CYBERSEGURANÇA E PREVENÇÃO

Lucas Marques Pacheco Fernandes
Jairo Oliveira de Castro

Colégio Passionista São Paulo da Cruz

Resumo

Esse projeto abordou a temática da cybersegurança, analisando os tipos de ataques que podem ser realizados, coletando dados sobre modos de prevenção e realizando uma pesquisa de campo por meio de um formulário online divulgado em lugares públicos como o metrô e parques.

Palavras-chave: Cybersegurança 1. Tecnologia 2. Malware 3. Prevenção 4.

Introdução

Usando pesquisas bibliográficas e de campo, dissertarei sobre diversos assuntos dentro da esfera da segurança digital e compartilharei métodos de prevenção a ataques sobre os quais aprendi no desenvolvimento do trabalho.

Objetivo

Com esse projeto, quero abordar um tema que se torna mais relevante com o passar do tempo: a segurança no meio digital. Procurei ampliar o meu conhecimento acerca do assunto e conscientizar o público geral sobre os diversos jeitos pelos quais um indivíduo pode ser prejudicado por pessoas mau-intencionadas e como melhorar a prevenção. Afinal, conhecimento sobre a proteção nas ruas já é difundido, mas o mesmo não acontece no meio cibernético.

Metodologia

Este trabalho utiliza a metodologia exploratória e descritiva. Utilizei um formulário online e divulguei-o a fim de obter o máximo de informação possível e usei artigos onlines para obter informação teórica.

Desenvolvimento

Privacidade: Por que importa?

Segundo o New York Times[1], um pai de São Francisco percebeu que seu filho estava com sua genitália inchada, e mandou foto da mesma para sua esposa, que então mandou-as para o médico. Isso fez com que Mark fosse alvo de uma investigação policial por mais de uma década. Sua conta Google foi banida e ainda não foi recuperada. Esse incidente mostra que, por mais que você não tenha nada para esconder, privacidade é SIM importante.

Empresas, em especial de redes sociais, coletam dados sobre seus usuários: O Observer, the Guardian e The New York Times[2] revelaram depois das eleições americanas de 2016 que uma empresa chamada Cambridge Analytica pegou diversos dados de usuários do Facebook e os usou para distribuir propaganda política na internet. A empresa disse ter "Colocado o Trump na Casa Branca", e o incidente gerou um debate de proporção gigantesca nos EUA.

Como provado pelos casos supracitados, não importa se você não tem nada para esconder na internet: sua informação ainda pode e é usada por empresas para o benefício delas, de terceiros ou usada para te prejudicar.

Como proteger sua privacidade?

Segundo a Fortinet[3], para proteger sua privacidade, é recomendado o uso de VPNs, que escondem sua localização ao introduzir um servidor intermediário entre o computador e o website que deseja-se acessar. Eles falam, ainda, que VPNs gratuitas muita vezes não oferecem segurança pois coletam dados de usuários e direcionam anúncios customizados para gerar lucro.

Também é essencial usar um navegador e um mecanismo de pesquisa que não coletem dados, como o Brave e Brave Search, respectivamente, visto que serviços como o Google e o Google Chrome coletam dados de uso[4].

Se o usuário estiver disposto a se adaptar a um novo workflow e menos compatiblidade de software, é recomendado que se use uma distribuição Linux.
Linux é um kernel, ou seja, o núcleo de um sistema operacional. Esse kernel pode ser usado com programas de terminal como os utilitários do GNU, interfaces gráficas como o GNOME e KDE Plasma e aplicações open-source diversas para criar um sistema operacional. Como o kernel e muitos dos sistemas feitos com ele são 100% open-source, ou seja, qualquer indivíduo pode acessar o código-fonte e verificar se há serviços de telemetria escondidos. Exemplos são Pop!OS, Linux Mint e Arch Linux.

DdoS

DDoS (Distributed Denial of Service) é um tipo de ataque cibernético onde um usuário mal-intencionado dirige uma grande quantidade de tráfico a um site por meio de uma botnet, ou seja, uma rede de computadores infectados os quais o autor do crime controla. A quantidade gigante de tráfico sobrecarrega o site e o deixa inusável, criando assim a "negação de serviço" que dá nome ao ataque.

Como previnir?

Infelizmente, muitas vezes um ataque DDoS de menor escala passa despercebido pois os sintomas, tal como lentidão, são comuns[5]. A lentidão como problema pode indicar um ataque de DDoS quando é em um horário que normalmente não apresenta tantos acessos[6]. No caso de investigação, pode-se analisar o IP de origem do tráfico ou comportamentos semelhantes entre as fontes.[6]
Porém, há maneiras de combater um ataque[6]:
Anycast Network: Fazer uma difusão do tráfico mal-intencionado com uma rede Anycast consiste em "dissipar" esse tráfico entre vários servidores ou nós a fim de que o ataque fique gerenciável
Black Hole: quando se usa essa técnica, todo tráfico é jogado para um black hole, ou um "buraco negro". Essa técnica limita tráfico legítimo e dá aos ofensores o que eles desejavam, ou seja, tornar o site inusável.
Limitar a quantidade de tráfico, ou "Rate Limiting", que pode entrar em um site, tomando cuidado para não limitar demais e bloquear usuários legítimos
Firewall: Um firewall pode identificar tráfico malicioso e eliminá-lo. Um exemplo de firewall muito usado em computadores empresariais é o Crowdstrike.

Malware

Malware é, segundo a Crowdstrike[7], "um termo geral para descrever um programa ou código criado para causar danos a um computador, rede, ou servidor.". Alguns tipos de malware são:

- Ransomware: Ransomware, segundo a IBM[8], é "um tipo de malware que faz do dispositivo ou informações pessoais do usuário reféns, ameaçando deixá-la bloqueada ao acesso – ou pior – caso o usuário não pague uma quantia em dinheiro"
- Adware[9]: Adwares são programas que visam ao ganho financeiro ao mostrar anúncios indesejados ao usuário, muitas vezes também deixando portas abertas para outros programas maliciosos se instalarem.
- Spyware[10]: Spyware é um software indesejado que, ao entrar no computador do usuário, coleta dados como padrões comportamentais e dados sensíveis. Então, esses dados são mandados para empresas que pagam pelos mesmos.
- Trojan[11]: Com o nome baseado no famoso Cavalo de Troia, esse tipo de programa malicioso se disfarça como software legítimo que o usuário é convencido a baixar por meio de manipulação do usuário mal-intencionado. Quando esse software é executado, ele obtém acesso à máquina
- PUP[12]: Você conhece alguém que já tenha apertado "próximo" em um instalador uma vez atrás da outra sem ver o que está sendo dito, e depois se encontra em um oceano de toolbars e outros programas que deixam o computador lento? Se sim, essa pessoa já foi vítima de PUPs, ou "potentially unwanted programs". Esses programas são na verdade instalados com o consentimento do usuário, que não se atenta aos detalhes que um instalador mostra. Eles não são malwares, mas ainda podem ser incômodos pois consomem recursos da máquina e coletam dados.
- Ataques Fileless[13]: Ataques fileless são ataques cujo modus operandi não é instalar código no computador do usuário, mas sim usar ferramentas legítimas para realizar ações ilegítimas. O hacker pode obter acesso a tais ferramentas por meio de técnicas como exploits que fornecem a entrada no computador por meio de e-mails maliciosos. Outro método é usar credenciais roubadas para acessar o Windows Management Instrumentation (A infraestrutura do Windows que gerencia dados) ou o Powershell
- Bombas Lógicas[14]: Bombas lógicas são programas maliciosos que só ativam quando uma condição é cumprida, como o enésimo login no computador.

Como se proteger?

Para se proteger de malwares, é de vital importância atenção aos sites visitados pelo usuário e

um software de segurança: o Microsoft Defender, que vem gratuitamente com o Windows, é uma ótima opção segundo o site CNET[15]. Malwarebites, Norton e Kaspersky são soluções famosas. Distros Linux e BSD são boas opções para quem tem segurança como prioridade máxima: além dos mecanismos de defesa do sistema serem melhores[16] (por exemplo, nenhum usuário tem permissão de administrador o tempo inteiro, sendo necessário o uso do Sudo), há menos ataques a esses sistemas por conta da base de usuários menor[17].
É de benefício do usuário que ele também mantenha seu sistema atualizado, pois novas brechas são sempre encontradas e consertadas.

Vazamentos de dados

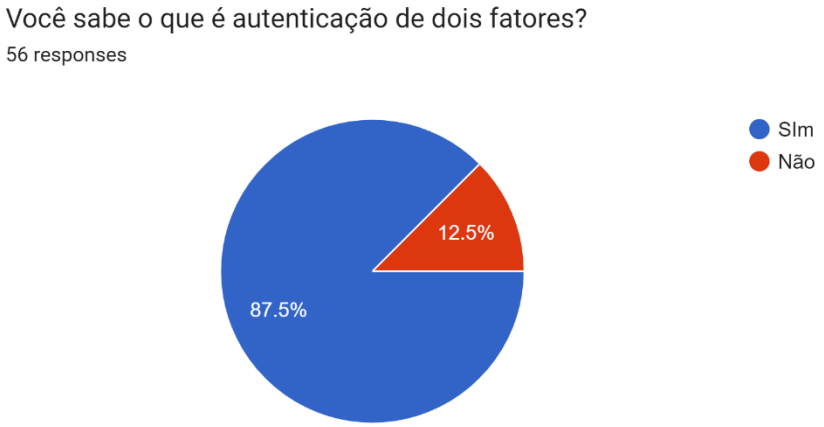
Em 2011, o serviço Playstation Network (PSN) foi hackeado e dados pessoais como endereço, nome, senha e aniversário de 77 milhões de usuários foram roubados[18]. Segundo a Forbes[19], 349.221.481 pessoas foram impactadas por vazamentos de dados em 2023. Conclui-se, por conseguinte, essa problemática tem amplo efeito no mundo.

Como se proteger?

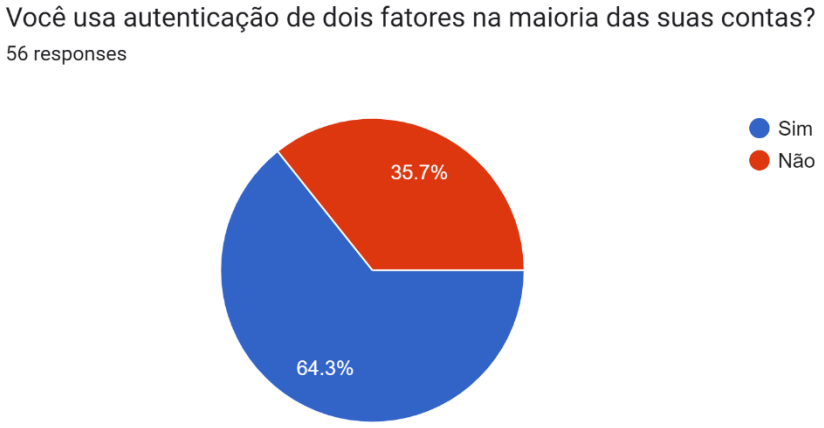
Segundo a Fortinet[20], para prevenir um vazamento de dados é necessário que se use senhas fortes (isto é, mistura de letras maiúsculas e minúsculas, números e caracteres especiais), se use autenticação multifator, ou seja, que além da senha, se use um mecanismo como uma mensagem de SMS para autenticar um login. É também recomendado que se atualize software e visite apenas sites que sejam com 100% de certeza seguros.

Pesquisa de Campo

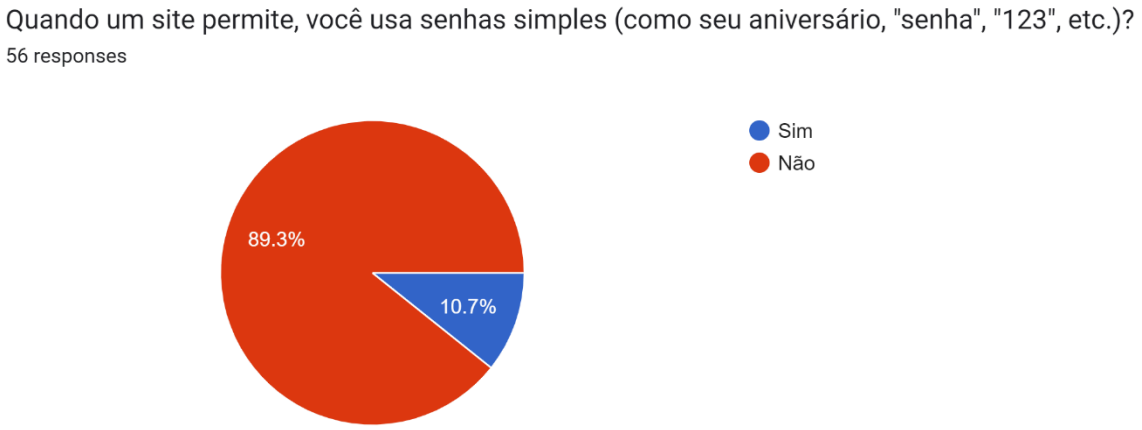
A pesquisa de campo foi realizada por meio de um formulário no Google Forms. Ele foi distribuído a indivíduos em lugares públicos como estações de metrô, dentro do ambiente escolar e em lugares públicos tais como praças públicas. Ao todo, foram obtidas 56 respostas, cujas estatísticas serão mostradas a seguir:



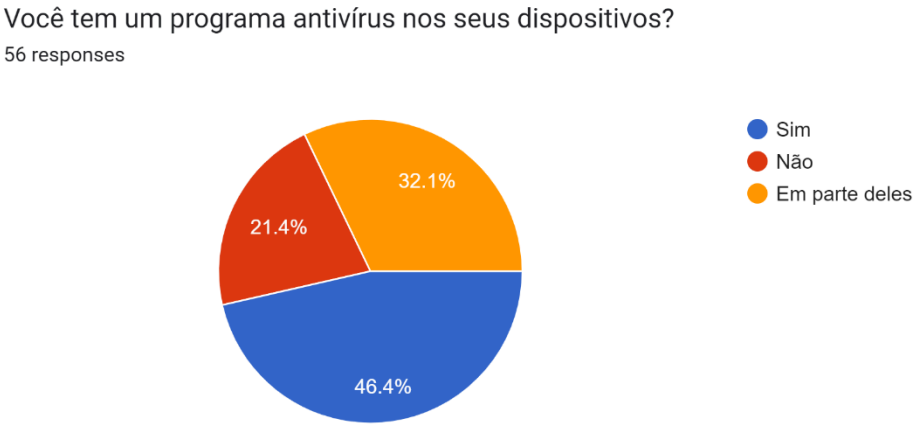
A maioria dos entrevistados estavam familiares com o termo Autenticação de Dois Fatores.



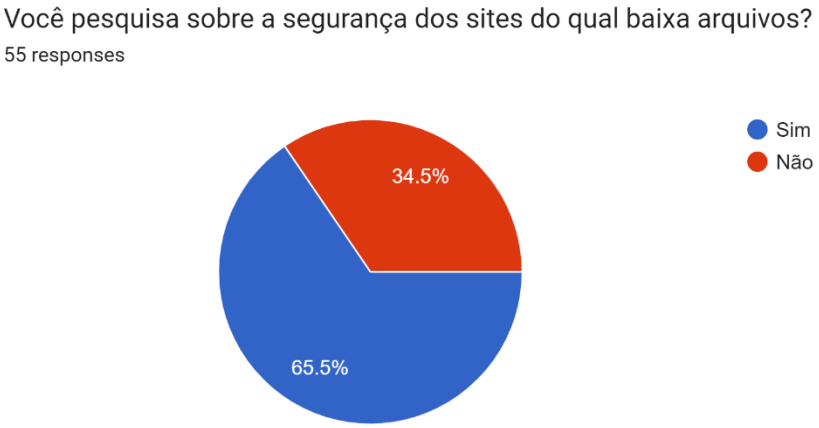
Aqui, percebemos uma discrepância de aproximadamente 20% entre pessoas que conhecem a ferramenta e que de fato usam-na.



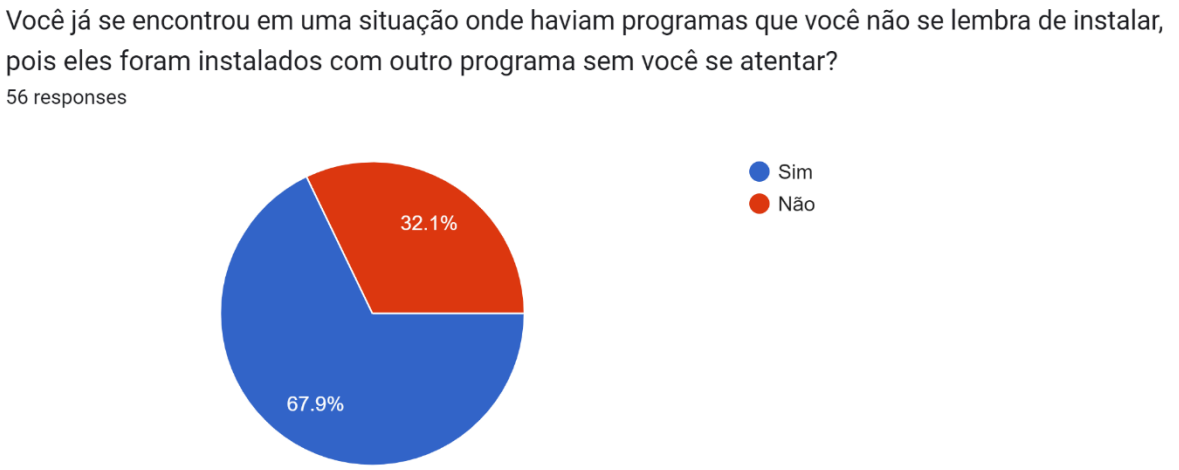
Aqui, vemos um bom resultado: A maior parte dos entrevistados não usam senhas simples quando um site permite (a maioria dos sites não permitem o uso de senhas desse tipo)



Aqui, vemos outro bom resultado: Aproximadamente 80% dos usuários usam, em algum nível, programas antivírus.



Aqui, encontramos um dado preocupante. Aproximadamente um terço dos entrevistados não verificam a segurança de um site antes de baixar arquivos. Obter vírus de um site disponibilizando programas maliciosos é o jeito mais tradicional de sofrer um ataque cibernético, o que mostra que, mesmo nas questões mais difundidas no conhecimento geral, ainda há trabalho de conscientização a fazer.



Como na pergunta anterior, um terço dos entrevistados mostram já ter instalado um Programa Potencialmente Indesejado em seus computadores por falta de atenção a o que estava sendo instalado de forma casada com outro software

Considerações Finais

Com os dados obtidos por meio de pesquisas, tanto bibliográficas quanto de campo, foi possível obter insights significantes sobre cybersegurança e principalmente a difusão desses conhecimentos no público geral. Constata-se, por meio da informação encontrada, que ataques com malware podem ser feitos de diversas maneiras, sem necessariamente utilizar arquivos baixados pelo usuário, o que cria a necessidade de cuidados ao abrir e-mails e utilizar um software antivírus de qualidade. Sobre esses, levando em conta apenas a amostra populacional obtida, a sociedade brasileira está em um bom caminho para a adoção deles, sendo ainda necessária mais conscientização para a expansão da prática do seu uso para aparelhos smartphone.

Constata-se, também, o alcance de vazamentos de dados não só no Brasil como no mundo inteiro. Acerca desse tema, percebe-se que medidas simples que podem ser tomadas para evitar tais males são utilizadas por boa parte da população, precisando ainda, contudo, de mais adoção.

A importância da privacidade, contudo, é o ponto sobre o qual achei mais importante dissertar neste trabalho. Há coisas as quais podemos contornar, mas com outras, devemos abrir mão de nossa privacidade ou abrir mão do produto em uso. O governo brasileiro tem a responsabilidade de limitar esse fenômeno, tal como a União Europeia vem fazendo. A razão de eu achar esse tópico de extrema importância depois das minhas pesquisas bibliográficas se dá pelo fato da maioria dos cidadãos saberem que um vírus é ruim, ou que vazamentos de dados sensíveis como números de cartões são um perigo imenso. Porém, a visibilidade do

problema da privacidade ainda é escassa, e quem reconhece as práticas de empresas por vezes não se importam, dizendo que não têm nada a esconder.
A conscientização é o meu principal objetivo com este trabalho, e espero que tal esperança se cumpra.

Referências Bibliográficas Citadas no Texto:

1 - https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html
2 - https://time.com/5197255/facebook-cambridge-analytica-donald-trump-ads-data/
3- https://www.fortinet.com/resources/cyberglossary/how-does-vpn-work
4-
https://www.cnet.com/news/privacy/theres-a-way-to-delete-the-frightening-amount-of-data-google-has-on-you/
5- https://www.fortinet.com/resources/cyberglossary/ddos-attack
6- https://www.cloudflare.com/pt-br/learning/ddos/what-is-a-ddos-attack/
7- https://www.crowdstrike.com/cybersecurity-101/malware/
8- https://www.ibm.com/topics/ransomware
9- https://www.kaspersky.com.br/resource-center/threats/adware
10-https://www.fortinet.com/resources/cyberglossary/spyware#:~:text=Spyware%20is%20malicious%20software%20that,device%20without%20the%20user's%20consent.
11- https://www.kaspersky.com.br/resource-center/threats/trojans
12- https://www.kaspersky.com/resource-center/definitions/what-is-pup-pua
13- https://www.crowdstrike.com/cybersecurity-101/malware/fileless-malware/
14- https://www.kaspersky.com/resource-center/threats/types-of-malware
15- https://www.cnet.com/reviews/microsoft-windows-defender-review/
16- https://ubuntu.com/blog/is-linux-secure
17-
https://truelist.co/blog/linux-statistics/#:~:text=How%20many%20people%20use%20Linux,to%201.6%20billion%20Android%20users.
18- https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data
19- https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/
20- https://www.fortinet.com/resources/cyberglossary/data-breach