

# The Ransomware Strikes Back

## Virus Bulletin 2013

**Ciprian Opreșă, George Cabău** and Andrea Takacs

Bitdefender

October 4, 2013

# Agenda

- 1 Introduction
- 2 Screen-locking ransomware
- 3 File encryptors
- 4 How about the money?
- 5 Conclusions

# Agenda

- 1 Introduction
- 2 Screen-locking ransomware
- 3 File encryptors
- 4 How about the money?
- 5 Conclusions

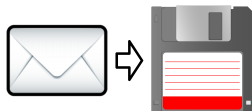
# An incursion into the past

1989



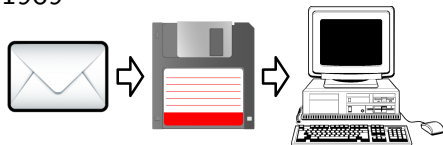
# An incursion into the past

1989



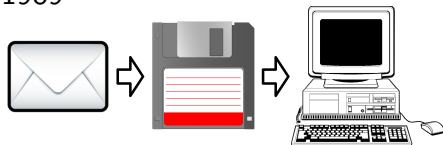
# An incursion into the past

1989



# An incursion into the past

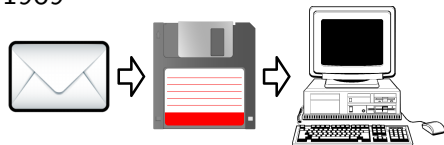
1989



INSTALL.EXE (including license agreement)

# An incursion into the past

1989



INSTALL.EXE (including license agreement)

- counts 90 boots
- scrambles file names
- displays ransom note
  - *send \$189 to a post office box in Panama*



# The present ransomware

## Definition (Ransomware)

Malware that restricts access to a computer system and demands a ransom in order to restore it.

# The present ransomware

## Definition (Ransomware)

Malware that restricts access to a computer system and demands a ransom in order to restore it.



# The present ransomware

## Definition (Ransomware)

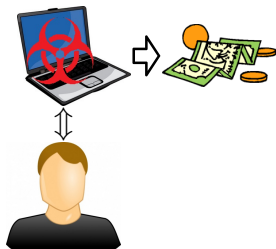
Malware that restricts access to a computer system and demands a ransom in order to restore it.



# The present ransomware

## Definition (Ransomware)

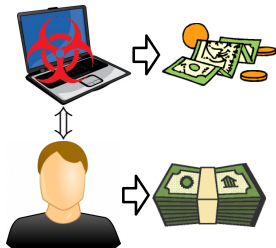
Malware that restricts access to a computer system and demands a ransom in order to restore it.



# The present ransomware

## Definition (Ransomware)

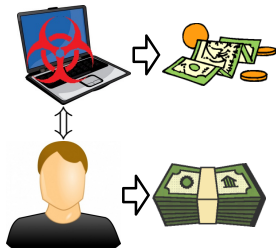
Malware that restricts access to a computer system and demands a ransom in order to restore it.



# The present ransomware

## Definition (Ransomware)

Malware that restricts access to a computer system and demands a ransom in order to restore it.



## Types of ransomware

- Screen lockers
- File encryptors

# Agenda

- 1 Introduction
- 2 Screen-locking ransomware**
- 3 File encryptors
- 4 How about the money?
- 5 Conclusions

# The screen lock anatomy



**ATTENTION! ILLEGAL ACTIVITY WAS REVEALED!**

Your operational system is locked as a result of Great Britain law violation!

The following violations were revealed: your IP address was detected on illegal pornographic sites including child pornography, zoophilia and violent scenes with children! Pornographic video with elements of violence and child pornography were revealed on your PC!

Illegal SPAM of terrorist orientation is also mailed from your PC.

This lockout is intended to eliminate possible distribution of the above materials from your PC in the Internet.

Your personal data: IP: Browser: Internet Explorer 7.0 OS: Windows XP Country: City: ISP:

For your PC to be unlocked you have to pay penalty equal to 100€! The penalty is to be paid during 24 hours from the moment when your PC was locked! If the penalty is not paid all the data will be removed from your PC!

There are 2 ways of payment:

- 1) You can buy the ukash coupon for the amount of 100€. Enter the ukash coupon number in payment field and press OK or send the coupon number by email mp.deposit@raho.com You can buy the ukash coupon at any available point.
- 2) You can pay the penalty by means of paysafecard. Payment by means of paysafecard is to be effected to the amount of 100€. Enter the pin code from your bill in payment field and press OK or send the pin code by email mp.deposit@raho.com

You can buy paysafecard at any available point  
As soon as payment is effected your PC will be unlocked during 24 hours from the moment of payment.

ukash

epoj pay safe P Panda

BUTTON

paysafe.com  
PIN CODE:  
1234 5678 1234 5678

paysafecard  
pay cash. pay safe.

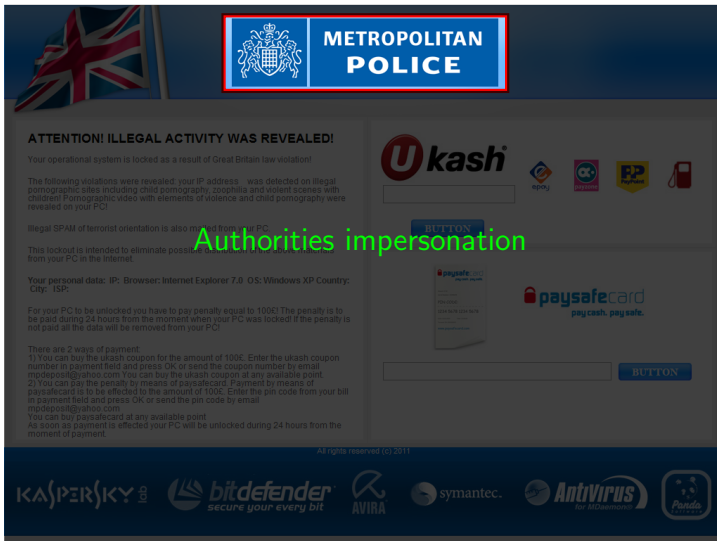
BUTTON

All rights reserved (c) 2011

KASPERSKY  
bitdefender  
secure your every bit  
AVIRA  
symantec.  
AntiVirus  
for McAfee  
Panda



# The screen lock anatomy



**METROPOLITAN POLICE**

**ATTENTION! ILLEGAL ACTIVITY WAS REVEALED!**

Your operational system is locked as a result of Great Britain law violation!

The following violations were revealed: your IP address was detected on illegal pornographic sites including child pornography, zoophilia and violent scenes with children! Pornographic video with elements of violence and child pornography were revealed on your PC!

Illegal SPAM of terrorist orientation is also mixed from your PC!

This lockout is intended to eliminate possible damage of the data retrieved from your PC in the Internet.

Your personal data: IP: Browser: Internet Explorer 7.0 OS: Windows XP Country: City: ISP:

For your PC to be unlocked you have to pay penalty equal to 100€! The penalty is to be paid during 24 hours from the moment when your PC was locked! If the penalty is not paid all the data will be removed from your PC!

There are 2 ways of payment:

- 1) You can buy the ukash coupon for the amount of 100€. Enter the ukash coupon number in payment field and press OK, or send the coupon number by email: [mp-deposit@ yahoo.com](mailto:mp-deposit@ yahoo.com). You can buy the ukash coupon at any available point.
- 2) You can pay the penalty by means of paysafecard. Payment by means of paysafecard is to be effected to the amount of 100€. Enter the pin code from your bill in payment field and press OK, or send the pin code by email: [mp-deposit@ yahoo.com](mailto:mp-deposit@ yahoo.com).

You can buy paysafecard at any available point!  
As soon as payment is effected your PC will be unlocked during 24 hours from the moment of payment.

Authorities impersonation

Ukash

pay safe card  
pay cash. pay safe.

Buttons: BUTTON, BUTTON

All rights reserved (C) 2011

KASPERSKY  
bitdefender secure your every bit  
AVIRA  
symantec.  
AntiVirus for Macintosh  
Panda

# The screen lock anatomy



**ATTENTION! ILLEGAL ACTIVITY WAS REVEALED!**

Your operational system is locked as a result of Great Britain law violation!

The following violations were revealed: your IP address was detected on illegal pornographic sites including child pornography, zoophilia and violent scenes with children! Pornographic video with elements of violence and child pornography were revealed on your PC!

Illegal SPAM of terrorist orientation is also mailed from your PC.

This lockout is intended to eliminate possible distribution of the above materials from your PC in the Internet.

Your personal data: IP: Browser: Internet Explorer 7.0 OS: Windows XP Country: City: ISP:

For your PC to be unlocked you have to pay penalty equal to 100€. The penalty is to be paid during 24 hours from the moment when your PC was locked if the penalty is not paid all the data will be removed from your PC!

There are 2 ways of payment!


- 1) You can buy the ukash coupon for the amount of 100€. Enter the ukash coupon number in payment field and press OK, or send the coupon number by email: [mp.deposit@siho.com](mailto:mp.deposit@siho.com) You can buy the ukash coupon at any available point.
- 2) You can pay the penalty by means of paysafecard. Payment by means of paysafecard is to be effected to the amount of 100€. Enter the pin code from your bill in payment field and press OK, or send the pin code by email: [mp.deposit@siho.com](mailto:mp.deposit@siho.com)

You can buy paysafecard at any available point  
As soon as payment is effected your PC will be unlocked during 24 hours from the moment of payment.

Known anti-malware companies make the things look even more serious

Logos at the bottom: KASPERSKY, bitdefender, AVIRA, symantec., AntiVirus, Panda

# The screen lock anatomy



**ATTENTION! ILLEGAL ACTIVITY WAS REVEALED!**

Your operational system is locked as a result of Great Britain law violation!

The following violations were revealed: your IP address was detected on illegal pornographic sites including child pornography, zoophilia and violent scenes with children! Pornographic video with elements of violence and child pornography were revealed on your PC!

Illegal SPAM of terrorist orientation is also mailed from your PC.

This lockout is intended to eliminate possible distribution of the above materials from your PC in the Internet.

Your personal data: IP: Browser: Internet Explorer 7.0. OS: Windows XP Country: City: ISP:

For your PC to be unlocked you have to pay penalty equal to 100£. The penalty is to be paid during 24 hours from the moment when your PC was locked! If the penalty is not paid all the data will be removed from your PC!

There are 2 ways of payment:

1) You can buy the ukash coupon for the amount of 100£. Enter the ukash coupon number in payment field and press OK, or send the coupon number by email: [mdkdep@satoh.com](mailto:mdkdep@satoh.com). You can buy the ukash coupon at any available point.

2) You can pay the penalty by means of paysafecard. Payment by means of paysafecard is to be effected by means of the coupon number printed on the paysafecard in payment field and press OK, or send the coupon number by email: [mdkdep@satoh.com](mailto:mdkdep@satoh.com).

You can buy paysafecard at any available point.

As soon as payment is effected your PC will be unlocked during 24 hours from the moment of payment.

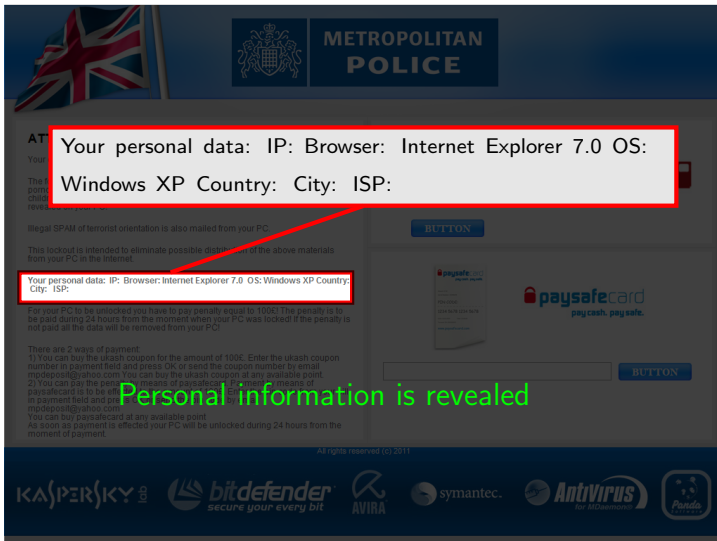
All rights reserved (c) 2011

KASPERSKY bitdefender AVIRA symantec. AntiVirus Panda

- child pornography
- zoophilia
- illegal spam of terrorist orientation

The user is blamed for illegal activities

# The screen lock anatomy



AT

Your

The f  
point  
child  
revea

illegal SPAM of terrorist orientation is also mailed from your PC.

This lockout is intended to eliminate possible distribution of the above materials from your PC in the internet.

Your personal data: IP: Browser: Internet Explorer 7.0 OS: Windows XP Country: City: ISP:

For your PC to be unlocked you have to pay penalty equal to 100€. The penalty is to be paid during 24 hours from the moment when your PC was locked if the penalty is not paid all the data will be removed from your PC!

There are 2 ways of payment:

- 1) You can buy the ukash coupon for the amount of 100€. Enter the ukash coupon number in payment field and press OK, or send the coupon number by email: mdeposits@ukash.com. You can buy the ukash coupon at any available point.
- 2) You can pay the penalty by means of paysafecard. Payment by means of paysafecard is to be effected by means of paysafecard. Payment by means of paysafecard is to be effected by means of paysafecard. Enter the paysafecard number in payment field and press OK.


You can buy paysafecard at any available point  
As soon as payment is effected your PC will be unlocked during 24 hours from the moment of payment.


PERSONAL INFORMATION IS REVEALED

ALL RIGHTS RESERVED (C) 2011

KASPERSKY  
bitdefender  
secure your every bit  
AVIRA  
symantec.  
AntiVirus  
for Mac OS  
Panda  
SECURITY

# The screen lock anatomy





**METROPOLITAN  
POLICE**

**ATTENTION! ILLEGAL ACTIVITY WAS REVEALED!**

Your operational system is locked as a result of Great Britain law violation!

The following violations were revealed: your IP address was detected on illegal pornographic sites including child pornography, zoophilia and violent scenes with children! Pornographic video with elements of violence and child pornography were revealed on your PC!

Illegal SPAM of terrorist orientation is also mailed from your PC.

This site is intended to eliminate possible distribution of the above materials from your PC!


Your personal data: IP: Browser: Internet Explorer 7.0 OS: Windows XP Country: City: (isp)





For your PC to be unlocked you have to pay penalty equal to 100€! The penalty is to be paid during 24 hours from the moment when your PC was locked! If the penalty is not paid all the data will be removed from your PC!

There are 2 ways of payment:

- 1) You can buy the ukash coupon for the amount of 100€. Enter the ukash coupon number in payment field and press OK, or send the coupon number by email: [mp-deposit@sihoo.com](mailto:mp-deposit@sihoo.com). You can buy the ukash coupon at any available point.
- 2) You can pay the penalty by means of paysafecard. Payment by means of paysafecard is to be effected to the amount of 100€. Enter the pin code from your bill in payment field and press OK, or send the pin code by email: [mp-deposit@sihoo.com](mailto:mp-deposit@sihoo.com).


You can buy paysafecard at any available point!  
As soon as payment is effected your PC will be unlocked during 24 hours from the moment of payment.




**BUTTON**







---





**BUTTON**

All rights reserved (C) 2011

The payment is as easy as possible

## Why does it work?

It's not that hard to regain control

- Live CD
- Restart in safe mode
- Restart without Internet
- Sometimes it won't even cover the entire screen

The trick is to prevent the user to get help

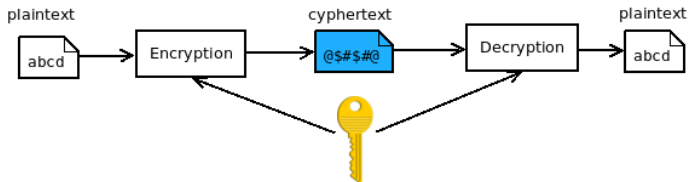
- The screen lock does part of the job
- Make him feel ashamed
- Limited time

# Agenda

- 1 Introduction
- 2 Screen-locking ransomware
- 3 File encryptors**
- 4 How about the money?
- 5 Conclusions

# A (very short) crash course in cryptography

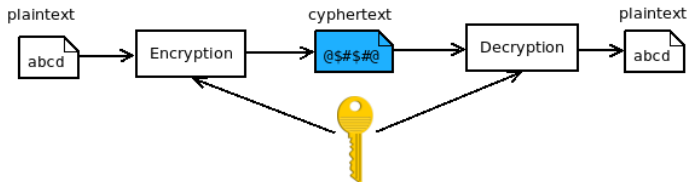
## Symmetric encryption



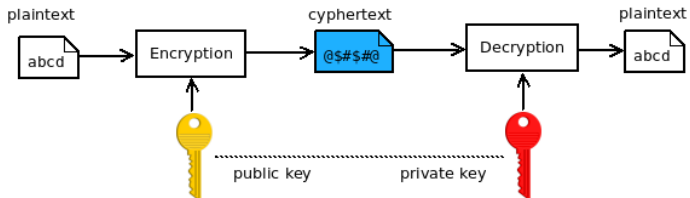


# A (very short) crash course in cryptography

## Symmetric encryption



## Asymmetric encryption



# Important features for file encryptors (1)

## Feature 1



The ability to encrypt files in a non-trivial manner. It shouldn't be possible to decrypt the encrypted files without a secret key.

## Feature 2



The decryption key should be impossible to obtain in a reasonable amount of time, given the malware sample and/or pairs of original/encrypted files.

## Important features for file encryptors (2)

### Feature 3



After a user has paid the ransom, the key/decryption tool should work for his system alone.

### Feature 4



The decryption key should be available to the attacker after a successful attack. The decryption key should not be lost, even if the victim is offline during the encryption.

# A proper file encryptor: GPCode (1)

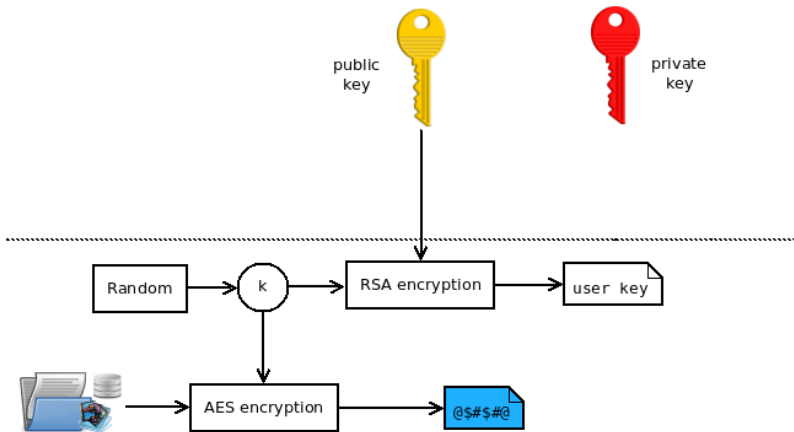
public  
key



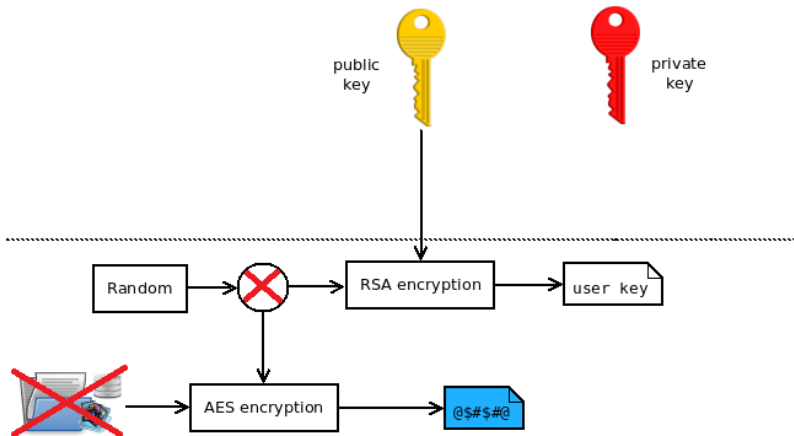
private  
key



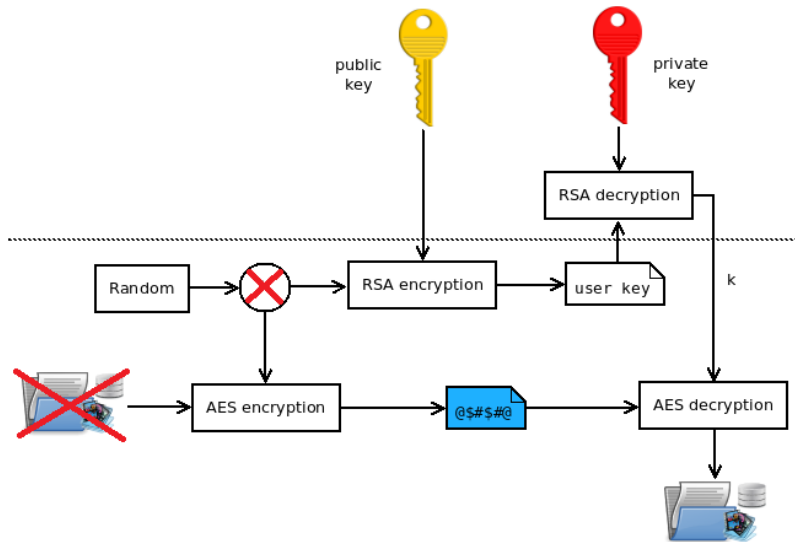
# A proper file encryptor: GPCode (1)



# A proper file encryptor: GPCode (1)



# A proper file encryptor: GPCode (1)







## A proper file encryptor: GPCode (2)









# A proper file encryptor: GPCode (2)



	✓	AES encryption
	✓	the AES key is encrypted with RSA
	✓	the AES key is random
	✓	the attacker can derive the AES key from the user key





# ACCDFISA evolution (1)

Version 1 (100\$)

	✓ (~)	encrypted RAR archive
	✗	static password
	✗	same static password for all users
	✓	password known to the attacker





# ACCDFISA evolution (1)

## Version 1 (100\$)

	✓ (~)	encrypted RAR archive
	✗	static password
	✗	same static password for all users
	✓	password known to the attacker







## Version 2 (300\$)

	✓ (~)	encrypted RAR archive
	✗	machine dependant password
	✓	different passwords for different machines
	✓	attacker can compute the password





# ACCDFISA evolution (2)

Version 2 (300\$)

	✓ (~)	encrypted RAR archive
	✗	machine dependant password
	✓	different passwords for different machines
	✓	attacker can compute the password





# ACCDFISA evolution (2)

## Version 2 (300\$)

	✓ (~)	encrypted RAR archive
	✗	machine dependant password
	✓	different passwords for different machines
	✓	attacker can compute the password







## Version 3 (900\$)

	✓ (~)	encrypted RAR sfx archive
	✓	random generated password
	✓	different passwords every time
	✓	the random password is sent to the server





# ACCDFISA evolution (3)

Version 3 (900\$)

	✓ (~)	encrypted RAR sfx archive
	✓	random generated password
	✓	different passwords every time
	✓	the random password is sent to the server





# ACCDFISA evolution (3)

## Version 3 (900\$)

	✓ (~)	encrypted RAR sfx archive
	✓	random generated password
	✓	different passwords every time
	✓	the random password is sent to the server







## Version 4 (500\$ in the first 48h or 1000\$ later)

	✓	encrypted RAR sfx archive + sdelete
	✓	random generated password
	✓	different passwords every time
	✓	the random password is sent to the server

# ACCDFISA evolution (4)





Version 4 (500\$ in the first 48h or 1000\$ later)

	✓	encrypted RAR sfx archive + sdelete
	✓	random generated password
	✓	different passwords every time
	✓	the random password is sent to the server



# ACCDFISA evolution (4)

Version 4 (500\$ in the first 48h or 1000\$ later)

	✓	encrypted RAR sfx archive + sdelete
	✓	random generated password
	✓	different passwords every time
	✓	the random password is sent to the server



Version 5 (5000\$)

- ✓ fake BSoD
- ✓ services killer

*"We know that you have money"*

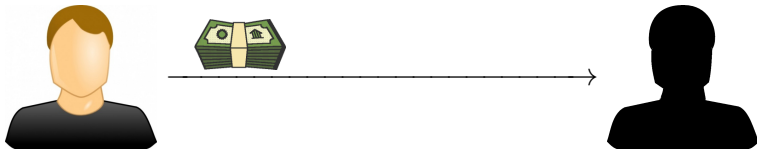
# Agenda

- 1 Introduction
- 2 Screen-locking ransomware
- 3 File encryptors
- 4 How about the money?**
- 5 Conclusions

# How about the money?

## PC Cyborg Trojan (1989)

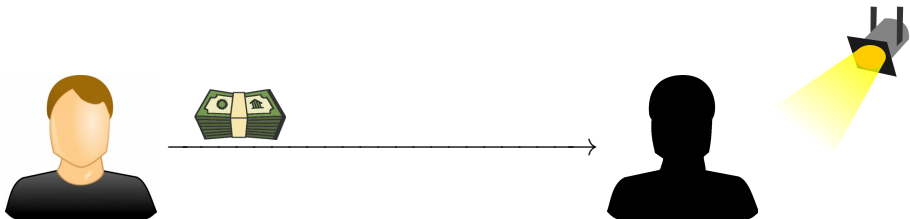
- post office box in Panama



# How about the money?

## PC Cyborg Trojan (1989)

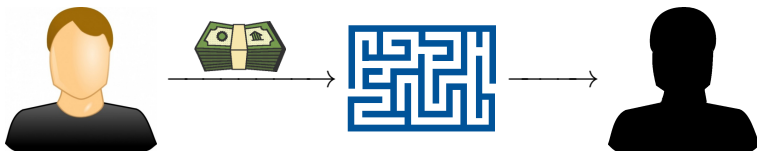
- post office box in Panama



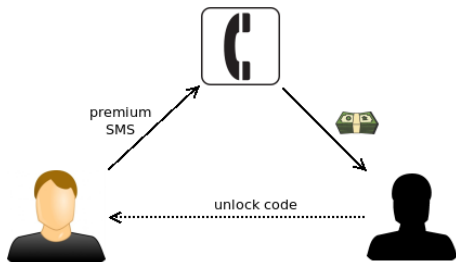
# How about the money?

## PC Cyborg Trojan (1989)

- post office box in Panama



# SMS money laundering



Alternative: ask the victim to send recharging codes for cell phone cards

Problems:

- only works in the same country
- small amount of money

# Outsourcing the money collection task

Your computer has been watching illegal pornographic movies, due to this, this screen will not start with the computer until you have done the following survey to verify that you are a human.  
**WARNING: IF YOU DO NOT DO THE SURVEY, ACTIONS WILL BE DONE.** When you are done with the survey, write the activation code in the textbox below. The website may take some time to load, when clicking a survey, your default browser will open. You have 30 minutes to do the survey. **IF YOU SHUTDOWN YOUR COMPUTER, IT WILL CRASH.** Click "Normal Download" to start the survey.



The screenshot shows a web browser window displaying the 'shrinkonce' website. The page has a dark navigation bar with links for Home, Login, Register, Payment Proofs, Community, Blog, FAQ, and Contact. Below the navigation bar, the text 'FILE DOWNLOAD' is prominently displayed in red. In the center, a file icon for 'keycode.txt' is shown with a size of '19 kb'. At the bottom of the page, there is a red box containing the text 'ACTIVATION CODE:' followed by a text input field containing 'xxx-xxx-xxx' and a 'CHECK' button.

If you are unable to the survey in the built-in browser, click [HERE](#) to open the website in the default browser(better).

ACTIVATION CODE:

CHECK

## Money transfer services

- prepaid coupons for online spending
- easy to buy
- easy to transfer
- hard to track



Exchange your money for a unique Ukash code



Use the code to spend or send money online instantly





## Liberty reserve

The most commonly used money transfer service on the black market.

- 1LR (1 Liberty Reserve) = 1\$
- 1% transaction fee
- 0.75\$ privacy fee



- only name, e-mail and date of birth required to open an account
- 55 million transactions
- more than \$6 billion laundered money so far

## Liberty reserve

The most commonly used money transfer service on the black market.

- 1LR (1 Liberty Reserve) = 1\$
- 1% transaction fee
- 0.75\$ privacy fee



- only name, e-mail and date of birth required to open an account
- 55 million transactions
- more than \$6 billion laundered money so far



# Where is it going?

- Other platforms are targeted
  - Mac OS
  - Android
- Ransomware gets more integrated into the malware industry
  - Recently discovered ransomware also exhibits bot behaviour (C&C server, DGA)

# Agenda

- 1 Introduction
- 2 Screen-locking ransomware
- 3 File encryptors
- 4 How about the money?
- 5 Conclusions

# Conclusions

- The amount of ransomware in the wild is increasing.
  - $> 10^5$  recent samples
- File encryptors can be a real threat
  - sometimes backup is the only option

## You are not safe!



Thank you!  
Questions?