

Unorthodox Case 001

Raw Document CJ2025/XII/DFIR-CS-1290

Overview

Our client is a managed private portfolio investment company, **CoreStocks** which suffered an internal breach happening in a constraint from November to December. They believe this attack yields a severe outcome:

- All the last state of stock analysis (macros perspective) are deleted
- All the user login credentials have been changed by the actor
- The server is **believed to be compromised by more than just one internal threat actor.**

Evidence

There are some collected artifacts which have been retrieved for us:

- **Packet Capture File (PCAP_Captured.pcap)**
 - SHA256:
883888DE7A8F84D079A771846FC37B9A12773CA1753371E74F4B3327F27DA
095
- **OVA File (CoreStock main VM server)**
 - SHA256:
499DF688F118D88B49C99197C2B68E03BB672E26DCC14BC048F3D997FEA2
A2E2
- **Binary Data (exfiltrated.bin)**
 - SHA256:
2F940284901830733A303E56F3C6AC655ABB14B8A09C0110681ED137C2DB
54B8

There's a screenshot from one of the employees showing a suspicious message whenever someone tries to login to the **CoreStocks** main VM server.

```
cj@192.168.100.43's password:  
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-88-generic x86_64)  
  
 * Documentation: https://help.ubuntu.com  
 * Management: https://landscape.canonical.com  
 * Support: https://ubuntu.com/pro  
  
System information as of Fri Dec 12 06:53:00 AM UTC 2025  
  
System load: 0.0  
Usage of /: 60.5% of 11.21GB  
Memory usage: 13%  
Swap usage: 0%  
Processes: 122  
Users logged in: 1  
IPv4 address for enp0s3: 192.168.100.43  
IPv6 address for enp0s3: 2001:448a:2098:1bf7:a00:27ff:fe10:39ef  
  
Expanded Security Maintenance for Applications is not enabled.  
25 updates can be applied immediately.  
To see these additional updates run: apt list --upgradable  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
Last login: Fri Dec 12 06:39:36 2025 from 192.168.100.157  
Berhasil :pcj@cj:~$ █
```

The screenshot was taken before the threat actor changed the credentials and removed their core stock data.