网络也不是法外之地——

国内外网络安全事件

1. 腾讯安全威胁情报中心检测到针对 Linux 服务器进行攻击的 WatchBogMiner 变种挖矿木马。该木马利用 Nexus Repository Manager、Supervisord、ThinkPHP 等服务器组件的远程代码执行漏洞进行攻击，在失陷机器安装多种类型的持久化攻击代码，然后植入门罗币挖矿木马进行挖矿。腾讯安全专家根据木马使用的算力资源推测已有上万台 Linux 服务器被黑客控制，已挖到 28 个门罗币，收益约 1.3 万元。

木马通过第三方网站 Pastebin 保存恶意代码以躲避检测，并且通过各类方法进行持久化，定期拉取挖矿木马加载到内存执行，同时会在启动后删除木马文件以达到“隐身”目的。和其他挖矿木马类似，WatchBogMiner 木马挖矿时，会清除其他挖矿木马以独占服务器。

WatchBogMiner 变种攻击代码还会通过失陷机器已认证过的 SSH RSA 进行 SSH 连接和执行远程命令进行横向移动，以扩大其影响范围。根据其钱包算力（120Kh/s）推测，木马已控制约 1 万台服务器进行挖矿。

2. 甘肃省人民检察院官方网站消息，在 2020 年 7 月 19 日（周天）上午组织的全省检察机关聘用制书记员线上笔试的职业素能测评阶段，前期系统正常，但在考试进行过程中，考试系统被黑客冲击，造成网络卡顿，使部分考生出现掉线、无法登陆的现象。为确保考试公平、公正，经研究，决定及时中止网上笔试，另行安排笔试工作。具体通知将通过甘肃省人民检察院官网进行发布。

网络安全防范措施

1、全面规划网络平台的安全策略。

2、制定网络安全的管理措施。

3、使用防火墙。

4、尽可能记录网络上的一-切活动。

5、注意对网络设备的物理保护。

6、检验网络平台系统的脆弱性。

7、建立可靠的识别和鉴别机制。

网络安全被成功入侵的因素

(1)人为的无意失误:如操作员安全配置不当造成的安全漏洞,用户安全意识不强，用.户口令选择不慎,用户将自己的帐号随意转借他人或与别人共享等都会对网络安全带 来威胁。(2)人为的恶意攻击 :这是计算机网络所面临的最大威胁,敌手的攻击和计算机犯罪就属于这一类。此类攻击又可以分为以下两种:-种是主动攻击,它以各种方式有选择地破坏信息的有效性和完整性;另-类是被动攻击,它是在不影响网络正常工作的情况下,进行截获、窃取、破译以获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄漏。(3)网络软件的漏洞和"后门”:网络软件不可能是百分之百的无缺陷和无漏洞的,然而,这些漏洞和缺陷恰恰是黑客进行攻击的首选目标，曾经出现过的黑客攻入网络内部的事件,这些事件的大部分就是因为安全措施不完善所招致的苦果。另外,软件的"后[门"都是软件公司的设计编程 人员为了自便而设置的，- -般不为外人所知，但一旦"后门“洞开,其造成的后果将不堪设想。