PR的盛宴之下，不能缺席的是技术的纯真——WannaCry事件之反思

茶码古刀 / 2017-06-01 15:20:46 / 浏览数 3241 安全技术 技术讨论 顶(0) 踩(0)

作者：小刀
公众号：wxcmgd

（2017-06-01晚进行少量修订和更新，发于阿里云先知技术社区）

楔子：

教授说：西雅图也开始下雨了……

今天是5月的最后一天，大家对WannaCry关注的热情怕是渐已退却。而对于一名技术人员，这个时候倒很适合来对WannaCry勒索蠕虫事件进行一次不那么严肃的反思。

5月之于安全圈，WannaCry毫无疑问是占据头条最长的事件。今天，小刀把自5月12日起国内有关WannaCry相关的报道、报告等全部理了一遍，内容可以说是"浩如烟海"

反思1：对于广为流传的事，不能迷信，不可无视。

在整个事件发展过程中，关于WannaCry的部分技术细节经常会让有心人产生疑问，当然，随着国内外安全研究人员和组织的不断努力，很多疑问也都逐渐有了确定的答案。

当时群里的热烈讨论

小刀印象比较深的是类似下图中COS给圈友们出的题2，当时这个问题很多人在不同场合讨论。

因为当时是在新闻宣传潮之后，刚刚开始进入技术分析环节。根据当时能看到的少数技术报告，勒索软件会将密钥传到云端，等支付了赎金再通过云端下发密钥进行解密（事

如果迷信了当时的技术报告中所提到的信息，那么对于这个问题就会难以解释。

在13日的一次非正式技术讨论中，盘古CEO
TB和微步CEO薛锋都指出了技术上的可行性——黑客手中只要掌握核心私钥，然后把核心公钥内置在蠕虫中，对于每台机器生成的密钥，可以用核心公钥加密起来存放在本

这是一个不迷信的例子，大牛们通过自己客观而理性的分析，解答了一个疑问，并且后续的详细技术报告证明了其正确性。

另外一个例子是关于"kill swith"（蠕虫启动时，会访问一个不存在的域名：http://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
如果能够访问该域名的80端口，则立即退出程序，什么都不做）。当时比较主流的观点认为，这是WannaCry作者给自己留的一个开关，在必要的时候，可以阻止蠕虫继续

事实上，技术人员可以换个角度思考——黑客怎么会把"自己可能会用到的域名"留给别人去注册呢？——如果这是黑客留给自己的开关，那么他应该注册下来暂不解析。而

而微步CEO薛锋则较早指出，这应该是一个对抗沙箱的行为——因为大部分沙箱，对于沙箱中的程序请求任何域名，都会给予响应，这是为了尽量保证恶意软件的正常运行

看了微步薛的分析，小刀深以为然，否则还以为这个黑客是为了保护特定的小群体呢。

当然，在这个问题上，还有很多细节值得推敲（盘古CEO TB也对这一观点的细节进行了多轮质疑），比如：

1、
为什么蠕虫选择判断"是否能访问80端口"，而不选择"能否解析域名"或"看80端口返回内容是否匹配"呢？（小刀的理解：这个蠕虫作者有很多折衷的考虑，比如他的部分代码

2、为什么蠕虫做完简单的沙箱对抗检测之后，仅仅是退出，而不进行自毁呢？（小刀的理解：他主要考虑的是不要让自动沙箱很轻松注意到它的恶意行为，而对于专业人员

3、 ……

这是另外一个不迷信的例子，告诉我们应该时刻保持着专业人士的专业素养，这可能是来源于自己的经验，也可能是出于自己的换位思考和不断质疑、不放过任何一个细节的

反思2：在不迷信的基础上，技术人员还要不厌其烦地认真求证。

在这一部分，小刀想说一下关于Windows XP能否被WannaCry感染的疑问，继续借用一下COS朋友圈的截图吧：

小刀在连篇累牍的报道中，似乎没有看到哪篇文章提到WannaCry感染Windows
XP存在疑问？——希望是我看到的文章还不够多，但也可以肯定我们主流的声音中缺乏对这种技术细节问题的及时关注、严密考证和客观阐述。

那么，这个问题是从何而来呢？我们从所有的报道中、报告中不都是在说Windows
XP会受影响吗？微软不是破例为XP和2003发布了漏洞补丁吗？各种指南不都在说XP应该怎么做吗？不是还有针对XP的文件恢复工具吗？……

是的，第一次看到这个问题，小刀也很诧异：WannaCry用了EternalBlue的攻击代码，EternalBlue利用的是MS07-010漏洞，只要这个漏洞能影响到的系统，就会成为感染

□

网上流传的"WannaCry幸存者参考"

事实上，反思之下还是能够发现，这个逻辑犯了常见的逻辑错误：MS07-010能够影响Windows XP和EternalBlue能够攻击Windows XP，只能说明“如果作者原意，WannaCry可以感染Windows XP”，但并不能证明“事实上WannaCry可以感染Windows XP”。

同时，可能也是迷信了广为传播的说法。

在国外，有几位安全研究人员提出并讨论了这个问题，其中最有代表性的是安全架构师Kevin Beaumont（https://twitter.com/GossiTheDog）的观点，他明确指出——WannaCry并不会感染Windows XP（和2003），并且也得到了一些安全企业的回应。

好吧，看来我们需要从技术上验证一下，虽然这个工作其实还挺繁琐的。

首先我们要确认一下，EternalBlue能不能攻击Windows XP？

小刀先用Eternalblue-2.2.0.exe（MD5：8c80dd97c37525927c1e549cb59bcbf3）进行了测试，发现无论从XP打XP还是从Win7x86打XP，都是失败的。

而从XP打Win7x86，和从Win7x86打Win7x86都是成功的。

当然仅仅做这样小范围的测试还不够。于是小刀在网上查阅了一些资料：

在一位日本同仁Neutral8□9eR（https://twitter.com/0x009AD6_810）的推特上看到，他用MSF做了测试：

□

未打补丁，攻击成功

□

打了补丁，攻击失败

不光有截图，还有视频。

这个测试，他用的是hardw00t开发的MSF插件（https://github.com/hardw00t/Eternalblue-Doublepulsar-Metasploit）。

我看了一下代码，的确是支持XP的：

而另外一个广为流传的MSF插件则据称尚不支持XP：

所以，基本上可以判断：EternalBlue肯定是可以攻击XP的，只不过在利用层面不同的工具表现可能不同，也可能在不同环境下利用的稳定性存在不一致的情况。

接下来看WannaCry。

测试方法比较暴力：开启4台虚拟机组成一个局域网，2台Windows XP SP3、2台Windows 7 x86。分别在XP-A和Win7-A上测试运行WannaCry原始样本（就是带传播功能的版本，我用的是MD5为db349b97c37d22f5ea1d1841e3c89eb4的这个），看局域网内其

直接贴我的测试结果：

1、 在XP-A（左上）上运行：XP-B没动静（右上）；Win7-A和Win7-B受攻击（但是蓝屏了）

2、 在Win7-A（左下）上运行：Win7-B受感染（右下）；XP-A和XP-B没动静

有（Tai）兴（Wu）趣（Liao）的同学可以看看动画（上面两台是XP，下面两台是Win7）：

GIF1：从XP-A上投放：wcry1_win7a_4m

GIF1：从Win7-A上投放：wcry1_winxpa_4m

其它发现：

在XP上运行WannaCry的时候，可能会无法在内网传播，只往公网随机IP传播，看上去像是故意避开了本地内网IP地址（通过netstat看445连接）。而在Win7上却一切正常

□

进一步思考：如果WannaCry真的不能感染XP，在XP上手工运行也不能正常攻击Win7，在XP上不能正常攻击本地网络，加上WannaCry的本地化勒索信息的显示也根本没有

□

□ XP中文版上的勒索信

□

Win7中文版上的勒索信

测试做完后，同样也查阅了各种信息，发现之前那个日本小哥也是非常认真地做了一遍测试，比小刀全面多了（不过结果不太一样）：

第一组：干净的机器

左上：蠕虫初始投放机器（Win7）；右上：WinXP SP3

左下：Win7；右下：Win2008 R2

□

初始状态

□

XP和Win7被打蓝屏了

□

2008中招

第二组：提前感染DoublePulsar的机器

左上：蠕虫初始投放机器（Win7）；右上：WinXP SP3

左下：Win7；右下：Win2008 R2

□

感染好DoublePulsar

□

Win7和2008沦陷（XP没事）

小刀觉得，并不是没有人注意到这个问题，也不是没有人研究这个问题，只是没人讨论，因此有点困惑。

当然，不管如何，微软已经针对XP和2003发布了补丁，还在使用这些系统的小伙伴，还是要打好补丁、做好系统加固工作。

反思3：希望国内安全研究者（机构）能够建立“重大安全事件联合攻关机制”。

用WannaCry蠕虫研究过程中最重要的一环——文件恢复或者解密——来谈这个问题吧。

这个问题很显然包括两个点：

一是无密钥的情况——文件恢复的问题。

这个已有各路英雄提供了很多方法，比如360较早发布的直接“找回已删除文件”的方法和工具；比如四川效率源公司较早发布的不同大小文件的不同加密方式（1.5MB）及可

这里有一个细节，当时并没有看到相关报告，那就是WannaCry对于某些文件，会先做随机填充后再删除，而不是直接删除。

例如下图中的“Blue hills.jpg ”文件，是原始文件，在Windows Explorer中是可以看到预览的缩略图的，同时蠕虫已经开始加密了（旁边有个.WNCRYT文件）：

□

而蠕虫完成加密后，将.WNCRYT重命名为.WNCRY文件，但是，仔细观察会发现“Blue hills.jpg
”文件已经无法预览了，这是因为这个文件已经被蠕虫修改，格式上已经不是合法的JPG文件了：

随后，蠕虫会移动并删除这个文件。很显然，这个文件，通过磁盘恢复的方式，就不能恢复了。（今天整理的时候看到360的报告中已经对这个问题进行了详细的阐述。）

二是“如何找到密钥”的问题。

为了便于讨论，小刀把WannaCry的密钥分为3类：文件密钥（加密文件的AES对称密钥，每个文件不同）、关键密钥（用于加密文件密钥的RSA非对称密钥，每台机器每次

因为国外研究者较早就复原了加密和解密流程，只要能拿到上述任何一种密钥，就可以解密文件——最彻底的就是拿到黑客手上的核心密钥私钥，那就可以拯救世界了；其

这里用到的解密工具是Benjamin Delpy开发的wanadecrypt。

作为研究，第一步当然是到内存里面去找找看，看它密钥在内存中什么时候生成、什么时候销毁（工具作者也说了）：

通过对微软的相关API下断点的方法可以找到密钥（比如CryptExportKey、CryptEncrypt什么的），当然，你还要对RSA的密钥格式有一点了解（在本例中是“07
02 00 00 00 A4 00 00”开头的16进制数据，总长度为1172字节）。

但是这个密钥在内存中存活的时间窗太短了，还有什么办法呢？

因为RSA密钥生成，是要用到素数的，如果能找到素数，也就有路可走了。当然这需要对密码学相关知识和微软的API原理更加熟悉才行。——小刀忍不住又要佩服那帮老外
Guinet提出：由于微软Windows CryptAPI中，CryptReleaseContext()并没有清除素数(prime numbers)，可以通过扫描WannaCry

进程的内存空间来找到相关素数，再恢复RSA私钥。同时完成了工具wannakey的开发，并开放源代码（https://github.com/aguinet/wannakey）。而Benjamin Delpy基于上述研究成果，开发了wanakiwi工具，可以自动扫描WannaCry 进程的内存空间来找到相关素数，再恢复RSA私钥，并完成解密工作。

这样，这个"可能找到关键密钥"的时间窗就要长很多了（直到相关内存空间被覆盖）。

为什么提到"重大安全事件联合攻关机制"呢？首先是因为可以用于研究的时间非常有限，每个研究人员、研究机构都在加班、熬夜，如果不能形成一定的共享，则很有可能大

比如，在当前研究进展下，还有没有什么方法可以在"寻找关键密钥"的道路上更进一步呢？

Benjamin Delpy在发布wanadecrypt 0.0版本的时候，写了一句话：

It's only a little help on the road to have maybe a version that can get the key at one point...

小刀认为，这句话非常好地描述了他从事这项研究工作的心态，也非常值得我们学习。

技术人员当勤于思考、勇于提问、敢于质疑，不放过每一个技术细节、不厌其烦地谨慎求证、不断朝着目标一步一步前进。

在重大的安全事件面前，我们应该放下品牌，抛弃成见，开放心态，精诚合作。

注：由于水平有限，文中难免出错，请大家多多海涵并严肃指正！

这样，这个"可能找到关键密钥"的时间窗就要长很多了。

为什么提到"重大安全事件联合攻关机制"呢？首先是因为可以用于研究的时间非常有限，每个研究人员、研究机构都在加班、熬夜，如果不能形成一定的共享，则很有可能大

Benjamin Delpy在发布wanadecrypt 0.0版本的时候，写了一句话：

It's only a little help on the road to have maybe a version that can get the key at one point...

小刀认为，这句话非常好地描述了他从事这项研究工作的心态，也非常值得我们学习。

在重大的安全事件面前，我们必须要放下品牌，抛弃成见，开放心态，精诚合作。

技术人员当勤于思考、勇于提问、敢于质疑、不厌其烦地谨慎求证。

番外篇：PR

5月12日起持续发酵的WannaCry勒索蠕虫事件，恰如网络安全界的一场临时大考。安全企业、安全研究机构和安全从业者各显神通，在收获丰硕果实的同时，也顺带给全社

回首WannaCry事件始末，小刀倒也学到几招PR套路，比如：

² "快"字当先：紧跟脱缰的WannaCry，抢尽一切PR先机，没研究清楚不要紧，先发了再说。

² 反复轰炸：素材反复用，不求详尽，不求创新，但求刷屏。

² 标题第一：事实没那么重要，标题就是一切，越劲爆越好。

最后，用两张图结束本文：

我们知道，很多IT业的巨头都提倡"顾问式销售方法论"——根据用户的采购流程制订自己的销售活动计划，例如：

WannaCry事件，经历了"发现 - 初步分析 - 紧急应对 - 深入分析 - 全面应对 - 解密方法 - 思考未来"等过程，根据小刀的观察，如果咱要做PR，就要紧跟这个过程，在每一个

我们可以照葫芦画瓢，根据安全事件发展中的民众心理，制订自己的PR活动计划，例如：

本文定位于反思，所以，还是希望国内的同行们能够多多携手、砥砺前行！

比如：PR的力道不妨轻一些，工作量适当少一些，标题更客观一些，对客户的尊重更多一些；对技术的反思更加深入一些，在细节的追求上更精进一些，彼此的成见小一些

借发于阿里云先知技术社区的机会，更新一个遗漏的信息：

在WannaCry勒索蠕虫席卷全球的那个周末，某些人在群里高声喊着"我们又可以卖防火墙啦"的时候，另一些人在忙着给PR文起个更夺人眼球的标题的时候，一个信息安全的

繁华落尽PR去，细水流年技术来。

自勉，共勉。并祝大家儿童节快乐，脸上常常荡漾着孩子般纯真的笑容！恰如你对技术的那般执着。

同时，热烈庆祝《中华人民共和国网络安全法》正式施行！

教授说：西雅图也开始下雨了……

无工具版.rar (1.8 MB) 下载附件

上一篇：Linux版"永恒之蓝"... 下一篇：Windows提权基础

1. 4 条回复


hades 2017-06-01 16:08:32

好文 值得大伙好好看看

0 回复Ta


simeon 2017-06-02 05:10:01

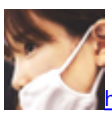
顶起来，不错。技术很全面

0 回复Ta


simeon 2017-06-02 05:12:01

要是能够找到那个素数，那就牛逼了。关键这个不太稳定，无迹可寻！

0 回复Ta


hades 2017-06-02 06:09:14
0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板