

COMP 6448 Week 5

程序代写代做 CS编程辅导

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 Philosophy doc in Discord

2. Find behaviour

- Think about verbs: What does the adversary 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.

QQ: 749389476
Email: tutorcs@163.com
<https://tutorcs.com>

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 12 options:

Only 12 options:

Initial Access

Exfiltration

Persistence

Privilege Escalation

Defense Evasion

Creation of Persistence

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 connector in order to command the malware to do something
→ Command and Control

WeChat: cstutors

Assignment Project Exam Help

- 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. QQ: 749389476

“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 <u>Socket Secure (SOCKS)</u> , as well as redirected/tunneled protocols, such as Serial over LAN (SOL).
---	---

BUBBLEWRAP can communicate using SOCKS.^[4]

- 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.

- Understand attack

- Trivial

- Find behaviour

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

程序代写代做 CS编程辅导

```

ipconfig /a
sc.exe \\ln334656-pc create
.\recycler.exe -fCzq5yKw C:\$Recycle.Bin\old
C:\$Recycle
ave network.vsdx
Commands captured: 10.2.13.44:32123 interactively via cmd.exe
128.29.32.4:32123
Flows from malware
  
```

10.2.13.44:32123 128.29.32.4:32123

Flows from malware

HKLM\Software\Microsoft\Windows\CurrentVersion\Run
WeChat: cstutorcs
New reg keys during an incident

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
- Email: tutorcs@163.com**

Pros and cons of mapping from different sources:

Pros/cons of Mapping from the Two Different Sources

Step	Raw	Finished
Find the behavior	Nearly everything may be a behavior (not all ATT&CK)	May be buried amongst prose, IOCs, etc
Research the behavior	May need to look at multiple sources, data types. May also be a known procedure	May have more info/context, may also have lost detail in writing
Translate the behavior into a tactic	Have to map to adversary intent, need domain knowledge/expertise	Often intent has been postulated by report author
Figure out what technique applies to the behavior	May have a procedure that maps straight to technique, or may require deep understanding to understand how accomplished	May be as simple as a text match to description/procedure, or may be too vague to tell
Compare your results to other analysts	May need multiple analysts to cover all data sources	More likely in a form where other analysts needed for coverage/hedge against bias

MITRE