# 2014：威胁“泛化”的年代漏洞频发

## —网络强国建设之漏洞

安天实验室 / 肖新光

**编者按：从 4 月份被称为 3 年来最严重的“心脏出血”漏洞出现，到 9 月更严重的漏洞“破壳”而出，再到外设与与智能硬件的“一切连接不可靠”，都似乎在说明 2014 年的 APT 攻击事件充满不寻常的漏洞利用技巧。关键漏洞的巨大能量和未知变数，已经在迫使我们去寻觅一个新的安全模型或思维。由此可见，威胁泛化的年代，网络强国建设的漏洞有必要涵盖包括思维模式在内的更广范围。**

早在一年前，在我们试图给出 2014 年的威胁预言时，给出了“Malware/Other”这个词，并把对应的中文名称为“泛化”。而 2014 年的安全漏洞与恶意代码的走向，俨然“一座座火山喷发，一个个神话破灭”，展开了威胁无所不在的泛化图景。

### 一、严重漏洞频发

2014 年 4 月 7 日，发生了被称为 3 年来最严重的漏洞 Heartbleed（心脏出血）漏洞，这个漏洞存在于开源密码技术库 OpenSSL，该漏洞会导致内存越界，攻击者可以远程读取存在漏洞版本的 OpenSSL 服务器内存中 64K 的数据，从而可以被用于获取内存中的用户名、密码、个人相关信息以及服务器证书私钥等敏感信息。由于 OpenSSL 使用非常广泛，因此这个漏洞影响到了包括 Google、Facebook、Yahoo 以及国内 BAT 在内的大型互联网厂商，以及大大小小的网银、电商、网络支付、电子邮件等各种网络服务厂商和机构。

漏洞存在于 OpenSSL 中已有两年之久，并后被谷歌研究员尼尔·梅塔（Neel Mehta）与网络安全公司 Codenomicon 的研究员发现，他们通知了 OpenSSL 组织进行漏洞修补工作。漏洞公告发布时已发布了修补漏洞的新版本 OpenSSL 1.0.1g，同时 Google 也比业界更早的修补了漏洞。而漏洞公布后，网络攻击者们也开始疯狂地获取数据，有人开玩笑地说，为了存放通过 Heartbleed 获取的数据，导致了硬盘价格的上涨。虽然言过其实，但其利用价值可见一斑。而当我们回看类似事件时，Codenomicon 等一些新锐公司为了提高知名度不负责任地发布 POC，也是威胁“泛化”的重要原因。

而到了 9 月，则再次曝光了比“心脏出血”更严重的漏洞——“Bash Shellshock”（破壳），由于 GNU Bash 更广泛的存在，导致其所威胁到的不仅仅是服务器系统，也包括了网络设备、网络交换设备、防火墙等网络安全设备，也包括摄像头、IP 电话等很多采用 Linux 剪裁定制的系统。经过研究发现，这个漏洞已经存在了近 20 年。而另一个致命的问题是，由于 GNU Bash 的分布蔓延极广，几乎是无法完全定位修复的；而且由于 Bash 灵活的语法，导致解析程序极为复杂，因此在几次修补方法公布后，都随即被发现了新的问题，从而使“破壳”演化了一系列的漏洞。

再之后一场持续的 DDoS 攻击，严重影响到了国内 DNS 体系的运行，而大量发起攻击的节点则是摄像头等在网智能设备，而经跟踪分析相关僵尸网络，其正是利用了“破壳”扩展获取了大量的节点。

其实在一些国产操作系统上，我们也同样发现了“破壳”漏洞的存在，理顺国产系统的借鉴、继承关系，及时联动地漏洞修补，对于依托开源体系发展的国产操作系统领域来说，依托开源软件的伪闭源系统，其实比开源软件本身有着更大的漏洞威胁。

此外，HTTPS 作为安全认证和加密通信的重要基础协议，在这一年被反复提起，微软 SERVER 的 SSL 实现也被发现存在问题，而多家网银亦都被暴露出不正确的代码实现。

## 二、外设与与智能硬件

2014 年前，还没有更多的目光关注到外设的安全之上，人们对“连接不可靠”的认知更多来自网络端。而 2014 年 7 月 BlackHat 演讲题目的公开，预告了柏林 SRLabs 的安全研究人员 JakobLell 和独立安全研究人员 Karsten Nohl 将在 8 月 7 日展示“BadUSB”的攻击思路后，关于 USB 一系列的攻击传说，就这样被呈现出来。

“BadUSB”利用了 USB 接口具有极大的通用性，以及可以用来连接存储、键盘、鼠标、打印机等很多外设的特点，通过使用控制器芯片模拟其他外设，可以在 U 盘等形态的掩盖下发动攻击。而这种“非正常的使用方式”已经超出了规划者的安全想象，从而使这种攻击极难防范，同时这种威胁的有效性和隐蔽性，远非软件层面的“Autorun”问题可比，也远非类似修正一个系统自动运行通告的配置所能防御。而如果在之前已经考虑了 1394 火线、PCMCIA、PCEXPRESS 等接口的问题，就会让人们深刻意识到“一切连接均不可靠”。

在斯诺登爆料出的“NSA 的 ANT 装备列表”中，部分专家推测其中的 COTTONMOUTH（水蟒蛇）的系列装备看起来已经使用了类似攻击方法（当然对此也有分歧，因为从其有限的描述上无法证实这点），相关装备列装的时间早在 2008–2009 年间。而 2008 年，也是安天在 XCon 上演示 USB 攻击打印机的那一年，现在我们可以公开谜底了，当年没有人猜对结果的、通过打印机实现远控终端的演示，其实就是采用了今天看起来已经非常简单的“BadUSB”的思路。

而 2014 年全年各种智能设备的安全问题“则如同秋天的熟苹果般纷纷坠落”，2014 年 10 月著名极客嘉年华活动 GeekPwn 就展示了一个未来智能设备可能受到威胁的途径和预言，在现场 Show 和 PWN 的环节则演示了包括了电动汽车、智能手环、智能电视、智能插座、智能马桶、智能灯泡等等智能产品的各方面安全问题。

## 三、APT 在继续

见证 APT 攻击，正在成为安全工作者的常态。而其中的威胁和漏洞利用，亦能看到很多有趣的技巧。

在 Havex 攻击中，WordPress 漏洞被攻击者用于构成窃密回传的体制，这种思路非常巧妙，它使 C&C Server 不再是那些“生僻”域名或者 IP，并使在过去几年被证明为非常有效的域名信誉，也不再像那些在 BLOG 系统上张贴 Base64 编码的攻击显得那样奇葩。而网络上存在着大量具有类似漏洞的 WordPress 主机，从而也使攻击会有很好的掩盖。

而 SandWorm 及其使用的 CVE–2014–4114 漏洞，基本上使微软建立的内存安全机制统统失效，其原因在于其本质上并不是一个溢出，而是一个执行逻辑漏洞，相反则是类似 UAC 这样的应用安全策略可能会有一定作用。尽管并不是第一个漏洞使用这样的技巧，但在微软溢出保护机制日臻成熟的时候，也许未来会看到更多另辟蹊径的攻击方法。而 SandWorm 给人留下深刻印象的另一个原因，是其在微软修补前将这个漏洞曝光，从而引发了大量利用这个漏洞的攻击行为，起到了“撒豆止骥”的效果，以保证正牌的攻击者“金蝉脱壳”。2014 年的 APT 攻击事件，似乎必须要提及索尼被攻击的事件。但当一个攻击以敲诈式的警告于前，而以破坏硬盘数据为结尾的时候，它还是一种 APT 吗？也许与 Michael 在《Why Stuxnet Isn't APT》那种质疑一样，索尼事件也许是一种作战行动。

同时，我们还要再次强调， APT 不是一个纯技术行为，而是具有明确战术甚至战略目标的体系化攻击行为。因此，不要幻想任何的单点技术手段可以解决问题。

## 四、“幻像”破灭与安全观的重建

2014 年，威胁泛化的年代，是一个打破幻像的时代。例如之前所谓的开源安全神话，当少数开源安全论者还在坚持着“开源是全世界一起做一个系统，闭源是少数人做一个系统”的时候，社区因安全能力不平衡所带来薄弱环节的影响正在凸显。Heartbleed 就在最常见的 OpenSSL 中展示了“灯下黑”的结果，并提醒业界这正是达成安全所需要聚合的安全专业性、研究能力以及配

套的安全成本。而另一方面，心脏出血后这场针对开源系统安全普查的业内联合行动，或许可以被看成一场灾难的“进步补偿（恩格斯语）”。这种活动让开源体系真的从全域威胁的角度获得了审视。而 Wirelurker（破界），同样让 iOS 的安全神话破灭。

2014 年，关键漏洞再度展示了“一览众山小”的巨大能量，其让原有的那些漏洞数量的比对和哪种系统更安全的空泛讨论完全失去了意义，关键漏洞给攻防双方都带来了很大的不确定性和偶然性，信息攻防强弱之能力可能在瞬间被一个关键漏洞拉平。

泛化的年代是一个盲目的时代，当新威胁被反复强化，我们很容易被吸引而目光游移，我们很容易完全去关注新威胁，而不去分析我们的基础和家底，而后者同样重要。比如在 Heartbleed 中，同样令人值得思考的问题是研究者们同时注意到，国内网站的 HTTPS 使用比率很底，大量网站依然采用 HTTP，包括有著名的网站（包括手机端）居然采用明文登录协议，安全措施只是口令计算了一个 Hash 而已。这实际上是中国和发达国家在安全基础意识和能力上的代差。

而今年同样流行着对“老三样”——即“防火墙”、“反病毒”、“打补丁”的口诛笔伐。这种声讨被用于支撑去寻觅一个新的安全模型或思维。但实际上，在中国更多政企用户中更真实的情况是大量防火墙被采购后，被束之高阁，从未被安装和加电；内网反病毒产品的病毒库几月到半年才升级一次，而“打补丁”更被视为有可能影响业务稳定性的危险举动。我们现有的安全问题更多的是来自“老三样”不管用，还是没有真正重视和有效使用？

从互联网安全服务规范到 IT 治理能力，我们在安全上有很多课要补，我们并非已经建立了充分夯实的体系，可以把目光充分转移去审视新威胁，而是需要同时面对新旧两种挑战。而如果我们漠视这些现状，就会催生不切实际的误判，特别是开始膜拜和憧憬所谓一劳永逸改变安全现状的“永动机”，而忘记了安全的本质就是永无休止的对抗与改进。

泛化的年代亦可能是一个麻木的时代，比“心脏出血”更为严重的“破壳”漏洞却难以得到更多来自国内媒体的关注，原因竟然是很多人认为“心脏出血没有造成那么大的影响”。当一些主流网站（包括电商）的内存数据被以 T 为计的获取时，我们实在无法想象，还有什么是更大的影响。只有大面积断网、大量的后台数据被直接公开才算重大影响吗？这是一种何其落后的安全判断标准，这种思维定式足以使人在即将喷发的火山口上载歌载舞。

威胁泛化出现的原因，首先是信息化大发展注定使其无所不在，而很多的陷阱、隐患和错误的思维在不断地被继承，这是威胁泛化注定的土壤；其次是攻击能力的普及化，正如 Bruce Schneier 在《The State of Incident Response》所说“正在发生而且真正重要的趋势是，越来越多战争中的战术行为被应用于更广泛的网络空间环境中”，这为加速威胁泛化提供了工具弹药；而地下黑产的蓬勃发展，追名逐利日益无底线，也成为威胁泛化的持续动力。

泛化的年代，让很多人重新萌生了计划经济式的预设情节，对安全的恐慌，导致很多关于“不设计好安全就不要发展的观点”重新浮出水面。这些观点忽略了需求的刚性，认为通过沙盘推演和标准设定能解决很多问题。

在威胁泛化的年代，更多人会想到 K.K 的《失控》，而一位我十分尊重的老师告诉我，在他的案头有两本书，一本是《失控》，而另一本是来自比尔 . 盖茨的《未来之路》，他说“从目前来看，对于一个未来的高技术的世界，前者带给人们的焦虑和恐慌远胜于后者曾带给人们的憧憬，但想一想，蒸汽机、电器机、原子能、基因技术……哪一项巨大的技术进步不曾带给人类巨大的、仿佛毗邻悬崖边缘的焦灼？但这一切尽管亦曾被用于破坏、犯罪和战争，但最终我们的世界始终是变得更文明、发达和美好。”

安全的存在意义从来都是用于保障应用价值，而不是用来限制应用价值，更不是用来捆住发展的手脚。而今天，尽管我们面对种种安全危机，以及伴生的对未来的种种焦虑，但我们一直坚信发展、进步才是最大的安全。

安全工作者要做实干者，而非预言家，也许这一选择更适用于“沧海横流”的时代。（感谢我的同事 Angel Li 及业内友人 Joe 对本文的贡献）