敬告攻击者

5 月 14 日以来，灵域游戏 Agatha 硬件系统遭到大流量 DDoS 攻击。攻击者尚未确定，但大家已经心知肚明。这篇文章将通过灵域游戏媒体矩阵发布，感谢您的拜读~

• 攻击情况如何?

目前为止，Agatha 所有带防御的机器，没有一台中断。不过，不带防御的机器已经中断了 73 小时。但久负盛名的 AgCT 系统早在攻击发生的第 7 秒，就启动了业务迁移。目前所有业务都完成了无感切换，显示的 1 分钟中断，是由检测主控机器维护造成的。

• 哪里被攻击了?

我们在历次通知中都称，遭攻击的系统是“Agatha 硬件系统”。在这里我可以确切地说，被攻击的系统是 Agatha 生存服外网入口 AB、OpenID 系统入口 A、Agatha 内部网络认证服务器 C。所有这些机器，都是带防御的。

• 为什么没有中断?

我们在大部分机器上都部署了华为防火墙。去年 8 月的大型攻击您应该非常熟悉，您对着它干了整整两周，丝毫没有反应。这样的感觉我相信您还想再来一次。同时，为了防止防火墙设备上的一粒灰尘掉进主板导致防火墙损坏，我们还部署了云防火墙。我大可以直接告诉您，防火墙部署在阿里云上海可用区 A，您如果把它攻破了，就不仅仅是私人恩怨了。不仅我们会收到阿里的赔付金，您也可以喜提牢饭，属于是双赢了。
PS：去年腾讯 HK 的攻击者已经进去了哦~

• 怎样才能打爆你们的系统?

因为系统设计架构原因，为了回答这个问题，我请教了 Aurora。
Agatha 所有的机器都通过 ARAEN 连成一体了。所以为了让我们的业务中断，您有两种方法：

打爆 ARAEN 总控设备

我们的总控设备没有公网带宽。为了做到这点，您需要通过内网进行打击。所以唯一的方式就是侵入 ARAEN 内网。这个方法我们下面再谈。

把 ARAEN 上所有的设备全打爆

为了做到这点，您需要同时让 Agatha 7 台入口机器进入黑洞状态。这意味着您需要同时向 32 个 IP 地址输出总共 2Tbps 的带宽。我粗略地算了一下，这大概需要三千美元。

• 怎样才能入侵 ARAEN 系统?

首先，您需要找到我们的任意一位管理员的密码。这点好说，您毕竟是用过内鬼的人。
然后，您需要在登录时完成 2FA 认证，此时您需要找您的内鬼 Get 他的 Google Authenticator。
接下来，您需要完成硬件认证，这意味着您需要使用我们授权的指定主板计算机登录，虚拟机、服务器也不行。
接着，您需要完成 FIDO 认证，这要求您按下您 Yubikey 上的认证按钮，系统会自动处理完您的登录请求。不幸的是，世界上没有两片完全相同的 Yubikey。
最后，您需要完成生物识别认证。您需要通过眨眼等方式混过人脸识别，不幸的是，我们采用了支付宝接口，所有这些都是金融级认证，您混过它之后，记得提醒我们领取故障赔付金。

• 祝您攻击顺利~