The Ransomware Strikes Back

Virus Bulletin 2013

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

Bitdefender

October 4, 2013

Agenda

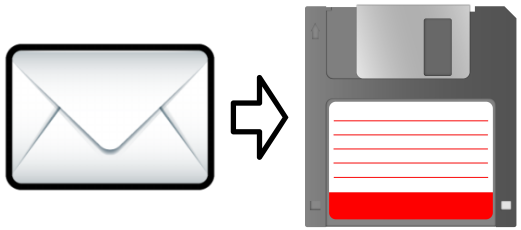
Agenda

An incursion into the past

1989

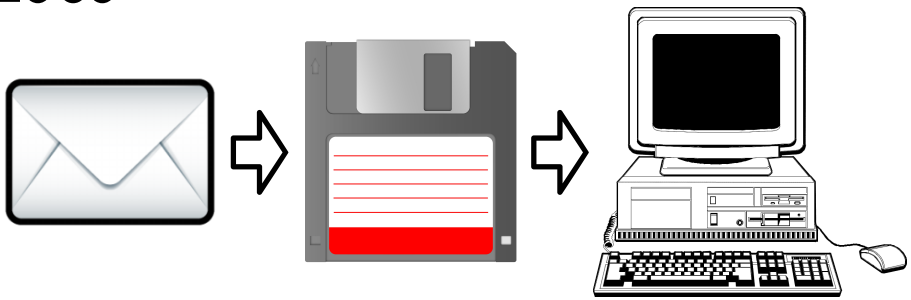
An incursion into the past

1989



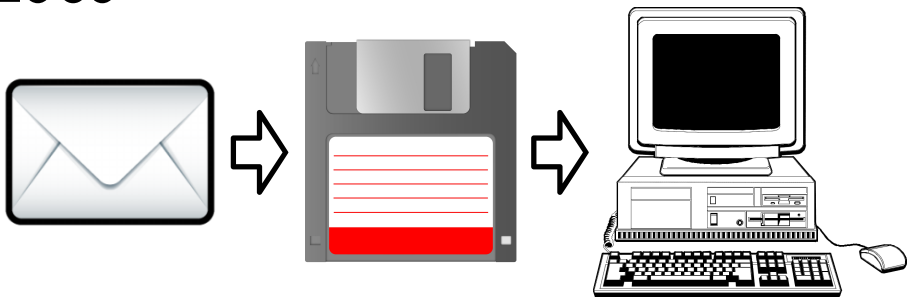
An incursion into the past

1989



An incursion into the past

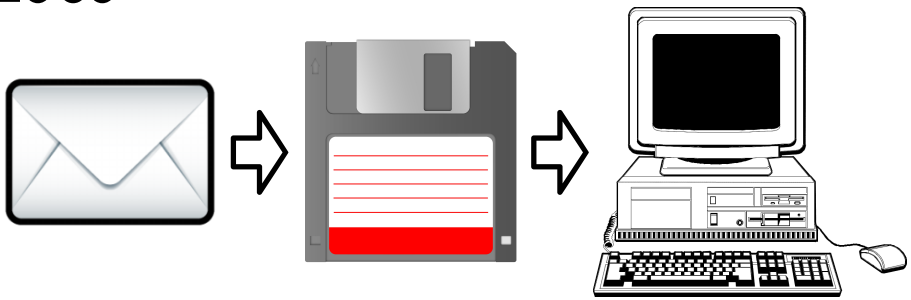
1989



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

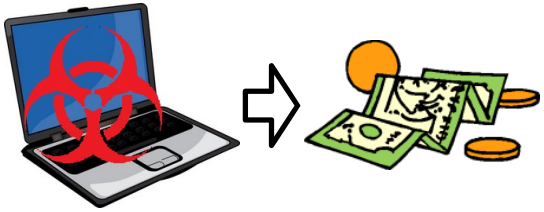
Definition (Ransomware)

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

The present ransomware

Definition (Ransomware)

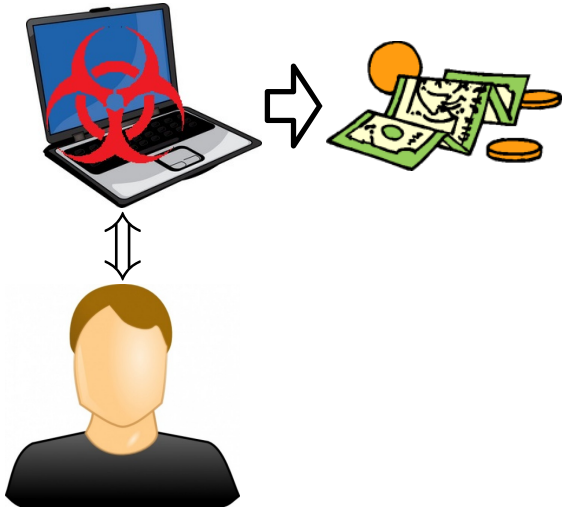
Malware that restricts access to a computer system and demands a ransom in order to restore it.



The present ransomware

Definition (Ransomware)

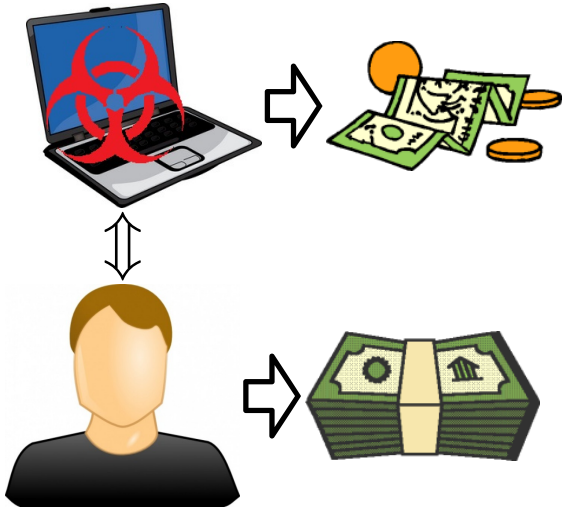
Malware that restricts access to a computer system and demands a ransom in order to restore it.



The present ransomware

Definition (Ransomware)

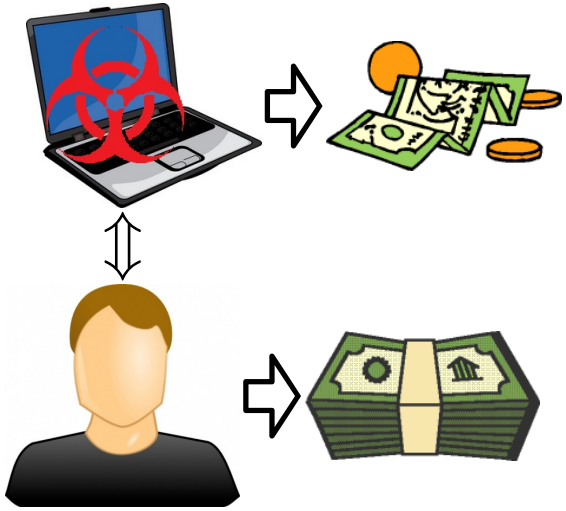
Malware that restricts access to a computer system and demands a ransom in order to restore it.



The present ransomware

Definition (Ransomware)

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



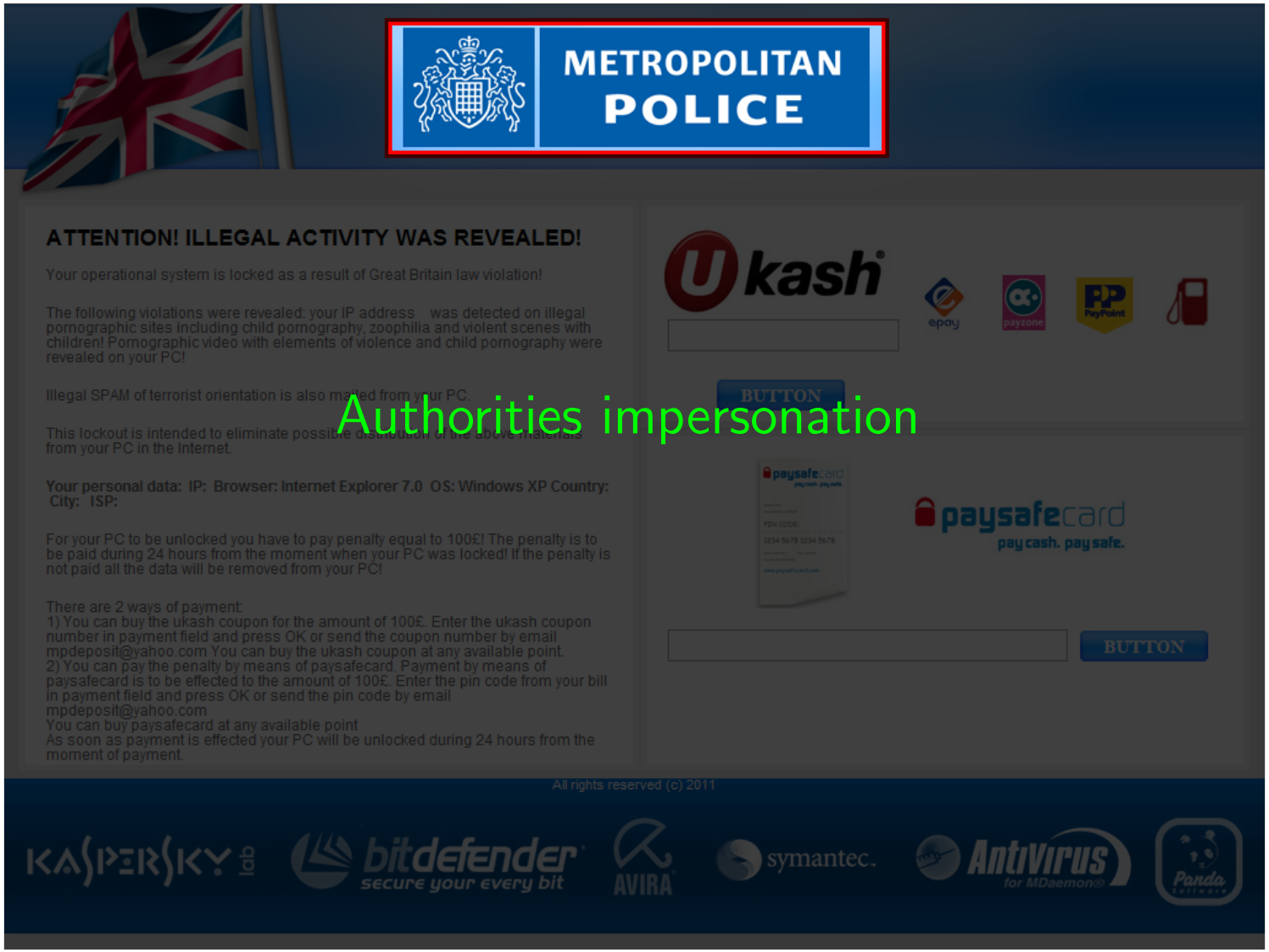
Types of ransomware

- Screen lockers
- File encryptors

Agenda

The screen lock anatomy

The screen lock anatomy



Authorities impersonation

The screen lock anatomy

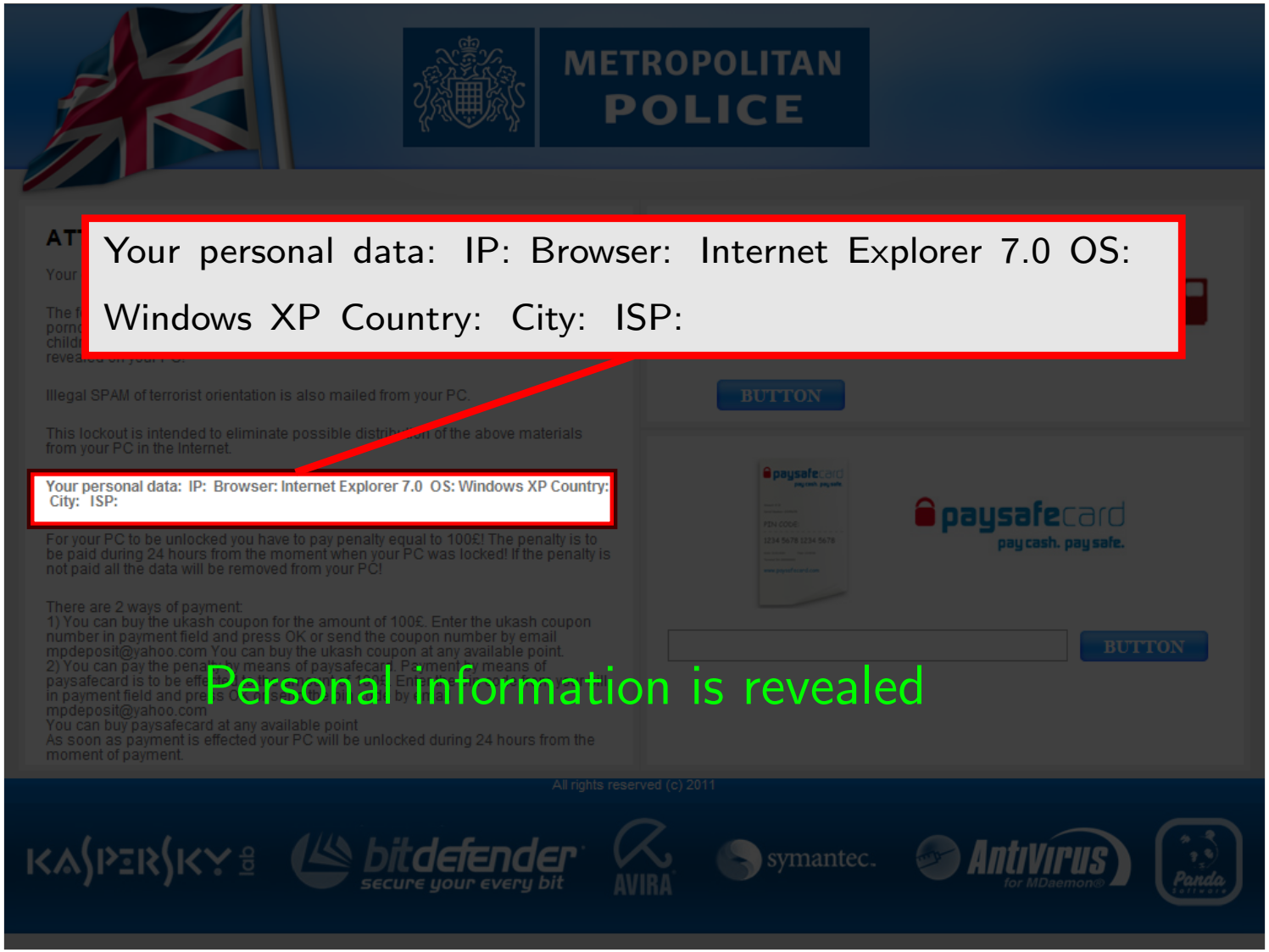
Known anti-malware companies make the things look even more serious

The screen lock anatomy

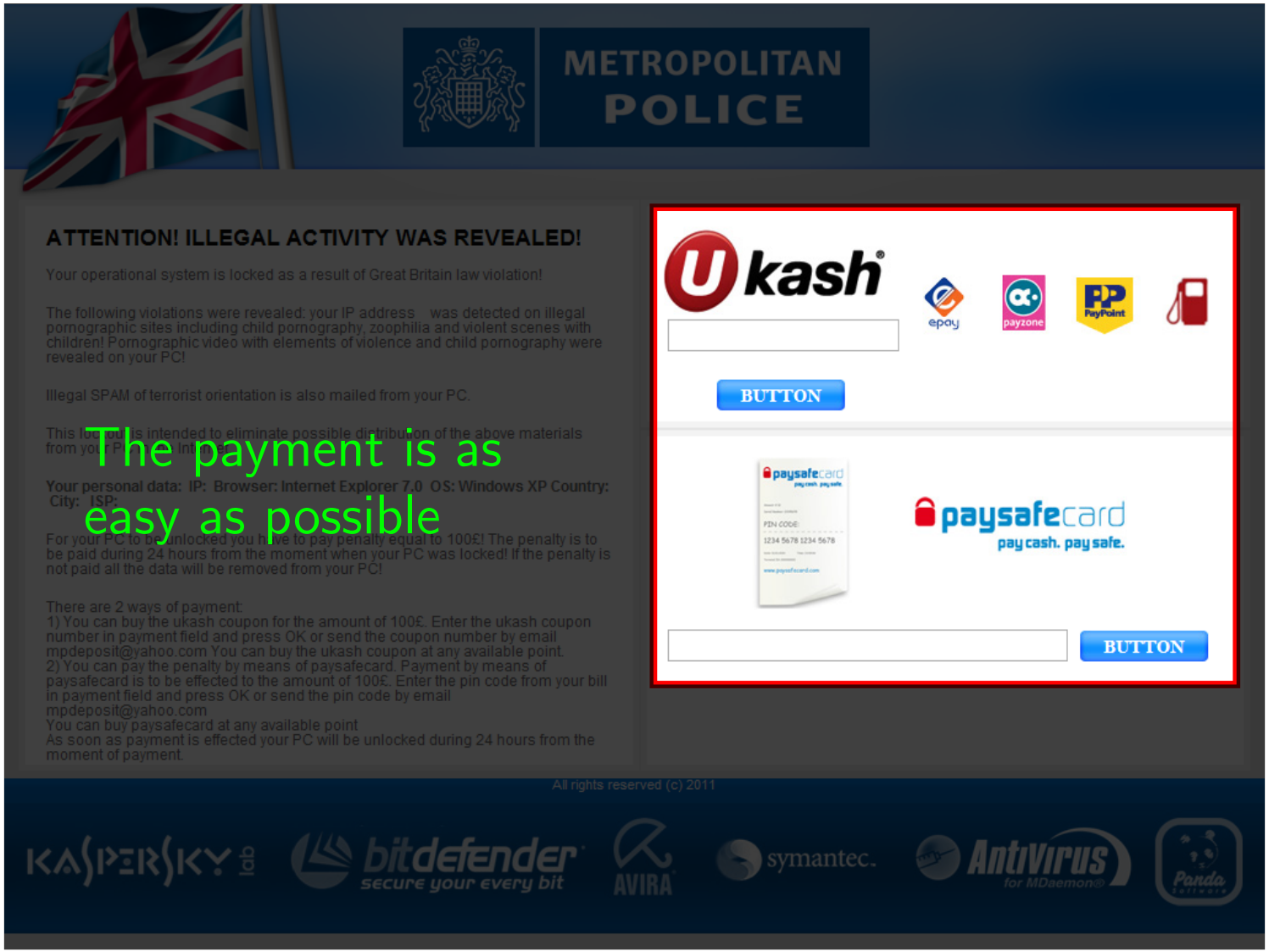
- child pornography
- zoophilia
- illegal spam of terrorist orientation

The user is blamed for illegal activities

The screen lock anatomy



The screen lock anatomy



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

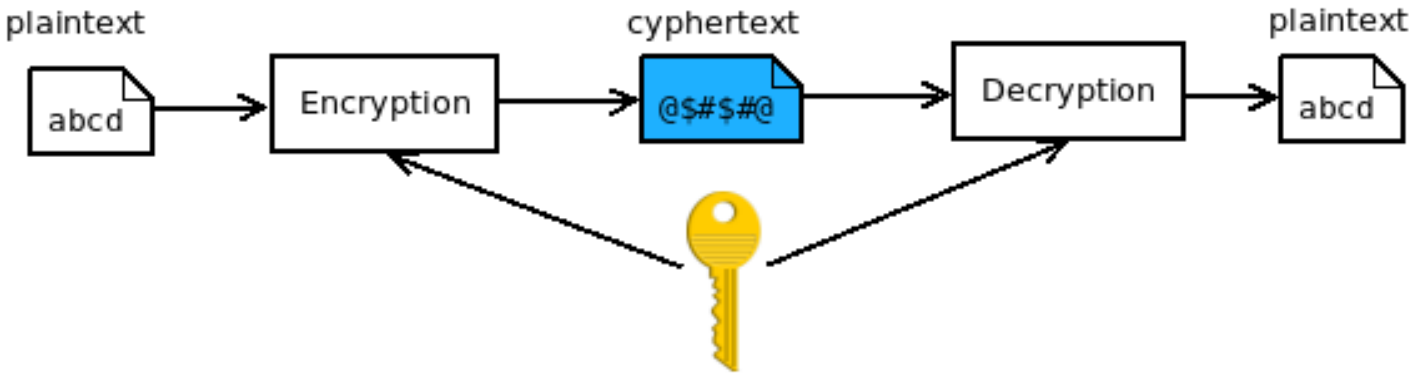
The trick is to prevent the user to get help

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

Agenda

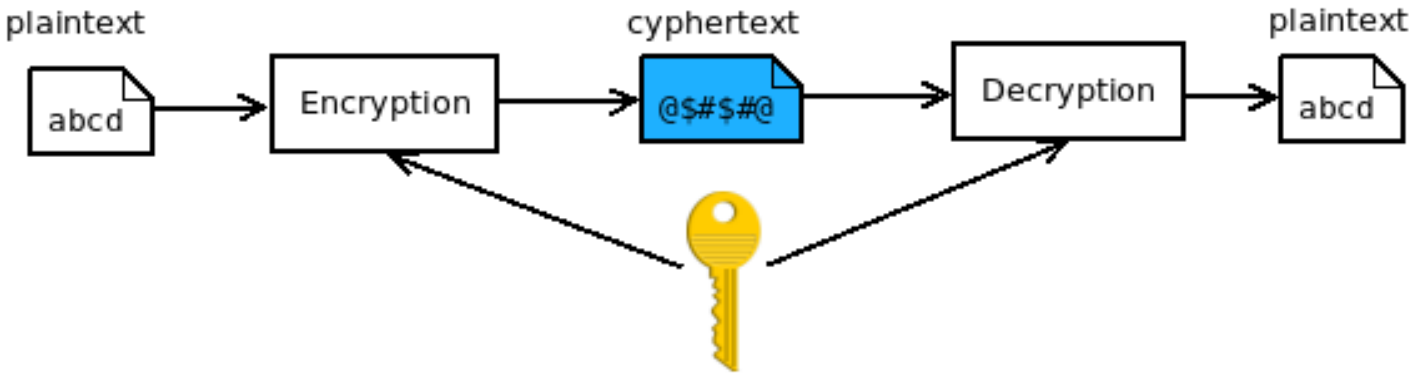
A (very short) crash course in cryptography

Symmetric encryption

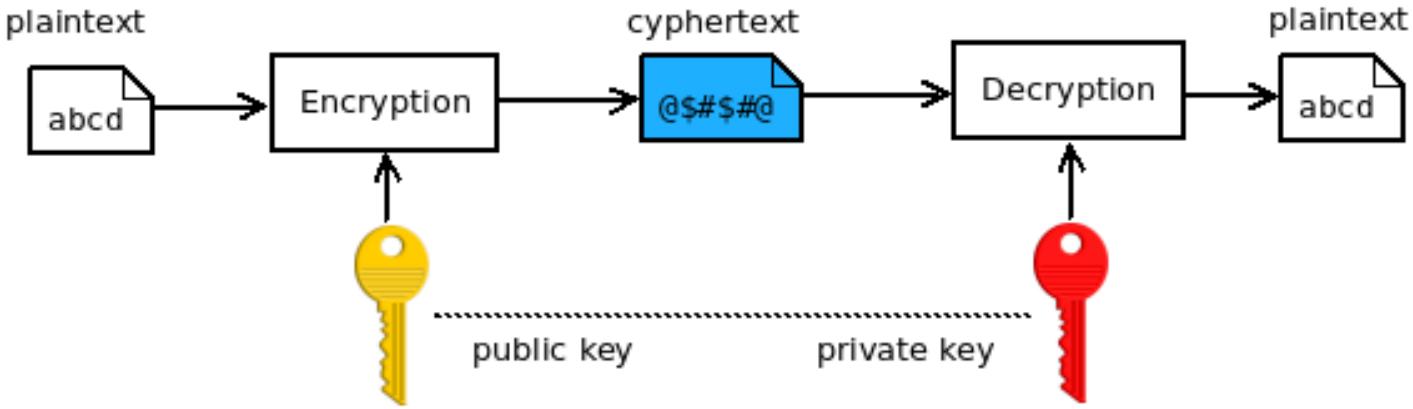


A (very short) crash course in cryptography

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

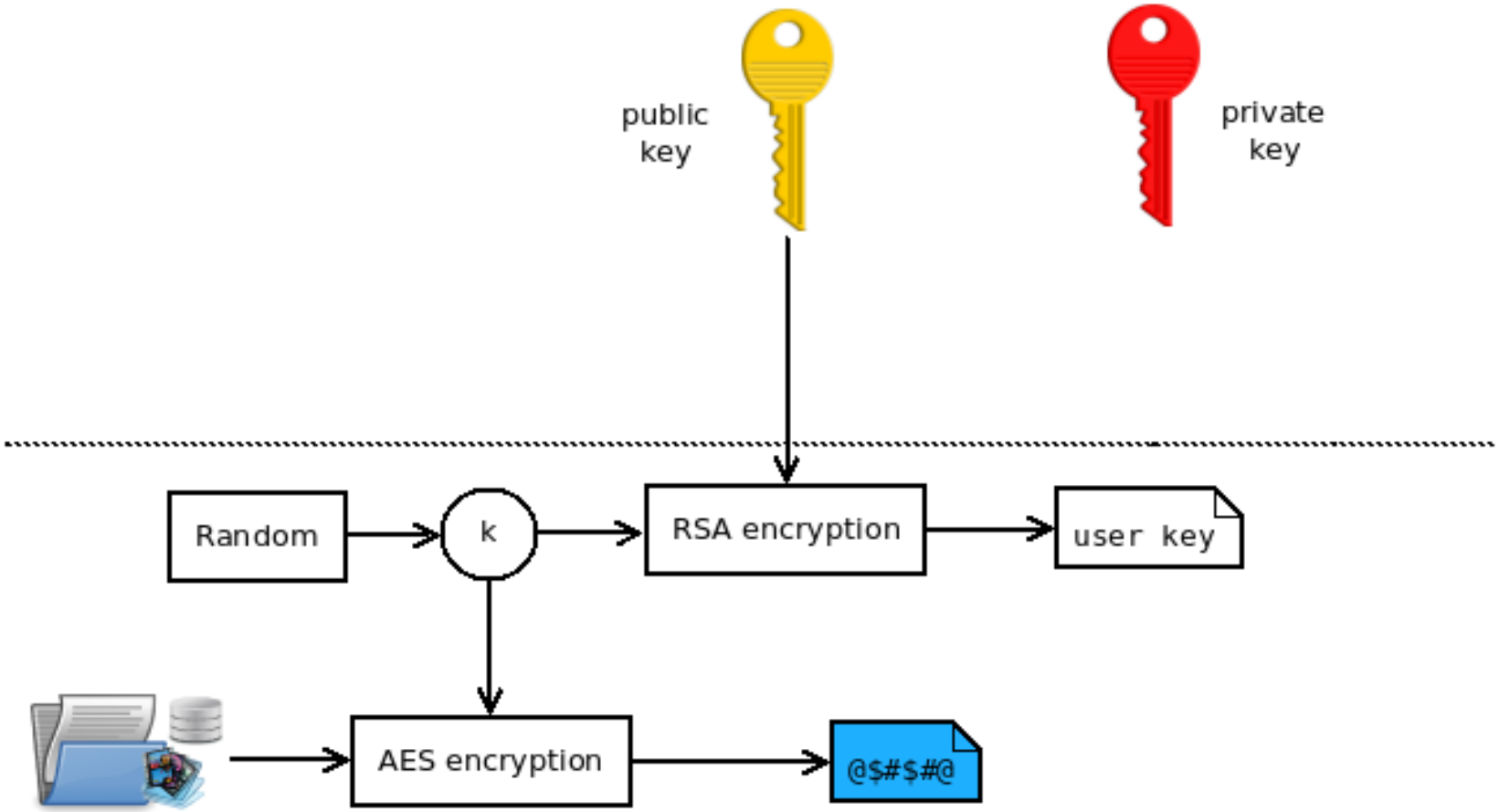
After a user has paid the ransom, the key/decryption tool should work for his system alone.

Feature 4

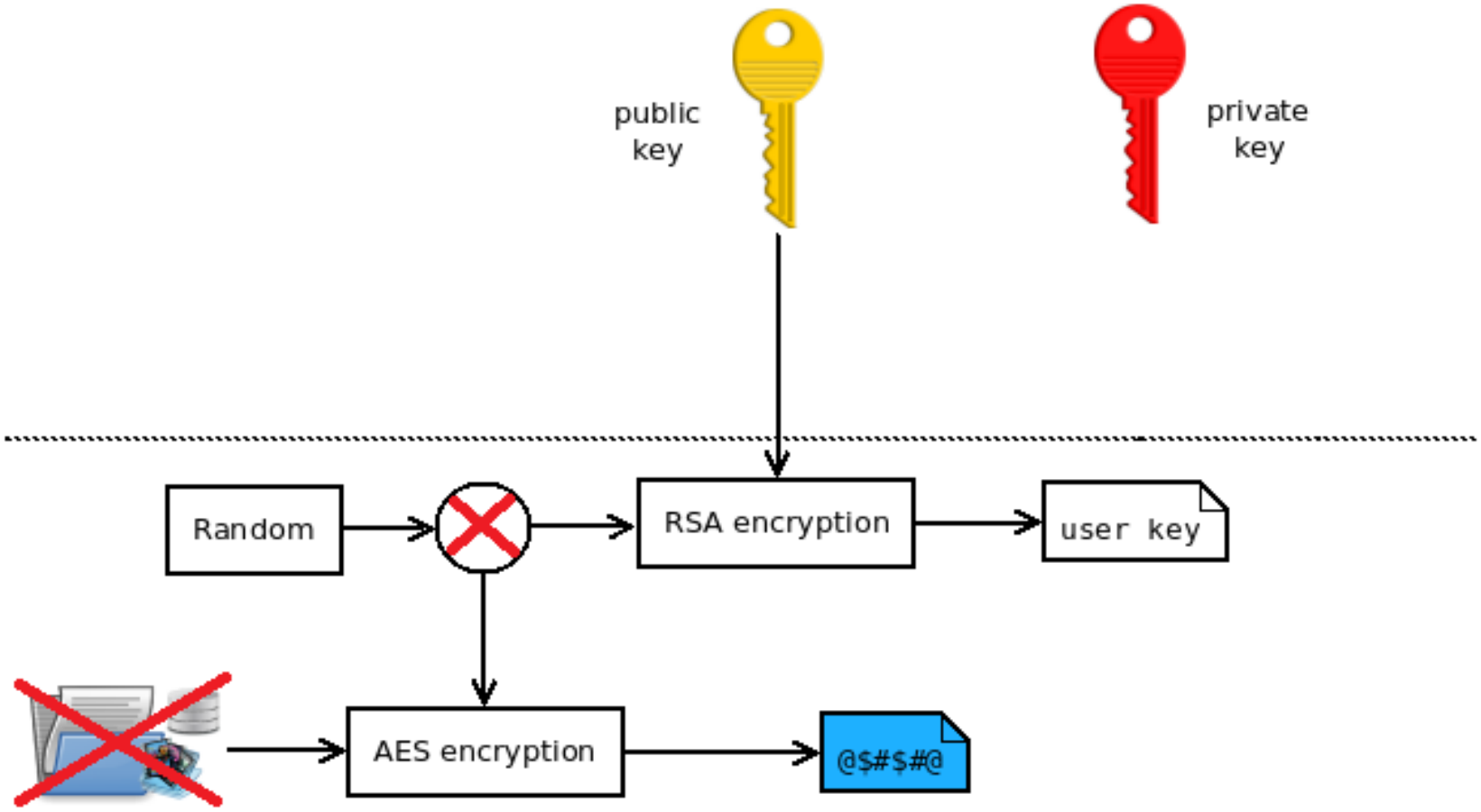
The decryption key should be available to the attacker after a successful attack. The decryption key should not be lost, even if the victim is offline during the encryption.

A proper file encryptor: GPCode (1)

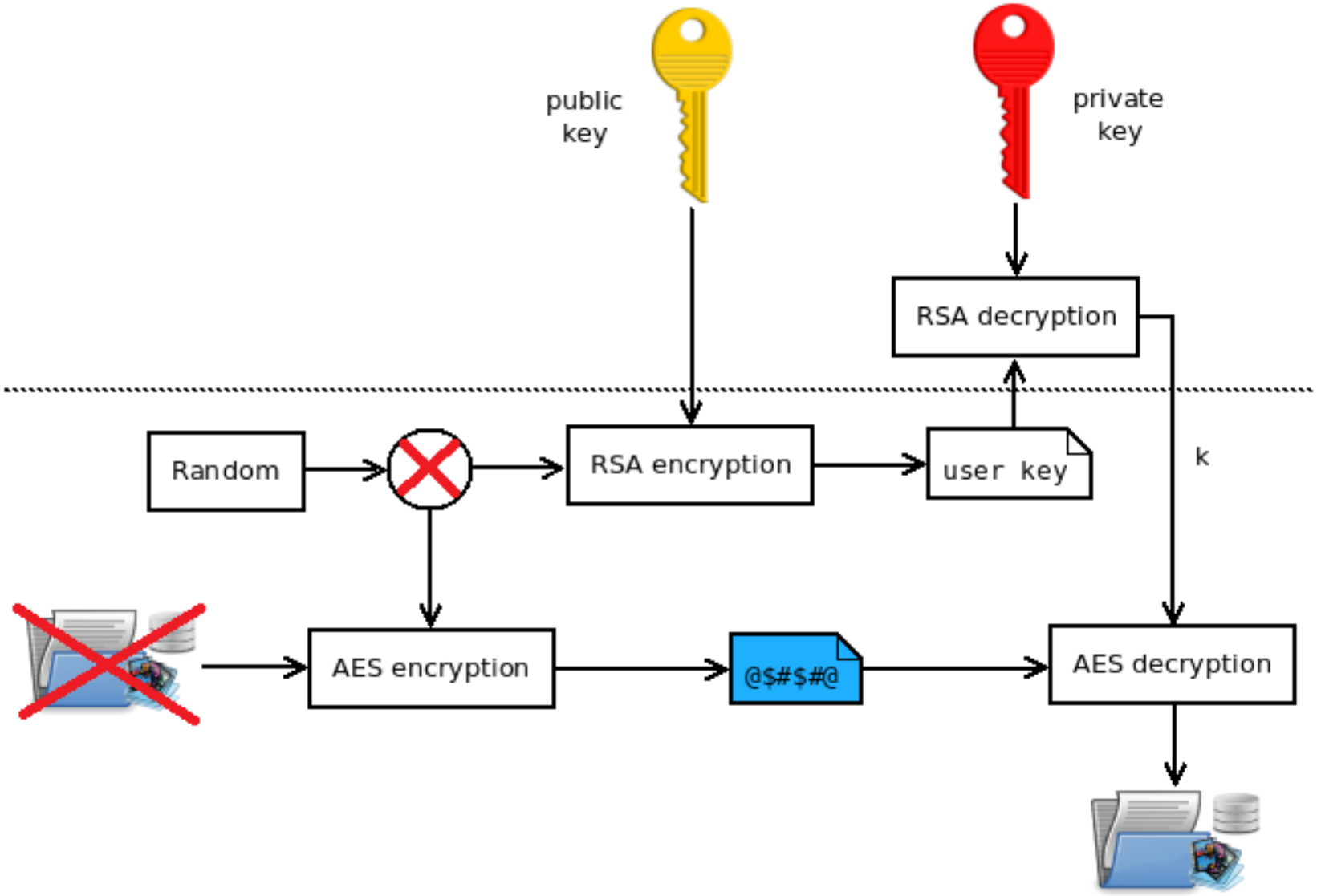
A proper file encryptor: GPCode (1)



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

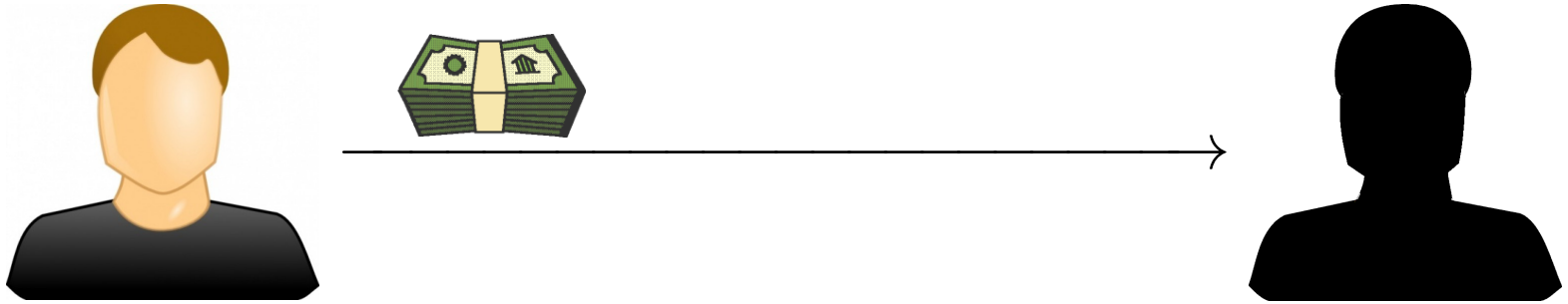
"We know that you have money"

Agenda

How about the money?

PC Cyborg Trojan (1989)

- post office box in Panama



How about the money?

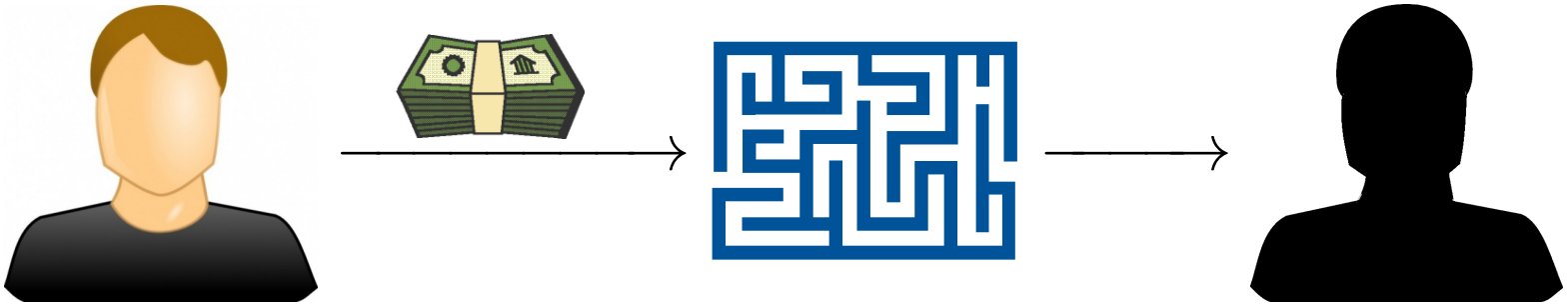
PC Cyborg Trojan (1989)

- post office box in Panama

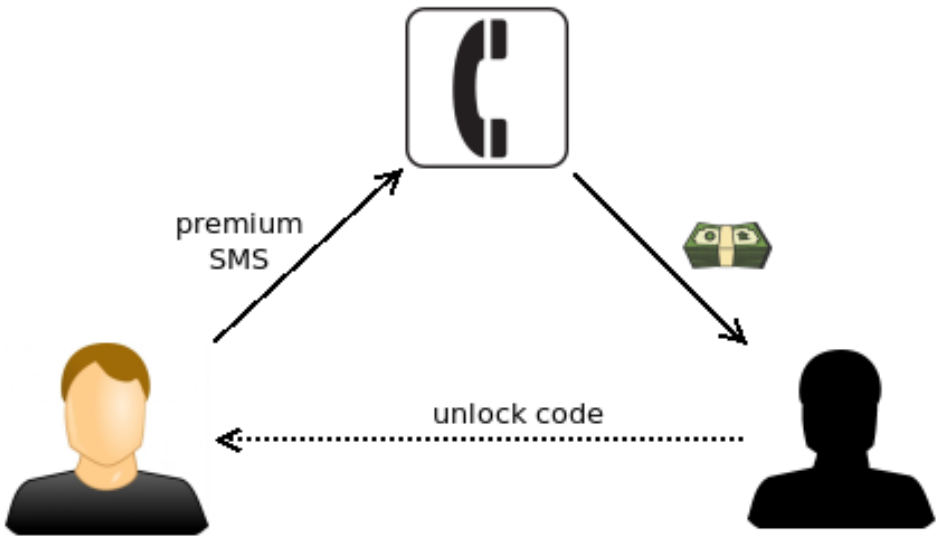
How about the money?

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

Money transfer services

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

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

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!

Bitdefender®

Thank you!

Questions?