UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0288

GOBRUTEFORCER TARGETS WEB SERVERS

DATE ISSUED: 13th March 2023

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	**MEDIUM**	EASY

OVERVIEW

Researchers at Palo Alto Networks' Unit 42 have discovered a new botnet malware written in Golang programming language that targets web servers, especially those running with phpMyAdmin, MySQL, FTP, and Postgres database management services.

BREAKDOWN

The malware dubbed as GoBruteforcer uses a brute force attack against accounts with weak/default passwords to hack into vulnerable servers. The malware targets multiple architectures, including x86, x64, and ARM. It uses Classless Inter-Domain Routing (CIDR) to multi-scan for a broad selection of targets running database management services. Then it uses hardcoded credentials to brute force the server. It deploys an Internet Relay Chat (IRC) on compromised systems to initiate communication with Command-and-Control (C2) server. Later, it uses a PHP web shell to query the victim system providing the attackers with reverse shell and bind shell capabilities. Interestingly, the malware uses CIDR block scanning to look for potential targets instead of a single IP address allowing it to expand the reach of the attack.

REMEDIATION STEPS

- Ensure that your organisation has up to date Web Application Firewall (WAF) to prevent unauthorised access to your systems.
- Network monitoring and analysis should be conducted regularly to detect and investigate any anomalous network behaviour.
- Set long and complex password for a web application or public server to mitigate brute-force attack. Always change default or factory passwords on all devices and applications.
- Please refer to Importance of Strong Passwords and Practices to create strong password policies for your organisation.

REFERENCES & RESOURCES

Bleeping Computer https://www.bleepingcomputer.com/news/security/new-gobruteforcer-malware-targets-phpmyadmin-mysql-ftp-postgres/

Palo Alto Unit 42 https://unit42.paloaltonetworks.com/gobruteforcer-golang-botnet/