OPM

　　所有政府工作人员的OPM(人事管理办公室)管理记录是包括美国军人的个人信息在内的。

　　OPM的数据泄漏事件发生在今年三月份，但是该事件直到今年六月份才曝光。最初的调查结果显示，此次数据泄漏事件泄漏了一千八百万条记录，但在随后的进一步调查之后发现，实际泄漏的记录比之前的还要多四百万。在七月底，泄漏的记录数量增加至了两千一百万。除此之外，研究人员还发现黑客从数据库中还盗取了五百六十万政府职员的指纹数据。

　　美国指责称，此次攻击是由中国发动的。而中国政府的官员承认了此次攻击的确与中国有关，但与中国政府无关，此次攻击是其他黑客组织的个人行为。根据中美间谍协定，中国政府在今年九月逮捕了这一黑客团伙。

　　JUNIPER(瞻博网络)

　　瞻博网络公司是榜单上最后一家遭受到数据泄漏的公司。安全研究人员在瞻博网络的ScreenOS[操作系统](http://soft.chinabyte.com/os/)中发现了[防火墙](http://www.chinabyte.com/keyword/%E9%98%B2%E7%81%AB%E5%A2%99/)设备的后门程序。

　　除此之外，研究人员还在ScreenOS操作系统的源代码中发现了“未经授权的程序代码”，这个后门程序可以允许攻击者访问物理设备，甚至还可以解码[VPN](http://www.chinabyte.com/keyword/VPN/)[通信](http://telecom.chinabyte.com/)数据。

　　该后门的来源目前仍不得而知，但是有些人觉得是中国政府所做的，而有些人却认为是美国国家安全局的行为。也许直到明年我们才能知道到底谁才是这一事件的罪魁祸首了。

　TALKTALK

　　今年，TALKTALK已经是不止一次发生数据泄漏事件了，仅在2015年，TalkTlak就发生了三次数据泄漏。二月份，TALKTALK泄漏了四百万用户的个人数据，今年十月份，TALKTALK又泄漏了两百四十万用户的数据，而在八月份，该公司的子公司(Carphone Warehouse)又泄漏了两百四十万用户的数据。

　　该公司总共泄漏了大约一千零四十万用户的个人纪录，在发生了如此大规模的数据泄漏之后，如果公司还不开除它的CSO，那么用户只能考虑更换[ISP](http://www.chinabyte.com/keyword/ISP/)服务提供商了。