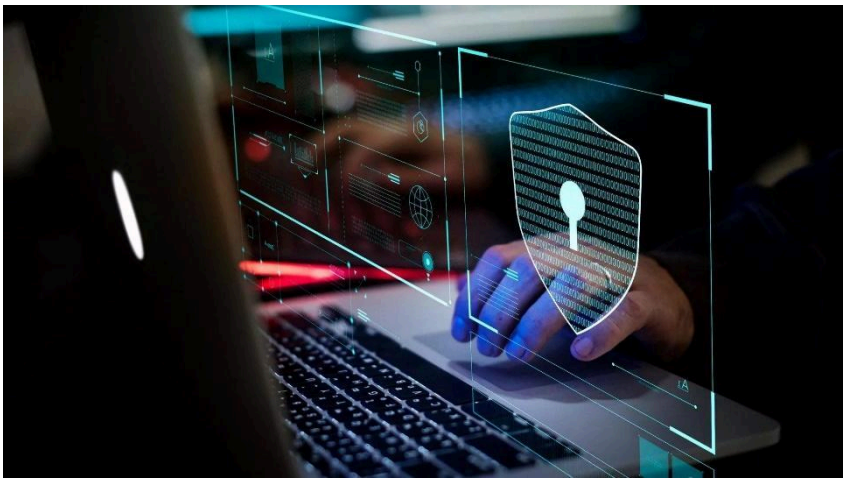
CiberSegurança

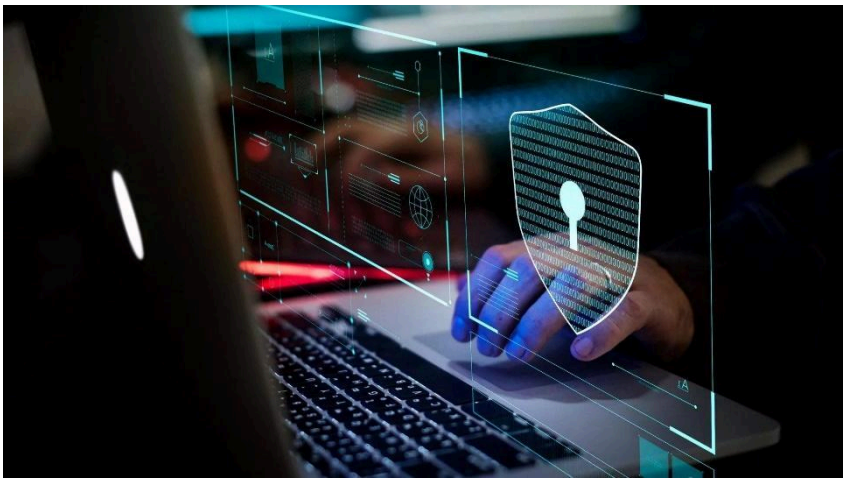


Escola Secundaria João Carlos Celestino Gomes

Aveiro, novembro 2023

Trabalho realizado pelo aluno Fernando Gonçalves da turma 12ºE , sob orientação do Professor, Sérgio Heleno, no ano letivo 2023/2024

CiberSegurança



Escola Secundaria João Carlos Celestino Gomes

Aveiro, novembro 2023

Trabalho realizado pelo aluno Fernando Gonçalves da turma 12ºE , sob orientação do Professor, Sérgio Heleno, no ano letivo 2023/2024

Índice

1 Introdução

Este trabalho surgiu no âmbito de Redes de Comunicação/FCT com a finalidade de aprender mais sobre a segurança na Internet. Trabalho realizado em fevereiro de 2021 na cidade de Esmoriz.

2 O que é a CiberSegurança

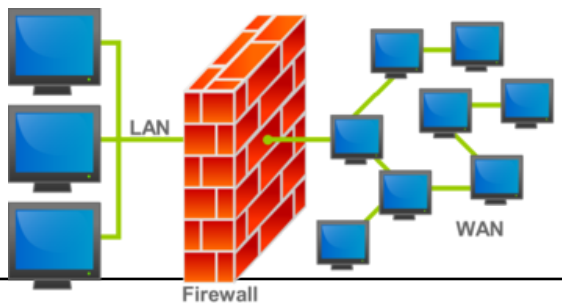
A cibersegurança, ou segurança cibernética, é o conjunto de práticas, técnicas, políticas e ferramentas projetadas para proteger sistemas de computadores, redes, dispositivos e dados contra ameaças, ataques e acessos não autorizados. O objetivo da cibersegurança é garantir a confidencialidade, integridade e disponibilidade da informação, além de proteger os sistemas contra danos e minimizar os riscos associados às atividades cibernéticas maliciosas.

3 O que é a Darkweb

A Darkweb é uma parte da World Wide Web que é intencionalmente oculta e acessada usando redes sobrepostas, como o Tor (The Onion Router). Ela é frequentemente associada a atividades ilegais devido ao anonimato que proporciona aos usuários, permitindo transações e comunicações que podem ser mais difíceis de rastrear. No entanto, é importante notar que nem todo o conteúdo da Darkweb é ilegal, e ela também pode ser usada para propósitos legítimos, como preservar a privacidade online.

4 O que é uma Firewall

Uma firewall é um sistema de segurança que monitora e controla o tráfego de dados entre redes, permitindo ou bloqueando o tráfego com base em um conjunto de regras predefinidas. O objetivo principal da firewall é proteger uma rede privada ou um dispositivo contra acessos não autorizados, ataques cibernéticos e ameaças maliciosas, controlando o tráfego de entrada e saída.



5 O que é um router

Um roteador é um dispositivo de rede que encaminha dados entre redes de computadores. Ele atua como um ponto de conexão entre diferentes redes e direciona o tráfego de dados da maneira mais eficiente possível. Roteadores são comumente usados em redes domésticas e empresariais para conectar dispositivos locais à internet e entre si.

6 O que é um switch

Um switch é um dispositivo de rede que opera na camada de enlace do modelo OSI (Open Systems Interconnection). Ele é usado para conectar vários dispositivos em uma rede local (LAN), permitindo a comunicação direta entre eles. Ao contrário de um hub, um switch inteligentemente direciona os dados apenas para o dispositivo de destino, melhorando a eficiência da rede.

7 O que é um antivírus

Um antivírus é um software projetado para detectar, prevenir e remover software malicioso, como vírus, worms, trojans, spyware e outros tipos de malware. Ele realiza varreduras no sistema para identificar padrões de código malicioso e proteger o computador ou dispositivo contra ameaças cibernéticas. Os antivírus também podem incluir recursos de proteção el tempo real para evitar a execução de malware.

8 Tipos de Hacker

8.1 O que é um Hacker

Um hacker é uma pessoa com habilidades avançadas em computação e redes, que pode usar essas habilidades para explorar sistemas, encontrar vulnerabilidades de segurança e, em alguns casos, comprometer a segurança de sistemas ou redes.

8.2 White Hats

White Hats são hackers éticos que utilizam suas habilidades para identificar e corrigir vulnerabilidades de segurança. Eles trabalham para empresas, organizações governamentais ou

provedores de segurança para fortalecer a cibersegurança.

8.3 Gray Hats

Gray Hats são hackers que não se enquadram estritamente nas categorias de "éticos" ou "maliciosos". Eles podem invadir sistemas sem permissão, mas o fazem com a intenção de alertar o proprietário sobre vulnerabilidades, muitas vezes buscando recompensas ou reconhecimento.

8.4 Black Hats

Black Hats são hackers maliciosos que exploram vulnerabilidades com o objetivo de causar danos, roubar informações ou realizar atividades ilegais. Eles representam uma ameaça significativa à segurança cibernética.

8.5 Hackeres organizados

Hackers organizados são grupos que trabalham juntos para realizar atividades cibernéticas maliciosas. Isso pode incluir ataques coordenados, espionagem cibernética, roubo de dados e outras ações prejudiciais.

9 Tipos de Malware

9.1 O que é o Malware

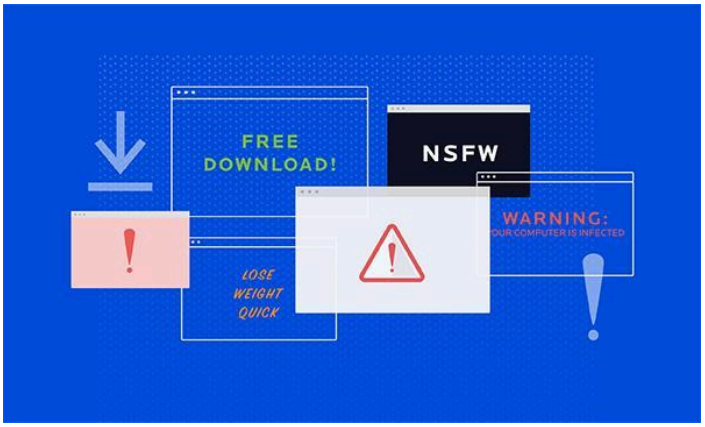
Malware (do inglês "malicious software") é um termo genérico que engloba vários tipos de software malicioso projetado para causar danos a um computador, rede ou usuário.

9.2 Spyware

Spyware é um tipo de malware que coleta informações sobre atividades do usuário sem o seu conhecimento, geralmente para fins de espionagem ou roubo de dados.

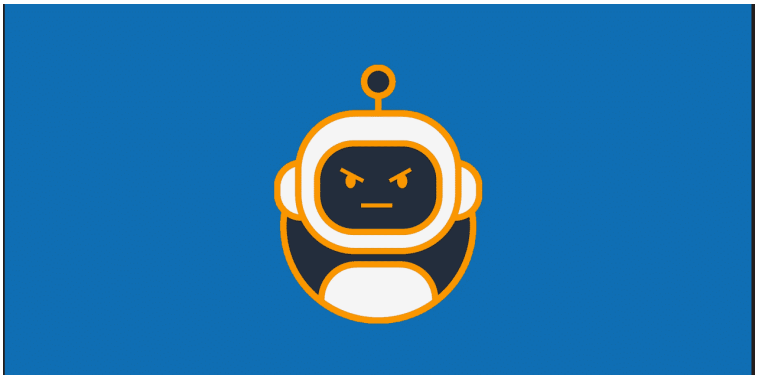
9.3 Adware

Adware exibe anúncios indesejados em um dispositivo, muitas vezes com o objetivo de gerar receita para os criadores do malware.



9.4 Bot

Bots são programas automatizados que realizam tarefas específicas na internet. Quando controlados por atacantes, podem ser usados para atividades maliciosas, como ataques distribuídos de negação de serviço (DDoS).

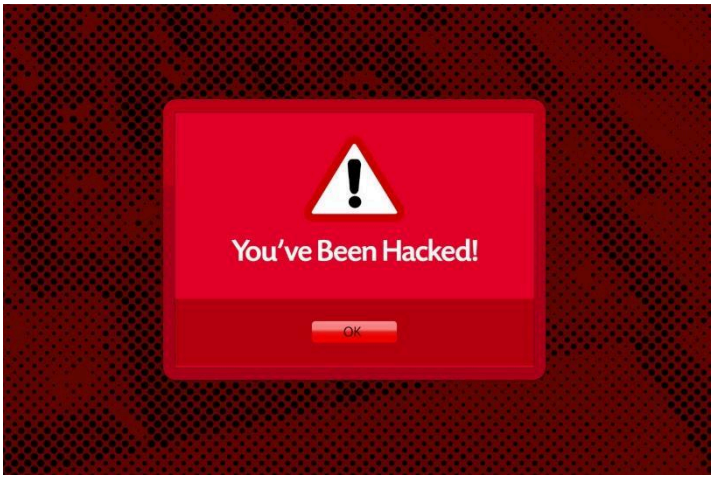


9.5 Ransomware

Ransomware é um tipo de malware que criptografa os dados de um usuário e exige um resgate em troca da chave de descriptografia.

9.6 Scareware

Scareware é um software fraudulento que tenta assustar os usuários, muitas vezes exibindo mensagens falsas de ameaças de segurança, para induzi-los a comprar software inútil ou perigoso



9.7 Rootkit

Um rootkit é um tipo de malware que oculta a presença de outros malwares no sistema, tornando-os difíceis de serem detectados por softwares de segurança convencionais.

9.8 Vírus

Um vírus é um tipo de malware que se anexa a um programa existente e se replica quando esse programa é executado. Ele pode causar danos ao sistema e se espalhar para outros programas e sistemas.

9.9 Trojan horse

Um cavalo de Troia, ou trojan horse, é um tipo de malware disfarçado como um programa aparentemente inofensivo, mas que, na realidade, executa funções maliciosas quando ativado.

9.10 Worm

Um worm é um tipo de malware que se replica e se espalha automaticamente, muitas vezes explorando vulnerabilidades em sistemas de computadores conectados em rede.

10 Engenharia Social

10.1 O que é a engenharia social

A engenharia social é uma técnica usada por indivíduos ou grupos para manipular e enganar as pessoas, a fim de obter informações confidenciais, acesso a sistemas ou realizar atividades maliciosas.

10.2 Pretexting

Pretexting envolve a criação de uma narrativa fictícia ou pretextos para obter informações de uma pessoa. Isso pode incluir fingir ser outra pessoa, como um colega de trabalho ou funcionário de suporte técnico.

10.3 Tailgating

Tailgating, ou "carona", refere-se à prática de seguir de perto alguém que tem acesso autorizado a um edifício ou área segura para ganhar entrada não autorizada.

11 Segurança

11.1 Segurança do posto de trabalho

A segurança do posto de trabalho refere-se às medidas e práticas destinadas a proteger os dispositivos individuais, como computadores e smartphones, contra ameaças cibernéticas. Isso inclui o uso de antivírus, firewalls pessoais e a conscientização do usuário.

11.2 Segurança de email

A segurança de email envolve práticas e tecnologias para proteger as comunicações por email contra ameaças como phishing, malware e spam. Isso pode incluir filtros de spam, autenticação de email e educação do usuário para evitar cair em golpes de engenharia social.

12 Conclusão

Com a realização deste trabalho fiquei a saber um pouco mais sobre cibersegurança.

Tive dificuldade em selecionar informação correta.

Gostei de elaborar em esta pesquisa, em especial dos malware.

13 Para pensar

Será que daqui a uns anos continuaram a existir os malwares?

14 Webgrafia

Chatgpt

Wikipedia.

Cibersegurança

Nome Apelido

Nome da escola

Esmoriz, fevereiro de 2021