# Catch-22: Uncovering Compromised Hosts using SSH Public Keys

Cristian Munteanu*, Georgios Smaragdakis^,

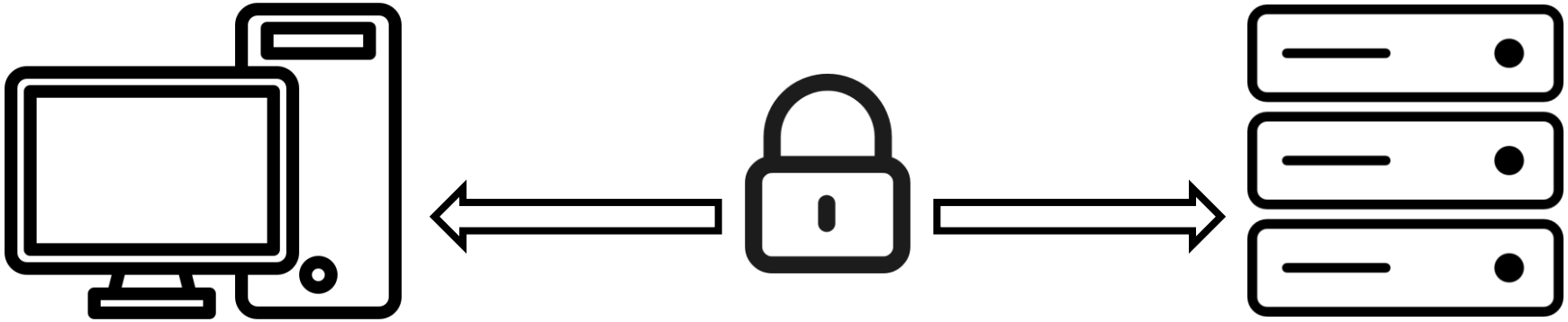
**Anja Feldmann***, Tobias Fiebig*

**Max Planck Institute for Informatics, ^Delft University of Technology*

# Secure SHell

Introduced in 1995

Used to securely connect to remote machines



Today: > **40 million** machines run SSH servers

# Compromised SSH

**SSH** is a popular target

Malicious actor also use it

- for **access**
- for **control**

# Compromised SSH

**SSH** is a popular target

Malicious actor also use it

- for **access**
- for **control**

# Compromised SSH

**SSH** is a popular target

Malicious actor also use it

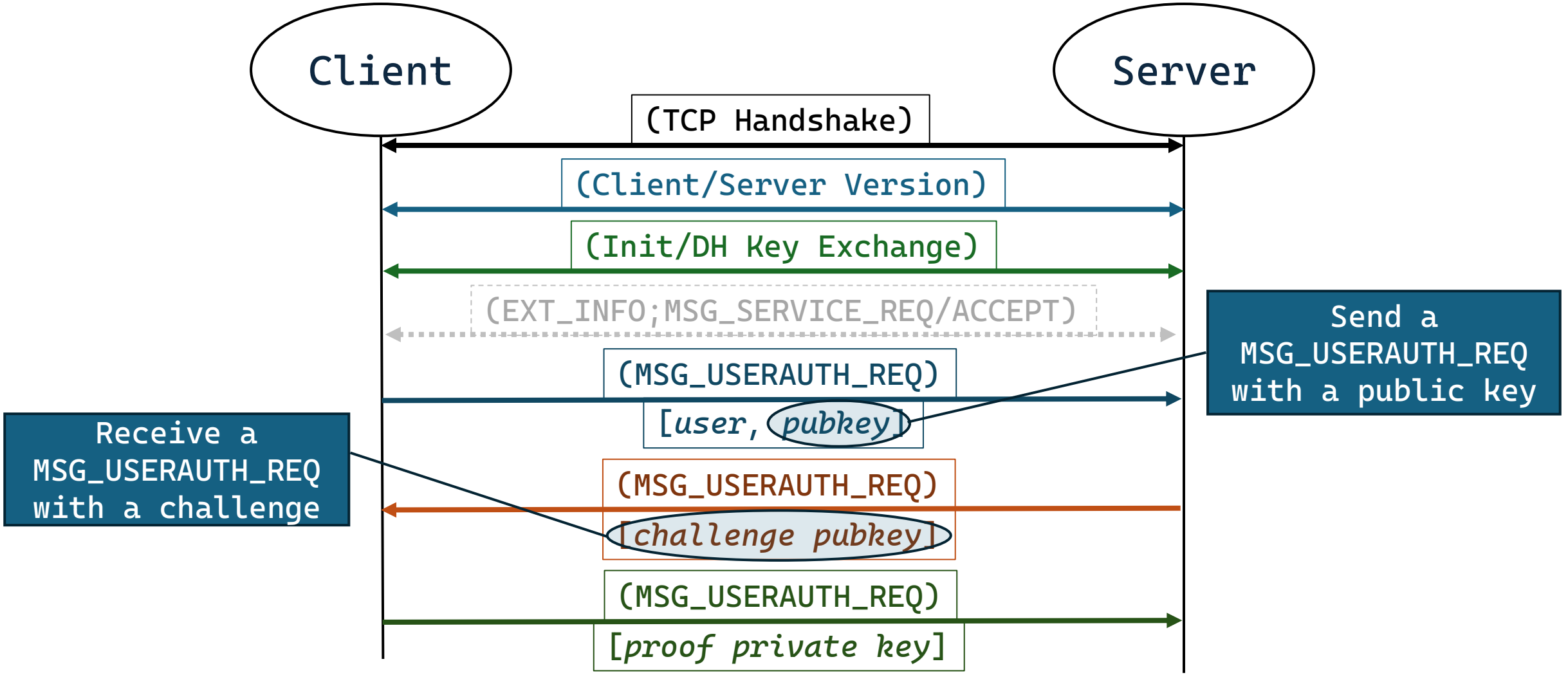
- for **access**
- for **control**

Installation of an **SSH** public key recorded by a honeypot

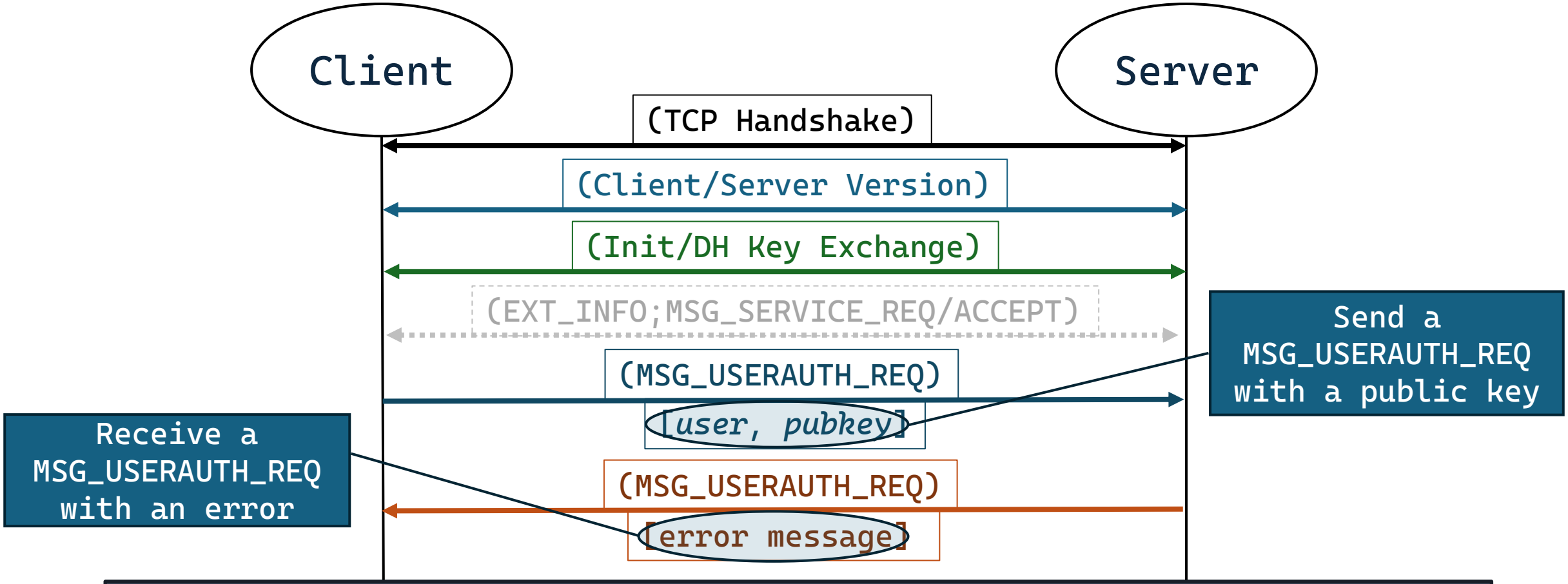
```
> # cd ~; chattr -ia .ssh; lockr -ia .ssh
> # cd ~ && rm -rf .ssh && mkdir .ssh &&
      echo "ssh-rsa AAAAB3....+oRw== mdrfckr">>.ssh/authorized_keys    &&
chmod -R go= ~/.ssh && cd ~
```

# Can we identify compromised systems?

# Recall: SSH handshake



# Recall: SSH handshake




The Client will receive a challenge for the key ONLY when the public key exists on the Server!

# Scan tool to find compromised hosts

1. Use **ZMap** to scan for open ssh ports
2. Use patched **ZGrab2** as “ssh client”
   - Send MSG_USERAUTH_REQ [*user*, *pubkey*]

# Scan tool to find compromised hosts

1. Use **ZMap** to scan for open ssh ports
2. Use patched **ZGrab2** as “ssh client”
   - Send MSG_USERAUTH_REQ [*user*, *pubkey*]
     1. Send **“*canary key*”** *(new generated key)*
     2. *Send “malicious key” (to find compromised hosts)*

***(If server accepts the “canary key” it is considered misconfigured (or a honeypot))***

# In-lab Testing

Tested the tool on:

- OpenSSH *v9.4-v2.1.1*
- Dropbear *v0.84-v0.23*
- BitviseSSH *v9-v6*
- WolfSSH *v1.4*

*Works on all versions deployed after 2005*

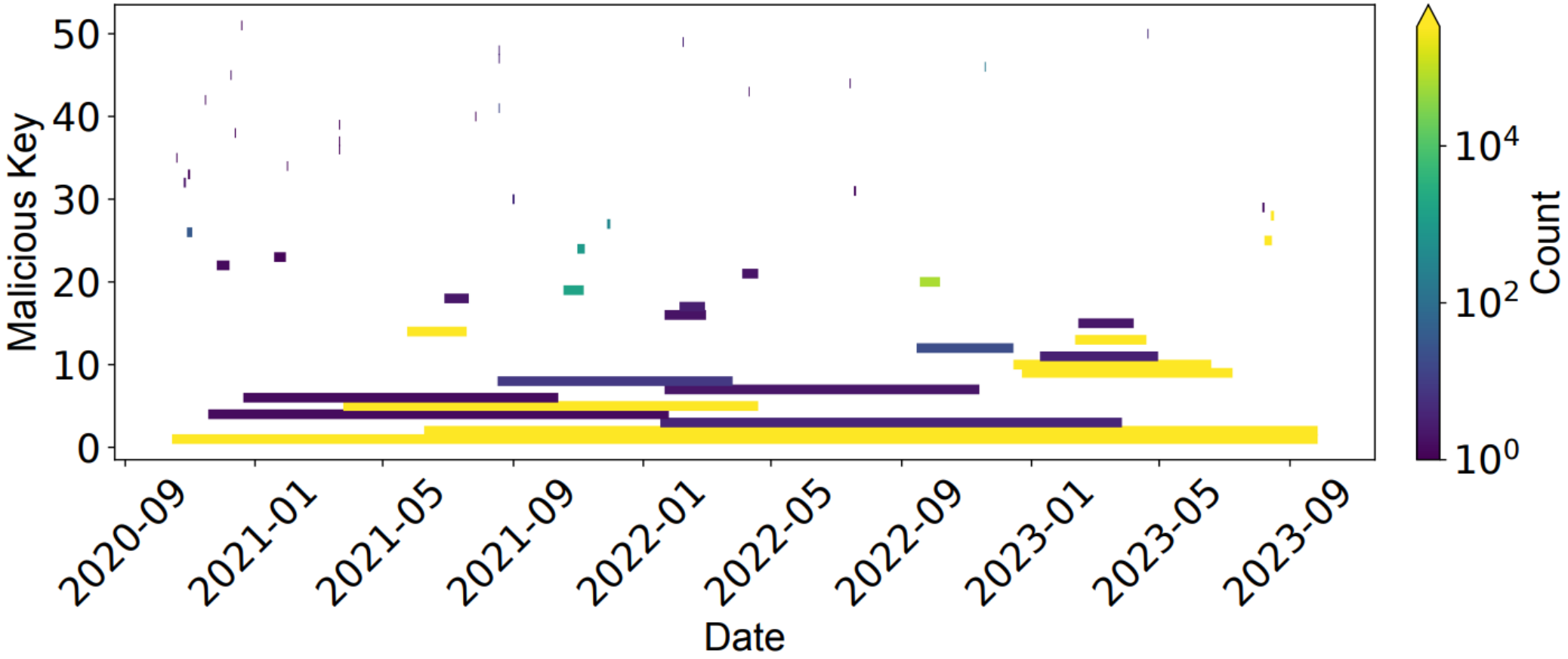
| | Year | Censys (all ports) 2024-04-16 | Our Scan (22, 2222) 2024-04-05 | Censys (22, 2222) 2024-04-24 | Deployment | Zmap | Zgrab2 | PubKey Login |
|---|---|---|---|---|---|---|---|---|
| **OpenSSH:** | | | | | | | | |
| 9.4 | 2024 | <0.01% | <0.01% | <0.01% | ✓ | ✓ | ✓ | ✓ |
| ... | 2016-2024 | 29.21% | 22.7% | 46.1% | ✓ | ✓ | ✓ | ✓ |
| 7.4 | 2016 | 23.01% | 17.00% | 18.08% | ✓ | ✓ | ✓ | ✓ |
| ... | 2001-2016 | 22.28% | 12.3% | 6.17% | ✓ | ✓ | ✓ | ✓ |
| 3.0 | 2001 | <0.01% | <0.01% | <0.01% | ✓ | ✓ | ✓ | ✓ |
| 2.9 | 2001 | <0.01% | <0.01% | <0.01% | ✓ | ✓ | ✗ | ✗ |
| ... | 2000-2001 | <0.01% | <0.01% | <0.01% | ✓ | ✓ | ✗ | ✗ |
| 2.1.1 | 2000 | <0.01% | <0.01% | <0.01% | ✓ | ✓ | ✗ | ✗ |
| **Dropbear:** | | | | | | | | |
| 0.84 | 2024 | <0.01% | <0.01% | <0.01% | ✓ | ✓ | ✓ | ✓ |
| ... | 2019-2024 | 2.42% | 0.91% | 0.77% | ✓ | ✓ | ✓ | ✓ |
| 0.78 | 2019 | 8.36% | 10.01% | 12.74% | ✓ | ✓ | ✓ | ✓ |
| ... | 2005-2019 | 3.51% | 1.23% | 3.80% | ✓ | ✓ | ✓ | ✓ |
| 0.47 | 2005 | <0.01% | <0.01% | <0.01% | ✓ | ✓ | ✓ | ✓ |
| 0.46 | 2005 | <0.01% | <0.01% | <0.01% | ✗ | ✗ | ✗ | ✗ |
| ... | 2004-2005 | <0.01% | <0.01% | <0.01% | ✗ | ✗ | ✗ | ✗ |
| 0.44 | 2004 | <0.01% | <0.01% | <0.01% | ✗ | ✗ | ✗ | ✗ |
| 0.43 | 2004 | <0.01% | <0.01% | <0.01% | ✓ | ✓ | ✓ | ✓ |
| ... | 2003-2004 | <0.01% | <0.01% | <0.01% | ✓ | ✓ | ✓ | ✓ |
| 0.39 | 2003 | - | - | - | ✓ | ✓ | ✓ | ✓ |
| 0.38 | 2003 | <0.01% | <0.01% | - | ✗ | ✗ | ✗ | ✗ |
| ... | 2003 | <0.01% | <0.01% | <0.01% | ✗ | ✗ | ✗ | ✗ |
| 0.23 | 2003 | <0.01% | - | - | ✗ | ✗ | ✗ | ✗ |
| **BitviseSSH:** | | | | | | | | |
| 9.31 | 2023 | <0.01% | - | <0.01% | ✓ | ✓ | ✓ | ✓ |
| 9.29 | 2023 | <0.01% | - | <0.01% | ✓ | ✓ | ✓ | ✓ |
| 8.49 | 2021 | <0.01% | - | <0.01% | ✓ | ✓ | ✓ | ✓ |
| 7.46 | 2018 | <0.01% | - | <0.01% | ✓ | ✓ | ✓ | ✓ |
| 6.51 | 2018 | <0.01% | - | <0.01% | ✓ | ✓ | ✓ | ✓ |
| **WolfSSH:** | | | | | | | | |
| 1.4.14 | 2023 | <0.01% | <0.01% | <0.01% | ✓ | ✓ | ✓ | ✓ |

# Ethical Considerations

- Follow MENLO Report
  - Rate limiting
  - Blocklist
  - 24/7 availability
  - Project webpage
  - Suggestive Reverse DNS entry
- Approved by IRB

Bitdefender

# Malicious Keys (as seen by Bitdefender)

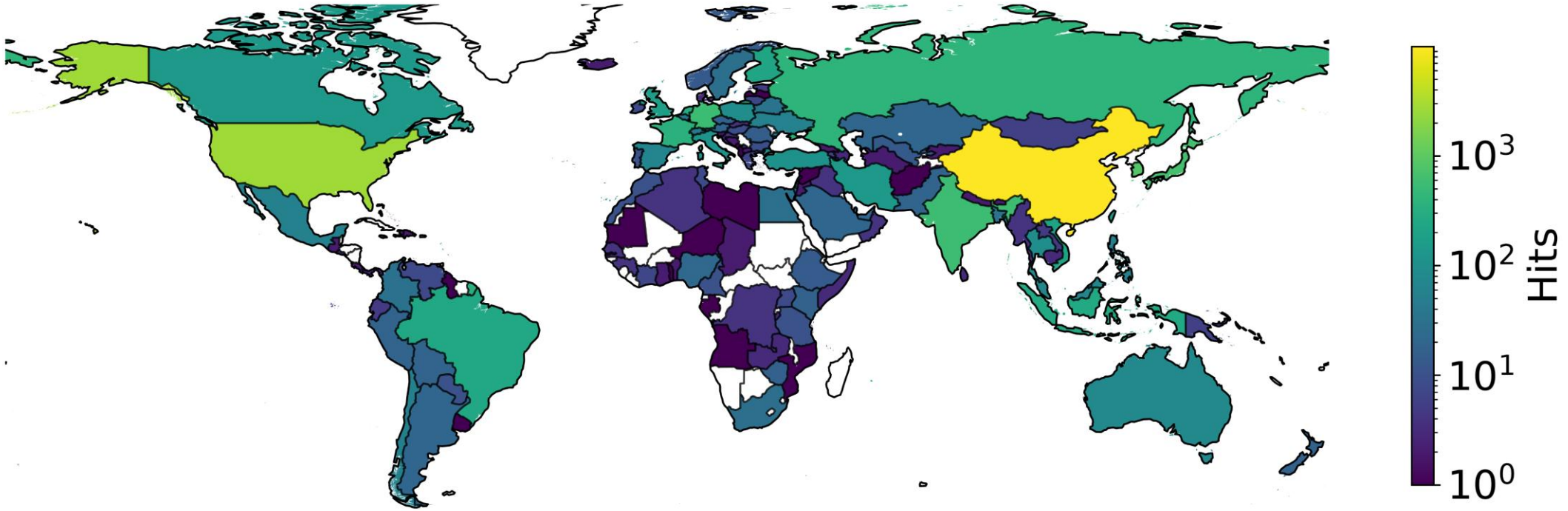


# Our Scan for compromised hosts

- Scan **port 22** and **port 2222**
- Use **3** usernames: *“root”*, *“admin”,* and *“udatabase”*
- Use **52** known to be malicious public SSH keys
- Scanned both **IPv4** and **IPv6** (hitlist)
- Started on 04.04.2024
- Scan still ongoing

# We can identify compromised systems!

# Results: 21,700 Hits



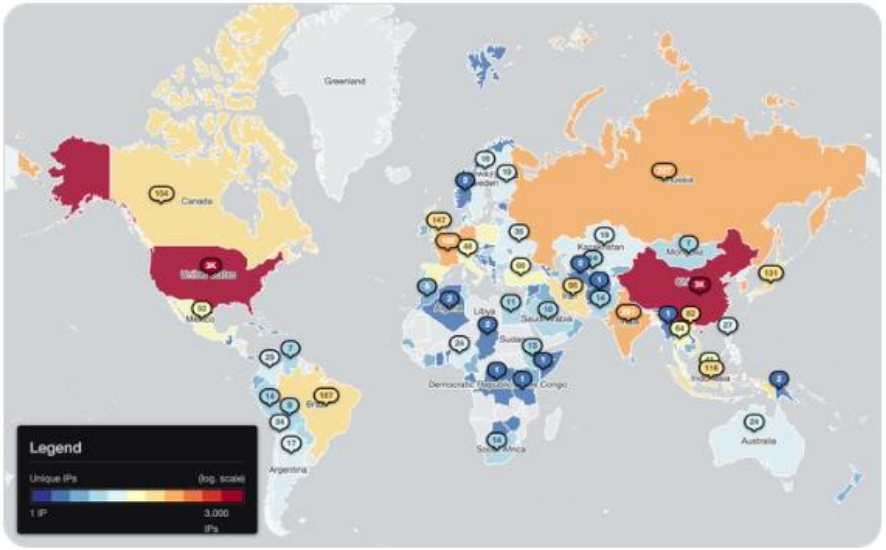

Port 22 and 2222 scans between April-August 2024

# Notifications – Examples

**The Shadowserver Foundation**
@Shadowserver

Heads up! We are sharing out a second Special Report on Compromised SSH hosts detected through leakage of malicious public SSH keys placed on them by attackers: shadowserver.org/what-we-do/net...

This time 10020 compromised hosts found. Top countries US (3K), China (2.9K), Singapore (423)

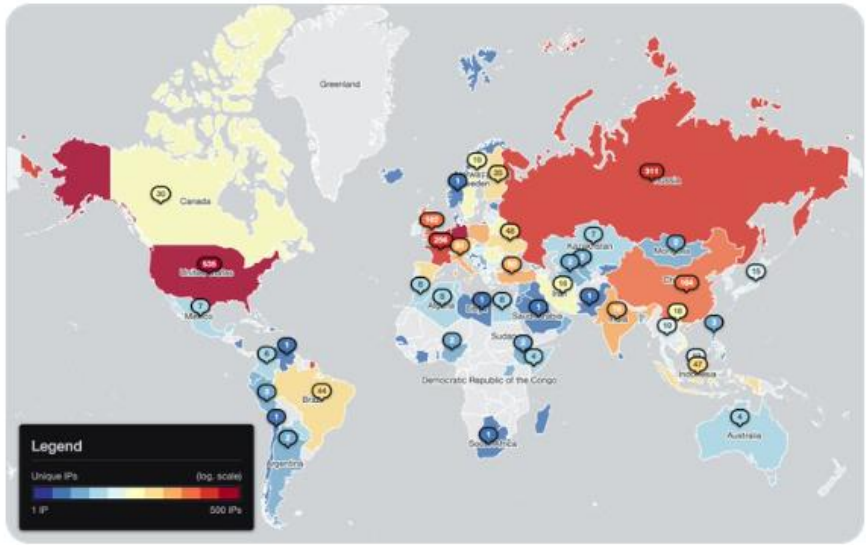



**The Shadowserver Foundation**
@Shadowserver

We are sharing out a Special Report on Compromised SSH hosts detected through leakage of malicious public SSH keys placed on them by attackers: shadowserver.org/what-we-do/net...

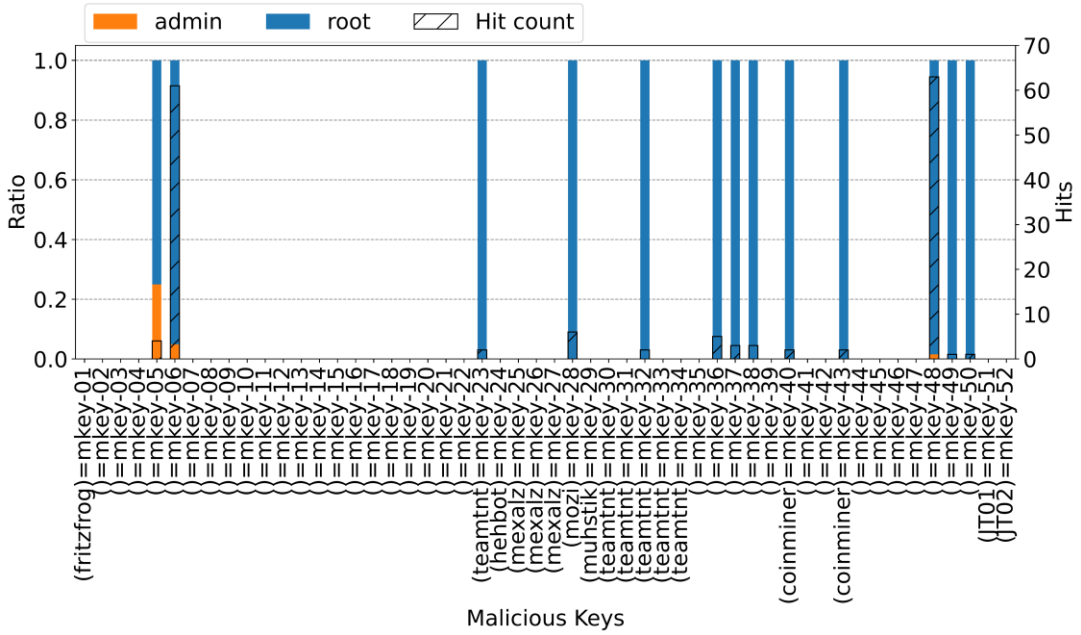
3327 compromised hosts detected on IPv4/IPv6 using this methodology.

For background: rushter.com/blog/public-ss...

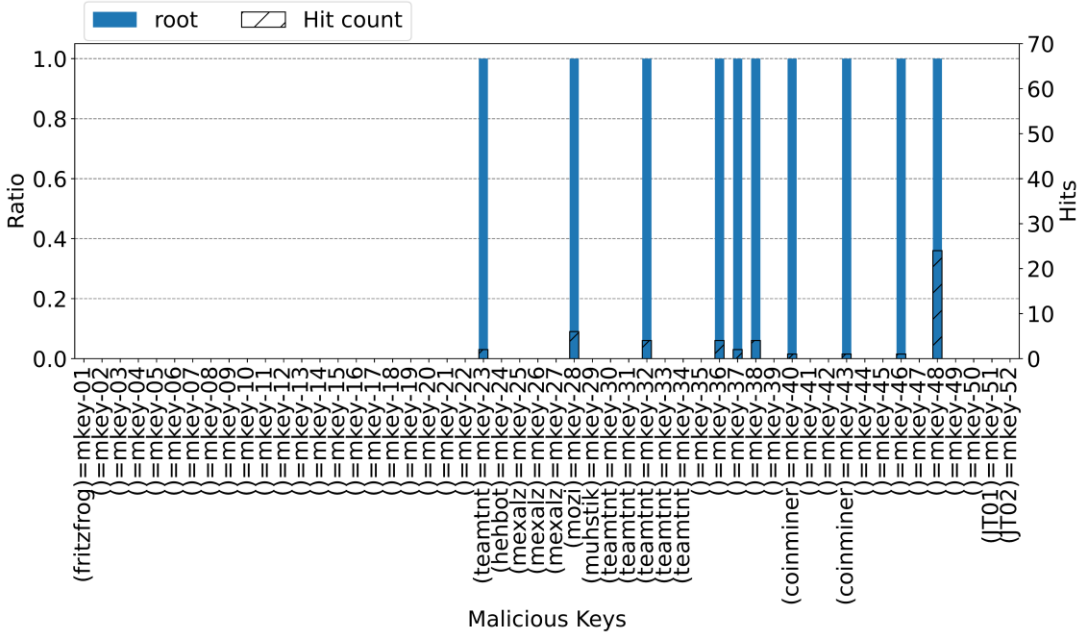


# Effects of our scans: Case of an EU Hosting Provider

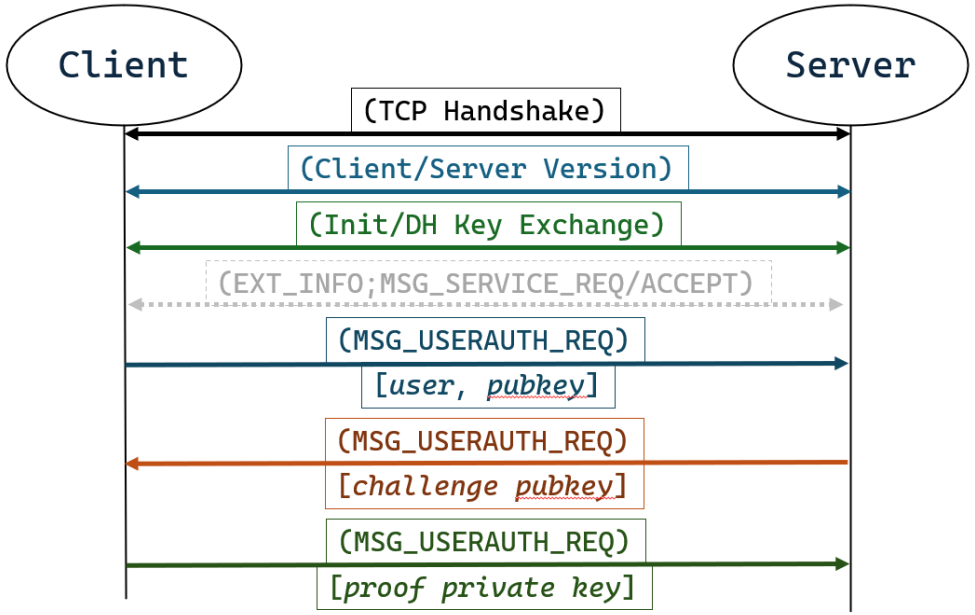
## First Scan Round – 152 hits



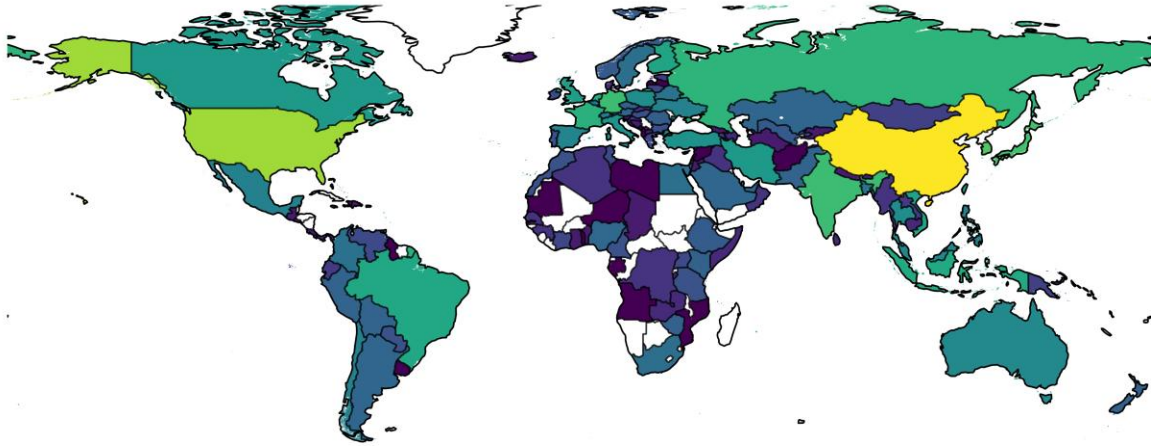

## Second Scan Round – 36 hits



# Conclusion




Found more than 21,700 (16,000) compromised hits (unique ssh hostkeys)!



Designed a tool that can find compromised ssh servers