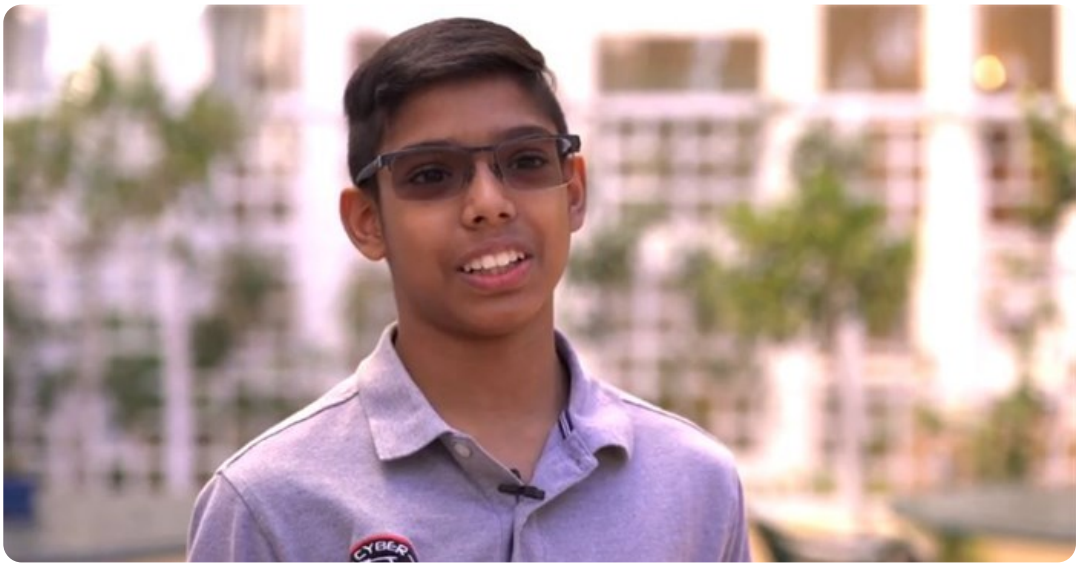
Teen hacks drone, warns of potential 'internet of threats'

Thirteen-year-old Reuben Paul, also known as 'Cyber Ninja', managed to hack into a drone duri Kaspersky Lab's annual Cyber Security Weekend 2019, exposing the gaping holes in the secur measures of millions of everyday gadgets and technology devices that are part of the internet c things (IoT).



Reuben Paul aka Cyber Ninja

Paul demonstrated that he could disconnect a user from his drone and then take complete control of it by exploiting its insecure protocols. The drone hack performed by the 13-year-old was a controlled stunt organised by Kaspersky Lab to highlight the urgent need for stricter measures from companies developin IoT-related devices such as drones, baby monitors, smart appliances, smart home devices, and connecte toys. Kaspersky Lab advises people to inquire about the security measures taken and to understand the associated risks before buying any connected device. While governments already have tight controls in place around devices such as drones, companies, on the other hand, still need to take the security aspect more seriously.

Invasion of privacy

“Many companies compete to get their connected products out to the market and the consumers at the fastest speed to start generating profit. But doing so often means they overlook the security features or ev completely ignore the security issues. Such devices can become lion’s meat for hackers and if they fall pr this could lead to invasion of privacy, loss of data, valuables and even life,” said Maher Yamout, senior security researcher in the global research and analysis team at Kaspersky Lab.

“It took me less than 10 minutes to hack the drone and I managed to take full control of it. The insecurities the drone are shared by other IoT devices. Now imagine if this had been done by cyber-criminals. If I can it, who’s not to say that more motivated cyber-criminals would not be able to do something very similar. Th consequences could be disastrous,” said Paul. “We need to reinvent cyber security because what we are doing so far is clearly not enough. It is important for manufacturers to implement security controls into thei devices and not put consumers at risk!” he added. Reuben ended by cautioning, “Let us be careful that th internet of things does not become the internet of threats.”

There are around seven billion internet connected devices in the world according to data from IoT analytic with the cyber security risk remaining phenomenal. The impacts of these hacks are seen already, with multiple IoT-related security incidents happening around the world. Kaspersky Lab experts therefore gathered to shed light on the consequences IoT threats as well as drone exploitation, whilst educating and raising awareness on potential dangers that could result due to such vulnerabilities.