|  |
| --- |
| 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- Trojan.PS1.POWLOAD.JKP |  | KB4538461 | | 病毒通告 |  | **亚信安全产品** | | 新型勒索病毒NEFILIM通告 |  | 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-Trojan.PS1.POWLOAD.JKP**  该病毒通过垃圾邮件传播，其使用意大利语，邮件主题则与新冠肺炎相关，诱导用户点击。其会窃取用户信息，链接恶意网站。 | | | |  | 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：15.771.60. | | |  | <http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/Pattern/> | | |  | 系统漏洞信息 |  |  |  | | --- | | **Windows安全更新 (**4538461**)**  Windows 10 Version 1903 for 32-bit Systems Windows 10 Version 1903 for x64-based Systems  Windows Server, version 1903 (Server Core installation)  Windows Server, version 1909 (Server Core installation) |  |  |  |  | | --- | --- | --- | | **描述：**<https://portal.msrc.microsoft.com/zh-cn/security-guidance> | | | |  | 亚信安全产品 |  | | **病毒码发布情况** | | | |  | 2020年03月23日发布病毒码15.757.60  2020年03月24日发布病毒码15.759.60 2020年03月25日发布病毒码15.761.60  2020年03月26日发布病毒码15.763.60 2020年03月27日发布病毒码15.765.60 | | | 截至目前，病毒码的最高版本为15.771.60.发布于2020年03月30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：** | | | |  | 2020年03月23日发布病毒码15.759.00 2020年03月24日发布病毒码15.761.00 2020年03月25日发布病毒码15.763.00 2020年03月26日发布病毒码15.765.00 2020年03月27日发布病毒码15.767.00 | | | 截至目前，病毒码的最高版本为15.773.00，发布于2020年03月30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，亚信安全截获新型勒索病毒NEFILIM，其威胁受害者，如果不支付赎金，将会公布窃取到的受害者数据信息。该病毒遍历磁盘，对磁盘中的文件进行加密，并为加密后的文件名添加NEFILIM后缀。病毒加密完成后，调用cmd命令进行自我删除，亚 信 安 全 将 其 命 名Ransom.Win32.NEFILIM.A。  **攻击流程**  捕获19  **详细分析**  病毒首先创建互斥体“Den'gi plyvut v karmany rekoy. My khodim po krayu nozha...”，防止病毒程序多次运行：  捕获5  创建并生成rsa公钥，为后续加密文件做准备：  捕获6  设置白名单，避免加密以下文件，保证电脑系统运行正常：  捕获10  避免加密以下路径中的文件：   * C:/Appdata * C:/Program files * C:/Program files(x86) * C:/Microsoft * C:/sophos   同时避免加密特定的扩展名文件，如系统文件、NEFILIM.txt 勒索文档等：   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | exe | log | cab | cmd | mp3 | NEFILIM-DECRYPT.txt | | ini | Dll | url | ttf | cpl | com | | NEFILIM | mp4 | msi | lnk | pif |  |   捕获11  病毒接下来获得可用的磁盘，遍历磁盘：  捕获8  从根目录开始对文件加密，通过分析hkey生成过程，我们发现其使用RSA算法加密文件：  捕获17  加密完成后，病毒在加密的文件名后添加.NEFILIM 后缀：  捕获22    病毒创建勒索提示文件NEFILIM-DECRYPT.txt：  捕获14  捕获12  完成上述操作后，病毒创建带有隐藏窗口的进程，利用cmd命令进行自我删除：  捕获9  **解决方案**   * 不要点击来源不明的邮件以及附件； * 不要点击来源不明的邮件中包含的链接； * 采用高强度的密码，避免使用弱口令密码，并定期更换密码； * 打开系统自动更新，并检测更新进行安装； * 尽量关闭不必要的文件共享； * 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15.759.60，云病毒码版本15.759.71，全球码版本15.759.00 已经可以检测，请用户及时升级病毒码版本。 | | | |  |  |  | | 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 | | | |