|  |  |
| --- | --- |
| **SUBJECT LINE** | MCTI CTF -TEAM BEASTS (Bisrat Dereje Kura & Xiaohai Wang) |
| **TLP** | **AMBER+STRICT** |
| **DATE** | February 26th 2025 |

***Please ensure track changes is on.***

**THE THREAT (Executive Summary)**

*Add a description (paragraph or bullet form) that describes the nature and origin of the threat.*

|  |
| --- |
| The Canadian Center for Cyber Security (CCCS), in coordination with various intelligence sharing partners, has identified a persistent hacktivist campaign targeting government organizations and private industry in Canada. The hacktivist collective EvAnon is actively calling for attacks to be performed against Canadian organizations; the group has stated that attacks are “in response to a failure by the Canadian government and companies to address global warming”. EvAnon is actively recruiting and promoting the campaign via their private Telegram channel. To date, observed attacks have specifically impacted Linux devices and resulted in the theft of data and its public release.  Organizations impacted by this campaign are at risk of the loss of sensitive data, reputational damage, and follow on attacks based on stolen information. Canadian companies are strongly recommended to hunt for known attacker tools and techniques. |

**Recommended Actions**

*Bullet form list.*

|  |
| --- |
| * Protect against common initial access methods:   + Ensure all accounts are protected via Multi-Factor Authentication (MFA)   + Enforce strict password policies   + Review Internet-facing applications and ensure they are up to date on security patches * Identify and investigate any use of the PSPY tool |

**Additional information**

*Useful context, referential information or related website info in bullet and/or paragraph form.*

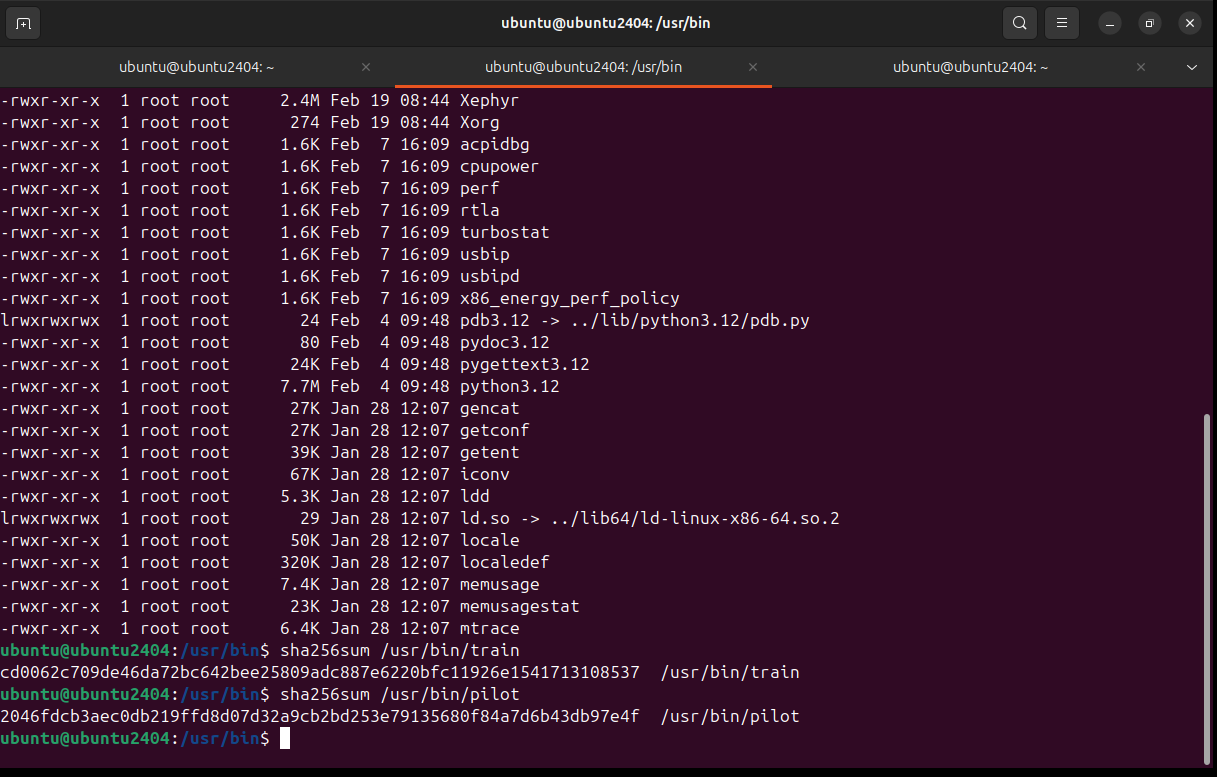
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Investigations into real-world attacks related to EvAnon activity are ongoing at the time of writing. The group is known to perform SSH BruteForce attacks against Internet-facing services for initial access into victim organizations. EvAnon has been observed both using and recommending the use of popular VPN services to obfuscate the source of malicious activity.  EvAnon is recommending that participating hacktivists make use of the open-source command line snooping tool PSPY. PSPY is designed to enable process snooping on Linux devices without the need to establish root privileges, by gathering information from procfs scans. CCCS is aware of recent attacks which included PSPY to enable privilege escalation and lateral movement.   |  |  | | --- | --- | | Indicators of Compromise | | | AS9009 | Autonomous System Numbers (ASA) | | Hash\_Breaker | Hex Value | | TekDestroyer | Username | | 146.70.65.142 | IP Address | | **99b1ff8f11781541f7f89f9bd41c4a17** | Flag |   References:  [1] https://github.com/DominicBreuker/pspy |

**Threat Intelligence Report Summary:**During our investigation multiple suspicious binaries were identified within the /usr/bin directory of an Ubuntu 24.04 system. Further investigation linked these files to the PSPY tool, a known Linux hack tool used for privilege escalation and process monitoring.

Analysis of the authentication logs (auth.log) revealed unauthorized SSH login attempts, indicating that initial access may have been achieved via brute-force attacks or credential stuffing techniques. The logs also showed privilege escalation activities and execution of potentially malicious commands that align with PSPY's behavior.

**Technical Details:**

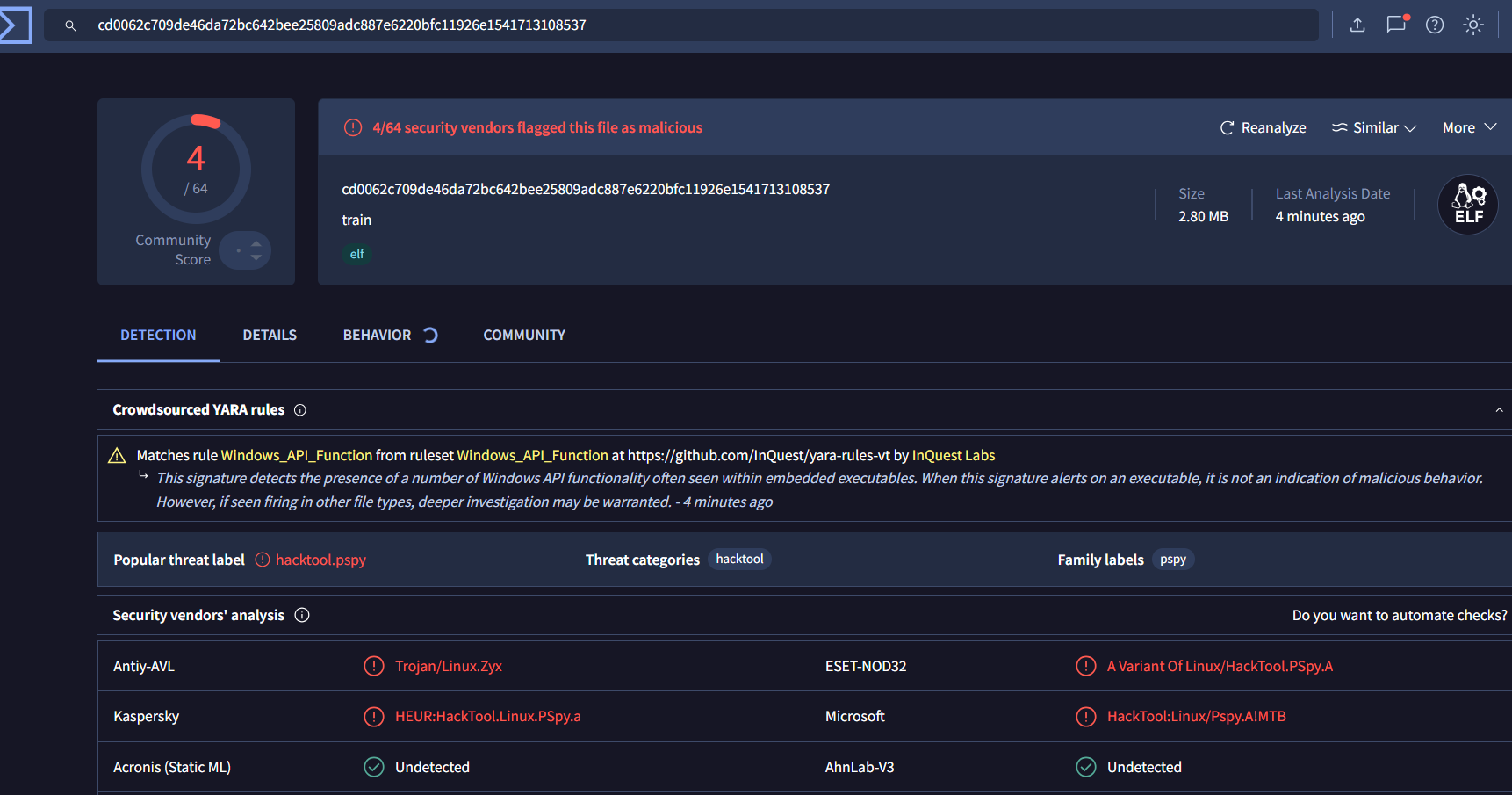
* **System Affected:** Ubuntu 24.04
* **Malicious Files Identified:**
  + /usr/bin/train
  + /usr/bin/pilot
* **SHA256 Hashes:**
  + train: cd0062c709de46da72bc642bee25809adc887e6220bfc11926e1541713108537
  + pilot: 2046fdcb3aec0db219ffd8d07d32a9cb2bd253e79135680f84a7d6b43db97e4f

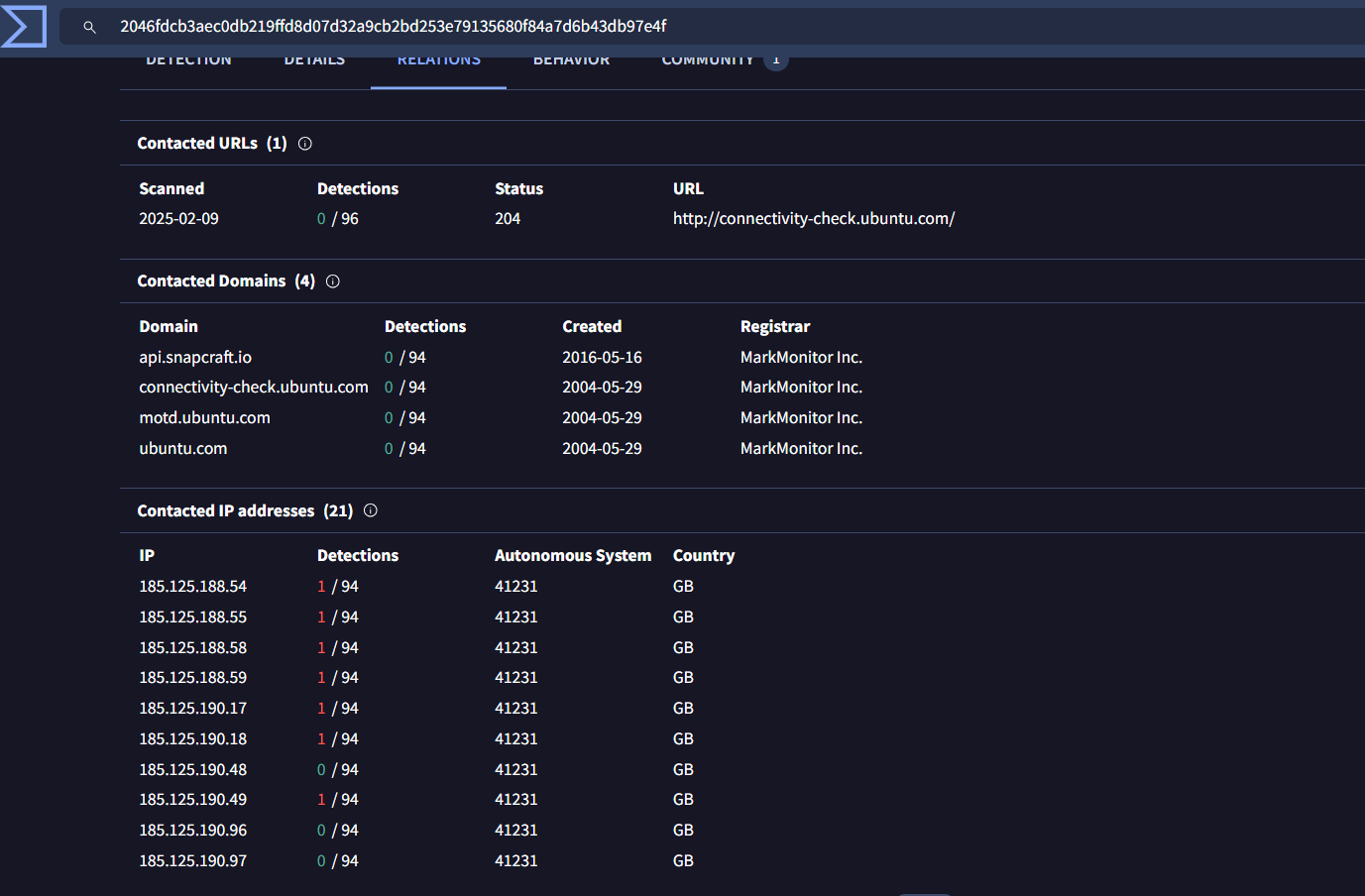
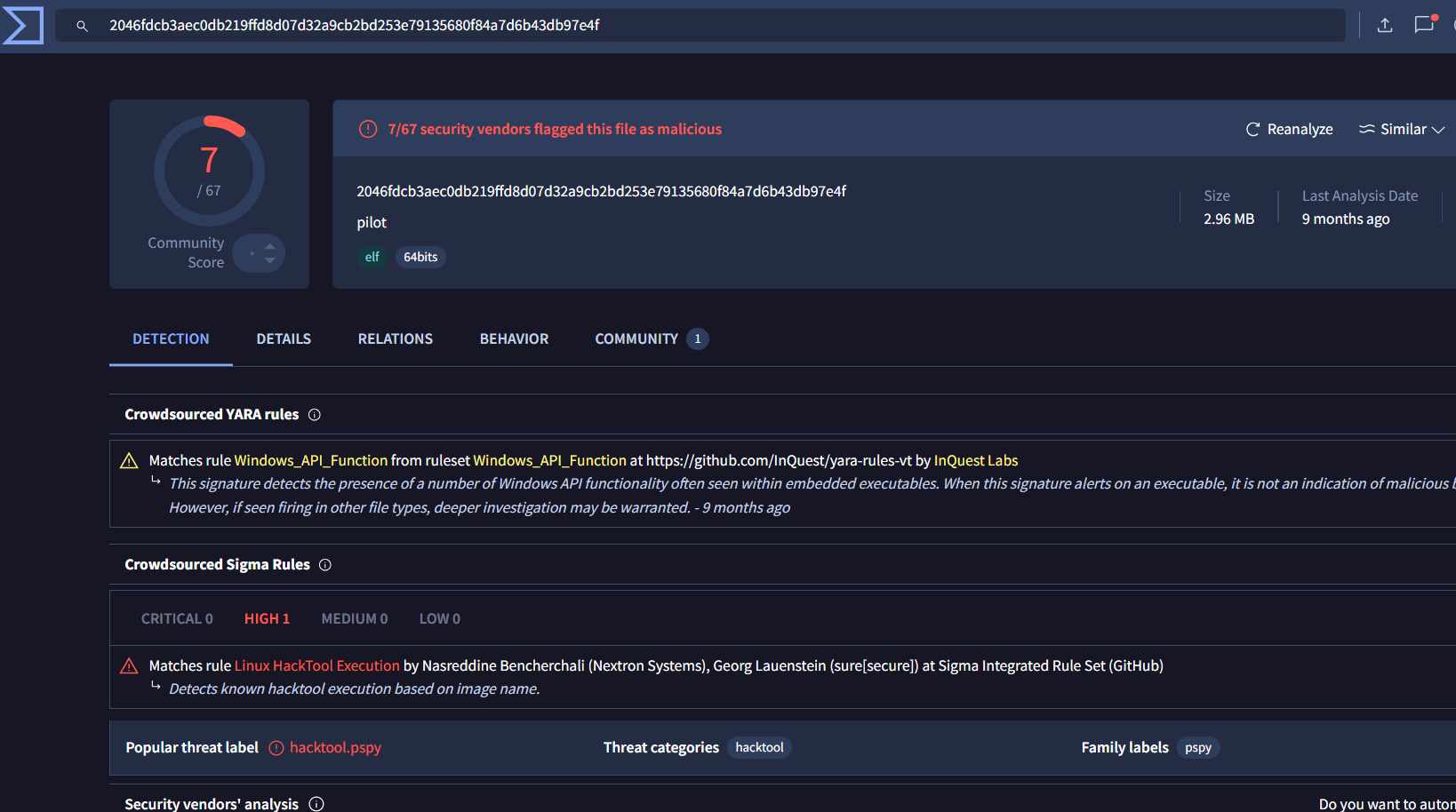


**Detection Methods:**

**VirusTotal Scan Results:**

* + pilot was flagged by 7/67 vendors as malicious, classified under HackTool.PSPY
  + train was flagged by 4/64 vendors, also linked to HackTool.PSPY
  + Both files matched YARA rule signatures detecting Hash\_Breaker behavior, confirming PSPY usage.





**YARA Rule Used:**

rule Detect\_PsPy\_HashBreaker {

meta:

description = "Detects PSPY variants with Hash\_Breaker"

author = "Team Beasts"

date = "2025-02-26"

strings:

$hash\_breaker = "Hash\_Breaker"

$file\_sig = { 7F 45 4C 46 } // ELF magic bytes for Linux binaries

$pspy\_fswatcher = "pspy.FSWatcher" // Unique dependency in PSPY

$pspy\_cmd = "pspy - unprivileged process snooping"

condition:

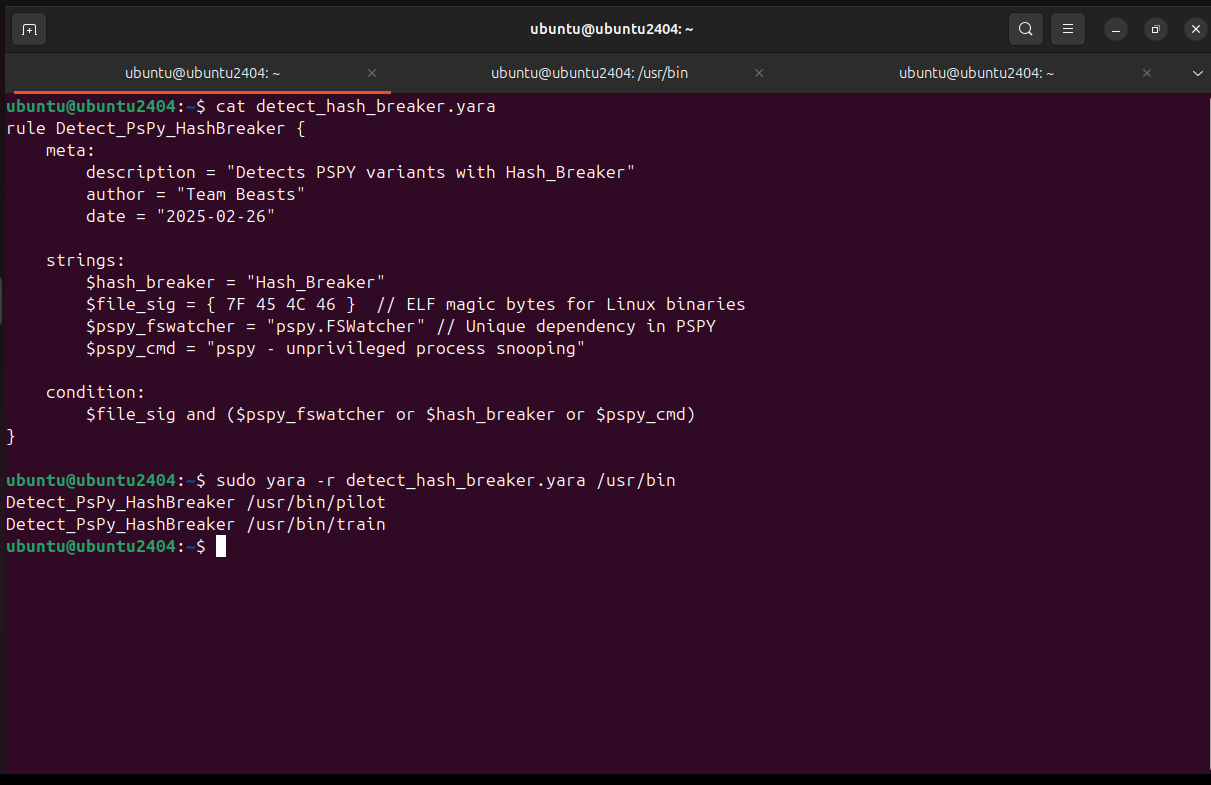
$file\_sig and ($pspy\_fswatcher or $hash\_breaker or $pspy\_cmd)

}

### Analysis of Your YARA Rule:

**Strengths (Precision & Recall Balance)**

* + Uses **multiple detection heuristics** (hash\_breaker, pspy\_fswatcher, pspy\_cmd), improving recall.
  + Checks for **ELF file signature** (7F 45 4C 46), reducing false positives.
  + Targets **specific PSPY functions** (pspy.FSWatcher), which strengthens precision.



**Indicators of Compromise (IoCs):**

* **File Paths:**
  + /usr/bin/train
  + /usr/bin/pilot
* **Suspicious Network Connections:**
  + api.apple-cloudkit.com (Potential exfiltration endpoint)
  + Multiple IPs in the GB region linked to snapcraft.io
* **Sigma Rule Triggered:** Linux HackTool Execution
* **Common Techniques Used:** Process snooping, privilege escalation

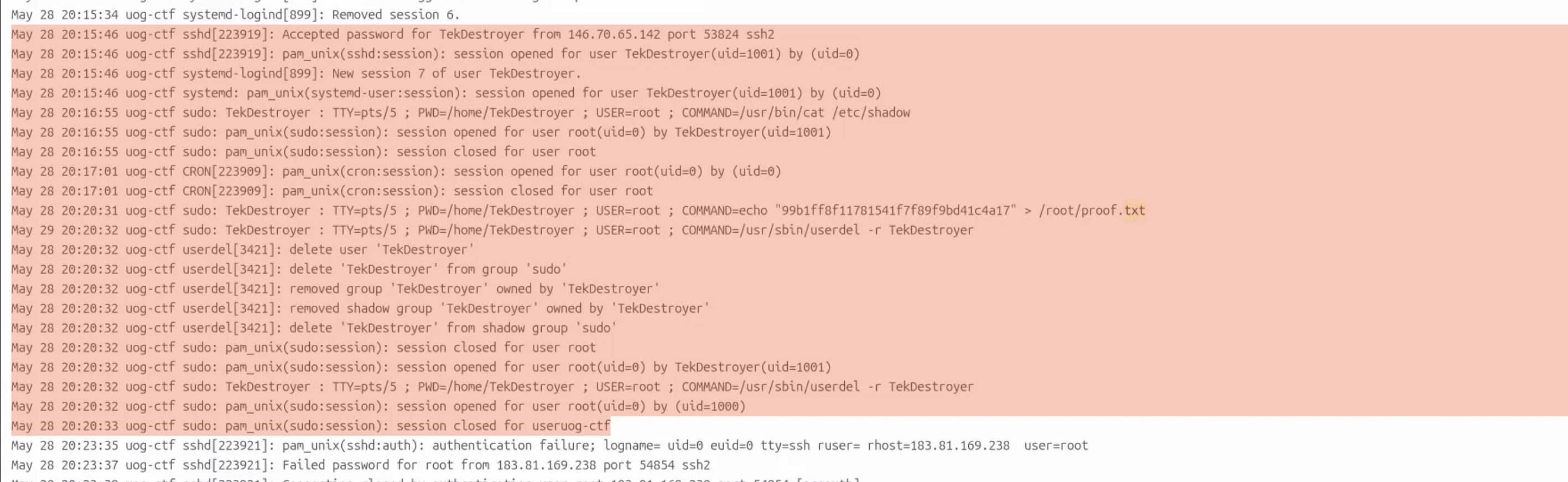
**Recommended Actions:**

1. **Immediate Containment:**
   * Remove /usr/bin/train and /usr/bin/pilot immediately.
   * Check system integrity with chkrootkit and rkhunter.
   * Validate all other binaries in /usr/bin using sha256sum.
2. **Network Analysis & Blocking:**
   * Monitor and block suspicious outbound connections.
   * Implement network monitoring rules to detect similar activity.
3. **Host Forensic Analysis:**
   * Investigate system logs (/auth.log
   * Review user activity for unauthorized privilege escalation attempts.
   * Audit installed packages with dpkg -S /usr/bin/\*.
4. **Strengthening Defenses:**
   * Restrict unnecessary user privileges.
   * Deploy real-time threat monitoring tools (Falco, Auditd).
   * Harden SSH configurations and enforce 2FA authentication.

### Analysis of auth.log for Part 3 of the CTF

he logs indicate multiple failed SSH login attempts from various IP addresses. The attempts include brute-force attacks targeting common usernames such as admin, root, pi, user, and ubuntu. The attack appears systematic and likely automated.

1. **What type of attack is happening?**
   * This log reflects a **brute-force SSH attack** where attackers attempt to gain unauthorized access by trying multiple usernames and passwords.
2. **What IP addresses are involved in the attack?**
   * Several IP addresses have attempted unauthorized access:
     + **152.89.198.106** (Most frequent attacker)
     + **45.55.157.158**
     + **85.209.11.254**
     + **47.236.95.19**
     + **194.169.175.36**
     + **45.79.128.205**
     + **80.94.95.81**
     + **210.99.41.174**
     + **193.201.9.156**
     + **45.128.232.41**
     + **91.92.251.164**
     + **103.203.57.11**
   * **152.89.198.106** appears most frequently, indicating it may be part of a botnet or dedicated attacker.



**May 28 20:15:46 uog-ctf sshd[223919]: Accepted password for TekDestroyer from 146.70.65.142 port 53824 ssh2**

**May 28 20:20:31 uog-ctf sudo: TekDestroyer : TTY=pts/5 ; PWD=/home/TekDestroyer ; USER=root ; COMMAND=echo "99b1ff8f11781541f7f89f9bd41c4a17" > /root/proof.txt**

1. **What usernames are being targeted?**
   * Common usernames include:
     + admin
     + root
     + test
     + ubnt
     + backup
     + service
     + ftp
     + operator
     + pi
     + postgres
     + wordpress
     + oracle
     + moxa
     + steam
     + support
     + ansadmin
     + craft
     + zjw
     + telnet
     + test1
     + boss
     + sam
     + max
     + emily
     + localadmin
   * Many of these are default or commonly used system accounts, reinforcing that this is an automated attack.
2. **What attack patterns can be identified?**
   * **Sequential brute-force attempts:** The log shows attempts on multiple usernames from the same IP within seconds, confirming an automated script.
   * **Changing usernames mid-session:** Some attempts show attackers switching usernames within a session, likely probing which usernames exist on the system.
   * **Repeated failures from the same IPs:** Attackers retry login attempts across multiple usernames.
   * **Multiple IP addresses involved:** The presence of different IPs indicates a distributed attack, possibly a botnet.
3. **Are there any successful logins?**
   * No successful logins are observed. All authentication attempts result in "Failed password for invalid user."
4. **How should this attack be mitigated?**
   * **Immediate Actions:**
     + **Block malicious IPs** using firewall rules (iptables or ufw).
     + **Disable password-based authentication** and enforce SSH key authentication.
     + **Change the default SSH port** from 22 to a non-standard port.
     + **Enable fail2ban** to automatically block repeated failed login attempts.
     + **Monitor and log SSH attempts** for continued attack patterns.
   * **Long-Term Security Measures:**
     + **Enforce Multi-Factor Authentication (MFA)** on SSH.
     + **Use a jump box/bastion host** to limit direct SSH access.
     + **Restrict SSH access** to known IPs (e.g., internal networks).
     + **Implement host-based intrusion detection (HIDS)** such as OSSEC or Wazuh.
     + **Regularly audit SSH logs** for signs of ongoing attacks.

**Conclusion:**

The discovery of train and pilot on an Ubuntu 24.04 system is indicative of an intrusion attempt leveraging PSPY, a known Linux privilege escalation tool. Analysis of auth.log confirms that attackers gained initial access via SSH brute-force techniques, followed by privilege escalation and system modifications. Organizations should take immediate remediation actions and bolster security monitoring to prevent future compromises. Continuous auditing and real-time anomaly detection are recommended to mitigate similar threats in the future.