网络安全监测工作动态

2018 第 3 期（总第 3 期）

陕西省网络与信息安全测评中心　　5 月 1 日-5 月 31 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 3 个，被恶意篡改的政府网站 11 个，存在严重高危漏洞的政府网站 15 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、巴西、保加利亚、韩国等国家和地区，占攻击总数的 4.5%，攻击手法主要为恶意扫描、CC 攻击、XSS 攻击等。

一、安全监测情况分析

（一）可用性监测情况

共监测发现 3 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 11 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 8 个网站被黑客攻击，将网站页面指向博彩网站；3 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 15 个网站存在高危漏洞，高危漏洞数量 25 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 SQL 注入、XSS 攻击、OpenSSL POODLE、信息泄露、弱口令、代码执行等。

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 6440 个，其中，境外 IP 数 287 个，境内 IP 数 6153 个。

从攻击源 IP 分布情况看，目前境外 IP 主要集中在美国、巴西、保加利亚、韩国等国家和地区（如图 1），境内 IP 主要集中在江苏、浙江、北京、上海、广东和河南等（如图 2）。

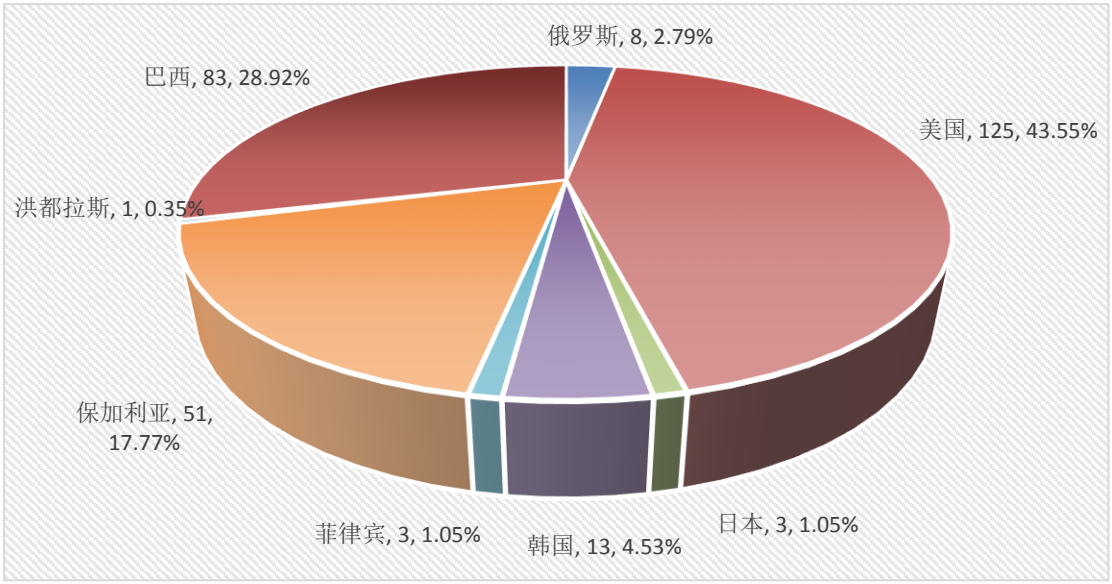

图 1 境外攻击源分布情况

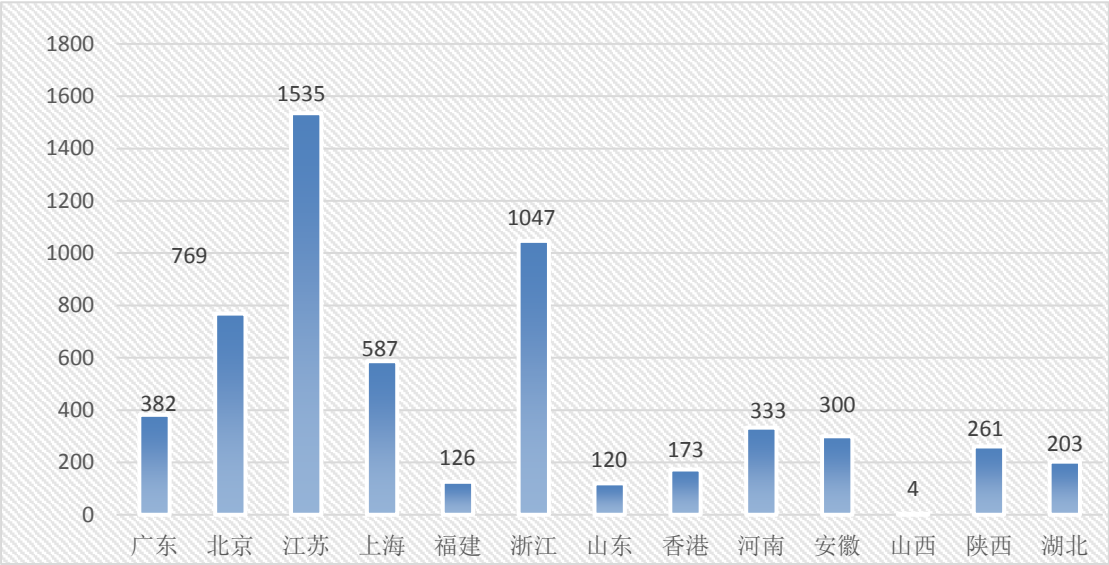

图 2 境内攻击源分布情况

（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恶意扫描和 CC 攻击,攻击者共发起了 117.4950 万次恶意扫描和 98.2048 万次 CC 攻击，所有攻击类型及数量的主要分布情况如图 3。

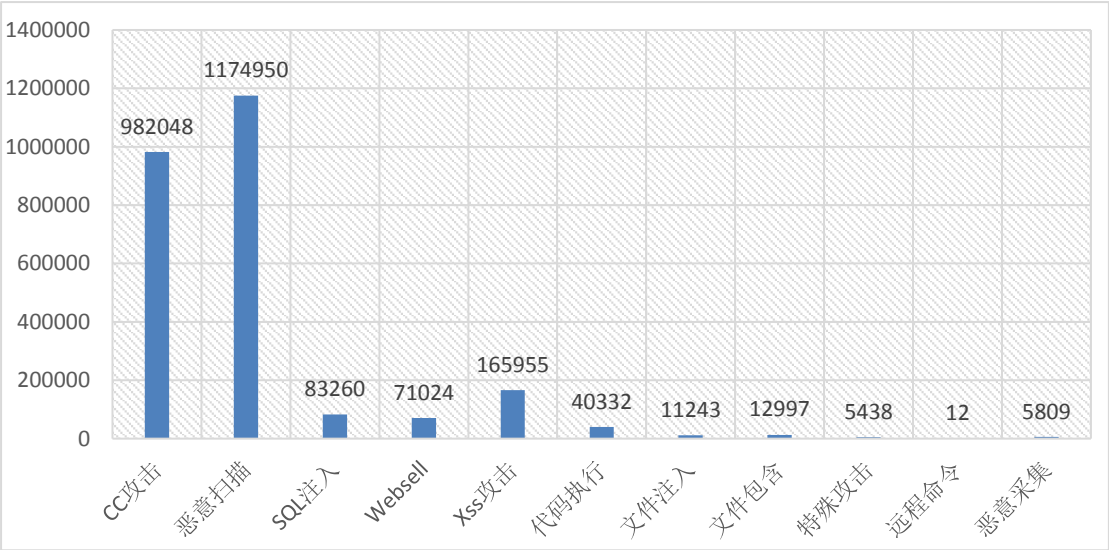

图 3 网站恶意攻击类型及数量分布

三、威胁播报

（一）关于 Windows 远程代码执行漏洞及 Microsoft

Excel 远程代码执行漏洞预警

近日，微软官方发布了 Windows 远程代码执行漏洞（CNNVD-201805-278、CVE-2018-8136）及Microsoft Excel 远程代码执行漏洞(CNNVD-201805-273和CNNVD-201805-272、CVE-2018-8147 和 CVE-2018-8148 ）的公告。成功利用 Windows 远程代码执行漏洞的攻击者，可以在目标系统上执行任意代码。Microsoft Windows Server 2016、Microsoft Windows Server 2012、Microsoft Windows Server 2008、Microsoft Windows 8.1、Microsoft Windows 7、Microsoft Windows 10 等版本均受漏洞影响。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 Excel 2010 Service Pack 2、Microsoft Excel 2013 Service Pack 1、Microsoft Excel 2016、Microsoft Office 2010 Service Pack 2、Microsoft Office 2013 RT Service Pack 1、Microsoft Office 2013 Service Pack 1、Microsoft Office 2016、Microsoft Office Compatibility Service Pack 3 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。

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 处理内存中对象的方式存在远程代码执行漏洞，攻击者可通过创建特制的文档利用该漏洞以提升的权限执行任意代码。

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。

Windows 远程代码执行漏洞，攻击者可通过创建特制的文档利用该漏洞以提升的权限执行任意代码。该漏洞涉及了多个版本，Windows 10 Version 1607、Windows 10 Version 1703、Windows 10 Version 1709、Windows 10 Version 1803、Windows 7 Service Pack 1、Windows 8.1、Windows RT 8.1、Windows Server 2008 Service Pack 2、Windows Server 2008 R2 Service Pack 1、Windows Server 2012、Windows Server 2012 R2 、Windows Server 2016、Windows Server Version 1709、Windows Server Version 1803 等版本均受漏洞影响。

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 Excel 2010 Service Pack 2、Microsoft Excel 2013 Service Pack 1、Microsoft Excel 2016、Microsoft Office 2010 Service Pack 2、Microsoft Office 2013 RT Service Pack 1、Microsoft Office 2013 Service Pack 1、Microsoft Office 2016、Microsoft Office Compatibility Service Pack 3 等版本均受该漏洞影响。[来源：国家信息安全漏洞库]

（二）关于 PHP 输入验证安全漏洞预警

近日，国家信息安全漏洞库（CNNVD）收到关于 PHP 输入验证安全漏洞（CNNVD-201805-054、CVE-2018-10547 ）情况的报送。成功利用漏洞的攻击者，可在用户不知情的情况下，在该用户浏览器中执行任意代码。PHP 5.6.36 之前的版本，7.0.27 之前的 7.0.x 版本，7.1.13 之前的 7.1.x 版本，7.2.1 之前的 7.2.x 等版本均受漏洞影响。目前，PHP 官方已经发布新版本修复了该漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

PHP（PHP: Hypertext Preprocessor，PHP: 超文本预处理器）是 PHP Group 和开放源代码社区共同维护的一种开源的通用计算机脚本语言。该语言主要用于 Web 开发，支持多种数据库及操作系统。

PHP 中的 PHAR 404 和 PHAR 403 错误页面存在输入验证

安全漏洞，该漏洞源于程序没有过滤用户的输入，通过 URI 地址访问 PHAR 程序触发 404 或 403 错误后，可以执行反射性跨站脚本攻击，进而通过用户浏览器，执行任意代码。

利用该漏洞，攻击者可以进行劫持用户浏览器会话、植入传播恶意代码等网络攻击，可能会造成用户账号被盗取、用户隐私泄露等危害。该漏洞涉及了多个版本，PHP 5.6.36 之前的版本,7.0.27 之前的 7.0.x 版本,7.1.13 之前的 7.1.x 版本，7.2.1 之前的 7.2.x 版本均受漏洞影响。[来源：国家信息安全漏洞库]

（三）各大操作系统误读英特尔文档致内核可被劫持或崩溃

Linux、Windows、macOS、FreeBSD 和 Xen 的某些实现都存在设计缺陷，攻击者可利用该缺陷导致英特尔和 AMD 计算机系统崩溃。

更糟的情况是，黑客还有可能获取到敏感内存信息或控制底层操作系统功能，也就是能窥探内核内存或劫持机器运行的关键代码。

恶意登录用户或计算机上运行的恶意软件都可以利用该漏洞。不过，这一几乎波及全行业范围的编程缺陷目前已有可用补丁加以缓解。

5 月 8 号 CERT 发布的公告称，该编号为 CVE-2018-8897 的安全漏洞，是因为微软、苹果和其他公司错误理解了英特

尔和 AMD 芯片处理某一特定异常的方式。

CERT 写道:“该错误似乎是因开发人员对现有文档的解释而产生的。”换句话说,程序员理解错了英特尔和 AMD 的手册,虽然这些手册可能写得不是特别清楚。

触发中断

问题的核心是 POP SS 指令。该指令从当前程序的堆栈取得用于堆段选择的值,并将该值放入 CPU 的堆栈选择寄存器。但现代操作系统大多忽略了内存分段问题。CPU 会特别处理 POP SS 指令,以便执行中遇到中断时堆栈能保持一致状态。

应用程序可为堆栈选择器即将被 POP SS 指令从堆栈中取出的内存位置设置调试断点。设置了该调试断点后,当应用程序调用 POP SS 指令时,只要处理器访问 RAM 特定位置读取该堆栈选择器,就会抛出一个特殊异常。

问题就出在这儿。要利用这一情况,紧跟在 POP SS 指令后的那条指令必须是触发中断的 INT 指令。这些由软件产生的中断有时候是用户程序用以激活内核,让内核为当前进程干活的,比如打开个文件之类。

在英特尔和 AMD 机器上,紧跟在 POP SS 后面的软中断指令会让处理器进入内核的中断处理过程。然后调试异常就出现了,因为 POP SS 导致该异常被延迟。

操作系统设计者并没有预期到这一点。他们阅读英特尔

的 x86-64 手册，认为内核中断处理过程是在不可中断的状态下开始的。但如今，中断处理过程在初期就遭遇到了非预期的调试异常。

漏洞发现者的技术报告中解释称，这导致了内核的混乱，特定情况下，内核的动作完全依赖于非特权用户所控制的数据。

如果 POP SS 指令执行时调试寄存器设置了堆栈位置访问的断点，且紧跟的指令就是 INT N，那么在进入中断门之后，挂起的 #DB 就会被触发，因为那是最有可能的分支指令。不是不可屏蔽的中断，也不是机器检查异常，操作系统开发人员直接为中断门语义假定了一个不可中断的状态。这会导致操作系统监管软件在设计时出现漏洞，使用中可能会错误地采用了非特权软件选择的状态信息。

这是操作系统提供商因为 POP SS 指令及其与中断门语义互动的文档不清晰不完整而犯下的严重安全疏漏。

其结果就是，在英特尔主机上，用户应用程序可使用 POP SS 和 INT 指令来利用上述的错误理解，控制中断处理过程中的特殊指针 GSBASE; 而 AMD 主机上，应用程序可控制 GSBASE 和堆栈指针。黑客可利用该漏洞触及未分配内存，抽取部分受保护内核内存，最终使内核崩溃; 或者调整其内部结构，扰乱系统运行。

虽然任何漏洞利用尝试都更容易搞崩内核而不是引起

什么严重伤害，但是与熔断之类的漏洞一样，这是整个行业的耻辱，应该尽快被补上。

操纵

FreeBSD 对该问题的解释则更进一步:“在 x86 架构的系统上，堆栈是由堆栈段和堆栈指针共同表示的，其正常运行需要二者协调一致。操作堆栈段的指令有特殊的处理过程来保持与堆栈指针的改变相一致。”

MOV SS 和 POP SS 指令会抑制调试异常直到下一条指令的边界。如果该指令是一条系统调用或者将控制传递到操作系统的类似指令，调试异常就会在内核环境中处理，而不是在用户环境中处理。

其结果就是通过了身份验证的本地攻击者可以读取到内核内存中的敏感数据，控制底层操作系统功能，或者直接搞崩系统。

微软的内核建议表明，在 Windows 主机上利用该漏洞，需要攻击者先登录到系统，再运行精心制作的应用程序以夺取受影响系统的控制权。

这并非危言耸听，除非你的主机上从来都不运行任何不可信的代码。

Red Hat 已经准备好放出补丁，Ubuntu 和 macOS 同样做好了补丁准备。

Linux 内核早在 2018 年 3 月 23 号就打上了补丁，版本

4.15.14、4.14.31、4.9.91、4.4.125 以及更老的 4.1、3.16 和 3.2 都已修复。

微软也解决了该问题，补丁覆盖 Windows 7 到 Windows 10，Windows Server 2008 到 Windows Server 1803。Xen 为版本 4.6 到 4.10 打了补丁。VMware 的虚拟机管理程序没有风险，但 vCenter Server 的一个工作区和 vSphere 集成的容器需要打补丁，但都只是“可能”受影响。[来源：安全牛]

（四）可模糊源端口数据的新型 DDoS 攻击方法

最近的分布式拒绝服务(DDoS)攻击展现通过模糊源端口数据绕过现有防御机制的新特性。

网络安全解决方案提供商 Imperva 称，除了常见的放大攻击方法，新观测到的攻击使用了 DDoS 防御者没想到的非常规源端口数据。该攻击方法利用的是著名的 UPnP（通用即插即用）协议漏洞。

UPnP 协议允许通过 UDP 1900 端口发现设备，并允许使用任意 TCP 端口进行设备控制。因此，很多 IoT 设备都用该协议在局域网(LAN)上相互发现并通信。

然而，开放远程访问的设备默认设置、身份验证机制的缺乏，以及 UPnP 远程代码执行漏洞，令该协议构成了安全风险。

UPnP 相关漏洞早在 20 年前就被安全研究人员披露了，

除此之外，简单对象访问协议(SOAP) API 调用也可用于通过广域网(WAN)远程重配置不安全设备。控制端口转发规则的AddPortMapping 指令同样能经 SOAP API 调用远程执行。

2018 年 4 月 11 日，Imperva 在缓解某简单服务发现协议(SSDP)放大攻击时，注意到某些攻击载荷不是来自UDP/1900，而是来自一个非预期的源端口。几周后的另一个攻击中，同样的方法再次出现。

Imperva 称:“对这些事件的调查，让我们构建出集成了UPnP 的攻击方法的概念验证代码(PoC)，可被用于模糊任意放大攻击载荷的源端口信息。”

想要使用该 PoC 执行 DNS 放大攻击,先得利用 Shodan 之类公开在线服务执行大范围 SSDP 扫描，找出开放 UPnP 路由器。

此类扫描能扫出 130 多万台此类设备，当然，不是全部设备都带有相应漏洞。但定位出一台可利用的脆弱设备依然相当容易，因为可以用脚本自动化该过程。

接下来，攻击者需要通过 HTTP 访问该设备的 XML 文件(rootDesc.xml)，用 Shodan 中的真实设备 IP 替换掉‘Location’ IP 就行。

rootDesc.xml 文件列出了所有可用 UPnP 服务和设备，下一步就是通过 AddPortMapping 指令修改设备的端口转发规则。

运用文件中的机制，可以使用 SOAP 请求来创建转发规则，将所有发送至端口 1337 的 UDP 包通过端口 UDP/53(DNS 端口)重路由至外部 DNS 服务器(3.3.3.3)。

虽然端口转发应仅用于将外部 IP 的流量映射到内部 IP 或反之，但大多数路由器并不验证所提供的内部 IP 是否真的是内部的，这就允许来自外部 IP 的代理请求到另一个外部 IP 了。

要使用该端口模糊的 DNS 放大攻击，发往设备并被 UPnP 设备在 UDP/1337 端口接收的 DNS 请求，需通过目的端口 UDP/53 被代理至 DNS 解析器。解析器通过源端口 UDP/53 响应设备，而设备在将源端口改回 UDP/1337 后再将该 DNS 响应转发回原始请求者。

真实攻击场景中，初始 DNS 请求会从被假冒的受害者 IP 发出，也就是说对该请求的响应也会返回给该受害者。

该设备可用于以能规避检测的端口发起 DNS 放大 DDoS 攻击，因为攻击载荷源于非常规的源端口，通过查看源端口数据检测放大攻击载荷的常见防御措施就会被绕过。该绕过检测的方法也能用于 SSDP 和 NTP（网络时钟协议）攻击，且能与其他放大攻击方法联合使用，比如 Memcached。[来源:安全牛]

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