INSTITUTO POLITÉCNICO DE BEJA
Escola Superior de Tecnologia e Gestão
Mestrado em Engenharia de Segurança Informática
Fundamentos de Cibersegurança

Trabalho Individual

Paulo António Tavares Abade - 23919

Beja, outubro de 2025

INSTITUTO POLITÉCNICO DE BEJA
Escola Superior de Tecnologia e Gestão
Mestrado em Engenharia de Segurança Informática
Fundamentos de Cibersegurança

Trabalho Individual

Paulo António Tavares Abade - 23919

Orientadores: Rui Silva & Rogério Bravo

Beja, outubro de 2025

Resumo

Resolução do trabalho

Keywords: cibersegurança

Abstract

Work Resolution

Keywords: cybersecurity

Índice

Índice de Figuras

1 Grupo I - Professor Rui Silva

Nesta secção serão respondidas as questões do Grupo I, focando-se na áreas do MITRE ATT&CK lecionadas pelo professor Rui Silva.

1.1 Pergunta

Em resposta à questão 1.1, foram escolhidas para apresentar as áreas de *Malware Protection* e *Incident Coordination*, que podem ser consideradas como mutualismo/simbiose, uma vez que ambas as áreas trabalham em conjunto para fortalecer a defesa contra ameaças. Caso uma ameaça seja detectada, pela área de *Malware Protection*, a área de *Incident Coordination* entra em ação para coordenar a resposta ao incidente, assegurando que as medidas adequadas sejam tomadas para mitigar o impacto da ameaça.

1.1.1 Malware Protection

A proteção contra malware envolve a implementação de medidas e tecnologias para prevenir, detectar e remover software malicioso que possa comprometer a segurança dos sistemas informáticos. No entanto, esta proteção não é infalível, podendo ser contornada por malware que esteja camuflado ou que nunca tenha sido identificado, no caso do último, é conhecido como *Zero-Day Malware*. Esta proteção funciona através da análise de padrões comuns em ataques (CAPE), sendo que estes padrões foram identificados através do MAEC (Malware Attribute Enumeration and Characterization), que é um padrão para a representação de informações sobre malware, permitindo a troca estruturada de dados entre diferentes ferramentas e sistemas de segurança. O objetivo principal do MAEC é facilitar a detecção, análise e resposta a ameaças de malware, promovendo a interoperabilidade entre diferentes soluções de segurança. Este é utilizado pelo Incident Coordination para ajudar a prevenir novos ataques com base no que a proteção de malware não conseguiu impedir.

1.1.2 Incident Coordination

A coordenação de incidentes envolve a gestão e resposta a incidentes de segurança informática que não tenham sido superados pela proteção de malware, garantindo que as ameaças sejam tratadas de forma eficaz e eficiente. Isto inclui a identificação, análise, contenção, erradicação e recuperação de incidentes de segurança. A coordenação eficaz de incidentes é crucial para minimizar o impacto das ameaças e garantir a continuidade das operações. Integrando e correlacionando informação de multiplicas fontes estáticos e dinâmicas, mais conhecidamente como IODEF (Incident Object Description Exchange Format), que é um padrão para a troca estruturada de informações sobre incidentes de segurança informática, sendo que isto permite detetar com cada vez mais qualidade a presença de malware através da análise da sua assinatura. Isto fica automatizado com o RID (Realtime Inter-network Defense), que é um protocolo que permite a troca automática e segura de informações sobre ameaças. Existem ainda outros prótocolos como o TAXII (Trusted Automated eXchange of Indicator Information) que é um protocolo para a troca automatizada de indicadores de ameaças, e o STIX (Structured Threat Information eXpression) que é uma linguagem padronizada para a representação de informações sobre ameaças cibernéticas, e estes são complementares sendo que o STIX é o formato que passa pelo TAXII para ser transmitido entre sistemas.

1.2 MITRE - Projeto de ATT&CK - Night Dragon

O projecto *Night Dragon* foi uma campanha de ciberespionagem que visou várias empresas de energia, petróleo e os seus derivados, sediadas no Cazaquistão, Taiwan, Grécia e Estados Unidos da América, e a campanha foi descoberta em novembro de 2009 pela McAfee. O objetivo principal desta campanha era roubar informações confidenciais e proprietárias relacionadas com a indústria de energia. Primeiramente, os atacantes compraram serviços para alojar os servidores que iriam controlar as vítimas e usavam os protocolos HTTP como meio de comunicação, pois estes ficavam disfarçados entre o tráfego legítimo. A partir de SQL Injection para obter os dados, era utilizado o software *Cain & Abel* para realizar ataques de brute-force para decifrar os hashes das palavras-passe dos administradores de sistemas, conseguindo assim aceder remotamente aos sistemas das vítimas, e com o *zwShell* implantado os atacantes podiam executar comandos remotamente.

Com isso, os atacantes começaram a obter ficheiros e outras informações sensíveis de sistemas comprometidos, enviando-os para os servidores que tinham sido comprados anteriormente.

Ainda utilizaram um RAT (Remote Access Trojan), usando os servidores afetados para fazer ataques a alvos internos através de e-mails de spear-phishing que continham anexos maliciosos que, quando abertos, instalavam o RAT nos sistemas das vítimas. O alvo principal desta parte do ataque eram portáteis que tinham contas de VPN e que permitiam obter ainda mais acesso aos sistemas internos. A estratégia baseava-se em usar ferramentas de roubo de palavras-passe e, ao entrar, deixar um RAT.

Após a investigação, a McAfee concluiu que o grupo responsável pelo *Night Dragon* tinha ligações à China, trabalhava entre as 9h e as 17h no horário de Pequim, e que o grupo tinha como alvo empresas específicas, sugerindo que a campanha era motivada por interesses económicos e estratégicos.

1.3 MITRE - Projeto ATT&CK - Tática de Initial Access

A tática de *Initial Access* tem o objetivo de conseguir o primeiro ponto de entrada numa rede e/ou alvo. Existem várias técnicas para alcançar este objetivo, sendo a mais conhecida o *Phishing/Spear-Phishing*, que envolve o envio de e-mails, SMS ou aplicações que aparentam ser legítimos, mas que contêm links ou anexos maliciosos. No caso do *Enterprise*, qualquer funcionário pode ser alvo deste tipo e-mails, enquanto que no *Mobile*, o alvo costuma ser o utilizador final e pode ser vitíma através de SMS, aplicações ou chamadas telefónicas. Por fim, no *ICS*, o alvo vai ser o funcionário ou grupo de funcionários de uma organização que possua acesso a sistemas industriais, e estes podem ser vítimas através de e-mails ou chamadas telefónicas.

Existem estas varias de *Phishing/Spear-Phishing* porque cada ambiente tem as suas particularidades, e o atacante deve adaptar-se a cada um deles, maximizando as chances de sucesso para cada situação, onde cada alvo tem os seus próprios hábitos e rotinas.