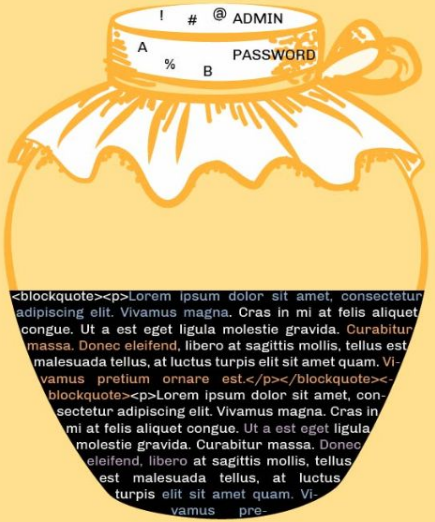
How Quickly Can Attackers Target Open SSH/Telnet Ports? Threat Hunting Analysis Using Cowrie Honeypot and Splunk

By: Bennett Nottingham

Project Objectives

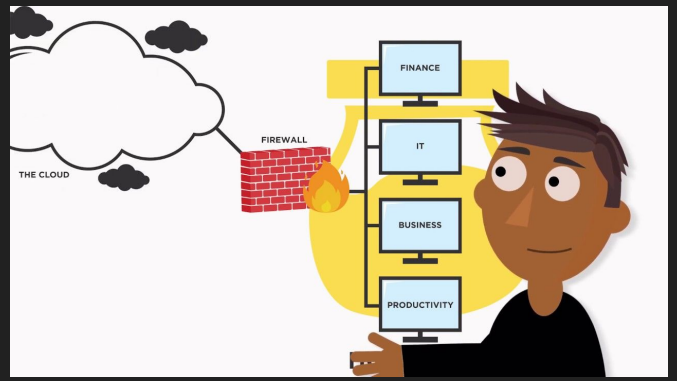
- Simulate SSH/Telnet server with Cowrie honeypot.
- Highlight vulnerabilities of SSH and Telnet services.
- Calculate time from honeypot deployment to first attacker connection.
- Analyze attack frequency and timing for persistence.
- Data exploration in Splunk.
- Provide actionable recommendations.

WHAT IS A HONEYPOT IN CYBER SECURITY



Honeypots

- Decoy servers or systems that attract attackers.
- Designed to be probed, attacked, and potentially compromised.
- Helps understand attacker behavior patterns (TTPs).
- Distracts attackers from real targets.



Why Did I Choose Cowrie Honeypot?

- Easy setup and configuration.
- Emulates a UNIX system with a fake filesystem.
- Realistic command responses for attackers.
- Automatically logs activity with log rotation (cowrie.log, cowrie.json).
- Stores session logs and collects attacker downloads.

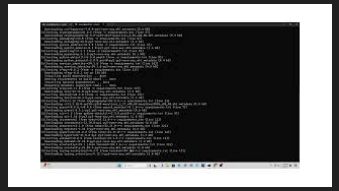
SSH (port 22) 

- Network protocol for remote device access.
- Data is encrypted via a secure channel.
- Can be vulnerable to brute force attacks.

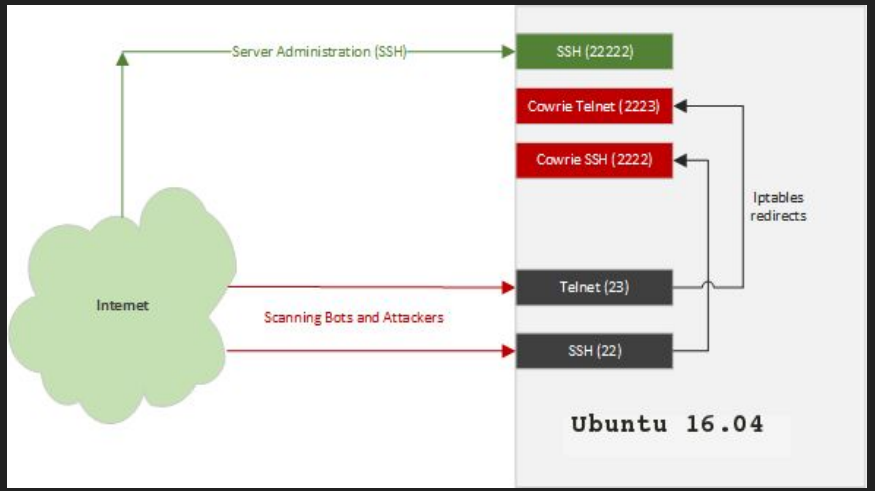
Telnet (port 23) 

- Standard TCP/IP protocol for virtual terminal service.
- Highly vulnerable to security attacks.
- Transfers data in plain text.
- Shouldn’t be used on any device.

Cowrie Setup



- Installed on Linode VPS running Ubuntu.
- Installed Cowrie-specific dependencies (https://github.com/cowrie/cowrie).
- sshd_config, change port 22 to 9022.
- sudo iptables (NAT)

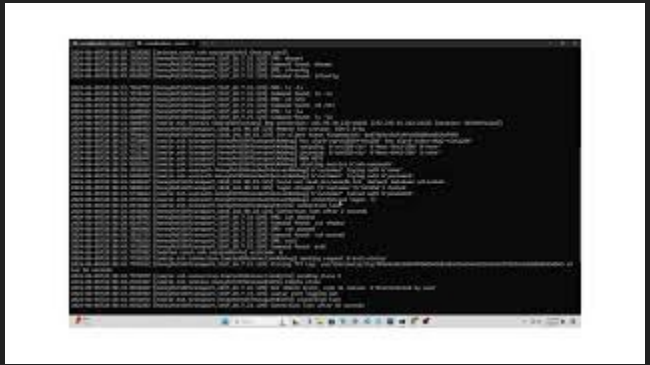



```
sysadmin@vm-image-ubuntu-dev-1:/$ nmap -p 22,23,2222,2223,9022 172.235.61.213
Starting Nmap 7.80 ( https://nmap.org ) at 2024-06-06 05:41 UTC
Nmap scan report for 172-235-61-213.ip.linodeusercontent.com (172.235.61.213)
Host is up (0.064s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
23/tcp   open  telnet
2222/tcp open  EtherNetIP-1
2223/tcp open  rockwell-csp2
9022/tcp open  paragent
```

Cowrie Honeypot Demonstration

- Show incoming connections in real-time.
- Simulate an attack by using ssh to gain root access.
- Investigate the session recording.
- Look at attacker downloads.



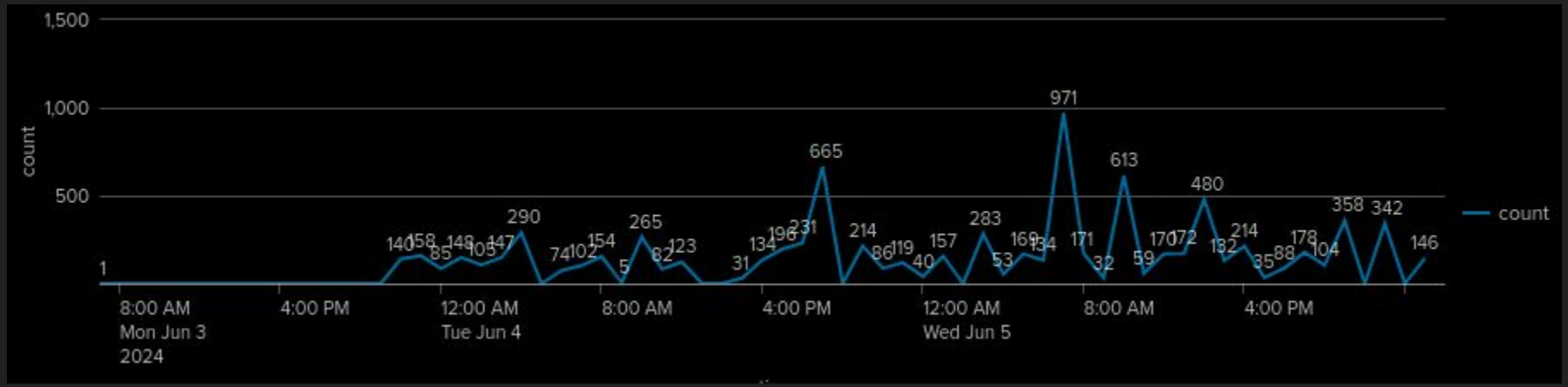
Cowrie Honeypot Findings

Time-to-First Attack

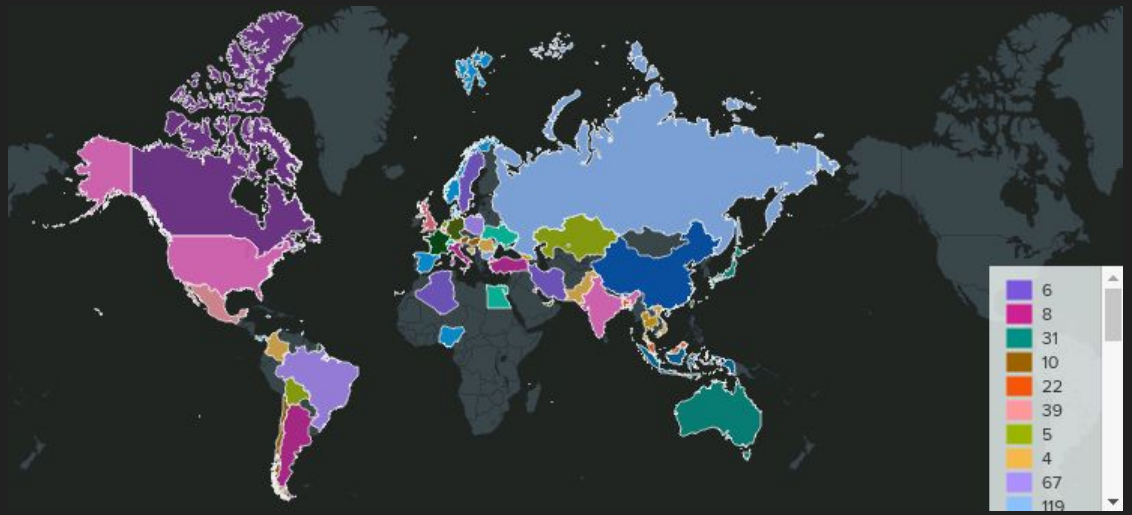
- Cowrie honeypot starts around June 3, 10:16:42 p.m.
- First telnet connection attempt is at 10:16:50 p.m. from IP 27.29.34.199 (Huanggang, China) 8 seconds after startup.
- First successful SSH login is at 10:23:16 p.m. from IP 183.81.169.238 (Amsterdam) about 7 minutes after startup (“root”, “0”).

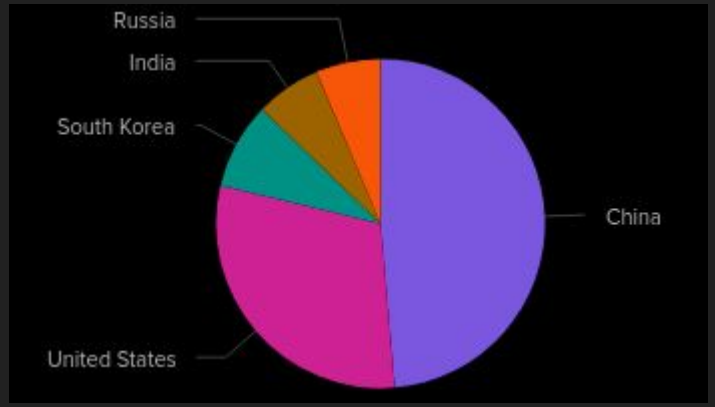
```
cowrie@localhost:~/cowrie/var/log/cowrie$ cat cowrie.log.2024-06-03
2024-06-03T22:16:42.296999Z [-] Python Version 3.10.12 (main, Nov 20 2023, 15:14:05) [GCC 11.4.0]
2024-06-03T22:16:42.297038Z [-] Twisted Version 24.3.0
2024-06-03T22:16:42.297056Z [-] Cowrie Version 2.5.0
2024-06-03T22:16:42.299689Z [-] Loaded output engine: jsonlog
2024-06-03T22:16:42.301053Z [twisted.scripts._twistd_unix.UnixAppLogger#info] twistd 24.3.0 (/home/cowrie/cowrie/cowrie-env/bin/python 3.10.12) starting up.
2024-06-03T22:16:42.301212Z [twisted.scripts._twistd_unix.UnixAppLogger#info] reactor class: twisted.internet.epollreactor.EPollReactor.
2024-06-03T22:16:42.308206Z [-] CowrieSSHFactory starting on 2222
2024-06-03T22:16:42.308557Z [cowrie.ssh.factory.CowrieSSHFactory#info] Starting factory <cowrie.ssh.factory.CowrieSSHFactory object at 0x7f7eb93164d0>
2024-06-03T22:16:42.309076Z [-] Generating new RSA keypair...
2024-06-03T22:16:42.410378Z [-] Generating new ECDSA keypair...
2024-06-03T22:16:42.411485Z [-] Generating new ed25519 keypair...
2024-06-03T22:16:42.416124Z [-] Ready to accept SSH connections
2024-06-03T22:16:42.416671Z [-] HoneyPotTelnetFactory starting on 2223
2024-06-03T22:16:42.416779Z [cowrie.telnet.factory.HoneyPotTelnetFactory#info] Starting factory <cowrie.telnet.factory.HoneyPotTelnetFactory object at 0x7f7eb93146d0>
2024-06-03T22:16:42.417533Z [-] Ready to accept Telnet connections
2024-06-03T22:16:50.936899Z [cowrie.telnet.factory.HoneyPotTelnetFactory] New connection: 27.29.34.199:48866 (172.235.61.213:2223) [session: 93b98ee40982]
```

Time Analysis of Events



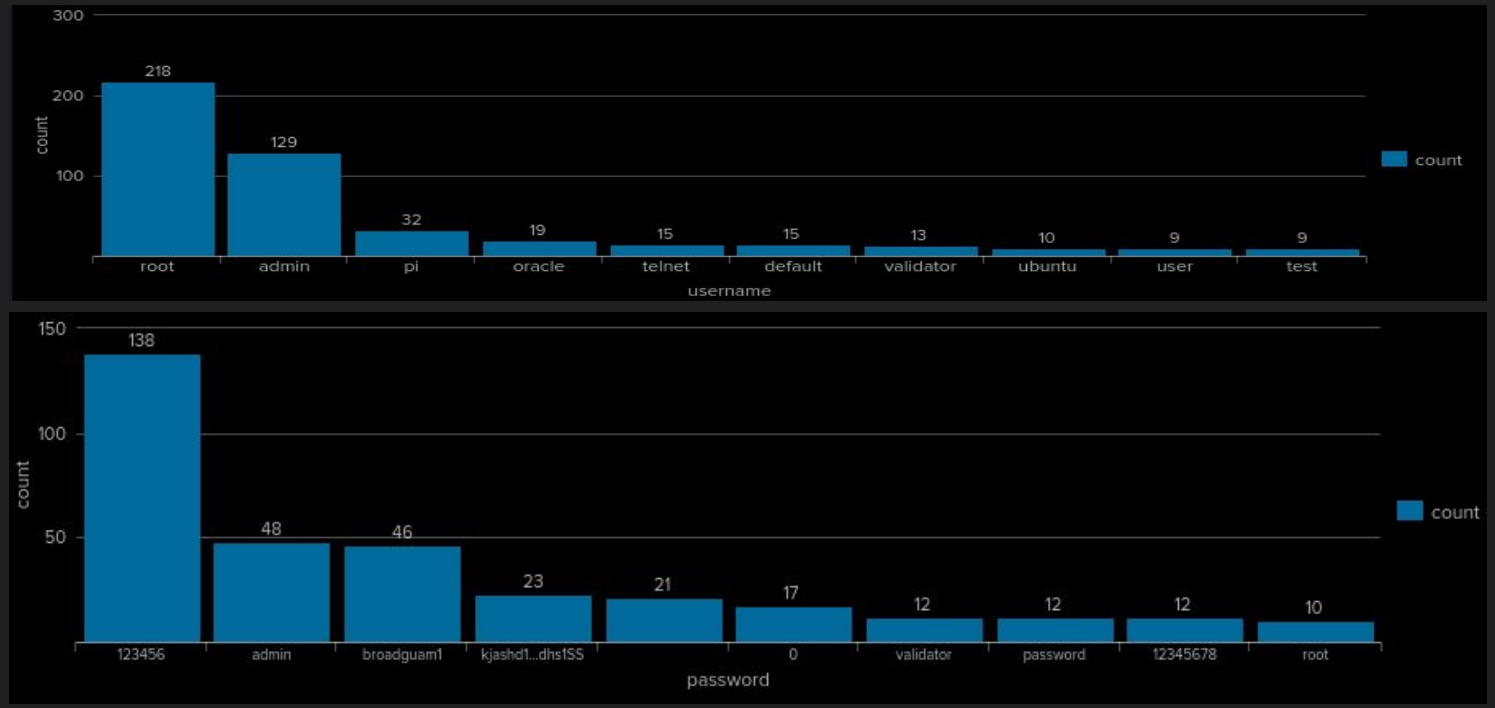
Origin of Attacks



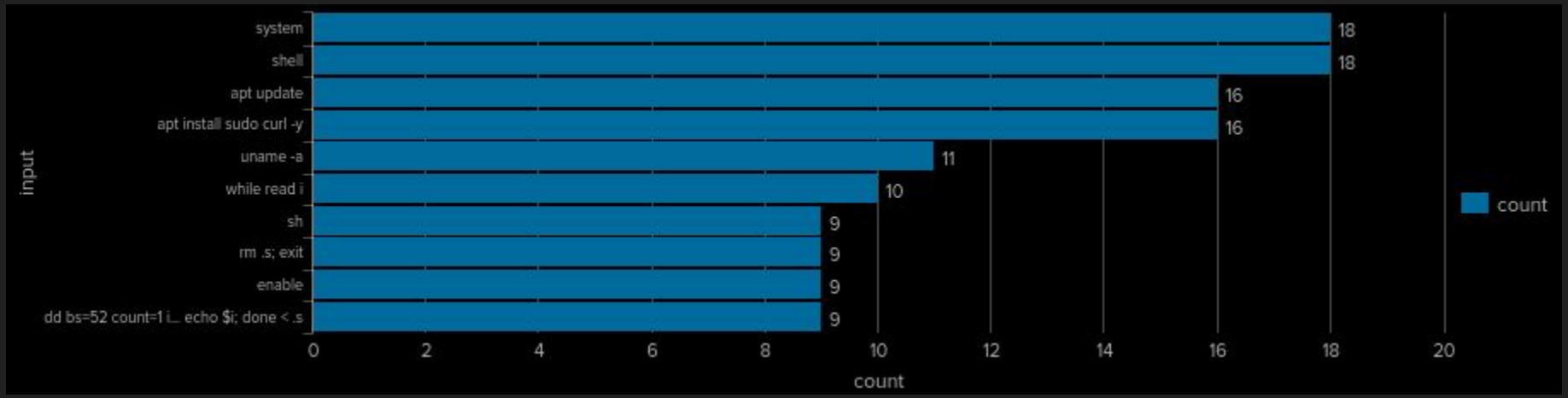


Country	count	percent
China	3225	37.034910
United States	1996	22.921452
South Korea	563	6.465319
India	425	4.880570
Russia	423	4.857602

Top 10 Usernames/Passwords



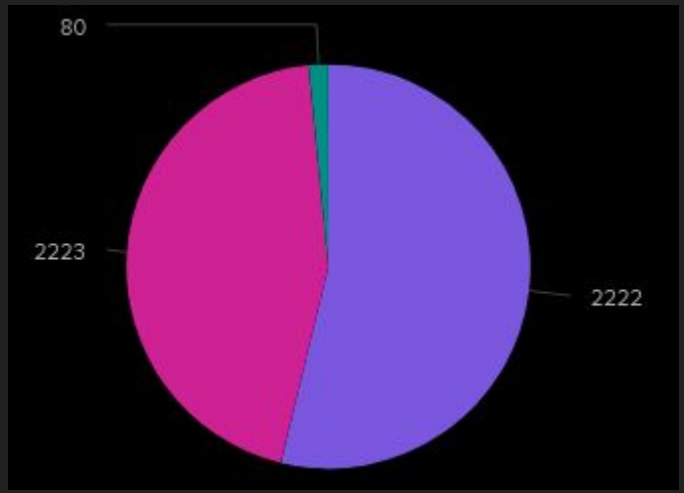
Top Commands Used



Total Events

8,708

Top 10 Values	Count	%
cowrie.session.connect	2,387	27.412%
cowrie.session.closed	2,386	27.4%
cowrie.client.version	1,174	13.482%
cowrie.client.kex	1,147	13.172%
cowrie.login.failed	833	9.566%
cowrie.command.input	238	2.733%
cowrie.login.success	186	2.136%
cowrie.session.params	97	1.114%
cowrie.log.closed	96	1.102%
cowrie.command.failed	82	0.942%



Securing SSH and Telnet Services

- Disable Telnet
- Disable root login
- Use strong passwords
- Use key-based authentication
- Utilize fail2ban which blocks IP addresses after a certain amount of failed login attempts.
- Use two-factor authentication

THANK YOU

ANY QUESTIONS?