赛门铁克：WannaCry勒索软件与朝鲜相关黑客组织有很强关联

2017-05-24 Dow Jones 道琼斯风险合规

图片来源：ritchie b. tongo/European Pressphoto Agency

WannaCry勒索软件攻击最终感染了超过100个国家的逾20万部电脑。

一名网络安全研究员称，本月爆发的全球勒索软件攻击事件背后的主谋很有可能是与朝鲜有关的一个组织，而且此次攻击更像是犯罪团伙所为而不是政府策划的行动。

网络安全公司赛门铁克(Symantec Corp., SYMC)在周一晚间发布的博客中称，WannaCry勒索软件与Lazarus有很强的关联，一个安全专家小组怀疑后者是去年孟加拉国央行8,100万美元被窃案以及2014年索尼影视娱乐(Sony Pictures Entertainment)被黑客攻击事件的背后主使。美国官员曾表示，他们认为朝鲜策划了针对索尼的攻击，联邦检察机关目前正在立案，可能指控朝鲜政府参与了孟加拉国央行被劫案。

包括Alphabet Inc.旗下的谷歌(Google)子公司、卡巴斯基实验室(Kaspersky Lab ZAO)和Comae Technologies在内的网络安全研究人员此前指出，WannaCry的一个变种与过去Lazarus袭击案中所使用的代码存在相似之处。但这些初步报告非常谨慎，没有对这些数字线索与Lazarus或朝鲜之间的关系得出更深层次的结论。

外界对于Lazarus知之甚少，但网络安全研究人士称，该组织自2009年以来一直很活跃。最初该组织主要在亚洲活动，但现在已经开始把目标瞄准全球银行。

赛门铁克最新分析显示，Lazarus此前网络攻击与WannaCry的工具和技术以及此次攻击中使用的网络基础设施之间存在很大的相同之处。赛门铁克称，由此看来，Lazarus很可能就是WannaCry扩散的幕后黑手。在本月冲击全球电脑网络的大范围攻击爆发前，2月、3月和4月份曾出现过一系列使用WannaCry软件的小规模攻击。

赛门铁克没有提及朝鲜是否直接参与了这起最新的WannaCry攻击。网络安全专家已表示，其他黑客也可能复制了相关代码，这意味该恶意软件也可能来自其他组织，而不一定是Lazarus。但这些专家称，即便Lazarus是罪魁祸首，该组织利用该恶意软件发动攻击也可能并非是获得了朝鲜政府的授命。目前尚不清楚谁在掌管Lazarus，也不清楚该组织的资金来源。

朝鲜官方媒体上周一否认该国政府与WannaCry攻击有关，并将韩国多篇暗示朝鲜参与此次攻击的媒体报道斥为不实报道和肮脏卑劣的诽谤。

Timothy W. Martin

内容转载自公众号

WSJ金融市场 了解更多

阅读原文