|  |
| --- |
| logo_top |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | **病毒情报中心** |  | **系统漏洞信息** | | 一周病毒情况报告 亚信安全热门病毒综述- Backdoor.Perl.SHELLBOT.AB |  | KB4507457 | | **系统安全技巧** |  | **亚信安全产品** | | GlobeImposter勒索病毒变种预警 |  | 病毒码发布情况 | |  |  |  | | | | |  | 一周病毒情况报告 |  | | **本周用户报告感染数量较多的病毒列表** | | | |  | TROJ\_EQUATED家族 | | |  | | | |  | 亚信安全热门病毒综述 |  | | **亚信安全热门病毒综述-** **Backdoor.Perl.SHELLBOT.AB**  该后门与挖矿程序捆绑在一起，通过僵尸网络传播，其连接到IRC服务器，并连接到如下网址下载恶意程序：  http://{BLOCKED}.{BLOCKED}.70.249/.x15cache。 | | | |  |  | | |  | 对该病毒的防护可以从下述链接中获取最新版本的病毒码：15.247.60 | | |  | <http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/Pattern/> | | |  | 病毒详细信息请查询： | | |  | https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/backdoor.perl.shellbot.ab | | |  | | | |  | 系统漏洞信息 |  |  |  | | --- | | **Windows安全更新 (4507457)**  Windows Server 2012 R2  Windows 8.1 for 32-bit systems  Windows 8.1 for x64-based systems |  |  |  |  | | --- | --- | --- | | **描述：**<https://portal.msrc.microsoft.com/zh-cn/security-guidance> | | | |  | | | |  | 亚信安全产品 |  | | **病毒码发布情况** | | | | **亚信安全在最近一周发布中国区病毒码情况如下：** | | | |  | 2019年07月15日发布病毒码15.231.60 2019年07月16日发布病毒码15.235.60 2019年07月17日发布病毒码15.237.60. 2019年07月18日发布病毒码15.239.60 2019年07月19日发布病毒码15.241.60 | | | 截至目前，病毒码的最高版本为15.247.60发布于2019年07月22日。 | | | |  | 病毒码下载地址为： | | |  | <http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/Pattern/> | | |  | 您也可以从以下链接下载TSUT工具进行趋势科技Windows平台产品的更新： | | |  | <http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/TSUT/> | | |  | | | | **趋势科技在最近一周发布全球病毒码情况如下：** | | | |  | 2019年07月15日发布病毒码15.235.00 2019年07月16日发布病毒码15.237.00 2019年07月17日发布病毒码15.239.00 2019年07月18日发布病毒码15.241.00 2019年07月19日发布病毒码15.243.00 | | | 截至目前，病毒码的最高版本为15.249.00，发布于2019年07月22日。 | | | |  | 病毒码下载地址为： | | |  | <http://support.asiainfo-sec.com/Anti-Virus/Main-Pattern/> | | |  | 您也可以从以下链接下载TSUT工具进行趋势科技Windows平台产品的更新： | | |  | <http://support.asiainfo-sec.com/Anti-Virus/TSUT/> | | |  |  | | |  | | | |  | 系统安全技巧 |  | | 近日，亚信安全截获Globelmposter勒索病毒最新变种，该勒索病毒首次出现在2017年5月，到目前为止已经更新过多个版本。2018年亚信安全曾经多次发布该病毒预警，在过去的版本中，该病毒曾使用十二生肖英文名+数字的方式命名加密文件后缀（如：Rabbit666、Dragon666）。本次变种与之前不同之处在于加密文件后缀改用古希腊十二神的英文名+数字的方式进行命名（如：Ares666，Hermes666）：    古希腊十二神的英文名：    其传播方式与以往版本类似，黑客通过入侵企业内网利用RDP/SMB暴力破解在内网扩散，投放此勒索病毒，在进入内网后通过多种方法获取登录凭证并在内网横向渗透传播。亚信安全将其命名为Ransom.Win32.FAKEGLOBE.MRY。  **攻击流程**    **病毒技术细节分析**  病毒首先会提升运行权限    修改注册表，添加启动项以及进行常规的本地持久化操作    通过调用CMD命令，停止常见的数据库服务    避免加密如下文件以及带有如下扩展名的文件    遍历系统上的磁盘，加密磁盘上的文件    通过删除注册表和Windows日志管理工具的方式进行删除日志，卷影和远程桌面登录等信息操作    调用命令删除自己    加密完成后，其会生成勒索赎金文件：    **解决方案**   * 不要点击来源不明的邮件以及附件； * 及时升级系统，打全系统补丁； * 尽量关闭不必要的文件共享权限和不必要的端口； * 采用高强度的密码，避免使用弱口令密码，并定期更换密码； * 请注意备份重要文档。备份的最佳做法是采取3-2-1规则，即至少做三个副本，用两种不同格式保存，并将副本放在异地存储。   **亚信安全解决方案：**   * 亚信安全病毒码版本15.225.60 ，云病毒码版本15.225.71，全球码版本15.225.00已经可以检测，请用户及时升级病毒码版本； * 使用防毒墙网络版(OfficeScan)开启针对勒索软件（Ransomware）的行为阻止策略，可以有效拦截勒索病毒对系统中的文件进行加密，设置如下图： | | | |  | | | |  | | | |  |  |  | | 详情可登陆亚信安全官网[www.asiainfo-sec.com](http://www.asiainfo-sec.com)或拨打免费咨询热线800-820-8876 | | | |