GlobeImposter 勒索病毒事件安全检测工具

使用手册

1. 工具简介

近日，国内某机构遭受 GlobeImposter 勒索病毒攻击，导致业务相关文件被加密，对业务的连续性造成严重影响。通过对本次勒索攻击事件的分析下，我们发现本次攻击相对普通的勒索事件的首要区别在于攻击者在突破企业防护边界后积极进行内网渗透，绕过安全防护，并释放勒索恶意代码，具有极强的破坏性及针对性。

本次事件中，黑客从外网打开突破口后，会以工具辅助手工的方式，对内网其他机器进行渗透，包括对内网其他主机进行口令暴破，从而达到在内网横向移动到新的主机进行攻击的目的。因此，对于存在弱口令的主机更容易遭到攻击者的侵害。

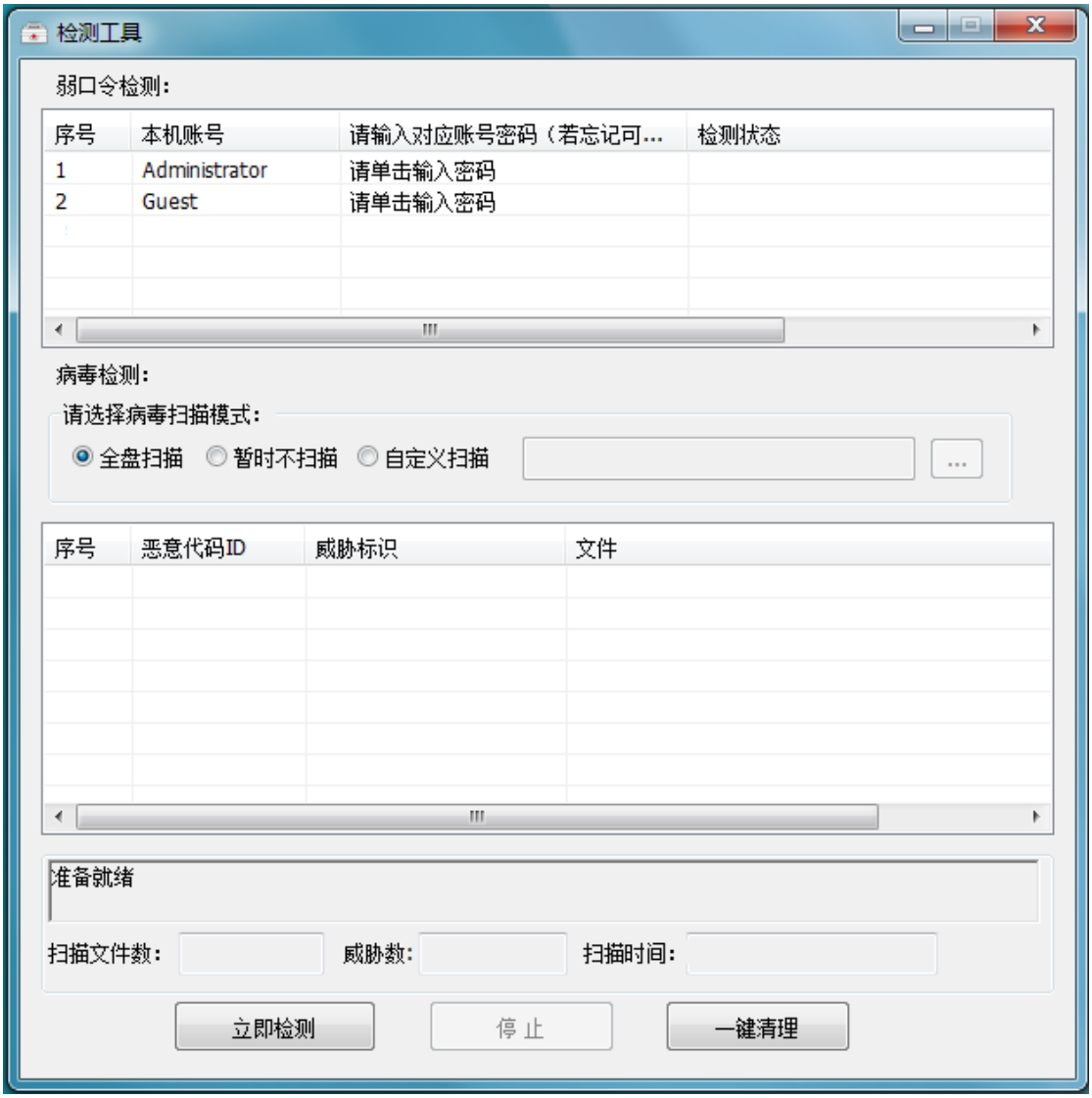
GlobeImposter 勒索病毒事件安全检测工具是 360 天擎团队针对这次勒索病毒事件推出的检测工具，主要检测终端用户的账户是否存在弱口令以及高危账号；并扫描终端文件，对 GlobeImposter 勒索病毒进行查杀。

2. 安装部署

支持系统：winserver2003、winserver2008、winserver2012、XP、win7、win8、win10

解压缩文件包 FocusTool.zip，运行解压的 Focus.exe 即可。

运行后的界面：

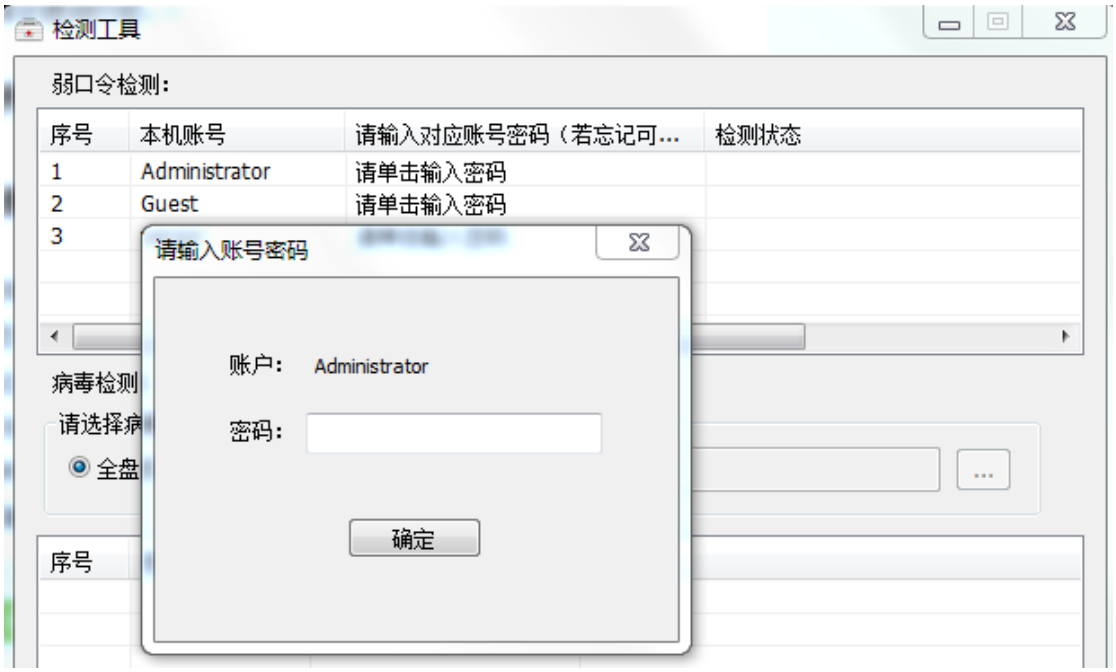

检测工具
弱口令检测：
序号
本机账号
请输入对应账号密码（若忘记可...
检测状态
1
Administrator
请单击输入密码
2
Guest
请单击输入密码
病毒检测：
请选择病毒扫描模式：
全盘扫描
暂时不扫描
自定义扫描
...
序号
恶意代码ID
威胁标识
文件
准备就绪
扫描文件数：
威胁数：
扫描时间：
立即检测
停止
一键清理

3. 基础功能

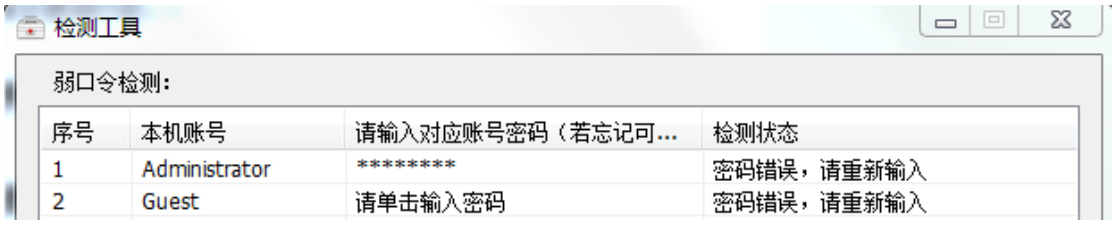
3.1 弱口令检测

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。

3.2 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。