SILIC

干涉香港的黑客 Strudalz

习科道展网络信息安全顾问

最具实力的网络安全专家

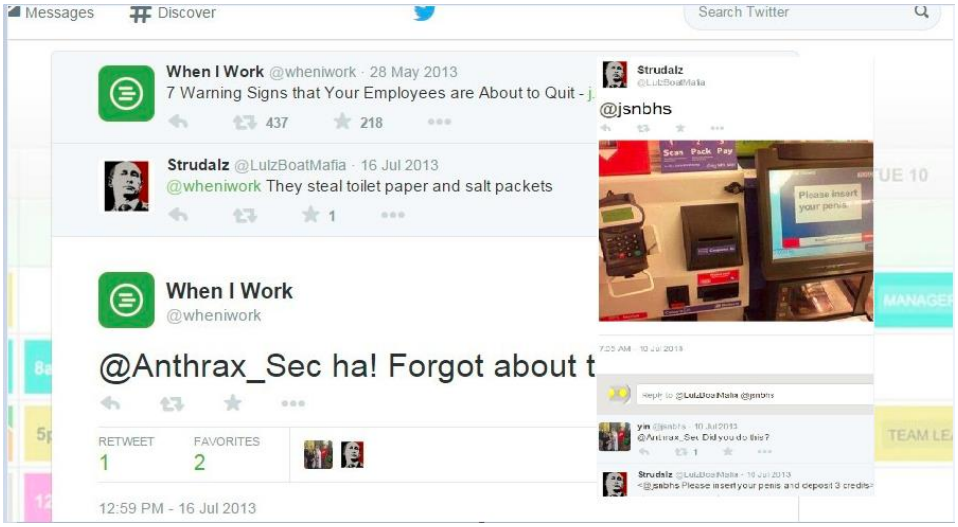
索引

1) 个人资料

近期在 twitter 等地方出现了一个名为“OpHongkong”的活动，旨在通过入侵以.cn、.hk 结尾的政府站点来进行反北京反香港的运动。通过对 OpHongKong 活动的摸索，我们发现一个名为 Strudals 的黑客会定期在聊天室发布入侵的目标，于是对 Strudals 进行了一定的调查。

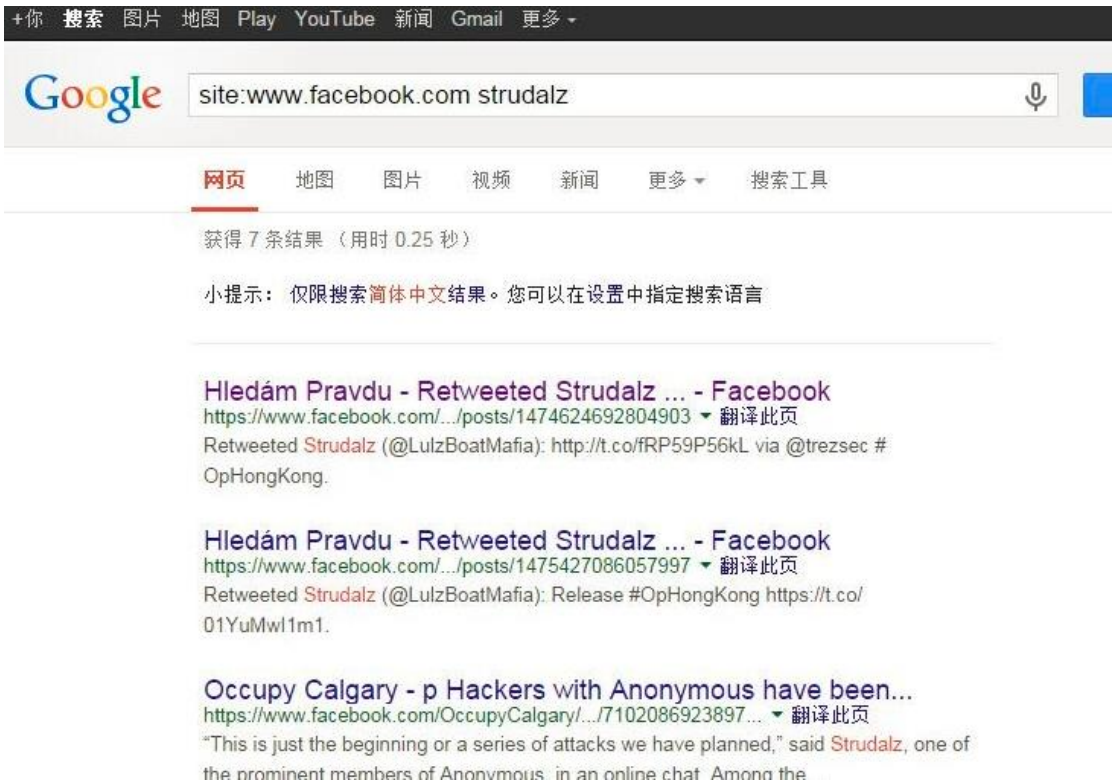
1.1 网上信息

twitter 中#OpHongkong 的账号是发起活动前后才新建的专用账号，在所谓的黑客行动中只发现由 Strudalz 推送入侵目标，因此直接从“Strudalz”开始查找其个人信息，而且通过对其朋友圈的排查，黑客 Strudalz 就是发起者。Strudalz 会组织黑客使用 anonops 聊天室进行入侵活动，还会通过 twitter 等发布消息，其 twitter 账号为 Strudalz 同名的@LulzBoatMafia。



其个人同名 twitter 中含有大量的旧的个人信息，根据前后内容、用词习惯以及交往的朋友圈子，可以确认@LulzBoatMafia(即 strudalz)这个推文账号一直都是由其本人发布的推文。

通过对其 twitter 账号中的推文进行检索，strudals 应该曾经有过 Facebook 账号，但是应该在最近(根据推文显示应该在 8 月份以后)注销掉了。通过搜索引擎搜索蛛丝马迹：



Strudalz 的 Facebook 页面虽然没了，但是可以确定他曾经有过 Facebook，并且也能通过搜索引擎的缓存找到一些敏感信息，如他的朋友圈，以及他一些曾经公开的信息指向，如曾经的地理位置：

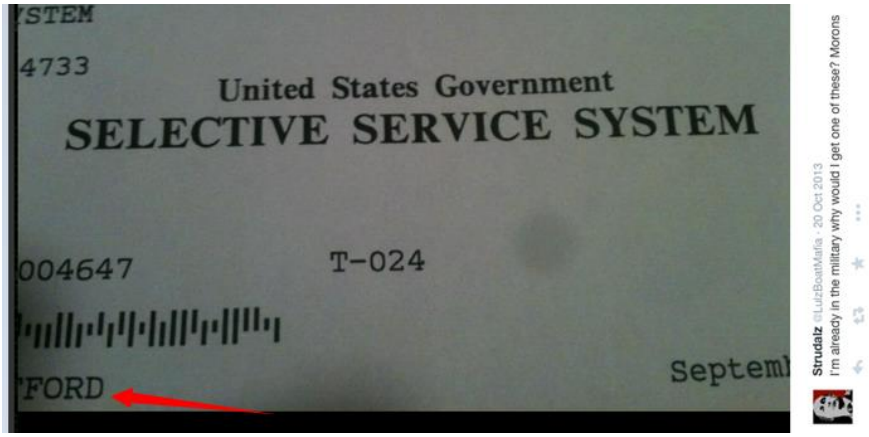
美国人的生活规律是通常不会在一个地方呆很长时间，通常也不会在“家乡”呆很长时间。后面可能更倾向于其在底特律(密歇根州，犯罪率极高)长大，或者也可能底特律是他的家乡。

接下来是看他的真实背景资料

1.2 真实背景资料

通过检索 Strudalz 的网上发布的敏感信息进行汇总，可以确认其一些真实身份和信息。

首先是国籍和真实姓名中的“Last Name”，其曾经在网上发布过一张美国的选举票，首先可以证明 Strudalz 已经是美国公民，其次是票上面印有“Ford”结尾的字串，应为姓名当中的“姓”。



但是这个姓并不全，F 前面还有字母，因此他的“Last Name”并不是“Ford”。根据另一张图中的细节可以推断出他完整的“姓”。

这张图是很久以前 Strudalz 给别人传的图片的评论，图片内容则是朋友圈中好友发的照

片，然后拿手机在屏幕上拍的，照片中的评论中有个长得相似度比较高的人对照片做了评论，这个人的名字叫做 Michael Gafford。通过读取缓存进行检索，发现#OpHongkong 发起人的推特账户曾经使用过“Michael The God”这个名字。

根据以上“Michael Gafford”朋友圈、选片名字、照片都能与黑客“Strudalz”的信息匹配上，所以基本确定网名为 Strudalz 的黑客就是现实中的 Michael Gafford。

有了这一条线索以后，就可以找到很多照片、信息和文件来证实。最有说服力的是他的学业证书。

游戏设计和编程专业，毕业于 2013 年。目前尚不清楚他的真实年龄，在他的推文中有大量的军队的照片等，怀疑他曾经在校期间服过兵役，而且可能是负责亚太地区的兵种。

这种图片是去年 10 月发的，通过对胸牌上的信息进行搜索和查找可以锁定这个人全名叫做 Josh Lempicki(个人主页 https://www.facebook.com/josh.lempicki)，居住地在密歇根，应该不仅仅是同学这么简单的关系，可能是战友、或者老乡。

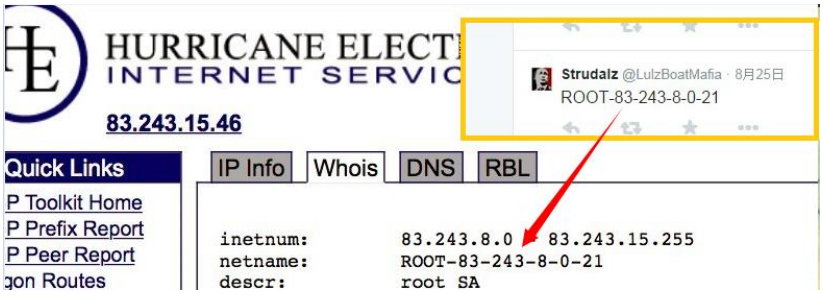
最后附上他的个人照片：

2) 政治倾向

null

2.1 攻击方向与常用攻击手段

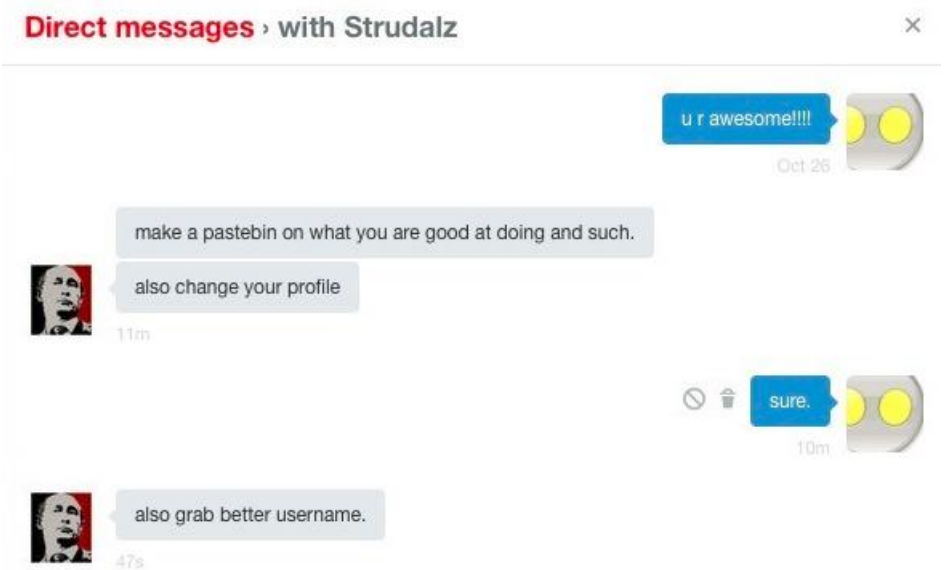
Strudalz 只对 gov.cn 和 gov.hk 结尾的网站发起攻击，通过对被入侵的服务器的日志进行分析，他(们)常用的攻击手段有上传解析漏洞、简单的 sql 注入等手段，而更多的则是 DDoS 拒绝服务攻击。下面是他购买的专门用来 DDoS 攻击的服务器。



从技术角度来看 Strudalz 以及其号召的人的整体水平一般。

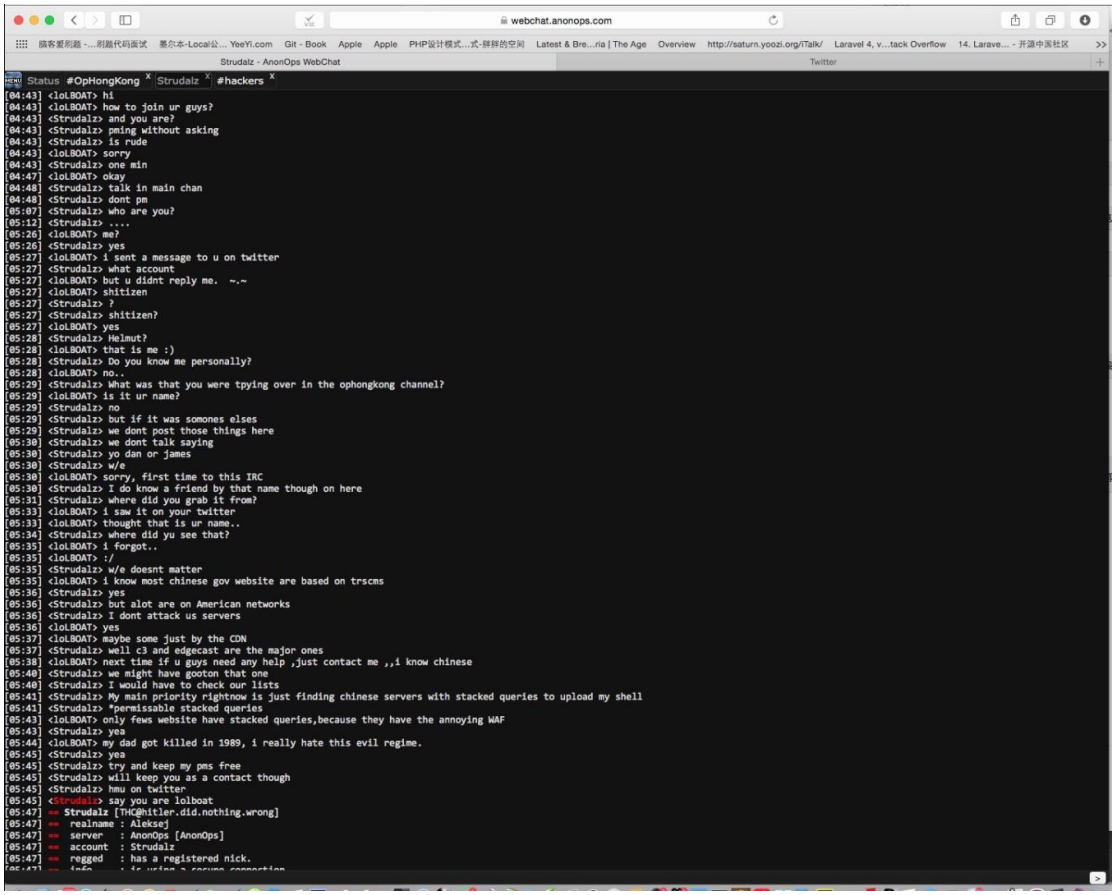
2.2 未来趋势预测

但凡是愿意追随 Strudalz 的号召的人，即使是技术水平不行的人，Strudalz 也会一步一步的教这个人怎么成为一名合格的“黑客”，从昵称、服从组织以及工具、目标等等。



通过在聊天室中和 Strudalz 聊天时，追问一些关于为什么入侵的原因的时候，Strudalz

首先的反应是强调他没有搞过美国的网站，反推他可能和 CIA 之类的人打过交道，一直聊都没有聊到“钱”这方面去，所以这个人不一定是给美国政府干活的。



从网上搜了一下他毕业的学校“William D.Ford Career Technical Center”发现里面有多位华裔校友。在北美上这类小学校的学生很普遍，但如果是从中国去留学报“Center”类学院的留学生则通常是一心为快速移民的，且在中国的条件可能并不理想。

根据已有信息推测有一定可能性 Strudalz 是受在外华裔的鼓动，但是不排除是美国政府暗中支持，如果他是个人主观针对香港和北京，则很有可能与他曾服兵役有关。我们还会继续尝试确认其背后的原因。