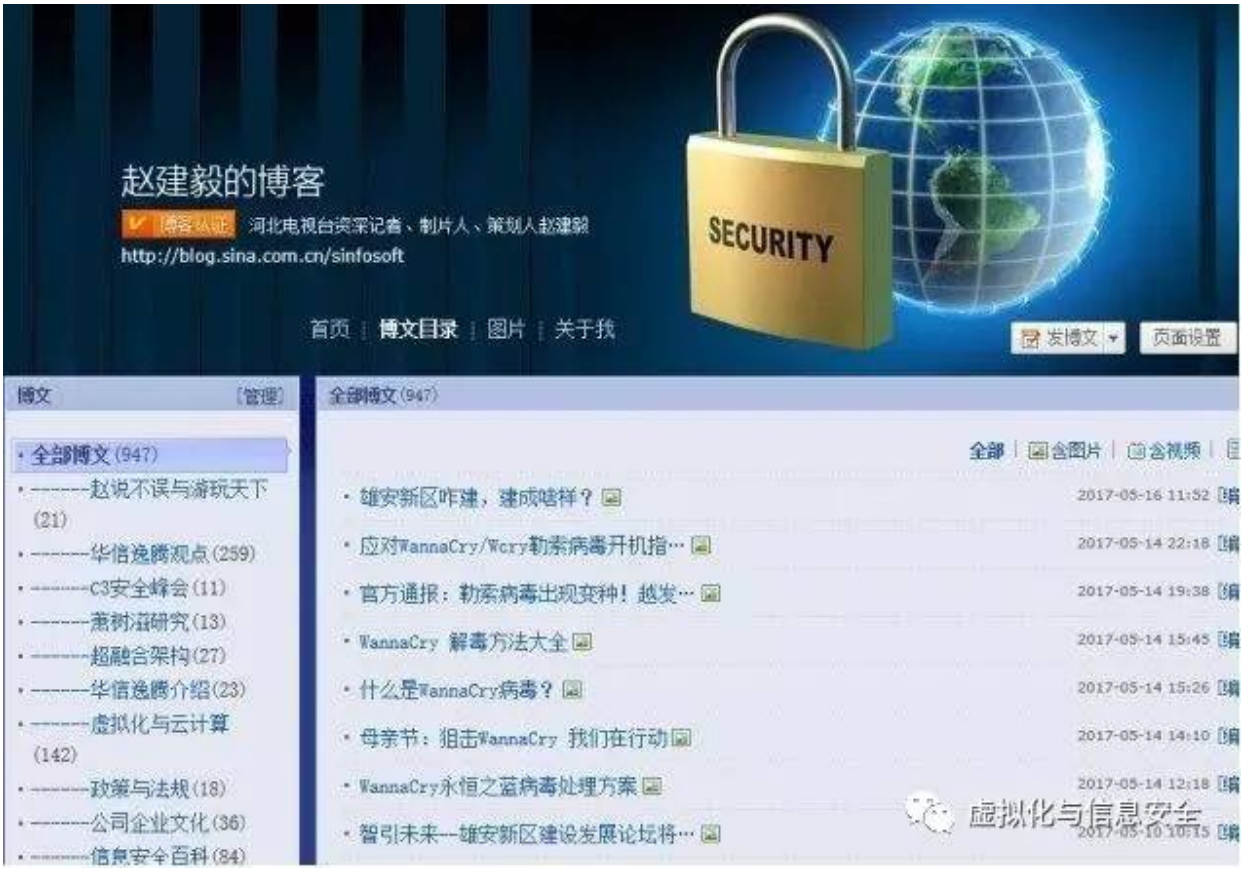
WannaCry：是勒索病毒更是网络武器！

2017-05-19 虚拟化与信息安全



勒索病毒“WannaCry”（永恒之蓝）在全球范围内的爆发，恐怕是这几天影响力最大的公共安全事件了。据笔者了解，河北的一些客户也先后中招，重要的文档被加密了，“在考虑是否给黑客付赎金?”，亚信、绿盟等各个厂家忙乎起来，一呼啦出了很多预防和解决方案。

中招了，能否有解？重要的文档被加密了，付赎金能还原？老赵都不看好，无论是安全厂家还是数据恢复公司目前都没有很好的解决方案。为什么？

简单来说，“WannaCry”（永恒之蓝）这一蠕虫勒索病毒，通过针对Windows中的一个漏洞攻击用户，对计算机内的文档、图片等实施高强度加密，并向用户索取以比特币支付的赎金，否则七天后“撕票”，即使支付

赎金亦无法恢复数据。其加密方式非常复杂，且每台计算机都有不同加密序列号，以目前的技术手段，解密几乎“束手无策”。
那么好，问题来了：这是谁干的？！

勒索病毒是2013年才开始出现的一种新型病毒模式。2016年起，这种病毒进入爆发期，到现在，已经有超过100种勒索病毒通过这一行为模式获利。比如去年，CryptoWall病毒家族一个变种就收到23亿赎金，近几年苹果电脑、安卓和iPhone手机也出现过不同类型的勒索病毒。

虽然下黑手者目前还找不到，但其所用的工具，却明确无误地指向了一个机构——NSA（National Security Agency），美国国家安全局。这一机构又称国家保密局，隶属于美国国防部，是美国政府机构中最大的情报部门，专门负责收集和分析外国及本国通讯资料。黑客所使用的“永恒之蓝”，就是NSA针对微软MS17-010漏洞所开发的网络武器。

事情是这样的：NSA本身手里握有大量开发好的网络武器，但在2013年6月，“永恒之蓝”等十几个武器被黑客组织“影子经纪人”（ShadowBreakers）窃取。

今年3月，微软已经放出针对这一漏洞的补丁，但是一是由于一些用户没有及时打补丁的习惯，二是全球仍然有许多用户在使用已经停止更新服务的WindowsXP等较低版本，无法获取补丁，因此在全球造成大范围传播。加上“蠕虫”不断扫描的特点，很容易便在国际互联网和校园、企业、政府机构的内网不间断进行重复感染。

又一个问题来了：NSA为什么会知道微软的漏洞，并且制作了专门的网络武器，然后这些武器中的一部分还落到了黑客的手里？
实事求是地说，作为操作系统之一，Windows的构成动辄几亿行代码，之间的逻辑关系不可能一个人说了算，因此出现漏洞是很难消除的。而Windows又是世界上使用最普遍的操作系统，因此被黑客看中而研究漏洞并攻击获利，是很“正常”的事情。

但作为美国国家安全局，盯着这个系统的漏洞也就罢了，还专门搞武器，这是什么道理？

事实上，在黑客组织曝光这一漏洞之前，微软自己也不知道漏洞存在。也就是说，只有NSA知道漏洞存在，至于知道了多久，也只有他们自己知道。在的网络安全专家看来，很可能的情况是，NSA早就知道这个漏洞、并且利用这一漏洞很久了，只不过这次被犯罪团队使用了，才造成如此大的危害。从这一点我们可以看出，美国的技术确实很强，在网络安全领域独步全球；同时，“漏洞”已经成为兵家必争的宝贵战略资源。

换言之，通过网络对现实发起攻击，已经不是科幻电影的场景专利，而是已经发生的现实。不信的话，给大家讲一个真实的故事——
斯诺登，披露美国政府对全球实施监控的“棱镜计划”的那位，就是NSA的前雇员。他证实的一则消息是，2009年，奥巴马政府曾下令使用网络攻击武器——代号“震网”的病毒，攻击了伊朗的核设施。其中原因复杂，简单说就是以色列设法通过马来西亚的软件公司，让伊朗购入了夹带着一病毒的离心机控制软件；2010年，病毒爆发，控制并破坏伊朗核设施的离心机如那件，最终造成1000余台离心机永久性物理损坏，不得不暂停浓缩铀的进程。

这也是史上首次通过虚拟空间对现实世界实施攻击破坏的案例，达到了以往只有通过实地军事行动才能实现的效果。而在去年，乌克兰的电网系统也曾遭到黑客攻击，导致数百户家庭供电中断。

NSA现在手中握有多少网络武器，当然是美国的机密。但根据维基解密的说法，不仅NSA手里有，CIA手里也有，他们的网络情报中心创造了超过1000种电脑病毒和黑客系统——这还是斯诺登2013年确认的数量。

微信咨询：85054458

长按二维码直接识别关注

专注云计算、虚拟化与信息安全的独立自媒体

河北华信逸腾科技有限公司是河北省领先的虚拟化和云计算解决方案咨询与服务提供商，河北省唯一一家Vmware企业级合作伙伴。公司成立于2004 年，一直专注于虚拟化数据中心建设、云平台建设与信息安全领域。公司有具国家信息安全服务一级、河北省政府信息安全应急响应支撑单位等资质，是河北首家全方位为客户提供信息安全解决方案、产品、服务、咨询、评估与认证的服务性企业。

阅读原文