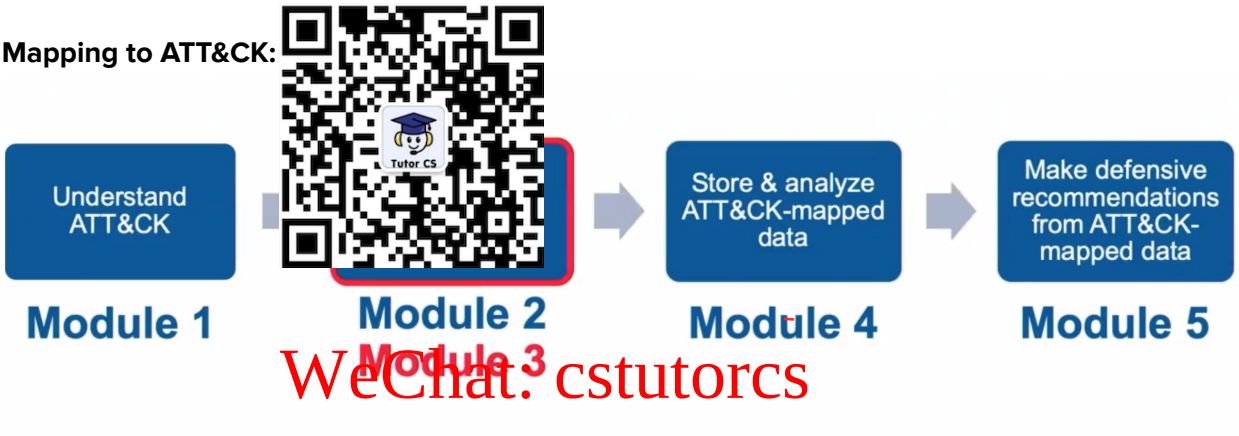
COMP6448 - Week 5

Security Engineering Masterclass

Mapping to ATT&CK:



1. Understand attack
   - Watch ATT&CK presentation like Sp4rkcon
   - Skim the technique list
   - Read the tactic descriptions
   - Read the Philosphy doc in Discord
2. Find behaviour
   - Think about verbs. What does the advisory do once they get in and how did they get in. As opposed to looking at IP addresses etc
   - Things that aren't as useful:
     - Static malware analysis
     - Infrastructure registration info
     - industry/victim targeting
   - E.g.

The most interesting PDB string is the "`4113.pdb`," which appears to reference CVE-2014-4113. This CVE is a local kernel vulnerability that, with successful exploitation, would give any user SYSTEM access on the machine.

The malware component, `test.exe`, uses the Windows command "`cmd.exe" /C whoami`" to verify it is running with the elevated privileges of "System" and creates persistence by creating the following scheduled task:

```
schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON     /ru "System"
```

When executed, the malware first establishes a SOCKS5 connection to 192.157.198.103 using TCP port 1913. The malware sends the SOCKS5 connection request "`05 01 00`" and verifies the server response starts with "`05 00`".

3. Research behaviour
   - If you haven't seen this behaviour before, go research it.
   - There's too many types of adversary behaviours to know them all! So it's ok to spend time to research.
   - E.g. researching a bit about SOCKS5. What is port1913 used for?

4. Translate the behaviour into a tactic

- What is the adversary trying to accomplish.
- There are 14 of 12 options:
  - **Only 12 options:**
    - Initial Access
    - Ex
    - Pe
    - Pri
    - De
    - Cr
    - Discovery
    - Lateral Movement
    - Collection
    - Command and Control
    - Exfiltration
    - Impact

- E.g.
  - **"When executed, the malware first establishes a SOCKS5 connection to 192.157.198.103 using TCP port 1913. … Once the connection to the server is established, the malware expects a message containing at least three bytes from the server. These first three bytes are the command identifier. The following commands are supported by the malware … "**
    - A connection in order to command the malware to do something
      → **Command and Control**

5. Figure out what technique applies to that behaviour.
   - The toughest because not every behaviour is necessarily a technique.
   - Look at the list of techniques for the identified Tactic.
   - Search attack.mitre.org.
   - E.g.

"the malware first establishes a SOCKS5 connection"

SOCKS

Techniques

Term found on page
Standard Non-Application Layer Protocol (ID: T1095)
Connection Proxy (ID: T1090)

Standard Non-Application Layer Protocol

Use of a standard non-application layer protocol for communication between host and C2 server or among infected hosts within a network. The list of possible protocols is extensive. [1] Specific examples include use of network layer protocols, such as the Internet Control Message Protocol (ICMP), transport layer protocols, such as the User Datagram Protocol (UDP), session layer protocols, such as Socket Secure (SOCKS), as well as redirected/tunneled protocols, such as Serial over LAN (SOL).

BUBBLEWRAP can communicate using SOCKS.[4]

6. Compare your results to other analysts

- Key sources
  - Finished reporting
  - Raw data

Mapping to ATT&CK from Raw Data:

- Could include shell commands, malware, logs, packets etc.

1. Understand attack
   - Trivial

2. Find behaviour

- E.g. Each command can correspond to a behaviour

3. Research behaviour
   - Try searching for commands in mitre.
   - Sometimes we can only make educated guesses but without enough context, we can't be certain.
4. Translate the behaviour into a tactic
5. Concurrent techniques
   a. Think of how something is happening, not just what.
   b. Some are specific (e.g. Netsch Helper DLL) and some are broad (e.g. scripting)
6. Figure out what technique applies to that behaviour.
7. Compare your results to other analysts

Pros and cons of mapping from different sources: