**A Cyber Attack on The Crazy Lab**

1. Checking the OS version using **winver** command.
2. The Crazy Researcher is launching a console app, which runs a driver:

**allocator.exe**

1. CR is creating a new file “secret\_formula.txt” and opening it in an exclusive mode:

**f\_open secret\_formula.txt**

1. CR is saving a secret formula into the file:

**f\_write phoenix feather + holly +AAA battery**

1. CR is checking the written data:

**f\_read**

1. It is a five o’clock, so the CR is having a tea break.
2. At this time an attacker is trying to steal the formula.  
   An attacker is launching its console app:

**attacker.exe**

1. An attacker is trying to open this file as usual:

**f\_open secret\_formula.txt**

1. He fails to open a file.
2. He decides to access the file illegally and he is coping the pointer to the FILE\_OBJECT of the opened file.
3. An attacker is hijacking the NTFS data structures by using the following:

**f\_open\_by\_hijacking\_fileobj\_internals FILE\_OBJECT**

1. An attacker is trying to read the secret-formula.txt

**f\_read**

1. An attacker is trying to overwrite the secret-formula.txt using “sandalwood+sharks teeth”

**f\_write sandalwood + sharks teeth**

1. Now, the CR’s break is over, and he decides to check the saved formula

**f\_read**

1. The secret has been stolen and damaged.
2. But let’s wait for PatchGuard reaction, which is designed to prevent such illegal memory modifications. Usually PatchGuard crashes the OS in less than one hour. We’ve been waiting for 8 hours it is quite a long time but nothing has happened. The OS has not been crushed. It means that PatchGuard fails and the OS is unable to guarantee an exclusive access. The system is not protected. Our lab is under attack.

**MemoryRanger Prevents the Attack on The Crazy Lab**

1. MemoryRanger console has been launched and it loads a driver and a hypervisor to protect OS.

**memory\_ranger.exe**

1. The Crazy Researcher (CR) is launching a console app, which runs a driver

**allocator.exe**

1. CR is creating a new file “secret\_formula.txt” and opening it in an exclusive mode to save a secret formula:

**f\_open secret\_formula.txt**

1. CR is saving a secret formula:

**f\_write phoenix feather + holly +AAA battery**

1. CR is checking the written data:

**f\_read**

1. It is a five o’clock, so the CR is having a tea break.
2. At this time the attacker is trying to steal the formula.  
   The attacker is launching its console app:

**attacker.exe**

1. The attacker is trying to open this file as usual:

**f\_open secret\_formula.txt**

1. He fails to open a file, and and he is coping the pointer to the FILE\_OBJECT of the opened file.
2. The attacker is hijacking the NTFS data structures by using the following:

**f\_open\_by\_hijacking\_fileobj\_internals FILE\_OBJECT**

1. The attacker is trying to read the secret

**f\_read**

1. He fails to gain an access to the secret data. Anyway, he trying to overwrite the data.

**f\_write sandalwood + sharks teeth**

1. Now, the PR’s break is over, and he decides to check the saved formula

**f\_read**

1. The secret is protected. It has not been stolen and damaged. The OS is protected!
2. MemoryRanger prevents the kernel-mode attack.