MARINHA DO BRASIL
DIRETORIA DE ENSINO DA MARINHA
CENTRO DE INSTRUÇÃO ALMIRANTE ALEXANDRINO

CURSO DE APERFEIÇOAMENTO AVANÇADO EM
SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

TRABALHO DE CONCLUSÃO DE CURSO

ANÁLISE DE VULNERABILIDADE DE SEGURANÇA CIBERNÉTICA EM DISPOSITIVOS MÓVEIS FUNCIONAIS NA MARINHA DO BRASIL

PRIMEIRO-TENENTE CLEYSON PINHEIRO DA SILVA

Rio de Janeiro
2023

PRIMEIRO-TENENTE CLEYSON

ANÁLISE DE VULNERABILIDADE DE SEGURANÇA CIBERNÉTICA EM DISPOSITIVOS MÓVEIS FUNCIONAIS NA MARINHA DO BRASIL

Monografia apresentada ao Centro de Instrução Almirante Alexandrino como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações.

Orientadores:
CF (RM1-T) Wagner Santana de Freitas
Prof. Dr. Davidson Rodrigo Boccardo

CIAA
Rio de Janeiro
2023

CLEYSON PINHEIRO DA SILVA

ANÁLISE DE VULNERABILIDADE DE SEGURANÇA CIBERNÉTICA EM DISPOSITIVOS MÓVEIS FUNCIONAIS NA MARINHA DO BRASIL

Monografia apresentada ao Centro de Instrução Almirante Alexandrino como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações.

Aprovada em _____

Banca Examinadora:

_____

CMG (RM1-EN) Gian KarloHuback Macedo de Almeida – CIAW

_____

CF (RM1-T) Wagner Santana de Freitas – CIAW

_____

Davidson Rodrigo Boccardo, D. Sc. – UNESP

AGRADECIMENTOS

Gostaria de expressar minha mais profunda gratidão às pessoas que estiveram ao meu lado durante esta jornada acadêmica, tornando possível a conclusão deste trabalho.

Primeiramente, minha eterna gratidão à minha esposa, Naíra Soares, por seu apoio incondicional, paciência e compreensão ao longo de todas as etapas deste projeto. Sua presença foi meu alicerce e motivação, e por isso, minha gratidão é imensurável.

Segundamente, aos meus filhos, Apollo e Athena, que são a base da minha vida e minha inspiração em ser o melhor de mim.

Aos meus pais, Cosmo e Maria, e meu irmão, Augusto, que sempre acreditaram em mim, me apoiaram nos momentos de dificuldade e celebraram comigo cada conquista. Seu amor e encorajamento foram fundamentais para eu alcançar este objetivo.

Aos meus instrutores do Curso de Segurança da Informação e Comunicações, que compartilharam seu conhecimento e experiência de forma dedicada e inspiradora. Suas orientações foram inestimáveis para o desenvolvimento deste trabalho.

Um agradecimento especial aos meus orientadores, o Prof. Davidson e o CF(RM-1) Wagner. Suas orientações, sugestões e incentivo foram cruciais para a conclusão deste trabalho. Sua expertise e dedicação moldaram não apenas o conteúdo deste TCC, mas também a minha compreensão do tema.

À atenção do CMG Huback, Coordenador do Curso de Segurança da Informação e Comunicações, desejo expressar minha sincera gratidão por todo o apoio e orientação fornecidos ao longo do curso. Sua postura cortês e compreensiva foi inestimável, e levarei sua liderança como um exemplo a ser seguido em minha jornada na carreira naval

“A força de uma corrente é a força de seus elos mais fracos. Se um elo se rompe, a corrente se quebra.”

(Arthur Schopenhauer)

ANÁLISE DE VULNERABILIDADE DE SEGURANÇA CIBERNÉTICA EM DISPOSITIVOS MÓVEIS FUNCIONAIS NA MARINHA DO BRASIL

Resumo

Este trabalho destaca a importância da segurança cibernética em dispositivos móveis, com ênfase na proliferação desses aparelhos e nas ameaças associadas a invasões, especialmente em dispositivos de autoridades. Também são identificadas possíveis brechas nas normas institucionais.O estudo revela a acessibilidade surpreendente de ferramentas para ataques cibernéticos, incluindo injeção e engenharia social. Uma simulação demonstra as graves conseqüências desses ataques, incluindo a exposição de dados sensíveis.Vulnerabilidades em aplicativos de fontes aparentemente seguras, como a Google PlayStore, são identificadas.Em resumo, o trabalho ressalta a necessidade de constante proteção em dispositivos móveis funcionais, dada a dependência crescente desses dispositivos e as ameaças em constante evolução.

Palavras-chave: segurança cibernética, dispositivos móveis, invasões, vulnerabilidades, ataques cibernéticos, normas institucionais, simulação, Google PlayStore.

SUMÁRIO

1 INTRODUÇÃO

A revolução digital está provocando uma profunda transformação em nossa sociedade. Nas últimas duas décadas, bilhões de pessoas experimentaram os frutos do acesso exponencial à internet, a rápida adoção das tecnologias de informação e comunicação e as vastas oportunidades econômicas e sociais que o mundo digital tem a oferecer (BRASIL, 2020).

Os avanços vertiginosos na área de tecnologia da informação e comunicação têm resultando na intensa utilização do ciberespaço para uma ampla gama de atividades, incluindo a prestação de serviços pelo governo federal, alinhando-se às tendências globais. Contudo, à medida que o ciberespaço floresce, novas e crescentes ameaças cibernéticas emergem, representando desafios consideráveis tanto para a administração pública quanto para a sociedade em geral (BRASIL, 2020).

Para proteger o ciberespaço de forma eficaz, é necessário um olhar vigilante e liderança capazes de gerenciar mudanças constantes em políticas, tecnologia, educação, regulamentação e cooperação internacional. Nesse contexto, torna-se essencial que o governo, a indústria, as instituições acadêmicas e a sociedade como um todo promovam a inovação tecnológica e adotem tecnologias de vanguarda, mantendo simultaneamente uma vigilância constante sobre questões relacionadas à segurança nacional, economia e preservação da liberdade de expressão (BRASIL, 2020).

As referências anteriores foram extraídas de trechos da Estratégia Nacional de Segurança Cibernética (ENSC) de 2020, que representa uma resposta crucial à crescente importância da segurança cibernética. Esta importância é reconhecida como um componente crítico para a salvaguarda dos interesses nacionais do Brasil no ambiente digital em constante evolução.

Neste contexto, não podemos subestimar a inegável importância dos dispositivos móveis na sociedade moderna. Eles desempenham um papel multifacetado, sendo essenciais para a comunicação, acesso instantâneo a informações, trabalho remoto, transações financeiras, entretenimento e uma gama diversificada de atividades cotidianas. A portabilidade e a conectividade desses dispositivos os consagram como elementos vitais que permeiam tanto a vida pessoal quanto o mundo dos negócios.

Com base nos dados mais recentes fornecidos pela ANATEL até julho de 2023, o Brasil encerrou o mês com um impressionante total de 252 milhões de dispositivos móveis,

registrando a inclusão de 480 mil novos aparelhos durante esse período (Referência: ANATEL, julho de 2023).

Vale destacar que nos dispositivos eletrônicos e computadores, os processadores desempenham um papel essencial no funcionamento. Eles são responsáveis por executar as instruções de software, que são as diretrizes utilizadas por aplicativos e sistemas operacionais para operar. Além disso, o crescente poder de processamento dos dispositivos móveis vem crescendo de maneira exponencial, ocasionando o aumento de uso para diversas ocasiões (Smith, 2020). Os dispositivos atuais frequentemente apresentam poder de processamento de hardware igual ou superior aos considerados "top de linha" de apenas alguns anos atrás. Isso evidencia a rápida evolução tecnológica que impulsiona o constante aprimoramento e desempenho dos dispositivos eletrônicos.

1.1 Apresentação do Problema

Nesse cenário, nos últimos anos o mercado de dispositivos móveis experimentou um crescimento significativo, resultando em uma disseminação amplamente difundida desses aparelhos em uma variedade de contextos. Eles são empregados tanto de maneira casual, em ambientes familiares e rotinas diárias, quanto em ambientes corporativos e grandes instituições. De fato, é plausível supor que o dispositivo a partir do qual você está lendo este texto neste momento seja um desses dispositivos, ou que possua um deles a seu alcance. Porém ele pode ser a porta de entrada de uma série de riscos, tais como a vulnerabilidade à invasão de redes e sistemas, bem como o potencial vazamento de informações confidenciais ou pessoais. Trata-se, portanto, de uma questão de vulnerabilidade que pode se materializar literalmente na palma da mão. O objetivo central deste estudo é realizar uma análisea das vulnerabilidades de segurança da informação que afetam dispositivos móveis utilizados por militares ocupantes de cargos de elevada sensibilidade. Além disso, busca-se demonstrar que mesmo indivíduos em posições de alto nível de liderança, como chefes de Estados, já experimentaram situações em que informações sensíveis foram indevidamente expostas.

1.2 Justificativa e Relevância

Políticos de alta patente, detentores de cargos de grande poder e influência, são alvos constantes de uma ameaça invisível que permeia o mundo moderno: ataques cibernéticos. Enquanto essas figuras desempenham papéis cruciais na condução de nações e decisões de política global, a sua crescente dependência de dispositivos móveis os coloca em uma posição

de vulnerabilidade única no ciberespaço. Esses ataques não apenas expõem informações confidenciais, mas também podem ter conseqüências de longo alcance, afetando a segurança mundial, a estabilidade política e a privacidade pessoal, segue alguns que gostaria de destacar na figura 1 em ordem cronológica.

Figura 1: Ataques Cibernéticos a dispositivos móveis de autoridades mundiais nos últimos 10 anos

Fonte: Autoria Própria

Tanto autoridades exteriores como nacionais sofrem com ataques cibernéticos em seus dispositivos móveis, Os riscos incluem vazamento de informações sensíveis, espionagem política, manipulação e difamação, roubo de identidade, ataques de phishing, ameaças à segurança nacional, acesso a redes internas e escutas. Seguem-se alguns casos conhecidos no território nacional descritos pela figura 2 em ordem cronológica.

Figura 2: Ataques Cibernéticos a dispositivos móveis de autoridades nacionais

Fonte: Autoria própria

Considerando as informações apresentadas, surge a questão de se todos os dispositivos móveis de funcionais na Marinha do Brasil necessitam de uma atenção mais rigorosa devido à extrema importância das informações a eles relacionadas, principalmente o

de autoridades navais. Esta preocupação tem raízes tanto na sensibilidade das informações quanto na crescente dependência de dispositivos móveis funcionais na rotina.

Dispositivos móveis de autoridades sejam eles smartphones ou tablets, podem armazenam informações sensíveis e estratégicas. Além disso, esses dispositivos podem ser acessados remotamente, o que pode resultar na captura de informações, incluindo dados de câmera, áudio e capturas de tela. Essas informações incluem dados críticos relacionados a operações marítimas, segurança nacional e comunicações confidenciais.

Paralelamente, a Marinha do Brasil adota dispositivos móveis funcionais em suas operações para aprimorar a comunicação, a logística e o acesso a informações em tempo real, tanto dentro quanto fora da instituição. A interseção desses dois cenários cria desafios significativos que precisam ser abordados de forma abrangente

1.3 Objetivos

A finalidade deste trabalho é promover a conscientização e a avaliação das vulnerabilidades de cibersegurança em dispositivos móveis funcionais utilizados na Marinha do Brasil.

1.3.1 Objetivo Geral

Este estudo tem como objetivo identificar e analisar possíveis ameaças à segurança da informação, destacando a importância de salvaguardar os dispositivos móveis que desempenham um papel crucial na instituição.

Ao longo deste projeto, será investigada a integridade e a segurança de dispositivos móveis, além de analise de aplicativo disponibilizado por plataforma oficial. O foco estará na identificação de vulnerabilidades potenciais que podem afetar a confidencialidade, integridade e disponibilidade das informações críticas.

A pesquisa destacará a necessidade de medidas proativas de cibersegurança para mitigar essas vulnerabilidades, garantindo a proteção de dados sensíveis, comunicações estratégicas e operações navais em geral. Isso incluirá a análise de políticas de segurança, a conscientização dos usuários e a implementação de práticas de segurança eficazes em dispositivos móveis funcionais.

A Marinha do Brasil tem a responsabilidade de manter a segurança e a eficácia de suas operações, e este trabalho pretende contribuir para o fortalecimento das defesas cibernéticas,

garantindo que os celulares funcionais utilizados pela instituição sejam uma ferramenta segura e confiável.

1.3.2 Objetivos Específicos

Para cumprir o objetivo geral deste trabalho, as seguintes etapas serão desenvolvidas:

- Identificar as vulnerabilidades de cibersegurança em dispositivos móveis;
- Analisar as práticas de segurança existentes na Marinha em relação aos dispositivos móveis funcionais;
- Elaborar um ataque de vulnerabilidade de dispositivos móveis demonstrando a facilidade de ser criar um ataque direcionado com aplicativos de fácil acesso;
- Realizar testes de vulnerabilidade de aplicativos da instituição disponível em plataformas digitais; e
- Sensibilizar os membros da Marinha sobre a importância da segurança cibernética e promover a adoção de práticas de segurança por parte dos usuários.

2 REFERENCIAL TEÓRICO

O presente capítulo tem por alicerce anunciar os conceitos imprescindíveis para o correto entendimento das seções subseqüentes. Serão abordados conceitos e idéias necessários que permitam a compreensão adequada da implementação da análise de vulnerabilidade a sistemas Android e IOS, além da melhor compreensão a simulação um dispositivo de ataque a dispositivo Android que será realizado e a análise de vulnerabilidade de aplicativo oriundo da plataforma Google Play Store.

2.1 Uso de Dispositivos Móveis na Marinha

No contexto da instituição naval, cabe o destaque das seguintes publicações como referência para uso de dispositivos móveis:

- DGMM-540: Normas de Tecnologia da Informação da Marinha; e
- MATERIALMARINST Nº 22-04: Utilização de dispositivos móveis inteligentes e celulares.

Este subcapítulo será dedicado à análise das informações presentes na norma DGMM-540 (Diretoria-Geral de Material da Marinha, 2019). Sendo assim, os dispositivos móveis podem ser dos seguintes tipos:

- -Smartphones;

- Tablet; e
- -Smartwatch.

Sendo categorizados em três tipos: pessoais, funcionais e de pessoal extra-MB. Os dispositivos pessoais são aqueles de propriedade dos membros da Marinha do Brasil (MB). Os dispositivos funcionais são de propriedade da MB, enquanto os dispositivos de pessoal extra-MB pertencem a pessoas não afiliadas à MB.

A Segurança da Informação Cibernética (SIC) da Marinha do Brasil é vital para proteger a disponibilidade, integridade, confidencialidade e autenticidade dos dados e serviços utilizados por seus usuários. As ameaças à SIC podem comprometer esses elementos essenciais por meio da exploração de vulnerabilidades. Tais vulnerabilidades podem surgir de maneira intencional ou não, desde a fase inicial de concepção de hardware e software embarcados, até a falta de conhecimento ou conscientização em relação à SIC por parte dos usuários, bem como a ausência de procedimentos que incorporem as boas práticas de segurança.

Tendo as seguintes causas:

- Operação inadequada;
- Perda, roubo ou furto;
- Interceptação de voz e dados; e
- Execução de códigos maliciosos.

A exposição da ameaças e vulnerabilidades pode resultar no vazamento de informações sigilosas. Uma vez que essas informações sejam compartilhadas na Internet ou acessadas por terceiros não autorizados, perde-se o controle sobre suas cópias, divulgação e conteúdo. As conseqüências disso podem ser profundas, incluindo o comprometimento da confidencialidade e integridade de dados sensíveis, o que pode resultar em sérias implicações para a segurança e privacidade das informações.

Sobre os Dispositivos moveis funcionais, deverão ser devidamente cadastrado e controlado pela Organização Militar (OM) através do Termo de Recebimento de Estação de Trabalho (TRE). (ver Anexo I para o modelo do Termo).Esse processo garante uma identificação única para cada dispositivo e estabelece a responsabilidade pelos usuários autorizados. Portanto, é necessário que seja gerado um TRE específico para cada usuário, ou no caso de dispositivos compartilhados, um TRE para cada conjunto de usuários. Importante destacar que não é permitido o armazenamento de dados sigilosos nos dispositivos móveis, além de ser vedado o uso durante missão operativa.

Sendo que os militares e servidores civis da Marinha do Brasil deverão ser orientados sobre os procedimentos de segurança relacionados aos dispositivos que lhes são fornecidos. Isso deve ser feito por meio da assinatura de um Termo de Responsabilidade Individual (TRI) (ver Anexo II para o modelo do Termo) da Organização Militar (OM) à qual pertencem. A falta de conhecimento sobre esses procedimentos não será aceita como justificativa em casos de uso indevido.

De acordo com a publicação, No âmbito da segurança dos dispositivos móveis empregados para acesso aos sistemas corporativos, tais como o serviço de correio eletrônico e o Portal da Marinha, é de suma importância a observância das seguintes diretrizes:

- Evitar armazenar informações confidenciais, agendas, anotações e contatos de pessoal da Marinha em serviços de nuvem privada, como o iCloud, Dropbox, Google Drive, entre outros;
- Desativar o serviço de localização para todos os aplicativos, garantindo maior privacidade;
- Restringir a instalação de aplicativos exclusivamente àqueles disponibilizados pela loja oficial do fabricante do sistema operacional;
- Abster-se de realizar o procedimento conhecido como "jailbreak" ou "rooting", que envolve o uso de ferramentas não homologadas para obter controle de administração sobre o aparelho;
- Desabilitar a capacidade do dispositivo móvel de se conectar automaticamente a redes sem fio, protegendo contra conexões não autorizadas;
- Desativar o uso da tecnologia Bluetooth, mitigando possíveis riscos de segurança;
- Desativar a função de compartilhamento de ponto de acesso à rede, restringindo o acesso não autorizado;
- Fortalecer a segurança do dispositivo, habilitando senhas de proteção. Sempre que a tecnologia do dispositivo permitir, é recomendável utilizar senhas mais complexas do que as tradicionais de 4 dígitos numéricos;
- Reforçar a segurança do dispositivo, habilitando a proteção de tela;
- Proteger o acesso ao cartão SIM habilitando o uso de um PIN (Número de Identificação Pessoal) do cartão SIM;
- Onde disponível, instalar soluções antivírus adequadas ao sistema operacional para fortalecer a segurança do dispositivo;
- Manter tanto o sistema operacional quanto as aplicações constantemente atualizados,

garantindo a aplicação de correções de segurança; e

- Em casos de perda, roubo ou extravio do dispositivo móvel funcional, garantir o apagamento seguro de informações sensíveis, impedindo o acesso não autorizado a dados confidenciais.

2.2 Segurança da Informação

Conforme estipulado pela Lei de Acesso à Informação, o termo "informação" é precisamente descrito como "dados passíveis de serem empregados na criação e compartilhamento do saber, independentemente do meio ou formato em que estejam registrados (BRASIL, Lei nº 12.527/2011, Art. 4).

A segurança da informação é um conjunto de medidas e ações que visam proteger as informações contra acesso, uso, divulgação, modificação, destruição ou perda não autorizados. Esses princípios são fundamentais para garantir a segurança da informação.

2.2.1 Confiabilidade

De acordo com Lyra (2008), a confiabilidade da informação é essencial para o funcionamento de qualquer organização. Ela é definida como:

"A confiabilidade da informação é um conceito que garante que a informação estará disponível para os usuários autorizados quando necessário, e que será correta e completa."

Para garantir a confiabilidade da informação, é importante implementar medidas de segurança que protejam contra acesso não autorizado, uso indevido, divulgação não autorizada, modificação não autorizada e destruição não autorizada.

2.2.2 Integridade

A integridade da informação é fundamental para garantir sua confiabilidade. Lyra (2008) a define da seguinte forma:

"A integridade da informação é um conceito que garante que a informação não será alterada ou destruída sem autorização."

Para assegurar a integridade da informação, é crucial implementar medidas de segurança que protejam contra alterações não autorizadas, destruição não autorizada e falsificação.

2.2.3 Confidencialidade

A confidencialidade da informação é crucial para proteger a privacidade e a propriedade intelectual. Segundo Lyra (2008):

"A confidencialidade da informação é um conceito que garante que a informação não será divulgada a pessoas não autorizadas."

Para manter a confidencialidade da informação, é imperativo implementar medidas de segurança que protejam contra acesso não autorizado.

2.2.4 Autenticidade

A autenticidade da informação é necessária para garantir sua confiabilidade. Nas palavras de Lyra (2008):

"A autenticidade da informação é um conceito que garante que a informação é originária da fonte que afirma ser."

Para garantir a autenticidade da informação, é importante implementar medidas de segurança que protejam contra adulteração e falsificação.

2.2.5 Disponibilidade

Lyra (2008) ressalta que a disponibilidade da informação é essencial para o funcionamento normal das operações e a define da seguinte maneira:

"A disponibilidade da informação é um conceito que garante que a informação estará disponível para os usuários autorizados quando necessário."

Para garantir a disponibilidade da informação, é fundamental implementar medidas de segurança que protejam contra perda, destruição ou indisponibilidade.

É crucial que os aspectos técnicos relacionados à informação e os princípios de segurança estejam em conformidade com a legislação relevante, a qual pode variar de acordo com o estado, país, entre outros.

Dentro do contexto deste trabalho, é essencial compreender o que define um acesso não autorizado, incluindo

Os acessos considerados válidos são aqueles efetuados por profissionais que possuem uma conta devidamente autorizada e válida em um sistema de computador, com o propósito de executar atividades previamente acordadas. Qualquer outra forma de acesso, incluindo a apropriação indevida de senhas, entrada furtiva obtida por meio da exploração de vulnerabilidades de segurança no sistema (seja local ou remota), modificações não autorizadas de privilégios (como a tentativa de acesso à máquina como conta com privilégios

de acesso elevados sem autorização), ou a introdução de qualquer tipo de vírus, é categorizada como acesso não autorizado (Masiero em 2013, p. 128).

2.3 Métodos de Ataque

Assim como ter o conhecimento de quem efetua algum tipo de ataque é indispensável ter conhecimento das práticas que comprometem a segurança da informação nos dispositivos móveis. Dentre eles, é possível destacar:

2.3.1 Phishing

O phishing é um tipo de ataque associado à engenharia social, cujo objetivo é induzir as vítimas a revelarem informações pessoais, como senhas e números de contas, por meio de mensagens fraudulentas. A vítima muitas vezes é levada a acreditar que está interagindo com uma fonte confiável. (CERT.BR, 2012, p. 6).

2.3.2 Trojan Horse (Cavalo de Troia)

O Trojan Horse, ou cavalo de Troia, é um programa que, além de executar funções aparentemente benignas, realiza ações maliciosas sem o conhecimento do usuário. Embora possa parecer inofensivo, um cavalo de Troia pode abrir portas para invasões e comprometer a segurança do sistema (CERT.BR, 2012, p. 28).

2.3.3 Spyware

O spyware é um programa espião que observa as atividades do sistema, coletando informações e, por vezes, roubando dados sensíveis para terceiros. Esse tipo de software ameaça a privacidade e a segurança dos dados armazenados em um sistema (CERT.BR, 2012, p. 27).

2.3.4 Backdoor

Uma "backdoor" (porta dos fundos, em português) é um termo usado em segurança da informação para se referir a uma forma de acesso oculto ou não autorizado a um sistema, aplicativo ou dispositivo de computação. Backdoors são normalmente criadas por desenvolvedores, administradores de sistema ou invasores com a intenção de permitir o acesso posterior ao sistema sem a necessidade de autenticação convencional. Essa porta dos fundos é uma brecha intencional que pode ser usada para contornar medidas de segurança.

As backdoors podem ser usadas para fins legítimos, como facilitar a manutenção de sistemas, ou com propósitos maliciosos, como permitir a entrada não autorizada em sistemas alheios. Elas podem ser implementadas em diversos níveis, desde o sistema operacional até aplicativos específicos.(Erickson, 2008)

2.3.5 Vírus

Os vírus de computador são programas maliciosos projetados para causar danos em sistemas computacionais, alterando seu funcionamento e comprometendo a disponibilidade das informações. Eles têm a capacidade de se multiplicar e se espalhar para afetar outros sistemas (Wiliam, 2008).

2.3.6 Engenharia Social

A engenharia social é uma técnica que envolve a manipulação de pessoas para que realizem ações ou revelem informações confidenciais. Essa abordagem explora vulnerabilidades humanas, como curiosidade, confiança ou medo, e é freqüentemente utilizada por cibercriminosos com o objetivo de obter acesso não autorizado a sistemas ou informações. (Clara, 2021)

Por meio da engenharia social, os atacantes podem empregar táticas como o phishing, que consiste no envio de e-mails ou mensagens falsas que aparentam ser provenientes de fontes confiáveis, com a finalidade de coletar senhas ou dados pessoais. Além disso, podem realizar chamadas telefônicas fraudulentas, nas quais se fazem passar por funcionários de organizações respeitáveis, visando a obtenção de informações confidenciais.

Portanto, a engenharia social representa uma técnica de manipulação psicológica, que busca explorar a confiança e a ingenuidade das pessoas para obter vantagens indevidas.

Ao compreender os recursos freqüentemente explorados pelos invasores, adquire-se uma visão mais clara dos riscos aos quais os dispositivos móveis estão expostos. No entanto, ao implementar mecanismos de segurança adequados, é possível reduzir ao mínimo, ou até mesmo eliminar, essas vulnerabilidades.

2.4 Normativas Jurídicas no Combate a Acessos Não Autorizados

No cenário brasileiro, a legislação abrange atualmente a classificação de ações de acesso não autorizado. A Lei 12.737/2012, em seu Art. 154-A, estabelece a definição de invasão de dispositivos informáticos alheios, estejam eles conectados ou não à rede de computadores. Tal invasão ocorre mediante violação indevida de mecanismos de segurança,

com a finalidade de obter, adulterar ou destruir dados ou informações sem a devida autorização expressa ou tácita do titular do dispositivo, ou até mesmo de instalar vulnerabilidades com o intuito de obter vantagem ilícita. As penalidades associadas a essa conduta incluem detenção de 3 (três) meses a 1 (um) ano, além de multa (BRASIL, 2012, p. 1).

Adicionalmente, o Marco Civil da Internet no Brasil busca a consolidação de princípios, garantias, direitos e deveres para todos os usuários da rede. No que tange à preservação da privacidade, a legislação reforça a importância da proteção e garante o respeito à intimidade, vida privada e ao sigilo das comunicações (BRASIL, 2014, p. 2).

Portanto, considerando a importância crítica da informação e a necessidade de assegurar sua integridade e confidencialidade, torna-se imprescindível a adoção de um conjunto abrangente de medidas. Essas medidas devem abranger aspectos técnicos, administrativos, legais e políticos, e devem ser observadas por todos aqueles que manuseiam ou detêm informações, garantindo eficácia na proteção e preservação desses dados.

2.5 Arquitetura dos Sistemas Operacionais dos Dispositivos Móveis

Segundo Jobs (2007, p. 128), "O sistema operacional é a fundação sobre a qual todos os outros programas são construídos."

No Brasil destaca-se por sua considerável preferência pelo sistema operacional Android em comparação com o iOS. Mais de 81% da população opta pelo Android, enquanto cerca de 18% utiliza o sistema iOS, restando apenas 1% dos usuários que adotam outro sistema operacional (ANATEL, julho de 2023). Essa disparidade revela uma clara predominância do Android no mercado de dispositivos móveis do país. Representado estatisticamente pela Figura 3.

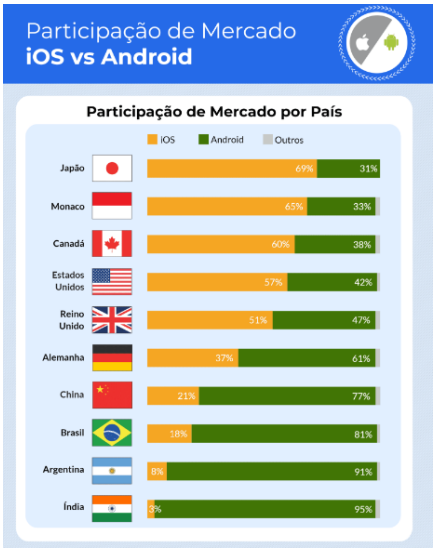

Figura 3: Comparativo de mercado dos Sistemas Operacionais em alguns países

Fonte: Statista (2023)

O sistema operacional Android possui uma arquitetura de software em camadas que é projetada para fornecer uma base sólida para a execução de aplicativos e serviços em dispositivos móveis. A arquitetura do Android é baseada principalmente em componentes de código aberto e é altamente personalizável pelos fabricantes de dispositivos (Android Developers, 2023). Segue-se uma visão geral das principais camadas da arquitetura do Android, baseada no artigo "Arquitetura da plataforma" do projeto Android Develops e representado pela figura 4.

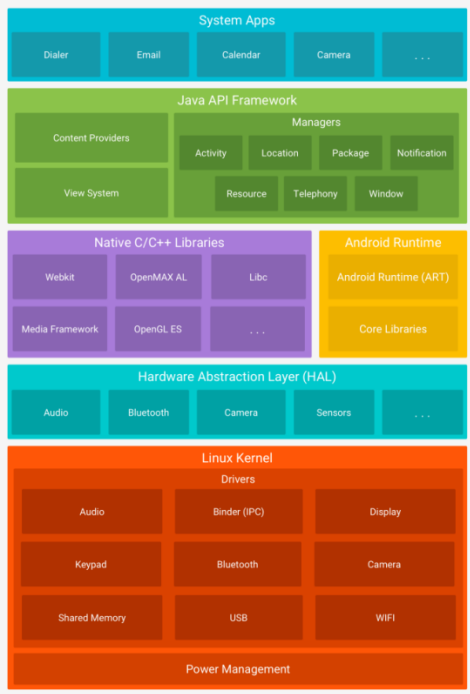

Figura 4: Representação em camadas da arquitetura Android

Fonte: Google(2023)

- **Kernel do Linux:** O Android utiliza o kernel do Linux como base, fornecendo funcionalidades essenciais de sistema operacional, como gerenciamento de hardware, gerenciamento de memória, gerenciamento de processos e suporte a drivers de dispositivo.
- **Camada de Abstração de Hardware (HAL - Hardware AbstractionLayer):** Esta camada atua como uma interface entre o kernel do Linux e o restante do sistema operacional. Ela fornece uma abstração para os drivers de hardware específicos do dispositivo, permitindo que o Android seja compatível com uma ampla variedade de hardware.
- **AndroidRuntime (ART):** Anteriormente, o Android usava a máquina virtual Dalvik (DVM), mas a partir do Android 5.0, o AndroidRuntime (ART) se tornou o padrão. ART é uma máquina virtual que executa aplicativos Android convertendo-os em código nativo durante a instalação, o que resulta em um desempenho mais eficiente.
- **Estrutura de Aplicativos:** Esta camada inclui os principais componentes para executar aplicativos Android. Isso inclui as bibliotecas padrão do Android, como a biblioteca Java Core, e as APIs que os desenvolvedores de aplicativos usam para criar aplicativos.
- **Camada de Aplicativos:** Nesta camada, encontram-se os aplicativos do usuário final, incluindo aplicativos nativos do Android (por exemplo, telefone, mensagens, navegador) e aplicativos de terceiros baixados da Google Play Store ou de outras fontes.
- **Serviços do Sistema Android:** Esta camada inclui serviços centrais do sistema, como o gerenciador de pacotes (responsável pela instalação e atualização de aplicativos), o gerenciador de energia, o gerenciador de notificações, o sistema de gerenciamento de janelas e muito mais.
- **Interface de Aplicativos (APIs):** As APIs do Android são fornecidas para permitir que os desenvolvedores criem aplicativos que interajam com o sistema operacional e com outros aplicativos. Isso inclui acesso a recursos como a câmera, sensores, armazenamento e muito mais.
- **Serviços do Google Play:** Embora não seja estritamente parte do Android em si, muitos dispositivos Android incluem serviços do Google Play, como a loja de

aplicativos Google Play e serviços relacionados, como autenticação do Google e armazenamento em nuvem.

A arquitetura do sistema operacional iOS é um tópico complexo que pode ser difícil de entender. Para ajudar os desenvolvedores a entender a arquitetura do iOS, a Apple oferece uma exposição detalhada no site Apple Developer. A exposição fornece uma visão geral das quatro camadas principais da arquitetura do iOS: núcleo do sistema, camada de serviços, camada de mídia e camada de núcleo.

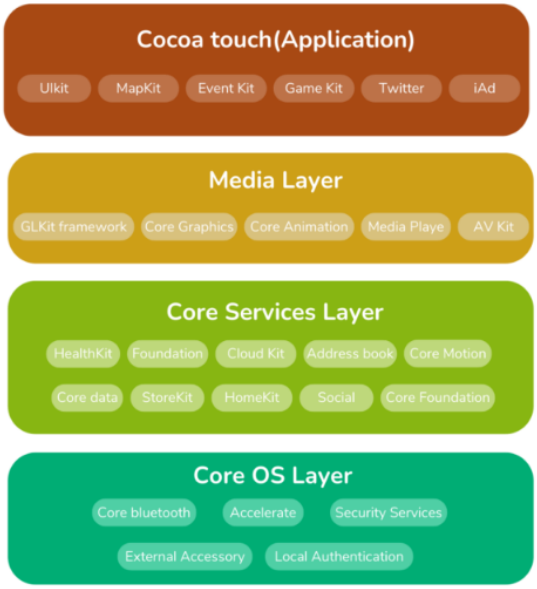

Figura 5: Representação em camadas da arquitetura iOS

Fonte: Red Fox Security (2022)

A arquitetura do sistema operacional iOS, desenvolvido pela Apple, difere do Android, pois é projetada exclusivamente para dispositivos móveis e é altamente controlada pela Apple. Aqui está uma visão geral da arquitetura do iOS tirada do site Apple Developer:

- **Núcleo do Sistema (Core OS):** Esta camada é a base do iOS e fornece funcionalidades essenciais, incluindo o kernel do sistema operacional (baseado no kernel do Unix), serviços de segurança, acesso a hardware e comunicação de baixo nível.
- **Camada de Serviços**: Esta camada fornece serviços essenciais para o sistema, como serviços de localização, serviços de notificação e serviços de rede.

- **Camada de Mídia (Media Layer):** Aqui estão as bibliotecas e frameworks relacionados a áudio, vídeo e gráficos. Isso inclui bibliotecas para reprodução de mídia, gravação de áudio e vídeo, manipulação de imagens e processamento de gráficos.
- **Camada de Núcleo (Core Services):** Essa camada fornece serviços fundamentais para o sistema, incluindo acesso a bancos de dados, suporte a redes e serviços de localização. Ela também inclui a API de iCloud para armazenamento em nuvem e sincronização de dados.
- **Bibliotecas e Frameworks**: Essas bibliotecas e frameworks fornecem funcionalidades específicas para o desenvolvimento de aplicativos iOS. Alguns exemplos incluem UIKit (para a interface do usuário), Core Data (para gerenciamento de dados), MapKit (para mapas) e muitos outros.
- **Camada de Aplicativos (ApplicationLayer):** Nesta camada, encontram-se os aplicativos nativos do iOS, como Mensagens, Safari, Fotos, Mapas e muitos outros. Além disso, inclui aplicativos de terceiros baixados da AppStore.
- **App Frameworks:** Estas são estruturas que permitem que os desenvolvedores criem aplicativos iOS. Isso inclui o UIKit para a criação de interfaces de usuário, o SwiftUI (introduzido mais recentemente) e muitos outros.
- **iOS SDK (Software Development Kit):** O iOS SDK fornece ferramentas, APIs e recursos para desenvolvedores criarem aplicativos iOS. Isso inclui o Xcode (ambiente de desenvolvimento integrado), simulador iOS para testes, depuração e perfis de desenvolvimento.
- **AppStore:** A AppStore é a loja oficial de aplicativos da Apple, onde os usuários podem baixar aplicativos e jogos desenvolvidos para iOS.

A arquitetura do iOS é altamente controlada pela Apple para garantir consistência, segurança e desempenho em todos os dispositivos iOS. Isso resulta em um ecossistema coeso, onde a Apple tem um controle estrito sobre os aplicativos que entram na AppStore e como o sistema operacional é atualizado em dispositivos iOS. Essa abordagem ajuda a garantir um alto nível de qualidade e segurança para os usuários do iOS.

2.6 CVE-2022-22822

Acordo Mitre Cooporation, O CVE-2022-22822 é uma vulnerabilidade de software que pode ser usada para hackear dispositivos Android. Essa vulnerabilidade está presente em um módulo chamado Expat, que é usado para processar arquivos XML.

Um atacante pode explorar essa vulnerabilidade enviando um documento XML malicioso para um dispositivo Android via aplicaitvo infectado. O documento XML malicioso deve conter um número excessivo de atributos com nomes longos. Quando o dispositivo Android tenta processar esses atributos, ele pode causar um estouro de buffer, o que pode levar à execução de código arbitrário no dispositivo.

Isso significa que um atacante pode usar essa vulnerabilidade para instalar malware no dispositivo Android, roubar dados ou até mesmo assumir o controle do dispositivo.

A vulnerabilidade pode ser explorada por um atacante para executar código arbitrário no sistema afetado. Isso pode levar a uma variedade de ataques, incluindo:

- Ataques de roubo de dados: O atacante pode usar o código arbitrário para roubar dados do sistema afetado, como senhas, números de cartão de crédito e outros dados confidenciais;
- Ataques de negação de serviço: O atacante pode usar o código arbitrário para interromper o funcionamento do sistema afetado; e
- Ataques de malware: O atacante pode usar o código arbitrário para instalar malware no sistema afetado.

3 METODOLOGIA

Neste capítulo, descreveremos a metodologia adotada na condução desta pesquisa. A metodologia desempenha um papel fundamental ao estabelecer o processo sistemático que empregamos para coletar, analisar e interpretar os dados essenciais com o intuito de abordar as perguntas de pesquisa formuladas e atingir os objetivos estabelecidos. A escolha da abordagem metodológica é de importância crítica para assegurar a validade e a confiabilidade dos resultados obtidos.

3.1 Classificação da Pesquisa

A metodologia aplicada nesta pesquisa é composta por uma análise prática de aplicativo oriundo de plataforma original e simulação de ataques cibernéticos, além de uma abrangente revisão bibliográfica. Essas etapas se mostraram essenciais para a obtenção de insights valiosos e aprofundados relacionados à segurança cibernética. A análise prática e

simulação de ataques cibernéticos proporcionaram uma compreensão prática das vulnerabilidades e riscos associados a dispositivos móveis funcionais.

Simultaneamente, a análise bibliográfica foi conduzida para embasar nossa pesquisa em conhecimento acadêmico e boas práticas estabelecidas na área de segurança cibernética. Essa revisão bibliográfica abordou teorias, modelos, técnicas e abordagens relevantes que contribuíram para a fundamentação e contextualização dos resultados obtidos na análise prática.

A combinação dessas abordagens metodológicas permitiu a realização de uma pesquisa abrangente e robusta, cujos resultados são apresentados ao longo deste trabalho.

3.1.1 Quanto aos fins

O objetivo principal desta pesquisa é analisar e destacar a importância das segurança cibernética em dispositivos móveis, demonstrando que a vulnerabilidade nessa área é de extrema relevância para nossa instituição. Por meio desta investigação, busca-se conscientizar sobre os desafios e as ameaças que a proliferação de dispositivos móveis traz consigo. O foco está na segurança de informações sensíveis, na proteção de autoridades e no combate às brechas nas normas institucionais que podem ser exploradas. Além disso, a pesquisa visa evidenciar a facilidade de acesso a ferramentas para ataques cibernéticos, como injeção e engenharia social, bem como a existência de vulnerabilidades em aplicativos de fontes aparentemente seguras. Em última análise, o propósito é promover uma mudança de mentalidade e estimular a adoção de medidas eficazes para proteger os dispositivos móveis funcionais na Marinha do Brasil.

3.1.2 Quanto aos meios

Para estabelecer uma base sólida para esta pesquisa, empreendemos uma ampla revisão bibliográfica. Consultamos diversas fontes, incluindo artigos científicos, livros, relatórios técnicos e documentos governamentais, a fim de compreender os princípios técnicos e teóricos relacionados às vulnerabilidades comuns em dispositivos móveis em geral, considerando sua possível ocorrência em dispositivos da nossa instituição. Também investigamos ferramentas de computação comumente utilizadas em ataques cibernéticos reais, que foram adaptadas e testadas em ambientes controlados, juntamente com ferramentas de análise de vulnerabilidades de aplicativos. Essa pesquisa ampla e aprofundada proporcionou uma compreensão abrangente das ameaças cibernéticas e vulnerabilidades que dispositivos

móveis funcionais podem enfrentar, fornecendo a base necessária para a análise crítica das questões de segurança cibernética na Marinha do Brasil e a formulação de estratégias de proteção eficazes.

4 ANÁLISE DAS NORMAS DA MARINHA DO BRASIL SOBRE DISPOSITIVOS MÓVEIS

No contexto da DGMM-540, que rege as normas para o uso de depósitos móveis na instituição, é relevante destacar os seguintes pontos que serão abordados em nosso estudo.

4.1 Atualizações de Sistemas Operacionais

"Manter tanto o sistema operacional quanto as aplicações constantemente atualizados, garantindo a aplicação de correções de segurança" (DGMM-540, 2019).

Embora a importância de manter tanto o sistema operacional quanto as aplicações constantemente atualizados, garantindo a aplicação de correções de segurança, seja indiscutível, é crucial reconhecer que essa prática pode ser desafiadora em modelos mais antigos de dispositivos móveis. Dispositivos Android e iOS mais antigos, por exemplo, muitas vezes enfrentam limitações de capacidade de memória que podem dificultar a aplicação de atualizações, além de restrições politicas do fabricante. Além disso, não podemos presumir que todos os usuários tenham a capacidade ou o conhecimento necessário para manter seus dispositivos atualizados. Portanto, embora a atualização seja essencial, é necessário considerar as barreiras práticas que alguns usuários podem enfrentar para garantir a segurança de seus dispositivos.

De acordo com a Apple, as atualizações de software para seus iPhones por um período de cinco anos, a partir da data de lançamento do dispositivo. Isso significa que os smartphones da marca lançados em 2017 ou mais tarde são elegíveis para atualizações de software. Sendo assim, somente os lançados após o modelo Xr possuem atualizações do Sistema Operacional disponíveis.

Sobre o Android, conforme afirmado pelo Google, fabricante do sistema operacional geralmente recebem atualizações de segurança por um período de três anos após o lançamento inicial do dispositivo. Além disso, algumas fabricantes estendem esse suporte por mais tempo, chegando a oferecer atualizações por até cinco anos.

No entanto, é importante observar que dispositivos mais antigos, com hardware limitado, podem ter um ciclo de suporte mais curto, uma vez que não suportam as versões mais recentes do Android devido as limitações de desempenho e armazenamento.

Dessa forma, os fabricantes não enviam os patches de segurança, que são correções de software enviadas pelos fabricantes de telefones, para corrigir falhas de segurança identificadas em seus sistemas operacionais. Essas correções são essenciais para manter os dispositivos protegidos contra ameaças cibernéticas. Embora os usuários freqüentemente recebam esses patches sem notar, eles desempenham um papel fundamental na segurança de seus telefones.

Usar um telefone sem suporte e, portanto, sem patches de segurança, é considerado arriscado. Vulnerabilidades críticas de segurança tornam-se de conhecimento público com freqüência, e dispositivos desatualizados podem ser explorados por hackers. Isso pode resultar no comprometimento de informações pessoais e empresariais, incluindo e-mails, contatos, dados bancários e conversas telefônicas. (Lanxon, 2022)

Nesse sentido, dispositivos móveis que possuem mais de 5 anos de fabricação ou com alguma restrição de desempenho e armazenamento podem ser considerados pontos vulneráveis em termos de segurança, devido às lacunas de proteção decorrentes da ausência de atualizações. Essa vulnerabilidade será demonstrada no Capítulo 5 deste trabalho.

4.2 Sobre instalação de Aplicativos e permissões de acesso

“Restringir a instalação de aplicativos exclusivamente àqueles disponibilizados pela loja oficial do fabricante do sistema operacional.” (DGMM-540, 2019).

Restringir a instalação de aplicativos exclusivamente àqueles disponibilizados pela loja oficial do fabricante do sistema operacional tem como objetivo principal garantir um nível mais elevado de segurança. No entanto, é importante reconhecer que mesmo as lojas oficiais não estão imunes a problemas de segurança. Podendo ser explorada as vulnerabilidades de segurança dos próprios aplicativos. O malware pode explorar falhas de segurança em aplicativos legítimos, aproveitando-se de vulnerabilidades de software existentes para se instalar e executar em dispositivos dos usuário. Tendo como destaque os Dados externos em consultas SQL (CWE-89): Essa vulnerabilidade é uma forma de injeção de SQL, o que significa que os atacantes conseguem injetar comandos SQL maliciosos em um aplicativo ou sistema.

Tendo um impacto significativo na segurança do sistema, pois permitem que os atacantes executem ações não autorizadas. Isso pode variar desde a exposição de dados

confidenciais até o controle total do sistema comprometido. Essa vulnerabilidade será relatada no Capítulo 6 deste trabalho.

5 SIMULAÇÃO DE ATAQUE DE INJEÇÃO DE CÓDIGO

Neste capítulo será apresentada uma análise sobre uma simulação de Ataque de Injeção de Código realizada em um ambiente baseado em máquinas virtuais, através do software Oracle VM VirtualBox com infecção através de aplicativo malicioso utilizando Engenharia Social. Na primeira máquina virtual foi utilizado o Sistema Operacional Linux e a segunda foi utilizado o Sistema Operacional Android. Para desempenhar o papel do atacante foram utilizadas as ferramentas presentes no SO Kali Linux versão 2023.3, que é baseado no sistema Debian. E, para representar o papel da vítima, foi escolhido uma máquina virtual com o Sistema Operacional Android 9 (Pie), representanda por um Samsung S9, smartphone lançado em 2018 e atualmente ainda comercializado, toda via, o suporte para atualização do seu sistema operacional foi encerrado em 2021, devido limitação na capacidade de armazenamento e executada pelo Genymotion. As duas máquinas foram configuradas na mesma rede local como o IP 192.168.56.1/24.

Os Sistemas Operacionais e softwares utilizados na simulação podem ser encontrados e baixados nos seguintes endereços:

- Oracle VM VirtualBox, disponível em https://www.virtualbox.org/wiki/Downloads
- SO Kali Linux, disponível em https://www.kali.org/downloads/
- SO Android, disponível em https://genymotion.com/download/

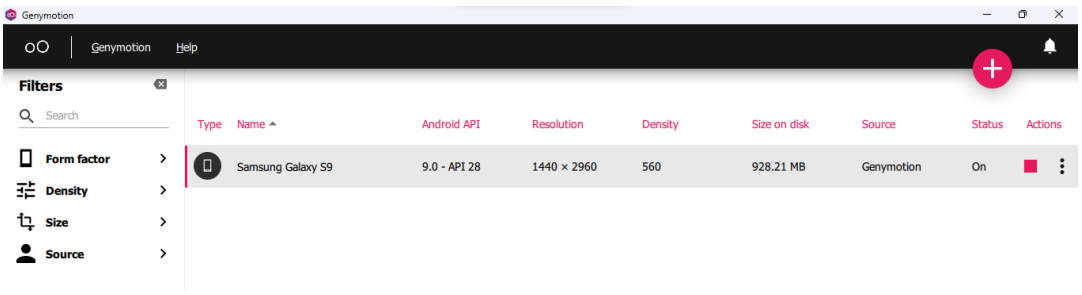

Figura 6: Genymotion com emulador do Samsung S9 utilizando o Android 9 (Pie)

Fonte: Próprio Autor

Figura 7: Emulador Samsung

Fonte: Próprio Autor

5.1 Simulação do Ataque

Para simulação foi escolhido a técnica de ataque de injeção de código baseado na CVE-2022-22822, que é uma vulnerabilida que afeta o Android 9 e versões anteriores. Sendo utilizando o seguinte comando visando gerar um aplicativo Android malicioso que contém um payload do Meterpreter* (O payload do Meterpreter é uma ferramenta de acesso remoto que pode ser usada pelo invasor para controlar o dispositivo Android)

```
┌──(root㉿kali)-[~]
└─# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.56.1 LPORT=4444 R > /var/www/html/MarinhadoBrasil.apk
```

Figura 8: Comando *msfvenom* no prompt de comando Kali Linux

Fonte: Próprio Autor

5.1.1 Primeiro comando tem os seguintes argumentos

- **-p:** O payload do Meterpreter que será usado. Neste caso, o payload é android/meterpreter/reverse_tcp.
- **LHOST:** O endereço IP do host local que o payload do Meterpreter usará para se conectar. Neste caso, o endereço IP é 192.168.56.1.
- **LPORT:** A porta que o payload do Meterpreter usará para se conectar. Neste caso, a porta é 4444, geralmente utilizadas para fins educativos.
- **R:** O modo de saída. Neste caso, o modo de saída é R, que significa que o payload

será gerado em um arquivo.

- **/var/www/html/MarinhadoBrasil.apk:** O arquivo onde o payload será gerado.

Quando este comando é executado, ele gera um aplicativo Android malicioso chamado MarinhadoBrasil.apk. O aplicativo malicioso contém o payload do Meterpreter, que é executado no dispositivo Android quando o usuário instala o aplicativo malicioso.

5.1.2 Segundo comando

Figura 9: Comando *msfconsole*

Fonte: Próprio Autor

O comando *msfconsole* é usado para iniciar a interface de linha de comando do Metasploit Framework* (O Metasploit Framework é uma plataforma de teste de penetração que pode ser usada para explorar vulnerabilidades em sistemas e aplicativos.).Esse comando abre uma interface de linha de comando que permite ao usuário executar comandos para explorar vulnerabilidades.

Saída do Comando *msfconsole*

Figura 10: Saída após comando *msfconsole*

Fonte: Próprio Autor

- **metasploit v6.3.31-dev**: indica a versão do Metasploit Framework que está sendo executado.
- **2346 exploits - 1217 auxiliary - 413 post**: indica o número de exploits, módulos auxiliares e módulos de pós-exploração disponíveis no Metasploit Framework.
- **1390 payloads - 46 encoders - 11 nops**: indica o número de payloads, encoders e nops disponíveis no Metasploit Framework.

- **9 evasion**: indica o número de técnicas de evasão disponíveis no Metasploit Framework.

A dica do Metasploit informa ao usuário que ele pode usar o comando *resource* para executar comandos de um arquivo.

A documentação do Metasploit informa ao usuário onde ele pode encontrar a documentação do Metasploit Framework no link: https://docs.metasploit.com/

5.1.3 Terceiro comando

Figura 11: Comando definindo o payload

Fonte: Próprio Autor

O comando define o payload, que será o código que será executado no dispositivo de destino,. a ser usado pelo Metasploit Framework. O payload é o

Neste caso, o payload definido é android/meterpreter/reverse_tcp. Este payload é um payload do Meterpreter para dispositivos Android. O Meterpreter é uma ferramenta de acesso remoto que permite ao usuário controlar o dispositivo de destino.

Sendo o payload *android/meterpreter/reverse_tcp* usado para conexão reversa. Isso significa que o dispositivo de destino se conectará ao host do invasor

5.1.4 Quarto comando

Figura 12: Comando selecionado o exploit multi/handler

Fonte: Próprio Autor

O comando é usado para selecionar o exploit *multi/handler*. Sendo um exploit genérico que pode ser usado para explorar uma variedade de vulnerabilidades.

5.1.5 Quinto e Sexto comandos

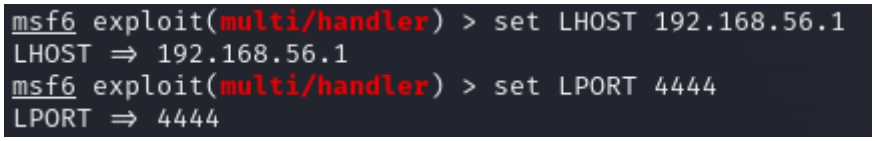

Figura 13: Comando especificando o endereço IP e porta Host do invasor

Fonte: Próprio Autor

O endereço IP e a porta do host do invasor foram especificados usando os parâmetros *LHOST* e *LPORT*, respectivamente.

5.1.6 Sétimo comando

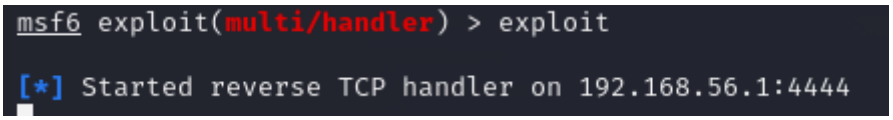

Figura 14: Comando *exploit*

Fonte: Próprio Autor

O comando *exploit* é usado para executar o *exploit multi/handler*.

A saída indica que o exploit iniciou um manipulador TCP reverso na porta 4444 do endereço IP 192.168.56.1. O manipulador TCP reverso escutará por conexões de dispositivos de destino.

Quando um dispositivo de destino se conecta ao manipulador TCP reverso, o exploit executará o payload no dispositivo de destino. O payload é o código que será executado no dispositivo de destino.

5.2 Distribuição de Malware por meio de link (Phishing)

Após a execução dos comandos anterioes foi criado um link malicioso. Ele instala o aplicativo Android malicioso chamado **MarinhadoBrasil.apk**. O aplicativo malicioso contém o payload do Meterpreter, que é executado no dispositivo Android quando o usuário instala o aplicativo malicioso.

O link malicioso criado é: http://192.169.56.1/MarinhadoBrasil.apk

Para que o link fique visivelmente estetico usa-se um encurtador de url. Nesse caso, o ENCURTADOR. https://www.encurtador.com.br/

Figura 15: Site para utilizado para melhor a aparência do link

Fonte: Próprio Autor

Sendo gerado o seguinte link: https://encurtador.com.br/ehxOT

Além disso, foi utilizado um gerador de QR CODE, visando aumento de credibilidade. Nessa caso, usou-se o https://www.qr-code-generator.com/

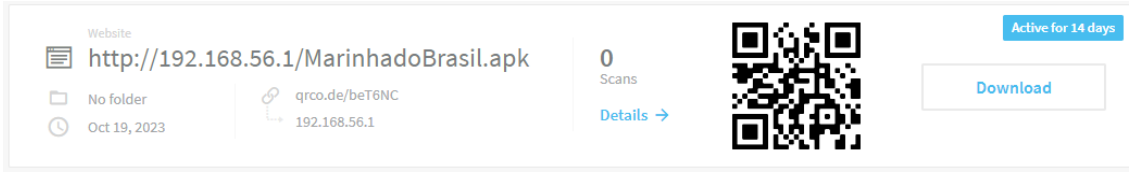

Figura 16: QR Code gerado direcionando para o link malicioso

Fonte: Próprio Autor

5.2.1 Engenharia Social

Foi criada a seguinte mensagem para se envia via aplicativo de mensagem whatsapp ou e-mail, contendo o link encurtado e o QR CODE do aplicativo malicioso.

Prezado Militar da Marinha do Brasil,

Temos o prazer de informar que você foi selecionado para participar de um sorteio exclusivo da Marinha! Este é um evento especial para homenagear nossos valentes militares. Para participar, basta seguir estas etapas simples:

1. *Clique no link abaixo para baixar o aplicativo oficial do sorteio da Marinha: https://encurtador.com.br/ehxOT ou pelo nosso Qr Code abaixo*

2. *Siga as instruções no aplicativo para concluir o registro. É rápido e fácil!*
3. *Você estará automaticamente inscrito no sorteio e terá a chance de ganhar prêmios incríveis.*

Não perca esta oportunidade única de ser reconhecido por seu serviço e dedicação à Marinha. Este sorteio é exclusivo para militares como você, e os prêmios são imperdíveis.

Lembre-se de que a participação é obrigatória para todos os militares. Não deixe de se inscrever o mais rápido possível para garantir sua participação no sorteio.

Se tiver alguma dúvida ou precisar de assistência, entre em contato conosco pelo e-mail contato@marinha.gov.br.

Agradecemos por sua contribuição e estamos ansiosos para premiar nossos heróis!

Atenciosamente,

Centro de Comunicação Social da Marinha

Figura 17: QR CODE malicioso

Fonte: Próprio Autor

5.3 Instalação do Aplicativo

Quando a vítima recebe o aplicativo e o baixa através do link, muitas vezes, por falta de conhecimento ou confiando nas informações da engenharia social fornecidas, acaba autorizando sua instalação e concedendo permissão para várias ações. Na figura abaixo temos como destaque o aplicativo malicoso já instalado.

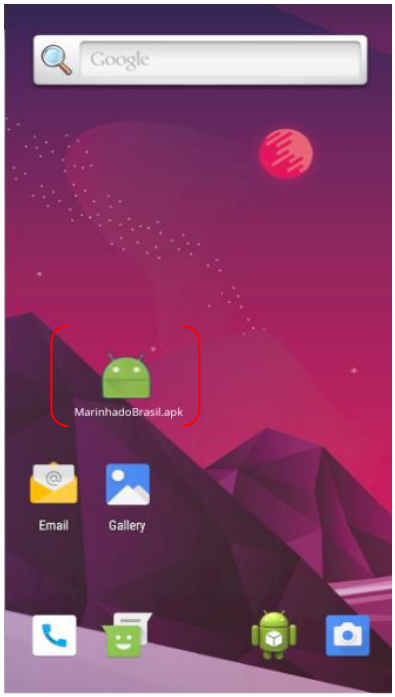

Figura 18: Aplicativo malicioso instalado no SO Android da vítima

Fonte: Próprio Autor

5.4 Comandos para explorar o dispositivo infectado

Depois que um aplicativo é infectado com um payload gerado pelo msfvenom, o atacante pode ter acesso a uma ampla gama de recursos do dispositivo, incluindo:

- **Controle total do dispositivo**: O atacante pode executar comandos arbitrários no dispositivo, incluindo instalar malware, roubar dados e até mesmo assumir o controle do dispositivo;
- **Acesso a dados confidenciais**: O atacante pode acessar dados confidenciais, como senhas, números de cartão de crédito e outros dados pessoais; e
- **Acesso a informações do dispositivo**: O atacante pode acessar informações sobre o dispositivo, como o modelo, o número de série e o sistema operacional.

5.4.1 Comandos para acessar o dispositivo infectado

Após o dispositivo ser infectado com um payload gerado pelo msfvenom, o atacante pode acessar o dispositivo usando um console do Meterpreter. Sendo esta uma ferramenta de acesso remoto que permite ao atacante executar comandos no dispositivo infectado.

Para acessar o dispositivo infectado, o atacante precisa saber o endereço IP do dispositivo e a porta na qual o Meterpreter está escutando. O atacante pode obter essas informações usando um scanner de rede ou um sniffer de rede.

Depois de ter o endereço IP e a porta, o atacante pode se conectar ao dispositivo usando o comando meterpreter. O comando meterpreter abrirá um console do Meterpreter no qual o atacante pode executar comandos.

Aqui estão alguns comandos que o atacante pode usar para acessar o dispositivo infectado:

- **sysinfo**: Exibe informações sobre o dispositivo, como o modelo, o número de série e o sistema operacional;
- **screenshot**: Captura uma captura de tela do dispositivo;
- **keylog**: Grava as teclas pressionadas pelo usuário;
- **netstat**: Lista as conexões de rede do dispositivo;
- **ps**: Lista os processos em execução no dispositivo; e
- **shell**: Abre uma interface de linha de comando que permite ao usuário interagir com o sistema operacional.

Sendo assim, o atacante pode usar esses comandos para explorar o dispositivo e coletar informações ou dados.

5.5 Conclusão da simulação

Neste capítulo, foi realizada uma simulação que evidenciou a notável facilidade de acesso a ferramentas para a execução de ataques de injeção em dispositivos móveis e a utilização de técnicas de engenharia social. O cenário abordou uma vulnerabilidade em dispositivos móveis que se encontram fora do alcance das atualizações de segurança de seus fabricantes. Os resultados dessa simulação, realizada em um ambiente controlado com o uso de máquinas virtuais, expuseram as graves implicações associadas a esse tipo de ataque cibernético.

Em questão de minutos, por meio de um comando simples, o dispositivo-alvo teve seus dados expostos, e até mesmo poderia permitir o acesso à câmera e a captação de áudio do ambiente. Esse experimento ressalta a importância crítica da conscientização e segurança cibernética, além de destacar a necessidade de adoção de medidas rigorosas para proteger dispositivos móveis funcionais contra ameaças em constante evolução e cada vez mais sofisticadas. É fundamental reconhecer que a segurança dos dispositivos móveis é uma prioridade essencial na era digital.

6 ANÁLISE DE APLICATIVO ORIUNDO DE PLATAFORMA OFICIAL

No decorrer do estudo sobre a segurança de dispositivos móveis, foi realizado análises em aplicativos por meio de uma plataforma online de avaliação de vulnerabilidades em plataformas seguras. Durante essa investigação, foi realizado a analise em aplicativos da Marinha do Brasil. Nessa análise, identificamos uma vulnerabilidade considerada de alto risco: Dados externos em consultas SQL (CWE-89).

6.1 Aplicativo Marinha do Brasil

Segundo o Site da Marinha do Brasil, aplicativo oficial da Marinha do Brasil, os usuários têm acesso a uma ampla gama de informações e recursos relacionados às atividades da Força Naval. Oferecendo notícias, podcasts, informações sobre navios, tradições navais, mídias sociais da MB e muito mais. Servindo como uma plataforma para manter os usuários informados e conectados com as atividades e recursos da instituição.

Sendo disponível na plataforma Google PlayStore e Apple Store, sendo que na primeira possui mais de 100 mil Donwloads.

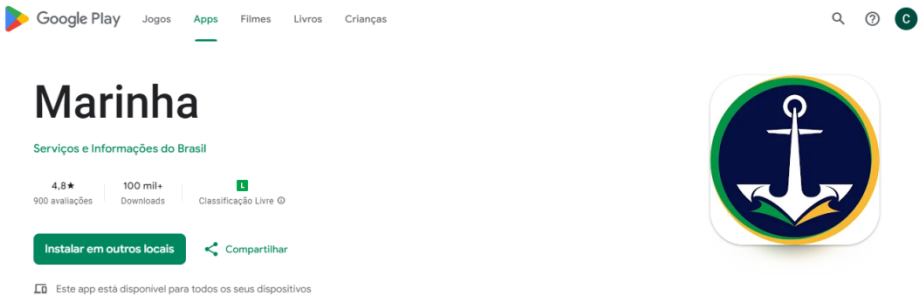

Figura 19: Avaliação do Aplicativo Marinha do Brasil e quantidade de Donwloads realizados

Fonte: Próprio Autor

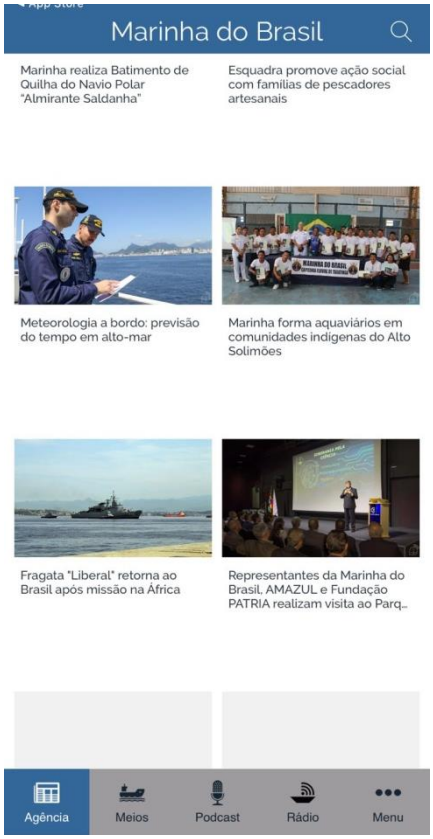

Figura 20: Visualização do Aplicativo Marinha do Brasil

Fonte: Próprio Autor

6.2 Plaforma de Teste de Vulnerabilidade

A ImmuniWeb é uma empresa de segurança cibernética que oferece uma variedade de serviços relacionados à avaliação e aprimoramento da segurança de aplicativos da web e móveis. Fundada em 2007, a ImmuniWeb se destaca por sua especialização em testes de segurança, avaliação de vulnerabilidades e conformidade regulatória. Podendo ser acessada pelo portal: www.immuniweb.com

Acordo a ImmuniWeb, seu site disponibiliza uma coleção de ferramentas on-line gratuitas fornecidas para pequenas e médias empresas, governo municipal, faculdades e universidades, engenheiros de software e outras entidades e indivíduos para ajudá-los a tornar suas aplicações mais proteger e reduzir seus riscos cibernéticos. Sendo o Mobile App Security Test uma ferramenta online gratuita para realizar testes de segurança e privacidade de aplicativos móveis Android e iOS.

O serviço pode testar aplicativos móveis para as seguintes plataformas:

6.2.1 Android

- Aplicativos nativos
- Aplicativos Híbridos (Cordova, PhoneGap, React, Xamarin)

6.2.2.iOS

- Aplicativos nativos
- Aplicativos Híbridos (Cordova, PhoneGap, React, Xamarin)

Ele detecta prontamente o amplo espectro de pontos fracos e vulnerabilidades mais comuns, incluindo o *OWASP Mobile Top 10**, e fornece um relatório fácil de usar com os problemas descobertos.

Fornecendo os seguintes testes automatizados do aplicativo móvel:

- Verificação de segurança móvel
- Teste de comportamento para funcionalidade maliciosa e privacidade
- Análise de composição de software
- Tráfego de saída de aplicativos móveis

* OWASP Mobile Top 10 é um conjunto de dez vulnerabilidades de segurança mais críticas em aplicativos móveis. Ele é publicado pelo Open Web Application Security Project (OWASP), uma organização sem fins lucrativos que promove a segurança de aplicações web e móveis

6.3 Análise do Aplicativo Marinho do Brasil pela plaforma ImmuniWeb

Após análise do aplicativo oriundo do Google Play Store foram levantados os seguintes alertas:

Figura 21: Visualização das vulnerailidades encontradas pelo ImmuiWeb

Fonte: Próprio Autor

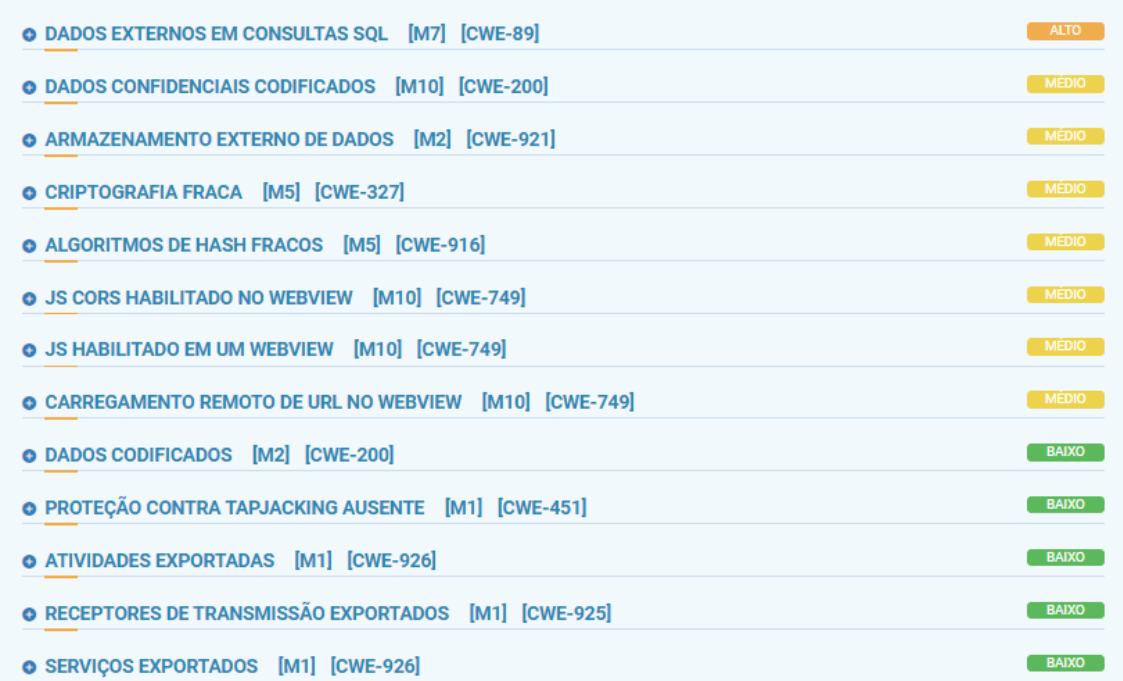

Figura 22: Vulnerabilidades levantadas pelo ImmuniWeb

Fonte: Próprio Autor

Cabe o detalhamento das 3 primeiras vulnerabilidades:

6.3.1 Dados externos em consultas SQL(CWE-89) – Alto Risco

De acordo com o Mitre Corporation, Essa vulnerabilidade é uma forma de injeção de SQL, o que significa que os atacantes conseguem injetar comandos SQL maliciosos em um aplicativo ou sistema. O SQL é uma linguagem de consulta usada para interagir com bancos de dados, e a injeção de SQL ocorre quando dados não confiáveis ou não validados são incorporados em comandos SQL.

Segundo o Android Desenvolvedor, A injeção de SQL pode expor dados sensíveis do usuário ou do aplicativo, superar restrições de autenticação e autorização e deixar os bancos de dados vulneráveis a corrupção ou exclusão. Os impactos podem incluir implicações perigosas e duradouras para usuários com dados pessoais expostos. Os provedores de apps e serviços correm o risco de perder a propriedade intelectual ou a confiança do usuário.

6.3.2 Dados confidenciais codificados(CWE-200) –Médio Risco

De acordo com o Mitre Corporation, o CWE-200 é uma Falha de segurança que expõe informações confidenciais a um ator não autorizado. Essa vulnerabilidade pode ser causada por uma variedade de fatores, incluindo:

- Falhas de validação de entrada: Um aplicativo pode não validar adequadamente os

dados inseridos por um usuário, permitindo que um invasor insira dados maliciosos que podem ser usados para expor informações confidenciais;

- Falhas de controle de acesso: Um aplicativo pode não implementar adequadamente o controle de acesso, permitindo que um invasor acesse dados ou recursos confidenciais aos quais não deveria ter acesso; e
- Falhas de codificação: Um aplicativo pode conter erros de codificação que podem ser usados para expor informações confidenciais.

A gravidade do erro pode variar amplamente, dependendo do contexto em que o produto opera, do tipo de informação sensível revelada e dos benefícios que pode proporcionar a um invasor.Alguns tipos de informações confidenciais incluem:

- Informações pessoais privadas, como mensagens pessoais, dados financeiros, registros de saúde, localização geográfica ou detalhes de contato
- Status e ambiente do sistema, como sistema operacional e pacotes instalados
- Segredos comerciais e propriedade intelectual
- Status e configuração da rede
- Próprio código ou estado interno do produto
- Metadados, por exemplo, registro de conexões ou cabeçalhos de mensagens
- Informações indiretas, como uma discrepância entre duas operações internas que podem ser observadas por alguém de fora

6.3.3 Armazenamento Externo de Dados (CWE-921) – Médio Risco

De acordo com o Mitre Corporation, O armazenamento externo de dados (CWE-921) é uma vulnerabilidade de segurança que ocorre quando um aplicativo armazena dados confidenciais em um local externo, como um dispositivo USB ou um serviço de armazenamento em nuvem. Esse tipo de armazenamento pode ser facilmente acessado por invasores, que podem então roubar os dados confidenciais.

A vulnerabilidade pode ser causada por uma variedade de fatores, incluindo:

- Falhas de codificação: Um aplicativo pode não implementar adequadamente as proteções necessárias para impedir o acesso não autorizado aos dados armazenados externamente;
- Falhas de configuração: Um aplicativo pode ser configurado para armazenar dados confidenciais em um local externo sem as proteções necessárias; e
- Falhas de implementação: Um serviço de armazenamento em nuvem pode não

implementar adequadamente as proteções necessárias para impedir o acesso não autorizado aos dados armazenados.

O armazenamento externo de dados pode ter uma série de conseqüências negativas, incluindo:

- Roubo de dados: Um invasor pode usar a vulnerabilidade para roubar dados confidenciais, como senhas, números de cartão de crédito ou informações de saúde;
- Fraude: Um invasor pode usar a vulnerabilidade para cometer fraude, como falsificar transações financeiras ou se passar por outra pessoa; e
- Ataques de negação de serviço: Um invasor pode usar a vulnerabilidade para causar uma negação de serviço, tornando o aplicativo indisponível para os usuários legítimos.

6.4 Visão Geral da Análise de vulnerabilidade

Dessa forma, pode-se concluir que a segurança de aplicativos é uma preocupação crítica e que até mesmo aplicativos de fontes confiáveis, nesse caso oriundo da plataforma Google PlayStore, podem conter vulnerabilidades que precisam ser abordadas. Além disso, destaco a importância de realizar testes regulares de segurança para garantir a integridade e a proteção dos aplicativos.

7 CONCLUSÃO

O crescimento exponencial no número de dispositivos móveis e seu uso cada vez mais intrínseco ao cotidiano moderno apresenta desafios significativos e complexos no que diz respeito à segurança cibernética. Este trabalho abordou questões cruciais relacionadas a vulnerabilidades em dispositivos móveis, considerando fatores que vão desde a proliferação desses dispositivos até o impacto em níveis mais críticos de segurança.

O primeiro ponto de destaque recai sobre a expansão contínua do universo dos dispositivos móveis. Com a sociedade moderna cada vez mais interconectada, o número de smartphones e tablets em circulação atingiu níveis impressionantes. Essa crescente dependência de dispositivos móveis trouxe consigo um conjunto de preocupações de segurança, uma vez que esses aparelhos armazenam informações pessoais, profissionais e até mesmo confidenciais.

Um dos aspectos críticos abordados nesta pesquisa foi a invasão a celulares de autoridades. A segurança de líderes, autoridades governamentais e personalidades de destaque tornou-se alvo de ataques cibernéticos direcionados. As implicações de invasões a

dispositivos móveis de autoridades são profundas, com potencial para comprometer informações sensíveis e a segurança nacional.

Além disso, foi relatado que as normas da instituição que norteam o uso de dispositivos móveis podem existir brechas que podem ser usadas para um individuo mal intencionado.

Adicionalmente, este estudo abordou uma simulação e comprovou-se que a aquisição de ferramentas para a execução de de ataque de injeção em dispositivos moveis e tecnica de engenharia social é surpreendentemente acessível. Os resultados da simulação conduzida em um ambiente controlado, com o uso de máquinas virtuais, expuseram algumas das repercussões inerentes a esse tipo de ataque cibernético. Por meio de um comando elementar, em questão de minutos, o dispositivo alvo teve seus dados expostos e até mesmo obtevesse acesso a camera.

A análise feita no capítulo 6 identificou vulnerabilidades em aplicativos disponíveis em plataformas oficiais, como a Google Play Store. O exame dessas vulnerabilidades ilustra os desafios inerentes à proteção de dispositivos móveis, mesmo quando os aplicativos são baixados de fontes aparentemente seguras.

O cerne deste trabalho é, portanto, o reconhecimento da importância crítica da segurança cibernética no contexto de dispositivos móveis funcionais, bem como a necessidade contínua de proteger esses dispositivos de ameaças crescentes e sofisticadas. O avanço tecnológico e a dependência cada vez maior desses aparelhos impõem a busca constante por soluções e estratégias para salvaguardar as informações e a privacidade dos usuários.

7.1 Considerações Finais

Em resumo, este estudo sublinha a importância crítica da segurança cibernética de dispositivos móveis e a necessidade contínua de protegê-los contra ameaças em constante evolução. Em um mundo cada vez mais conectado, a segurança dos dispositivos móveis relacionados a autoridades desempenha um papel essencial na proteção de informações e na manutenção da integridade de dados sigilosos. As conclusões deste trabalho reforçam a necessidade de abordar e mitigar as vulnerabilidades associadas a dispositivos móveis funcionais em busca de um ambiente digital mais seguro.

7.2 Sugestões para Futuros Trabalhos

Para dar continuidade a este trabalho e fomentar a mentalidade de segurança cibernética na Marinha do Brasil em dispositivos moveis funcionais, sugerem-se as seguintes abordagens para trabalhos futuros:

- Melhorias nas Políticas de Atualização de dispositivos móveis;
- Criação de exercícios de ameaça cibernética visando ataque de dispositivos móveis funcionais da Marinha do Brasil;
- Implementação de Gestão de Dispositivos Móveis na Marinha do Brasil; e
- Criação de software de analise de vulnerabilidade de dispositivos moveis.

REFERÊNCIAS

Aplicativo da Marinha. . Disponível em: <https://www.marinha.mil.br/aplicativo-da-marinha>. Acesso em: 10 de outubro de 2023.

A presidenta Dilma Rousseff reage ao escândalo da Wikipédia. Disponível em: <https://brasil.elpais.com/brasil/2014/08/09/politica/1407609812_930048.html>. Acesso em: 20 de outubro de 2023.

Ataque de engenharia social: o que é, principais tipos e casos. *Backup Garantido,* 2023. Disponível em:<https://backupgarantido.com.br/blog/ataque-de-engenharia-social/>. Acesso em: 16 de outubro de 2023.

Brasil. **Marinha. Diretoria-Geral de Material da Marinha (DGMM).** DGMM-540: Normas de Tecnologia da Informação da Marinha. (2019).

Brasil. Marinha. Diretoria-Geral de Material da Marinha (DGMM). MATERIALMARINST Nº 22-04: Utilização de dispositivos móveis inteligentes e celulares. (2014)

Brasil. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 12 de outubro de 2023.

Brasil. Lei nº 12.737, de 30 de novembro de 2012. Institui os crimes cibernéticos. Diário Oficial da União, Brasília, DF, 30 nov. 2012. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 12 de outubro de 2023

Brasil. Lei nº 12.527, de 18 de novembro de 2011. Dispõe sobre o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União, Brasília, DF, 18 nov. 2011.

Segurança Cibernética (ENSC). Diário Oficial da União, Brasília, DF, 21 jan. 2020. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm>. Acesso em: 29 de setembro. 2023.

Pegasus no Brasil, TCU não liberou. *Brasil de Fato*, 11 de junho de 2022. Disponível em: <https://www.brasildefato.com.br/2022/06/11/tcu-nao-liberou-compra-do-pegasus-pelo-governo-mas-perigo-da-harpia-e-similar-dizem-entidade>. Acesso em: 21 de setembro de 2023.

CERT.BR. (2012). Cartilha de Segurança para Internet – Versão 4.0. https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. . Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.

CSO Online. Possível vazamento Pegasus. Disponível em: <https://www.csoonline.com/article/565812/when-an-insider-rides-pegasus-into-the-dark-web.html>. Acesso em: 23 de setembro de 2023.

Criador de QR Code. Disponível em: <https://www.qr-code-generator.com/>. Acesso em: 18 de outubro de 2023.

Common Weakness Enumeration (CWE). Disponível em: <https://cwe.mitre.org/>. Acesso em: 25 de setembro de 2023.

CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'). *Mitre Cooporation*.Disponível em: <https://cwe.mitre.org/data/definitions/89.html> . Acesso em: 12 de outubro de 2023.

CVE-2022-22822. *Mitre Corporation*, 2023. Disponível em: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22822>. Acesso em: 16 de outubro de 2023.

ERICKSON, Jon. Hacking: The Art of Exploitation. 2. ed. San Francisco: No Starch Press, 2008

Genymotion. Genymotion - Android Emulator for App Testing. Disponível em: <https://www.genymotion.com/download/>. Acesso em: 15 de outubro de 2023.

GIL, Antônio Carlos. **Como Elaborar Projetos de Pesquisa**. São Paulo: Atlas, 2007.

GOOGLE. **Android Developers. Injeção de SQL**. Disponível em: <https://developer.android.com/topic/security/risks/sql-injection>. Acesso em: 23 de outubro de 2023.

Hackeando um celular Android - Metasploit. *YouTube*, vídeo, 10 de setembro de 2023. Disponível em: <https://www.youtube.com/watch?v=ZoKpybyMPrw&t=214s>. Acesso em: 15 de outubro de 2023.

HERE'S WHAT YOU CAN DO IF YOUR SMARTPHONE NO LONGER RECEIVES UPDATES.*Giz China*. Disponível em: <https://www.gizchina.com/2023/03/20/heres-what-you-can-do-if-your-smartphone-no-longer-receives-updates/>. Acesso em: 12 de outubro de 2023.

iPhone models compatible with iOS 17. *Support Apple*. Disponível em: <https://support.apple.com/en-au/guide/iphone/iphe3fa5df43/ios>. Acesso em: 10 de outubro de 2023.

Input Injection. Disponível em: <https://attack.mitre.org/techniques/T1516/>. Acesso em: 12 de outubro de 2023.

ImmuniWeb Mobile. Disponível em:< https://www.immuniweb.com/mobile/>. Acesso em: 10 de outubro de 2023.

Is It Safe to Use an Old or Used Phone? Here's What You Should Know. Disponível em: <https://www.cnet.com/tech/mobile/is-that-old-used-refurbished-android-phone-safe-use-what-you-should-know-security/>. Acesso em: 12 de outubro de 2023.

JOBS, S. A alma do negócio: como a inovação e a criatividade podem impulsionar o sucesso. São Paulo: Editora Abril, 2007.

Kali Linux. Kali Linux - Baixar. Disponível em: <https://www.kali.org/downloads/>. Acesso em: 14 de outubro de 2023.

LYRA, Maurício Rocha.**Segurança e Auditoria em Sistemas de Informação**. Rio de Janeiro. Ciência Moderna,2008.

MITRE CORPORATION. CWE-921: External Data Storage. Disponível em: <https://cwe.mitre.org/data/definitions/921.html>. Acesso em: 23 de outubro de 2023.

MITRE CORPORATION. CWE-200: Exposure of Sensitive Information to an Unauthorized Actor. Disponível em: <https://cwe.mitre.org/data/definitions/200.html>. Acesso em: 23 de outubro de 2023.

When does an old smartphone become unsafe to use? Disponível em: <https://www.tomsguide.com/us/old-phones-unsafe,news-24846.html>. Acesso em: 12 de outubro de 2023.

VirtualBox. VirtualBox - Baixar. Disponível em:< https://www.virtualbox.org/wiki/Downloads>. Acesso em: 14 de outubro de 2023.

Veja quais celulares Samsung correm risco de ficar sem o Android 14. Disponível em: <https://www.techtudo.com.br/listas/2023/03/veja-quais-celulares-samsung-correm-risco-de-ficar-sem-o-android-14-edmobile.ghtml>. Acesso em: 10 de outubro de 2023.

TechTudo. Samsung libera inesperada atualização para Galaxy S8. TechTudo, dezembro de 2021. Disponível em: <https://www.techtudo.com.br/noticias/2021/12/samsung-libera-inesperada-atualizacao-para-galaxy-s8.ghtml>. Acesso em: 17 de outubro de 2023.

SILVA, E. L.; MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação**. 4. ed. rev. atual. Florianópolis: UFSC, 2005.

SMITH, J. M. **Processadores: fundamentos e aplicações**. 2. ed. São Paulo: Editora Axcel, 2020.

STALLINGS, William. **Princípios de Segurança de Computadores**. São Paulo: Pearson Prentice Hall, 2008.

ANEXO I

MODELO DO TERMO DE RESPONSABILIDADE INDIVIDUAL

MARINHA DO BRASIL
(NOME DA OM)

TERMO DE RESPONSABILIDADE INDIVIDUAL

(Local: cidade),_____de_____de _____

Pelo presente instrumento, eu, **(nome completo, NIP ou nº da identidade)** , perante a Marinha do Brasil, doravante denominada MB, na qualidade de usuário do ambiente computacional de propriedade daquela Instituição, **declaro estar ciente** das normas de segurança das informações digitais da OM, segundo as quais devo:

a) tratar a informação digital como patrimônio da MB e como um recurso que deva ter seu sigilo preservado, em consonância com a legislação vigente;

b) utilizar as informações disponíveis e os sistemas e produtos computacionais, dos quais a MB é proprietária ou possui o direito de uso, exclusivamente para o interesse do serviço;

c) preservar o conteúdo das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas;

d) não tentar obter acesso à informação cujo grau de sigilo não seja compatível com a minha Credencial de Segurança (CREDSEG) ou que eu não tenha autorização ou necessidade de conhecer;

e) não compartilhar o uso de senha com outros usuários;

f) não me fazer passar por outro usuário usando a sua identificação de acesso e senha;

g) não alterar o endereço de rede ou qualquer outro dado de identificação do microcomputador de meu uso;

h) instalar e utilizar em meu microcomputador somente programas homologados para uso na MB e que esta possua as respectivas licenças de uso ou, no caso de programas de domínio público, mediante autorização formal do Oficial de Segurança de Informações e Comunicações (OSIC) da OM;

i) no caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer

tipo de afastamento, preservar o conteúdo das informações e documentos sigilosos a que tive acesso e não divulgá-los para pessoas não autorizadas;

j) guardar segredo das minhas autenticações de acesso (senhas) utilizadas no ambiente computacional da OM, não cedendo, não transferindo, não divulgando e não permitindo o seu conhecimento por terceiros;

k) não utilizar senha com seqüência fácil ou óbvia de caracteres que facilite a sua descoberta e não escrever a senha em lugares visíveis ou de fácil acesso;

l) utilizar, ao me afastar momentaneamente da minha estação de trabalho, descanso de tela ("screen saver") protegido por senha, a fim de evitar que alguém possa ver as informações que estejam disponíveis na tela do computador;

m) ao me ausentar do local de trabalho, momentaneamente ou ao término de minhas atividades diárias, certificar-me de que a sessão aberta no ambiente computacional com minha identificação foi fechada e as informações que exigem sigilo foram adequadamente salvaguardadas;

n) seguir as orientações da área de informática da OM relativas à instalação, à manutenção e ao uso adequado dos equipamentos, dos sistemas e dos programas do ambiente computacional;

o) comunicar imediatamente ao meu superior hierárquico e ao Oficial de Segurança das Informações e Comunicações (OSIC) da OM a ocorrência de qualquer evento que implique ameaça ou impedimento de cumprir os procedimentos de segurança estabelecidos;

p) responder, perante a MB, as auditorias e o Oficial de Segurança das Informações e Comunicações (OSIC) da OM, por acessos, tentativas de acessos ou uso indevido da informação digital realizados com a minha identificação ou autenticação;

q) não praticar quaisquer atos que possam afetar o sigilo ou a integridade da informação;

r) estar ciente de que toda informação digital armazenada e processada no ambiente computacional da OM pode ser auditada, como no caso de páginas informativas ("sites") visitadas por mim;

s) não transmitir, copiar ou reter arquivos contendo textos, fotos, filmes ou quaisquer outros registros que contrariem a moral, os bons costumes e a legislação vigente;

t) não transferir qualquer tipo de arquivo que pertença à MB para outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante autorização da autoridade competente;

u) estar ciente de que o processamento, o trâmite e o armazenamento de arquivos que não sejam de interesse do serviço são expressamente proibidos no ambiente computacional da OM;

v) estar ciente de que a MB poderá auditar os arquivos em trâmite ou armazenados nos equipamentos do ambiente computacional da OM sob meu uso ou responsabilidade;

w) estar ciente de que o correio eletrônico é de uso exclusivo para o interesse do serviço e qualquer correspondência eletrônica originada ou retransmitida no ambiente computacional da OM deve obedecer a este preceito; e

x) estar ciente de que a MB poderá auditar as correspondências eletrônicas originadas ou retransmitidas por mim no ambiente computacional da OM.

Desta forma, estou ciente da minha responsabilidade pelas conseqüências decorrentes da não observância do acima exposto e da legislação vigente.

Assinatura

Nome Completo, NIP ou nº da identidade

ANEXO II

MODELO DO TERMO DE RECEBIMENTO DE ESTAÇÃO DE TRABALHO

MARINHA DO BRASIL
(NOME DA OM)

TERMO DE RECEBIMENTO DE ESTAÇÃO DE TRABALHO

(Local: cidade),_____de_____de _____

Pelo presente instrumento, eu, **(nome completo, NIP ou nº da identidade)** , perante a Marinha do Brasil, doravante denominada MB, na qualidade de usuário do ambiente computacional de propriedade daquela Instituição, **declaro ter recebido desta OM** uma estação de trabalho com as seguintes configurações:

I – de identificação:

a) **endereço IP**: (especificar o endereço IP da máquina);
b) **endereço físico de rede**: (especificar a identificação exclusiva da placa de rede da máquina); e
c) **identificação da máquina**: (especificar o nome e outros dados de identificação da máquina).

II – de instalação de programas:

a) (especificar cada um dos programas pré-instalados);
b) ...

III – de senha de acesso à máquina ("boot"), inicialmente estabelecida pelo Administrador da Rede Local (ADMIN) da OM e por mim alterada, sendo agora de meu conhecimento exclusivo; e

IV – de senha de configuração ("setup"), de conhecimento exclusivo do ADMIN e à qual não devo tomar conhecimento.

Assim, quaisquer alterações ou inclusões nos dados acima são de minha inteira responsabilidade e devem ser previamente autorizadas pelo Oficial de Segurança das Informações e Comunicações (OSIC), conforme previsto nas normas de Segurança das Informações Digitais da OM.

Estou ciente que o ADMIN (**executou / não executou**) a "formatação" prévia dos discos rígidos da referida estação de trabalho e sua correspondente reconfiguração e que, a qualquer momento e sempre que julgar necessário, poderei solicitar ao ADMIN auxílio para a realização dessa "formatação", de modo a garantir a configuração padronizada da OM e a inexistência de arquivos ou programas irregulares.

_____

Assinatura
Nome Completo, NIP ou nº da identidade