Who’s who in the Zoo

By Alexey Firsh

Published: 2018-05-03 · Archived: 2026-04-06 00:29:13 UTC

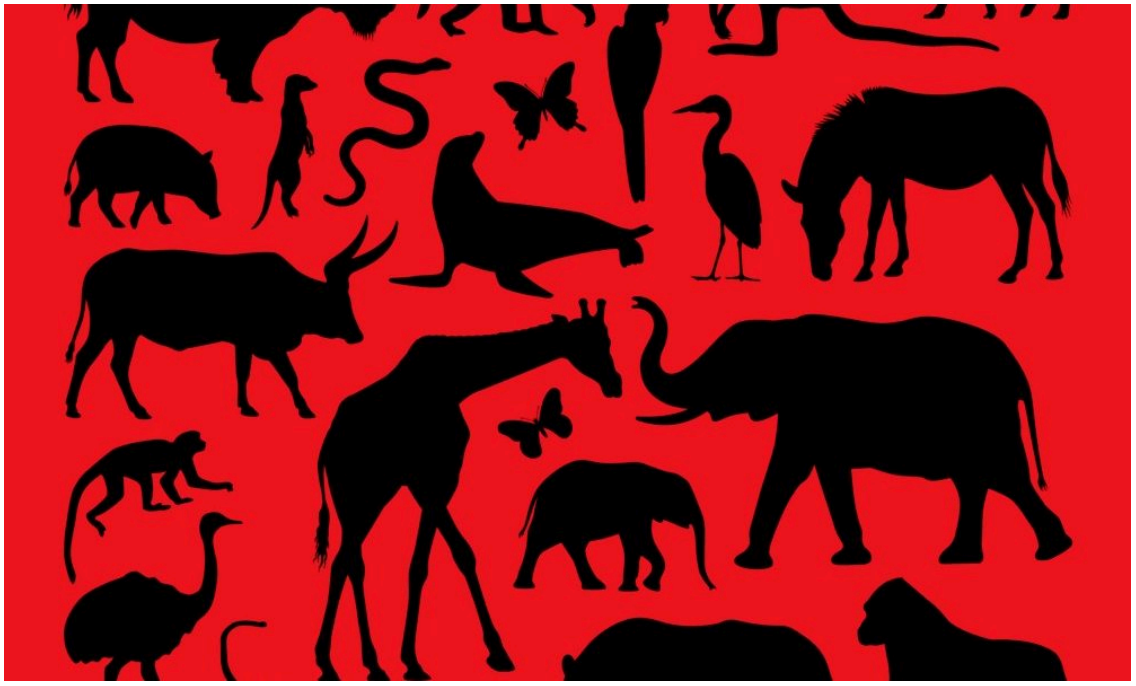
APT reports

APT reports

03 May 2018

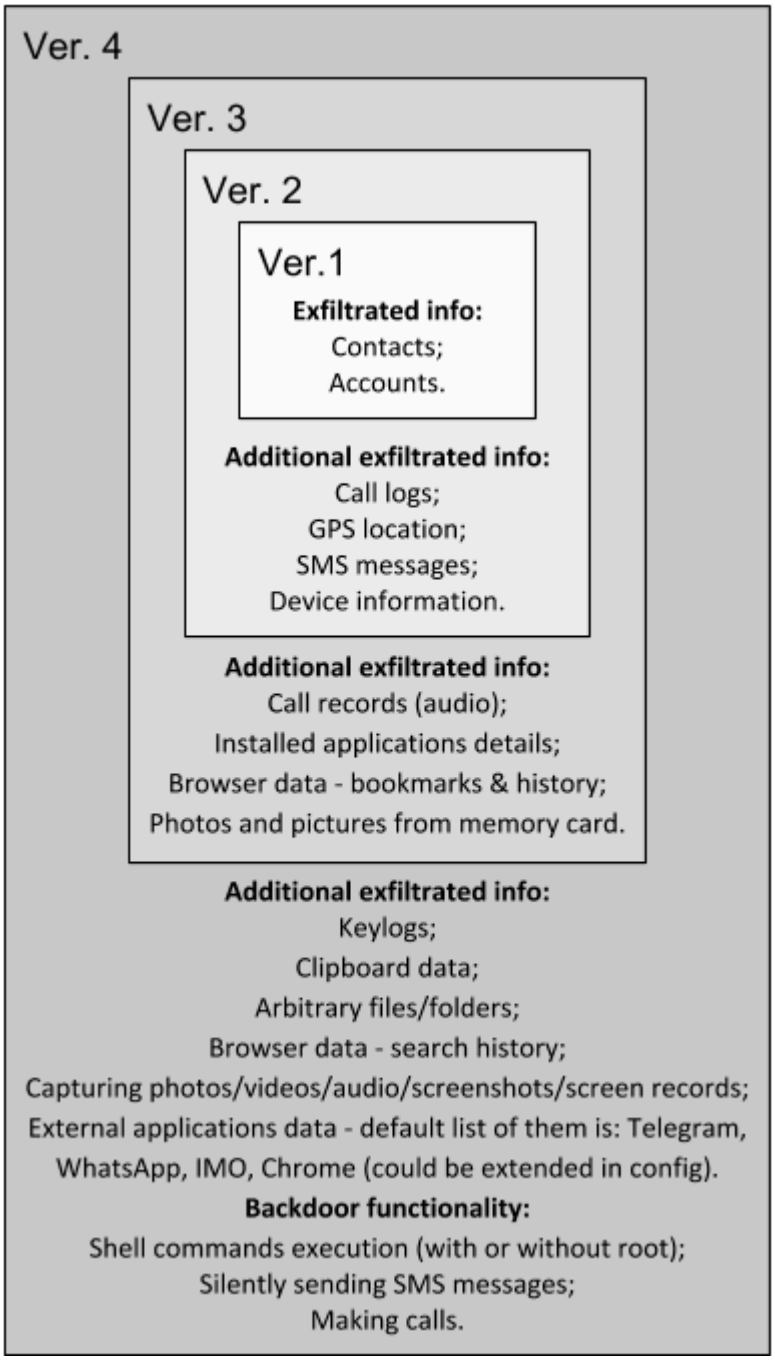
1 minute read

- Expert Alexey Firsh



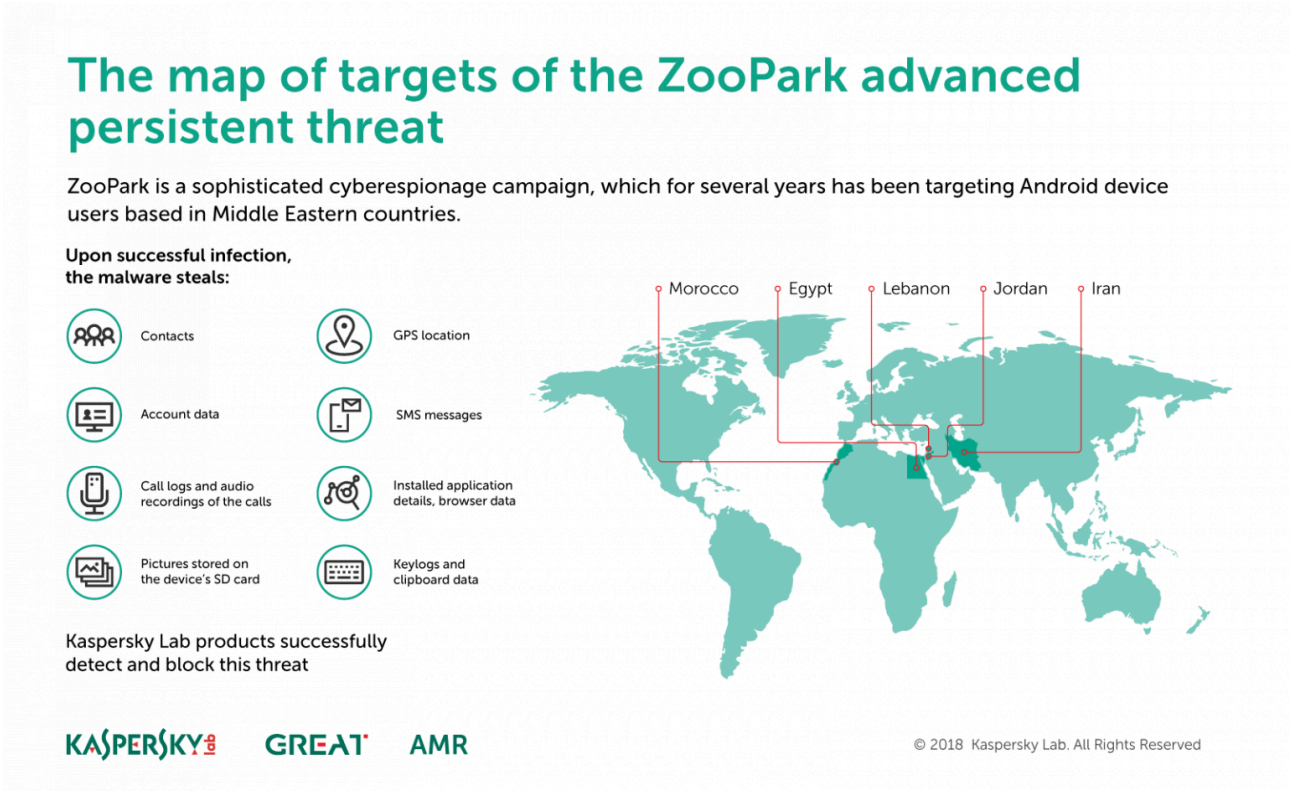
Cyberespionage operation targets Android users in the Middle East

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.



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.

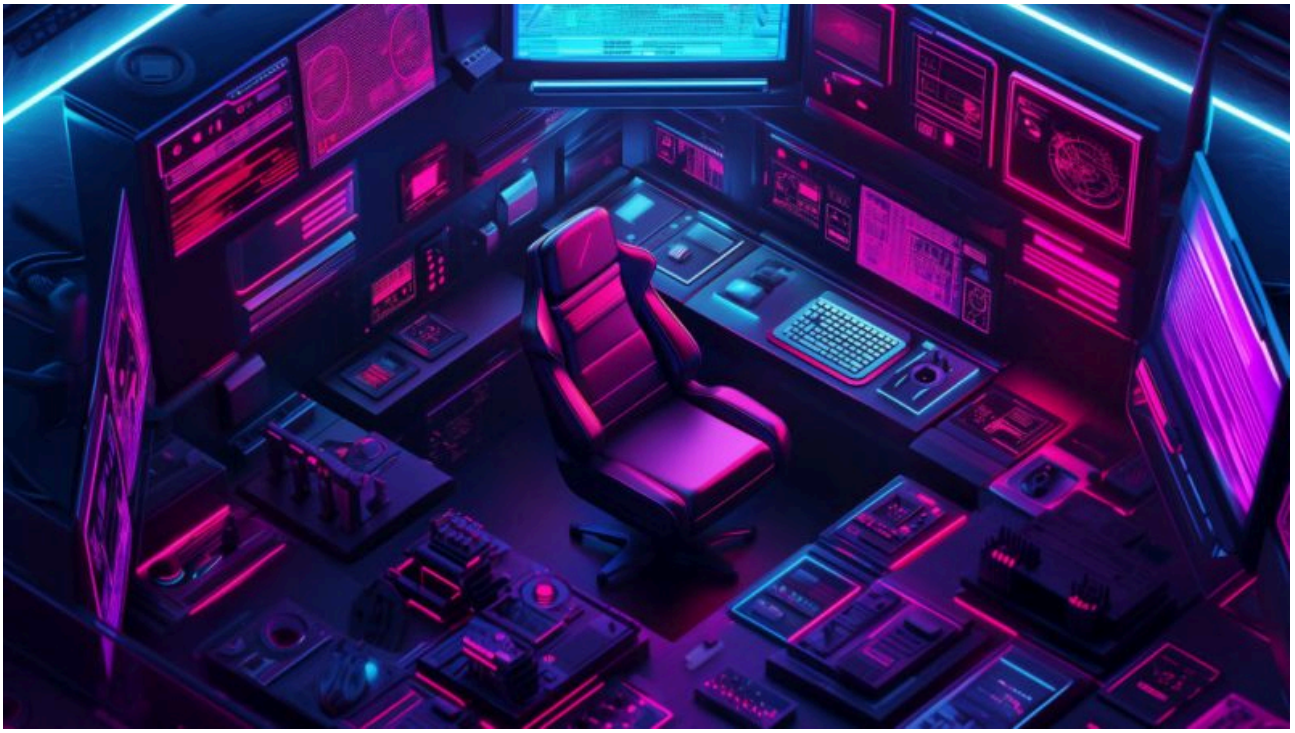


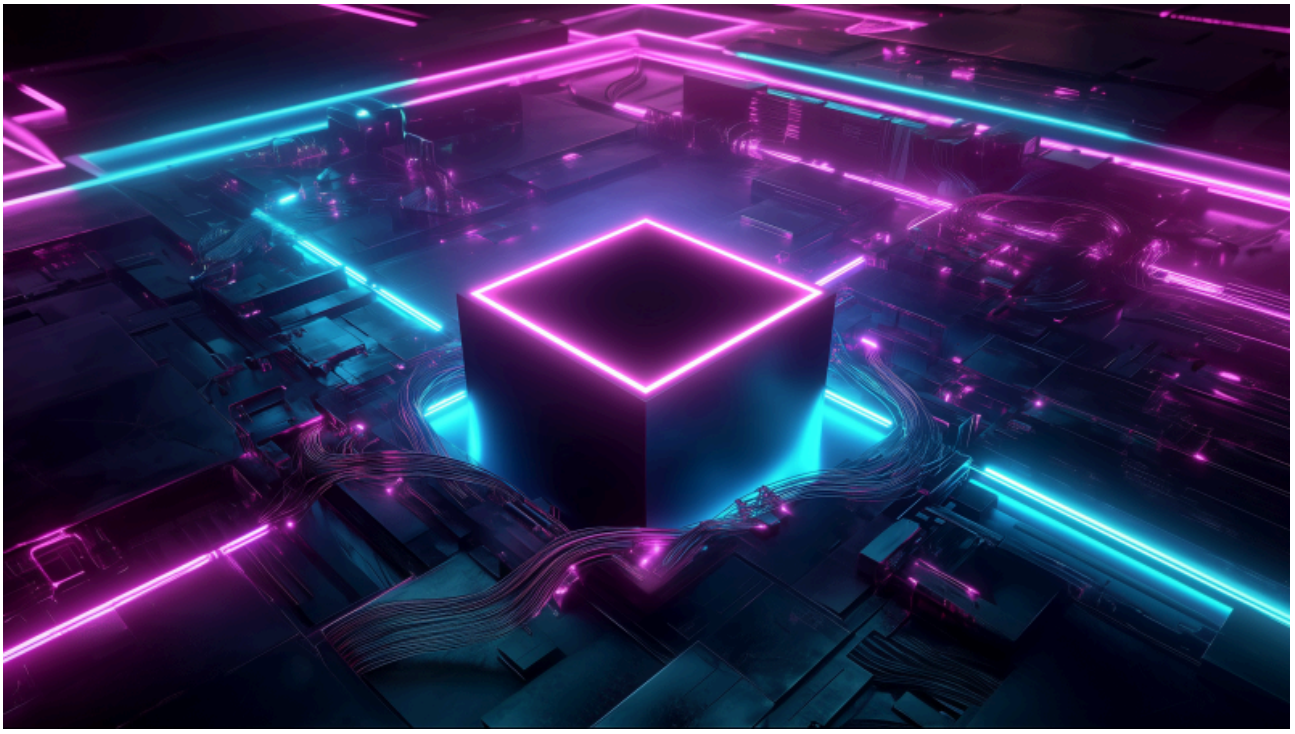
Target profile has evolved during the last years of campaign, focusing on victims in Egypt, Jordan, Morocco, Lebanon and Iran.

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.

Read the full "Who's who in the Zoo. Cyberespionage operation targets Android users in the Middle East." report

Latest Webinars





Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.
