|  |  |  |  |
| --- | --- | --- | --- |
| **MODALIDADE:** | Curso de Especialização Tecnológica (CET) | **Ficha 12: Matrix MITRE\_ATT&CK®** | |
| **CURSO:** | Técnico especialista em cibersegurança | | |
| **UFCD:** | Wargamming | **CÓDIGO UFCD:** | 9197 |
| **FORMADOR/A:** | Ricardo Lobo | **DATA:** | 16/05/2023 |
|  |  |  |  |
| **OBJETIVOS** | | | |
| * Desenvolver os procedimentos de segurança de informação de acordo com o tipo de ameaças e incidentes. * Caracterizar os diferentes tipos de operações em redes de computadores no contexto da cibersegurança e ciberdefesa. | | | |

# Enquadramento

Os ataques cibernéticos são uma realidade e os riscos que as pessoas, organizações e países correm são maiores do que nunca. Os atacantes evoluíram, possuindo agora mais recursos, melhor formação e habilidades para lançar campanhas de intrusão cuidadosamente planeadas, conhecidas como Ameaças Persistentes Avançadas (APT). A segurança e a prosperidade das nações dependem de um conjunto de infraestruturas críticas. Proteger tais ativos implica compreender claramente os atacantes, as suas motivações e estratégias.

O MITRE ATT&CK® é uma base de conhecimento globalmente acessível sobre tácticas e técnicas de atacantes, baseada em observações do mundo real.

# Atividades propostas

1 - Considere o seguinte relatório de um incidente.

|  |  |
| --- | --- |
| **Relatório do incidente** | |
| **Data do incidente:** | 2023-05-09 |
| **Descrição do incidente:** | Comandos **cmd.exe** foram executados através de *Remote Access Trojan* (RAT).  Os comandos foram recolhidos através do sistema de monitorização ***Sysmon*** (https://download.sysinternals.com/files/Sysmon.zip) |
| **Comandos executados:** | ipconfig /all  arp -a  echo %USERDOMAIN%\%USERNAME%  tasklist /v  sc query  systeminfo  net group "Domain Admins" /domain  net user /domain  net group "Domain Controllers" /domain  netsh advfirewall show allprofiles  netstat -ano |

|  |
| --- |
| **Informações sobre os comandos:**   * <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/windows-commands> * <https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc754051(v=ws.11)> |

|  |
| --- |
| **LINKS ÚTEIS:**  MITRE ATT&CK®: <https://attack.mitre.org/>  MITRE ATT&CK® Navigator: <https://mitre-attack.github.io/attack-navigator/> |

1.1 - Utilizando a MITRE ATT&CK® - *Enterprise*, identifique para cada comando do *log*, as **tácticas** e **técnicas** aplicadas pelo atacante na fase de **Descoberta** de informação, conhecimento e preencha a seguinte tabela.

|  |  |
| --- | --- |
| Comando: **ipconfig /all** | |
| **NOME DA TÁCTICA:** | Discovery |
| **ID DA TÁCTICA:** | TA0007 |
| **NOME DA TÉCNICA:** | System Network Configuration Discovery: Internet Connection Discovery |
| **ID DA TÉCNICA:** | T1016 |
| **ID DA SUB-TÉCNICA:** | T1016.001 |
| **PLATAFORMAS AFETADAS PELA TÉCNICA ANTERIOR:** | Linux, Windows, macOS |
| **ID DO *SOFTWARE*:** | S0106 |
|  | |
| Comando: **arp -a** | |
| **NOME DA TÁCTICA:** | Discovery |
| **ID DA TÁCTICA:** | TA0007 |
| **NOME DA TÉCNICA:** | System Network Configuration Discovery: Internet Connection Discovery |
| **ID DA TÉCNICA:** | T1016 |
| **ID DA SUB-TÉCNICA:** | T1016.001 |
| **PLATAFORMAS AFETADAS PELA TÉCNICA ANTERIOR:** | Linux, Windows, macOS |
| **ID DO *SOFTWARE*:** | S0099 |
|  | |
| Comando: **echo %USERDOMAIN%\%USERNAME%** | |
| **NOME DA TÁCTICA:** | Discovery |
| **ID DA TÁCTICA:** | TA0007 |
| **NOME DA TÉCNICA:** | Account Discovery: Domain Account |
| **ID DA TÉCNICA:** | T1087 |
| **ID DA SUB-TÉCNICA:** | T1087.002 |
| **PLATAFORMAS AFETADAS PELA TÉCNICA ANTERIOR:** | Linux, Windows, macOS |
| **ID DO *SOFTWARE*:** | S0106 |
|  | |

|  |  |
| --- | --- |
| Comando: **tasklist /v** | |
| **NOME DA TÁCTICA:** | Discovery |
| **ID DA TÁCTICA:** | TA0007 |
| **NOME DA TÉCNICA:** | Process Discovery |
| **ID DA TÉCNICA:** | T1057 |
| **ID DA SUB-TÉCNICA:** | N/A |
| **PLATAFORMAS AFETADAS PELA TÉCNICA ANTERIOR:** | Linux, Network, Windows, macOS |
| **ID DO *SOFTWARE*:** | S0057 |
|  | |
| Comando: **sc query** | |
| **NOME DA TÁCTICA:** | Discovery |
| **ID DA TÁCTICA:** | TA0007 |
| **NOME DA TÉCNICA:** | System Service Discovery |
| **ID DA TÉCNICA:** | T1007 |
| **ID DA SUB-TÉCNICA:** | N/A |
| **PLATAFORMAS AFETADAS PELA TÉCNICA ANTERIOR:** | Linux, Windows, macOS |
| **ID DO *SOFTWARE*:** | S0106 |
|  | |
| Comando: **systeminfo** | |
| **NOME DA TÁCTICA:** | Discovery |
| **ID DA TÁCTICA:** | TA0007 |
| **NOME DA TÉCNICA:** | System Information Discovery |
| **ID DA TÉCNICA:** | T1082 |
| **ID DA SUB-TÉCNICA:** | N/A |
| **PLATAFORMAS AFETADAS PELA TÉCNICA ANTERIOR:** | IaaS, Linux, Network, Windows, macOS |
| **ID DO *SOFTWARE*:** | S0096 |
|  | |
| Comando: **net group "Domain Admins" /domain** | |
| **NOME DA TÁCTICA:** | Discovery |
| **ID DA TÁCTICA:** | TA0007 |
| **NOME DA TÉCNICA:** | Account Discovery: Domain Account |
| **ID DA TÉCNICA:** | T1087 |
| **ID DA SUB-TÉCNICA:** | T1087.002 |
| **PLATAFORMAS AFETADAS PELA TÉCNICA ANTERIOR:** | Linux, Windows, macOS |
| **ID DO *SOFTWARE*:** | S0106 |
|  | |
| Comando: **net user /domain** | |
| **NOME DA TÁCTICA:** | Discovery |
| **ID DA TÁCTICA:** | TA0007 |
| **NOME DA TÉCNICA:** | Account Discovery: Domain Account |
| **ID DA TÉCNICA:** | T1087 |
| **ID DA SUB-TÉCNICA:** | T1087.002 |
| **PLATAFORMAS AFETADAS PELA TÉCNICA ANTERIOR:** | Linux, Windows, macOS |
| **ID DO *SOFTWARE*:** | S0106 |
|  | |
| Comando: **net group "Domain Controllers" /domain** | |
| **NOME DA TÁCTICA:** | Discovery |
| **ID DA TÁCTICA:** | TA0007 |
| **NOME DA TÉCNICA:** | Account Discovery: Domain Account |
| **ID DA TÉCNICA:** | T1087 |
| **ID DA SUB-TÉCNICA:** | T1087.002 |
| **PLATAFORMAS AFETADAS PELA TÉCNICA ANTERIOR:** | Linux, Windows, macOS |
| **ID DO *SOFTWARE*:** | S0106 |
|  | |
| Comando: **netsh advfirewall show allprofiles** | |
| **NOME DA TÁCTICA:** |  |
| **ID DA TÁCTICA:** |  |
| **NOME DA TÉCNICA:** |  |
| **ID DA TÉCNICA:** |  |
| **ID DA SUB-TÉCNICA:** |  |
| **PLATAFORMAS AFETADAS PELA TÉCNICA ANTERIOR:** |  |
| **ID DO *SOFTWARE*:** |  |
|  | |
| Comando: **netstat -ano** | |
| **NOME DA TÁCTICA:** | Discovery |
| **ID DA TÁCTICA:** | TA0007 |
| **NOME DA TÉCNICA:** | System Network Connections Discovery |
| **ID DA TÉCNICA:** | T1049 |
| **ID DA SUB-TÉCNICA:** | N/A |
| **PLATAFORMAS AFETADAS PELA TÉCNICA ANTERIOR:** | IaaS, Linux, Network, Windows, macOS |
| **ID DO *SOFTWARE*:** | S0106 |

2 - A lista seguinte apresenta algumas das técnicas, tipicamente utilizadas durante a cadeia de ataque.

* *Phishing: Spearphishing Attachment*
* *Phishing: Spearphishing Link*
* *Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder*
* *System Network Configuration Discovery*
* *Abuse Elevation Control Mechanism: Bypass User Account Control*

2.1 - Para **mitigar** os riscos de cada uma das técnicas apresentadas na lista anterior, que **medidas de** **defesa** podem ser utilizadas?

|  |  |
| --- | --- |
| **Técnica:** *Phishing: Spearphishing Attachment* | |
| **ID DA TÉCNICA:** | T1566.001 |
| **MEDIDAS DE DEFESA**  **OU DE**  **MITIGAÇÃO:** | Antivirus/Antimalware; Restrição para não correr certos tipos de ficheiros (ex: .exe, .vbs, .cpl); Treino de utilizadores |

|  |  |
| --- | --- |
| **Técnica:** *Phishing: Spearphishing Link* | |
| **ID DA TÉCNICA:** | T1566.002 |
| **MEDIDAS DE DEFESA**  **OU DE**  **MITIGAÇÃO:** | Restrição de acesso a certos *websites* (ex: DMZ) |

|  |  |
| --- | --- |
| **Técnica:** *Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder* | |
| **ID DA TÉCNICA:** | T1547.001 |
| **MEDIDAS DE DEFESA**  **OU DE**  **MITIGAÇÃO:** | Bloquear a linha de comandos |

|  |  |
| --- | --- |
| **Técnica:** *System Network Configuration Discovery* | |
| **ID DA TÉCNICA:** | T1016 |
| **MEDIDAS DE DEFESA**  **OU DE**  **MITIGAÇÃO:** | Bloquear a linha de comandos |

|  |  |
| --- | --- |
| **Técnica:** *Abuse Elevation Control Mechanism: Bypass User Account Control* | |
| **ID DA TÉCNICA:** | T1548.002 |
| **MEDIDAS DE DEFESA**  **OU DE**  **MITIGAÇÃO:** | Gestão de administradores locais no sistema; Gestão do controlo de acesso de utilizadores (UAC) |

3 – O grupo **APT38** efetuou um ataque a um casino e causou um dano financeiro bastante considerável.

Obtenha informações sobre este grupo e preencha a tabela abaixo.

|  |  |
| --- | --- |
| **NOME DO GRUPO:** | NICKEL GLADSTONE, BeagleBoyz, Bluenoroff, Stardust Chollima |
| **ID DO GRUPO (MITRE ATT&CK):** | G0082 |
| **PAÍS QUE PATROCINA ESTE GRUPO:** | Coreia do Norte |
| **QUAL O ANO EM QUE FOI DETECTADO PELA PRIMEIRA VEZ?** | 2014 |
| **LISTA DE OUTROS GRUPOS ASSOCIADOS:** | NICKEL GLADSTONE, BeagleBoyz, Bluenoroff, Stardust Chollima |
| **INDIQUE 3 TÉCNICAS UTILIZADAS POR ESTE GRUPO:** | T1204.002 - User Execution: Malicious File  T1588.002 - Obtain Capabilities: Tool  T1027.002 - Obfuscated Files or Information: Software Packing |
| **INDIQUE 3 SOFTWARES UTILIZADOS POR ESTE GRUPO:** | S0334 – DarkComet; S0002 - Mimikatz; S0607 - KillDisk |

Depois de realizada a ficha de trabalho, submeta este ficheiro na tarefa criada para o efeito.

**Bom trabalho**