BOLETIM DE SEGURANÇA

Novo golpe desvia pagamentos via PIX em compras online pelo método de copiar e colar

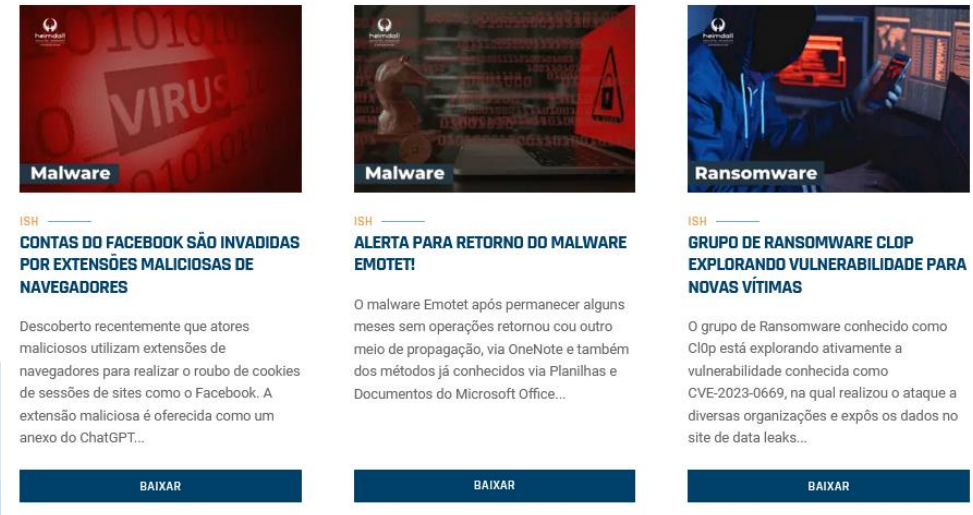
heimdall
security research
A DIVISION OF ISH

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



heimdall
security research

Sumário

Lista de Tabelas

1 SUMÁRIO EXECUTIVO

O PIX, sistema de pagamentos instantâneos do Brasil, oferece conveniência e eficiência para transações financeiras. No entanto, como muitas tecnologias que surgem, este também, tornou-se um alvo para fraudadores. Golpes via PIX têm se proliferado, colocando usuários e instituições financeiras em alerta. Esses golpes variam em complexidade, indo desde engenharia social simples até operações sofisticadas de phishing e malwares. As táticas comuns incluem solicitações fraudulentas de pagamento, mensagens de texto ou e-mails falsos que direcionam os usuários para sites de phishing. A velocidade do PIX, que é um de seus maiores atrativos, também facilita a ação rápida dos fraudadores antes que as vítimas ou os bancos possam reagir.

Recentemente pelo identificado pela **Kaspersky** um novo golpe via meios de pagamentos Pix. A fraude que envolve o desvio de pagamentos via PIX em compras online pelo método de copiar e colar tem atraído atenção recentemente.

2 FUNCIONAMENTO DO GOLPE

O golpe envolvendo desvio de pagamentos PIX através da técnica de copiar e colar em compras online foi descoberto pela empresa de segurança digital Kaspersky e tem atraído atenção recentemente. Abaixo, damos detalhes de como o golpe funciona:

Infecção inicial

- A infecção acontece pelo vírus, chamado GoPIX, começa com anúncios maliciosos no Google. Os criminosos compram espaço para anúncios no motor de busca e usam termos com erros de ortografia, como "WhatsApp Web" ou "Correios", para atrair e enganar as vítimas.

Execução do golpe

- Quando a pessoa clica no anúncio fraudulento, seu computador é infectado com o GoPIX, que então monitora a vítima e detecta quando ela realiza uma compra online e escolhe o pagamento via **PIX copia e cola**.
- Na tela de pagamento, quando o cliente copia um código e o cola no sistema PIX para realizar o pagamento, o malware intercepta esse código e o altera, inserindo a chave PIX do criminoso no lugar da chave da loja, desviando assim o pagamento para a conta do criminoso.

Aspectos técnicos

- O golpe é executado através de um vírus que afeta apenas computadores, alterando o código PIX copiado para o pagamento no site do banco, sendo que o esquema instala o vírus na máquina da vítima e, ao fazer o pagamento de uma compra, o malware intercepta o código e faz a alteração necessária para que o dinheiro seja desviado para a conta do criminoso.

Semelhança com golpes anteriores

- Este golpe tem semelhanças com fraudes anteriores que alteravam os códigos de barras de boletos bancários. No entanto, a técnica foi

adaptada para o PIX, marcando a primeira vez que tal golpe ocorre com este método de pagamento. Vale notar que o golpe não ocorre em dispositivos móveis, apenas em computadores ou notebooks

3 DESVIO DO PAGAMENTO VIA PIX

Conforme a Kaspersky após a instalação do GoPIX, o malware fica em modo de espera até que a vítima faça um pagamento digital via PIX. O aspecto intrigante do golpe é que os criminosos não estão atrás de transferências entre indivíduos, mas sim de pagamentos para compras online. Uma possível razão para isso pode ser a intenção de evitar alertar sobre a infecção em transações de menor valor, já que as compras online geralmente envolvem valores mais significativos, visando assim uma maior rentabilidade. Em relação à substituição da chave PIX, o método não é inovador.

A técnica de monitoramento da área de transferência (local onde as informações copiadas são armazenadas temporariamente) já é conhecida, entretanto, essa é a primeira ocasião em que um trojan bancário a utiliza para manipular pagamentos via PIX. Importante ressaltar que, para efetuar um pagamento via PIX, o comerciante cria uma espécie de cobrança digital. O cliente só precisa copiar um código e colá-lo no sistema PIX para concluir o pagamento. O malware captura esse código e o modifica para que a chave PIX do fraudador seja inserida no lugar da chave do comerciante.

A ameaça foi interceptada 10.443 vezes nos produtos da Kaspersky desde janeiro deste ano, com os ataques direcionados exclusivamente a clientes brasileiros.

4 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

- **Desconfie de notificações de endereços desconhecidos**, evite clicar em anúncios falsos ou links de promoção que chegam via e-mail, e sempre prefira comprar em sites que você conhece.
- **Revise as informações do destinatário do Pix**, ao realizar um pagamento digital, revise o nome do destinatário para verificar se está correto. Desconfie quando aparecer nomes desconhecidos ou que não estão ligados ao vendedor ou à empresa.
- **Baixe aplicativos apenas de lojas oficiais**, evite baixar aplicativos de links encontrados na internet, pois podem estar infectados com vírus. Prefira baixar aplicativos pelas lojas oficiais, como a Play Store (para dispositivos Android) e a App Store (para dispositivos iOS).
- **Mantenha os aplicativos atualizados**, a maioria das atualizações de versões dos aplicativos visa corrigir problemas de segurança. A demora na atualização pode deixar seu dispositivo vulnerável a ataques.
- **Não forneça dados bancários e senhas para sites desconhecidos**, compre em sites que você conheça e evite fornecer seus dados bancários e senhas em sites suspeitos.
- **Tenha um antivírus no celular**, o antivírus pode identificar arquivos maliciosos no dispositivo e protegê-lo contra golpes durante o pagamento

5 IoCs

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	eb0b4e35a2ba442821e28d617dd2daa2
sha1:	b7cfedf9346bc1a4f497396d35360c599663725d
sha256:	7ee681e494d942d7dcc399f5f81fa48cad01e41742d1882790ad4d8d115e25ca
File name:	7ee681e494d942d7dcc399f5f81fa48cad01e41742d1882790ad4d8d115e25ca

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	6ba5539762a71e542ecac7cf59bddf79
sha1:	75c691f8163c0b8d3bc80d3a034856ff50ff8865
sha256:	3dc6f9019e500a28ff1bb54f51ff14bc5687b37859a5417a230dc139e4276c27
File name:	Rastreio.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	333A34BD2A7C6AAF298888F3EF02C186
sha1:	F7D17FA6034DF5F3E39B3E816978E7007D5EE1E6
sha256:	20A12DF8B07176AB4F20248E736A50F547C81C7937349CC02D18645C9C7DB394

Tabela 1 – Indicadores de Compromissos.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Kaspersky
- g1

heimdall
security research
A DIVISION OF ISH