

# 互联网网络安全信息通报

2012 年第 2 期 ( 总第 120 期 )

国家互联网应急中心 ( CNCERT )

2012 年 02 月 03 日

## 关于一些汉化版 SSH 管理软件存在后门导致 用户信息泄露的情况通报

近日，互联网上披露了 Putty、WinSCP 等 SSH 管理软件中文版本（另称汉化版）存在后门程序导致用户信息泄露的事件情况。依托中国反网络病毒联盟（简称 ANVA），国家互联网应急中心（CNCERT）组织知道创宇公司、金山公司、奇虎 360 公司等 ANVA 成员单位对事件进行了跟踪分析，相关情况汇总通报如下：

### 一、事件演进情况

互联网上最早出现事件讨论是在 1 月 25 日新浪微博用户发布的博文中。至 1 月 30 日、31 日，网络安全企业、相关博客论坛以及业内人士等纷纷披露并确认后门程序存在的情况，同时还披露了黑客通过后门程序窃取大量 SSH 管理软件用户信息系统相关的账号和口令信息、存储在后门程序服务器的情况。随后，由于黑客的后门程序服务器存在 SQL 注入漏洞以及目录权限漏洞，导致其存储的窃取信息被更多的人获得。

## 二、事件情况分析

至 2 月 2 日，ANVA 成员单位通过公开渠道获得的存在后门程序的 SSH 管理软件样本涉及 Putty、Winscp、SSHSecure、Psftp 等多款软件产品中文版本，主要来源于 putty.org.cn、putty.ws、winscp.cc 和 sshsecure.com 等站点提供的下载点，而对应的非中文版本未发现存在后门程序。分析结果表明，黑客植入的后门程序具备记录用户输入和通讯、发送记录信息至指定服务器的功能。目前，暂未发现后门程序常驻系统内存或文件系统的情况，窃取信息行为发生在使用 SSH 管理软件过程中。

值得注意的是，黑客用作窃取信息管理的后门程序服务器域名为 1.ip-163.com。经验证，1.ip-163.com 与 www.putty.org.cn (Putty 中文站) 位于同一 IP 服务器。至 2 月 2 日，后门程序服务器和 Putty 中文站已经不可访问。

ANVA 成员单位获得了记录窃取信息相关的多个数据文件，共得到 27261 条记信息记录。这些记录包含受害信息系统 IP 或域名、连接账号、连接密码、连接时间、通讯端口、对应 SSH 管理软件产品等信息，可直接用于发起指定信息系统主机的攻击，获得系统管理权限。根据知道创宇公司提供的信息，去除无效、重复信息后，得到受害信息系统 IP 或域名共 1512 个，当中涉及 64 个政府网站域名 (.gov.cn)。此外，统计得到受害用户使用的 SSH 管理软件的分布情况如

下图所示，使用 Putty 和 Winscp 的受害用户占大部分。

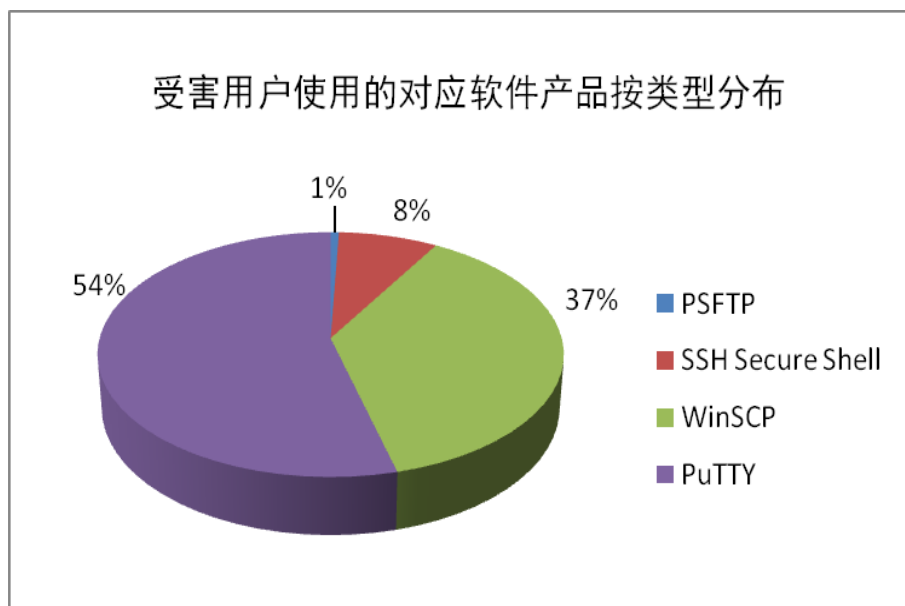


图 受害用户使用的对应软件产品按类型分布（来源：知道创宇公司）

### 三、应对措施建议

鉴于 SSH 管理软件应用广泛，且有可能出现后门程序窃取的信息被恶意传播或用于地下交易的情况，将严重威胁到用户信息系统的安全，CNCERT 提出如下应对建议：

（一）建议国家有关部门积极介入事件的调查，严惩造成严重危害或造成恶劣影响的行为。建议互联网行业主管部门加强对软件下载站特别是开源软件下载站的安全监管，对传播恶意代码、危害用户利益和行业秩序的的进行严厉打击。

（二）涉事厂商应及时发布安全公告，积极做好用户的应急处置工作。此前也出现过一些应用广泛的操作系统软件、应用软件官方下载文件特别是一些重新编译或汉化的开源软件被植入后门的情况，对开源软件的推广应用造成了负面影响。相关生产者（厂商）应以此为鉴，严格自律，同时

要加强下载站的安全管理。

（三）建议使用了上述 SSH 管理软件产品的用户及时更换所管理信息系统的账号和口令，同时对系统进行安全审计，以免被黑客控制。同时，提醒广大用户注意软件应用安全问题，注意加强主机的安全防护，对下载文件进行查杀，更不要去下载来源不明的软件。

（四）呼吁掌握后门程序服务器存储数据信息的安全企业、业内人士不再擅自传播相关信息，以免造成更严重的后果。同时，呼吁安全企业加强技术分析和跟踪，在终端防护产品中加强对此类后门程序的识别查杀力度。

CNCERT 将继续跟踪事件后续情况，如需技术支持，请联系 CNCERT。电子邮箱：[cncert@cert.org.cn](mailto:cncert@cert.org.cn)，联系电话：010-82990286。

---

报：工业和信息化部通信保障局

送：工业和信息化部信息中心

抄：互联网网络安全信息通报成员单位、中国反网络病毒联盟成员单位

---