****1.****

### This report documents a digital forensics investigation conducted on a suspected compromised Linux system. Immediately upon discovery of the potential incident, the team implemented appropriate evidence preservation protocols and began analysis. ****2. First signs of compromise****

Based on initial system reviews, the following signs of compromise were observed:

• Presence of unknown scripts in the Downloads directory

• Suspicious activity in the browser history (by analyzing the browser history)

• Collected traces of e-mail addresses that were potentially used for communication by attackers

• TCP traffic captured by **Wireshark** indicates malicious activity and reveals the attacker's IP address

### ****3. The team's first response****

* A forensic image of the **entire disk** of the compromised system is **IMMEDIATELY** created to preserve all data for analysis and prevent further damage or modification.
* The disk image is used as the main source for the analysis and there was no direct work on the original system.

### ****4. Network traffic analysis****

The **Wireshark tool** was used to monitor network communication in detail:

• We monitored the **TCP streams** and reconstructed the data streams generated by the attacker

• We managed to identify the attacker's **IP address: 3.67.15.169**

• **Whois** analysis reveals that the IP address is owned by **Amazon Technologies Inc.**

• Unfortunately, the IP address did not lead directly to the identity of the attacker - contacting Amazon technical support is necessary for further steps

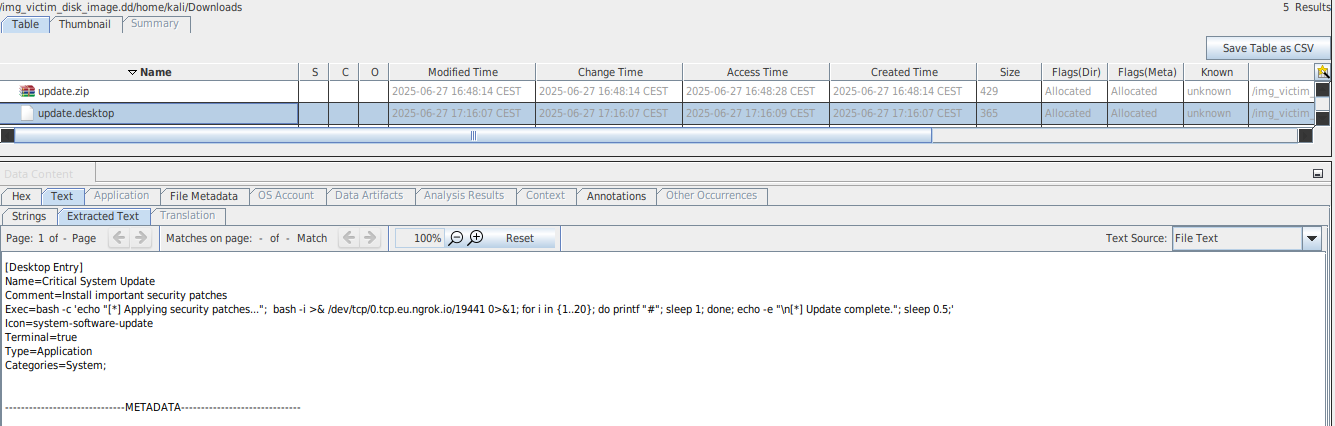
### ****5. Analysis of user activity****

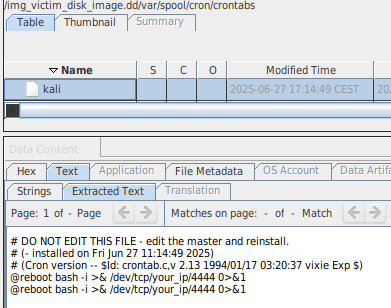
* Browser history has indicated visits to suspicious sites that may be associated with the delivery of malware
* Collected e-mail addresses were analyzed in the context of compromised accounts or communication with the attacker

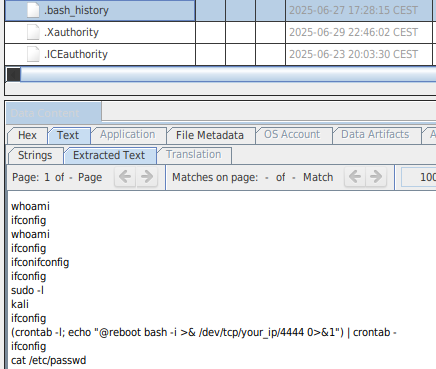
### ****6. Forensic analysis of the disk image****

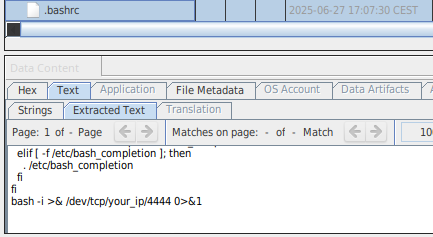
**The tool we used: Autopsy**

* The disk image was analyzed using the Autopsy tool (autopsy images attached)
* Suspicious scripts were found in user folders









# Recommended measures:

* Resetting user access
* Safety training for employees
* Detailed log analysis and IDS system setup
* Mandatory reporting of the incident to the relevant bodies
* Further cooperation with Amazon Tech Support to find the source of the attack