****1.****

### Ovaj izveštaj dokumentuje digitalnu forenzičku istragu sprovedenu na Linux sistemu za koji se sumnjalo da je kompromitovan. Tim je odmah po otkrivanju potencijalnog incidenta primenio odgovarajuće protokole očuvanja dokaza i započeo analizu. ****2. Prvi znaci kompromitovanja****

Na osnovu prvih pregleda sistema, uočeni su sledeći znaci kompromitovanja:

* Prisustvo nepoznatih skripti u direktorijumu Downloads
* Sumnjiva aktivnost u istoriji pregledača (analizom browser history-a)
* Prikupljeni tragovi e-mail adresa koje su potencijalno korišćene za komunikaciju napadača
* TCP saobraćaj beležen pomoću **Wireshark**-a ukazuje na zlonamernu aktivnost i otkriva IP adresu napadača

### ****3. Prvi odgovor tima****

* **ODMAH** je napravljena forenzička **slika celog diska** kompromitovanog sistema, kako bi se sačuvali svi podaci za analizu i sprečilo njihovo dalje oštećenje ili modifikacija.
* Snimak diska se koristi kao glavni izvor za analizu i nije bilo direktnog rada na originalnom sistemu.

### ****4. Analiza mrežnog saobraćaja****

Korišćen je alat **Wireshark** za detaljno praćenje mrežne komunikacije:

* Pratili smo **TCP tokove** i rekonstruisali tokove podataka koje je napadač generisao
* Uspeli smo da identifikujemo **IP adresu napadača: 3.67.15.169**
* **Whois** analiza otkriva da se IP adresa nalazi u vlasništvu kompanije **Amazon Technologies Inc.**
* Nažalost, IP adresa nije dovela direktno do identiteta napadača – kontaktiranje Amazon tehničke podrške je neophodno za dalje korake

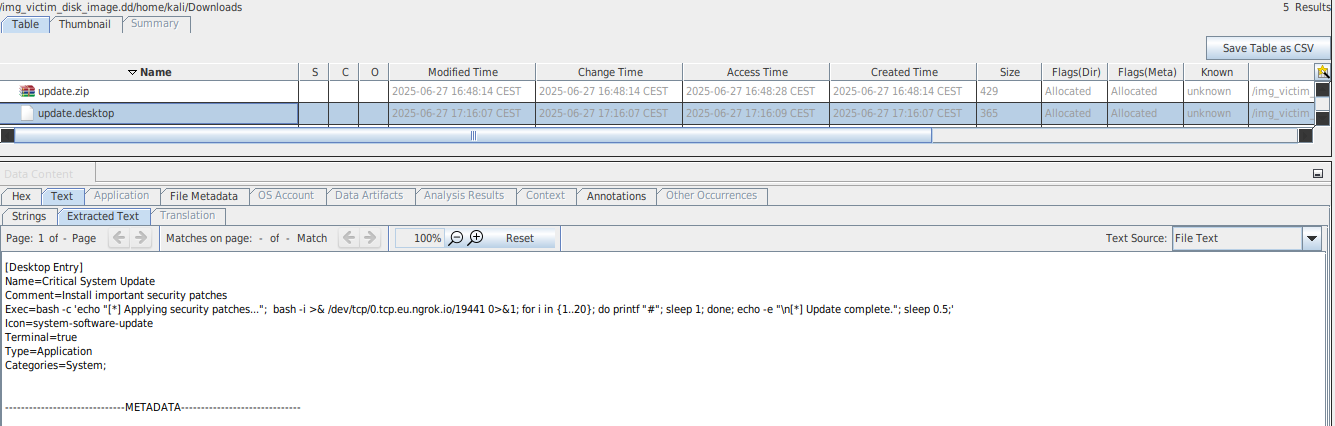
### ****5. Analiza korisničke aktivnosti****

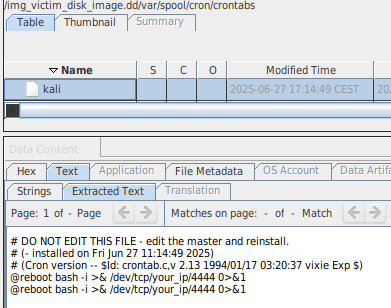
* Istorija pregledača je ukazala na posete sumnjivim sajtovima koji mogu biti povezani sa isporukom malvera
* Sakupljene e-mail adrese su analizirane u kontekstu kompromitovanih naloga ili komunikacije s napadačem

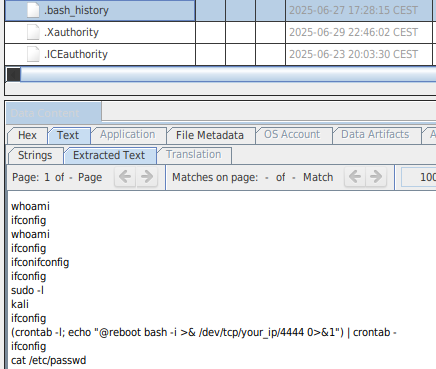
### ****6. Forenzička analiza slike diska****

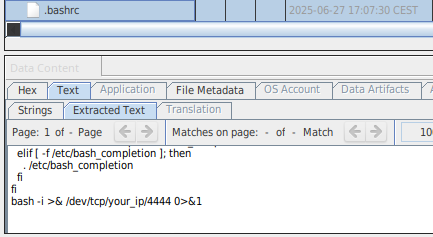
Alat koji smo koristili: **Autopsy**

* Slika diska je analizirana koristeći Autopsy alat (priložene slike iz Autopsy-ja)
* Pronađene su sumnjive skripte u korisničkim folderima









# Preporučene mere:

* Resetovanje pristupa korisnicima
* Bezbednostni trening za zaposlene
* Brisanje svih fajlova i prekid veza napadača
* Detaljna analiza logova i postavljanje IDS sistema
* Obavezna prijava incidenta relevantnim telima
* Dalja saradnja s Amazon Tech podrškom radi pronalaženja izvora napada