GoBruteForcer

Threat: **Brute-Force Malware**

Author: **Jeffrey Farnan** Date Originally Published: **March 29th, 2023**

1. SUMMARY

- A new Botnet has been found in the wild called GoBruteForcer, written in the Golang language, it scans and infects web servers running phpMyAdmin, MySQL, FTP and Postgres services. GoBruteforcer tries to get access to server accounts with weak or default passwords via brute-force. Once an account is accessed an IRC Bot (Internet Relay Chat Bot) is deployed. The next phase GoBruteforcer will contact its command-and-control server and wait for instructions. Instructions will be delivered either by the IRC bot or a web shell, allowing other malicious activities to be carried out such as installing other malware.

2. MALWARE FAMILY

- **Type** = Brute-Force Malware.
- **Sub-type** = Bot, Dropper.
- **Brute-Force Malware:** An application which is programmed to guess a user's password using all possible combinations until the correct one of found.
- **Bot:** Designed to infect many devices and gain control of those devices.
- **Dropper:** Malicious program created to deliver other malware payloads to a victim's computer.

3. MALWARE CHARATERISTICS

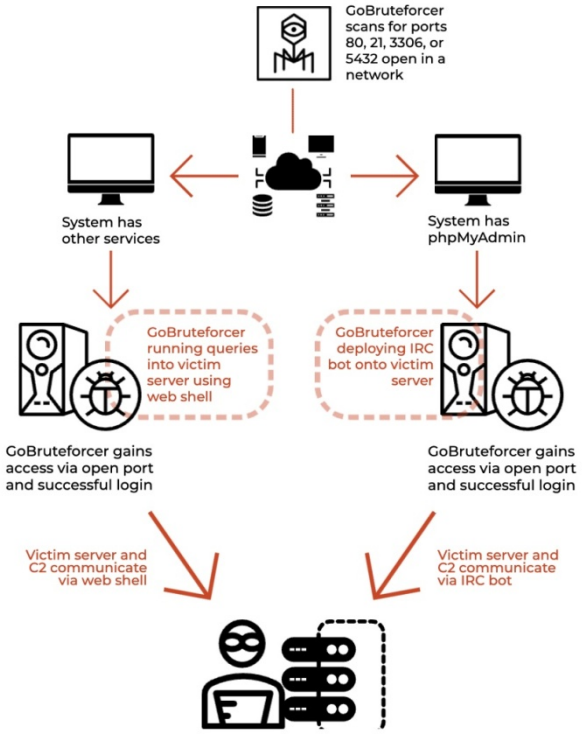
- **Suspected country of origin** = Unknown.
- **First seen date/period** = January 2022.
- **Still active** = Yes.
- **Last submitted sample as of writing this article** = February 20th, 2023.

4. MALWARE HISTORY

- Hackers have been trying to crack passwords for many decades, as a method to gain access to secure systems either for malicious purposes or simply to prove that they can. The hackers would simply guess a password or use default passwords to gain entry. As users have become more security aware and systems ask for more secure passwords such as longer passwords including unusual characters, this means systems are harder to get into. Brute-force applications are designed to run through a series of common passwords or come up with different combinations of passwords to try and find the correct one, this is referred to as brute forcing.
- The Golang or Go programming language is a programming language developed by Google. Recently it has become popular with malware programmers, being versatile enough to develop all different types of malwares.
- Security researching with Palo Alto Networks' Unit 42 were the first to spot this malware in the wild and dubbed it GoBruteforcer.

5. MALWARE DESCRIPTION

- GoBruteforcer is designed to target multiple platforms running x86, x64 and ARM architectures. The malware attempts to obtain access via a brute-force attack using a list of credentials hard-coded into the binary.
- **Spread:** This 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. CIDR block scanning is a way to get access to a wide range of target hosts on different IPs within a network instead of using a single IP address as a target.
- **Brute-force:** With targeted IP addresses acquired, the malware scans for phpMyAdmin, MySQL, FTP and Postgres services. After detecting an open port accepting connections, it will attempt to gain access by brute-force using hard-coded credentials.
- **IRC bot:** Once the malware has gotten access, it deploys and IRC bot on the compromised phpMyAdmin systems or a PHP web shell on servers running other targeted services. IRC is a classic chat protocol of the internet. Allows real-time messaging between internet-connected computers created in 1988. Text-based protocol, messages are encoded in plain ASCII, used for group discussions in chat rooms called "channels". It also supports data transfers, various server-side and client-side commands. The Internet Relay Chat Bot is an application that performs automated tasks within an IRC-based chat room or channel. It is used by botnet owners to send commands to individual computers in their botnet. This can be done in a specific channel, on a public network, or a separate IRC server. The IRC server containing the channel used to control the bots is referred to as a "command and control" or C2 server.
- **Command-and-Control:** GoBruteforcer will reach out to its C2 server via a web shell or IRC Bot and wait for instructions.



- GoBruteforcer deploys a variety of different types of malware as payloads one of which is coinminers. GoBruteforcer is still likely under development, attackers could change the techniques they use to target different web servers in the future.

6. POTENTIAL CUSTOMER DEFENSE

- The best protection against brute force attacks of either hackers or malware applications is to have very strong passwords and to change them regularly.
- Some other helpful techniques to protect yourself and your organization:
    - Restrict Access to Authentication URLs.
    - Limit Login Attempts.
    - Use Two-Factor Authentication (2FA).
- **Use Brute force protection:** Safeguards against a single IP address attacking a single user account. When a given IP address tries and fails multiple times to log in as the same user brute-force protection blocks the suspicious IP address from logging in as that user, notifies the victim by sending an alert email notifying that unusual activity is taking place. After a period of time the user can unblock their account and change the password.

Research Sources:

- https://www.bleepingcomputer.com/news/security/new-gobruteforcer-malware-targets-phpmyadmin-mysql-ftp-postgres/
- https://unit42.paloaltonetworks.com/gobruteforcer-golang-botnet/
- https://www.radware.com/security/ddos-knowledge-center/ddospedia/irc-internet-relay-chat/
- https://www.securityweek.com/new-gobruteforcer-botnet-targets-web-servers/
- https://auth0.com/docs/secure/attack-protect