秘密行动倒计时丨DC86021行动指挥部致全体极客伙伴的一封密信

转载

Ms08067安全实验室 于 2020-08-20 08:08:00 发布 452 收藏
文章标签： 安全 信息安全 软件测试 数据安全 eclipse
原文链接：https://www.bugbank.cn/live/salon/live

DEFCON GROUP 86021是受全球性黑客大会DEFCON授权的官方社区，021是中国·上海区号。8月21日即将举办线上技术沙龙，秉承DC交流活动的宗旨，将最纯正的极客精神延续下去。

特别请关注15:55这场由**MS08067安全实验室-SRSP小组核心-TtssGkf**带来的《从零开始weblogic的反序列化漏洞》的分享，带领大家了解weblogic的工作模式，明白漏洞原理，从而掌握调试weblogic反序列化漏洞的基本能力。从漏洞组件探究漏洞成因，最后思考漏洞利用方法，希望帮助大家构建出属于自己的POC，摆脱"脚本小子"的称号。

*本文所有剧情及设定纯属虚构，请勿代入现实生活，否则因此造成的后果我们概不负责^-^(手动滑稽)

!

时间：公元DC86021·β年

地点：极沪城，网络及通信数据总调度中心；中国

“报告队长，∪组织对我们的网络攻击愈演愈烈，仅凭我们现役队员的力量已经抵挡不了多久了。”

“即刻派遣五位精英领队，并发送密信向广大安全极客伙伴求助，集结力量筑建安全盾墙！”

error 404

不要回复！

不要回复！

不要回复！

尊敬的极客英雄候选人，

你好。

这里是极沪城网络及通信数据总调度中心。

你现在看到的是我们通过DC86021编码特殊加密的内容。若在你的终端本文能正常显示，即表明，**你是我们选中的极客英雄候选人之一。**

现今，互联网高速发展，可伴随着网络功能不断增多，开发体系日渐庞大，网络漏洞也始终不可避免地存在着。网络攻击如洪水猛兽，时刻威胁着互联网安全。极沪城作为重要的网络中心城市，在暗处，许多不法分子对我们虎视眈眈。

近日，根据可靠情报，名为**“U”**的非法组织正在谋划一次对我们网络系统的总攻。此次攻击来势汹汹，仅凭我们现有的力量，恐怕难以抵御。因此，我们决定采取**秘密行动**。我们将派遣五位精英领队和两位经验丰富的前线作战指挥官，尝试筑建**五座城市安全盾墙**。若成功筑起盾墙，U组织的进攻便不足为惧。

本次行动将秘密进行，代号“**DC86021·β**”。

盾墙建造是一项庞大而周密的工程，但我们的时间所剩不多。为如期完成行动，我们需要更多人的力量。

尊敬的极客英雄候选人，请加入我们！

以下为DC86021·β行动完整说明。包括**行动计划书、安全盾墙规划、资源补给站**及**补给品图鉴**，请查收。

若你愿意加入，**请于行动当日前往行动地点**（详见下文）。无需回复信件，也请尽可能不要透露关于本次秘密行动的信息。

***01** 行动计划书*

行动时间：8月21日(本周五) 13:00 - 20:00

行动地点：电子战坐标

https://www.bugbank.cn/live/salon/live

行动计划（以实际情况为准）：

时间	行动安排	领队
13:05	**前线指挥官致辞**	张雪松
13:10	**特邀指挥官致辞**	李均
13:20	**《内网路由劫持谁之过》**	剑思庭
14:55	**《浅谈蜜罐技术在红蓝对抗中的实用性》**	KBLoow
15:55	**《从零开始weblogic的反序列化漏洞》**	TtssGkf
17:05	**《Understanding and Bypassing AMSI》**	lengyi
18:35	**《打造CTF的“新秀状元”》**	Pet3r.Wu

02 安全盾墙规划

五位精英领队将带领极客英雄们共筑安全盾墙。行动过程中，极客英雄们通过**在线互动助力**，将积攒安全能量。安全能量蓄满，既可成功筑起安全盾墙！

行动指挥官：张雪松 Madison

漏洞银行联合创始人兼技术总监，拥有12年网络安全研究经验，擅长系统底层安全与网络协议栈分析技术。中国安全认证工程师、CISAW认证专家、OWASP国际组织会员、检察院受邀技术顾问、网安等保协会专家、中商联智库顾问。

特邀指挥官：李均 Selfighter

360未来安全研究院研究员，中国首个DEFCON GROUP —— DC010发起者，DEFCON GROUPs Review Board 中国区成员，《无线电攻防大揭秘》《智能汽车安全攻防大揭秘》作者，Blackhat&DEFCON、HITB、CanSecWest、KCon、Syscan360等安全峰会演讲者

精英领队：剑思庭

IRTeam工控红队联合创始人

破晓团队工控成员

国际知名工控厂商网络安全负责人

盾墙一：

《内网路由劫持谁之过》

在制造业的内部，会采用大量三层交换机来组成内网，不同的子网会采用VLAN间动态路由模式，组成一个高可靠性的企业内网。但由于动态路由的非规则化的部署而造成轻易互联网出口路由劫持，从而造成制造业内部信息被窥探和泄露。本议题会介绍制造业内网架构和路由原理同时从红队攻击PoC角度阐述在这样场景中如何劫持互联网出口，同时讲述如何抵御这种攻击。

精英领队二：KBLoow

兰州大方电子安全研究员

丝路安全团队核心成员

DC860931核心成员

盾墙二：

《浅谈蜜罐技术在红蓝对抗中的实用性》

在近些年的护网中，蜜罐越来越常见。那么当我们遇到蜜罐时该怎么办？如何将蜜罐化为己用，又如何防止蜜罐被人利用？本议题将从红队和蓝队的角度出发，详细分析蜜罐在实战中的用途及其对红蓝队的影响。

精英领队：TtssGkf

Ms08067实验室 - srsp team成员

盾墙三：

《从零开始weblogic的反序列化漏洞》

本议题从开发的角度，带领大家了解weblogic的工作模式，明白漏洞原理，从而掌握调试weblogic反序列化漏洞的基本能力。从漏洞组件探究漏洞成因，最后思考漏洞利用方法，希望帮助大家构建出属于自己的POC，摆脱"脚本小子"的称号。

精英领队：lengyi

鸿鹄实验室成员

08sec成员

信息安全爱好者

盾墙四：

《Understanding and Bypassing AMSI》

在.NET Framework v4.8版中，AMSI（Anti-Malware Scan Interface）机制被用于阻止攻击者从内存中运行潜在风险，AMSI会扫描有害或被管理员阻止运行的软件。本议题从红队角度出发，详细的讲解AMSI执行原理与绕过方法。

精英领队：Pet3r.Wu

就职于360企业安全集团

渗透测试 应急响应 CTF培训等

盾墙五：

《打造CTF的“新秀状元”》

近几年网络安全行业迅速发展，CTF竞赛也引来诸多业内优秀人士的积极响应。但CTF竞赛的难度较大，很多初学者会感到迷茫。那么该怎样正确打开CTF之路呢？本议题主要从Web、Reverse、PWN、Crypto、Misc五个方面对CTF进行介绍，将讲解学习方法以及一些常见题型，尽可能以直观简单的方式让更多人了解CTF。

03 资源补给站

建造安全盾墙将造成巨大的能源消耗。因此，**每面安全盾墙成功筑起后**，总指挥部将开启**2座**资源补给站，向辛苦助力的极客英雄们**发放补给品奖励**！但因补给资源有限，为保证分配公平，极客英雄们需要通过总部设置的**能力小测试**，来获取补给。资源补给站共有以下**5型**：

//N型补给站 - 专注测试

///

NOCITCE

开放条件：每座安全盾墙成功筑起后，100%概率开放

站点说明：本站考察极客英雄们在行动过程中的专注度。由精英领队出题，题目内容与对应的**盾墙能力**相关。最先答对的极客英雄获得补给品。

补给品：DC86021胸卡、DC86021贴纸

X1型补给站 - 智力测试●●

开放条件：每座安全盾墙成功筑起后，33.33%概率开放

测试内容：本站考察极客英雄们的**基础知识**。由领队助理出题，最先答对的极客英雄获得补给品。

补给品：DC86021贴纸、BUGBANK文化衫、小米公仔、小米车载香薰

X2型补给站 - 欧气测试●●

开放条件：每座安全盾墙成功筑起后，33.33%概率开放

测试内容：本站考察极客英雄们的**欧气**。输入指定的口令后，领队助理通过倒计时截屏的方式选出获得补给的极客英雄。

补给品：DC86021黑科技风扇、DC86021迷幻手提袋、DC86021贴纸、ByteSRC保温杯、ByteSRC旅行充电器、ByteSRC帆布袋

X3型补给站 - 艺能测试●●

开放条件：每座安全盾墙成功筑起后，33.33%概率开放

测试内容：本站考察极客英雄们的**音乐曲库储备**。随机播放歌曲伴奏，最快猜出对应歌名的极客英雄获得补给品。

补给品：DC86021贴纸、四叶草晴雨伞、四叶草数据线、四叶草笔记本、四叶草书签、BSRC公仔套装、BSRC手机自拍套装

//R型补给站 - ???

///

NOCITCE

开放条件：未知

站点说明：未知

补给品：神秘超稀有补给品

NOTICE。

KNOW IT

HACK IT


VIDEO
XXX
OPEN

04 补给品图鉴

名称	图鉴	属性	物品描述	稀有度
DC86021 文化衫		颜值+86021	全球限量，只送不卖，总部嘉奖专用	? ? ? ? ?

DC86021 胸卡		智力+50 发量-86021	掷重金及 Angel 表哥熬夜脱发所炼成の超高难度解密胸卡，拿到 Flag 算你赢	★★★★☆
DC86021 迷幻手提袋		时尚+86021 背包容量+5	极沪城保卫组织专用收纳袋，因在日光下闪耀七彩光芒变幻莫测，便于乔装时尚达人混淆视听	★★★★★
DC86021 黑科技风扇		清凉+86021 发量-1000	使用极沪城尖端技术，镌刻 DC86021 及神秘暗号等待破解，吹出电子科技之风	★★★★★
DC86021 贴纸		气质+50	就是普通的贴纸	★★★☆☆
漏洞银行 文化衫		气质+100	挖洞精英伪装道具，长期与 BUGBANK 表哥表姐同处一室，自带挖洞 BUFF，助你早日致富	★★★★★
ByteSRC 保温杯		健康+100	黑科技蝴蝶不倒杯设计，守护你的键盘安全	★★★★☆
ByteSRC 旅行充电器		手机电量+∞	随带随充，永不断电，为应急响应时刻准备着	★★★★☆
ByteSRC 帆布袋		背包容量+10	文艺青年清凉一夏，极客道具藏匿百宝袋	★★★★☆
四叶草 数据线		手机电量+∞	借给小姐姐，可获得脱单机会；借给兄弟，hxd 爱不释手有借无还	★★★☆☆
四叶草 晴雨伞		健康+100	全自动一键开合 ， 对单臂残障人士十分友好	★★★★★

四叶草 书签		武力+50	精选幸运山稀有矿石锻造而成，必要时可用作防身武器	★★★☆☆
四叶草 笔记本		记忆力+50	挖洞思路幸运冒出，不错过每一个 0day 灵感瞬间	★★★☆☆
小米 公仔		可爱+100 少女心+520	猛男必备解压神器，如女友般柔软，伴你度过每一个孤单的夜晚	★★★★★
小米 车载香薰		情调+100	神秘香味激发你的驾驶欲望，为你的爱车增光添彩，下一个秋名山车神就是你	★★★★☆
BSRC 公仔套装		可爱+500	五只小可爱，一次全拥有，无论摆在哪里都是一道靓丽风景线，隔壁小孩馋哭了	★★★★☆
BSRC 手机自拍套装		颜值+100 时尚+100	谁是世界上最帅的表哥？便携自拍套装，记录你的每个帅气瞬间。搭配女朋友使用效果更佳	★★★★☆

error 404

尊敬的极客英雄候选人，感谢你看到这里。

再次诚挚地向你发出邀请，请加入我们，加入这场关乎全国乃至全人类命运的极沪城网络安全保卫战！本次DC86021·β行动的成败，五面安全盾墙能否成功筑起，正取决于你的选择。

8月21日，我们在云端等你。

此致

敬礼

极沪城网络及通信数据总调度中心

暨 DC86021·β行动总指挥部

再次重申：

不要回复！

不要回复！

不要回复！

!

“报告队长，经调查，我们已经成功获取了关于∪组织真实身份的情报。”

“什么？！竟然是他……”

(未完待续)

主办方

承办方

社区伙伴

技术支持

赞助支持

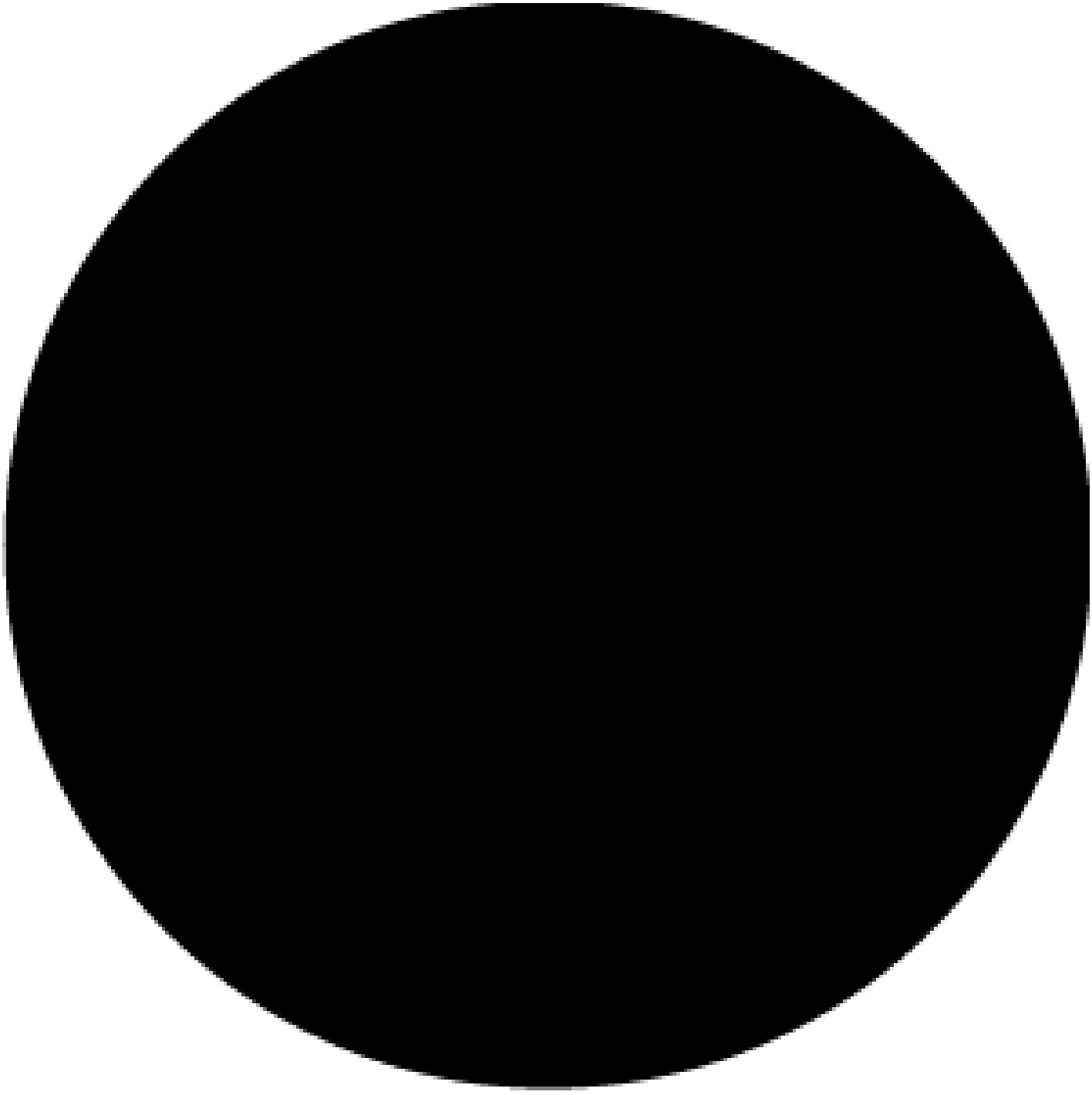
活动支持

*以上排名不分先后

扫描下方二维码加入星球学习

加入后会邀请你进入内部微信群，内部微信群永久有效！

目前28000+人已关注加入我们



点击“阅读原文”，即刻空降至DC86021行动地点