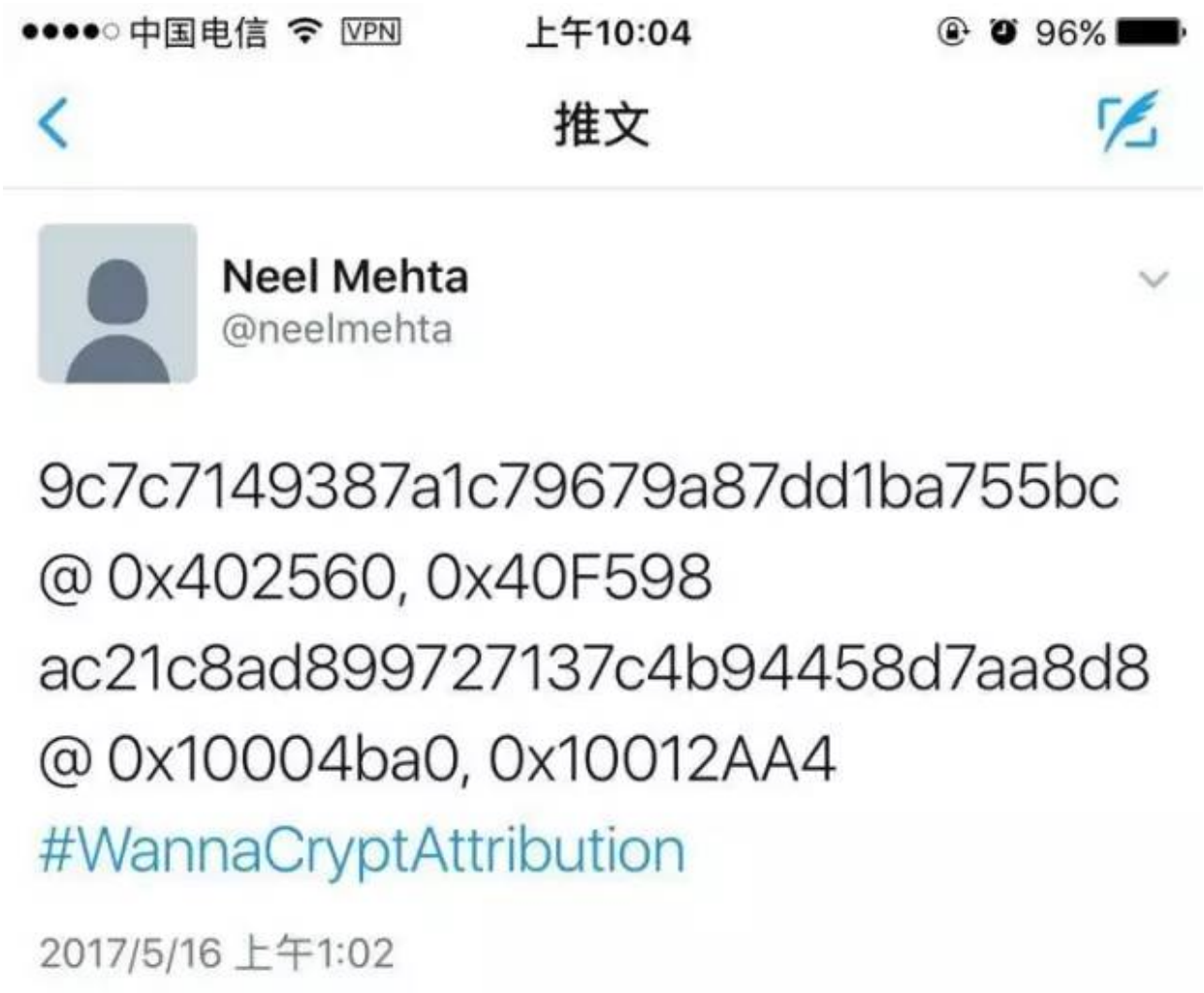
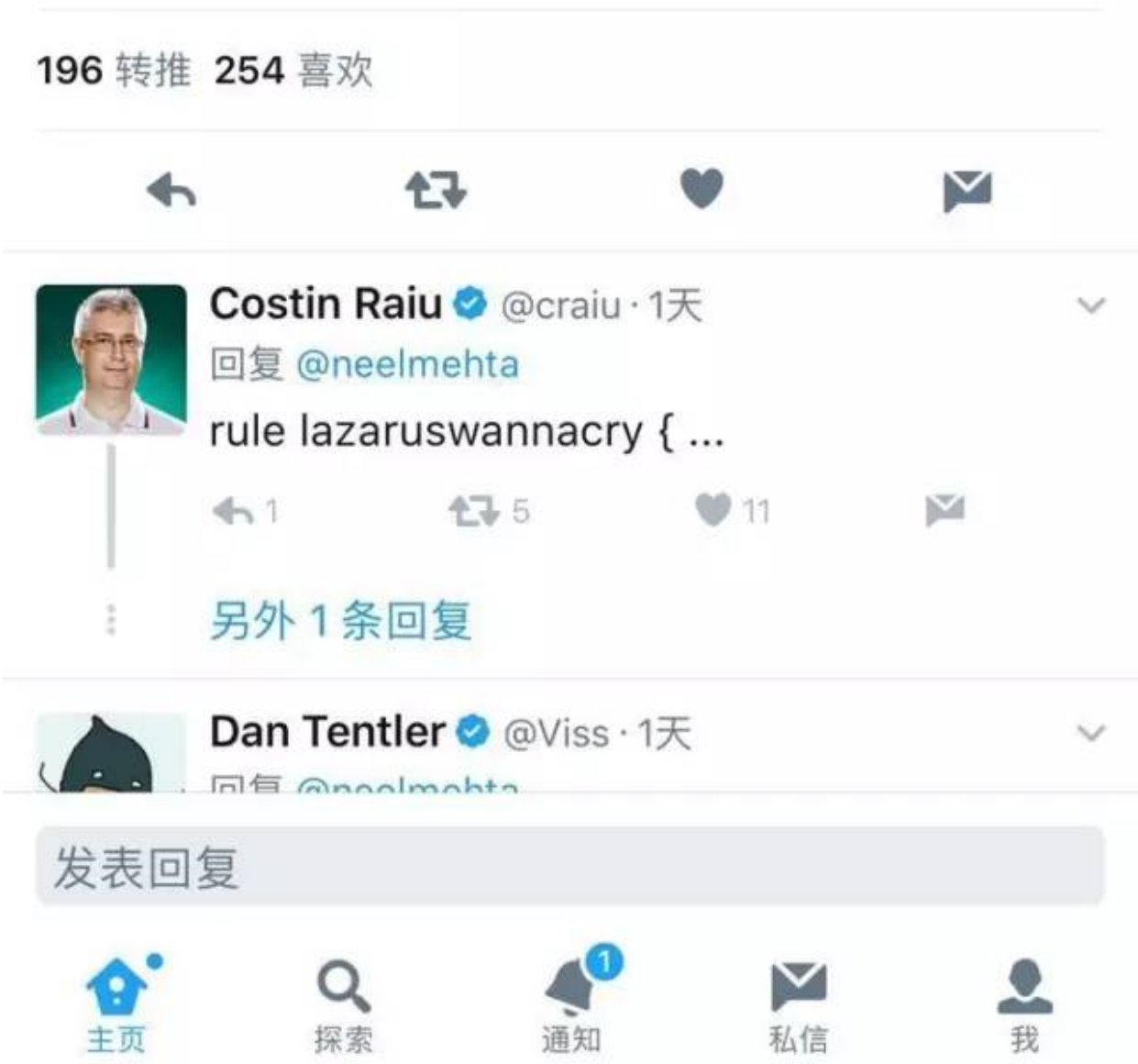
WannaCry源头的蛛丝马迹惊现！什么意思呢？

2017-05-17 Softnext守内安

在信息安全社群的多位专家已将WannaCry勒索软件与Lazarus组织关联起来，什么意思呢？

Google的信息安全研究员Neel Mehta用了#WannaCryptAttribution的hashtag发布了一则神秘的推文。他是什么意思呢？





根据卡巴斯基的专家介绍：

> 该字符串是Neel在2017年2月发现的WannaCry勒索软件的早期版本中注意到的程序代码的一部份，以及恶名昭彰的Lazarus APT组织在2015年2月以前使用的恶意软件之一。

这是什么意思呢？

Lazarus组织的活动在2014年和2015年激增，其成员大多采用自行开发的恶意软件进行攻击，对其成员进行了调查之后发现其复杂度高。

这个威胁实体至少在2009年以来一直活跃起来，可能早在2007年就参加了网络间谍活动与破坏性的活动，旨在破坏数据与系统。

Symantec的专家曾经发现：

> 该组织使用至少三种恶意软件，集Backdoor.Fimlis, Backdoor.Fimlis.B与Backdoor.Contopee，这些恶意软件已被用于对金融机构的针对性攻击。

攻击者利用『水坑式』攻击，以感染具有以前未知恶意软件的特定受害机器。

研究人员推测，该组织可能就是最新一波对全球银行攻击、Sony遭骇事件、黑暗首尔行动的罪魁祸首。

WannaCry背后的攻击者有可能打着这个虚假的旗帜吗？

卡巴斯基的专家认为，打着虚假旗帜的说法是不可能的，因为共享程序代码的部分只出现在WannaCry的早期版本中，但稍后被删除了。

Kaspersky实验室分享的最新文章：

> 现在，WannaCry的旧版本需要更多的研究。我们相信这可能是解决环绕着这次攻击的一些奥秘的关键。有一件事是肯定的 - Nell Mehta的发现是关于WannaCry起源的最重要的线索。

问题是：
在2月初WannaCry变种和最近的大规模网络攻击中使用的样本之间是否有关联？

根据Kaspersky的答案是『是的』。最近的变种能够针对更多的文件扩展名目标进行加密。

Kaspersky表示：

> 我们坚信，2017年2月的样本是由同一个人编译的，或者是获得与5月11日赵波攻击中使用的2017年5月的WannaCry加密程序的程序代码相同的人。

Kaspersky分享了用于找出WannaCry样本的YARA rule。

让我更进一步的从Comae的Matthieu Suiche分享的分析：『**Lazarus组织的归属对于他们的叙述是有意义的，过去这些叙述主要是渗透金融机构的目的是偷钱。**』

如果这个验证是对的，这意味着WannaCry的最新迭代实际上将成为第一个国家级发动的勒索软件。

这也意味着一个外国敌对国家将利用方程式组织失去的主动进攻能力来创造全世界的混乱。

在这个时间，野外又出现了第三个『杀手锏』开关 ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf.com - 它包含的事实『lmao』意味着 laugh my ass off (外国常用缩写词lmao，意指笑到不行，超爆笑)，如果上述的归纳是真的，那攻击者是故意在传达多种信息：

- 被翻译为『继续尝试』向执法与信息安全研究员社群发出的全球挑衅信息；
- 最近发生的WannaCry是实作政治混乱破坏性操作的理论

另外，

WannaCry的攻击者与恶名昭彰的Lazarus黑客集团有很大的关联，而Lazarus亦与北韩政府关系匪浅。

新证据是由Google研究员Neel Mehta率先公布，他在个人Twitter账号公布了两段字符串，但没做任何说明。随后卡巴斯基实验室研究总监Costin Raiu与Comae创办人Matt

Suiche证实，这两段字符串分别取自2017年2月份早期的WannaCry勒索蠕虫程序，以及2015年2月份的Contopee后门程序的片段，这两段程序代码几乎相同，而经调查Contopee后门程序为Lazarus黑客集团所为。

(两个程序有着两段几乎一模一样的程序代码)

然而根据程序代码类似就能判定WannaCry的幕后藏镜人是Lazarus吗？说不定是有心人士复制Contopee的代码段，以嫁祸给Lazarus。

卡巴斯基实验室指出：

> 确实有这种可能，然而比对目前流行的5月份的WannaCry程序代码，却没发现这段从2月份版本发现的程序代码，可合理推测攻击者在2月开始测试攻击程序时仍使用Contopee旧的程序代码，而在5月真正发动攻击时才删掉与Contopee相关的程序代码，由此行径可高度怀疑WannaCry与Lazarus有相当的关系，若非是Lazarus黑客集团发动攻击，就是有办法取得Lazarus程序代码的组织。

But, anyway....

p民冒着生命危险发布这消息， 真担心会被三月半暗杀。。。

But, anyway & anyway...

补丁更新还是时刻要装的，世界上像微软这样的良心企业还是不少的，比如我们——Softnext守内安（害羞.gif）,毕竟信息安全事业需要的不仅是国家的关注，更需要我们人民的关注，与意识的不断提高！

阅读原文