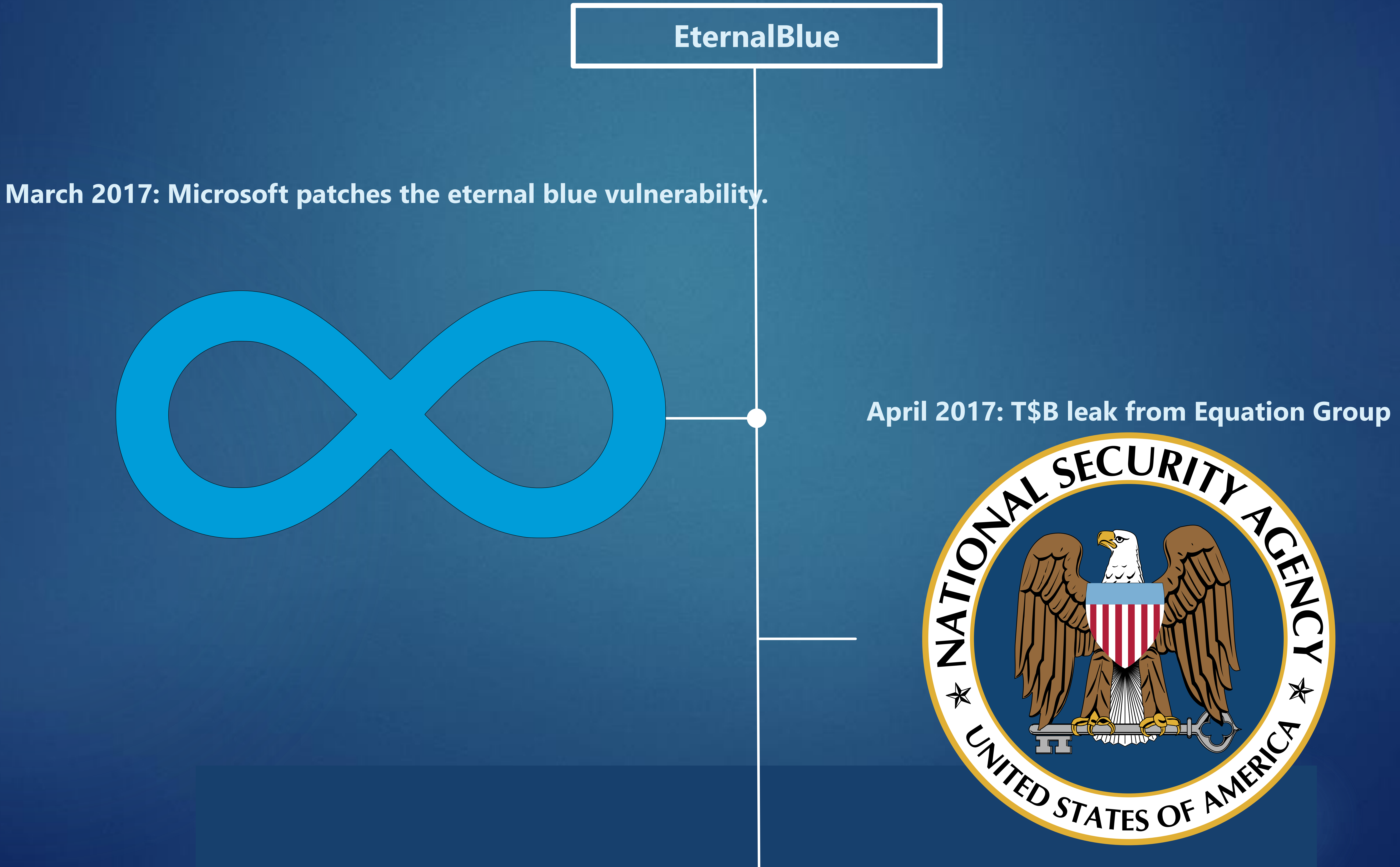
Software Exploitation

INTRODUCTION

RE TACTICS

EternalBlue

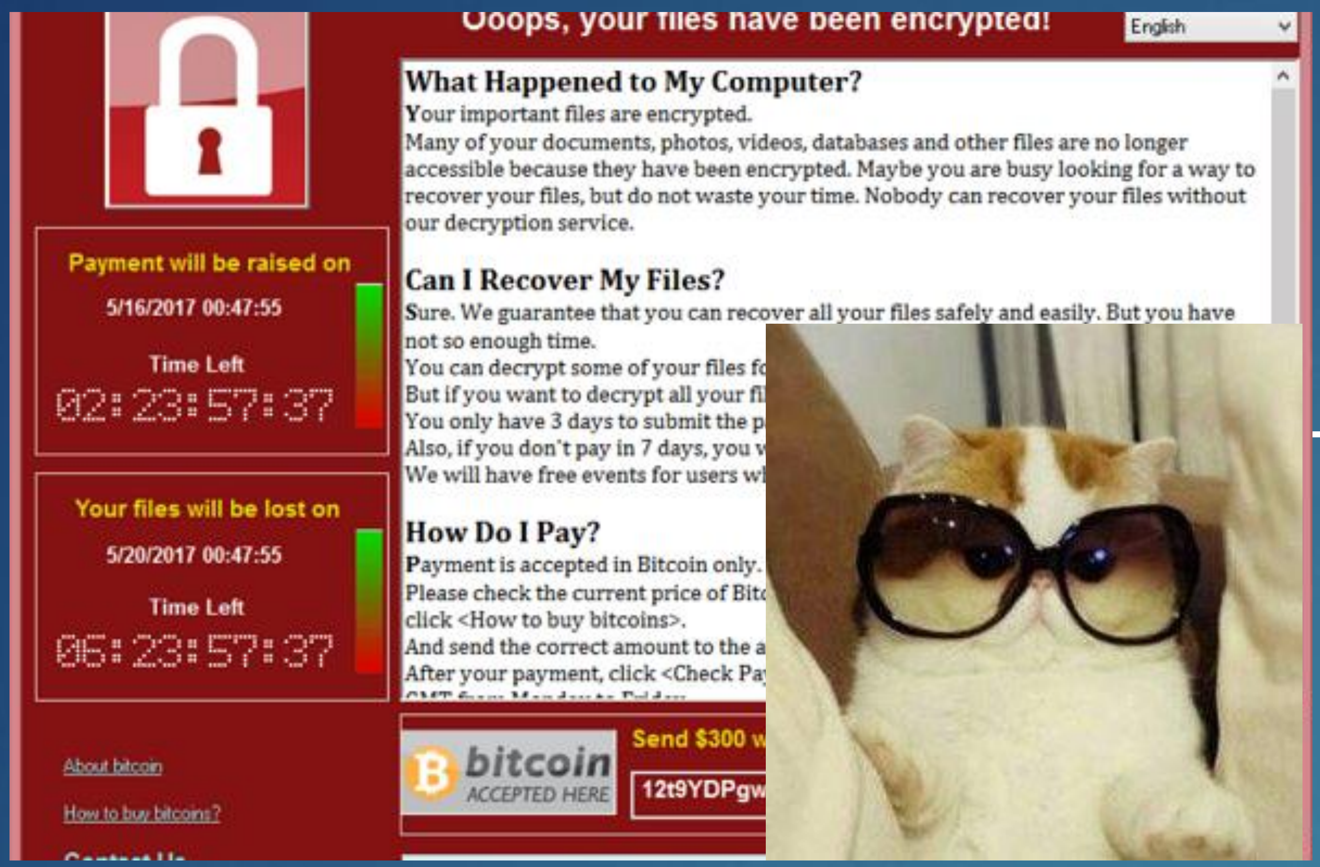


EternalBlue

March 2017: Microsoft patches the eternal blue vulnerability.

April 2017: T$B leak from Equation Group

May 2017: WannaCry & MalwareTech



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files fo

But if you want to decrypt all your fi

You only have 3 days to submit the p

Also, if you don't pay in 7 days, you w

We will have free events for users wh

How Do I Pay?

Payment is accepted in Bitcoin only.

Please check the current price of Bitc

click <How to buy bitcoins>.

And send the correct amount to the a

After your payment, click <Check Pa

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

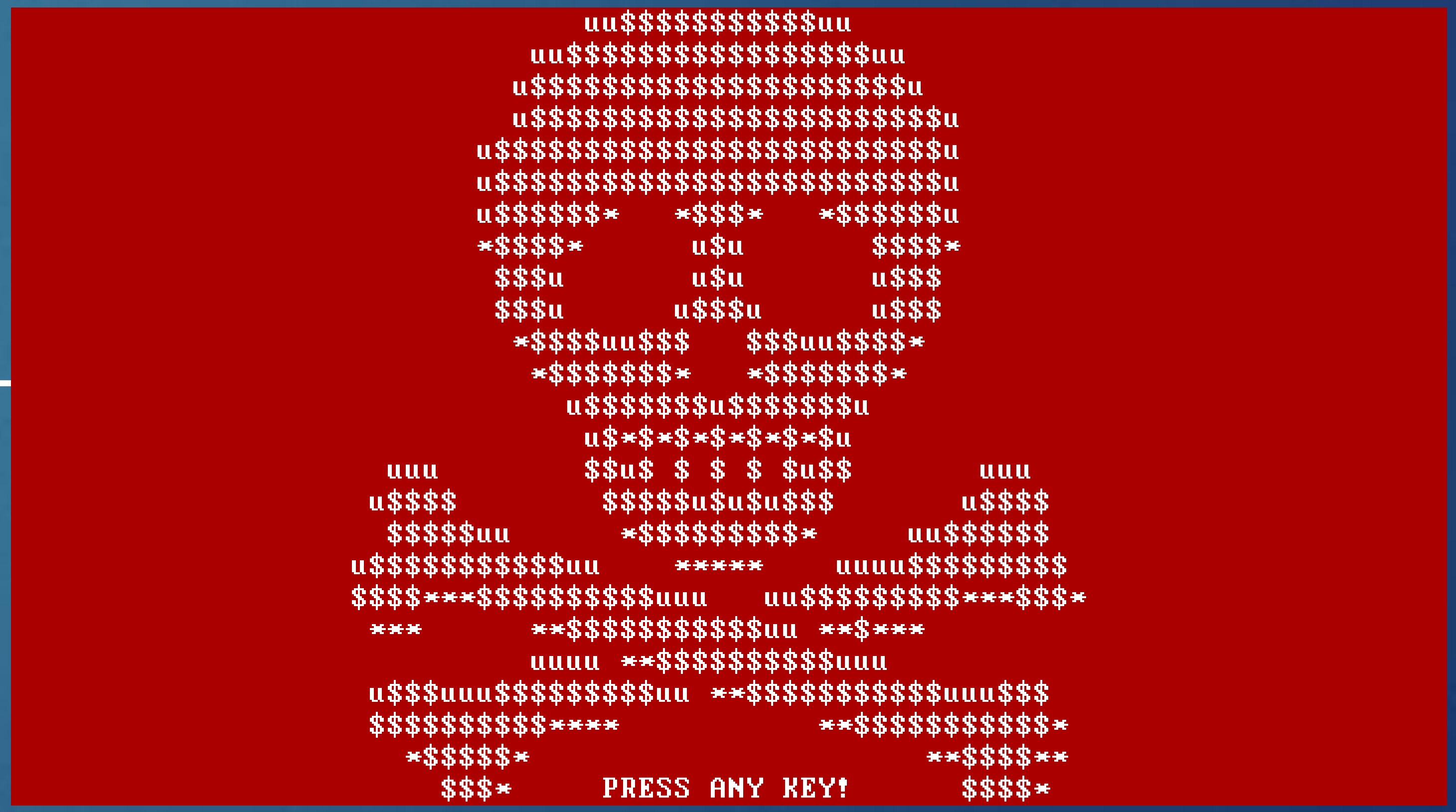
Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

June 2017: NotPetya



Who am I ?

Independent security researcher. Specialized in low-level software Reverse Engineering & Exploitation, and in particular:

- UEFI firmware
- Kernel & virtualization.
- Embedded Software

BRUNO PUJOS

Who Are You ?

Lecture Format

Discuss

Ideas

No Monitoring

Practice

RE TACTICS

Evaluation

- Graded exercises
  - Make the exercise works.
  - Call me and **explain it to me**.
  - Points validation is “manual”.
- WARNING: This means that I will not be giving solution for most exercises.
  - But I will still help you as usual.
  - Call me!
- Team: up to 3 person
  - Was made for being done individually

Name	Nb Points
sbof103	1
sbof200	2
format101	1
format102	2
rop100	2
rop200	3
rop300	3
heap101	1
heap300	4
uaf100	2
heap500	4
int100	1
int300	3
uninit300	2

Setup

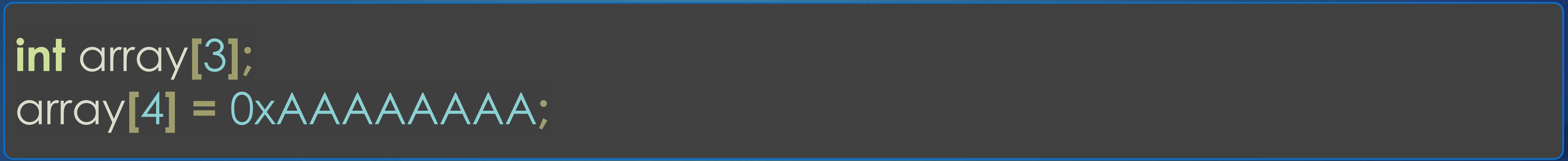
- You will need several VMs, for Windows & Linux.
  - Advises making snapshots for being able to reset in a clean state.
- Several tools will be necessary as we go.
  - Make sure to have them all ready for the CTFs!
  - Might not have the code source for some exercises: be sure to have something for being able to reverse!
- Most practice will be online:
  - CTF interface at http://51.15.171.241:9000/
- Materials & exercises are always made available.

What is binary exploitation ?

What kind of vulnerability may we find ?

Memory Corruptions

- **Memory Corruptions** are bugs which occurs when memory is modified without the original intent to be.
  - Common in (old) low level languages (mainly C and C++) which do not perform bound checks.



```
int array[3];
array[4] = 0xAAAAAAAA;
```

- Those would generally generate segfault as error.

- Some of those memory corruptions bugs can be exploited and become vulnerabilities.
  - Buffer Overflow (BOF), Format String (Format), Use-After-Free (UAF), …

Lecture Parts

01

Basics To Modern

02

Heap Exploitation

03

Other Vulnerabilities

THANK YOU

Bruno Pujos