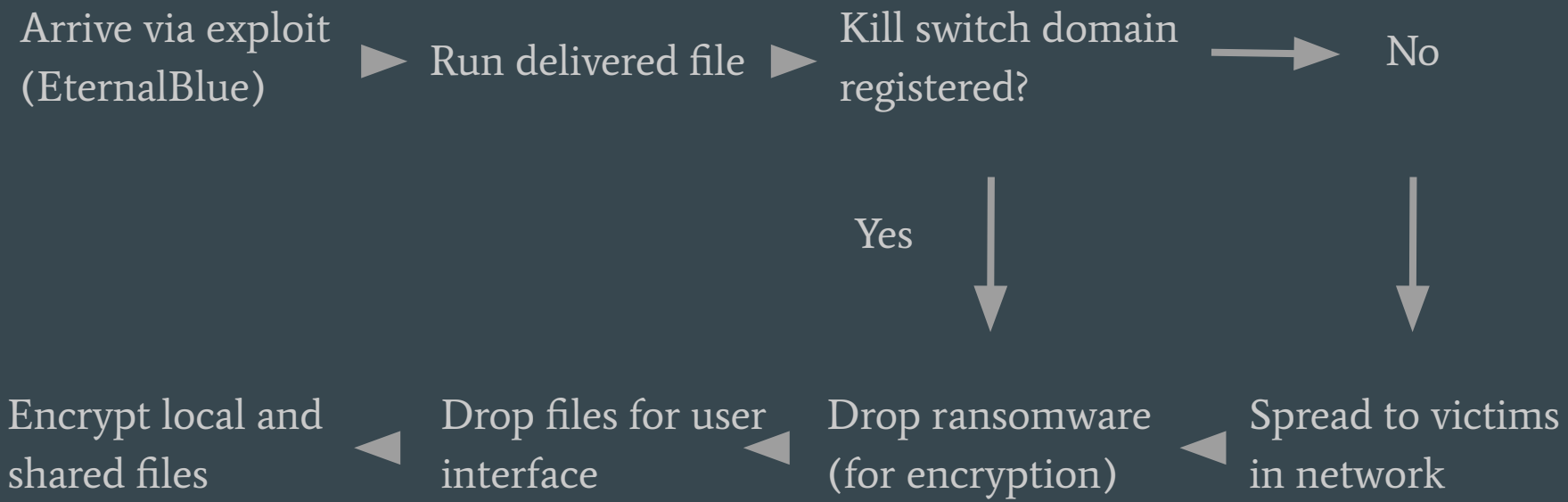
WannaCry and EternalBlue

27th May 2020

Chronology and Damage

- Targeted Windows machines
- Attack occurred in May 2017
- Self propagated between computers both within and outside network
- Encrypted all files & demanded payment for decryption key
- Over 200,000 afflicted computer
- $4 billion in damages
- Backdoor found within a few days and exploit patched shortly afterward
- Still thousands of unpatched computers

WannaCry Program Flow



EternalBlue - Mechanism

Bug 1 - Casting

32-bit ulong field updated with 16-bit ushort

```
0x1234 5678 <- 0xabcd
```

MSBs remain unchanged

```
0x1234 abcd
```

Bug 2 - Parsing

Different request types with different header field sizes

Assume first request type for following requests

Triggers bug 1

Bug 3 - Allocation

Details of bug 1

Memory spaces in non-paged pool are tightly linked

Overflow into next chunk leads ro remote code execution

How it could have been prevented

- Bug 1: Static code analysis should have found dangerous casting
- Bug 2: Fuzzing random request sequences should have triggered bug 1 which could have been backtraced to wrong parsing
- Bug 3: Verifying memory allocation sizes for related packages, verifying that write access do not overwrite chunk boundaries should have found the issues