CST0204-Ameaças, vulnerabilidades e ataques a Segurança Cibernética: Parte 4 - Ataques a dispositivos móveis sem fio

Data do Post	@July 8, 2022 9:00 AM
Status	Done
Palavras-chave	Ameaças vulnerabilidades e ataques a Segurança Cibernética
Fonte	
Pronto	Preparado
IG post	☑
Publicado	☑

Post-Linkedin

A tecnologia evoluiu de tal modo que algumas décadas atrás um computador podia ocupar um espaço de 180 metros quadrados e pesava mais de 30 toneladas. Hoje em dia podemos transportar um computador para qualquer lado que vamos.
A tecnologia também proporcionou-nos a possibilidade usarmos os nossos telefones sem precisarem de estarem conectados por cabos num ponto de acesso instalado por um fornecedor de serviço de telefonia.

Toda essa mobilidade e comodidade gera conforto e permite que tenhamos uma vida mais simples. Mas, com toda essas "boas novas" surgiram situações que colocam em risco a nossa privacidade incluindo os nossos dados.

O artigo de hoje aborda alguns dos ataques que os dispositivos móveis e sem fios estão sujeitos. Leia o artigo na íntegra.

Siga-me e veja outros posts no meu Instagram @idaleciosilvatech
Deixe o like para medirmos a repercussão do conteúdo.
Guarde para rever noutro momento.
Compartilha o conteúdo com os amigos e não só
Comente o que acha do conteúdo e da iniciativa e deixe sugestões.
Link do perfil no IG: https://www.instagram.com/idaleciosilvatech/
#cybersecurity #technology #linux #ataquescibernéticos #hacking #crimesvirtuais #despositivosmóveis #mobilidade #protection

Introdução

O que seria da vida das pessoas se não tivéssemos a mobilidade de comunicação que os telemóveis e computadores portáteis nos oferecem?
Já imaginou voltar no tempo e ter que fazer sempre cabeamento para ter uma ligação de internet na sua casa ou escritório?

Com a evolução das redes móveis foram surgindo novas formas de se conectar a redes e de transmissão de dados. Mas, isso possui o outro lado da moeda - existem riscos e ameaças ao usarmos essas novas tecnologias.

Considere a seguir alguns dos principais ataques a dispositivos móveis e sem fios que todos estamos sujeitos.

Man-In-The-Mobile (MiTMO)

Esse tipo de ataque uma variação do man-in-middle, aonde um atacante procura assumir o controlo de um dispositivo móvel. O dispositivo móvel infectado envia informação sensível do utilizador aos invasores, e da possibilidade que os atacantes capturem silenciosamente mensagens (SMS) de verificação em 2 passos enviadas aos utilizadores. Por exemplo, quando um utilizador configura um Apple ID, deve fornecer um número de telefone compatível com SMS para

receber um código de verificação temporária numa mensagem de texto para provar a identidade do utilizador. O malware espia este tipo de comunicação e retransmite a informação de volta para os criminosos.

Um ataque de retransmissão (replay attack) ocorre quando um invasor captura uma parte de uma comunicação entre dois dispositivos anfitrião e, posteriormente, retransmite a mensagem capturada. Os ataques de retransmissão contornam os mecanismos de autenticação.

Grayware

O Grayware está a tornar-se num problema na segurança móvel com a popularidade dos smartphones. O Grayware inclui aplicações que se comportam de forma irritante ou indesejável. O Grayware pode não ter malware reconhecível oculto, mas ainda pode representar um risco para o utilizador. Por exemplo, o Grayware pode rastrear a localização do utilizador. Os autores do grayware geralmente mantêm legitimidade, incluindo as capacidades de uma aplicação na pequena impressão do contrato da licença de software. Os utilizadores instalam muitas aplicações móveis sem realmente considerar as suas capacidades.

SMiShing

SMiSing é abreviatura de phishing por SMS. SMiSing usa o Serviço de Mensagens Curtas (SMS) para enviar mensagens de texto falsas. Os criminosos enganam o utilizador para ele visitar um ‘website’ ou ligar para um número de telefone. Vítimas inocentes podem então fornecer informação sensível, como os dados de um cartão de crédito. Visitar um ‘website’ pode resultar no utilizador inconscientemente descarregar malware que infecta o dispositivo.

Access points não autorizados

Um ponto de acesso não autorizado é um ponto de acesso sem fios instalado numa rede segura sem autorização explícita. Um ponto de acesso não autorizado pode ser configurado de duas formas:

1. Quando um funcionário bem-intencionado tenta ser útil, facilitando a ligação de dispositivos móveis.
2. Quando um criminoso ganha acesso físico a uma organização, esgueirando-se e instala o ponto de acesso não autorizado.

Visto que ambos não são autorizados, ambos representam riscos para a organização.

Um ponto de acesso não autorizado também pode referir-se ao ponto de acesso de um criminoso. Neste exemplo, o criminoso configura o ponto de acesso como um dispositivo MiTM para capturar a informação de login dos utilizadores.

Um ataque Twin Evil usa o ponto de acesso do criminoso melhorado com antenas de maior potência e maior ganho para se apresentar com uma melhor opção de ligação para os utilizadores. Depois que os utilizadores se ligarem ao ponto de acesso falso, os criminosos podem analisar o tráfego e executar ataques MiTM.

Congestionamento de RF

Os sinais sem fios são suscetíveis à interferência eletromagnética (EMI), interferência de radiofrequência (RFI), e podem até ser suscetíveis a relâmpagos ou ao ruído de luzes fluorescentes. Os sinais sem fios também são suscetíveis as interferências deliberadas. O bloqueio de radiofrequência (RF) interrompe a transmissão de uma estação de rádio ou satélite para que o sinal não atinja a estação recetora.

A frequência, a modulação, e a potência do jammer RF precisam de ser iguais às do dispositivo que o criminoso pretende interromper de modo a interromper com sucesso o sinal sem fios.

Bluejacking e Bluesnarfing

O Bluetooth é um protocolo de curto alcance e baixa potência. O Bluetooth transmite dados numa rede de área pessoal, ou PAN, e pode incluir dispositivos como telemóveis, portáteis e impressoras. Várias versões do Bluetooth já foram lançadas. A fácil configuração é uma característica do Bluetooth, não havendo a necessidade de endereços de rede. O Bluetooth usa o emparelhamento para estabelecer a relação entre dispositivos. Ao estabelecer o emparelhamento, ambos os dispositivos usam a mesma chave de acesso (passkey).

As vulnerabilidades Bluetooth tem surgido, mas devido ao alcance limitado de Bluetooth, a vítima e o atacante precisam de estar no alcance um do outro.

- Bluejacking é o termo usado para enviar mensagens não autorizadas para outro dispositivo Bluetooth. Uma variação disso é enviar uma imagem chocante para o outro dispositivo.

- Bluesnarfing ocorre quando o atacante copia informações da vítima do seu dispositivo. Estas informações podem incluir e-mails e listas de contatos.

Ataques de WEP e WPA

Wired Equivalent Privacy (WEP) é um protocolo de segurança que tentou fornecer uma rede de área local sem fios (WLAN) com o mesmo nível de segurança que uma LAN com fios. Como as medidas de segurança física ajudam a proteger uma LAN com fios, a WEP procura fornecer proteção semelhante para dados transmitidos pela WLAN com criptografia.

O WEP usa uma chave para criptografia. Não há um mecanismo de gestão de chaves com o WEP, portanto, o número de pessoas que partilham a chave crescerá continuamente. Como todos usam a mesma chave, o criminoso tem acesso a um excesso de tráfego para ataques analíticos.

O WEP também tem vários problemas com o seu vetor de inicialização (IV), um dos componentes do sistema criptográfico:

- É um campo de 24 bits, o que é muito pequeno.
- É texto claro, o que significa que é legível.
- É estático, de modo que fluxos de chave idênticos irão se repetir numa rede carregada.

O Wi-Fi Protected Access (WPA) e, depois, o WPA2 surgiram como protocolos melhorados para substituir o WEP. O WPA2 não tem os mesmos problemas de criptografia porque um invasor não pode recuperar a chave através da observação do tráfego. O WPA2 é suscetível ao ataque porque os criminosos virtuais podem analisar os pacotes que viajam entre o ponto de acesso e um utilizador legítimo. Os cibercriminosos usam um packet sniffer e depois executam ataques offline à frase-passe secreta.

Defesa contra-ataques a dispositivos móveis e sem fio

Existem várias medidas a serem tomadas para se defender contra-ataques a dispositivos móveis e sem fios. A maioria dos produtos WLAN usa as configurações padrão. Aproveite os recursos básicos de segurança sem fios, como autenticação e criptografia alterando as configurações padrão.

Restringir o posicionamento do ponto de acesso na rede colocando estes dispositivos fora do firewall ou dentro de uma zona desmilitarizada (DMZ) que contenha outros dispositivos não confiáveis, como servidores de e-mail e Web.

Ferramentas de WLANs, como o NetStumbler, podem descobrir pontos de acesso não autorizados ou estações de trabalho não autorizadas. Desenvolva uma política de convidado para atender às necessidades quando os convidados legítimos precisam se ligar à Internet durante a visita. Para funcionários autorizados, utilize uma rede privada virtual (VPN) de acesso remoto para acesso WLAN.

Outras maneiras de nos proteger contra-ataques a dispositivos móveis sem fios é a utilização de recursos que incluem:

- Bloqueio de tela forçado;
- Limpeza remota do dispositivo;
- Proteção sempre ativa contra malware;
- Prevenção do carregamento paralelo de aplicativos;
- Os dispositivos permanecem seguros mesmo após a redefinição de fábrica;
- Criptografia de dados como padrão;

Todos os dispositivos podem ser visualizados e gerenciados remotamente em caso de perda ou roubo.

Conclusão

Dispositivos móveis são grandes facilitadores para o trabalho remoto. No entanto, a utilização desses aparelhos demanda especial por parte do usuário para evitar riscos e o comprometimento de dados sensíveis.

Uma das medidas válidas é o uso de um antivírus capaz de monitorar periodicamente os dispositivos e assegurar que não representem um problema tanto para a empresa quanto para o usuário.

Siga-me e veja outros posts no meu Instagram @idaleciosilvatech
Deixe o like para medirmos a repercussão do conteúdo.
Guarde para rever noutro momento.
Compartilha o conteúdo com os amigos e não só
Comente o que acha do conteúdo e da iniciativa e deixe sugestões.
Link do perfil no IG: https://www.instagram.com/idaleciosilvatech/
#cybersecurity #technology #linux #ataquescibernéticos #hacking #crimesvirtuais #despositivosmóveis #mobilidade #protection