**GlobeImposter勒索病毒应急处置方案**

****

网神信息技术（北京）股份有限公司

2019年03月10日

|  |  |
| --- | --- |
| 文档编号 | 编写人员 |
| XBAF-360AFZGS-17 | 耿浩杰 |

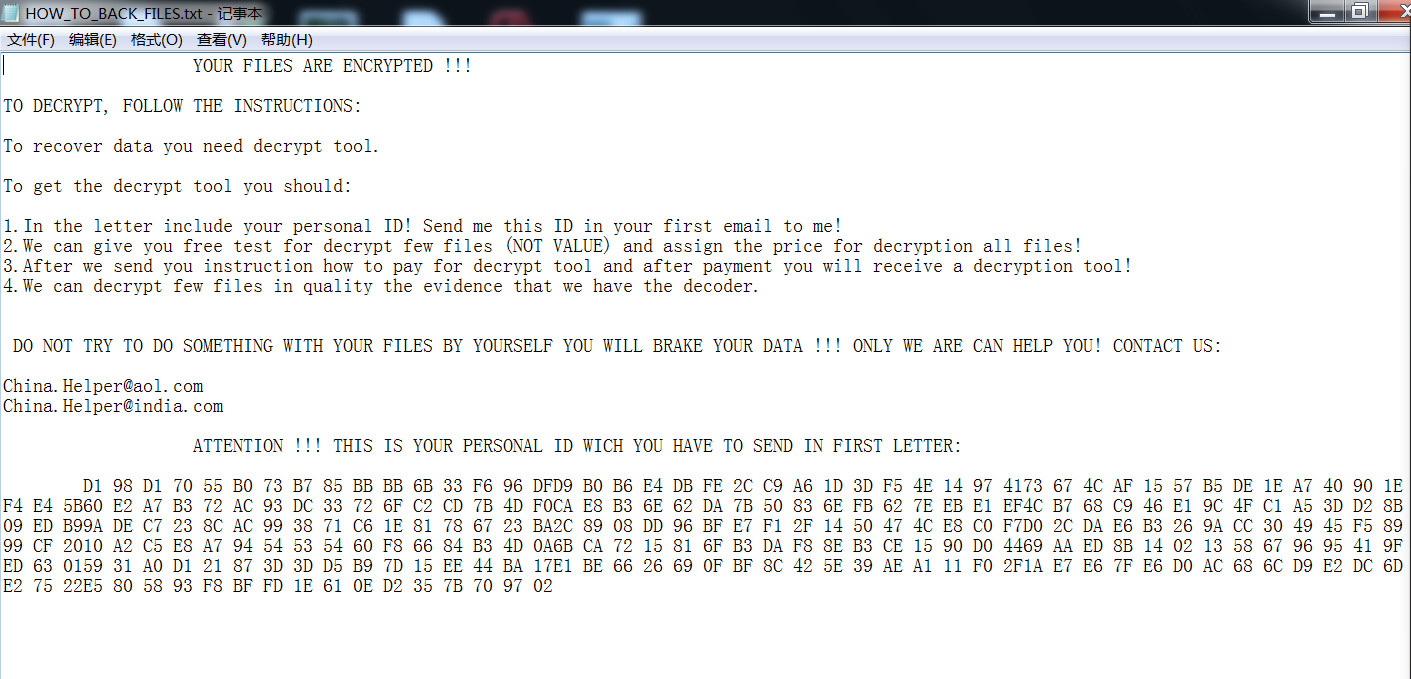
# 事件概述

2019年3月10日上午8点，甘肃全省多家单位GlobeImposter勒索病毒事件， 经过定性分析判断定向爆破和定向投递勒索病毒，通过RDP远程桌面攻击服务器，利用KprocessHacker 结束杀毒软件进程，并利用其它黑客工具如扫描器、密码抓取工具进行进一步攻击，随后执行勒索软件，文件被加密，病毒感染后的主要特征包括windows服务器文件被加密、加密后缀 \*.snake4444。

根据本次事件特征分析，除已受到攻击单位外，其它同类型单位也面临风险，需积极应对。

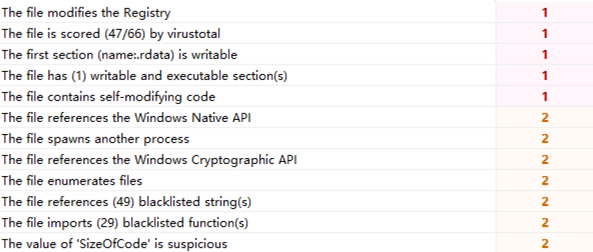
# 样本分析情况

本次样本为GlobeImposter勒索病毒变种，MD5为AEC05756F4616839C8DA2919004598AC与早期出现样本类似，黑客攻击方式通过RDP爆破后手工投毒，勒索采用RSA+AES的加密方式



## 样本静态信息

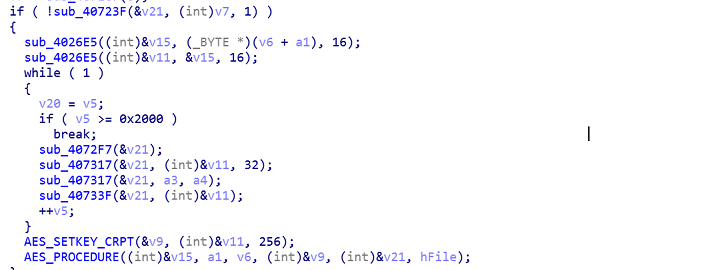
样本静态可疑信息



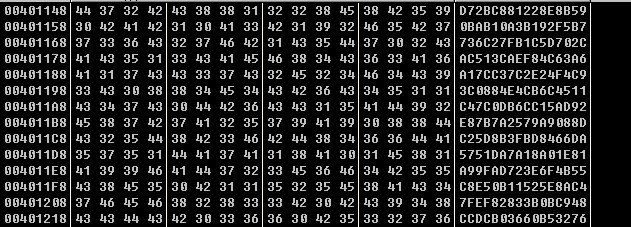
## 样本流程分析

样本首先调用AES算法解密内置的加密的字符串





解密后的内容



随后解密加密后文件的后缀名



# 紧急处置方案

【紧急处置】

1. 控制已发现被攻陷主机，采取措施防止蔓延：下线已发现招攻陷主机，扫描暴露到公网的主机和端口、紧急关停。

2. 摸清楚受害主机范围，对中招主机进行处置：通过天眼网络流量分析、天擎病毒扫描或漏洞扫描等方式，筛查出受害主机范围，对中招主机下线然后查杀、打补丁。

3.对已确定感染的主机和服务器，和扫描发现存在风险的主机可进行加固，加固需在客户授权同意协助客户处理；对重要业务服务器加固、打补丁、增强口令强度，封禁端口等

【未感染主机与加固】

1、在网络边界防火墙上全局关闭3389端口或只对特定IP开放。

2、开启Windows防火墙，尽量关闭3389、445、139、135等不用的端口。

3、每台服务器设置唯一口令，且复杂度要求采用大小写字母、数字、特殊符号混合的组合结构，口令位数足够长（15位、两种组合以上）。

4、安装天擎最新版本（带防爆破功能）和天擎服务器加固版本防止被黑。

5、如用户处存在虚拟化环境，建议用户安装360网神虚拟化安全管理系统，进一步提升防恶意软件、防暴力破解等安全防护能力。

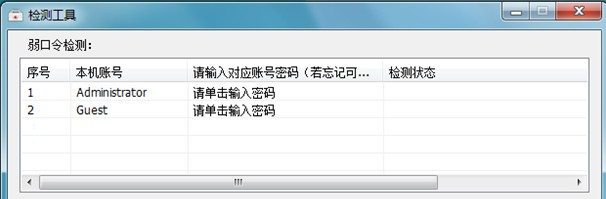
# 病毒检测工具

针对此次出现勒索病毒由于暂时没有解密工具，建议尽快对感染主机进行断网隔离；然后使用工具进行检测查杀。

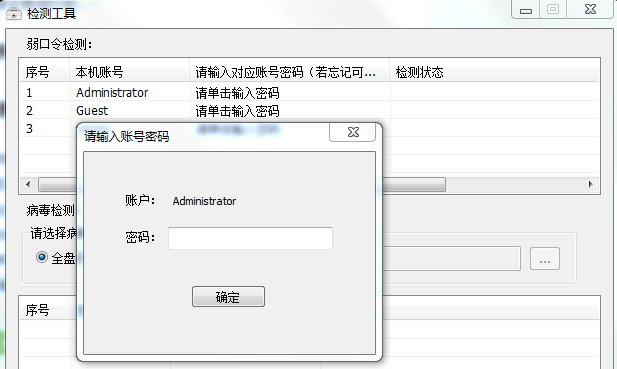


## 1、弱口令检测

检测工具在初始运行时，就会检测当前终端存在的所有的账户，遍历在当前窗口里：



用户需要单击每个账号后的输入框，输入对应的密码，若是忘记可以跳过：



输入完成后，检测状态会改变：



点击“立即检测”，则会开始对输入的弱口令进行检测。

注意：

1. 若密码输入错误、或者留空，检测状态都会显示“密码错误，请重新输入”；
2. 修改密码，重新输入后，检测状态都会进行变更；
3. 若检测到密码为弱口令，建议用户按提示进行密码重置，提高密码强度后再进行检测。

## 2、勒索病毒检测

需要在管理员权限下运行检测工具，用户可以根据实际需要，选择对应的扫描模式：全盘扫描、暂时不扫描、自定义扫描：



选择好模式后，点击“立即检测”，则会开始对选择的路径进行扫描。若是选择“暂时不扫描”，则会跳过扫描，只是检测弱口令。若点击“停止”则会终止这一次的检测操作。

当检测出病毒文件时，点击“一键清理”，则会将所有的病毒文件进行删除处理。