Attack Scenario

I. INDRIK SPIDER

INDRIK SPIDER is a sophisticated eCrime group that has been operating Dridex since June 2014. In 2015 and 2016, Dridex was one of the most prolific eCrime banking trojans on the market and, since 2014, those efforts are thought to have netted INDRIK SPIDER millions of dollars in criminal profits

Scenarios

1. **Drive by Compromise–JavaScript Redirection to Download Fake Update.**
   - Description
     - Setting up a simulated third-party website which is frequently accessed by the member of victim's organization. The student needs design a set of JavaScript based malicious code with minimal edition of the controllable web page to profiling victim's browser and redirect them to download fake update binary.
   - Requirement
     - Assuming the fake update binary is for Chrome update. It must contain:
       - Reverse shell binary that connect to C&C server which designed by student.
       - The mechanism above must be able to be executed once the fake update binary clicked.
       - (Bonus) Bypass windows defender
       - (Bonus) Bypass windows "Untrusted Binary Warning".
     - Design a set of malicious JavaScript code with following functionalities.
       - Profiling victim's browser.
         - Browser's type, eg. Chrome, Edge, Firefox…
         - Browser's version
         - Browser's plugins and the version of plugin
         - Browser's operating system
       - Redirect victim to download fake update binary.
   - Keyword
     - Reverse Shell

        - JavaScript for profiling browser
        - JavaScript redirection

2. **Drive by Compromise–HTTP based Redirection to Download Fake Update.**
    - Description
        - Setting up a simulated third-party website which is frequently accessed by the member of victim's organization. The student needs design a set of JavaScript based malicious code with as less as possible edition of the controllable web page to profile victim's browser and use HTTP based redirection to redirect them to download fake update binary.
    - Requirement
        - Assuming the fake update binary is for Chrome update. It must contain:
            - Reverse shell binary that connect to C&C server which designed by student.
            - The mechanism above must be able to be executed once the fake update binary clicked.
            - (Bonus) Bypass windows defender
            - (Bonus) Bypass windows "Untrusted Binary Warning".
        - Design a set of malicious JavaScript code with following functionalities:
            - Profiling victim's browser.
                - Browser's type, eg. Chrome, Edge, Firefox…
                - Browser's version
                - Browser's plugins and the version of plugin
                - Browser's operating system
        - Using HTTP based redirection to redirect victim to download fake update binary.
    - Keyword
        - Reverse Shell
        - JavaScript for profiling browser
        - HTTP redirection
3. **Spearphishing–Self-Build Phishing website with Profiling Victim's Browser.**
    - Description
        - The student needs deploy a phishing website using sites.google.com, which is provided by google.

- Requirement
  - The website needs to:
    - Look like legal website. (Public html, CSS template are allowed)
    - Profile victim's browser.
      - Browser's type, eg. Chrome, Edge, Firefox…
      - Browser's version
      - Browser's plugins and the version of plugin
      - Browser's operating system
    - Assuming there are only two kinds of browser will browse the website: Chrome and Firefox. According to the browser agent, redirect to download the fake update binary hosted on attackers google drive. For instance, if the browser is chrome, the fake update binary should be chrome update.
- Keyword
  - JavaScript for profiling browser

4. Supply Chain Compromise–Infected Installer of Supply Chain Attack

- Description
  - Assume that victims' organization will widely use Adobe Acrobat PDF Reader. In this case, the student needs merge a backdoor or Trojan into the official installer of Adobe Acrobat PDF Reader.
- Requirement
  - The merged executable(.exe) need to have the following functionalities:
    - Normal Adobe Acrobat PDF Reader installation functionality
    - Reverse shell functionality.
    - (Bonus)Bypass windows defender.
    - (Bonus)Don't let windows show untrusted executable warning.
- Keyword
  - Reverse shell
  - Repacking (For merging adobe and reverse shell program)

5. Spearphishing–Phishing Email with Malicious Macro Enabled Document

- Description
  - The student needs to craft a macro enabled Microsoft document as phishing attachment which can download malware.
- Requirement

        - A macro enabled Microsoft document with the macro that:
            - Download a downloader from url and store it to %temp% folder to evade defense.
            - Execute the downloader.
        - The downloader will download another malware (In this case use a text file for proof of concept.).
    - Keyword
        - VBA (Visual Basic for Applications)
        - Macro

6. **Brute Force–RDP Brute Force Attack**
    - Description
        - Given a windows virtual machine, which is the host of the main target for student to compromise. This machine will host a remote desktop server which allow legal user (including admin) to login to desktop GUI remotely. However, the legal user is using weak <username> and <password>. The student needs to guess username and password to login to the machine.
    - Requirement
        - Using rainbow table, weak password list or simply try every possible solution to break into the system.
    - Keyword
        - Rainbow table
        - Weak password list
7. **Credentials from Password Stores–Dump Browser Credential using Exploit tools**
    - Description
        - The student can use SSH or RDP to access the remote machine. The student needs to figure other way to dump the credential from browsers. The designed victims' host has following application:
            - Chrome
            - Firefox
    - Requirement
        - Dump password and/or other information of the victim's browser using open source tools (such as LaZagne, Empire etc..).
    - Keyword
        - Credential dumping
8. **BIT (Background Intelligent Transfer Service) Jobs–Background Intelligent Transfer Service**

- Description
  - The student needs to craft a malware (either .exe or macro document) to gain persistent access to victims' host using Background Intelligent Transfer Service. This mechanism is widely used by windows update to download image, even sharing the downloaded image.
- Requirement
  - Craft a malware which will:
    - Add a persistent job with BIT Jobs.
    - Keep updating(downloading) malware from remote server.
    - Execute the malware when download finished.
- Keyword
  - VBA (if using macro document malware).
  - BIT

II. OilRig

OilRig is a suspected Iranian threat group that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its operations within the Middle East.

Scenarios

9. Spearphishing–Phishing attachment & Download 2nd stage payload & Persistent with schedule task

- Description
  - The student needs to make a phishing email with a malicious attachment which is macro enabled **word** document.
- Requirement
  - The macro needs to have these functionalities:
    - Download a PowerShell script from internet (Google Drive, Dropbox or other sources).
      # The PowerShell script needs to create a reverse shell to your computer.
    - Make a schedule task to launch the PowerShell script every 10 minutes.
- Keyword

    - Reverse shell
    - PowerShell script
    - VBA (Visual Basic for Application)
    - Schedule task

10. **Spearphishing–Phishing attachment & Extract file content from Excel & Persistent with schedule task**
    - Description
        - The student needs to make a phishing email with a malicious attachment which is macro enabled **excel** document
    - Requirement
        - The macro needs to have these functionalities:
            - Extract PowerShell script from worksheet and write to a ".ps1" file.
              # The PowerShell script needs to create a reverse shell to your computer.
            - Make a schedule task to launch the PowerShell script every 10 minutes.
    - Keyword
        - Reverse shell
        - PowerShell script
        - VBA (Visual Basic for Application)
        - Schedule task
11. **C&C through Web Protocols–Command & Control through HTTP & Collect information**
    - Description
        - The student needs to survey an open source tools to establish C&C communication over HTTP. Then establish C&C communication with the victim host and collect system and network information.
    - Requirement
        - Collect information based on the following discovery techniques:
            - System information Discovery
            - System Network Configuration Discovery
            - System Network Connection Discovery

          # See MITRE ATT&CK techniques description
    - Keyword
        - HTTP Command and Control
12. **Credentials from Password Stores–Collect credentials using an open source tool called Mimikatz**

- Description
  - The student needs to first establish connection with the victim host by SSH/RDP or other C&C tools. After you get control of the victim host, you need to use Mimikatz to perform credential dumping to steal credentials.
- Requirement
  - Use Mimikatz to steal credentials like password.
- Keyword
  - Mimikatz
  - Credential dumping

13. Credentials from Password Stores–Collect credentials using an open source tool called LaZagne

- Description
  - The student needs to first establish connection with the victim host by SSH/RDP or other C&C tools. After you get control of the victim host, you need to use LaZagne to perform credential dumping to steal credentials.
- Requirement
  - Use LaZagne to steal credentials like password.
- Keyword
  - LaZagne
  - Credential dumping

14. Exfiltration Over Alternative Protocol–Discovery and Exfiltration through DNS tunneling

- Description
  - The student needs to first establish connection with the victim host by SSH/RDP or other C&C tools. After you get control of the victim host, you need to perform multiple system and network discovery and store the result into a file for each discovery technique then exfiltrate those file content to attacker's server by embedding the file content in subdomain of attacker's domain.
- Requirement
  - Collect information based on the following discovery techniques:
    - System information Discovery
    - System Network Configuration Discovery
    - System Network Connection Discovery

    # See MITRE ATT&CK techniques description
  - Store the result into a file.

    - Read the file and embedding the file content in subdomain of attacker's domain and send the query.
- Keyword
    - DNS tunneling

15. Exfiltration Over Alternative Protocol–Discovery and Exfiltration through HTTP Post

- Description
    - The student needs to first establish connection with the victim host by SSH/RDP or other C&C tools. After you get control of the victim host, you need to perform multiple local account discovery and store the result into a file for each discovery technique then exfiltrate those file content to attacker's server by embedding the file content in HTTP POST body.
- Requirement
    - Collect information based on the following discovery techniques:
        - Account Discovery: Domain Account
        - Account Discovery: Local Account
        - Password Policy Discovery
        - Query Registry

      # See MITRE ATT&CK techniques description
    - Store the result into a file.
    - Read the file and embedding the file content into HTTP POST body and send the packet to attacker's web server.
- Keyword
    - HTTP POST

16. Exfiltration Over Alternative Protocol–Discovery and Exfiltration through Cloud Storage

- Description
    - The student needs to first establish connection with the victim host by SSH/RDP or other C&C tools. After you get control of the victim host, you need to perform Permission Groups discovery and store the result into a file for each discovery technique then exfiltrate those file content to attacker's cloud storage by upload those files to cloud storage (Google Drive, Dropbox or other cloud storage).
- Requirement
    - Collect information based on the following discovery techniques:
        - Account Discovery: Domain Account

        - Account Discovery: Local Account
        - Password Policy Discovery
        - Query Registry

        # See MITRE ATT&CK techniques description
    - Store the result into files.
    - Upload those files to cloud storage (Google Drive, Dropbox or other cloud storage).
- Keyword
    - Data Exfiltration to Cloud Storage

III. UNC2452

UNC2452 is a suspected Russian state-sponsored threat group responsible for the 2020 SolarWinds software supply chain intrusion. Victims of this campaign include government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East

Scenarios

17. Drive by Compromise–Fake Updater in official website

- Description
    - Setting up a simulated third-party website with official updater on the website. The student needs to replace the official updater with the malware which will collect system information and transfer them to attacker's server.
- Requirement
    - Replace the download link of the website to download your malware.
    - The malware needs to have the following functionalities:
        - Collect system information with these techniques:
            - System information Discovery
            - System Network Configuration Discovery
            - System Network Connection Discovery

            # See MITRE ATT&CK techniques description
        - Send the result to attacker's server.
- Keyword
    -

18. Spearphishing–Phishing Email with Attachment

- Description

        - The student needs to design a phishing e-mail which contain malicious link, victim click link and download malware to collect all .doc file and archived into .zip file and store at %temp%.
    - Requirement
        - A phishing email
        - The malware needs to have the following functionalities:
            - Collect all .doc file
            - Archived them into .zip file
    - Keyword
        - Phishing link

19. Boot or Logon Autostart Execution–Registry run keys

- Description
    - The student needs to write a PowerShell script to modify registry to execute another PowerShell script every time the computer boot. And the 2nd Script will collect system and network information then store the result into a file in %APPDATA%.
- Requirement
    - A PowerShell script to modify registry to run another PowerShell script whenever the computer boot.
    - A PowerShell script to collect system and network information then store the result into a file in %APPDATA%.
        - Collect system information with these techniques:
            - System information Discovery
            - System Network Configuration Discovery
            - System Network Connection Discovery

              # See MITRE ATT&CK techniques description
- Keyword
    - Registry modification
    - PowerShell script

20. Scheduled Task/Job–Schedule task

- Description
    - The student needs to write a PowerShell script to create a schedule task to execute another PowerShell script every 10 minutes. And the 2nd Script will collect system and network information then store the result into a file in %APPDATA%.
- Requirement
    - A PowerShell script to create a schedule task to run another PowerShell script every 10 minutes.

        - A PowerShell script to collect system and network information then store the result into a file in %APPDATA%.
            - Collect system information with these techniques:
                - System information Discovery
                - System Network Configuration Discovery
                - System Network Connection Discovery

                  # See MITRE ATT&CK techniques description
- Keyword
    - Schedule task
    - PowerShell script

21. Application Layer Protocol: Web Protocols–HTTP-based C&C communication

- Description
    - The student needs to survey open source tool to establish HTTP-based C&C communication. And use it to collect all .pdf files in victim's computer then archive them into a .zip to %APPDATA%.
- Requirement
    - Establish C&C communication with the victim.
    - Search and archive all .pdf file into a .zip file.
- Keyword
    - Command and Control over HTTP

22. Application Layer Protocol: Web Protocols–HTTPS-based C&C

- Description
    - The student needs to write a program that will fetch command script from Dropbox or other cloud storage and execute the script then store the result in %APPDATA%.
- Requirement
    - Write a program that can fetch files from cloud storage and execute them.
    - Put the script in cloud storage for execution.
        - The script needs to collect system information with these techniques:
            - System information Discovery
            - System Network Configuration Discovery
            - System Network Connection Discovery

              # See MITRE ATT&CK techniques description
- Keyword

23. Non-Application Layer Protocol–ICMP-based C&C communication

- Description
  - The student needs to survey open source tool to establish ICMP-based C&C communication. And use it to collect all .pdf files in victim's computer then archive them into a .zip to %APPDATA%.
- Requirement
  - Establish C&C communication with the victim.
  - Search and archive all .pdf file into a .zip file.
- Keyword
  - Command and Control over ICMP

24. Non-Standard Port–Using arbitrary port to perform Command and Control

- Description
  - The student needs to write or using open source client-server program to establish Command and Control communication then collect user information.
- Requirement
  - Using client server program to establish C&C
  - Collect information based on the following discovery techniques:
    - Account Discovery: Domain Account
    - Account Discovery: Local Account
    - Password Policy Discovery
    - Query Registry

    # See MITRE ATT&CK techniques description
- Keyword
  - Client Server Program

IV. Lazarus Group

Lazarus Group is a threat group that has been attributed to the North Korean government. The group has been active since at least 2009 and was reportedly responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment as part of a campaign named Operation Blockbuster by Novetta.

Scenarios

25. Drive by Compromise–Drive-by Compromise + User Execution (Malicious File)

- Description

    - Setting up a simulated website. The student needs to inject malicious JavaScript code to the website. Once victims visit the website, malicious JavaScript will automatically download a PowerShell script which will establish a reverse shell.
- Requirement
    - A JavaScript code to download the PowerShell Script.
    - The PowerShell Script needs to create a reverse shell to the attacker.
- Keyword
    - Reverse Shell
    - PowerShell script

26. Spearphishing–Phishing Attachment + User Execution (Malicious File)

- Description
    - The student needs to write a macro enabled Microsoft document which can establish reverse shell from the victim to the attacker then perform user information discovery.
- Requirement
    - Write a macro enabled Microsoft document which will establish reverse shell to the attacker.
    - Collect user information based on the following discovery techniques:
        - Account Discovery: Domain Account
        - Account Discovery: Local Account
        - Password Policy Discovery
        - Query Registry

      # See MITRE ATT&CK techniques description
- Keyword
    - VBA (Visual Basic for Application)
    - Reverse Shell

27. Registry Run Keys / Startup Folder–Boot or Logon Autostart Execution

- Description
    - The student needs to write a PowerShell script to modify registry to execute another PowerShell script every time the computer boot. And the 2nd Script will establish reverse shell to the attacker.
- Requirement
    - A PowerShell script to modify registry to execute another PowerShell script every time the computer boot.
    - A PowerShell script to establish reverse shell.

- Keyword
  - Reverse Shell
  - PowerShell script

28. Application Layer Protocol: Web Protocols–C&C over HTTP + System Network Configuration Discovery

- Description
  - The student needs to implement a C&C malware which can deploy it on victim's host and communicate with student designed C&C server.
- Requirement
  - The malware needs to communicate using HTTP/HTTPS protocol.
  - The malware collects the network configuration ie. IP, MAC, Domain, domain controller IP, user name.
  - The C&C server must be able to handle HTTP requests sent by malware and print it on screen.
- Keyword
  - HTTP C&C
  - Network Configuration (ipconfig)

29. Input Capture (Keylogging) + Remote Desktop Protocol

- Description
  - The student needs to craft a malware to capture the input of the account name and password on a single machine, and using the stolen user/password to login to other machines.
- Requirement
  - The crafted malware can capture the input of keyboard, mouse click.
  - After receiving the user/password, try to login to other machines automatically using RDP.
- Keyword
  - Remote Desktop
  - Remote Desktop Protocol
  - Keylogging

30. Brute Force + Windows Management

- Description
  - Given a windows virtual machine. One has been compromised by student. The student needs to use brute force attack with WMI to access the other machine.
- Requirement

        - The student first needs to brute force to get user name and password
        - After that the student needs to try to login the other machine through WMI using the user name and password obtained from brute force.
    - Keyword
        - Brute Force
        - WMI (wmic.exe)

31. Data staged (Local Data Staging) + Exfiltration (Exfiltration Over C2 channel)

- Description
    - The student must gather information to a specific directory and exfiltrate over HTTP protocol to the student's server.
- Requirement
    - Obtain %USER% directory files information (creation date, size, owner)
    - Exfiltrate the information through HTTP protocol to C&C server.
- Keyword
    - HTTP Protocol
    - User directory collection

V. APT29

APT29 is threat group that has been attributed to the Russian government and has operated since at least 2008. This group reportedly compromised the Democratic National Committee starting in the summer of 2015.

Scenarios

32. Registry Run Keys/Startup Folder

- Description
    - The student needs to add a registry run key to trigger a reverse shell to the designed server. It needs to be triggered whenever the computer boot.
- Requirement
    - Modifying either registry run keys or startup folder to trigger the malware every time the computer boot.
- Keyword

        - Registry Key
        - Startup Folder
        - Persistence

33. Shortcut Modification

- Description
    - The student needs to add a windows shortcut file to trigger a reverse shell to your server or any other persistence whenever the victim executes your crafted short cut file.
- Requirement
    - The shortcut must do at least one of the things list below:
        - Establish reverse shell to student designed C&C server
        - Trigger any persistence scheme eg. Schedule Task, Registry Key, Startup Folder to make the victim's host run reverse shell every time the host boots.
- Keyword
    - Shortcut modification
    - Reverse Shell

34. Scheduled Task/Job: Scheduled Task + Command and Control

- Description
    - The student needs to modify the scheduled task list or add a new schedule task to make the host run the C&C agent to establish connection with the attacker.
- Requirement
    - The scheduled task needs to have the following functionalities:
        - Grab command from cloud service like Dropbox, Google Drive and execute to collect information.
        - Collect user information based on the following discovery techniques:
            - Account Discovery: Domain Account
            - Account Discovery: Local Account
            - Password Policy Discovery
            - Query Registry

        # See MITRE ATT&CK techniques description
        - Save the execution result in %APPDATA%.
- Keyword
    - Scheduled task

35. User Execution: Malicious File (Word)

- Description

        - The student needs to design a Word document which can trigger a reverse shell. When victim open the file, not only normal content of the file must be shown, but also trigger reverse shell.
    - Requirement
        - Arbitrary normal content is allowed.
        - The designed file must have normal functionality.
        - The designed file must also contain reverse shell. When victim open the file, reverse shell must execute automatically.
    - Keyword
        - VBA
        - Reverse shell

36. User Execution: Malicious File (PDF)

- Description
    - The student needs to make a PDF file which can trigger a reverse shell. When victim open the file, not only normal content of the file must be shown, but also trigger reverse shell.
- Requirement
    - Arbitrary normal content is allowed.
    - The designed file must have normal functionality.
    - The designed file must also contain reverse shell. When victim open the file, reverse shell must execute automatically.
    - You can assume any PDF reader application victim used.
- Keyword
    - Repacking (merge pdf file with the reverse shell malware)
    - Reversed Shell
    - metasploit

37. Acquire Infrastructure: Web Services

- Description
    - The student needs to make a malware (open source tools are allowed) and a C&C server (open source tools are allowed). The C&C server can be connected through network.
- Requirement
    - The C&C server must have its own domain/ip. And the C&C server must be able to receive connection from victim.
    - The malware must:
        - Retrieve C&C IP/domain from third-party website, eg. Github, Twitter, Facebook, Dropbox.
        - After get the IP of C&C server, it needs to connect to the

server.

- Keyword

38. Data Obfuscation: Steganography

- Description
  - The student must make the malware that execute and hide instruction in an image.
  - The student needs to make two agents. One agent can hide malicious instruction into normal image (png, gif, or jpg). The other
- Requirement
  - The student needs to make two agents:
    - One agent can hide malicious instruction (shell code) into normal image. The image must be able to viewed normally by human after the agent hided the instruction in it.
    - The other agent needs to decode malicious instruction from crafted image.
- Keyword
  - Steganography

Privilege Escalation

39. Abuse Elevation Control Mechanism: Bypass User Account Control

- Description
  - The student needs to bypass the UAC consent.exe to gain admin's right.
- Requirement
  - The student needs to describe UAC mechanism and how to modify it.
  - The student can use any method to bypass the consent.exe to gain a privilege access with the admin's account.
- Keyword
  - UACME
  - Bypass UAC

VI. Chimera

Chimera is a suspected China-based threat group, targeting the semiconductor industry in Taiwan since at least 2018.

Scenarios

40. Scheduled task/Job-Set up scheduled task to collect information periodically

- Description
  - The student needs to first establish connection with victim's host using SSH/RDP or other C&C tools. After gain control of victim host, write a schedule task to collect system, network information and store them into a file then archived the file into .rar file with password every 10 minutes.
- Requirement
  - Write a schedule task to execute script to:
    - Collect system and network information with these techniques:
      - System information Discovery
      - System Network Configuration Discovery
      - System Network Connection Discovery
        # See MITRE ATT&CK techniques description
    - Store the result into a file
    - Archive the file into .rar with password
  - The script can be written in any language.
- Keyword
  - Scheduled task

41. Credentials from Password Stores–Collect credentials and exfiltrate the data to cloud storage

- Description
  - The student needs to first establish connection with victim's host using SSH/RDP or other C&C tools. After gain control of victim's host, use Mimikatz to collect credentials then store them into a file. After that, exfiltrate the data through upload then to attacker's cloud storage.
- Requirement
  - Use Mimikatz to collect credentials and store them into files.
  - Upload file to cloud storage (Google drive, Dropbox …)
- Keyword
  - Mimikatz

42. Data Exfiltration- Exfiltration over C2(Command and Control) channel

- Description
  - The student needs to first establish connection with victim's host using HTTP C&C tools. After gain control of victim's host, collect

system and network information then store them into files. Read the file content and embedded them in HTTP Post body then send to attacker's server.

- Requirement
  - Establish connection with the victim host using open source HTTP based C&C tools (or implement it).
  - Collect information and store into files with these techniques:
    - System information Discovery
    - System Network Configuration Discovery
    - System Network Connection Discovery

      # See MITRE ATT&CK techniques description
  - Exfiltrate file content through HTTP Post using open source tools (or implement it).
- Keyword
  - HTTP Command and Control
  - HTTP Data Exfiltration