ILLINOIS
CSL | Coordinated Science Lab
COLLEGE OF ENGINEERING

# Mining Threat-intelligence from Billion-scale SSH Brute-Force Attacks

**Yuming Wu[1§],**

Phuong M. Cao[1§], Alexander Withers[2], Zbigniew T. Kalbarczyk[1], Ravishankar K. Iyer[1]

**[1] University of Illinois at Urbana-Champaign (UIUC)**

**[2] National Center for Supercomputing Applications (NCSA)**

csl.illinois.edu

[§] Joint first authors

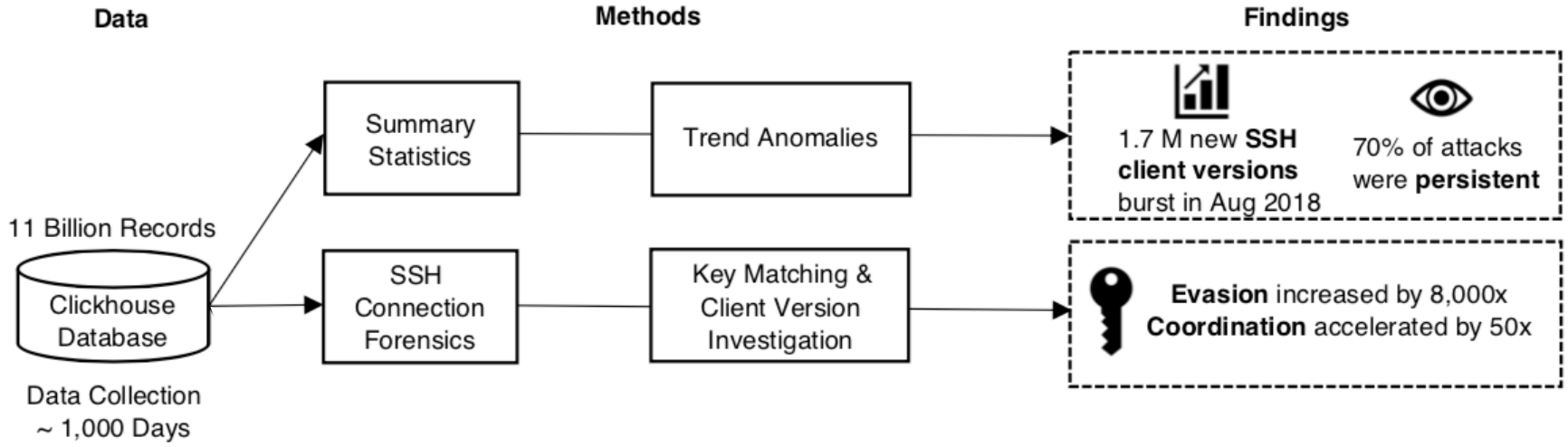
# Key Findings

- Over **70%** are persistent attackers
- Identification of **7** SSH keys related to outdated vulnerabilities
- Globally distributed IPs massively spoofed over **one million** fake client versions
- Discovery of **human-supervised** versus **fully automated** botnets

# Implications

- Discerning global coordination efforts in SSH key exploitation and client version spoofing
- Alerting cloud providers and IoT vendors regarding stolen SSH keys
- Deterring large-scale evasion techniques using anomaly detectors or rate limiters
- Preparing for resourceful and strategic human-supervised attacks

# Analysis Workflow



# Exploitation, Coordination, and Evasion - *Leaked SSH Keys*

| SSH Key (SHA256) | Key Owner | Appliance Type | Public Disclosure Year | 1st Attack Attempt Year | Username |
|---|---|---|---|---|---|
| 1M4Rz...quOZA | Vagrant | Base box for development environments | 2010 | 2018 | root |
| 9prMb...Ghro4 | F5 | BigIP appliances | 2012 | | |
| MEc4H...UfTww | Loadbalancer | Virtual load balancer | 2014 | | |
| VtjqZ...PiQPc | Quantum | Virtual deduplication backup appliance | | | |
| /JLp6...POCc0 | Array Networks | Virtual application delivery controllers<br>Secure access gateways | | | sync |
| Z+q4X...8kIxM | Ceragon | IP traffic router | 2015 | | mateidu |
| f+1oG...zEDhc | VMware | Data Protection appliances | 2016 | | admin |

- We identified 7 keys related to outdated vulnerabilities – indicating some devices still unpatched

*Attackers had adequate details (i.e., credentials) about relevant vulnerabilities that were related with these 7 keys, when plotting the targeted attacks*

# Exploitation, Coordination, and Evasion - *Leaked SSH Keys: Attack Origins*

| Autonomous System | Client Version [SSH-2.0-] | SSH Key (SHA256) & Key Owner | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 1M4Rz... | 9prMb... | MEc4H... | VtjqZ... | /JLp6... | Z+q4X... | f+1oG... |
| | | Vagrant | F5 | Loadbalancer | Quantum | Array Networks | Ceragon | VMware |
| Google LLC | libssh_0.7.0 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Charter Communications | Ruby/Net::SSH... | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Portlane | libssh-0.6.1 | | | ✓ | ✓ | | | |

Ruby/Net::SSH...refers to Ruby/Net::SSH_5.0.2 x86_64-linux-gnu.

- Attackers leveraged Google LLC (Google), Charter Communications, and Portlane to exploit the 7 identified leaked keys
  - Attackers from Google-registered IPs attempted all 7 keys with four other unknown keys on the same day

*Speculation: Attackers were rapidly switching ASes to evade detection, and possibly switching targets*

# Exploitation, Coordination, and Evasion - *Key-based Collaboration*

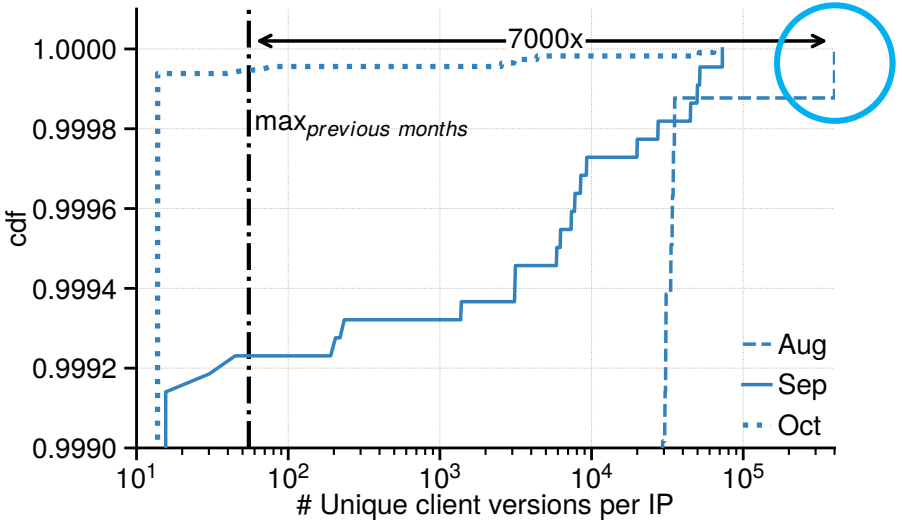
- An SSH key was exploited by 20 countries
  - The globally coordinated botnet exploited a single SSH key 90 times within only 4 days
- The last key was persistently used one single country for 2,700 times spanning 5 months

| SSH Key (SHA256) | # Countr(y/ies) | # AS(es) | # IPs | Client Version [SSH-2.0-] |
|---|---|---|---|---|
| **qlIN/...** | **20** | **38** | **64** | **Go** |
| B6kr4... | 1 | 1 | 25 | libssh-0.5.2 |
| mumiE... | | | 49 | |
| jSCqa... | | | 42 | |
| V6OOC... | | | 28 | |
| zPA6Y... | | | 23 | |
| NH5Y7... | | | 19 | |
| OyHmn... | | | 17 | |
| 8blLD... | | | 16 | |
| +UJNI... | | | 71 | kthrssh__x00 |

*The globally coordinated bot wrapped up its fruitless attacks and shifted targets 50× faster than the persistent, single-country botnet*

# Exploitation, Coordination, and Evasion
# - *Client Version-based Collaboration and Evasion*

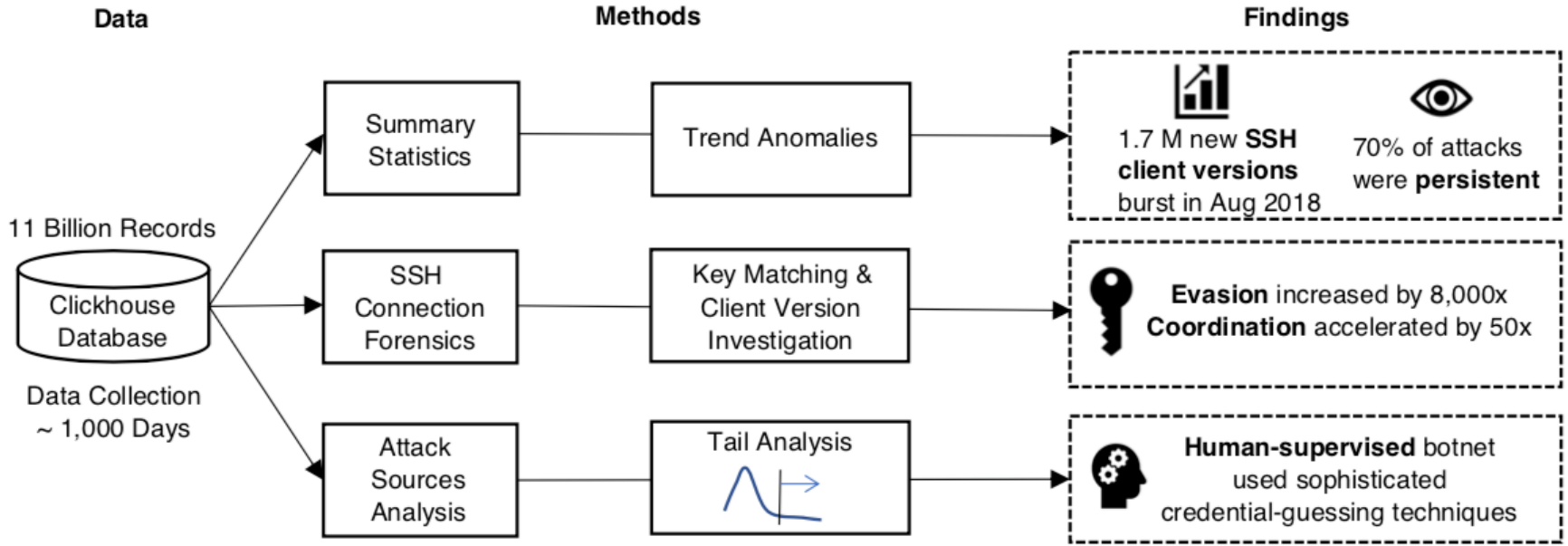
- More than 1.7 million new client versions were spoofed in August alone
  - Only several hundred globally-distributed IPs were spoofing (e.g. SSH-2.0-OpenSSH_+qLfH)
  - Yet 90% IPs used only 1 client version
  - The top-spoofing IP advertised 400,000 unique client versions during its 200-hour attack campaign



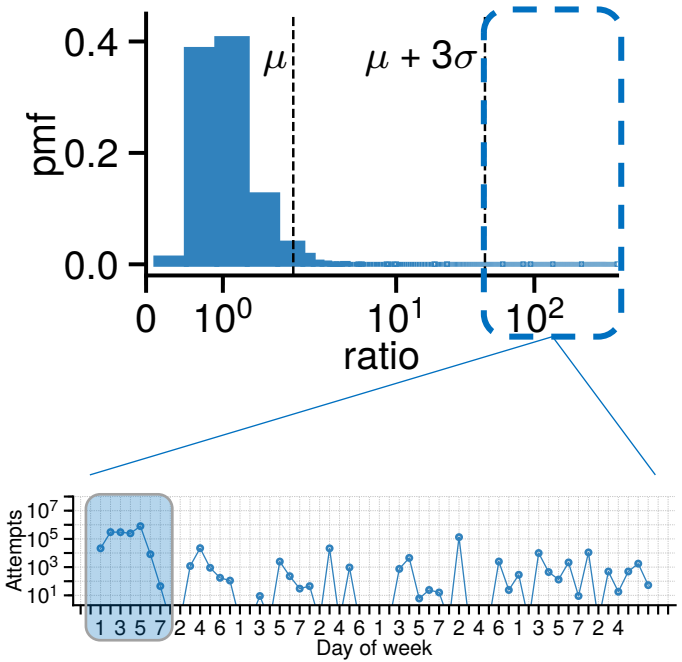

*A globally-coordinated botnets were involved in forging a million permutations of client versions at high frequencies*

*Voids signature-based detectors*

# Analysis Workflow



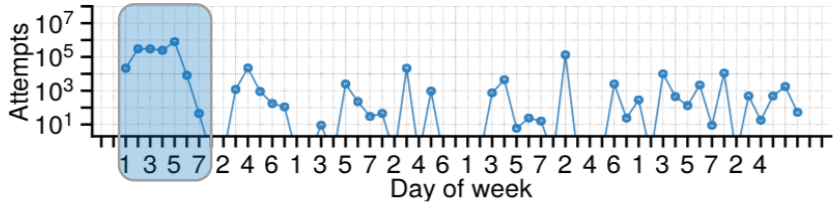
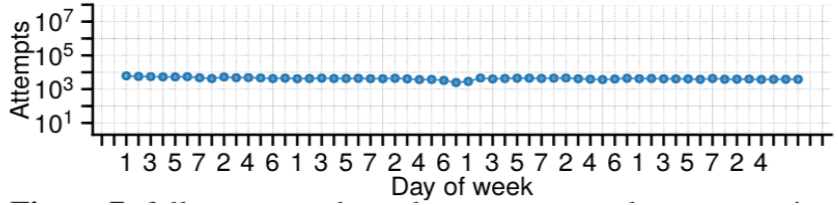
# Human-supervised Attack Techniques
# - *Data-driven Methodology*




Purpose: identify evidence of human attackers

- Time zone and duration selection
- Ratio: average weekday to weekend attempt computation for each IP
- Tail analysis of ratio distribution
- All IPs in the tail present similar activity patterns; used the same group of credentials; came from the same /8 subnet
  - Periodic variations with decreasing activities on weekends (especially Sundays)

# Human-supervised versus Fully Automated Bots

| Type | Illustration of Daily Attempts [May 27 – July 21, 2019 (8 weeks)] | List of Unique Client Versions [SSH-2.0-] | List of Unique Username(s) | # Unique Passwords |
|---|---|---|---|---|
| **Human-supervised** |   | PuTTY<br>OpenSSH_5.3<br>OpenSSH_6.2p2...<br>nsssh2_4.0... | root | 35,952 |
| **Fully automated** |   | sshlib-0.1 | root, user, admin, ubnt, usuario, pi, supervisor, support, service, mother | 42 |

OpenSSH_6.2p2... refers to OpenSSH_6.2p2 Ubuntu-6;
nsssh2_4.0... refers to nsssh2_4.0 NetSarang Computer, Inc.

*Human-supervised botnet is more resourceful, ambitious, and strategic than full automated one*

# Conclusions

- Investigated a broad scope of SSH attack strategies
- Discovered large-scale, persistent, and evasion attacks
- Contributed a scientific data-driven approach to differentiate between human-supervised and fully automated botnet

# Future

- Landscape of unidentified, unknown SSH keys
- Resourceful attackers with relatively large number of legitimate client versions
- Threat intelligence sharing across peer sites with preservation of privacy

# Thank you!

# Acknowledgements


- SDAIA: https://wiki.ncsa.illinois.edu/display/cybersec/SDAIA

- NSF Grant: CICI: Secure Data Architecture: Shared Intelligence Platform for Protecting our National Cyberinfrastructure. Award Number: 1547249

- NSF Grant: SI2-SSE: AttackTagger: Early Threat Detection for Scientific Cyberinfrastructure. Award Number: 1535070

- DEPEND group Symphony Cluster

# References


- “Ssh bad keys,” 2017, https://github.com/rapid7/ssh-badkeys.
- “Packet storm,” 2019, https://packetstormsecurity.com/.