Fucking勒索软件分析

菠菜 / 2017-06-04 09:49:00 / 浏览数 3453 技术文章 技术文章 顶(0) 踩(0)

一 背景：

近期，一款新型的勒索软件在网上流传，与一般勒索文档型的勒索软件最大不同有以下两点，一是该勒索软件会加密用户的所有文件格式，而不仅仅是文档类型的格式文件。

该勒索软件会将加密后的文件扩展名重新定义为.fucking，因此，我们将其命名为fucking勒索软件。由于赎金的支付方式也没有在勒索软件中有所体现，这看起来更像是定

该勒索软件并没有支付赎金的说明文件等内容，更可能是通过在社交群中或者共享盘中传播，恶意软件作者在传播勒索软件时，会通过另外的方式留下自己的联系方式。一种

勒索成功后，弹出的解密对话框如下：

文件加密后的显示结果如下：

二 分析：

恶意软件的详细的文件信息：

而勒索程序体积很小，只有125,952 字节。

勒索程序使用C#编号，反编译后，代码结构图如下，可以看到程序的代码做了一定的混淆：

通过分析勒索程序的窗口类，可以看到程序带有3个form界面，其中的form1隐藏运行，并不会显示出窗口，用于遍历文件和加密文件。Form2用来显示提示用户输入解密密

每个form控件的功能如下：

Form1 加密文件，隐藏运行

Form2 提示用户输入解密密码

Form3 解密文件，只有在form2中输入了正确的密码才会显示

我们将分析其对文件的加密与解密过程。

加密过程

在加密时，会隐藏加载form1界面，Form1界面中会有listbox控件，用来存放遍历到的要加密的文件路径，遍历指定文件夹下的文件，将文件路径加入到form1中的listbox1

Form1的隐藏运行：

遍历目录，遍历的根目录到盘符Z：

遍历到文件后，判断文件名是不是以fucking结尾，如果不是fucking后缀，就将文件名加入到listbox1列表中。

最后程序会设置一个计时器，当计时器到达时间时，会将listbox1控件中的文件取出来，进行加密，下面为生成加密KEY及加密文件的过程

对文件的加密使用了AES对称加密算法。

AES算法中使用的 Key 和 IV的计算过程如下：

计算硬编码的字符串"FucktheSystem"的sha512的hash值，hash结果的十六进制表示如下：

```
DB 5D 07 9E FA 07 AE A3 EE 81 64 DB 76 D9 6A BE
EB BE 3E 71 8F 36 B1 E7 E0 DA 94 16 90 C8 18 84
62 F1 01 62 03 F2 D1 89 E6 39 34 6B 5B 24 35 D3
72 1F ED 11 C7 0C 3C 29 0F 7F 72 EE F5 1B 64 62
```

取该hash值最前面的0x20字节做为Key, 下图中的绿色框部分

取该hash 偏移0x20-0x30的内容做为IV，下图中的红色框部分

计算key的代码如下：

计算IV的过程与上面计算key的过程类似，在此不再赘述。

Timer1时间间隔100ms，到达时间后，就是调用加密过程

对文件的加密过程的调试，可以看到

将“C:\Users\forrest\Documents\desktop.ini”

加密成“C:\Users\forrest\Documents\desktop.ini.fucking”

使用的key和IV分别如下图所示

解密过程：

form2窗口对应着解密窗口，显示如下：

但用户输入密码后，程序会在后台判断是否与指定的密码相同，如果密码正确就会弹出form3进行解密文件，否则就会弹出下面的出错提示。

对密码的判断逻辑，可以看到程序将用户输入的密码与一个函数的返回值进行了比较，如果相同，就调用form3的显示函数，并把form2隐藏，如果不相同，刚弹出出错对话

其中的m4bpguG5abU260W8Ln类为程序作者自定义的字符串操作类，m4bpguG5abU260W8Ln类的iAGT7PZUW方法为取得指定偏移处的字符串，类似于C语言中的sub

iAGT7PZUW函数内部实现过程：

从上面的代码可以看出密码保存在偏移1124(十进制)的位置。在此时，也可以将字符表dump出来，保存到本地进行查看。

第一个DWORD为字符大小，这里为0000002c

通过下面可以看到偏移1124(十进制)位置处的字符串长度为：0x2c,字符串内容为：“maaf saya lupa passnya”

因此，可以得到Form2的解密密码“maaf saya lupa passnya”。

输入正确的密码后，form2界面会隐藏，form3界面会显示出来 ,程序会在后台遍历保存的文件名，利用AES将其解密成原始文件。

三 数据恢复：

在弹出的窗口中输入密码：maaf saya lupa passnya，就可成功解密文件

解密成功后的截图如下：

四 总结

Fucking勒索软件与传统的aes+rsa的勒索软件不同，它设计思路简单，与我们以前分析的sega勒索相比，它的设计思路简直就是渣渣。与我们以前分析的CryptoShield勒索家族相比，CryptoShield
家族至少做到了一机一密，而Fucking勒索软件的密码是固定的，对所有的机器都使用统一的密码，这一方面因为它不是面向大众传播的，而是针对特定的人群，通过特定的

如果您被此类勒索软件勒索，建议尝试使用密码“maaf saya lupa
passnya”进行解密尝试，如果不能成功解密，可能是恶意软件作者进行了代码升级，建议联系专业的安全研究人员进行分析解密。

CryptoShield 勒索分析请参照：https://xianzhi.aliyun.com/forum/read/726.html

sega勒索分析请参照：https://xianzhi.aliyun.com/forum/read/799.html

上一篇：“安全帮”大型目标渗透 - 01信息搜集 下一篇：如何优雅的维持一个Webshell

1. 0 条回复
   - 动动手指，沙发就是你的了！