ITG18 operational security errors plague Iranian threat group

By Allison Wikoff, Richard Emerson, Wei Gao

Published: 2021-08-04 · Archived: 2026-04-05 16:59:36 UTC

Allison Wikoff

Strategic Cyber Threat Analyst

IBM Security

Richard Emerson

Cyber Threat Intelligence Analyst

Wei Gao

Malware Reverse Engineer

This blog supplements a Black Hat USA 2021 talk given August 2021.

IBM Security X-Force threat intelligence researchers continue to track the infrastructure and activity of a suspected Iranian threat group ITG18. This group's tactics, techniques and procedures(TTPs) overlap with groups known as Charming Kitten, Phosphorus and TA453.

Since our initial report on the group's training videos in May 2020, X-Force has uncovered additional operational security errors by this group. Our continued analysis led to the discovery of a malicious tool that has not been previously linked to this threat actor, a custom Android backdoor we named "LittleLooter." LittleLooter has only been observed being used by ITG18. X-Force is not aware of other threat actors leveraging this backdoor.

Additionally, from August 2020 through May 2021, X-Force observed ITG18 successfully compromise multiple victims aligned with the Iranian reformist movement. Given the timing and focus of the activity, this may have been in support of surveillance objectives leaving up to the June 2021 presidential elections in Iran. Finally, despite continued OPSEC errors, ITG18 appears to conduct a sizeable and often successful operation that heavily focuses on compromising personal webmail and social media accounts.

LittleLooter, ITG18's Android surveillance tool

X-Force researchers discovered a file named "WhatsApp.apk" (md5: a04c2c3388da643ef67504ef8c6907fb) on infrastructure associated with ITG18 operations.

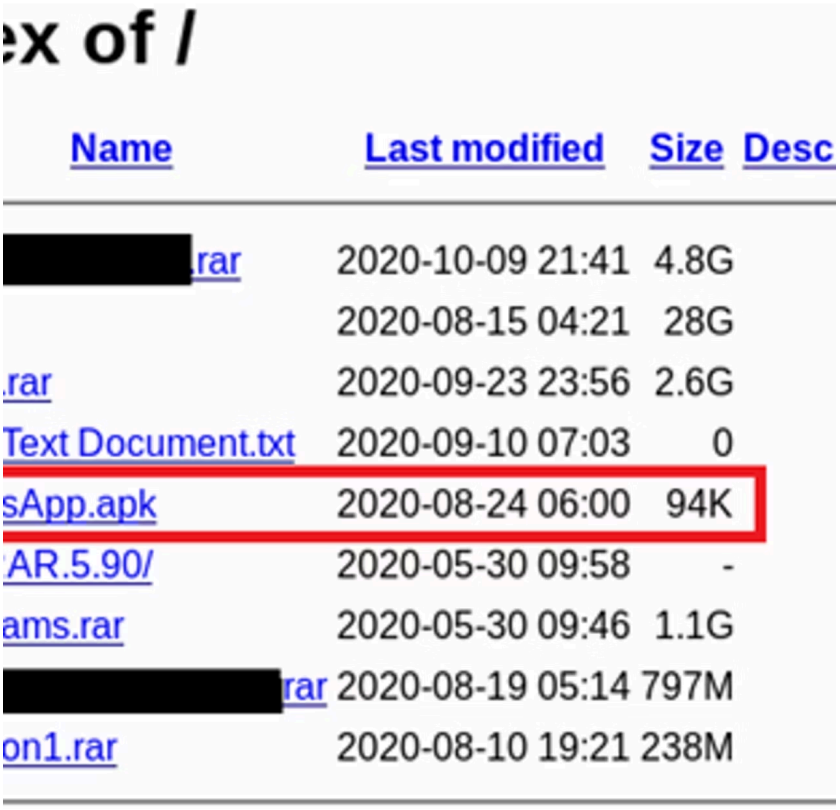

Figure 1: Open Directory listing for ITG18 server hosting victim exfil and LittleLooter (Source: X-Force)

Upon further analysis, X-Force determined “WhatsApp.apk” was Android malware that we named “LittleLooter” based on its information stealing capabilities..

For C2 communication, LittleLooter attempts to establish communication to the C2 server via HTTP POST requests and responses. The C2 server masquerades as an American flower shop and has been active since July 2020. The communication between the malware and the C2 server is compressed via GZIP, AES encrypted and BASE64 encoded. The AES key and initialization vector (IV) are hardcoded into the sample:

KEY:3544c085656c997

IV:4fcff6864c594343

LittleLooter is functionally rich, providing ITG18 operators the following capabilities on an infected Android device:

• Record video	• Call a number
• Record live screen	• Upload/download/delete a file

• Record sound	• List storage information
• Record voice call	• Gather GPS- or GSM-based location
• List device information	• Show network activity
• Determinate whether screen is on or off	• Show network speed
• List installed apps	• Show network connectivity
• Send browser history	• Turn on/off Wi-Fi
• Turn on/off Bluetooth	• Turn mobile data on/off
• List contact information	• List SIM card information
• List SMS inbox/outbox/drafts	• Take a picture
• List calls including received and missed calls	

The LittleLooter sample X-Force analyzed had the version number “5”, as well as an update capability if LittleLooter detected it was running a previous version. The tool updates itself by downloading a zip file from a URL on the C2 server: “*http[:]//[C2server]/updates/update_[class name].zip”* and replacing the old “classes.dex” file with the newer version from the zip file. Finally, LittleLooter is a modified version of Android malware reported by third party researchers several years ago and has likely been in use by ITG18 for years prior to our association with this threat group.

New targeting supports possible surveillance objectives

In addition to the discovery of LittleLooter, X-Force researchers discovered ITG18 targeted Iranian individuals from late summer 2020 through spring 2021, which supports ITG18’s long-standing operations against Iranian citizens of interest. X-Force has found that despite public reporting of their OPSEC mistakes, ITG18 continues to leave archive files containing exfiltrated victim information on open servers and in open directories. The new

analysis by X-Force revealed ITG18 exfiltrated roughly 120 gigabytes of information from approximately 20 individuals aligned with the Reformist movement in Iran.

Similar to exfiltrated information X-Force observed ITG18 steal last summer, this new stolen data was frequently extracted using legitimate utilities associated with the compromised accounts. Most recently, those were Telegram accounts, one of the most popular instant messaging services used in Iran. Telegram is one of the only foreign social media services permitted for use in Iran and was heavily used during the 2009 Green Movement to organize protests. X-Force researchers believe the victims' Telegram data was possibly targeted during the summer 2020 through spring-2021 time frame to support monitoring any dissent or protests around Iran's 2021 June Presidential Election.

While X-Force did not observe how initial access to the accounts was gained, ITG18 could have leveraged LittleLooter's capabilities or used phishing/social engineering to gather account credentials from their targets.

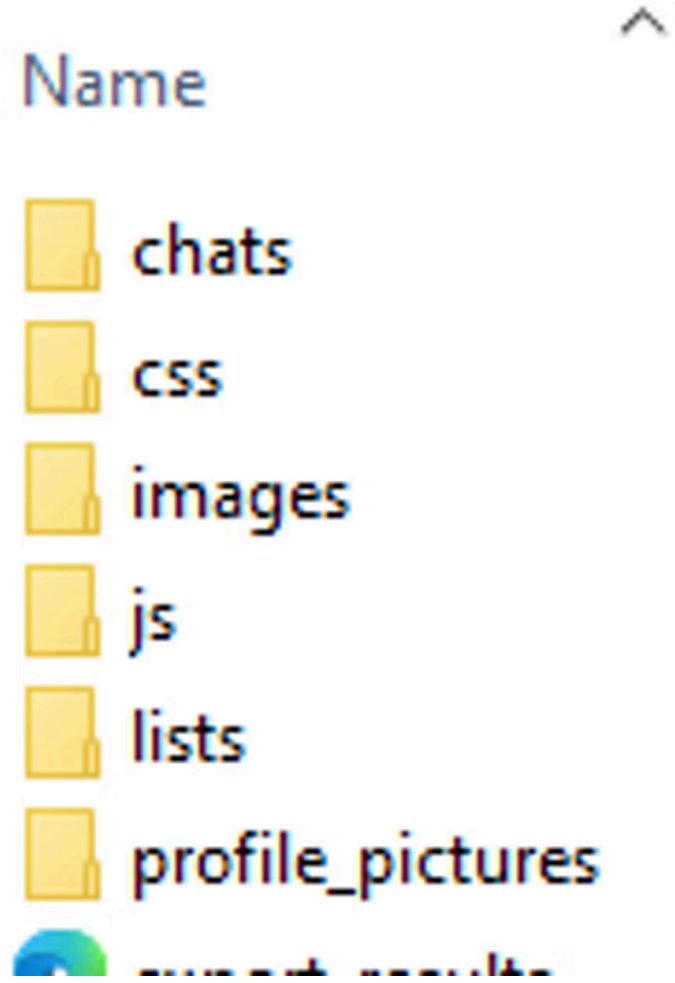

Figure 2: Victim's Telegram account data exported by ITG18 (Source: X-Force)

Based on the exfiltrated information X-Force observed, most of the victims were associated with Iran's Reformist movement, a political faction within Iran that supports more leftist policies versus the current, conservative regime. The stolen data contained photos associated with the victim, contact lists, group memberships and conversations.

A sizable operation marches on

The information X-Force has gleaned on ITG18's activity, in conjunction with the training videos X-Force found in the summer of 2020, continues to paint a picture of a threat actor that likely leverages a considerable number of personnel. This is underpinned by how manual and labor-intensive ITG18 operations appear to be, from gaining initial access to individual victim accounts to carefully reviewing exfiltrated data.

Several open-source reports have noted how ITG18 operators, beyond simply sending phishing messages, will also attempt to chat, call, and even video conference with targets. This personalized attention to each compromised individual likely requires hands-on work from a large number of operators. While X-Force cannot confirm how many individuals and organizations ITG18 has targeted recently, what has been observed so far in 2021 is identification of over 60 servers hosting more than 100 phishing domains, which suggests there may be a large number of victims.

X-Force has also observed how manual ITG18 operations can be when reviewing exfiltrated information. Through some of the videos that X-Force discovered last summer, an ITG18 operator was observed spending hours in manual work. They were seen validating credentials by copying and pasting stolen victim usernames and passwords into a wide variety of websites, for just two victims. X-Force alone has observed almost 2 terabytes of compressed exfiltrated data on publicly accessible ITG18 servers since 2018. This likely represents only a small portion of the data actually stolen by this adversary. Coupled with the training videos X-Force discovered, suggesting ITG18 has enough turnover or growth to warrant training, this likely indicates ITG18 requires a significant number of personnel for operations, as well as for processing and evaluating exfiltrated information.

Anticipate activity for the foreseeable future

ITG18 operations persist despite numerous public disclosures of their insecure activity and stolen data, speaking to the ability of this group to continue on its mission. X-Force researchers have high confidence that ITG18 activity will continue regardless of public reporting due to their broad objectives and continued success of their operations. We recommend reviewing the indicators below to identify potential malicious activity on your networks and on mobile devices.

If you have experienced a cyber incident and would like immediate assistance from IBM Security X-Force incident response, please call our hotline at 1-888-241-9812 (US) or +001-312-212-8034 (global). Learn more about X-Force's threat intelligence and incident response services.

Indicators of compromise

Indicator	Type	Context

c2c1d804aeed1913f858df48bf89a58b1f9819d7276a70b50785cf91c9d34083	sha256 hash	LittleLooter, Filename WhatsApp.apk
c760adecea4dbb4dd262cb3f3848f993d5007b2e	sha1 hash	LittleLooter, Filename WhatsApp.apk
a04c2c3388da643ef67504ef8c6907fb		

Complete list of LittleLooter commands

Command	Description
apps_list	List installed apps
browser_history	Send browser history
call_number	Call a number
calls_log_incoming	List received calls
calls_log_missed	List missed calls
calls_log_outgoing	List calls
calls_recorder	Record voice call
camera_list	List camera devices
contacts	List contact information
device_info	List device information
directory_list	List files in a directory
error_list	Send error log
file_delete	Delete a file
file_download	Download a file
file_list	List files in storage
file_upload	Upload a file
live_stream	Record live screen
location_gps	GPS based location

location_gsm	GSM based location
network_activity	Show network activity
network_speed	Show network speed
network_state	Show network connectivity
off_bluetooth	Turn off Bluetooth
off_data	Turn mobile data off
off_wifi	Turn off Wi-Fi
on_bluetooth	Turn on Bluetooth
on_data	Turn mobile data on
on_wifi	Turn on Wi-Fi
picture_take	Take a picture
screen_state	Determinate whether screen is on or off
sim_card	List SIM card information
sms_drafts	List SMS drafts
sms_inbox	List SMS inbox
sms_outbox	List SMS outbox
sms_send	Send SMS message
sound_recorder	Record sound
storage_activity	List storage information
video_recorder	Record video
