1. Сменить пароли пользователей

2. Удалить пользователя deploy(так как пароль от учётной записи равен логину)

3. Запретить логиниться под рут через ssh настройки в файле /etc/sshd-config

4. Создать пару ключей для подключения через ssh

5. Оставить подключение по ssh только через приватный ключ настройки в файле /etc/sshd-config

6. Настроить фаервол через iptables оставить доступ только через порты, которые необходимы остальные необходимо закрыть.

7. Установить все обновления безопасности для OS.

8. Закрыть возможность логина для гостевой сессии

9. Установить сертификат подписанный центром сертификации

10. Вероятно вредоносный код маскируется под программу rsync и запускается через запись в планировщике крон. Из каталога /tmp/.ssh/rsync/\*start.