来自Clone的攻击恶意软件高明技巧欺骗用户 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/469/2021_2022__E6_9D_A5_E8_87_AAClon_c67_469467.htm 恶意软件（aka “ rogue反间谍软件 ”）从没停止去用高明的社会工程以及窍门来从用户那里骗来他们的血汗钱。最近我们注意到此类软件大幅地增加了。最近我们遇到一个叫做AVSystemCare实例就说明了这种趋势。 该恶意程序的独特之处有两个方面： -在查询和执行的时候，它使用了很容易地生成无限大的Clone的高明技巧。 -它支持很多种语言版本。 AVSystemCare使用了一种很高明的技巧来让它的Clone利用同样的文件，但是还没有不同名字。安装这些clone中的任何一个你都得从clone网站上下载一个小文件。用户执行了该文件后，它就会下载主程序软件。所有的程序文件，包括从clone网站下载的文件都是一致的（同一种语言的clone的文件）。 因此，如果每个clone的这些文件都相同，那么安装程序在安装程序的时候怎么知道应该用哪个名字呢？答案就在用户cookie里。访问clone 网站下载程序后，你的电脑里就会储存一些cookie。访问了一些clone站点后，我们可以发现每个域的这些cookie非常类似： 执行下载的文件，它会将用户Cookie解析，以寻找带有‘ gli ’‘ gai ’和‘ gI ’的cookies。拥有这些cookie的域也会有随机命名的cookie，这些cookie的内容域中包含了clone程序的名字： 安装程序在随后的安装中使用该名字。它将使用匹配的最新Cookie，如果你碰巧下载的是Clone A，而访问了Clone B的网站，那么你安装应用后它的名字就叫clone B。 你可能正想知道如果在安装之前删掉了cookie会怎样。如果安装程序找不

到它要找的cookie，那么它就会使用默认名称。英语clone版的默认名字是AVSystemCare。我们的测试也显示出AVSystemCare cookie引擎成功地解析了IE和FireFox的cookie，但是它无法解析Opera或者Safari的。 如果你不喜欢AVSystemCare clone的名字，你可以很容易地在安装之前修改cookie，从而自己选择名字： AVSystemCare的作者也没有只是局限于英语clones；到目前为止，我们发现了11种不同语言版本的clone-英语、葡萄牙语、德语、丹麦语、西班牙语、意大利语、法语、日语、荷兰语、挪威语以及瑞典语。同时，存有不同语言版本AVSystemCare的clone的域有70多个；例如，avsystemcare，virenfrierpc，norwayvirus等等。 跟往常一样，给定语言的所有的Clone除了名字不同都使一样的，就像列出的日语和挪威语clone一样： 如下视频证明了AVSystemCare与它的一些Clone的类似之处。 随着AVSystemCare机制连续地生成clone，用户需要格外当心。赛门铁克的关于恶意程序的新的子站提供了此类威胁的深度信息，包括他们如何攻击以及如何保护自己。 