电脑 马桶 手机 汽车 微波炉 心脏起搏器 冰箱 ……

黑客用什么方法黑了它们?

说起黑客,不少人会联想到《黑客帝国》中戴着墨镜狂霸酷炫跩的男主角,也能脑补出一个宅男盯着电脑屏幕猛敲键盘,眼中滚过一行行绿色代码的画面。说起黑的内容,也大都是某不合民心的网站、某漏洞百出的软件。然而实际上,现实中黑客的"工作范围",早已超越了电脑,延伸到一部手机、一辆豪华车、一台ATM,甚至一个智能的抽水马桶……渗入到我们生活中的黑客技术,似乎已经高超到有点吓人了。 现代快报记者 吴怡

美国超级黑客逝世

可以让ATM吐钱,可以用心脏起搏器杀人

据近期的新闻报道,美国旧金山著名的黑客巴纳比·杰克(BarnabyJack)被发现身亡,年仅35岁。

这名超级黑客曾在2010年的黑帽子大会上成功地演示了如何入侵安装有两种不同系统的ATM,并当场让ATM吐出钱,他将那种入侵称作是"jackpotting"。他因为那次演示而一战成名,迅速成为黑客社区的名人。

据了解,杰克本来计划在今年的黑帽子大会上演示另一项备受期待的黑客技术,内容是如何入侵心脏除颤器和心脏起搏器。他已经研究出一种方法,可以在距离目标50英尺的范围内侵入心脏起搏器,并让起搏器释放出足以致人死亡的830V电压。

原理

ATM是如何被黑的

用Google搜索型号,根据型号编写代码

说起不法分子利用ATM的漏洞来取钱,新闻中也曾经有过报道,多是通过伪造密码键盘,或是张贴虚假告示的方法引人上当。而巴纳比·杰克所演示的入侵ATM,却能够指挥ATM当场吐钱,无需银行卡。这种操作的原理何在?

根据美国杂志《连线》(Wired)2011年1月31日的报道,杰克在大会上证明了自己的实力,在不到一分钟的时间内,用脚本的窍门让ATM自动吐出了一叠叠现金,其使用到的只是一些简单的工具和Google搜索。首先搜索到ATM的品牌型号,网络上都能够查出它的硬件型号、操作指南等等。

之后针对不同的ATM型号编写代码,当然,这是一个恶意的软件。再找机会打开ATM的控制板盖子,将记忆卡或者SD卡插入ATM的主板,系统会误认为正在升级,从而写入恶意软件。

这种行为非法暂且不说,但能证明的是,在黑客们高超的电脑软件技术面前,含有电子系统的设备漏洞显露无疑。

心脏起搏器是如何被黑的

截取电磁波频率,改变操作命令

这位狂妄的黑客在演示了侵入ATM之后,又将目光放在了心脏除颤器和心脏起搏器上,这未免让人惊恐万分:如果这项技术真的被人掌握,那杀人还不是分分钟的事情?

类似的情况,在美剧《国土安全》(Homeland)中也有出现。主角Brody把副总统心脏起搏器的序列号告诉恐怖分子,直接导致副总统的起搏器错误工作,杀人于无形。

让人费解的是,心脏起搏器位于人体内,又无法导入恶意软件,如何能被外界操控呢?现代快报记者咨询了南京大学微电子设计研究所副教授潘红兵。

"这种黑客技术与电脑无关,与电磁脉冲有关。"潘红兵介绍。据了解,心脏起搏器经常用于那些罹患慢速心率失常的患者。在发病时,患者的心跳会突然减慢,严重威胁到患者的生命安全。而起搏器的作用,就是在此时短促多次的触发电脉冲刺激心肌,带动心脏正常跳动,挽救生命。目前的心脏起搏器都是植入患者体内,小巧而强大。国外有些先进的起搏器能够监测患者的心跳情况,在预设的治疗模式中选择最合适的,简直能称得上智能。

"像这种智能的仪器,虽然小,也存在风险,因为它能够发射出电磁波。"潘红兵表示,只要心脏起搏器自身能发射接收电磁波,这种频率就能够被有心的黑客所截取,并且读出它的序列号,从而改变仪器的设置、操作命令等等。"只要给心脏起搏器接上一个超级电容,就有可能生成瞬间高压电,因而像杰克那样释放出830V的高压,理论上是可行的。"因此看来,一个全新的心脏起搏器,虽然能够智能操控,远程操作,但安全性有时还比不上纯手动控制。

应对

马桶、汽车、冰箱、微波炉……黑客能入侵的范围远超我们想象

除了心脏除颤器、心脏起搏器,黑客所能侵入的范围远远超出了我们能想到的。几天前,有媒体报道,日本新出了一款智能马桶,能够通过手机控制,然而也有弊端,那就是容易遭到黑客的攻击。据了解,这种名为"萨蒂斯"(Satis)的自动马桶,可以通过免费的蓝牙应用程序进行控制。使用者只需用装有这项应用的安卓手机,就可以控制马桶盖的起落,或开启坐浴盆和冲水等功能。虽然如此,IT安全公司却警告称,这种智能马桶存在严重的蓝牙安全漏洞,任何人都可以下载应用程序,对马桶进行控制。如果真有人要开玩笑,估计使用者会抓狂。

"很多智能的汽车也容易被黑,"潘红兵拿最近几年新出的Google汽车举例。 据了解,这种车是谷歌发布的无人驾驶汽车,无需人工控制,就能够自动驾驶。"这种汽车的各种关键部位都有电子感应装置,比如油门、刹车,都能够自动感应位置,调整液压系统,改变各个部位的压力,从而决定车子是否前行、速度如何。除了Google汽车,实际上很多高档汽车也都安装了电子操控设备。"潘红兵告诉现代快报记者,目前普通的汽车上,也分布着一些电子设备,例如导航、倒车雷达影像、智能空调等等,而高档车为什么那么贵,实际上有40%的钱都花在了安装智能设备上,车载雷达、发动机管理、导航管理、碳总线管理等等。"但是有利也有弊,高档汽车的风险大,开在路上,有时候车载的电脑自动死机,或者被黑,车子就会半路抛锚,难以抢救,或者脱离控制。"潘红兵表示,从技术上来说,要做这种车辆的远程操控易如反掌,并不是高难度。所以这个时候,还不如传统的车子,靠手动前进。

随着家电的信息化,能被黑客黑的还不止这些,一台智能调节温度的冰箱,一个智能定时的微波炉,都有可能成为黑客的目标。

防止被黑最简单的方法就是物理隔绝

虽然黑客的下手范围如此广泛,但也并非没有办法防止。潘红兵表示,最简单的方法就是物理隔绝。

"与外界不建立互联通道,黑客自然也就没有下手之地。"简单地说,就是在区域范围内,不使用外界的网络,而是建立内部的局域网,信息都在局域网内传递。"基本上所有的保密机构都不会有外网,而是用自己的局域网。"

除了建立局域网,另一种直接而"粗暴"的方式,就是利用微电波易被隔绝的特点。"比如起搏器、微波炉,如果怕被黑客入侵,可以直接在外面套一层金属壳。"这种方法也被用来减少外界电磁辐射。"就比如南京河西靠近广播发射塔那块,而这种情况下电磁辐射是挺强的,曾经有人想在那里买房,请我出主意,我就建议他在窗户上围一层钢丝纱窗,能够有效防辐射。"虽然有效,但结果有利有弊。"在阻挡了辐射的同时,却也隔绝了电话信号,因此每次要在家里打电话,都很难有信号,只能出去打。"

总而言之,不管哪种方法,都难以十全十美。在科技如此发达的今天,要想完全保证自己的私人信息,杜绝黑客侵入的隐患,最好的办法只能是归隐山林,回归自然。

除了电脑、马桶和冰箱也有可能被黑 本版均为资料图片