TLP: CLEAR

BOLETIM DE SEGURANÇA

Novo malware FireScam para Android se disfarça de Telegram Premium para roubar dados

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

Um novo malware para Android, denominado '**FireScam**', está sendo distribuído como uma versão premium do aplicativo Telegram através de sites de phishing no GitHub que imitam o RuStore, o mercado de aplicativos móveis da Rússia. O RuStore foi lançado em maio de 2022 pelo grupo russo de internet VK (VKontakte) como uma alternativa ao Google Play e à App Store da Apple, após sanções ocidentais que afetaram o acesso de usuários russos a softwares móveis.

O FireScam é um malware projetado para roubar informações e atuar como spyware em dispositivos Android. Ele pode monitorar diversas atividades no dispositivo infectado, como notificações, mensagens, respostas USSD e conteúdo da área de transferência. Além disso, o FireScam pode enviar os dados capturados para servidores remotos usando o Firebase Realtime Database, permitindo que invasores obtenham acesso a informações sensíveis.Este malware é propagado como um falso APK 'Telegram Premium' através de um site hospedado no domínio github[.]io. Esse site é uma tentativa de phishing que imita o RuStore (rustore.ru), uma loja de aplicativos criada pelo grupo russo de internet VK. O malware se disfarça como um aplicativo legítimo para enganar os usuários e induzi-los a instalá-lo, permitindo assim o roubo de informações confidenciais e a exfiltração de dados para o endpoint Firebase C2.

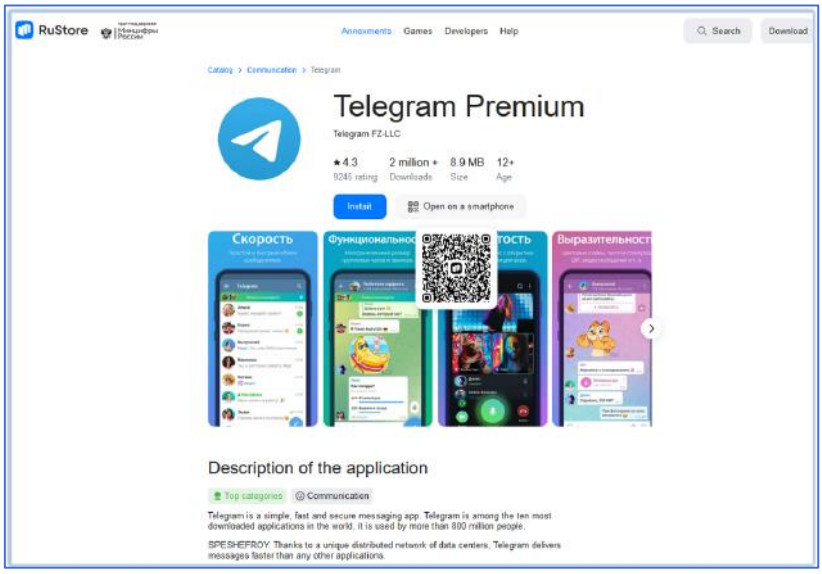

Figura 1 – Site para download do app Telegram Premium.

O APK é obtido a partir do site de phishing e atua como um dropper, instalando posteriormente o malware FireScam, que se passa pelo aplicativo "Telegram Premium". Os dados roubados são inicialmente armazenados temporariamente no Firebase Realtime Database na URL "***https[:]//androidscamru-default-rtdb[.]firebaseio[.]com***". Depois, eles são removidos, possivelmente após a filtragem e armazenamento das informações importantes em outro local privado.

O dropper é instalado sob o nome 'GetAppsRu'. Ao clicar no ícone do aplicativo, a BaseActivity do dropper é iniciada, exibindo uma opção 'Install' para 'Telegram Premium' – o payload principal que está contido em seus recursos como 'child.apk'.

Figura 2 – BaseAtividade do Dropper.

O FireScam utiliza o NP Manager para proteger o pacote principal ru.get.app contra análise e engenharia reversa, empregando criptografia, ofuscação e ocultação de detalhes. Ele verifica se o nome do processo é incomum, como em emuladores ou ferramentas de análise, para decidir se deve operar normalmente ou de forma diferente, evitando comportamento malicioso em ambientes de sandbox ou depuração. O aplicativo registra um serviço para receber notificações do Firebase Cloud Messaging (FCM), acionando o serviço (MessagingService) quando uma mensagem é recebida.

Um receptor define uma permissão personalizada para controlar o acesso, permitindo que apenas aplicativos assinados com o mesmo certificado interajam com ele. Isso pode permitir que invasores acessem eventos ou dados confidenciais ao controlar o receptor de transmissão dinâmica, criando um backdoor para comunicação entre o aplicativo malicioso e outros aplicativos comprometidos. Após a instalação, o aplicativo malicioso envia informações confidenciais do dispositivo para uma URL do Firebase Realtime Database, incluindo detalhes como nome do dispositivo, nome do aplicativo, texto de notificação e data e hora do evento.

O malware monitora a atividade do aplicativo Mensagens no dispositivo comprometido e exfiltra o conteúdo das mensagens de texto, marcando os dados com o rótulo “appName: Messages” e enviando-os para uma URL designada do Firebase Realtime Database. Isso permite que invasores acessem dados de comunicação confidenciais, facilitando vigilância e roubo de dados. Após a instalação, o aplicativo pede permissões para acessar Contatos, Telefone e Mensagens. Em seguida, ele faz uma solicitação POST ao Firebase para registrar a instalação com um ID exclusivo 'androidscamru' na URL fornecida. Esse ID será utilizado para futuras operações, como o Firebase Cloud Messaging (FCM).

2 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Initial Access	T1660	Consiste em técnicas que usam vários vetores de entrada para ganhar sua posição inicial dentro de uma rede.
Persistence	T1624.001	Consiste em técnicas que os adversários usam para manter o acesso aos sistemas em reinicializações, credenciais alteradas e outras interrupções que podem cortar seu acesso.
Privilege Escalation	T1626.001	Consiste em técnicas que os adversários usam para obter permissões de nível mais alto em um sistema ou rede.
Defense Evasion	T1628 T1628.002 T1406 T1633	Consiste em técnicas que os adversários usam para evitar a detecção durante seu comprometimento.
Credential Access	T1517 T1414 T1417	Consiste em técnicas para roubar credenciais como nomes de contas e senhas. Técnicas usadas para obter credenciais incluem keylogging ou credential dumping.
Discovery	T1424 T1418 T1426 T1422	Consiste em técnicas que um adversário pode usar para obter conhecimento sobre o sistema e a rede interna.
Collection	T1517 T1414 T1417	Consiste em técnicas que os adversários podem usar para reunir informações e as fontes de onde as informações são coletadas que são relevantes para seguir os objetivos do adversário.
Command and Control	T1437 T1437.001 T1521 T1521.003 T1481	Consiste em técnicas que adversários podem usar para se comunicar com sistemas sob seu controle dentro de uma rede de vítima.

Tabela 1 – Tabela MITRE ATT&CK.

3 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:

Segurança de Endpoint

- Utilize soluções robustas para monitoramento em tempo real e detecção de ameaças, como pacotes de segurança Antimalware e sistemas de prevenção de intrusão baseados em host.

Monitoramento de rede

- Realize monitoramento contínuo da atividade de rede com NIDS/NIPS e use firewalls de aplicativos web para filtrar e bloquear atividades suspeitas.

Configuração de firewalls

- Configure firewalls para bloquear comunicações de saída para IPs maliciosos conhecidos e domínios associados aos servidores de comando e controle do FireScam.

Monitoramento comportamental

- Implemente monitoramento baseado em comportamento para detectar atividades incomuns, como processos suspeitos tentando fazer conexões não autorizadas.

Lista de permissões de aplicativos

- Permita que apenas aplicativos aprovados sejam executados nos endpoints, impedindo a execução de executáveis não autorizados ou maliciosos.

Avaliações de vulnerabilidades

- Realize avaliações de vulnerabilidades e testes de penetração periodicamente para identificar e corrigir brechas de segurança.

Plano de Resposta a Incidentes

- Desenvolva um plano abrangente de resposta a incidentes, detalhando as etapas a serem seguidas em caso de infecção por malware.

Conscientização e treinamento

- Promova programas de conscientização e treinamento de segurança para proteger contra ataques de engenharia social.

4 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 do artefato	
md5:	5d21c52e6ea7769be45f10e82b973b1e
sha1:	88f45210b4af5f15544518a256a818f7c63cf89d
sha256:	b041ff57c477947dacd73036bf0dee7a0d6221275368af8b6dbbd5c1ab4e981b
File name:	GetAppsRu.apk

Indicadores do artefato	
md5:	cae5a13c0b06de52d8379f4c61aece9c
sha1:	4efe9ea478a86b0eca8cb0e7e43236dc22e716a2
sha256:	12305b2cacde34898f02bed0b12f580aff46531aa4ef28ae29b1bf164259e7d1
File name:	child.apk

Tabela 2 – Indicadores de Comprometimento

Indicadores de URL

Indicadores de URL	
URL	https[:]//androidscamru-default-rtdb[.]firebaseio[.]com https[:]//rustore-apk[.]github[.]io/telegram_premium

Tabela 3 – 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.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Cyfirma**
- **Bleepingcomputer**

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH