Mphasis SOC – Information Security News
Date & Time Issued: 24-06-2024, 06:00 IST

Title	A Deep Dive into the Zergeca Botnet	
Summary	• Zergeca is a botnet implemented in Golang and supports six different attack methods, as well as proxying, scanning, self-upgrading, file transfer, reverse shell, and collecting sensitive device information.	
Severity	Medium	
Attack Vectors	• Upon analysis, it was confirmed that Zergeca is a botnet implemented in Golang. The botnet's name, Zergeca, is inspired by the swarming Zerg in StarCraft, reflecting its aggressive and expansive nature. Zergeca is not just a typical DDoS botnet; it supports six different attack methods and boasts additional capabilities such as proxying, scanning, self-upgrading, persistence, file transfer, reverse shell, and collecting sensitive device information. • From early to mid-June 2024, Zergecaprimarily targeted regions such as Canada, the United States, and Germany. The main type of attack was ackFlood (atk_4), with victims distributed across multiple countries and different Autonomous System Numbers (ASNs). The reverse analysis of Zergeca revealed that the botnet is designed for the x86-64 CPU architecture and targets the Linux platform. Zergeca achieves persistence on compromised devices by adding a system service named geomi.service. • This service ensures that the Zergeca sample automatically generates a new geomi process if the device restarts or the process is terminated. • After obtaining the C2 IP, the bot reports sensitive device information to the C2 and awaits commands, supporting six types of DDoS attacks, scanning, reverse shell, and other functions. The discovery of Zergeca highlights botnets' continuous evolution and increasing sophistication. • With its advanced scanning, persistence features, and multi-functional capabilities, Zergeca poses a significant cybersecurity threat.	
Indicator of Compromise	INDICATOR	INDICATORS
	TYPE	
	Domain	• bot[.]hamsterrace[.]space
	File Hash	• 23ca4ab1518ff76f5037ea12f367a469 • d78d1c57fb6e818eb1b52417e262ce59 • 604397198f291fa5eb2c363f7c93c9bf • 6ac8958d3f542274596bd5206ae8fa96 • 980cad4be8bf20fea5c34c5195013200
	IP	• 84.54.51.82
Recommendations	• Understand Botnet Infiltration. • Restrict the access. • Use strong device authentication. • Install patches. **NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre -Prod or test environment before implementing. diligence and impact analysis.**	
References	• https://gbhackers.com/beware-of-zergeca-botnet/	