FREEBUF

BUF早餐铺 | Intel实测CPU漏洞补丁对性能影响不大；macOS再现严重漏洞；恶意软件LockPoS使用新的注入技术来避免检测；《绝地求生》国内外挂太多，国外玩家Steam刷屏求锁区

Andy 2018-01-12 共52947人围观，发现 2 个不明物体 资讯

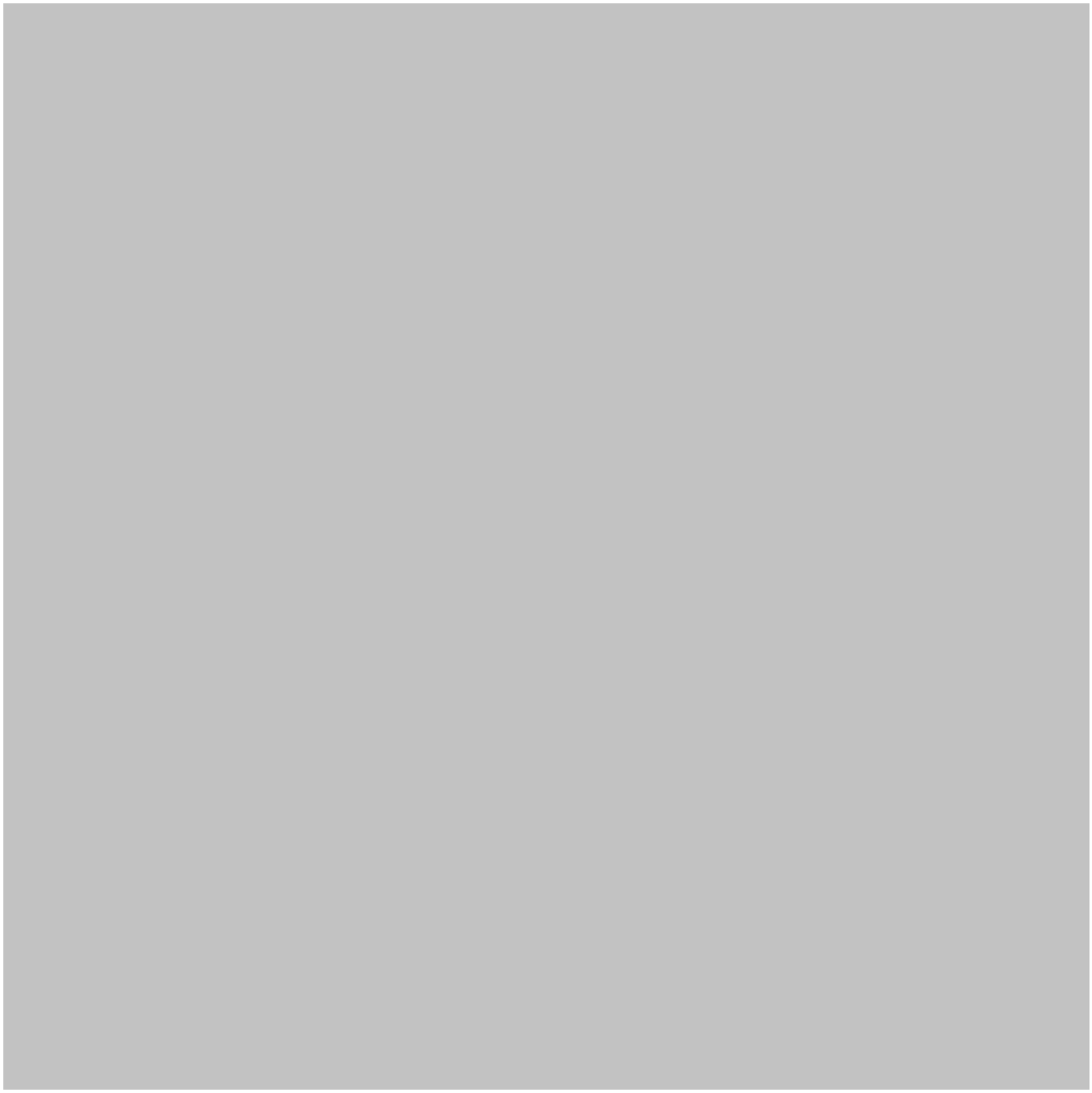
又到周五，想必很多**FreeBufer**已经开启周末模式了，但也不能错过今天的早餐啦：英特尔为了消除大家的误解，发布实测结果——**CPU**漏洞补丁对性能影响不大；**macOS**漏洞导致本地管理员可以使用任何密码解锁**App Store**系统设置；恶意软件 **LockPoS**使用新的注入技术来避免检测；中国男子因黑客入侵 和勒索旅行社被捕；因《绝地求生》国内外挂太多，国外玩家**Steam**刷屏求锁区。

【系统安全】

Intel实测CPU漏洞补丁对性能影响不大

这段时间关于CPU漏洞 每天都有新的信息出来，而大家最关心的依然是CPU漏洞补丁对于性能究竟有多大影响。根

结果。



评估结果（点击查看大图）

对于配备固态存储设备的第八代酷睿平台（Kaby Lake、Coffee Lake），防御措施对性能的影响很小。在各种工作负上，包括SYSMark2014SE基准测试中所代表的办公软件和媒体制作在内，预计影响不到6%。在特定情况下，用户可受到更大影响。例如，使用涉及复杂的JavaScript操作的Web应用的用户可能受到更大影响（英特尔的初步测试表明最高可达10%）。游戏等图形密集型工作负载或财务分析等计算密集型工作负载受到的影响最低。

测试表明，第七代Kaby Lake-H高性能移动平台受到的影响，与第八代平台相似（在SYSMark2014SE基准测试中大为7%）。

对于第六代Skylake-S平台，我们的测试表明，性能所受影响稍高，但与第八代、第七代平台所受影响仍然大体上一

见操作系统，尤其是在办公环境中。测试观察到的影响很小（在SYSMark2014SE基准测试中大约为6%），甚至低于备硬盘的系统。

英特尔官方测试结果：https://newsroom.intel.cn/news-releases/press-release-2018-jan-11-02/

macOS漏洞导致本地管理员可以使用任何密码解锁App Store系统设置

macOS 10.13.2系统中被爆出一个新漏洞，利用漏洞可以让本地管理员用任何用户名密码解锁App Store系统设置。也是说如果你在办公室里离开时没有锁屏，别人就可以更改你的App Store设置。

使用这个漏洞非常简单，只需要打开App Store系统设置，如果小锁被锁住，点击它，macOS会提示输入密码。输入任何密码点击解锁，App Store系统设置就被解锁了，之后黑客就可以操作其他的选项，包括如何安装更新、从什么渠安装软件等。

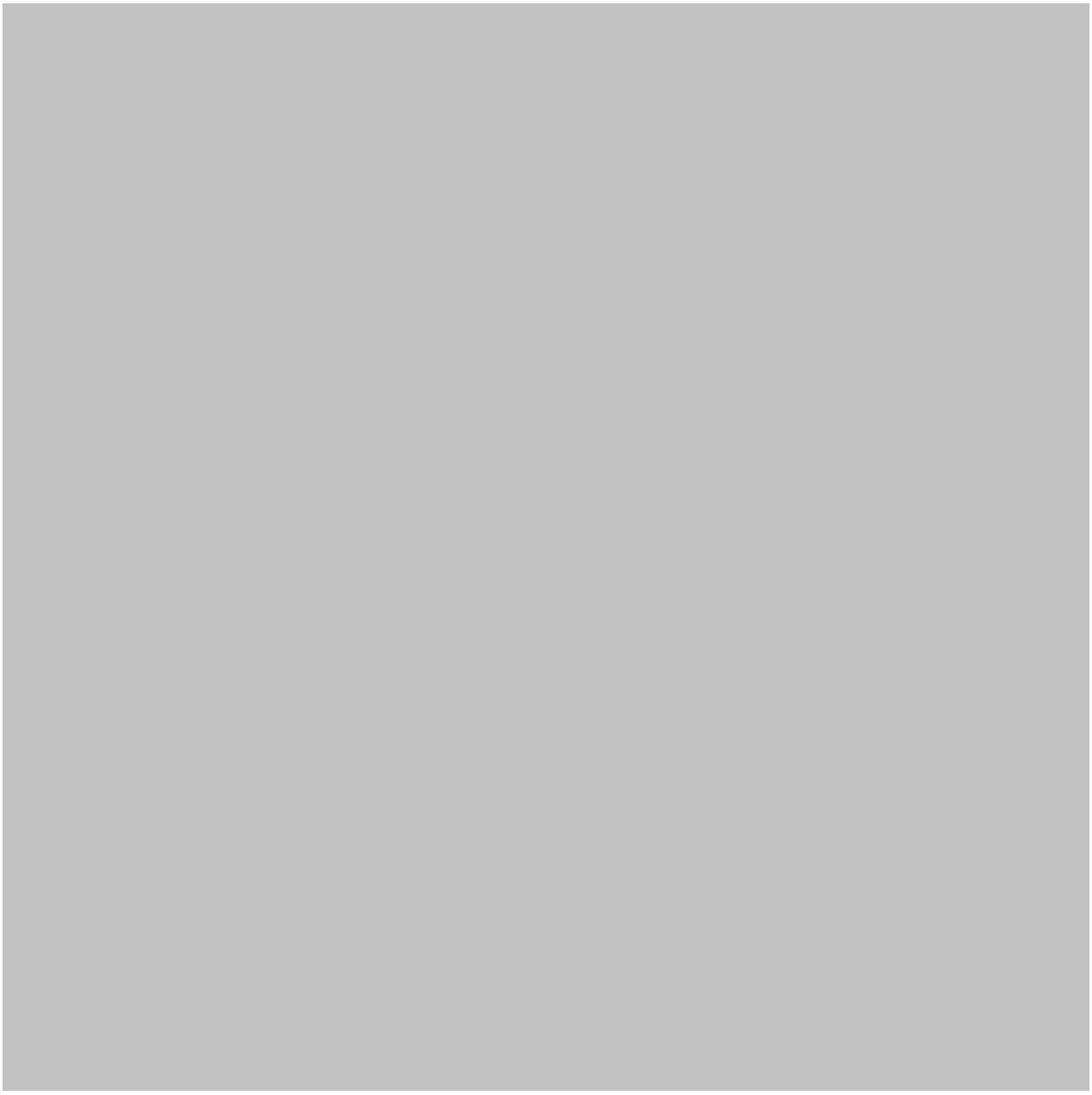
经过测试，漏洞在macOS 10.13.1版本上无效。另外macOS High Sierra 10.13.3的第三和第四个测试版也无效，因此漏可能只对10.13.2和10.13.3的早期beta版有效。

[来源：BleepingComputer]

【数据安全】

恶意软件LockPoS使用新的注入技术来避免检测

Cyberbit安全研究员发现Flokibot恶意软件变种LockPoS，使用了一种新的恶意软件注入技术，可以避免被检测。Cyber Bit发现的PoS恶意软件有三个主要的程序用于在远程进程中注入代码：NtCreateSection，NtMapViewOfSection和NtCreateThreadEx。

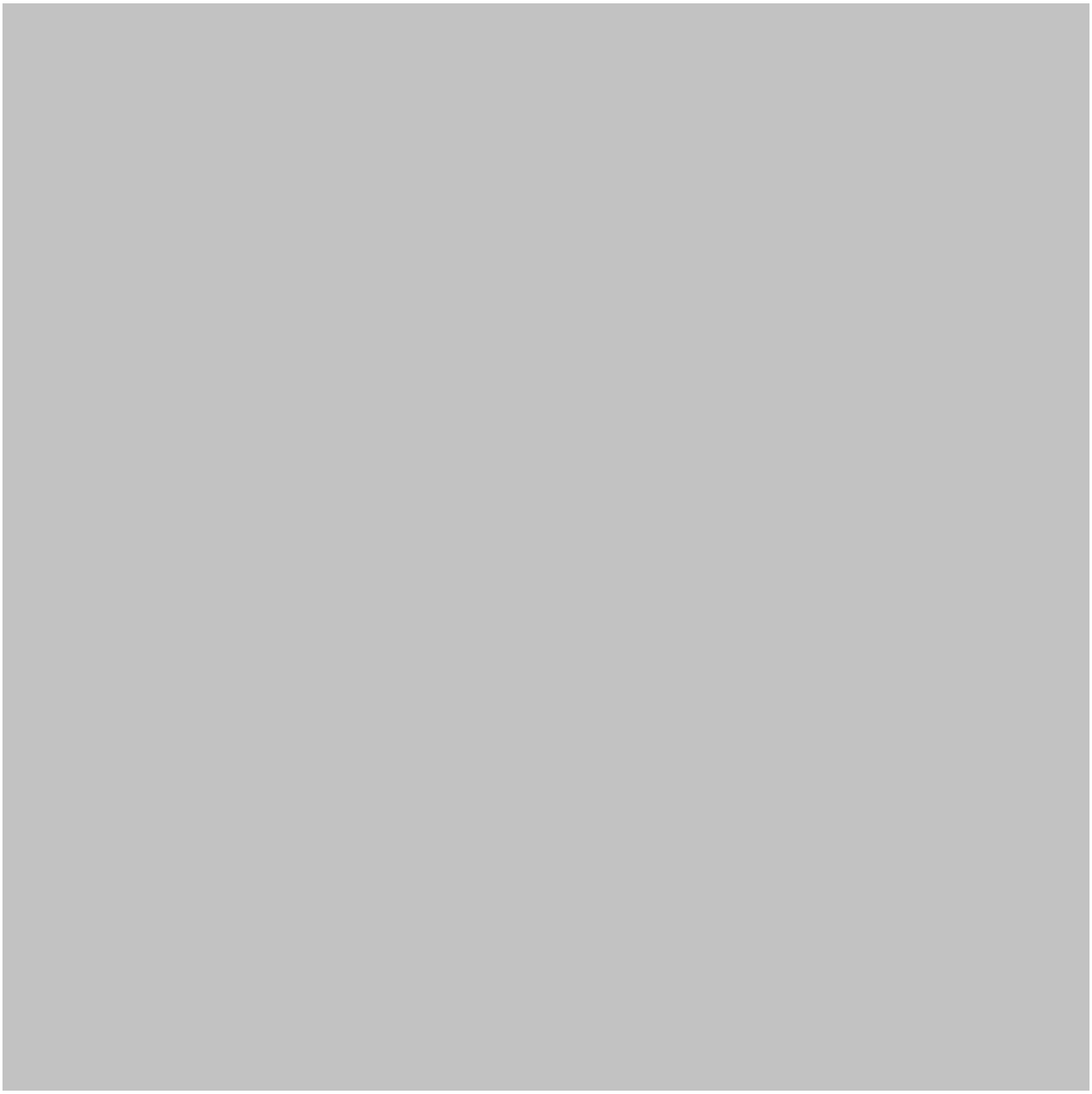


注入技术中使用了Windows系统原生的核心dll文件ntdll.dll。与ntdll相关的程序（前缀为“NT”）与Windows API分离户空间和内核空间相关联。注入技术涉及在内核中创建一个段对象，使用NtCreateSection将NtMapViewOfSection作一个映射来查看其他进程中的段，然后将代码复制到段中，并使用NtCreateThreadEx或CreateRemoteThread创建一个程线程执行代码。

[来源：securityaffairs]

中国男子因黑客入侵 和勒索旅行社被捕

中国警方只用了四天的时间就逮捕了一个涉嫌入侵两家香港旅行社服务器的黑客，并且在窃取数据后要求支付比特赎金。



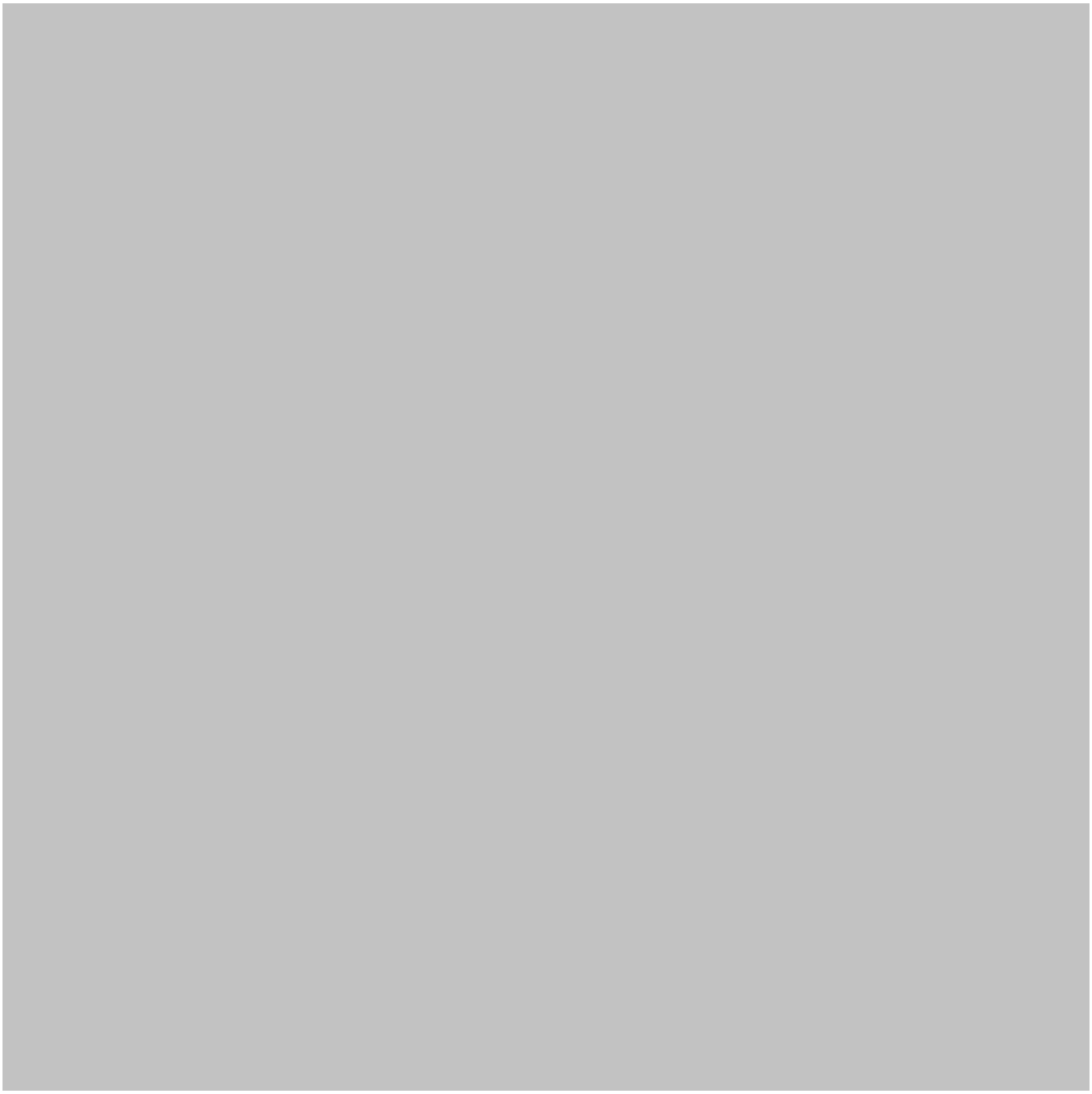
该男子声称已经获取旅行社20万用户的信息，包括姓名、身份证号码、护照号码、 手机号等，如不支付赎金变将其
布到网上。

而在去年11月份，一名黑客入侵了香港最大旅行社WWPKG Holdings的服务器，盗取了20万客户的数据。目前警方
在调查该男子与去年作案的黑客是否为同一人。

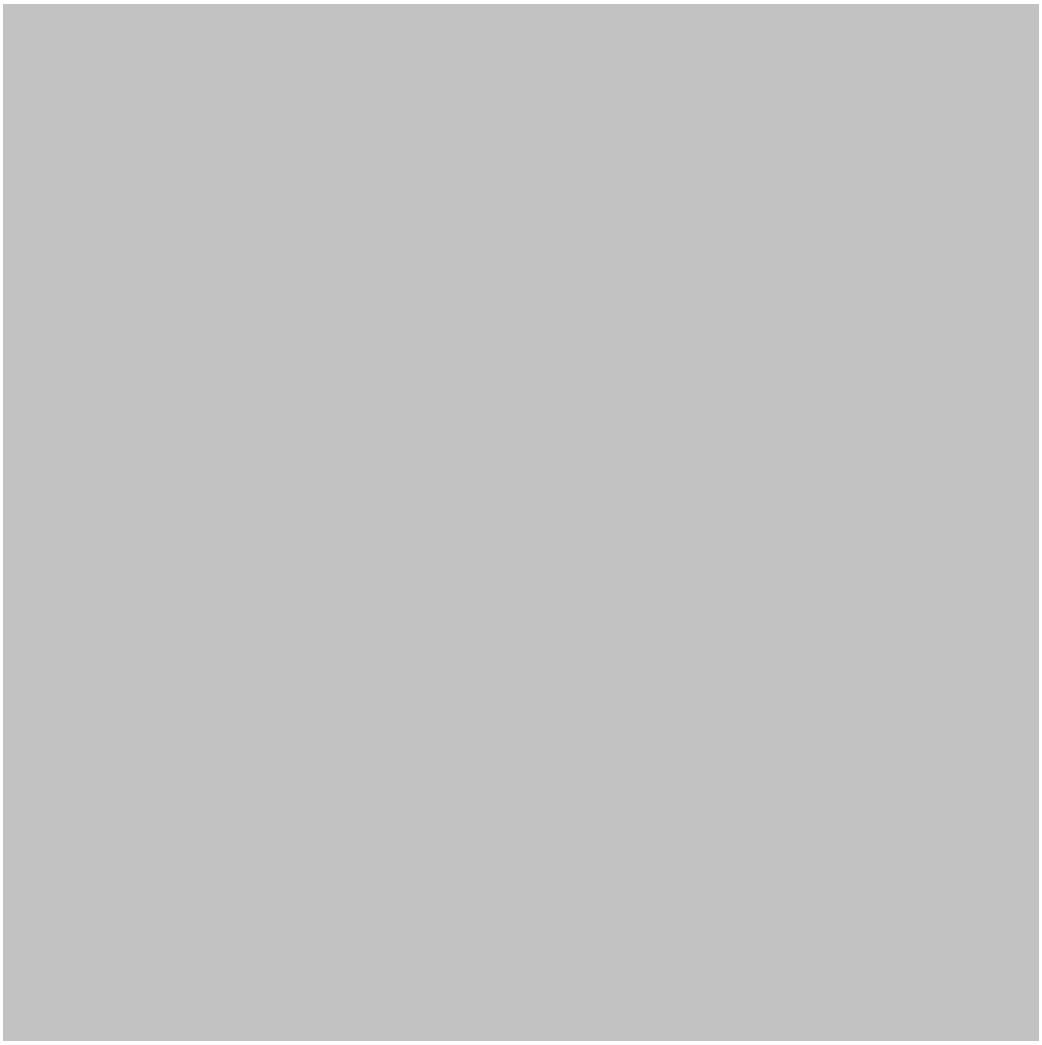
【其他】

因《绝地求生》国内外挂太多，国外玩家Steam刷屏求锁区

此前《绝地求生》的游戏监制和创始人Brendan Greene承认，目前游戏中有99%的外挂都来自中国，但也同时坦言不
因此锁区，毕竟仍然有许许多多的中国玩家并不使用外挂。



吃鸡游戏太火，也因为外挂泛滥，为病毒、木马提供了绝佳传播渠道。与此同时，近期国外玩家集体在Steam刷屏要
《绝地求生》锁国区，不让国内玩家出现在其他国家服务器。



面对这种情况，不知道《绝地求生》运营方会如何处理。此外，在腾讯代理成为国内《绝地求生》官方代理方之后也表示将尽最大力度打击外挂。

*Andy编译整理，转载请注明来自 FreeBuf.COM

上一篇：
芯片漏洞新进展：英特尔公布补丁对性能影响的测试结果；Meltdown的POC在Github上公开；NVIDIA更新GPU驱动以
下一篇：本篇已是最新文章

已有 2 条评论

幕刃 2018-01-12 1楼 回

没有Blackhat EUROPE 2017的PPT么

亮了

mickey80 (1级) 2018-01-12 2楼 回

666

亮了

选择文件 未选择任何文件

昵称

请输入昵称

必须 您当前尚未登录。登陆? 注册

邮箱

请输入邮箱地址

必须（保密）

表情 插图

提交评论(Ctrl+Enter) 取消 有人回复时邮件通知我

Andy

曾梦想仗剑走天涯，看一看世界的繁华。

26 文章数

10 评论数

最近文章

- BUF早餐铺 | Intel实测CPU漏洞补丁对性能影响不大；macOS再现严重漏洞；恶意软件LockPoS使用新的注入技术来避免检测；《绝地求生》国内外挂太多，国外玩家Steam刷屏求锁区

  2018.01.12

- 不止于小程序，APICloud推出React Native纯翻译模式的UI引擎

  2018.01.11

浏览更多

相关阅读

数据分析告诉你：Php最不安全，Ngin…

卡巴斯基实验室揭示RDP暴力破解呈…

别用Chrome浏览这篇文章，会崩溃！

快讯：黑客宣称盗取Dropbox700W数据

中国教授在BlackHat现场演示破解SIM…

特别推荐

willhuang 2017-10-21

【已结束】第三届中国(北京)军民融合技术装备博览会现场实况

Elaine_z 2017-07-03

毒舌评论砖家 2015-06-03

Windows 10新变化：系统自动更新将“强制化”，用户不再可选

dawner 2015-07-20

css.php