

# OmniRAT Takes Over Android Devices Through Social Engineering Tricks

 [securityintelligence.com/news/omnirat-takes-over-android-devices-through-social-engineering-tricks/](https://securityintelligence.com/news/omnirat-takes-over-android-devices-through-social-engineering-tricks/)



[Home](#)&nbsp;/

OmniRAT Takes Over Android Devices Through Social Engineering Tricks



November 6, 2015

By [Shane Schick](#) 2 min read

Remote administration tools can be hugely helpful to the increasingly mobile workforce, but malware analysts say a product called OmniRAT has turned into a highly effective means of stealing data.

The research team at [Avast](#) provided details of security incidents involving OmniRAT, which is made in Germany and not necessarily intended for cybercriminal activity. In at least one case, however, victims were fooled into thinking the Android Stagefright vulnerability was preventing them from receiving an MMS and they needed to click on a bit.ly link to get it. They would then enter a code based on a malicious SMS that gives cybercriminals control over an Android device. This meant cybercriminals were also able to more easily distribute malware by accessing users' contact lists.

Unfortunately, remote administration tools have a history of being hijacked for nefarious purposes. Before OmniRAT, there was DroidJack, [SecurityWeek](#) pointed out, which was also co-opted by India-based cybercriminals to take over Android devices. The malicious use of DroidJack is still under investigation by European law enforcement authorities.

What may make OmniRat even more attractive to cybercriminals is its price tag. For a mere \$25, they have access to a tool that can be paired with fairly straightforward social engineering techniques to target mobile users. This compares with \$210 for DroidJack on the black market, [TechWorm](#) reported. Besides stealing data, the tool could also be used to probe browser histories and record conversations, so the potential for damage, particularly among smartphone users conducting business remotely, is huge.

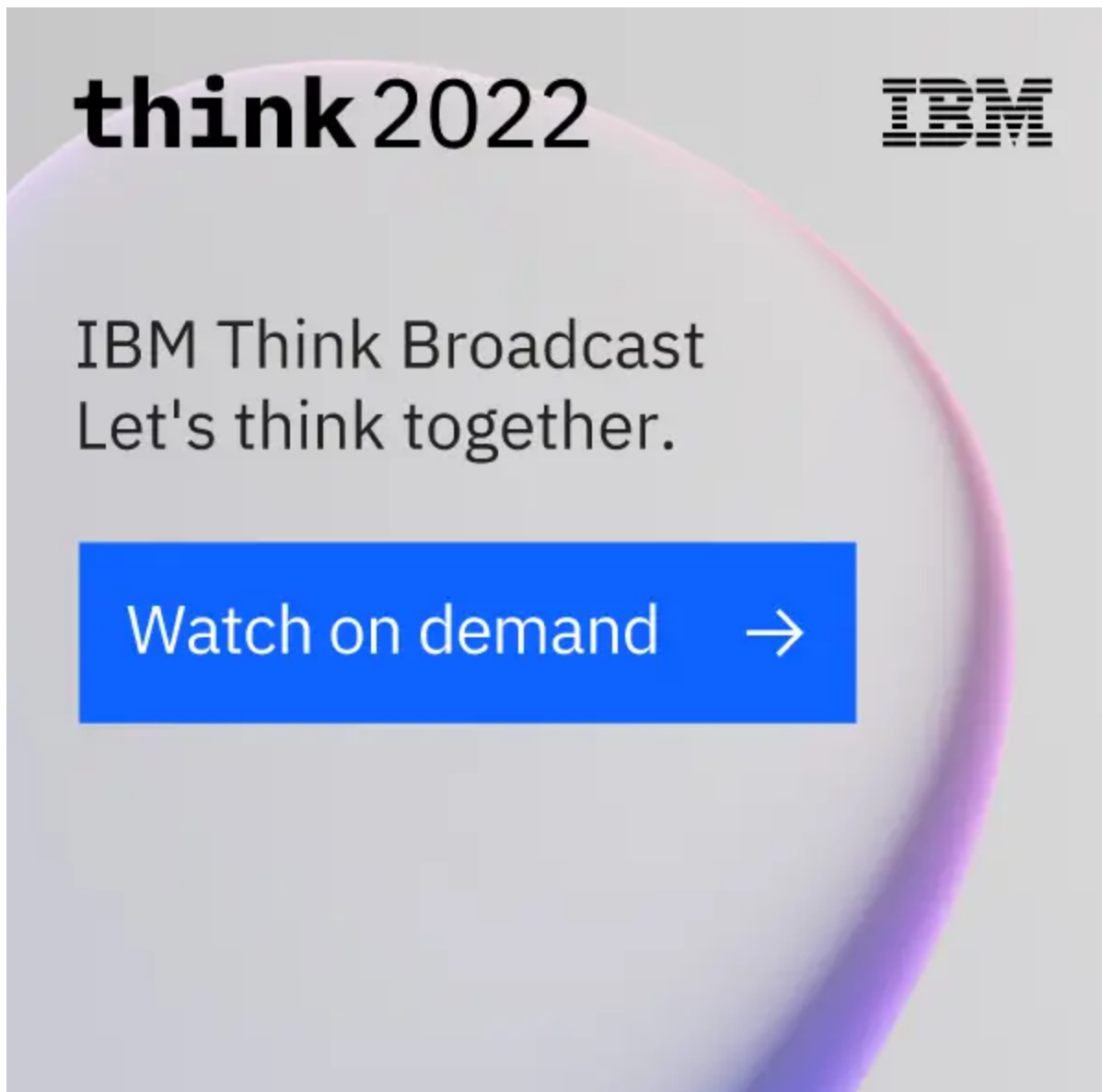
The misuse of software like OmniRAT has gotten so bad that they've begun to be called remote-access Trojans, according to [Softpedia](#). On the other hand, it's difficult if not impossible to outlaw remote administration tools entirely because they can also be put to good use. For example, they can be used for testing or as a tool for staff developers.

You're safe from something like OmniRAT if you ignore an [SMS that comes from attackers](#). If you're a CISO or part of an IT security team, it would also help to educate or remind staff to make sure they aren't too quick to bypass permissions popups that could prevent cybercriminals from taking the next step and controlling their devices.

[Android](#) | [Android Security](#) | [Android Vulnerability](#) | [Cybercrime](#) | [Data Security](#) | [Malware](#) | [Remote-Access Trojan \(RAT\)](#) | [Social Engineering](#)

[Shane Schick](#)  
Writer & Editor

Shane Schick is a contributor for SecurityIntelligence.

The image is a promotional graphic for the IBM Think 2022 broadcast. It features a light gray background with a large, stylized, curved shape in shades of purple and pink on the right side. In the top left, the text "think 2022" is written in a bold, lowercase, sans-serif font. In the top right, the IBM logo is displayed in its characteristic eight-stripe font. Below the "think 2022" text, the words "IBM Think Broadcast" are written in a smaller, uppercase, sans-serif font, followed by the tagline "Let's think together." in a similar font. At the bottom, there is a prominent blue rectangular button with the white text "Watch on demand" and a white right-pointing arrow.



**more from**

---



[Intelligence & Analytics](#) May 26, 2022

## **Black Basta Besting Your Network?**

This post was written with contributions from Chris Caridi and Kat Weinberger. IBM Security X-Force has been tracking the activity of Black Basta, a new ransomware group that first appeared in April 2022. To date, this group has claimed attribution of 29 different victims across multiple industries using a double extortion strategy where the attackers [...]



[Application Security](#) May 26, 2022

## **Lessons Learned by 2022 Cyberattacks: X-Force Threat Intelligence Report**

---

Every year, the IBM Security X-Force team of cybersecurity experts mines billions of data points to reveal today's most urgent security statistics and trends. This year's X-Force Threat Intelligence Index 2022 digs into attack types, infection vectors, top threat actors, malware trends and industry-specific insights. This year, a new industry took the infamous top spot: [...]



News May 25, 2022

## **IBM Develops AI-Powered z16 to Help Thwart Quantum Cyberattacks**

---

On April 5, IBM unveiled IBM z16, the company's next-generation system with an integrated on-chip artificial intelligence (AI) accelerator to deliver latency-optimized inferencing. With this innovation, clients will be able to analyze real-time transactions at scale. IBM z16 is even more valuable for mission-critical workloads such as credit card, health care and financial transactions. Inference [...]



Identity & Access May 24, 2022

## **Cybersecurity Tips for a Safer Vacation**

---

The beauty of having different climates around the world is that there is always somewhere we can travel for leisure all year round. These are times when we tend to relax and let our guard down. The reality, though, is that cyber crime knows no vacation. Attackers are relentless and are always on the lookout [...]

Analysis and insights from hundreds of the brightest minds in the cybersecurity industry to help you prove compliance, grow business and stop threats.