**Final Project**

**and**

**Report**

**The Android Cyberespionage Campaign: ZooPark**

**Prepared by Ramy Attia**

**UID: U31434879**

Table of Contents

[Abstract 3](#_Toc449870271)

[Scenario Introduction 3](#_Toc449870272)

[Threat Actor 3](#_Toc449870273)

[Target 3](#_Toc449870274)

[Campaign 4](#_Toc449870275)

[The Exploit 4](#_Toc449870276)

[Versions of The Malware.....................................................................................……………………….5](#_Toc449870282)

[Stages of the Attack 9](#_Toc449870277)

[Reconnaissance 9](#_Toc449870278)

[Weaponizing 9](#_Toc449870279)

[Delivery 9](#_Toc449870280)

[Exploit 9](#_Toc449870281)

[Install 10](#_Toc449870284)

[Command and Control 11](#_Toc449870285)

[Actions on Objectives 12](#_Toc449870286)

[Incident Handling Process 13](#_Toc449870287)

Soltra/Edge Representation………………………………………………………………………………..14

STIX Presentation of The Campaign……………………………………………………………………15

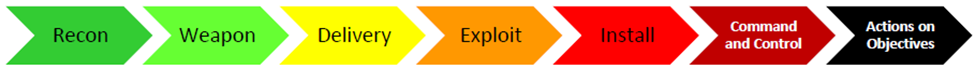
[Lessons Learned Phase 16](#_Toc449870290)

[Exploit References 17](#_Toc449870291)

[References 17](#_Toc449870292)

# Abstract

This report provides an in-depth analysis of the ZooPark cyberespionage campaign, a sophisticated series of incidents targeting Android users in the Middle East since 2015. It identifies ZooPark as a major threat player and links it to various campaigns aimed at exploiting specific targets, in particular Iran, Jordan, Lebanon, Egypt and Morocco. It focuses on the tactics, techniques and procedures (TTPs) used by ZooPark, including the distribution of malware through deceptive apps and exploiting Android system vulnerabilities. These campaigns are characterized by a methodical approach to compromise devices and data protection. The main indicators of compromise and observables, such as malware signatures and suspicious network activities, are highlighted in order to outline the attack patterns. The report concludes with recommendations for action, which include strategic countermeasures and defensive tactics to mitigate the impact of such cyber threats. The aim of this comprehensive overview is to provide actionable intelligence and to enhance the understanding of ZooPark operations and their broader cybersecurity implications. document the phases of the attack will be broken down using the DHS “Kill Chain”, which is represented below:



# Scenario Introduction

In this section, we outline the key actors involved in the ZooPark cyberespionage campaign and categorize them into their respective roles using STIX (Structured Threat Information eXpression) attributes for clarity and organization.

Threat Actor

The ZooPark group, a sophisticated threat actor known for its cyberespionage activities, targeted Android operating systems in the Middle East. This group, identified by cybersecurity researchers, demonstrated advanced technical skills with a specific focus on infiltrating mobile devices to gather sensitive information for espionage purposes.

Target

The ZooPark campaign's primary targets were Android mobile devices within the Middle East. The affected devices were commonly used by government officials, activists, and other individuals who were of interest to the threat actor. The campaign exploited various Android vulnerabilities to gain access to sensitive data.

Campaign

The ZooPark group conducted operations by exploiting publicly known vulnerabilities within the Android operating system, often employing social engineering tactics to distribute malware-laced applications. The group managed to establish a foothold within the networks of targeted individuals and organizations. They utilized crafted network packets to exploit SQL servers, which facilitated further penetration into the networks and allowed for command and control activities. The group's activities resulted in the successful exfiltration of data and surveillance of the victims' activities, showcasing their ability to conduct sophisticated and targeted cyber espionage operations.

The Exploit

In ZooPark's cyberespionage campaign, exploitation was crucial for obtaining unauthorized access to the victims' devices. ZooPark exploited several attack vectors to exploit vulnerabilities in the Android operating system.

Malware Distribution: This group ingeniously crafted malware to appear as legitimate applications. These applications were then distributed through various channels, such as phishing emails, messaging apps, and compromised websites that were frequented by the target demographic.

Vulnerability Exploitation: The group exploited known vulnerabilities in the Android system, which were either unpatched or unknown to the users, exploited these security gaps to infiltrate the device systems.

Elevation of Privilege: After successful exploitation, the malware attempts to increase the privilege level of the Android operating system. This enabled the ZooPark malware to gain unlimited access, allowing it to bypass security mechanisms and achieve persistence.

Data Exfiltration Methods: With this exploit, the malware activated various modules designed to exfiltrate sensitive information. These modules were able to control keylogging, access SMS messages, call logs, and files stored on the device.

Remote Control and Surveillance: This exploit also allowed attackers to remotely control devices and initiate surveillance actions, such as recording audio, taking pictures, or capturing content on the screen, effectively turning the infected mobile device into a surveillance tool.

Stealth and Persistence: The ZooPark malware was designed to operate stealthily so as not to be detected by both users and security software. Techniques have been used to ensure persistence on the devices, keeping the malware active even after rebooting the device.

These exploitation tactics highlight the technical skill of the ZooPark group and their determination to maintain access to valuable information over a long period of time.

# Versions of the Malware

The ZooPark campaign is notable for its evolution through at least four different versions of its malware, and every iteration has refined and expanded its capabilities for espionage and data extraction. Here's an overview of the differences among the versions:

Version 1:

It is likely that the original version served as a proof of concept or testing ground. It had a basic functionality for data extraction and could also include simple surveillance capabilities. The main aim would be to determine the ability of the malware to infiltrate and communicate with the command and control server.

A screenshot of a computer

Description automatically generated

Version 2:

On the basis of the original framework, Version 2 would have introduced more sophisticated surveillance features. It could improve data extraction capabilities, better evasion techniques for hiding from antivirus software, and, if necessary, the initial steps towards remote control.

A document with text and numbers

Description automatically generated

Version 3:

This version has achieved significant improvements, especially in terms of stealth and persistence. It could include the use of encryption for communication, advanced modules for data collection, and additional functions for remote surveillance, such as the activation of cameras and microphones without user knowledge.

A screenshot of a computer program

Description automatically generated

Version 4:

In the most advanced version, all previous features would be refined and more complex capabilities added. This may include self-updating mechanisms, the ability to spread laterally across networks, advanced data harvesting techniques and, where appropriate, the use of zero-day vulnerabilities for more effective use.

Each version of the ZooPark malware was more sophisticated than the previous one, demonstrating the increasing expertise of the threat actor and the evolving threat landscape. The differences between versions highlight a strategic development approach aimed at increasing the effectiveness of the malware and avoiding detection, thus ensuring the longevity of the ZooPark campaign.

A close-up of a word

Description automatically generated

A screenshot of a computer code

Description automatically generated

# 

# Stages of the Attack

## Reconnaissance

## In the first stage, the ZooPark group was engaged in extensive intelligence gathering. They found vulnerabilities in the Android operating system and identified potential victims, focusing on the selection of effective attack vectors. It is likely that this reconnaissance involved researching security weaknesses, understanding the habits of potential targets, and evaluating the network defenses of the environments they intended to infiltrate.

## Weaponizing

At this point, the threat actors have developed or modified malware tools specifically designed to exploit the identified vulnerabilities in Android devices. This malware has been meticulously designed to be stealthy and multifunctional, capable of conducting surveillance and extracting data without detection by users or security systems.

## 

## Delivery

In the delivery stage, the weaponized malware was deployed to the intended target. The ZooPark group has used a number of methods, including spear-phishing campaigns, social engineering, and compromising legitimate applications by embedding malicious code into them.

## Exploit

As soon as the malware reaches its target, it activates and exploits the vulnerabilities of the devices to execute its malicious payload. This decisive step allowed attackers to obtain the first access to the devices and, in many cases, increase their privileges within the system.

## Install

The installation phase of the ZooPark malware leveraged two primary distribution vectors, each exploiting the trust and habits of the target audience:

A screenshot of a phone

Description automatically generated

* The ZooPark group has created a malicious application that pretends to be a legitimate application to vote in the Iranian Kurdistan province. They used Telegram channels, a popular social media platform, to distribute the app. The application has been advertised as a tool for downloading election software with online statistics that can be accessed through a specified channel. By exploiting a politically active user base and the popularity of Telegram in the region, the attackers successfully forced users to download and install the malicious application.

A screenshot of a computer

Description automatically generated

* In addition, the attackers used a watering hole technique where they compromised legitimate websites frequented by the target audience. In the present case, the malware was used on popular news sites such as Al-Nahar, which is highly ranked in Egypt. The website was used as a platform for discreet distribution of malware when users visited pages, such as pages detailing the dollar exchange rate on the black market. Visitors to these compromised pages were at risk of installing version 3 of the malware silently on their devices.

A screenshot of a computer

Description automatically generated

Al-Nahar Website

* These sophisticated distribution methods facilitated the installation of the malware on a large number of devices, thus advancing the espionage objectives of the ZooPark. They highlight the strategic approach of the attackers in selecting distribution channels that are likely to achieve a high concentration of the intended targets.

## Command and Control

When the malware was fully installed, the compromised devices established communication with the command and control server. This allowed for two-way communication: the infected devices could receive further instructions from ZooPark operators and start exfiltrating the data collected. This remote control aspect is crucial to the ongoing espionage and data collection efforts.

## Actions on Objectives

The Actions on Objectives phase is the culmination of the cyber-kill chain, in which the threat actor executes the prepared actions. For the ZooPark campaign, this phase was characterized by a series of sophisticated actions across different versions of malware:

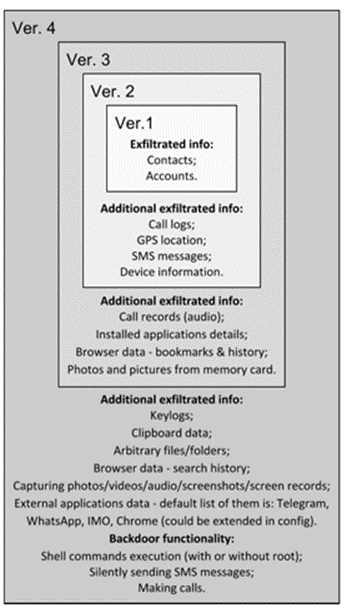
The first and second iterations of ZooPark are likely to focus on establishing a foothold within the target devices and beginning the data harvesting process. These versions would allow the collection of basic user data, such as contacts and text messages.

In the third version of ZooPark, more advanced surveillance capabilities have been added. This version was able to record audio, take photographs, or even capture video, making the compromised devices a real spy tool. The malware can now carry out one of its main objectives: to monitor the activities of the target persons and gather information.

The fourth version represents the peak of the campaign's capabilities. In this version, ZooPark can carry out full-scale espionage activities. It's probably equipped with keyloggers, the ability to intercept calls, and advanced data extraction methods. This version would allow the threat actors not only to collect a wide range of data but also to monitor the communication of the device in real time.

Throughout its versions, ZooPark's objectives focused on espionage—gathering as much information as possible from the victims for intelligence or leverage purposes. The gradual increase in the sophistication of the malware versions shows that the threat actors have learned from each stage, refined their techniques, and expanded their capabilities to achieve their objectives more effectively.

The image below shows the capabilities of each version:



# Incident Handling Process

**Identification Phase**

As regards the ZooPark campaign, the identification phase is essential. Network administrators must be vigilant for signs of compromise, such as unusual network traffic, which may indicate malware communication with command and control servers, or unexpected data flows indicating exfiltration activities. The devices affected by ZooPark may also have performance problems, such as slowdowns or rapid battery depletion, because the malware is often resource-intensive. In addition, the presence of new or altered applications that behave suspiciously should raise red flags. These apps may require extensive permissions that are not necessary for their function and serve as a front for malicious operations. Security solutions, such as IDS and antivirus programs, may provide alerts on detected activities related to known ZooPark IoCs, which require immediate investigation.

**Eradication and Recovery Phases**

After confirmation of ZooPark infection, the eradication and recovery phase starts. This includes the application of the latest security patches to all devices in order to avoid exploiting known vulnerabilities. Isolating affected systems is a crucial first step in halting the spread of the malware and any data breaches that continue. Malicious applications linked to ZooPark must be identified and removed. In the event of a credential breach, a complete reset of passwords and authentication tokens is required. The network traffic should be closely monitored to detect unusual outgoing connections or data flows that could indicate continued malware activity or secondary infections. Restoring the affected systems from clean and verified backups can help to eliminate all malware traces. In addition, security configurations should be reviewed and strengthened, unnecessary services should be disabled and strict access control measures should be implemented. Finally, it is necessary to educate users about the risks of phishing and malicious downloads in order to prevent reinfection and strengthen the organization's first line of defense against such sophisticated threats. These structured phases of identification, eradication, and recovery can effectively manage and mitigate the impact of the ZooPark campaign. This is evidence of the need for a proactive and informed approach to cybersecurity in the face of evolving digital threats.

# Soltra/Edge Representation

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

# STIX Presentation of The Campaign

A computer screen shot of a network

Description automatically generated

## Lessons Learned Phase

In the aftermath of the ZooPark cyberattack, the lessons learned phase plays a crucial role in strengthening future defenses and response strategies. This phase involves a thorough review of the incident, identifying the success factors of the attack, the effectiveness of the organization's response, and identifying any procedural weaknesses. These insights should lead to concrete improvements in security, such as enhanced monitoring systems, updated incident response plans, and advanced user training programmes to mitigate the risk of social engineering attacks. In addition, these lessons can inform the development of more stringent access controls and network segmentation to prevent similar threats.

The sharing of the knowledge and experience gained from this incident with the wider cybersecurity community is also invaluable and contributes to a common defence mechanism. By understanding the nuances of the ZooPark attack and applying these lessons, organizations will be able to strengthen their resilience against such complex threats. The iterative process of learning and adapting is crucial because cyber threats are constantly evolving and require a dynamic and proactive approach to cybersecurity.

# Exploit References

* CVE-2019-2215
* CVE-2016-5195 (Dirty COW)
* CVE-2014-3153 (Towelroot)
* Webview Vulnerabilities

# References

1. Kaspersky Lab. "Who’s Who in the Zoo: Cyberespionage Operation Targets Android Users in the Middle East." Kaspersky Lab, May 2018.
2. MITRE. "CVE-2019-2215, CVE-2016-5195, CVE-2014-3153 " *MITRE Corporation*, 2019. Web.

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2215>.

1. Chin, Erika, and David Wagner. "Bifocals: Analyzing WebView Vulnerabilities in Android Applications." *Information Security Applications*, 2014, SpringerLink, <https://link.springer.com/chapter/10.1007/978-3-319-05149-9_9>.