



E-book

pix Malware

Como os principais malwares
operam contra instituições
financeiras no Brasil

 **AXUR**



Sumário executivo

Desde o lançamento do Pix, em 2020, a Axur tem acompanhado de perto as reações dos cibercriminosos e as tentativas de aplicar fraudes nesse modelo de transação.

O Axur Research Team (ART), nosso time de investigações e engenharia reversa, analisou diversos artefatos para compreender as particularidades técnicas e o funcionamento de cada aplicativo malicioso, além de mapear a infraestrutura tecnológica dos criminosos.

Ao longo dos anos, verificamos que as fraudes ficaram mais sofisticadas, adaptando-se às evoluções das plataformas mobile e às tentativas das instituições financeiras de coibir as fraudes.

A insistência dos criminosos é esperada, uma vez que o Pix se transformou no método preferido dos brasileiros para transferir dinheiro a amigos e pagar contas, sendo utilizado inclusive também para compras on-line e na contratação de serviços.

De acordo com dados do Banco Central, os brasileiros movimentaram R\$ 26,4 trilhões em transferências via Pix durante o ano de 2024, uma alta de 52% em relação ao ano anterior.

Muitas dessas transferências são realizadas pelo canal mobile, o que explica a motivação por trás da criação de softwares maliciosos dedicados a atacar este canal. A Pesquisa Febraban de Tecnologia Bancária 2024, que trouxe os dados de 2023, apontou que Pix é a transação financeira mais realizada no canal mobile, com mais de 16 bilhões de transações – superando inclusive o pagamento de contas.



Além disso, o canal mobile tem crescido todos os anos para quase todos os tipos de interações bancárias, sendo responsável por 70% de todas as transações.

No entanto, o Android e o iOS impõem vários desafios aos criminosos que buscam realizar fraudes no ambiente mobile. Neste relatório, poderemos observar que todas as pragas digitais se destinam exclusivamente a um desses sistemas – o Android.

Isso não significa que o iPhone seja imune a fraudes, mas sim que as fraudes envolvendo aplicativos maliciosos são mais comuns no Android. Afinal, o sistema do Google tem menos restrições para a distribuição de aplicativos do que a plataforma da Apple. Contudo, é possível lembrar que os criminosos também podem realizar outros tipos de fraude que não exigem o uso de aplicativos.

Nesse sentido, outra semelhança perceptível nos golpes que descrevemos aqui é a abordagem "Ghost Hand", que contorna limitações de segurança usando engenharia social para convencer a vítima a conceder permissões de acessibilidade. Assim, o criminoso realiza transferências a partir do aplicativo legítimo instalado no dispositivo do correntista, diminuindo as chances de que a transação seja considerada suspeita por ser realizada a partir de um local ou dispositivo desconhecido.

O que muda de um malware para outro é o nível de sofisticação e a flexibilidade que o golpista tem para atingir um número maior de instituições financeiras e aumentar a probabilidade de que o golpe seja bem-sucedido, seja por garantir que as permissões necessárias sejam concedidas ou por utilizar uma narrativa de engenharia social mais convincente.

Entendendo essas diferenças entre as diferentes famílias de malware e como os criminosos operam seus esquemas fraudulentos, as instituições financeiras podem tomar as medidas necessárias para permanecer um passo à frente dos golpistas, orientando seus clientes ou implementando medidas técnicas que obstruam o funcionamento desses aplicativos maliciosos.



Os pilares dos malwares do Pix



Ghost Hand



MaaS





Ghost Hand

Ghost Hand ("mão fantasma") é uma abordagem para a criação de malwares para Android que utiliza indevidamente os mecanismos de acessibilidade do sistema operacional para extrair informações e interagir com aplicativos.

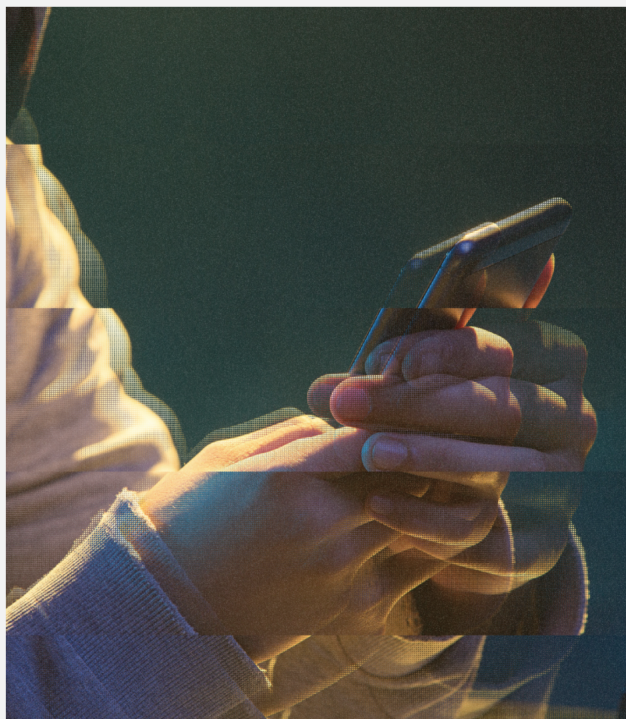
O nome desta abordagem remete à ideia de que os aplicativos maliciosos podem realizar toques na tela e interagir com aplicativos como a "mão" de um usuário fantasma.

Ao contrário do Windows e outros sistemas para desktop, o Android minimiza as possibilidades de interação entre os aplicativos e o acesso às informações digitadas no teclado virtual. Além disso, a maioria dos smartphones não permite que aplicativos assumam o controle total do dispositivo com permissões de superusuário (root).

Essas medidas de segurança bloqueiam o roubo de informações e a leitura das informações exibidas por outros aplicativos, impedindo a criação dos mesmos tipos de pragas digitais que existem no desktop.

Os recursos de acessibilidade do Android contornam quase todas essas restrições, uma vez que os apps que auxiliam pessoas com deficiência precisam ser capazes de ler qualquer informação e interagir com o sistema como se fosse o usuário.

Para restringir o uso indevido da acessibilidade, o Android vem aumentando as restrições e os alertas exibidos para os usuários durante a configuração desse tipo de serviço. Para os criadores de malware, isso significa que é preciso criar narrativas de engenharia social que não acabam com a instalação do aplicativo malicioso, como ocorre em computadores. A narrativa precisa sustentar alguma razão para convencer a vítima a também conceder as permissões de acessibilidade que viabilizam o uso da abordagem Ghost Hand.





MaaS

O conceito de malware-as-a-service (malware como serviço) descreve um arranjo criminoso em que um indivíduo ou grupo desenvolve um software malicioso e comercializa o acesso a ele, normalmente por meio de uma assinatura periódica, para que outros criminosos se encarreguem da distribuição e uso do malware.

Nesse arranjo, vários golpistas financiam o desenvolvimento de uma mesma praga digital, aumentando os recursos disponíveis para a sofisticação do software. Por outro lado, também significa que há muitos ataques tecnicamente semelhantes por utilizarem as mesmas ferramentas.

Como a comercialização desses softwares ocorre em canais criminosos, também é possível colher inteligência a partir das explicações fornecidas pelos próprios criminosos.



Os malwares do Pix



PixStealer



MalRhino



BrasDex



PixPirate



GoatRAT



FantasyMW



PixBankBot



CriminalMW



PixPirate 2



GhostSpy



PixStealer



Detectado:
Julho de 2021

O PixStealer definiu as características fundamentais dos golpes realizados com malware especializados em transferências Pix. Por regra, esses aplicativos falsos precisam convencer a vítima a autorizar o uso do serviço de acessibilidade do Android, exigindo uma narrativa de **engenharia social**.

No caso do PixStealer, os golpistas conseguiram cadastrar aplicativos no Google Play, a loja oficial de aplicativos do Android, usando termos como **"CashBack"** e outras promessas chamativas.

Após orientar a vítima a abrir o aplicativo bancário, o PixStealer usa a Acessibilidade do Android e a técnica Ghost Hand para **ler do saldo da vítima e realizar uma transferência Pix** com todo o valor disponível.

Durante a fraude, o PixStealer exibe uma tela sobreposta com o texto "Sincronizando seu acesso" para esconder as atividades do malware e evitar que o correntista possa acompanhar a realização da transferência ilegítima.

```
public void teste(AccessibilityNodeInfo paramAccessibilityNodeInfo, int paramInt) {
    if (mInstance == null)
        return;
    if (paramAccessibilityNodeInfo == null)
        return;
    try {
        Rect rect = new Rect();
        this();
        paramAccessibilityNodeInfo.getBoundsInScreen(rect);
        if (paramAccessibilityNodeInfo.getViewIdResourceName() != null && paramAccessibilityNodeInfo.getViewIdResourceName().equals("android:id/statusBarOverride")) {
            if (paramAccessibilityNodeInfo.getText().toString().contains(".")) {
                mostrar_saldo();
            } else {
                Log.d("aok", paramAccessibilityNodeInfo.getText().toString());
                Configuracoes.setString((Context)mInstance, "valor", paramAccessibilityNodeInfo.getText().toString());
                this.Utills.Telas.Abre();
                this.Utills.Telas.Abre_TravaBlock();
                clicar_pix();
            }
        }
        if (paramAccessibilityNodeInfo.getText() != null) {
            if (paramAccessibilityNodeInfo.getText().toString().contains("utilizando a chave ou os"))
                clicartf();
            if (paramAccessibilityNodeInfo.getText().toString().contains("CPF ou CNPJ"))
                clicarCPF();
            if (paramAccessibilityNodeInfo.getText().toString().contains("Insira o CPF ou CNPJ"))
                escreverCPF();
            if (paramAccessibilityNodeInfo.getText().toString().contains("Insira a descrição"))
                clicar_descricao();
        }
    } catch (Exception e) {
        Log.e("aok", e.getMessage());
    }
}
```




MalRhino



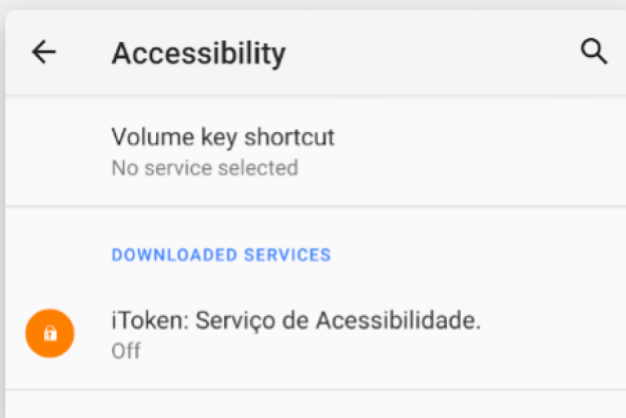
Detectado:
Julho de 2021

O MalRhino é assim chamado por ser desenvolvido com a biblioteca rhino-android, uma versão do RhinoJS adaptada para uso no Android. Embora seja uma biblioteca de código aberto legítima criada para facilitar a criação de aplicativos em JavaScript, essa particularidade acabou por definir essa família de aplicativos fraudulentos.

Os códigos JavaScript executados pela biblioteca podem ser obtidos de fontes online, permitindo que as capacidades do MalRhino sejam facilmente ampliadas ou atualizadas.

Os criadores do MalRhino tiraram proveito dessa facilidade de desenvolvimento para criar um malware mais sofisticado que o PixStealer, já sendo capaz de **criar telas falsas para solicitar PIN, interagir com outros aplicativos, realizar gestos e digitar textos**.

Assim como a maioria dos malwares que viriam depois dele, o MalRhino já contava com uma infraestrutura de Comando e Controle (C2).





BrasDex

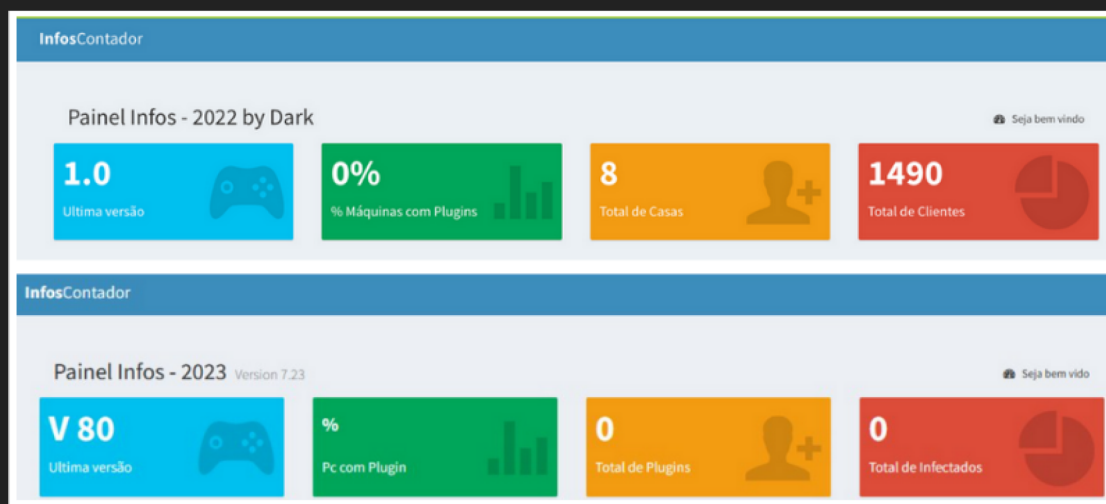


Detectado:
Dezembro de 2022

Utilizando os mesmos princípios já estabelecidos pelo PixStealer e pelo MalRhino, o BrasDex demonstrou sofisticação usando um painel gráfico em sua infraestrutura C2.

Já o aplicativo falso chamou atenção pelos recursos antiemulação.

O BrasDex verifica as características do hardware e não funciona corretamente em emuladores ou outros ambientes virtuais, demonstrando a intenção de dificultar a engenharia reversa do malware.





PixPirate



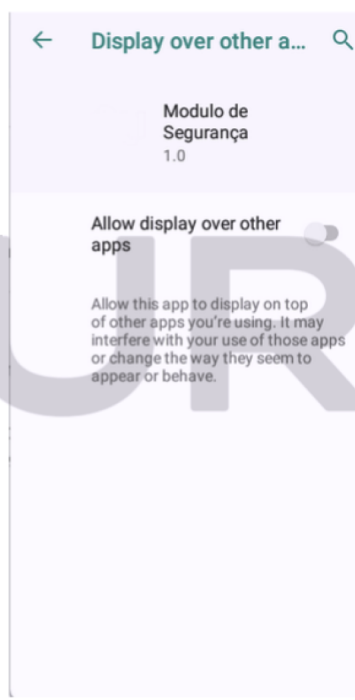
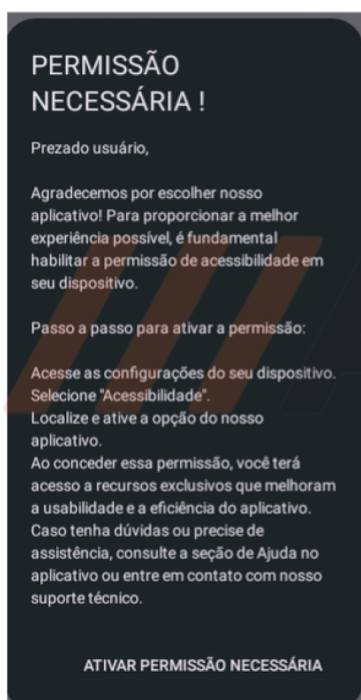
Detectado:
Fevereiro de 2023

Seguindo a tendência de desenvolvimento em JavaScript já vista no MalRhino, o PixPirate foi desenvolvido com o Auto.js, um framework para criar automatizações usando os serviços de acessibilidade do Android.

Além das automatizações ligadas ao Pix, o PixPirate também é capaz de **interceptar mensagens SMS e enviar mensagens para os contatos da vítima no WhatsApp** através de um módulo chamado wsMine.js.

Outro diferencial do PixPirate é o uso dos recursos de acessibilidade para **impedir que o dono do aparelho desinstale o aplicativo malicioso**.

Além dos serviços de acessibilidade, a engenharia social dessa fraude tenta convencer a vítima a permitir que o aplicativo falso instale outros aplicativos, escondendo o malware da tela inicial (Launcher) do smartphone.



Narrativa de engenharia social do PixPirate promete ganhos financeiros para a vítima em troca de permissões especiais que o malware precisa para funcionar.



GoatRAT



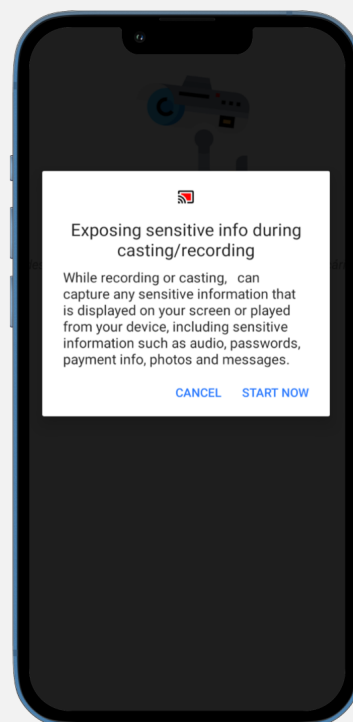
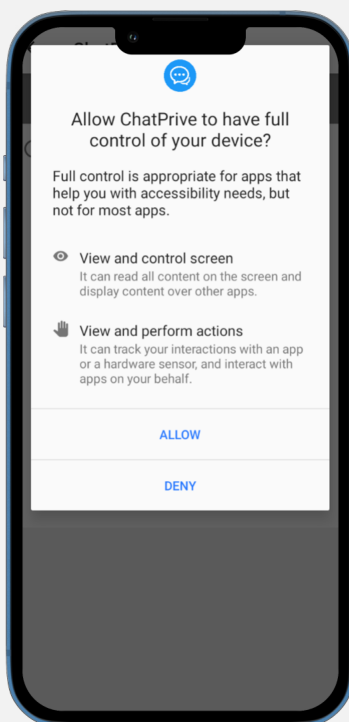
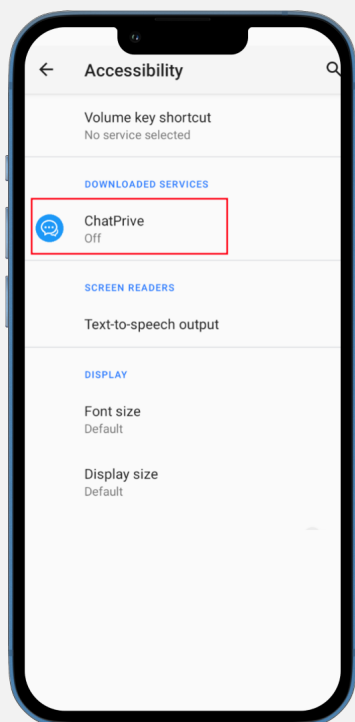
Detectado:
Março de 2023

Ao contrário dos outros malwares dedicados à realização de transferências Pix, o GoatRAT faz parte de uma classe de programas maliciosos de administração remota, como seu nome sugere (RAT é a sigla para Remote Administration Tool).

Apesar de sua funcionalidade não ter sido criada especificamente para o Pix, módulos foram criados para realizar operações em aplicativos bancários brasileiros, permitindo que toda a capacidade do malware fosse aproveitada nas fraudes com Pix.

Por ser um RAT, esse malware é capaz de simular quase qualquer interação por meio dos serviços de acessibilidade: tocar na tela, deslizar (swipe), digitar, abrir notificações e enviar aplicativos para o segundo plano. Essas funções podem ser usadas em conjunto com a gravação e transmissão da tela utilizando o Janus para controlar o smartphone remotamente.

Sua infraestrutura C2 utiliza a rede de chat Discord por meio de webhooks, dispensando a criação de uma infraestrutura própria para esse fim.



Além da acessibilidade, o GoatRat também pede outras permissões para interagir com o sistema e gravar a tela.



FantasyMW



Detectado:
Abril de 2023

O FantasyMW, também chamado de FantasyRAT, é uma versão personalizada do GoatRAT focada em fraudes no Pix.

Graças aos recursos do GoatRAT, esse malware alcança uma sofisticação considerável, trazendo recursos como o bloqueio de desinstalação e uma verificação regular das permissões necessárias para o funcionamento da fraude

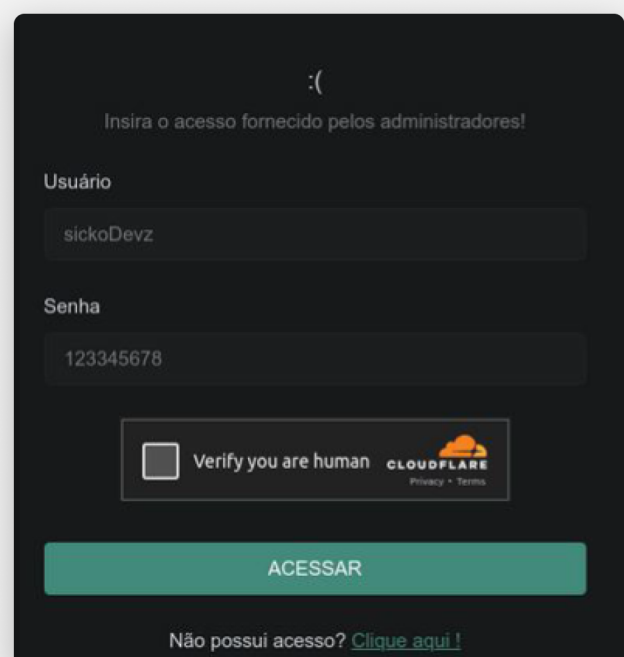
Caso alguma das permissões necessárias não esteja disponível, o malware insistirá para que a vítima conceda as permissões. Em algumas versões do malware, o nome do serviço de

acessibilidade é chamado de "Investimentos" para aumentar a chance de que a vítima autorize a solicitação.

Assim como outros malwares, é utilizada uma tela sobreposta (overlay) para ocultar a operação fraudulenta, que transfere todo o saldo da vítima. Para facilitar a operação do malware, a infraestrutura C2 foi personalizada e simplificada, como normalmente ocorre em ferramentas oferecidas na modalidade de malware como serviço (MaaS).



Mensagem promovendo o FantasyMW/FantasyRAT



Painel de controle da infraestrutura de C2 do FantasyMW



PixBankBot



Detectado:
Maio de 2023

O PixBankBot foi observado usando uma narrativa de engenharia social envolvendo a leitura de um suposto **documento PDF** para justificar a concessão das permissões de acessibilidade, demonstrando algumas características únicas das campanhas de fraude com esse malware.

Outra característica deste malware é o uso de **endereços do site Pastebin** para extrair as chaves Pix que serão usadas na fraude. Em paralelo, o malware utiliza uma infraestrutura de Comando e Controle para enviar detalhes das operações executadas e informações do dispositivo e da conta bancária da vítima.

O malware não realiza transferências quando o saldo da vítima é inferior a R\$ 500. Essa decisão pode ter sido tomada para evitar que vítimas com saldo menor percebam a atividade maliciosa, aumentando as chances de que pessoas com saldo elevado sejam vítimas da fraude.





CriminalMW

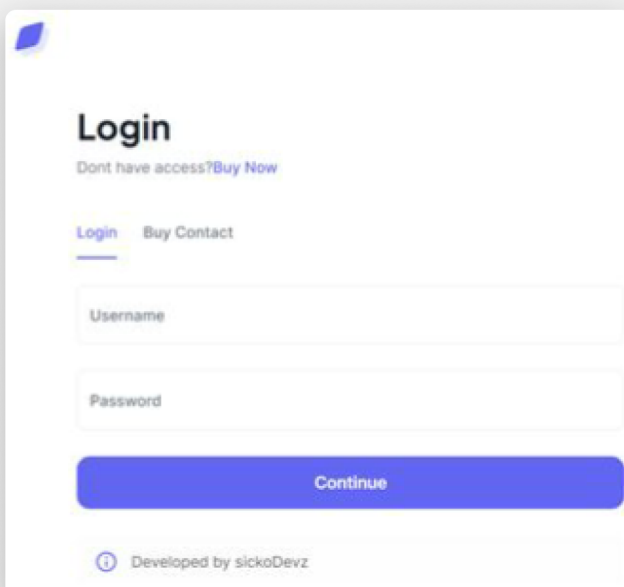


Detectado:
Julho de 2023

O CriminalMW é uma versão atualizada do FantasyMW que promete realizar fraudes "sem muito esforço". Assim como o FantasyMW, é comercializado para outros criminosos e configurado por meio de um painel de controle personalizado.

O serviço de acessibilidade passou a ser chamado de "Módulo de Segurança", o que ajuda a evitar que a vítima fique desconfiada nos casos em que o sistema do smartphone exibe uma notificação a respeito da ativação da acessibilidade.

Essa versão do malware é capaz de monitorar a execução de pelo menos 16 aplicativos bancários. Ele exibe telas falsas sobrepostas para esconder sua atividade personalizadas para cada instituição.



Painel de controle do CriminalMW para criminosos que adquiriram o direito de usar o malware.



PixPirate 2



Detectado:
Março de 2024

O PixPirate 2 é bem semelhante à primeira versão. Também foi desenvolvido com Auto.js e ainda solicita permissões para instalar outros aplicativos. No entanto, as funcionalidades do malware foram simplificadas e atualizadas. O componente wsMine.js, que enviava mensagens por WhatsApp de acordo com instruções recebidas do servidor de comando e controle, foi removido desta versão.

Os arquivos do malware sugerem que ele é compatível com aplicativos de 14 instituições financeiras.

A principal mudança técnica do PixPirate 2, no entanto, está no método utilizado para monitorar as notificações, que passou a usar um recurso do Android apropriado para esse fim, de modo que o próprio sistema chama o serviço do malware quando há uma nova notificação.

O monitoramento de notificação pode ser usado para que o malware leia códigos de segurança ou outras informações sobre as transações realizadas.





GhostSpy



Detectado:
Novembro de 2024

O GhostSpy é o quarto malware da linhagem do GoatRAT, sendo a versão atualizada do CriminalMW. Ele chega ao smartphone da vítima como um Loader, ou seja, um malware responsável por instalar outro aplicativo em plano de fundo e esconder o software que foi instalado no dispositivo.

Ao ser executado, ele solicita as permissões de Acessibilidade e envia a lista de aplicativos instalados para o servidor C2. É possível que essa lista possa ser usada para enviar instruções específicas ao malware, especialmente porque o GhostSpy também envia imagens da tela e gravações do microfone da vítima ao criminoso. Um dos destaques do GhostSpy é a capacidade de monitorar mensagens SMS e apagá-las para que a vítima não seja notificada sobre as transações bancárias irregulares.

✓ Correção do Google Play Protect: O aplicativo não é mais detectado como vírus.

✓ Maximização: Tornamos o sistema ainda mais leve.

✓ Velocidade: Melhoramos significativamente o controle do dispositivo.

✓ Java Atualizado: Painel atualizado com a versão mais recente do Java.

✓ Criptografia AES: Adicionamos uma nova camada de segurança para maior proteção.

✓ Inteligência Artificial: Incorporamos IA no código para contornar mecanismos de segurança em aplicativos com flags avançadas contra acesso remoto.

Contato: @ghostspyvip

```
private void getAllSMS() {  
    Uri inboxUri = Uri.parse("content://sms/inbox");  
    Cursor cursor = getContentResolver().query(inboxUri, null, null, null, null);  
    if (cursor != null && cursor.moveToFirst()) {  
        do {  
            String address = cursor.getString(cursor.getColumnIndexOrThrow("address"));  
            String body = cursor.getString(cursor.getColumnIndexOrThrow("body"));  
            String date = cursor.getString(cursor.getColumnIndexOrThrow("date"));  
            System.out.println("From: " + address + ", Message: " + body + ", Date: " + date);  
        } while (cursor.moveToNext());  
        cursor.close();  
    }  
}
```

Código responsável por ler as mensagens SMS.



Conte com quem tem experiência

A Axur dispõe de uma equipe especializada em análise de artefatos maliciosos que conhece a realidade brasileira e acompanha diariamente as mudanças no cenário de ameaças e fraudes.

A plataforma Axur oferece uma solução abrangente e avançada para o combate a fraudes que ocorrem fora do perímetro corporativo, detectando campanhas phishing, domínios maliciosos e aplicativos mobile que usam sua marca de forma indevida para prejudicar a experiência dos seus clientes.



Por meio da nossa plataforma, é possível criar fluxos de automação para mitigar o impacto das fraudes, graças à taxa de sucesso de 98.9% do nosso Takedown.

Para quem precisa conhecer as fraudes a fundo, o Axur Research Team (ART) produz relatórios e realiza investigações para que você tenha uma visão completa das ameaças.

Conheça nossas
soluções para
instituições
financeiras

CLIQUE AQUI E SAIBA MAIS



Descubra todas as nossas soluções em axur.com

///AXUR