GlobeImposter勒索样本分析

深信服千里目安全实验室 / 2018-02-28 09:50:30 / 浏览数 14775 安全技术 漏洞分析 顶(0) 踩(0)

样本简介

最近接到客户举报，服务器文件被勒索软件加密，联系客户拿到样本之后，判定该样本为GlobeImposter家族的变种样本。

GlobeImposter家族首次发现在2017年5月份，这次发现的样本为GlobeImposter家族的最新样本，没有内网传播功能，其加密文件使用.TRUE扩展名，取消了勒索付款的比

行为分析

1.勒索样本在运行后，首先判断%LOCALAPPDATA%或%APPDATA%环境变量是否存在，如果存在则将自身复制到%LOCALAPPDATA%或%APPDATA%目录，如图所示

相关的反汇编代码如图所示：

2.复制自身到%LOCALAPPDATA%或%APPDATA%目录之后，进行持久化操作，设置自启动项，注册表项为HKEY_CURRENT_USER\Software\Microsoft\Windows\Curr

3.通过内存解密，得到如下图所示的目录字符串列表：

勒索软件在进行加密的时候，会判断是否是以上目录，如果是以上目录则不进行加密操作，如图所示：

4.生成RSA私钥并使用硬编码公钥加密，之后将加密后的密文转换为ASCII码，最后将密文写入%ALLUSERSPROFILE%变量路径中，生成的密钥ID文件如图所示：

5.样本通过RSA算法进行加密，先通过CryptGenRandom随机生成一组128位密钥对，然后使用样本中的硬编码的256位公钥生成相应的私钥，最后生成受害用户的个人ID序

6.用户感染相应的勒索样本之后，样本会加密相应的文件夹下的文件，并生成how_to_back_file.html的超文本文件，如图所示：

生成的超文件文件，显示了个人的ID序列号，以及恶意软件作者的联系方式，如图所示：

7.加密完成之后，进行自删除操作，如图所示：

防御方式

千里目安全实验室提醒各位小伙伴，平时注意以下安全防范措施：

■■■■■■■■■■■■■■■■

■■■■■■■■■■■■■

■■■■■■■■■■■■■■■■■■■

■■■■■■■■/■■■■■■■■■■

Globelmposter■■■■■■■■■■■■■RDP(■■■■■■■■■■■■■■■■■■■■■■RDP(■■■■■■■■

■■■■■■■■■■■■■■■■■■■■■■■■■■■■■445,135,139,3389■

上一篇：SQL和NoSQL注入浅析（上） 下一篇：OSS对象存储上传解析漏洞

1. 2 条回复


addin****@aliyun 2018-03-02 09:37:44

你好，你能恢复被这个病毒感染的文件么？怎么联系你恢复？

0 回复Ta


hades 2018-03-04 23:43:52

@addin****@aliyun 由于GlobeImposter采用RSA2048算法加密，目前该勒索样本加密的文件无解密工具

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