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:

	rssn.notty rssh: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 jinmm	ssh:notty	222.200.184.58	Thu Apr 15 03:12 - 03:12	(00:00)
4258 jinmm	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 lel	ssh:notty	222.200.184.58	Thu Apr 15 03:12 - 03:12	(00:00)
4262 lel	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 Thu Apr 15 03:12 - 03:12	(00:00)
4275 Ix 4276 Ix	ssh:notty	222.200.184.58 222.200.184.58	Thu Apr 15 03:12 - 03:12 Thu Apr 15 03:12 - 03:12	(00:00) (00:00)
4276 lx 4277 tangmin	ssh:notty ssh:notty	222.200.184.58	Thu Apr 15 03:12 - 03:12 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)
4279 fengwf	ssh:notty	222.200.184.58	Thu Apr 15 03:12 - 03:12	(00:00)
4280 fengwf	ssh:notty	222.200.104.58	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 yangix	ssh:notty	222.200.184.58	Thu Apr 15 03:12 - 03:12	(00:00)
4284 yangix	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:

值得注意的是本机ip也进行了多次失败连接,怀疑是获得了用户密码后尝试获得root密码。

对连接进行分析,发现实验室成员的姓名全拼和缩写均出现在记录中,每个用户名尝试十余次,怀疑攻击者爬取中山大学学生及教师名单,并用预设简单密码暴力破解。

分析发现,至今有外部链接尝试我服务器密码,分析后认为服务器密码更改后未泄露,怀疑攻击者在本机放置公钥后密钥登陆。遂在root目录下发现两条无人认领公钥,该authorized_keys文件更新日期为4月6日,与服务器遭受攻击日期相符。

```
A AAAAB3NzaC1yc2EAAAABJQAAAQEApQXSg+ZYkvQ4vQ0ThTHmJrqJ8yQq9ceYrRRYLwKhjr39bGHVL1rkwTCP5n1UuMBQ4CeYzLBoYjBrcbytGoB+67xQkoQZJzp6RoPy1tQG4hQsKLpeXNbs/u8d7PzIXQp9quTSdzUDuhm3Pkbgq7VBEtoqkNtnFkQQwyf2cf9DDZ+haKXQV9otU+FPZru2KboL9/C3xrQ4ocqkuv7F5RH5468ekaV2bu/N01wHmtZMpQsqH2/PkJF2YN7axi25dBfMAEqbii3eo/EWVQMeQIqQWvz4M9TaW8G+E/FQbudc1btmwkXQQwJ2ZkmAFoS+8ATRb1FxUHaI2Xz/a1YNXNRubQ== rsa-key-20200913
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDIU9RTCRzyzb8Ak9BndGQ2nQ4bxqswpBQQA68MRH/NsU669Pkb16+kaYCqTbkej2QDKcoXqQ8kW9xaANQsM8Qv9AanE1rbi8ZyH7ZTdZDWAhQQbhnEXXiNfjhuqvDBTRs6Lr36P9iBgV611aNYxgJbS1IFfMzciBhCQ9nSIIhv8ytIRjeK+AVxw6crG/Xr2g7kI3sZw9Qkt3M4f09nZGE9TdQq7DDvVZeJZ8R98Y/PFij01Nh63iJMxPkDSQtQCF4WQmj8Uk9pcd+y+Ap5u12mL+HI/9Am43vnjSmhPvLLzRpi71V/pVAIZk3LMMIdA79dWhyLYTaIHwuQa8bhw8wui0iKv/Cs6TpyIxfgQ7dK6Jjob1av6Y4M9IbIFvQx3mIolzShyi33ILLQ5PyEiCqtujp5aT32efcBqeYTPMF16mWH5jkyyfBiG+oE9K9E4yB5vM85WVjaSisyp4aHRyh+Hw55NHQZFdBMZk+QcNHKsu9ffEUKkNxtzIMKZuEAWZQU= root@locaIhost
```

处理:

删除无人认领公钥;

再次更换密码;

未来计划全面禁用密码ssh登录。