系统安全

特别企划

WannaCry数据恢复方案

亚信安全 2017-05-18 18:07:14 416776 2

5月12日，黑客驱动WannaCry/Wcry蠕虫病毒，向全球用户发出“勒索”挑战。一些从来不知道“打补丁”，不清楚什么是445端口的无辜群众因此受难。随后，网上流言四起，一种说法是“数据可以自行解密”，另一种说法是“数据可以通过软件恢复”，为了查明真相，亚信安全技术支持中心通过逆向病毒行为分析，发现了数据恢复中的“重大秘密”。

数据恢复不等于解密

近期，网上流传一些“解密方法”，甚至有人说病毒作者良心发现，已经公布了解密密钥，通过验证，这些都是谣言。亚信安全建议广大公众，轻信谣言的结果，还可能面临“二次中毒”的风险。

针对本次爆发的勒索蠕虫WannaCry, 到目前为止还没有公布私钥，而从黑客采用的加密技术原理来讲，除非拿到对称密钥，否则无法实现解密。亚信安全网络监测实验室测试发现：目前，能减少客户损失的方法只有通过数据恢复技术，而非解密技术来还原数据。

WannaCry勒索蠕虫的3种加密行为

这一次WannaCry病毒引发的全球勒索蠕虫风暴，不仅是全球首款通过系统漏洞实现传播的勒索蠕虫，更在加密手段上独树一帜。经过亚信安全对已经获取到的病毒样本的逆向分析后发现，编写病毒的黑客，为了提高加密效率，WannaCry病毒有3中不同的加密行为：

第一种加密行为：桌面文件被“重写”，数据不可恢复

亚信安全技术支持中心发现，WannaCry勒索病毒首先会选择用户的“桌面”进行加密，同时使用垃圾数据填充原文件（文件经过多次重写），然后删除。黑客充分研究了普通用户保存数据文件的行为，利用了大多数人将手头重要文件保存在桌面的“坏习惯”。而在这种情况下，因为原文件已经被覆盖填充，所以这种方式处理过的文件是不可能被恢复的！

第二种加密行为：系统盘文件可部分恢复，“文件名”彻底丢失

针对系统盘（一般是C盘），勒索病毒在加密文件后，会重命名原文件为$数字.WNCRYT。如1.WNCRYT; 2.WNCRYT等，然后把这些文件移动到“%TMP%目录”下。这种方式处理过的文件，只能部分被恢复为*.WNCRYT文件。需要查看文件头，确定文件类型后，手动修改为原始原件类型。例如1.WNCRYT修改为xxx.doc后可以恢复为原始的WORD文件。

第三种加密行为：其他盘符文件恢复可能性较大，概率由“磁盘剩余空间”决定

针对其他盘符（如D,E盘等），勒索病毒在加密文件后，直接删除原文件。这种方式处理过的文件是有可能被恢复的。至于能恢复多少，要取决于原文件所在的扇区是否被重写或者覆盖过。通过测试发现，当一个盘符里面的数据量较少时（例如使用了30%），几乎能恢复所有数据；当一个盘符里面的数据量较大时（例如使用了90%），只能恢复部分数据，有一部分数据丢失；当磁盘空间已满时，有的原始文件根本没有被加密， 这种情况下，与普通数据恢复原理相同，大多数数据可以恢复。

3种加密行为下的数据恢复实验

为了证实以上3种行为与数据恢复之间的关联性，亚信安全技术支持中心分别进行了相关实验。

实验一：

使用病毒样本感染测试机， 然后尝试使用数据恢复软件恢复桌面上的文件。测试步骤和结果如下：

1. 病毒加密之后，桌面文件被加密。
2. 尝试数据恢复，可以发现所有C盘可恢复的用户文件都在%TMP%下。
3. 恢复之后发现，恢复的文件都是C盘其他目录下的文件。 桌面文件无法恢复。

实验二：

使用病毒样本感染测试机， 然后尝试使用数据恢复软件恢复系统盘文件。测试步骤和结果如下：

1. 图1所示，病毒在加密之后，可以在%TMP%目录下看到很多以WNCRYT为后缀的文件

亚信安全2020第五空论坛成功举行 2020-11-16

EMOTET银行木马仍ode释放方式、基础

2020-07-02

伪装成屏保程序的Ag马分析 2020-06-24

浏览更

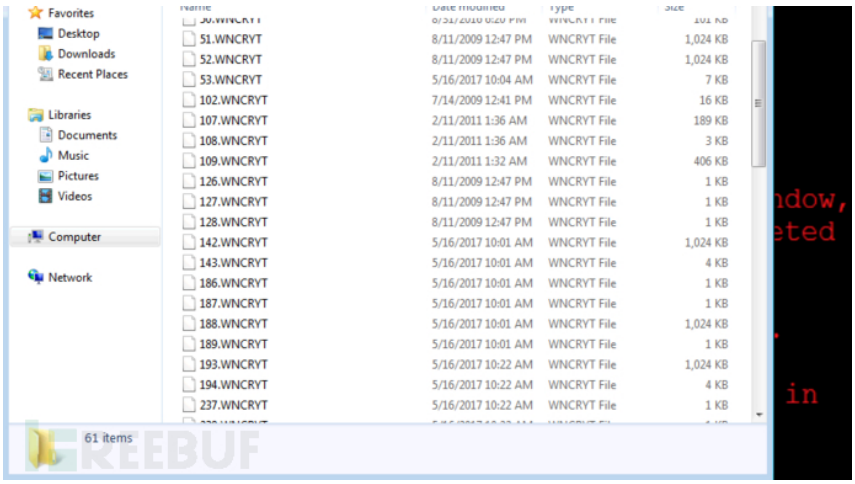


图1：文件名后缀被修改为WNCRYT

2. 使用数据恢复软件恢复出来的数据也是WNCRYT格式的文件。可以使用工具查看文件头信息。 图2中可以看到8.WNCRYT文件的真实文件类型是docx文件。

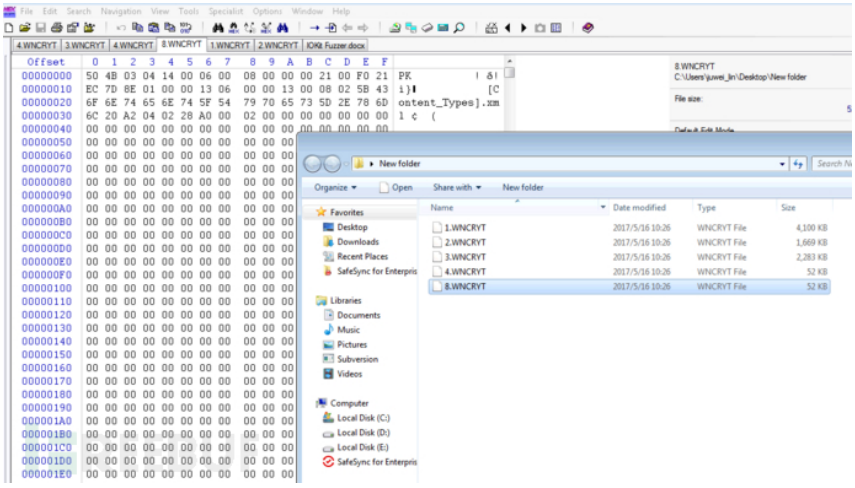
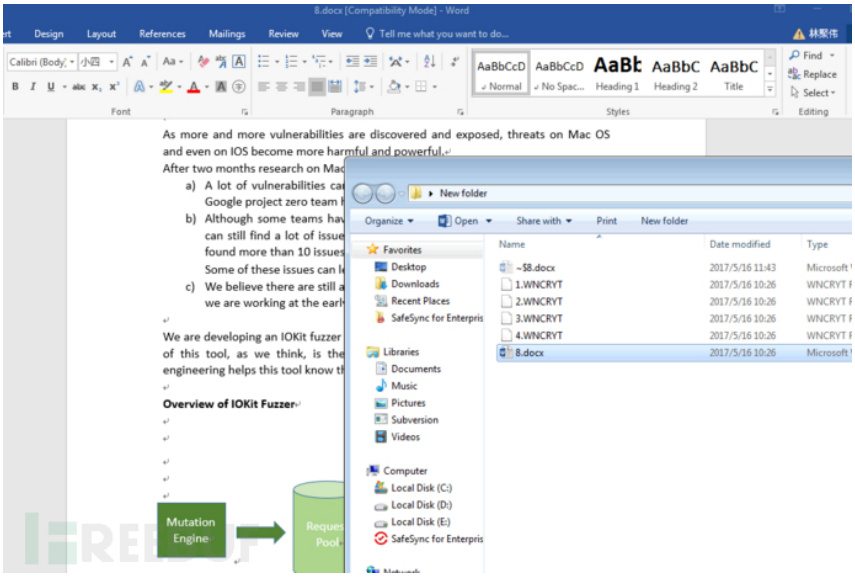


图2：WNCRYT文件的真实文件类型是docx文件

3. 可以直接重命名文件格式， 就可以恢复该文件。 但是原始文件名是无法恢复的。



WannaCry数据恢复方案

系统安全

特别企划

1. 在磁盘有空余的情况下，几乎能100%恢复数据。
2. 在磁盘满的情况下，只有部分文件被加密。 很多原文件直接被保留在磁盘上。

正确选择数据恢复顺序

为了保证测试的准确有效，亚信安全技术支持中心测试了两种操作系统、两个病毒样本、两种数据恢复软件，测试结果一致。结论如下：

桌面文件无法恢复。
系统盘文件可部分恢复，但恢复难度较大。
其他盘符内的文件容易被恢复，且被恢复的可能性较大。

WannaCry 勒索软件是不法分子通过改造之前泄露的NSA黑客武器库中“永恒之蓝”攻击程序发起的网络攻击事件，利用了微软基于445 端口传播扩散的 SMB 漏洞MS17-010。在提醒用户及时安装相关补丁和网络安全软件、开启防火墙封堵网络端口的同时，亚信安全经过上述实验，建议受到WannaCry感染的客户，请优先恢复D，E等其他盘符内的文件，对系统盘内的文件用户请选择性恢复。

***本文作者：亚信安全（企业帐号），转载请注明Freebuf.COM**

评论 2

按时间排序

1455018613 LV.4 (1455018613)

2017-05-18 21:30:38 18 回复

fuck you LV.1 来自新浪微博

你看着我的眼睛再说一遍

2017-05-19 00:41:43 12 回复

请登录/注册后在FreeBuf发布内容哦

相关推荐

针对小程序的漏洞挖掘

Web安全

原文来自SecIN社区—作者：Zeva0x00 前言承接上一篇APP业务挖洞的碎碎念，此篇文章主要是针对小微信程序的漏洞挖掘，微信小程序默认...

WannaCry数据恢复方案

系统安全

特别企划

观点

在不同的情境下，个人隐私应处在何种位置，不同主体或者说个人信息所有者应该如何处理信息，这些问题今天想和大家一起来聊一聊。

Sandra1432 已有17255人围观 · 发现1个不明物体 2020-11-20

40万条用户信息被泄露，企业如何有效防范员工成内鬼?

观点

据新京报报道，邯郸市公安局近期侦办的一起案件中，发现不法分子与快递企业多位“内鬼”勾结，通过有偿租用快递企业员工系统账号，盗取公民个人信息，...

腾讯安全 已有8715人围观 2020-11-20

FreeBuf早报 | DeepFake换明星脸违法分子被抓；任天堂起诉黑客贩卖switch破解工具

资讯

DeepFake是目前相当流行的深度换脸AI程序，不过常常被歪用。

Megannainai 已有43708人围观 · 发现2个不明物体 2020-11-19

苹果被曝重大系统漏洞：root权限秒获取，新款MacBook、iPhone 12统统波及!

漏洞

这两天，苹果M1爆锤老同志英特尔的测评，刷了屏。

Doraemon 已有45507人围观 2020-11-19

文章目录