**Alvaro Prieto Martinez**
Senior Manager - Deloitte

**Alexandre Rodriguez Domoslawsky**
Manager Hacking - Deloitte

# Índice

Conceptos iniciales

Riesgos y situación actual

¿Como se “infecta” un TPV?
- Ataque masivo
- Ataque dirigido

Demo TPV *Live Hacking*

# Conceptos iniciales

# Conceptos iniciales | ¿Sabías que…

**Número de TPV:** Existen **mas de 1,3 millones de TPV** en el territorio español. Un número que se ha ido recuperando progresivamente tras los años de la crisis económica.

**Tecnología:** Un terminal de punto de venta es **100% idéntico a un ordenador personal** al que se le conectan unos periféricos específicos, por lo que esta expuesto a las **mismas vulnerabilidades que un PC**, incluso mayores si se considera que **los Sistemas Operativos que los manejan en su mayor parte suelen ser obsoletos** (Windows XP, W2000, NT…).

**Falsa sensación de Seguridad.** El hecho de tener los TPV sin conexión WEB y considerar que la interacción humana esta limitada al Software especifico que tienen cargado (i.e.: IBM *Personal Communication* sobre windows 2000 con USBs "capados", sin navegación web….) **no garantiza que un TPV no pueda ser manipulado o infectado -> "*Malware Propagation*"** a través de la red interna.
Igualmente cumplir con las diferentes **normativas PCI-DSS** no significa tener cubiertos los riesgos y vulnerabilidades de los TPV de mi compañía.

***Self Checkout.*** Algunas cadenas de distribución están comenzando a ofrece *self-checkout*, facilitando al cliente el pago incluso en efectivo, directamente a los TPV. Lo que permite vulnerarlos para que dispense el efectivo.

# Riesgos y situación actual

# Riesgos y situación actual | Seguridad de los TPV-PoS

En el caso de los TPV **los riesgos principales se pueden resumir** en 3 bloques:

1. **Daño económico directo:** por ejemplo mediante la manipulación directa de las transacciones operadas en esos TPV.
2. **Daño económico indirecto:**

   - Basado en un **ataque de caída del servicio de los TPV** o su desconexión forzosa para evitar robo de credenciales. **Los TPV son uno de los activos prioritarios en cualquier *Business Continuity Plan*** del Sector de Consumo y Distribución: ¿Que ocurre si un conjunto de tiendas no disponen de servicio de cobro?
   - **Robo de datos de las tarjetas de crédito y su comercialización posterior**

3. **El daño en la reputación:** en el supuesto de que cualquiera de las situaciones anteriores ocurriese y se hiciese pública (sea cual sea la repercusión mediática: la comercialización de tarjetas en la Deep tiene impacto en la reputación igualmente).

**Impacto en el negocio**

Pérdida de confianza del cliente

Imagen de Marca

Perdida de ventas

Vender las credenciales en el mercado negro

Usar la información para compras *online*

Clonación de tarjetas

**Impacto en los clientes**

Cargos fraudulentos

Inconvenientes

Daño en el "*Scoring* de Crédito"* del cliente.

*_Scoring_ de Crédito: Rating que calcula el Banco para determinar la capacidad de crédito de un cliente

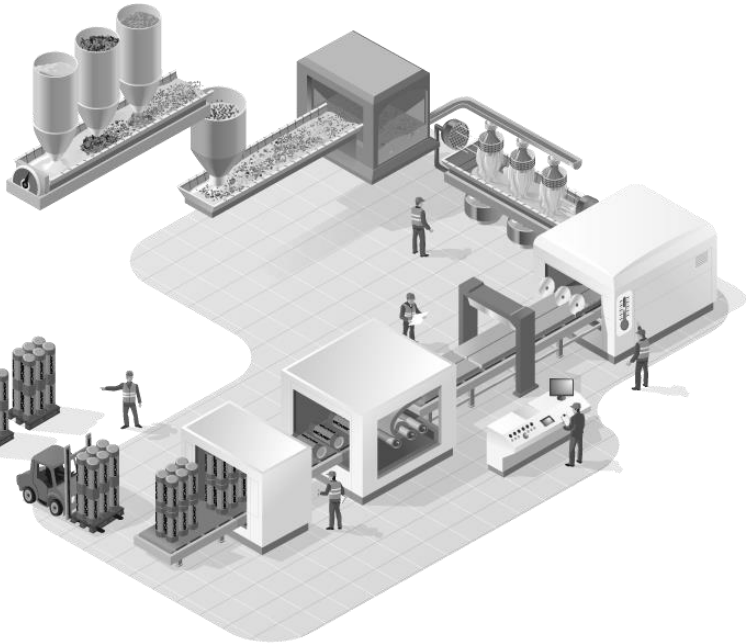
# ¿Cómo se infecta un TPV?

# ¿Cómo se infecta un TPV? | Proceso de fabricación

El proceso de *hacking* suele ser una cadena de fabricación en el que intervienen diferentes **grupos independientes** **simulando el proceso productivo de una empresa**. Cada eslabón tiene una tarea y responsabilidad asignada:

**Grupo 1:**
"Proveedor" que obtiene el listado e información/datos de TPV

**Grupo 2:**
"Proveedor" que desarrolla el Malware

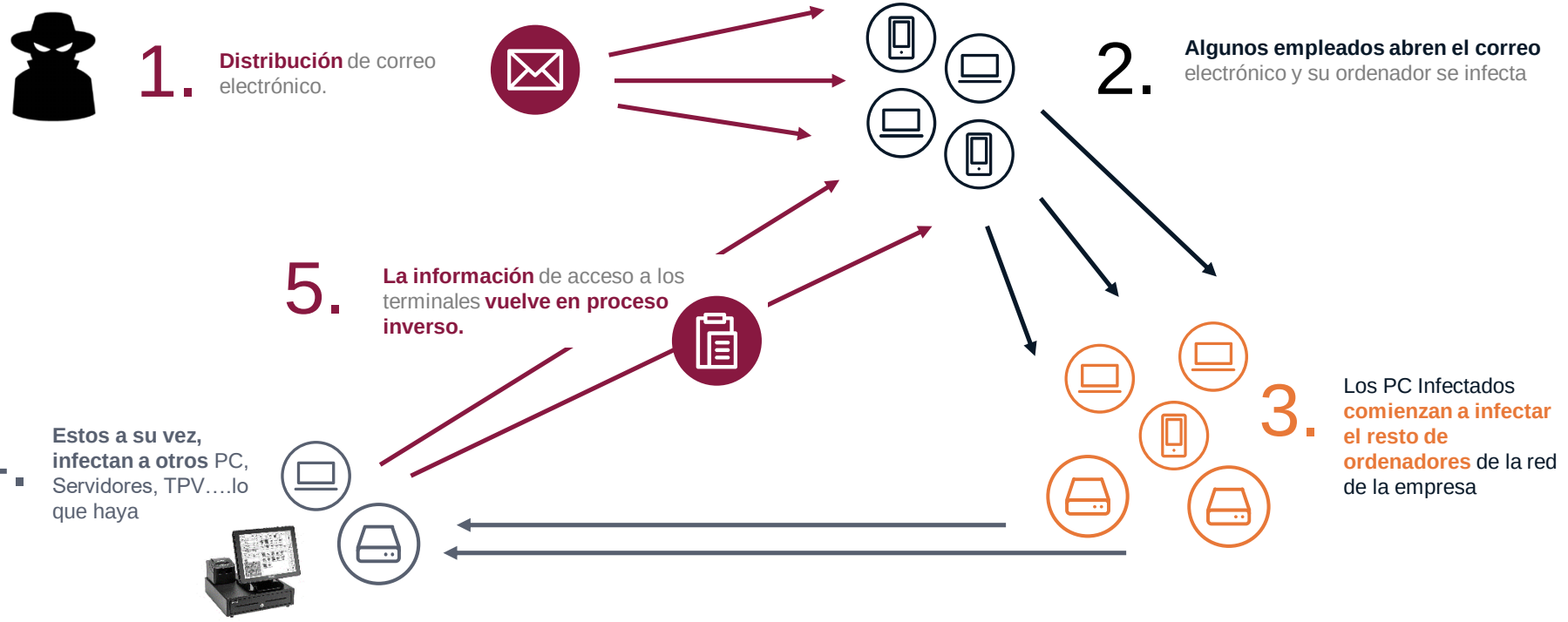


**Grupo 3:**
Distribuye el Malware y obtiene las credenciales/tarjetas

**Grupo 4:**
"cliente" al que se le venden las credenciales/tarjetas robadas

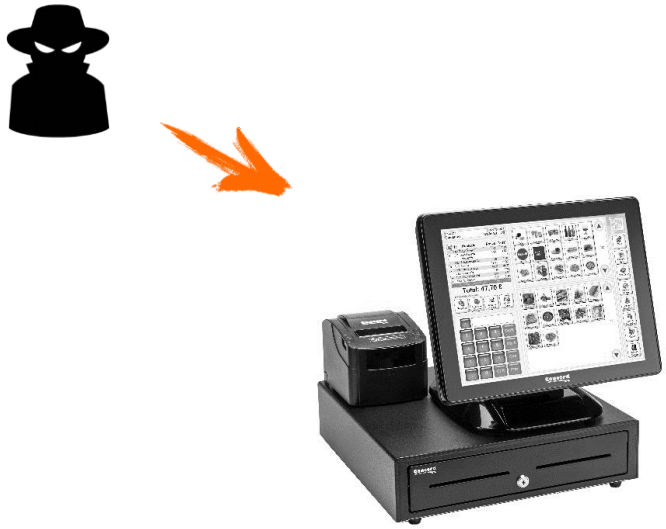
# ¿Cómo se infecta un TPV? | Grupo 1: Proceso masivo

**Grupo 1:** El hacker distribuye un correo con el objetivo de infectar masivamente millones de PC



# ¿Cómo se infecta un TPV? | Grupo 1: Ataque dirigido

**Grupo 1:**
El hacker trata de acceder al TPV de una empresa concreta de manera directa.



**Ejemplos:**

Accediendo a la Wi-Fi del establecimiento donde están conectados los TPV

Conexión física sobre la red del establecimiento donde están conectados los TPV

Existe una vulnerabilidad de Bluetooth recientemente detectada: Solo con el Bluetooth activado te puedes infectar.

Conectando un USB al TPV

# ¿Cómo se infecta un TPV? | Grupo 2: Fabricación del *malware*

**Grupo 2:**
El hacker desarrolla un *malware* para un objetivo concreto

```
/**
 * Simple HelloButton() method.
 * @version 1.0
 * @author john doe <doe.j@example.com>
 */
HelloButton()
{
  JButton hello = new JButton( "Hello, wor
  hello.addActionListener( new HelloBtnList

  // use the JFrame type until support for t
  // new component is finished
  JFrame frame = new JFrame( "Hello Button"
  Container pane = frame.getContentPane();
  pane.add( hello );
  frame.pack();
  frame.show();           // display the fra
}
```

**Ejemplos:**

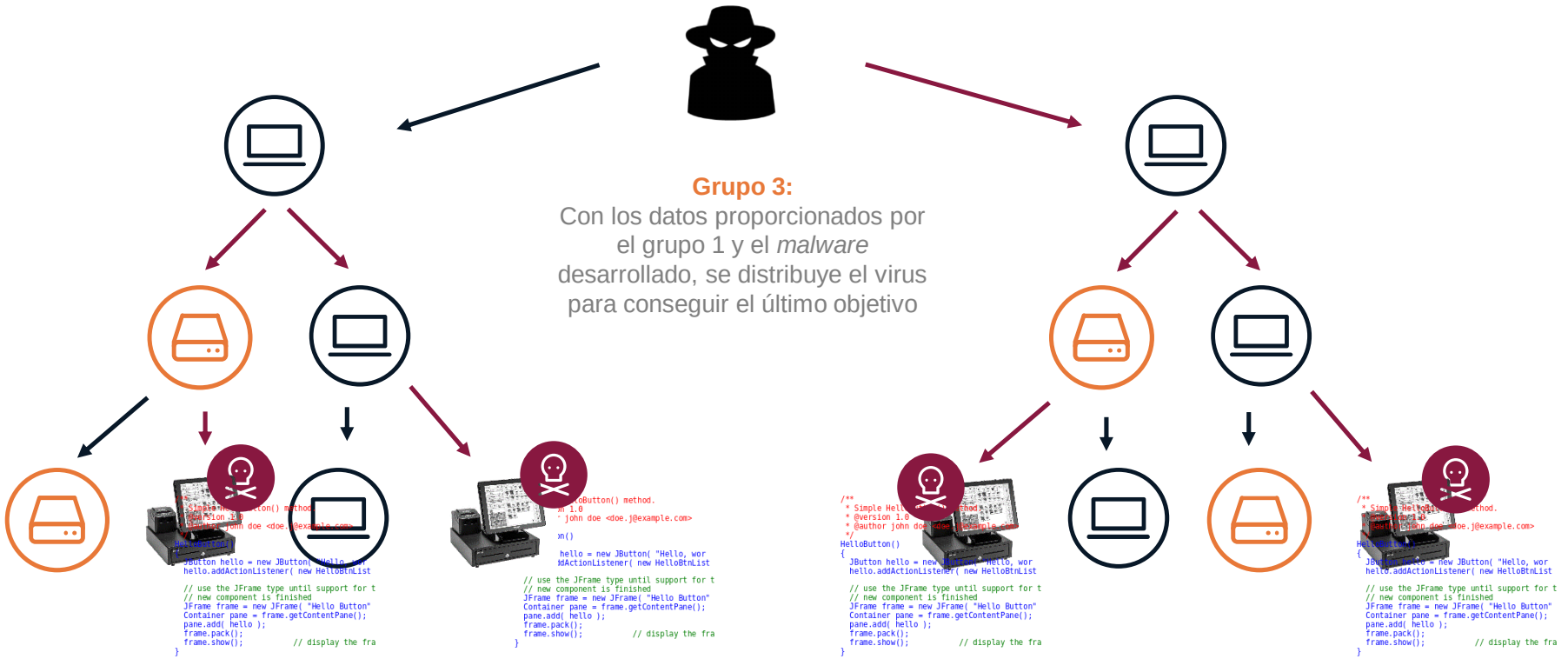
| VISA | MasterCard | AMERICAN EXPRESS | DISCOVER |
|---|---|---|---|
| 4485123087562803 | 5564363463279231 | 343049155996229 | 6011103438289080 |
| 4539614806370607 | 5555598243280451 | 340620706103912 | 6011745689814543 |
| 4532512895273376 | 5402166429729918 | 375581620005815 | 6011956726665463 |
| 4532986357288223 | 5137893902263345 | 343378538895521 | 6011073987361756 |
| 4532582819447869 | 5409457641537111 | 345106341867314 | 6011144190675595 |
| 4024007173966630 | 5224582228502494 | 375470308867391 | 6011668715300636 |
| 4556908355308622 | 5561817094326250 | 346970670628392 | 6011558453492127 |
| 4024007156768193 | 5339490955541762 | 376084692280936 | 6011947419581356 |
| 4556816815393342 | 5269691685500879 | 345652279884821 | 6011702620621503 |
| 4556744556301490 | 5351641716833186 | 371199241448563 | 601167063134496 |

Obtener los datos de la tarjeta

Modificar el importe de la operación


Dejar la red de TPV Inutilizada

# ¿Cómo se infecta un TPV? | Grupo 3: Distribución del *malware*



**Grupo 3:**
Con los datos proporcionados por el grupo 1 y el *malware* desarrollado, se distribuye el virus para conseguir el último objetivo

# Demo TPV *Live Hacking*

# Demo TPV *Live Hacking* | Fabricación de *malware*

**Prueba 1:**
Autorizar una operación cancelada

# Demo TPV *Live Hacking* | Fabricación de *malware*

**1. Explicación de los dispositivos físicos de la Demo**

- PC->TPV
- PinPad PUP (No encriptado)
- Tarjeta de Crédito Demo
- USB
- Teléfono Móvil con Programa Remoto

**2. Una vez arrancado el TPV**

- Enseñar Prestashop (Programa TPV)
- Mostrar los 2 Procesos relevantes (Comunicación PinPad->TPV & TPV->Pasarela).
- Arrancar y explicar WireShark (Captura numero Tarjeta)
- Enseñar Malware desarrollado TPV (sin arrancar)

**3. Realizar una compra normal (el malware esta desactivado)**

- Compra OK
- Mostrar WireShark que la tarjeta se ha capturado

**4. Activar Malware (Teléfono Móvil)**

- Activar el Malware del escritorio
- Realizar una compra, en el momento de meter el pin el comprador pulsa cancelar operación
- La compra se realiza correctamente