WannaCry勒索病毒与朝鲜的神秘联系

原创 2017-05-18 哈拿 煎蛋

credit: 123RF

卡巴斯基安全实验室的研究员发布了一项最新证据，显示WannaCry勒索病毒的代码与朝鲜有一定的联系。实验室团队早前公布了一段代码的细节，显示这段代码除了出现在WannaCry的早期变体里，还曾经出现在黑客团体“拉撒路组织”(Lazarus Group)在2015年2月发布的病毒的样本里。而这个团体曾被卡巴斯基研究员追踪到跟朝鲜政府有关。谷歌的研究人员尼尔-莫他(Neal Mehta)也曾经宣布发现WannaCry和朝鲜政府的关系。卡巴斯基方面认为，这两处相似的样本并不仅仅只是共享代码的结果。

“我们可以很肯定地认为， 5月11日爆发的WannaCry勒索病毒，跟2015年2月的病毒样本是出自同一组人的手笔，”卡巴斯基的公告里写到：“或者说拥有同样的源代码权限。”

另一家网络安全公司赛门铁克(Symantec)也发现了类似的证据，不过这家公司认为光凭这些证据还很难弄清楚这些相同代码背后的真正意义。这家公司认为：“就现存的证据而言，只能表示它们之间(病毒和朝鲜政府)某种薄弱的联系。我们还将继续调查更加强有力的证据。”

就某种程度而言，我们确实很难去了解是什么原因造成这两端代码的相似。WannaCry的攻击行为体现了典型的勒索犯罪病毒特征。因此在更有力的证据被发现之前，我们没

有理由认为它是被某个国家政府操控的。这种对早期代码的分析只是一种必需的推测。同样的，WannaCry的制造者从朝鲜病毒的样本中提取相应代码的推测也并非不可能，鉴于他们就利用过美国国家安全局(NSA)开发的漏洞程序“永恒之蓝(EternalBlue)”里的代码。就算证实卡巴斯基的假设是正确的，这也可能是数据泄漏的结果，而非政府操作。

但是仍然，这一令人充满好奇的证据，可能最终将会揭示这场前所未有的病毒危机的谜底。如果证实WannaCry和朝鲜之间确实存在什么联系，那么这网络攻击的因由可能超乎所有人预料之外。

阅读原文