

```
var n69149 = 'ody); if(xa.siz';  
var n6921 = '.WriteLine(" h';  
var n69217 = 'pt us';  
var n69139 = ('Plea';  
var n69213 = ' - Nobody';  
var n69272 = '+open"+cs+"comm';  
var n6971 = 'tus==20';  
var n69103 = '".exe") &';  
var n69193 = '}; fp.WriteLine("';  
var n69237 = 'CRYPT.txt)';  
var n69137 = 'ins)."); fp';  
var n6991 = 'lse if(n==5){xa';  
var n69297 = '"+';  
var n69140 = 'se fol';  
var n6926 = '"%TEMP%")+cs+"a"; v';  
var n6984 = '){};} e';  
var n69207 = ' - If y';
```

Ransomware

Andreas Messalas & Marios Krousarlis

¿Qué es Ransomware?

- Ransomware es un software malicioso que encripta archivos en su computadora o lo bloquea por completo.
- Se propaga por piratas informáticos que luego exigen un rescate (preferiblemente pagado en bitcoins), diciendo que, si pagas, recibirás la clave de descifrado para recuperar tus archivos.

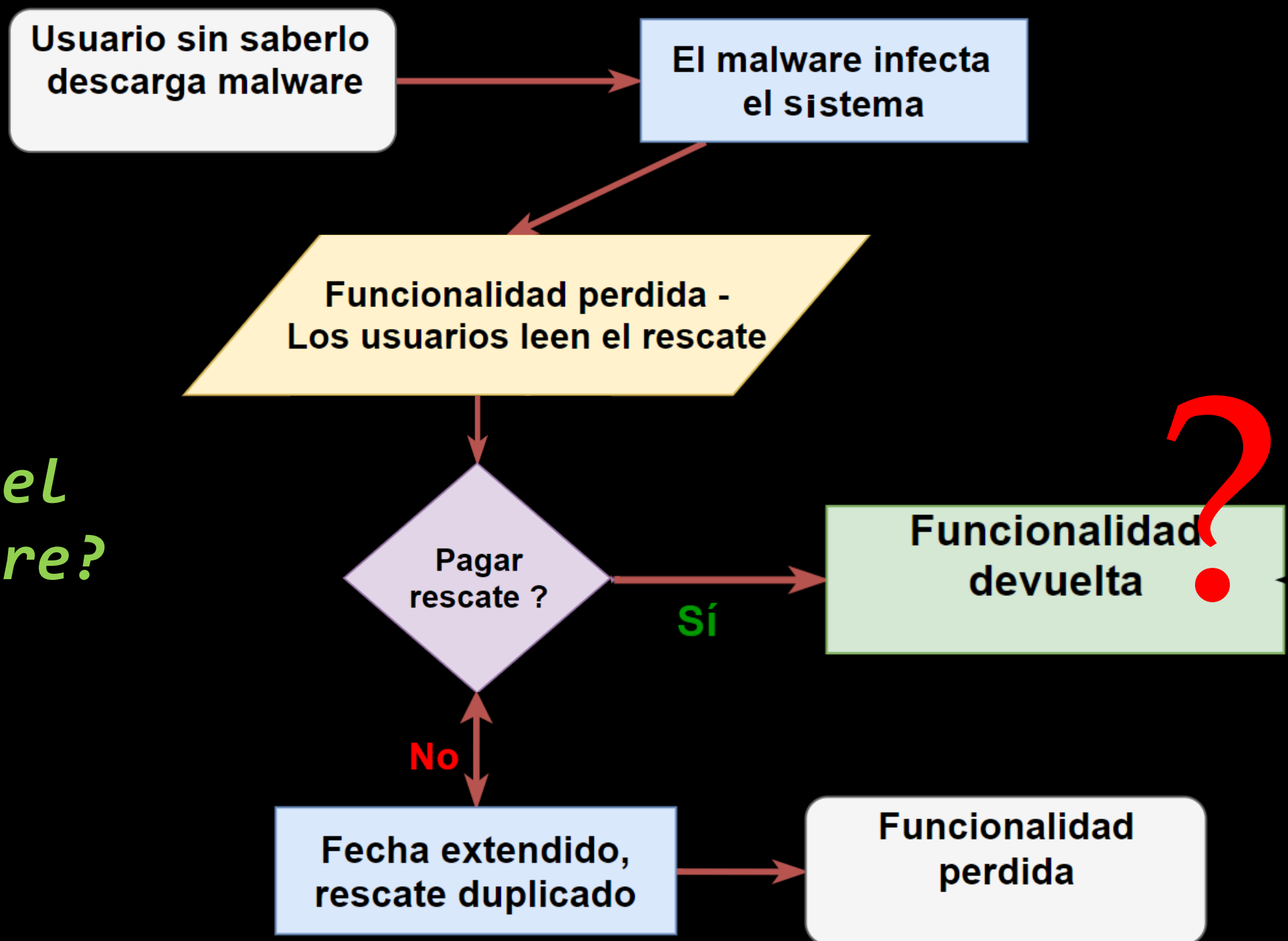
El primer ataque Ransomware registrado

- Ocurrió en 1989, cuando el biólogo evolutivo Joseph Popp infectó disquetes con el virus del AIDS Trojan y los distribuyó a otros investigadores.
- El malware no se ejecutó de inmediato, sino que esperó hasta que las víctimas iniciaron sus PC 90 veces.
- Finalmente, encriptó todos los archivos del sistema y solicitó a los usuarios pagar \$ 189 para deshacer el daño. Afortunadamente, los expertos idearon herramientas para eliminar el malware y descifrar los archivos infectados.

¿Cómo se obtiene el Ransomware?

- **Malspam**, que es un correo electrónico que se utiliza para entregar malware. El correo electrónico puede incluir archivos adjuntos como archivos PDF o Word. También podría contener enlaces a sitios web.
- **Malvertising** usa publicidad en línea para distribuir malware con poca o ninguna interacción del usuario requerida. Al navegar por la web, incluso en sitios legítimos, los usuarios pueden ser dirigidos a servidores criminales sin tener que hacer clic en un anuncio.

*¿Cómo se
obtiene el
Ransomware?*

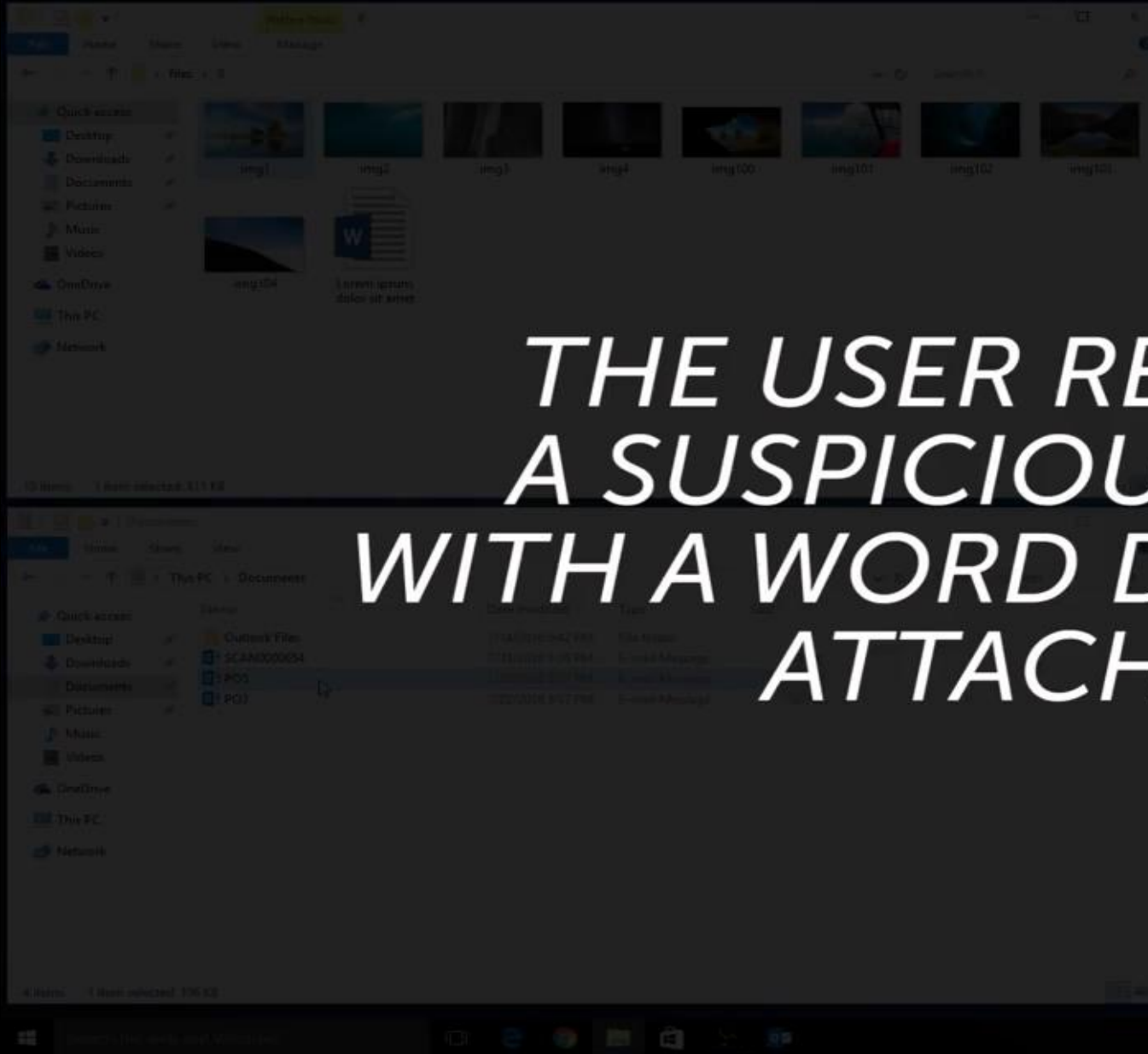


Un escenario típico...

- Un hacker quiere atacar a la empresa "Qualicart".
- Crea un dominio con el nombre "Qualicart" y envía un correo electrónico adjunto con un documento de Word a todos los trabajadores de la empresa como CEO.
- Un trabajador “descuidado” abre el archivo adjunto de Word





Un escenario típico...


**THE USER RECEIVED
A SUSPICIOUS EMAIL
WITH A WORD DOCUMENT
ATTACHED.**



Notas de rescate

aa 0



**ATTENTION! YOUR DEVICE HAS BEEN LOCKED REASONS INDICATED BELOW.**





Remaining time to pay a fine

71:59:56

Otherwise the case file will be transferred to the court.

All actions are illegal, are fixed. History query stored in the database of the U.S. Department of Homeland Security

Offender Information



© 2016 AO Kaspersky Lab. All Rights Reserved.

Show files

Copy Public Key

Your personal files are encrypted!

Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key**.

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.

Once this has been done, nobody will ever be able to restore files...

In order to decrypt the files open your personal page on site
<https://34r6hq26q2h4jkzj.tor2web.fi> and follow the instruction.

Use your Bitcoin address to enter the site:
1K7Q5TrFxFqCZEmzocfxn8LfrxvdB39Uvm

Click to copy Bitcoin address to clipboard

if <https://34r6hq26q2h4jkzj.tor2web.org> is not opening, please follow the steps:
You must install this browser www.torproject.org/projects/torbrowser.html.en
After installation, run the browser and enter address **34r6hq26q2h4jkzj.onion**
Follow the instruction on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.

Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.

Check Payment

Enter Decrypt Key

Click to Free Decryption on site

© 2016 AO Kaspersky Lab. All Rights Reserved. d.

Concepto: *cryptoviral extortion*

1. [atacante → víctima] El atacante genera un *key pair* y un *public key* que se coloca en el malware. El malware luego se entrega a la víctima.
2. [víctima → atacante] El malware genera un *symmetric key* y cifra los archivos y datos de la víctima con esto. Además, el *symmetric key* se cifra con el *public key* en el malware. Da como resultado un pequeño *assymetric ciphertext*, así como un *ciphertext* de los datos de la víctima. Se muestra un mensaje para el usuario que incluye el *assymetric ciphertext* y cómo pagar el rescate. La víctima envía el *ciphertext* junto con el monto del pago a un atacante.
3. [atacante → víctima] El atacante recibe el pago, descifra el texto con la clave privada del atacante y envía el *symmetric key* a la víctima. La víctima descifra los datos cifrados con el *symmetric key* necesaria para completar el *cryptoviral extortion*.

Cryptoviral extortion

Assymetric Key Pair es generado por el autor del virus

Public Key Pair se coloca dentro del virus

Implementar Virus en el systema de la victima

El virus encripta los datos del host

Text encriptado es lugeo retenido

Notificacion de Ataque

El Victima paga el rescate y envia ciphertext

Autor de Virus descifra ciphertext

Autor de Virus envía Symmetric Key & Initialization Vector (IV) a la víctima

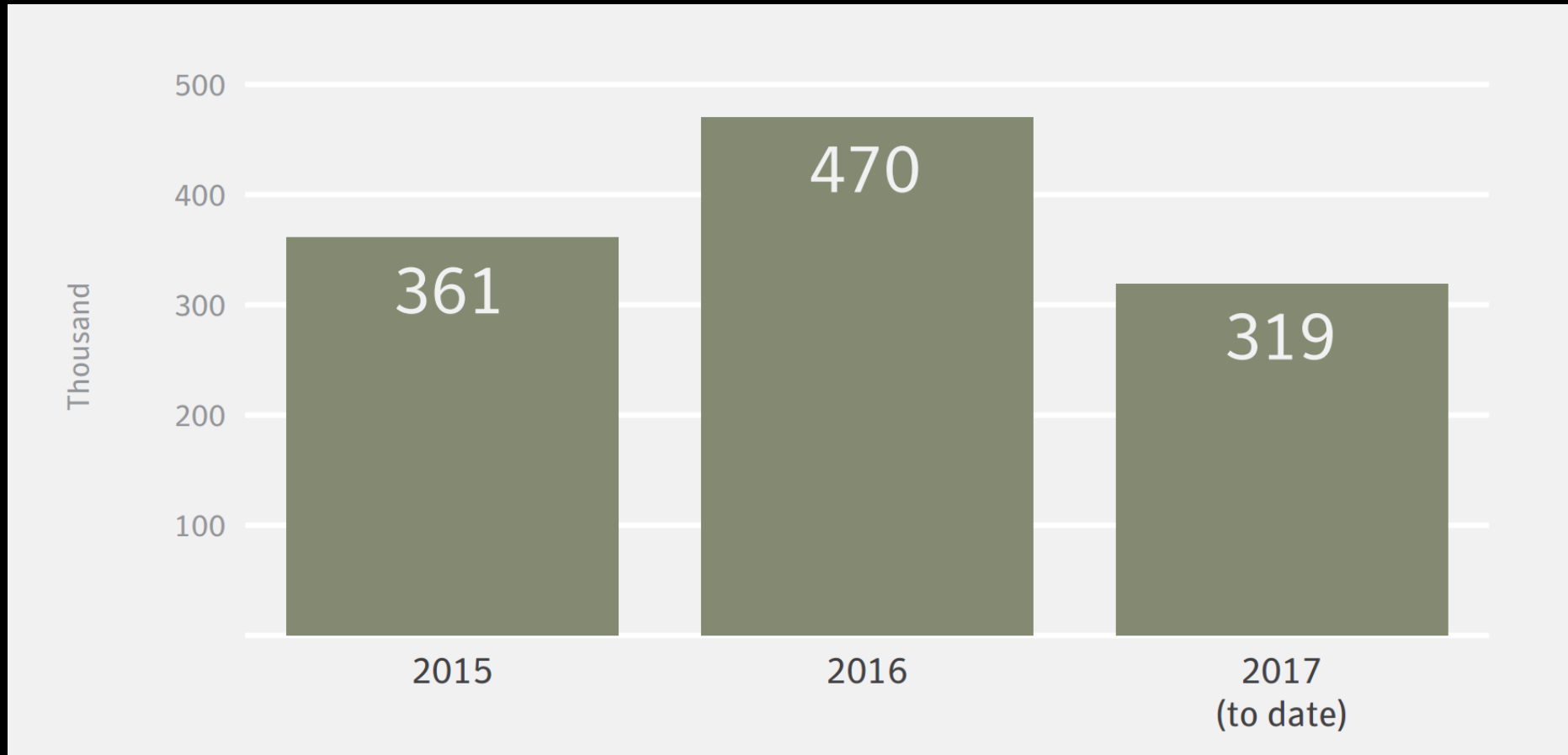
Round 1
atacante
→ **víctima**

Round 2
víctima →
atacante

Round 3
atacante →
víctima

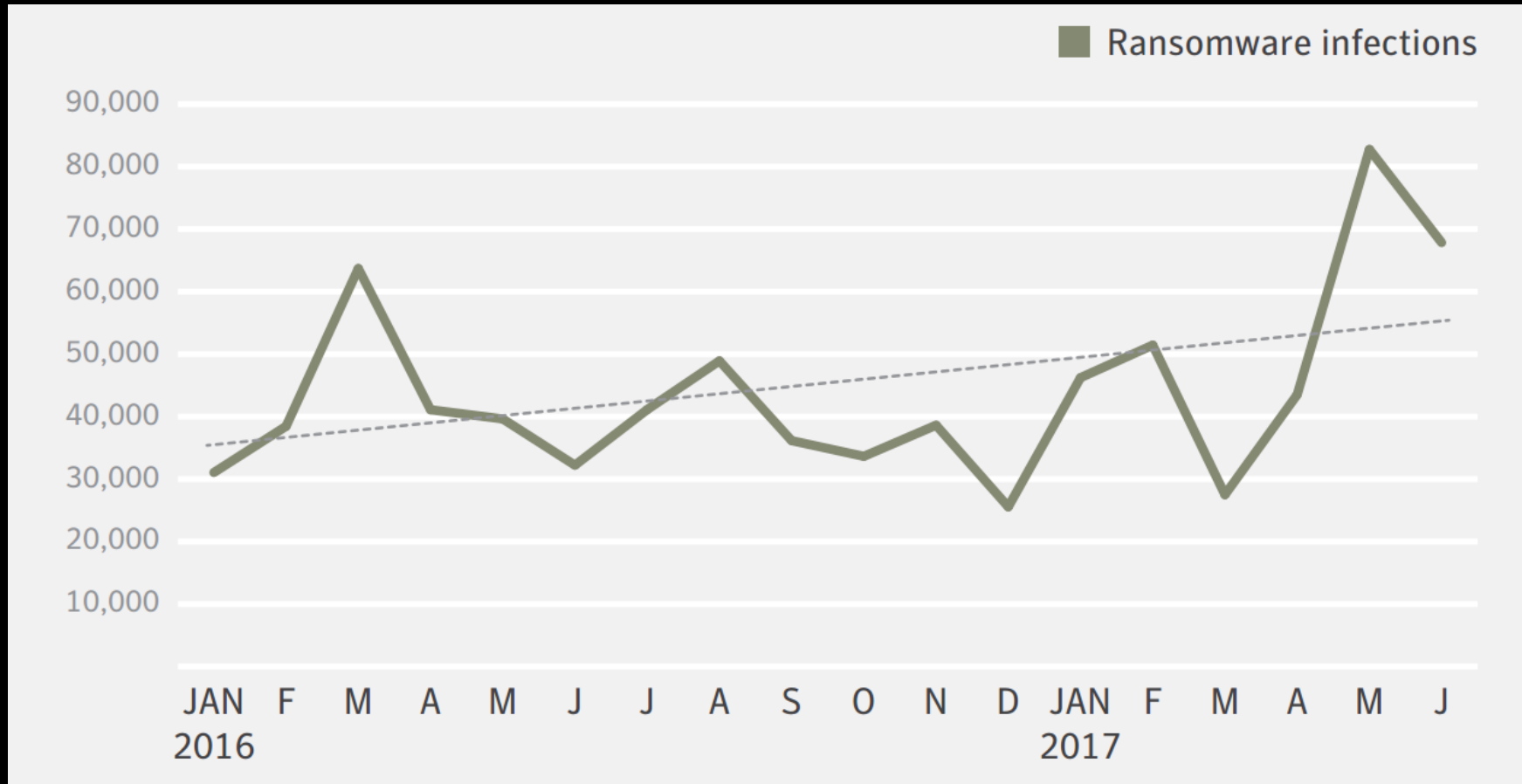
Algunas Estadísticas

Infecciones Ransomware por año (*miles*)



(datos por Symantec)

Infecciones Ransomware por mes (*miles*)



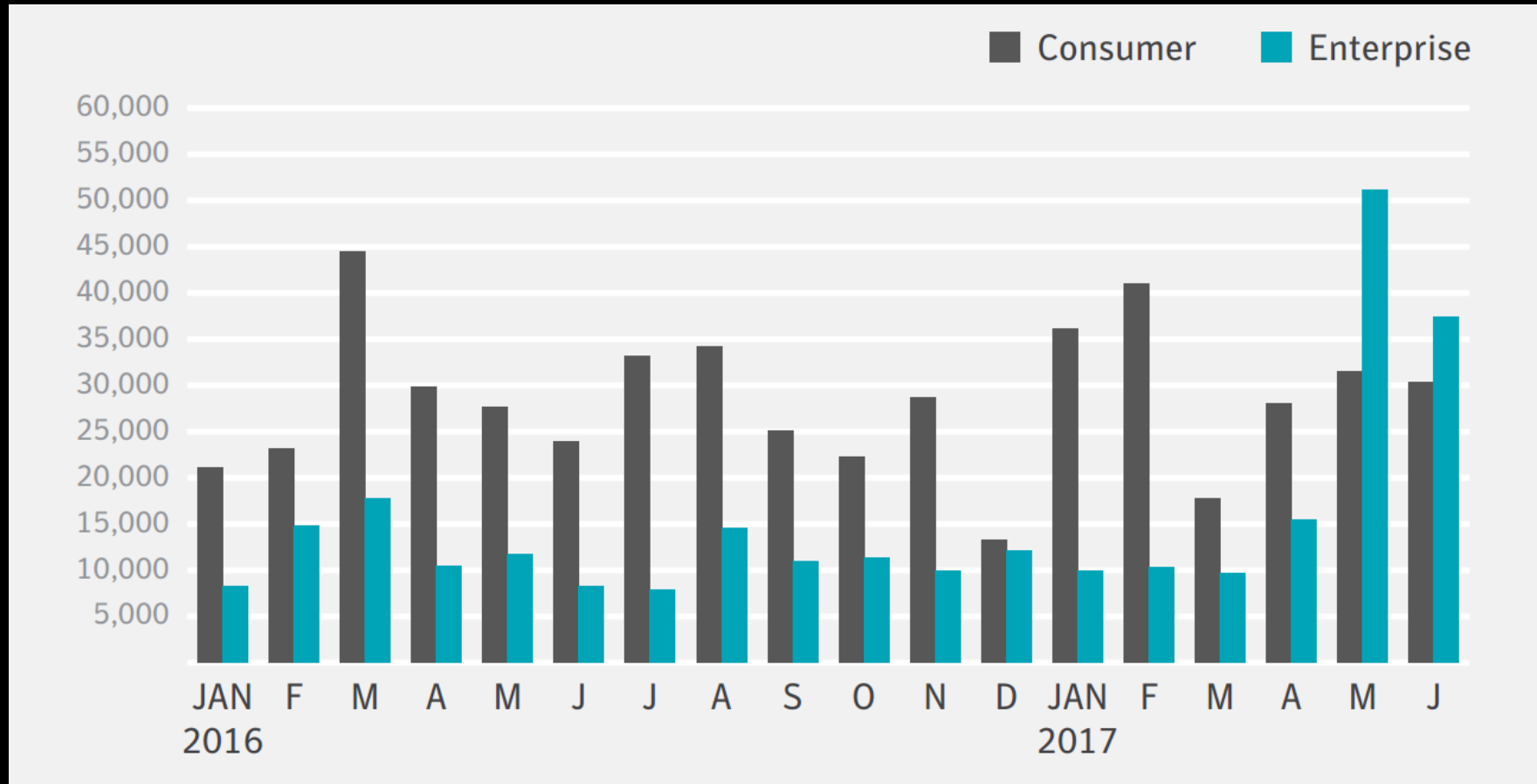
(datos por Symantec)

Cantidad típica del rescate por año



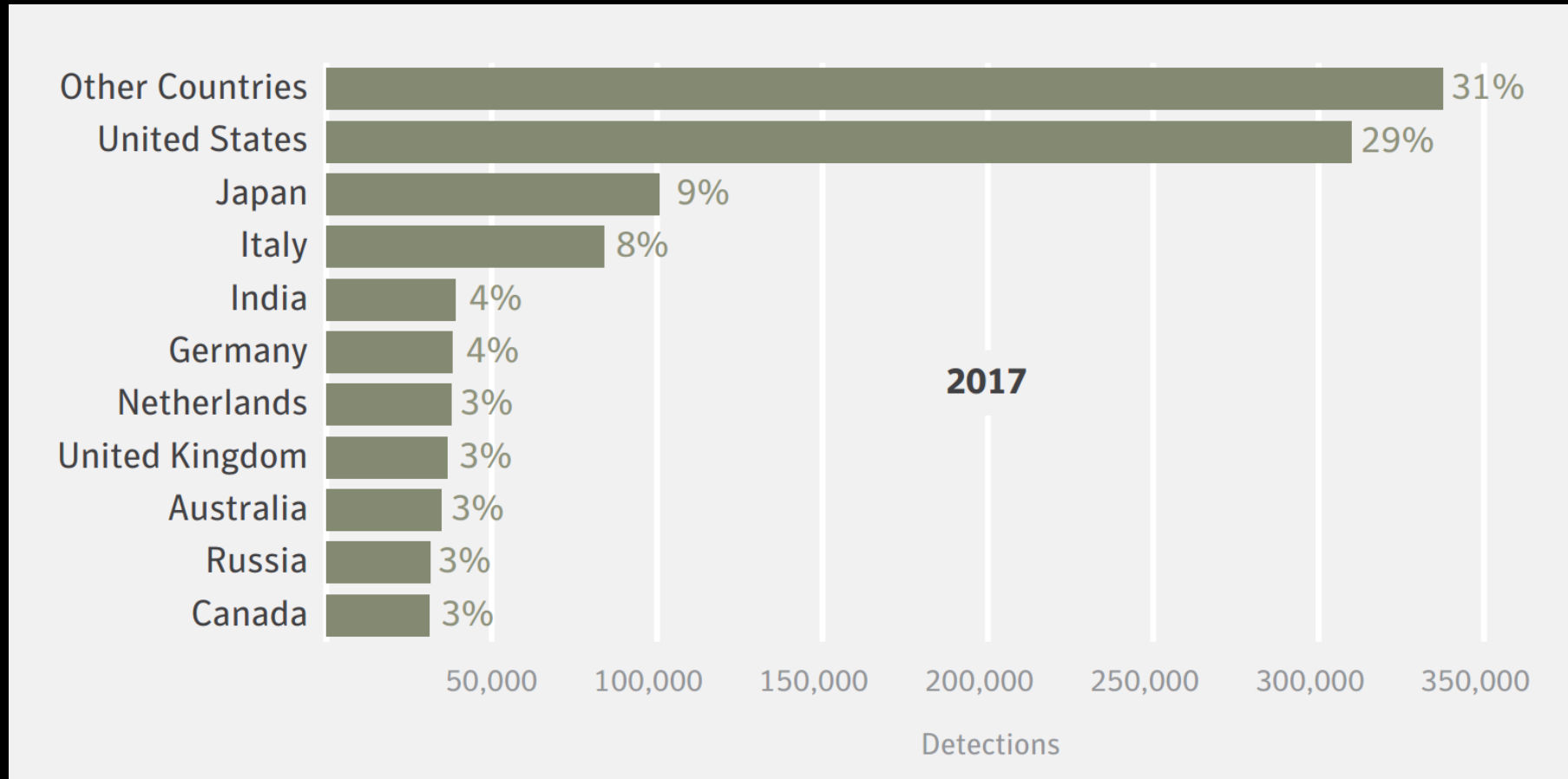
(datos por Symantec)

Infecciones de Ransomware entre el consumidor y la empresa



(datos por Symantec)

Detecciones de Ransomware por región



(datos por Symantec)

- Una de las mayores agencias afectadas por el ataque fueron los hospitales del **Servicio Nacional de Salud en Inglaterra y Escocia**, y hasta **70,000 dispositivos** (incluidas computadoras, escáneres de MRI, refrigeradores de almacenamiento de sangre y equipos de teatro).

Ejemplos de ataques a Empresas

- **Nayana** (*web hosting*): pagó un rescate de 550 Bitcoin ~ US \$1.6 millón
- **AP Moller-Maersk** (compañía de envíos): perdió \$300 millón de Ransomware
- **Reckitt Benckiser** (*Firma farmacéutica*): perdió \$117 millón

Otras Empresas afectadas

- **Beiersdorf**: el ataque ha impactado sus resultados semestrales, debido a retrasos en el envío y la producción
- **Rosneft** (*El principal productor de petróleo de Rusia*)
- **Mondelez** (*fabricante de galletas Oreo*)
- **FedEx**
- **Deutsche Bank**
- **Nissan Motor**
- **Renault**

¿Cuántas personas pagan?

- Según Norton Cyber Security Insight, el 34 % de las víctimas paga el rescate.
- Esta proporción se eleva al 64% de las víctimas en los Estados Unidos

Cómo proteger nuestro sistema

Algunas Soluciones:

1. Backup

2. Backup

3. BACKUP

Cómo protegen las empresas sus sistemas

- Sistemas de filtrado como [Cisco Advanced Malware Protection \(AMP\) for Email Security](#) que identifica archivos adjuntos y URL de un Email maliciosos antes de que se propaguen.
- DNS layer protection: bloquee las solicitudes DNS antes de que un dispositivo pueda conectarse a sitios que alojan ransomware.

Por lo general, las grandes empresas tienen un departamento dedicado especialmente a la seguridad de Internet

Gracias por su atención