|  |
| --- |
| 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- Worm.Win32.BLASQUI.A |  | KB4503269 | | **系统安全技巧** |  | **亚信安全产品** | | 利用CVE-2019-2725漏洞和证书混淆传播的挖矿病毒预警 |  | 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-** **Worm.Win32.BLASQUI.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，该病毒试图对SQLservers进行暴力破解，其还利用了如下漏洞：   * EternalBlue CVE-MS17-010 * DoublePulsar * ThinkPHP Exploit * ApacheTomcat CVE-2017-12615 * CVE-2017-8464 * CVE-2014-6287 | | |  | 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：15.177.60 | | |  | <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/worm.win32.blasqui.a | | |  | | | |  | 系统漏洞信息 |  |  |  | | --- | | **Windows安全更新 (4503269)**  Windows Server 2008 R2 for x64-based Systems Service Pack 1  Windows 7 for x64-based Systems Service Pack 1  Windows 7 for 32-bit Systems Service Pack 1 |  |  |  |  | | --- | --- | --- | | **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06月10日发布病毒码15.159.60 2019年06月11日发布病毒码15.163.60 2019年06月12日发布病毒码15.169.60 2019年06月13日发布病毒码15.173.60 2019年06月14日发布病毒码15.175.60 | | | 截至目前，病毒码的最高版本为15.177.60发布于2019年06月17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06月10日发布病毒码15.163.00 2019年06月11日发布病毒码15.165.00 2019年06月12日发布病毒码15.167.00 2019年06月13日发布病毒码15.169.00 2019年06月14日发布病毒码15.171.00 | | | 截至目前，病毒码的最高版本为15.179.00，发布于2019年06月17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，亚信安全截获新型挖矿病毒，该病毒利用了Oracle WebLogic Server的反序列化漏洞（CVE-2019-2725）进行传播，该漏洞曾经用于传播Sodinokibi勒索病毒。除了漏洞利用外，该病毒还使用了新型传播手段，将恶意代码隐藏在证书里，达到躲避杀毒软件检测的目的。亚信安全将该病毒命名为Coinminer.Win32.MALXMR.TIAOODCJ。  攻击流程    **详细分析**  病毒感染系统后，首先利用CVE-2019-2725漏洞执行如下命令    上述命令主要是利用PowerShell执行一系列恶意行为：   * 从远端C&C服务器下载证书文件cert.cer，并将该文件保存在%APPDATA%目录下（亚信安全将其命名为Coinminer.Win32.MALXMR.TIAOODCJ.component）； * 使用管理Windows中的证书组件CertUtil来解码文件，并将解码的文件保存为%APPDATA%\ update.ps1   （亚信安全将其命名为Trojan.PS1.MALXMR.MPA）；   * 使用PowerShell执行update.ps1文件后，其会通过CMD命令删除下载的cert.cer文件。   当我们下载该证书时，发现其看起来像一个普通的PEM格式证书，如下图所示：  https://blog.trendmicro.com/trendlabs-security-intelligence/files/2019/06/CVE-2019-2725-certificate-2.png  然而我们使用base64解码该内容时发现，该证书并不是常用的X.509 TLS文件格式，而是PowerShell命令，如下图所示：    证书文件中的PowerShell命令会下载另外PowerShell脚本，并在内存中执行，该脚本主要功能也是下载并执行文件，其下载文件列表如下：    该病毒将包含已解码证书文件的update.ps1文件替换为新的update.ps1。然后创建一个计划任务，每30分钟执行一次新的update.ps1。  **解决方案**   * 利用系统防火墙高级设置阻止向445端口进行连接（该操作会影响使用445端口的服务）； * 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； * 打开系统自动更新，并检测更新进行安装。 * 升级WebLogic Server版本，打上CVE-2019-2725对应的补丁程序，参考链接： * https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html   **亚信安全解决方案**   * 亚信安全病毒码版本15.163.60 ，云病毒码版本15.163.71，全球码版本15.165.00已经可以检测，请用户及时升级病毒码版本。 * 亚信安全DS DPI开启以下规则拦截该漏洞：   1009707-Oracle Weblogic Server Remote Code Execution Vulnerability (CVE-2019-2725)   * 亚信安全深度发现设备TDA 检测规则如下：   2903 : HTTP\_POSSIBLE\_ORACLE\_WEBLOGIC\_EXPLOIT | | | |  | | | |  | | | |  |  |  | | 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 | | | |