SECURITY NSFOCUS

NSFOCUS

2014 H1 DATA BREACH REPORT

2014 H1 绿盟科技反数据泄露报告

内容摘要

目前就信息安全威胁来说，最为常见的两种形式是拒绝服务和数据泄露。随着国内信息技术的不断发展，“拖库”之类的数据泄露事件也越来越多。为此，绿盟科技威胁响应中心每天都在持续追踪及研究，并定期发布相关报告。此报告即为《2014 H1 绿盟科技 DDoS 威胁报告》的姊妹篇，用以快速反馈数据泄露的发展态势，给大家提供更多这方面的信息。

目前，数据泄露的尚无统一定义，例如：

- 美国审计总署（GAO, Government Accountability Office）对数据泄露（data breach）的定义是：“ **unauthorized** or unintentional exposure, disclosure, or loss of sensitive information, including PII（Personally Identifiable Information）”[1]；
- US-CERT 对数据泄露的定义：“The **unauthorized** movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.”[2]

虽然两个定义在细节方面略有差异，但其共同之处是：**在未授权的情况下，数据被外部获取**。此处“数据”载体是电子形式或纸质形式。

目录

更多资源请访问：

HTTP://WWW.NSFOCUS.COM/4_RESEARCH/4_6.HTML

关键发现

2

2014 年上半年共记录数据泄露事件 485 起，平均每天数据泄露事件超过 2 起

40%

2014 年上半年企业（例如科技公司、零售业）遭受数据泄露事件占总数 40%

Tuesday

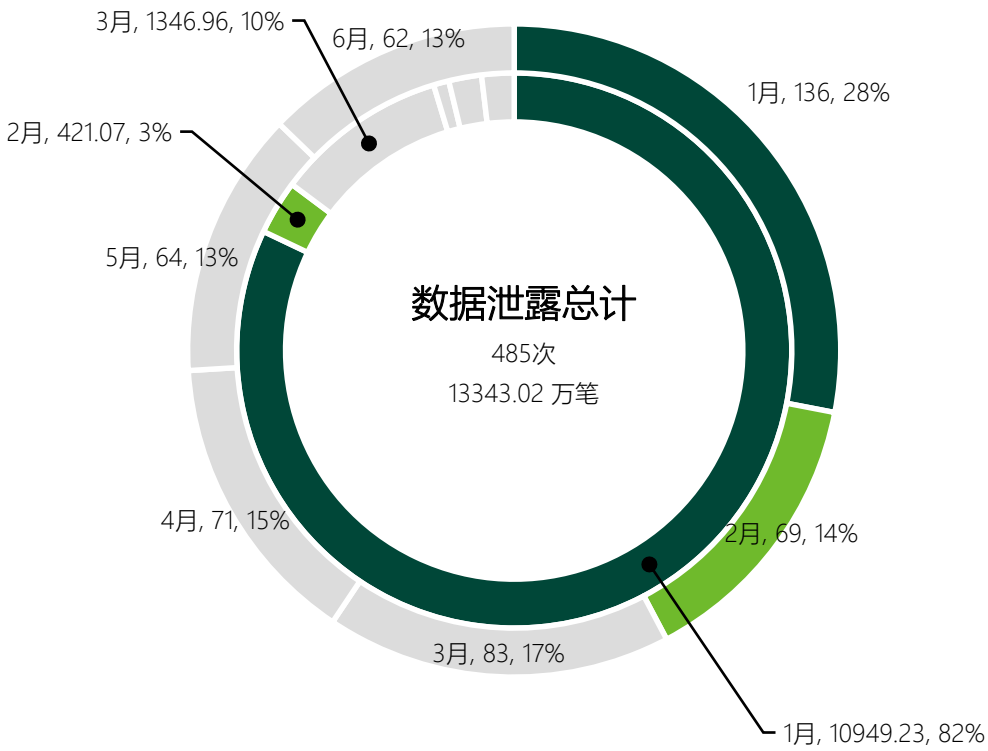
2014 年上半年周二记录的数据泄露事件最多，而周日记录的数据泄露事件最少

[1] http://www.gao.gov/assets/670/662227.pdf
[2] http://niccs.us-cert.gov/glossary

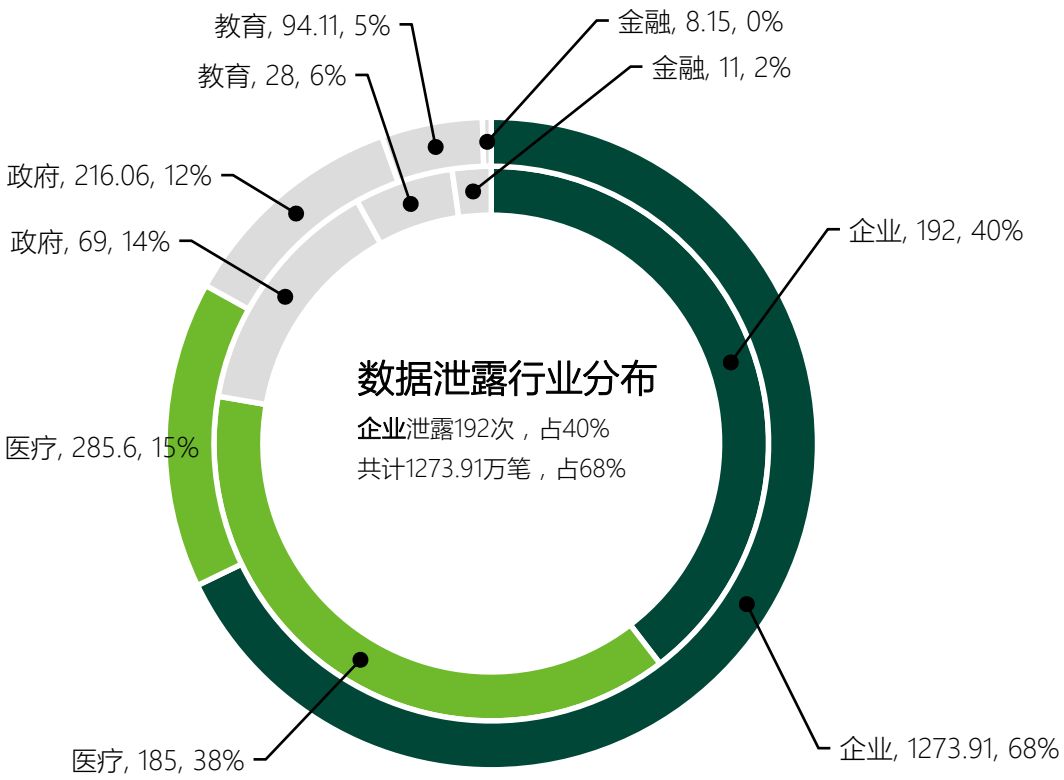
数据分析

2014 年上半年在全球范围内相继爆出 eBay、Michaels Stores 等重大事件数据泄露事件。5 月 21 日全球最大拍卖网站 eBay 官网发布通告，称因数据泄露呼吁其用户更新密码。eBay 事件只是一个缩影，它反映了当前数据泄露问题所面临的挑战。

首先，数据泄露事件层出不穷，简略看一下近期数据泄露事件，UPS（8.20）、WSJ（7.22）、CNET（7.14）、Cupid（6.25）……需要注意的是，在媒体上出现的数据泄露事件其实只是很小的一部分。根据绿盟科技威胁响应中心监测到的数据泄露数据，在 2014 年上半年共记录数据泄露事件 485 起，平均每天数据泄露事件超过 2 起。

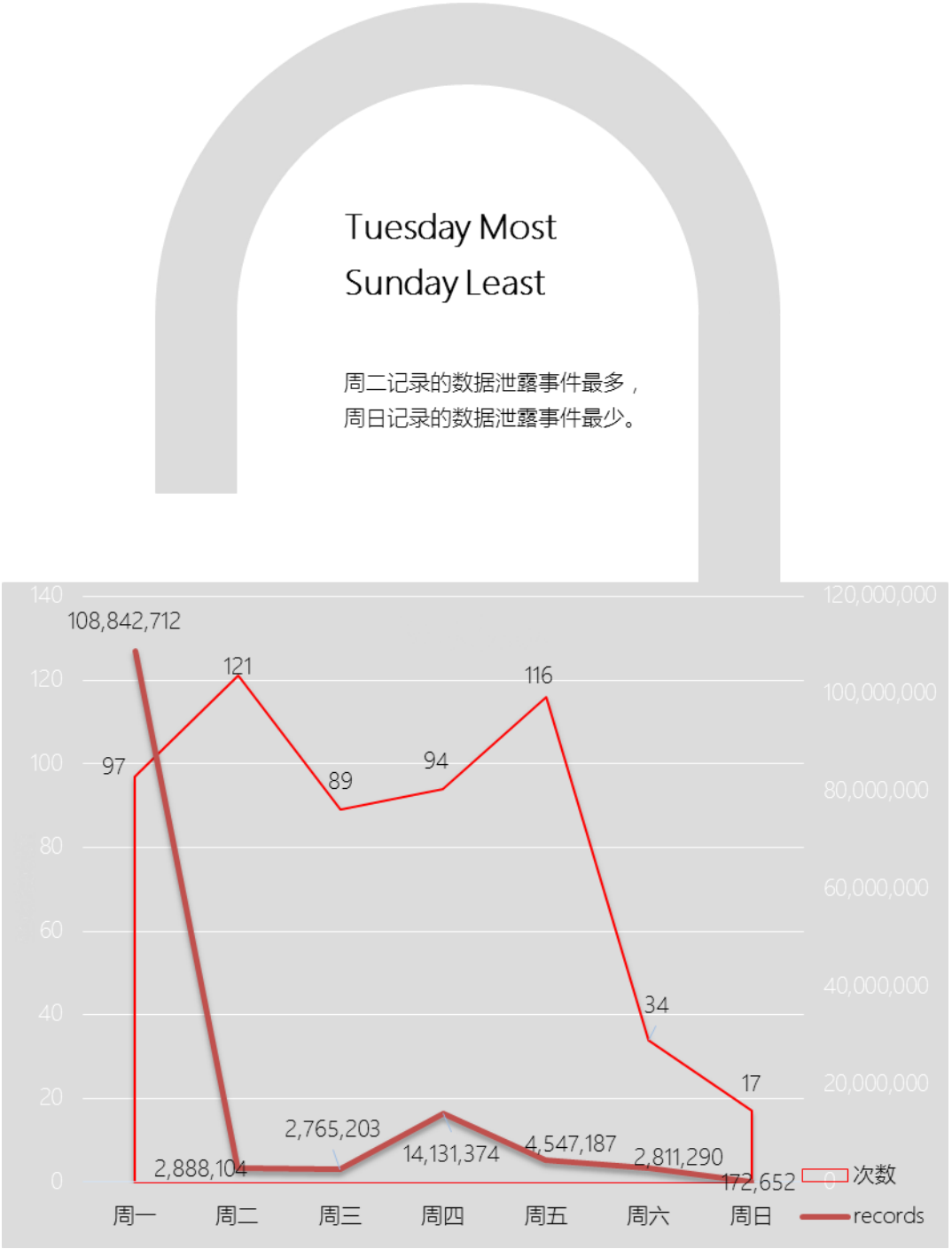


其次，数据泄露事件受影响对象的构成日趋广泛。从全球范围看，近年各行业数据泄露事件呈上升趋势。金融行业占据的比例较小，一方面的原因是由于金融行业是网络犯罪分子的明显目标之一，与其它行业相比，金融行业在网络安全方面给予更多的关注，并且在安全信息共享方面建立了交流渠道，例如：FS-ISAC[3]以及监管方面有来自类似 FFIEC[4]机构的规范与指导，与此相对应的是企业（例如：科技公司、零售业），最近 4 年的重大数据泄露事件均属于该类别，例如：Adobe（2013 年）， Sony（2011 年）以及 Target（2013 年），下图从一定程度上反映了各行业面对数据泄露的严峻程度。



[3] https://www.fsisac.com/
[4] http://www.ffiec.gov/

2014 年上半年数据泄露事件按周统计如下图，通过观察可看到到周二记录的数据泄露事件最多，而周日记录的数据泄露事件最少。



从上述几幅图中可以了解到时间、行业与数据泄露事件存在的若干关联，即通过统计数据从整体描述数据泄露现状，下一节“案例分析”将通过具体案例剖析现实数据泄露事件，以直观形式说明数据泄露事件的过程与后果。

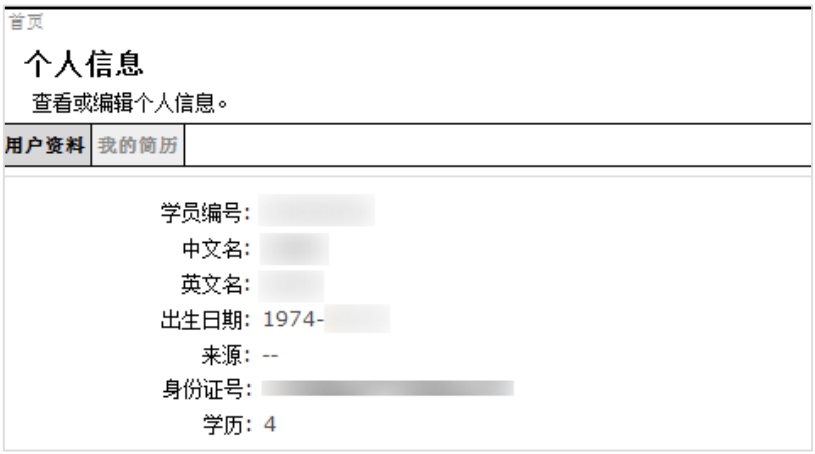
案例分析

国内案例

绿盟科技云安全运营中心近期监测到一起由编程错误导致的严重数据泄露事件，事件涉及企业在国内具有相当高的知名度。这家企业官网存在身份验证绕过漏洞，攻击者利用该漏洞绕过认证机制，执行未授权的用户个人信息访问。

绿盟科技云安全运营中心在第一时间检测到对个人信息的未授权访问，并及时响应处理，最大程度较少了该企业用户因数据泄露所导致的损失。

下图是该企业个人信息所包含的部分内容，例如：姓名、出生日期、身份证号以及用户组等信息，



经分析发现该网站使用 WebSphere 应用服务器 8.5.5 版本搭建。身份验证绕过的常见方法包括：SQL injection、Session prediction、Parameter modification 等，对于此泄露事件，使用基本的绕过方法 Direct request[5]即可绕过这家企业官网的身份验证。Direct request 是指网站开发人员原本设想是由登录用户才能访问的网页，却能被非登录攻击者直接访问。这种编程方式存在错误，网站开发人员在网页设计中，仅在登录页面实施了访问控制，即假设如果网页可以被打开，那么访问者必定有相应权限。攻击者利用该漏洞绕过身份验证，“顺藤摸瓜”最终导致数据泄露事件的发生。针对此绕过漏洞的基本解决方法也较为简单，即先验证访问者身份，再确定是否有权限访问。

类似这样的编程错误，在 Verizon 2014 DBIR（Data Breach Investigations Report）报告中称为“Miscellaneous Errors”。该报告将安全事件划分为九个威胁模式，编程错误所导致的数据泄露所占比例是 3%[6]。

[5] http://cwe.mitre.org/data/definitions/425.html

[6] http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf

国外案例

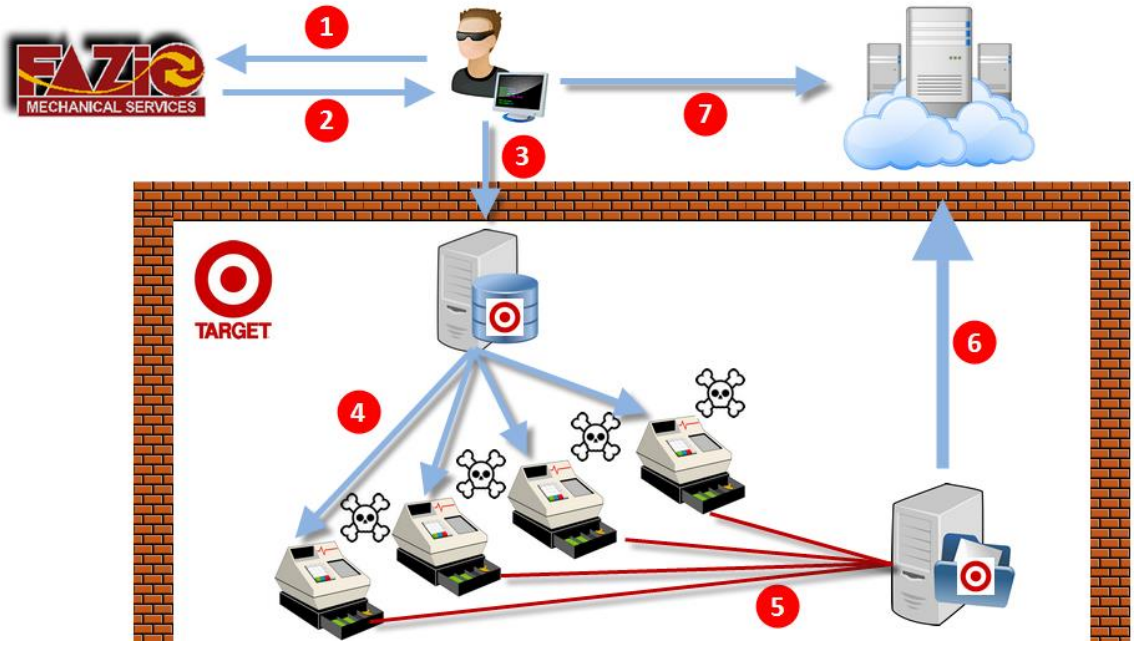
简述

2014 年上半年全球公开的部分数据泄露事件：

上图数据泄露事件中，eBay、Korea Credit Bureau （韩国信用评价公司，简称 KCB）与 Michaels Stores 三者因影响用户数量众多，故受到公众的关注。eBay 事件是由攻击者在对该公司员工进行成功 spear phishing 攻击后，利用员工的登录帐户信息进入未授权访问公司网络，最终导致 eBay 用户数据泄露。KCB 事件是由 KCB 内部员工利用职务之便复制及倒卖用户信用卡数据，从而导致 KCB 持卡人数据泄露。Michaels Stores 事件是由 Michaels Stores 的 POS（Point of Sale）系统被入侵，进而导致 Michaels Stores 顾客数据泄露。Michaels Stores 事件、Target 事件与 Neiman Marcus 事件是近期零售业遭受数据泄露的三大案例，由于 Target 事件的典型性以及该事件引发的深远影响，例如：Target 超市 CIO 与 CEO 先后引咎辞职后，触动许多公司管理层开始审视自身的网络安全状况；美国零售联合会（NRF，National Retail Federation）开始建立安全信息分享平台[7]；美国国会已考虑通过新的立法，以加强零售行业的安全防护等，所以本次报告重点分析 Target 超市的数据泄露案例，并且坚信 Target 事件会成为数据泄露史上的经典研究案例之一。

以下简述 2013 年 11 月俄罗斯攻击者窃取美国第 2 大超市 Target （NYSE：TGT） 4 千万用户银行卡数据的攻击过程[8]。

[7] https://nrf.com/media/press-releases/national-retail-federation-announces-information-sharing-platform
[8] http://krebsonsecurity.com/



- **第 I 阶段**：城门失火，殃及鱼池　　时间：2013 年 9 月
  - 1：攻击者通过 spear phishing 攻击，在 Fazio Mechanical Services 公司（该公司主营 HVAC [即空调暖通]，以下简称为 Fazio）系统上安装恶意软件 Citadel；
  - 2：通过恶意软件 Citadel 窃取了 Fazio 公司远程访问 Target 超市（以下简称为 Target）Ariba 计费系统的账户信息。这种“假道伐虢”的跳板攻击又被称为 island-hopping 攻击[9]；
- **第 II 阶段**：千里之堤，溃于蚁穴　　时间: 2013 年 11 月 15 日 ~ 2013 年 11 月 30 日
  - 3：攻击者将恶意软件 BlackPOS（RAM scraper）变种 POSRAM 上传到 Target 超市 POS 程序升级服务器上；
  - 4：恶意软件 POSRAM 被安装到 Target 超市各 POS 终端（POS 终端品牌：Retalix[NCR]）；
- **第 III 阶段**: 巧偷豪夺，瞒天过海　　时间: 2013 年 12 月 2 日 ~ 2013 年 12 月 15 日
  - 5：恶意软件 POSRAM 开始从各 POS 终端收集的银行卡等数据上传到 Target 超市的文件共享服务器上；
  - 6：从 Target 超市文件共享服务器将收集的数据（11GB）上传到 FTP（迈阿密、巴西）服务器上；
  - 7：攻击者（IP 归属俄罗斯），通过 VPS（Virtual Private Server）访问该 FTP 服务器，并取走数据。

反思

数据泄露事件发生后，最常见的场景是：A.用户抱怨 B.媒体质疑 C.业界批评 D.政府追查

应急措施（即遭受数据泄露的企业/组织对其用户采取相应的例行做法），例如：

- 针对网站账户信息泄露: 重置用户密码、请勿密码重用、谨防诈骗邮件
- 针对银行卡信息泄露: 监视信用卡异常、提供身份信息窃取防护

[9] Varun Dutt, http://www.hss.cmu.edu/departments/sds/ddmlab/papers/Duttetal2011.pdf

上述场景在 Target 事件后再次重现，后续安全建议/事后分析即使称不上不绝于耳，也至少是屡有耳闻，例如下述分析角度：

A.重视应急计划[10] B.PCI 只是最低纲领[11] C.正确处理安全告警[12] D.考虑安全薄弱环节[13]

这四个观点从不同观察角度总结了 Target 事件中警示与教训，若以此为鉴无疑将有助于着眼未来。在 Target 事件中其 1797 家门店受到波及。连锁店经营方式经常为了统一部署简化 IT 运维而使用类似/一致的系统，其优点在于标准化、规模化与低成本、高效率有着近似直接的换算关系；但从另一角度看：由于部署相同终端系统，从而可能导致同一漏洞暴露于攻击者的准星下。无疑，Target 在安全防护方面曾给予不少投入。2013 年 5 月投资购买 FireEye 的恶意软件检测工具；2013 年 9 月通过 PCI DSS（Payment Card Industry Data Security Standard）认证。目前这种安全管理思路较为常见：企业/组织寄希望于通过单纯购置安全防御设备方式提高安全防护水平，但忽视周期性安全服务检查等方面。

Target 数据泄露事件发生后，Target 发言人称“Target was among the **best-in-class** within the retail industry”[14]，与此形成反衬的是，对于攻击者技术水平，安全业界人士认为“this class of attack is **far** from advanced”[15]。诚然，Target 事件暴露出其若干安全问题，它也理所应当应为自己的管理和疏忽担负责任，因为先进的工具与行业的标准毕竟需要人去使用与执行，但是 Target 最大问题可能在于它对当前网络安全现状缺乏足够 vision（前瞻性），例如：Target SOC （Security Operations Center）团队的主要职责仍是对超市卖场区域的安全监控，而不是防范网络攻击（Target 在班加罗尔的安全团队监测到异常

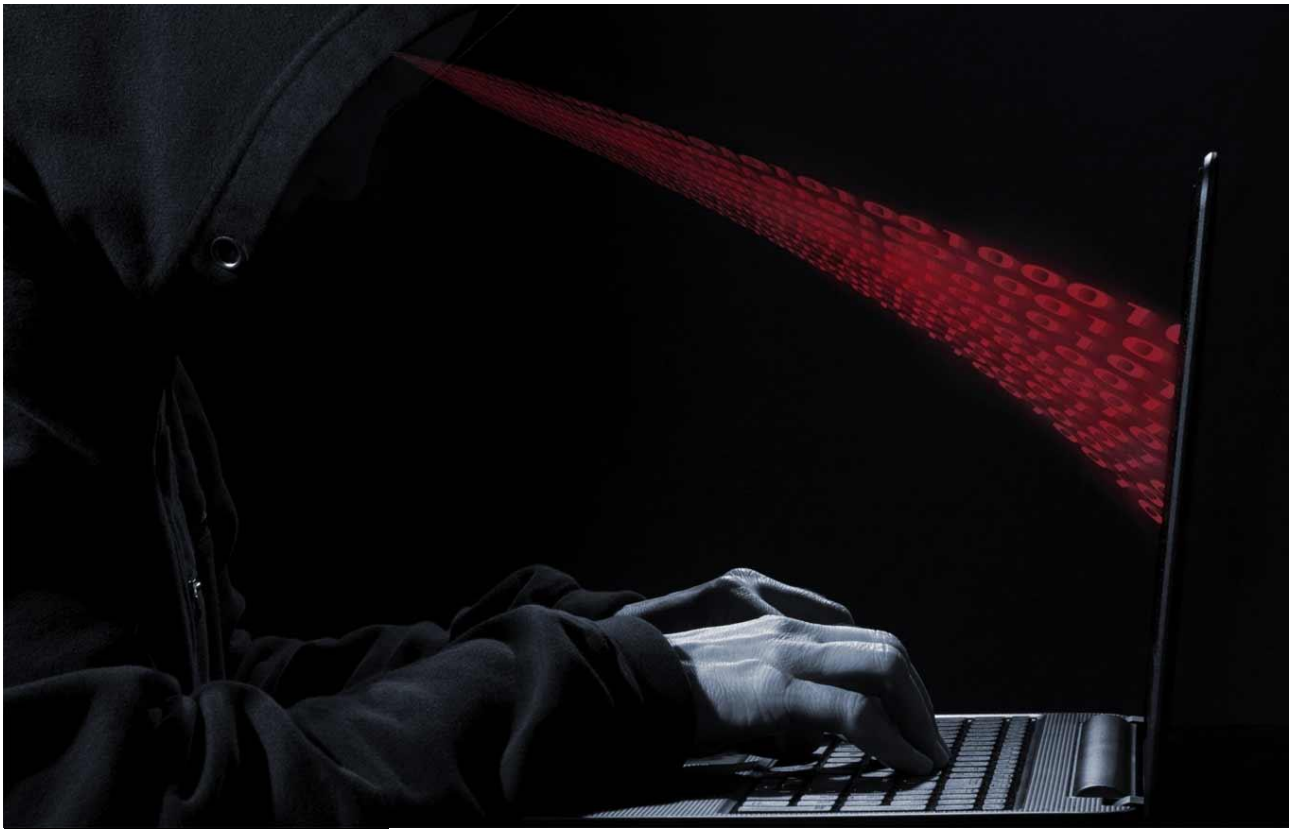
[10] http://blogs.wsj.com/riskandcompliance/2013/12/20/how-to-prepare-for-a-target-type-data-breach/
[11] http://www.technewsworld.com/story/80160.html
[12] http://www.darkreading.com/attacks-and-breaches/target-ignored-data-breach-alarms/d/d-id/1127712
[13] http://www.cio.co.uk/insight/security/lessons-cios-can-learn-from-target-breach/
[14] http://www.nytimes.com/2014/05/29/business/advisory-group-opposes-re-election-of-most-of-targets-board.html
[15] 《Mcafee Labs Threats Report Report Q4 2013》 (第 7 页)

状况后已通知 Target SOC，但未引起后者重视）[16]。面对日趋严峻的网络安全现状，难道 Target 真的是不了解“今是何世，乃不知有”pwned 吗？

毋庸置疑，Target 数据泄露事件也反映了目前安全防护技术需要进一步提升，例如 Target 同时部署了 FireEye 恶意软件检测工具与 Symantec 终端防护产品，前者使用 MVX（Multi-Vector Virtual Execution, 一种 VM-based 的 signature-free 检测方法）检测恶意软件，虽具有自动删除恶意软件功能，但因其存在误报，所以 Target SOC 团队手动关闭了该项功能；后者使用 signature-based 检测技术，只能检测出 45%的恶意软件，因此 Symantec 高级副总裁 Brian Dye 在 2014 年 5 月称“（Traditional）**antivirus is dead**”[17]。简言之，这两个安全产品一个使用 signature-free 检测方法，一个使用 signature-based 的检测技术，但存在着误报（FP，False Positive）等问题，误报对用户的影响就像一遍遍的喊叫“狼来了，狼来了……”，结果狼没来，却使得用户对安全告警信息逐渐麻痹，等到狼真正来时只能嗟悔无及。

虽然现有安全产品存在不足，但从误报问题看如果将各安全产品告警与本地其它日志等信息之间自动关联起来并给予告警相应威胁等级，即通过信息关联监测用户网络的安全状况，从而可以提高安全告警的准确性。Verizon DBIR（Data Breach Investigations Report）报告曾指出 84%数据泄露事件可以在遭受数据泄露企业/组织的日志中发现蛛丝马迹[18]。当然，这种方法实现起来并不就是 plain sailing，例如关联日志事件的时间开销等问题。目前，网络安全研究课题除了关注在攻击时综合多种信息源发现攻击者等方向外，还有关注于通过收集多种信息对攻击提前预警（而不是攻击时的告警）的研究，例如：BlackForest[19]。总之，面对今日之网络攻防现状，目前的安全防护技术需要有动力去“Change!”

“案例分析”这部分提及的建议是面对数据泄露事件的事前事中事后，检讨值得今后改进的若干地方，但现实燃眉之急是层出不穷地数据泄露事件如何最大程度减小或阻止，具体反制对策请看下一节"方法分析"介绍的 Intrusion Kill Chain 模型。



16 http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data
17 http://betanews.com/2014/05/07/symantec-antivirus-software-is-dead-and-only-catches-45-of-cyberattacks
18 http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf
19 http://gtri.gatech.edu/casestudy/blackforest-gtri-aggregates-cyber-threat-informati

方法分析

Intrusion Kill Chain（或称为 Cyber Kill Chain）模型由 Lock Martin 公司 Eric M. Hutchins 等三位安全研究员在 2011 年 3 月举行的 ICIW 大会[20]（International Conference on Information Warfare and Security）上公布。

“Intrusion Kill Chain”模型精髓在于明确提出网络攻防过程中攻防双方互有优势，防守方若能阻断/瓦解攻击方的进攻组织环节，即是成功地挫败对手的攻击企图，毕竟没有一个防御战局完全由防御因素组成（no defensive campaign is composed of purely defensive elements）[21]。Intrusion Kill Chain 模型是将攻击者的攻击过程分解为如下七个步骤: Reconnaissance（踩点）、Weaponization（组装）、Delivery（投送）、Exploitation（攻击）、Installation（植入）、C2（控制）、Actions on Objectives（收割），如下图：

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	“chroot” jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

来源: Lockheed Martin[22]

上图第一栏的七步组成“Intrusion Kill Chain”；第五栏的 Tarpit 源于 tar pit （沥青坑），其含义是指提高网络连接延迟以慢制快。攻击者如能完成整个过程，则表明其进行了一次成功攻击（七步一杀）。Intrusion Kill Chain 是从防御者角度看“Kill Chain”，攻击者需要“步步为营”以完成攻击，而防御者可以在任一环节进行阻断。虽然具体阻断措施需要数据、经验等因素支持，但是从该模型角度看，防御者不一定处于被动角色，而攻击者也并无本质优势（即使攻击者手中有 0day 漏洞）。

在 Target 事件后，美国参议院 CCST 委员会使用 Intrusion Kill Chain 方法对此事件进行案例分析[23]，其出发点是引导美国公众/公司有效使用 Intrusion Kill Chain 方法，进而提高安全防护水平。该分析报告指出，从 Intrusion Kill Chain 角度看，Target 一而再、再而三的错失良机，最终了导致攻击者成功窃取数据。

[20] http://academic-conferences.org/iciw/iciw2011/iciw11-timetable.htm
[21] Clausewitz,《On War》, On The Culminating Point Of Victory
[22] Eric M. Hutchins, www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
[23] U.S. Senate Committee on Commerce, Science & Transportation (**CCST**), 《A "Kill Chain" Analysis of the 2013 Target Data Breach》

需要注意的是 Intrusion Kill Chain 适用的场合，例如该模型假设攻击者在攻击过程中会 Installation（植入）后门程序，然而一些攻击场景（例如窃取身份信息）并不需要此步骤，案例如 2013 年 FBI 利用 Firefox 漏洞追踪 Tor 网络用户身份的攻击方法[24]。

“案例分析”这部分推荐的 Intrusion Kill Chain 模型是一种框架具有较强的普适性，实际运用的要点在于具有识别攻击者踪迹的能力以及比攻击者更快的反制措施实施能力，否则一步之差，可致乾坤逆转！

数据泄露报告

在网络攻防双方持续多年的魔道之争中，攻击方的动机多样化体现了时代的变迁，for fun（geek and nerd）、for money（cybercriminal）、for politics（hacktivist）与 for data（state- sponsored cyber-warrior，以下简称为 cyber-warrior），而 cybercriminal、hacktivist 与 cyber-warrior 也正是造成近年众多数据泄露事件的“3 大主力”，这些屡见不鲜的数据泄露事件促使数据泄露与 DDoS 攻击、高危漏洞一同被列为当前组织/企业面临的重大安全威胁。

本报告分别从宏观（数据统计）和微观（案例分析）两个角度说明数据泄露的严峻现状、典型案例和对策思考，最后介绍 Intrusion Kill Chain 模型作为数据泄露的反制对策，期望组织/企业在数据泄露事件中可以用系统的方法积极有效地应对。

如果您希望与我们一起持续关注这个项目，都可以联系我们：

- 按 Ctrl+P，将本报告打印出来，便于在旅途中阅读。
- 将本报告发送给您的朋友，与他们分享。
- 访问更多安全报告：http://www.nsfocus.com/4_research/4_6.html
- 点击左侧微博按钮，与绿盟科技的官方微博在线互动：http://weibo.com/300369

[24] https://blog.torproject.org/blog/hidden-services-current-events-and-freedom-hosting

附录

关于作者

赵刚，绿盟科技　　Email：zhaogang@nsfocus.com

您可以联系报告作者，将您的见解与我们分享！先行致谢！

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于 2000 年 4 月，总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测/防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。

巨 人 背 后 的 专 家
THE EXPERT BEHIND GIANTS