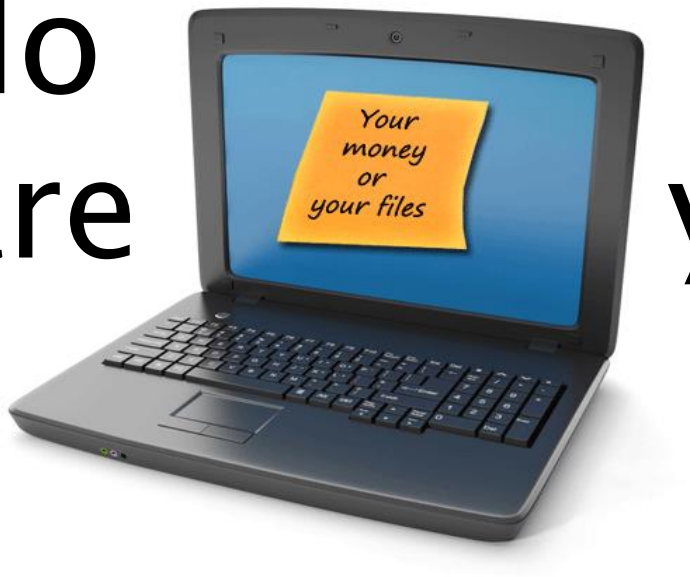
Entendiendo Ransomware y Bitcoin



Alejandro Hevia
Depto. Cs. de la Computación, U. de Chile y CLCERT

Seminario Delitos Económicos Emergentes, PDI
9 de Julio 2014

Agenda

- Qué es el Ransomware
- La Prehistoria del Ransomware
- Profesionalización: Cryptolocker
- Qué es Bitcoin

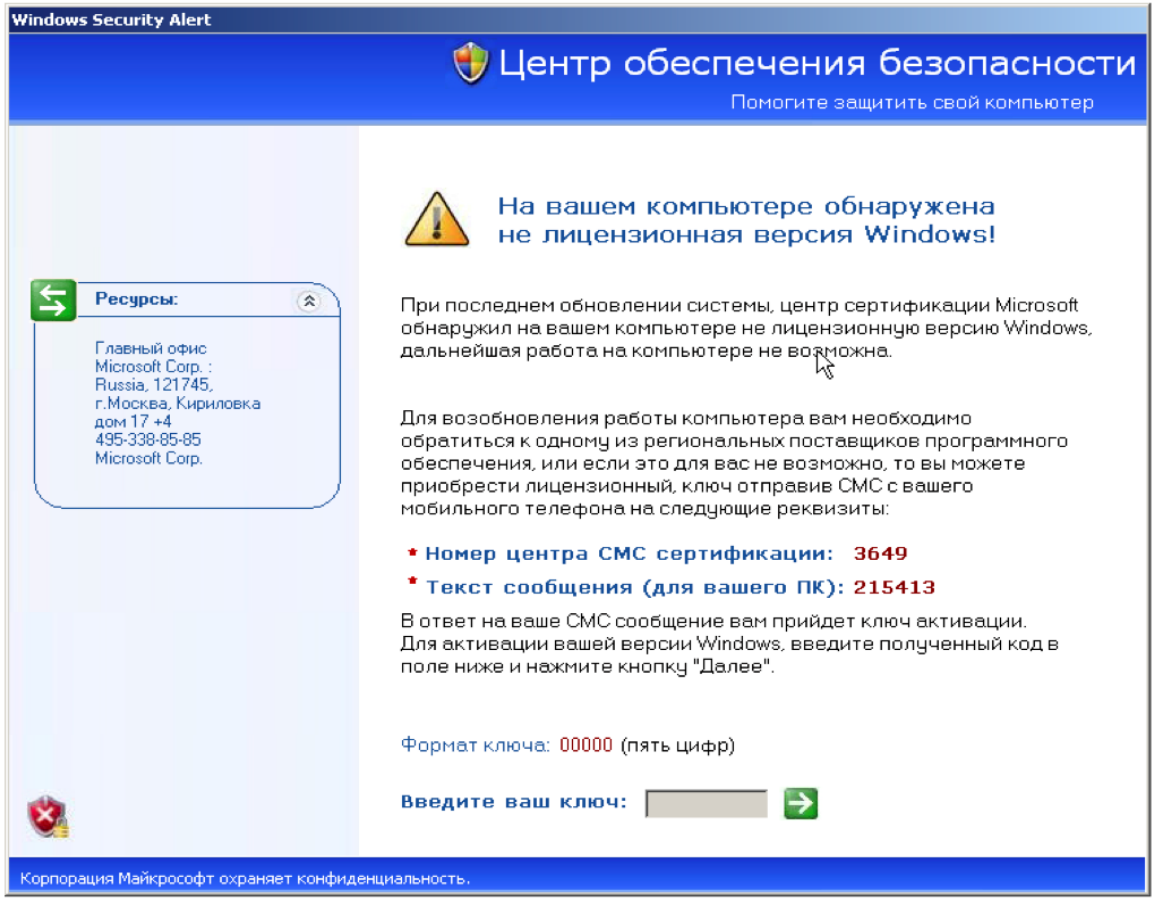
Ransomware o Secuestro-ware

Software malicioso (malware) que desabilita el computador de alguna manera y pide $$ a cambio de devolver lo deshabilitado.



Prehistoria

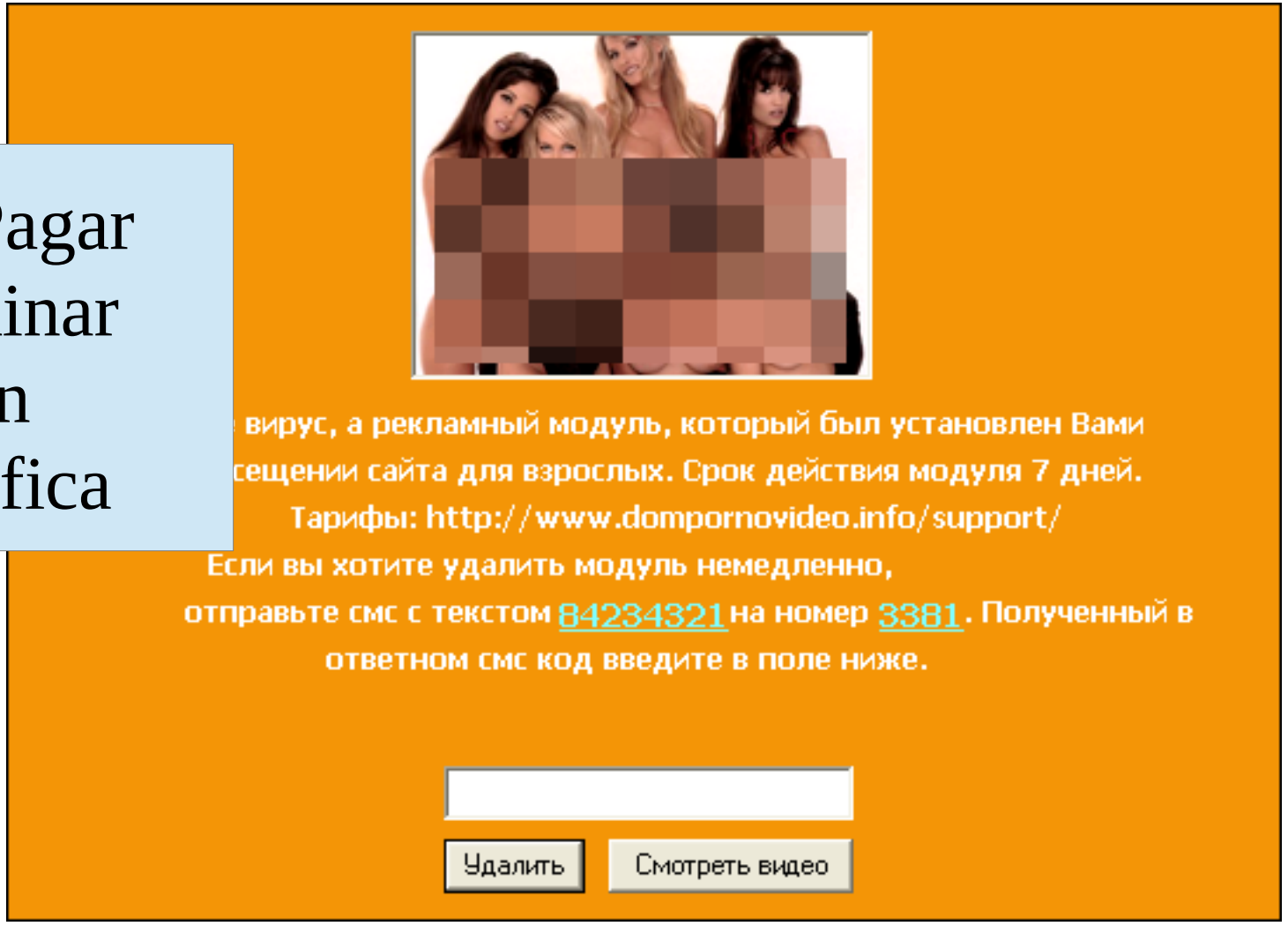
- Inicialmente en Ucrania y Rusia (2009), luego EU y EEUU
- Vía *drive-by-dowload* o *phishing*



Cuento: Activar Windows vía SMS a nro. *premium*

Prehistoria (2009-2010)

Cuento: Pagar para eliminar imágen pornográfica



Prehistoria (2011)



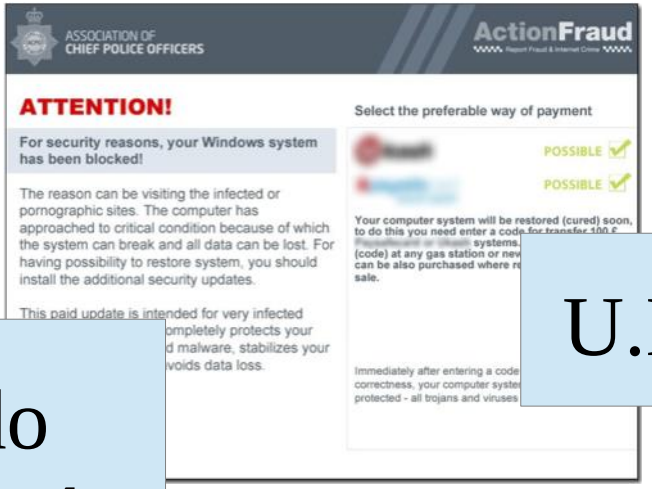
Cuento: Pagar multa por visitar sitio pornográfico

Uso de medios de pago electrónicos

Prehistoria (2011)

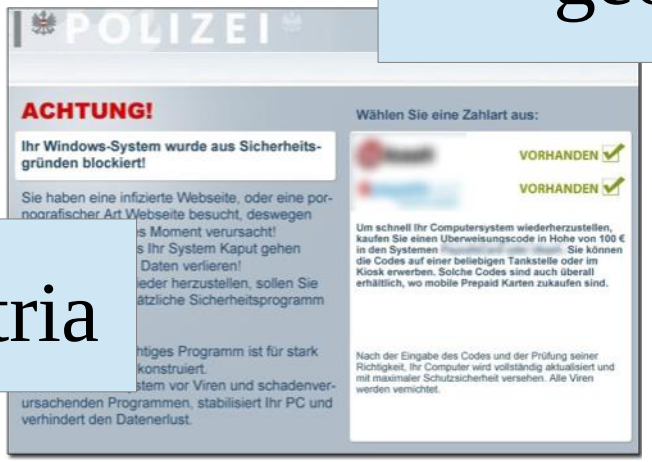


EE.UU.

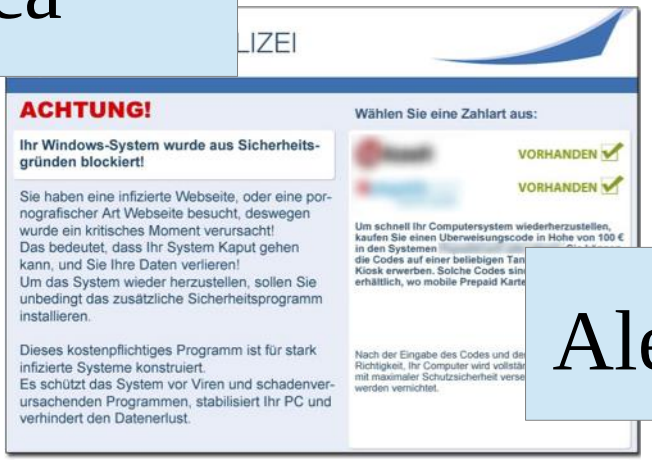


U.K.

Personalizado según localización geográfica



Austria



Alemania

Prehistoria (2012)

- Técnicamente poco sofisticados
  - Encriptación “crackeable” (XOR por constante o similar)
  - Fáciles de remover



Prehistoria (2012)

- Análisis 1 familia
  - 2.9% pagan
  - 68.000 infecciones (por mes, 2012)
  - US$ 394 mil
- Ganancias estimadas
  - e$ 4-5 millones (2012)



Cryptolocker

- Apareció el 5 de Sept. 2013 en EE.UU.
  - Vía phishing email con ZIP (+EXE)
- Luego (Oct. 2013), instalado por malware GameOver Zeus
  - Distribuído por botnet de spam “Cutwail”



Cryptolocker

- Usa bien criptografía de clave pública
  - Microsoft CryptoAPI (RSA, AES)
- Encripta archivos útiles: documentos, música, películas (.docx, .xls, .mov, etc.) en el disco duro
- También en discos de red y externos (!)
- Resiste *reboots*
- Se esconde hasta que contacta servidor y encripta archivos objetivo

Cryptolocker: Cómo Opera

1) Luego de infectar computador, se esconde

2) Genera pseudo-aleatoriamente 1000 dominios nuevo (al día) donde contacta al servidor C&C

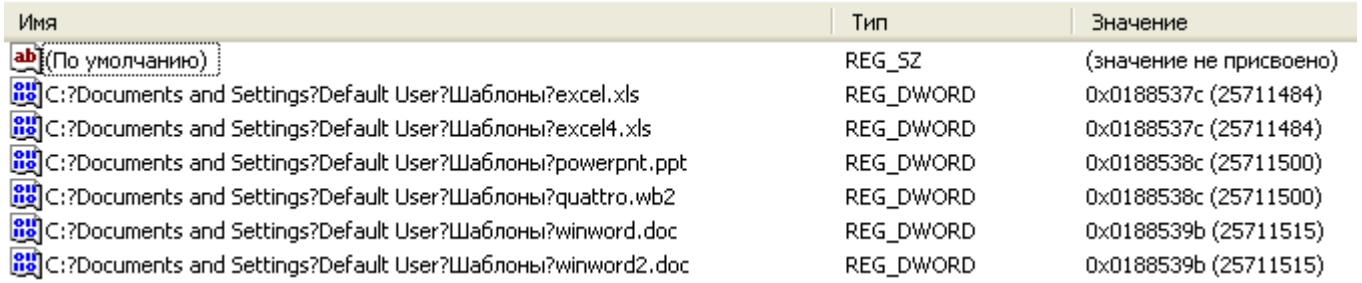
DNS	77	Standard query A jrptmvpllmmt.info
DNS	137	Standard query response, No such name
DNS	76	Standard query A wfkvpbluiejf.com
DNS	149	Standard query response, No such name
DNS	76	Standard query A dlvuoacqawxb.net
DNS	149	Standard query response, No such name
DNS	76	Standard query A qyqwrfxawoum.biz
DNS	138	Standard query response, No such name
DNS	75	Standard query A fhtlyqhgbctr.ru
DNS	136	Standard query response, No such name
DNS	76	Standard query A suoncvdpxtqd.org
DNS	139	Standard query response, No such name
DNS	78	Standard query A laamdqmehouq.co.uk
DNS	94	Standard query response A 212.71.250.4

Cryptolocker: Cómo Opera (cont.)

3) Envía mensaje encriptado con clave pública (incluída en el ejecutable), mensaje incluye un ID para el computador víctima

4) Recibe clave pública específica para víctima

5) Genera clave AES (256 bits) la cual usa para encriptar archivos. Reemplaza originales con encriptados pero guarda registro.



Имя	Тип	Значение
(По умолчанию)	REG_SZ	(значение не присвоено)
C:?Documents and Settings?Default User?Шаблоны?excel.xls	REG_DWORD	0x0188537c (25711484)
C:?Documents and Settings?Default User?Шаблоны?excel4.xls	REG_DWORD	0x0188537c (25711484)
C:?Documents and Settings?Default User?Шаблоны?powerpnt.ppt	REG_DWORD	0x0188538c (25711500)
C:?Documents and Settings?Default User?Шаблоны?quattro.wb2	REG_DWORD	0x0188538c (25711500)
C:?Documents and Settings?Default User?Шаблоны?winword.doc	REG_DWORD	0x0188539b (25711515)
C:?Documents and Settings?Default User?Шаблоны?winword2.doc	REG_DWORD	0x0188539b (25711515)

Cryptolocker: Cómo Opera (cont.)

6) Presenta mensaje con el contador

7) Escanea periódicamente por nuevos archivos



Cryptolocker: Cómo Opera (cont.)

8) Entrega varias alternativas para pagar (US$300)

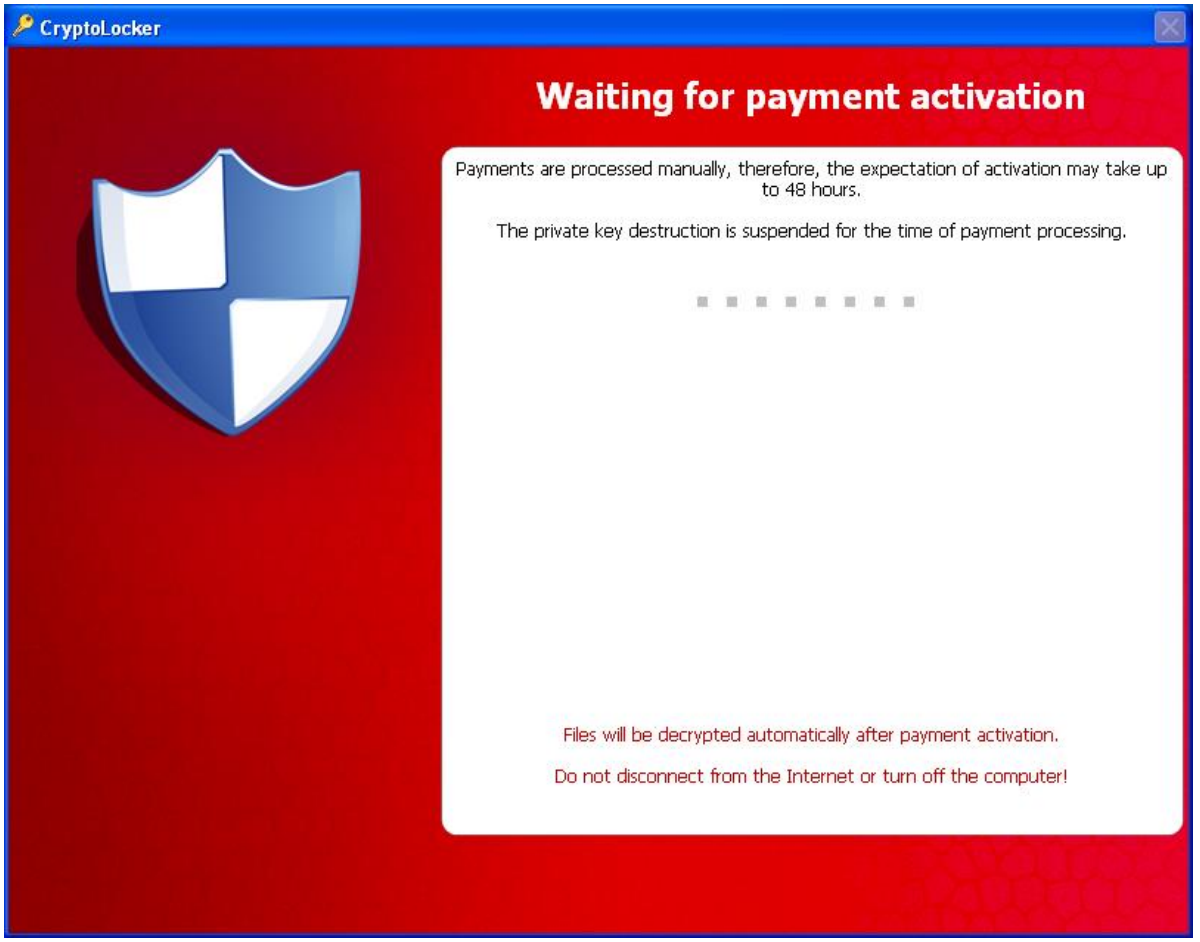




Cryptolocker: Cómo Opera (cont.)

8) Si paga, procesamiento toma de min. a semanas

9) Indica como desencriptar archivos y se borra (?)



Adaptándose a la demanda

- Pagar no es simple (Moneypack, Bitcoin): por lo que variantes extienden el plazo

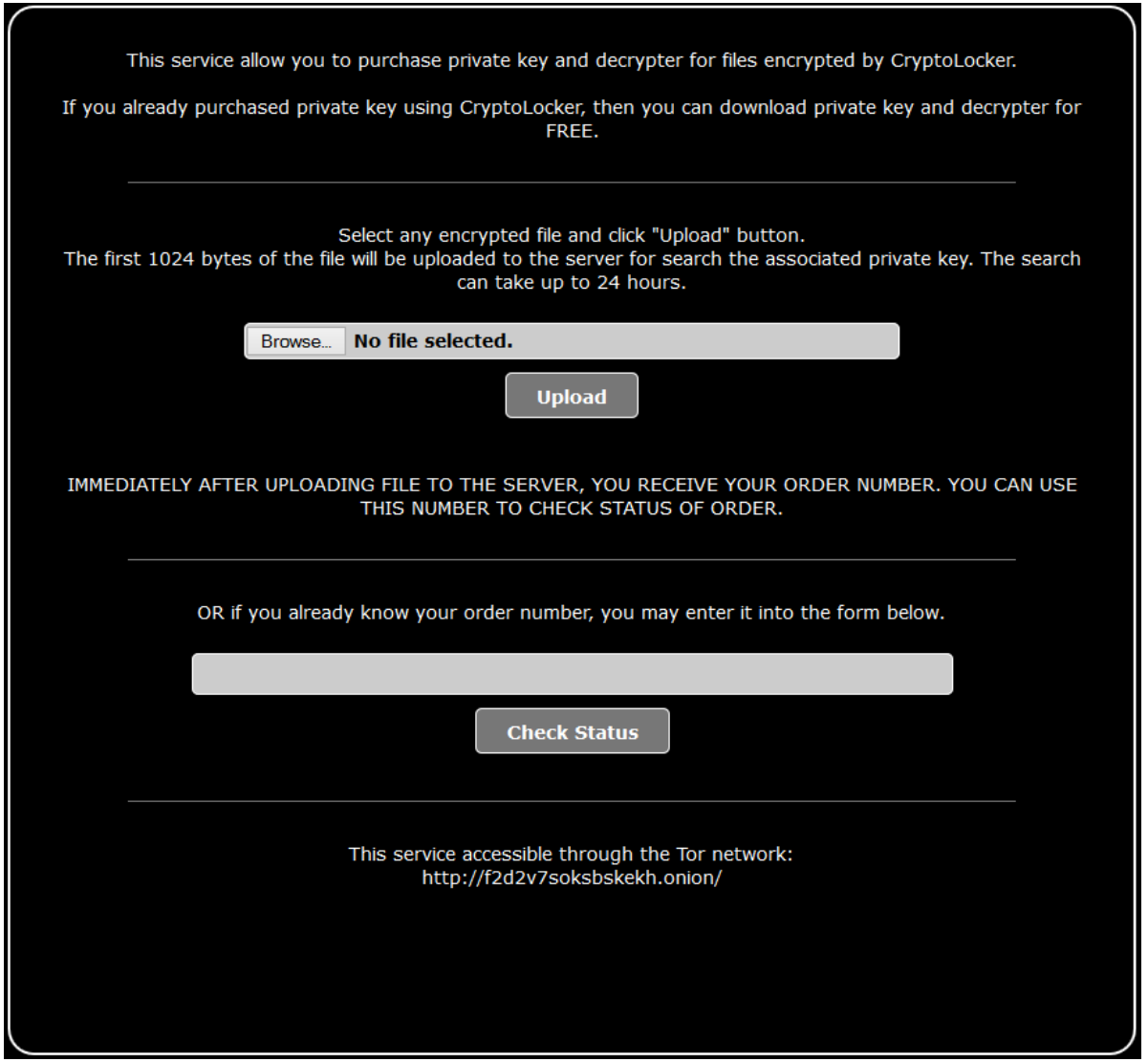
- Antivirus: obliga a bajarlo de nuevo!

Si lo detecta el antivirus...



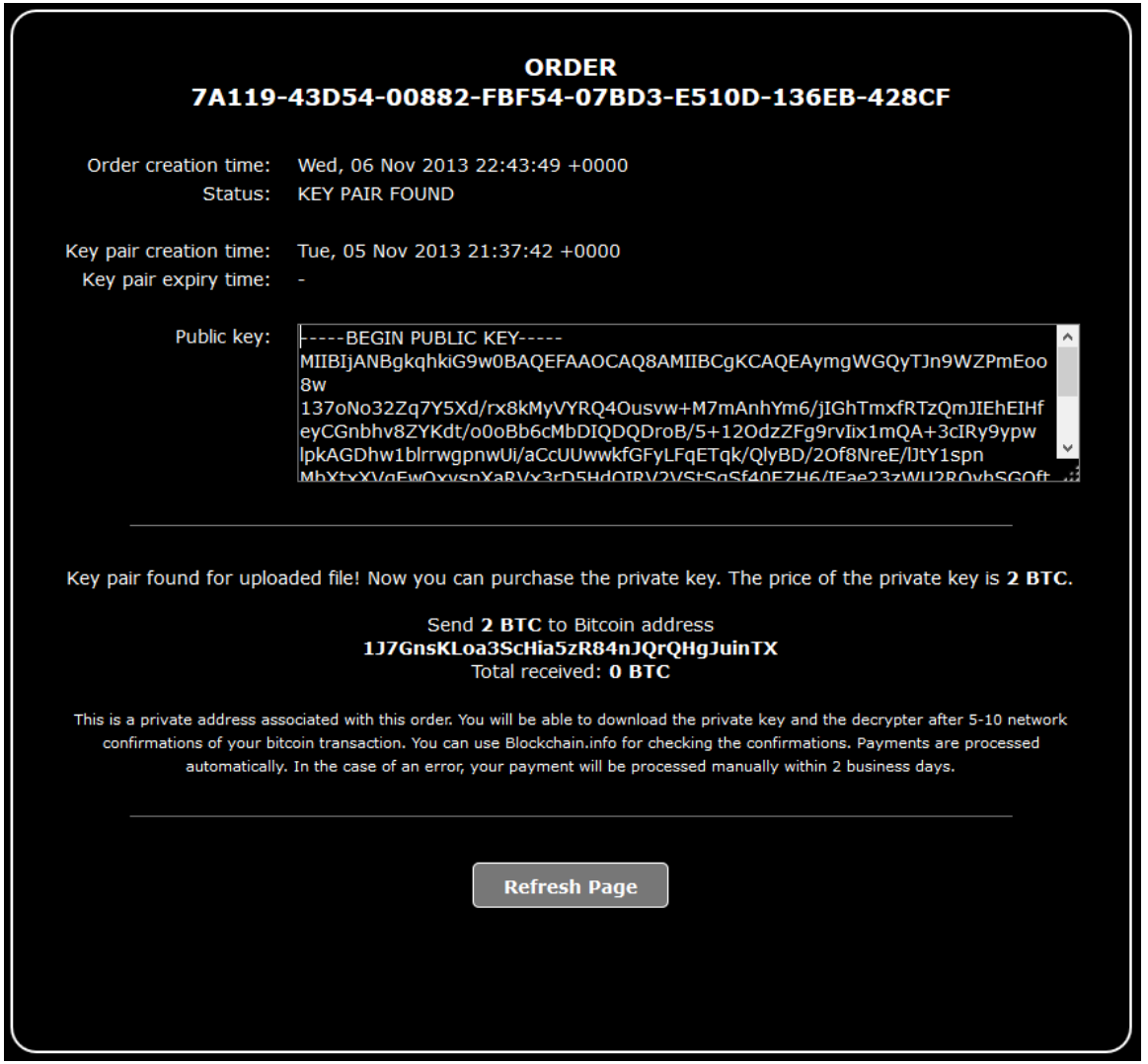
Adaptándose a la demanda (cont.)

- En Nov. 2013, aparece nuevo servicio “CryptoLocker Decryption Service”
- Permite pagar “fuera de plazo”



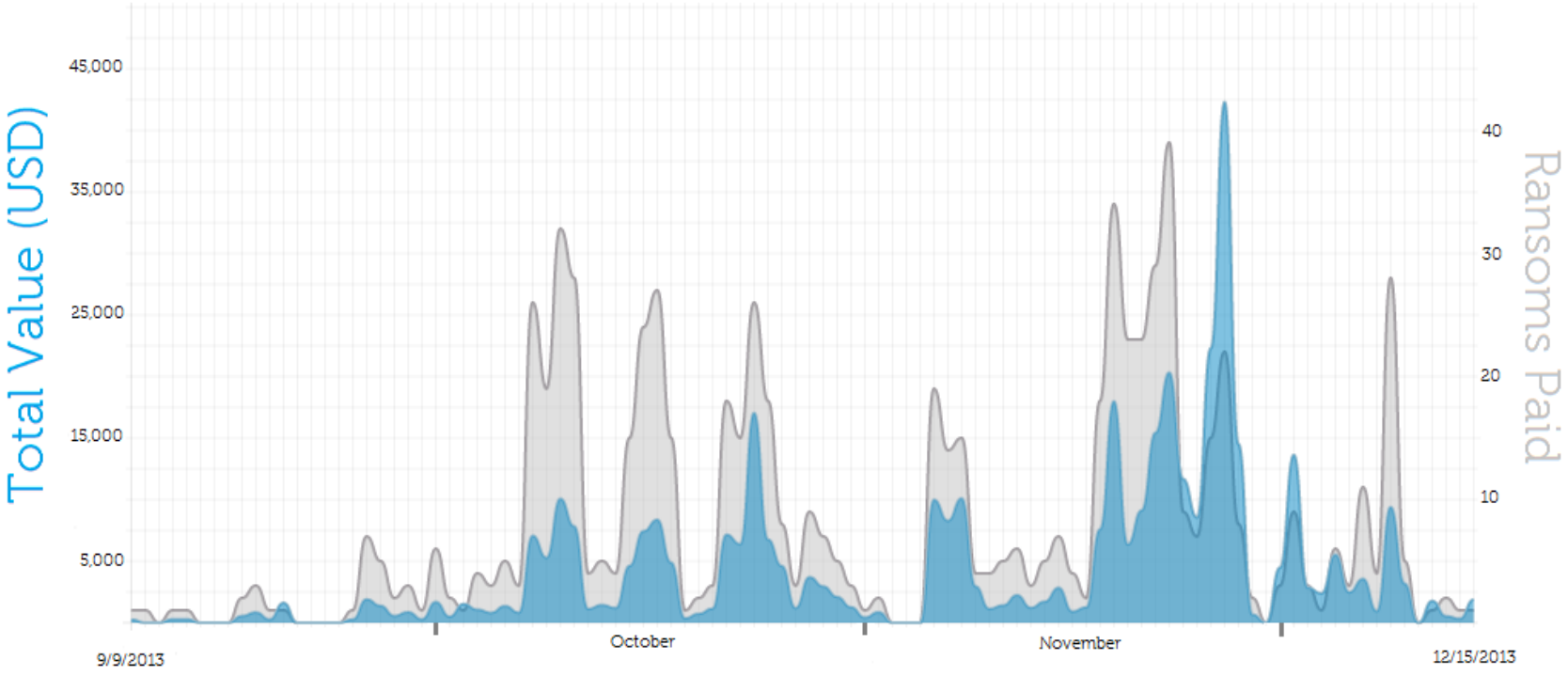
Adaptándose a la demanda (cont.)

- Sube header de archivo encriptado
- Recupera ID de víctima
- Cobra 2 BTC (US$300)
  - llegó a ser 10BTC

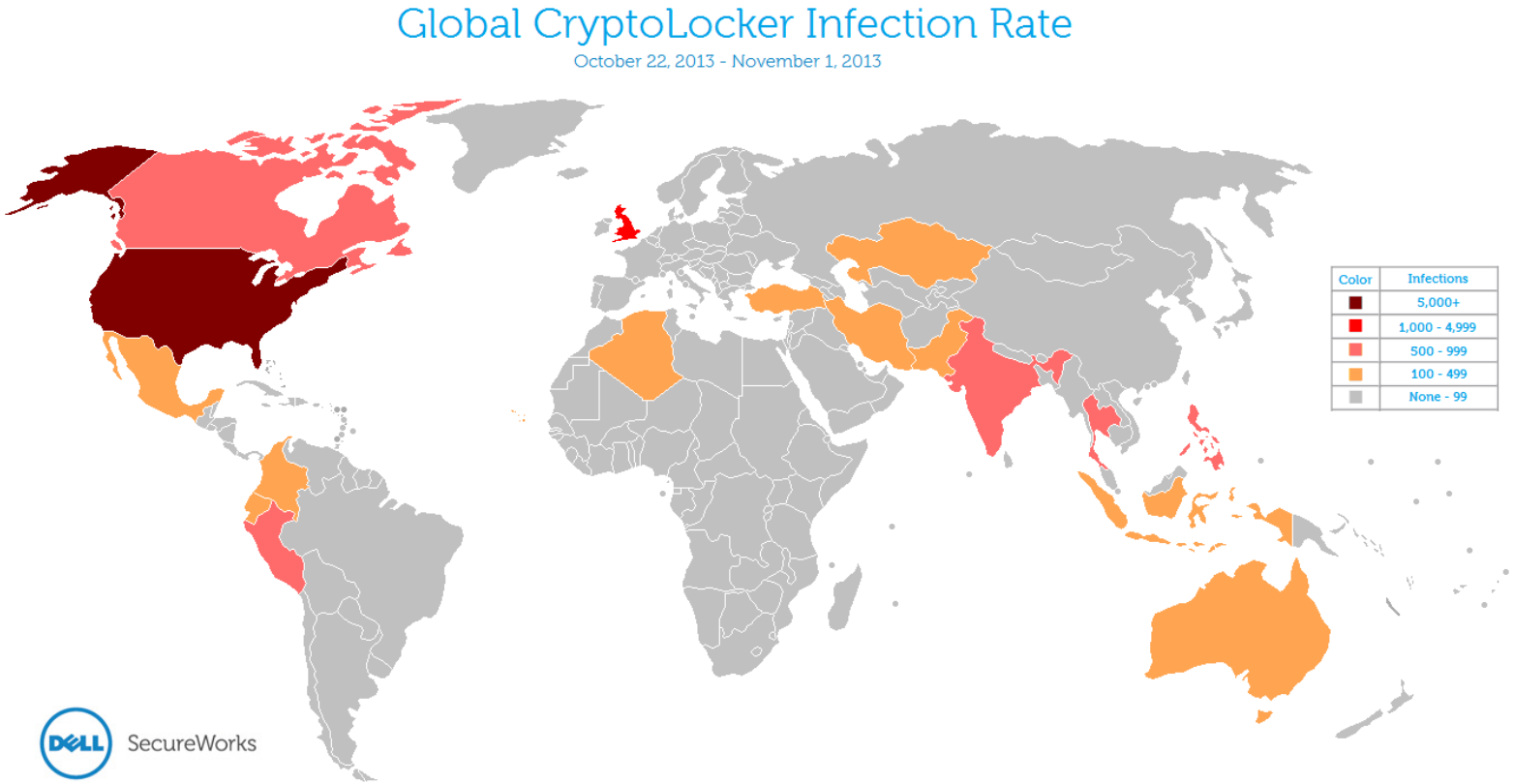


Ganancias

- Análisis tesis Michele Spagnuolo (2013)
  - 0.4% víctimas paga
  - Sep-Dic 2013: US$ 380.000 – US$ 980.000



Víctimas



- Estudio de *Dell SecureWorks Counter Threat Unit*
- 22 Oct – 1 Nov, 2013: 31.866 víctimas
- Entre 200.000 – 250.000 infectados (<100 días)

Mitigaciones

- Prohibir EXEs en correo (phishing)
- Blacklist rápido de dominios C&C conocidos
- Reducir permisos de escritura en discos compartidos
- Restringir permisos para escribir en registro de Windows
- Hacer backups “en frío” (desconectados)

Bitcoins



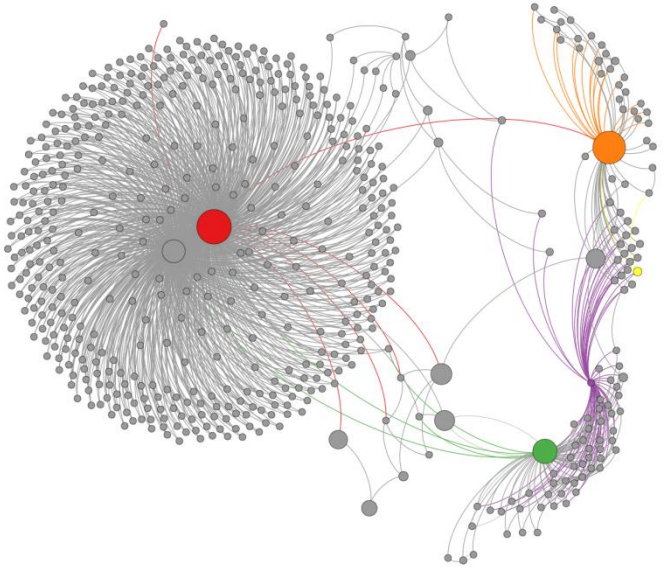
- Sistema distribuido de dinero electrónico
- Monedas pueden ser generadas por participantes, pero requiere resolver problema matemático difícil
  - Encontrar pre-imágenes de funciones de hash que produzcan valores de una cierta forma (con un cierto número de 0´s como prefijo)
  - Se hace cada vez más difícil: número de monedas tiene un tope teórico

Bitcoins

- Pseudo-anónimo
  - No hay identidades, sólo claves públicas
  - Usadas para firmar el transpaso de monedas
- Sin control central
  - Hay una bitácora de transacciones mantenida en forma distribuida entre los participantes
  - Consistencia se mantiene pues cada nuevo registro debe ser *encadenado* al anterior (vía aplicar función de hash) con lo cual es difícil “cambiar el pasado”.

Bitcoins: Puntos Claves

- No es anónimo
  - Puede hacerse tracking de *quién transfirió a quién*
  - Pero no hay nombres, sólo identificadores de claves públicas!



Bitcoins: Puntos Claves

- Con información adicional, investigadores han podido des-anonimizar parcialmente a usuarios
  - Ver http://anonymity-in-bitcoin.blogspot.com/2011/07/bitcoin-is-not-anonymous.html
  - http://eprint.iacr.org/2012/596
- Hay iniciativas para hacerlo realmente anónimo
  - zerocoin.org

Referencias

- Estudio “CryptoLocker Ransomware”, 18 Dic 2013
  - Author: Keith Jarvis,
  - Dell SecureWorks Counter Threat Unit(TM) Threat Intelligence
  - http://www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware/
- Bitcoins
  - Tutorial operación (Inglés) http://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-what-is-it