|  |
| --- |
| 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.Win32.CARBANAK.A |   | KB4493467 |
| **系统安全技巧** |   | **亚信安全产品** |
| “侠盗”勒索病毒（GANDCRAB V5.3）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** |
|  | ALS\_BURSTED家族 |
|  |
|   | 亚信安全热门病毒综述 |   |
| **亚信安全热门病毒综述-** **Backdoor.Win32.CARBANAK.A** |
|  | 该病毒由其它恶意软件生成或者用户访问恶意网站不经意下载感染本机，其会监听443端口，利用如下漏洞:* CVE-2013-3660
* CVE-2013-5065
* CVE-2014-4113
 |
|  | 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：14.965.60 |
|   | <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.win32.carbanak.a |
|   |
|  | 系统漏洞信息 |   |

|  |
| --- |
| **Windows安全更新 (4493467)**Windows Server 2012 R2Windows 8.1 for 32-bit systemsWindows 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04月22日发布病毒码14.951.602019年04月23日发布病毒码14.953.602019年04月24日发布病毒码14.955.602019年04月25日发布病毒码14.957.602019年04月26日发布病毒码14.959.60 |
| 截至目前，病毒码的最高版本为14.965.60发布于2019年04月29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04月22日发布病毒码14.953.002019年04月23日发布病毒码14.955.002019年04月24日发布病毒码14.957.002019年04月25日发布病毒码14.959.002019年04月26日发布病毒码14.961.00 |
| 截至目前，病毒码的最高版本为14.967.00，发布于2019年04月29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，亚信安全截获最新“侠盗”勒索病毒（GANDCRAB）5.3版本，该版本与之前的5.2版本无明显差异，不同之处在于其缴纳赎金方式，攻击者将暗网缴纳赎金方式改为通过邮件联系缴纳赎金。亚信安全将其命名为Ransom.Win32.GANDCRAB.SMILC。GANDCRAB 勒索病毒是目前我国境内最为活跃的勒索病毒之一，该病毒经历了多次更新，亚信安全网络监测实验室也曾多次发过该勒索病毒的预警信息，其主要传播方式：* 垃圾邮件传播；
* 网页挂马攻击；
* RDP和VNC爆破入侵；
* U盘、移动硬盘传播；
* 捆绑、隐藏在一些破解、激活、游戏工具中传播；
* 感染Web/FTP服务器目录传播；

【GANDCRAB V5.3 勒索信息】【GANDCRAB V5.2勒索信息】GANDCRAB V5.3放行的国家与5.2版本相比较，没有变化，其白名单如下：

|  |  |
| --- | --- |
| 419(LANG\_RUSSIAN俄罗斯)  | 422(LANG\_UKRAINIAN乌克兰) |
| 423(LANG\_BELARUSIAN白俄罗斯) | 428(LANG\_TAJIK塔吉克) |
| 42B(LANG\_ARMENIAN亚美尼亚) | 42C(阿塞拜疆，拉丁美洲) |
| 437(LANG\_GEORGIAN格鲁吉亚) | 43F(LANG\_KAZAK哈萨克) |
| 440(LANG\_KYRGYZ吉尔吉斯) | 442(LANG\_TURKMEN土库曼) |
| 443(乌兹别克斯坦，拉丁语) | 444(LANG\_TATAR鞑靼斯坦) |
| 82C(LANG\_AZERI阿塞拜疆，西里尔) | 843(LANG\_UZBEK乌兹别克) |

**解决方案*** 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；
* 尽量关闭不必要的文件共享；
* 采用高强度的密码，避免使用弱口令密码，并定期更换密码；
* 不要点击来源不明的邮件以及附件；
* 浏览网页时不下载运行可疑程序；
* 及时更新系统，更新应用程序；打全系统及应用程序补丁程序；
* 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14.957.60，云病毒码版本14.957.71，全球码版本14.959.00已经可以检测，请用户及时升级病毒码版本。

**总结**GANDCRAB勒索病毒并不是一只新型病毒，其首次出现在去年1月份，因其不断的变种，一直活跃至今，备受关注。亚信安全提醒广大用户，不仅要预防新型病毒，还要时刻警惕老病毒新变种，做好勒索病毒防护工作。 |
|  |
|  |  |  |
| 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 |

 |