陕西省互联网网络安全情况月报

2016 年 11 月　　（第 W011 期）　　总第 37 期

陕西省通信管理局

国家计算机网络应急技术处理协调中心陕西分中心

目　录

1 情况综述

2016年11月，全省公共互联网网络安全状况整体评价为良。

本月，我省互联网基础设施运行平稳，全省范围内未发生造成重大影响的基础设施运行安全事件，未发生网络安全方面重大事件。

通过国家计算机网络应急技术处理协调中心陕西分中心（以下简称陕西互联网应急中心、SNCERT）监测及电信运营企业、安全厂商、安全通报成员单位报送,我省境内被木马僵尸程序控制的主机（受控端）IP数为27,494个，较上个月减少3.45%，占全国总数的2.05%；木马僵尸控制服务器（控制端）IP数为15个，较上个月减少89.58%，占全国总数的0.56%；省内被篡改网页的网站数为56个，较上个月增加19.15%，占全国总数的1.06%；省内被植入后门网站数为73个，较上个月增加58.70%，占全国总数的1.38%；省内感染飞客蠕虫的主机IP数为12,734个，较上个月增加0.47%，占全国总数的2.13%。

2 安全事件分析

2.1 木马、僵尸网络事件分析

2016年11月，CNCERT/CC对木马僵尸的活动状况进行了抽样监测，发现中国大陆地区1,339,014个IP地址对应的主机被木马或僵尸程序秘密控制。事件高发的三个省份分别为广东省（约占12.5%）、江苏省（约占7.8%）、河南省（约占7.8%），分布情况如图1所示。

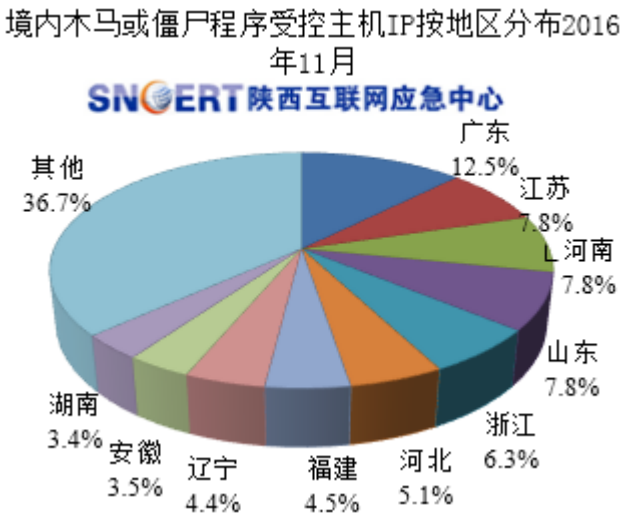

图 1：中国大陆地区木马或僵尸程序受控主机地区分布图

2015 年 12 月-2016 年 11 月境内木马或僵尸程序受控主机 IP 数量月度统计情况如图 2 所示。

图 2：中国大陆地区木马或僵尸程序受控主机 IP 数量月度统计

2016 年 11 月，陕西省有 27,494 个 IP 地址对应的主机被境内外黑客通过木马或僵尸程序控制，约占全国总数的 2.05%，居全国第 17 位；有 15 个 IP 地址对应的主机被用作木马和僵尸程序控制主机与境外进行通信，约占全国总数的 0.56%，居全国第 23 位。

2.2 “飞客”蠕虫病毒事件分析

2016 年 11 月，CNCERT/CC 对“飞客”蠕虫的活动状况进行了抽

样监测，发现境内感染“飞客”蠕虫的主机 IP 地址共 598,769 个。事件高发的三个省份分别为广东（约占 25.3%）、江苏（约占 11.0%）和浙江（约占 6.4%）；其中陕西省 12,734 个 IP 地址，约占全国总数的 2.13%，排名第 14 位。其分布情况如图 3 所示。

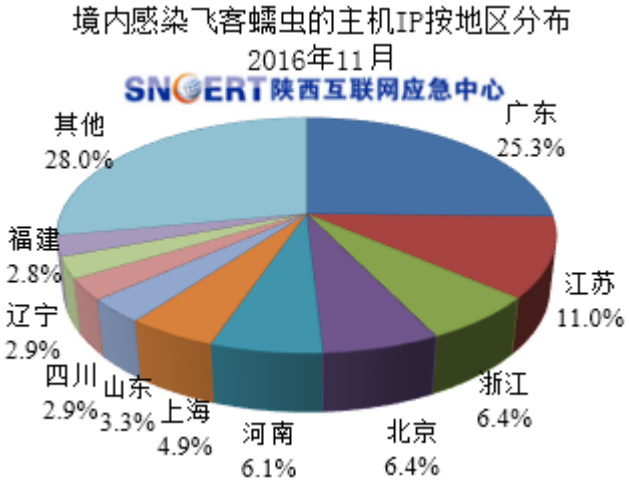

图 3：境内感染飞客蠕虫的主机 IP 按地区分布图

2.3 网页篡改事件分析

2016 年 11 月，CNCERT/CC 监测发现中国大陆地区被篡改网站 5,294 个，其中境内被篡改政府网站（.gov）数量为 142 个。被篡改网站分布情况如图 4 所示，最多的地区分别为广东省（约占 25.2%）、北京市（约占 19.5%）和河南省（约占 14.9%）。

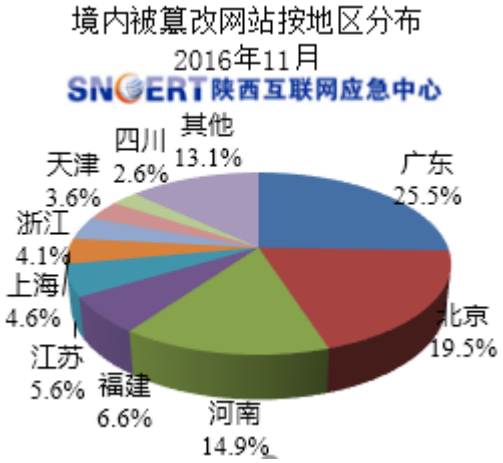

图 4：境内被篡改网站按地区分布

2015 年 12 月-2016 年 11 月境内被篡改网站数量按月度统计如图 5 所示。

图 5：境内被篡改网站数量月度统计

其中，2015 年 12 月-2016 年 11 月境内政府网站被篡改数量月度统计如图所示。

2.4 网站后门事件分析

2016 年 11 月，CNCERT/CC 监测发现中国大陆地区网站被植入后门数量 5,283 个。网站被植入后门分布情况如图 6 所示，最多的地区分别为广东省（约占 29.2%）北京市（约占 19.7%）和河南省（约占 14.2%）。

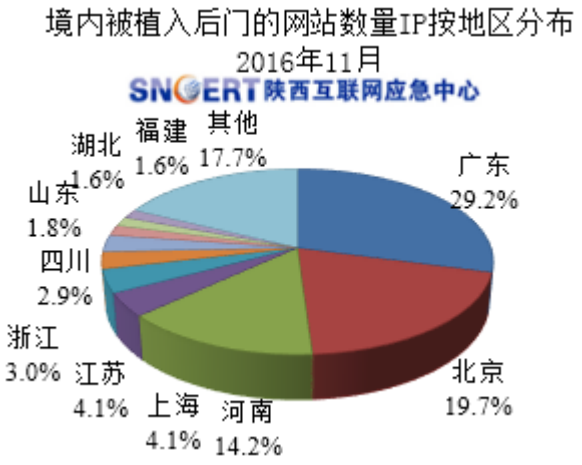

图 6：境内网站被植入后门按地区分布

2016年11月,陕西省境内监测发现网站被植入后门数量73个，约占全国总数的1.38%，全国排名第11名。

3 安全事件处置情况

2016年11月，陕西互联网应急中心共协调处理各类网络安全事件12,191起，僵尸木马受控事件6992起，控制事件390，飞客病毒事件4792起。政府网站安全事件17起,其中16起高危漏洞，1起网页篡改事件；包括弱口令漏洞2起，SQL注入漏洞13起，远程命令执行漏洞2起，任意文件漏洞2起，跨站脚本漏洞2起；陕西互联网应急中心及时向用户作了情况通报并指导用户进行系统恢复,使事件在最快时间内得到处理，消除了不良影响。

4 安全预警信息

4.1 本月重要安全漏洞信息通报

2016年11月，CNCERT/CC收到的来自国家信息安全漏洞共享平台（CNVD）报告的漏洞数量1,013个，其中高危漏洞404个、中危漏洞543个、低危漏洞66个，其中0day漏洞229个，可远程攻击漏洞894个。

2015年12月-2016年11月CNVD收录漏洞按月统计情况分布如图7所示。

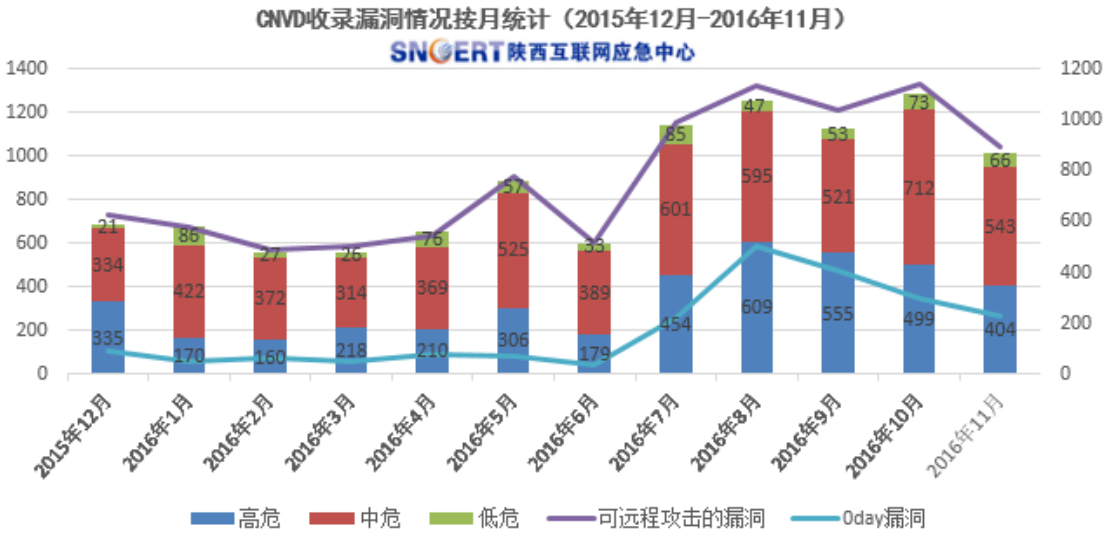

图 7： CNVD 收录漏洞按月统计情况

2016 年 11 月 CNVD 收录漏洞按类型统计情况分布如图 8 所示。

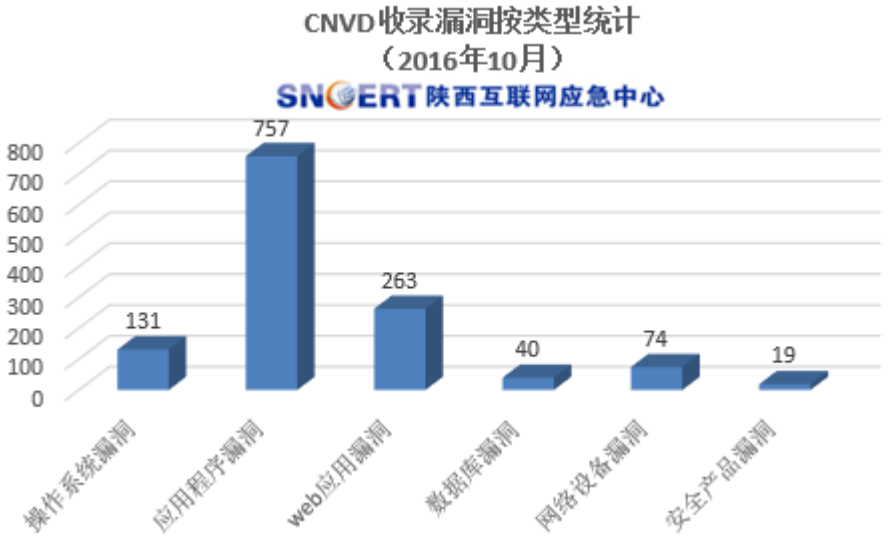

图 8： CNVD 收录漏洞按类型统计情况

2016 年 11 月，国家信息安全漏洞共享平台（CNVD）收录漏洞的补丁总数 1013 个，其中高危漏洞补丁 404 个、中危漏洞补丁 543 个、低危漏洞补丁 66 个。

（一）关关于 NTPD 存在多个拒绝服务漏洞的有关情况通报

近期，国家信息安全漏洞共享平台（CNVD）收录了 Nginx 存在权限提升漏洞（CNVD-2016-10448，对应 CVE-2016-1247）。综合利用该漏洞，本地及远程攻击者可利用该漏洞获取 root 权限。该产品

广泛应用于构建网站服务器，由于漏洞验证信息已经公开，该漏洞可能诱发以控制为目的大规模攻击。CNCERT第一时间对上述漏洞的相关情况进行了解和分析，具体通报如下：

一、漏洞情况分析

Nginx是俄罗斯软件开发者Igor Sysoev所研发的一款HTTP和反向代理服务器，也可以作为邮件代理服务器，被广泛应用于网站服务器搭建。Ubuntu官方发布的安全公告称，Nginx程序在日志文件处理权限错误，远程攻击者利用该漏洞可获取系统ROOT权限。Debian官方公告称，由于Debian 系统上的Nginx服务器包处理日志文件的方式，本地攻击者利用漏洞可访问/var/log/nginx目录，读取日志文件。

CNVD对上述漏洞的综合评级均为“高危”

二、漏洞影响范围

该漏洞影响基于Debian操作系统的Nginx 1.6.2-5+deb8u3之前的版本、基于Ubuntu16.04 LTS操作系统的1.10.00ubuntu0.16.04.3之前版本、基于Ubuntu 14.04 LTS操作系统的1.4.6-1ubuntu3.6之前版本和基于Ubuntu 16.10操作系统的1.10.1-0ubuntu1.1之前版本。应用Nginx搭建的其他web服务器也可能存在同类安全风险。

根据CNVD秘书处普查情况，受到漏洞影响的运行于Debian操作系统平台的Nginx服务器达到118万，而受影响的Ubuntu平台Nginx服务器更多，达到676万。整体看，受影响较大的排名前五名

的国家和地区分别是美国（占比52.4%）、德国（7.1%）、中国(6.3%)、英国(6.8%)、法国(4.4%)。

三、漏洞修复建议

目前，多个系统厂商已发布了漏洞修复方案，用户可将程序分别升级至基于Debian操作系统的Nginx 1.6.2-5+deb8u3版本、基于Ubuntu16.04 LTS操作系统的1.10.0-0ubuntu0.16.04.3版本、基于Ubuntu 14.04 LTS操作系统的1.4.6-1ubuntu3.6版本、基于Ubuntu 16.10操作系统的1.10.1-0ubuntu1.1版本。CNCERT建议用户关注厂商主页，升级到最新版本，避免引发漏洞相关的网络安全事件。

（二）关于OpenSSL存在多个拒绝服务漏洞的安全公告

近日，国家信息安全漏洞共享平台（CNVD）收录了OpenSSL存在多个拒绝服务漏洞（CNVD-2016-11090、CNVD-2016-11095、CNVD-2016-11093，对应CVE-2016-7054、CVE-2016-7053、CVE-2016-7055）。远程攻击者利用上述漏洞，可发起拒绝服务攻击，导致内存或CPU资源耗尽。

一、漏洞情况分析

OpenSSL是OpenSSL团队开发的一个开源的能够实现安全套接层（SSL v2/v3）和安全传输层（TLS v1）协议的通用加密库，它支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。

（一）OpenSSL拒绝服务漏洞（CNVD-2016-11090）

由于TLS链接使用的*-CHACHA20-POLY1305密码组件，通过破坏大量的有效荷载易受到拒绝服务攻击，可能导致

OpenSSL的崩溃。远程攻击者利用该漏洞，可造成应用程序拒绝服务，导致内存或CPU资源耗尽。CNVD对该漏洞的综合评级为“高危”。

（二）OpenSSL空指针废弃拒绝服务漏洞（CNVD-2016-11095）

程序在试图释放某些无效编码时，错误处理OpenSSL 1.1.0中的ASN.1选择类型，可导致一个NULL值被传递给回调结构，当NULL指针解析无效的CMS结构可导致应用程序崩溃。仅使用不处理空值的回调函数的选择结构时受到影响。CNVD对该漏洞的综合评级为“中危”。

（三）OpenSSL拒绝服务漏洞（CNVD-2016-11093）

当Broadwell-specific Montgomery乘法运算程序在处理输入长度超过256bits数据时，可导致应用程序崩溃。分析表明，由于存在问题的子程序不使用私钥本身的操作和攻击者的直接输入，攻击者不能攻击RSA，DSA和DH密钥。在EC算法中只有Brainpool P-512 curves受到影响，有可能存在针对ECDH的密钥协商攻击。CNVD对该漏洞的综合评级依次为“低危”。

二、漏洞影响范围

上述漏洞影响OpenSSL 1.1.0版本。

三、漏洞修复建议

目前，厂商已发布了漏洞修复程序，用户可将程序升级至1.1.0c版本。

附：参考链接：

https://www.openssl.org/news/secadv/20161110.txt

https://www.openssl.org/（补丁地址）

http://www.cnvd.org.cn/flaw/show/CNVD-2016-11090

http://www.cnvd.org.cn/flaw/show/CNVD-2016-11095

http://www.cnvd.org.cn/flaw/show/CNVD-2016-11093

（三）关于Memcached 存在多个远程代码执行高危漏洞的有关情况通报

近日，国家信息安全漏洞共享平台（CNVD）收录了Memcached存在的多个远程代码执行漏洞（CNVD-2016-10468、CNVD-2016-10467、CNVD-2016-10466，对应CVE-2016-8704、CVE-2016-8705、CVE-2016-8706）。综合利用上述漏洞，远程攻击者通过发送特制的命令到目标系统，进而可远程执行任意命令，有可能诱发以控制为目的大规模攻击。CNCERT第一时间对上述漏洞的相关情况进行了解和分析，具体通报如下：

一、漏洞情况分析

Memcached是一个高性能的分布式内存对象缓存系统，用于动态Web应用以减轻数据库负载。由于Memcached用于插入、添加、修改键值对的函数process_bin_append_prepend和process_bin_update以及Memcached在编译过程中启用的SASL验证存在整数溢出漏洞。远程攻击者利用漏洞通过构造特制的Memcached命令，可在目标系统执行任意系统命令，获取敏感进程信息，进而绕过通用的漏洞缓解机制，最终可获取系统控制权限。

CNVD对上述漏洞的综合评级均为“高危”。目前，相关利用代码已经在互联网上公开。

二、漏洞影响范围

上述漏洞影响Memcached 1.4.31版本。由于攻击者可绕过常规的漏洞缓解机制利用漏洞，可直接在公网访问的Memcached服务受漏洞威胁严重。根据CNVD普查，超过2.8万集成memcache的主机暴露在互联网上（暂未区分版本情况）。按国家和地区分布排名，位居前五的分别是中国（53.2%）、美国（38.9%）、中国香港（3.3%）、英国（2.5%）、德国（2.0%），其中境内IP分布方面，阿里云上承载的服务器主机占比较高，占境内比例约为29.2%。按前端承载容器分布，排名前三分别是：Apache（62.0%）、Nginx（32.3%）、IIS（3.6%）。

三、漏洞修复建议

目前，官方厂商已发布了漏洞修复方案，用户可将程序升级至1.4.33版本。CNCERT建议用户关注厂商主页，升级到最新版本，避免引发漏洞相关的网络安全事件。

（四）Linux kernel权限提升漏洞（CNVD-2016-11670）

Linux kernel是美国Linux基金会发布的操作系统Linux所使用的内核

Linux kernel 4.4.22至4.4.28版本中的arch/x86/include/asm/uaccess.h文件中的__get_user_asm_ex宏存在安全漏洞。本地

攻击者可借助特制的应用程序利用该漏洞获取non-SMEP平台上的root权限。

影响产品：Linux Kernel >=4.4.22，<=4.4.28 。

目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：

http://www.securityfocus.com/bid/94545

http://www.openwall.com/lists/oss-security/2016/11/07/4。

（五）Wordpress Olimometer插件SQL注入漏洞

WordPress是WordPress软件基金会的一套使用PHP语言开发的博客平台,该平台支持在PHP和MySQL的服务器上架设个人博客网站。

WordPress插件Olimometer 2.56版本及之前的版本olimometer_id参数存在SQL注入漏洞。攻击者可以通过该漏洞控制应用程序，访问或修改数据，或利用底层数据库中潜在的漏洞。

影响产品：WordPress Olimometer <=2.56，属于高危漏洞，其CNVD-ID为CNVD-2016-11652。

用户可联系供应商获得补丁信息：

https://wordpress.org/plugins/olimometer/

https://www.exploit-db.com/exploits/40804/。

（六）华为部分手机TrustZone驱动程序存在特权提升漏洞

Huawei P9、P9 Lite、P8 Lite为华为智能手机。

华为部分手机TrustZone驱动程序存在特权提升漏洞。攻击者可能诱使用户安装恶意应用程序，应用程序利用该漏洞可向TrustZone驱动发送特定参数，导致系统重启或用户权限提升。

该漏洞影响产品为：Huawei P9 <EVA-AL10C00B352、Huawei P9 Lite <VNS-L21C185B130、Huawei P8 Lite <ALE-L02C636B150，属于高危漏洞，其CNVD-ID为CNVD-2016-11633、CVE ID为CVE-2016-8763。

厂商已提供漏洞修补方案，请关注如下链接及时更新：

http://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20161123-01-smartphone-cn。

（七）多款Symantec产品本地权限提升漏洞

Symantec Norton Security with Backup等都是美国赛门铁克（Symantec）公司的安全系列软件。

多款Symantec产品中存在本地提权漏洞。本地攻击者可利用该漏洞以SYSTEM权限执行任意代码。

影响产品：Symantec Norton Security with Backup，属高危漏洞，CNVD-ID为CNVD-2016-11651，CVE ID为CVE-2016-5311。

用户可参考如下厂商提供的安全补丁以修复该漏洞：

http://www.securityfocus.com/bid/94295

（八）TP-LINK TDDP缓冲区溢出漏洞

TP-LINK TDDP是一个设备调试协议。

TP-LINK TDDP 存在缓冲区溢出漏洞。攻击者利用漏洞通过发送手工构造包含 v1 包的"set configuration"消息到 TDDP 服务，可执行任意代码。

影响产品：TP-LINK WA5210g（Firmware v1 and v2 ），属高危漏洞，CNVD-ID 为 CNVD-2016-11463。

目前没有详细解决方案提供：

http://www.tp-link.com/

4.2 本月活跃网络病毒情况

活跃网络病毒 TOP5

病毒名称	病毒特点
Trojan.DL.Tibs.iwt 木马病毒	病毒运行后，自我复制至系统目录 C:\WINDOWS\system32\adirss.exe，添加启动项实现开机自启动，后台连接黑客指定网址，下载恶意程序并伪装成系统文件。电脑一旦中毒，用户将面临网络账密被盗、隐私信息泄漏等风险。截至到 2016 年 12 月 1 日云端捕获感染台数为 547563 台
Worm.Win32.Agent.yzs（蠕虫病毒）	病毒通过在系统关键目录下释放伪装的自身副本，并以系统关键进程命名，然后添加其自启动的方式侵入用户电脑，并借由用户主动下载、网页挂马、即时通信软件传播等途径释放的自身副本，交叉感染系统。
Worm.VB.fa（蠕虫病毒）	病毒运行后，劫持原系统文件，供恶意软件加载，并修改注册表键值，隐藏文件扩展名实现自身为开机自启动，设置不显示系统隐藏文件，劫持安全模式启动。电脑一旦中毒，用户将面临系统运行缓慢乃至宕机的风险。
Worm.Netsky!1.A4B9（蠕虫病毒）	病毒系统创建线程搜索磁盘中的相关文件，从中提取 email 地址并发送带毒邮件。还会将自己复制到系统共享目录下，从而借助用户主动下载、邮件、共享目录等途径释放大量恶意软件。
Worm.VBcode!1.6521（蠕虫病毒）	病毒运行后，会在系统文件夹复制大量病毒文件，并改成如 lsass.exe、smss.exe、svchost.exe 等系统文件名，之后运行多个此类副本，占用大量 CPU 时间和系统资源，造成系统异常缓慢。利用全局消息钩子注入指定文件到其他进程，添加开机自启动项，设置文件属性为隐藏。

表 1：活跃网络病毒 TOP5

4.3 本月恶意代码捕获和传播情况

以下表 2 为中国反病毒联盟（ANVA）近期监测发布的散布恶意代码的 URL，登陆这些 URL，会弹出下载指令，如点击下载，将使用户主机感染恶意程序。

http://cl2.qnxzq.com/download/rpg120423arzy1_20@64903.exe
http://cl2.qnxzq.com/download/rpg120423arzy1_20@64903.exe
http://c6.97you.net/download/xfwmzzII4_20@74810.exe
http://url.222bz.com/down/Adobe%20Flash%20CS3%20Pro%20CS3@191_539.exe
http://dl.wylbdml.com/download/ctfmon.exe%D0%DE%B8%B4%B9%A4%BE%DF_31@19571.exe
http://qptest.ru/Photo.zip
http://url.222bz.com/down/@154_25869.exe
http://cl2.dhfszh.com/download/ZBrush%204R7%203D_18@187298.exe
http://d20.97you.net/download/EditPlus_60@2745.exe
http://121.18.168.141/af.92app.com/20160902_14_131172739669036250.gz?wsiphost=ipdb
http://dl.wylbdml.com/download/pc_31@63295.exe
http://cl2.qnxzq.com/download/alkatip%E8%BE%93%E5%85%A5%E6%B3%95_61@32404.exe
http://url.222bz.com/down/debloater@271_82186.exe
http://dl.cjsdxz.com/download/iBackupBot_1@530009.exe
http://dl.dldhyx.com/download/Microsoft_33@12498.exe
http://url.tudown.com/down/Visual%20C++%202005%20SP1%20-%20VC2005@67_48274.exe
http://url.222bz.com/down/msicuu2.exe
http://cl2.wylbdml.com/download/UltraISO_31@24845.exe
http://dl.cjsdxz.com/download/PDFImageExtractionWizard_1@60661.exe
http://7.kuai8.com/patch/bd353.zip

表 2：恶意 URL 列表

4.4 本月钓鱼网站统计情况

本月钓鱼网站 Top5：

序号	钓鱼类型	钓鱼 URL	危害
1	假冒 APPID 类	http://tozze.nl/administrator/appleid-verify/applhtee/ http://admain3111.wapka.mobi/site_0.xhtml http://gps-supporting.esy.es/	骗取用户账号及密码信息
2	假冒支付类	http://wap.dbsbzc.cn/index1.asp http://www.ccbtnq.cc/default.asp http://wap-tsccb.cc/ http://wap.sjzcbbw.cc/register.asp	骗取用户卡号及密码信息

		http://www.tolmatica.es/modules/domz.html	
3	假冒邮箱类	http://capital4u.org/jjj/GD/ http://taxmail01.com/GOG/yGnHFKdhsd.php http://www.drillingcompany.ru/includes/js/Ymail/ http://www.tolmatica.es/modules/domz.html http://www.wilderweb.net/new/GD	骗取用户账号及个人信息
4	假冒facebook类	http://loginmasketig.mbastudios.info/	骗取用户账号及密码
5	假冒Paypal类	http://admain3111.wapka.mobi/site_0.xhtml http://paypal.configration.account.verify.someofpoy.com/	窃取用户私密信息

4.5 本月重要漏洞修补信息

（一）w3m存在多个拒绝服务漏洞的补丁

w3m是一款开源的基于文本的Web浏览器。 w3m 0.5.3-33之前的版本中存在拒绝服务漏洞。攻击者可利用该漏洞在受影响程序上下文中执行任意代码，失败的攻击将导致拒绝服务。

目前，供应商发布了安全公告及相关补丁信息，修复了此漏洞。

补丁链接：

https://github.com/tats/w3m

（二）Xen权限提升漏洞（CNVD-2016-11648）的补丁

Xen是英国剑桥大学开发的一款开源的虚拟机监视器产品。该产品能够使不同和不兼容的操作系统运行在同一台计算机上，并支持在运行时进行迁移，保证正常运行并且避免宕机。 Xen存在权限提升漏洞，攻击者可利用该漏洞获取权限提升。

目前，供应商发布了安全公告及相关补丁信息，修复了此漏洞。

补丁链接：

http://xenbits.xenproject.org/xsa/advisory-192.html

（三）TYPO3远程安全绕过漏洞的补丁

TYPO3是瑞士TYPO3协会维护的一套免费开源的内容管理系统(框架)(CMS/CMF)。 TYPO3存在远程安全绕过漏洞，攻击者可利用该漏洞绕过安全限制，执行未授权操作。

目前，供应商发布了安全公告及相关补丁信息，修复了此漏洞。

补丁链接：

https://typo3.org/teams/security/security-bulletins/typo3-core/typo3-core-sa-2016-023/

（四）Linux内核空指针引用本地拒绝服务漏洞的补丁

Linux kernel是美国Linux基金会发布的操作系统Linux所使用的内核。 Linux内核空指针引用存在本地拒绝服务漏洞。攻击者利用漏洞可使主机内核崩溃，导致拒绝服务条件。

目前，供应商发布了安全公告及相关补丁信息，修复了此漏洞。

补丁链接：

https://bugzilla.redhat.com/show_bug.cgi?id=1395187

（五）Apache Tomcat拒绝服务漏洞（ CNVD-2016-11592）的补丁

Apache Tomcat是一个流行的开源JSP应用服务器程序。Apache Tomcat存在拒绝服务漏洞，攻击者可利用漏洞使HTTP/2标头解析器进入无限循环，导致拒绝服务。

目前，供应商发布了安全公告及相关补丁信息，修复了此漏洞。

补丁链接：

http://tomcat.apache.org/security-9.html

（六）IBM iNotes跨站脚本漏洞的补丁

IBM iNotes（又名IBM Lotus iNotes）是美国IBM公司的一套基于Web的电子邮件软件。该软件可帮助不同类型的用户（在线用户和离线用户）有效地管理关键业务信息和协作。 IBM iNotes 8.5.3 FP6 IF2之前的版本中存在跨站脚本漏洞。远程攻击者可借助特制的URL利用该漏洞注入任意Web脚本或HTML。

目前，供应商发布了安全公告及相关补丁信息，修复了此漏洞。

补丁链接：

http://www-01.ibm.com/support/docview.wss?uid=swg21991722

（七）多款IBM产品跨站脚本漏洞的补丁

IBM Rational Collaborative Lifecycle Management（CLM）等都是美国IBM公司的产品。IBM Rational CLM、Rational Team Concert（RTC）和Rational Engineering Lifecycle Manager都是协作化生命周期管理解决方案；Rational Quality Manager（RQM）是一套协作的、基于Web的质量管理解决方案；Rational Requirements Composer和Rational DOORS Next Generation都是需求管理解决方案。 多款IBM产品中存在跨站脚本漏洞。远程攻击者可借助特制的URL利用该漏洞注入任意Web脚本或HTML。

目前，供应商发布了安全公告及相关补丁信息，修复了此漏洞。

补丁链接：

http://www-01.ibm.com/support/docview.wss?uid=swg21991478

（八）Lepton远程代码执行漏洞的补丁

Lepton是一套无损压缩JPEG格式文件的工具。 Lepton存在远程代码执行漏洞，攻击者可利用该漏洞在受影响的程序上下文中执行任意脚本代码。

目前，供应商发布了安全公告及相关补丁信息，修复了此漏洞。

补丁链接：

http://www.lepton-cms.org/posts/important-lepton-2.3.0-101.php

（九）多款Lenovo ThinkPad产品安全绕过漏洞的补丁

Lenovo Yoga 11e等都是中国联想（Lenovo）公司的电脑产品。 多款Lenovo ThinkPad产品中存在本地安全绕过漏洞。本地攻击者可利用该漏洞绕过安全限制，执行未授权操作。

目前，供应商发布了安全公告及相关补丁信息，修复了此漏洞。

补丁链接：

https://support.lenovo.com/us/zh/solutions/LEN_8327

5 业界动态

5.1 陕西省第三届网络通信安全管理员职业技能大赛成功举办

11月18日，由陕西省通信管理局与省总工会、省人力资源和社会保障厅联合主办的第三届陕西省网络通信安全管理员职业技能大赛成功举办。我局党组书记、局长高彩玲，纪检组长、王平凡现场观摩了竞赛。

本次大赛共有全省基础电信企业网络安全人员共56人参加，大赛内容主要包括网络安全相关理论知识和技术实操，比较全面地考查了各位选手在网络安全方面的实战能力。比赛分为笔试和机试两个部分，机试部分采用CTF竞赛模式，有20个题目环境，选手可选择任意一个环境，利用工具和技术手段，获得该环境中的KEY并提交得分。经过为期一天的激烈角逐，来自陕西移动的李佳选手获得冠军，陕西电信谢文博选手和陕西联通郭夏选手分获二、三名，陕西电信获团体优胜奖。

这次大赛的举办，进一步检验了我省通信企业的网络安全工作水平，提升了我省通信行业网络通信安全管理员的职业技能，促进了网络安全人才的相互交流和共同提高，有利于充分发挥员工的积极性、主动性和创造性，全面推动我省通信行业网络安全事业的快速发展。

5.2 第十一届政府行业信息化安全年会在京召开 聚焦大数据安全

11月4日至5日，由公安部网络安全保卫局、工业和信息化部网络安全管理局等单位指导，公安部第三研究所《信息网络安全》杂志主办的“第十一届政府/行业信息化安全年会”在北京召开。

本次会议主题是“新形势下的大数据安全”。会上，多位相关部委代表、行业代表和专家就大数据信息安全建设、大数据流量分析、网络边界数据安全等热点议题进行了交流探讨。

中国科学院院士郑建华结合当前信息技术发展趋势以及大数据技术的广泛应用做了“新形势下密码研究的思考”的主题发言。他表示，密码研究要紧紧围绕国家信息安全需求，面向实际应用，而当前我们的密码理论研究和密码实际应用的结合有待进一步加强。

公安部网络安全保卫局总工程师郭启全在讲话中提到，信息安全等级保护制度是我国的一项基本制度，这在网络安全法（草案）中已经得到了明确。互联网存在大量的安全风险，我们要进一步健全完善以保护国家关键基础设施安全为重点的等级保护制度。

国家信息中心网络安全部副主任李新友介绍到，大数据时代的各种不同的身份认证系统各自为政，身份认证在朝着简单易用、安全适应应用、柔性部署、低成本的方向发展。多安全等级、多认证模式、跨域互认的统一身份认证服务平台是一个解决之道。

来自80余家部委、行业、科研院所的代表，以及信息安全厂商代表共计140余人参加了此次年会。

5.3 我国网络空间防御技术取得重大突破 将改变网络安全游戏规则

11月13日消息 经科技部授权上海市科学技术委员会组织的测试评估，由解放军信息工程大学、复旦大学、浙江大学和中国科学院信息工程研究所等科研团队联合承担的国家“863计划”重点项目研究成果“网络空间拟态防御理论及核心方法”近期通过验证，测评结果与理论预期完全吻合。这标志着我国在网络防御领域取得重大理论和方法创新，将打破网络空间“易攻难守”的战略格局，改变网络安全游戏规则。

拟态，是指一种生物模拟另一种生物或环境的现象。2008年，中国工程院院士邬江兴从条纹章鱼能模仿十几种海洋生物的形态和行为中受到启发，提出了研发拟态计算机的构想。在科技部和上海市的共同支持下，拟态计算原理样机研制成功并入选“2013年度中国十大科技进展”。在此基础上，研发团队针对网络空间不确定性威胁等重大安全问题，开展基于拟态伪装的主动防御理论研究并取得重大突破，所提出的“动态异构冗余体制架构”，能够将基于未知漏洞后门的不确定性威胁或已知的未知风险变为极小概率事件。

2016年1月起，由国内9家权威评测机构组成的联合测试验证团队，对拟态防御原理验证系统进行了为期6个月的验证测试，先后有21名院士和110余名专家参与不同阶段的测评工作。测评专家委员会发布的《拟态防御原理验证系统测评意见》认为：拟态防御机制能够独立且有效地应对或抵御基于漏洞、后门等已知风险或不确定威胁。受测系统达到拟态防御理论预期，并使利用“有毒带菌”构

件实现可管可控的信息系统成为可能，对基于“后门工程和隐匿漏洞”的“卖方市场”攻势战略具有颠覆性意义。

邬江兴介绍说，我国是遭受网络攻击最严重的国家之一。据国家互联网应急中心数据显示，仅２０１５年的抽样监测，我国有１９７８万余台主机被１０．５万余个木马和僵尸网络控制端控制。由于现有的网络防御体制采用的是“后天获得性免疫”机制，先“亡了羊”，才能通过打补丁、封门堵漏来“补牢”，对于不能感知和认知的网络攻击几乎不设防，而拟态防御理论与方法能够有效应对这些问题。

邬江兴还表示，网络空间拟态防御理论与方法是全人类的共同财富，中国科学家愿意将这一技术与世界分享，为构建网络空间命运共同体作出贡献。

5.4 Three UK遭黑客入侵 600万用户的个人信息存在被窃危险

１１月18日，Three UK的网络数据库遭黑客入侵，黑客是使用其员工账号登录到客户升级数据库，并进入储存有超过600万用户个人信息的服务器内。这些个人信息包括姓名、电话号码、地址和出生日期等。Three UK公司方面称，他们已经在与警方和相关人员调查此事，黑客的目的是盗窃其高端智能手机，用户的财务方面信息将不会有危险。另外，公司还称将尽快调查清楚有多少用户受到这件事情影响，并会及时与他们取得联系。

Three UK称黑客此次入侵是为了盗取该公司的新款智能手机。他们通过8名Three用户的客户升级账号盗取了8台旗舰手机，另外入室盗取了近400台高端智能手机。目前警方已经抓获了3名犯罪嫌

疑人，分别是 48 岁的男子肯特、39 岁的男子艾什顿和来自曼彻斯特莫斯顿的一名男子。

术语解释：

❖ **漏洞：**指信息系统中的软硬件或通信协议中存在缺陷或不适当的配置，从而可使攻击者在未授权的情况下访问或破坏系统，导致信息系统面临安全风险。

❖ **恶意代码：**是指在未经授权的情况下，在信息系统中安装、执行以达到不正当目的的程序。

❖ **僵尸网络：**僵尸网络是被黑客集中控制的计算机群，其核心特点是黑客能够通过一对多的命令与控制信道操作感染僵尸程序的主机执行相同的恶意行为，如可同时对某目标网站进行分布式拒绝服务攻击，或发送大量垃圾邮件等。

❖ **拒绝服务攻击：**指向某一目标信息系统发送密集的攻击包，或执行特定攻击操作，以期致使目标系统停止提供服务。

❖ **网页篡改：**指恶意破坏或更改网页内容，使网站无法正常工作或出现黑客插入的非正常网页内容。

❖ **恶意链接（暗链）：**也称为黑链,被插入后将会被搜索引擎降权;对网站访问者造成不良影响;将会协助恶意网站(可能为钓鱼网站、反动网站、赌博网站等)提高搜索引擎排名，也意味着能被篡改页面。

❖ **网络仿冒：**指通过构造与某一目标网站高度相似的页面（俗称钓鱼网站），并通常以垃圾邮件、即时聊天、手机短信或页面虚假广告等方式发送声称来自于被仿冒机构的欺骗性信息，诱骗用户访问钓鱼网站，以获取用户个人私密信息（如银行帐号和账户密码）。

❖ **网页挂马：**指通过破坏网页并植入恶意代码或链接，致使用户计算机在访问页面时被植入恶意代码。

❖ **网站后门：**指黑客在网站的特定目录中上传远程控制页面从而能够通过该页面秘密远程控制网站服务器的攻击事件。

❖ **0Day：**指在系统商在知晓并发布相关补丁前就被掌握或者公开的漏洞信息。

❖ **APT攻击：**高级持续性威胁(Advanced Persistent Threat，APT)，APT是黑客以窃取核心资料为目的，针对客户所发动的网络攻击和侵袭行为。这种行为往往经过长期的经营与策划，并具备高度的隐蔽性。APT的攻击手法，在于隐匿自己，针对特定对象，长期、有计划性和组织性地窃取数据，这种发生在网络空间的偷窃资料、搜集情报的行为，就是一种“网络间谍”的行为。

❖ **域名劫持：**是通过拦截域名解析请求或篡改域名服务器上的数据，使得用户在访问相关域名时返回虚假IP地址或使用户的请求失败。

❖ **非授权访问：**指没有访问权限的用户以非正当的手段访问数据信息。非授权访问事件一般发生在存在漏洞的信息系统中，黑客利用专门的漏洞利用程序（Exploit）开获取信息系统访问权限。

❖ **路由劫持：**路由劫持是通过欺骗方式更改路由信息，以导致用户无法访问正确的目标，或导致用户的访问流量绕行黑客设定的路径，以达到不正常的目的。

关于我们：

国家互联网应急中心是国家计算机网络应急技术处理协调中心的简称（英文为 CNCERT 或 CNCERT/CC），成立于 1999 年 9 月，是一个非政府盈利的网络安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网网络安全事件预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络上重要系统的运行。国家计算机网络应急技术处理协调中心陕西分中心（简称陕西互联网应急中心或SNCERT）作为国家互联网应急中心在陕的分支机构，根据业务范围开展陕西省内互联网网络安全事件的预防、发现、预警和协调处置等工作，并负责编制印发《陕西省互联网网络安全情况通报》的具体工作。

联系我们：

联系人：戴小平　张修

电话：029-88450692

传真：029-88324040

网址：www.shxca.gov.cn