The Future

Of Malware in ATM

Rafael Revert

Rafael.revert@cyttek.com

Experiencia

- Llevamos mas de 7 años en el sector de seguridad de la información Defensa y Banca
- Hemos auditado modelos de Cajeros ATM de Múltiples marcas (casi todas), además somos la empresa que mas experiencia tiene auditando cajeros de la región.
- Tenemos experiencia en Software XFS (casi todos los software XFS)
- En total mas de 44,000 ATMs cubren algunas de nuestras recomendaciones
- Mas de 30,000,000 USD en resolución de casos de faltantes de efectivo
- Monitorizamos miles de ATMs mediante nuestras soluciones de ATMs
- Hemos dictado cursos de Seguridad en Cajeros automáticos a mas de 50 instituciones bancarias en latino américa.
- Formamos parte de varias asociaciones y consejos de seguridad en ATMs
- Desarrollamos soluciones para Seguridad y monitorización para Cajeros Automáticos

E.A.S.T
European ATM Security Team
Associate Member

International Association Of Financial Crimes Investigators

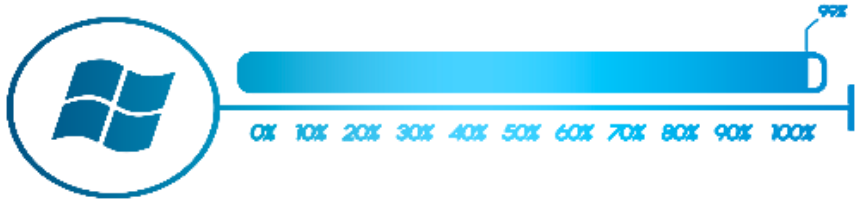
ATMIA
Cyttek Group
Proud member since 2016

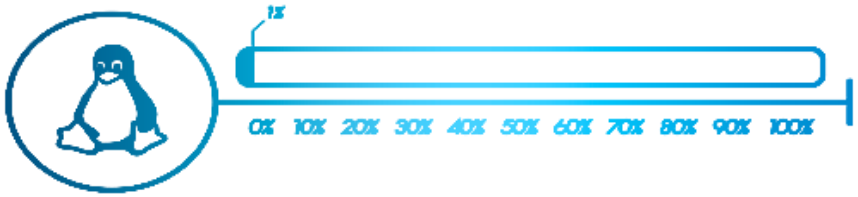
ATEFI
LATINOAMERICA

cyttek GROUP

Cajeros
Automáticos

www.cyttek.com


99%
0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%


1%
0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%


NCR SelfServ™
NCR SelfServ™

Hardware Anti skimming

TMDSECURITY
ANTI-SKIMMING TECHNOLOGY

ase ng Anti Skimming Eye New Generation

Software

checker ATM SECURITY
THE FIRST CUSTOM DESIGNED PRODUCT FOR FINANCIAL SELF-SERVICE PLATFORMS
FRAUD PREVENTION AND PCI-DSS COMPLIANCE FOR YOUR ATM NETWORK

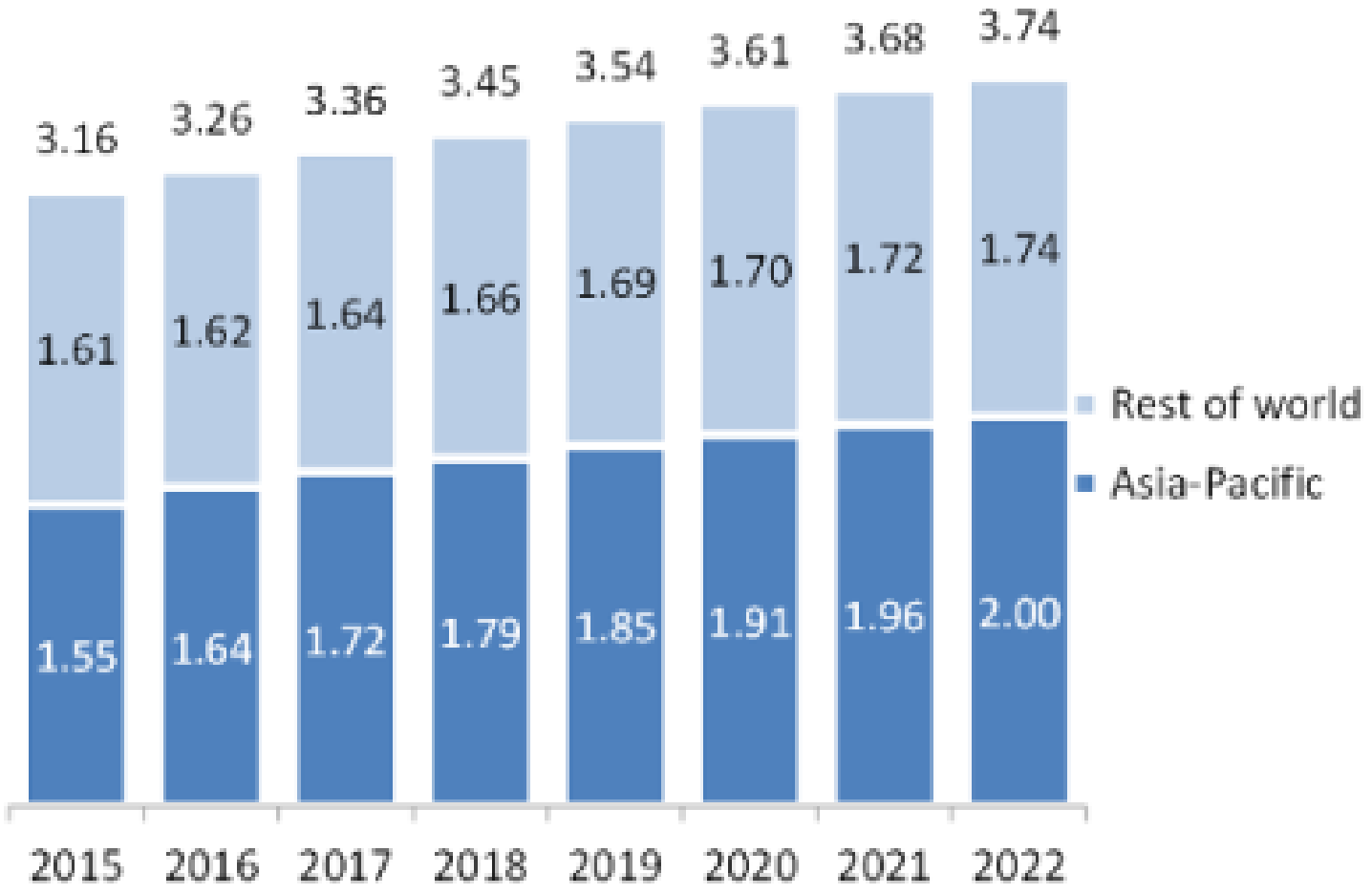
McAfee®

Symantec

S21sec

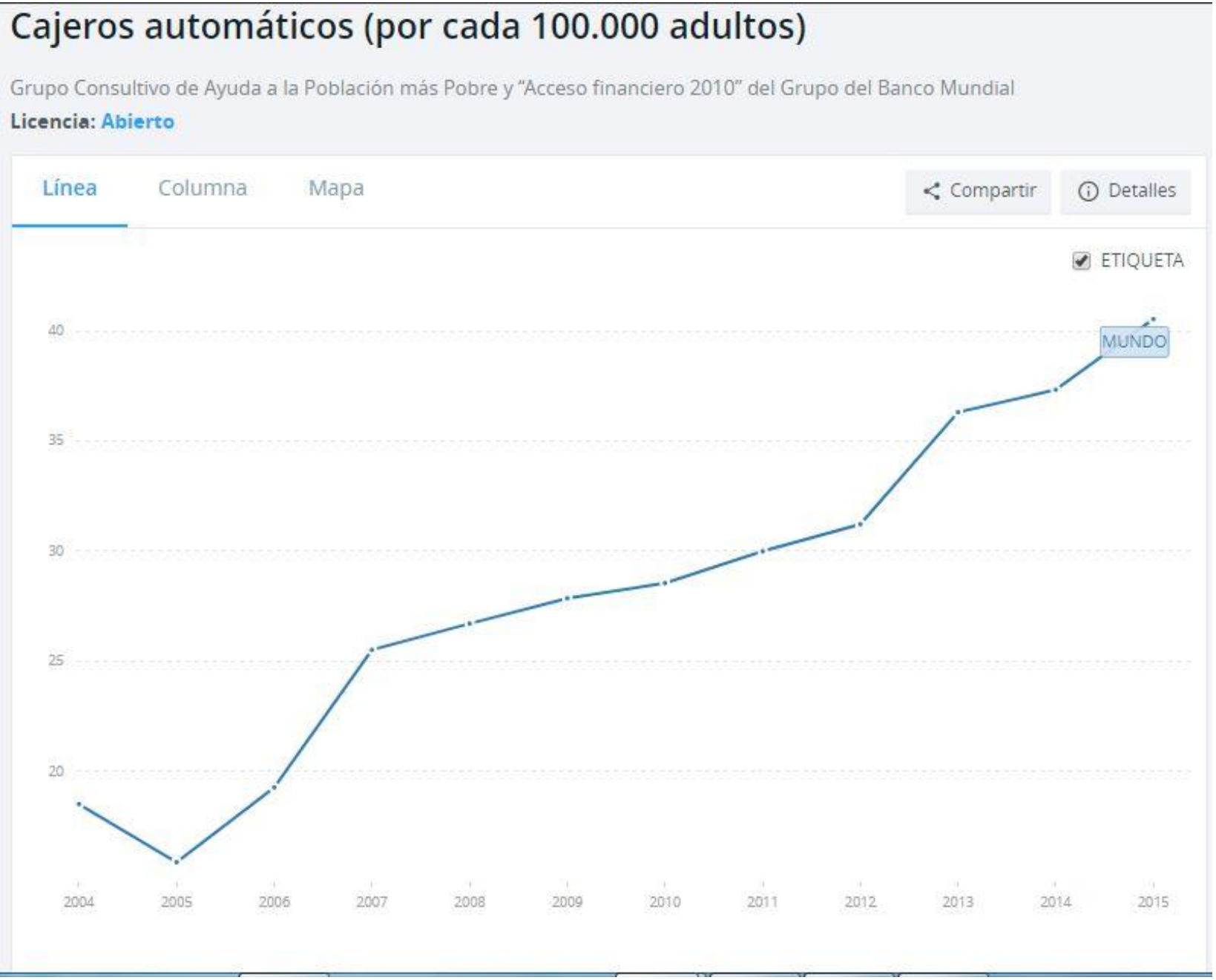
TREND MICRO™

Sensores, Anti-cash trapping, Cámaras etc..



Numero de ATMs en millones en todo el mundo

The number of ATMs installed worldwide grew by 3% to 3.3 million in 2016. As in recent years, the vast majority of new ATMs were installed in Asia-Pacific

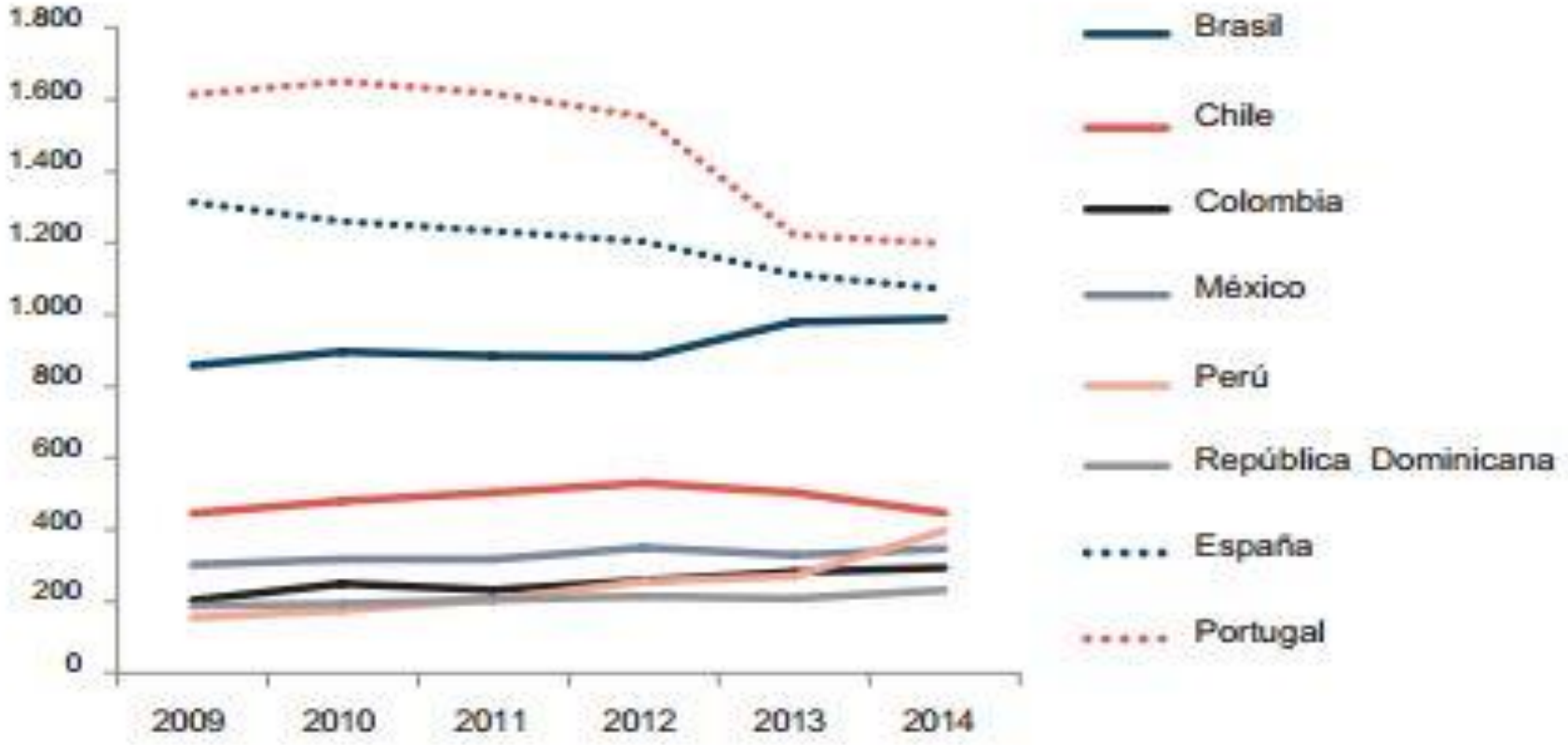


Cantidad de ATMs por persona en latino América

https://datos.bancomundial.org/indicador/FB.ATM.TOTL.P5?view=chart

Cantidad de ATMs por persona en latino América

Figura 14. Número de cajeros automáticos por cada millón de habitantes, 2009-2014



Fuente: bancos centrales y superintendencias de bancos.

http://www.tecnocom.es/-/crece-el-uso-de-cajeros-y-terminales-punto-de-venta-en-latinoamerica

Reportes de Ataques ATMs EUROPA

EUROPEAN ATM CRIME STATISTICS - SUMMARY						
ATM Related Fraud Attacks	**H1 2012**	**H1 2013**	**H1 2014**	**H1 2015**	**H1 2016**	**% +/- 15/16**
Total reported Incidents	9,595	12,676	7,345	8,421	10,820	**+28%**
Total reported losses	€131m	€124m	€132m	€156m	€174m	**+12%**
ATM Related Physical Attacks	**H1 2012**	**H1 2013**	**H1 2014**	**H1 2015**	**H1 2016**	**% +/- 15/16**
Total reported Incidents	968	1,007	1,032	1,232	1,604	**+30%**
Total reported losses	€8m	€10m	€13m	€26m	€27m	**+3%**

EAST also reported a 28% increase in ATM related fraud attacks, up from 8,421 in H1 2015 to 10,820 in H1 2016.
This rise was mainly driven by a 281% increase in Transaction Reversal Fraud *(up from 1,270 to 4,840 incidents).*
The downward trend for card skimming continues with 1,573 card skimming incidents
reported, down 21% from 1,986 in H1 2015.

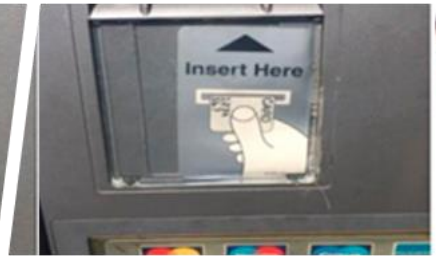
EUROPOL

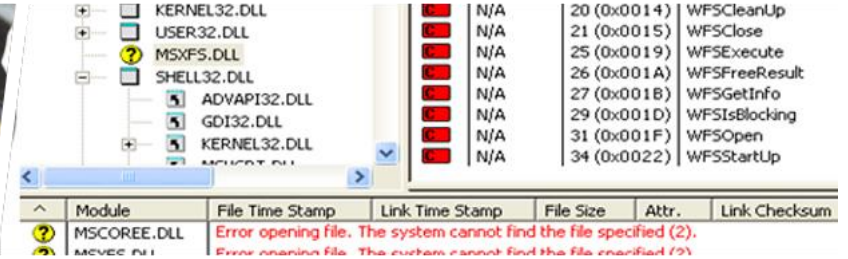
26 September 2017 - 20H00

Europol warns banks ATM cyber attacks on the rise

Share 6 Tweet Share submit Share

Malware

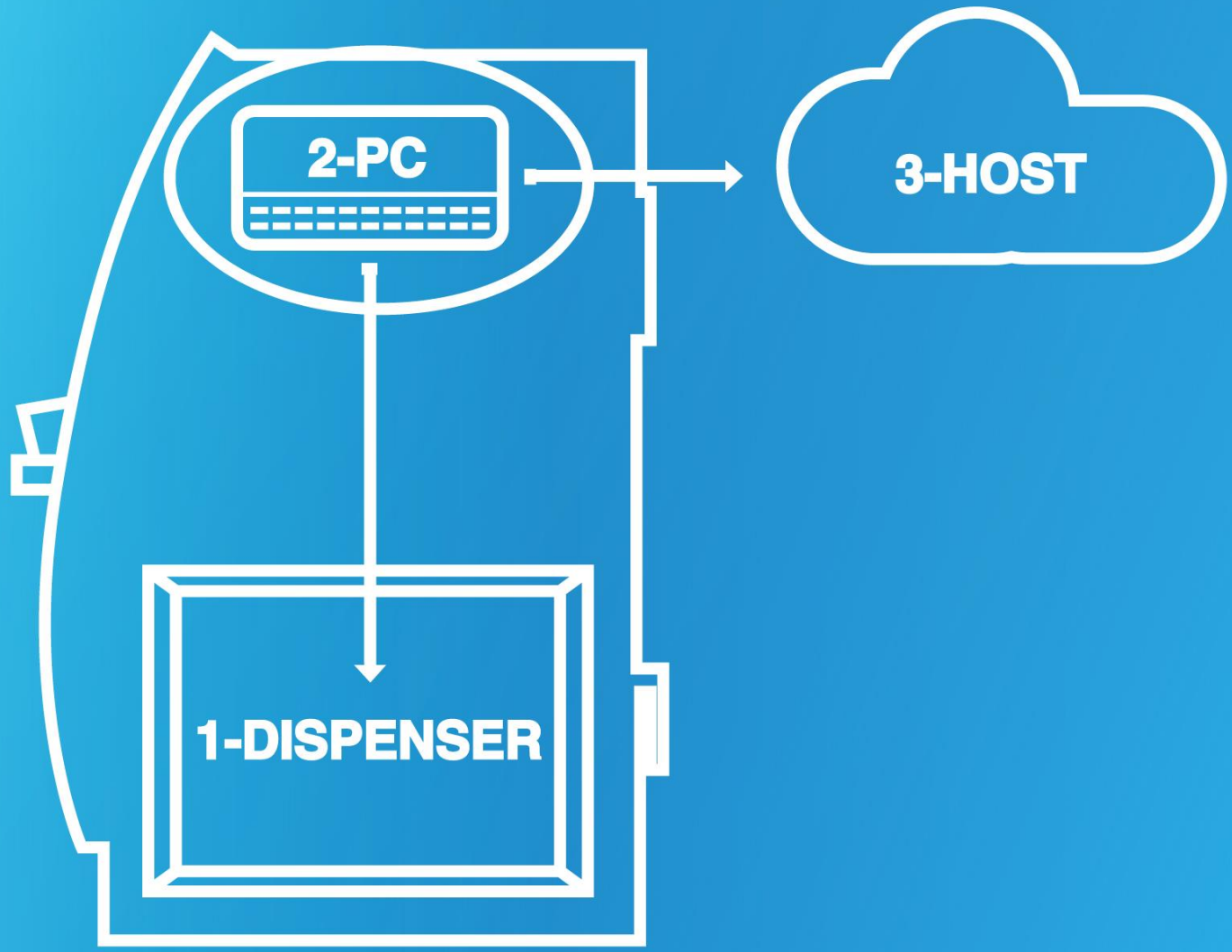

Insert Here


KERNEL32.DLL
USER32.DLL
MSXFS.DLL
SHELL32.DLL
ADVAPI32.DLL
GDI32.DLL
KERNEL32.DLL
N/A 20 (0x0014) WFSCleanUp
N/A 21 (0x0015) WFSClose
N/A 25 (0x0019) WFSExecute
N/A 26 (0x001A) WFSFreeResult
N/A 27 (0x001B) WFSGetInfo
N/A 29 (0x001D) WFSIsBlocking
N/A 31 (0x001F) WFSOpen
N/A 34 (0x0022) WFSStartUp
Module
File Time Stamp
Link Time Stamp
File Size
Attr.
Link Checksum
MSCOREE.DLL
Error opening file. The system cannot find the file specified (2).


CASH OPERATION PERMITTED.
INVALID CASSETTE NUMBER. TRY AGAIN.
TO START DISPENSE OPERATION -
ENTER CASSETTE NUMBER AND PRESS ENTER.

cyttek GROUP

Software



Skimer

First found: 2009
Language: Delphi
Goal: Dispense/skim

Ploutus

First found: 2013
Language: .Net
Goal: Dispense

Suceful

First found: 2015
Language: Borland C++
Goal: Prototyping tool

Green Dispenser

First found: 2015
Language: Visual C++
Goal: Dispense

Padpin

First found: 2014
Language: .Net
Goal: Dispense

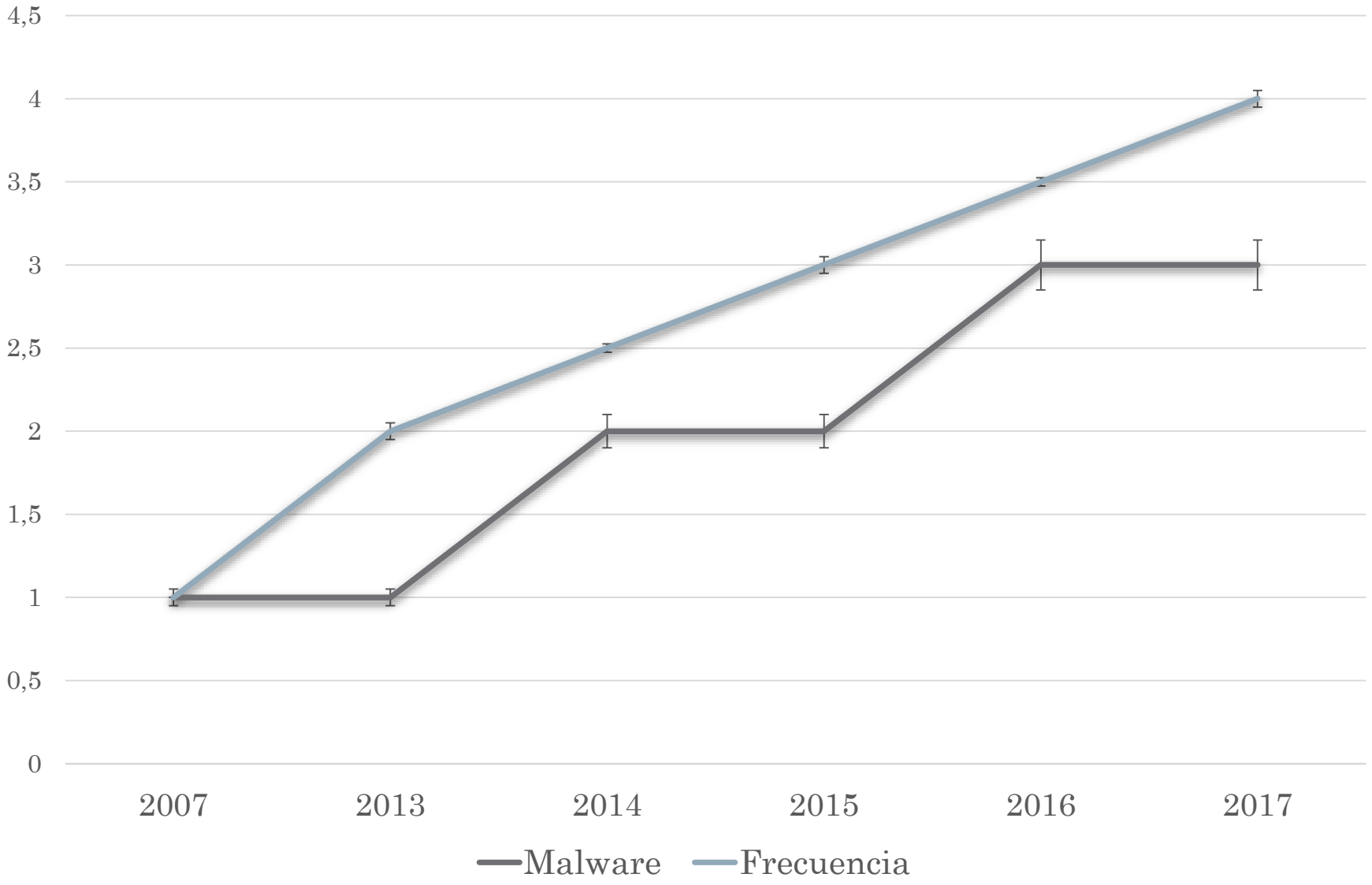
NeoPocket

First found: 2014
Language: VB
Goal: Skim

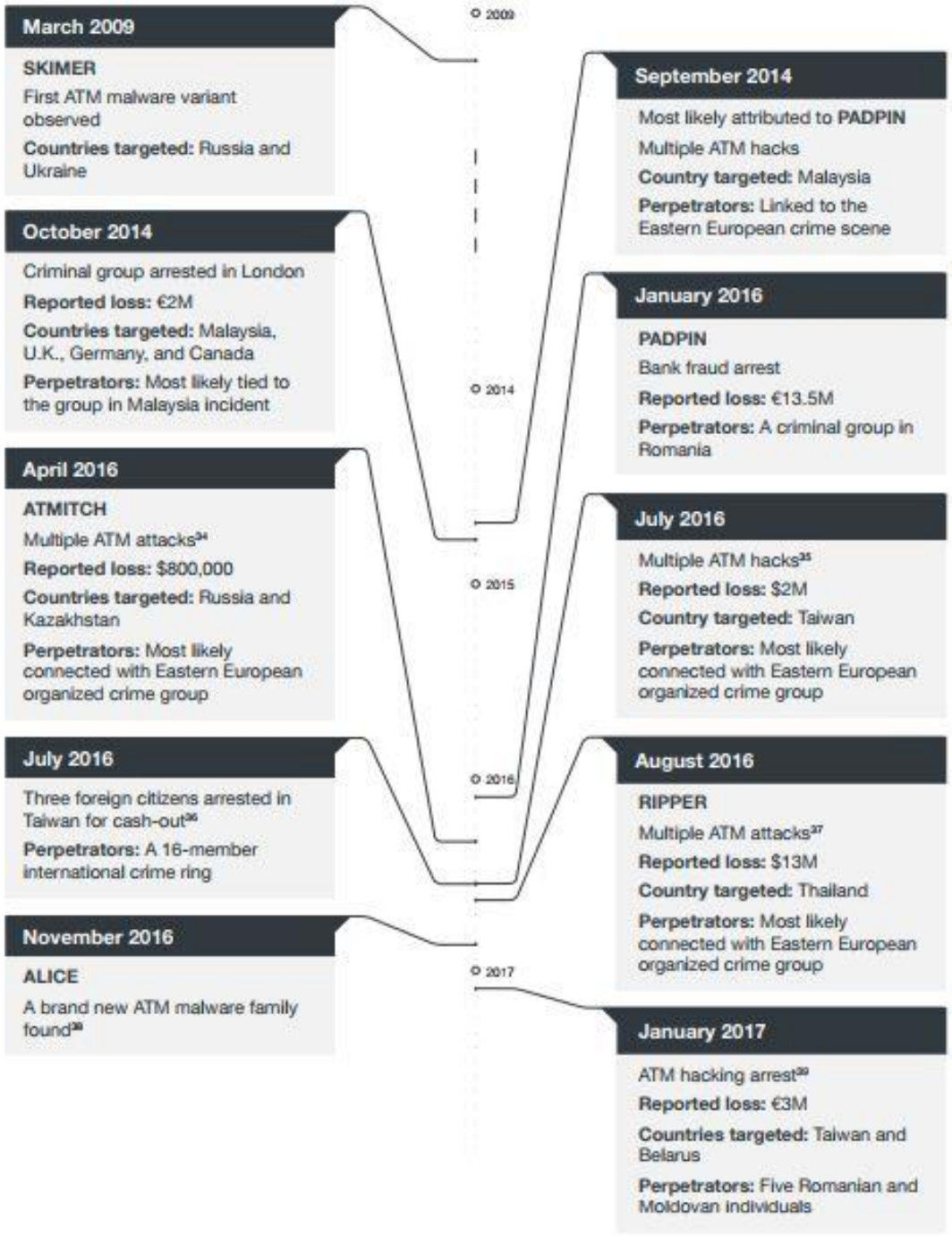
	Skimer	Ploutus	Padpin/ Tyupkin	NeoPocket	Suceful	Green Dispenser	Ripper	Malware Echo en LATAM XD
Año Descubierto	2007	2013	2014	2014	2015	2015	2016	2016 Sept.
Regiones Afectadas	Rusia, Ukraine, y EU	México	Europa, sur este Asia	N/A	N/A	Mexico	Thailand	México
Proveedor afectado	Diebold	NCR	NCR	Diebold	Diebold, NCR	Wincor	Diebold, NCR, Wincor	Diebold, NCR,
Tipo de instalación en el ATM	Desconocida	CD-ROM	CD-ROM	Desconocida	N/A	Desconocida	Desconocida	USB
Múltiples familias o variantes	Si	Si	No	No	No	No	No	SI
Lenguajes de programacion	Delphi	C# compiled into .NET	C# compiled into .NET	VB	Borland C++	Visual C++	Visual C++	C# compiled into .NET
Librería para acceder a los perimetrales	DbdDevAPI.dll	ncr.aptra.axfs.dll activexfscontrols.dll	MSXFS.dll	No accede perimetrales	MSXFS.dll	MSXFS.dll	MSXFS.dll	MSXFS.dll
Control de acceso implementado	Si	Si	Si	Si	No	SI	Desconocido	Desconocido
Dispensa efectivo	Si	Si	Si	No	No	Si	Si	Si
Roba información	Si	No	No	Si	Si	No	Desconocido	Si
Menú de usuario	Si	Si	Si	No	Si	Si	Si	No

	Skimer	Ploutus	Padpin/Tyupkin	NeoPocket	Suceful	GreenDispenser	Ripper	Malware Echo en LATAM XD
Comandos recibidos via	PIN pad	Keyboard, PIN pad, SMS	PIN pad	Raw socket, files	Keyboard, Mouse	PIN pad	Keyboard, PIN pad, bank card	Keyboard, PIN pad, raw socket
Lenguaje de Strings	Español	Ingles, Español	Ingles	Español	Ruso	Ingles	Ingles	Español
Roba datos cifrados	Si	No	No	Si	No	No	No	No
Campaña de ataque limitada a tiempo	No	Needs activation every 24hrs	Operates only at certain times	Operates before May 21st, 2014	No	Operates Jan 1st – Aug 31st2015	No	No
Persistente entre Reboots	Si	Si	Si	Si	No	No	Si	Si
Desabilita antivirus	No	No	Si (via otra herramienta)	Si	No	No	No	Si
Desabilita sensores ATM	No	No	No	No	Si	No	No	No

En este análisis no incluimos Malware Plotus.d, Alice, ATMitch

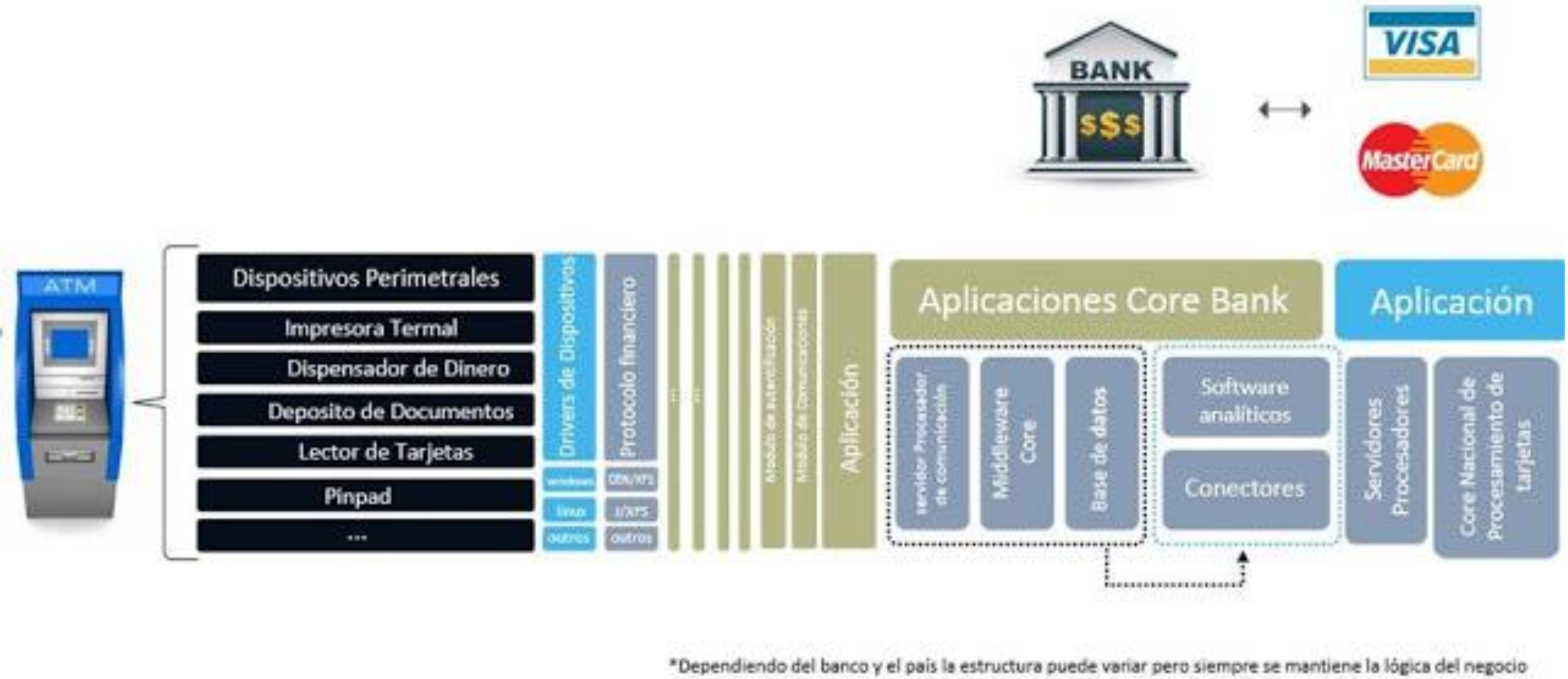


Frecuencia en cantidad de veces al año
Cantidad de software malicioso identificado durante el año en cuestión



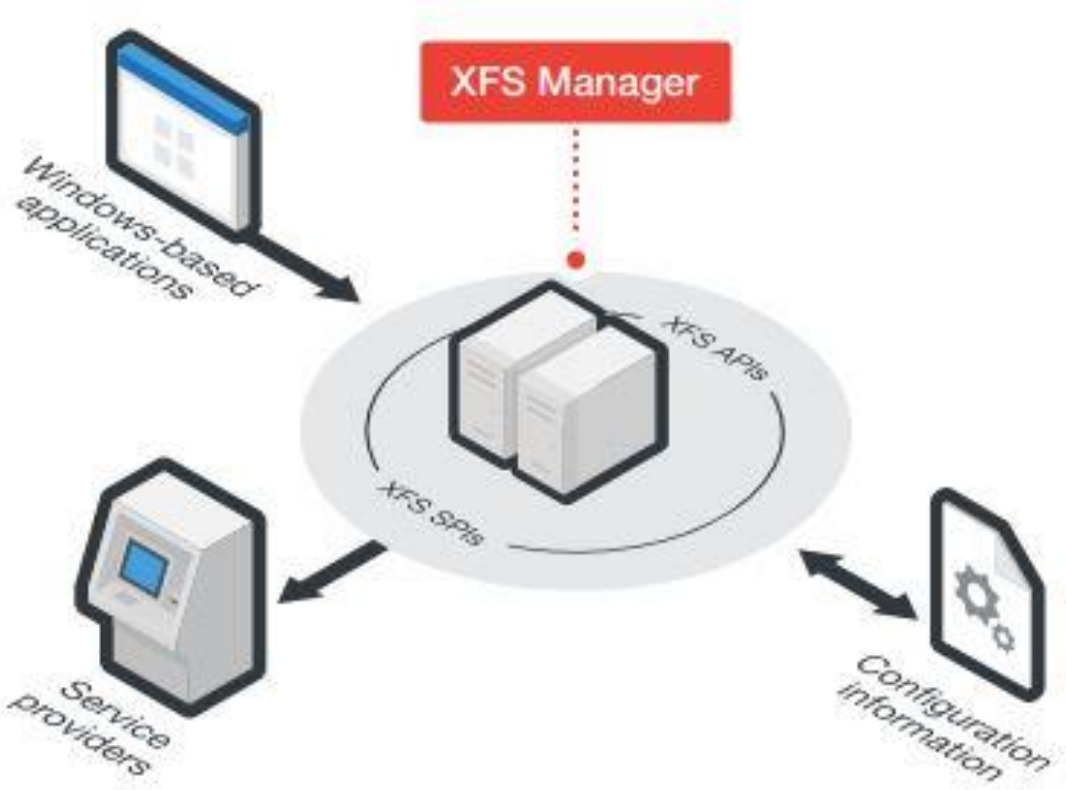
Frecuencia en cantidad de veces al año

Cantidad de software malicioso identificado durante el año en cuestión



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

Arquitectura XFS



Arquitectura XFS

El API del XFS tiene las siguientes funciones, estas funciones pueden usarse tanto para la operatividad normal como para el uso indiscriminado del malware:

- Funciones básicas – StartUp/CleanUp, Open/Close, Lock/Unlock, y Execute, son funciones comunes a todas las clases y dispositivos XFS.

- Funciones Administrativas – como son “Iniciación de dispositivo ”, reset, suspender y Resume.

- Comandos específicos – son usadas para requerir información del servicio o dispositivo en concreto y inicializar funciones puntuales.

Estos comandos específicos se envían a los dispositivos y son parámetros como GetInfo y Execute

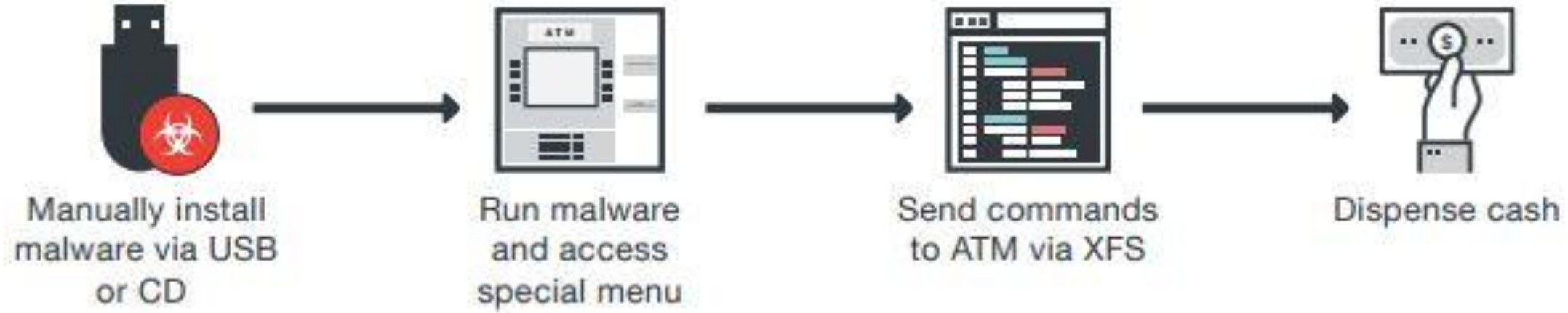
WOSA XFS Multivendor

- void DispenseAndPresent(long Amount, VARIANT NoteCounts, BSTR Currency, BSTR MixAlgorithm, long Timeout)

XFS – Agilis

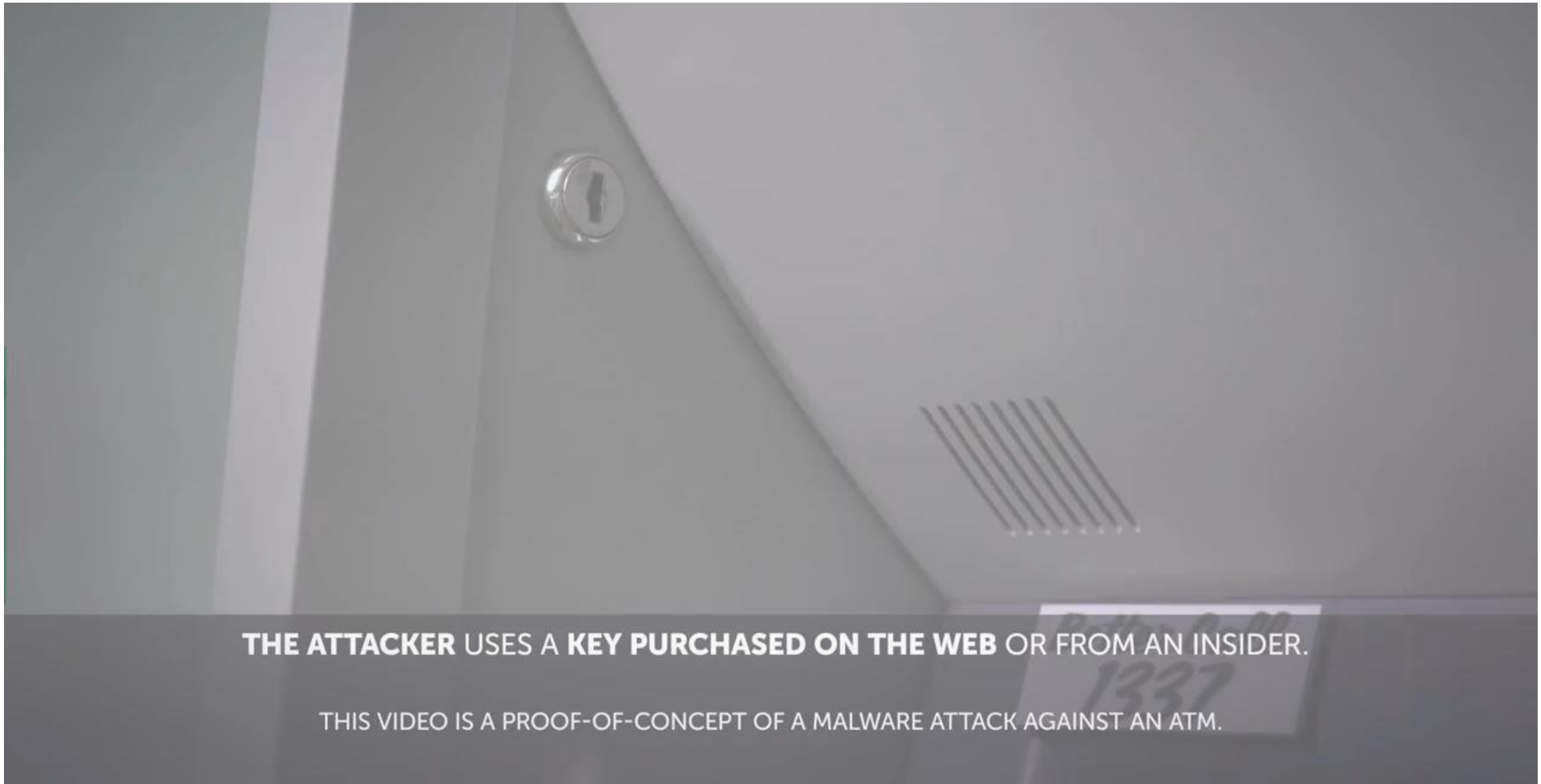
- WFSExecute(hServ, WFS_CMD_CDM_DISPENSE, (LPVOID) &cmdData, dwTimeOut, &wfsResult);

Ataques que requieren acceso fisico



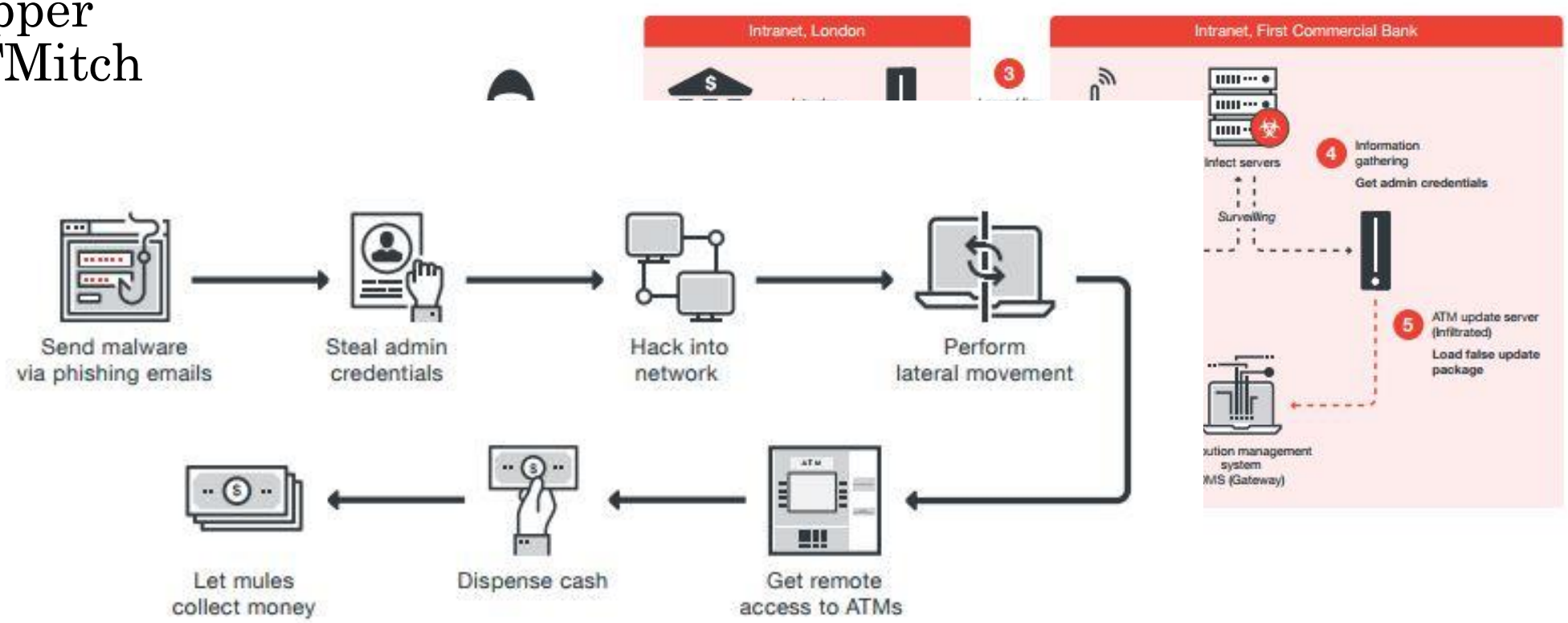
- Skimmer
- Plotus
- Padpin/Tyupkin
- GreenDispenser
- Alice

Ataques


THE ATTACKER USES A KEY PURCHASED ON THE WEB OR FROM AN INSIDER.
THIS VIDEO IS A PROOF-OF-CONCEPT OF A MALWARE ATTACK AGAINST AN ATM.

Ataques Mediante la Red

- Ataque en Taiwan en Julio 2016
- Cobalt Strike
- Anunak/Carbanak
- Ripper
- ATMitch



Software Exchange

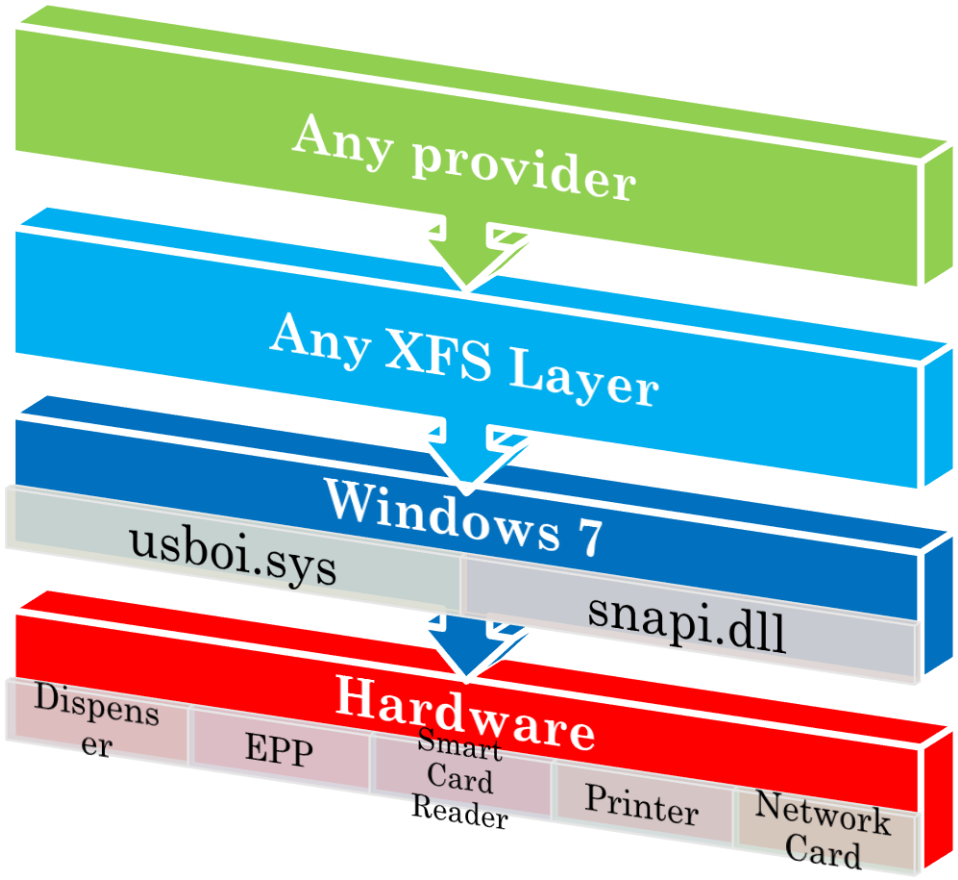
Financial Services MALWARE

XFS:
- Agilis
- Phoenix

WOSA XFS
- KAL
- NCR

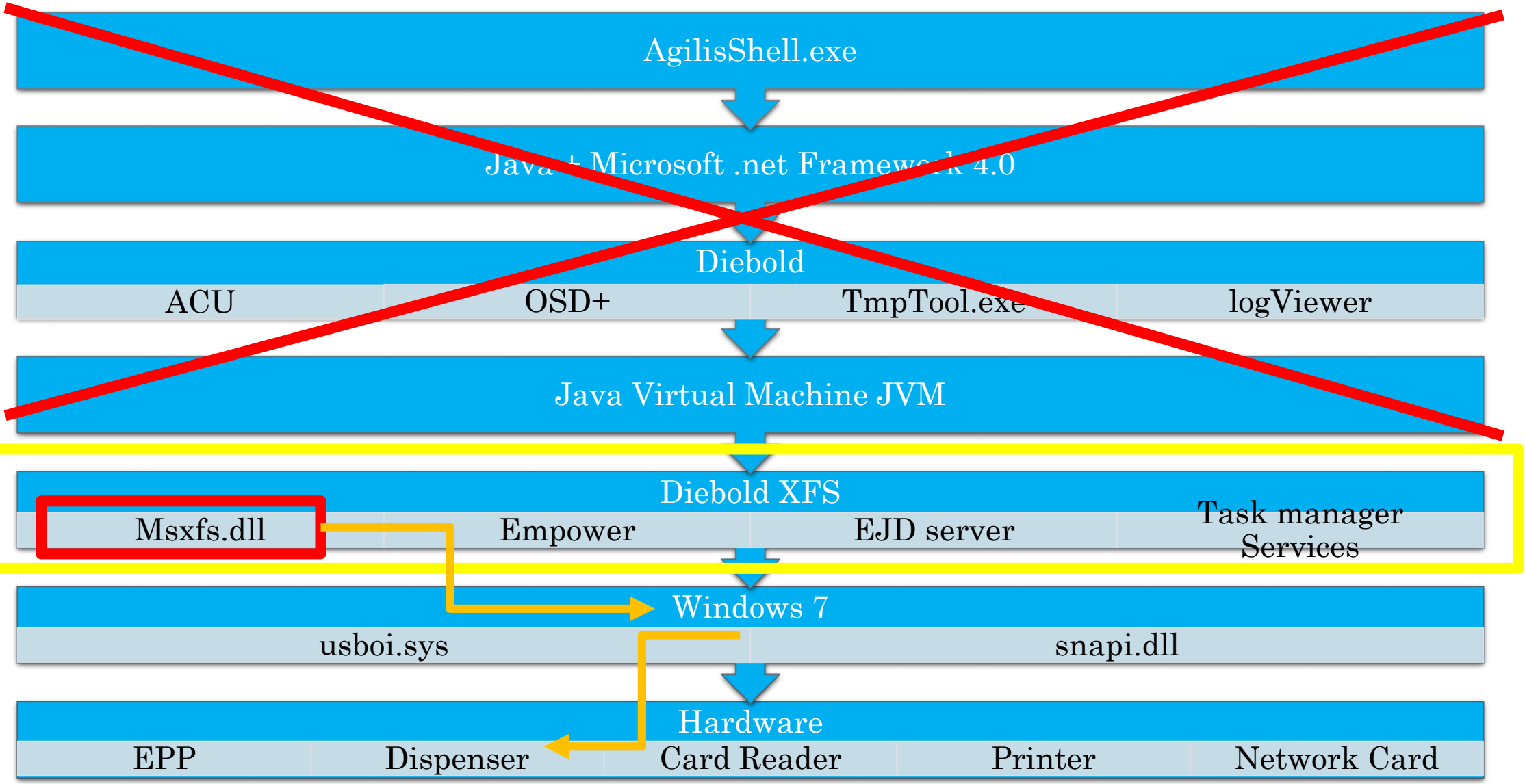
J/XFS
- Procash/Probase

- Comunicación Host – ATM
  - ISO 8583
  - NDC/DDC

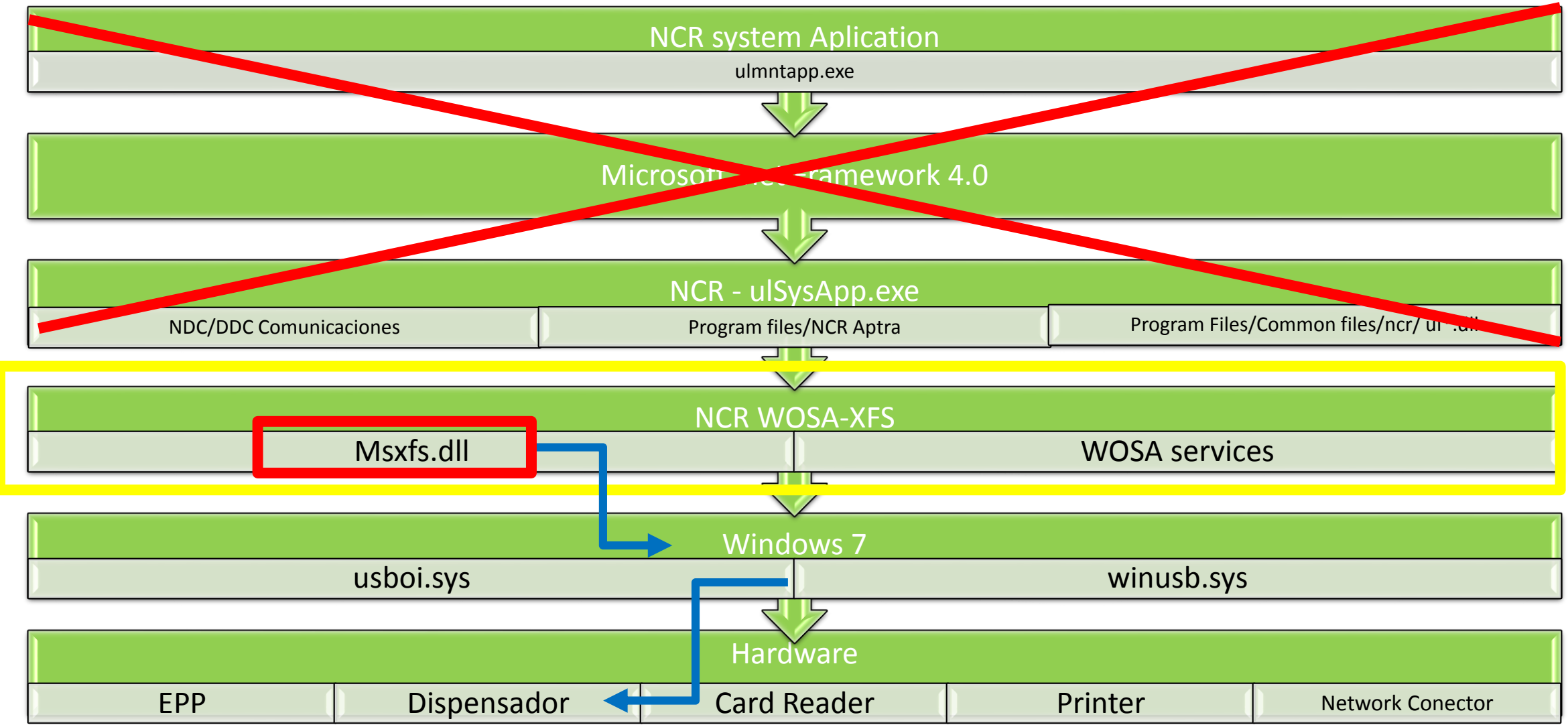


- **Dispenser communications can encrypted**
- **EPP can be connected to HSM**
- **Network Communications can have VPN configured**
- **Windows you can find a White listing (end-point security)**

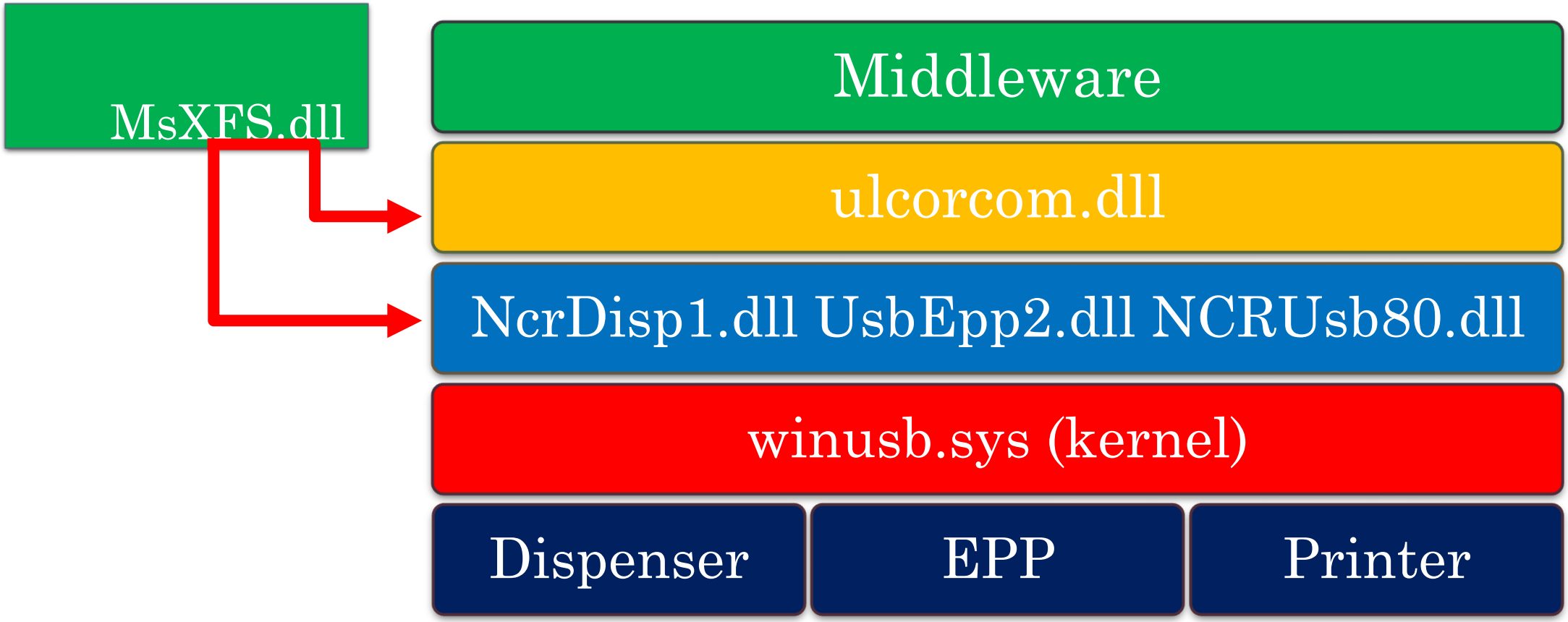
MALWARE


AgilisShell.exe
Java + Microsoft .net Framework 4.0
Diebold
ACU
OSD+
TmpTool.exe
logViewer
Java Virtual Machine JVM
Diebold XFS
Msxfs.dll
Empower
EJD server
Task manager
Services
Windows 7
usboi.sys
snapi.dll
Hardware
EPP
Dispenser
Card Reader
Printer
Network Card

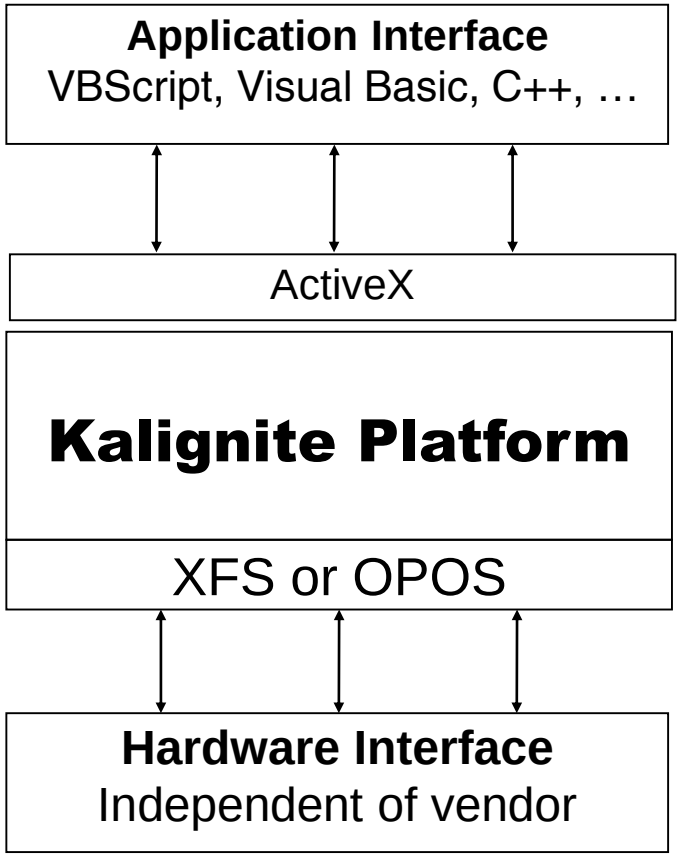
MALWARE


NCR system Aplication
ulmntapp.exe
Microsoft .Net Framework 4.0
NCR - ulSysApp.exe
NDC/DDC Comunicaciones
Program files/NCR Aptra
Program Files/Common files/ncr/
NCR WOSA-XFS
Msxfs.dll
WOSA services
Windows 7
usboi.sys
winusb.sys
Hardware
EPP
Dispensador
Card Reader
Printer
Network Conector

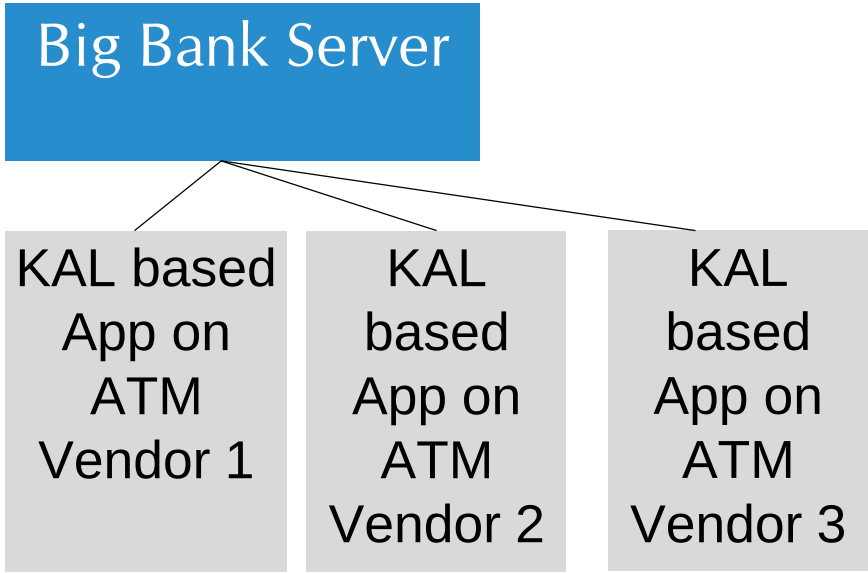
MALWARE

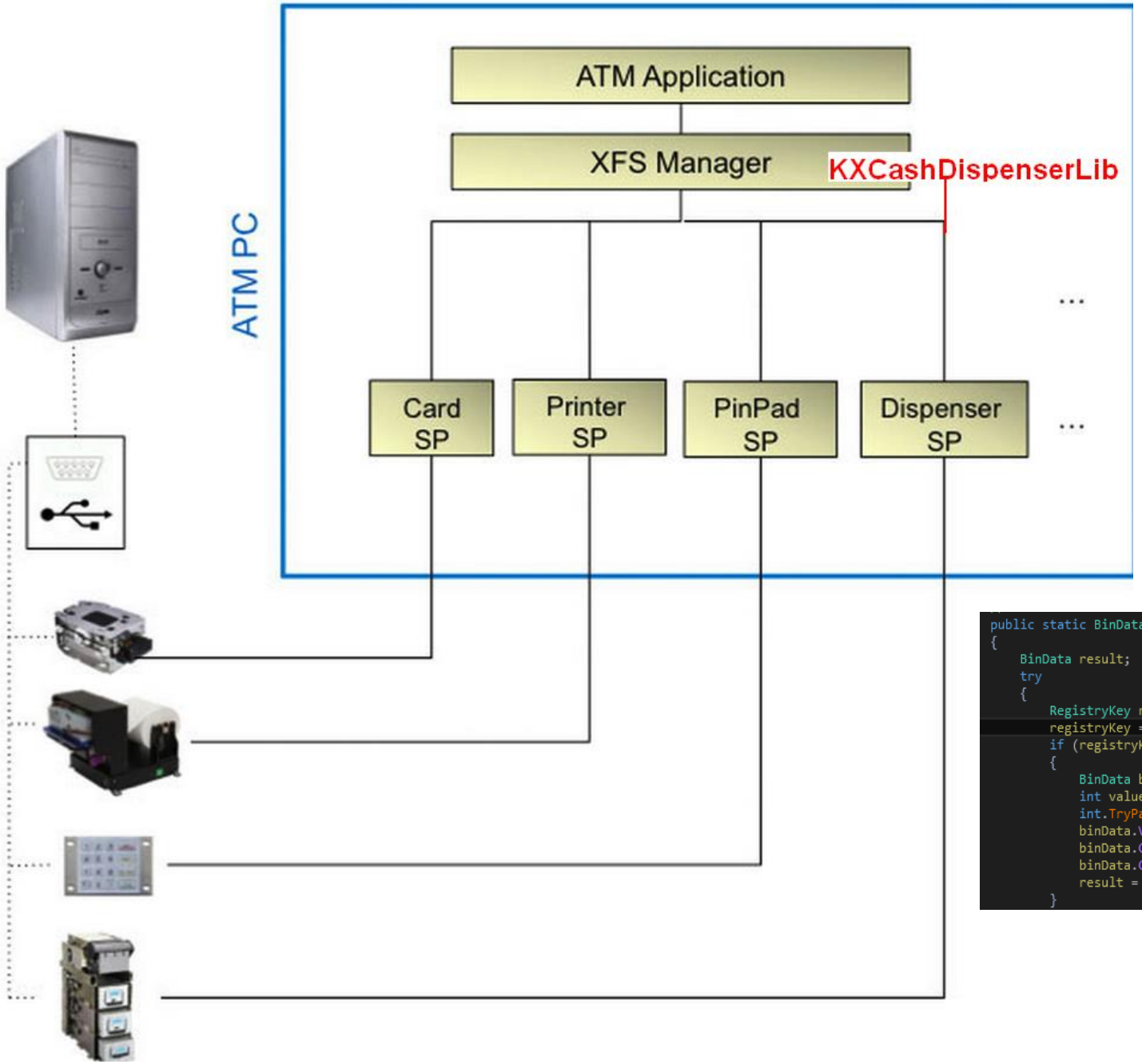

MsXFS.dll
Middleware
ulcorcom.dll
NcrDisp1.dll UsbEpp2.dll NCRUsb80.dll
winusb.sys (kernel)
Dispenser
EPP
Printer

Kalignite Platform is open at both the application interface and the hardware interface.



The Big Bank application based on the Kalignite Platform works on all vendor hardware.






```
public static BinData GetBIN(int BinNo)
{
    BinData result;
    try
    {
        RegistryKey registryKey = Registry.LocalMachine;
        registryKey = registryKey.OpenSubKey("SOFTWARE\\XFS\\PHYSICAL_SERVICES\\DBD_AdvFuncDisp\\Cassettes\\BIN" + BinNo,
        if (registryKey != null)
        {
            BinData binData = new BinData();
            int values = 0;
            int.TryParse(registryKey.GetValue("Values").ToString(), out values);
            binData.Values = values;
            binData.Cassette_ID = registryKey.GetValue("Cassette ID").ToString();
            binData.Cassette_Status = registryKey.GetValue("Cassette Status").ToString();
            result = binData;
        }
```

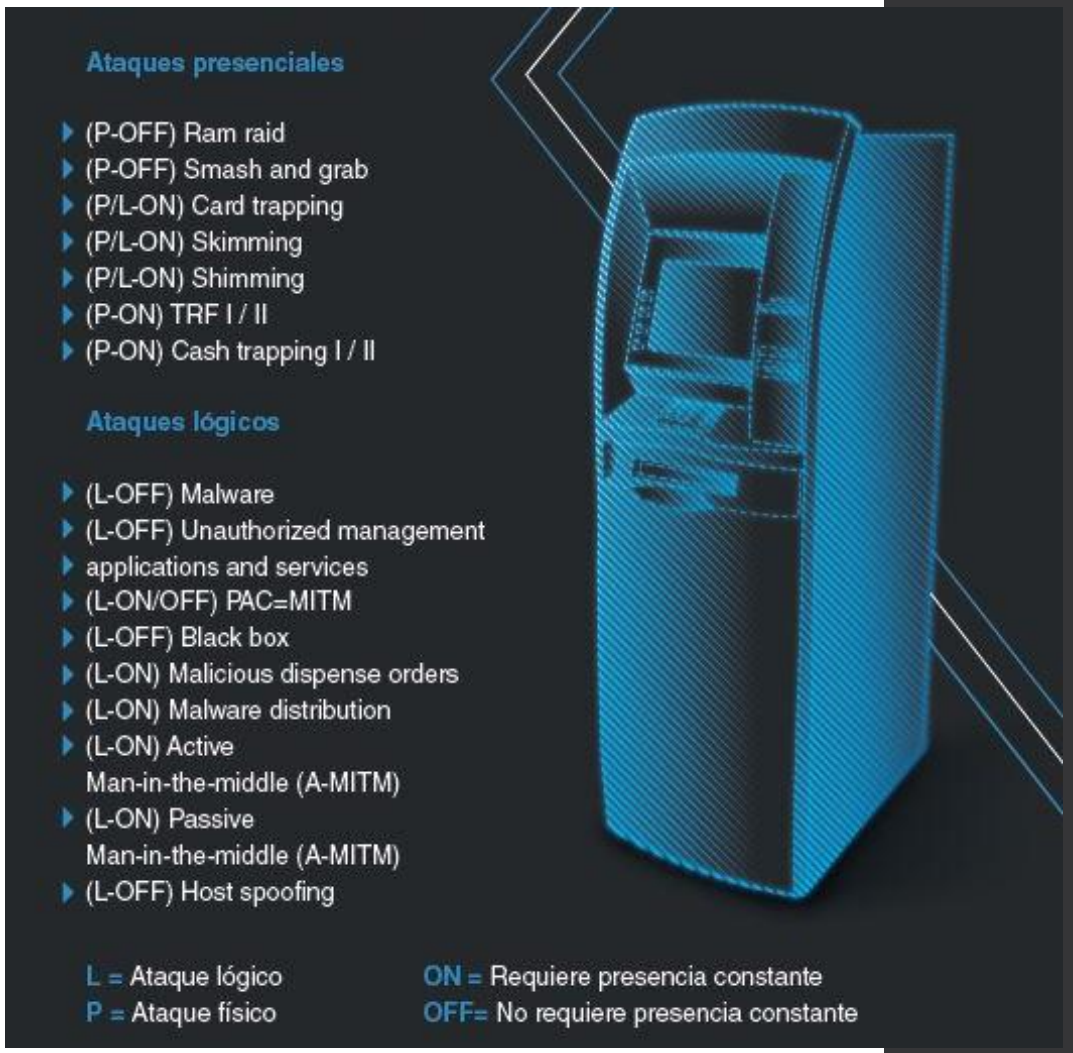
Taxonomía de UN ATAQUE

Taxonomía Seguridad Lógica

Vector de ataque	Tipo de ataque	Sub tipo
Dispensador	Lógico	Black box
Dispensador	Lógico	Insider (ETV/ING)
CPU	Lógico	PAC–MITM
CPU	Lógico	Utilerías no autorizadas
CPU	Lógico	Malware
Canal de comunicación	Lógico	Active Man-in-the-middle (A-MITM)
Canal de comunicación	Lógico	Passive Man-in-the-middle (P-MITM)
Canal de comunicación	Lógico	Host spoofing
Host	Lógico	Malicious dispense orders
Host	Lógico	Malware

Taxonomía Seguridad Física

Vector de ataque	Tipo de ataque	Sub tipo
Dispensador	Físico	Explosivos (Líquido)
Dispensador	Físico	Explosivos (Sólido)
Dispensador	Físico	Explosivos (Gaseoso)
Dispensador	Físico	Perforación - Incisión
Dispensador	Físico	Perforación - Calor
Dispensador	Físico	Robo
CPU	Físico	Perforación - Incisión
CPU	Físico	Perforación - Calor
CPU	Físico	Robo
CPU	Físico	Lectora de tarjetas - Skimming / Shimming
CPU	Físico	Vandalismo
Canal de comunicación	Físico	Robo
Canal de comunicación	Físico	Vandalismo
CPU - Dispensador	Físico	TRF I / II



RECOMENDACIONES

RECOMENDACIONES

Rule 1: Secure the BIOS

Rule 2: Establish an Adequate Operational Password Policy for all Passwords

Rule 3: Implement Communications Encryption

Rule 4: Establish a Firewall

Rule 5: Remove Unused Services and Applications

Rule 6: Deploy an Effective Anti-Malware Mechanism

RECOMENDACIONES

Rule 7: Establish a Policy for Applying Secure Operating System Hotfixes

Rule 8: Establish a Regular Patching Process for all Software Installed

Rule 9: Disable Windows Auto-play

Rule 10: Ensure the Application Runs in a Locked Down Account with Minimum Privileges

Rule 11: Define Different Accounts for Different User Privileges

Rule 12: Deploy a Remotely Authenticated Hard Disk Encryption Solution

RECOMENDACIONES

Rule 13: Ensure Communications between the ATM core and the Dispenser is protected

Rule 14: Perform a Penetration Test of your ATM annually

Rule 15: Use Software Distribution

Rule 16: Consider the Physical Environment of ATM deployment

Herramienta para colaborar en la información de los tipos de ataques

http://atmalerts.org/

Especialistas en seguridad para canales alternos

Rafael Revert

Rafael.revert@cyttek.com

www.cyttek.com

Gracias …