

Security   Malware

# Predator Spyware Using Zero-day to Target Android Devices



BY DEEBA AHMED · MAY23, 2022 · ⌚ 2 MINUTE READ



**Spyware developer firm Cytrox is under Google's radar for developing exploits against five 0-day flaws in Android and Chrome.**

---

^target Android users with spyware.

According to the details shared by TAG, threat actors are using the infamous Predator spyware in three different campaigns. Predator was previously analyzed in a report from the University of Toronto's [Citizen Lab](#).

## 0-days used with n-days to Deploy Spyware

The exploits are developed for four Chrome 0-days and one Android 0-day flaw. In their [blog post](#), TAG researchers Clement Lecigne and Christian Resell explained that the 0-days are used in conjunction with n-day exploits.

Moreover, the attackers are trying to benefit from the time difference between the patching of some critical bugs, which weren't declared severe security issues, and "when these patches were fully deployed across the Android ecosystem."

## Spyware Details

According to Google, the North Macedonian-based commercial surveillance firm Cytrox has packaged and sold the exploits to different state-backed threat actors in Greece, Egypt, Serbia, Madagascar, Indonesia, Spain, Côte d'Ivoire, and Armenia.



	\$4,600	\$6,400	
	\$3,150	\$7,500	

It is alleged that the buyers have used these bugs in at least three campaigns so far. The Predator spyware is similar to [NSO Group's Pegasus spyware](#), allowing threat actors to penetrate Android and iOS devices.

## About the Three Campaigns using Predator

TAG examined three campaigns and concluded that attackers send one-time URLs to Android users through spear-phishing emails. These links are shortened using a common use URL shortener while the attackers target only a handful of victims. When users click on this malicious URL, they are redirected to a malicious webpage that automatically deploys the exploits and redirects them to a legitimate website.

Once there, the attackers deploy Alien Android malware that loads Cytrox's Predator. In case the shortened link doesn't work, the victim is directly taken to the legit website.

## List of Exploits

- 
- × CVE-2021-37975
  - × CVE-2021-37976
  - × CVE-2021-38000
  - × CVE-2021-38003



The primary aim of attackers behind this operation is distributing Alien malware that is a precursor for deploying Predator spyware onto infected devices. It receives commands from Predator through an IPC (inter-process communication) mechanism and can record audio, hide apps, and add CA certificates to evade detection.

The first campaign was launched in August last year on Google Chrome, targeting the Samsung Galaxy S21 device. One month later, the second campaign targeted an updated Samsung Galaxy S10, while the third was detected in October 2021.

## More Android Spyware News

---

1 [New Android malware Predator found stealing data, intercepting SMS](#)

5 [New Russian Android Malware Tracks GPS Location and Spies on Victims](#)



Android

Chrome

Cytrox

Malware

Predator

security

Spyware

---

Author

**DEEBA AHMED**





## SUBSCRIPTION FORM

Enter your name

Enter your email

Subscribe >

☐

By checking this box, you confirm that you have read and are agreeing to our terms of use regarding the storage of the data submitted through this form.



**IPVanish** ✓ Super secure VPN

★ 9.6/10

✓ Minimal data logging

✓ Favorable privacy policy

Visit IPVanish ►

## RECENT POSTS

**Predator Spyware Using Zero-day to Target Android Devices**

**5 Casual Games You Can Play on Your Mobile Browser Now**

**A Short Guide to Understanding the Exciting Realm of Fintech**

**Avoiding Risks by Using Secure Online Crypto Platform**



**Malware, Microsoft, Security**

## **Windows Registry now Providing Shelter to Destructive Kovter Malware**

BY **WAQAS** · SEPTEMBER 30, 2015



**Security, How To**

## **How Your Smartphone Can Be Used to Steal Your Data**

BY OWAIS SULTAN · FEBRUARY 8, 2022

**Android, Apple, Security, Technology**

## **iPhone Encryption Debate Lingers On – Google Extends Support to Apple**

BY CAROLINA · FEBRUARY 18, 2016





**Cyber Crime, Hacking News, Security**

## **Hell is back with Hell Reloaded on the Dark Web**

BY **ALI RAZA** · JANUARY 5, 2016

### **Sign Up for Our Newsletter**

Don't worry we will never spam.

Enter your email

Subscribe >



HACKREAD is a News Platform that centers on InfoSec, Cyber Crime, Privacy, Surveillance and Hacking News with full-scale reviews on Social Media Platforms & Technology trends. Founded in 2011, HackRead is based in the United Kingdom.

Copyright © 2022 HackRead

[Home](#) [Advertise](#) [Privacy Policy](#) [Contact Us](#)

Hackread.com is among the registered trademarks of Gray Dot Media Group Ltd. Company registration number 12903776 in regulation with the United Kingdom Companies House. The registered address is 85 Great Portland Street, London, England, W1W 7LT The display of third-party trademarks and trade names on the site do not necessarily indicate any affiliation or endorsement of Hackread.com. If you click an affiliate link and buy a product or service, we may be paid a fee by that merchant.

