ViperRAT: The mobile APT targeting the Israeli Defense Force that should be on your radar

blog.lookout.com/blog/2017/02/16/viperrat-mobile-apt/

February 16, 2017

By Michael Flossman, Security Researcher

ViperRAT is an active, advanced persistent threat (APT) that sophisticated threat actors are actively using to target and spy on the Israeli Defense Force.

The threat actors behind the ViperRAT surveillanceware collect a significant amount of sensitive information off of the device, and seem most interested in exfiltrating images and audio content. The attackers are also hijacking the device camera to take pictures.

Using data collected from the Lookout global sensor network, the Lookout research team was able to gain **unique visibility into the ViperRAT malware, including 11 new, unreported applications.** We also discovered and analyzed live, misconfigured malicious command and control servers (C2), from which we were able to identify how the attacker gets new, infected apps to secretly install and the types of activities they are monitoring. In addition, we uncovered the IMEIs of the targeted individuals (IMEIs will not be shared publicly for the privacy and safety of the victims) as well as the types of exfiltrated content.

Lookout has determined ViperRAT is a very sophisticated threat that adds to the mounting evidence that targeted mobile attacks against governments and business is a real problem.

In aggregate, the type of information stolen could let an attacker know where a person is, with whom they are associated (including contacts' profile photos), the messages they are sending, the websites they visit and search history, screenshots that reveal data from other apps on the device, the conversations they have in the presence of the device, and a myriad of images including anything at which device's camera is pointed.

Lookout has determined ViperRAT is a very sophisticated threat that adds to the mounting evidence that targeted mobile attacks against governments and business is a real problem.

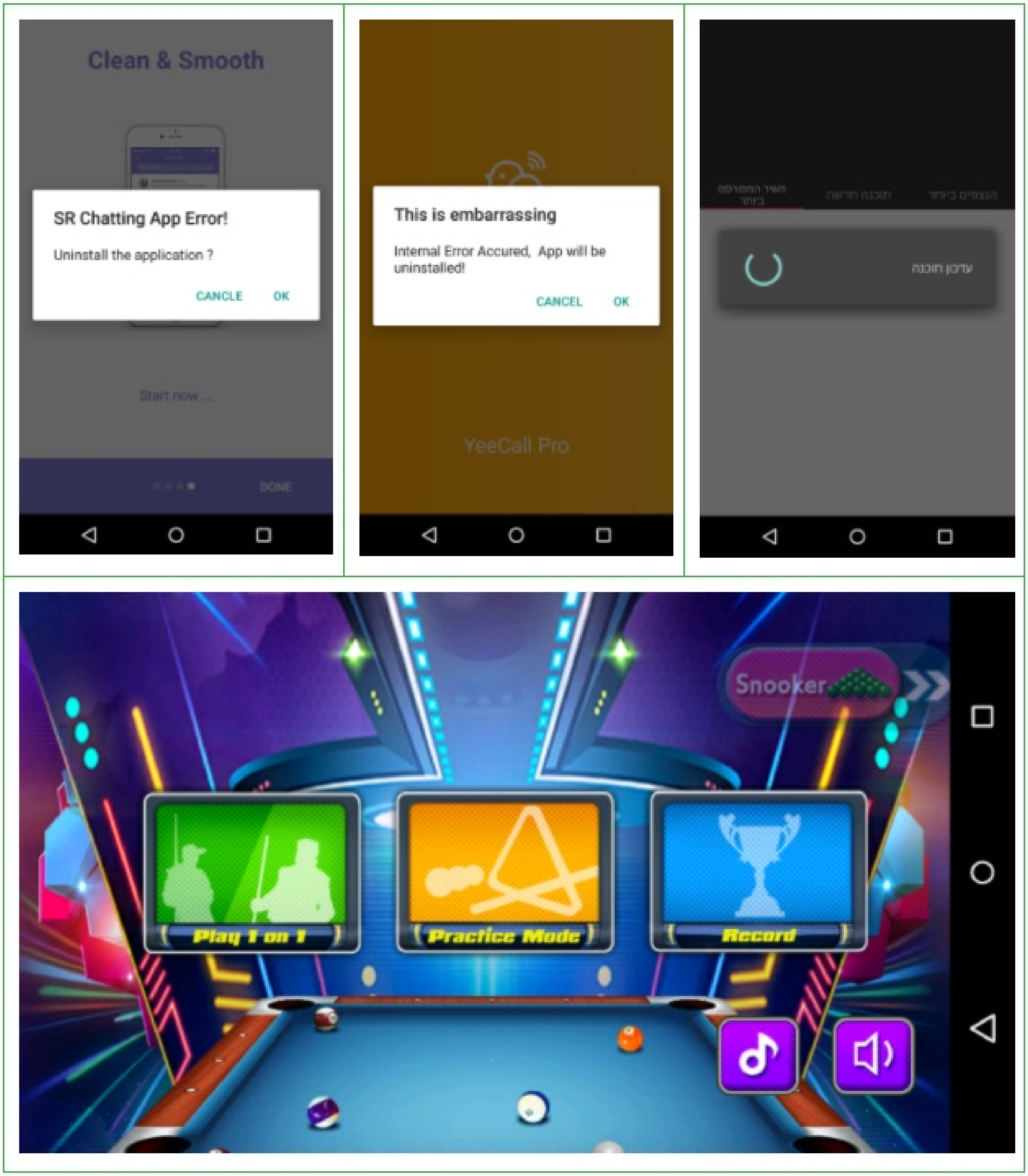
Lookout researchers have been tracking this threat for the last month. Given that this is an active threat, we've been working behind-the-scenes with our customers to ensure both personal and enterprise customers are protected from this threat and only decided to come forward with this information after the research team at Kaspersky released a report earlier today.

Additionally, we have determined that though original reports of this story attribute this surveillanceware tool to Hamas, this may not be the case, as we demonstrate below.

The increasing sophistication of surveillanceware

The structure of the surveillanceware indicates it is very sophisticated. Analysis indicates there are currently two distinct variants of ViperRAT. The first variant is a "first stage application," that performs basic profiling of a device, and under certain conditions attempts to download and install a much more comprehensive surveillanceware component, which is the second variant.

The first variant involves social engineering the target into downloading a trojanized app. Previous reports alleged this surveillanceware tool was deployed using ‘honey traps’ where the actor behind it would reach out to targets via fake social media profiles of young women. After building an initial rapport with targets, the actors behind these social media accounts would instruct victims to install an additional app for easier communication. Specifically, Lookout determined these were trojanized versions of the apps SR Chat and YeeCall Pro. We also uncovered ViperRAT in a billiards game, an Israeli Love Songs player, and a Move To iOS app.



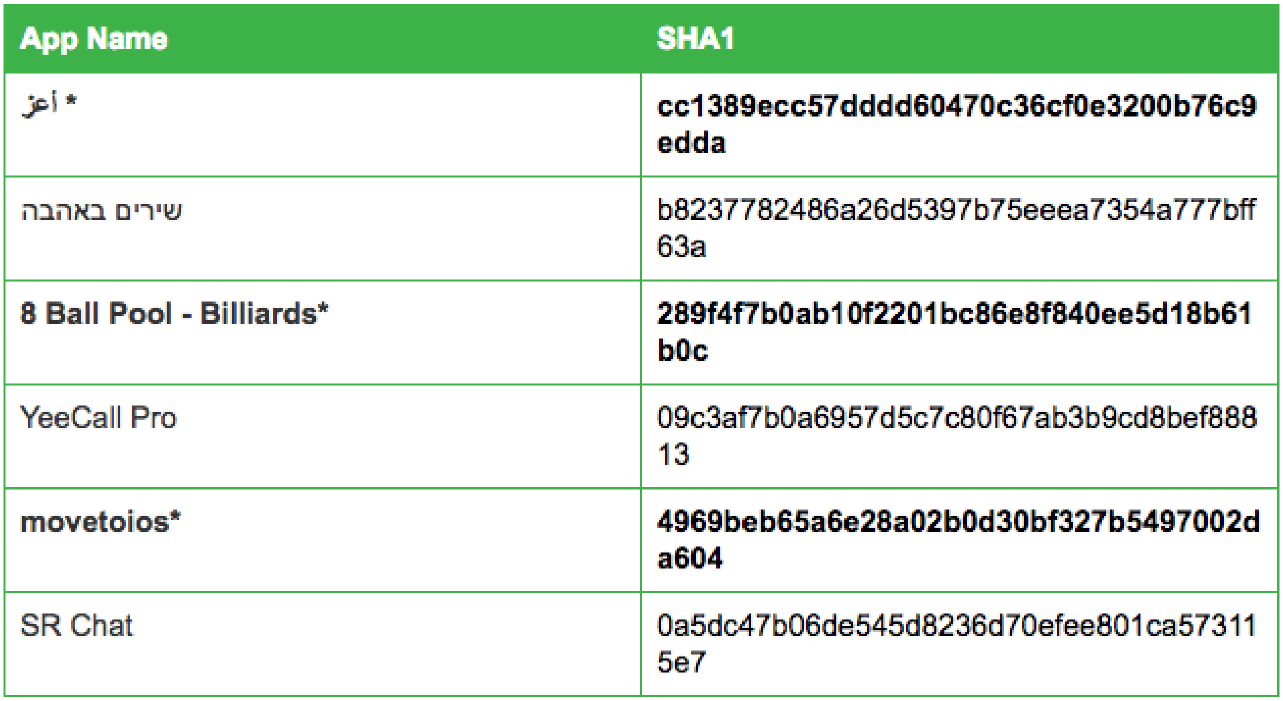
SR Chatting App Error!

Uninstall the application ?

This is embarrassing

Internal Error Accured, App will be uninstalled!

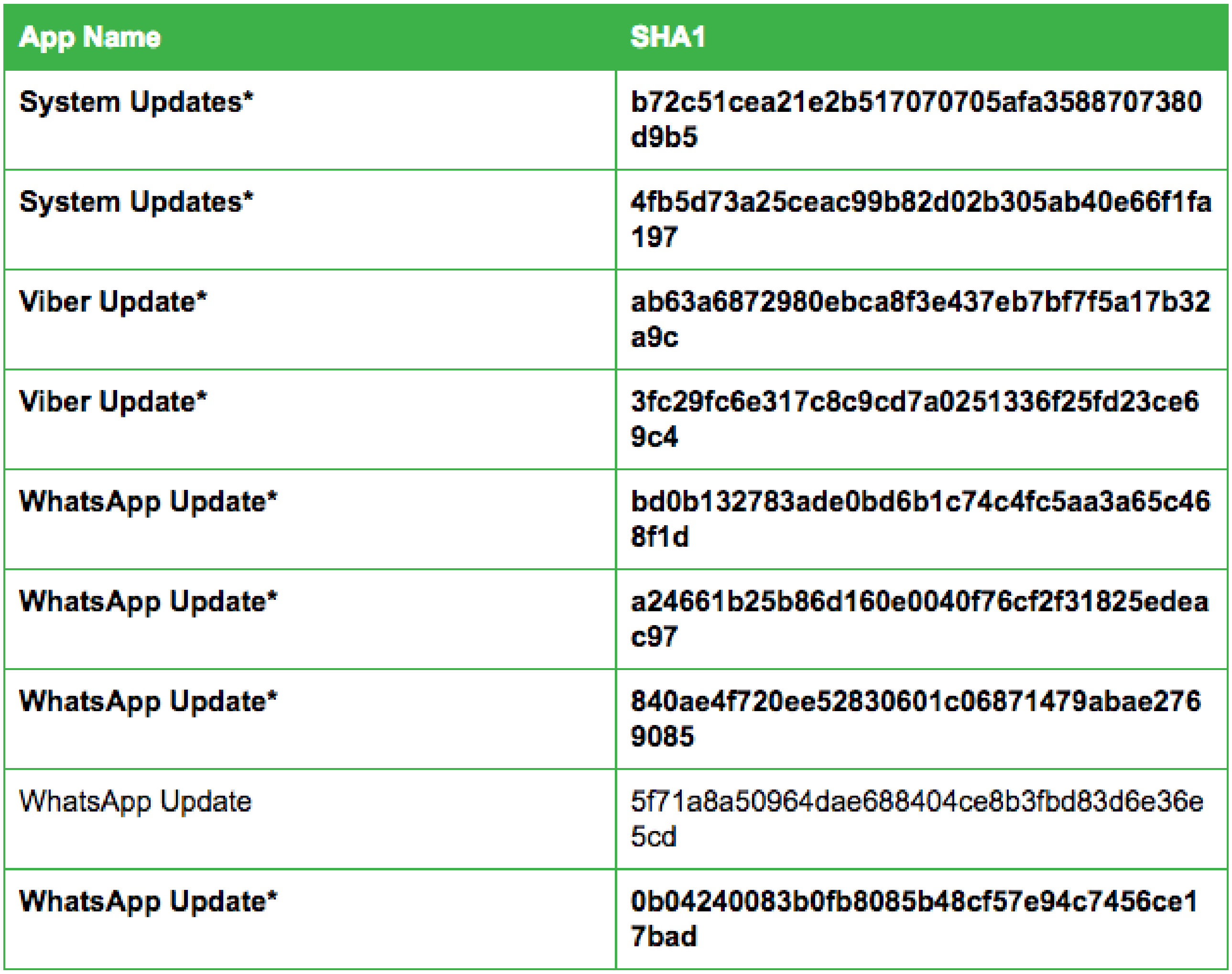
עדכון תוכנה



App Name	SHA1
أعز *	**cc1389ecc57dddd60470c36cf0e3200b76c9edda**
שירים באהבה	b8237782486a26d5397b75eeea7354a777bff63a
8 Ball Pool - Billiards*	**289f4f7b0ab10f2201bc86e8f840ee5d18b61b0c**
YeeCall Pro	09c3af7b0a6957d5c7c80f67ab3b9cd8bef88813
movetoios*	**4969beb65a6e28a02b0d30bf327b5497002da604**
SR Chat	0a5dc47b06de545d8236d70efee801ca573115e7

The second stage

The second stage apps contain the surveillanceware capabilities. Lookout uncovered nine secondary payload applications:



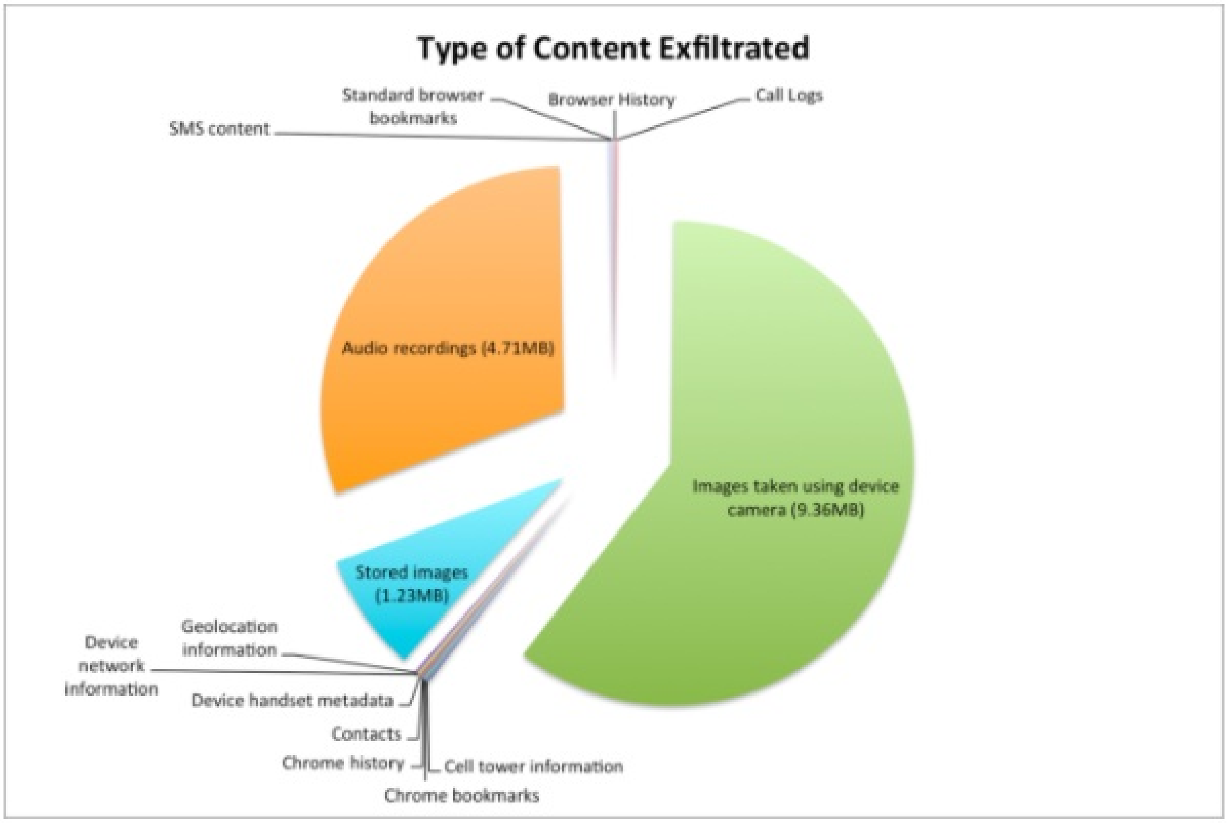
App Name	SHA1
System Updates*	**b72c51cea21e2b517070705afa3588707380d9b5**
System Updates*	**4fb5d73a25ceac99b82d02b305ab40e66f1fa197**
Viber Update*	**ab63a6872980ebca8f3e437eb7bf7f5a17b32a9c**
Viber Update*	**3fc29fc6e317c8c9cd7a0251336f25fd23ce69c4**
WhatsApp Update*	**bd0b132783ade0bd6b1c74c4fc5aa3a65c468f1d**
WhatsApp Update*	**a24661b25b86d160e0040f76cf2f31825edeac97**
WhatsApp Update*	**840ae4f720ee52830601c06871479abae2769085**
WhatsApp Update	5f71a8a50964dae688404ce8b3fbd83d6e36e5cd
WhatsApp Update*	**0b04240083b0fb8085b48cf57e94c7456ce17bad**

** These apps have not been previously reported and were discovered using data from the Lookout global sensor network, which collects app and device information from over 100 million sensors to provide researchers and customers with a holistic look at the mobile threat ecosystem today.*

Naming additional payload applications as system updates is a clever technique used by malware authors to trick victims into believing a threat isn't present on their device. ViperRAT takes this one step further by using its dropper app to identify an appropriate second stage 'update' that may go unnoticed. For example, if a victim has Viber on their device, it will choose to retrieve the Viber Update second stage. If he doesn't have Viber, the generically-named System Updates app gets downloaded and installed instead.

What was taken

The actors behind ViperRAT seem to be particularly interested in image data. We were able to identify that 8,929 files had been exfiltrated from compromised devices and that the overwhelming majority of these, 97 percent, were highly likely encrypted images taken using the device camera. We also observed automatically generated files on the C2, indicating the actor behind this campaign also issues commands to search for and exfiltrate PDF and Office documents. This should be highly alarming to any government agency or enterprise.

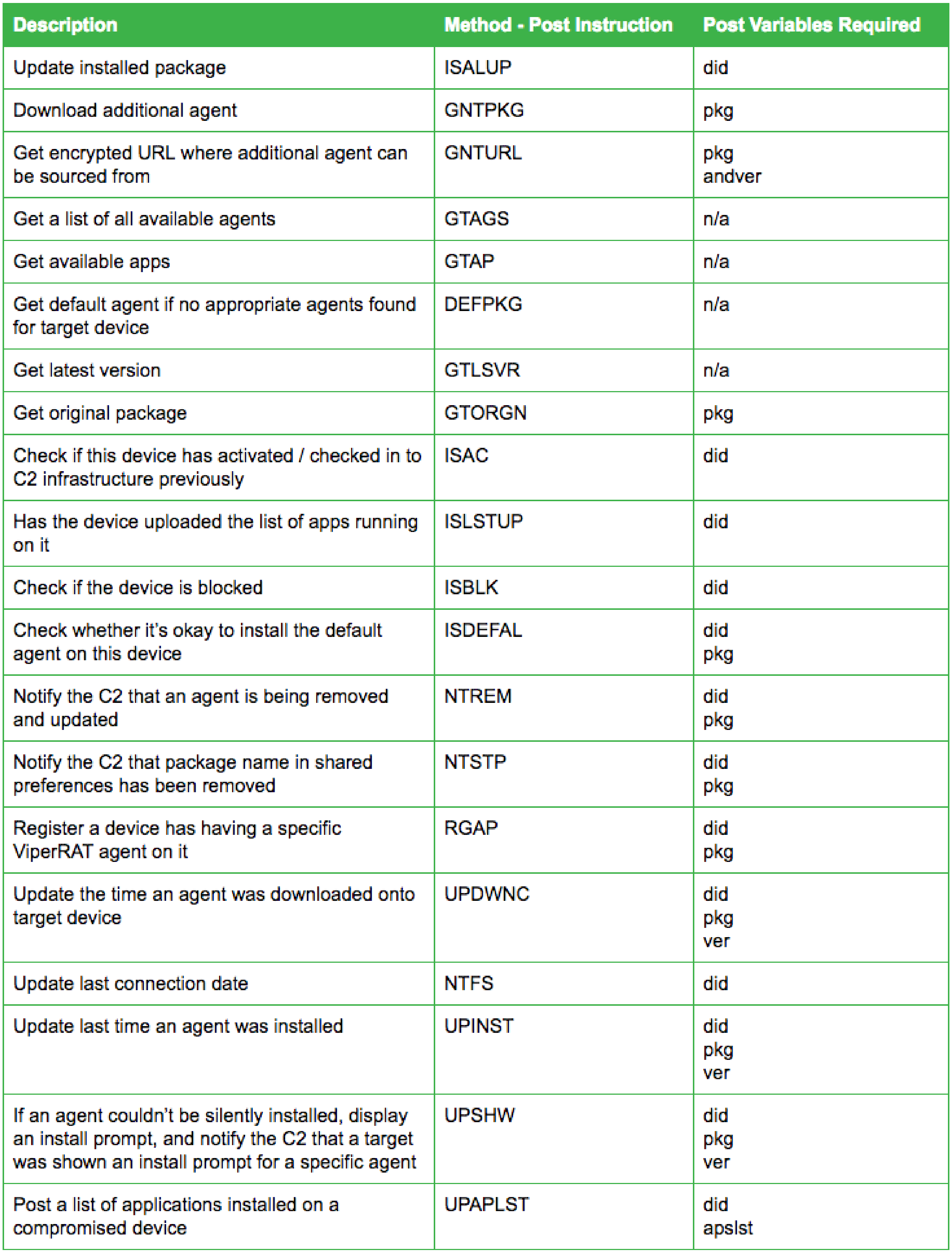


We observed legitimate exfiltrated files of the following types of data:

- Contact information
- Compressed recorded audio in the Adaptive Multi-Rate (amr) file format
- Images captured from the device camera
- Images stored on both internal device and SDCard storage that are listed in the MediaStore
- Device geolocation information
- SMS content
- Chrome browser search history and bookmarks
- Call log information
- Cell tower information
- Device network metadata; such as phone number, device software version, network country, network operator, SIM country, SIM operator, SIM serial, IMSI, voice mail number, phone type, network type, data state, data activity, call state, SIM state, whether device is roaming, and if SMS is supported.
- Standard browser search history
- Standard browser bookmarks
- Device handset metadata; such as brand, display, hardware, manufacturer, product, serial, radio version, and SDK.

Command and control API calls

ViperRAT samples are capable of communicating to C2 servers through an exposed API as well as websockets. Below is a collection of API methods and a brief description around their purpose.



Description	Method - Post Instruction	Post Variables Required
Update installed package	ISALUP	did
Download additional agent	GNTPKG	pkg
Get encrypted URL where additional agent can be sourced from	GNTURL	pkg andver
Get a list of all available agents	GTAGS	n/a
Get available apps	GTAP	n/a
Get default agent if no appropriate agents found for target device	DEFPKG	n/a
Get latest version	GTLSVR	n/a
Get original package	GTORGN	pkg
Check if this device has activated / checked in to C2 infrastructure previously	ISAC	did
Has the device uploaded the list of apps running on it	ISLSTUP	did
Check if the device is blocked	ISBLK	did
Check whether it's okay to install the default agent on this device	ISDEFAL	did pkg
Notify the C2 that an agent is being removed and updated	NTREM	did pkg
Notify the C2 that package name in shared preferences has been removed	NTSTP	did pkg
Register a device has having a specific ViperRAT agent on it	RGAP	did pkg
Update the time an agent was downloaded onto target device	UPDWNC	did pkg ver
Update last connection date	NTFS	did
Update last time an agent was installed	UPINST	did pkg ver
If an agent couldn't be silently installed, display an install prompt, and notify the C2 that a target was shown an install prompt for a specific agent	UPSHW	did pkg ver
Post a list of applications installed on a compromised device	UPAPLST	did apslst

On attribution

Media reporting on ViperRAT thus far attributes this surveillanceware tool to Hamas. Israeli media published the first reports about the social networking and social engineering aspects of this campaign. However it’s unclear whether organizations that later reported on ViperRAT performed their own independent research or simply based their content on the original Israeli report. Hamas is not widely known for having a sophisticated mobile capability, which makes it unlikely they are directly responsible for ViperRAT.

ViperRAT has been operational for quite some time, with what appears to be a test application that surfaced in late 2015. Many of the default strings in this application are in Arabic, including the name. It is unclear whether this means early samples were targeting Arabic speakers or if the developers behind it are fluent in Arabic.

This leads us to believe this is another actor.

What this means for you

All Lookout customers are protected from this threat. However, the existence of threats like ViperRAT and Pegasus, the most sophisticated piece of mobile surveillanceware we’ve seen to date, are evidence that attackers are targeting mobile devices.