UC.yber; Meeting 22

Cuckoo Sandbox Demo

Announcements

- **August 16th** We will be visiting **UCRI**
- October **27/28th ACM** programming challenge
- We are now integrated into **ESOC** (Engineering Student Org. Council)
- Will be participating in **Philanthropy Week** with Chem Club
- Society of Black Engineers wants us to have a booth for **STEM Fest**
- Attended **AngelHack** and built **Cuckoo**

Cuckoo

- Recently Updated to V2.0.3
- No documentation for it so we made it
- Malware Sandboxing system
- Connects very well with a bunch of other open source projects.

Yara

IN A NUTSHELL:

- Helps identify and classify malware.

How:

- Places malware into families based on textual or binary patterns.
- “Config” files are set to your preference. We will use open source resources for this.

https://virustotal.github.io/yara/

Yara Example:

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        thread_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

https://virustotal.github.io/yara/

Volatility

IN A NUTSHELL:

- “extraction of digital artifacts from volatile memory (RAM) samples”

TCPdump

IN A NUTSHELL:

- Tool used to print and save packets over a network.

MITMproxy

IN A NUTSHELL:

- An interactive console program that allows traffic flows to be intercepted, inspected, modified and replayed

Distorm

IN A NUTSHELL:

- Converts AMD assembly instruction from static text to binary for analysis