《2021 年恶意挖矿威胁趋势分析报告》

CNCERT 与安恒信息联合发布

2022 年 4 月

目录

摘要

随着加密货币的飞速发展以及货币的价值提高，收益透明、见效性快的恶意挖矿业务成了网络犯罪分子的首选，导致恶意挖矿活动长期在全球各地持续活跃。

恶意挖矿是一种网络中常见的威胁类别，这种威胁具有良好的隐蔽性和非破坏性的特点，目的是感染并长久驻留在用户设备上，通过侵占设备计算资源挖掘加密货币，当攻击者侵占的设备越多，其获利就越多，因此有不少的黑客团体通过非法入侵从而实现牟利操作。

根据 CNCERT 和安恒威胁情报中心的监测数据，联合发布《2021 年恶意挖矿威胁趋势分析报告》，该报告首先将介绍挖矿活动的相关介绍，对 2021 年第四季度我国主机挖矿态势进行简要分析，接着从流行恶意挖矿威胁、挖矿木马传播方式以及恶意挖矿趋势等方面向社会公众发布 2021 年恶意挖矿威胁趋势分析情况。

一、挖矿活动介绍

1. 挖矿、恶意挖矿与加密货币

什么是加密货币？

加密货币是没有物理形式，且仅存在于网络的数字货币，因其前瞻性设计、价值增长潜力和匿名性而广受欢迎。最著名以及最成功的加密货币是 2009 年问世的比特币，比特币的成功激发了数以千计的其他加密货币诞生，截止 2021 年 11 月，全球加密货币种类超过 9000 种，总市值达 2.7 万亿美元，并且还处于不断增长当中，来自世界各地的投资者都使用加密货币来进行买卖以及投资。

加密货币由“密码学”和“货币”两个词组合而成，是一种基于复杂的数学加密原理来确保交易安全及控制交易单位创造的交易媒介。所有加密货币都以加密的去中心化货币单位存在，可在网络参与者之间自由转移。

什么是挖矿？

挖矿就像是求解一道数学题，最先破获数学答案就可以获得对应的数字货币奖励，“挖”指的是利用计算资源求解并验证数字猜想的过程，“矿”指的是某种数字货币，而协助破解数字答案的设备就称为“矿机”，运算能力越强的设备产出虚拟货币的时间就越短，而整个过程极其耗费计算资源和电力资源。而“矿池”简单来说就是挖矿的集合地，可以将全球的算力资源集合到一起进行挖矿，这样可以大大提高挖到“矿”的概率。

什么是恶意挖矿？

恶意挖矿是指在未经用户同意或知情的情况下使用设备（计算机、智能手机、平板电脑甚至服务器）挖掘加密货币，并以隐蔽、不易察觉的方式使用其设备的计算资源的行为，这个劫持系统运算资源挖掘加密货币的过程被称为“加密劫持”，也就是俗称的“恶意挖矿”。**通常情况下，恶意挖矿与设备感染挖矿木马有关。**

2. 感染挖矿木马的迹象

根据某些迹象，用户可以初步怀疑设备已感染挖矿木马恶意软件，例如 CPU 使用率大幅高于正常数值，甚至 100%，以及电脑过热、系统运行速度变慢、设备比正常情况下更频繁地使用冷却风扇等，即便重启也不能解决问题，这些都是显著的感染挖矿木马的症状。

其中一些挖矿木马家族会对自身的行为进行限制，只在 CPU 资源闲置时进行挖矿，当用户查看 CPU 资源时，将停止挖矿，导致用户很难察觉是否存在感染挖矿木马的异常行为。

3. 恶意挖矿是如何工作的？

恶意挖矿通常分为基于浏览器的驱动式网页挖矿和二进制文件的恶意挖矿。

驱动式网页挖矿与恶意广告攻击类似，攻击者将一段 JavaScript 代码嵌入到目标网页中。当用户访问该页面时将执行 JS 脚本，进行加密货币挖掘，缺点是用户退出页面时将结束挖矿。

而二进制文件的恶意挖矿与网页挖矿不同，一旦计算机感染恶意挖矿程序，受害设备将开始全天候的虚拟货币挖矿，同时将恶意进程隐藏在后台，并启用多种持久手段在目标设备上驻留，直到威胁被清除为止。另外，这种恶意程序所针对的设备通常是具备高性能和强大计算资源的服务器资源，因为其可以更快地挖掘产出虚拟货币。

4. 为什么会感染挖矿木马软件？

挖矿木马软件与其他恶意家族一样，可以借助多种传播方式进行感染，例如钓鱼邮件附件、植入网页挖矿的网站，或与来历不明的第三方应用进行捆绑下载传播，如激活工具、游戏外挂程序、盗版软件、浏览器拓展等程序将威胁下发到目标环境。

而一些技术能力较强的黑产团伙则会配备漏洞 POC 用作入侵企业网络，在目标网络中意图扩散挖矿木马程序。

5. 恶意挖矿的危害

用户作为挖矿的受害者，通常不会注意到自身已被感染，因为大多数挖矿木马软件都具备隐藏自身的功能，但这并不意味着它不会对你的设备造成损害。实际上，这种对计算资源的窃取会大幅降低运行速度，加大电力消耗，并缩短设备的使用寿命，从而影响业务或生产环境的正常运营。

受感染的设备通常会产生以下较为明显的负面影响：

- 系统运行速度变慢
- 增加处理器使用率
- 设备过热
- 增加电力消耗

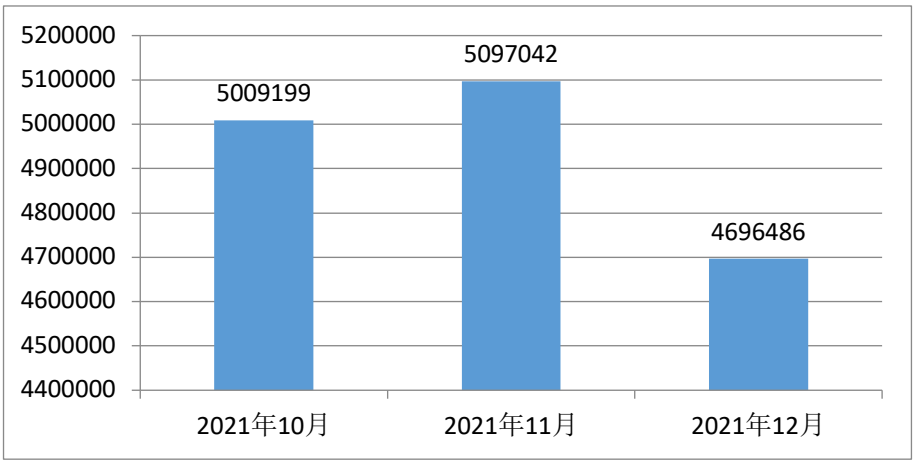
恶意挖矿活动对单台设备的影响相对较小，但如果网络环境遭遇大范围传播感染的情况，网络将会出现明显卡顿、运行过慢等异常现象，导致性能降低甚至死机的情况发生，如果感染的是来自公用事业、制造业、能源行业、金融业的实体组织，恶意挖矿还可能影响其重要业务和数据的安全性，从而引起一系列的连锁反应，造成难以评估的运营、生产损失。

二、2021 年第四季度我国主机挖矿态势分析

CNCERT 通过对流行的挖矿木马及挖矿行为开展抽样监测，形成 2021 年第四季度我国主机挖矿态势分析。下面分别从挖矿主机及矿池服务器两个维度开展分析。

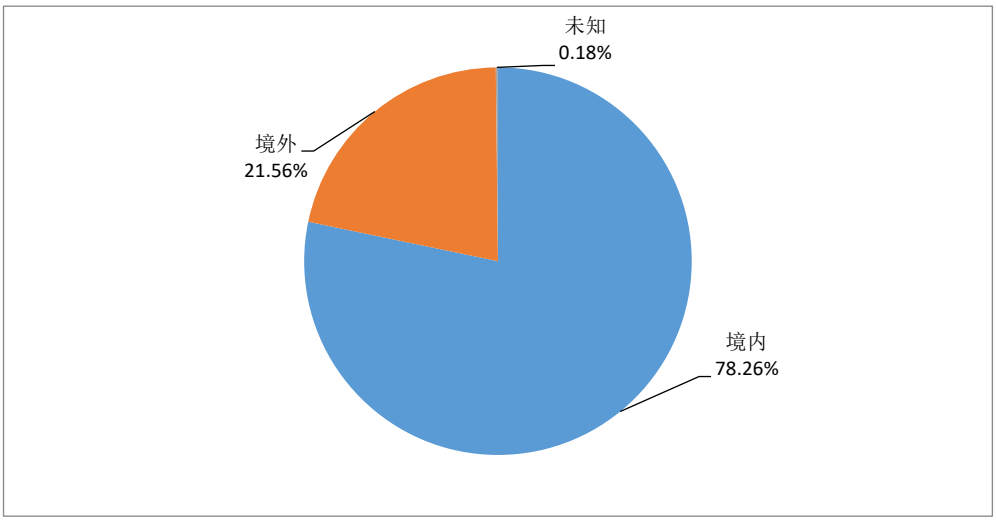
1.2021 年第四季度活跃挖矿主机分析

2021 年第四季度，CNCERT 监测到涉及挖矿的通信行为 1309 亿次，共涉及约 1072 万个挖矿主机 IP。其中监测发现的活跃挖矿主机数量按月分布如下图所示，可以发现 11 月份的挖矿事件较多，12 月份较少。



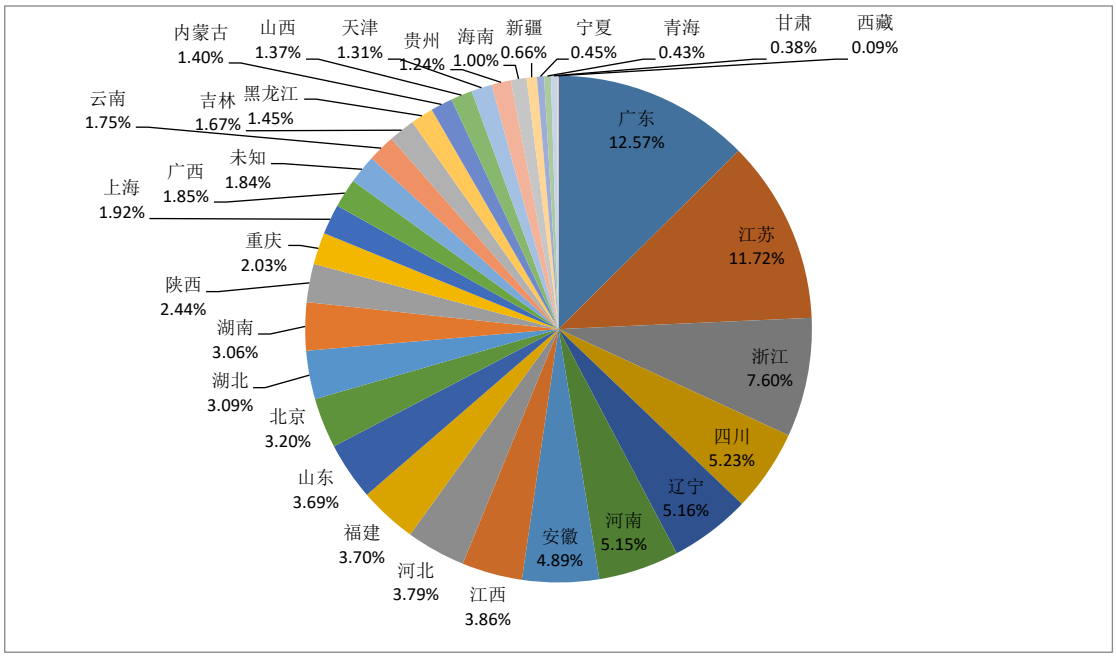
图：2021 年第四季度活跃挖矿主机 IP 数量按月分布

如下图所示，在监测发现的 1072 万个活跃挖矿主机 IP 中，78.26%为境内 IP。



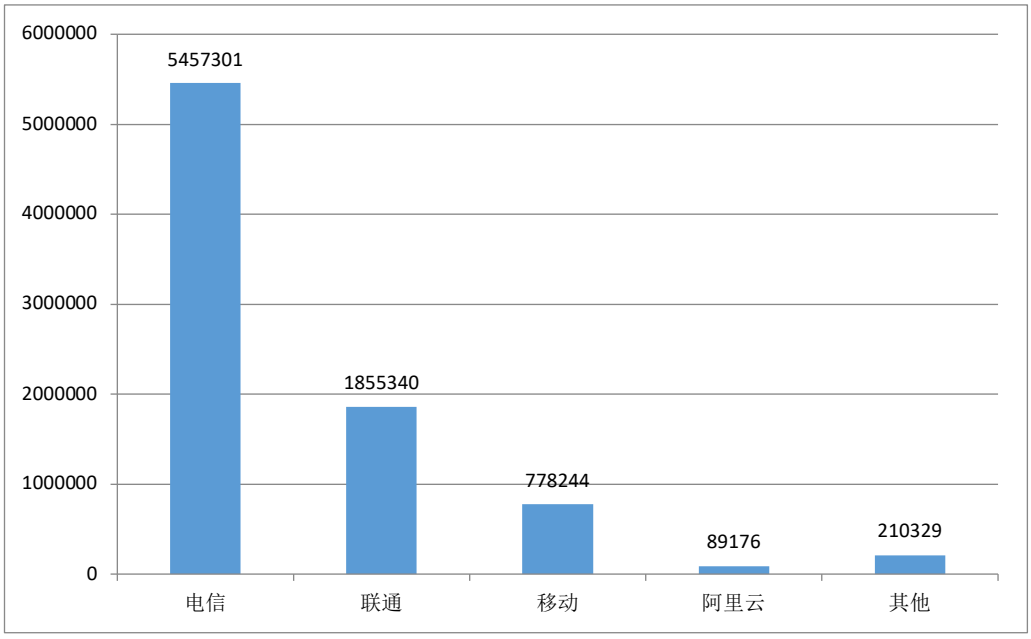
图：挖矿主机 IP 境内外分布

如下图所示，在境内的挖矿主机 IP 中，归属于广东、江苏、浙江等省份的挖矿主机 IP 较多，分别占 12.57%、11.72%、7.6%。



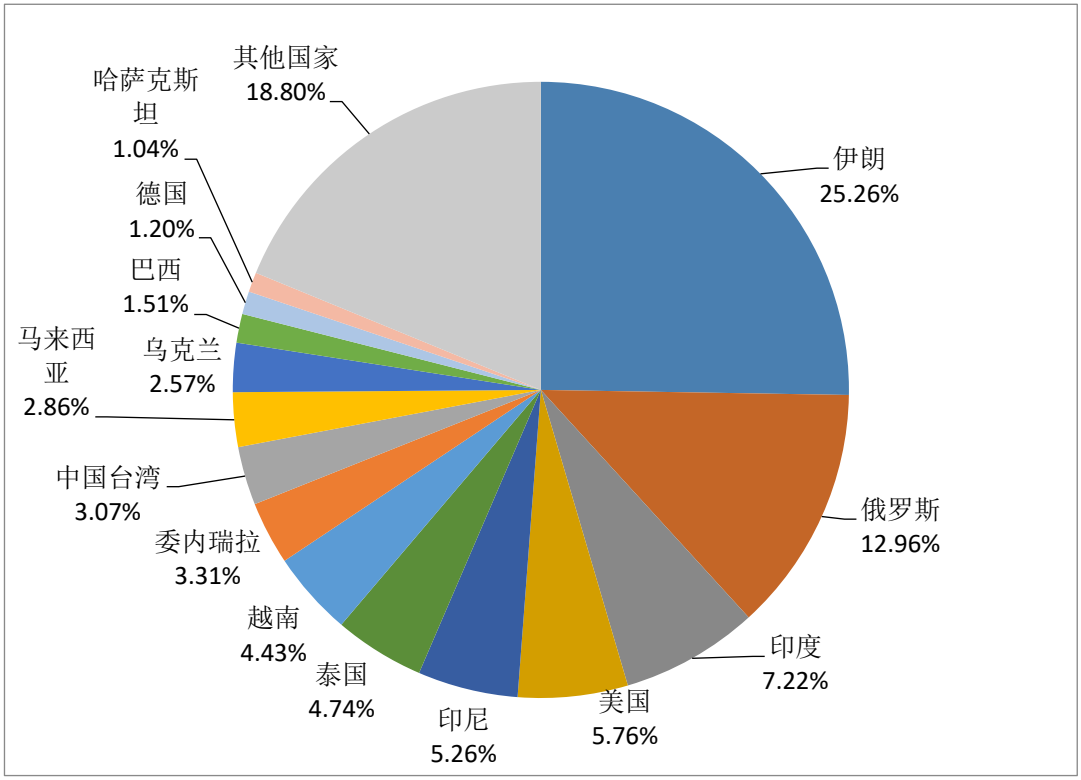
图：境内挖矿主机 IP 按省份分布

此外，电信、联通等运营商的挖矿主机 IP 较多。电信运营商的境内挖矿主机 IP 有 546 万个，占本季度挖矿主机 IP 数量的 65.04%，联通有 189 万个，占 22.11%。



图：境内挖矿主机 IP 所属运营商分布

21.56%的境外挖矿主机 IP 中，来自伊朗、俄罗斯、印度等国家的 IP 较多，分别占 25.26%、12.96%、7.22%。



图：境外挖矿主机 IP 按国家和地区分布

值得关注的是，部分挖矿主机 IP 非常活跃，发起较多的与矿池服务器的连接。以下 20 个 IP 为值得关注的挖矿主机 IP 地址。

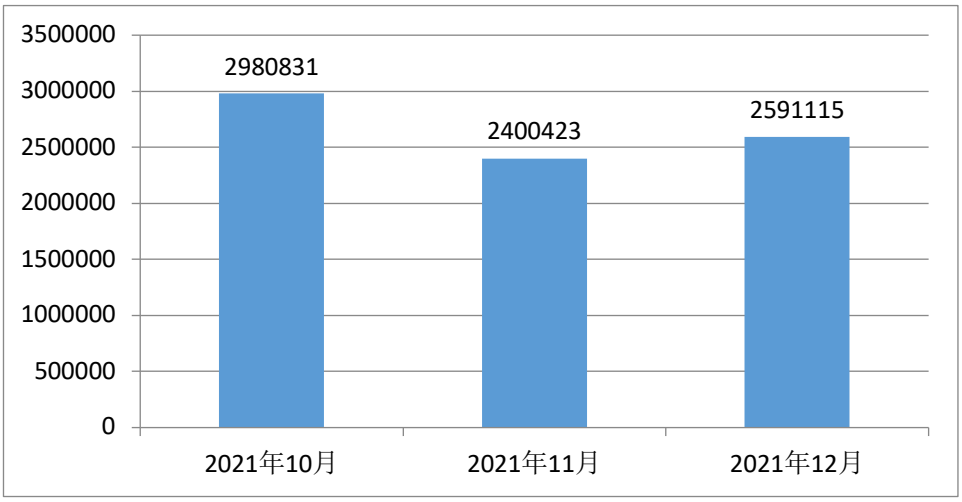
表：活跃挖矿主机 IP Top20

IP*	地理位置	与矿池连接次数
106.**.**.19	上海	2300781183
120.**.**.167	广东	1618222028
117.**.**.207	河南	994100508
120.**.**.229	广东	944055649
193.**.**.173	广东	836239278
122.**.**.116	河南	506139247
182.**.**.158	四川	500180722
47.**.**.17	广东	436102159
139.**.**.147	四川	398089749
193. **.**.254	俄罗斯	394709478

111.**.**.51	广东	384548560
58.**.**.106	湖北	378751989
182.**.**1.11	广东	373948017
120.**.**.57	广东	370649924
8.**.**.43	中国	345367736
120.**.**.58	广东	338583049
47.**.**.18	广东	323556945
58.**.**.98	北京	316176652
49.**.**.135	北京	309107681
113.**.**.157	湖北	303368231

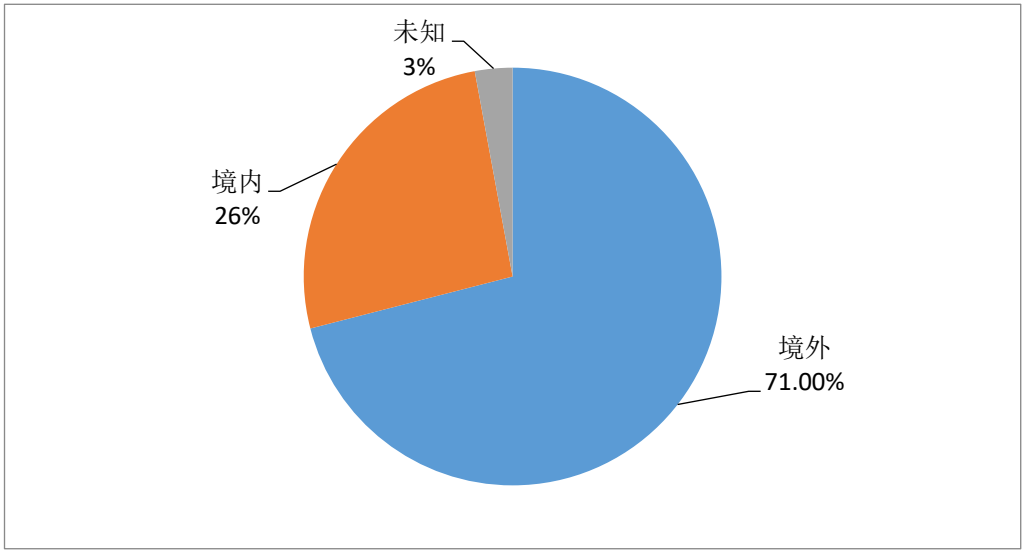
2.2021 年第四季度矿池服务 IP 分析

2021 年第四季度，CNCERT 监测发现约 585 万个矿池服务 IP。其中活跃矿池服务 IP 数量按月分布如下图所示：



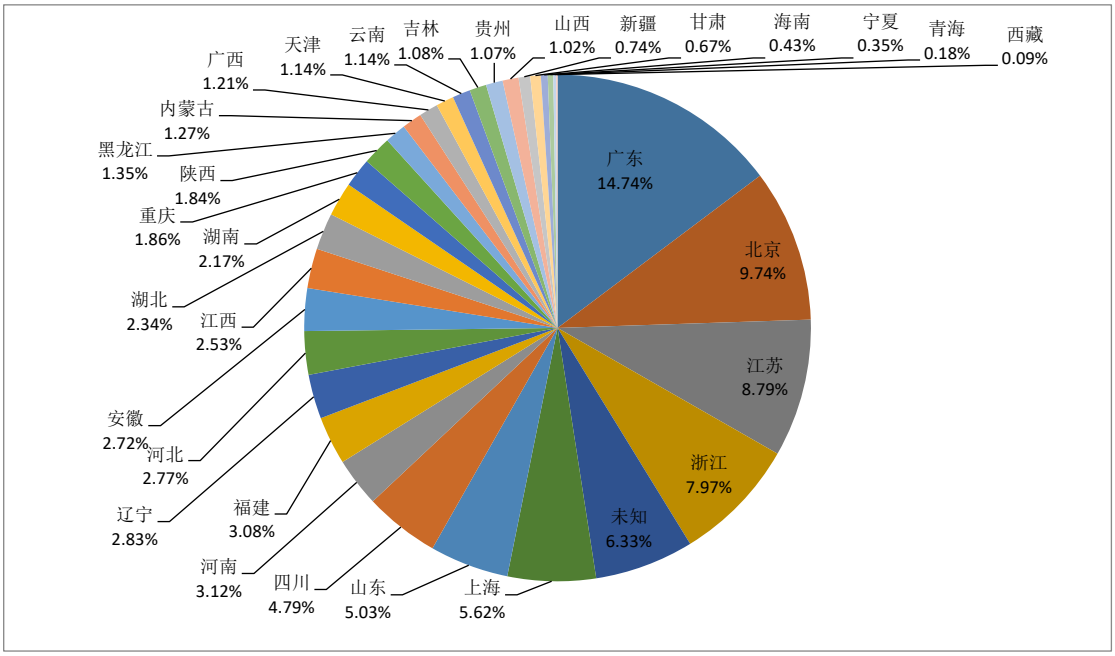
图：矿池服务 IP 数量按月分布

585 万个矿池服务 IP 中，26.10%为境内 IP。



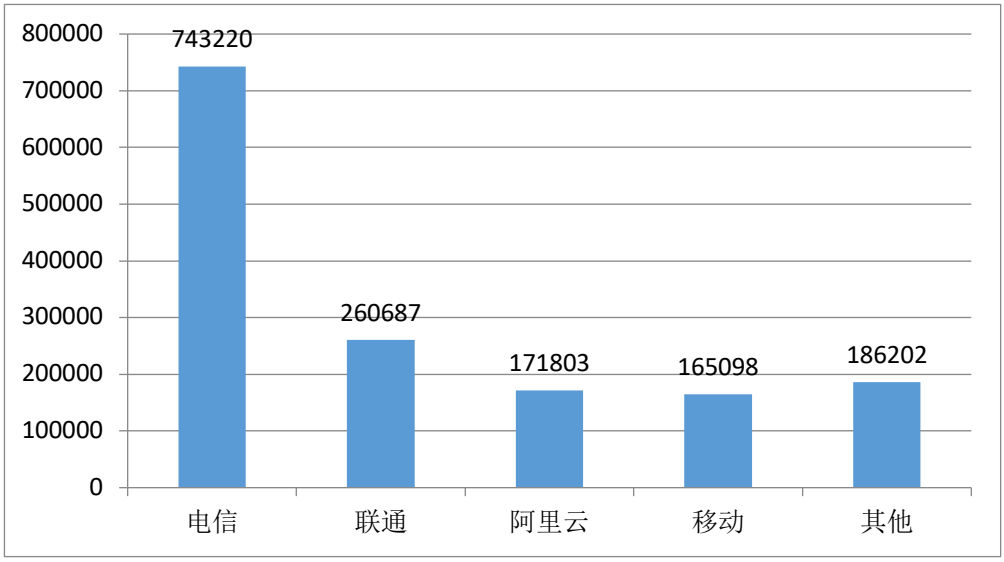
图：矿池 IP 境内外分布

境内矿池以广东、北京、江苏的服务 IP 较多，分别占 17.40%、17.33%、9.93%。



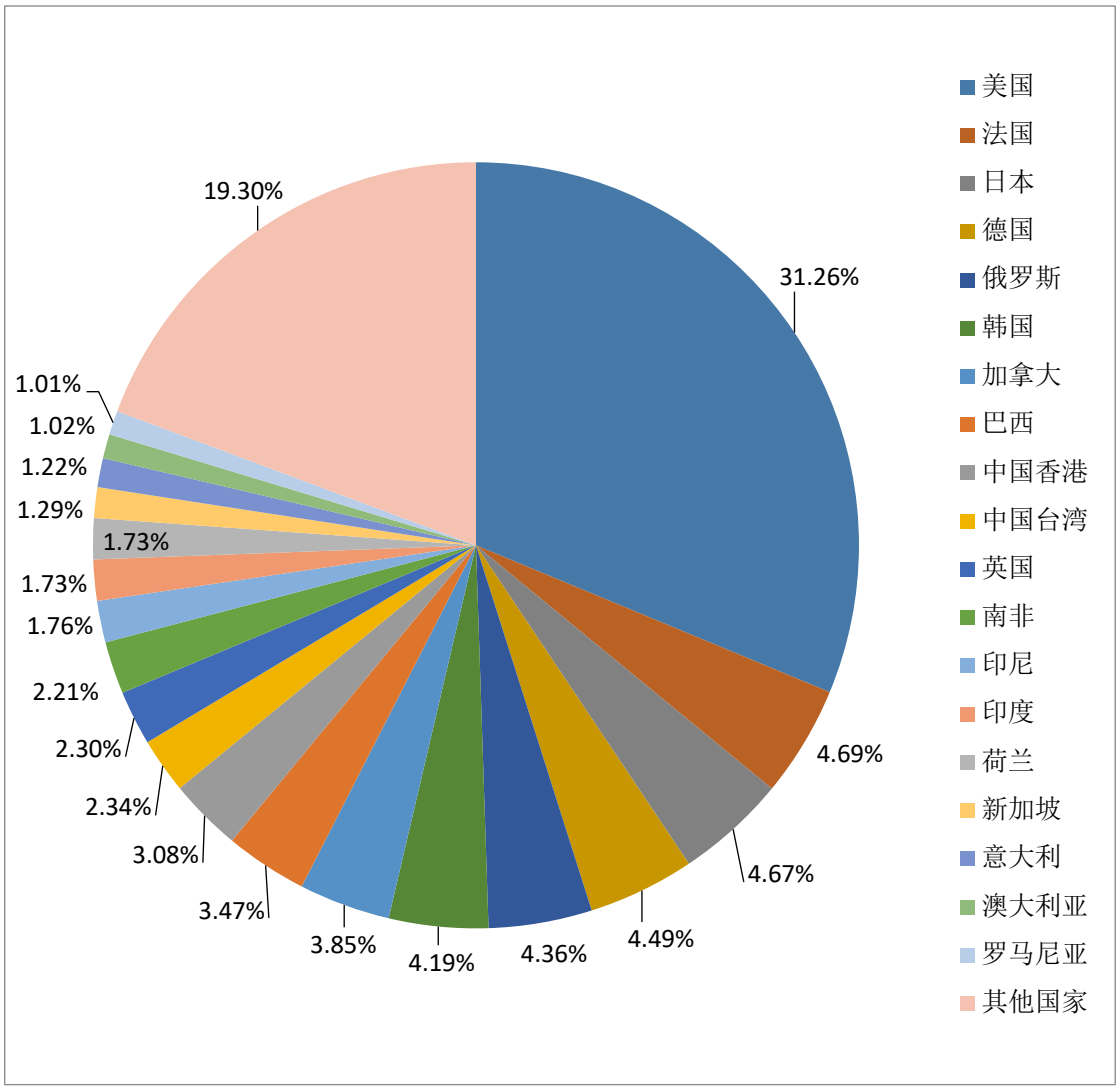
图：境内矿池 IP 按省份分布

此外，电信、联通等运营商的境内矿池 IP 较多。其中 IP 地址运营商为电信的境内矿池 IP 约有 74 万个，占 2021 年第四季度所有矿池服务 IP 的 48.67%，其次为联通和阿里云，约有 26 万个和 17 万个，分别占 17.07%、11.25%。



图：境内矿池 IP 所属运营商分布

在 71%的境外矿池服务 IP 中，美国的矿池 IP 数量最多，共监测发现约 130 万个 IP，占本季度所有活跃矿池 IP 数量的 31.26%、其次为法国和日本，IP 数量是 194817 个、193995 个，分别占本季度矿池 IP 总数的 4.69%、4.67%。



图：境外矿池服务 IP 按国家和地区分布

值得关注的是，部分矿池 IP 非常活跃，有较多的挖矿主机 IP 与其进行通信连接，下表为活跃矿池的相关列表。

表：活跃矿池 IP Top20

IP	地理位置	通联次数	历史解析域名
138. 68. 44. 84	美国	1568961	host. voiceusit. com ait. pilutce. com
157. 245. 77. 105	美国	1562371	host. voiceusit. com repomaa. 3cx. fi ait. pilutce. com
96. 126. 117. 129	美国	1560309	ait. pilutce. com host. voiceusit. com

194. 195. 223. 249	德国	1183541	sim. miniast. com cake. pilutce. com o. auntions. com bit. pilutce. com tie. presuant. com iot. tenchier. com iron. tenchier. com coco. miniast. com
139. 177. 196. 162	美国	1180841	bit. pilutce. com iron. tenchier. com coco. miniast. com tie. presuant. com aliyuncs. com cake. pilutce. com o. auntions. com iot. tenchier. com sim. miniast. com
139. 59. 109. 18	新加坡	1116214	iron. tenchier. com bit. pilutce. com sim. miniast. com tie. presuant. com iot. tenchier. com coco. miniast. com cake. pilutce. com o. auntions. com
139. 59. 182. 191	英国	923187	rim. miniast. com chrisbuckle. com wgc. witmone. com
159. 89. 161. 1	印度	922308	wgc. witmone. com rim. miniast. com
159. 203. 63. 223	加拿大	724273	hot. tenchier. com tech. tositive. com
109. 74. 196. 239	英国	713608	hot. tenchier. com tech. tositive. com
134. 209. 40. 198	美国	707798	hot. tenchier. com tech. tositive. com
199. 247. 27. 41	荷兰-	464821	randomx. xmrig. com

			donate. ssl. xmrig. com donate. v2. xmrig. com
178. 128. 242. 134	荷兰-	452515	randomx. xmrig. com donate. v2. xmrig. com donate. ssl. xmrig. com randomx-benchmark. xmrig. com
203. 107. 32. 162	中国	409164	dcr. vvpool. com wbtc. vvpool. com backup-zec. f2pool. com bch. vvpool. com gf. f2pool. com raven. f2pool. com vip-cmcc. f2pool. com btc. f2pool. com stratum. fkpool. cn clo. vvpool. com eth-backup. f2pool. com dcr. f2pool. com vip-chengdu. f2pool. com eth. f2pool. com stratum. f2pool. com sc. f2pool. com backup-eth. f2pool. com btc. sr. f2pool. com sha256d. f2pool. com xmr. f2pool. com mona. f2pool. com btm. f2pool. com btcchenzhuang-nm. f2pool. com bcx. vvpool. com btn. vvpool. com btcksy-qh. f2pool. com
50. 116. 34. 212	美国	332654	wgc. witmone. com rim. miniast. com
106. 54. 138. 202	中国	280037	other. xmrpool. ru
47. 241. 198. 198	美国	256814	mine. c3pool. com geo. c3pool. com

			rvn-asia. c3pool. com
47. 241. 208. 216	美国	247972	sg. c3pool. com geo. c3pool. com rvn-asia. c3pool. com asia. c3pool. com mine. c3pool. com
39. 107. 236. 106	中国	230999	cn-bch. ss. btc. com cn-beta. ss. btc. com cn-bcc. ss. btc. com cn-bsv. ss. btc. com cn. ss. btc. com
39. 102. 48. 53	中国	227140	cn-bch. ss. btc. com cn. ss. btc. com cn-bcc. ss. btc. com cn-bsv. ss. btc. com

三、流行挖矿威胁浅析

通常，攻击者是出于经济动机才进行挖矿恶意活动，因为挖矿是一项非常有利可图的业务，与勒索软件网络犯罪业务相比，恶意挖矿业务的攻击成本更低，且易于实施，收益直接可见，单靠个人就能完成整个攻击流程，这也是恶意挖矿业务受到广大攻击者青睐的原因之一。

下面介绍一些常见的黑产挖矿团伙和流行挖矿木马家族。

1. 挖矿团伙

TeamTNT 组织

TeamTNT 是一个针对云环境的德语加密劫持黑客组织，自 2020 年 4 月以来一直处于活跃状态。该组织不断对其挖矿木马进行迭代升级，主要的攻击目标是 Kubernetes 和 Docker。TeamTNT 攻击目标环境也随着该组织的技术迭代而拓

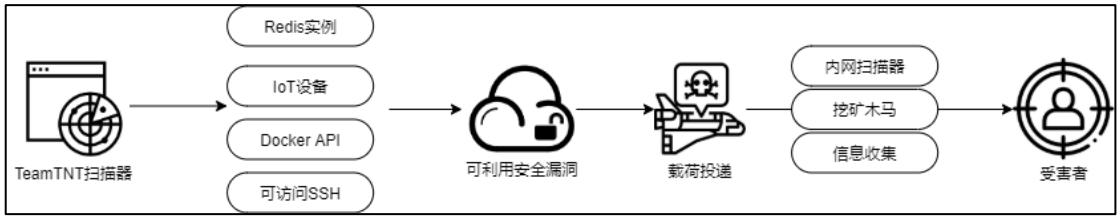
宽，目前该组织的恶意活动已经能够针对 AWS、Docker、GCP、Linux、Kubernetes 和 Windows 平台，覆盖几乎各类环境了。

TeamTNT 组织使用的部分导入工具包括：Masscan 和端口扫描程序，以搜索新的感染目标；用于直接从内存中执行 bot 的 libprocesshider；适用于多种 Web 操作系统的开源工具 Lazagne，可用于从众多应用程序中收集存储的凭据。

2021 年 5 月，研究人员发现 TeamTNT 黑客组织以 Kubernetes 集群为目标，攻击了近 50000 个 IP，且大部分 IP 来自中国和美国。

自 2021 年 7 月 25 日以来，TeamTNT 组织运行了一项针对多个操作系统和应用程序的新活动“Chimaera”，该组织使用新的开源工具从受感染的机器上窃取用户名和密码。活动中使用多个 shell 批处理脚本、新的开源工具、加密货币矿工、TeamTNT IRC bot 等，在全球范围内引起了数千起感染。

TeamTNT 主要使用扫描器来寻找攻击目标，在锁定攻击目标后，选取 payload 投递，入侵成功后部署挖矿和横向攻击工具，整体流程见下图：



图：TeamTNT 组织攻击流程

H2Miner 组织

H2Miner 挖矿组织自 2019 年开始活跃，攻击目标包括 Windows 和 Linux 服务器。该组织掌握了众多漏洞武器，擅长利用这些漏洞向受害机传播恶意脚本，进而部署挖矿木马，同时部署扫描器向外扩散。

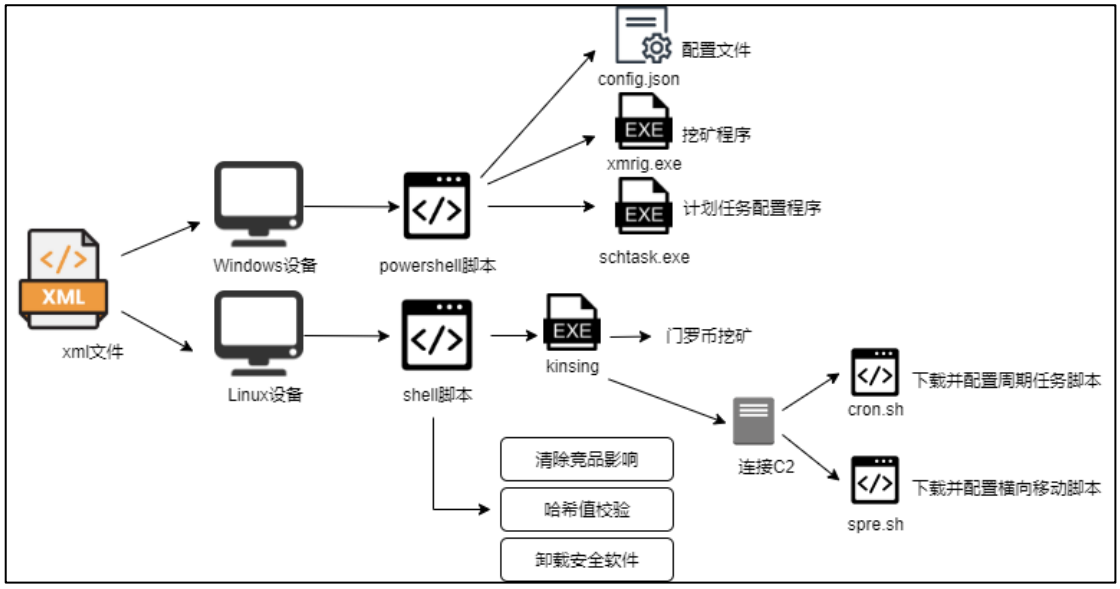
H2Miner 组织掌握的漏洞主要是 RCE 漏洞，包括：

- Supervisor 远程代码执行漏洞（CVE-2017-11610）
- Hadoop Yarn REST API 未授权远程代码执行漏洞（CVE-2017-15718）
- ThinkPHP 远程代码执行漏洞（CVE-2018-20062）
- 任意 PHP 执行漏洞（CVE-2017-9841）
- Solr dataimport 远程代码执行漏洞（CVE-2019-0193）
- Citrix ADC 和 Citrix Gateway 远程代码执行漏洞（CVE-2019-19781）
- Confluence 未授权远程代码执行漏洞（CVE-2019-3396）
- SaltSTack 远程代码执行漏洞（CVE-2020-11651(2)）
- WordPress 文件管理器远程代码执行漏洞（CVE-2020-25213）
- Confluence 服务器网络 OGNL 注入漏洞（CVE-2021-26084）
- Weblogic 未授权远程代码执行漏洞（CVE-2020-14882/14883）

2020 年 2 月，H2Miner 第一次被研究人员披露，此时 H2Miner 的攻击目标主要为 Redis 服务器。攻击者利用 Redis 的远程代码执行漏洞和弱口令入侵服务器，修改服务器设置，并下载名为 kinsing 的挖矿木马。

2020 年 11 月，研究人员捕获到 H2Miner 针对 Windows 平台攻击的变种挖矿木马。攻击者向主机发送一个构造好的数据包，触发漏洞后，主机会请求并解析执行远程服务器的 xml 文件。并在下载执行分发的恶意 powershell 脚本后，实现 Windows 平台的挖矿。

H2Miner 针对这两个平台的攻击流程在这之后没有出现大规模更新，整体流程见下图：



图：H2Miner 攻击流程

8220 挖矿团伙

8220 挖矿团伙疑似来自国内，自 2017 年起开始活跃，攻击目标包括 Windows 以及 Linux 服务器，该团伙早期会利用 Docker 镜像传播挖矿木马，后来又使用多种漏洞进行攻击，进而部署挖矿木马。研究人员后来在 2020 年发现其开始通过 SSH 爆破进行横向攻击传播。

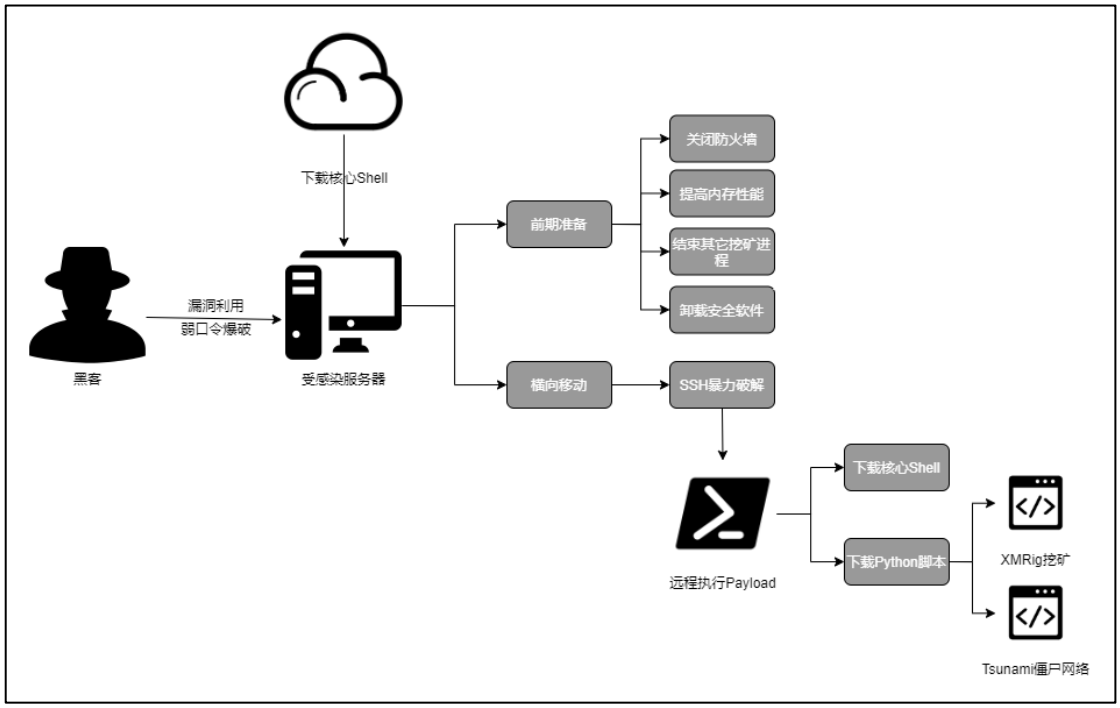
该团伙利用的漏洞包括：

- Confluence 远程代码执行漏洞（CVE-2019-3396）
- Weblogic 反序列化漏洞（CVE-2017-10271、CVE-2019-2725）
- WebLogic XMLDecoder 反序列化漏洞
- Drupal 的远程任意代码执行漏洞
- JBosss 反序列化命令执行漏洞
- Couchdb 的组合漏洞
- Redis 未授权访问漏洞
- ActiveMQ 未授权访问漏洞
- Hadoop 未授权访问漏洞

2018 年 8 月，研究人员首次发现 8220 团伙的攻击活动，攻击者利用 Hadoop Yarn 资源管理系统 REST API 未授权漏洞入侵服务器，部署了 Linux 挖矿木马。

2021 年 5 月，研究人员发现了 8220 团伙使用自定义挖矿程序“PwnRig”和 Tsunami IRC Bot 进行的恶意活动。PwnRig 是一个基于 XMRig 的自定义挖矿工具变体，试图隐藏其配置详细信息，并利用一个代理来防止公众监视其池详细信息。攻击者在受感染主机上配置挖矿环境，下载并执行正确版本的 PwnRig 矿工和 Tsunami IRC 机器人，获得持久性，并尝试横向移动。

该团伙首先利用 CVE-2019-7238 等远程代码执行漏洞入侵目标服务器，然后下载核心 Shell 程序并执行。Shell 程序在前期准备中会执行关闭防火墙、结束其它挖矿进程、卸载安全软件等操作。然后执行横向移动模块，该模块会利用 SSH 爆破等手段入侵其它内网主机，然后从远程服务器下载 Python 脚本执行挖矿和僵尸网络等操作。

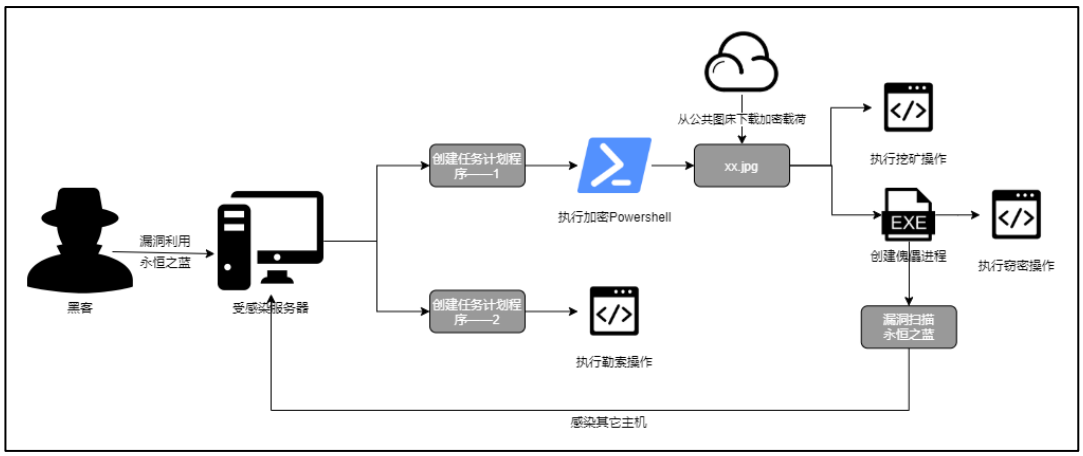


图：8220 挖矿团伙攻击流程图

匿影挖矿团伙

匿影挖矿团伙于 2019 年 2 月被发现，该团伙利用大量功能网盘和图床存放病毒模块和隐藏自身，而且利用“永恒之蓝”漏洞在企业内网进行横向传播，以在多个终端上执行挖矿作业。该团伙现已添加勒索软件攻击组件，研究人员发现其多次使用拼音首字母缩写，其勒索信中存在明显语法问题，推测该团伙为国内黑产组织。

该组织首先利用永恒之蓝漏洞入侵目标服务器，然后分别创建任务计划执行不同操作。任务计划程序会通过执行 Powershell 脚本，从公共图床下载加密载荷。然后分别执行挖矿、窃密和勒索操作。最后通过漏洞扫描程序以同样的方式感染其余内网用户。



图：匿影挖矿团伙攻击流程图

2. 挖矿木马家族

Crackonosh

“ Crackonosh ”是一种新型挖矿恶意软件，通过非法下载版本的流行游戏进行传播，如侠盗猎车手 V、NBA 2K19 等。恶意软件隐藏在游戏代码中，一旦下载游戏，恶意软件就会在后台秘密运行加密货币挖矿程序。“Crackonosh”在捷克民间传说中是“山神”的意思，因此研究人员推测恶意软件背后的黑客可能

是捷克人。Crackonosh 已感染 22.2 万台计算机，黑客已通过该软件获利 200 万美元。

Crackonosh 通过流行游戏软件的非法破解副本传播，安装后，恶意转件会搜索并禁用流行的防病毒程序，卸载所有安全软件并禁用 Windows 更新。Crackonos 在后台运行的加密货币挖掘程序会在受害者不知情的情况下减慢他们的计算机速度，受害者的计算机会由于过度使用而磨损组件，同时受害者的电费也会增加。

Lemon Duck

小黄鸭（LemonDuck）背后的攻击者为具有一定专业能力的境外黑产组织，曾发起或参与过大规模的网络攻击活动（如构建僵尸网络等）。如今，Lemon Duck 已发展成针对全球多个系统终端设备的有组织、有计划的、以挖矿为目的威胁组织。被其感染的受害者遍及全球，主要集中在亚洲地区，包括中国、新加坡、菲律宾等。

LemonDuck 最初是由针对“驱动人生”发起的供应链攻击演变而来的，攻击者利用“驱动人生”作为跳板，使蠕虫尽可能广泛地传播。Lemon Duck 在短时间内快速迭代更新，一直在积极更新新的漏洞利用和混淆技巧，它还通过其无文件矿工来逃避检测，现在已成为技术最高明的挖矿软件之一。

自 2020 年 8 月起，Lemon Duck 的感染传播速度疯狂增长，这可能得以与它使用了几乎所有可用媒介进行传播，例如热门主题钓鱼电子邮件、漏洞利用、无文件 powershell 模块和暴力破解等。

图：安恒信息捕获到的 Lemon Duck 恶意挖矿攻击行为

Lemon Duck 感染目标除了 Windows 平台之外，还包括运行嵌入式 Windows 7 系统的 IoT 设备、智能电视，智能扫描仪，工业 AGV 等，该组织还在近期新增了针对 Linux 设备的攻击模块。受到感染的机器中绝大部分来自于政府与企业。值得注意的是“小黄鸭（LemonDuck）”发动的攻击中会上传十分详尽的系统环境信息，这意味着为其筛选“特定目标”进行下一步定向攻击做好了准备。

Sysrv-hello

Sysrv-hello 僵尸网络于 2020 年 12 月首次被国内安全研究人员发现，由于具备木马、后门、蠕虫等多种恶意软件的综合攻击能力，使用的漏洞攻击工具也较新，目前已具备一定规模大小的僵尸网络，对政企机构危害较大。集合了木马、后门、蠕虫功能，旨在攻击的 Windows 和 Linux 企业服务器，并通过自传播式恶意软件载荷进行门罗币挖矿恶意活动。

Sysrv-hello 僵尸网络使用的是带有矿工和蠕虫（传播器）模块的多组件体系结构，后来升级为使用单个二进制文件，能够将挖矿恶意软件自动传播到其他设备。Sysrv-hello 的传播器组件能够主动扫描互联网，寻找更易受攻击的系统，利用其可远程执行恶意代码的漏洞，将受害设备添加到 Monero 采矿机器人大军中。

sysrvhello 是一种综合性僵尸网络，具有以下几个特点：

- 功能强大，集后门、木马、蠕虫等多种恶意软件为一体。
- 具有多种传播途径，包括通过 JBoss 远程命令执行、weblogic 远程代码执行、worldpress 暴力破解、thinkphp 远程代码执行、Redis 远程代码执行、Hadoop 未授权访问漏洞、Laravel 远程代码执行等漏洞传播。
- 跨平台僵尸网络，攻击目标包括 Windows 和 Linux 操作系统。

Sysrv-hello 僵尸网络的活动在 2021 年三月份激增之后，研究人员发现了被其使用的以下六种漏洞：

- Mongo Express RCE（CVE-2019-10758）
- XML-RPC（CVE-2017-11610）
- Saltstack RCE（CVE-2020-16846）
- Drupal Ajax RCE（CVE-2018-7600）
- ThinkPHP RCE（无 CVE）
- XXL-JOB Unauth RCE（无 CVE）

GuardMiner

GuardMiner 是自 2019 年开始活跃的挖矿木马，可以针对 Windows 平台和 Linux 平台进行攻击传播。GuardMiner 木马具有多种传播手法，包括：

- 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

2021 年 3 月，研究人员检测到了 GuardMiner 挖矿木马团伙的攻击活动，该团伙新增利用 Elasticsearch 远程代码执行漏洞（CVE-2015-1427），针对云上主机发起攻击，受害主机已过数万台。

四、挖矿木马的常见感染传播方式

这里将介绍挖矿木马的常见感染传播方式，如钓鱼邮件传播、非法网页进行传播、软件捆绑下载传播、僵尸网络下发及漏洞传播等手段。

1. 钓鱼邮件传播

攻击者伪造邮件，通过邮件附件传播恶意软件，或者通过邮件中的恶意链接诱导用户点击下载恶意软件，当用户打开恶意软件时，将导致系统被植入病毒，并执行脚本自动化横向渗透网络，部署挖矿程序进行作业获利。

2. 通过非法网页进行传播

攻击者通常会在色情网站和在线赌博等非法站点上内嵌网页挖矿脚本，由于这类站点打开后往往需要停留一段时间才出现界面，不会轻易引起用户的怀疑，这也是黑客选择这些非法网站部署网页挖矿的原因之一，用户一旦进入此类网站，JS 脚本就会自动执行，并占用大量的 CPU 资源以挖取门罗币，致使电脑出现卡顿。

3. 软件捆绑下载传播

在一般情况下，激活工具、破解软件、游戏外挂以及盗版游戏等来历不明的下载站点是感染挖矿木马的温床。攻击者通过捆绑下载方式植入恶意挖矿程序，当用户下载执行激活工具、破解软件、游戏外挂以及盗版游戏时，将执行恶意程序，在后台进行挖矿恶意活动。这些站点通常有着很高的下载需求，大量用户通过搜索引擎进入这些带毒网站，并且可能将其分享到各大技术论坛，形成二次传播的情况，造成广泛的影响。

4. 通过僵尸网络进行分发

攻击者会选择组建一个规模庞大的挖矿僵尸网络进行恶意活动，并通过各种方式入侵目标设备，例如网页挂马、MySQL 数据库弱口令爆破等方法传播僵尸程序，这些僵尸程序一般内置蠕虫模块，使受害机器成为新的攻击源，从而迅速传播爆发，并通过多个主机组成僵尸网络。攻击者可以在控制端中通过僵尸网络下发指令到受害主机，执行分发挖矿木马等恶意操作。目前，这种构建僵尸网络下发挖矿木马的方法已成为挖矿黑产团伙的主要手段。

5. 通过漏洞传播

通常，企业可能会提供对外的网站服务，但其服务器操作系统却存在仍未修补的漏洞，给了攻击者可乘之机。漏洞利用一直是挖矿木马用作传播感染的重要手段，其通过配备各种可利用的通用漏洞对目标网络资产进行扫描，如果设备未及时修补漏洞，将很有可能导致入侵事件的发生。

在众多类型的漏洞当中，最受挖矿木马欢迎的是 Web 应用漏洞，因为其适用性广，利用代码编写简单，可快速配备到各种攻击组件当中，例如最常见的 Weblogic 反序列化漏洞和 redis 未授权访问漏洞。另外，一些技术能力较强的僵尸网络则会在其攻击模块中集成多个漏洞探测模块，例如永恒之蓝、weblogic、MySQL、ThinkPHP、redis、Confluence 等漏洞。

以下表格是 2021 年常被挖矿木马利用的漏洞列表。

表：2021 年常被挖矿木马利用的漏洞列表

漏洞类型	漏洞编号	相关的恶意挖矿攻击家族
EternalBlue（永恒之蓝）系列漏洞	CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0148、ms17-010	MsraMiner，WannaMiner，CoinMiner、bulehero

Weblogic web 服务漏洞		MinerGuard
WebLogic Fusion 中间件远程代码执行漏洞	CVE-2019-2725	bulehero
WebLogic XML Decoder 反序列化漏洞	CVE-2017-10271	RunMiner、MinerGuard、ibus
Weblogic RCE 漏洞	CVE-2020-14882	LemonDuck、z0Miner、kworkerds
Weblogic 任意文件上传漏洞	CVE-2018-2894	ibus
Confluence RCE 漏洞	CVE-2021-26084	kerberods、z0Miner、iducker、h2miner、kwroksminer、8220Miner、mirai、BillGates
Confluence 未授权 RCE 漏洞	CVE-2019-3396	H2Miner
ThinkPHP web 服务漏洞		bulehero、MinerGuard、ibus
ThinkPHP 5 漏洞	CNVD-2018-24942	buleHero
ThinkPHP 5.X RCE 漏洞		H2Miner、GuardMiner
PHPUnit RCE 漏洞	CVE-2017-9841	H2Miner
ElasticSearch RCE 漏洞	CVE-2015-1427	MinerGuard
ElasticSearch 未授权访问漏洞	CVE-2014-3120	MinerGuard、CryptoSink
Hadoop Yarn 未授权访问漏洞		systemdMiner、8220Miner、MinerGuard
Docker 未授权访问漏洞等多个 web 服务漏洞		8220Miner、TeamTNT
Spring RCE 漏洞	CVE-2018-1273	MinerGuard
java 反序列化漏洞		ibus
Jenkins RCE 漏洞	CVE-2019-1003000	ImposterMiner
redis 未授权访问漏洞		ibus、MinerGuard、H2Miner
SSH 免密登录漏洞		SysupdataMiner
Supervisord RCE 漏洞	CVE-2017-11610	H2Miner
Drupal 框架漏洞	CVE-2018-7600	MinerGuard

Struts2 RCE 漏洞	CVE-2017-5638	BuleHero
Redis 4.x/5.x 主从同步命令执行漏洞	CNVD-2019-21763	H2Miner
Windows 打印机远程代码执行漏洞 PrintNightmare	CVE-2021-34527	紫狐
文件管理器插件中的文件上传漏洞	CVE-2020-25213	H2miner
Atlassian Jira 未授权模板注入漏洞	CVE-2019-11581	WatchBog
Exim 邮件服务器 RCE 漏洞	CVE-2019-10149	WatchBog
Apache Solr Deserialization RCE 漏洞	CVE-2019-0192	WatchBog
Windows 内核漏洞 BlueKeep	CVE-2019-0708	WatchBog
SaltStack RCE 漏洞	CVE-2020-11651、CVE-2020-11652	H2Miner

6. 利用软件供应链感染传播

供应链感染可在短时间内获得大量的计算机资源，而备受黑产青睐，例如近日发生的“恶意 NPM 软件包携带挖矿恶意软件”安全事件就证明了通过开源软件包存储库进行软件供应链攻击的有效性，事实上在这之前就发生过多起类似的安全事件，例如 2021 年 6 月初研究人员就曾在 PyPI 软件包仓库中发现恶意挖矿程序。

7. 通过浏览器插件传播

攻击者通过将恶意插件伪装成正常的 Chrome 浏览器插件，上传到插件商店供用户使用，而该插件实则上被内置了恶意代码，当用户下载安装后，将执行挖矿等恶意操作。例如之前就曾有一款超过 10 万人下载的浏览器插件被发现存在恶意代码，插件名为 Archive Poster，原本的功能是协助用户在社交平台汤不热（Tumblr）上进行多账号协作，该恶意插件会劫持电脑资源去挖掘虚拟货币 Monero，背地里却在未经用户同意的情况下，利用 Coinhive 软件开始挖矿作业。

谷歌浏览器 Chrome 具备丰富的插件功能，有来自世界各地开发者提供的丰富的扩展程序或应用，极大地方便了用户的使用，但由于浏览器插件的安全性一直没有引起重视，导致滥用浏览器插件进行恶意活动的安全事件仍在不断发生。

8. 容器镜像污染

随着云原生容器的应用越来越流行，黑产团伙也将目光瞄向了这个领域。在云容器当中，最为著名的是 Docker Hub 公共容器镜像仓库，黑产团伙并没有放过这个机会，他们利用 Docker Hub 上传恶意挖矿镜像，污染容器镜像，当用户下载执行镜像时，将导致其 docker 主机被感染，攻击者还会通过容器服务器的漏洞传播蠕虫病毒，以尽可能地感染更多的 docker 主机，并执行挖矿程序进行牟利。

由于攻击者可以制造多个恶意镜像扩大污染源，导致实际上的感染和影响范围比预想的还要广泛，例如专门针对云容器的 TNTteam 黑产挖矿团伙就经常使用这种方法作为其感染手段。这种容器镜像污染的攻击方式所造成的下载传播量通常能达数十万，甚至数百万以上，给云原生环境造成严重的污染。

9. 利用移动存储介质传播

在 2015 年就出现了通过 USB 设备和其他可移动媒体传播挖矿程序的攻击案例，例如著名的 Lemon Duck 挖矿团伙就曾利用 CVE-2017-8464 快捷方式漏洞作为感染传播的途径。通过将恶意的 Windows*.lnk 快捷方式文件和恶意 DLL 文件一起植入文件夹中，当使用解析.lnk 快捷方式文件打开驱动器时，快捷方式将执行恶意的 DLL 组件，从而触发 CVE-2017-8464LNK 远程执行代码漏洞，导致可移动 USB 驱动器和网络驱动器被感染。

在用户不知道移动介质已被感染的情况下，很可能会将受感染的设备携带到其他不联网的环境中，导致原本安全的环境被病毒渗透，从而扩大内部感染范围，并影响工作环境的正常运作。

五、恶意挖矿趋势解析

1. 虚拟货币价格激增，通过各种手段提高挖掘效率

攻击者会尝试使用各种技术以提高挖矿效率，例如研究人员发现的一个 Golang 蠕虫挖矿木马就使用了一种新策略提升挖矿效率。

这个挖矿木马通过特定型号的寄存器（MSR）驱动程序来禁用硬件预取器。硬件预取器是一种新的技术，处理器会根据内核过去的访问行为来预取数据，处理器（CPU）通过使用硬件预取器，将指令从主内存存储到二级缓存中。然而，在多核处理器上，使用硬件预取会造成功能受损，并导致系统性能整体下降。XMRig 需要依赖机器的处理能力来挖掘 Monero 币，禁用 MSR 能够有效阻止系统性能下降，从而提升挖矿效率。

文中描述的这种挖矿方式虽然不会对设备造成损害，但不排除攻击者未来可能会为了提升挖矿效率而做出一些加速设备损耗的操作，例如解除硬件性能限制，超频使用等。

2. 黑吃黑，黑产组织争夺挖矿资源

在恶意挖矿活动中，可能会出现两个挖矿家族相互争夺受害计算机资源的情况，这种较量通常在 Linux 和云环境中进行，挖矿木马会利用多种手法清理或阻止、干扰受害主机上其他家族的挖矿行为，从系统中删除竞争对手来独享资源，常见手法有以下几种：

1. 配置 IP 筛选器，阻止竞争对手向指定矿池 IP 地址发起 TCP 连接；
2. 删除竞争对手的挖矿进程，并将该进程和其使用的 IP 添加到黑名单，禁止其进程运行或发起网络连接；
3. 修复访问权限漏洞，防止系统感染其他恶意软件；
4. 删除竞争对手添加的驻留手段，例如注册表、启动服务、计划任务等。

其中，比较广为人知的是 Pacha 和 Rocke 黑产组织的云上资源争夺事件，这两个组织所使用的技术、战术、方法都极其相似，这种同行之间相互竞争的现象有助于提高操作员的技能水平。Pacha 组织还特别关注识别和删除 Rocke 的挖矿活动，以试图清除对方，这两个组织都是通过进行大规模扫描来寻找开放或未打补丁的 Linux 服务器和云端服务，然后使用多功能恶意软件感染目标设备。Pacha 还具有一个 IP 黑名单列表，该名单中的 IP 是 Rocke 组织过去在挖矿活动中所使用的网域。当 Pacha 感染受害系统后，将自动移除 Rocke 挖矿程序，而且受感染系统无法再连接黑名单中的网域。虽然 Rocke 组织也使用从受感染的服务器上清除竞争对手的手法，但与 Pacha 组织相比，规模相对较小。

这种黑吃黑争夺设备资源的情况在物联网上也经常发生，因为设备资源数量是有限的，也经常会发生多个挖矿家族感染同一台设备的情况，这种时候只有技术高明的一方才能存活下来，因为你不清除对方，就会被对方清除，这种同行竞争的情况也逐渐成为了一种趋势。

3. 利用工业控制系统进行挖矿

随着时间流逝，挖矿活动所产出虚拟货币越来越少，对算力的需求越来越大，一些攻击者已经不满足选择诸如 PC 或移动设备作为其挖矿工具，而是将目光瞄向了具有高性能、高处理能力的基础设施。工业控制系统的内部网络还可能存在过时或未打补丁的软件，因为部署新的操作系统和更新可能会无意中破坏关键的传统平台，所以系统可能仍停留在旧版本当中。

在 2017 年起，研究人员就发现针对工业控制系统的挖矿攻击有所上升，这类攻击会对工业企业的计算机造成大量负载，由此对企业 ICS 组件的运行产生负面影响并威胁其稳定性，从而构成更大的威胁。而在 2018 年的另一个工业系统进行恶意挖矿的事件中，犯罪分子还在欧洲自来水公司控制系统中进行加密劫持挖矿，该活动降低了自来水公司管理公共设施的能力。攻击者还使用了检测和禁

用标记自身的安全防御工具操作，这相当于被其他类型的网络威胁开启了大门，导致原本就感染挖矿程序的系统更加脆弱。

对于从事恶意挖矿活动的攻击者而言，工厂是一个诱人的目标，由于许多基线操作不会使用大量处理能力，但会消耗大量电力，这使得挖掘恶意软件能够相对容易地掩盖其 CPU 和功耗，即使查到到系统异常，但排查控制系统上的网络威胁也需要相当多的时间成本。另外，挖矿活动还增加系统处理器和网络带宽的使用，这可能会导致工业控制应用程序因系统过载而无响应、暂停甚至崩溃，导致工厂操作员降低或失去管理工厂的能力，严重时甚至会破坏和影响业务及基础设施的关键流程。

六、防范建议

无论是在本地系统还是通过浏览器被恶意挖矿，一般事后都较难通过手动检测找到入侵路径，而且也很难快速排查出高 CPU 使用率的原因。因为恶意挖矿软件可能会隐藏自身或伪装成合法的进程，以避免被用户删除。当计算机以最大性能模式运行时，系统速度将会非常慢，因此更难排除故障，所以预防恶意挖矿软件的最好方法，是在成为受害者之前采取安全措施。

最常见的方法是在常用的浏览器中阻止 JavaScript 脚本运行。虽然该功能可以有效阻止路过式网页挖矿攻击，但同样也会阻止用户使用浏览器插件功能，另外一种方法是安装专门用于防范浏览器挖矿的拓展程序，例如“No Coin”和“MinerBlock”，两者都有适用于 Chrome、Firefox 和 Opera 的扩展程序。

另一种防范本地系统感染恶意挖矿的方法与常规恶意软件基本相同：

1. 提高个人安全意识，从正常的应用市场和渠道下载安装应用程序，不轻易安装来历不明的第三方软件，或随意点击和访问一些具有诱导性质的不良网页；
2. 安装终端安全防护并定时进行全盘查杀；

3. 及时修复系统漏洞，更新系统版本、软件版本和应用版本。

七、总结

恶意挖矿产业背后的攻击者一直在积极提高技能水平，并不断更新其攻击手法，并开始针对各种平台的硬件设备，其功能迭代及漏洞配备速度将更加迅速。

随着数字化技术的不断发展，网络威胁对于大众的影响越来越与现实紧密相连，虽然恶意挖矿活动所造成的破坏性远低于勒索软件等恶意软件，但是其造成的广泛影响和感染数量远超于其他恶意软件，是一种不容小觑的网络威胁。

关于 CNCERT

国家计算机网络应急技术处理协调中心（英文简称 CNCERT/CC），成立于 2001 年 8 月，为非政府非盈利的网络安全技术中心，是中国计算机网络应急处理体系中的牵头单位。作为国家级应急中心，CNCERT/CC 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，运行和管理国家信息安全漏洞共享平台（CNVD），维护公共互联网安全，保障关键信息基础设施的安全运行。

联系方式：

电子邮件：cncert@cert.org.cn

电话：+8610 82990999，82991000（EN）

传真：+8610 82990399

关于杭州安恒信息技术股份有限公司

安恒信息成立于 2007 年，于 2019 年登陆科创板，是 2020 年信息技术产业最具成长上市公司。作为行业领导者，已形成覆盖网络信息安全全生命周期的产

品体系，是国家级核心安保单位，参与了近乎全部国家重大活动网络安保，实现零失误。

网址：www.dbappsecurity.com.cn

客户服务热线：400 6059 110