

- # The Carbanak Hack

EECS 3482: Computer Security

## ● This Presentation

○ What happened?

○ How did it happen?

○ Implications



Let's Start with a video...

The Carbanak Hack



1

# What Happened?

Let's explain the event itself

● What happened?

## What is Carbanak?

Cybergang whose attack was targeting Financial Institutions.  
Discovered by Kaspersky Lab in 2015

## What happened first?

In late 2013, an ATM in Kiev started distributing cash at random times during the day! (Lucky customers being here...)



The Carbanak Hack



**1,000,000,000\$**

Whoa!

1 billion dollars: Estimated amount of money stolen by the cybergang Carbanak.

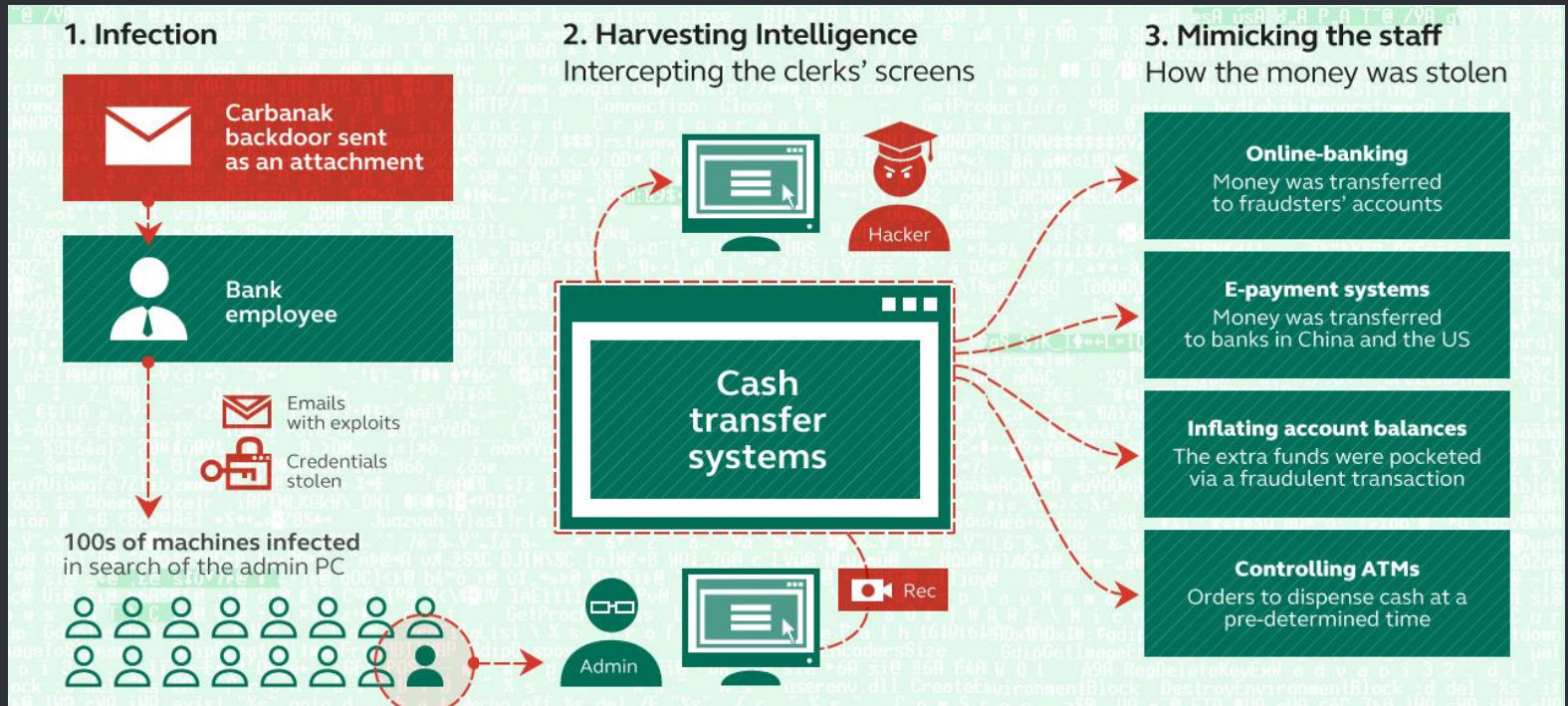


2

## How did it Happen?

Let's explain the hack

# How the Cabarnak Gang stole 1 billion





“

One of the most sophisticated  
cyber-attacks ever.

Chris Dogget,  
Managing Director of Kaspersky North America

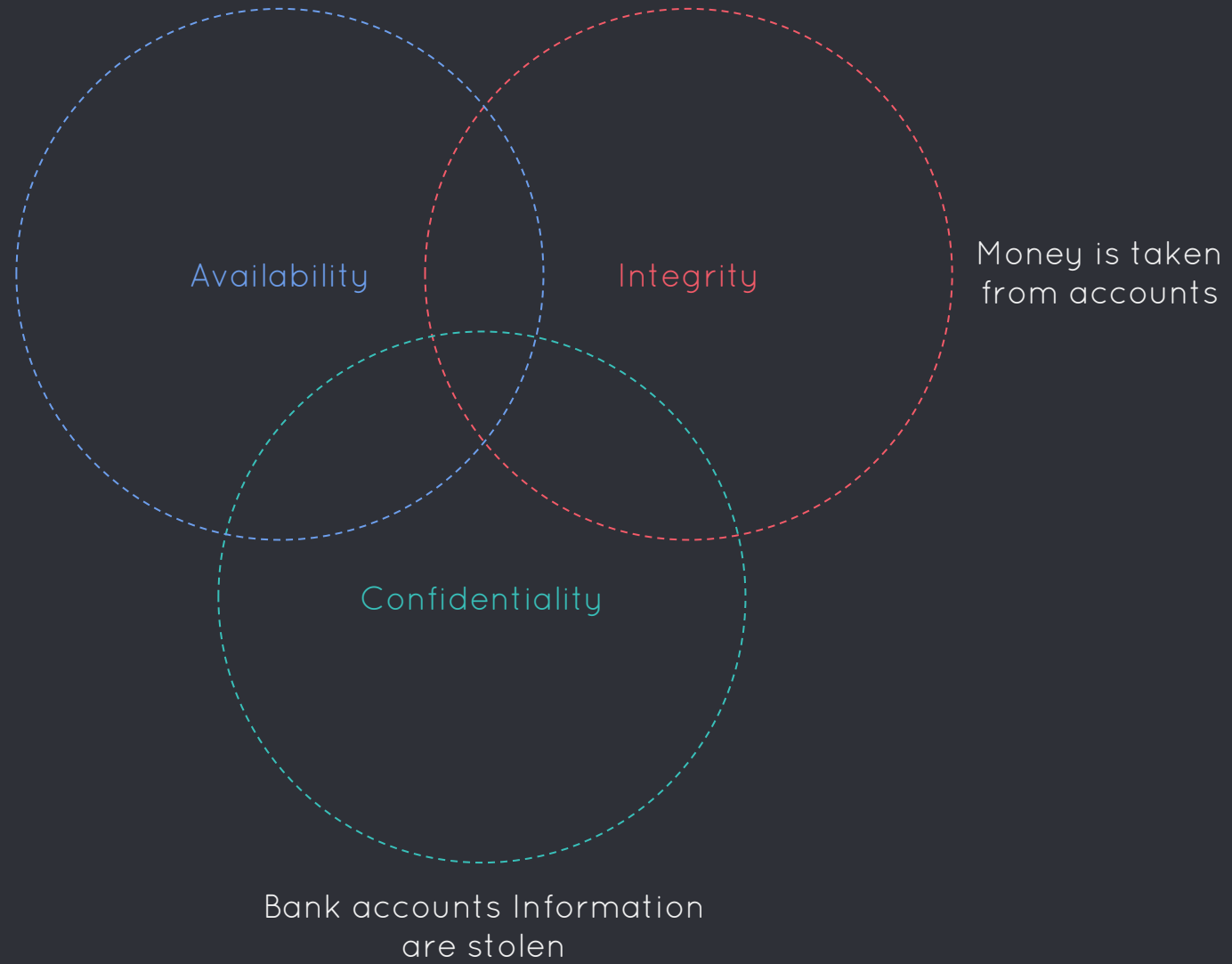


3

# Implications

Society and Security

● CIA Implications



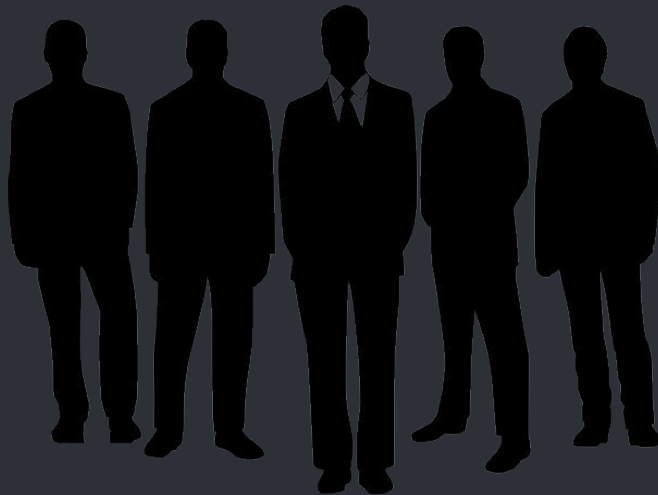
## ● Problems

### ○ Invisibility

The Malware remained undetected for almost two years

### Organized Crime

E.G: ATMs are dispensing cash while mules are here to pick it up



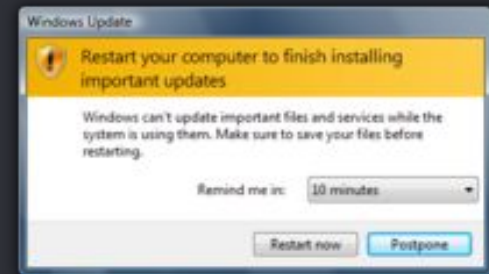
● What can we do against it?

## Kaspersky Lab

- Company working to secure bank systems against malwares.

## Measures

- Awareness of employees and updating frequently.
- Detect malwares in existing banking systems and communication channels.



The Carbanak Hack

## What can we do against it?

# Every bank should know

## Traces of Carbanak infection

**CARBANAK DETECTED**

Indirect attributes of Carbanak's presence in a bank network

### A Paexec file

In Windows\ catalogue helping to run commands on a remote machine



© 2015 Kaspersky Lab

The billion-dollar advanced persistent threat is in your bank's network, if:

- 1 There are **files with .bin extension** at the following location:  
\\All Users\%AppData%\Mozilla\  
or c:\ProgramData\Mozilla
- 2 There is **a svchost.exe file** in Windows\System32\com\ catalogue (or Windows\Syswow64\com\ catalogue - for 64-bit OS Windows)
- 3 Among the active Windows services **the Services ending in "sys"** were found, duplicating a similar service stored without the "sys"  
**Example:** you find an instance of the aspnet service while the legal aspnet service is active on the system.

GREAT

KASPERSKY

## ● Questions

○ Approximately how much money was stolen?

Around 1 billion Dollars.

Why did the hackers wait for so long before going on the attack?

For the malwares to stay undetected and because of bad detection systems.

What measures could help prevent attacks like Carbanack in the future?

Awareness of employees, frequent updates and search for malwares

## ● Actual References

- <https://securityintelligence.com/carbanak-how-would-you-have-stopped-a-1-billion-apt-attack/>
- [http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-viamalware.html?partner=socialflow&smid=tw-nytimes&\\_r=1](http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-viamalware.html?partner=socialflow&smid=tw-nytimes&_r=1)
- <http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide>



Thanks!

ANY QUESTIONS?