网络安全监测工作动态

2018 第 4 期（总第 4 期）

陕西省网络与信息安全测评中心　　6 月 1 日-6 月 30 日

本月，陕西省网络与信息安全测评中心（以下简称“测评中心”）对受委托的 257 个政府网站进行了安全监测，共发现无法正常访问的政府网站 5 个，被恶意篡改的政府网站 10 个，存在严重高危漏洞的政府网站 59 个。从安全防御情况来看，目前针对我省政府网站的境外攻击主要来自于美国、俄罗斯、日本、保加利亚等国家和地区，占攻击总数的 11.2%，攻击手法主要为 CC 攻击、恶意扫描、Webse11 等。

一、安全监测情况分析

（一）可用性监测情况

共监测发现 5 个网站存在无法访问情况，主要集中在各市级政府网站，主要原因有：网站域名解析错误；网站程序设计不合理，有过度消耗主机资源的操作发生；网站存在安全隐患，被他人恶意攻击等。

（二）安全事件监测情况

共监测发现 10 个网站被恶意篡改，主要集中在市级政府部门网站，篡改主要分为页面篡改和暗链两种形式，其中 9 个网站被黑客攻击，将网站页面指向博彩网站；1 个网站被黑客插入了隐形恶意链接，链接类型主要为广告、博彩等。

（三）安全漏洞检测情况

共发现 59 个网站存在高危漏洞，高危漏洞数量 90 个。主要集中在市级以下政府、事业单位网站，漏洞类型主要为 XSS 攻击、SQL 注入、OpenSSL POODLE、后门、弱口令、信息泄露等。

二、安全防御情况分析

（一）攻击源分析

经分析统计，网站攻击的 IP 总数为 7053 个，其中，境外 IP 数 789 个，境内 IP 数 6264 个。

从攻击源 IP 分布情况看，目前境外 IP 主要集中在美国、俄罗斯、日本、保加利亚等国家和地区（如图 1），境内 IP 主要集中在广东、浙江、江苏、上海、北京和陕西等（如图 2）。

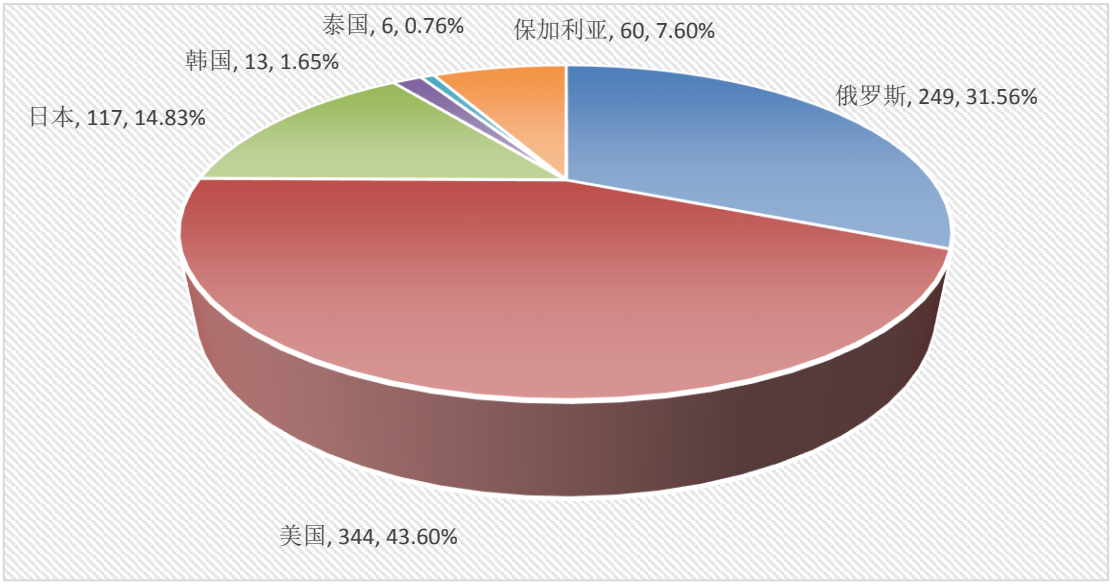

图 1 境外攻击源分布情况

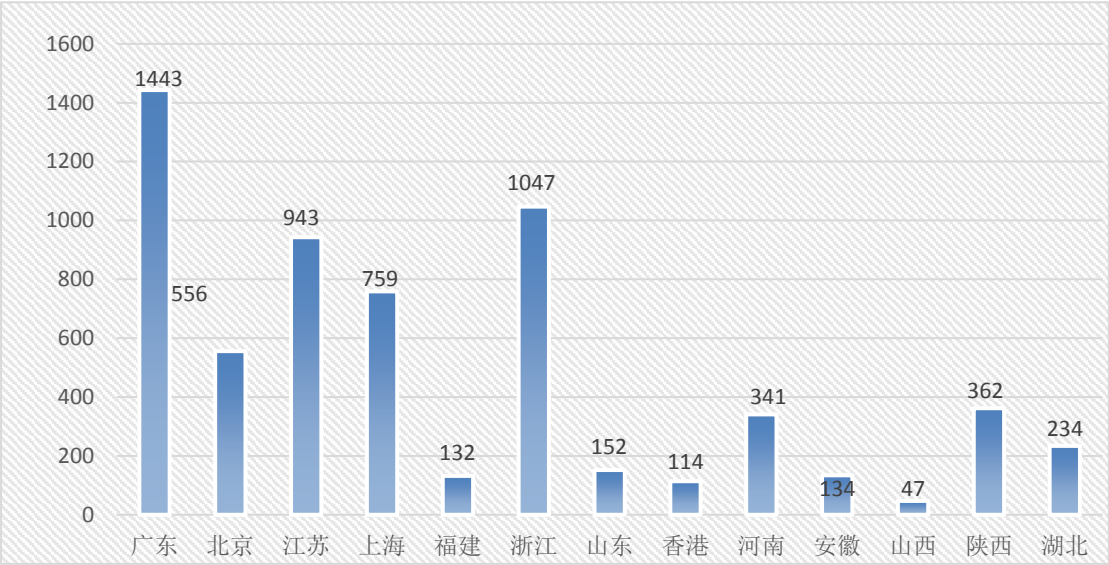

图 2 境内攻击源分布情况

（二）攻击类型分析

经分析统计，网站攻击最常见的攻击类型为 CC 攻击和恶意扫描，攻击者共发起了 65.5934 万次 CC 攻击和 41.4291 万次恶意扫描，所有攻击类型及数量的主要分布情况如图 3。

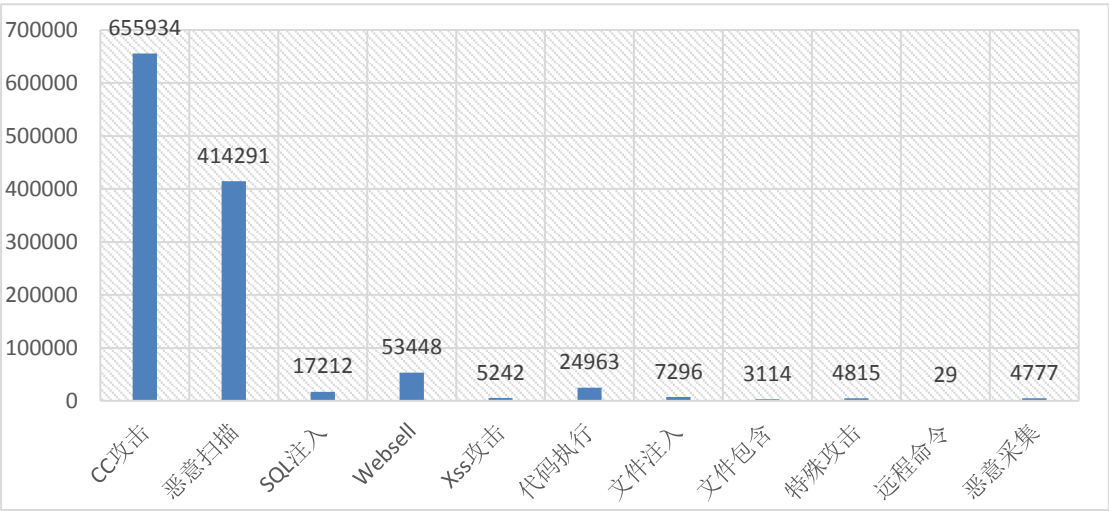

图 3 网站恶意攻击类型及数量分布

三、威胁播报

（一）英特尔芯片又现漏洞：数学运算单元可泄露密钥

英特尔 Core 及 Xeon 处理器上的安全漏洞可被利用来盗

取芯片上数学处理单元中的敏感数据。恶意软件或恶意用户能利用该设计缺陷偷取其他软件在芯片上执行的计算输入或计算结果。

利用存储在 FPU 寄存器中运算输入数据和结果数据，攻击者可推算出用于保护系统中数据的加密密钥。比如说，英特尔的 AES 加解密指令就用 FPU 寄存器存放密钥。

简言之，该安全漏洞可用于在特定情况下抽取或猜出其他程序中的加密密钥。

现代 Linux(2016 年发布的 4.9 内核及其后续内核版本)，包括 Server 2016 在内的最新 Windows，以及最新版的 OpenSD 和 DragonflyBSD，不受该漏洞影响(CVE-2018-3665)。

Windows Server 2008 需打补丁，其他受影响的微软系和非微软系内核的补丁正在研发过程中。Linux 内核团队正将缓解补丁应用到 4.9 之前的内核上。

总之，如果你的机器用了受影响的英特尔芯片，请关注相应补丁的发布情况。CVE-2018-3665 不是世界末日，恶意软件需得已经植入系统才可以利用该漏洞，且即便能够利用该漏洞，一次也就能取到一点点数据。

这是又一个复杂的推测执行相关处理器设计缺陷，对行业观察家来说很有看点，对某些内核程序员来说相当讨厌，对系统管理员和普通用户来说是又一个需要打补丁的东西。

比它更糟的漏洞不仅有，还有很多，Word 字处理程序、PDF 阅读器、Web 浏览器等等等等，一大堆。

懒惰的协处理器是漏洞利用产生的源头

该安全缺陷源于所谓的懒 FPU 状态恢复。操作系统内核只会在程序真正用到数学单元时才会存储和恢复浮点运算单元(FPU)寄存器。

然而，如今，通过英特尔芯片设计中与幽灵-熔断变种 3A 相关的安全漏洞，该特性却能使程序从 FPU 中获取到其他程序的上下文。变种 3A 能让应用程序读取本应只能由特权代码查看的寄存器内容。

修复措施就是应用现代 Linux、Windows 和其他内核使用的急 FPU 状态恢复机制。该缓解措施不会带来性能下降的影响，事实上，急切状态切换反而能提升性能。

英特尔定于 6 月 14 日凌晨 5 点后发布该漏洞更多信息。其原计划是在 6 月 27 日才公开，但 OpenBSD 和 DragonflyBSD 项目本周早些时候就推出了相应的补丁包，将问题摆上了台面。BSD 团队是在英特尔拒绝私下合作而选择与大型操作系统供应商共进退后，自行展开漏洞修复与披露行动的。

英特尔发言人表示，多名研究人员分别向这家占据芯片市场半壁江山的公司警示了该漏洞，包括亚马逊的研究人员:

这个被称为懒 FPU 状态恢复的问题与变种 3A 类似。操作系统和很多客户及数据中心产品中所用虚拟机管理程序

早已解决了该问题。我们的业界合作伙伴目前为剩下的受影响环境开发相应软件更新，未来几周更新即会上线。

我们一直信奉协同披露策略，感谢亚马逊德国的 Julian Stecklina、Cyberus Technology GmbH 的 Thomas Prescher、SYSGO AG 的 Zdenek Sojka 和 Colin Percival 向我们报告该问题。我们强烈建议业界其他人士遵从协同披露策略。

英特尔认为该威胁不算太严重。谷歌称其系统不受懒 FPU 状态恢复漏洞影响。亚马逊和微软的发言人没有任何回复。

Red Hat 公布了更多技术细节，未修改过内核的 RHEL 5/6/7 和 Enterprise MRG 2 受此漏洞影响。在声明中，该 Linux 供应商阐明了这是潜在的“任务到任务”信息窃取:

Red Hat 已被告知该问题。运行在常见现代(x86)微处理器上的操作系统和虚拟机，在应用进程间上下文切换时可能选择浮点状态“懒恢复”策略，而不是用“急恢复”策略存储和恢复浮点寄存器状态。

攻击者可利用浮点状态懒恢复来获取其他应用活动的信息，包括加密操作。与其他最近的边信道漏洞类似，该漏洞也影响 CPU 预测执行。

利用该最新漏洞，进程被“懒恢复”的浮点寄存器可能被攻击者控制的其他进程读取。Red Hat 通过软件(内核)补

丁和配置修改推出了各阶段的缓解措施。

缓解无需微代码更新。大多数案例中，Red Hat Enterprise Linux 7 客户无需采取任何操作，其他用户则可能需要应用一下软件更新。

AWS 称其服务已受到保护。

英特尔发布的漏洞咨询中解释称:“系统软件可能在上下文切换时选择采用懒浮点状态恢复而非急恢复策略。懒恢复的状态可能会经由预测执行边信道漏洞利用泄露给其他进程。”

目前尚无已知漏洞利用代码切实针对该安全漏洞下手。Cyberus 发布了一份该漏洞的背景介绍与咨询。[来源: 安全牛]

（二）CNNVD 关于 Microsoft Excel 及 Microsoft Windows HTTP 协议堆栈远程代码执行漏洞的通报

近日，微软官方发布了 Microsoft Excel 远程代码执行漏洞（CNNVD-201806-800、CVE-2018-8248）及 Microsoft Windows HTTP 协议堆栈远程代码执行漏洞（CNNVD-201806-771、CVE-2018-8231）的公告。成功利用 Microsoft Excel 远程代码执行漏洞的攻击者，能在当前用户环境下执行任意代码，如果当前用户使用管理员权限登录，攻击者甚至可以完全控制该用户的系统。Microsoft Office 2010 Service Pack 2、Microsoft Office 2013 RT Service Pack 1、

Microsoft Office 2013 Service Pack 1、Microsoft Office 2016、Microsoft Office 2016 Click-to-Run (C2R)等版本均受漏洞影响。成功利用Microsoft Windows HTTP 2.0协议堆栈远程代码执行漏洞的攻击者，可在目标系统上执行任意代码，并控制该用户的系统。Windows 10、Windows 10 Version 1607、Windows 10 Version 1703、Windows 10 Version 1709、Windows 10 Version 1803、Windows Server 2016、Windows Server 2016 (Server Core installation)、Windows Server version 1709 (Server Core Installation)、Windows Server version 1803 (Server Core Installation)等版本均受漏洞影响。目前，微软官方已经发布补丁修复了上述漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

漏洞介绍

Microsoft Excel 是美国微软公司为使用 Windows 和 Apple Macintosh 操作系统的电脑编写的一款电子表格软件。Microsoft Excel 存在远程代码执行漏洞，该漏洞源于该软件未能正确处理内存中的对象，攻击者可通过向用户发送经过特殊构造的文件并诱使用户打开该文件，从而触发远程代码执行漏洞。

Microsoft Windows 是美国微软公司研发的一套采用了图形化模式的操作系统。Windows 中的 HTTP 协议是一种通信

协议，即超文本传输协议。Microsoft Windows HTTP 协议存在堆栈远程代码执行漏洞。该漏洞源于 HTTP 协议堆栈未能正确处理内存中的对象，攻击者可以向目标 http.sys 服务器发送经过特殊构造的数据包，从而触发远程代码执行漏洞。

危害影响

Microsoft Excel 远程代码执行漏洞。攻击者可以远程执行代码，如果当前用户使用管理员权限登录，攻击者甚至可以完全控制该用户的系统，任意安装程序、更改或删除数据、创建管理员帐户等。该漏洞涉及了多个版本，Microsoft Office 2010 Service Pack 2、Microsoft Office 2013 RT Service Pack 1、Microsoft Office 2013 Service Pack 1、Microsoft Office 2016、Microsoft Office 2016 Click-to-Run (C2R)等版本均受漏洞影响。

Microsoft Windows HTTP 协议堆栈远程代码执行漏洞，攻击者可以在目标系统上执行任意代码，并控制该用户的系统。该漏洞涉及了多个版本，Windows 10、Windows 10 Version 1607、Windows 10 Version 1703、Windows 10 Version 1709、Windows 10 Version 1803、Windows Server 2016、Windows Server 2016 (Server Core installation)、Windows Server version 1709 (Server Core Installation)、Windows Server version 1803 (Server Core Installation)等版本均受该漏洞影响。

修复建议

目前，微软官方已经发布补丁修复了上述漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。[来源：国家信息安全漏洞库]

（三）钓鱼邮件攻击防范指南

钓鱼邮件是指黑客伪装成同事、合作伙伴、朋友、家人等用户信任的人，通过发送电子邮件的方式，诱使用户回复邮件、点击嵌入邮件正文的恶意链接或者打开邮件附件以植入木马或间谍程序，进而窃取用户敏感数据、个人银行账户和密码等信息，或者在设备上执行恶意代码实施进一步的网络攻击活动。

1、钓鱼邮件要当心，几招助你来识别

图钓鱼邮件示例

主要的识别钓鱼邮件方法如下:

（1）看发件人地址。如果是公务邮件，发件人多数会使用工作邮箱，如果发现对方使用的是个人邮箱帐号或者邮箱

账号拼写很奇怪，那么就需要提高警惕。钓鱼邮件的发件人地址经常会进行伪造，比如伪造成本单位域名的邮箱账号或者系统管理员账号。

（2）看邮件标题。大量钓鱼邮件主题关键字涉及“系统管理员”、“通知”、“订单”、“采购单”、“发票”、“会议日程”、“参会名单”、“历届会议回顾”等，收到此类关键词的邮件，需提高警惕。

（3）看正文措辞。对使用“亲爱的用户”、“亲爱的同事”等一些泛化问候的邮件应保持警惕。同时也要对任何制造紧急气氛的邮件提高警惕，如要求“请务必今日下班前完成”，这是让人慌忙中犯错的手段之一。

（4）看正文目的。当心对方索要登录密码，一般正规的发件人所发送的邮件是不会索要收件人的邮箱登录账号和密码的，所以在收到邮件后要留意此类要求避免上当。

（5）看正文内容。当心邮件内容中需要点击的链接地址，若包含“&redirect”字段，很可能就是钓鱼链接；当心垃圾邮件的“退订”功能，有些垃圾邮件正文中的“退订”按钮可能是虚假的。点击之后可能会收到更多的垃圾邮件，或者被植入恶意代码。可以直接将发件人拉进黑名单，拒收后续邮件。

2、钓鱼邮件防范五要、五不要

防范钓鱼邮件要做到以下“五要”：

（1）杀毒软件要安装。安装杀毒软件并定期更新病毒库，开启杀毒软件对邮件附件的扫描功能。同时定期下载和安装系统和软件的更新;

（2）登录口令要保密。要做到不向任何人主动或轻易地泄露邮箱的密码信息。不要将登录口令贴在办公桌或者易于被发现的记事本上。办公邮箱的密码要定期更换。

（3）邮箱账号要绑定手机。将邮箱帐号与个人手机号码绑定，不光可以找回密码，也可以接收“异地登录提醒”信息。

（4）公私邮箱要分离。不用工作邮箱注册公共网站的服务，也不要用工作邮箱发送私人邮件。

（5）重要文件要做好防护。①及时清空收件箱、发件箱和垃圾箱内不再使用的重要邮件；②备份重要文件，防止被攻击后文件丢失；③重要邮件或附件应加密发送，且正文中不能附带解密密码。

防范钓鱼邮件要做到以下“五不要”:

（1）不要轻信发件人地址中显示的“显示名”。因为显示名实际上是可以随便设置的，要注意阅读发件邮箱全称。

（2）不要轻易点开陌生邮件中的链接。正文中如果有链接地址，切忌直接打开，大量的钓鱼邮件使用短链接（例如http://t.cn/zWU7f71）或带链接的文字来迷惑用户。如果接到的邮件是邮箱升级、邮箱停用等办公信息通知类邮件，在

点开链接时，还应认真比对链接中的网址是否为单位网址，如果不是，则可能为钓鱼邮件。

（3）不要放松对“熟人”邮件的警惕。攻击者常常会利用攻陷的组织内成员邮箱发送钓鱼邮件，如果收到了来自信任的朋友或者同事的邮件，你对邮件内容表示怀疑，可直接拨打电话向其核实。

（4）不要使用公共场所的网络设备执行敏感操作。不要使用公共场所的电脑登入电子信箱、使用即时通讯软件、网上银行或进行其它涉及敏感资料的操作。在无法确定其安全性的前提下，请不要在连接 Wi-Fi 后进行登录和收发邮件，慎防免费无线网络因疏于管理被别有用心人士使用数据截留监侦手段获取用户信息。

（5）不要将敏感信息发布到互联网上。用户发布到互联网上的信息和数据会被攻击者收集。攻击者可以通过分析这些信息和数据，有针对性的向用户发送钓鱼邮件。

3、感染钓鱼邮件莫要慌，应急招数来帮忙

当点开钓鱼邮件，造成感染后，不要惊慌，可以开展以下几种应急工作，减小钓鱼攻击产生的危害。

（1）及时报告。及时报给邮箱管理员，请专业的安全人员进一步处理和开展后续系统清理以及恢复工作。

（2）修改登录密码。邮箱的登录密码可能已经泄露，应在另外的机器上及时修改密码，防止攻击者获取邮箱中的邮

件、联系人等敏感信息，遏制黑客进一步的攻击渗透。

（3）全盘杀毒。钓鱼邮件中的链接或者附件等可能带有病毒、木马或勒索程序。发现异常应及时做全盘扫描杀毒，最好使用多个杀毒软件交叉杀毒。

（4）隔离网络。切断受感染设备的网络连接（拔掉网线或者禁用网络），避免网络内其他设备被感染渗透，使安全事件范围得到控制，防止敏感文件被窃取，降低安全事件带来的损失。[来源：国家互联网应急中心]

（四）关于第三方支付平台 JAVA SDK 存在 XXE 漏洞的安全公告

2018 年 7 月 3 日，国家信息安全漏洞共享平台（CNVD）收录了第三方支付平台 JAVA SDK 存在 XXE 漏洞（CNVD-2018-12508）。综合利用上述漏洞，攻击者可实现商户服务器端系统的 XML 外部实体注入攻击。目前漏洞的利用细节已被公开，厂商已发布补丁进行修复。

漏洞情况分析

可扩展标记语言（XML，eXtensible Markup Language）用于标记电子文件使其具有结构性的标记语言，可以用来标记数据、定义数据类型。XML 具备在任何应用程序中进行数据读写的简单特性，使其很快成为数据交换的唯一公共语言，被广泛应用于第三支付平台与商户之间交换数据的格式定义。

XML 语言标准支持与外部进行实体数据交换的特性。应用程序在解析 XML 输入时，没有禁止外部实体加载功能，会导致 XML 外部实体注入漏洞（XML External Entity Injection，XXE）。2018 年 7 月 2 日，境外 SecLists 网站发布了微信支付 JAVA 软件工具开发包（SDK）存在 XXE 漏洞。利用该漏洞，攻击者可在使用信息泄露、扫描爆破等特殊手段获知商户的通知接口（callback）地址的前提下，发送恶意 XML 实体，在商户服务器上执行代码，实现对商户服务器的任意文件读取。如果攻击者进一步获得商家的关键安全密钥，就可能通过发送伪造信息实现零元支付。

CNVD 对该漏洞的综合评级为“高危”。

漏洞影响范围

该漏洞影响商户服务器后台系统的安全，目前已知微信支付 JAVA SDK7 月 3 日之前发布的版本、陌陌和 vivo 商户系统受此漏洞影响。

陌陌公司、腾讯公司和 vivo 商户系统已分别于 7 月 2 日、7 月 3 日、7 月 4 日完成修复。

漏洞修复建议

建议第三方支付平台对本公司开发的 SDK 工具进行自查，发现安全隐患请及时通知下属商户，及时消除漏洞攻击威胁。

1、腾讯公司已发布 JAVA SDK 修复版本，建议商户及时更新至最新版本：https://pay.weixin.qq.com/wiki/doc/a

pi/jsapi.php?chapter=11_1

2、用户可使用开发语言提供的禁用外部实体的方法，JAVA 禁用外部实体的代码如下:

DocumentBuilderFactory dbf =DocumentBuilderFactory.newInstance();

dbf.setExpandEntityReferences(false);

3、过滤用户侧提交的 XML 数据，过滤关键词: DOCTYPE、ENTITY、SYSTEM、PUBLIC。[来源: 国家互联网应急中心]

四、联系我们

欢迎与我们就《网络安全监测工作动态》进行交流。

本期编辑: 王楠、赵少飞

联系电话: 029-88319550-8017、8019

邮箱地址: wangnan@sntec.org.cn

网　　址: http://www.sntec.org.cn