关于 “魔窟”（WannaCry）勒索蠕虫变种情况的进一步分析

安天安全研究与应急处理中心（安天 CERT）

报告初稿完成时间：2017 年 05 月 15 日 19 时

首次发布时间：2017 年 05 月 15 日 19 时

一、 有关“新样本变种”的说法来源

5 月 13 日，来自英国的 “MalwareTech”发现“魔窟”（WannaCry）预留了一个中止条件，即蠕虫运行时如果能访问到“开关域名”（也有部分机构称之为灭活域名）www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com 则会退出程序，文件也不会被加密；如果访问“开关域名”失败则执行加密用户文件等恶意行为，而该域名当时并未被注册，因此“MalwareTech”注册了这一域名来阻断这一恶意代码传播。5 月 14 日，网上开始流传该蠕虫已经出现“WannaCry 2.0”版本的消息，“开关域名”机制已经失效的信息。但从当时的信息来看，这一信息实施上在当时是国内媒体是对卡巴误发布信息以讹传讹。

5 月 13 日，卡巴斯基 Costin Raiu 在推特上发出消息（该已经于 13 日中午删除），认为存在所谓无“开关域名”的样本。

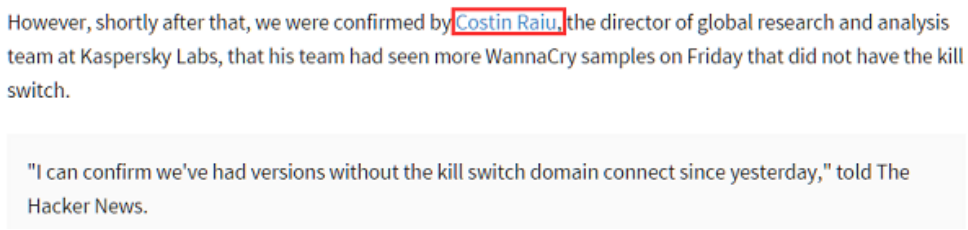

图 1 卡巴斯基发出“发现无域名开关的样本”的错误消息

5 月 14 日，卡巴已经澄清了相关消息，承认当时并未发现无“开关域名”的样本：

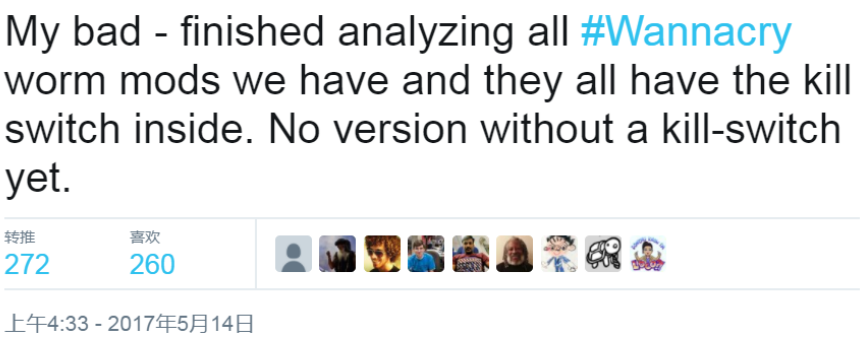

图 2 卡巴斯基承认误判，暂未发现“无域名开关的样本”

截止到此时，应该说这是一起乌龙事件。但以上消息经过进一步转发，开始产生了很多错误解读和谣传：如有分析团队将样本母体释放的**勒索程序本身**误解读为无“域名开关”的母体样本，声称这就是该蠕虫的 2.0 版本。

实际上，该病毒确实有两个版本，其 1.0 版本最早于 3 月 29 日被安天捕获，其并无主动传播模块，是一个不同的勒索恶意代码，但并非一个蠕虫，也不受开关域名的约束，而此时 NSA“永恒之蓝”相关漏洞利用工具也尚未泄露。其 2.0 版本就是在 2017 年 5 月 12 日大规模爆发并被各安全厂商所分析的版本。安天此前分析已经指出，“魔窟”蠕虫，分成传播框架和释放出来的加密模块。其中传播框架受到开关域名的约束，但而其加密模块与此前的 1.0 版本基本一致，自身不具备主动传播的属性，其内部均未设置开关域名条件（可以参见此前安天分析报告的样本集合列表说明）。安天认为，不能判断 1.0 版本和 2.0 版本是否来自同一个攻击者，因为 2.0 版本攻击者有可能选择一个已有的勒索软件进行二进制加工，达到其自身目的。

同时由于该开关域名，在样本中以明文存在，加之该病毒并没有使用更多加密混淆手段，因此无论修改该域名，还是修改跳过该机制都是比较容易的因此在《勒索蠕虫“魔窟（WannaCry）”FAQ 之三》中安天工程师指出，**“我们必须冷静的看到，攻击者可以非常容易的将目前的蠕虫修改为开关域名无效的版本，或者修改为其他的开关域名条件。而其他攻击者，即使没有源码，也只需要修改几个字节的二进制就会导致开关域名的失效。”**

当时安天在样本检索中，找到两个开关域名被修改的病毒版本，安天在上述文档中公布了其修改过的域名“截止到 2017 年 5 月 14 日 22:00，并未出现所谓开关域名失效的版本。但通过样本交换通道发现有其他开关域名被篡改的版本”

但在后续样本检索中，安天分析小组发现自己漏过了一个样本，该样本的开关域名被清零。为此我们就这一问题做出进一步说明。

二、 当前捕获样本情况

当前，除了两个带有新的“开关域名”的版本外，确实已经存在一个 “开关域名”被“抹去”的样本。经过分析我们确认，这 3 个样本是从最早出现的该蠕虫的 2.0 版本的 3 个母体文件其中的两个修改而来，截止发稿前目前除这三个样本外，还未发现其他修改的样本文件。但由于相关修改比较容易，不排除会迅速产生新的样本。

原始母体两个文件详情如下：

MD5	文件大小	最早出现时间	出现次数
F107A717F76F4F910AE9CB4DC5290594	3,723,264 bytes	2017-05-12 09:57:51	11
DB349B97C37D22F5EA1D1841E3C89EB4	3,723,264 bytes	2017-05-12 09:57:51	73

表格 1 原始母体样本最早发现时间

而已经出现的 3 个“开关域名”条件，出现变化的版本，在知名多引擎扫描站点的 Virustotal 的情况如下：

MD5	文件大小	最早出现时间	出现次数
80CE983D22C6213F35867053BEC1C293	3,723,264 bytes	2017-05-14 10:42:29	4
D724D8CC6420F06E8A48752F0DA11C66	3,723,264 bytes	2017-05-14 13:05:36	6
D5DCD28612F4D6FFCA0CFEAEFD606BCF	3,723,264 bytes	2017-05-14 12:03:51	6

表格 2 三个通过原始母体修改的样本

三、 被修改的样本的修改内容和特点：

1. 修改了“开关域名”的样本，只是在原有两个样本基础上修改了域名处的两字节，将域名中的字符“uq”改为“ff”，其他部分未修改。

   原域名：www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

   新域名：www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

2. 抹去“域名开关”的样本是在原有样本上将域名字符串全部替换为|00|，其他部分未修改，显然这个版本并非来自修改代码重新编译，而来自于直接在样本上进行的二进制修改。
3. 由于样本 1 中资源节的勒索程序打包错误，导致勒索程序不能运行，因此样本 1 和通过样本 1 修改的样本只会通过漏洞进行传播，但不会对计算机内的数据进行加密操，也不会弹出勒索窗体。

   需要指出的是，这种简单的二进制字符串资源修改，不会导致新样本绕过杀毒软件检测，因为对杀毒软件来说，病毒的特征码，不会选择在易于修改的字符串上。

原始样本文件 MD5	是否有加密行为	新发现的对应样本 MD5	修改点
F107A717F76F4F910AE9CB4DC5290594（样本 1）	否	80CE983D22C6213F35867053BEC1C293（样本 1A）	新域名
		D724D8CC6420F06E8A48752F0DA11C66（样本 1B）	抹去域名开关，强制触发
DB349B97C37D22F5EA1D1841E3C89EB4（样本 2）	是	D5DCD28612F4D6FFCA0CFEAEFD606BCF（样本 2A）	新域名

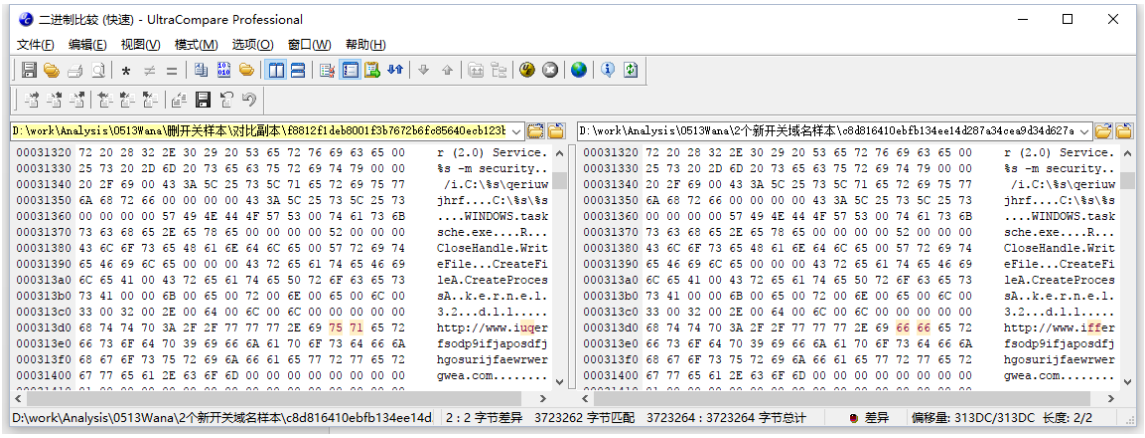

图 3 样本 1（左）与样本 1A（右，新域名）对比

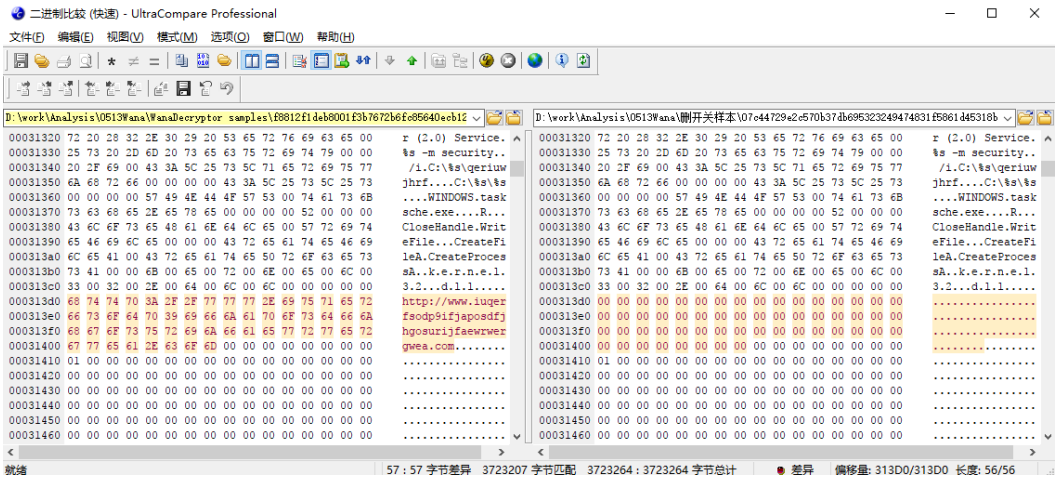

图 4 样本 1（左）与样本 1B（右，删除域名的样本）对比

新修改的样本不仅删除了域名，还修改跳转，强制执行恶意行为，不过由于原母体文件的勒索文件就是错误的，因此新修改的样本只能传播，不会进行勒索行为。

图 5 删除域名的样本修改跳转强制执行恶意行为

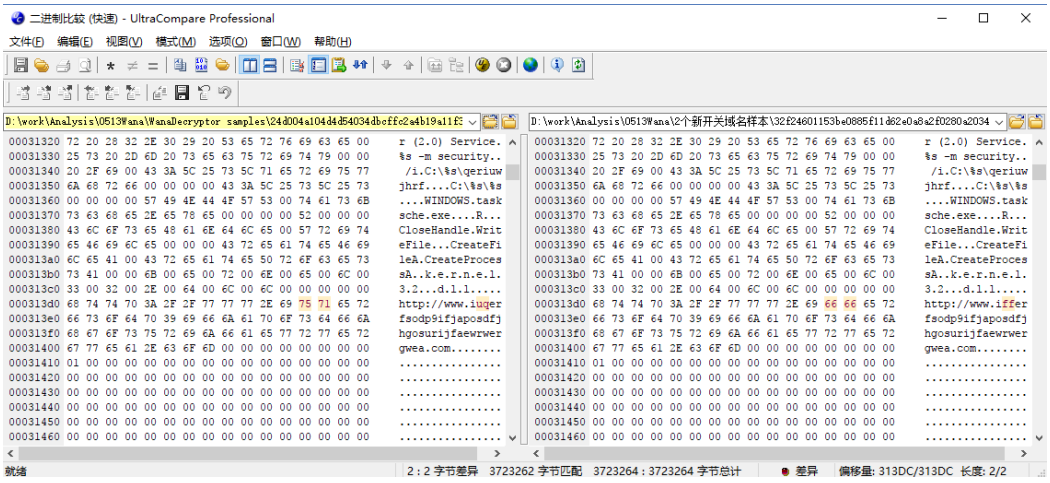

图 6 样本 2 与样本 2A（新域名样本）对比

四、 小结

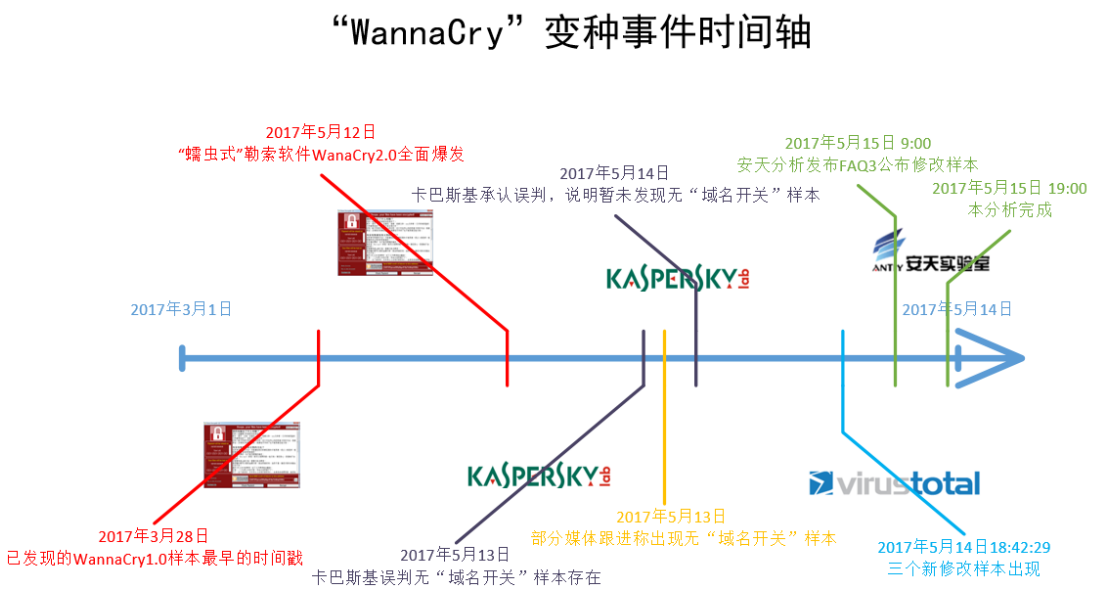

图 7“WannaCry”变种事件时间轴

安天就在分析中出现的样本遗漏表示歉意，但安天依然严肃的指出，这不能改变国内最早对新变种出现的报道是对卡巴误判信息以讹传讹的事实。在安全威胁的瞬息万变的情况下，确实会出现恐慌和误判导致传言；但传言后来又会一语成谶的情况，但网络安全永远需要的是严谨和实证。

同时我们需要注意，抹掉开关域名的样本，原则上不受当前开关灭活机制的控制，应该有更大的传播面积（但事实上，业内并未监控到其大面积传播）。修改者选择了一个实际不能完成加密勒索的版本来修改，这是巧合还是偶然，是值得思考的。修订者究竟是希望造成更大面积的传播，还是因其他原因修改样本，甚至只是为了证明这个样本的存在，目前还很难判断动机。同时，我们也需要思考和警惕的是,正如我们在安天 2016 基础威胁年报中所指出的那样，“威胁情报也是情报威胁”。类似 Virustotal 多引擎扫描等威胁情报来源，构成了能够精准分发“样本”到全球所有主要安全厂商的通道，他们即是重要的威胁来源，但也是一个信息干扰与反干扰的斗争舞台。

从另一个角度来看，威胁的快速变化演进证明了，我们在此前文档中已经指出的 **“显然，将这一蠕虫的响应，完全寄托在攻击者预留的这个彩蛋和四两拨千斤式的开关域名条件建立上，是不可靠的。”**