C3iHub
भारतीय प्रौद्योगिकी संस्थान कानपुर
Indian Institute of Technology Kanpur

Module 3.2
MITRE ATT&CK:
Mapping to ATT&CK from Finished Cyber Incident Reports

Sandeep K. Shukla
IIT Kanpur

Acknowledgement

- This material is based on the ATT&CK material created by Katie Nickels and Adam Pennington (MITRE Corporation)

Outline

- What is ATT&CK? (Module 3.1)
- Mapping to ATT&CK from Finished Cyber Incident Reports (Module 3.2)
- Mapping to ATT&CK from Raw Data from Cyber Incident (Module 3.2)
- ATT&CK Navigator (Module 3.3)
- From ATT&CK Mapping to Defence Recommendation (Module 3.4)

Cyber Threat Intelligence (CTI)

- To defend an organizational cyber infrastructure, you need to know
  - Who might be attacking you and their motivations
  - Frequency and volume of the attacks
  - The various attack surfaces they tend to exploit
  - The tactics used by different groups of attackers
  - The techniques they use to implement their tactics
  - The procedures they use to make the technique work
  - What kind of malware they use
  - Their Command-and-Control Infrastructure
  - Indicators of compromise
  - Artifacts – e.g. IP addresses, URLs, Malware, credentials, files. Certificates etc.

ATT&CK and CTI

- Knowledge of Adversary behaviour is helpful in planning defence
- Structuring CTI with ATT&CT TTPs help us:
  - Compare behaviours
    - Between threat groups
    - Same group over time
    - Groups to defences
  - Communicate in a common language for sharing CTI across organizations

Communicating to defenders

  - APT 18 used legitimate credentials to log into external remote services
  - APT 29 used compromised identities to access networks via VPNs and Citrix
  - APT 41 compromised an online billing/payment service using VPN access between a 3rd party service provider and the targeted payment service
- All are using T1133 (External Remote Services) technique

Mapping from Finished Reports to ATT &CK

CTI and ATT&CK

- To a lot of defenders CTI = IOC (Indicators of Compromise)
- Threat Intelligence is often shared as STIX format
- STIX = Structured Threat Information Expression
- To map to ATT&CK you need to consider a threat or attack in terms of behaviours of the attacker
- The tactics are the self-contained goals set by the attacker to make progress
- Subsequent tactics build on successes of previous tactics
- There are 14 tactics, and over 300 techniques

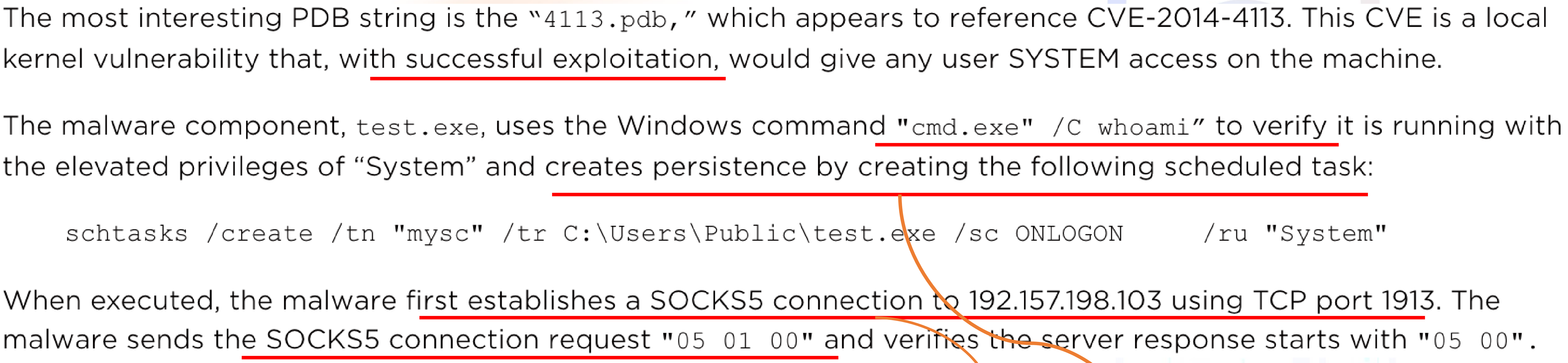
Mapping Adversary Behaviour to ATT&CK

- Understand ATT &CK
  - Find the adversary behaviour rather than IOCs
  - Do your own research on the behaviour
  - Translate the behaviour into one or more tactics
  - Figure out the technique(s) applied to play the tactics
  - Compare your mapping to other analysts
- Sources of Adversary Behaviour Data
  - Finished Reports from Threat Intelligence Agencies
  - Raw Data from Forensic Analysis

Finding the adversary behaviour

- Focus on the verbs
  - What did the adversary do on the systems it compromised
  - How did it get its initial access
  - How did it find the vulnerability
  - How did it create persistence in the system
  - Did it attempt to become root user
  - Did it compromise multiple devices via vulnerable protocols
  - Did it exfiltrate any data
  - Did it change any settings
  - Did it use any malware
  - What kind of information did they look for
  - What kind of systems or information it attempted or succeeded to access

Finding behaviour of adversary



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"`.

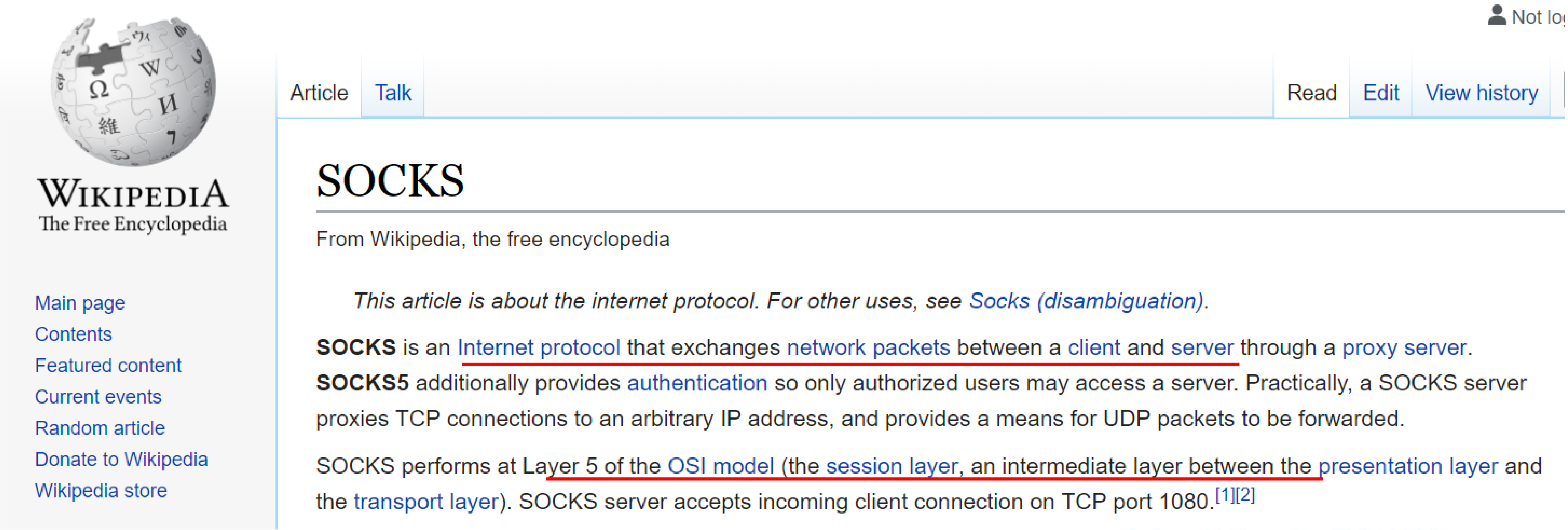
Operation Double Tap | Mandiant

Tactic and Technique

Research the behaviour

- If you are not familiar with the behaviour described
  - Research which tactics and techniques may have been used in the behaviour
  - Discuss with the red-team members in your organization
  - Refer to the attack.mitre.org website
- Give enough time to the research
- Understanding the behaviour will help with the next steps in mapping to the correct tactics/techniques/procedures

Research the behaviour



SOCKS

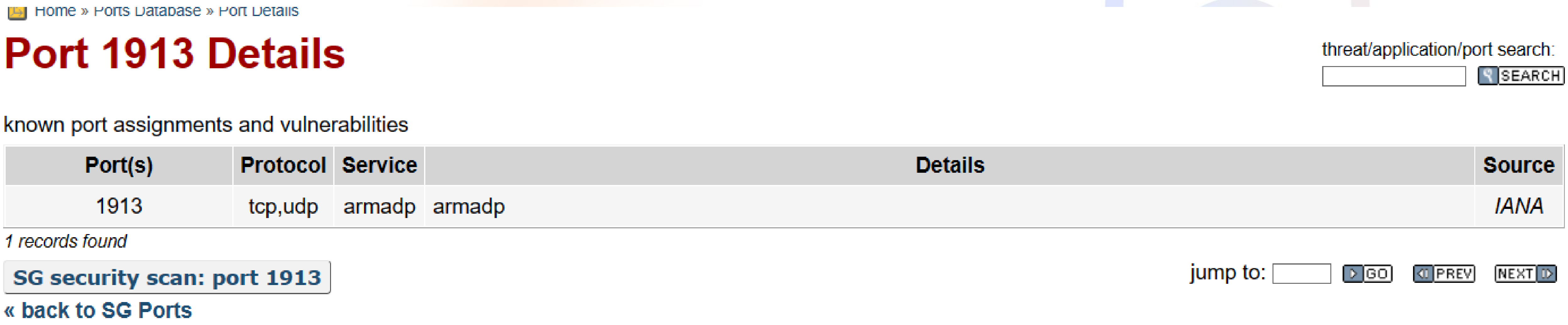
From Wikipedia, the free encyclopedia

This article is about the internet protocol. For other uses, see Socks (disambiguation).

SOCKS is an Internet protocol that exchanges network packets between a client and server through a proxy server. **SOCKS5** additionally provides authentication so only authorized users may access a server. Practically, a SOCKS server proxies TCP connections to an arbitrary IP address, and provides a means for UDP packets to be forwarded.

SOCKS performs at Layer 5 of the OSI model (the session layer, an intermediate layer between the presentation layer and the transport layer). SOCKS server accepts incoming client connection on TCP port 1080.[1][2]

Research the behaviour



Home » Ports Database » Port Details

Port 1913 Details

threat/application/port search:

SEARCH

known port assignments and vulnerabilities

Port(s)	Protocol	Service	Details	Source
1913	tcp,udp	armadp	armadp	*IANA*

1 records found

SG security scan: port 1913

jump to: GO PREV NEXT

« back to SG Ports

Translate the behaviour into a tactic

- Try to understand what the adversary might be trying to accomplish (subgoal)
- May require domain expertise
  - For example, the port number may indicate the protocol being used
- To map to a tactic, you have only 14 choices

reconnaissance, weaponization (preparation), initial access, execution, persistence, privilege escalation, defence evasion, credential access, discovery, lateral movement, collection, command & control, exfiltration, impact

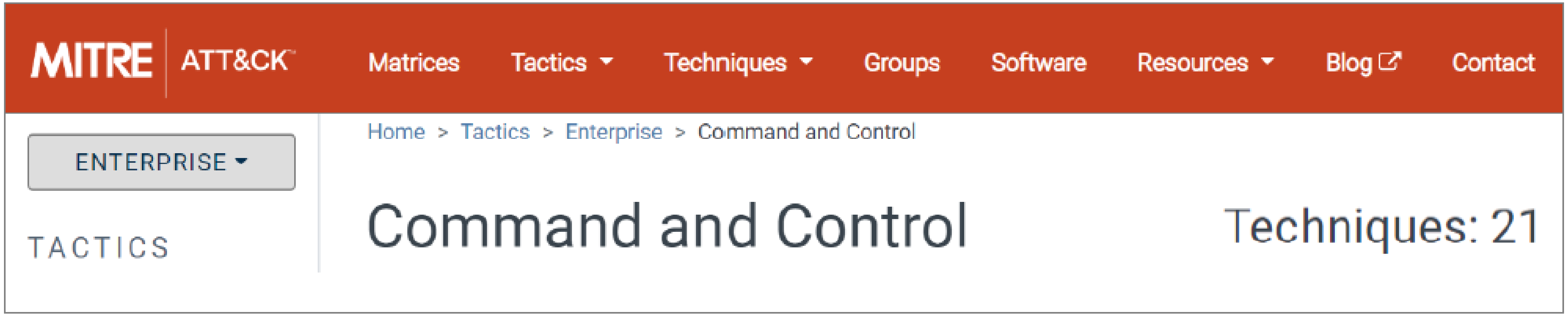
Translate the behaviour into a tactic

- "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

Figure out what techniques apply

- This is harder than finding tactics as there are over 300 choices
- Look at the techniques identified in the ATTACK matrix for identified tactics
- Search the attack.mitre.org website for technique details and figure out matches with the behaviour
- Some behaviours may not have an existing technique
  - You may consider reporting to the attack.mitre.org

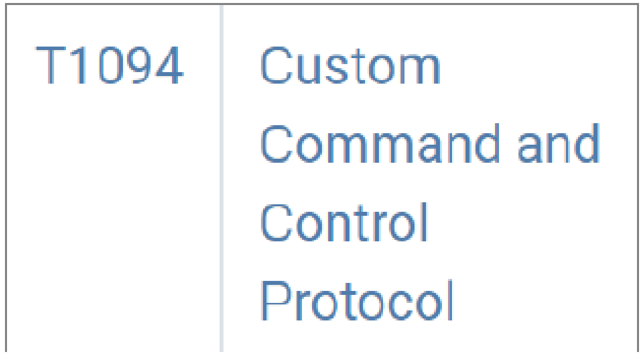
Figure out what techniques apply



Home > Tactics > Enterprise > Command and Control

Command and Control

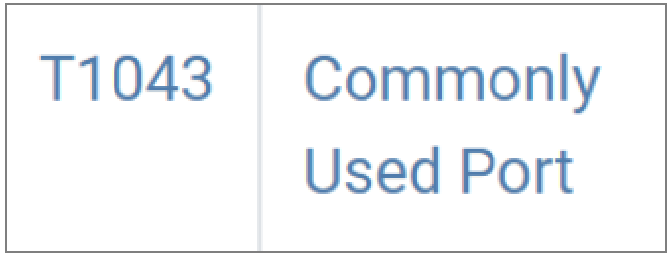
Techniques: 21



T1094	Custom Command and Control Protocol

Protocol vs. Port

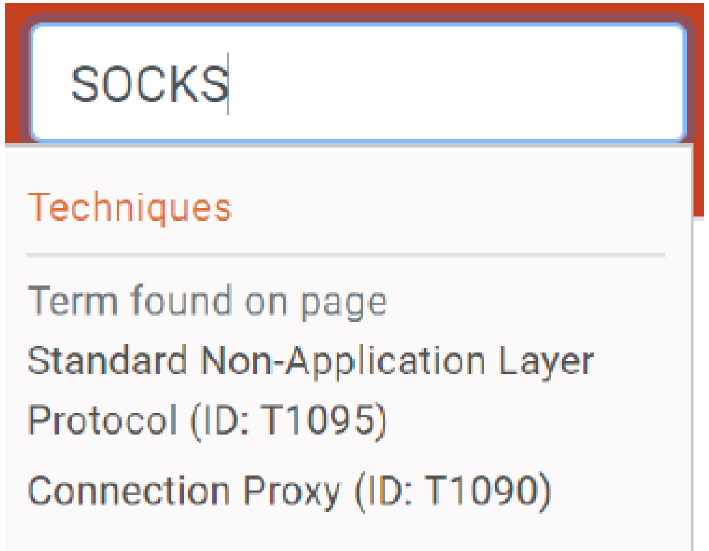
→ 2 techniques?



T1043	Commonly Used Port

Figure out what techniques apply

“the malware first establishes a SOCKS5 connection”



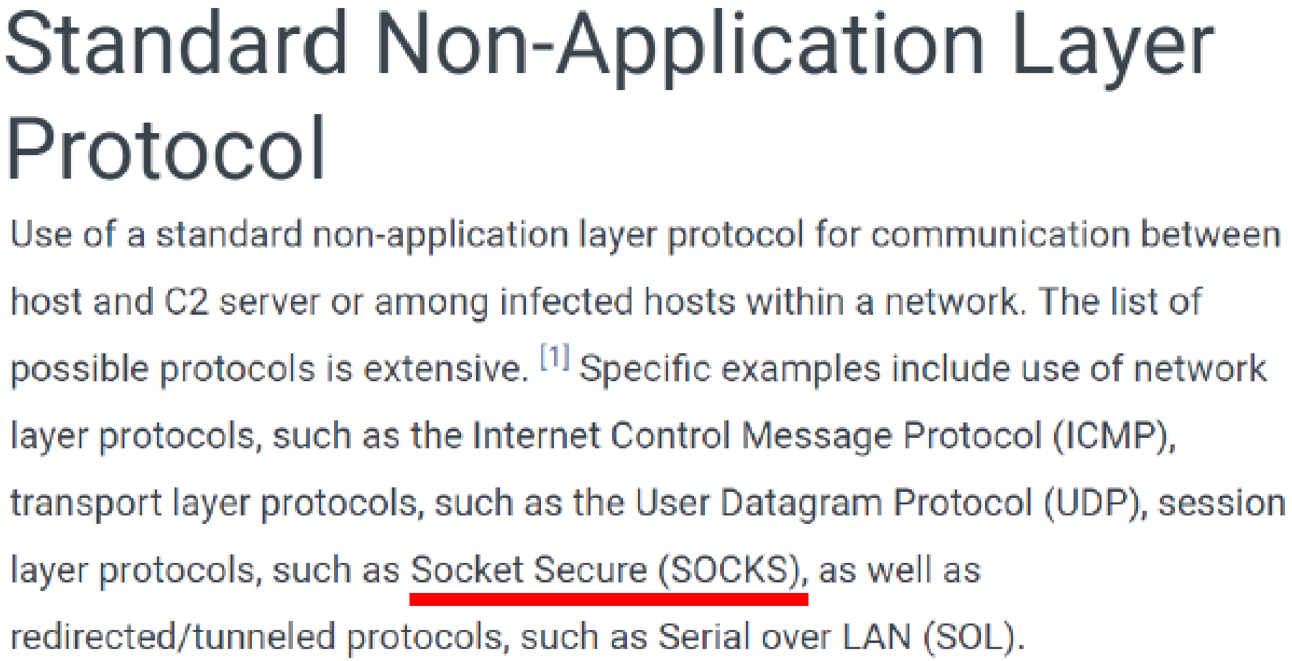
SOCKS

Techniques

Term found on page

Standard Non-Application Layer Protocol (ID: T1095)

Connection Proxy (ID: T1090)

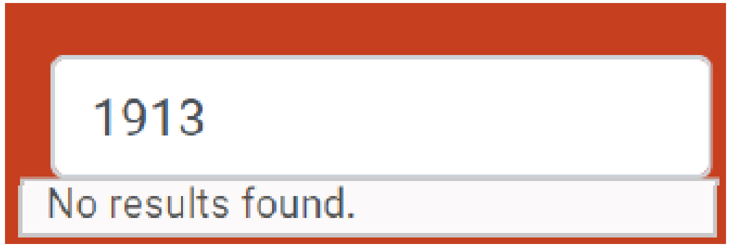


Standard Non-Application Layer Protocol

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).

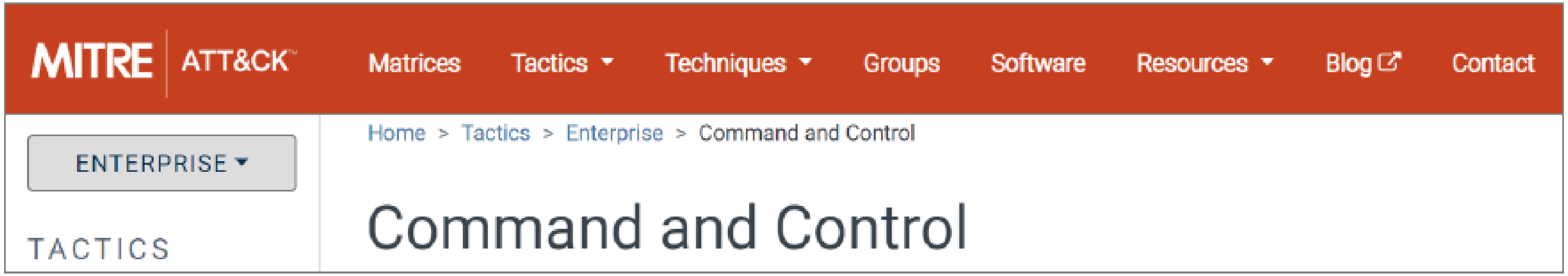
Figure out what techniques apply

"establishes a SOCKS5 connection to 192.157.198.103 using TCP port 1913"

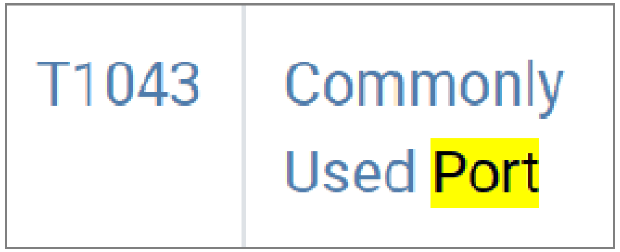


1913

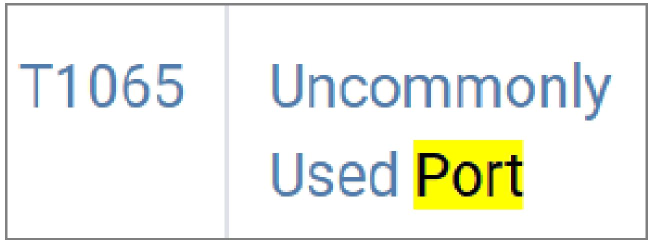
No results found.



Command and Control

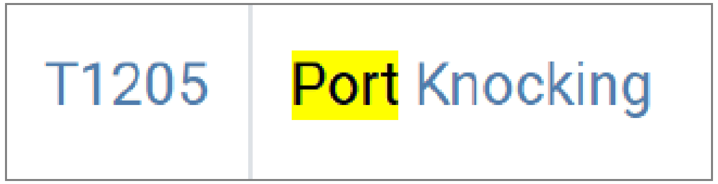


T1043	Commonly Used Port



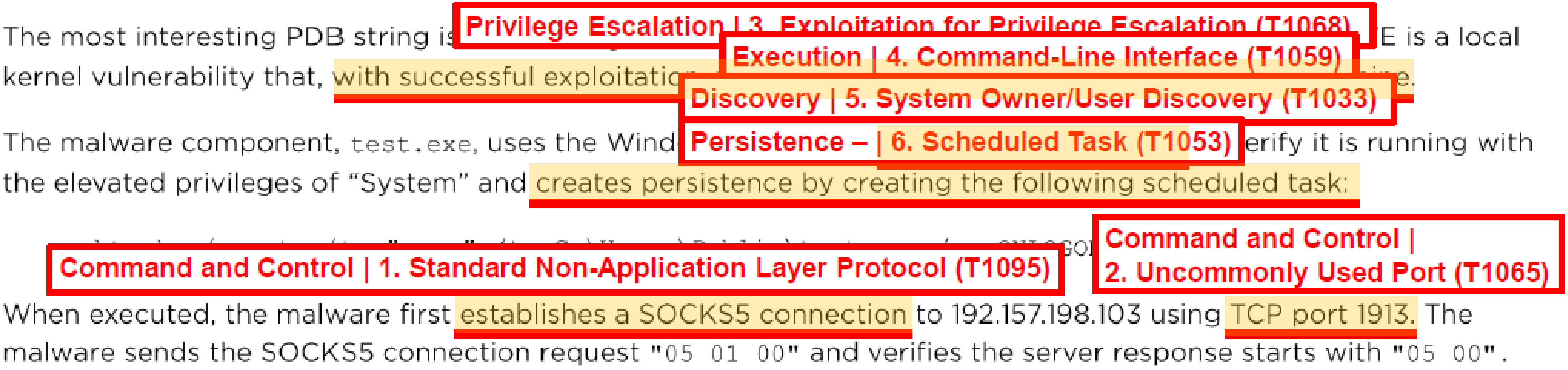
T1065	Uncommonly Used Port

"CTRL+ F" FTW



T1205	Port Knocking

Repeat the process



The most interesting PDB string is **Privilege Escalation | 3. Exploitation for Privilege Escalation (T1068)** E is a local kernel vulnerability that, with successful exploitatio **Execution | 4. Command-Line Interface (T1059)** **Discovery | 5. System Owner/User Discovery (T1033)** e.

The malware component, `test.exe`, uses the Wind **Persistence – | 6. Scheduled Task (T1053)** erify it is running with the elevated privileges of "System" and creates persistence by creating the following scheduled task:

```
[illegible] GON
```

Command and Control | 1. Standard Non-Application Layer Protocol (T1095)

Command and Control |
2. Uncommonly Used Port (T1065)

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"`.

Exercise: Cybereason Cobalt Kitty Report

- **Analyze a threat report to find the Enterprise ATT&CK techniques**
  - 22 highlighted techniques in the Cybereason Cobalt Kitty report
- **Choose a PDF from attack.mitre.org/training/cti under Exercise 2**
  - Choose your own adventure: start with “highlights only” or “tactic hints”
- **Use the PDF or a text document/piece of paper to record your results**
- **Write down the ATT&CK tactic and technique you think applies to each highlight**
- **Tips:**
  - Do keyword searches of the website: https://attack.mitre.org
  - Remember that you don’t have to be perfect
  - Use this as a chance to dive into ATT&CK

Compare with the results of other analysts

- **Compare your results to other analysts**
- **Helps hedge against analyst biases**
  - More likely to identify techniques you’ve previously identified

Analyst 1

- Command-Line Interface (T1059)
- System Owner/User Discovery (T1033)
- Scheduled Task (T1053)
- Standard Non-Application Layer Protocol (T1095)
- Uncommonly Used Port (T1065)
- Multi-Stage Channels (T1104)

Analyst 2

- Exploitation for Privilege Escalation (T1068)
- Command-Line Interface (T1059)
- Scheduled Task (T1053)
- Custom Command and Control Protocol (T1094)
- Uncommonly Used Port (T1065)

Discuss why it’s different

https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

Cybereason Cobalt Kitty Report

1. **Two types of payloads were found in the spear-phishing emails … link to a malicious site**
   - Initial Access - Spearphishing Link (T1192)
2. **Two types of payloads were found in the spear-phishing emails … Word documents**
   - Initial Access - Spearphishing Attachment (T1193)
3. **Two types of payloads were found in the spear-phishing emails … Word documents with malicious macros**
   - Defense Evasion/Execution – Scripting (T1064)
4. **Two types of payloads were found in the spear-phishing emails**
   - Execution – User Execution (T1204)

- https://cybr.ly/cobaltkitty

Cybereason Cobalt Kitty Report

5.

cmd.exe
Parent process

   – Execution - Command-Line Interface (T1059)

6. **The two scheduled tasks are created on infected Windows**

   – Execution/Persistence - Scheduled Task (T1053)

7.schtasks /create /sc MINUTE /tn "Windows Error Reporting" /tr "mshta.exe about:'<script language=\"vbscript\“…

   – Execution/Defense Evasion - Mshta (T1170)

8. **That downloads and executes an additional payload from the same server**

   – Command and Control - Remote File Copy (T1105)

https://cybr.ly/cobaltkitty

Cybereason Cobalt Kitty Report

9.

powershell.exe

Parent process

   – Execution - PowerShell (T1086)

10. **it will pass an <span style="color:red">obfuscated and XOR'ed</span> PowerShell payload to cmd.exe**

   – Defense Evasion - Obfuscated Files or Information (T1027)

11. **The attackers used trivial but effective persistence techniques .. Those techniques consist of: Windows Registry Autorun**

   – Persistence - Registry Run Keys / Startup Folder (T1060)

12. **the attackers used NTFS Alternate Data Stream to hide their payloads**

   – Defense Evasion - NTFS File Attributes (T1096)

https://cybr.ly/cobaltkitty

Cybereason Cobalt Kitty Report

13 & 14. The attackers created and/or modified Windows Services

- Persistence – New Service (T1050)
- Persistence – Modify Existing Service (T1031)

15 & 16. The attackers used a malicious Outlook backdoor macro … edited a specific registry value to create persistence

- Persistence – Office Application Startup (T1137)
- Defense Evasion – Modify Registry (T1112)

17. The attackers used different techniques and protocols to communicate with the C&C servers … HTTP

- Command and Control - Standard Application Layer Protocol (T1071)

https://cybr.ly/cobaltkitty

Cybereason Cobalt Kitty Report

18. :80 *(in traffic from compromised machine to C&C server)*
   - Command and Control - Commonly Used Port (T1043)

19 & 20. **The attackers downloaded COM scriptlets using regsvr32.exe**
   - Command and Control - Remote File Copy (T1105)
   - Execution - Regsvr32 (T1117)

21.**binary was renamed "kb-10233.exe", masquerading as a Windows update**
   - Defense Evasion - Masquerading (T1036)

22. **network scanning against entire ranges…looking for open ports…**
   - Discovery - Network Service Scanning (T1046)

https://cybr.ly/cobaltkitty

More Practice

- If you’d like more practice mapping finished reporting to ATT&CK, work through the FireEye APT39 report in the same manner. The PDF is available at attack.mitre.org/training/cti under Exercise 2. (No tactic hints option this time!)
- Answers are provided in a separate PDF.

C3iHub
भारतीय प्रौद्योगिकी संस्थान कानपुर
Indian Institute of Technology Kanpur

भारतीय प्रौद्योगिकी संस्थान कानपुर
INDIAN INSTITUTE OF TECHNOLOGY KANPUR