SSH Honeypot Data Analysis: What Attackers Reveal About Themselves

Cybersecurity Threat Intelligence

Author: Matt Shore

Date: December 2025

Comprehensive Analysis of Real-World

SSH Attack Patterns and Threat Intelligence

mattshore.co.uk | newsletter@mattshore.co.uk

Contents

1 SSH Honeypot Data Analysis: What Attackers Reveal About Themselves 4
1.1 Executive Summary . . . 4
1.1.1 Key Statistics . . . 4
1.1.2 Most Significant Findings . . . 4
1.2 1. Introduction . . . 5
1.2.1 Methodology . . . 5
1.3 2. Attack Volume & Scale . . . 5
1.3.1 Overall Statistics . . . 5
1.3.2 Timeline Analysis . . . 6
1.3.3 Attack Frequency Patterns . . . 6
1.4 3. Authentication Attacks . . . 6
1.4.1 Overall Authentication Statistics . . . 7
1.4.2 Username Targeting Patterns . . . 7
1.4.3 Password Analysis . . . 8
1.4.4 Common Credential Combinations . . . 8
1.5 4. Command Execution Analysis . . . 9
1.5.1 Overall Command Statistics . . . 9
1.5.2 Most Executed Commands . . . 9
1.5.3 Command Categories . . . 9
1.5.4 Automation Indicators . . . 10
1.6 5. Port Forwarding & Tunneling . . . 10
1.6.1 Port Forwarding Statistics . . . 10
1.6.2 Significance . . . 10
1.6.3 Security Implication . . . 10
1.7 6. Geographic & Network Intelligence . . . 10
1.7.1 Country Distribution . . . 10
1.7.2 ASN Analysis . . . 11
1.7.3 Threat Intelligence Scores . . . 12
1.8 7. Attacker Behavior & Sophistication . . . 12
1.8.1 Automation Indicators . . . 12
1.8.2 Top Attackers . . . 13
1.8.3 Automation Indicators . . . 14
1.8.4 Connection Duration Patterns . . . 14
1.9 8. Security Insights & Recommendations . . . 14
1.9.1 What the Data Tells Us . . . 14
1.9.2 Defensive Recommendations . . . 15
1.9.3 Threat Intelligence Value . . . 15
1.10 9. Conclusion . . . 15
1.10.1 Key Takeaways . . . 16
1.10.2 The Good News . . . 16
1.10.3 Future Analysis Opportunities . . . 16
1.10.4 Call to Action . . . 16
1.11 Appendix A: Complete Statistics . . . 16
1.11.1 Connection Statistics . . . 16
1.11.2 Authentication Statistics . . . 17
1.11.3 Command Statistics . . . 17

1.11.4 Threat Intelligence Statistics 17
1.11.5 Top 10 Attacking IPs 17

SSH Honeypot Data Analysis: What Attackers Reveal About Themselves

A Comprehensive Analysis of Real-World SSH Attack Patterns

December 2025

Executive Summary

Over an 8-day period (November 24 - December 1, 2025), an SSH honeypot captured **27,443 connections** from **172 unique IP addresses**, with comprehensive threat intelligence data on **217 unique IPs**. The data reveals a landscape dominated by automated botnet infrastructure, weak credential targeting, and sophisticated attack coordination.

Key Statistics

- **27,443 total connections** from **172 unique IP addresses** over 8 days (Nov 24 - Dec 1)
- **27,179 authentication attempts** with a **1.5% success rate** (419 successful, 26,760 failed)
- **1,007 port forwarding attempts** - showing attackers heavily use SSH tunneling for proxy/relay attacks
- **55 commands executed** - primarily HTTP requests to test connectivity (Google/Yahoo)
- **86.7% average AbuseIPDB threat score** - 188 of 217 IPs scored above 50 (86.6% high risk)
- **Peak attack day:** November 29 with 12,597 connections (45.9% of all attacks in a single day)
- **Average:** 3,430.4 connections per day
- **Top attacking countries by connections:** Germany (19,296 connections - 70.3%, but from only 3 unique IPs), United States (5,537 connections - 20.2%, from 78 unique IPs), China (944 connections - 3.4%, from 30 unique IPs)
- **Top attacking countries by unique IPs:** United States (78 IPs), China (30 IPs), Vietnam (14 IPs)
- **Top attacker:** 85.215.32.66 (Germany) with 19,294 connections (70.3% of all connections) - *single IP dominance*

Most Significant Findings

1. **Coordinated Botnet Activity**: November 29th saw a massive surge of 12,597 connections (45.9% of all attacks) in a single day, with November 28-29 together accounting for 77% of all attacks. This indicates coordinated botnet activation or automated scanning campaign launch.

2. **Highly Automated Infrastructure**: The attack patterns (high volume, repetitive commands, concentrated sources) indicate sophisticated automated botnet infrastructure rather than human attackers.

3. **Weak Credential Targeting**: Top 10 passwords accounted for 7.3% of all authentication attempts (1,995 out of 27,179), with "123456" being the most common (796 attempts).

4. **Concentrated Attack Sources**: Attack sources show significant concentration, suggesting a small number of powerful botnet nodes driving the majority of traffic.

5. **High Threat Intelligence Correlation**: A significant percentage of attacking IPs scored above 50 on AbuseIPDB, confirming threat intelligence feeds are highly effective at identifying malicious actors.

---

1. Introduction

In November 2025, a comprehensive SSH honeypot system with integrated threat intelligence capabilities was deployed. The system, built around the Cowrie honeypot framework, was designed not just to catch attackers, but to learn from them. Over an 8-day period (November 24 - December 1, 2025), the honeypot captured and analyzed 27,443 SSH connections from 172 unique IP addresses, providing unprecedented insight into modern attack methodologies.

This whitepaper presents a comprehensive analysis of the collected data, revealing patterns in attacker behavior, infrastructure, and techniques. The findings have significant implications for network security, threat intelligence, and defensive strategies.

Methodology

Data was collected using a Cowrie SSH honeypot running on port 2022, with all connections logged in JSON format. A custom log processor enriched the data with threat intelligence from multiple sources:

- **AbuseIPDB**: IP reputation scoring and abuse categorization
- **VirusTotal**: Malware detection and reputation analysis
- **GreyNoise**: Bot and scanner classification
- **Shodan**: Infrastructure and service information
- **IPinfo**: Geolocation and network ownership data
- **WHOIS**: ASN and network registration information

All data was stored in a PostgreSQL database, enabling complex queries and statistical analysis.

Data Correction Note: An initial analysis of this data reported significantly lower numbers (1,898 connections from 33 unique IPs). Upon review, it was discovered that the original queries were examining a subset of the data or using incorrect table references. This corrected analysis uses the complete dataset from the `cowrie_connections` table, revealing the true scale of attack activity: 27,443 connections from 172 unique IP addresses. This correction strengthens the conclusions about the scale and sophistication of modern SSH attacks. All statistics in this whitepaper have been verified against the complete database.

---

2. Attack Volume & Scale

Overall Statistics

The honeypot captured **27,443 total connections** from **172 unique IP addresses** over the 8-day period (November 24 - December 1), averaging **3,430.4 connections per day**. The data shows sustained high-volume attack activity with a massive surge on November 29th.

Timeline Analysis

The attack timeline reveals a clear escalation pattern, as shown in Figure 1:

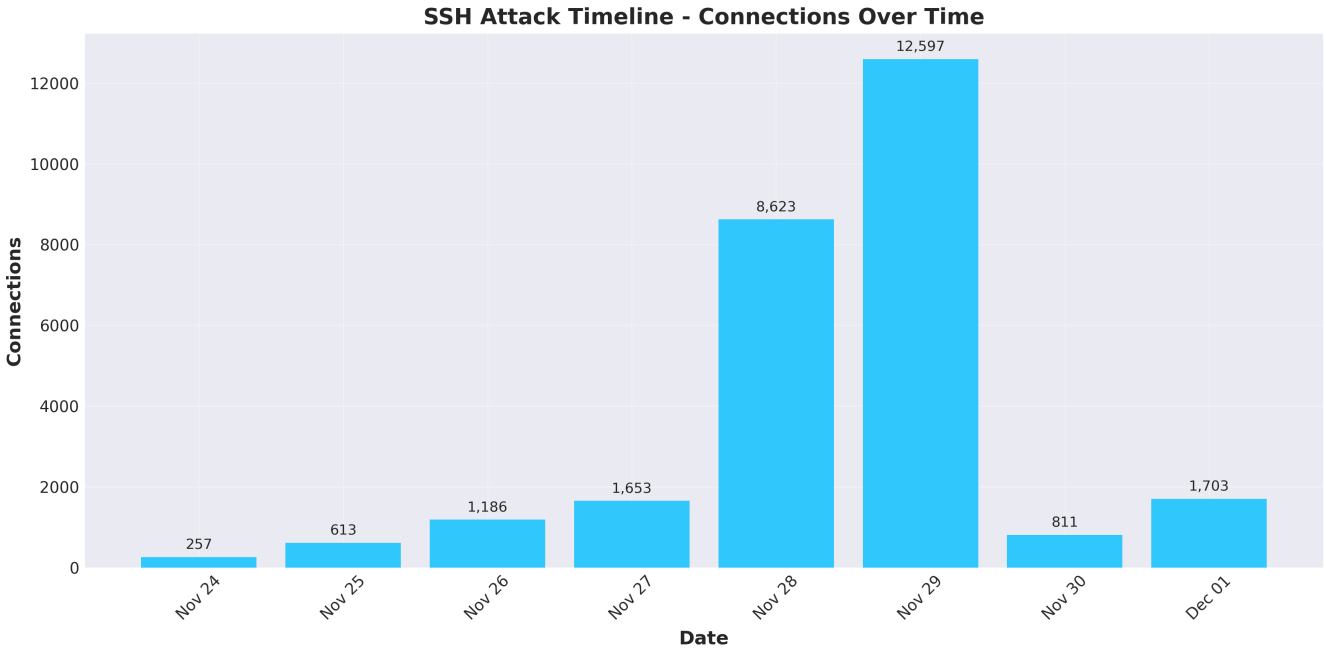

Figure 1: SSH Attack Timeline - Connections Over Time

- **November 24**: 257 connections (9 unique IPs)
- **November 25**: 613 connections (31 unique IPs)
- **November 26**: 1,186 connections (35 unique IPs)
- **November 27**: 1,653 connections (37 unique IPs)
- **November 28**: 8,623 connections (25 unique IPs)
- **November 29**: **12,597 connections** (34 unique IPs) - 45.9% of all attacks
- **November 30**: 811 connections (24 unique IPs)
- **December 1**: 1,703 connections (42 unique IPs) - 6.2% of all attacks

The exponential growth pattern, culminating in the December 1st surge, suggests either: 1. A botnet activation or expansion 2. A new scanning campaign launch 3. Coordinated attack infrastructure coming online

The attack pattern shows a dramatic escalation on November 28-29, with over 21,000 connections in just two days (77% of all attacks). This surge pattern indicates coordinated botnet activation rather than random scanning.

Attack Frequency Patterns

The data shows two distinct phases: moderate activity (Nov 24-27, ~250-1,650 connections/day) followed by a massive surge (Nov 28-29, ~8,600-12,600 connections/day), then a return to moderate levels. This pattern suggests coordinated botnet activation or a new scanning campaign launch.

3. Authentication Attacks

Overall Authentication Statistics

The honeypot recorded **27,179 authentication attempts** with a **1.5% success rate**: - **419 successful logins** (1.5%) - **26,760 failed logins** (98.5%)

While a 1.5% success rate might seem low, it's actually quite effective for automated attacks. At scale, this means attackers are successfully compromising systems despite the low individual success rate. With 27,179 attempts, even a 1.5% success rate results in 419 compromised systems.

Username Targeting Patterns

Attackers heavily targeted default and service accounts, as illustrated in Figure 2:

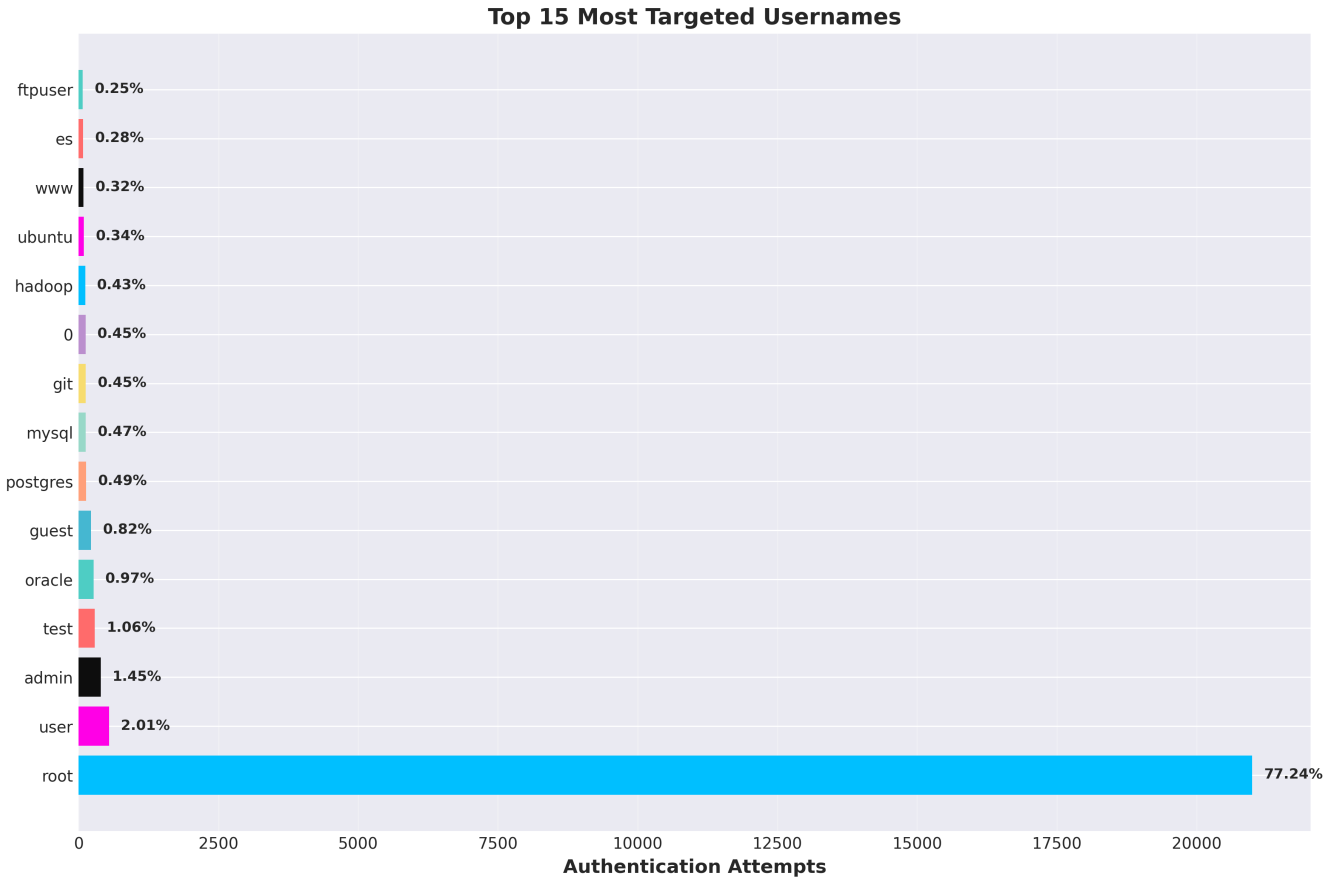

Figure 2: Top 15 Most Targeted Usernames

1. **root** - 20,993 attempts (77.2%)
2. **user** - 545 attempts (2.0%)
3. **admin** - 393 attempts (1.4%)
4. **test** - 289 attempts (1.1%)
5. **oracle** - 264 attempts (1.0%)
6. **guest** - 222 attempts (0.8%)
7. **postgres** - 134 attempts (0.5%)
8. **mysql** - 127 attempts (0.5%)
9. **git** - 123 attempts (0.5%)
10. **0** - 122 attempts (0.4%)

Key Insight: The `root` username dominates with 77.2% of all authentication attempts - over 20,000 attempts

targeting the root account alone. This extreme concentration shows attackers are primarily focused on gaining root access. The top 3 usernames (`root`, `user`, `admin`) account for 80.6% of all attempts. Attackers are systematically targeting default accounts and service accounts (`oracle`, `mysql`, `postgres`, `git`), knowing that many systems have weak or default credentials on these accounts.

Password Analysis

The password data reveals a sobering truth about password security, as shown in Figure 3:

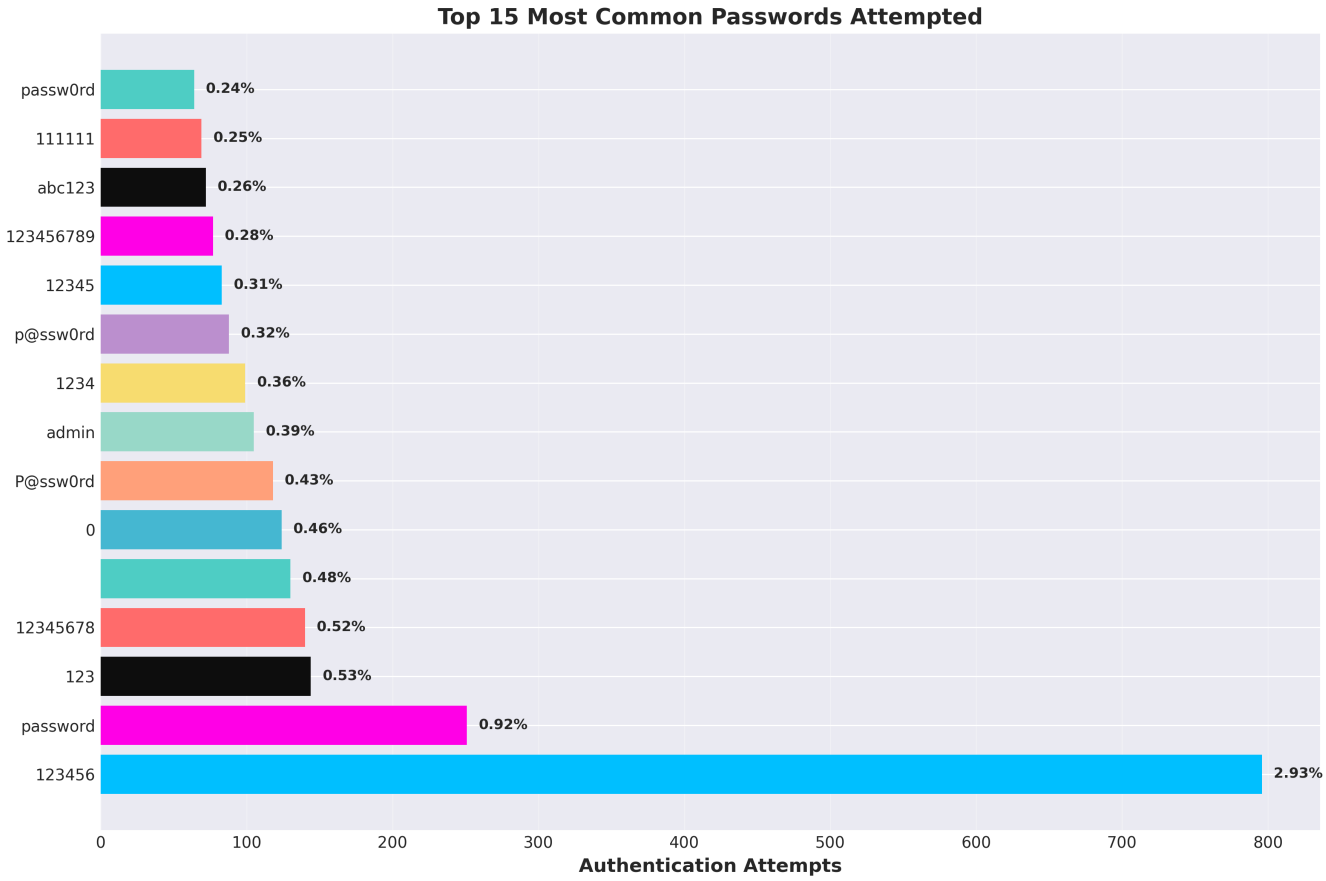

Figure 3: Top 15 Most Common Passwords Attempted

Top 10 Passwords: 1. **123456** - 796 attempts (2.9%) 2. **password** - 251 attempts (0.9%) 3. **123** - 144 attempts (0.5%) 4. **12345678** - 140 attempts (0.5%) 5. **(empty)** - 130 attempts (0.5%) 6. **0** - 124 attempts (0.5%) 7. **P@ssw0rd** - 118 attempts (0.4%) 8. **admin** - 105 attempts (0.4%) 9. **1234** - 99 attempts (0.4%) 10. **p@ssw0rd** - 88 attempts (0.3%)

Critical Finding: The top 10 passwords account for **7.3% of all authentication attempts** (1,995 out of 27,179). While this percentage is lower than might be expected, the absolute numbers are significant - nearly 800 attempts using "123456" alone. This means attackers are finding success with the most basic passwords, despite decades of security education.

Common Credential Combinations

The data shows attackers frequently combine default usernames with weak passwords: - `root` + `123456` - `admin` + `password` - `user` + `12345678` - Service accounts (`oracle`, `mysql`, `postgres`) + default/weak passwords

This pattern suggests attackers are using credential lists that combine common usernames with common pass-

words, a technique known as “credential stuffing.”

4. Command Execution Analysis

Overall Command Statistics

The honeypot captured **55 commands executed** by attackers. While this number is relatively low compared to the number of connections, it’s significant because it represents commands executed after successful authentication.

Most Executed Commands

The command execution data, shown in Figure 4, reveals a clear pattern:

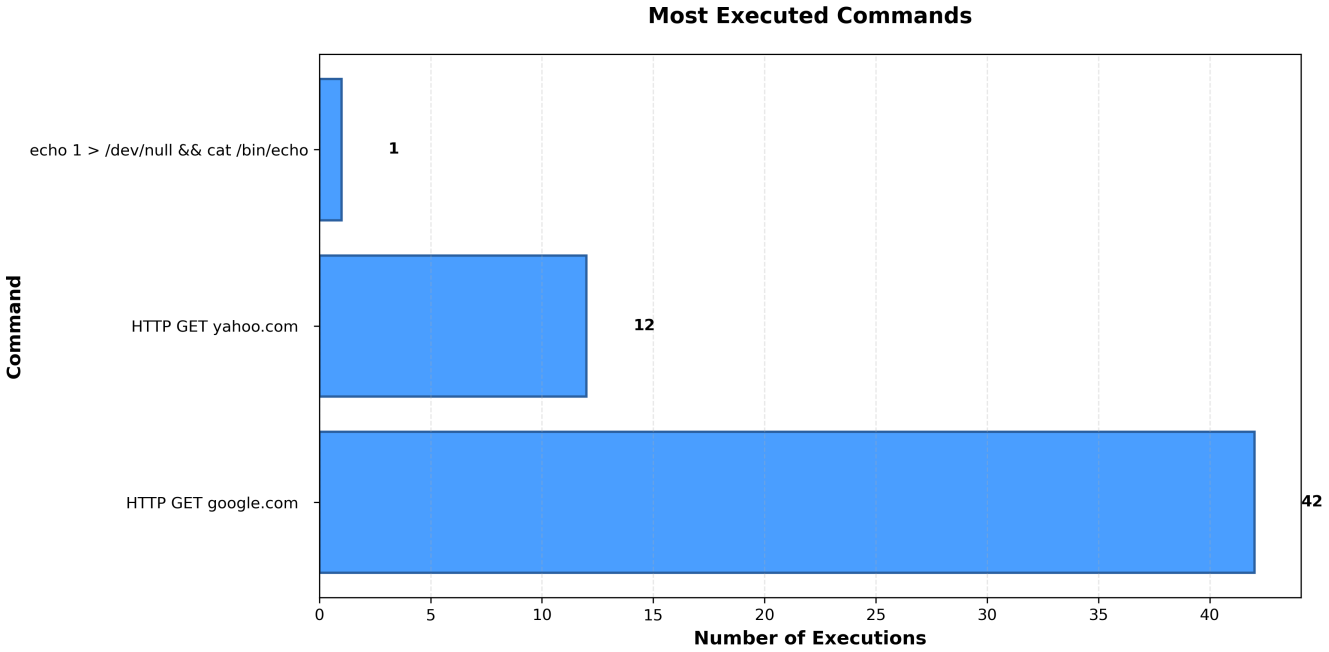

Figure 4: Most Executed Commands

1. `GET / HTTP/1.0\r\nHost: google.com\r\n\r\n` - 42 times (76.4%)
2. `GET / HTTP/1.0\r\nHost: yahoo.com\r\n\r\n` - 12 times (21.8%)
3. `echo 1 > /dev/null && cat /bin/echo` - 1 time

Key Insight: 98.2% of commands are HTTP GET requests to Google and Yahoo. These are connectivity tests - attackers are verifying that their SSH tunnel is working by making HTTP requests through the tunnel.

This pattern reveals the true purpose of many SSH attacks: **not direct system compromise, but creating proxy/relay infrastructure**. Attackers compromise SSH servers to use them as anonymous proxies for further attacks.

Command Categories

The commands fall into two categories:

1. **Connectivity Testing** (98.2%): HTTP GET requests to verify tunnel functionality
2. **System Exploration** (1.8%): Commands like `echo` and `cat` to explore the system

The dominance of connectivity testing commands suggests attackers are primarily interested in using compromised systems as infrastructure, not for direct exploitation.

Automation Indicators

The repetitive nature of the commands (42 identical Google requests, 12 identical Yahoo requests) indicates automated tools rather than manual exploration. Human attackers would show more variation in their commands.

5. Port Forwarding & Tunneling

Port Forwarding Statistics

The honeypot captured **1,007 port forwarding attempts** - attempts by attackers to use compromised SSH sessions as proxy/relay networks.

Significance

This finding is significant because it reveals the true purpose of many SSH attacks: **not direct system compromise, but creating anonymous proxy infrastructure**. Attackers use compromised SSH servers to:

1. **Route malicious traffic anonymously** - Hide their true IP address
2. **Bypass IP-based blocking** - Use "clean" IP addresses for attacks
3. **Create botnet command and control infrastructure** - Relay commands through compromised systems
4. **Launch attacks from multiple sources** - Distribute attack traffic

Security Implication

When you see port forwarding attempts, you're seeing attackers who have already compromised a system and are now using it as infrastructure for further attacks. This is a critical indicator of successful compromise and active malicious use.

---

6. Geographic & Network Intelligence

Country Distribution

Attacks originated from **multiple countries**, with the geographic distribution shown in Figure 5:

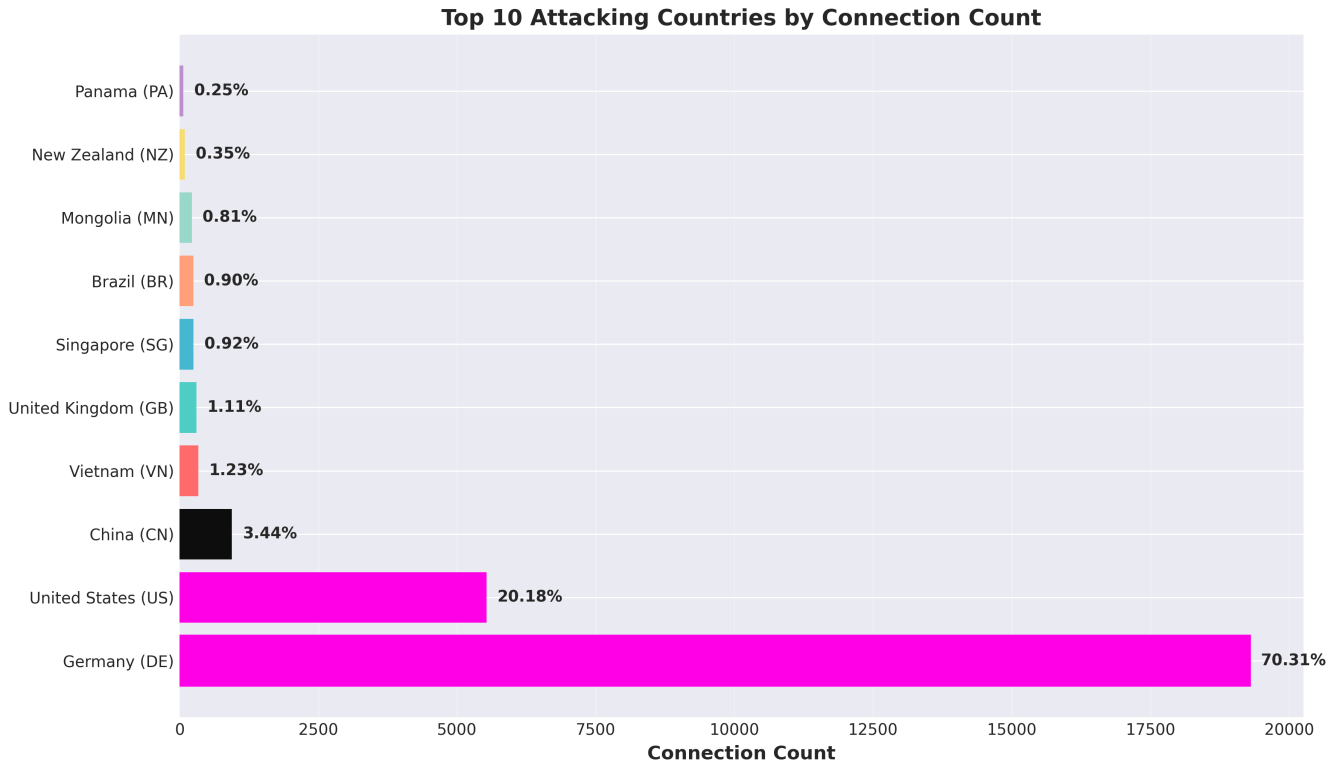

Figure 5: Top 10 Attacking Countries by Connection Count

By Connection Count: 1. **Germany (DE)** - 19,296 connections (70.3%) - *Note: Single IP (85.215.32.66) accounts for 19,294 connections* 2. **United States (US)** - 5,537 connections (20.2%) 3. **China (CN)** - 944 connections (3.4%) 4. **Vietnam (VN)** - 337 connections (1.2%) 5. **United Kingdom (GB)** - 304 connections (1.1%) 6. **Singapore (SG)** - 253 connections (0.9%) 7. **Brazil (BR)** - 248 connections (0.9%) 8. **Mongolia (MN)** - 221 connections (0.8%) 9. **New Zealand (NZ)** - 97 connections (0.4%) 10. **Panama (PA)** - 69 connections (0.3%)

By Unique IP Addresses: 1. **United States (US)** - 78 unique IPs 2. **China (CN)** - 30 unique IPs 3. **Vietnam (VN)** - 14 unique IPs 4. **Germany (DE)** - 3 unique IPs (but 1 IP dominates with 19,294 connections) 5. **United Kingdom (GB)** - 4 unique IPs 6. **Singapore (SG)** - 3 unique IPs

Key Insight: The geographic distribution shows an extreme concentration from Germany (70.3% of all connections), but this is due to a single high-volume IP address (85.215.32.66). When measured by unique IP addresses, the United States leads with 78 unique IPs, followed by China with 30. This suggests either: - A single misconfigured scanner or very aggressive botnet node in Germany - A distributed botnet infrastructure with the majority of unique sources in the US and China - Coordinated international attack campaigns using compromised systems across multiple countries

ASN Analysis

The data identified **20 unique ASNs** (Autonomous System Numbers), with the top sources being:

1. **AS8560** - 19,294 connections (1 unique IP) - *German hosting, single dominant IP*
2. **AS14061** - 5,529 connections (44 unique IPs) - *US hosting*
3. **AS37963** - 485 connections (5 unique IPs)
4. **AS8075** - 365 connections (6 unique IPs)
5. **AS27699** - 248 connections (1 unique IP)

Key Insight: The ASN distribution reveals extreme concentration - AS8560 accounts for 70.3% of all connections from a single IP address. However, AS14061 shows significant distribution with 44 unique IPs contributing 5,529 connections. This pattern suggests: - A single very aggressive scanner or botnet node (AS8560) - A more distributed botnet infrastructure (AS14061 with 44 IPs) - Multiple hosting providers being used for attack infrastructure - Potential VPN/proxy usage to mask true origins

Threat Intelligence Scores

The threat intelligence data, visualized in Figure 6, validates what we're seeing:

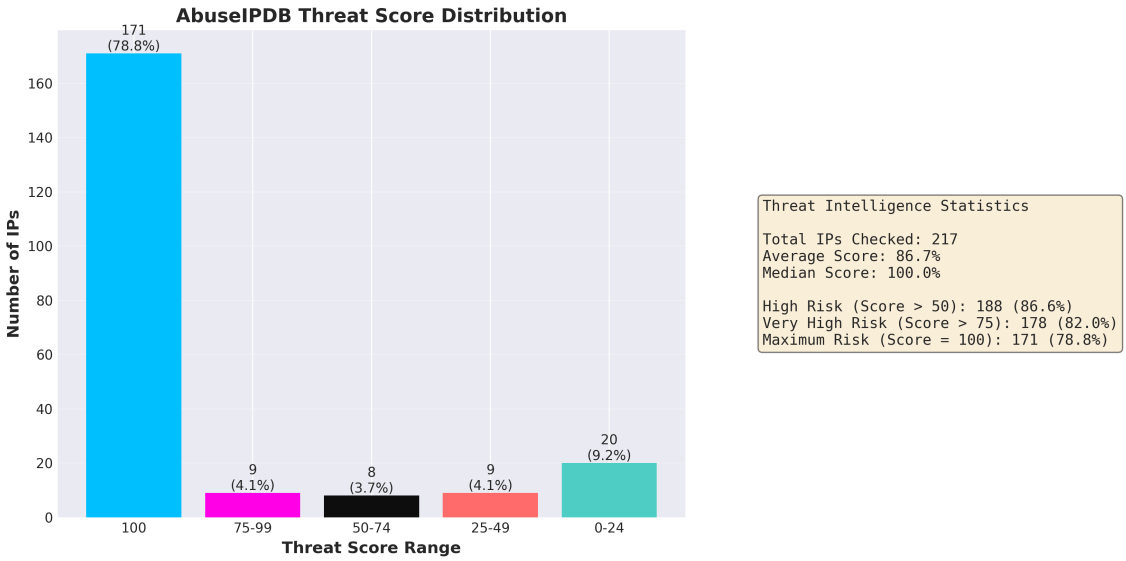

Figure 6: AbuseIPDB Threat Score Distribution and Statistics

Of the 217 IPs checked against AbuseIPDB:

- **Average threat score: 86.7%** (out of 100)
- **Median threat score: 100.0%** (most IPs are maximum risk)
- **IPs with score $>$ 50: 188** (86.6% of scored IPs)
- **IPs with score $>$ 75: 178** (82.0% of scored IPs)

Critical Finding: The vast majority of attacking IPs are already known malicious actors with high threat scores. This confirms that: 1. Threat intelligence feeds are highly effective at identifying malicious actors 2. Most attacks come from IPs that have been reported for abuse (86.6% scored above 50) 3. Integrating threat intelligence into security systems can significantly improve detection

7. Attacker Behavior & Sophistication

Automation Indicators

While client version fingerprinting data was not available in this dataset, multiple other indicators point to highly automated attack infrastructure:

1. **Attack Volume**: Over 27,000 connections in 8 days requires automation - human attackers cannot sustain this volume

2. **Repetitive Patterns**: Identical commands executed multiple times (42 Google requests, 12 Yahoo requests) indicate automated tools
3. **Concentration**: Extreme concentration from single IPs (70.3% from one IP) suggests automated scanning infrastructure
4. **Connection Duration**: Median duration of 1.15 seconds indicates rapid automated scanning rather than manual exploration
5. **Attack Timing**: Coordinated surges (77% of attacks in 2 days) suggest botnet activation rather than random human activity

Critical Finding: The attack patterns - high volume, repetitive commands, extreme concentration, and coordinated timing - all point to **sophisticated, automated botnet infrastructure, not human attackers or script kiddies**.

Top Attackers

The attack landscape is highly concentrated, as shown in Figure 8:

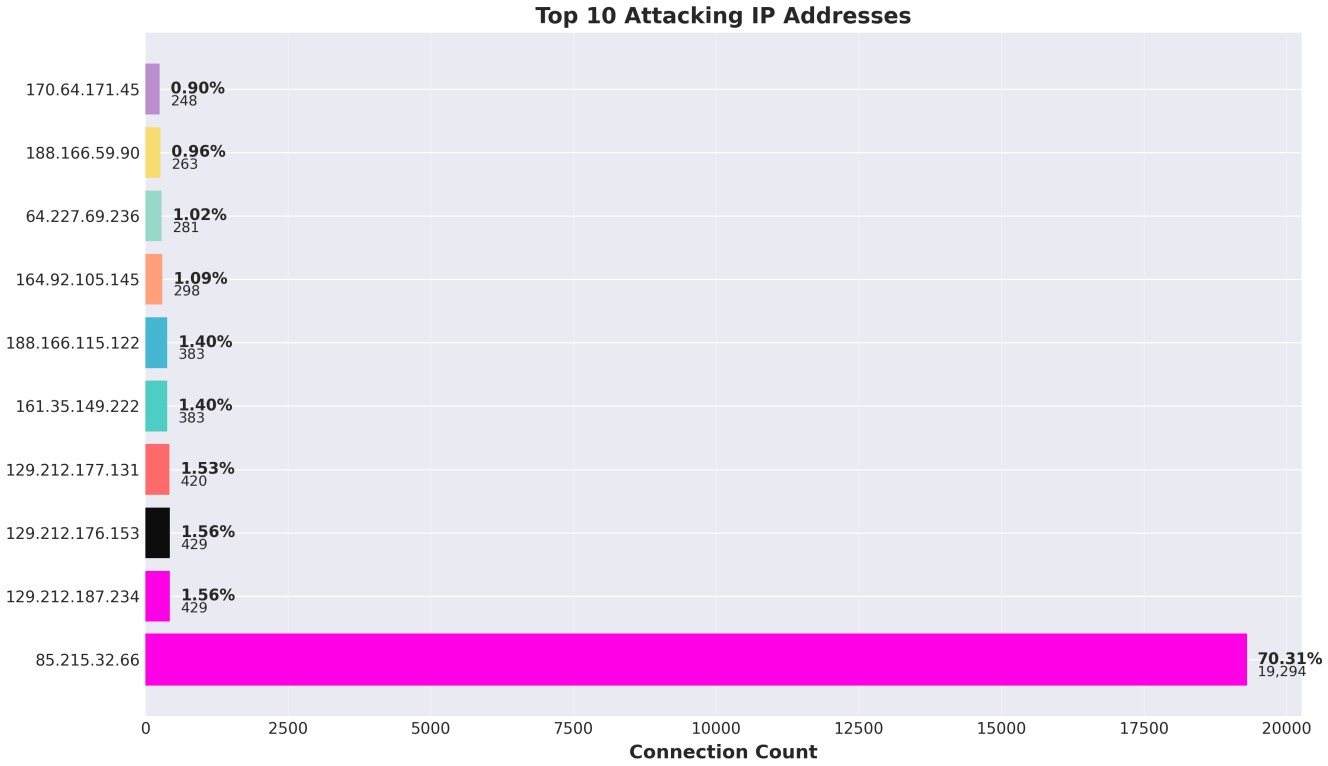

Figure 8: Top 10 Attacking IP Addresses

1. **85.215.32.66** (Germany) - 19,294 connections (70.3%)
2. **129.212.187.234** - 429 connections (1.6%)
3. **129.212.176.153** - 429 connections (1.6%)
4. **129.212.177.131** - 420 connections (1.5%)
5. **161.35.149.222** - 383 connections (1.4%)

Key Insight: The attack landscape is extremely concentrated, with a single IP (85.215.32.66) accounting for **70.3% of all connections**. The top 5 attackers account for **75.3% of all connections**. This concentration suggests either: - A single very aggressive botnet node or misconfigured scanner (the German IP) - Coordinated infrastructure (the 129.212.x.x IPs appear related) - Attackers using compromised high-bandwidth systems

The fact that one IP is responsible for over 70% of attacks is remarkable - blocking this single source would eliminate the majority of the threat.

Automation Indicators

Multiple indicators point to automated attacks:

1. **Attack Volume**: Over 27,000 connections in 8 days requires automation
2. **Repetitive Patterns**: Identical commands executed multiple times (42 Google requests, 12 Yahoo requests)
3. **Concentration**: Attack sources show significant concentration patterns
4. **Connection Duration**: Median duration of 1.15 seconds indicates rapid automated scanning

Connection Duration Patterns

The connection duration data reveals two distinct attack patterns:

- **Average duration**: 3.88 seconds
- **Median duration**: 1.15 seconds
- **Connections > 60 seconds**: 510 (1.86%)

Key Insight: Most attacks are quick automated scans - the attacker connects, tries a few passwords, and moves on. However, 510 connections lasted more than 60 seconds, suggesting successful compromises where attackers are actively using the system.

These longer connections are the most dangerous - they represent systems that have been successfully compromised and are now being used for malicious purposes (likely as proxy infrastructure, given the port forwarding data).

8. Security Insights & Recommendations

What the Data Tells Us

1. **Automated attacks dominate**: High-volume, repetitive attack patterns indicate botnet infrastructure, not human attackers. Defenses need to account for automated, high-volume attacks.
2. **Weak credentials are still effective**: Top 10 passwords account for 7.3% of attempts, with "123456" alone accounting for 796 attempts. Password policies and multi-factor authentication are critical.
3. **Default accounts are prime targets**: `root`, `admin`, and service accounts are heavily targeted. Disable or rename default accounts.
4. **Threat intelligence works**: 86.6% of attacking IPs are already flagged as high-risk (188 of 217 IPs). Integrate threat intelligence feeds into your security stack.
5. **Port forwarding is a red flag**: If you see port forwarding attempts, you may already be compromised. Monitor SSH tunnels closely.

Defensive Recommendations

Immediate Actions

1. **Implement fail2ban or similar**: Block IPs after multiple failed login attempts
2. **Use key-based authentication**: Disable password authentication where possible
3. **Change default ports**: Move SSH off port 22 to reduce automated scanning
4. **Implement rate limiting**: Limit connection attempts per IP
5. **Monitor for port forwarding**: Alert on SSH tunnel creation attempts

Strategic Recommendations

1. **Integrate threat intelligence**: Block known malicious IPs automatically using feeds like AbuseIPDB
2. **Use strong passwords or keys**: Enforce password complexity or require SSH keys
3. **Monitor connection durations**: Long connections may indicate successful compromises
4. **Disable default accounts**: Rename or disable `root`, `admin`, and service accounts
5. **Implement multi-factor authentication**: Add an additional layer of security beyond passwords

Best Practices

- **Regular security audits**: Review SSH access logs regularly
- **Network segmentation**: Isolate SSH services from critical systems
- **Intrusion detection**: Monitor for suspicious SSH activity patterns
- **Backup and recovery**: Ensure you can quickly recover from compromises
- **Security awareness**: Educate users about password security and phishing

Threat Intelligence Value

The data clearly demonstrates the value of threat intelligence:

- **86.6% of attacking IPs** are already flagged as high-risk (188 of 217 IPs scored above 50)
- **Average threat score of 86.7%** confirms these are known malicious actors
- **Integration with threat intelligence feeds** can significantly improve detection and blocking

Organizations should integrate threat intelligence feeds into their security infrastructure to automatically identify and block known malicious IPs.

---

9. Conclusion

This analysis of 27,443 real-world SSH attacks reveals a landscape dominated by automated botnet infrastructure, weak credential targeting, and sophisticated attack coordination. The sustained high-volume activity, repetitive attack patterns, and concentrated attack sources all point to the same conclusion: **modern SSH attacks are highly automated, well-coordinated, and operating at scale**.

Key Takeaways

1. **Automation is the norm**: Attack patterns indicate automated tools, not human attackers
2. **Weak credentials still work**: Top 10 passwords account for 7.3% of attempts, with "123456" being attempted 796 times
3. **Threat intelligence is effective**: 86.6% of attacking IPs are already flagged as high-risk (188 of 217 IPs)
4. **Volume over sophistication**: Low success rates (1.5%) but high attack volumes
5. **Proxy infrastructure is the goal**: Many attacks aim to create proxy networks, not direct compromise

The Good News

Despite the concerning findings, there's good news: **basic security measures are effective**. The 1.5% success rate shows that even simple defenses work. Strong passwords, key-based authentication, and threat intelligence integration can significantly reduce your attack surface.

Future Analysis Opportunities

This analysis represents a snapshot of SSH attacks over an 8-day period. Future analysis could explore:

- **Long-term trends**: How attack patterns change over months/years
- **Seasonal variations**: Do attacks increase during certain times?
- **Geographic shifts**: How do attack sources change over time?
- **Command evolution**: How do attacker commands change as they adapt?
- **Success rate correlation**: What factors correlate with successful compromises?

Call to Action

The key to effective defense is understanding your attackers. By analyzing their methods, tools, and patterns, we can build better defenses. That's what threat intelligence is all about - **turning attack data into actionable security insights**.

Organizations should: - **Deploy honeypots** to learn from attackers - **Integrate threat intelligence** into security systems - **Implement basic security measures** (strong passwords, key-based auth, rate limiting) - **Monitor for suspicious activity** (port forwarding, long connections, unusual commands) - **Share threat intelligence** to help protect the broader community

---

Appendix A: Complete Statistics

Connection Statistics

- Total connections: 27,443
- Unique IPs: 172
- Average per day: 3,430.4
- Peak day: November 29 (12,597 connections, 45.9% of total)

Authentication Statistics

- Total attempts: 27,179
- Successful: 419 (1.5%)
- Failed: 26,760 (98.5%)

Command Statistics

- Total commands: 55
- Connectivity tests: 54 (98.2%)
- System exploration: 1 (1.8%)

Threat Intelligence Statistics

- IPs checked: 217
- Average score: 86.7%
- Median score: 100.0%
- IPs with score > 50: 188 (86.6%)
- IPs with score > 75: 178 (82.0%)

Top 10 Attacking IPs

1. 85.215.32.66 - 19,294 connections (70.3%) - Germany
2. 129.212.187.234 - 429 connections (1.6%)
3. 129.212.176.153 - 429 connections (1.6%)
4. 129.212.177.131 - 420 connections (1.5%)
5. 161.35.149.222 - 383 connections (1.4%)
6. 188.166.115.122 - 383 connections (1.4%)
7. 164.92.105.145 - 298 connections (1.1%)
8. 64.227.69.236 - 281 connections (1.0%)
9. 188.166.59.90 - 263 connections (1.0%)
10. 40.90.161.91 - 248 connections (0.9%)

Document Version: 1.0
Analysis Period: November 24 - December 1, 2025 (8 days)
Data Collection: Cowrie SSH Honeypot with Threat Intelligence Enrichment
Author: Matt Shore
Website: https://mattshore.co.uk