AutoSpoilt - - -

现今的年轻人是有史以来**技术最精湛**的一代。为孩子们教授程序编码技能的游戏，让他们成长为一个无与伦比的技术控。在**万物互联**的浪潮下，企业信息技术部门承诺提供更为宽泛的**安全岗位**就业机会，使父母尽过早地鼓励孩子获得网络技能知识。当然，**安全文化**转型也带来了一些负面影响。



年轻一代的黑客正在崛起，他们有一个标签“脚本小子”。这些青少年黑客往往兼备核心的编程能力。然而，他们对于围绕在他们身边的技术感到舒适和熟悉。脚本小子是心中的理想主义者。今天初显反叛和个人主义的表现，像美剧[《黑客军团》](http://mp.weixin.qq.com/s?__biz=MzA3MTM0NTQzNA==&mid=2455684216&idx=1&sn=8c8c11ef8a8f6d8dba868c98866d1e2f&chksm=8884900dbff3191ba656cc183e5e56be754020d829db515f59ae2b508a6a425c0112dde9795a&scene=21" \l "wechat_redirect" \t "_blank)Robot先生这样（角色）的电视节目引起了一场激动人心的追剧潮，还有【匿名者】Anonymous这样的真实黑客组织。

**HK黑 客 工 具**

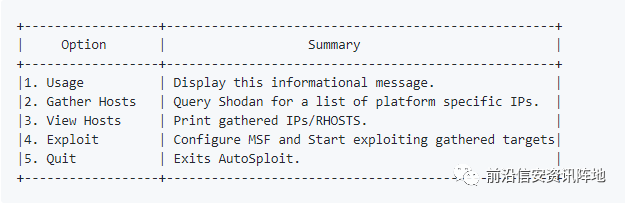
“**黑客工具**”是专用软件的名称，使得发起网络攻击的工作变得更容易。像**Eternal Blue**这样的高性能黑客工具是这类软件的精髓所在。这个特殊的工具从国家安全局得来，在被暗网卖掉之前，被用来去执行去年臭名昭着的**WannaCry**攻击。

本周，一种新的安全工具（**AutoSpoilt**）在GitHub上发布，该工具基于Python 2.7，辅助**Shodan**搜索引擎及**MSF**平台，可以自动查找并破解易受攻击的互（物）联网设备，从而对现今的互联网产生较大的**威胁风险**和**不可预见性**。

**AutoSpoilt**是一个由匿名安全研究员Vector开发的开源程序，可以在网站GitHub上免费下载 | **https://github.com/NullArray/AutoSploit**

顾名思义，AutoSploit为查找和利用目标带来了**全新的功能**。通常情况下，黑客必须努力寻找特定的目标，检查目标是否容易受到特定的攻击，然后发起**成功的攻击**。

另一方面，AutoSploit通过将许多不同的黑客工具合并到一个工具中来实现自动化。最有幸的是，它利用了一种名为Shodan的网络搜索工具的强大功能，以及Metasploit[**MSF**]的强大黑客工具（通常被**“白帽子**”黑客用于**渗透测试**）。



**AutoSploit解释了该工具的基本工作原理：**

“开始使用这个工具，然后输入一个搜索查询，就像'**Apache**'一样。之后，该工具使用Shodan API来查找在Shodan上被描述为“Apache”的框[电脑]。

“之后，根据您的搜索查询加载和排序Metasploit模块列表。一旦选择了适当的模块，它就会开始顺序地在你获得的目标列表上运行它们。