三零卫士紧急安全公告

新型变种勒索病毒 GlobeImposter

上海三零卫士信息安全有限公司

2018 年 11 月 20 日

漏洞概述

工作发现，近期国内多家大型企业遭到新型变种勒索病毒 GlobeImposter 的攻击，导致受感染系统无法正常运行，日常工作难以开展。

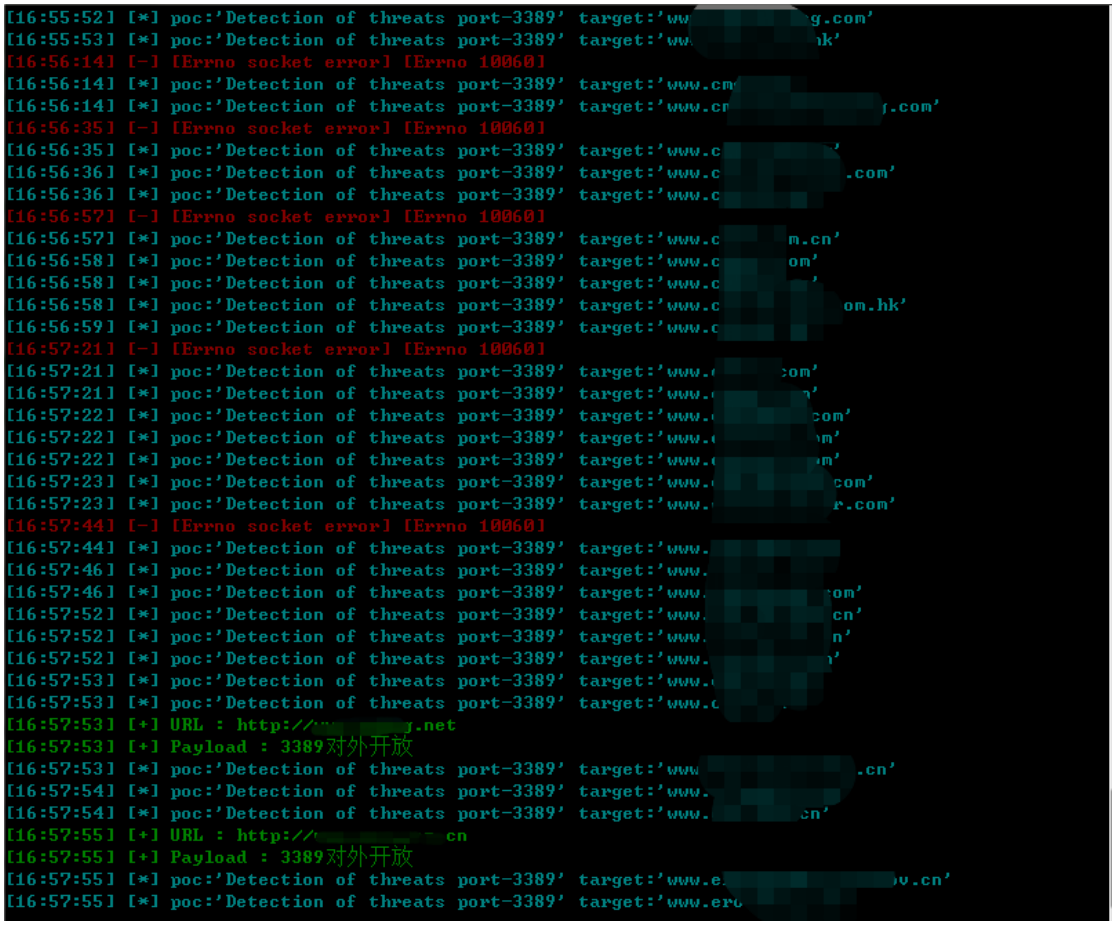
该漏洞为 GlobeImposter 家族的新型变种，且威胁级别为高危，三零卫士 STeam 团队已高度关注，并对 soc 平台中所有边界资产进行漏洞检测，结果显示仍然存在部分客户网站对外开启了远程桌面服务，存在安全威胁。故三零卫士发布此通告提醒用户和企业采取必要防御和应对措施，并对自身所有资产进行针对性自检。该漏洞 STeam 将持续跟进。

漏洞详情

GlobeImposter 勒索病毒是一种新型变种勒索病毒，主要以 Windows 远程桌面服务密码暴力破解的手段来突破边界防御。黑客组织会对开启了远程桌面服务的服务器进行筛选，选取高价值目标服务器后利用密码抓取工具获取管理员密码，并人工投放勒索病毒。勒索病毒利用各种非对称加密算法对服务器文件进行加密，被加密文件后缀名为*.RESERVE，被感染者一般无法解密，必须拿到解密的私钥才有可能破解。病毒文件一旦进入本地，就会自动运行，并在内网横向扩散，寻找加密对象，文件一旦加密完成，就无法被正常打开使用，进而导致服务器无法正常工作，信息系统或局域网络瘫痪必须缴纳所谓“赎金”方可解密。

漏洞检测

检测中发现仍然存在部分客户网站对外开启了远程桌面服务，如下图所示：



风险等级

高危

影响范围

部分使用微软 Office 的公式编辑器工具或部分对外开启远程桌面服务的服务器。

修复方法

1、 对外关闭 RDP 远程桌面协议(3389）、SSH（22）、telnet（21）等危险端口；

2、 及时更新系统补丁，修复漏洞；

3、 安装专业的终端/服务器安全防护软件并及时更新病毒库；

4、 对重要的数据文件定期进行非本地备份；

5、 不要点击来源不明的邮件以及附件。

如您遇到任何安全方面问题可以来电联系我们，三零卫士将尽全力为您解决！

地址：上海市徐汇区宜山路 810 号 11 楼

网址：http://www.30wish.net

邮件：30services@30wish.net

传真：021-54363095

热线：800-820-5530(400-820-5530)

或下述地区

上海请拨打：021-55313030

北京请拨打：010-57533163

广州请拨打：020-38288430

成都请拨打：028-86082220

杭州请拨打：0571-87203030 28913098

南京请拨打：025-86222703

武汉请拨打：027-88612165