AL2025_30 PumaBot Botnet Targets IoT Devices Using SSH Brute Force Attacks (June 11, 2025)

Description

A newly identified Go-based Linux malware, dubbed **PumaBot**, is targeting Internet of Things (IoT) devices through SSH brute force attacks to gain unauthorized access and establish persistence. First reported by **Darktrace** on May 28, 2025, PumaBot is not a typical scattergun botnet. Instead of indiscriminately scanning the internet for open targets, it takes a more **targeted approach**, receiving pre-defined IP addresses from its command-and-control (C2) server. Notably, PumaBot seems to focus on surveillance and traffic cameras, particularly those potentially manufactured or distributed by **Pumatronix**, based on signature strings observed during infection attempts.

Attack Details

PumaBot employs a strategic and sophisticated infection chain, showcasing the evolution of modern botnet tactics. The attack begins with target acquisition, where the malware retrieves a list of specific IP addresses from its command-and-control (C2) server, ssh.ddos-cc.org, instead of scanning the internet indiscriminately. It then attempts brute-force login attacks over port 22 (SSH) on these selected targets. Once access is gained, PumaBot runs the uname -a command to collect operating system and hardware information, which helps it avoid honeypots and confirm the device is a legitimate IoT target. For persistence, the malware installs its main binary (jierui) in the /lib/redis directory and sets up a malicious systemd service named redis.service to survive system reboots. Additionally, it adds its own SSH key to the authorized_keys file to maintain ongoing access. PumaBot's malicious capabilities include credential harvesting through a modified PAM module (pam_unix.so) that logs SSH login details. These credentials are stored in a file named con.txt, which is monitored by a daemon binary (1) that exfiltrates the data back to the C2 server. Afterward, the malware erases con.txt to remove evidence of the breach. PumaBot also supports modular updates, enabling it to download and execute new payloads or scripts, enhancing its functionality and threat level over time.

Indicators of Compromise (IOCs)

Below are some key IOCs associated with PumaBot:

1. **C2 Domain:**
   - ssh.ddos-cc.org
2. **Binary Names:**
   - jierui (main payload)

- 1 (daemon for exfiltration)
- pam_unix.so (malicious PAM module)
- con.txt (temporary credential log file)

3. **File Paths:**
    - /lib/redis/jierui
    - /etc/systemd/system/redis.service

Remediation

Organizations and individuals must take proactive steps to mitigate the risks posed by PumaBot and similar IoT-targeting threats. Recommended actions include:

1. Change Default Credentials
    - Immediately change all default usernames and passwords on IoT devices.
2. Isolate IoT Devices
    - Place IoTs on separate network segments away from core systems to limit lateral movement.
3. Firmware Updates
    - Regularly update device firmware to patch known vulnerabilities.
4. Use Strong Authentication
    - Disable password-based SSH logins where possible and use public key authentication.
5. Enable Firewalls and Port Restrictions
    - Restrict access to SSH ports using firewalls or VPN-based management systems.
6. Monitor for IOCs and Unusual Activity
    - Continuously monitor logs and network traffic for signs of PumaBot-related activity or unauthorized SSH access.
7. Implement Endpoint Security
    - Use lightweight endpoint protection solutions for embedded systems where feasible.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- PumaBot - a new botnet on the rise. (n.d.). Retrieved from broadcom.com https://www.broadcom.com/support/security-center/protection-bulletin/pumabot-a-new-botnet-on-the-rise
- Toulas, B. (2025, May 28). New PumaBot botnet brute forces SSH credentials to breach devices. Retrieved from BleepingComputer.

https://www.bleepingcomputer.com/news/security/new-pumabot-botnet-brute-forces-ssh-credentials-to-breach-devices/