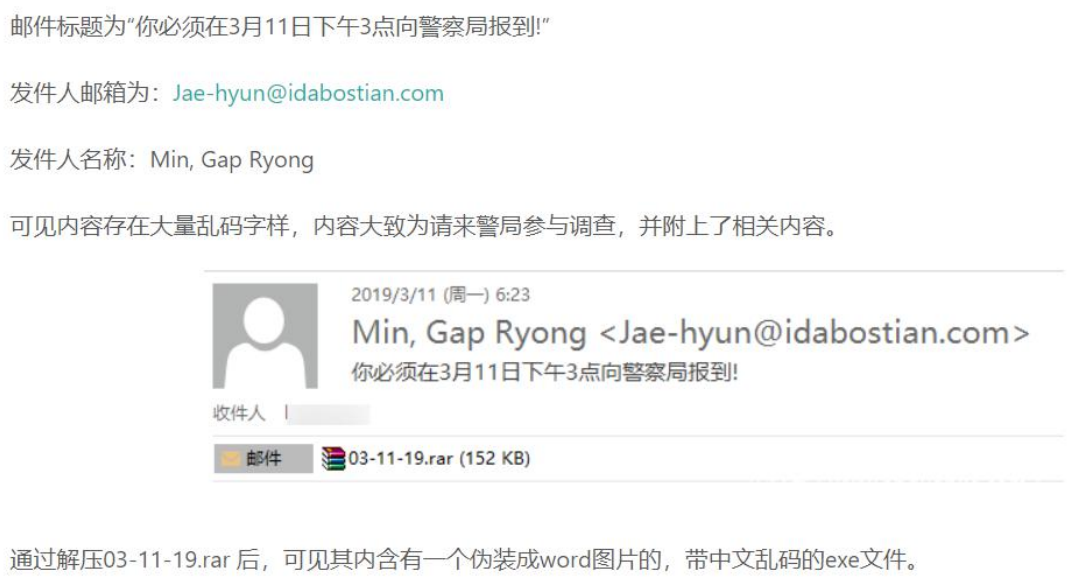
GandCrab V5.2 病毒安全防范工作的提醒

据国家网络与信息安全信息通报中心监测发现，2019年3月11日起,境外某黑客组织对我国有关政府部门开展勒索病毒邮件攻击。邮件主题为“你必须在3月11日下午3点向警察局报到！”，发件人名为“Min，GapRyong”，邮件附件名为“03-11-19.rar”。如下图所例示：



经分析研判，该勒索病毒版本号为GandCrabV5.2，是2019年2月最新升级的勒索病毒版本，运行后将对用户主机硬盘数据全盘加密,并让受害用户访问网址下载Tor浏览器，随后通过Tor浏览器登录攻击者的数字货币支付窗口，要求受害用户缴纳赎金。

此勒索病毒的传播感染方式多种多样,使用的技术也不断升级。电脑一旦被感染，病毒会对磁盘内的文件进行加密

并提示支付赎金进行解密。由于病毒使用高强度算法进行加密，目前业内暂无解密和恢复文件的办法。目前已知的传播方式如下：

1、定向鱼叉攻击邮件投放

2、垃圾邮件批量投放传播

3、网页挂马攻击

4、利用 CVE-2019-7238(Nexus Repository Manager 3 远程代码执行漏洞)进行传播

5、利用 weblogic 漏洞进行传播

6、利用自动化机制病毒进行传播

传播方式包括:

a)通过 RDP、VNC 等途径进行爆破并入侵

b)利用 U 盘、移动硬盘等移动介质进行传播

c)捆绑、隐藏在一些破解、激活、游戏工具中进行传播

d)感染 Web/FTP 服务器目录并进行传播

主要传播端口为： 445、135、139 、3389、5900 等端口

GandCrab V5.2 勒索病毒目前已经感染了数千台中国电脑，接下来还将通过 RDP 和 VNC 扩展攻击影响中国更多的电脑。该病毒目前主要是通过邮件形式攻击，请提高警惕不要随意打开不明邮件，具体防范措施如下：

1、不要打开陌生人或来历不明的邮件；

2、尽量不要点击 office 宏运行提示，避免来自 office 组件的病毒感染；

3、需要的软件从正规（官网）途径下载，不要双击打开.js、.vbs 等后缀名文件；

4、 及时安装主流杀毒软件，升级病毒库，对相关系统进行全面扫描查杀；

5、在 Windows 中禁用 U 盘的自动运行功能；

6、及时升级操作系统安全补丁，升级 Web、数据库等服务程序，防止病毒利用漏洞传播；

7、尽量关闭不必要的端口，如 445、135、139 等，对 3389、5900 等端口可进行白名单配置，只允许白名单内的 IP 连接登陆；

8、相关服务器采用高强度的密码，避免使用弱口令密码，并定期更换密码。有条件的客户应部署应用防火墙或者漏洞扫描设备，及时发现和阻止通过漏洞进行的攻击；

9、尽快备份数据并定期进行媒介（独立存储设备）或者异地备份；

10、对已感染主机或服务器采取断网措施，防止病毒扩散蔓延，并找可靠的数据恢复公司解密。

安徽龙讯信息科技有限公司

2019 年 4 月