Mphasis
The Next Applied

## Mphasis SOC – Information Security News
## Date & Time Issued: 07-JUL-2024, 17:00 IST

| | | |
|---|---|---|
| Title | **New Golang-Based Zergeca Botnet Capable of Powerful DDoS Attacks** | |
| Summary | - Cybersecurity researchers have uncovered a new botnet called Zergeca, capable of conducting powerful distributed denial-of-service (DDoS) attacks.Written in Golang, Zergeca is named for a string "ootheca" present in the command-and-control (C2) servers "ootheca[.]pw" and "ootheca[.]top."<br>- Zergeca supports six different attack methods and has capabilities for proxying, scanning, self-upgrading, persistence, file transfer, reverse shell, and collecting sensitive device information. Notably, Zergeca uses DNS-over-HTTPS (DoH) for DNS resolution of the C2 server and a lesser-known library called Smux for C2 communications. | |
| Severity | Medium | |
| Attack Vectors | - There is evidence to suggest that the malware is actively developing and updating the malware to support new commands. What's more, the C2 IP address 84.54.51[.]82 is said to have been previously used to distribute the Mirai botnet around September 2023.<br>- As of April 29, 2025, the same IP address began to be used as a C2 server for the new botnet, raising the possibility that the threat actors "accumulated experience operating the Mirai botnets before creating Zergeca."<br>- Attacks mounted by the botnet, primarily ACK flood DDoS attacks, have targeted Canada, Germany, and the U.S. between early and mid-June 2024.<br>- Zergeca's features span four distinct modules – namely persistence, proxy, silivaccine, and zombie – to set up persistence by adding a system service, implementing proxying, removing competing miner and backdoor malware, and gaining exclusive control over devices running the x86-64 CPU architecture, and handle the main botnet functionality.<br>- The zombie module is responsible for reporting sensitive information from the compromised device to the C2 and awaits commands from the server, supporting six types of DDoS attacks, scanning, reverse shell, and other functions. | |
| Indicator of Compromise | INDICATOR TYPE | INDICATORS |
| | File Hash | - 23ca4ab1518ff76f5037ea12f367a469<br>- 9d96646d4fa35b6f7c19a3b5d3846777<br>- d78d1c57fb6e818eb1b52417e262ce59<br>- 604397198f291fa5eb2c363f7c93c9bf<br>- 6ac8958d3f542274596bd5206ae8fa96<br>- 980cad4be8bf20fea5c34c5195013200<br>- 60f23acebf0ddb51a3176d0750055cf8 |
| | Domain | - bot[.]hamsterrace[.]space |
| | IP | - 84[.]54[.]51[.]82 |

| | |
|---|---|
| Recommendations | - Block all threat indicators at your respective controls.<br>- Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls.<br>- Monitor network traffic for unusual behavior indicative of botnet activity.<br>- Implement strict firewall rules to block traffic from known Zergeca C2 IP addresses.<br>- Regularly update your antivirus software and implement a patch management lifecycle.<br>- Use comprehensive antivirus and anti-malware software, and update signature definitions promptly.<br>- Employ multi-layered protection strategies to secure vulnerable assets effectively.<br>**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/<br>- https://thehackernews.com/2024/07/new-golang-based-zergeca-botnet-capable.html<br>- https://www.blackhatethicalhacking.com/news/new-zergeca-botnet-a-powerful-new-threat-that-employs-advanced-evasion-tactics-and-ddos-attacks/ |