New Antidot Trojan Disguised As Fake Google Play Updates

Published: 2024-05-16 · Archived: 2026-04-05 13:22:53 UTC

Key Takeaways

- A new Android Banking Trojan, “Antidot,” masquerading as a Google Play update application, displays fake Google Play update pages in multiple languages, indicating a wide range of targets.
- Antidot incorporates a range of malicious features, including overlay attacks and keylogging, allowing it to compromise devices and harvest sensitive information.
- Antidot maintains communication with its Command and Control (C&C) server through WebSocket, enabling real-time, bidirectional interaction for executing commands.
- The malware executes a wide range of commands received from the C&C server, including collecting SMS messages, initiating USSD requests, and even remotely controlling device features such as the camera and screen lock.
- Antidot implemented VNC using MediaProjection to remotely control infected devices.

Overview

In April, Cyble Research and Intelligence Labs (CRIL) released a detailed analysis of a newly surfaced Android Banking Trojan named Brokewell, created by malware developer Baron Samedit and capable of taking over devices.

Recently, we’ve discovered another new Android Banking Trojan, “Antidot,” initially spotted on May 06, 2024 (a6f6e6fb44626f8e609b3ccb6cbf73318baf01d08ef84720706b205f2864b116). This Trojan leverages overlay attacks as its primary method for gathering credentials.

This malware incorporates several features, including:

- VNC
- Keylogging
- Overlay attack
- Screen recording
- Call forwarding
- Collecting contacts and SMSs
- Performing USSD requests
- Locking and unlocking the device

We're referring to this Android Banking Trojan known as "Antidot," identified by the presence of the string "Antidot" within its source code, utilized for logging across different classes. This malware employs a custom encryption code for string obfuscation, along with gibberish class names, making analysis more challenging.

Figure 1 – Mentions of "Antidot" strings in malware source code

The malware masquerades as a Google Play update application, displaying a counterfeit Google Play update page upon installation. Our observations reveal that this fake update page has been crafted in various languages, including German, French, Spanish, Russian, Portuguese, Romanian, and English. This indicates that the malware is targeting Android users in these language-speaking regions.

Figure 2 – Fake update pages crafted in different languages

The next section presents a detailed technical analysis of the Antidot Android Banking Trojan.

Technical Details

As previously mentioned, after installation, the malware displays a fake update page featuring a “Continue” button that redirects the user to the Accessibility settings. Like other Android Banking Trojans, Antidot also relies on the Accessibility service to carry out its malicious activities.

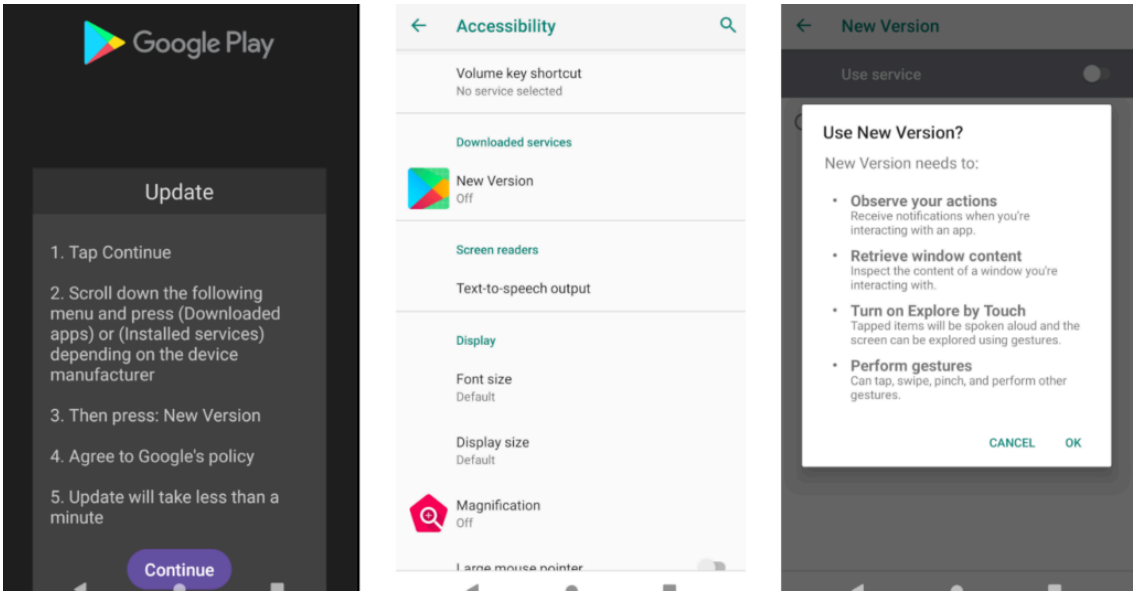

Figure 3 – Antidot prompting user to grant Accessibility permission

Command and Control server communication

In the background, the malware initiates communication with its Command and Control (C&C) server at “hxxp://46[.]228.205.159:5055/”. In addition to the HTTP connection, the Antidot Banking Trojan establishes WebSocket communication using the socket.io library, which enables real-time, bi-directional communication between the server and client. The malware maintains this communication through “ping” and “pong” messages.

From the client side, the malware uses the “ping” message and sends Base64 encoded data. An example of a ping message sent by the client is shown below:

42[“ping”,”1715751904″,”WyJyZXNTY3JlZW4iLCIxMDgwIiwiMTkyMCJd\n”]

From the server side, the malware receives “pong” messages containing plain text data. These pong messages typically include commands that the server wants to execute. An example of a pong message received from the server is:

42[“pong”,[“sos”,”1″]]

Once the user grants Accessibility service, the malware sends the first “ping message” to the server along with the Base64 encoded data, which contains below information:

- Malware application name
- SDK version
- MODEL
- MANUFACTURER
- Locale (language + country code)
- Installed application package list

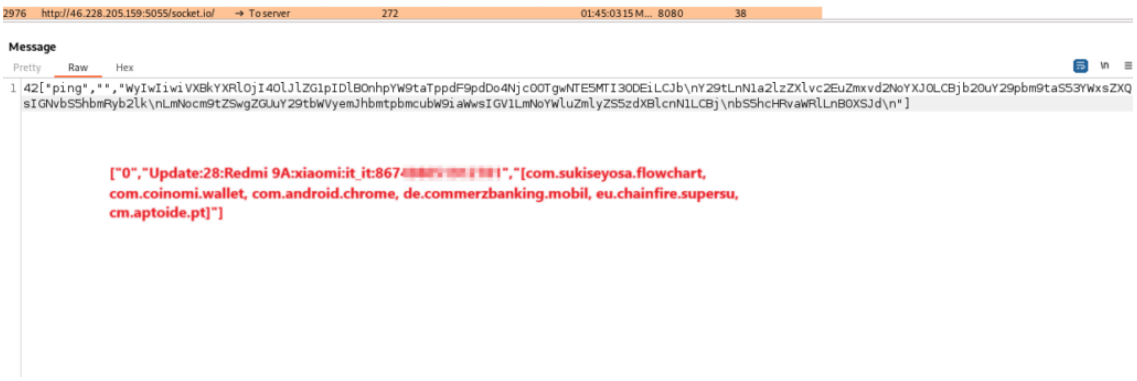

Figure 4 – First ping message to the server

After receiving the initial ping message, the server responds with a “pong” message that includes the bot ID generated for the infected device, as illustrated in the figure below:

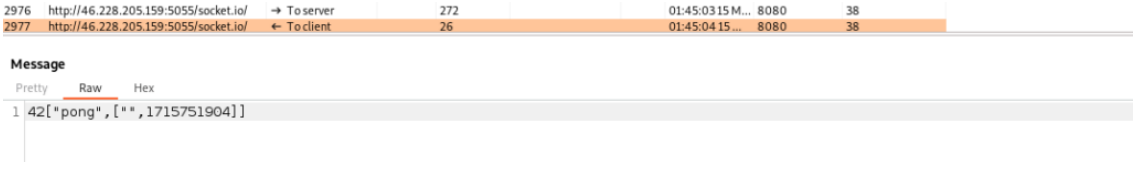

Figure 5 – Pong message with bot ID

During communication with the C&C server “hxxp://46[.]228.205.159:5055”, the malware obtains three additional server URLs. These can serve as backup options to maintain communication if the current C&C server becomes inactive. Below are the additional C&C servers received from the server:

- hxxp://213.255.246[.]209:5055

- hxxp://193.181.23[.]70:5055
- hxxp://188.241.240[.]75:5055

Commands Executed by malware

Once the server generates the bot ID, the Antidot Banking Trojan begins sending bot statistics to the server and receiving commands. During execution, we observed several commands received by the malware, including "sos", "setSettings," "getApps," and "getSMS."

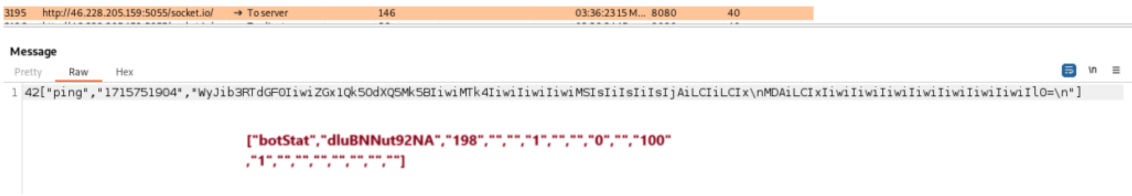

Figure 6 – Malware sends bot stats

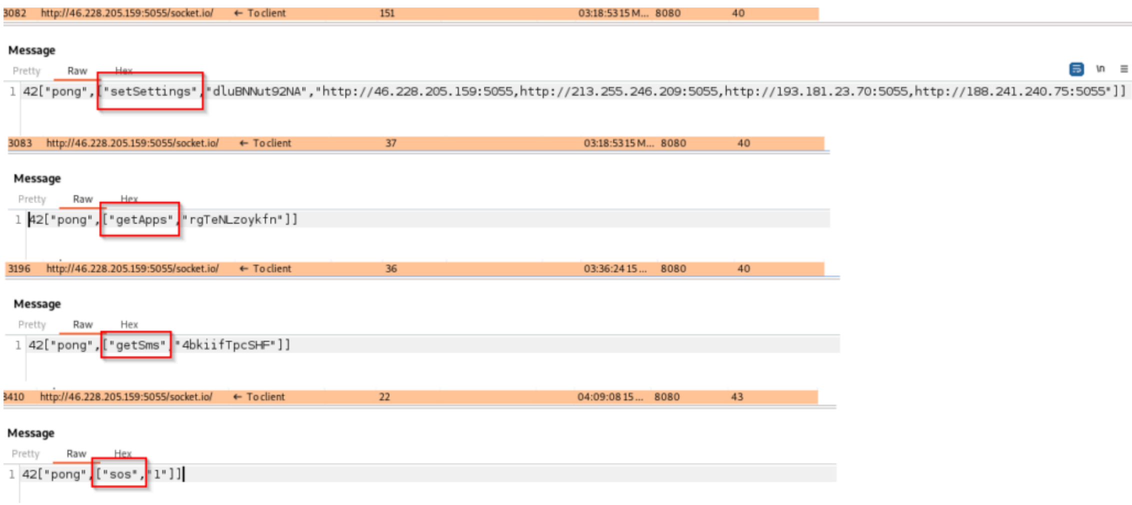

Figure 7 – Commands received from the server

The malware has implemented a total of 35 commands, which we have listed below.

Command	Description
speedMod	Updates application scope list
pauseInject	Updates shared preference value with 1 to pause overlay activity
stopAverlay	Stops overlay activity
stopCamera	Stops camera
setInjections	Saves injection overlay data in a hashmap
unlockDevice	Unlock device
startSleep	Save parameters related to the sleep feature in shared preference

sleepNow	Put the device on sleep mode
onFocus	Increases the brightness of the overlay window
openApp	Opens application specified by the server
getSms	Collects SMSs
callForward	Makes call from infected device
setSettings	Receives additional C&C server URLs
offFocus	Reduces the brightness of overlay windows
deleteApp	Uninstall application
deleteBot	Uninstall itself
updateShow	Displays updated content in the WebView
getApps	Collects installed application package name list
getKeys	Collects keystrokes
sos	Prompts the user to uninstall the application
actionVnc	Receives actions to perform on the infected device
lockDevice	Locks device
vncShow	Displays VNC into WebView
waitBar	Displays waiting bar overlay page
resumeInject	Resume showing overlay page
sendPush	Push notification
sendUssd	Makes USSD service call
startVnc	Initiates VNC
treeMode	Sends VNC content
onScreen	Adds overlay window
getContacts	Collects contact list
stopSleep	Wake up the device screen
stopSound	Mute device
startCamera	Opens camera and sends captured photo to the C&C server

sendSms	Sends SMS from an infected device

Antidot's VNC Feature

The Antidot malware utilizes the MediaProjection feature to capture the display content of the compromised device. It then encodes this content and transmits it to the Command and Control (C&C) server. The malware then initiates the VNC activity when it receives the command "startVNC" from the C&C server.

Figure 8 – Starts VNC after receiving the command

Once the screen content is transmitted, the malware can receive the command "actionVNC," along with the actions to perform on the current display screen of the infected device. Utilizing Accessibility service methods, the malware executes these actions as directed. Below is the list of VNC actions received from the server:

Action	**Description**
tap	Dispatch tap gesture
swipe	Makes swipe gesture
global-recent	Shows overview of recent apps
global-home	Execute action go home
global-back	Performs go back action
global-bar	Executes this action to open the notification
global-power	Opens power long press dialog
scroll-up	Dispatch gesture to scroll up
scroll-down	Dispatch gesture to scroll down
swipe-up	Dispatch gesture to swipe up
swipe-down	Dispatch gesture to swipe down

swipe-left	Dispatch gesture to swipe left
makeGesture	Dispatch gesture on x and y coordinates
textset	Collect text from the clipboard
unknown	Set text to the clipboard

Overlay Attack

The overlay attack module of the Antidot malware is akin to that of other well-known banking Trojans such as Ermac, Chameleon, and Brokewell. It employs HTML phishing pages designed to resemble authentic banking or cryptocurrency applications, loading them into WebView and creating an overlay window on the genuine application to capture credentials.

As mentioned earlier, the malware sends the installed application's package name list to the C&C server, which will be used to find the targeted application. Once the targeted applications are found on the infected device, the server then sends the command "SetInjections" along with the package name and Base64-encoded HTML injection page URL.

```
case -1786648450:
    if (d4.equals(N0.s(-117142734485206L))) {
        C1185o8 c1185o85 = AbstractC0132df.a;
        String s9 = N0.s(-120462744205014L);
        String d7 = c0247gh.d(2);
        AbstractC1283qt.h(d7, N0.s(-120522873747158L));
        c1185o85.getClass();
        h(s9, d7);
        try {
            C0322ih c0322ih = new C0322ih(c0247gh.d(3));
            Iterator keys = c0322ih.keys();
            while (keys.hasNext()) {
                String valueOf = String.valueOf(keys.next());
                String str = c0322ih.getString(valueOf).toString();
                AbstractC0132df.a.getClass();
                h(valueOf, str);
            }
            return;
        } catch (Throwable th) {
            th.printStackTrace();
            return;
        }
    }
    return;
```

setInjections

Figure 9 – Getting injections from the server

When the malware detects that the victim is using a targeted application by verifying the package name against its injection list, it creates an overlay window over the legitimate application and loads the injection URL into the WebView.

Figure 10 – Overlay attack activity

Keylogging

The Antidot Android Banking Trojan has incorporated keylogging alongside its overlay attack to harvest credentials. Whenever a victim initiates typing, the malware produces a “ping message” and transmits the exfiltrated keystrokes using Base64 encoding. To dispatch the stolen key logs, along with a timestamp and application name, the malware employs the “getKeys” command.

The figure below displays an example of the keylogger message sent by the malware.

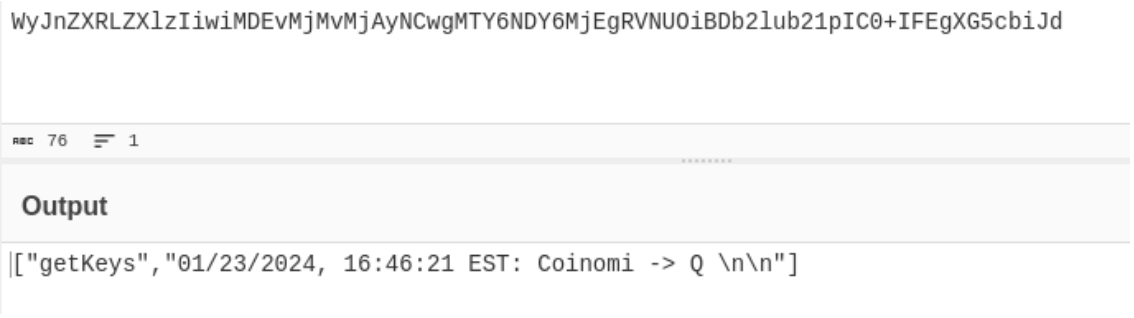

Figure 11 – Keylogger message example

Antidot’s SOS Command

Once the malware gains access to the accessibility service, it transmits data concerning the device and the package names of installed applications. If the server determines that the device is not the intended target, it sends the “SOS” command to the malware. This prompts the display of a dialog box, prompting the victim to uninstall the application, and ceases any further command transmission to the bot.

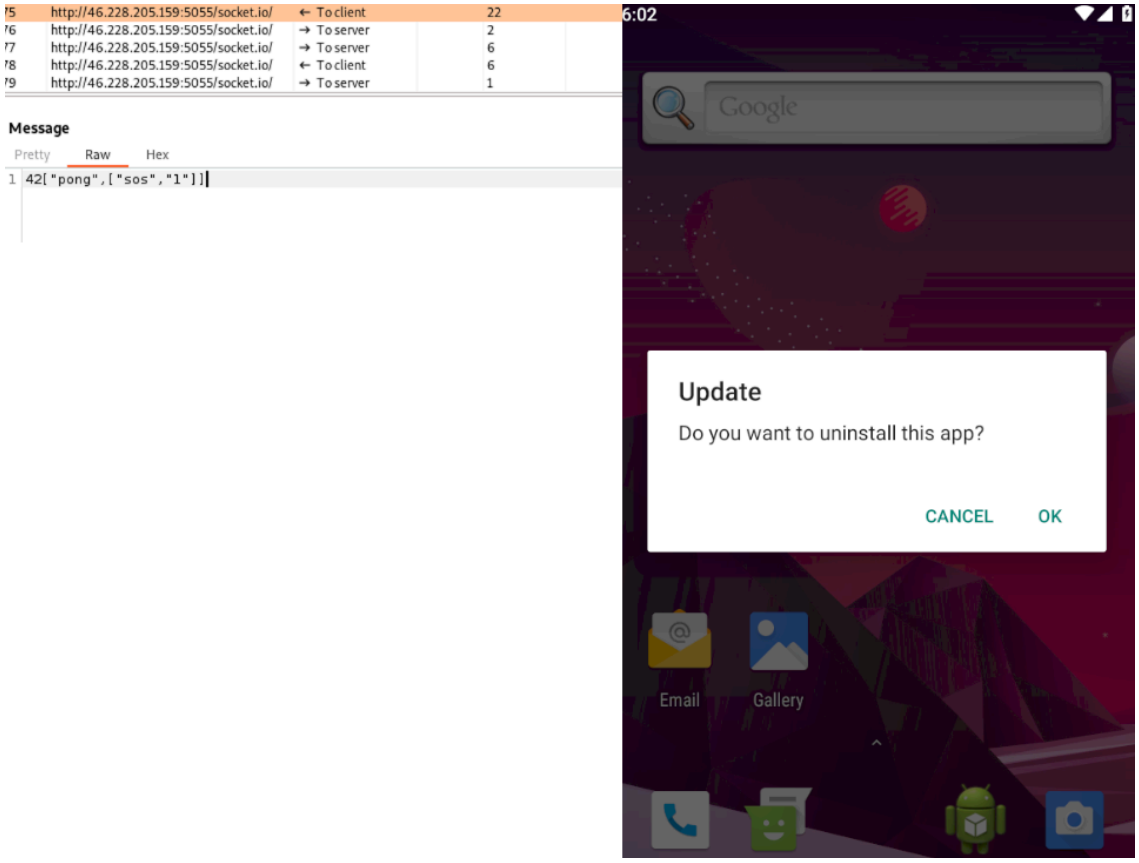

Figure 12 – SOS activity

Conclusion

The emergence of sophisticated Android Banking Trojans poses a significant threat to users' security and privacy. Among these, the newly surfaced "Antidot" Banking Trojan stands out for its multifaceted capabilities and stealthy operations. Its utilization of string obfuscation, encryption, and strategic deployment of fake update pages demonstrate a targeted approach aimed at evading detection and maximizing its reach across diverse language-speaking regions.

Analyzing its intricate workings sheds light on the evolving landscape of mobile malware and the ingenuity of cybercriminals. With its multifaceted capabilities, including overlay attacks, keylogging, and VNC features, Antidot poses a significant threat to users' privacy and financial security.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

- Only install software from official app stores such as the Play Store or the iOS App Store.
- It is recommended that connected devices, including PCs, laptops, and mobile devices, use a reputed antivirus and internet security software package.
- Use strong passwords and enforce multi-factor authentication wherever possible.
- Be careful while opening links received via SMS or emails sent to your mobile device.
- Google Play Protect should always be enabled on Android devices.

- Be wary of any permissions that you give an application.
- Keep devices, operating systems, and applications up to date.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Procedure
Defense Evasion (TA0030)	Masquerading: Match Legitimate Name or Location (T1655.001)	Malware pretending to be the Google Play Update application
Defense Evasion (TA0030)	Application Discovery (T1418)	Collects installed application package name list to identify target
Defense Evasion (TA0030)	Virtualization/Sandbox Evasion (T1633)	Malware implemented an anti-emulation check, which checks if the debugging is on.
Defense Evasion (TA0030)	Indicator Removal on Host: Uninstall Malicious Application (T1630.001)	Malware can uninstall itself
Defense Evasion (TA0030)	Input Injection (T1516)	Malware can mimic user interaction, perform clicks and various gestures, and input data
Collection (TA0035)	Input Capture: Keylogging (T1417.001)	Malware can capture keystrokes
Discovery (TA0032)	Software Discovery (T1418)	Malware collects installed application package list
Discovery (TA0032)	System Information Discovery (T1426)	The malware collects basic device information.
Collection (TA0035)	Screen Capture (T1513)	Malware can record screen content
Collection (TA0035)	Capture Camera (T1512)	Malware opens camera and takes pictures
Collection (TA0035)	Audio Capture (T1429)	Malware captures Audio recordings
Collection (TA0035)	Call Control (T1616)	Malware can make calls

Collection (TA0035)	Protected User Data: Call Log (T1636.002)	Malware steals call logs
Collection (TA0035)	Protected User Data: SMS Messages (T1636.004)	Steals SMSs from the infected device
Exfiltration (TA0036)	Exfiltration Over C2 Channel (T1646)	Sending exfiltrated data over C&C server

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
a6f6e6fb44626f8e609b3ccb6cbf73318baf01d08ef84720706b205f2864b116 c48240ce763e07b690e4fe79d6dfe69eeeebf8bd ac79187fd3024fb9cb5d1a872461503c	SHA256 SHA1 MD5	Antidot Android Banking Trojan
hxxps://wgona[.]click/	URL	C&C server
7a0664c3a9914531c84d875669f6249b433d09155b1c06ad3654c210a1798ee0 13479bb7364b710b2bb4a55ded4877d8232c0d90 0b6f0790c32a16e413c89bf65018ec6d	SHA256 SHA1 MD5	Antidot Android Banking Trojan
hxxp://46.228.205[.]159:5055/	URL	C&C server
9f8a49432e76b9c69d33ea228cc44254bc0a58bfa15eb0c51a302c59db81caa3 1c1d2fc881ea0565a372f71baf26454756bd3243 588d01860865256c378715ad728757cf	SHA256 SHA1 MD5	Antidot Android Banking Trojan
654cfe773e92261a7e2c74f4b16bd36be9286a95840b49139cf18c8d4333345b bb2a1b5909f31f1c4d694899d502b1d9f95c66c2 b877636c060e5fb47f467e557acdc9ac	SHA256 SHA1 MD5	Dropper file hash
hxxp://213.255.246[.]209:5055 hxxp://193.181.23[.]70:5055 hxxp://188.241.240[.]75:5055	Domain	C&C server

---

Source: https://cyble.com/blog/new-antidot-android-banking-trojan-masquerading-as-google-play-updates/