网络安全监测工作动态

2018 第 2 期（总第 2 期）

陕西省网络与信息安全测评中心　　4 月 1 日-4 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 9 个，存在严重高危漏洞的政府网站 55 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韩国、日本、美国、俄罗斯等国家和地区，占攻击总数的 1.62%，攻击手法主要为恶意扫描、CC 攻击、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 9 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 6 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 55 个网站存在高危漏洞，高危漏洞数量 56 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、信息泄露、弱口令等。

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 6913 个，其中，境外 IP 数 112 个，境内 IP 数 6801 个。

从攻击源 IP 分布情况看，目前境外 IP 主要集中在韩国、日本、美国、俄罗斯等国家和地区（如图 1），境内 IP 主要集中在江苏、浙江、北京、广东、上海和香港等（如图 2）。

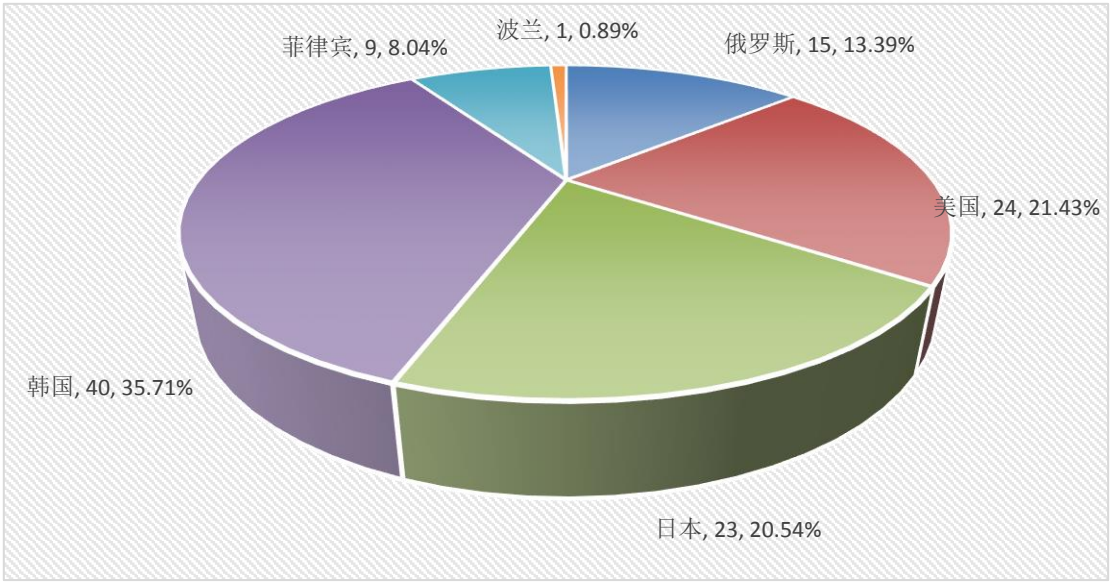

图 1 境外攻击源分布情况

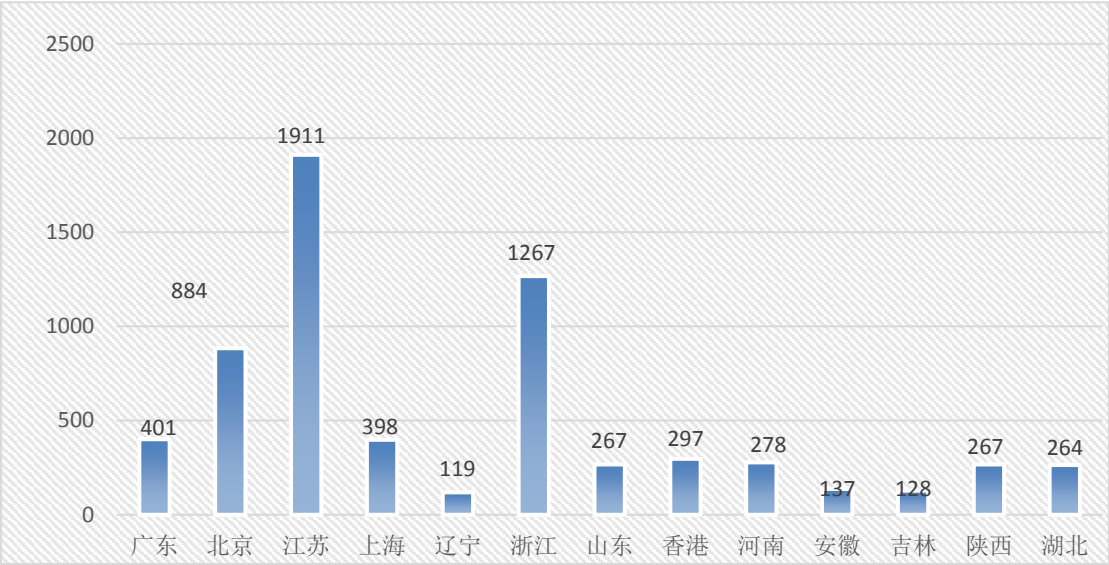

图 2 境内攻击源分布情况

（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 72.4942 万次恶意扫描和 58.2909 万次 CC 攻击，所有攻击类型及数量的主要分布情况如图 3。

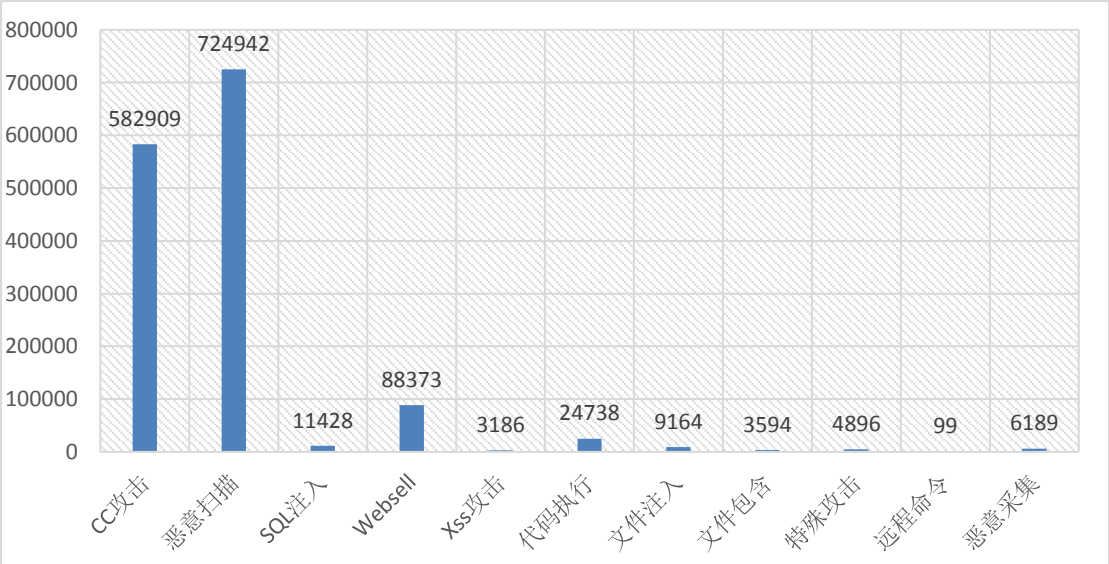

图 3 网站恶意攻击类型及数量分布

三、威胁播报

（一）Weblogic 反序列化远程代码执行漏洞预警

日前，发现Oracle（甲骨文）公司高危漏洞：Weblogic反序列化漏洞(CVE-2018-2628)，该漏洞由绿盟科技首先发现，并及时上报给了Oracle官方。

4月18日凌晨，Oracle（甲骨文）官方发布了4月份的关键补丁更新CPU（Critical Patch Update）,其中包含一个高危的Weblogic反序列化漏洞(CVE-2018-2628)，通过该漏洞，攻击者可以在未授权的情况下远程执行代码。

以下版本均在受影响范围内:

Weblogic 10.3.6.0

Weblogic 12.1.3.0

Weblogic 12.2.1.2

Weblogic 12.2.1.3

以上均为官方支持的版本

Oracle 官方已经在今天的关键补丁更新（CPU）中修复了该漏洞，强烈建议受影响的用户尽快升级更新进行防护。Oracle 官方补丁需要用户持有正版软件的许可账号，登陆https://support.oracle.com后即可下载最新补丁。[来源:安全牛]

（二）字体沦为“圈钱“工具 勒索软件无孔不入

更新字体、更换壁纸是很多网友的日常习惯，甚至是爱好，但在无孔不入的网络攻击面前，这种看似单一、安全的行为也变得“危机四伏”。近期，安全人员发现，新型勒索软

件 GandCrab2 会伪装成字体程序而感染用户电脑，加密照片、文档、视频等资料，并勒索高额赎金。趋势科技提醒消费者在使用电脑的任何环节都要警惕勒索软件的防范，并最好安装能够阻断勒索病毒恶意加密行为的安全软件，保护重要文件的安全性。

为了达到感染用户电脑的目标，网络不法分子首先通过网页挂马的方式，将部分网页改成乱码的方式显示，“提醒”网民只有更新字体才能完全显示网页。但实际上，该网页提供的“字体更新”程序却是经过伪装的勒索软件 GandCrab2，一旦消费者下载并安装，勒索软件将侵入到用户电脑，将照片、文档、视频等资料加密，并在原文件名之后加上.GDCB 后缀。

要避免 GandCrab2 等勒索软件的攻击，建议网民遵循以下几点建议:

1.不要轻易打开安全情况未知的网页或是软件，并留意安全软件的风险提示。如果确实需要更新字体等文件，应该尽量选择官方平台。

2.最好能养成定期备份重要文件的好习惯，备份的最佳做法是采取 3-2-1 规则，即至少做三个副本，用两种不同格式保存，并将副本放在终端以外的介质上。

3.安装安全软件，例如 PC-cillin 2018 ，其不仅能保护多个电脑资料夹，还可同时保护储存在云盘以及 USB 外

接储存装置上的文件。只要预先设定需要保护的文件夹，一旦有勒索病毒企图实施加密行为，“勒索克星”就能立即予以封锁，妥善的保护消费者重要文件的安全。[来源：安全牛]

（三）关于Drupal Core远程代码执行漏洞的安全公告

2018年4月26日，国家信息安全漏洞共享平台（CNVD）收录了Drupal Core远程代码执行漏洞（CNVD-2018-08523，对应CVE-2018-7602）。综合利用上述漏洞，攻击者可实现远程代码执行攻击。部分漏洞验证代码已被公开，近期被不法分子利用进行大规模攻击的可能性较大，厂商已发布补丁进行修复。

1.漏洞情况分析

Drupal是一个由Dries Buytaert创立的自由开源的内容管理系统，用PHP语言写成。Drupal在业界常被视为内容管理框架，而与一般意义上的内容管理系统存在差异。

2018年3月29日，CNVD收录了Drupal 6，7，8多个子版本存在远程代码执行漏洞，远程攻击者可利用该漏洞执行任意代码（http://www.cnvd.org.cn/webinfo/show/4463）。但由于Drupal官方对该漏洞修复不完全，导致补丁可以被绕过，造成任意代码执行：Drupal官方发布的漏洞补丁通过过滤带有#的输入来处理请求数据（GET，POST，COOKIE，REQUEST），但是Drupal应用还会处理path?destination=URL形式的请求，发起请求需要对destination=URL中的URL

进行编码，攻击者对 URL 中的#进行两次编码即可绕过 sanitize()函数的过滤，从而实现远程代码执行。

CNVD 对该漏洞的综合评级为“高危”。

2.漏洞影响范围

受影响版本：Drupal 的 7.x 和 8.x 版本受此漏洞影响。

修复版本：Drupal 7.59，Drupal 8.5.3，Drupal 8.4.8

CNVD 秘书处对该系统在全球的分布情况进行了统计，全球系统规模约为 30.9 万，用户量排名前五的分别是美国（48.5%）、德国（8.1%）、法国（4%）、英国（3.8%）和俄罗斯（3.7%），而在我国境内分布较少（0.88%）。[来源：国家信息安全漏洞共享平台]

（四）高危预警：无文件挖矿恶意软件 GhostMiner

来自 Minerva 实验室的安全研究人员最近就发现了这样一款被称为“GhostMiner”的新型加密货币挖矿恶意软件，该恶意软件采用了其他恶意软件家族所使用的最有效的技术，包括无文件（fileless）感染攻击。

所谓“文件攻击（fileless attack）”，其本质思想即攻击者希望恶意软件尽可能保持隐身来减少它们被检测到的概率，所以就要对受感染系统进行最少次数的干扰，以及在系统中留下最少的痕迹。恶意软件保持不被发现的时间越长，它们就越有可能实现其攻击目标。

因此，无文件恶意软件就要删除它在受感染系统磁盘中

保存的所有文件，在注册表中保存加密数据，注入代码到正在运行的进程，并使用 PowerShell、Windows Management Instrumentation 和其他技术使其难以被检测到。

据悉，该新型挖矿软件主要针对 Monero 加密货币，它使用了 PowerShell 规避框架——Out-CompressedDll 和 Invoke-ReflectivePEInjection，通过无文件技术来隐藏其恶意代码。

该恶意软件的每个组件都被设计用于不同的目的：一个 PowerShell 脚本用于确保将恶意软件传播到新机器，另一个用于执行实际的挖矿操作。

Minerva Labs 的两名研究人员 Asaf Aprozper 和 Gal Bitensky 透露称：“这种规避方法在绕过许多安全工具方面效果非常显著：我们分析的部分该恶意软件的有效载荷完全未被所有安全厂商发现。”

安全研究人员对比了使用和不适用无文件方法的恶意可执行文件的检测结果，并发现一旦无文件模块被移除，大多数 VirusTotal 供应商都能够成功地检测出这些有效载荷。

研究人员分析后发现，负责感染新设备的 PowerShell 脚本主要针对运行 Oracle WebLogic（利用 CVE-2017-10271 漏洞）、MSSQL 和 phpMyAdmin 的服务器。

不过，研究人员也表示，此次攻击只是试图利用了 WebLogic 服务器。在针对 WebLogic 服务器的攻击中，

GhostMiner 恶意代码会通过随机扫描 IP 地址，每秒创建大量新的 TCP 连接，试图找到易受攻击的目标设备。

通过基于 Base64 编码的请求和回复，就可以执行与命令和控制（C&C）服务器的通信。该恶意软件用来交换消息的协议涉及一个简单的握手，然后是执行各种任务的请求。一旦任务完成，一个新的请求就会被发送到服务器。

该挖矿组件是开源 XMRig 矿工（高性能的门罗币 CPU 矿工）的轻量定制版本，能够从内存中直接启动。

Minerva Labs 研究人员表示，在我们发现该恶意软件之时，其挖矿活动已经运行了大约 3 个星期，但是根据追踪到的加密货币钱包发现，攻击者到目前为止只获取了 1.03 个 Monero（约合 200 美元）。也许，攻击者还在使用研究人员尚未发现的加密货币钱包地址来获取收益。

GhostMiner 挖矿活动收益较低的另一个潜在原因是采矿活动的竞争过于激烈。潜在的受害者数量确实很多，但是他们使用的攻击和技术都是公开的，攻击者意识到他们的竞争对手共享相同的工具集，并尝试感染相同的易受攻击的目标设备。

研究人员表示，被分析的恶意软件样本中还包含各种技术，可以结束目标设备上运行的任何其它恶意挖矿进程。在 GhostMiner 的编码中，有一份采用硬编码的黑名单，通过 exe 文件格式将 GhostMiner 开发人员所知晓的一些其他挖矿恶

意软件列入黑名单中，然后通过使用 PowerShell 的“Stop-Process -force”命令行参数来终止和删除在目标设备上运行的其他挖矿程序。

最后，Minerva Labs 安全研究人员建议称，防御者可以使用与这些“竞争对手杀手”类似的方法来防止恶意挖矿程序在终端上运行。他们甚至提供了一个杀手脚本，可以为此目的进行修改。[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