

Who's who in the Zoo

Cyberespionage operation targets Android users in the Middle East

By [Alexey Firsh](#) on May 3, 2018. 10:00 am

ZooPark is a cyberespionage operation that has been focusing on Middle Eastern targets since at least June 2015. The threat actors behind the operation infect Android devices using several generations of malware, with the attackers including new features in each iteration. We label them from v1-v4, with v4 being the most recent version deployed in 2017. From the technical point of view, the evolution of ZooPark has shown notable progress: from the very basic first and second versions, the commercial spyware fork in its third version and then to the complex spyware that is version 4. This last step is especially interesting, showing a big leap from straightforward code functionality to highly sophisticated malware.

[Energetic Bear/Crouching Yeti: attacks on servers](#)

[A Slice of 2017 Sofacy Activity](#)

[Sofacy APT hits high profile targets with updated toolset](#)

[APT Trends report Q3 2017](#)

[From Linux to Windows – New Family of Cross-Platform Desktop Backdoors Discovered](#)



**KASPERSKY LAB:
PLATINUM AWARD**

Gartner Peer Insights Customer Choice Award for Endpoint Protection Platforms

[Find out more >](#)

Ver. 4

Ver. 3

Ver. 2

Ver. 1

Exfiltrated info:

Contacts;
Accounts.

Additional exfiltrated info:

Call logs;
GPS location;
SMS messages;
Device information.

Additional exfiltrated info:

Call records (audio);
Installed applications details;
Browser data - bookmarks & history;
Photos and pictures from memory card.

Additional exfiltrated info:

Keylogs;
Clipboard data;
Arbitrary files/folders;
Browser data - search history;
Capturing photos/videos/audio/screenshots/screen records;
External applications data - default list of them is: Telegram,
WhatsApp, IMO, Chrome (could be extended in config).

Backdoor functionality:

Shell commands execution (with or without root);
Silently sending SMS messages;
Making calls.

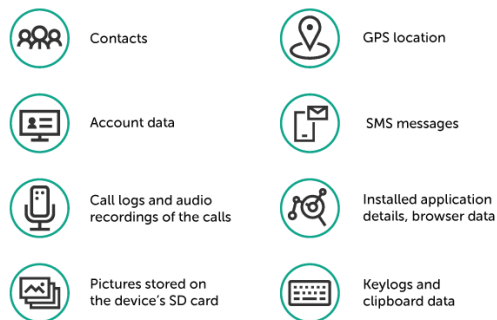
Evolution of ZooPark malware features

We have observed two main distribution vectors for ZooPark – Telegram channels and watering holes. The second one was the preferred vector: we found several news websites that have been hacked by the attackers to redirect visitors to a downloading site that serves malicious APKs. Some of the themes observed in campaign include “Kurdistan referendum”, “TelegramGroups” and “Alnaharegypt news”, among others.

The map of targets of the ZooPark advanced persistent threat

ZooPark is a sophisticated cyberespionage campaign, which for several years has been targeting Android device users based in Middle Eastern countries.

Upon successful infection, the malware steals:



Kaspersky Lab products successfully detect and block this threat



KASPERSKY **GREAT** **AMR**

© 2018 Kaspersky Lab. All Rights Reserved

Target profile has evolved during the last years of campaign, focusing on victims in Egypt, Jordan, Morocco, Lebanon and Iran.

If you would like to learn more about our intelligence reports or request more information on a specific report, contact us at: intelreports@kaspersky.com.

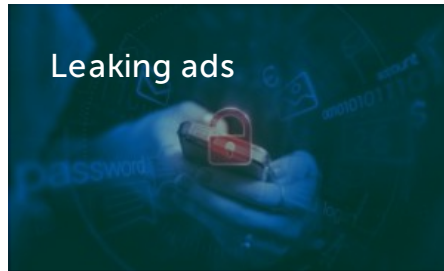
Android users in the Middle East." report

APT BACKDOOR CYBERESPIONAGE GOOGLE ANDROID MALWARE DESCRIPTIONS WATERING HOLE ATTACKS

Share post on:



Related Posts



LEAVE A REPLY

Your email address will not be published. Required fields are marked *

Enter your comment here

Name *

Email *

Notify me when new comments are added.

SUBMIT



Please upgrade to a [supported browser](#) to get a reCAPTCHA challenge.

Alternatively if you think you are getting this page in error, please check your internet connection and reload.

[Why is this happening to me?](#)



© 2018 AO Kaspersky Lab. All Rights Reserved.

Registered trademarks and service marks are the property of their respective owners.

[Contact us](#) | [Privacy Policy](#) | [License Agreement](#)

Email

SUBSCRIBE

