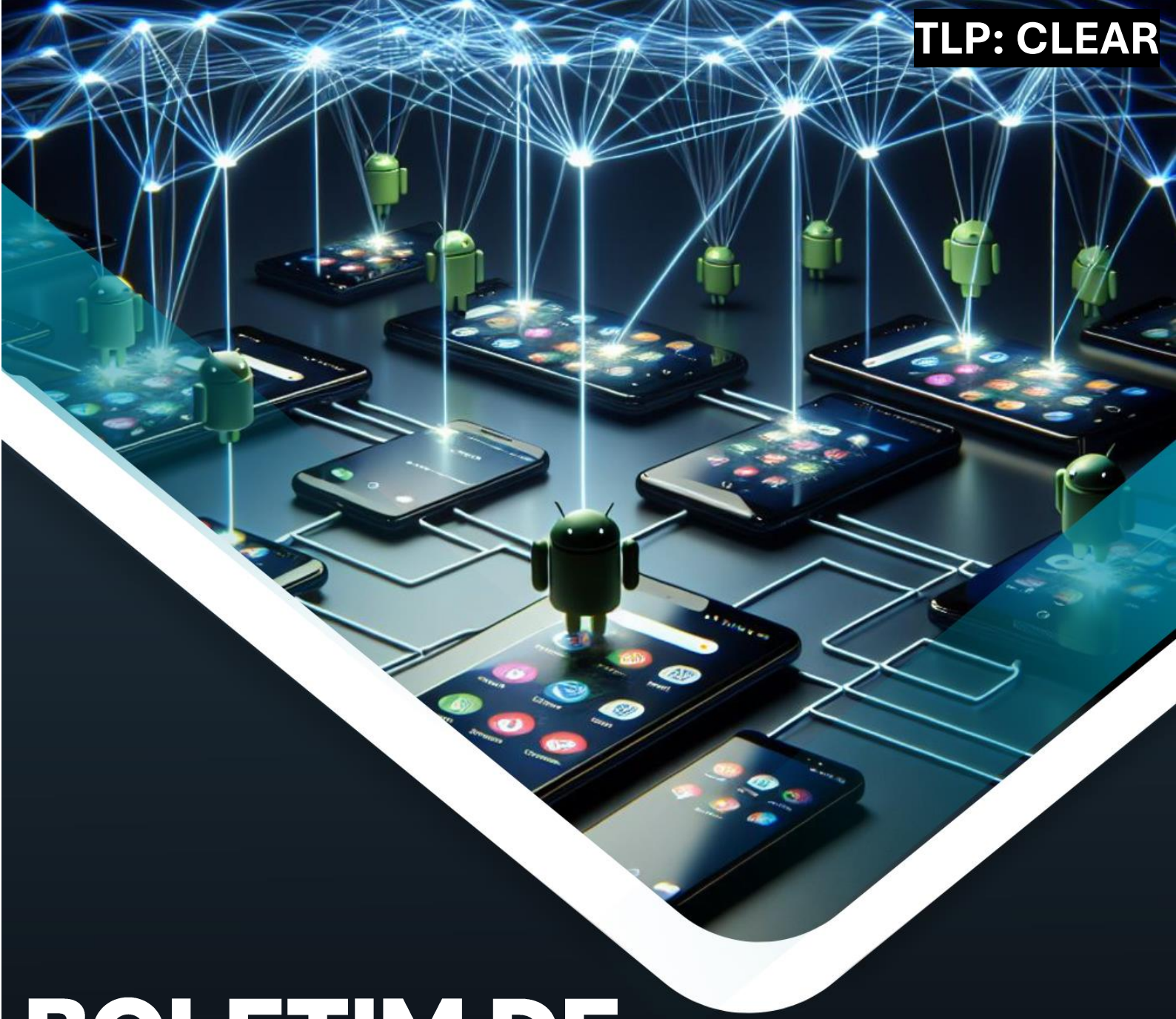
TLP: CLEAR



BOLETIM DE SEGURANÇA

Botnet BADBOX compromete 74.000 dispositivos Android com malware personalizável

heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

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 INFORMAÇÕES SOBRE A AMEAÇA

Uma operação cibercriminosa chamada BADBOX tem se destacado envolvendo a venda de dispositivos Android, como caixas de TV e smartphones de marcas desconhecidas, já infectados com malware. Isso significa que os dispositivos vêm comprometidos antes mesmo de serem entregues aos consumidores.

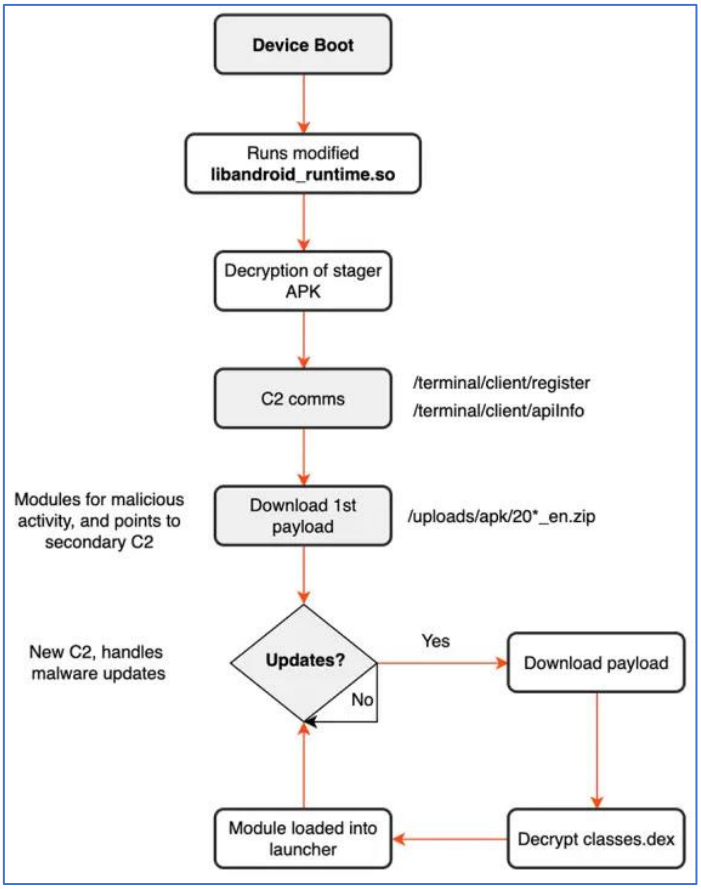


Figura 1 – Cadeia de infecção.

O BADBOX é um malware que compromete dispositivos para usá-los como proxies residenciais, instalar código remotamente, abusar de contas e cometer fraudes em anúncios. Um dos aspectos mais perigosos do BADBOX é sua capacidade de adicionar código ou módulos sem o consentimento do usuário, permitindo a implantação de novos ataques.

Pesquisadores descobriram que o BADBOX pode ser pré-instalado em dispositivos, sugerindo que ele pode ser inserido durante a fabricação, através de imagens de sistema personalizáveis, ou durante a cadeia de suprimentos, em qualquer etapa do desenvolvimento, fabricação, envio ou venda.

Após análises, foi observado que o malware infectou dispositivos logo ao serem inicializados e enviou telemetria imediatamente para tentar se conectar a um servidor de comando e controle (C2), aguardando novas instruções. A URL **coslogdydy[.]in** foi o destino de várias comunicações relacionadas ao BADBOX. Os dados mostraram que diariamente mais de 160.000 IPs únicos estão se comunicando, e esse número continua a aumentar de forma constante.

A maior parte das comunicações vem da Rússia, utilizando o modelo YNDX Smart TV, seguida pela China com o smartphone Hisense Instwall_T963. Outros locais menos comuns incluem Índia, Ucrânia e Belarus. Além disso, há tráfego residual (menos de 1300 IPs diários) da Arábia Saudita, Cazaquistão, República Tcheca, Estados Unidos, França e Holanda.

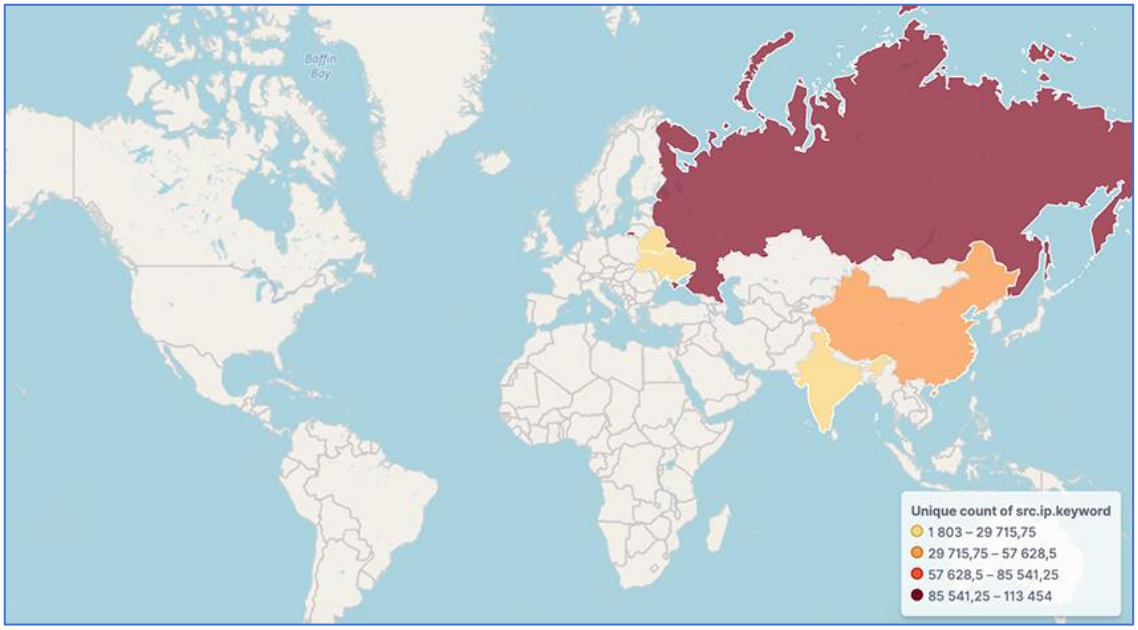


Figura 2 – Telemetria das comunicações coletadas.

A operação BADBOX revela como os criminosos cibernéticos estão aprimorando suas técnicas para utilizar cadeias de suprimentos globais na disseminação de malware. Embora o foco inicial tenha sido em dispositivos infectados na Rússia e na China, o malware BADBOX se tornou uma epidemia global, afetando diversos dispositivos Android. É importante destacar que os agentes de ameaças estão ampliando seu alcance, não apenas atacando dispositivos de marcas desconhecidas, mas também alvejando marcas renomadas como Yandex e Hisense.

2 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:

Adquira de fornecedores confiáveis

- Adquira dispositivos Android apenas de fabricantes e vendedores conhecidos e confiáveis para minimizar o risco de receber dispositivos já infectados.

Atualize o firmware regularmente

- Mantenha o firmware do seu dispositivo sempre atualizado com as últimas versões fornecidas pelo fabricante, pois essas atualizações frequentemente incluem correções de segurança.

Use software de segurança

- Instale e mantenha atualizado um software de segurança confiável que possa detectar e remover malware em dispositivos Android.

Evite aplicativos de fontes desconhecidas

- Baixe aplicativos apenas de lojas oficiais, como Google Play Store, para reduzir o risco de instalar aplicativos maliciosos.

Monitore o tráfego de rede

- Utilize ferramentas de monitoramento de rede para detectar atividades suspeitas que possam indicar a presença de malware no dispositivo.

Desative permissões desnecessárias

- Revise e desative permissões de aplicativos que não são necessárias para o funcionamento deles, limitando o acesso a dados sensíveis.

Eduque-se sobre segurança digital

- Mantenha-se informado sobre as últimas ameaças e práticas recomendadas de segurança para proteger seus dispositivos e dados pessoais.

3 INDICADORES DE COMPROMETIMENTO (IOC)

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 Comprometimento (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
Domínio	coslogdydy[.]in yydsmr[.]com logcer[.]com

Tabela 1 – Indicadores de Comprometimento 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.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Bitsght**
- **GoHackers**

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH