

解读Wannacry背后的匿名网络

腾讯电脑管家 F

2017-05-23 共56852人围观，发现 6 个不明物体

专题

网络安全

一、导语

本周Wannacry勒索病毒肆虐全球，由于病毒利用了Windows系统的网络服务(SMB)漏洞，具有主动传播的特性，在全球范围内已经对多家医院、服务机构、学校等进行了勒索攻击。用户一旦中招，电脑中的文档就会全部被高强度的加密算法所加密，原始文件相应的会被删除。由于攻击者使用了Tor匿名网络和比特币交易等技术方法，鉴于沟通的不确定性，即使缴纳赎金，也无法保证可以解密，导致解密之日遥遥无期。

本文将会深挖Wannacry勒索软件背后的匿名网络，从网络分析层面揭露该病毒的狡猾伎俩。

二、整体概况

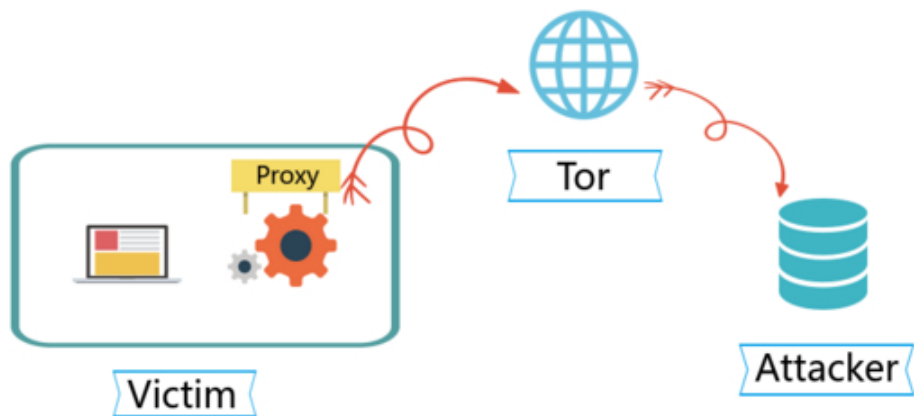
Wannacry 病毒首先会将自身注册成为系统服务，然后释放攻击程序，该程序利用微软MS17-010漏洞进行传播，传播过程无需人工参与，这也是该病毒全球爆发的主要原因之一。

该病毒敲诈加密的手法娴熟，使用混合加密体系，即公钥加密(RSA 2048) 配合对称加密(AES 128)。这做的好处是公钥加密保证了只有手握私钥的攻击者才能解密文件，对称加密保证了加密效率，在短时间受害者硬盘上的全部资料进行加密。

最后，该病毒使用了Tor (The Onion Router，洋葱路由器) [4]网络同远控服务器进行信息通信。该网最大的特点是匿名通信，这也是攻击者仍然逍遥法外的主要原因之一。

三、网络通信

本节会对Wannacry病毒的网络通信模块进行梳理和解析。如图所示，样本的通信流程主要有以下步骤



REEBUF

制图工具: canvas.qq.com

3.1 安装Tor软件

勒索软件为了能够匿名和服务器进行通信，“@WanaDecrypTor<@.exe”运行后会去检查是否已安装or软件。如果没有安装，“@WanaDecryp Tor@.exe”进程会分两步进行安装：首先是从官网下载，i方式能够保证下载到最新版本的Tor，但是如果遇到网络问题.第二步会从自身释放Tor浏览器，这样虽然致病毒体积增大，但是能够避免网络问题导致的文件缺失。下图是安装Tor软件的逻辑和URL地址。



样本通过使用官方的Tor程序接入Tor网络，好处是这些程序不会被杀软认为是病毒，减少了被查杀的可能性。同时样本会将tar.exe复制为taskhsvc.exe在后续操作中使用，这样做的目的是减少Tor的曝光度。

下图是样本Tor程序相关的文件结构图。



当安装完Tor软件后，会立即启动Tor服务taskhsvc.exe，用来和匿名网络中的服务器进行通信。taskhsvc.exe启动后以socks代理的工作模式监听本地127.0.0.1:9050端口，接收勒索主程序 “@WanaDecryp Tc@.exe” 的网络请求：



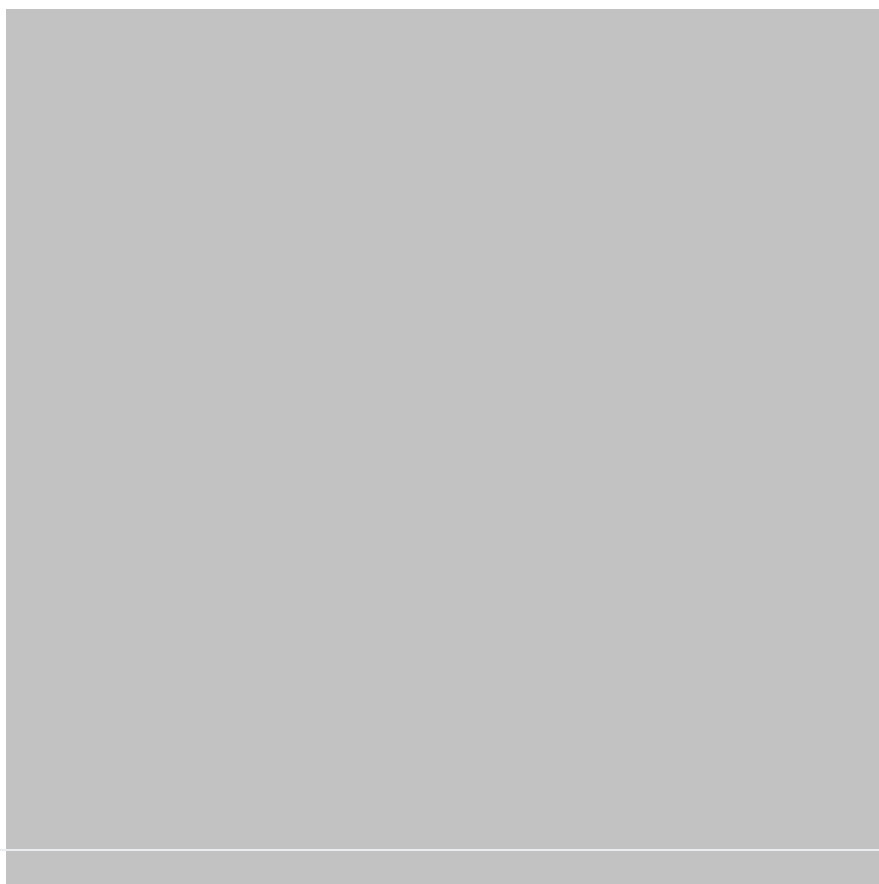
3.2 发送数据

当用户点击勒索界面的“Contact Us”和“Check Payment”按钮时，如下图所示 “@WanaDecryp Tc@.exe” 进程会向代理服务器taskhsvc.exe监听的127.0.0.1:9050端口发送消息。





比如，当我们点击“Contact Us”输入信息进行发送时，“@WanaDecryp Tor@.exe”进程会获取计算机名、计算机账户名以及其他的一些信息，连同要发送的信息发送到127.0.0.1:9050端口，然后由 Tor 进行转发，注意发送之前该数据会被简单异或加密，下图是加密之前的明文：



1. 红色框标注的是00000000.res文件的前8个字节，而00000000.res是针对用户的一个信息标识文件。
2. 绿色框标注的是计算机名和计算机账户名。
3. 蓝色框标注的是发送的实际内容，即“ just a test.” 。

当Tor代理服务taskhsvc.exe监听到127.0.0.1:9050端口有数据时，会向以下暗网地址转发相关数据，而网地址则配置在c.wnry文件。

3.3 CC服务器

经过逆向分析，样本会从如下5个洋葱地址中选择某个进行通信。

gx7ekbenv2riucmf.onion

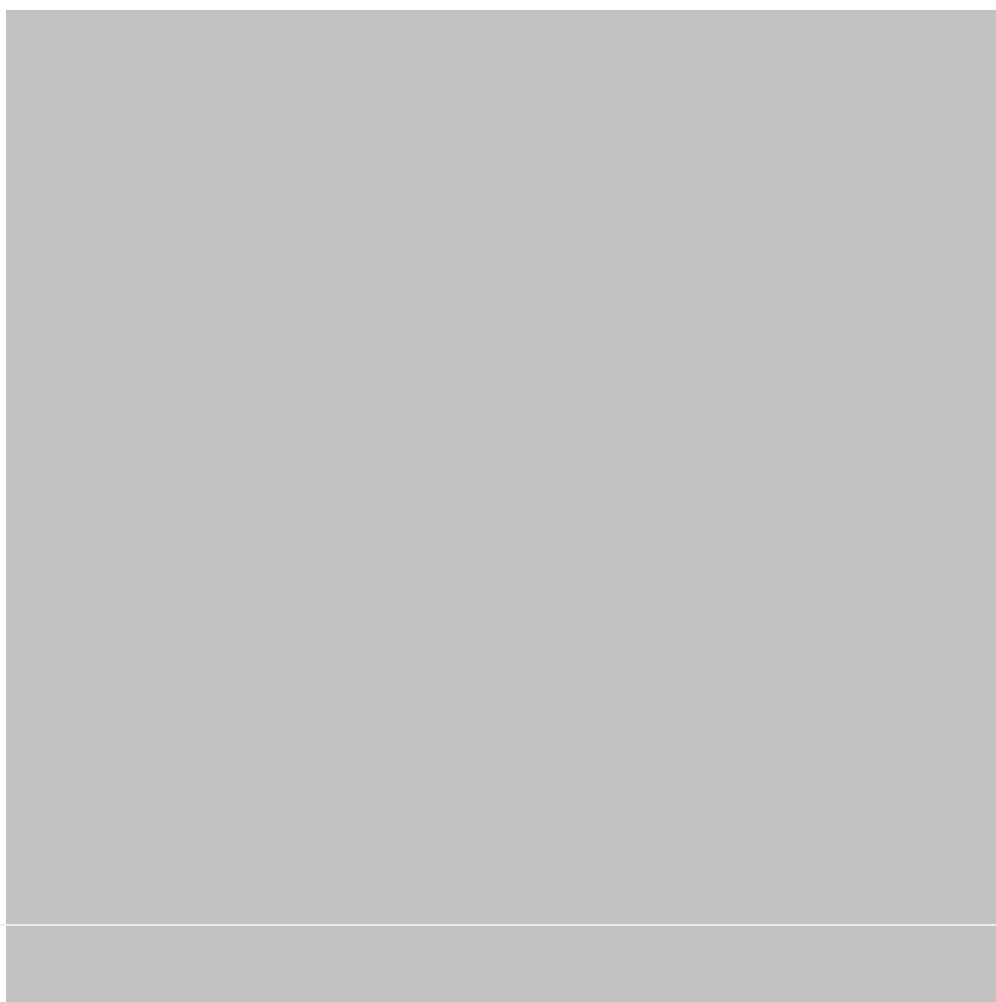
57g7spgrzlojinas.onion

xxlvbrloxvriy2c5.onion

76jdd2ir2embyv47.onion

cwwnhwhlz52maq7.onion

下图是样本尝试连接onion地址的情况。



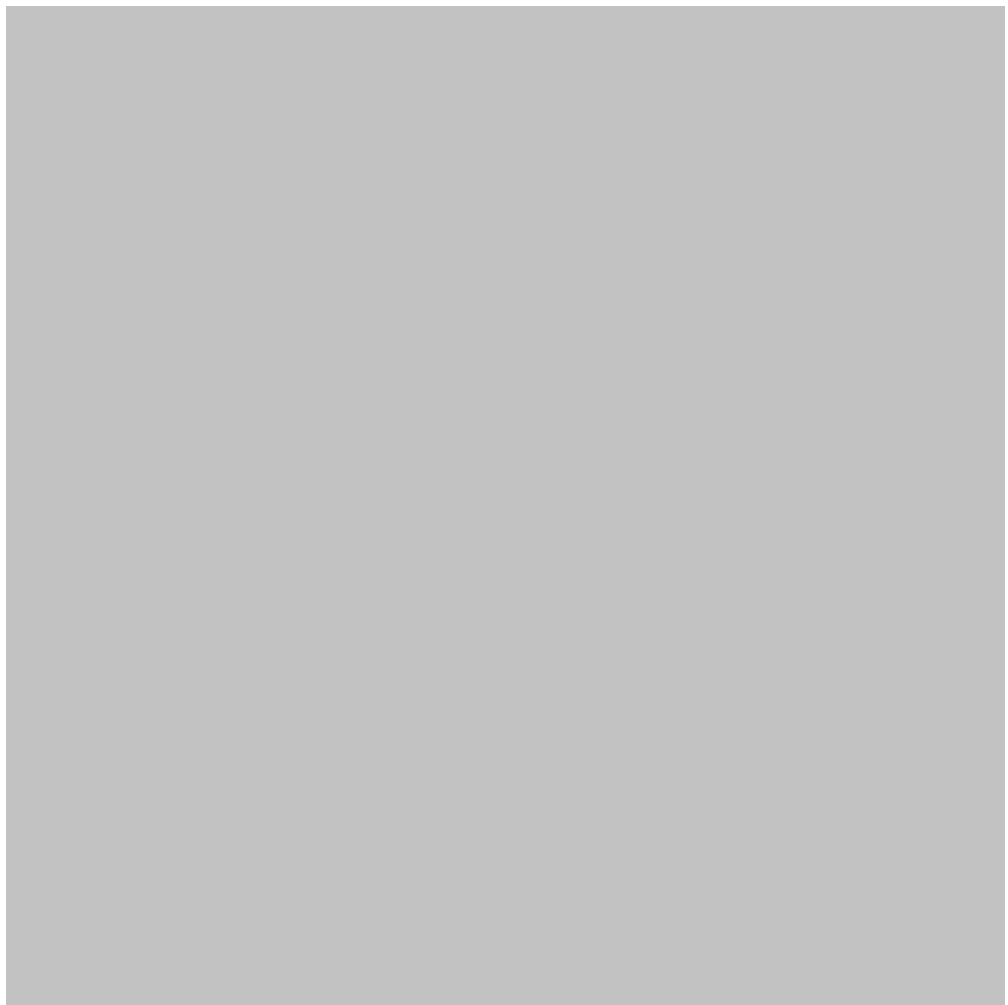
下图是网络分析中，onion地址的使用情况（57g7spgrzlojinas.onion）。



3.4 中继节点

Tor网络中，中继节点可以使用不加密的TCP协议(9001端口)，也可以使用加密的TLS链路通信(443端口)并且每次使用的中继节点都不相同，为溯源设置了障碍。下图是使用9001端口的TCP协议进行中继。





下图是lif.cubox.me的信息，整个Tor网络中有无数个类似的中继节点。





3.5 回包分析

回包中，最重要的操作是更新付款的bitcoin地址。下面三个bitcoin是默认的付款地址：

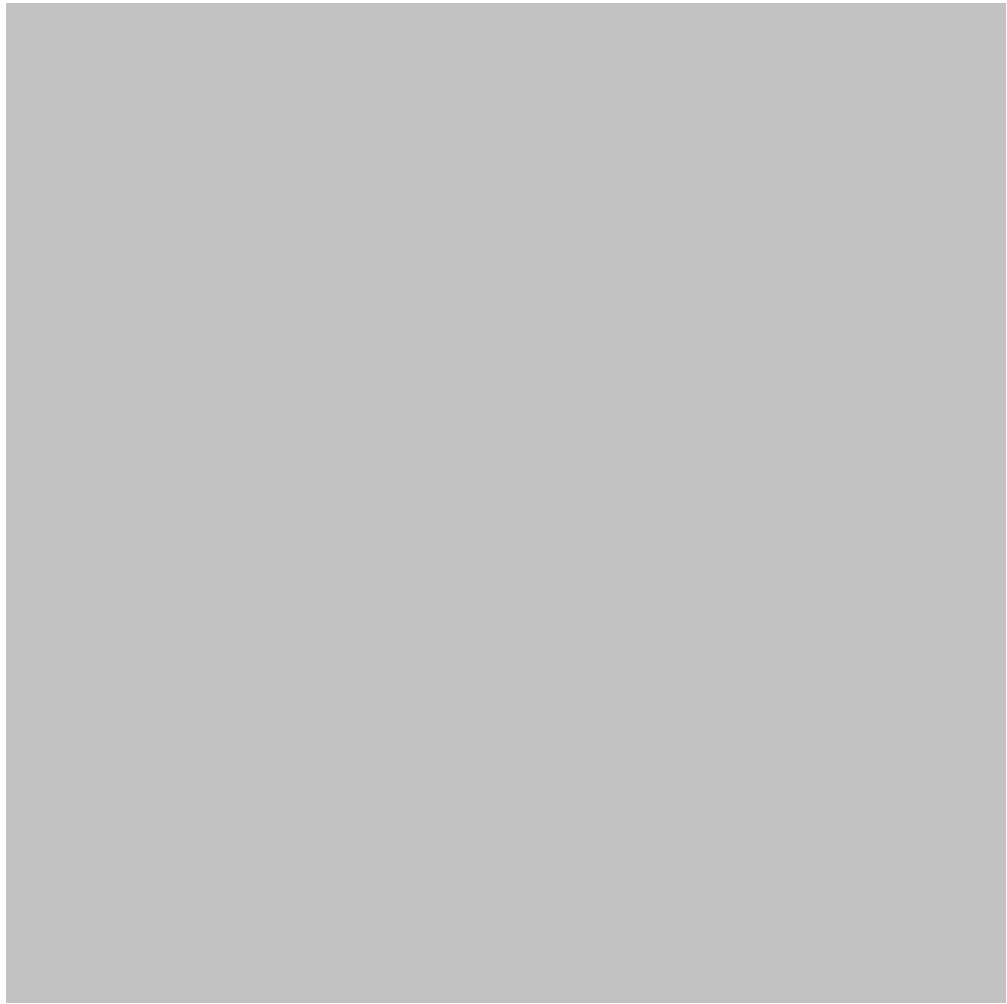
115p7UMMngo1pMvkpHijcRdfJNXj6LrLn

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

当wannacry完成加密过程后，会启动一个带 fi 参数的 “@wannaDecryptor@.exe” 程序，该程序接受包后，会更新c.wnry文件，该文件保存了新的支付地址。如下图所示，该bitcoin地址同默认的三个地址同。





这样每台受害者的电脑都会得到一个不同的付款地址，分析人员也无法统计攻击者使用了多少个付款地址。牵扯到的勒索金额也无法确切统计。这也是此次勒索软件的狡猾之处。

四、Tor网络介绍

Tor (The Onion Router , 洋葱路由器) 是实现匿名通信的自由软件。Tor用户在本机运行一个洋葱代理服务器，这个代理周期性地与其他Tor交流，从而在Tor网络中构成虚电路 (virtual circuit) 。而它之所以称为onion，是因为它的结构就跟洋葱相同，你只能看出它的外表，而想要看到核心，就必须把它层层剥开。即每个路由器间的传输都经过点对点密钥 (symmetric key) 来加密，形成有层次的结构。它中间所过的各节点，都好像洋葱的一层皮，把客户端包在里面，是保护信息来源的一种方式，这样在洋葱路由器间可以保持通讯安全。如下图所示[5]：





(Tor网络结构示意图)

五、总结

本文分析了Wannacry样本的网络通信行为，同时介绍了Tor洋葱网络的相关信息。该样本使用了Tor网络CC服务器进行匿名的加密通信，通信的方式是在本地9050端口搭建代理服务器，然后由代理服务器连接到部的中继节点。这种方式增加了隐蔽性和对抗网络分析的能力，也是攻击者目前仍然逍遥法外的主要原因之一。

六、参考资料

- 1.<https://habo.qq.com/tool/detail/smbdetect>
- 2.<http://slab.qq.com/news/tech/1575.html>
- 3.<http://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx>
- 4.<https://zh.wikipedia.org/wiki/Tor>
- 5.http://network.pconline.com.cn/701/7017738_all.html

*本文作者：腾讯电脑管家（企业帐号），转载请注明FreeBuf.COM

上一篇：[SMB漏洞引发的“血案”，远不止WannaCry](#)

下一篇：[本篇已是最新文章](#)

这些评论亮了



[eval0day](#) (3级) freebuf手机贴膜
大波种子还有10秒到达战场，榨干他们

[回复](#)

[亮了\(7\)](#)

已有 6 条评论

金山杀毒 2017-05-23

1楼 [回复](#)

我一有360NSA武器库免疫系统在手二有瑞星之剑在手，什么这那的，今晚我就开启看片模式。

[亮了\(1\)](#)

幕刃 2017-05-23

[回复](#)

@ 金山杀毒 我看片从来不用开杀软

[亮了](#)

瑞星 2017-05-23

[回复](#)

@ 金山杀毒 臭不要脸的..好意思开着我去看片...有种单独只开自己看片试试

[亮了](#)

[eval0day](#) (3级) freebuf手机贴膜 2017-05-23

2楼 [回复](#)

大波种子还有10秒到达战场，榨干他们

[亮了\(1\)](#)

[屌丝绅士](#) (4级) 做自己的自己 和平年代的炮灰，战争年代的爆破鬼才 2017-05-23

[回复](#)

@ eval0day 老铁 神评给你了 没毛病

[亮了](#)

[Beck_zmz](#) (1级) 也许我没有天分，但我有梦的天真，我将会去证明 用我的一生 2017-05-23

@ 屌丝绅士 +1,都是大神 膜拜，求带

[亮了](#)

浏览...

昵称

请输入昵称

必须 您当前尚未登录。 [登陆?注册](#)

邮箱

请输入邮箱地址

必须 (保密)

表情

插图

提交评论(Ctrl+Enter)

[取消](#)



有人回复时邮件通知我



腾讯电脑管家

腾讯电脑管家官方账号

60 篇文章 0 条评论

关键字查找

相关阅读

[WannaCry勒索病毒分析报告](#)

[BlackHat议题：SMB不只是共享你的...](#)

[上海地区WannaCry蠕虫式勒索软件传...](#)

[CNNVD关于WannaCry勒索软件攻击...](#)

[解读Wannacry背后的匿名网络](#)

特别推荐






关注我们 分享每日精选文章

不容错过

| | | |
|--|---|--|
| 网络小黑揭秘系列之私服牧马人 | 【WitAwards 2016 “年度安全产品” 参评巡礼】做最干净的杀毒软件——杀木马金数据检测 | |
| 360天眼实验室 2015-12-01 | FreeBuf研究院 2016-09-27 | |
| 2016 FreeBuf互联网安全创新大会（FIT）：共探安全创新源动力 | Splunk+蜜罐+防火墙=简易WAF | |
| FB独家 2015-12-03 | RipZ 2016-12-05 | |



Copyright © 2013 WWW.FREEBUF.COM All Rights Reserved [沪ICP备13033796号](#)

 阿里云 提供计算与安全服务