


《2021 年恶意挖矿威胁趋势分析报告》

C CE 与安 信 合发布

2022 年 4

目录

- 4
- 一、 简介 5
 - 1. 、 与加密货币 5
 - 什么 加密货币? 5
 - 什么 ? 5
 - 什么 ? 5
 - 2. 6
 - 3. 如何工作 ? 6
 - 4. 为什么会 件? 6
 - 5. 危害 7
- 二、2021 年 四季度 国主 势分 7
 - 1.2021 年 四季度 主 分 8
 - 2.2021 年 四季度 主 分 11
- 三、 威 17
 - 1. 团伙 17
 - 17
 - H2 18
 - 8220 团伙 20
 - 匿 团伙 22
 - 2. 家 22
 - C 22
 - L D 23
 - 24
 - G 25
- 四、 常 26
 - 1. 件传 26
 - 2. 传 26

- 3. 件 下 传 26
- 4. 僵尸 分发 27
- 5. 传 27
- 6. 利 件供应 传 29
- 7. 器 件传 29
- 8. 容器 像 30
- 9. 利 动存储介 传 30
- 五、 势 31
 - 1. 币价 增, 各 31
 - 2. 吃 , 产 争夺 31
 - 3. 利 工业 制 32
- 六、  33
- 七、 34
- 关于 C CE 34
- 关于 州安 信 份 公司 34

摘要

加密货币发展以及币价值，、业务了分子，导动在全各地。一 中常 威 别， 威 具 好 和坏， 并 久 在 备上， 侵占 备加密货币，当攻击 侵占 备 多，其 利就 多，因此 不少 客团体入侵从 实现牟利操作。

根据 C CE 和安 威 情报中心 测数据， 合发布《2021 年 威 势分 报告》， 报告 先将介 动 关介， 对 2021 年 四季度 国主 势 分，接 从 威、 传 以及 势 向 会公众发布 2021 年 威 势分 情况。

一、挖矿活动介绍

1. 挖 、 恶意挖 与加密 币

什么 加密 币？

加密 币 没 物 形 ， 且仅存在于 数字 币，因其前 、 价值增 潜力和匿名 广受欢 。最 名以及最 功 加密 币 2009 年 世 比 币，比 币 功 发了数以千 其他加密 币 ，截止 2021 年 11 ，全 加密 币 9000 ， 市值 2.7 万亿 元，并且 处于不 断增 当中，来 世 各地 投 使 加密 币来 买卖以及投 。

加密 币 “密 学”和 “ 币众 攻 学” †††€E†Tr!#!\$...

2. 感染挖矿木

根据某些 ， 可以初步怀疑 备已 件，例如 C 使 大幅 于正常数值， 100%，以及 热、 度变慢、 备比正常情况下更 地使 冷却 扇 ，即便 启也不 决 ， 些 显 状。

其中一些 家 会对 为 制，只在 C 时 ，当 查 C 时，将停止 ，导 很 察 否存在 异常 为。

3. 恶意挖 是如何工作 ？

常分为基于 器 驱动 和二 制文件 。

驱动 与 广告攻击 似，攻击 将一 J 代 嵌入 到 标 中。当 访 时将执 J 脚本， 加密 币 ，缺 退出 时将 束 。

二 制文件 与 不同，一旦 序， 受害 备将开始全天候 币 ，同时将 藏在后台，并启 多 久 在 标 备上 ，直到威 清除为止。另外， 序所针 对 备 常 具备 和强大 服务器 ，因为其可以更 地 产出 币。

4. 为什么会感染挖 木 件？

件与其他 家 一样，可以借助多 传 ，例如 件附件、植入 站，或与来历不 三 应 下 传 ，如 工具、游戏外挂 序、盗版 件、 器拓展 序将威 下发到 标环境。

一些算力较强的产团伙则会配备 C 作入侵企业，在标中图扩散序。

5. 恶意挖矿危害

作为受害者，常不会注意到自己，因为大多数件具备藏功，但并不味它不会对你备损害。实际上，对窃取会大幅降低度，加大力消，并缩备使寿命，从响业务或产环境正常营。

受备常会产生以下较为显负响：

- 度变慢
- 增加处器使
- 备热
- 增加力消

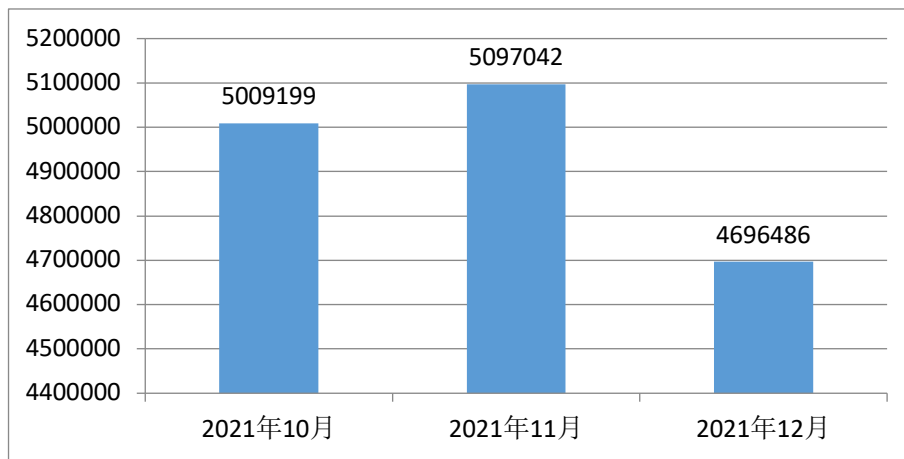
动对单台备响耐较小，但如果环境遭遇大围传情况，将会出现显卡顿、慢异常现，导降低死情况发，如果来公事业、制业、业、金融业实体，可响其业务和数据安全，从引一系列连锁反应，以评估营、产损失。

二、2021 年第四季度我国主机挖矿态势分析

C CE 对及为开展抽样测，形 2021 年四季度国主势分。下分别从主及池服务器两个维度开展分。

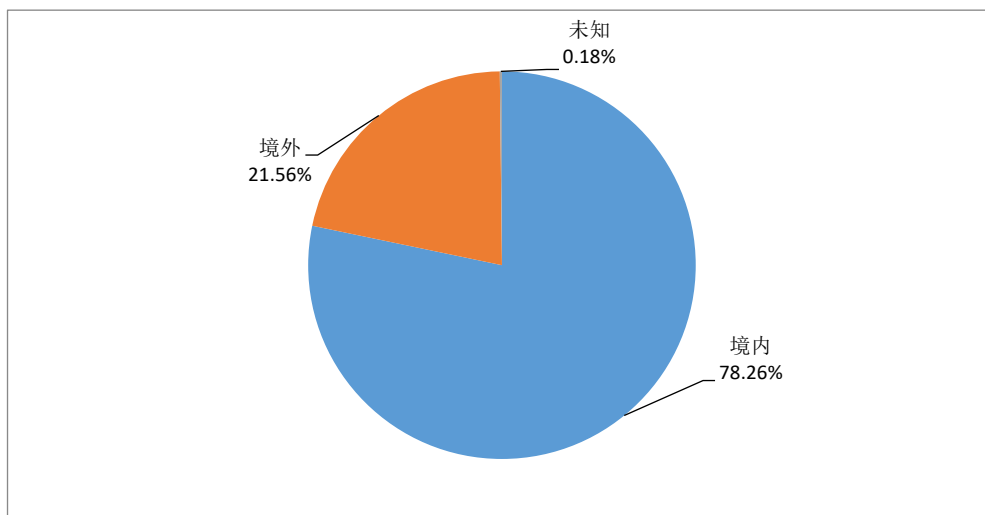
1.2021 年 四季度活 挖 主机分析

2021 年 四季度, C CE 测到涉及 信 为 1309 亿次, 共涉及约 1072 万个 主 I 。其中 测发现 主 数量按 分布如下图所示, 可以发现 11 份 事件较多, 12 份较少。



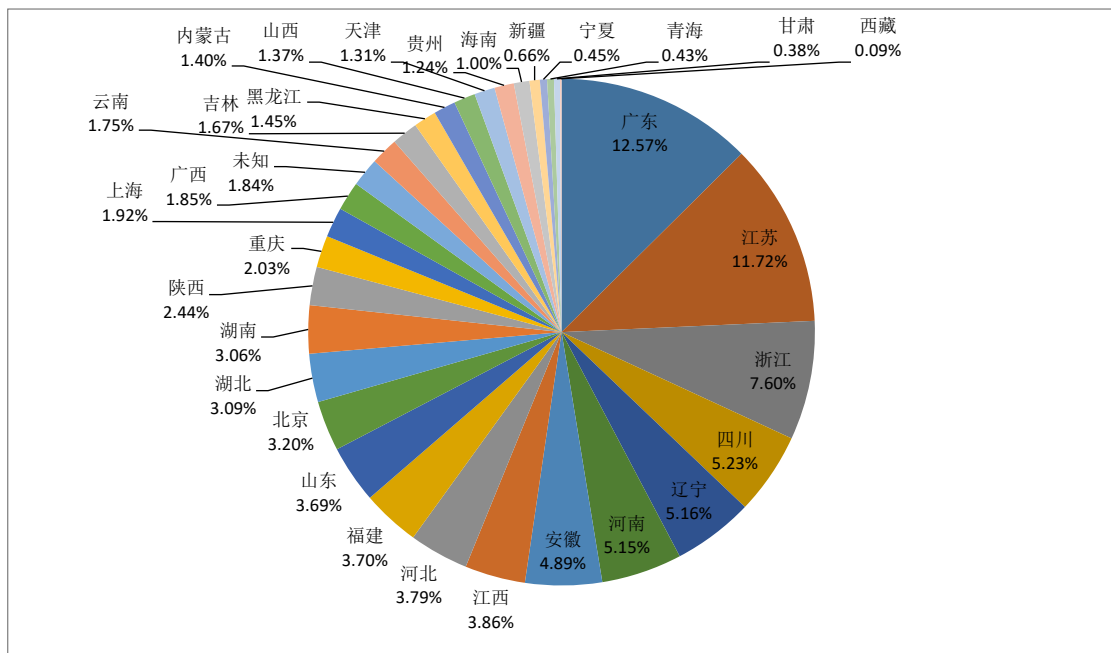
图：2021 年 四季度 主 I 数量按 分布

如下图所示, 在 测发现 1072 万个 主 I 中, 78.26%为境内I 。



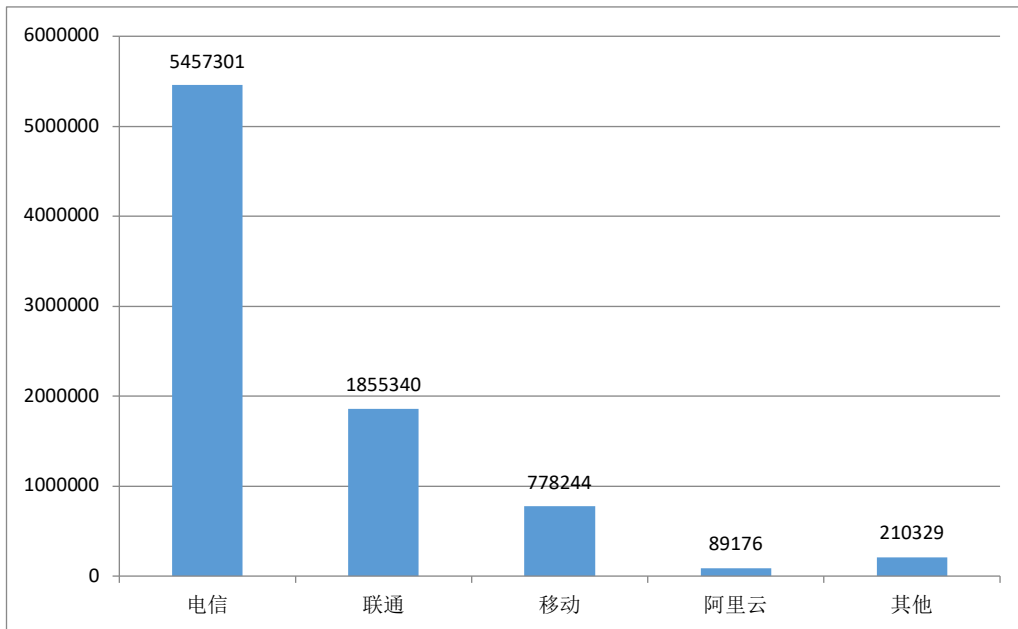
图： 主 I 境内外分布

如下图所示, 在境内 主 I 中, 归属于广东、江苏、浙江 省份 主 I 较多, 分别占 12.57%、11.72%、7.6%。



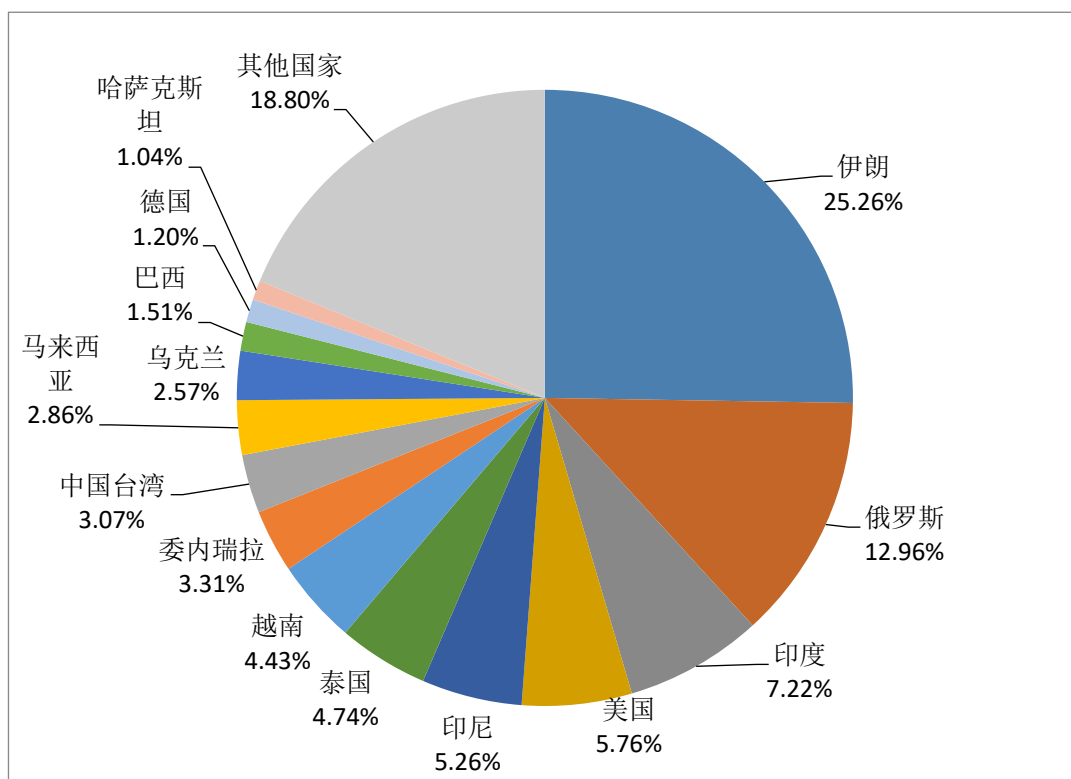
图：境内 主 I 按省份分布

此外，信、营商 主 I 较多。信营商境内主 I 546 万个，占本季度主 I 数量 65.04%， 189 万个，占 22.11%。



图：境内 主 I 所属 营商分布

21.56% 境外 主 I 中，来 伊朗、俄罗斯、印度 国家 I 较多，分别占 25.26%、12.96%、7.22%。



图：境外 主 I 按国家和地区分布

值得关注 ，部分 主 I 常 ，发 较多 与 池服务器 连接。以下 20 个 I 为值得关注 主 I 地址。

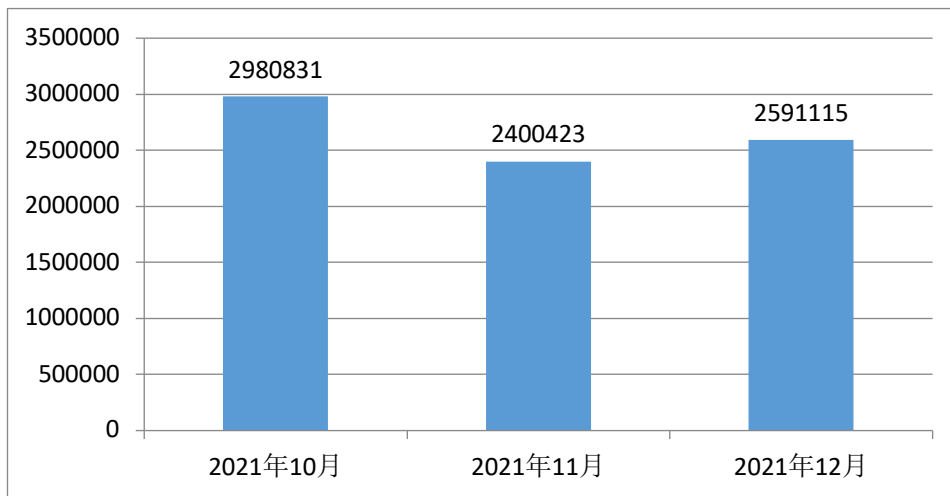
表： 主 I 20

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

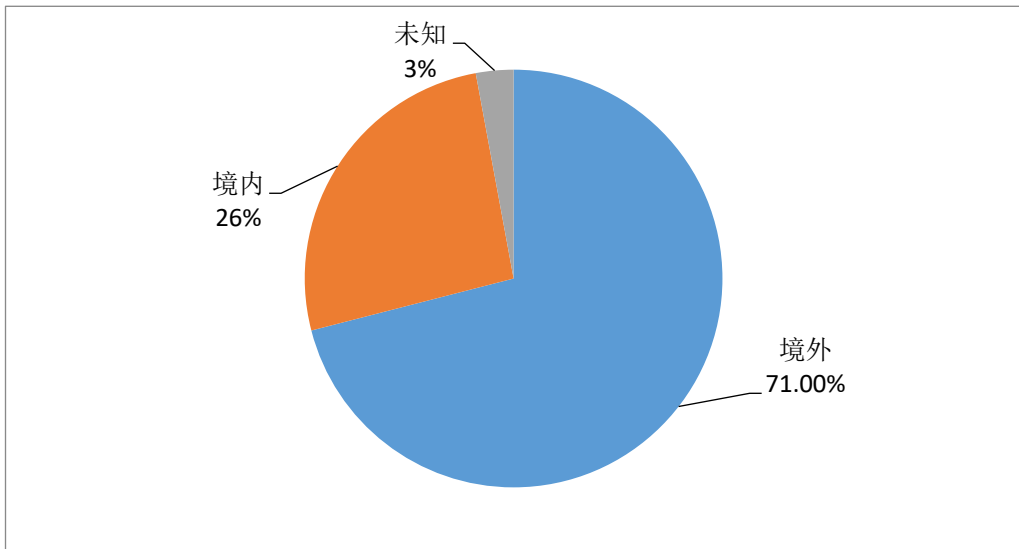
2.2021 年 四季度 池服务 分析

2021 年 四季度，C CE 测发现约 585 万个 池服务 I 。其中 池服务 I 数量按 分布如下图所示：



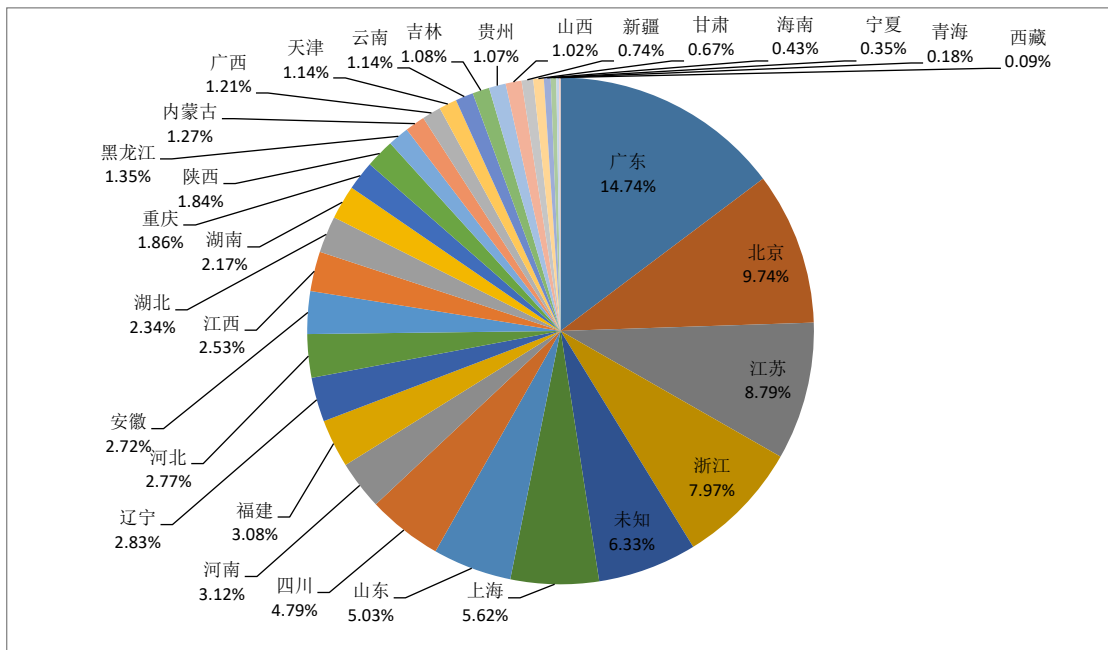
图： 池服务 I 数量按 分布

585 万个 池服务 I 中，26.10%为境内 I 。



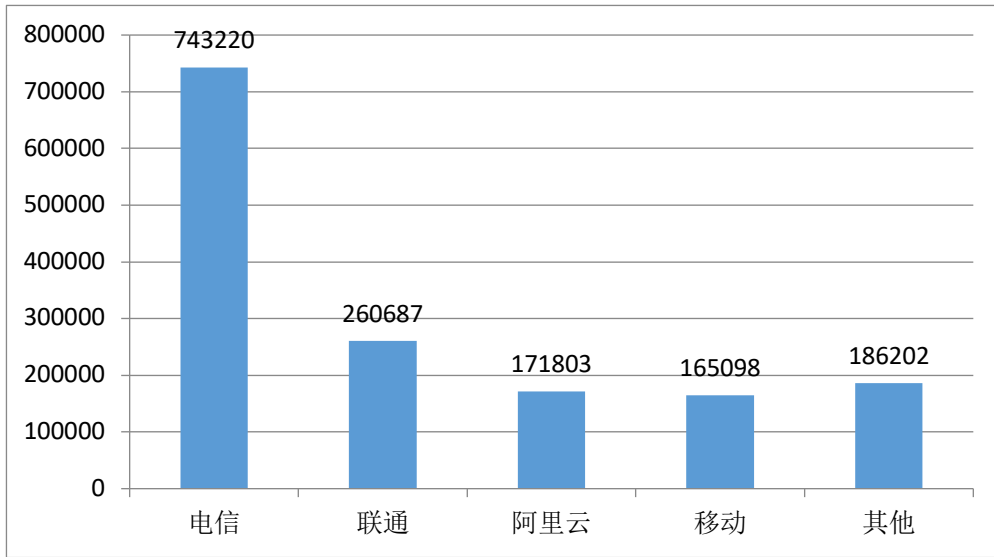
图： 池 I 境内外分布

境内 池以广东、北京、江苏 服务 I 较多,分别占 17.40%、17.33%、9.93%。



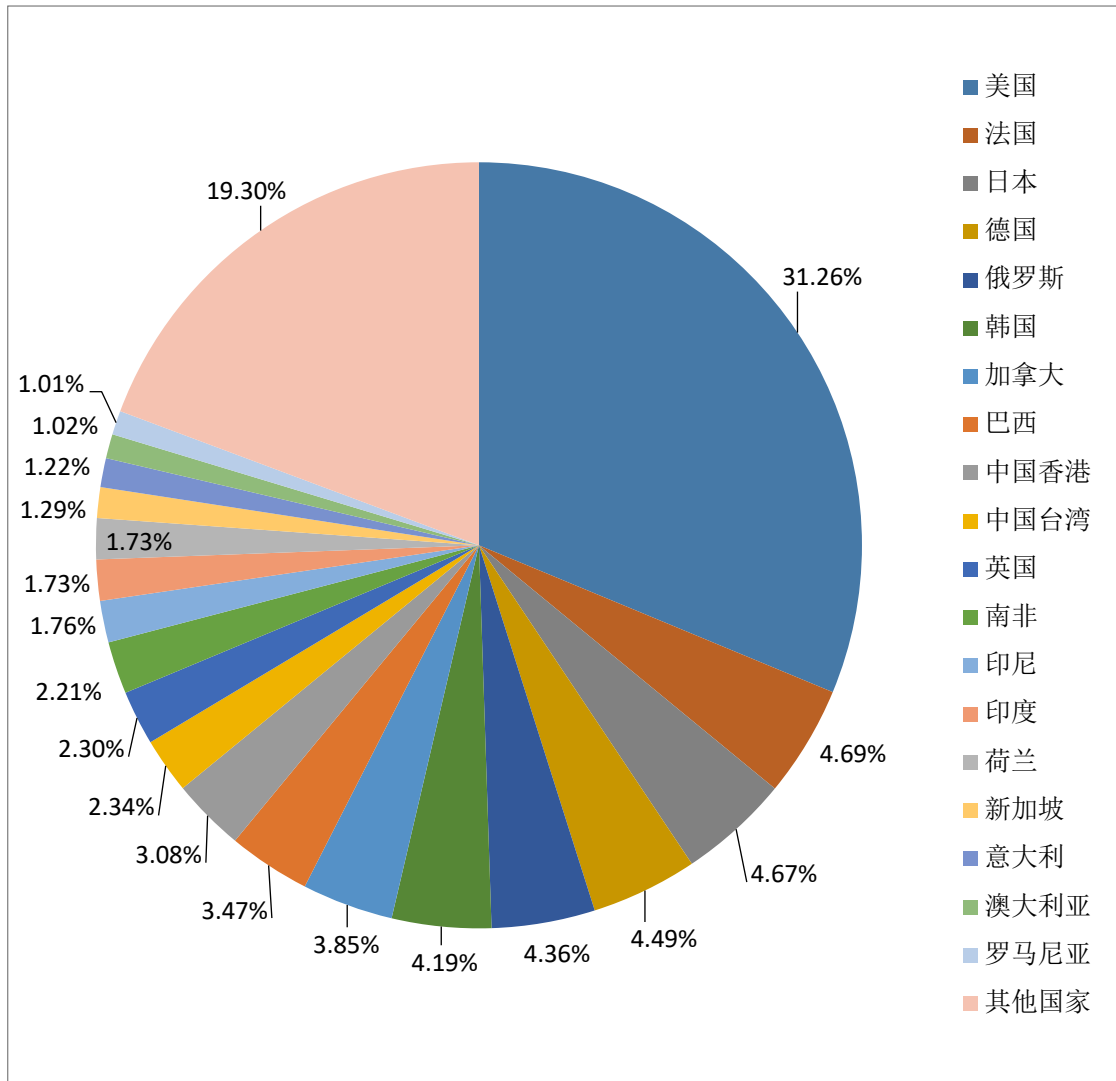
图：境内 池 I 按省份分布

此外，信、营商境内池I较多。其中I地址营商为信境内池I约74万个，占2021年四季度所池服务I48.67%，其次为和阿里云，约26万个和17万个，分别占17.07%、11.25%。



图：境内 ICP 所属 运营商分布

在 71% 境外 ICP 服务 I 中，中国 ICP 数量最多，共测发现约 130 万个 I，占本季度所测 ICP 数量 31.26%、其次为美国和日本，I 数量 194817 个、193995 个，分别占本季度 ICP 数量 4.69%、4.67%。



图：境外池服务I按国家和地区分布

值得关注，部分池I常，较多主I与其信连接，下表为池关列表。

表：池I 20

IP	地理位置	通联次数	历史解析域名
138. 68. 44. 84	美国	1568961	. .
157. 245. 77. 105	美国	1562371	. . . 3 .
96. 126. 117. 129	美国	1560309

194. 195. 223. 249	德国	1183541
139. 177. 196. 162	美国	1180841
139. 59. 109. 18	新加坡	1116214
139. 59. 182. 191	英国	923187
159. 89. 161. 1	印度	922308
159. 203. 63. 223	加拿大	724273
109. 74. 196. 239	英国	713608
134. 209. 40. 198	美国	707798
199. 247. 27. 41	兰-	464821

		 2. .
178. 128. 242. 134	兰-	452515 2. - . . .
203. 107. 32. 162	中国	409164 - . 2 2 . . 2 . - . 2 . . 2 - . 2 . . 2 . - . 2 . . 2 . . 2 . . 2 . - . 2 . . . 2 . 256 . 2 . . 2 . . 2 . . 2 . - . 2 - . 2 .
50. 116. 34. 212	美国	332654
106. 54. 138. 202	中国	280037	. . .
47. 241. 198. 198	美国	256814	. 3 . . 3 .

			- . 3 .
47. 241. 208. 216	美国	247972	. 3 .
			. 3 .
			- . 3 .
			. 3 .
			. 3 .

39. 107. 236. 106

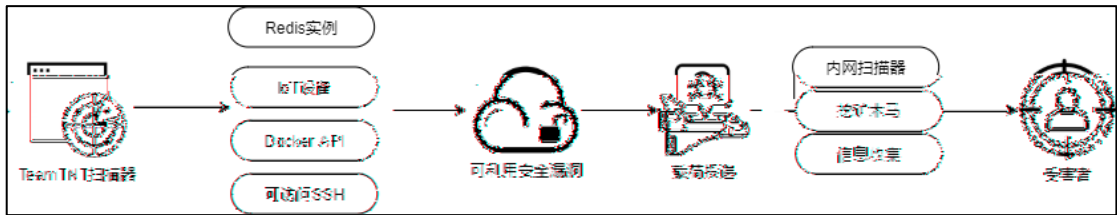
宽，前 动已 够针对 A 、D 、GC 、L 、K 和 平台，覆盖几乎各 环境了。

使 部分导入工具包括： 和端口扫描 序，以搜索新 标； 于直接从内存中执 于多 操作 开 工具 L ，可 于从众多应 序中 存储 凭据。

2021 年 5 ，研究人员发现 客 以 K 群为 标，攻击了近 50000 个 I ，且大部分 I 来 中国和 国。

2021 年 7 25 日以来， 了一项针对多个操作 和 应 序 新 动“C ”， 使 新 开 工具从受 器上窃取 名和密 。 动中使 多个 批处 脚本、新 开 工具、加密 币 工件 I C ，在全 围内引 了数千 。

主 使 扫描器来寻找攻击 标，在锁定攻击 标后， 取 投递，入侵 功后部署 和横向攻击工具，整体 下图：



图： 攻击

H2Miner

H2 2019 年开始 ，攻击 标包括 和 L 服务器。 掌握 武器，擅 利 些 向受害 传 脚本， 部署 ，同时部署扫描器向外扩散。

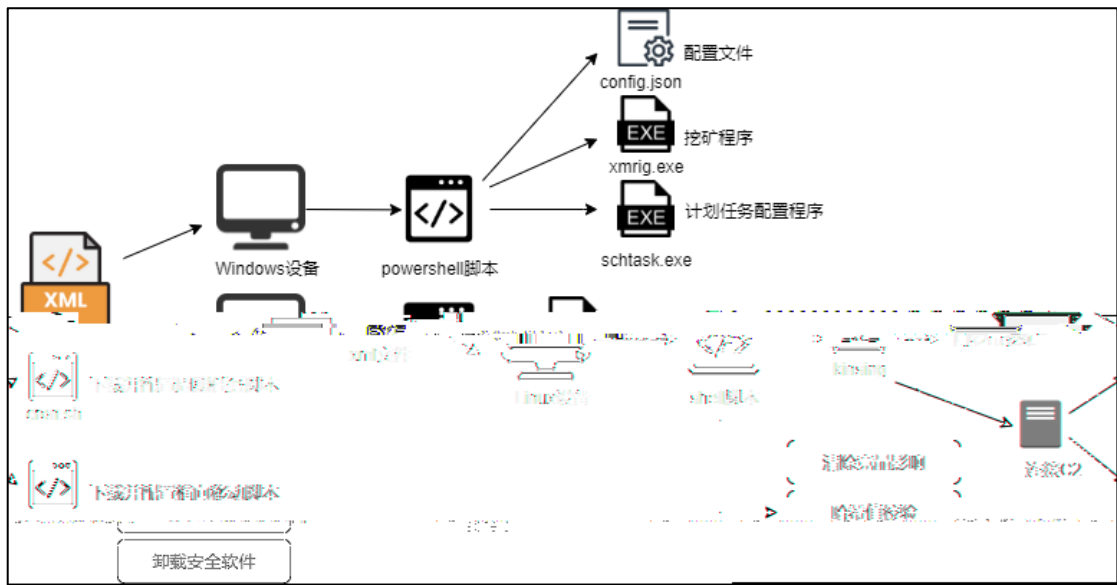
H2 掌握 主 CE ，包括：

- 执 (C E-2017-11610)
- H E A I 未授权远 代 执 (C E-2017-15718)
- H 远 代 执 (C E-2018-20062)
- 任 H 执 (C E-2017-9841)
- 远 代 执 (C E-2019-0193)
- C ADC 和 C G 远 代 执 (C E-2019-19781)
- C 未授权远 代 执 (C E-2019-3396)
- 远 代 执 (C E-2020-11651(2))
- 文件管 器远 代 执 (C E-2020-25213)
- C 服务器 G L 注入 (C E-2021-26084)
- 未授权远 代 执 (C E-2020-14882/14883)

2020 年 2 月，H2 一次 研究人员披露，此时 H2 攻击 标 主 为 服务器。攻击 利 远 代 执 和弱口令入 器，修改服务器 ，并下 名为 。

2020 年 11 月，研究人员捕 到 H2 针对 平台攻击 变 。攻击 向主 发送一个构 好 数据包，后，主 会请求并 执 远 服务器 文件。并在下 执 分发 脚本后，实 现 平台 。

H2 针对 两个平台 攻击 在 之后没 出现大规模更新，整体 下图：



图：H2 攻击

8220 团伙

8220 团伙 似来 国内， 2017 年 开始 ，攻击 标包括 以及 L 服务器， 团伙早 会利 D 像传 ，后来又使 多 攻击， 部署 。研究人员后来在 2020 年发现其开始 H 爆 横向攻击传 。

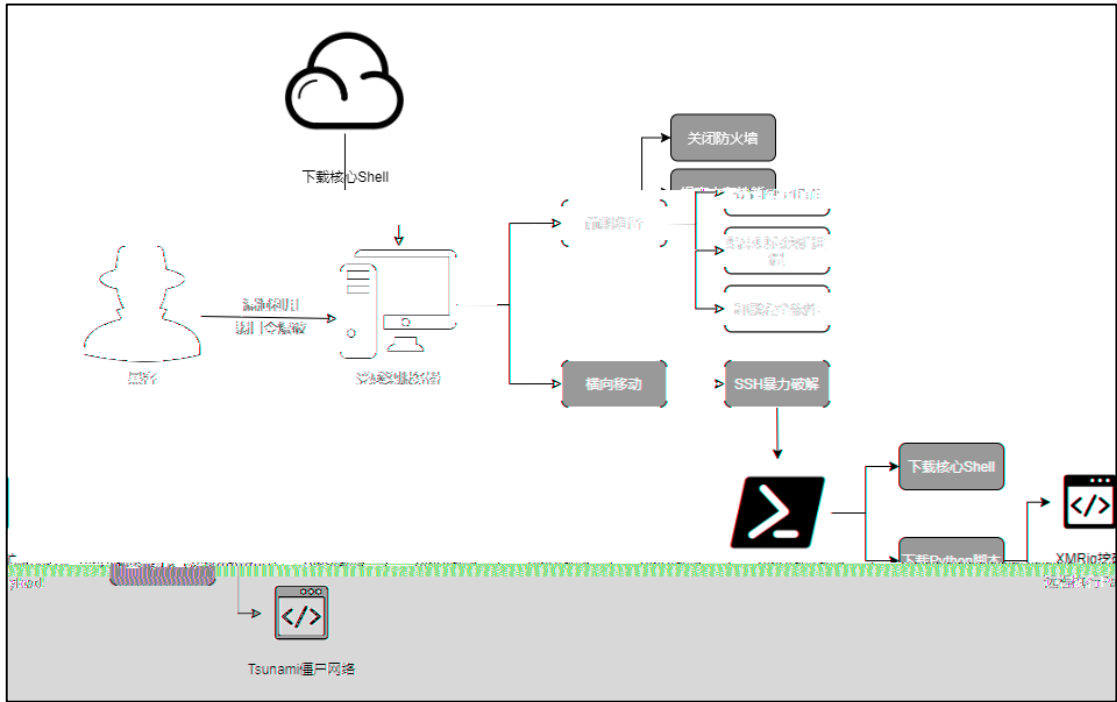
团伙利 包括：

- C 远 代 执 (C E-2019-3396)
- 反序列化 (C E-2017-10271、C E-2019-2725)
- L LD 反序列化
- D 远 任 代
- JB 反序列化命令执
- C 合
- 未授权访
- A 未授权访
- H 未授权访

2018 年 8 月，研究人员首次发现 8220 团伙攻击活动，攻击利 H 管 E A I 未授权入侵服务器，部署了 L 。

2021 年 5 月，研究人员发现了 8220 团伙使 定义 序“ ”和 I C B 动。 一个基于 定义 工 具变体，试图 藏其配 详细信 ，并利 一个代 来 止公众 视 详细信 。攻击 在受 主 上配 环境，下 并执 正 版本 工 和 I C 器人， 得 久 ，并尝试横向 动。

团伙 先利 C E-2019-7238 远 代 执 入侵 标服务器，然 后下 核心 序并执 。 序在前 准备中会执 关闭 防火墙、 束 其它 、卸 安全 件 操作。然后执 横向 动模块， 模块会利 H 爆 入侵其它内 主 ，然后从远 服务器下 脚本执 和僵尸 操作。

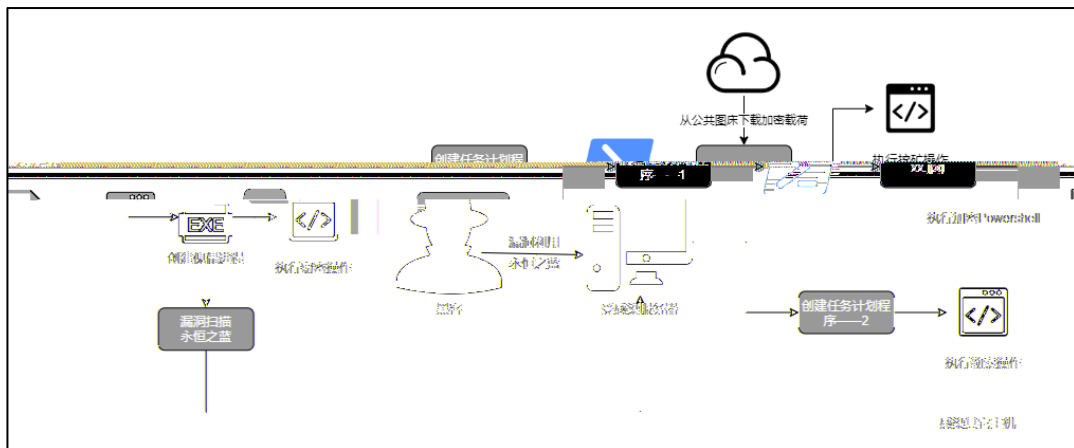


图：8220 团伙攻击 图

匿 团伙

匿 团伙于 2019 年 2 月 发现， 团伙利用 大量功 盘和图床存放病毒模块和 藏 ， 且利用 “永 之蓝” 在企业内 横向传 ， 以在多个终端上执 作业。 团伙现已添加勒索 件攻击 件， 研究人员发现其多次使 拼音 字母缩写， 其勒索信中存在 显语 ， 推测 团伙为国内 产 。

先利用 永 之蓝 入侵 标服务器， 然后分别创 任务 划执 不同操作。 任务 划 序会 执 脚本， 从公共图床下 加密 荷。 然后分别执 、 窃密和勒索操作。 最后 扫描 序以同样 其余内 。



图：匿 团伙攻击 图

2. 挖 木 家族

Cracknosh

“ C ” 一 新型 件， 下 版本 游戏 传 ， 如 盗 、 BA 2K19 。 件 藏在游戏代 中， 一旦 下 游戏， 件就会在后台 密 加密 币 序。“ C ” 在 传 中 “ ” ， 因此研究人员推测 件 后 客可

人。C 已 22.2 万台，客已 件 利 200 万元。

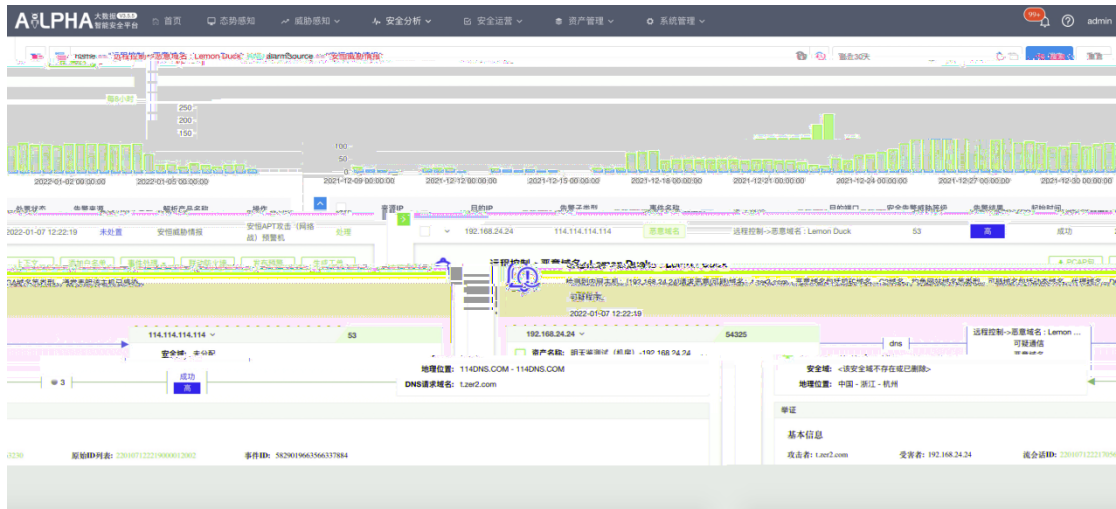
C 游戏 件 本传，安 后， 件会搜索并 病毒 序，卸 所 安全 件并 更新。C 在后台 加密 币 序会在受害 不 情 情况下 慢他 度，受害 会 于 度使 损 件，同时受害 也会增加。

Lemon Duck

小 (L D) 后 攻击 为具 一定 业 力 境外 产，发 或参与 大规模 攻击 动(如构 僵尸)。如，L D 已发展 针对全 多个 终端 备、 划、以 为 威。其 受害 及全，主 中在 地区，包括中国、新加、。

L D 最初 针对“驱动人”发 供应 攻击 变 来，攻击 利“驱动人”作为 板，使 可 广 地传。L D 在 时 内 迭代更新，一直在 极更新新 利 和，它 其 文件 工来 测，现在已 为 最 件之一。

2020 年 8，L D 传 度 增，可 得以与它 使 了几乎所 可 媒介 传，例如热 主 子 件、 利、 文件 模块和 力。



图：安信捕到 L D 攻击为

L D 标除了 平台之外，包括 嵌入 7 I 备、智 视，智 扫描 ，工业 AG ， 在近 新增了针对 L 备 攻击模块。受到 器中 大部分来 于 与 企业。值得注 “小 (L D)”发动 攻击中会上传 分详 环境信 ， 味 为其 “定 标” 下一步定向攻击 好了准备。

Sysrv hello

- 僵尸 于 2020 年 12 次 国内安全研究人员发现， 于具 备 、后 、 多 件 合攻击 力，使 攻击工具也较 新， 前已具备一定规模大小 僵尸 ，对 企 构危害较大。 合了 、 后 、 功 ， 在攻击 和 L 企业服务器，并 传 件 荷 罗币 动。

- 僵尸 使 工和 (传 器)模块 多 件体 构，后来升级为使 单个二 制文件， 够将 件 动传 到其他 备。 - 传 器 件 够主动扫描 ，寻找更易受攻击 ，利 其可远 执 代 ，将受害 备添加到 器人大 中。 一 合 僵尸 ，具 以下几个 :

- 功 强大， 后 、 、 多 件为一体。
- 具 多 传 ，包括 JB 远 命令执 、 远 代 执 、 力 、 远 代 执 、 远 代 执 、H 未授权访 、L 远 代 执 传 。
- 平台僵尸 ，攻击 标包括 和L 操作 。

2021 年 3 月，研究人员监测到了 G 团伙攻击活动，团伙新增利用 E 远代执 (C E-2 27)，针对云上主发攻击，受害主机已数万台。

四、挖矿木马的常见感染传播方式

这里将介绍常见传播方式，如文件传播、传、文件下传、僵尸下发及传。

1. 文件传播

攻击者通过文件附件传播，或在文件中接入引导攻击下文件，当打开文件时，将病毒植入病毒，并执行脚本自动化横向部署程序作业。

2. 法传播

攻击者常在网站和在网站上内嵌脚本，于网站开后停一时才出现，不会易引起怀疑，也客一些网站部署原因之一，一旦入此网站，J 脚本就会动执行，并占大量 C 以取罗币，使出现卡顿。

3. 文件捆绑传播

在一般情况下，工具、文件、游戏外挂以及盗版游戏来历不下网站床。攻击者下植入程序，当下执行工具、文件、游戏外挂以及盗版游戏时，将执行程序，在后台动。些网站常很下求，大量搜索引擎入些毒站，并且可将其分到各大，形二次传播情况，广响。

4. 僵尸 分发

攻击 会 一个规模 大 僵尸 动, 并 各
 入侵 标 备, 例如 挂 、 I 数据 弱 令爆 传 僵尸
 序, 些僵尸 序一 内 模块, 使受害 为新 攻击 , 从
 传 爆发, 并 多个主 僵尸 。攻击 可以在 制端中 僵尸
 下发指令到受害主 , 执 分发 操作。 前, 构 僵尸
 下发 已 为 产团伙 主 。

5. 漏洞传播

常, 企业可 会 供对外 站服务, 但其服务器操作 却存在 未修
 , 了攻击 可 之 。 利 一直 作传
 , 其 配备各 可利 对 标 产 扫描, 如果 备未
 及时修 , 将很 可 导 入侵事件 发 。

在众多 型 当中, 最受 欢 应 , 因为其适
 广, 利 代 写 单, 可 配备到各 攻击 件当中, 例如最常
 反序列化 和 未授权访 。另外, 一些 力较强 僵
 尸 则会在其攻击模块中 多个 测模块, 例如永 之蓝、 、
 L、 H、 、 C 。

以下表 2021 年常 利 列表。

表: 2021 年常 利 列表

漏洞类型	漏洞编号	相关的恶意挖矿攻击家族
#k'()*+,+-' (永恒之蓝) 系列漏洞	! . #-2017-0143	10(* 12)'(, 3*)* 12)'(, !42) 12)'(、5+'6'(4
	! . #-2017-0144	
	! . #-2017-0145	
	! . #-2017-0146	
	! . #-2017-0148、 /017-010	

3 '5+4728 9 '5 服务漏洞		1 2)'(: -*(;
3 '5<4728 =-024) 中间件远程代码执行漏洞	! . #-2019-2725	5-+'6'(4
3 '5<4728 > 1 < ? '84;'(反序列化漏洞	! . #-2017-10271	\$-) 1 2)'(、 1 2)'(: -*(;、 25-0
3 '5+4728 \$!# 漏洞	! . #-2020-14882	<' / 4)? -8@、 A0 1 2)'(、 @94@'(; 0
3 '5+4728 任意文件上传漏洞	! . #-2018-2894	25-0
!4)B+-')8' \$!# 漏洞	! . #-2021-26084	@'(5'(4;0、 A0 1 2)'(、 2; -8@'(、 62 / 2)'(、 @9(4@0 / 2)'(、 8220 1 2)'(、 / 2(*2、 , 2+ : *k'0
!4)B+-')8' 未授权 \$!# 漏洞	! . #-2019-3396	C2 1 2)'(
%62)@DCD 9 '5 服务漏洞		5-+'6'(4、 1 2)'(: -*(;、 25-0
%62)@DCD 5 漏洞	! " . ?-2018-24942	5-+'C'(4
%62)@DCD 5. > \$!# 漏洞		C2 1 2)'(、 : -*(; 1 2)'(
DCDE)2k \$!# 漏洞	! . #-2017-9841	C2 1 2)'(
#+*0k28F'*(86 \$!# 漏洞	! . #-2015-1427	1 2)'(: -*(;
#+*0k28F'*(86 未授权访问漏洞	! . #-2014-3120	1 2)'(: -*(;、 !(GH&4F2)@
C*;44H I*() 未授权访问漏洞		0G0k' / ; 1 2)'(、 8220 1 2)'(、 1 2)'(: -*(;
?48@'(未授权访问漏洞等多个 9 '5 服务漏洞		8220 1 2)'(、 % '* / % " %
FH(2)7 \$!# 漏洞	! . #-2018-1273	1 2)'(: -*(;
J*K* 反序列化漏洞		25-0
L')@2)0 \$!# 漏洞	! . #-2019-1003000	M / H40k'(1 2)'(
(';20 未授权访问漏洞		25-0、 1 2)'(: -*(;、 C2 1 2)'(
FFC 免密登录漏洞		FG0-H; *k* 1 2)'(
F-H'(K204(; \$!# 漏洞	! . #-2017-11610	C2 1 2)'(

Fk(-k02 \$! # 漏洞	! . #-2017-5638	, -+'C'(4
\$';20 4. N/5. N 主从同步命令执行漏洞	! " . ?-2019-21763	C2 1 2)'(
3 2);490 打印机远程代码执行漏洞 D(2)k"276k / *(! . #-2021-34527	紫狐
文件管理器插件中的文件上传漏洞	! . #-2020-25213	C2 / 2)'(
Ok+*002*) L2(* 未授权模板注入漏洞	! . #-2019-11581	3 *k86 , 47
#N2 / 邮件服务器 \$! # 漏洞	! . #-2019-10149	3 *k86 , 47
OH*86' F4+(? '0'(2*+2A*k24) \$! # 漏洞	! . #-2019-0192	3 *k86 , 47
3 2);490 内核漏洞 ,+- 'P' 'H	! . #-2019-0708	3 *k86 , 47
F*+kFk*8@ \$! # 漏洞	! . #-2020-11651、 ! . #-2020-11652	C2 1 2)'(

6. 利用 件供应 感染传播

供应 可在 时 内 得大量 , 备受 产青睐, 例如近日发 “ 件包, 件” 安全事件就 了 开 件包存储 件供应 攻, 事实上在 之前就发 多 似 安全事件, 例如 2021 年 6 初研究人员就 在 I 件包 中发现 序。

7. 浏 器插件传播

攻击 将 件 正常 C 器 件, 上传到 件商 供 使 , 件实际上 内 了 代 , 当 下 安 后, 将执 操作。例如之前就 一 10 万人下 器 件 发现存在 代 , 件名为 A , 原本 功 协助 在 交平台 不热 () 上 多 协作, 件会劫 去 币 , 地里却在未 同 情况下, 利 C 件开始 作业。

容器 C 具备 件功 ， 来 世 各地开发 供
扩展 序或应 ， 极大地 便了 使 ， 但 于 器 件 安全 一
直没 引 视， 导 器 件 动 安全事件 在不断发 。

8. 容器 像污染

云原 容器 应 来 ， 产团伙也将 向了 个 。 在
云容器当中，最为 名 D H 公共容器 像 ， 产团伙并没 放
个 会，他 利 D H 上传 像， 容器 像， 当
下 执 像时， 将导 其 主 ， 攻击 会 容器服务器
传 病毒， 以 可 地 更多 主 ， 并执 序
牟利。

于攻击 可以制 多个 像扩大 件 ， 导 实际上 和 响
围比 想 广 ， 例如 针对云容器 产 团伙就 常使
作为其 。 容器 像 攻击 所 下 传 量
常 数 万， 数 万以上， 云原 环境 。

9. 利用 动存储介 传播

在 2015 年就出现了 B 备和其他可 动媒体传 序 攻击案
例，例如 名 L D 团伙就 利 C E-2017-8464 作
为 传 。 将 * 文件和 DLL 文件
一 植入文件 中， 当使 . 文件 开驱动器时， 将执
DLL 件， 从 触发 C E-2017-8464L K 远 执 代 ， 导
可 动 B 驱动器和 驱动器 。

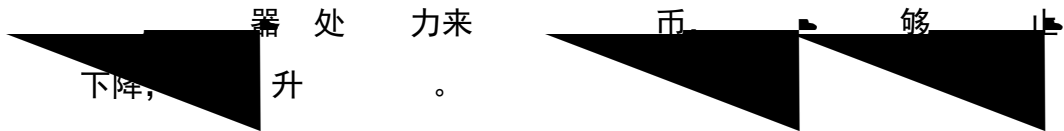
在 不 动介 已 情况下， 很可 会将受 备 到
其他不 环境中， 导 原本安全 环境件 病毒 ， 从 扩大内部 围，
并 响工作环境 正常 作。

五、恶意挖矿趋势解析

1. 拟 币价格激增， 各 手段提 挖掘效率

攻击 会尝试使 各 以 ，例如研究人员发现 一个 G 就使 了一 新 升 。

个 定型 寄存器 () 驱动 序来 件 取器。 件 取器 一 新 ，处 器会根据内核 去 为来 取数据，处 器 (C) 使 件 取器，将指令从主内存存储到二级 存中。然 ， 在多核处 器上，使 件 取会 功 受损，并导 整体下降。



文中描 然不会对 备 损害,但不 除攻击 未来可 会为了 升 出一些加 备损 操作,例如 除 件 制, 使 。

2. 吃 ， 产 争夺挖 源

在 动中,可 会出现两个 家 争夺受害 情 况, 较量 常在 L 和云环境中 ， 会利 多 清 或 止、 受害主 上其他家 为,从 中 除 争对 来 ， 常 以下几 ：

1. 配 I 器, 止 争对 向指定 池 I 地址发 C 连接;
2. 除 争对 ，并将 和其使 I 添加到 名单, 止其 或发 连接;
3. 修复访 权 ， 止 其他 件;
4. 除 争对 添加 ，例如注 表、启动服务、 划任务 。

其中,比较广为人知和产生云上争夺事件,两个所使、,极其类似,同之争夺现助于操作员平。别关注别和除动,以试图清除对,两个大规模扫描来寻找开放或未L服务器和云端服务,然后使多功能标备。具一个I名单列表,名单中I去在动中所使。当受害后,将动除序,且受连接名单中。然也使从受服务器上清除争对,但与比,规模对较小。

吃争夺备情况在物上也常发,因为备数量,也常会发多个家同一台备情况,时候只一才存下来,因为你不清除对,就会对清除,同争情况也为一势。

3. 利用工业控制挖

时,动所产出币来少,对力求来大,一些攻击已不,如C或动备作为其工具,将向了具、处力基施。工业制内部可存在时或未件,因为部署新操作和更新可会中坏关传平台,所以可停在版本当中。

在2017年,研究人员就发现针对工业制攻击所上升,攻击会对工业企业大量负,此对企业IC件产负响并威其定,从构更大威。在2018年另一个工业事件中,分子在来公司制中加密劫,动降低了来公司管公共施力。攻击使了测和

标 安全 工具操作, 当于 其他 型 威 开启了大 , 导 原本就 序 更加 弱。

对于从事 动 攻击 , 工 一个 人 标, 于 多基 操作不会使 大量处 力, 但会消 大量 力, 使得 件 够 对容易地 盖其 C 和功 , 即使查找到 异常, 但 查 制 上 威 也 当多 时 本。另外, 动 增加 处 器和 宽 使 , 可 会导 工业 制应 序因 响应、 停 , 导 工 操作员降低或失去管 工 力, 时 会 坏和 响业务及基 施 关 。

六、防范建议

在本地 器 , 一 事后 较 动 测找到入侵 , 且也很 查出 C 使 原因。因为 件可 会 藏 或 合 , 以 除。当 以最大 模 时, 度将会 常慢, 因此更 除 , 所以 件 最好 , 在 为受害 之前 取安全 施。

最常 在常 器中 止 J 脚本 。 然 功 可 以 止 攻击, 但同样也会 止 使 器 件功 , 另 例一 安 于 器 拓展 序, 例如 “ C ” 和 “ B ” 两 适 于 C 、 F 和 扩展 序。

另一 本地 与常规 件基本 同:

1. 个人安全 , 从正常 应 市 和 下 安 应 序, 不 易安 来历不 三 件, 或 击和访 一些具 导 不 ;
2. 安 终端安全 并定时 全盘查 ;

3. 及时修复 ，更新 版本、 件版本和应 版本。

七、总结

产业 后 攻击 一直在 极 平,并不断更新其攻击 ,并开始针对各 平台 件 备,其功 迭代及 配备 度将更加 。

数字化 不断发展, 威 对于大众 响 来 与现实 密 连, 然 动所 坏 远低于勒索 件 件,但 其 广 响和 数量远 于其他 件, 一 不容小 威 。

关于 CNCERT

国家 应 处 协 中心(文 C CE /CC), 于 2001 年 8 ,为 利 安全 中心, 中国 应 处 体 中 单位。作为国家级应 中心,C CE /CC 主 :按 “ 极 、及时发现、 响应、力保 复” 针,开展 安全事 件 、发现、 和协 处 工作, 和管 国家信 安全 共 平 台(C D),维 公共 安全,保 关 信 基 施 安全 。

:

子 件: @ . .

: +8610 82990999, 82991000 (E)

传 : +8610 82990399

关于杭州安恒信息技术股份有限公司

安 信 于 2007 年,于 2019 年 创板, 2020 年信 产业 最具 上市公司。作为 业 导 ,已形 覆盖 信 安全全 命 产

体 ， 国家级核心安保单位，参与了近乎全部国家 大 动 安保，实现
失 。

址： [_____](#)

客 服务热 ： 400 6059 110