aPIXcalipse

Como o PIX influenciou os golpes digitais e turbinou o cibercrime

Anchises Moraes

Apura Cyber Intelligence

bttNG boitatá

apura

Contributor
2023 Verizon Data Breach Investigations Report

AGENDA

Sério, preciso explicar o que é o PIX?

Aspectos negativos do PIX

Seis Ondas de ataque

Mais alguns golpes com PIX

Faz um PIX ?

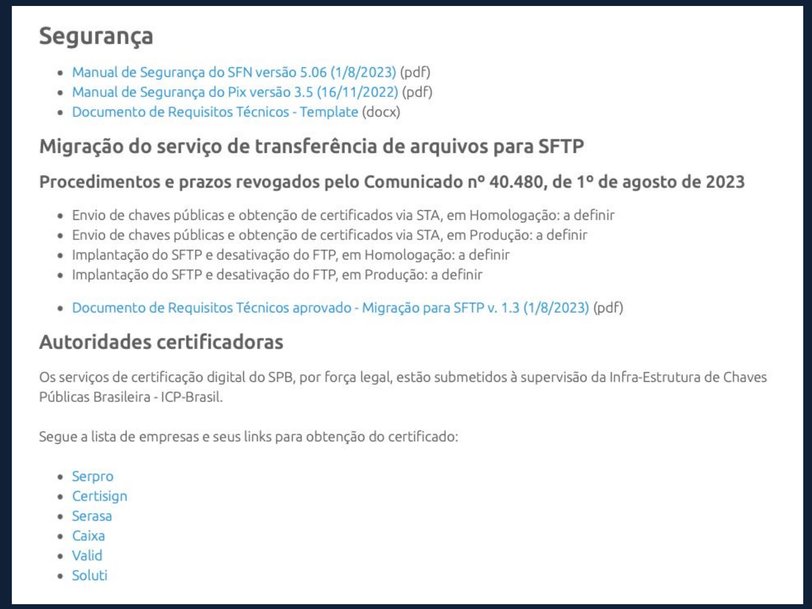
Lançado em Outubro/2020

Sim, é seguro !

Adoção muito rápida

Aumentou o uso de aplicativos bancários

Tempo de transação caiu de 1 hora (ou 1 dia) para 1 segundo



Segurança

- Manual de Segurança do SFN versão 5.06 (1/8/2023) (pdf)
- Manual de Segurança do Pix versão 3.5 (16/11/2022) (pdf)
- Documento de Requisitos Técnicos - Template (docx)

Migração do serviço de transferência de arquivos para SFTP

Procedimentos e prazos revogados pelo Comunicado nº 40.480, de 1º de agosto de 2023

- Envio de chaves públicas e obtenção de certificados via STA, em Homologação: a definir
- Envio de chaves públicas e obtenção de certificados via STA, em Produção: a definir
- Implantação do SFTP e desativação do FTP, em Homologação: a definir
- Implantação do SFTP e desativação do FTP, em Produção: a definir

- Documento de Requisitos Técnicos aprovado - Migração para SFTP v. 1.3 (1/8/2023) (pdf)

Autoridades certificadoras

Os serviços de certificação digital do SPB, por força legal, estão submetidos à supervisão da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil.

Segue a lista de empresas e seus links para obtenção do certificado:

- Serpro
- Certisign
- Serasa
- Caixa
- Valid
- Soluti

Fonte: Banco Central

Eu pixo
Tu pixas
Ele Pixa
Nós pixamos
Vós pixais
Eles pixam

Fonte: Banco Central, 16/11/2023

Aspectos negativos

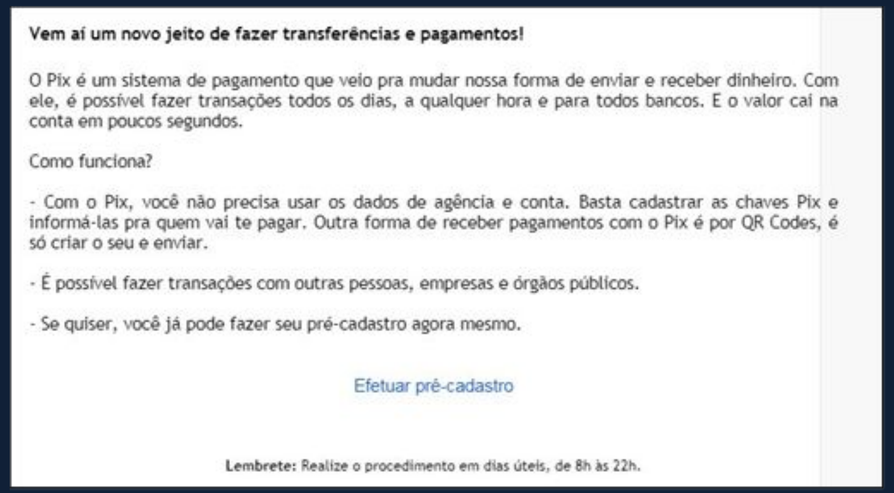
> **Desinformação** explorada por golpistas

> **Rápido e fácil** para transferir fundos roubados

> Criminosos fazem o dinheiro “desaparecer” rapidamente, pulverizado em muitas contas bancárias

> Cibercrime e fraude viram **24 x 7** **:(**

Onda #1 Cadastro de chave PIX



Vem aí um novo jeito de fazer transferências e pagamentos!

O Pix é um sistema de pagamento que veio pra mudar nossa forma de enviar e receber dinheiro. Com ele, é possível fazer transações todos os dias, a qualquer hora e para todos bancos. E o valor cai na conta em poucos segundos.

Como funciona?

- Com o Pix, você não precisa usar os dados de agência e conta. Basta cadastrar as chaves Pix e informá-las pra quem vai te pagar. Outra forma de receber pagamentos com o Pix é por QR Codes, é só criar o seu e enviar.

- É possível fazer transações com outras pessoas, empresas e órgãos públicos.

- Se quiser, você já pode fazer seu pré-cadastro agora mesmo.

Efetuar pré-cadastro

Lembrete: Realize o procedimento em dias úteis, de 8h às 22h.

E-mail de phishing identificado pela Kaspersky usava o Pix como isca

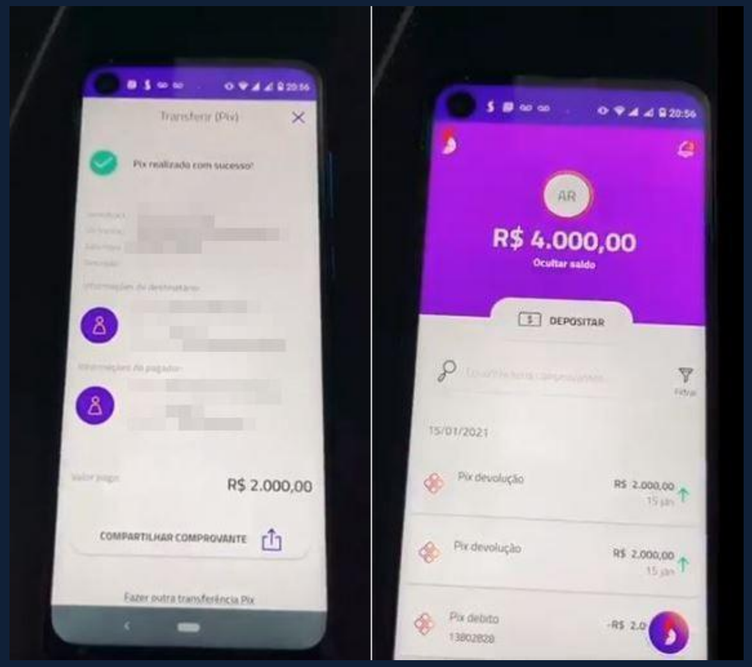
> Usuários precisam cadastrar sua **Chave PIX** (ID único) para realizar transferências eletrônicas

> Golpes de **phishing** surgiram rapidamente (SMS e e-mail)

> Sites maliciosos com logins/formulários falsos para permitir que as pessoas “registrem” suas chaves

Imagem: Kaspersky

Onda #2
Bugs no PIX e Robô do PIX



> Poucos casos de bugs em alguns aplicativos bancários após o lançamento do PIX inspiraram o **boato** de que bugs ou chaves PIX específicas causariam devolução de dinheiro à mais

> Vídeos falsos no YouTube mostravam supostos bugs e prometiam "dinheiro em dobro"

> Os golpistas publicavam sua própria Chave PIX para receber as transferências

Imagem: Canaltech

Onda #2
Bugs no PIX e Robô do PIX

> Golpistas oferecem esquema de **"investimento"** com PIX

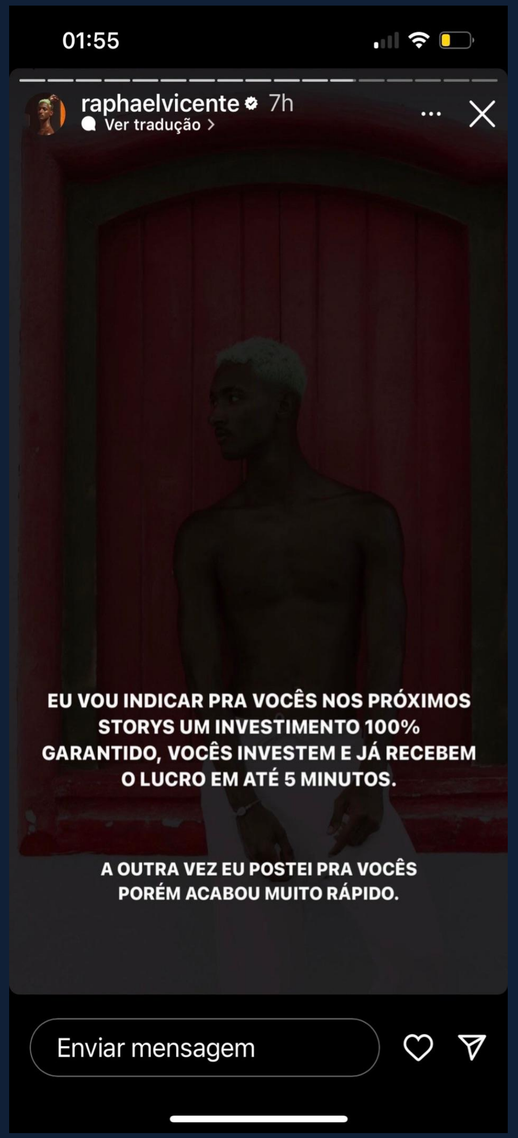
> Promessa de receber uma grande quantia de dinheiro se fizer a transferência para uma chave PIX específica

> Alguns afirmam que isso é possível devido a um bug do PIX

Imagem obtida no Instagram

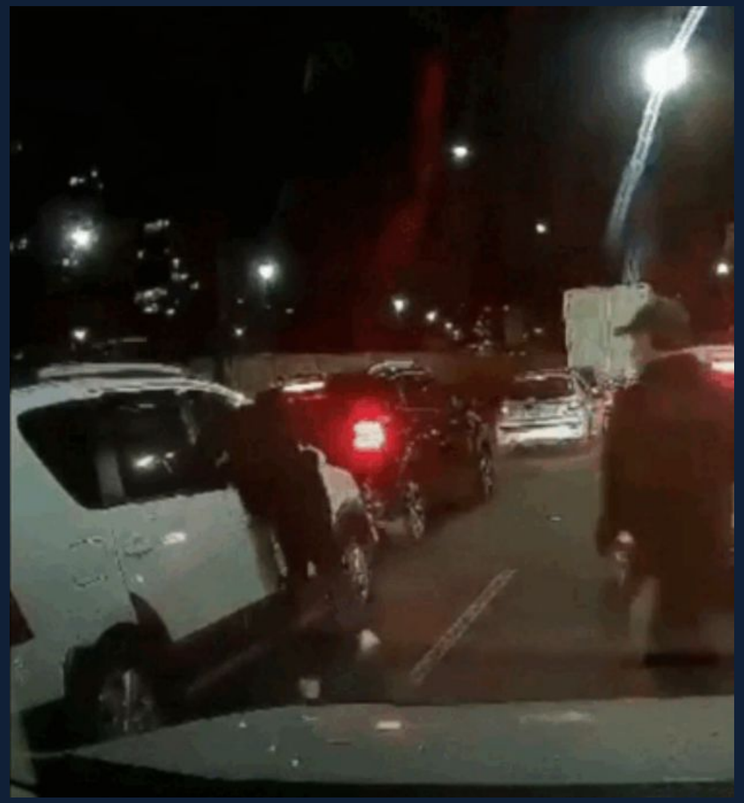
Onda #2
Bugs no PIX e Robô do PIX

Caso recente (01/12/2023)



Imagens obtidas no Instagram

Onda #3 Aparelho celular vira alvo



- Sequestro relâmpago ressurge
- Roubo/furto de celulares para **acesso a apps bancários** das vítimas

Imagem da Internet

Onda #3
Aparelho celular vira alvo

Reação dos Bancos:

> Configurar limites de transferência mais baixos à noite

> “Locais seguros”: locais configurados pelo usuário, com limites menores e sem acesso a investimentos

> Seguro

Onda #4
Contas Laranjas com esteróides

> Grande **demanda** por contas de laranja
  - **Contas fake, aluguel de contas**
> PIX usado para transferência de fundos após acesso às contas das vítimas
> Fundos enviados para contas diferentes em poucos minutos
> Difícil ser rastreado e recuperado

Imagem: BTTng / Telegram

Onda #4
Contas Laranjas com esteróides

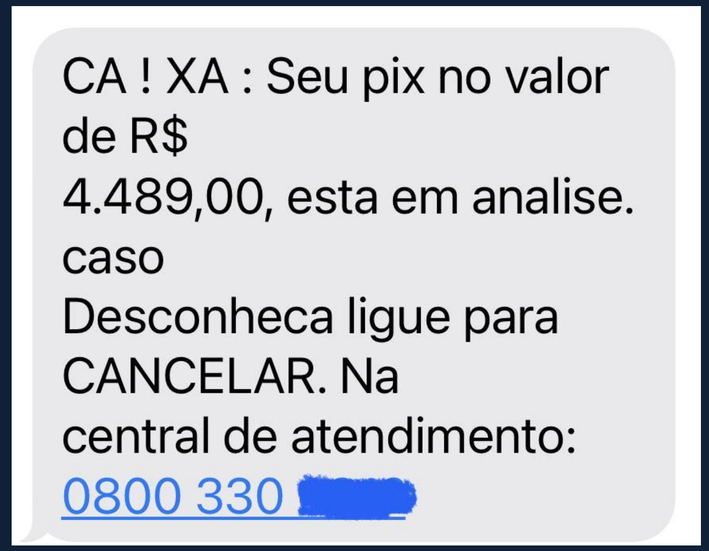
Reação dos Bancos:

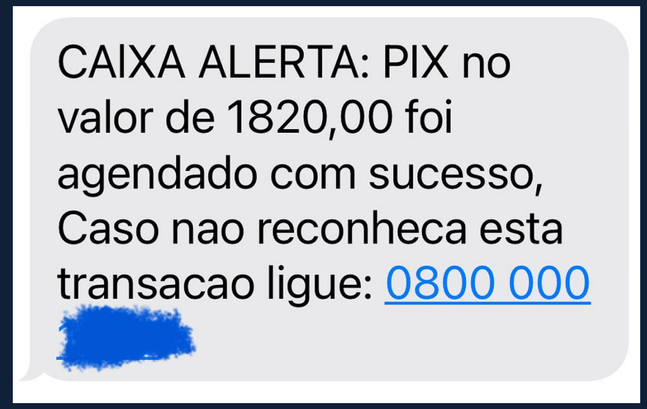
> “Mecanismo Especial de Devolução” (MED)

> Clientes podem solicitar a devolução do dinheiro após realizar uma transação
… se o dinheiro ainda estiver na conta de destino !

> Criminalização do "aluguel de contas"

Onda #5 Golpes com tema do PIX





- Alerta / mensagem de confirmação de **transação falsa** via PIX
- Pede às vítimas que entrem em contato com o banco por meio de um número 0800 falso (falsa central de atendimento)

Imagem: Arquivo pessoal

Onda #6
Vírus do PIX

Nove famílias de trojans bancários direcionados a transações PIX desde Dezembro/2022

> PixStealer/MalRhino

> BrazKing

> PixPirate

> BrasDex

> GoatRAT

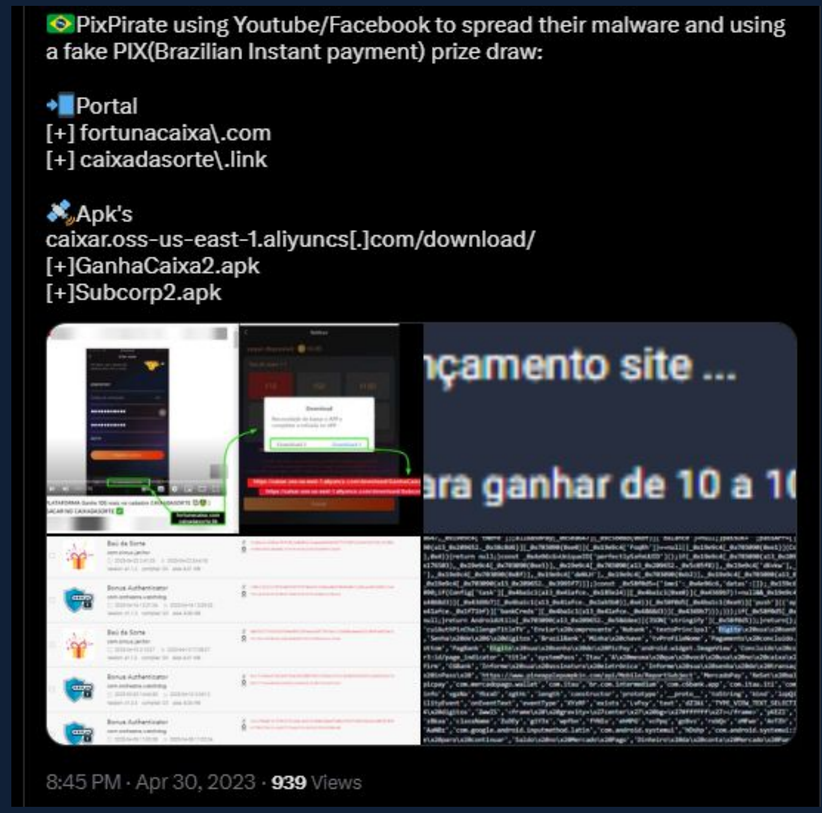
> PixBankBot

> Brat

> GoPIX

> ParaSiteSnatcher (*)

(*) Extensão maliciosa do Chrome



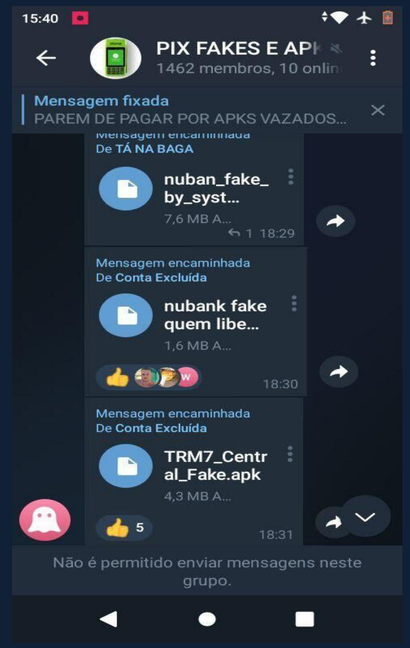
Onda #6
Vírus do PIX

> Direcionados a celulares **Android**

> Infecção via **engenharia social** na vítima

> Técnicas de acesso remoto (RAT) ou automação (ATS)

Outros golpes



- Falsos comprovantes de PIX
- Golpe da quitação de empréstimo e dívidas (desconto para pagamento via PIX)
- Quishing com chaves PIX / Pagamentos com PIX

Lições Aprendidas

> Mais países adotando sistemas de pagamento similares (A2A)

> Difícil detectar e interromper transações instantâneas

> As abordagens antifraude tradicionais não são suficientes

> O cibercrime reage muito rapidamente

> A população está desprotegida !

Dúvidas?

Anchises Moraes

Threat Intel Lead

@anchisesbr

www.apura.com.br

@mastersofpwnage

Mantenha-se atualizado

www.apura.com.br

news.apura.com.br

Mantenha-se atualizado

- news.apura.com.br
- anchisesbr.blogspot.com
- Cartilhas do CERT.br
  https://cartilha.cert.br
- E-book "É bom demais para ser verdade"
  https://occ.org.br/e-book-50-tipos-golpes-digitais/
- Portal da Febraban:
  https://antifraudes.febraban.org.br
- Perfis no Instagram:
  - Delegado Barreto: @delbarreto19
  - Delegado Meneses: @delegadomeneses
  - Dicas de Cyber Segurança: @dicasdecyberseguranca
  - Proteção Digital para Você: @protecaodigitalpravc
  - Um Golpe por Dia: @umgolpepordia

APURA CYBER INTELLIGENCE

Empresa 100% brasileira especializada em:

> **segurança e inteligência cibernética** e

> **apuração em meios digitais**.

Desenvolvedora do **BTTng** - poderosa plataforma de inteligência em fontes abertas (OSINT) e inteligência em ameaças cibernéticas (CTI).

O **BTTng** engloba um completo pacote de serviços que envolve desde **ações de busca ativa de ameaças em fontes abertas**, até **configuração direcionada dos robôs de coleta**, além de disponibilizar **boletins** frequentes sobre ameaças e incidentes em destaque no cenário de cibersegurança nacional e internacional.

Benefícios de uma plataforma e serviço especializado em Osint

- Coleta de informações em fontes abertas (meios digitais);
- Automação na coleta e correlacionamento dos eventos;
- Proteção dos executivos;
- Proteção da marca;
- Melhores e mais precisas informações para o time de resposta à incidentes;
- Alertas mais proativos relativos a fraudes e vazamentos de dados;
- LGPD/GDPR: melhora na conformidade antevendo ameaças e traçando melhores estratégias de proteção e detecção de vazamentos, de incidentes de segurança e golpes;
- Monitoramento de fraudes, golpes, risco cibernético, problemas com segurança física, monitoramento de marca, campanhas de *phishing*, vazamento de credenciais e informações, *hacktivismo*, etc.

APURA CYBER INTELLIGENCE S/A

BRASÍLIA
SHN Quadra 1 Lote A,
Ed. Le Quartier, 14o andar
CEP: 70.701-010
Telefone: 61 3255-1245

SÃO PAULO
Av. Paulista 2.421, 1o andar
CEP: 01310-300
Telefone: 11 5504-1966