New ‘GoBruteforcer’ Botnet Targets Web Servers

A recently identified Golang-based botnet is targeting web servers running FTP, MySQL, phpMyAdmin, and Postgres services, Palo Alto Networks reports.

Dubbed GoBruteforcer and found hosted on a legitimate domain, the malware targets multiple architectures, including x86 and ARM, and was seen deploying an internet relay chat (IRC) bot on a compromised server, for communication purposes.

The malware spreads using classless inter-domain routing (CIDR) block scanning to identify target hosts within a network, and then attempts to compromise the identified server using brute force.

Upon successful compromise, it deploys the IRC bot on the server. At a later stage, it uses a PHP web shell to query the victim system.

GoBruteforcer, which appears to still be in development, is packed with UPX Packer and has a multi-scan module it uses to identify open ports for targeted services. Once a port is identified, it uses hardcoded credentials to brute-force the server.

For phpMyAdmin services, it scans for any open port 80, after which it attempts to deploy the IRC bot for communication.

For MySQL and Postgres services, the malware checks for open ports 3306 and 5432, then pings the host’s database using specific credentials. For FTP services, it checks for open port 21, and then attempts to authenticate using the Goftp library.

On victim servers, Palo Alto Networks found a PHP web shell that provides attackers with reverse shell and bind shell capabilities.

“The GoBruteforcer bot comes with a multiscan capability, which gives it a wide range of targets that it can use to get into a network. GoBruteforcer also seems to be in active development, so attackers could change the techniques they use to target web servers in the near future,” Palo Alto Networks concludes.

Related: HeadCrab Botnet Ensnares 1,200 Redis Servers for Cryptomining

Related: Zerobot IoT Botnet Adds More Exploits, DDoS Capabilities

Related: Multi-Purpose Botnet and Infostealer ‘Aurora’ Rising to Fame

New ‘GoBruteforcer’ Botnet Targets Web Servers