Exploiting a Vulnerability to Deepen Our Knowledge of an OS

Arnold Smithson
Justin Guerrero
Jada Bryant
Teyler Halama

November 15, 2020

CSCI 460 - Operating Systems, Fall 2020
Professor Travis Peters

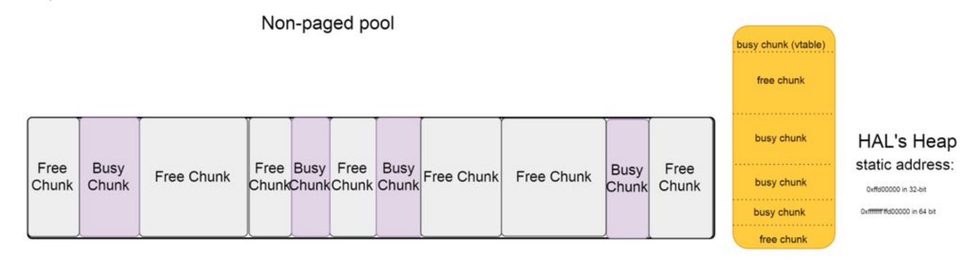
General Overview

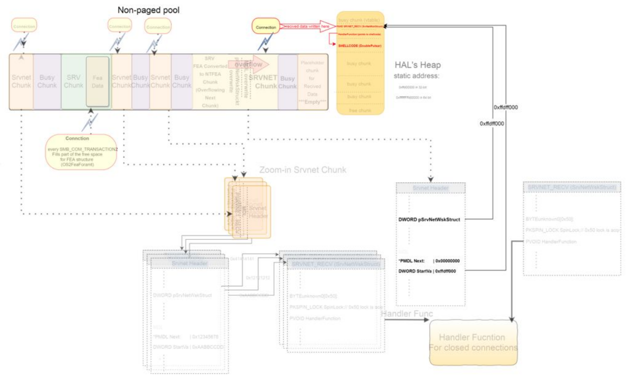
- Why did we want to do this topic?
- How does malware tie into CS460
- Key Ideas
- What was learned?

How Malware Relates to CSCI-460

- Security
    - Malware is created to attack the OS
    - Malware that uses EternalBlue is mostly ransomware
        - Attacks the file system via encryption and overwriting
- Preparing the OS for attacks
    - To create an OS we need to understand how to attack it

Key Idea: Exploits are a creative uses of bugs





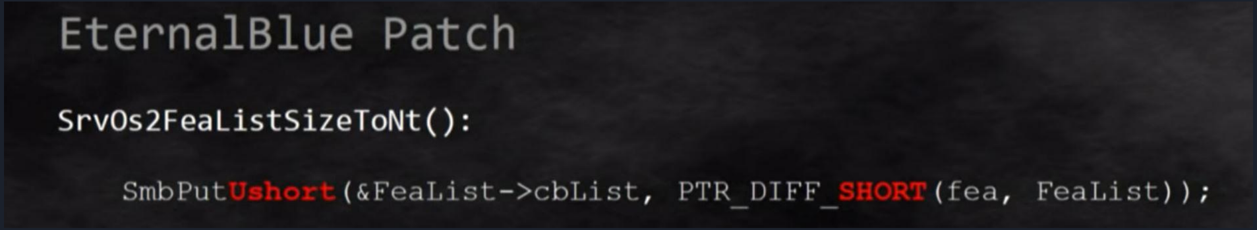
3 SMB Bugs for OS Manipulation in Eternal Blue

- Bug 1: Create a buffer overflow in memory.
- Bug 2: Parsing Bug. Overlay in memory
- Bug 3: Grooming

(Images from Check Point Research 2019)

Key Idea: Avoiding the threat of EternalBlue

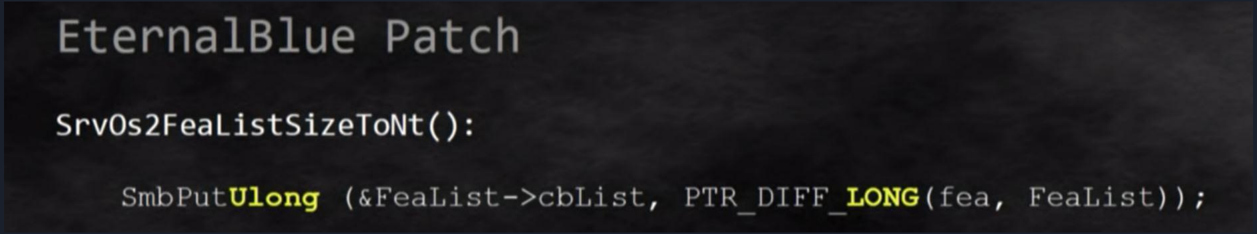
- Microsoft SMB Patch was issued in 2017 under MS17-010
- Closes possibility of Buffer OverFlow
- Unsigned Short vs Unsigned Long values were the root of all evil
- Over 1 million computers still left unpatched



EternalBlue Patch

```
SrvOs2FeaListSizeToNt():

    SmbPutUshort(&FeaList->cbList, PTR_DIFF_SHORT(fea, FeaList));
```



EternalBlue Patch

```
SrvOs2FeaListSizeToNt():

    SmbPutUlong (&FeaList->cbList, PTR_DIFF_LONG(fea, FeaList));
```

What We Learned

- Deeper knowledge of the following OS Topics:
    - Files
    - I/O
    - Virtual Memory/Memory Management
    - Security
- How an Exploit works
    - How it infects
    - How to stop it
    - How malware uses EternalBlue
- Future work
    - Examine descendants
    - Highlight differences to increase security