feedzai | Report

Nexus Malware Threat Report

#ProtectYourCustomers

feedzai.com

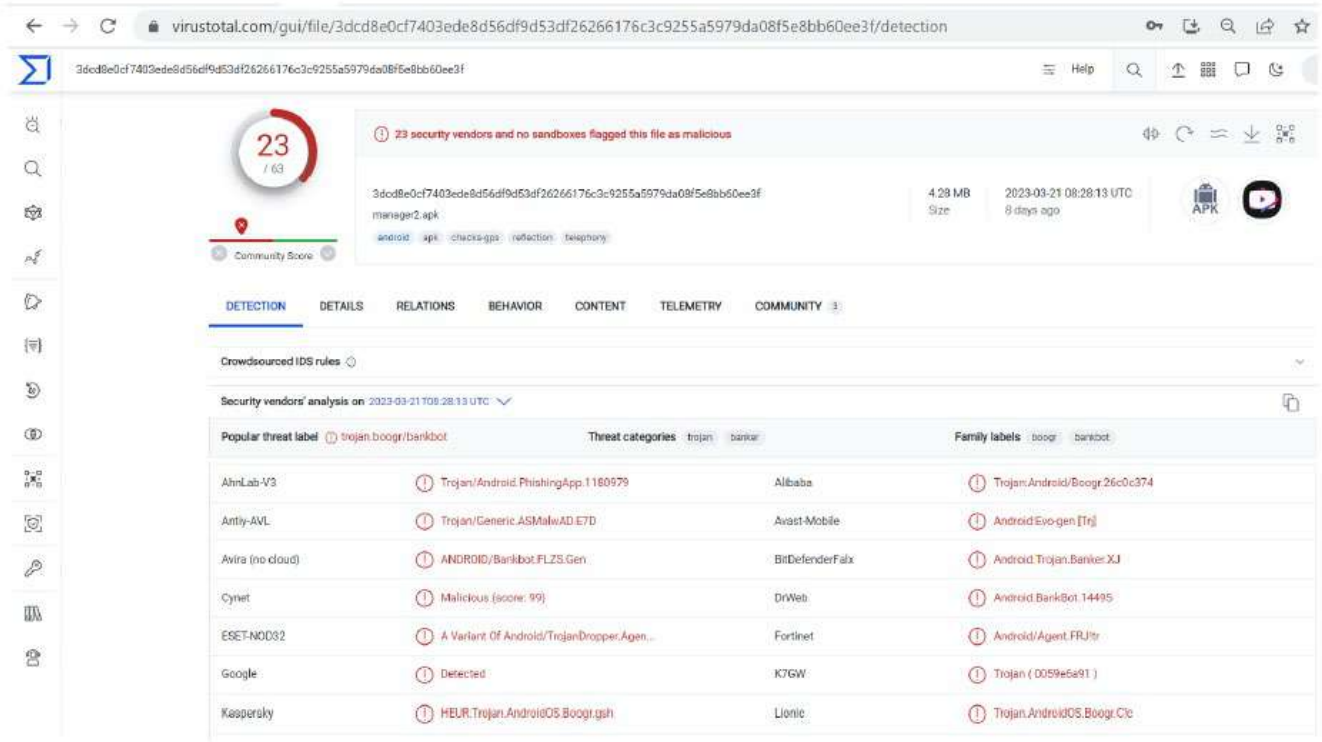
Contents

Introduction

Banking malware, also known as “financial malware”, has evolved significantly since its appearance in the 1990s. In its early days, banking malware focused primarily on collecting users’ passwords and financial data, mainly through the use of Trojans and keyloggers. Over time, banking malware has evolved to include new techniques and features, such as the ability to evade detection by security systems, the use of social engineering to trick users, and the implementation of encryption techniques to protect stolen data.

In addition, banking malware has adapted to new financial technologies, such as mobile payments and cryptocurrencies, leading to the creation of new types of malware designed specifically to attack these platforms. The banker Nexus goes a step further, as its ‘threat actors’ have included more than 450 targets recently, apart from a ransomware functionality, something that hasn’t been seen much to date.

This malware is more than well known by antivirus houses due to the fact that part of the code used has been recycled from the S.O.V.A. malware. We can see it in the following image, when searching for its hash in the VirusTotal platform.



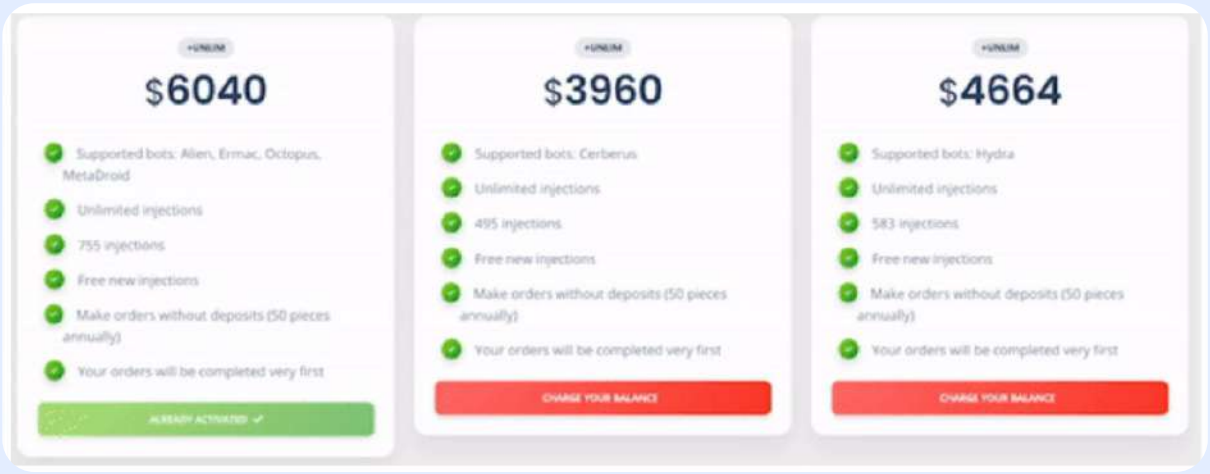
General Information of Nexus

Some information has been obtained from samples of this malware. The first thing we found is that the applications of this family are signed, which means that they are more likely to go undetected by antivirus engines.

Although the initial attacks took place in June of the previous year, it was not until January 2023 that researchers were able to locate the threat. The malware has spread through numerous hacking forums, where its developers explained that the source code of the malware is practically new, although after performing the relevant analysis it has been discovered that it recycles part of the code of the S.O.V.A. malware.

> **They are more likely to go undetected by antivirus engines.**

In the initial release, in which the malware's creators demonstrated how it works, the software was made available for rent for a fee of $3,000 per month. The fee is well below those of other malware, e.g. Hydra ($4664), Alien/Ermac/Octopus/Metadroid ($6040) and Cerberus ($3960).

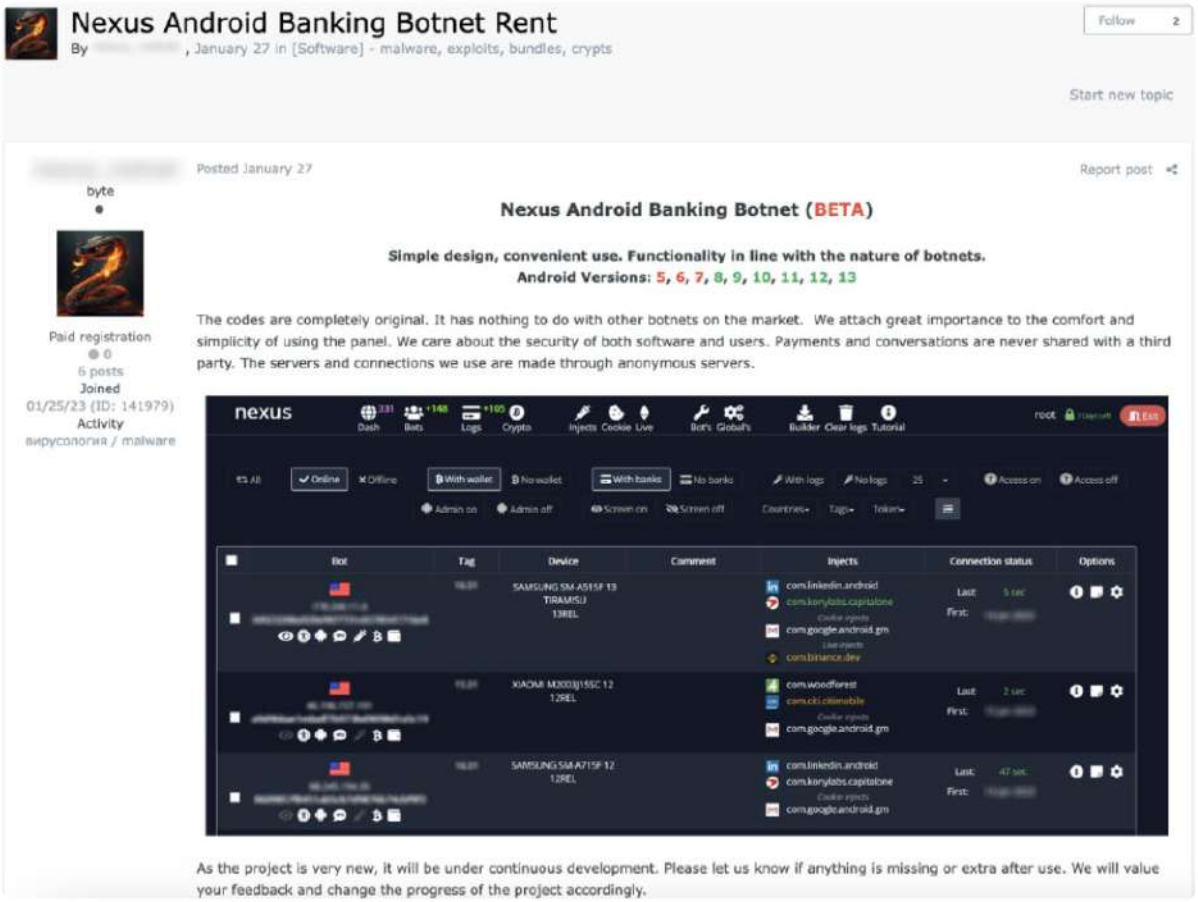


Although Nexus is still in the early stages of its development, cybersecurity experts have determined that it is already being used in some attack campaigns around the world. In this regard, it has been possible to identify signs of malware in some malicious applications masquerading as well-known programs, such as YouTube Vanced, which is the replacement for the ad-free YouTube app with additional features.

Propagation, Characteristics and Functionality

In an investigation carried out by the Hispasec team, they have gained access to a forum where information about this new family has been published. Threat actors often use these forums to promote themselves. Information about some of the functionalities and Android versions that are affected has been obtained. The Android versions affected range from 8 to 13 and are for sale in a forum on the dark web.

Attackers often advertise their malware on cybercrime forums, as this allows them to profit from illicit activities, enhance their reputation among other cybercriminals and expand the distribution of their malware to a wider audience.

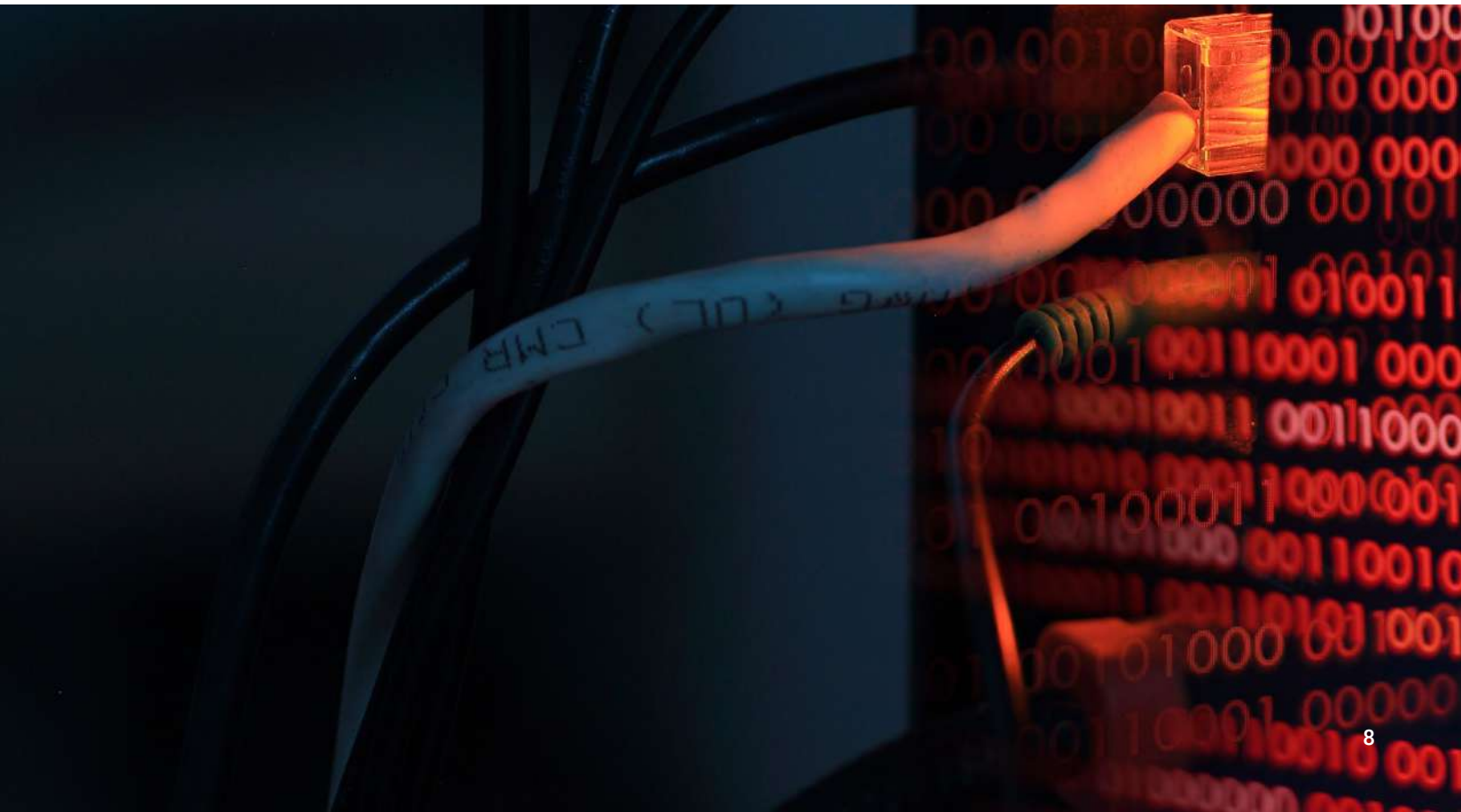


The attackers also mention that the project is new and under development. The ransomware functionality is one of the parts of the project they are still working on and apparently it is not currently active.

It is interesting to mention that the creators of Nexus have set explicit rules prohibiting the use of their malware in several countries, including among others Azerbaijan, Armenia and Russia. This banking Trojan has the ability to take over bank and cryptocurrency accounts through overlay and keylogging attacks, allowing it to steal users' credentials. In addition, it can read two-factor authentication codes and delete SMS messages. It can also enable or disable the 2FA theft module and update its software through a command and control server.

Apart from the rules already mentioned we also find:

- We do not reimburse third party services
- Any form of work in Russia and CIS is prohibited.



Permissions on Android

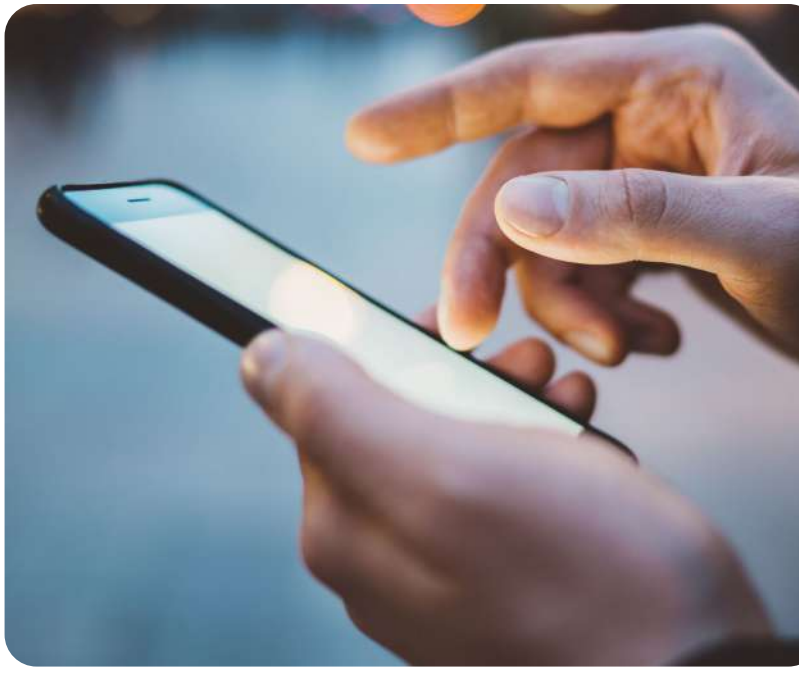
Nexus applies for almost 50 permits. Some of the most “dangerous” permissions are named at the end of the report, in the appendix section.

A banking Trojan is a malicious program designed to damage, steal information or take control of devices without the user’s consent. In the case of Android, these programs can request permissions that allow access to certain system functions and the user’s personal data, which can pose a great danger to security and privacy.

When an application is installed on an Android device, the system prompts the user for permissions necessary for the application to function properly. These permissions may include access to the user’s camera, microphone, contacts, messages, location and other personal data.

If malware is installed on an Android device, it may request permissions that allow access to system functions and data that are not necessary for its operation, such as access to the camera for no apparent reason. This may indicate that the malware is trying to take control of the device or steal personal information.

> **Nexus applies for almost 50 permits**



In addition, some malware may use permissions to install additional software without the user's knowledge, send text messages or make calls to premium rate numbers, which can result in unexpected charges on the user's bill.

Therefore, it is important to use caution when installing apps on Android devices and carefully review the permissions they request. If an application requests permissions that do not seem necessary for its operation, it is advisable not to install it. It is also important to keep the operating system updated and use security software to detect and eliminate possible malware threats.

Screenshot of the requested permits

Conclusions

Nexus is compatible with the latest versions of Android and has incorporated new techniques, such as ransomware functionality. In addition, the malware (MaaS) is on sale for a lower price than usual ($3000) so it would not be surprising if more samples of this family start to be detected.

Like other banking Trojans, this malware spreads through various methods such as fake websites, smishing, email phishing and social engineering campaigns. To prevent device infection, it is recommended that Android users be careful when installing applications and only download them from official sources and developers, such as the Google Play Store, and not from other sites. This will reduce the chances of the device being compromised by this type of malware.

Appendix

Hazardous permits requested:

- **android.permission.RECEIVE_SMS:** It allows the app to listen to all the SMS's that are received on the user's phone while he/she is using the app.
- **android.permission.READ_SMS:** It allows the app to read all the SMS's(currently present) on the user's phone
- **android.permission.READ_CONTACTS:** Allows the app to read data about your contacts stored on your phone, including the frequency with which you've called, emailed, or communicated in other ways with specific individuals. This permission allows apps to save your contact data, and malicious apps may share contact data without your knowledge.
- **android.permission.GET_ACCOUNTS:** Allows access to the list of accounts in the Account Service.
- **android.permission.ACTION_MANAGE_OVERLAY_PERMISSION:** Display screen to control which apps can draw on top of other apps.
- **android.permission.CALL_PHONE:** Allows an application to initiate a phone call without going through the Dialer UI for the user to confirm the call.
- **android.permission.WRITE_EXTERNAL_STORAGE:** Allows an application to write to external storage.
- **android.permission.SYSTEM_ALERT_WINDOW:** Allows an app to create windows using the WindowManager.LayoutParams.TYPE_APPLICATION_OVERLAY type, displayed on top of all other apps. Very few apps should use this permission; these windows are intended for system-level user interaction.
- **android.permission.WRITE_CONTACTS:** Allows an app to write the user's contact data.
- **android.permission.SEND_SMS:** It allows applications to access network information.
- **android.permission.REQUEST_INSTALL_PACKAGES:** Allows an application to request the installation of packages.
- **android.permission.READ_PHONE_STATE:** Allows read-only access to the phone's status, including current cellular network information, the status of any ongoing calls, and a list of any PhoneAccounts registered on the device.
- **android.permission.READ_PHONE_NUMBERS:** Allows read-only access to the device's phone numbers. This is a subset of the capabilities granted by READ_PHONE_STATE, but is exposed to instant applications.
- **android.permission.READ_EXTERNAL_STORAGE:** Allows an application to read from external storage.

```
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
<uses-permission android:name="android.permission.QUICKBOOT_POWERON"/>
<uses-permission android:name="android.permission.QUERY_ALL_PACKAGES"/>
<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<uses-permission android:name="android.permission.USE_FINGERPRINT"/>
<uses-permission android:name="android.permission.INSTALL_PACKAGES"/>
<uses-permission android:name="android.permission.FOREGROUND_SERVICE"/>
<uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS"/>
<uses-permission android:name="android.permission.GET_ACCOUNTS"/>
<uses-permission android:name="com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA"/>
<uses-permission android:name="android.permission.ACCESS_CONTENT_PROVIDERS_EXTERNALLY"/>
<uses-permission android:name="android.permission.ACTION_MANAGE_OVERLAY_PERMISSION"/>
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
<uses-permission android:name="android.permission.GET_PACKAGE_SIZE"/>
<uses-permission android:name="android.permission.CALL_PHONE"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE"/>
<uses-permission android:name="android.permission.REQUEST_DELETE_PACKAGES"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.RECEIVE_LAUNCH_BROADCASTS"/>
<uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.VIBRATE"/>
<uses-permission android:name="com.moutai.mall.permission.PUSH_PROVIDER"/>
<uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
<uses-permission android:name="android.permission.WRITE_CONTACTS"/>
<uses-permission android:name="android.permission.GET_TASKS"/>
<uses-permission android:name="android.permission.QUERY_ALL_PACKAGES"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.SEND_SMS"/>
<uses-permission android:name="android.permission.CLEAR_APP_CACHE"/>
<uses-permission android:name="android.permission.DISABLE_KEYGUARD"/>
<uses-permission android:name="com.moutai.mall.permission.PROCESS_PUSH_MSG"/>
<uses-permission android:name="com.meizu.flyme.permission.PUSH"/>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="com.google.android.gms.permission.ACTIVITY_RECOGNITION"/>
<uses-permission android:name="android.permission.REORDER_TASKS"/>
<uses-permission android:name="android.permission.REQUEST_INSTALL_PACKAGES"/>
<permission android:name="com.moutai.mall.permission.PROCESS_PUSH_MSG" android:protectionLevel="signatureOrSystem"/>
<permission android:name="com.moutai.mall.permission.PUSH_PROVIDER" android:protectionLevel="signatureOrSystem"/>
<permission android:name="com.moutai.mall.permission.PUSH_WRITE_PROVIDER" android:protectionLevel="signatureOrSystem"/>
<uses-permission android:name="android.permission.CHANGE_NETWORK_STATE"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/> c
<uses-permission android:name="android.permission.READ_PHONE_NUMBERS"/>
<uses-permission android:name="android.permission.BLUETOOTH"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
```

Information of one of the app “Youtube Vanced”

- **APP name:** Youtube Vanced
- **Package name:** com.toss.soda

```
package="com.toss.soda"
```

- **Main Activity:** com.tapston.burgerking.ui.LauncherActivity

```
android:name="com.tapston.burgerking.ui.LauncherActivity"
```

Hash

- **MD5:** d87e04db4f4a36df263ecbfe8a8605bd
- **SHA-1:** 1c99c658e30c672927dccbd8628107abf36d990d
- **SHA-256:** 3dcd8e0cf7403ede8d56df9d53df26266176c3c9255a5979da08f5e8bb60ee3f

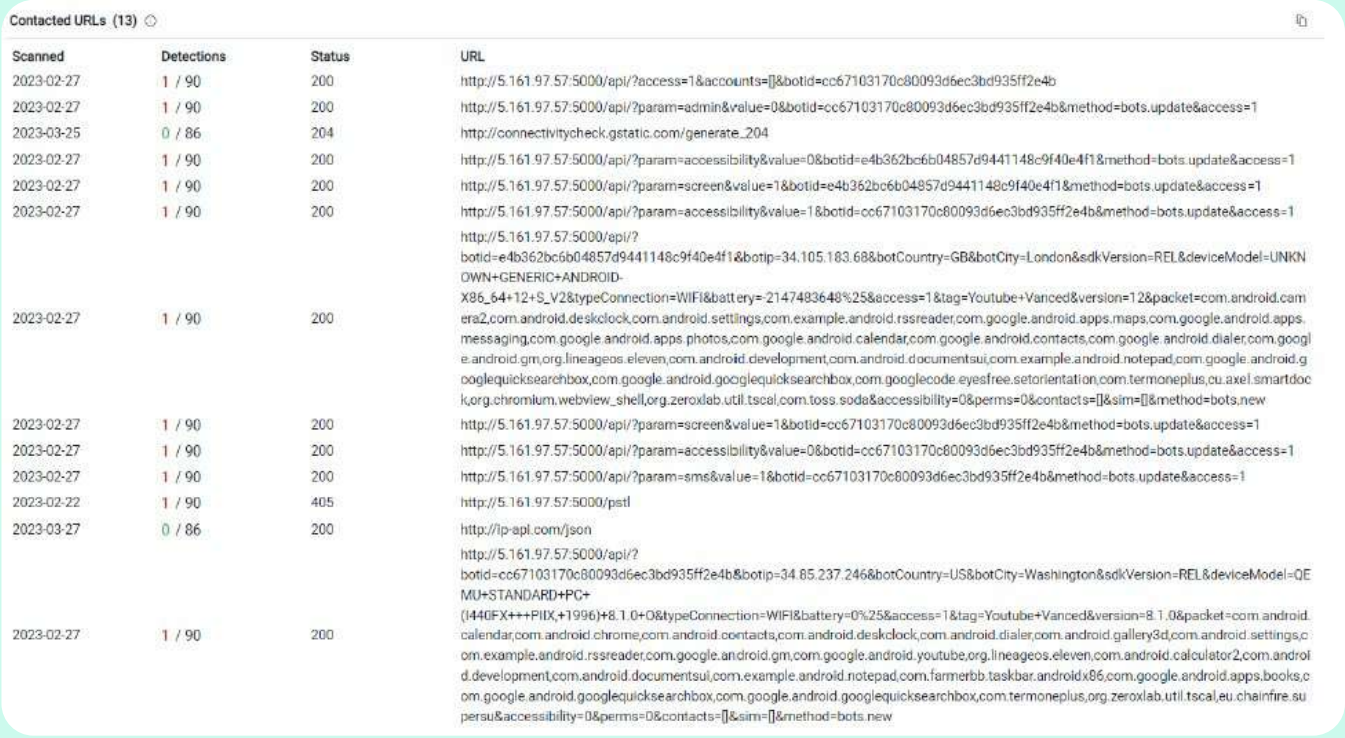
Android Type	APK
Package Name	com.toss.soda
Main Activity	com.tapston.burgerking.ui.LauncherActivity
Internal Version	7
Displayed Version	7.2
Minimum SDK Version	24
Target SDK Version	32

```
APK signature verification result:

Signature verification succeeded
Valid APK signature v2 found

    Signer 1

        Type: X.509
        Version: 3
        Serial number: 0x232eae62
        Subject: CN=Android Debug, OU=Android, O=Unknown, L=Unknown, ST=Unknown, C=US
        Valid from: Tue Dec 31 23:35:04 CET 2013
        Valid until: Wed May 01 00:35:04 CEST 2052

        Public key type: RSA
        Exponent: 65537
        Modulus size (bits): 2048
        Modulus: 18540476933856063472742644372492167470984374466101418965964602200346658256331617876341540619853874089691681l

        Signature type: SHA1withRSA
        Signature OID: 1.2.840.113549.1.1.5

        MD5 Fingerprint: 20 F4 61 48 B7 2D 8E 5E 5C A2 3D 37 A4 F4 14 90
        SHA-1 Fingerprint: 5E 8F 16 06 2E A3 CD 2C 4A 0D 54 78 76 BA A6 F3 8C AB F6 25
        SHA-256 Fingerprint: FA C6 17 45 DC 09 03 78 6F B9 ED E6 2A 96 2B 39 9F 73 48 F0 BB 6F 89 9B 83 32 66 75 91 03 3B 9C
```

Application metadata information

The C2 information can be obtained from VirusTotal.

• **C2:** 5.161.97.57:5000



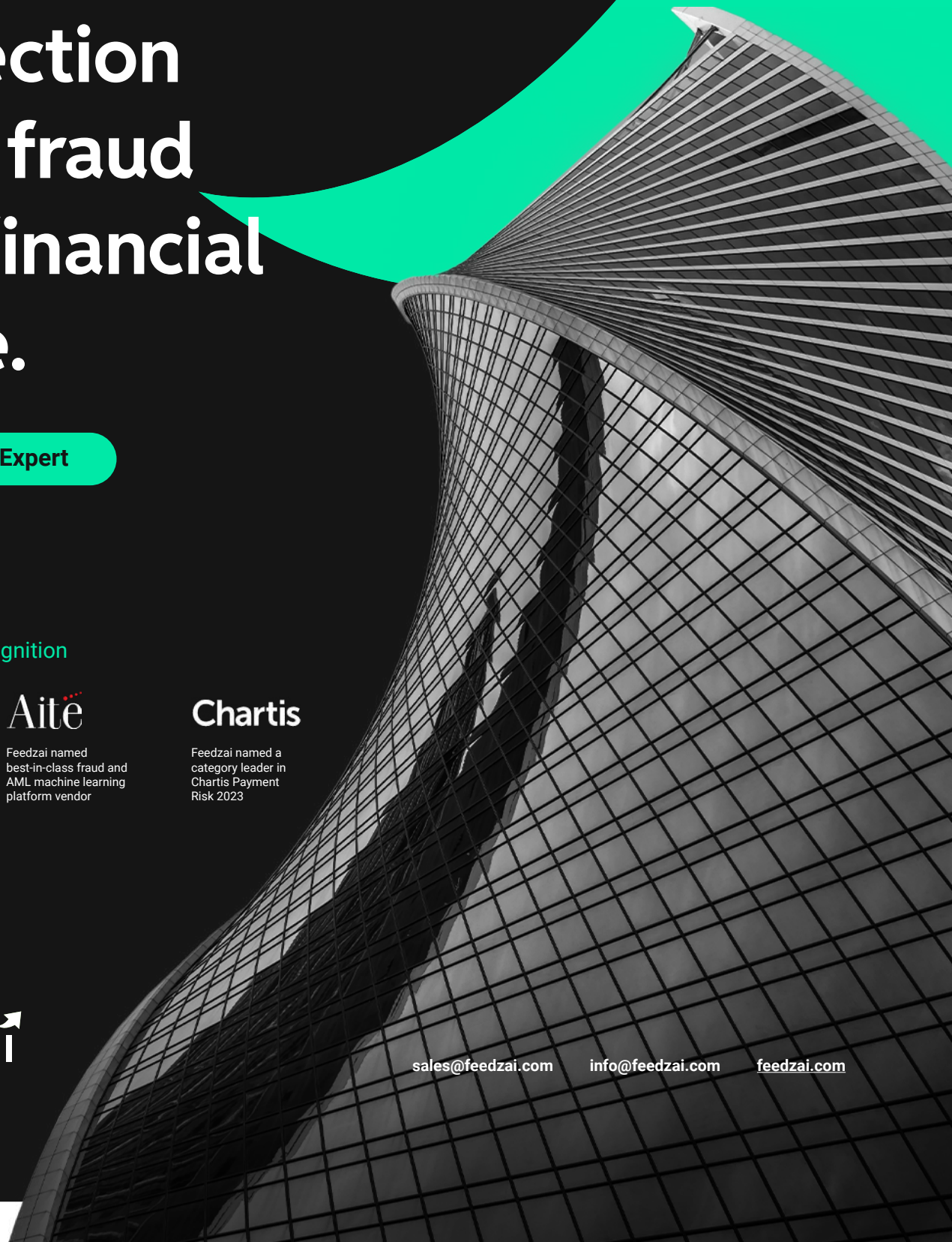
Contacted URLs (13)

Scanned	Detections	Status	URL
2023-02-27	1 / 90	200	http://5.161.97.57:5000/api/?access=1&accounts=[]&botid=cc67103170c80093d6ec3bd935ff2e4b
2023-02-27	1 / 90	200	http://5.161.97.57:5000/api/?param=admin&value=0&botid=cc67103170c80093d6ec3bd935ff2e4b&method=bots.update&access=1
2023-03-25	0 / 86	204	http://connectivitycheck.gstatic.com/generate_204
2023-02-27	1 / 90	200	http://5.161.97.57:5000/api/?param=accessibility&value=0&botid=e4b362bc6b04857d9441148c9f40e4f1&method=bots.update&access=1
2023-02-27	1 / 90	200	http://5.161.97.57:5000/api/?param=screen&value=1&botid=e4b362bc6b04857d9441148c9f40e4f1&method=bots.update&access=1
2023-02-27	1 / 90	200	http://5.161.97.57:5000/api/?param=accessibility&value=1&botid=cc67103170c80093d6ec3bd935ff2e4b&method=bots.update&access=1
2023-02-27	1 / 90	200	http://5.161.97.57:5000/api/?botid=e4b362bc6b04857d9441148c9f40e4f1&botip=34.105.183.68&botCountry=GB&botCity=London&sdkVersion=REL&deviceModel=UNKNOWN+GENERIC+ANDROID-X86_64+12+S_V2&typeConnection=WIFI&battery=-2147483648%25&access=1&tag=Youtube+Vanced&version=12&packet=com.android.camera2,com.android.deskclock,com.android.settings,com.example.android.rssreader,com.google.android.apps.maps,com.google.android.apps.messaging,com.google.android.apps.photos,com.google.android.calendar,com.google.android.contacts,com.google.android.dialer,com.google.android.gm,org.lineageos.eleven,com.android.development,com.android.documentsui,com.example.android.notepad,com.google.android.googlequicksearchbox,com.google.android.googlequicksearchbox,com.googlecode.eyesfree.setorientation,com.termoneplus,cu.axel.smartdock,org.chromium.webview_shell,org.zeroxlab.util.tscal,com.toss.soda&accessibility=0&perms=0&contacts=[]&sim=[]&method=bots.new
2023-02-27	1 / 90	200	http://5.161.97.57:5000/api/?param=screen&value=1&botid=cc67103170c80093d6ec3bd935ff2e4b&method=bots.update&access=1
2023-02-27	1 / 90	200	http://5.161.97.57:5000/api/?param=accessibility&value=0&botid=cc67103170c80093d6ec3bd935ff2e4b&method=bots.update&access=1
2023-02-27	1 / 90	200	http://5.161.97.57:5000/api/?param=sms&value=1&botid=cc67103170c80093d6ec3bd935ff2e4b&method=bots.update&access=1
2023-02-22	1 / 90	405	http://5.161.97.57:5000/pstl
2023-03-27	0 / 86	200	http://ip-api.com/json
2023-02-27	1 / 90	200	http://5.161.97.57:5000/api/?botid=cc67103170c80093d6ec3bd935ff2e4b&botip=34.85.237.246&botCountry=US&botCity=Washington&sdkVersion=REL&deviceModel=QEMU+STANDARD+PC+(I440FX+++PIIX,+1996)+8.1.0+O&typeConnection=WIFI&battery=0%25&access=1&tag=Youtube+Vanced&version=8.1.0&packet=com.android.calendar,com.android.chrome,com.android.contacts,com.android.deskclock,com.android.dialer,com.android.gallery3d,com.android.settings,com.example.android.rssreader,com.google.android.gm,com.google.android.youtube,org.lineageos.eleven,com.android.calculator2,com.android.development,com.android.documentsui,com.example.android.notepad,com.farmerbb.taskbar.androidx86,com.google.android.apps.books,com.google.android.googlequicksearchbox,com.google.android.googlequicksearchbox,com.termoneplus,org.zeroxlab.util.tscal,eu.chainfire.supersu&accessibility=0&perms=0&contacts=[]&sim=[]&method=bots.new

Transact in Trust

End-to-end protection from fraud and financial crime.

Speak to an Expert



Awards and Recognition

Quadrant

Feedzai named a leader in SPARK Matrix AML.

Aite

Feedzai named best-in-class fraud and AML machine learning platform vendor

Chartis

Feedzai named a category leader in Chartis Payment Risk 2023

feedzai

sales@feedzai.com info@feedzai.com feedzai.com