BOLETIM DE SEGURANÇA

Trojan Rocinante disfarçado como aplicativos bancários visando usuários de Android no Brasil

heimdall
security research
A DIVISION OF ISH

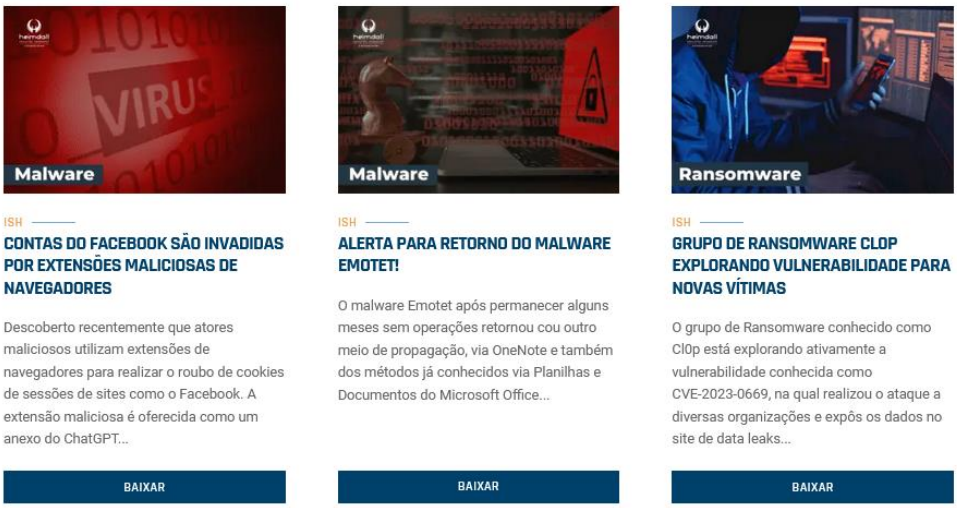
TLP: CLEAR

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

[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]



SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Recentemente, foi descoberta uma nova cepa de malware originária do Brasil, conhecida como **Rocinante**, que exemplifica a nova onda de trojans bancários. Essa família de malware tem a capacidade de realizar keylogging utilizando o Serviço de Acessibilidade e também pode roubar informações pessoais identificáveis (PII) de suas vítimas através de telas de phishing que se passam por diferentes bancos. Além disso, o Rocinante pode utilizar todas essas informações exfiltradas para realizar o controle total do dispositivo (*Device Takeover, DTO*), aproveitando os privilégios do Serviço de Acessibilidade para obter acesso remoto completo ao dispositivo infectado.

2 DETALHES SOBRE O MALWARE E SUAS OPERAÇÕES

Conforme os pesquisadores, a cadeia de ataques do malware Rocinante segue conforme descrito abaixo:

Distribuição

- O Rocinante é distribuído principalmente por meio de ***sites de phishing*** que enganam os usuários para instalar aplicativos maliciosos disfarçados de soluções de segurança, aplicativos de courier ou até mesmo aplicativos bancários. Esses sites apresentam falsas telas de login, configuradas para cada banco-alvo específico.

Ataque inicial (Exploração de Serviços de Acessibilidade)

- Assim que a vítima instala o aplicativo malicioso e concede privilégios de Serviços de Acessibilidade, o malware ganha controle total sobre o dispositivo. Isso permite que ele registre todas as interações do usuário com a interface, incluindo keylogging (registro de pressionamentos de teclas) e captura de informações exibidas na tela.

Comunicação com servidor de Comando e Controle (C2)

- O Rocinante usa uma combinação de protocolos como Firebase Messaging, HTTP e WebSockets para se comunicar com seus servidores de C2. Inicialmente, ele registra o dispositivo infectado e obtém um token único. Esse token é usado para correlacionar a comunicação subsequente via WebSocket, permitindo que os atacantes recebam comandos e monitorem as atividades do dispositivo.

Coleta de Informações Pessoais (PII)

- O malware coleta informações pessoais (PII) das vítimas por meio de falsas telas de login de bancos. Essas informações incluem números de contas bancárias, senhas e dados de autenticação em dois fatores, como interceptação de notificações SMS ou push. O Rocinante também pode exfiltrar essas informações diretamente para um bot no Telegram, usado pelos atacantes para receber os dados.

Ações remotas

- O Rocinante permite que os atacantes executem ações remotas no dispositivo infectado, incluindo simulação de toques e gestos, preenchimento de campos de texto, e navegação pela interface do usuário. Essas ações são controladas diretamente pelos atacantes e usadas para iniciar e autorizar transações fraudulentas sem o conhecimento da vítima.

Persistência e resiliência

- O malware possui mecanismos para manter controle contínuo sobre o dispositivo. Ele evita sua remoção e se atualiza constantemente, permitindo que os atacantes mantenham acesso a longo prazo, mesmo se o usuário tentar desinstalar o aplicativo.

Características e capacidades do malware

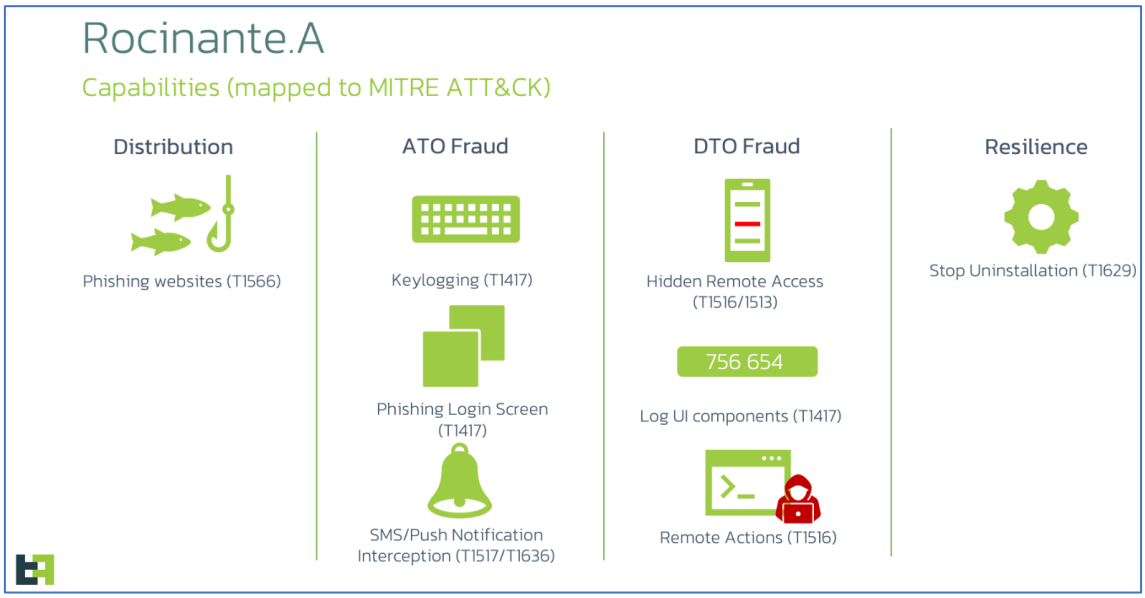


Figura 1 – Capacidades do Rocinante.

O Rocinante apresenta características similares à maioria das famílias de malware focadas no Brasil que analisamos nos últimos anos. Em grande parte dos casos, os malwares bancários obtêm sua lista de alvos de forma dinâmica a partir de um servidor C2. Essa abordagem oferece maior flexibilidade aos cibercriminosos, permitindo que o mesmo malware seja usado com alvos distintos conforme as necessidades geográficas. Além disso, possibilita a suspensão temporária da campanha, bastando desconectar o servidor C2.

3 CAMPANHAS IDENTIFICADAS

O ThreatFabric detectou várias campanhas distintas, que se disfarçam como atualizações de segurança, aplicativos de e-mail, programas de recompensas e até aplicativos bancários, como já mencionado, o principal mecanismo de distribuição é por meio de sites de phishing, que induzem o usuário a instalar o APK malicioso que se apresenta como uma solução de segurança ou aplicativos de instituições bancárias. Abaixo segue imagens das campanhas identificadas:

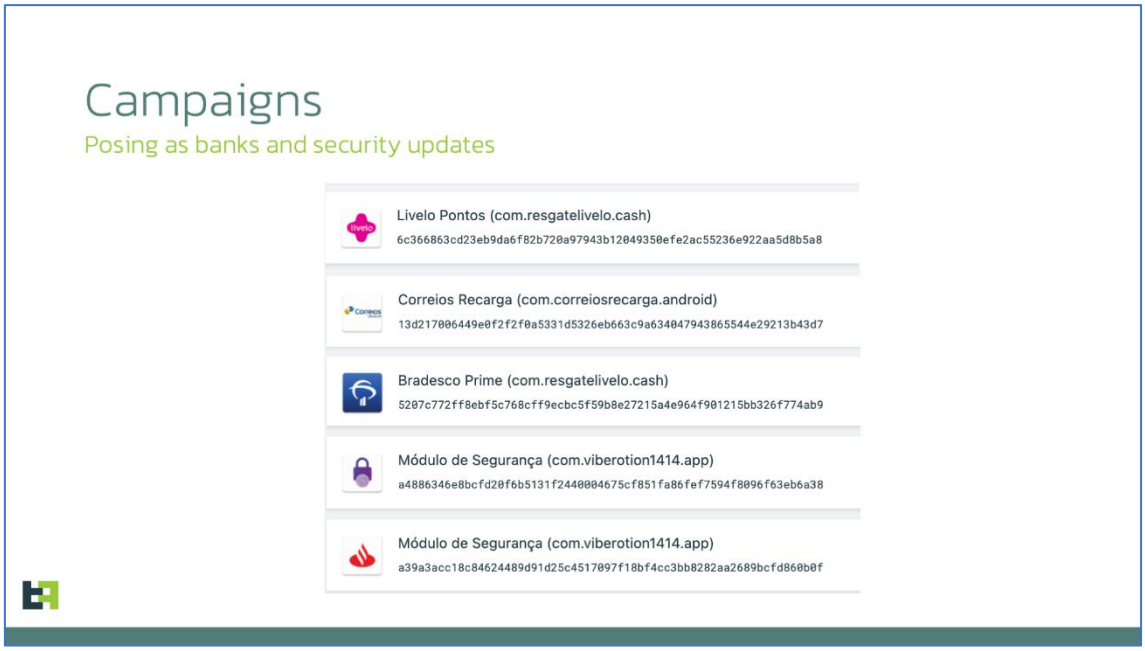


Figura 2 – Campanhas identificadas.

Alvos do malware

A lista mais recente de alvos obtidos das amostras inclui instituições que compõem a maior parte da fatia de mercado do Brasil e oferecem uma base de alvos potenciais muito grande para criminosos.

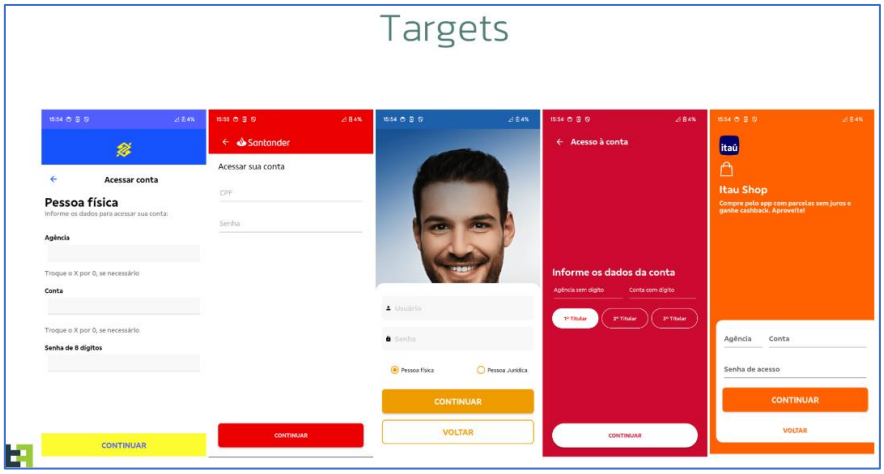


Figura 3 – Instituições alvos do malware.

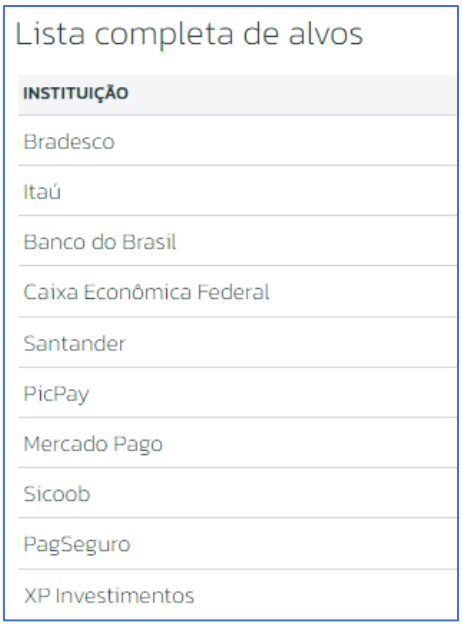


Figura 4 – Lista completa de instituições alvos.

Comandos suportados pelo malware

Abaixo segue a lista de comandos suportados pelo malware em suas operações.

Comando	Descrição
touch	Simula um evento de toque em coordenadas especificadas
livemode	Simula um evento de toque em coordenadas especificadas
left	Deslize para a esquerda
right	Deslize para a direita
up	Deslize para cima
down	Deslize para baixo
aov	Definir tela para tela de phishing
aov2	Definir tela para tela de phishing
aov3	Definir tela para tela de phishing
overpic	Definir tela para tela de phishing para PicPay
overbra	Definir tela para tela de phishing para Bradesco
overmp	Definir tela para tela de phishing para Mercado Pago
overps	Definir tela para tela de phishing para PagSeguro
oversic	Definir tela para tela de phishing para Sicoob
overcai	Definir tela para tela de phishing da Caixa Econômica Federal
oversant	Definir tela para tela de phishing para Santander BR
overxp	Definir tela para tela de phishing para XP Investimentos
overlay	Definir tela para tela de phishing para sobreposição genérica

Tabela 1 – Comandos suportados pelo malware.

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:

- **Conscientização e educação dos usuários**, para evitar baixar aplicativos de fontes desconhecidas ou links, especialmente aqueles recebidos por meio de campanhas de phishing.
- **Permissões de aplicativos**, aconselhando os usuários a serem cautelosos ao conceder permissões de acessibilidade a aplicativos.
- **Soluções de segurança**, com o uso de soluções de segurança móvel abrangentes que possam detectar e bloquear malwares, especialmente aquelas capazes de identificar comportamentos suspeitos, como o acesso não autorizado ao Serviço de Acessibilidade.
- **Atualizações regulares**, garantindo que tanto o sistema operacional Android quanto todos os aplicativos sejam regularmente atualizados para as versões mais recentes.
- **Aplicativos bancários legítimos**, baixar e usar aplicativos bancários apenas de fontes confiáveis e a verificarem a autenticidade do aplicativo antes da instalação.

5 INDICADORES DE COMPROMISSOS

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 do artefato	
md5:	c09e5ec180e2ba9ef8229136b7edfd06
sha1:	548747e87edf2d49c1182ce46735517b2a92a613
sha256:	23c51ed174a6014b3207b41a82c2aee0eea16df8fa1cd14c2864fb3307215070
File name:	2tcrvk.apk

Indicadores de compromisso do artefato	
md5:	3766405b872dbf9f43b01e2c4fc395c2
sha1:	49e89188664a5226e31bfe3ee9e501a474cfd79a
sha256:	64ec090ea5e22648e46651b12569107f94b10c1e8e4635ef42716aaec28fd6bd
File name:	Livelo.apk

Indicadores de compromisso do artefato	
md5:	6e391db56536e2d04277ba1d1cebba63
sha1:	fe46f801ecb976373809e9a25b97d20c2b37104e
sha256:	a4886346e8bcfd20f6b5131f2440004675cf851fa86fef7594f8096f63eb6a38
File name:	0tfnkg.apk

Indicadores de compromisso do artefato	
md5:	faa3f13e99ea9f0355c389b0e670919c
sha1:	0ba8c9b22238dbf19ad6b2fd10e310c1d74b98ba
sha256:	a39a3acc18c84624489d91d25c4517097f18bf4cc3bb8282aa2689bcfd860b0f
File name:	a39a3acc18c84624489d91d25c4517097f18bf4cc3bb8282aa2689bcfd860b0f.apk

Tabela 2 – Indicadores de Compromissos de artefatos

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Threatfabric**

7 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH