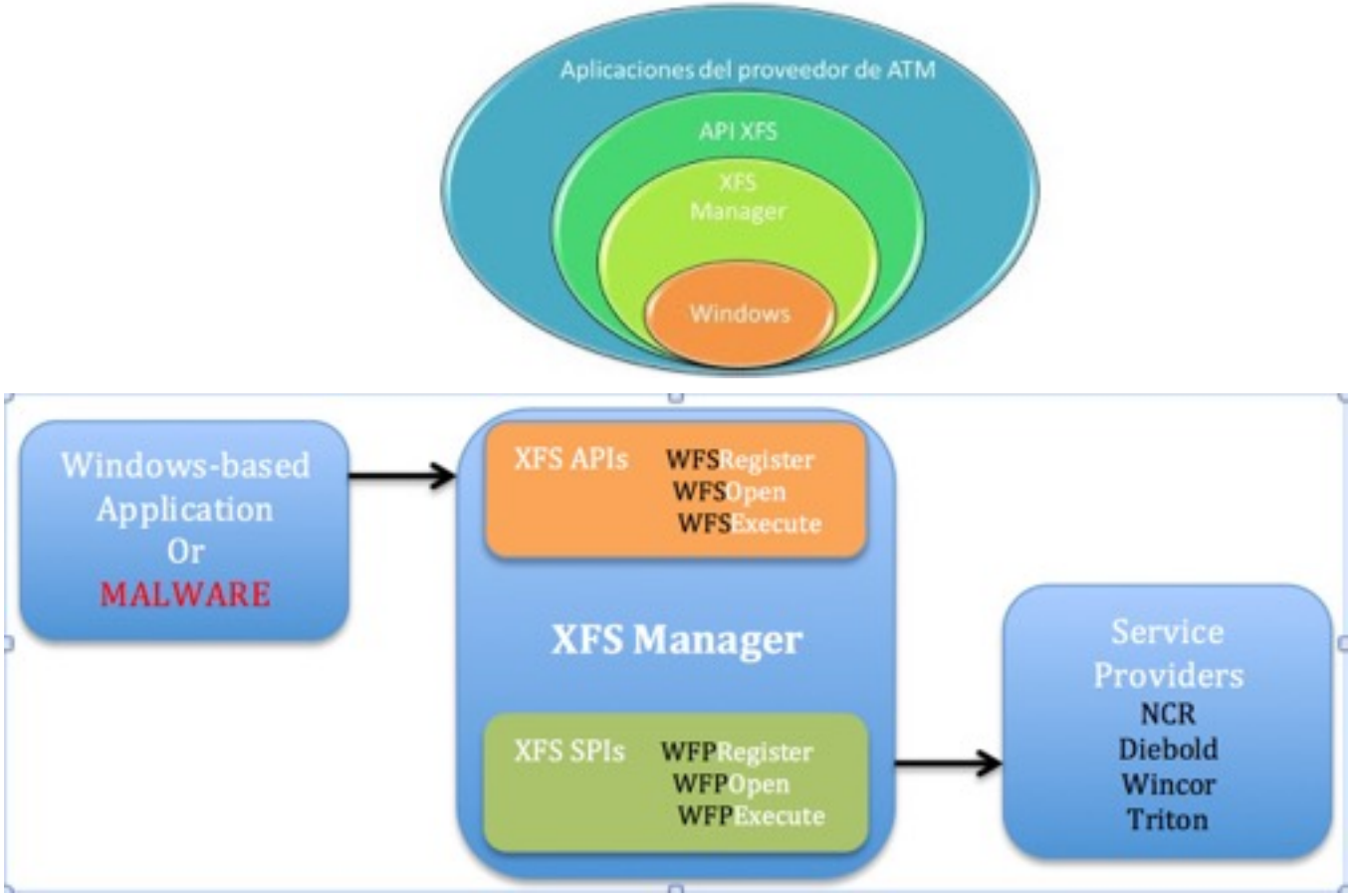
New ATM malware **Backdoor.ATM.Suceful** (the name comes from a typo made by the malware authors)

- targets cardholders and is able to retain debit cards on infected ATMs, disable alarms, or read the debit card tracks.
- the features provided are shocking and never seen before in ATM malware.

Suceful


Form1
Window
Window 2
Regvest
StartUP
OpenSessions Diebok
READ
EDJEKT
RETAIN
ChancelAsincRegvest
test free
?????????
????????? 2
DBD_MOTOCARDRDR
Memo1
Memo2
SUCEFUL
Window
Startap
Open
OPENncr
???
1
????
color=1
Button21
Button22
Button33
StaartUP
OpenDIEBOLD
read
edjekt
Canchel
ncr
Retain
EPP
Open
Get key
GetKey2
test

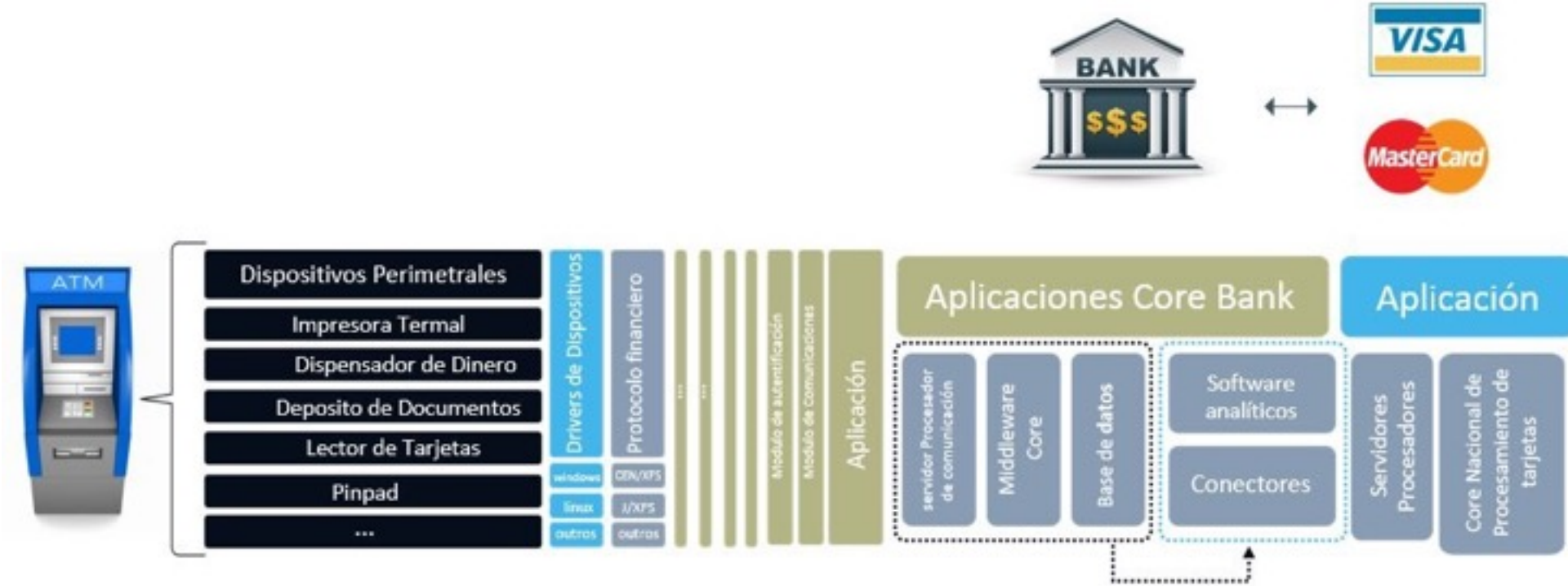
Suceful


Aplicaciones del proveedor de ATM
API XFS
XFS Manager
Windows
Windows-based Application Or MALWARE
XFS APIs
WFSRegister
WFSOpen
WFSExecute
XFS Manager
XFS SPIs
WFPRegister
WFPOpen
WFPExecute
Service Providers
NCR
Diebold
Wincor
Triton

Suceful

- WFSOpen or WFSAsyncOpen APIs (open sessions with the peripheral devices via the Service Providers (XFS SPIs) through the XFS Manager by calling)
- WFSExecute or WFSAsyncExecute (specific operations to the peripheral devices)
- WFS_CMD_IDC_READ_RAW_DATA (read all the track data and chip)
- The WFS_CMD_IDC_RETAIN_CARD (retain the card)
- WFS_CMD_IDC_EJECT_CARD (eject the card)
- WFS_CMD_PIN_GET_DATA (Interact with the Malware via PIN pad=
- WFS_CMD_SIU_SET_PORTS (Disabling ATM Sensors)
- WFSAsyncExecute API (DLL Hooking:allows control and monitor all the commands issued to the peripheral devices)
- SUCEFUL is the first multi-vendor ATM Malware targeting cardholders, created to steal the tracks of the debit cards but also to steal the actual physical cards, which is definitely raising the bar of sophistication of this type of threats.

Context

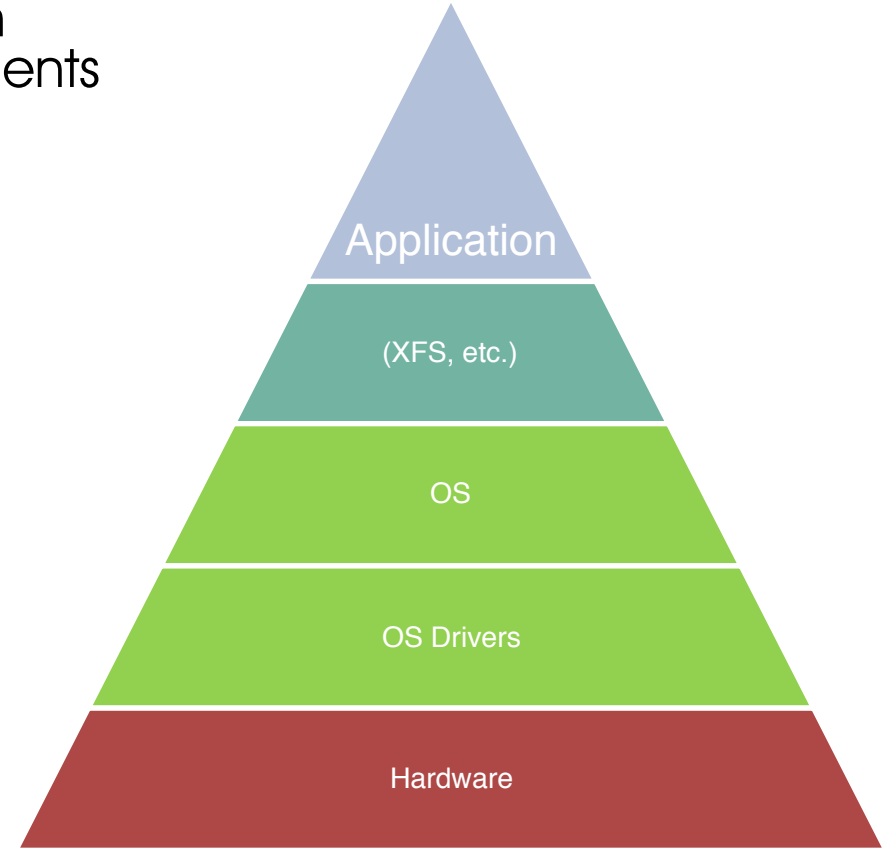


*Dependiendo del banco y el país la estructura puede variar pero siempre se mantiene la lógica del negocio

Atm Software Layers

ATM Application accessed by clients and operators

Transactional Operations



Ncr

Restringido

Diebold

Restringido

Recommendaciones

Recomendaciones

- ATM Physical Access Controls
- Prevent & Detect unusual things (DLLs, exe, etc etc etc…)
- Protect BIOS
- OS and Application Hardening
- Change Atm Application Default Users and password
- Enforce encrypted pairing authentication for key ATM components, particularly between cash dispenser and ATM controller
- Set Dispenser protection to higher level for Physical Protection and Encryption
- Hard Disk Encryption
- Patching
- Encrypted Comms (not just VPN)

Cursos Lnx

Foro LatinoAmericano de Seguridad en Medios de Pago - Asunción

mi. 18 noviembre - ju. 19 noviembre 2015

El Foro Latinoamericano de Seguridad en Medios de Pago (SMP) se fundo como una colaboración entre ATEFI y LiquidNexxus con el objetivo de elevar los niveles de conocimien...

Más información

Lead ATM Security Auditor [LASA] - Ciudad de Panamá

lu. 23 noviembre - mi. 25 noviembre 2015

El primer curso practico dedicado a la auditoria logica del entorno de Cajero Automaticos.

Más información

PCI DSS: Implementación y Gestión - Ciudad de Panamá

ma. 23 febrero - mi. 24 febrero 2016

PCI DSS, PA DSS y PTS son los estándares de la industria de tarjetas de pago. Todas las instituciones o entidades que almacenan, procesan o transmiten datos de tarjetas d...

Más información

PCI ISA (Asesor de Seguridad Interno Certificado) - Ciudad de Panamá

ju. 25 febrero - vi. 26 febrero 2016

El Programa para Asesores Internos PCI ISA (Internal Security Asessor) ofrece la oportunidad de tener personas internas

Cursos Lnx

- **Foro LatinoAmericano de Seguridad en Medios de Pago** - Asunción - mi. 18 noviembre - ju. 19 noviembre 2015
- **Lead ATM Security Auditor [LASA]** - Ciudad de Panamá - lu. 23 noviembre - mi. 25 noviembre 2015
- **PCI DSS: Implementación y Gestión** - Ciudad de Panamá - ma. 23 febrero - mi. 24 febrero 2016
- **PCI ISA (Asesor de Seguridad Interno Certificado)** - Ciudad de Panamá - ju. 25 febrero - vi. 26 febrero 2016
- **Riesgo en Banca Electrónica y Canales Alternos (RBECA)** - Lima - ma. 01 marzo 2016
- PCI DSS: Implementación y Gestión - Lima - mi. 02 marzo - ju. 03 marzo 2016
- PCI DSS: Implementación y Gestión - Ciudad de Mexico - mi. 13 abril - ju. 14 abril 2016
- Riesgo en Banca Electrónica y Canales Alternos (RBECA) - Bogota - vi. 27 mayo 2016
- Seguridad de Cajeros Automáticos - Asuncion - ju. 21 julio - vi. 22 julio 2016
- Lead ATM Security Auditor [LASA] - Santiago de Chile - lu. 25 julio - mi. 27 julio 2016
- Lead ATM Security Auditor [LASA] - Quito - lu. 05 septiembre - mi. 07 septiembre 2016
- PCI DSS: Implementación y Gestión - Quito - ju. 08 septiembre - vi. 09 septiembre 2016
- PCI DSS: Implementación y Gestión - Ciudad de Panamá - ma. 18 octubre - mi. 19 octubre 2016
- PCI ISA (Asesor de Seguridad Interno Certificado) - Ciudad de Panamá - ju. 20 octubre - vi. 21 octubre 2016

Gracias!

Lucas Allen | Managing Director/CEO
E: lallen@liquidnexxus.com

London: +44 20 33229095
Paris: +33 970730003
Johannesburg: +27 875504648
Sao Paulo: +55 3139560606
Mexico City: +52 8141707161
W: www.liquid-nexxus.com