Mysterious malware threatens millions of routers and IoT devices

Cybersecurity researchers at AT&T Alien Labs (USA) have discovered a new form of malware that can threaten millions of routers and IoT devices.

This mysterious malware called **BotenaGo** can use a number of methods to attack targets, then creates a 'backdoor' on the compromised devices.

Some anti-virus software detects this new malware because it has the same original way of spreading data as the Mirai botnet virus, the virus that caused the majority of distributed denial-of-service (DDoS) attacks in 2016. .

BotenaGo is written in Go, a programming language popular with software developers and malware authors in recent years.

First, BotenaGo will scan the internet for vulnerable targets. The malware then analyzes it to look for security holes.

Attackers can exploit security holes in internet-connected devices and can execute commands remotely to infiltrate the wider network, if they are not properly secured. Or bad guys can also use this option to spread malicious viruses.

Because BotenaGo appears to have been removed from a server hosted by the attackers, researchers are currently unable to analyze them.

According to the researchers, there are three possibilities for this mysterious malware.

1. BotenaGo is just one module of a larger malware suite, and it's not currently being used in attacks.

2. BotenaGo is likely linked to Mirai.
3. BotenaGo is still in development. For some reason its beta was accidentally released early. So it still doesn't work.

However, even if BotenaGo were to stay idle, the sheer number of vulnerabilities it could exploit would leave millions of devices potentially vulnerable.

Security experts warn that, as companies need to install security updates as soon as possible, IoT devices must have the appropriate firewall configuration installed to protect and not be widely exposed. with the internet.