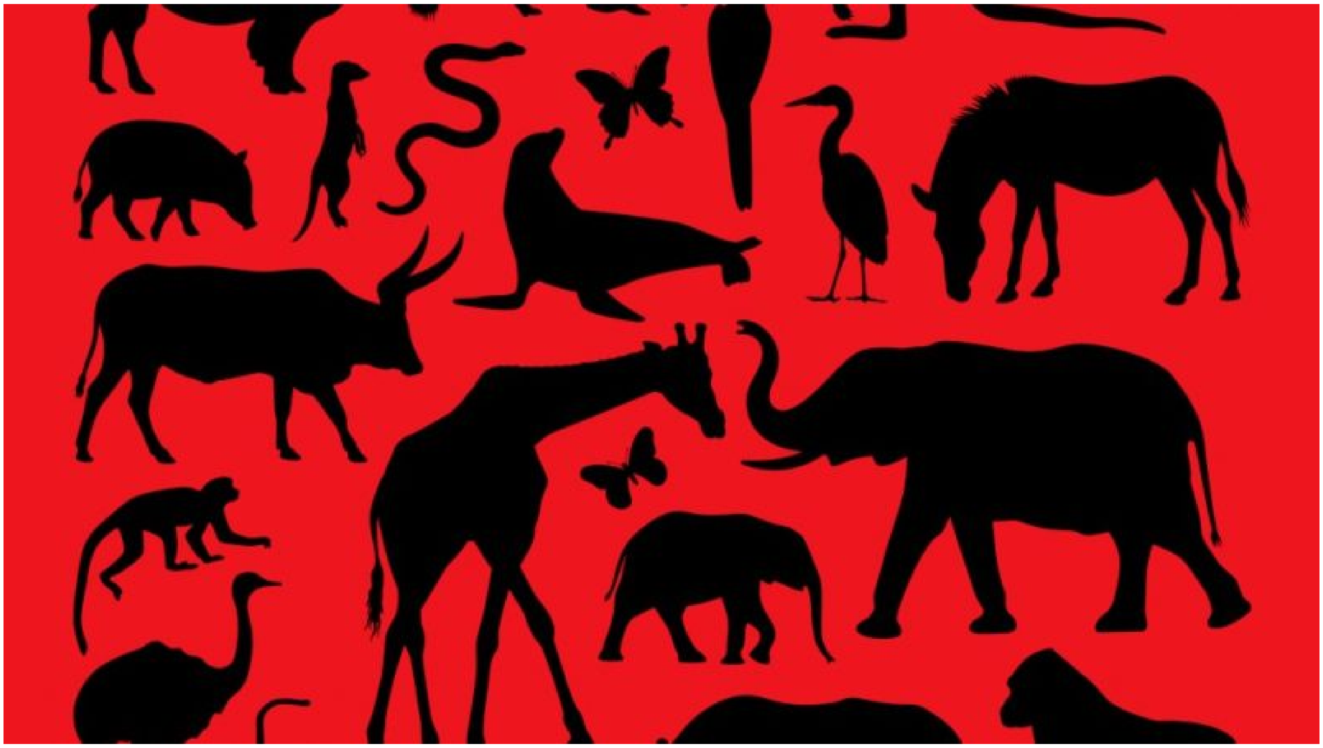
Who’s who in the Zoo

SL securelist.com/whos-who-in-the-zoo/85394

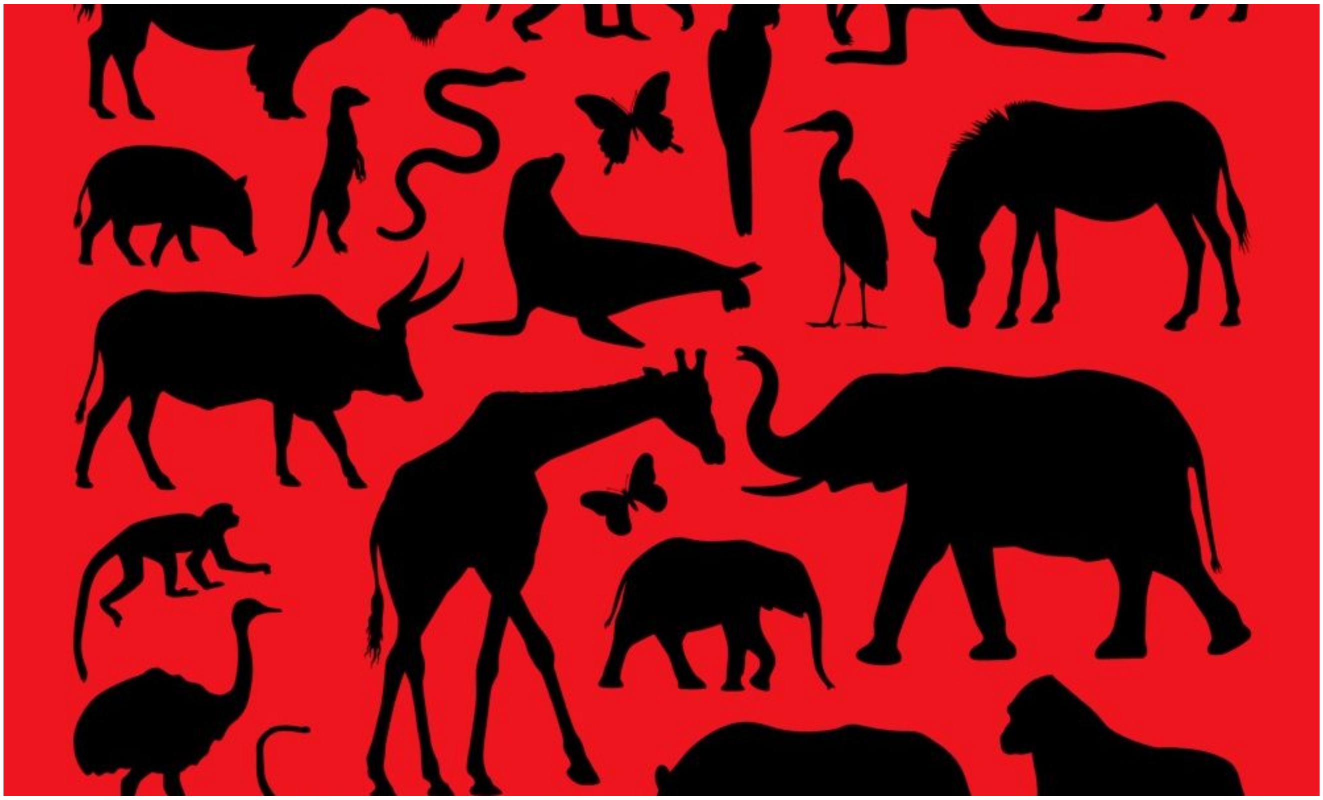


APT reports

APT reports

03 May 2018

minute read

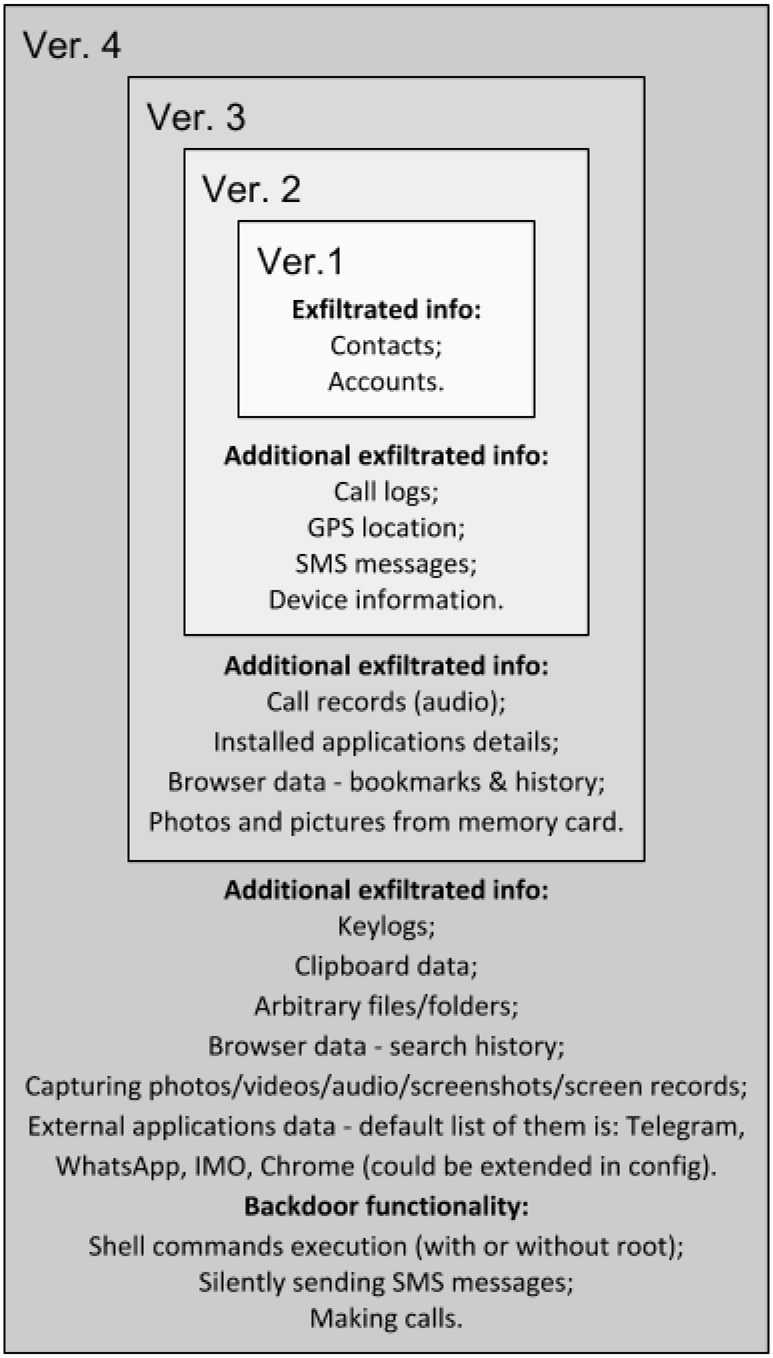


Authors

Expert Alexey Firsh

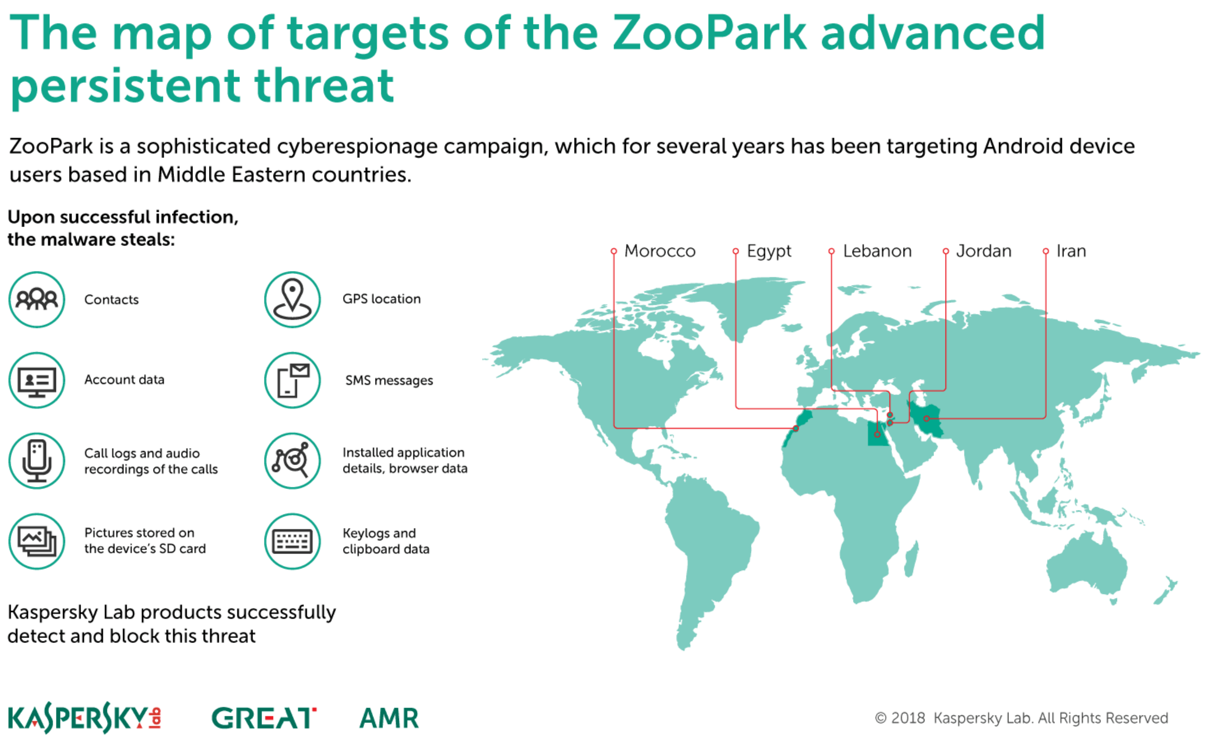
Cyberespionage operation targets Android users in the Middle East

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.


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:

- Contacts
- Account data
- Call logs and audio recordings of the calls
- Pictures stored on the device's SD card
- GPS location
- SMS messages
- Installed application details, browser data
- Keylogs and clipboard data

Kaspersky Lab products successfully detect and block this threat

© 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.

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

- APT
- Backdoor
- Cyber espionage
- Google Android
- Malware Descriptions
- Watering hole attacks

Authors

Alexey Firsh

Who’s who in the Zoo

Your email address will not be published.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

GReAT webinars

13 May 2021, 1:00pm

GReAT Ideas. Balalaika Edition

26 Feb 2021, 12:00pm
17 Jun 2020, 1:00pm
26 Aug 2020, 2:00pm
22 Jul 2020, 2:00pm
From the same authors

Hiding in plain sight: PhantomLance walks into a market

iOS exploit chain deploys LightSpy feature-rich malware

Beware of stalkerware

BusyGasper – the unfriendly spy

Zero-day vulnerability in Telegram

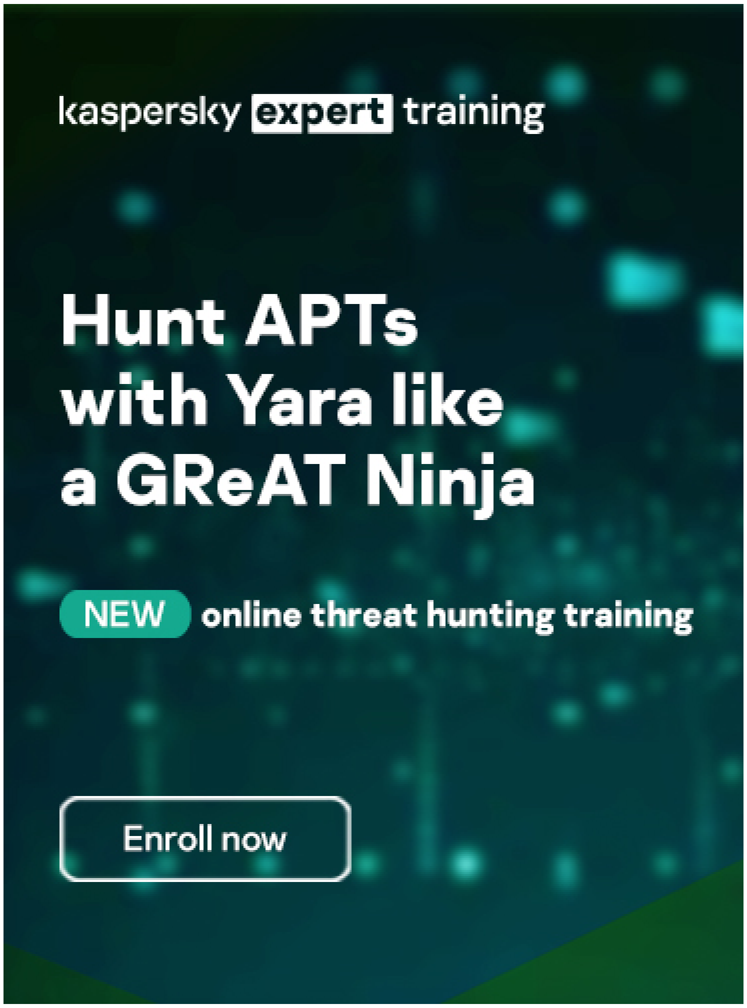
Subscribe to our weekly e-mails

The hottest research right in your inbox

-

-
-

-


kaspersky expert training
Hunt APTs with Yara like a GReAT Ninja
NEW online threat hunting training
Enroll now

Reports

APT trends report Q1 2022

This is our latest summary of advanced persistent threat (APT) activity, focusing on events that we observed during Q1 2022.

Lazarus Trojanized DeFi app for delivering malware

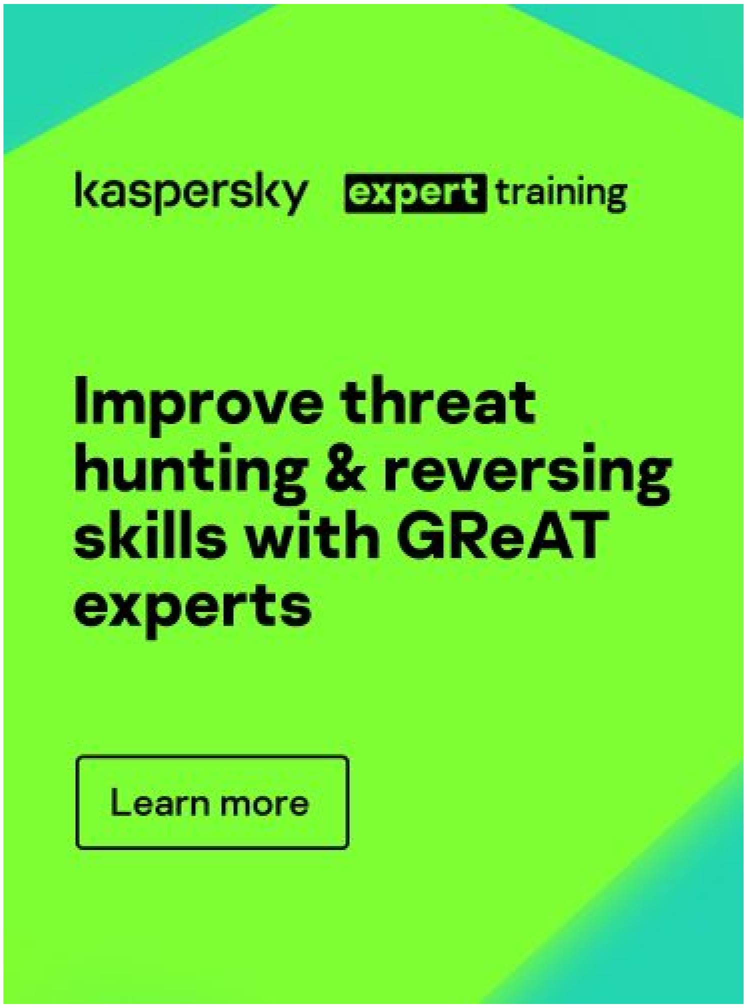
We recently discovered a Trojanized DeFi application that was compiled in November 2021. This application contains a legitimate program called DeFi Wallet that saves and manages a cryptocurrency wallet, but also implants a full-featured backdoor.

MoonBounce: the dark side of UEFI firmware

At the end of 2021, we inspected UEFI firmware that was tampered with to embed a malicious code we dub MoonBounce. In this report we describe how the MoonBounce implant works and how it is connected to APT41.

The BlueNoroff cryptocurrency hunt is still on

It appears that BlueNoroff shifted focus from hitting banks and SWIFT-connected servers to solely cryptocurrency businesses as the main source of the group’s illegal income.


kaspersky
expert training
Improve threat hunting & reversing skills with GReAT experts
Learn more

Subscribe to our weekly e-mails

The hottest research right in your inbox

-
-
-