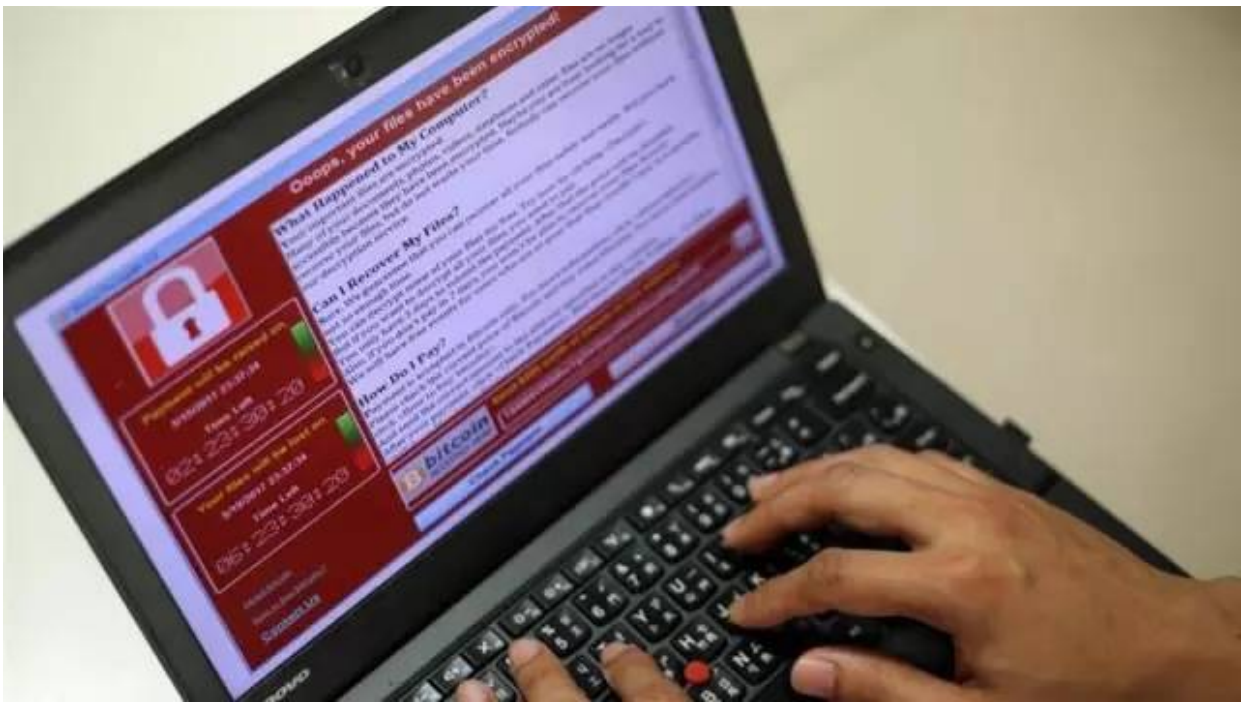
WannaCry勒索病毒犯错之业余令高手很想哭

2017-05-17 九一智库

WannaCry勒索病毒会对受害者机器文件进行加密，如果不交出赎金的话所有数据将化为乌有。这引发了全球范围的恐慌，但安全研究人员发现，病毒背后的制造者其实犯了一连串的低级错误，而且其获益极其有限。就勒索的专业水平而言，这完全是一次彻底地灾难性事故。有人怀疑，这次行动的目的不在金钱，而是让NSA难堪。



WannaCry 勒索软件攻击迅速变成了近年来冲击互联网的最糟糕的一场数字灾难，对全球的交通和医院系统造成了严重后果。但情况愈发显示出这并非黑客行家的作品。相反，网络安全调查者在这次灾难中看到的是一次草率的网络犯罪计划，几乎在每一个节

点都暴露出了业余水平的错误。

随着 WannaCry（或Wcrypt）这款史无前例的勒索软件攻击的展开，网络安全团体开始对该恶意软件作者犯下的令人费解的错误感到好奇。这次攻击利用了 NSA 创建的 Windows 黑客技巧，感染了150个国家超过20万套系统，尽管它留下了巨大的足迹，但恶意软件分析师说 WannaCry 创作者做出的糟糕选择既限制了它的攻击范围，也影响了它的获利。

这些错误包括嵌入了一个基于 web 的“杀戮开关”从而影响了病毒的传播，对比特币支付的处理相当不熟练，使得跟踪该黑客团体的利润情况变得容易很多，里面甚至还有一个做得很差劲的赎金功能。一些分析师说该系统使得犯罪分子不可能获知究竟是谁或没有支付赎金。

这种错漏百出的攻击仍然造成了那么大的损失，这不仅让人清醒地意识到：如果真正专业的犯罪分子改进了这个黑客团体的手段，那么结果将不堪设想。

有哪些业余错误？

最新统计显示，WannaCry 幕后的团体从这次攻击当中赚到的钱只是55000美元多一点，跟动辄几百万美元的专业秘密勒索软件产生的利润相比只不过是毛毛雨。思科Talos 团队的网络安全研究人员 Craig Williams 说：“从勒索的角度来说，这是一次灾难性事故。高破坏性，非常高的曝光度，非常高的执法可见性，而它的利润率可能比我们见过的任何一般甚至小规模的勒索行动都要低。”

安全公司 Hacker House 的研究人员 Matthew Hickey 说，获利这么少的部分原因可能是因为 WannaCry 做出来的赎金功能只是勉强能用。Hickey 周末的时候研究了 WannaCry 的代码，发现该恶意软件并没有通过分配唯一比特币地址来自动验证特定受害者是否支付了要求的价值300美元的比特币赎金。相反，它提供额度只是硬编码进来的4个比特币地址之一，这意味着受到的支付并没有身份细节，从而也就无法对解密过程进行自动化。相反，当赎金入账时犯罪分子自己得找出要对哪一台计算机进行解密，鉴于受感染的设备量达到了数十万，光靠人力显然是难以为继的。Hickey 说：“另一头其实是手工过程，而且必须有人确认并发出密钥。”

Hickey 警告说这种做法不可避免会导致犯罪分子无法对计算机进行解密，哪怕是收到了赎金之后。他说他一直在监控一名受害者，此人12小时前就已经支付了赎金，但至今仍未收到解密的密钥。Hickey 说：“他们其实并没有为这种规模的爆发做好准备。”

恶意软件里面只用了4个硬编码的比特币地址不仅会导致支付问题，而且还会令安全团体和执法部门跟踪兑现 WannaCry 赃款的任何尝试容易得多。比特币的公共会计总账，也就是所谓的区块链上所有的比特币交易都是可见的。

Errata Security 的安全顾问 Rob Graham 说：“这看起来极其令人印象深刻，因为你以为能把 NSA 漏洞利用集成进病毒里面的人一定是聪明绝顶的代码写手。但世上，这帮人就只懂这些了，除此以外他们就是空架子。他们把比特币地址硬编码进去，而不是每受害者一个比特币地址，这表明他们的思考能力有限。”

思科研究人员说他们发现该勒索软件的一个“检查支付”按钮实际上并不检查任何比特币是否已经发出。相反 Williams 说，它只是随机提供4个回答中的1个——其中3个是假冒的错误信息，而另一个是“解密”的信息，但也是假冒的。如果黑客加密了任何人的文件的话，Williams 认为对方是通过恶意软件的“联络”按钮人工与受害者沟通来进行解密的，或者随便给一些用户发送密钥，让受害者发生幻觉，以为支付赎金的确让他们的文件得到解放。而且跟更完善和自动化的勒索软件相比，这种差劲的做法几乎不会有什么人有付款的动机。Williams 说：“这破坏了整个令勒索软件有效的信任模型。”

规模重于实质

公平而言，WannaCry 的传播速度和规模是此前的勒索软件所不能比的。它利用了最近 NSA 泄露的一个 Windows 漏洞，叫做永恒之蓝（EternalBlue），制造了恶意加密迄今最糟糕的一场大瘟疫。

但就算只是从传播能力上来评判，WannaCry 的创作者也犯下了巨大错误。他们令人费解地在代码里面植入了一个“杀戮开关”，旨在通过这个开关访问某个独特的web地址，然后在进行一次成功连接之后屏蔽其加密负荷。研究人员怀疑这一功能可能是一项秘密举措，为的是避免代码在虚拟测试机器中运行时被侦测到。但这也导致一位化名 MalwareTech 的匿名研究人员只需注册该独特域名即可避免对受害者文件进一步的锁定。

周末之后，一个带有不同“杀戮开关”地址的新版 WannaCry 出现了。几乎与此同时，安全研究人员 Matt Suiche 也注册了这个域名，令这个改进版病毒的传播被打断了。Suiche 无法想象为什么这些黑客还没有用随机的方式生成 URL，而是在赎金软件中植入静态地址。Suiche 说：“我找不到任何明显的解释来说明为什么里面仍然有一个杀戮开关。”同样的错误犯了两次，尤其是这相当于把 WannaCry 干掉了，这么做简直是毫无意义。他说：“这似乎是一个逻辑bug”。

所有这一切都极大限制了 WannaCry 的获利，尽管该勒索软件已经导致了医院救命设备的关停和列车、ATM 以及地铁系统的瘫痪。与目前为止他们5位数的收益相比，思科的 Williams 指出，之前没那么出名的一次名为 Angler 的勒索行动在2015年被终止的1年之前估计拿到了6000万美元。

实际上，WannaCry 导致了那么大的伤害收到的利润却那么少以至于一些研究人员开始怀疑这项计划的目的根本就不是赚钱。相反，他们怀疑这也许是有人想利用 NSA 泄露的黑客工具造成的破坏来令其难堪——原先偷走这些工具的 Shadow Brokers 可能也是这个目的。Hacker House 的 Hickey 说：“我绝对认为这次是有人故意想造成尽可能大的破坏。”

“鉴于 NSA 对 WCry 的抨击以及屏蔽该勒索软件只容易，合理的推断是这是出于政治目的而不是金钱。”

— Don A. Bailey (@DonAndrewBailey)

“认为#Wannacry 与shadowbrokers背后的某人存在关联的人不在少数。”

— Stefan Esser (@i0n1c)

猜测归猜测，黑客的蹩脚办法还给我们带来另一个教训：一次更加专业的操作可能改进 WannaCry 的技术，从而造成比这大得多的损害。思科的 Williams 说，蠕虫基于网络的自我传播加上勒索软件的潜在有利可图是不会消失的。

他说：“这显然是恶意软件的下一代演进。肯定会吸引别人的效仿。在扩散瘟疫以及从中牟利方面，下一波犯罪分子可能会娴熟得多。”

来源：**36氪**