FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI
Curso Superior de Tecnologia em Segurança da Informação

Gustavo Alves

SEGURANÇA NA UTILIZAÇÃO DE APLICATIVOS EM SMARTPHONES

Americana, SP
2023

FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI
Curso Superior de Tecnologia em Segurança da Informação

Gustavo Alves

SEGURANÇA NA UTILIZAÇÃO DE APLICATIVOS EM SMARTPHONES

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Me. Edson Roberto Gaseta

Área de concentração: Segurança da Informação.

Americana, SP.
2023

Gustavo Alves

SEGURANÇA NA UTILIZAÇÃO DE APLICATIVOS EM SMARTPHONES

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana – Ralph Biasi.
Área de concentração: Segurança da informação.

Americana, 29 de novembro de 2023

Banca Examinadora:

Edson Roberto Gaseta
Mestre
Fatec-Americana

Maria Cristina Aranda
Doutora
Fatec-Americana

Diógenes de Oliveira
Mestre
Fatec-Americana

SEGURANÇA NA UTILIZAÇÃO DE APLICATIVOS EM SMARTPHONES

Gustavo Alves

Curso Superior de Tecnologia em Segurança da Informação – Faculdade de Tecnologia de Americana (FATEC Americana)

Americana – SP - Brasil

gustavo.alves23@fatec.sp.gov.br

Abstract. *This article highlights the importance of mobile device security, addressing common threats, secure development practices, and preventive measures. The growing dependence on mobile devices has increased security vulnerabilities. The article emphasizes the need to maintain information security, discussing data confidentiality, integrity, and availability. It also provides guidelines for protecting devices and data, including updates, antivirus software, strong passwords, and secure development practices.*

Resumo. *Este artigo destaca a importância da segurança em dispositivos móveis, abordando ameaças comuns, boas práticas de desenvolvimento e medidas preventivas. Os dispositivos móveis estão cada vez mais vulneráveis devido ao aumento da dependência deles. O artigo enfatiza a necessidade de manter a segurança da informação, discutindo a confidencialidade, integridade e disponibilidade dos dados. Também fornece orientações para proteger dispositivos e dados, incluindo atualizações, antivírus, senhas fortes e práticas seguras de desenvolvimento.*

1. Introdução

Segundo um artigo do BBC News Brasil (2021), desde sempre o ser humano gostou da ideia de ter mobilidade junto com tecnologia, muito se via quando foi lançado o primeiro *walkman*, a ideia de ter as músicas que se gosta no momento que quiser onde quiser é incrível, porém com o passar do tempo a tecnologia foi evoluindo e cada vez mais trazendo mais disso para a população. Vive-se no mundo onde a mobilidade tecnológica está fortemente ativa em nos dispositivos móveis, podendo controlar músicas, carros, casas e etc. Basicamente as vidas pessoais, profissionais, públicas e/ou privadas, tornaram-se acessíveis aos celulares, segundo Cashell (2004), o mundo apresenta uma grande dependência dos sistemas computacionais, o que por um lado facilitou muito o cotidiano, por outro trouxe uma nova visão sobre segurança, pois como será possível se defender das pessoas que querem fazer mal por esse meio.

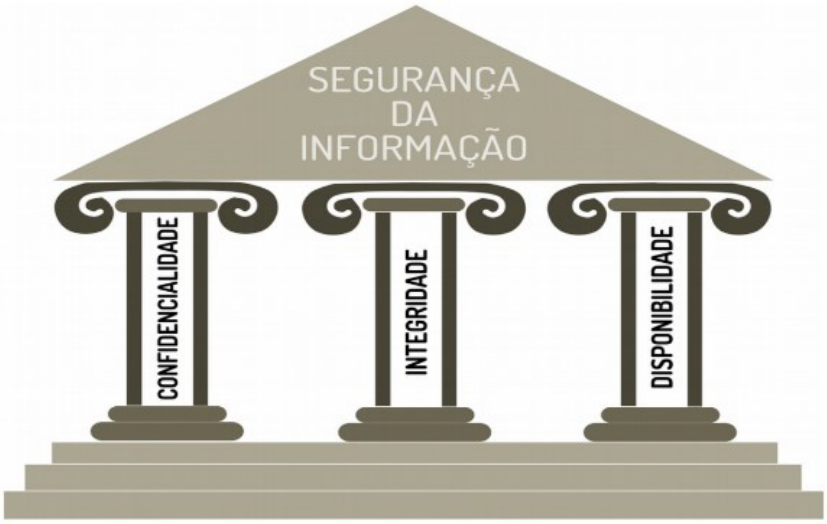
Os ataques mais realizados em dispositivos *mobilem* acabam sendo o de *phishing*, conseguindo assim acessos a dados sensíveis dos usuários, como nome completo, número de documento, dados bancários entre outros. Seguidos de *malwares* instalados de forma indevida, acabam infectando os *smartphones* e tendo acesso além dos dados anteriormente citados, também a funções nativas do aparelho, como câmera e microfone (SCHAEFFER, 2022)

O objetivo deste trabalho, é mostrar quais os tipos mais comuns de ataques e vulnerabilidades, tal qual as formas de mitigar ou acabar de vez com essas situações, mostrando que os pilares da segurança da informação, são essenciais para manter uma boa segurança nos dispositivos móveis.

2. Pilares da segurança.

O artigo levará em conta os 3 pilares fundamentais na segurança da informação conforme citado por Hintzbergen (2018), sendo eles confidencialidade, integridade e disponibilidade. A figura 1, exemplifica a importância e quão fundamental são esses pilares para que haja segurança.

Figura 1 - Pilares da segurança.



Fonte: Hintzbergen, 2018.

Hintzbergen (2018), define de forma muito complexa sobre cada um dos pilares, sendo eles sintetizado logo a seguir:

- Confidencialidade: Garante a aplicação do sigilo necessário em todos os estágios de processamento de dados, evitando divulgações não autorizadas. Isso deve ser mantido desde o armazenamento nos sistemas e dispositivos de rede até a transmissão e o recebimento dos dados. Para exemplificar, usar uma criptografia para que possa haver esse nível de segurança, usando um preenchimento de tráfego na rede, controle de acesso, há várias formas de se ter uma confidencialidade.

- Integridade: A "[...] definição para integridade da informação vem dos dicionários. Integridade significa que a informação é completa, perfeita e intacta (não necessariamente correta). Significa que nada está faltando na informação, ela está completa e em um desejado bom estado" (DONN PARKER *apud* HINTZBERGEN*,* 2018, p. 23). Ou seja, a informação pode estar correta e autêntica, mas faltar a integridade ou a informação pode ser incorreta e/ou não autêntica e ainda ser integra.

Ambientes seguros evitam que invasores ou erros de usuários comprometam a integridade dos sistemas e dados. Ataques como vírus, bombas lógicas e *backdoor,* prejudicam a integridade do sistema, afetando os dados com corrupção ou modificações. Medidas como controle de acesso, detecção de intrusão e *hashing* combatem essas ameaças.

Usuários, por engano, também podem afetar a integridade. Por exemplo, ao deletar arquivos críticos por engano ou inserir informações incorretas, resultando em uma cobrança de $3.000.000,00 em vez de $300,00 de um cliente.

- Disponibilidade: A disponibilidade do sistema pode ser afetada por falhas de dispositivos ou software. Para garantir a continuidade, *backups* devem ser prontamente disponíveis para substituir sistemas críticos. Funcionários qualificados devem estar prontos para restaurar o sistema quando necessário. Questões ambientais, como temperatura, umidade, eletricidade estática e contaminantes, também podem impactar a disponibilidade, então medidas de proteção, aterramento adequado e monitoramento são cruciais.

Hackers frequentemente usam ataques de negação de serviço (*DoS*) para interromper a disponibilidade de sistemas empresariais. Para proteção, apenas os serviços essenciais devem estar ativos e os sistemas de detecção de intrusão (*IDS*) devem monitorar o tráfego e a atividade da rede.

O quadro 1 traz de forma mais sucinta cada um dos pilares.

Quadro 1 - Resumo dos pilares da segurança da informação

Pilar	Significado
Confidencialidade	Assegurar que as informações sejam transmitidas exclusivamente ao seu destinatário, sem possibilidade de visualização por parte de outros usuários do sistema ou qualquer indivíduo com acesso ao canal de transmissão. A abordagem mais prevalente para garantir a confidencialidade consiste em combinar autenticação e criptografia.
Integridade	A informação que está sendo transmitida precisa chegar ao seu destino de forma íntegra, sem sofrer modificações ou interferências indesejadas. A segurança do sistema pode ser colocada em risco devido à presença de softwares maliciosos inseridos por um agente externo. Para prevenir essa situação, é possível implementar a detecção de intrusões ou recorrer à utilização de funções de *hash*.
Disponibilidade	A garantia de disponibilidade é alcançada quando os seguintes três elementos são observados: - Oportunidade: A informação está prontamente acessível quando requisitada. - Continuidade: Possibilita o acesso, mesmo que de forma parcial, no caso de ocorrerem falhas. - Robustez: Demonstra a capacidade de suportar acessos simultâneos de acordo com a demanda.

Fonte: Baseado em Hintzbergen (2018). Elaborado pelo autor.

2.2 Ameaças *mobile*

Vulnerabilidade é uma fraqueza em um sistema ou aplicação que pode ser explorada por ameaças, levando a incidentes indesejados. Geralmente, resulta de proteções insuficientes ou ausentes (HINTZBERGEN, 2018).

Felt, e*t al.* (2011), diz que algumas definições são necessárias para tornar claro o tipo de ameaça que deve ser tratada. Essas ameaças ferem os pilares da segurança da informação em sua totalidade.

Há uma classificação de aplicativos que representam um risco potencial à segurança dos usuários ou de seus dados, feito pela Google, através do seu sistema operacional Android, ela classifica esses riscos como *Potentially Harmful Applications* (*PHAs*) termo que em português significa "Aplicações Potencialmente Nocivas" (GOOGLE, 2017).

Sendo eles:

- *Malware*: Este *software* age de forma desonesta ao realizar ações como roubar, modificar ou apagar dados de aplicativos ou do sistema operacional do usuário, tudo isso sem consentimento prévio ou autorização.

- *Backdoors*: Aplicações que controlam remotamente um dispositivo, executando operações indesejadas e potencialmente prejudiciais.

- *Comercial Spyware*: Qualquer informação que transmita informações confidenciais do dispositivos sem o consentimento do usuário e não exibe uma notificação de que está acontecendo

- *Data Collection*: Qualquer aplicação que colete informações sobre aplicativos instalados, como informações de conta, nomes, dados sensíveis etc. Sem o consentimento do usuário.

- *Denial-of-Service (DoS)*: Aplicações que tem por objetivo deixar indisponível uma funcionalidade importante ou até mesmo o próprio sistema, sem o consentimento do usuário.

- *Hostile Downloader*: Aplicações que por si só não são hostis, porém realizam *download* de outras aplicações que são potencialmente prejudiciais.

- *Mobile Billing Fraud*: Aplicações que cobram de forma enganosa o usuário de forma intencional.

- *SMS Fraud*: Aplicações que cobram um certo *SMS premium* sem o consentimento do usuário ou disfarçam suas atividades, ocultando acordos de divulgação ou mensagens de *SMS* da operadora de celular, notificando o usuário sobre cobranças ou confirmando assinatura.

- *Call Fraud*: Aplicações que de forma dispendiosa podem adicionar cobranças à conta de celular sem informar o usuário previamente.

- *Toll Fraud*: Aplicações que enganam os usuários para comprar ou se inscreverem em conteúdos através da conta de telefone celular.

- *Non-Android Threat*: Aplicações que contém ameaças não *Android*. Essas aplicações não podem causar algum tipo de dano ao usuário ou ao dispositivo, mas contém comportamentos potencialmente prejudiciais a outras plataformas.

- *Phishing*: Envio de mensagens enganosas com o objetivo de se passar por um emissor legítimo para levar o usuário a fornecer informações sigilosas como senhas e informações bancárias.

- *Privilege Escalation*: Aplicações que comprometem a integridade do sistema, quebrando a caixa de proteção do dispositivo, alterando ou desativando o acesso às funções principais relacionadas à segurança.

- *Ransomware*: Algo que pode-se traduzir como sequestro, são aplicações que tomam controle parcial ou total de um dispositivo ou de dados e exigem um pagamento para liberação do controle novamente.

- *Rooting*: Aplicações que realizam escalonamento de privilégios criando um *root* no dispositivo.

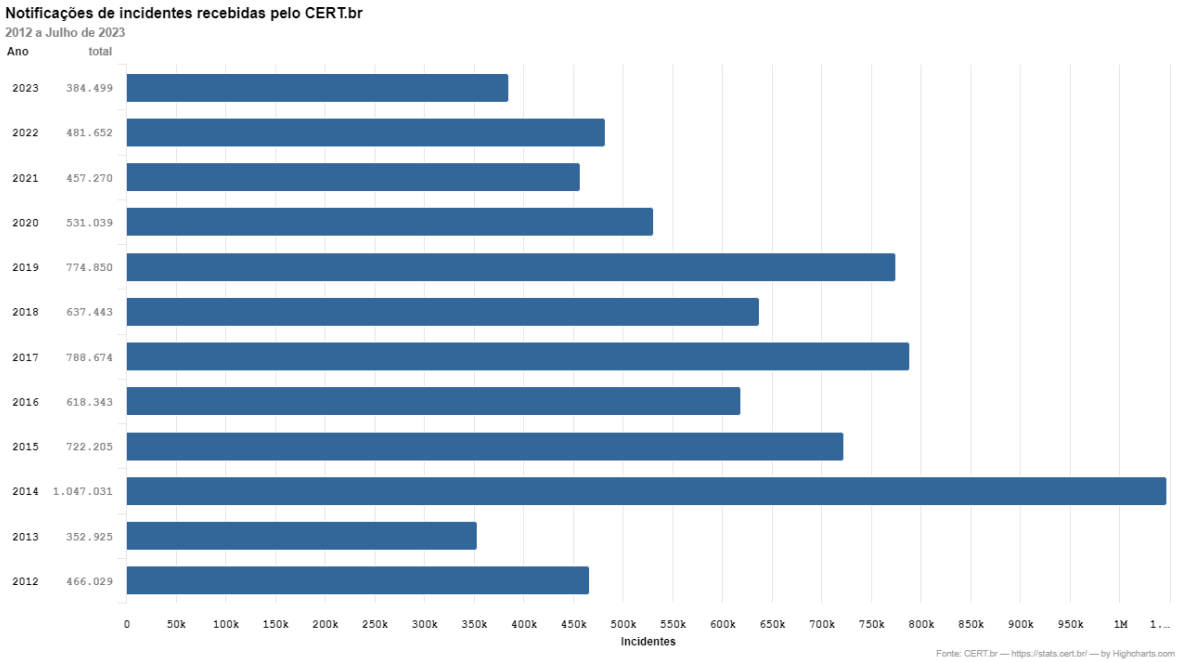
- *Spam*: Envio de mensagens não solicitadas para os contatos do usuário ou usando o dispositivo como uma retransmissão de *spam* por *e-mail*.

- *Spyware*: Aplicações que transmitem informações confidenciais do dispositivo como lista de contatos, *logs* de *SMS*, fotos, outros arquivos não pertencentes ao aplicativo entre outros.

- *Trojan*: Aplicações disfarçadas de algo benigno, porém executam ações indesejadas contra o usuário.

Segundo o CERT.br (2018), os incidentes envolvendo *PHAs* têm variado consideravelmente nos últimos anos, na figura 2 podemos ver que em 2018, foram registradas 676.514 notificações, o que representa uma redução de 19% em relação a 2017. Por outro lado, em 2017, houve um aumento de 29% em comparação com 2016, com um total de 833.775 notificações. Vale destacar que em 2014, o número de notificações foi significativamente maior, atingindo 1.047.031, um aumento de 197% em relação a 2013. Esse aumento foi principalmente atribuído a ataques de negação de serviço (*DoS*), que visam comprometer a "disponibilidade" de um sistema.

Figura 2 - Incidentes CERT.br



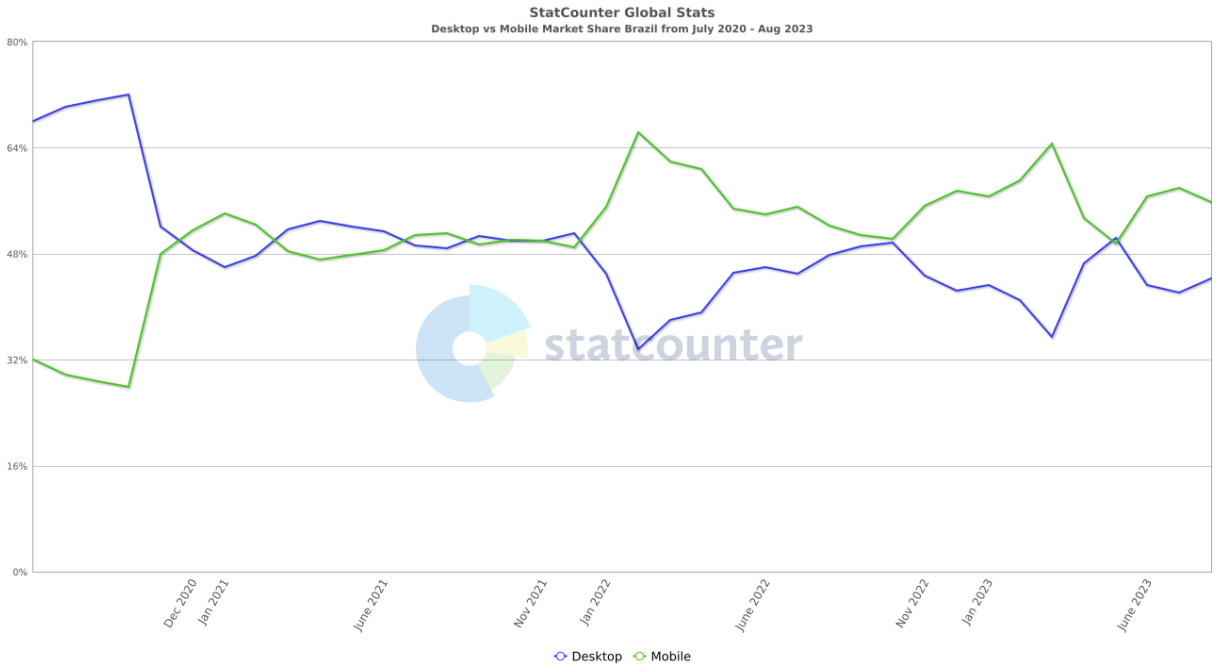
Fonte: CERT.br, 2018.

2.3 - Evolução dos ataques

Segundo os dados apresentados pelo *site* StatCounter (2023), há menos de 2 anos atrás o número de *desktops* era maior que os números de dispositivos *mobile* no Brasil, como mostrado na figura 3, nota-se que no final de 2021 e início de 2022 o número de dispositivos móveis ultrapassa o de *desktop*, mostrando que eventualmente os ataques irão acompanhar os dispositivos mais usados. Como os dispositivos móveis não possuem uma maturidade tão alta quanto os *desktops*, suas capacidades de segurança acabam ficando um pouco mais atrasada, por mais parecido que possam ser de um *notebook*, por

exemplo, eles não possuem a mesma arquitetura física e o sistema operacional também acaba sendo de forma mais limitada, deixando um pouco mais de aberturas para eventuais ataques.

Figura 3 - Números disponíveis móveis.



Fonte: StatCounter, 2023.

McNeil e Jones (2022) para a revista *ProofPoint* diz que, os ataques entre janeiro e março de 2022 cresceram por volta de 500% na Europa em dispositivos móveis, sendo quase todos voltados para dispositivos Android, já que os dispositivos iOS não permitem *downloads* de aplicativos de terceiros em seu Sistema Operacional (SO). Como os dispositivos Android, possuem mais liberdade sobre o SO, as vezes ao fazer *download* de um aplicativo na PlayStore (loja virtual oficial do Android), ocorre de outros *apps* serem instalados juntos e possuírem um *malware*. Também dentro dos celulares Androids, existe a opção de baixar aplicativos sem ser da loja oficial, tornando assim mais inseguro e propenso a comprometer a segurança dos aparelhos móveis. Os ataques realizados pelos *malwares* citados por McNeil e Jones (2022), não fazem apenas o roubo de credenciais dos usuários, as vulnerabilidades estão tendo acesso a partes nativas do aparelho e conseguindo também acesso a câmera, microfone, ligações, mensagens e etc.

As ameaças não são específicas de uma região ou país, elas são totalmente adaptativas com o lugar da onde agem, elas são enviadas por meio de *phishing*s, engenharias sociais ou *softwares* terceiros. Conforme a figura 4, mostra as regiões, SO 's mais afetados e qual tipo de *malware* usado.

Figura 4 - Malwares x SO's afetados.

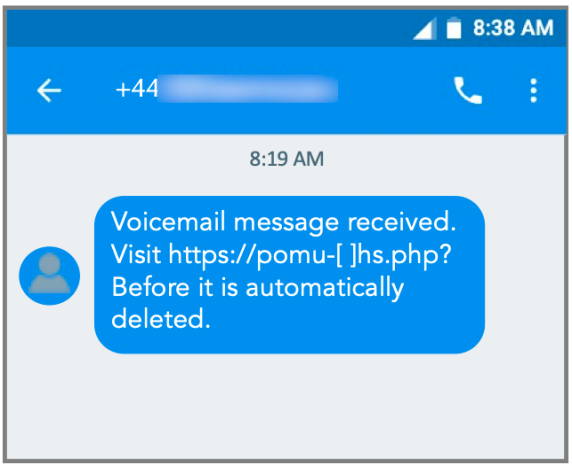
	Target OS	App Impersonation	Financial Impersonation	Multi-Modal (Social Media)	Credential Theft	Microphone and Camera	SMS Spreading	Privilege Escalation	Primary Geography
FluBot		✓	✓	✗	✓	✗	✓	✓	Asia, UK, & Europe
TeaBot		✓	✓	✓	✓	✗	✓	✓	UK & Europe
TangleBot		✗	✓	✓	✓	✓	✗	✓	North America
MoqHao		✓	✓	✓	✓	✗	✓	✗	Asia & Japan
BRATA		✓	✓	✗	✓	✗	✓	✗	UK, Europe, Latin Amer.
TianySpy		✓	✓*	✗	✓	✗	✗	✗	Japan
KeepSpy		✓	✓*	✗	✓	✗	✗	✗	Japan

Fonte: ProofPoint, 2022.

Para não ficar muito extenso, terá o enfoque no TeaBot mostrado na figura 4, pois é o que mais abrange a maioria dos cenários de um aparelho.

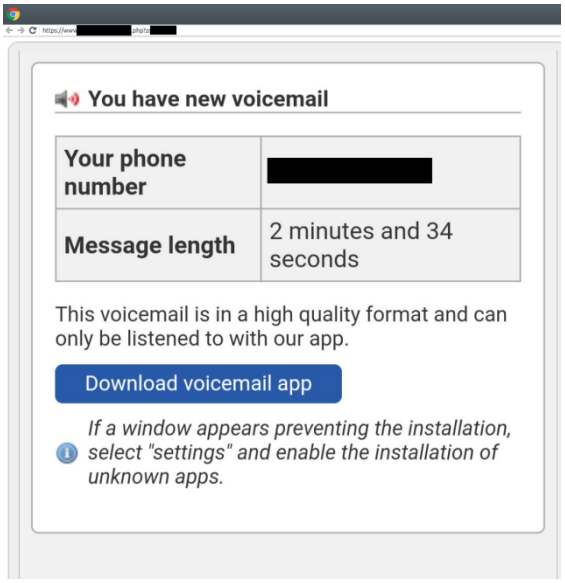
O TeaBot, mostrado na figura 6, é um *Trojan* versátil que foi inicialmente identificado na Itália. Esse *malware* é capaz de roubar informações de *login*, mensagens e também de compartilhar a tela de dispositivos infectados com os invasores. O TeaBot, figura 6, foi configurado para atingir mais de 60 bancos na Europa, com um foco específico em instituições financeiras na Espanha e na Alemanha. Ele se propaga por meio de mensagens *SMS* semelhantes às usadas pelo FluBot como na figura 5 e utiliza técnicas de *keylogging* (registro de teclas digitadas) e interceptação de códigos gerados pelo Google Authenticator. Essas funcionalidades o tornam uma ferramenta poderosa para invadir contas e realizar roubos financeiros nas vítimas.

Figura 5 - Mensagem FluBot.



Fonte: ProofPoint, 2022.

Figura 6 - Mensagem de voz fraudulenta do TeaBot.



Fonte: ProofPoint, 2022.

3. Formas de prevenção

O cenário de ameaças de *malware* em dispositivos móveis está em constante mutação, com novos atores e capacidades emergindo continuamente. Simultaneamente, os métodos de engenharia social empregados pelos atacantes estão sendo aprimorados constantemente. A conscientização é fundamental, mas muitos usuários ainda não compreendem completamente o perigo representado pelo *malware* em dispositivos móveis (MCNEIL E JONES, 2022).

Para proteger seu dispositivo, é importante ficar alerta em relação a mensagens inesperadas ou não solicitadas que contenham *links*, *URLs* ou solicitações de dados. Da mesma forma que fazemos com computadores de mesa e *laptops*, é aconselhável utilizar um aplicativo antivírus móvel de uma fonte confiável. McNeil e Jones (2022), afirma que um estudo recente da Security.org, revelou que 76% dos usuários não têm um aplicativo antivírus instalado em seus *smartphones*.

No artigo escrito por Neris (2023), é passado alguns passos para proteção e garantia à segurança nos dispositivos móveis o máximo possível.

- Manter-se atualizado - Reforçando defesa: Uma das primeiras medidas de segurança contra ameaças cibernéticas envolve manter o sistema operacional e os aplicativos atualizados. Os fabricantes regularmente lançam atualizações de segurança para corrigir vulnerabilidades conhecidas e aprimorar a proteção contra novas ameaças. Essa prática é essencial para reduzir os pontos de entrada potenciais para invasores no dispositivo.

- O Papel do antivírus: Além das atualizações regulares, é crucial instalar um antivírus confiável. Um antivírus robusto não apenas identifica vírus e *malware* conhecidos, mas também oferece uma camada adicional de segurança contra ameaças futuras. É preciso manter o antivírus sempre atualizado para garantir sua eficácia máxima.

- Construindo barreiras virtuais com senhas fortes: A criação de senhas sólidas é um componente fundamental da proteção de seus dispositivos. Ou seja, reforçar é a primeira linha de defesa, faz-se necessário a utilização de senhas complexas para desbloquear os dispositivos. Evitar combinações previsíveis, como datas de nascimento, e opte por senhas que incluam letras maiúsculas, minúsculas, números e caracteres especiais. Essa abordagem torna muito mais difícil para invasores comprometerem a segurança das contas.

- Proteção de contas com senhas robustas: Lembrar-se de que senhas fortes não se aplicam apenas ao desbloqueio do dispositivo. As contas de aplicativos também merecem proteção. Optar por senhas igualmente resistentes para todas as contas nos aparelhos móveis, e evitar reutilizá-las. Dessa forma, mesmo se uma senha for comprometida, as outras contas permanecerão seguras.

- Duplicar a segurança com autenticação de dois fatores (2FA): Aumentar a segurança digital significa adotar medidas além das senhas. A autenticação de dois fatores (2FA) é uma dessas medidas. Além da senha, a 2FA exige um código adicional para acessar a conta. Isso torna praticamente impossível para cibercriminosos obterem acesso não autorizado, pois eles precisam não apenas da senha, mas também do dispositivo associado à conta.

- Navegar com prudência - Ficar à frente: Quando conectado à internet em locais públicos, como cafés e aeroportos, é absolutamente essencial evitar redes *Wi-Fi* públicas não seguras. Em vez disso, utilizar uma *VPN* (Rede Virtual Privada) confiável. Uma *VPN* criptografa os dados, protegendo-os contra olhares curiosos e interceptações indesejadas.

- Cuidado com *links* suspeitos: Uma das estratégias mais comuns usadas por cibercriminosos é atrair vítimas para *sites* maliciosos por meio de *links* suspeitos. Portanto, é crucial manter um olhar crítico sobre os *links* que é recebido em mensagens de texto ou *e-mails*. Evitar clicar em *links* não verificados e sempre verificar a autenticidade das fontes desconhecidas.

- Baixar com confiança: Optar por fontes seguras: Ao fazer o *download* de aplicativos, é crucial escolher fontes confiáveis, como a App Store da Apple ou a Google Play Store. Essas lojas de aplicativos oficiais implementam medidas de segurança rigorosas para minimizar o risco de baixar aplicativos maliciosos. Evitar fontes desconhecidas, pois aplicativos não verificados podem conter *malware* que compromete a segurança do dispositivo.

- Proteja os dados: Uma das etapas mais cruciais para proteger as informações envolve a realização de *backups* regulares. A importância dos *backups* não pode ser subestimada. Manter os contatos, fotos e documentos importantes seguros, fazendo *backup* em um serviço de nuvem confiável ou em um dispositivo externo. Isso garante que, mesmo em caso de um incidente de segurança, os dados permanecerão protegidos e recuperáveis.

Seguindo essas estratégias de proteção, o usuário estará investindo na segurança de dispositivos móveis e na salvaguarda de informações pessoais. A tecnologia e as ameaças cibernéticas estão em constante evolução. Portanto, manter-se vigilante e adotar medidas proativas é fundamental para permanecer um passo à frente dos cibercriminosos. A segurança dos dispositivos está sob responsabilidade do usuário. Certificar de mantê-la constantemente reforçada e pronta para enfrentar qualquer desafio digital que possa surgir.

Por fim, é importante destacar que não é necessário investir em equipamentos caros ou realizar processos complexos para garantir a segurança. Em vez disso, tomar sempre cuidado com os conteúdos acessados e não ficar baixando qualquer coisa de qualquer lugar, ter um antivírus instalado nos dispositivos móveis, já elimina e/ou mitiga grande parte dos problemas já apresentados.

3.1. Desenvolvimento Seguro

Para evitar também ao máximo esse problemas que podem causar em um dispositivo *mobile*, também torna-se necessário o desenvolvimento mais seguro, a fim de evitar que alguma vulnerabilidades possam ser facilmente exploradas, para um desenvolvimento *mobile* deve-se sempre ter em mente alguns pontos específicos, conforme Dsilva (2022)

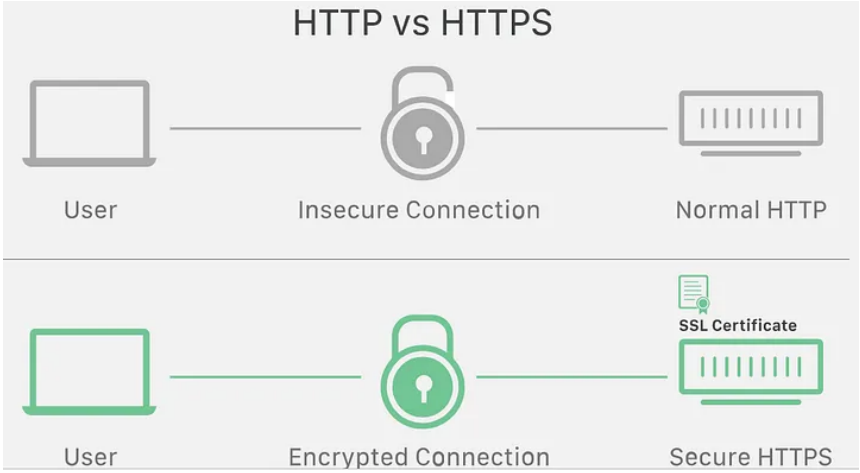
cita em seu artigo que alguns pontos são importantes para desenvolver um código em segurança.

No caso ele aborda aparte de desenvolvimento *mobile*, utilizando Dart/Flutter, *framework* criado pela Google para desenvolvimento multiplataforma, podendo ser desenvolvido aplicativos tanto nativo para iOS quanto para Android. Porém é aplicável a todos os casos de linguagens *front-end*, sendo pontuado algumas das abordagens que Dsilva (2022) cita em seu artigo:

1- Utilizar pacotes ou o mínimo de pacotes possível: Muitas vezes as aplicações não conseguem englobar 100% do que se precisa utilizando a própria linguagem, ou então pode demorar muito para que seja desenvolvido a tarefa, nesses casos, utiliza-se pacotes de terceiros, porém muitas vezes esses pacotes podem ser maliciosos e então deixar falhas ou vulnerabilidades no seu código e aplicação. Por isso sempre utilizar o máximo possível que a linguagem nativa que se está trabalhando, ou pacotes de confiança;

2- Sempre comunicar em *HTTPS* invés de *HTTP*: Caso a aplicação realize algum tipo de comunicação externa seja com um servidor, *API's* ou banco de dados sempre priorizar a utilização de comunicação *HTTPS*, pois esse protocolo encripta a comunicação como mostrado na figura 7, dificultando assim um possível roubo de informação;

Figura 7 - Protocolos de segurança para navegação Web.



Fonte: Ryan Dsilva, 2022.

3- Tratamento adequado das mensagens de erro: Pode parecer algo até meio que idiota, mas muitas vezes erros do servidor podem vir com dados sensíveis, o que ja é um erro, porém não pode-se expor esses dados para os usuários por isso o tratamento correto das mensagens de erro são importante, colocar sempre que possível os blocos de *try-catch* no código, principalmente em comunicações com servidores externos, facilita na trativa do que será mostrado para o usuário no final. Levando em conta o seguinte cenário quando o usuário realizar um *login* numa página qualquer e errar essas credenciais, ao invés de trazer um texto de senha incorreta no campo de senha, seria mais seguro se a aplicação retornar *login* e/ou senha incorreta em um campo separado, englobando os dois campos digitados, dessa forma quem está atacando não saberá discernir qual dos dois estão incorretos, dificultando a invasão.

4- Mínimo de permissões necessária: Quando se desenvolve para aplicativos móveis, torna-se necessário solicitar algumas permissões para acessar conteúdos de caráter nativo como, câmera, pastas, contatos e etc. Porém, sempre que desenvolver um app, tentar-se utilizar apenas as permissões necessárias para o app. Se terá acesso aos contatos, por exemplo, não solicitar essa permissão, assim deixa o app mais confiável e menos suscetível a invasões.

5- Encriptar sempre os dados: Casos de aplicações que trabalham com dados sensíveis de usuários, a grande maioria no caso, ou aplicações que necessitam de uma sessão para permanecerem logadas, sempre encriptar esses dados, pois dessa forma caso haja uma quebra do código do *app*, por mais que ele tenha alguns acessos, a encriptação não deixará ter acesso tão facilmente as informações sensíveis. No caso do Flutter existe um pacote muito conhecido chamado de *flutter_secure_storage*, esse pacote simplesmente salva um par de chaves com valor, porém ele encripta todo o dado colocado nele, deixando muito difícil desencriptar, pois a chave sempre muda, por isso é muito recomendado caso vá guardar essas informações dentro da aplicação. Há outras também, porém essa é hoje a mais segura disponível.

6- Ofuscação do código: Guzman (2023) diz que, a ofuscação de código é a prática de transformar código legível por humanos em código aparentemente sem sentido, tornando mais difícil para o atacante compreender se o pacote da aplicação foi descompilado para fins de engenharia reversa. As plataformas nativas já fazem isso por padrão na versão 2.0 do Flutter, para ofuscar o código Dart, podemos incluir a *flag --obfuscate* juntamente com a *flag --split-debug-info* e a localização dos símbolos de ofuscação. Esses símbolos podem ser usados para converter o código ofuscado de volta em código legível, caso seja necessário solucionar problemas.

7- *SSL Pinning*: O *SSL Pinning* é uma medida de segurança que fixa a identidade de certificados confiáveis em aplicativos móveis e impede que documentos desconhecidos de servidores suspeitos sejam carregados. Aplicativos com certificados *SSL* fixados dependem de seus certificados armazenados, em vez de depender de licenças de autoridade de certificação. Com essa técnica, pode-se fixar o *host* do certificado *SSL* - uma lista de certificados confiáveis - no aplicativo durante o desenvolvimento e posteriormente, comparar os certificados do servidor com a lista durante a execução. Isso ajuda a aumentar a segurança da comunicação entre o aplicativo e os servidores.

Também há outras coisas que devem ser levadas em conta para que haja uma segurança maior no desenvolvimento a fim de proteger o código, como bloquear os screenshots da tela, proteger contra gravações, utilizar-se de dois fatores de autenticação (SILVA, 2022).

Há diversas formas de proteger o código enquanto se trabalha nele, por isso deve-se sempre utilizar o máximo possível dessas formas, com o projeto o qual incluso, nem sempre será disponibilizado o tanto de ferramentas quanto de tempo para implementar todas as forma de segurança, mas utilizar o máximo a dentro do alcance sempre que possível.

4. Conclusão

Para concluir, a importância da segurança em aplicativos móveis, destacando as ameaças comuns, as práticas de desenvolvimento seguro e medidas preventivas. Os dispositivos móveis desempenham um papel crucial em nossas vidas, facilitando o acesso a informações pessoais e profissionais. No entanto, com essa crescente dependência, surgem riscos significativos à segurança.

Focando os três pilares fundamentais da segurança da informação: confidencialidade, integridade e disponibilidade. Cada pilar é explicado em detalhes, ressaltando sua importância na manutenção da segurança dos dados.

Em relação às ameaças em dispositivos móveis, várias categorias são mencionadas, como *malware*, *phishing*, *backdoors*, *ransomware* e muito mais. A gravidade dessas ameaças é acentuada pelo aumento do número de dispositivos móveis em uso, particularmente Android. Além disso, a proliferação de aplicativos não verificados e a vulnerabilidade desses dispositivos tornam a segurança um tópico crucial.

Para prevenir essas ameaças, o artigo fornece dicas úteis, incluindo a importância de manter sistemas e aplicativos atualizados, usar antivírus móveis confiáveis e tomar medidas para proteger suas contas, como usar senhas fortes e autenticação de dois fatores (2FA). Além disso, a navegação segura, o cuidado com *links* suspeitos e o *download* de aplicativos apenas de fontes confiáveis são enfatizados.

No contexto do desenvolvimento seguro de aplicativos móveis, a minimização do uso de pacotes de terceiros, a comunicação segura por *HTTPS*, o tratamento adequado de mensagens de erro, a concessão mínima de permissões, a criptografia de dados e a ofuscação de código. O uso de *SSL Pinning* também é abordado, destacando sua utilidade na validação de servidores.

Em resumo, destaca que, embora a segurança em dispositivos móveis possa ser desafiadora, a conscientização, a educação e a implementação de práticas de segurança eficazes podem reduzir significativamente os riscos e proteger dados pessoais e profissionais. Portanto, é crucial estar ciente das ameaças e tomar medidas proativas para mitigá-las, tanto como usuário quanto como desenvolvedor de aplicativos móveis.

5. Referências

BBC NEWS BRASIL. **Internet móvel:** a revolução tecnológica do smartphone. 07 de dezembro de 2021. Disponível em: <https://www.bbc.com/portuguese/internacional-55973855>. Acesso em: 11 set. 2023.

CASHELL, B.; JACKSON, W.D.; JICKLING, M.; WEBEL, B. The economic impact of cyber-attacks. Government and Finance Division**. Congressional Research Service**. The Library of Congress. 1th Apr, 2004. n. RL32331. Acesso em: 12 set. 2023.

CERT.br. Estatísticas dos incidentes reportados ao CERT.br. 2018. Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 08 Ago. 2023.

DSILVA, R. Securing your Flutter applications. **Medium**. 05 de Julho de 2022. Disponível em: <https://medium.com/flutter-community/securing-your-flutter-applications-77c2bf3ff25e>. Acesso em: 16 Out. 2023.

FELT, A. P.; FINITER, M.; CHIN, E.; HANNA, S.; WAGNER, D. A survey of mobile malware in the wild. 17 de Outubro de 2011. Disponível em: < https://dl.acm.org/doi/10.1145/2046614.2046618>. Acesso em: 17 Ago. 2023.

GOOGLE, INC. The Google android security team's classifications for potentially harmful applications. 2017. Disponível em: < https://developers.google.com/android/play-protect/potentially-harmful-applications?hl=pt-br>. Acesso em: 15 Ago. 2023.

GUZMAN, J. Obfuscate Dart code, Flutter.dev. 07 de Ferevereiro de 2023. Disponível em: <https://docs.flutter.dev/deployment/obfuscate?ref=joshuamdeguzman.com>. Acesso em: 16 Out. 2023.

HINTZBERGEN, J.; HINTZBERGEN, K; SMULDERS, A.; BAARS, H. **Fundamentos Segurança da Informação**: com base na ISO 27001 e na ISO 27002. 3a ed. Rio de Janeiro: Brasport, 2018.

MCNEIL, A. JONES, W. S. Mobile malware threats are surging in Europe: A look at the biggest threats. **ProofPoint.** 09 de março de 2022. Disponível em: <https://www.proofpoint.com/us/blog/email-and-cloud-threats/mobile-malware-surging-europe-look-biggest-threats>. Acesso em: 15 Set. 2023.

NERIS, A. Aprenda a proteger dispositivos móveis contra ameaças cibernéticas. 25 de Agosto de 2023. Disponível em: < https://amti.com.br/blog/aprenda-a-proteger-dispositivos-moveis-contra-ameacas-ciberneticas/>. Acesso em: 27 Out. 2023.

SCHAEFFER, C. “Ataques cibernéticos a smartphones crescem 500%; saiba como se proteger”. **TecMaster**, 12 de março de 2022. Disponível em: <https://tecmasters.com.br/smartphones-ataques-crescem-500-saiba-proteger/>. Acesso em: 15 Set. 2023.

SILVA, G. Flutter Application — how to build a secure app. **Medium**, 21 de Dezembro de 2022. Disponível em: <https://medium.com/@gustavodev60/flutter-application-how-to-build-a-secure-app-9d9441abd068>. Acesso em: 15 Set. 2023.

STATCOUNTER. Desktop vs mobile market share in Brazil - Setembro, 2023

Disponível em: <https://gs.statcounter.com/platform-market-share/desktop-mobile/brazil/#monthly-202007-202308>. Acesso em: 15 Set. 2023.