

DDoS

《黑神话：悟空》发行平台遭DDoS攻击的更多细节



Alex.Turing, Wang Hao, Acey9, daji

2024年8月28日 • 16 min read



事件回顾

[关于此次事件XLab的观察](#)

[攻击时段分析](#)

[Steam被攻击的服务](#)

[攻击动机推测](#)

[主要涉事僵尸网络](#)

[AISURU僵尸网络技术细节](#)

[字符串解密](#)

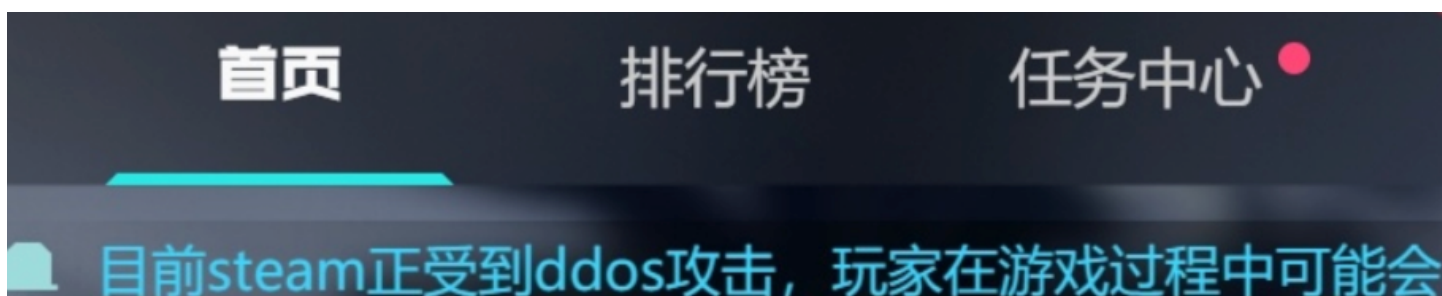
[网络协议](#)

i. [C2获取](#)

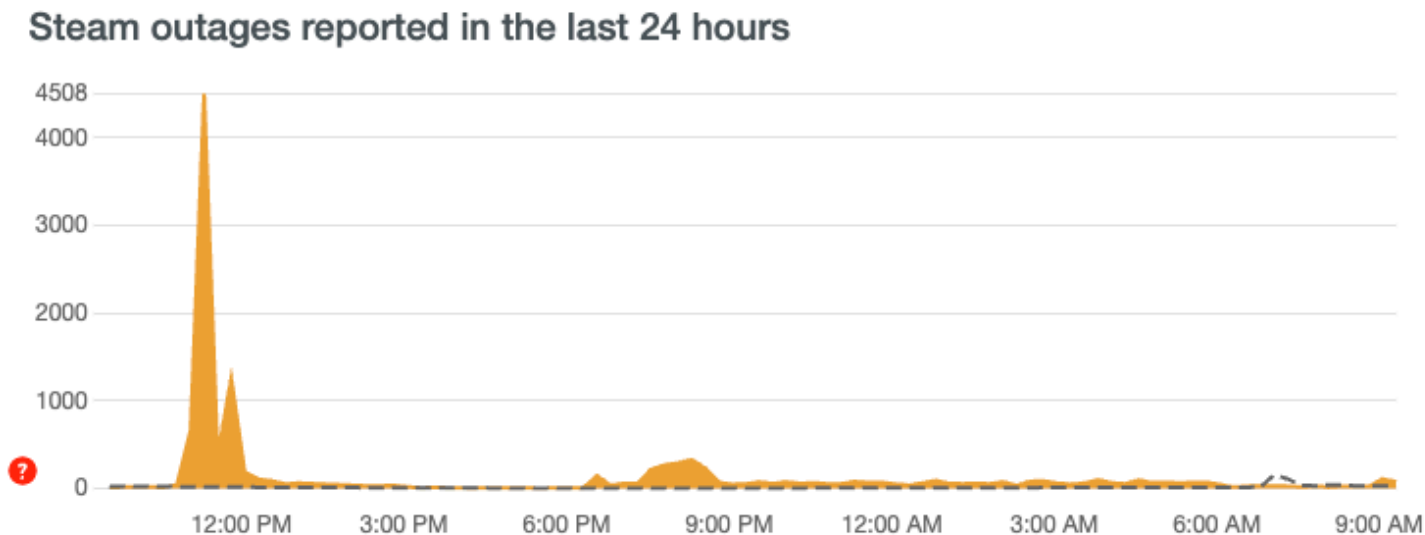
i. [通信用途](#)

事件回顾

8月24日晚，Steam平台突然崩溃，国内外玩家纷纷反馈无法登录。许多玩家猜测崩溃是由于《黑神话：悟空》在线人数过多导致。然而，根据完美世界竞技平台的公告，此次Steam崩溃实际上是因为遭受了大规模DDoS攻击。



完美世界公告



[Downdetector用户报告的Steam 中断情况](#)

关于此次事件XLab的观察

XLAB大网威胁感知系统对最近的DDoS攻击事件进行了深入观察。我们注意到，此次攻击涉及了近60个僵尸网络主控节点，这一规模远超过常规僵尸网络的控制范围。这些主控节点协同指挥了大量被感染的bots，以波次方式发起了攻击。

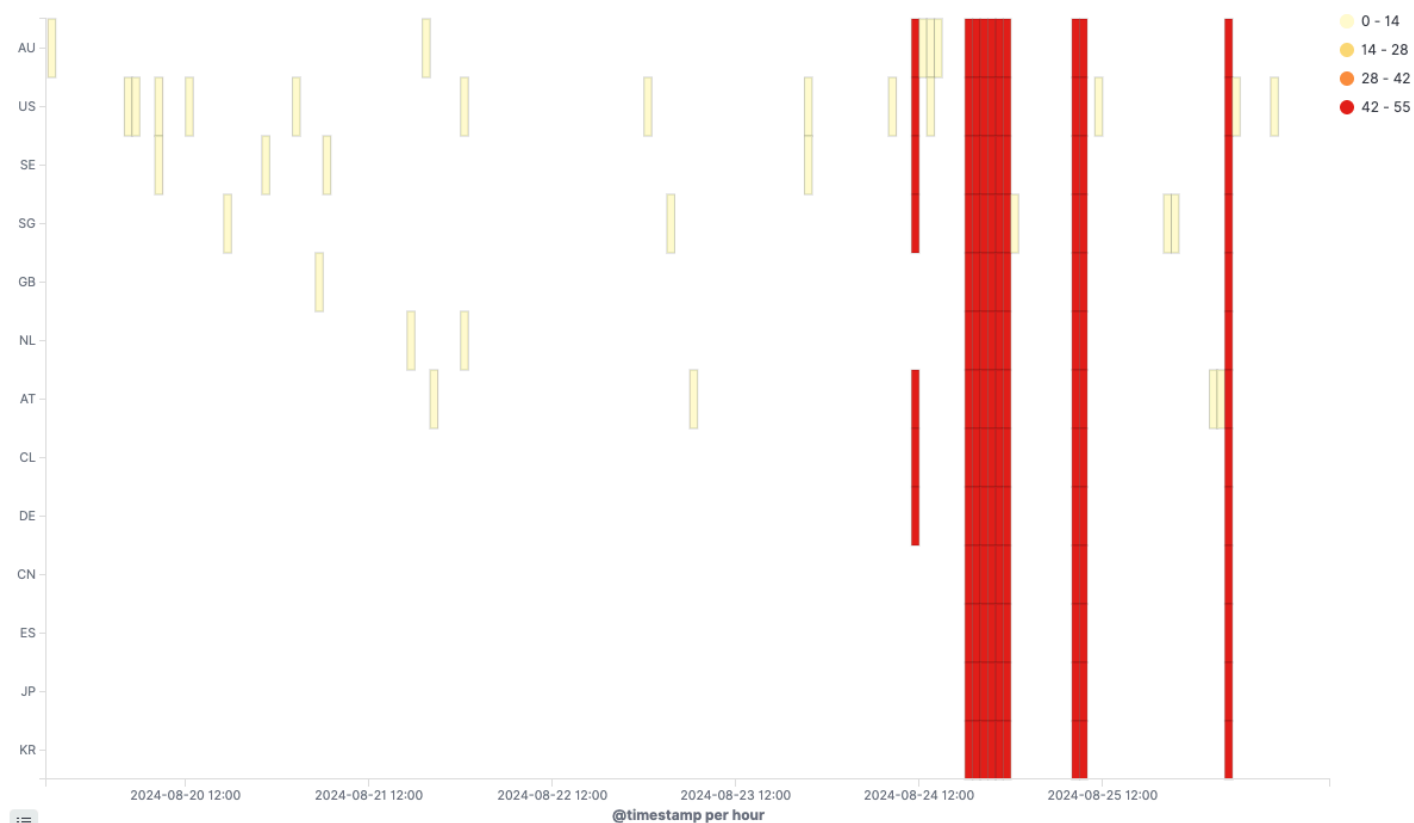
攻击的目标包括Steam在全球13个地区的服务器IP，包括中国、美国、新加坡、瑞典、德国、奥地利、西班牙、英国、日本、韩国、澳大利亚、智利和荷兰。值得注意的是，除了Steam自身的服务器外，国内完美世界代理的Steam服务器也被列为攻击目标。总计，有107个服务器IP遭到了攻击。

攻击行动主要分为四个波次，攻击者似乎有意选择在各个时区的游戏玩家在线高峰时段发起攻击，以实现最大的破坏效果。

从攻击的时间选择、地域分布，以及同时针对国内外Steam服务器的策略来看，攻击者的目的显然是在重点扰乱中国市场的同时，在全球范围内对Steam平台的正常运营造成全面干扰。这种有组织的攻击行为表明了攻击者在策略上的计划性和对目标的明确针对性。

攻击时段分析

此次攻击事件主要分4个批次、追着时区打。分别是东半球周六中午、东半球周六晚间、西半球周六晚间和欧洲地区周日晚间、都是游戏玩家在线的高峰时段。具体攻击时段和地区如下图：（图表说明：横坐标为攻击时间、纵坐标为被攻击地区、色块表示该地区被攻击的服务器数量）



详细攻击时间线

- 北京24日11点前后，第一波尝试攻击，影响7个地区Steam服务器，攻击持续时间近1小时（东半球周六中午）
- 北京24日21点前后，第二波攻击，影响13个地区Steam服务器，断断续续攻击将近5小时（东半球周六晚间）
- 北京25日09点前后，第三波攻击，影响13个地区Steam服务器，攻击将近15分钟（西半球周六夜晚）
- 北京26日04点前后，第四波攻击，影响13个地区Steam服务器，攻击持续时间近2分钟（欧洲周日夜晚）

四波攻击的详细时间和地区

Steam被攻击的服务

从这些Steam服务器的关键字猜测，被攻击的主要是：内容服务器、ingest、broadcasts，相关的服务。

```
27 ext1
18 cm2
18 cm1
11 ext3
9 ext4
5 cm5
5 cm4
5 cm3
4 cm6
3 ext5
1 ingest
1 ext6
1 cm05
1 broadcastcs
```

攻击动机推测

此次攻击事件我们一共观察到了28万条针对Steam平台的攻击指令，根据我们的长期观察，作为知名的游戏平台，Steam的攻击日常发生，但往往都是零散的服务器被小规模的攻击，攻击指令数目几次到几十次不等。此次事件攻击指令直接暴涨2万多倍，峰值时攻击指令25万，这种涨幅是非常罕见的(见下图，攻击指令趋势图，巨大的尖峰)。Steam全球各地区机房服务器被轮着打，包括国内完美世界代理的Steam服务器也一并被扒出来攻击，《黑神话：悟空》上线之前我们没看到完美世界Steam服务器遭遇过成规模的DDoS攻击。且攻击时长多达几个小时，专挑各地区玩家在线高峰期攻击。这是极其少见的。

过去一年针对steam平台的攻击事件攻击指令趋势

下图是我们的大网威胁感知系统的截图，大家看到是被攻击企业排名，可以看到在过去一个月的数据里，Steam（Valve公司）和完美世界排在第一第二，远超后续的Verizon等知名企业。

结合最近火出圈的国产游戏《黑神话：悟空》在Steam平台上线，包括主要为国内游戏玩家服务的完美世界Steam服务器也遭到攻击，《黑神话：悟空》上线之前我们没看到完美世界Steam服务器遭遇过成规模的DDoS攻击。又是周末夜晚，广大游戏玩家在线的高峰时期，Steam平台遭遇如此大规模的DDoS攻击，很难让人不联想此次攻击事件不是针对国产3A游戏大作《黑神话：悟空》。

主要涉事僵尸网络

Steam作为一个的世界性的游戏平台，不可能被区区一，俩僵尸网络打崩，肯定是非常多的僵尸网络被组织起来协同攻击。世界上没有任何组织可能拥有全知视野，本文只是从XLab的视野出发，就此次攻击事件进行分析。

在我们视野中多个僵尸网络参与此次攻击，其中的的主力是自称AISURU僵尸网络，在其telegram频道中声称拥有超过30000个bot节点，攻击能力在1.3 - 2T左右。

下图是该僵尸网络的能力测试图：

此外该频道还提到了国外厂商GSL的一篇[Blog](#)，Blog声称是有史以来向公众报告的最大规模的攻击，我们也在该僵尸网络的攻击日志中找到相同时间节点发出的攻击：

部分读者可能对于这些数字没有概念，让我们看一看当下最火的人工智能大模型的回答。

一个僵尸网络 (botnet) 拥有30000个节点，并且其攻击能力在1.3 Tbps（太比特每秒）到2 Tbps之间，这代表了一个非常强大的网络攻击能力。要理解这个概念，可以从以下几个方面来分析：

- 攻击规模：**1.3 Tbps 到 2 Tbps 的攻击流量已经非常巨大，足以造成严重的分布式拒绝服务攻击 (DDoS)，这类攻击会使目标服务器、网络或应用程序瘫痪。一般来说，传统的企业网络带宽远低于这个水平，因此这样的攻击会对目标产生毁灭性影响。
- 节点数量：**30000个节点意味着有25000台受控设备参与了攻击。每个节点可能会贡献一定的带宽来发起攻击，集合起来的总攻击流量达到1.3 Tbps 至2 Tbps。
- 实际影响：**这种规模的DDoS攻击可以轻松压垮大部分互联网服务，除非被攻击方拥有非常强大的防护措施和足够的带宽冗余。这类攻击常见于高调

的黑客活动，针对大型企业、政府机构或关键基础设施。

相信读者现在已经有了一定的认识，总体来说，像AISURU这样的僵尸网络是一种**非常强大的网络武器**，能够通过数量巨大的设备同时发起攻击，使得几乎任何没有特别强大防护措施的在线服务都可能被击垮。这种攻击不仅对目标造成直接影响，还可能影响到大量依赖这些服务的普通用户，正如此次攻击，让大量玩家无法登录平台，畅玩悟空，喊出那一句“广智救我”。

AISURU僵尸网络技术细节

正所谓罗马并非一天建成，AISURU僵尸网络也有自身的发展历程。其实我们在2023年10月就捕获到该僵尸网络的样本，不过它在短暂运营之后便销声匿迹，直到今天5月初以'NAKOTNE'的名字再次进入我们视野，随后进入高速发展期，先后投入十几个Nday漏洞组建网络，最终进化为今天的AISURA。

AISURA的在战术、技术层面都和2022年我们发现并命名的僵尸网络Fodcha有着千丝万缕的关系。Fodcha因参与攻击健康码、Navicat等一系列有影响力的事件而在安全圈内臭名昭著，被我们戏称为“DDoS狂魔”。最终，在我们一系列的曝光和打击下，它被迫关停。

在我们看来，AISURA像是Fodcha的“追随者”或“信徒”，它在技术与战术层面很好的继承了Fodcha的遗产，但同时也发展出了独特的风格，其威胁性不弱于Fodcha。

首先从战术层面上来说，它也和Fodcha一样，喜欢挑衅安全公司，希望被知名安全公司点名曝光，为自己带来流量热度，通过这种另类的广告方式，为自己在激烈的黑产竞争中赢得优势，似乎深谙“酒香也怕巷子深”之理。

AISURA在最早的样本中是这样表达它对安全社区的“尊重”，`"N3tL4b360G4y"`，`"paloaltoisgaytoo"`。paloalto，即Palo Alto Networks，是美国一家非常著名的安全公司，市值超过千亿；那“N3tL4b360”呢？其实是一种在安全圈颇为流行的Hexspeak，它指的是我们前团队的名字。当我们披露这批样本后，它马上很知趣的在新样本中将`N3tL4b360G4y`替换成`xlab`

gay”。毫无疑问，这又迎来了我们的曝光。此外AISURU非常关注我们blog的动态，在最新的样本中又增加了一条消息 `today at xlab, botnet operators learn how to dance macarena`，这让我们想起了之前公开的[Rimasuta僵尸网络](#)：曾经在样本中留言 `this week on netlab 360 botnet operator learns chacha slide`。过去学chachaslide，现在跳macarena，俩个都是跳舞，难道僵尸网络的作者多为舞蹈爱好者？对此，我们想对僵尸网络团体说，“好好练，将来开发出更精彩的 `botnet之舞` 惊艳我们！”。

另外样本中的C2域名 `foxnointel.ru`，实在让我们有些忍俊不禁。读者或许会问，笑点何在呢？请容许我们解释一下黑客的幽默，在X平台上有一个非常活跃的安全研究员，ID是**Fox_threatintel**，他几乎每天都会分享一些威胁情报（threatintel）；AISURA使用C2域名foxnointel，即 `fox no intel`，“嘲讽”他其实根本没有情报。

接着我们来看技术层面，AISURA在 `代码结构` 上保留了部分Fodcha的风格，比如使用和Fodcha类似的switch-case进行各个阶段的处理；在 `基础设施投入` 上延续了Fodcha的“危机意识”，即将C2映射到20多个IP，而且分布在美国、英国、韩国、日本、俄罗斯等多个国家，同时分散在Azure、Linode、Vdsina、Google等多个平台，极大的增加了处置的难度。AISURA主控地理位置分布如下：

```
8 United States
3 United Kingdom
3 South Korea
3 Russia
2 Singapore
2 Japan
2 India
1 The Netherlands
1 Switzerland
1 Poland
1 Brazil
```

当然喜欢彰显特立独行的黑产团体，肯定不甘心被人贴上模仿者的标签，AISURA在 `加密，网络通信` 等方面实现了自己独特的创新。

字符串解密

早期版本使用CHACHA20对样本中的字符串进行加密，在后期的版本中使用XXTEA加密。

NAKOTEN_XXTEA_KEY_HEX: 1234567890ABCDEFEDCBA9876543210

在最新的版本中，样本中仍保留了之前的KEY，但长度缩短为4，算法也在朝着简单的方向发展，更换为BYTES_XOR。

AISURU_BYTES_KEY_HEX: 12345678

```
0x1a42c snow slide
0x1a6d0 a|b|c|d|e|f|g|h|i|j|k:printerconsulting.ru|foxnointel.ru
0x1a438 reports.printerconsulting.ru
0x1a708 5.35.45.162|5.35.44.21|166.1.160.38|194.147.35.35
0x1a458 /login|/products|/contact|/register|/user
0x1a484 /dev/null
0x1a490 /dev/tty
0x1a49c /dev/pts/1
0x1a4a8 /dev/console
0x1a4b8 /.ai
0x1a4c0 /proc/
0x1a4c8 /proc/self/exe
0x1a4d8 /proc/net/tcp
0x1a4e8 /cmdline
0x1a4f4 /exe
0x1a4fc /proc/uptime
0x1a50c /maps
0x1a514 /fd/
0x1a51c socket
0x1a524 wget|curl|ftp|ntpdate|echo
0x1a540 telnetd|upnpc-static|udhcpc|/usr/bin/inetd|ntpcclient|boa|lighttpd|httpd|goa
0x1a5f4 /dev/watchdog
0x1a604 /dev/misc/watchdog
0x1a618 TSource Engine Query
0x1a630 xlab gay
0x1a63c paloaltoisgaytoo
0x1a650 shell
0x1a658 system
0x1a660 enable
0x1a668 sh
0x1a73c /bin/busybox AISURU
0x1a66c AISURU: applet not found
0x1a688 ncorrect
0x1a694 today at xlab, botnet operators learn how to dance macarena
```

网络协议

2023年10月的版本以 `N3tL4b360G4y` 作为上线包，并将该字符串明文硬编码在样本中。被曝光之后，我们收到了新的“回应”：从 `NAK0TNE` 版本开始，以 `xlab gay` 作为上线包，并且将其加密编码到字符串表中。

C2获取

在8月初我们在新样本中收到留言：`today at xlab, botnet operators learn how to dance macarena`，以往域名或IP被直接加密编码在字符串表中，而新样本中加入了新的机制获取C2。

通过解密字符串表，我们发现以下可疑字符串：

```
[1] a|b|c|d|e|f|g|h|i|j|k:printerconsulting.ru|foxnointel.ru  
[2] 5.35.45.162|5.35.44.21|166.1.160.38|194.147.35.35  
[3] /login|/products|/contact|/register|/user
```

经过分析后，使用以下机制获取C2：

1. 通过 `:` 分割[1]中的子域名和二级域名，再通过 `|` 分割每一项
2. 随机选择一个子域名和一个二级域名，拼接后得到C2
3. 若解析上述C2失败，则用 `|` 分割[2]、[3]，得到IP和URI
4. 根据IP和URI构造GET请求并发送
5. 以4字节为单位获取返回包中的C2

C2使用的端口被硬编码在样本中，从21个端口中随机选择一个

```
2348,12381,8932,8241,38441,23845,8745,6463,7122,1114,6969,1337,4200,3257,7214,2474,
```

通信过程

通信过程在多个版本中都没有发生变化，使用和 `Fodcha` 类似的switch-case进行各个阶段的处理：

1. 上线包发送： `xlab gay`
2. 协商密钥
 - 使用XXTEA解密得到CHACHA20_KEY、CHACHA20_Nonce
 - 硬编码的NET_XXTEA_KEY_HEX:
`428723212B0106344C7A095322236921`
3. 密钥验证
 - 使用协商后的密钥解密数据，通过对比字符串
`paloaltoisgaytoo` 验证双方密钥一致性。
4. 发送bot分组信息
 - 先发送明文的分组长度，再发送CHACHA20加密的分组信息

至此，AISURU僵尸网络的主要技术细节介绍完毕。DDoS这一古老的网络威胁，游戏行为行业的天敌之一，就是如此朴实无华但粗暴有效。

总结

我们团队在大规模僵尸网络发现&跟踪领域已经专注超过10年，参与过全球众多知名和未公开的各种攻击事件预警，防御和协作，但此次攻击的组织度，烈度依然让我们觉得很惊奇。中国出了一款登顶全球的游戏，有人这么不开心吗？

最后引用一句伟人的诗做为本文的结束，"金猴奋起千钧棒，玉宇澄清万里埃"，祝福悟空，祝福中国的游戏产业。

部分IOC

SHA1:







```
b6e5c9e65682ccac071b65743595dae475f7a8b8
458d541bc93937ae6d0139f3f9d42b50fe255636
f0760aeaa0d667a1c100e3d348dbc383451587b1
```

Domain:

```
nakotne.pirate
nvr.libre
a.printerconsulting.ru
```

What do you think?

56 Responses

- 
Upvote
- 
Funny
- 
Love
- 
Surprised
- 
Angry
- 
Sad

0 Comments

 Login ▾

G

Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS 

Name

