

实验室服务器遭挖矿病毒攻击报告II

在之前经历过挖矿攻击之后，今天（2021.4.15）吴梓凡再次报告GPU跑满，查看占用GPU的进程发现是在同样一个位置运行了挖矿脚本。

重要结论：

禁用密码登录，采用公钥登录SSH

所有用户即刻使用强密码

查证过程：

上轮攻击之后所有用户设置了强密码，并更改了root密码，自此服务器的安全得到了基本保障。但在今天再次报告了GPU挖矿。分析后怀疑对方再次破解密码，遂查询lastb，获得失败的历史连接请求，发现有暴力尝试密码行为：

| | | | | | |
|------|----------|-----------|----------------|--------------------------|---------|
| 4251 | linyufen | ssh:notty | 222.200.184.58 | Thu Apr 15 03:13 - 03:13 | (00:00) |
| 4252 | linyufen | ssh:notty | 222.200.184.58 | Thu Apr 15 03:13 - 03:13 | (00:00) |
| 4253 | liugang | ssh:notty | 222.200.184.58 | Thu Apr 15 03:13 - 03:13 | (00:00) |
| 4254 | liugang | ssh:notty | 222.200.184.58 | Thu Apr 15 03:13 - 03:13 | (00:00) |
| 4255 | cheng | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4256 | cheng | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4257 | jimm | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4258 | jimm | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4259 | jidlin | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4260 | jidlin | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4261 | lei | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4262 | lei | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4263 | Cpz | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4264 | Cpz | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4265 | fh | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4266 | fh | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4267 | linj | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4268 | linj | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4269 | wangmy | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4270 | wangmy | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4271 | zongct | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4272 | zongct | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4273 | lrp | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4274 | lrp | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4275 | lx | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4276 | lx | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4277 | tangmin | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4278 | tangmin | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4279 | fengwf | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4280 | fengwf | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4281 | plan | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4282 | plan | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4283 | yangjx | ssh:notty | 222.200.184.58 | Thu Apr 15 03:12 - 03:12 | (00:00) |
| 4284 | yangjx | ssh:notty | 222.200.184.58 | Thu Apr 15 03:11 - 03:11 | (00:00) |
| 4285 | hugy | ssh:notty | 222.200.184.58 | Thu Apr 15 03:11 - 03:11 | (00:00) |
| 4286 | hugy | ssh:notty | 222.200.184.58 | Thu Apr 15 03:11 - 03:11 | (00:00) |
| 4287 | hongzl | ssh:notty | 222.200.184.58 | Thu Apr 15 03:11 - 03:11 | (00:00) |
| 4288 | hongzl | ssh:notty | 222.200.184.58 | Thu Apr 15 03:11 - 03:11 | (00:00) |
| 4289 | tanli | ssh:notty | 222.200.184.58 | Thu Apr 15 03:11 - 03:11 | (00:00) |
| 4290 | tanli | ssh:notty | 222.200.184.58 | Thu Apr 15 03:11 - 03:11 | (00:00) |
| 4291 | heyue | ssh:notty | 222.200.184.58 | Thu Apr 15 03:11 - 03:11 | (00:00) |
| 4292 | heyue | ssh:notty | 222.200.184.58 | Thu Apr 15 03:11 - 03:11 | (00:00) |
| 4293 | jinmu | ssh:notty | 222.200.184.58 | Thu Apr 15 03:11 - 03:11 | (00:00) |
| 4294 | jinmu | ssh:notty | 222.200.184.58 | Thu Apr 15 03:11 - 03:11 | (00:00) |
| 4295 | redis | ssh:notty | 222.200.184.58 | Thu Apr 15 03:11 - 03:11 | (00:00) |
| 4296 | redis | ssh:notty | 222.200.184.58 | Thu Apr 15 03:11 - 03:11 | (00:00) |

分析连接发起者，得到几个非实验室主机的高失败链接ip:

