深度报道：黑客开始瞄上Linux发起攻击事件

http://www.sina.com.cn 2003年12月11日 08:40 ZDNet China

ZDNet China 12月11日 专稿(记者RobertLemos)：最近连续发生数起攻击自由开放源代码软件服务器事件，使得开发人员不得不谨慎应对这种最新局势。

过去四月来，不明入侵者接连攻破Linux核心开发小组、Debian Project、Gentoo LinuxProject与GNUProject等专门放置程序与源代码的服务器。GNUProject更是管理许多Linux与其他类Unix系统所使用的重要程序开发。接二连三的攻击事件也让这些专案领导人纷纷 回头查看自己的安全。

“这批主要针对开放源代码服务器与核心开放源代码开发服务器的攻击的确引人侧目。”负责GentooLinux源代码扩散系统的成员CoreyShields表示。“大家担心的是有人意图不轨，刻意变更核心软件，那使用者用到的都是被动过手脚的产品。”

虽然微软的Windows向来是黑客主要瞄准对象，但在开放源代码模式逐渐成为气候之后，现在也成了攻击者觊觎的对象。LinuxOS与其他开放源代码应用越来越热门，黑客兴趣也跟着大增。即使自认为已经做好相关安全措施的开发人员现在也不禁开始担心这种趋势。

“大家都不希望自己是下一个受害者，必须跑在黑客之前做好保护措施才行。”SambaProject(可兼容于Windows网络的热门开放源代码文件服务器计划)共同创始人暨开发人员JeremyAllison表示。

一连四起

12月1日，专门提供Gentoo源代码下载的一台服务器(总数105台)遭入侵，所幸主要的源代码数据库并没有遭到威胁。遭入侵的服务器上所安装的安全软件立即侦测到这种攻击，并做了完整的纪录。

在此之前，11月份的一起攻击则瞄准Linux核心(kernel)，此次是一位开发人员的系统被入侵用来当作攻击踏板，该入侵者利用被入侵的电脑来发送源代码给另一台服务器，若有人安装该源代码，便可能遭到攻击者取得系统权限。该起攻击事件在24小时便被侦测到。

其他攻击事件则更为严重。入侵者取得进入GNUProject开发系统Savannah的权限；另一起事件中，四台用来管理Debian版本开发与社群作为的DebianProject服务器也被取得完整权限。

两起攻击行径都相当类似：入侵者先取得合法的使用者登入帐号密码，再利用一个最近被发现的Linux核心漏洞取得系统所有人的权限。Debian与GNU计划领导人目前先把系统下线，开发人员全都无法存取，直至确定安全无虞后才会再开放。

GNU Project表示最近这起攻击事件，加上稍早三月FTP服务器被侵入事件，导致领导阶层开始做些改变以为应对。

新增数字签名

“我们预期在Savannah事件后会采取一些行动，”自由软件基金会法律长EbenMoglen表示，该基金会负责GNUProject，专门提供Unix与Linux系统专用的自由软件。这些行动包括，专案领导人会强迫开发人员在所有贡献的源代码中做数字签名程序，同时也会在公开给大众的开放源代码维护系统中新增额外的功能，在接受任何变更前会先检查开发人员的数字签名。

“我们认为新增数字签名是最有效的办法，可确保我们接受源代码的完整性。”Moglen表示。

GNUProject将自己所提供的程序称为自由(free)软件，因为这些程序在扩散时都得受GNU公共授权书约束，它允许大家变更并自行重新散播软件，但前提是变更过的源代码也必须一起扩散出来。其概念是希望借由大众的共同参与来自由共享、改善、使用软件。

但批评者认为，这样的软件开发模式也必须付出看不见的代价。微软信息安全总经理GregWood表示，“用在商业流程上，开放源代码有其代价，企业必须自行做好安全检查，所有流程建立也必须自行负担。”

微软也有自己的问题。例如，在2000年十月，入侵者便通过某位开发人员的电脑取得微软网络的使用权限。自此之后，微软发起信赖运算计划(TrustworthyComputing)，力图保护软件与开发流程的安全性。

开发人员指出，最近几起攻击事件虽然导致不肖份子取得部分电脑的权限，但对于开发部分并不受影响，因为这些计划已经采取相关的安全措施作为回应。

“最近几次入侵事件都能很被快发现，主因是主网站多半没有对外开放，入侵者若在第二层网站进行变更就会被数个安全机制察觉到，”Linux核心使创者以及现行维护者LinusTorvalds表示。

Torvalds多次改变安全策略。早期还在芬兰赫尔辛基大学念书时，他将Linux核心版本放在一台可通过校园网络存取的机器上。现在，Linux核心服务器则由多道防火墙保护着，并通过SSH加密通讯与加密签名来确保完整性。

Torvadls现在所使用的开放源代码核心维护应用是由BitMore所研发，该公司创始人LarryMcVoy强调，每个计划都应该使用这类签名(或称checksums)来确保开放源代码没有被乱改。

“若你的信息没经过checksum检验，你觉得不会有事，那你就是在自找麻烦。”McVoy说。

包括Debian Project、GentooLinux、SambaProject都已开始采用外部checksums来检验文件是否在遭受入侵期间被动过手脚。MandrakeSoft创始人GaelDuval表示，这类技术让专案维护工作轻松不少。

“安全问题不是始于今日，解决方案也早已存在市场，”Duval说。“最重要的是系统管理员与用户必须重视安全性。”

不怕被动手脚 只怕小虫

不过Apache软件基金会的开发人员JustinErenkrantz则表示开放源代码的开发模式其实让安全问题减轻不少，由于开发属于分散式模式，因此还有其他许多信息储存器(repository)可用来查看主服务器内的源代码是否完整。

“若apache.org遭到入侵，我们可查看每个开发人员都能与信息储存器同步化，没有被加入恶意源代码。”Erenkrantz表示。

Torvalds也同意这种看法，他表示若核心开发主服务器遭入侵，开放源代码社群还是有其他检验平衡措施可做补救。

“最重要的是，最后总会被查出来，”Torvalds说，“核心源代码不断被复制，我们总是找得出哪里被偷放了不该放的程序。”

Torvalds认为，一些简单的错误反而比恶意攻击者来得可怕。

“我个人比较担心一些常见的臭虫，”Torvalds表示，“大部分被发现的核心漏洞都是一些很愚蠢的小虫，就像Debian被咬到的那只，而非什么特别厉害的黑客在干坏事。”(陈?璁)