安全+
SECURITY
2017/07 总第035
技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

★ 本期焦点

当4G遇上DDoS 实战鹰眼溯源

金融行业未知威胁检测探知之道

工业控制系统安全服务实施方法设计

物联网安全公司及产品介绍

绿盟科技官方微信

NSFOCUS

本期看点 HEADLINES

主办：绿盟科技
策划：绿盟内刊编委会
地址：北京市海淀区北洼路4号益泰大厦三层
邮编：100089
电话：(010)6843 8880-8669
传真：(010)6872 8708
网址：www.nsfocus.com

2017/07 总第 035

欢迎您扫描封面左下角的二维码，关注绿盟科技官方微信，分享您的建议和评论，或者来信nsmagazine@nsfocus.com与我们交流。

安全+ SECURITY

目录 CONTENTS

绿盟科技获评国家网安通报机制先进技术支持单位

3 月 2 日，由公安部第十一局、国家网络与信息安全信息通报中心主办的“国家网络与信息安全信息通报机制技术支持 2016 年度工作总结会议”在公安部第一研究所召开。

公安部第一研究所副所长冯曰铭、国家网络与信息安全信息通报中心十处处长黄小苏、公安部网络安全保卫局总工程师郭启全出席了本次会议，并发表了重要讲话。北京神州绿盟科技有限公司（绿盟科技）被授予“2016 年度国家网络与信息安全信息通报机制先进技术支持单位”证书。

大会主要总结了上一年度信息通报技术支持情况，通报了网络安全形势，并部署了信息通报机制技术支持工作。会上，黄小苏处长重点对 2016 年度在监测预警、研判分析、网络安全事件分析、平台总体方案的设计与标准规范编制工作、演习等几个方面有突出技术支持的厂商进行表扬，绿盟科技获高度认可。

公安部网络安全保卫局郭启全总工程师从网络安全法及相关法律的贯彻落实、全国“两会”网络技术支持工作部署、如何做好国家网络安全技术支持工作等三个大的方面进行了重点说明和部署。同时对如何长期做好国家网络安全技术支持工作提出了关键性建议。

随着现代化进程的加快，涉及国计民生的各个重要领域信息化程度的不断提高，信息系统的脆弱性和高风险性日益加剧，看似“无关紧要”的网络安全事件处理不当很有可能诱发大的安全案件，直接影响社会稳定和经济安全。对此，冯曰铭所长也重点指出，加强信息安全事件的发现、通报和预警工作的重要性。

绿盟科技获得国家网络与信息安全信息通报机制先进技术支持单位，是国家政府部门对绿盟科技通报预警机制、技术实力和安全保障能力的高度认可。凭借十余年安全技术和经验积累，绿盟科技已经多次在国际大会上做出过安保贡献，包括北京奥运会、上海世博会、深圳大运会，G20、安全周等，为大会提供全方位的信息安全保障服务。

目前，绿盟科技并具备一体化的态势感知和漏洞管理平台，可及时应对瞬息万变的安全问题，并与上千家组织和机构建立商业合作关系安全产品和解决方案已被广泛应用在金融、运营商、能源、政府等各大行业。依托于完备的感知体系，绿盟科技出色完成了国家网络与信息安全信息通报中心技术支持任务，并且对我国信息安全建设提出了更有成效的建议，帮助国家各行业和机关单位构建应对信息安全威胁的强大防御网络。

未来，绿盟科技将充分发挥自身的优势，持续为网络与信息安全的信息通报工作贡献力量，积极发挥安全公司技术支撑的作用，通过安全防护技术真正帮助企业“解内忧，排外患，知未知，见未见。”

绿盟科技携手中国移动苏州研发中心护航云计算安全

绿盟科技凭借在云计算安全方面多年的技术积累和研究创新，成功中标中国移动苏州研发中心研发云安全软件采购项目。绿盟的云安全能力与苏研的云管理平台成功对接，联合推出云平台安全解决方案，通过统一的调度管理给云租户提供安全防护服务，全面保障了云计算环境的安全。

中国移动苏州研发中心，又称中移（苏州）软件技术有限公司，是中国移动通信集团公司的全资子公司。公司依托中国移动雄厚的技术积累、海量的数据资源以及海内外高级专业人才，在云计算、大数据和 IT 支撑领域建立了完善的产品体系，并将业务范围覆盖产品研发、软件销售、系统集成及运营支撑等领域。

目前项目已在快速实施落地，通过该项目的成功中标和部署实施，绿盟科技与中国移动苏州研发中心形成了安全领域的技术合作，期待后续能继续为中国移动集团的云计算安全保驾护航。

软件定义的安全解决方案

针对中国移动现有云计算业务的特点以及其相关安全防护需求，中国移动苏州研发中心与绿盟科技共同研究出了基于软件定义安全的云安全管理平台解决方案，该方案与苏研现有的云平台进行适配集成，实现了云计算环境中的安全防护。

该项目所采用的软件定义安全架构，通过将安全数据与控制平面的分离，对物理及虚拟的网络安全设备与其接入模式、部署方式、实现功能进行解耦，底层抽象为安全资源池里的资源，顶层统一通过软件编程的方式进行智能化、自动化的业务编排和管理，以完成相应的安全功能，从而实现了灵活的安全防护。

集中部署的安全资源池

该项目中提供了专有的安全资源池，用于集中部署多种虚拟化安全设备。安全资源池是一种安全资源独占的物理安全结点，通过虚拟化技术在结点上生成虚拟安全设备实例并独立进行管理，形成安全资源池。该安全资源池能与云平台松耦合，易于快速对接。

统一展现的安全管理平台

云安全管理平台是集成了安全运维和安全服务管理两部分主要功能的一个统一的管理平台。安全服务部分包括了租户服务中心、安全资源管理和安全控制管理几个模块。安全运维部分提供了安全设备管理、告警管理、日志处理和用户管理等功能。

种类多样的云安全服务

通过云安全管理平台，能够把安全设备的安全能力以服务的方式提供给云租户。安全应用提供模块化配置能力，可根据需求提供漏洞扫描、安全配置核查、Web 安全防护和网络入侵检测等多种安全服务。安全应用实现了云平台中虚拟化安全设备实例的生命周期管理，实现虚拟化设备从创建、开机、配置、关闭和删除等操作的完全自动化，并且可通过安全管理平台获得虚拟安全设备的状态。安全应用还提供了用户视角的操作管理功能，用户可通过安全应用轻松完成一系列的配置操作，从而实现安全防护服务。

绿盟NTI牵手日本TOP运营商 护航1.7亿IP资产安全

2016 年底，绿盟科技签约一家日本跨国电信运营商，项目为其日常运营的 1.7 亿 IP 提供威胁情报及相关咨询服务，该项目的成功签约对海外市场威胁情报项目具有借鉴意义。另悉，该企业是日本三大运营商之一。

日本客户向来以严谨及高要求而知名。在此项目中，该运营商对多家国际主流 TI 厂商的威胁情报平台，进行了多轮严格的情报数据对比测试，最终给出评价认为，绿盟威胁情报中心 NTI 具有比其他平台更为高质量的威胁情报。在后续的工作中，绿盟科技将为客户定期监测其所运营的 1.7 亿个 IP，提供恶意 IP 定期趋势和分析报告，并为客户提供整改咨询服务，实现大范围 IP 资产的闭环安全管理。

绿盟威胁情报中心 Portal（https://nti.nsfocus.com）

项目中主要的支撑平台是绿盟威胁情报中心（NSFOCUS Network Threat Intelligence center 简称 NTI），NTI 是绿盟科技依赖多年的安全经验和情报数据积累推出的一款威胁情报分析和共享平台，可为用户提供及时准确的威胁情报数据。利用 NTI 的威胁情报支撑，用户可及时洞悉公网资产面临的安全威胁进行准确预警，实施积极主动的威胁防御和快速响应策略，结合安全数据的深度分析全面掌握安全威胁态势，并准确地进行威胁追踪和攻击溯源。

此次威胁情报项目的成功签约，彰显了日本运营商客户对绿盟科技威胁情报能力的信心，同时作为海外威胁情报市场开拓性案例，该项目也将为绿盟科技在英国、马来西亚、新加坡、加拿大等市场的相关项目，提供借鉴意义。这些举措都标志着绿盟科技在威胁情报这一前沿领域，又迈进了坚实的一步。

WAF再次入选Gartner应用 安全测试魔力象限

2 月，国际权威咨询机构 Gartner 发布 2017 年《Magic Quadrant for Application Security Testing》（以下简称 AST）报告，绿盟科技作为国内唯一一家厂商蝉联入选。

报告涉及企业首选的 Web 应用安全评估利器——绿盟科技 Web 应用漏洞扫描系统（WVSS），以及帮助企业构建完善网站安全体系的网站监测类产品——绿盟科技网站安全监测系统 (WSM) 和网站安全监测服务。

报告指出，如果企业在找寻具有竞争力的 Web 应用程序安全测试的工具和服务，绿盟科技值得选择。在满足企业 Web 安全建设需求的同时，绿盟科技还提供广泛的服务支持和响应。WVSS 和 WSM 提供了全面的 Web 应用安全检测，检测范围覆盖商用（COTS）和开源组件、应用程序，覆盖了门户网站，电子政务、论坛和电子商务应用系统等。此外，WVSS 还提供了具有参考价值的交互式检测技术，提升了漏洞检测的准确率。

Gartner 研究认为，随着 Web 应用安全需求的增长 AST 部署和能力也在成倍增长，企业安全团队在进行 Web 安全解决方案建设时仍然需要考虑 Web 安全产品的有效性和可扩展性。[1]

作为亚太地区唯一一家同时入选 Gartner 最新应用安全测试和 WAF 魔力象限的厂商，绿盟科技提供 WVSS(亚太唯一入选 2015 年 Gartner 应用安全测试魔力象限) 和 WAF(国内唯一入选 2016 年 Gartner WAF 魔力象限) 联动解决方案，通过提供“一键式”的智能补丁，实现了“检测”与“防护”的安全闭环管理。

绿盟 Web 应用漏洞扫描系统（WVSS）是基于绿盟科技多年对 Web 应用安全的研究与积累研发的产品。自上市以来，将不断的创新型技术及对用户的使用需求了解快速转化为产品能力，受到了用户的一致认可与好评。作为国内市场领先的 Web 应用漏洞扫描产品，绿盟 WVSS 已经覆盖多家企业机构，其中包括中国移动、中国电信、中国建设银行、中国电力科学院等绿盟网站安全监测系统（WSM）能够根据站点管理者的监管要求，通过对目标站点进行不间断的页面爬取、分析、匹配，为客户的互联网网站提供远程安全监测、安全检查、实时告警，是构建完善的网站安全体系的最好补充，是多家监管机构的网站监测首选产品!“绿盟网站安全监测服务”主要包括四方面内容，脆弱性检测、完整性检测、可用性检测和认证检测，通过服务模式帮助用户提升网站整体安全水平。

[1] Gartner “Magic Quadrant for Application Security Testing” by Dionisio Zumerle AyalTirosh February 28 2017.

About the Magic Quadrant Gartner does not endorse any vendor product or service depicted in its research publications and does not advise technology users to select only those endors with the highest ratings. Gartner research publications consist of the opinions of Gartner’ s research organization and should not be construed as tatements of fact. Gartner disclaims all warranties expressed or implied with respect to thisresearch including any warranties of merchantability or fitness for a particular purpose.

网络安全威胁月报 201704

威胁情报与网络安全实验室 陈颐欢

关键词：高危漏洞 DDoS 攻击事件 安全会议
绿盟科技漏洞库 绿盟科技博客

摘要：绿盟科技网络安全威胁周报及月报系列，旨在简单而快速有效的传递安全威胁态势，呈现重点安全漏洞、安全事件、安全技术。获取最新的威胁月报，请访问绿盟科技博客 http://blog.nsfocus.net/

一．2017 年 4 月数据统计

1.1 高危漏洞发展趋势

2017 年 4 月绿盟科技安全漏洞库共收录 175 个漏洞，其中高危漏洞 86 个，微软高危漏洞 39 个，上月监测到 CVE 公布高危漏洞数量为 316 个。相比 3 月份的高危漏洞数量持续上升。

1.2 互联网安全漏洞

VMSA-2017-0008.1

来源：http://blog.nsfocus.net/vmsa-2017-0008-1/

简述：当地时间 2017 年 4 月 19 日（北京时间 2017 年 4 月 20 日），VMWARE 官方发布安全通告，VMware Unified Access Gateway, Horizon View and Workstation 产品存在多个严重漏洞。

Squirrelmail 远程代码执行漏洞

来源：http://blog.nsfocus.net/squirrelmail-remote-code-execution-vulnerability/

简述：Squirrelmail 被爆出存在一个远程代码执行漏洞（CVE-2017-7692, CNNVD-201704-561）。该漏洞是由于在传递一个字符串给 popen 调用之前，没有对其进行过滤和无害化处理。因此攻击者有可能利用此漏洞在远程服务器上越权执行任意代码。

mbed TLS 远程代码执行漏洞

来源：http://toutiao.secjia.com/dahua-webcam-vulnerability-analysis-protection

简述：ARM 旗下的 mbedTLS 被爆出存在一个远程代码执行漏洞（CVE-2017-2784）。ARM mbedTLS 2.4.0 的 x509 证书解析代码中存在无可用的栈指针漏洞。 由 mbedTLS 库解析时，特制的 x509 证书可能造成无效的栈指针，从而导致潜在的远程代码执行

Jackson 框架 Java 反序列化远程代码执行漏洞

来源：http://blog.nsfocus.net/jackson-framework-java-vulnerability-analysis/

简述：Jackson 框架被发现存在一个反序列化代码执行漏洞。该漏洞存在于 Jackson 框架下的 enableDefaultTyping 方法，通过该漏洞，攻击者可以远程在服务器主机上越权执行任意代码，从而取得该网站服务器的控制权。

HPE Vertica Analytics Platform 远程特权访问漏洞

来源：http://blog.nsfocus.net/hpe-vertica-analytics-platform-remote-privilege-access-vulnerability/

简述：地时间 2017 年 4 月 17 日（北京时间 2017 年 4 月 18 日），HP 官方发布安全通告，披露了一个由 Fortinet 提供的关于 HPE Vertica Analytics Platform 产品存在远程特权访问的漏洞，CVE 编号为 CVE-2017-5802。

Microsoft Office OLE2Link(CVE-2017-0199) 漏洞

来源：http://toutiao.secjia.com/struts2-vulnerability-analysis-and-protection-cve-2017-5638

简述：2017年4月7日McAfee与FireEye的2名研究员爆出微软（Microsoft）Office Word的一个0-day漏洞（CVE-2017-0199）的相关细节。攻击者可以向受害人发送一个带有OLE2link对象附件的恶意邮件，诱骗用户打开。

Apache Log4j 反序列化漏洞

来源：http://blog.nsfocus.net/apache-log4j-deserialization-vulnerability/

简述：北京时间 18 日清晨，Apache Log4j 被曝出存在一个反序列化漏洞（CVE-2017-5645）。攻击者可以通过发送一个特别制作的 2 进制 payload，在组件将字节反序列化为对象时，触发并执行构造的 payload 代码。

phpcms v9.6 注册功能远程 getshell 0day 漏洞分析

来源：http://blog.nsfocus.net/phpcms-v9-6-getshell-0day-vulnerability-analysis/

简述：phpcms 在国内应该使用很多，前几天被爆出来一个 getshell 的 0day，这个漏洞无需登录即可远程直接 getshell，所以影响很大。phpcms 官方 4 月 12 日发布了 9.6.1 版本，对漏洞进行了补丁修复。

phpcms v9.6 注册功能远程 getshell 0day 漏洞分析

来源：http://blog.nsfocus.net/phpcms-v9-6-getshell-0day-vulnerability-analysis/

简述：phpcms 在国内应该使用很多，前几天被爆出来一个 getshell 的 0day，这个漏洞无需登录即可远程直接 getshell，所以影响很大。phpcms 官方 4 月 12 日发布了 9.6.1 版本，对漏洞进行了补丁修复。

方程式组织泄漏大量针对 Windows 攻击工具威胁

来源：http://blog.nsfocus.net/microsoft-windows-large-0-day-vulnerability/

简述：Shadow Brokers 组织公布了此前窃取的部分方程式（Equation Group）组织的机密文件。这部分被公开的文件曾经被 Shadow Brokers 组织以数亿美金拍卖，因为这部分文件包含了数个令人震撼的黑客工具，用来攻击包括 Windows 在内的多个系统漏洞。此次泄漏的文件包括三部分：Windows, Swift 以及 Odd。

（来源：绿盟科技威胁情报与网络安全实验室）

1.3 绿盟科技漏洞库十大漏洞

声明：本十大安全漏洞由NSFOCUS(绿盟科技)安全小组 <security@nsfocus.com>根据安全漏洞的严重程度、利用难易程度、影响范围等因素综合评出，仅供参考。

http://www.nsfocus.net/index.php?act=sec_bug&do=top_ten

1. 2017-04-12 Microsoft Office OLE 功能远程代码执行漏洞 (CVE-2017-0199)

NSFOCUS ID: 36350

链接：http://www.nsfocus.net/vulndb/36350

综述：Microsoft Office 是微软公司开发的一套基于 Windows 操作系统的办公软件套装。Microsoft Office 在实现上存在远程代码执行漏洞，可使攻击者执行任意代码，完全控制受影响系统。

危害：远程攻击者可以通过诱使受害者打开恶意文档来利用此漏洞，从而控制受害者系统

2. 2017-04-12 Microsoft Internet Explorer 远程权限提升漏洞 (CVE-2017-0210)

NSFOCUS ID: 36356

链接：http://www.nsfocus.net/vulndb/36356

综述：Internet Explorer 是微软公司推出的一款网页浏览器。Internet Explorer 未正确实现跨域策略时，在实现上存在特权提升漏洞，可使攻击者获取访问域中信息并将其插入其他域。

危害：远程攻击者可以通过诱使受害者打开恶意网页来利用此漏洞，从而控制受害者系统

3. 2017-04-21 SAMSUNG Tizen 系统多个安全漏洞

NSFOCUS ID: 36488

链接：http://www.nsfocus.net/vulndb/36488

综述：Tizen 是三星产品主流操作系统，广泛使用在三星智能电视、智能手表和 Z 系列智能手机中。Tizen 系统在实现中存在多个安全漏洞，攻击者可以利用这些漏洞控制三星设备，植入任意恶意代码等。

危害：攻击者可以利用这些漏洞控制三星设备，植入任意恶意代码等

4. 2017-04-14 Adobe Flash Player 释

放后重利用远程代码执行漏洞（APSB17-10）

NSFOCUS ID: 36397

链接:http://www.nsfocus.net/vulndb/36397

综述:Flash Player是多媒体程序播放器。Adobe Flash Player 25.0.0.127及之前版本在sound类中存在释放后重利用漏洞，成功利用后可导致任意代码。

危害：攻击者可以通过诱使受害者打开恶意swf文件来利用此漏洞，从而控制受害者系统

5. 2017-04-21 Action Message Format (AMF3) Java 远程代码执行漏洞

NSFOCUS ID: 36487

链接:http://www.nsfocus.net/vulndb/36487

综述:AMF3是Adobe Action Message Format的最新版本，用于ActionScript对象图形序列化的压缩二进制格式。Java AMF3在功能实现上存在多个漏洞，多个应用了AMF3的产品都受此漏洞的影响。

危害：远程攻击者可以利用这些漏洞控制受害者系统

6. 2017-04-10 Apple iOS 任意代码执行漏洞 (CVE-2016-6975)

NSFOCUS ID: 36325

链接:http://www.nsfocus.net/vulndb/36325

综述:iOS是由苹果公司为移动设备所开发的操作系统，支持的设备包括iPhone、iPod touch、iPad、Apple TV。Apple iOS < 10.3.1版本在Wi-Fi实现中，未能防止通过构造的访问点造成的栈缓冲区溢出。

危害：攻击这可以通过此漏洞在Wi-Fi芯片上执行代码

7. 2017-03-27 Microsoft Windows Server ScStoragePathFromUrl 函数缓冲区溢出漏洞 (CVE-2017-7269)

NSFOCUS ID: 36239

链接:http://www.nsfocus.net/vulndb/36239

综述:Windows Server是微软发布的一系列服务器操作系统。Microsoft Windows Server 2003 R2在Internet Information Services (IIS)6.0的WebDAV服务实现中，ScStoragePathFromUrl函数存在缓冲区溢出漏洞。

危害：远程攻击者可以通过向服务器发送恶意请求来利用此漏洞，从而控制服务器

8. 2017-04-05 Google Android 权限提升漏洞 (CVE-2017-0554)

NSFOCUS ID: 36301

链接:http://www.nsfocus.net/vulndb/36301

综述:Android是基于Linux开放性内核的手机操作系统。Google Android在CameraBase实现上存在权限提升漏洞，可使本地恶意应用执行任意代码。

危害：本地攻击者可以利用此漏洞来提升权限，对系统进行非授权的访问

9. 2017-04-18 Apache Log4j 远程代码执行漏洞 (CVE-2017-5645)

NSFOCUS ID: 36412

链接:http://www.nsfocus.net/vulndb/36412

综述:Apache Log4j是一个基于Java的日志记录工具。Apache Log4j 2.x < 2.8.2版本，若使用TCP或UDP套接字服务器接收其他应用的序列化日志事件。

危害：攻击者发送构造的二进制负载，反序列化时，可执行任意代码

10. 2017-04-21 VMware Workstation/Horizon Client 堆缓冲区溢出漏洞 (CVE-2017-4909)

NSFOCUS ID: 36480

链接:http://www.nsfocus.net/vulndb/36480

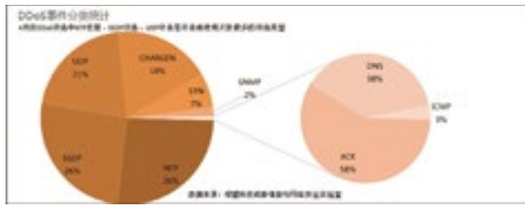
综述:VMware Workstation 是一款功能强大的桌面虚拟计算机。VMware Workstation /Horizon Client在TPView.dll的True Type Font解析器及JPEG2000解析器中存在多个堆缓冲区溢出漏洞。

危害：攻击者可以通过诱使受害者打开恶意文件来利用此漏洞，从而控制受害者系统。

（来源：绿盟科技威胁情报与网络安全实验室）

1.4 DDoS 攻击类型

4月份绿盟科技科技威胁情报及网络安全实验室收集及梳理了超过2.5万次攻击，与3月份相比，攻击次数下降，但在这个月的攻击类型中，相比上个月 CHARGEN 攻击占比增长很明显



小提示

• Chargen Flood：Chargen 字符发生器协议（Character Generator Protocol）是一种简单网络协议，设计的目的是用来调试TCP或UDP协议程序、测量连接的带宽或进行QoS的微调等。但这个协议并没有严格的访问控制和流量控制机制。流量放大程度在不同的操作系统上有所不同。有记录称，这种攻击类型最大放大倍数是358.8倍。

• NTP Flood：又称NTP Reply Flood Attack，是一种利用网络中时间服务器的脆弱性（无认证，不等价数据交换，UDP协议），来进行DDoS行为的攻击类型。有记录称，这种攻击类型最大放大倍数是556.9倍。

• SSDP Flood：智能设备普遍采用UPnP（即插即用）协议作为网络通讯协议，而UPnP设备的相互发现及感知是通过SSDP协议（简单服务发现协议）进行的。

攻击者伪造了发现请求，伪装被害者IP地址向互联网上大量的智能设备发起SSDP请求，结果被害者就收到了大量智能设备返回的数据，被攻击了。有记录称，这种攻击类型最大放大倍数是30.8倍。

更多相关信息，请关注绿盟科技DDoS威胁报告。

二．博文精选

RSA会议主题回顾

2016年DDoS威胁报告

日前，绿盟科技联合中国电信云堤发布《2016年DDoS威胁报告》，报告总结及分析了2016全年DDoS攻击发展态势，并就DDoS防护生态环境给出了相关建议，其中DDoS防护策略、方案及技术手段，可以帮助各组织及机构持续改善自己的DDoS防护技术及体系。

http://blog.nsfocus.net/2016-annual-ddos-threat-report/

金融行业需要关注《网络安全法》

《网络安全法》正式出台，对于加强互联网和网络安全方面的法

律约束具有重要意义，对金融机构提出新的网络安全工作思路和要求，起到推进作用。本文梳理的关注点分布在工作依据、工作原则、网络运行、个人信息、监测与预警、内部审计 6 个方面，期许通过完善和加强这些方面的管理机制和技术防护措施，从而整体提升金融行业网络安全防护水平。

http://blog.nsfocus.net/network-security-law-points/

恶意样本分析手册

在计算机系统中，我们是以字节为单位的，每个地址单元都对应着一个字节，一个字节为 8bit。但是在 C 语言中除了 8bit 的 char 之外，还有 16bit 的 short 型，32bit 的 long 型（要看具体的编译器），另外，对于位数大于 8 位的处理器，例如 16 位或者 32 位的处理器，由于寄存器宽度大于一个字节，那么必然存在着一个如何将多个字节安排的问题。

http://blog.nsfocus.net/sample-analysis-manual-theory/

（来源：绿盟科技博客）

三．安全会议

安全会议是从近期召开的若干信息安全会议中选出，仅供参考。

Gartner 安全风险管理峰会

时间：2017 年 6 月 12-15 日

简介：安全、风险管理和业务连续性管理领导者的重要会议，gartner 的《安全和风险管理峰会 2017》为您的组织提供洞察力，以实现安全数字业务的未来。全面议程涉及最新的威胁、灵活的新安全体系结构、治理战略、首席信息安全官角色等。根据 gartner 可信的独立研究和实际建议，这是一个独特的机会，可以重塑您对数字时代的安全和风险方法。

网址：http://www.gartner.com/events/na/security

Infosecurity 欧洲会议

时间：2017 年 6 月 06-08 日

简介：Infosecurity 欧洲 (Infosec) 欧洲范围内的最大最全面的会议，有超过 360 个参展商向 13500 访问者展示相关的信息安全解决方案和产品。

网址：http://www.infosecurityeurope.com/

AppSec 欧洲会议

时间：2017 年 5 月 8-12 日

简介：欢迎光临 OWASP 年度 AppSec 欧洲安全会议，为欧洲开发商和安全专家提供卓越的应用安全交流机会。AppSec 欧洲会议上您可以看到思想领袖，丰富的议程及不可多得的经验交流。

https://2017.appsec.eu/

2016 DDoS威胁报告

中国电信云堤：张敏 常力元 刘紫千 刘长波 陈林
绿盟科技： 潘文欣 何坤 孙叶 杨旭 王洋

关键词：DDoS 威胁报告
2016 DDoS 报告 安全报告

摘要：纵观 2016 全年 DDoS 威胁态势，DDoS 攻击次数和规模依然不断上升，攻击目标也早已涉及各行各业；物联网设备大面积沦陷，僵尸网络持续扩张，相关的 DDoS 攻击规模屡创新高，不断刷新人们对 DDoS 攻击的认知。

面对不断升级的 DDoS 威胁，为了跟踪及呈现 DDoS 攻击的变化趋势，进而帮助各组织和机构持续改善自己的 DDoS 防护技术体系，中国电信云堤联合绿盟科技发布《2016 DDoS 威胁报告》。

本文对报告的 DDoS 攻击态势方面做内容提要如下，完整报告请访问该地址下载

http://nsfocus.com/research/report.html

一．态势：2016 年攻击态势总体上扬

• 2016 对比 2015 年，DDoS 攻击次数同比增长 18.6%，攻击流量总值同比增长 25%，攻击流量峰值大于 300Gbps 成为常态。

• 2016 DDoS 短时攻击增加，在 30 分钟以内结束的占 51.4%。

• 2016 攻击流量最大的 2 种攻击类型依然是 SYN 和 UDP Flood。2016 反射攻击仍然流行，NTP 和 SSDP Reflection Flood 猖獗。

• 从全球来看，中国依然是受 DDoS 攻击最严重地区，其次

是美国、法国、英国、德国；从国内来看，发起 DDoS 攻击的源头主要来自广东、浙江、北京、江苏、上海。

• 2016 物联网僵尸网络规模迅速扩张，2016 来自物联网的 DDoS 攻击增长明显，应用层 DDoS 的防护难度增大。2016 各国开始推动 IoT 安全立法，治理 IoT 刻不容缓。

报告将数据与多个相关因素进行关联分析之后，逐步描绘出 2016 DDoS 攻击者的特征画像。

二．画像：2016 DDoS 攻击者呈现 5 个特点

2016 年的 DDos 攻击具有 5 个方面的特点，包括专注、精细、嗅探、整合、黑吃黑。

专注

• 攻击者专业、专注

• 一年当中 6-8 月份，是 DDoS 攻击者最忙碌的月份

• 攻击者在一天之中 11-16 点、17-21 点发起攻击最多（网络使用最频繁）

• 3 点 -7 点攻击较少（业务低谷期）

精细

• 攻击者也有自己的老板，也需要考虑投入产出比

• 大流量攻击凶猛而短暂，百 G 以上的攻击大多 5 个小时就结束了

• 小流量攻击持续不断，甚至可以持续数天

• 反射型攻击，以其隐藏性高、成本低，相当多的攻击者都选择它

嗅探

• 为了更大流量和隐蔽，攻击者不断寻找更多可利用的资源

• 2016 年 BotMaster 主要分布在中国、俄罗斯、美国、巴西和土耳其

• 除了传统网络，僵尸网络已经渗透进入了物联网

整合

• 如果自己的能力不具备，DDoS 攻击者也会进行资源整合

• DDoS 攻击者常常利用木马，控制更大规模及类型的僵尸网络

• 台风 DDoS 控制端，14% 的 C&C 都来自国内多家知名云

• 黑产者已经将 DDoS 攻击能力平台化，任何人都可以购买攻击服务

黑吃黑

• 黑产充满了邪恶，攻击者之间互相厮杀

• 僵尸网络的资源一旦聚集在某个组织手里，它就会成为撕咬的对象

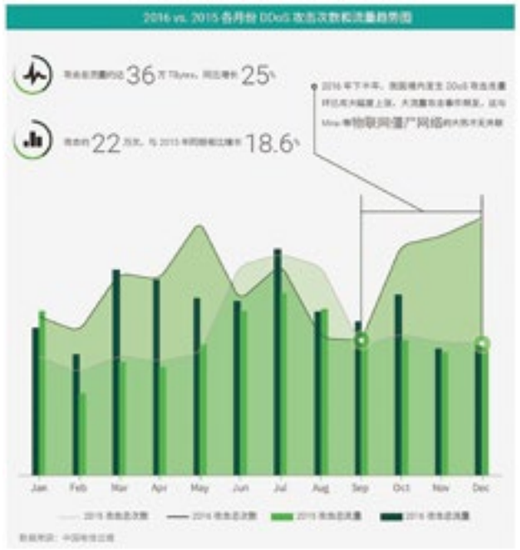
• 黑产者甚至会攻击政府组织，攻击 CIA、FBI 的事件屡见不鲜

• 勒索软件等先进的攻击工具，也成为互相绑架的对象

三．攻击：年度攻击次数和流量 同比增长 18.6% 及 25%

2016 年我国境内共发生 DDoS 攻击约 22 万次，与去年同期相比增长 18.6%，除了 1 月份外，其余各月份攻击次数均高于 15 年同期。攻击总流量约达 36 万 TBytes，同比增长 25%。

2016 年上半年，我国境内发生 DDoS 攻击呈现波动上升的趋



势，下半年攻击总量环比有大幅度上涨，大流量攻击事件频发，这与 Mirai 等物联网僵尸网络的大热不无关联。

四．峰值：大于 300Gbps 的攻击 Q3 同比增长 522.2%

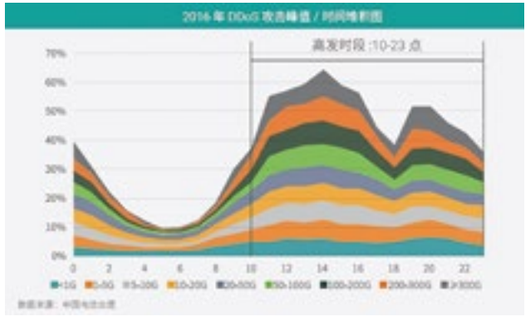
2016 年下半年攻击总量环比有大幅度上涨，大流量攻击事件频发。2016 全年峰值超过 300Gbps 以上超大流量攻击 358 次，其中 Q3 季度就 168 次，占全年总数的 46.9%，与 2015 年同期相比增长 522.2%

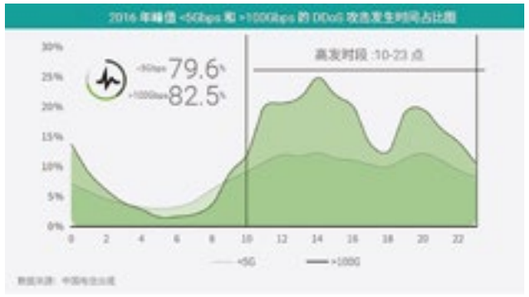
从 2015 年到 2016 年各月份我国国内发生攻击的最高攻击峰值看，整体趋势缓慢上升，且各月份最高峰值都已经高出 300Gbps，大流量攻击已成为常态，且最高峰值不断刷新纪录。

五．时间：业务高峰期 DDoS 攻击最频繁

2016 年的攻击多发生在 10-23 点这一时段，这通常也是互联网业务在线用户数量最多的时间段。选在攻击目标业务使用高峰期发起攻击，往往会给被攻击目标带来巨大损失，反映了他们以期用有限的资源达到对目标的更精准的打击，使破坏力最大化。

从不同流量区间看，5Gbps 以下小流量攻击，发生在 10-23 点





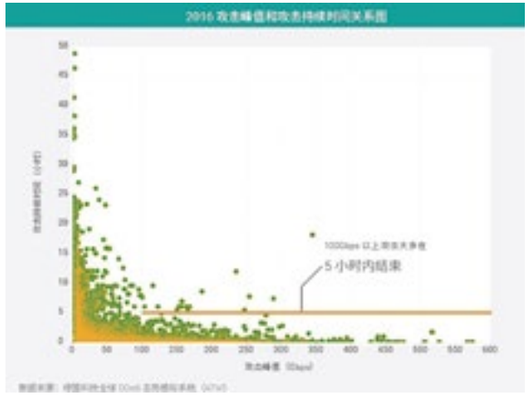
之间的攻击次数占总体攻击次数的 79.6%；大于 100Gbps 的大流量攻击，发生在 10-23 点之间的攻击次数占总体攻击次数的 82.5%。

六．时长：短时攻击增加 大流量可持续时间变长

2016 年，攻击时长在 30 分钟以下的 DDoS 攻击，占全部攻击的一半以上（51.4%），而且大多是小于 5 分钟的短时攻击。

从下面的 2016 年各季度 DDoS 攻击持续时间占比图中也可以看到，短时攻击呈增加的趋势。短时攻击，也叫瞬时攻击，特点是攻击时间极短，这对安全防护者的应急等能力是极大的考验，如果没有很好的应对经验和流程，很可能攻击已经打完了，安全团队还没开始应对。过多的短时攻击可能会牵制安全团队的大部分精力，使其无暇顾及网络中其他安全隐患。通常，大部分 DDoS 攻击背后都隐藏着入侵、数据窃取等其他安全事件。

攻击流量越小，则攻击可持续的时间越长；反之，攻击流量越大，则攻击可持续的时间越短。100Gbps 以上攻击大多在 5 小时内结束，与去年相比，大流量的攻击持续时间变长。

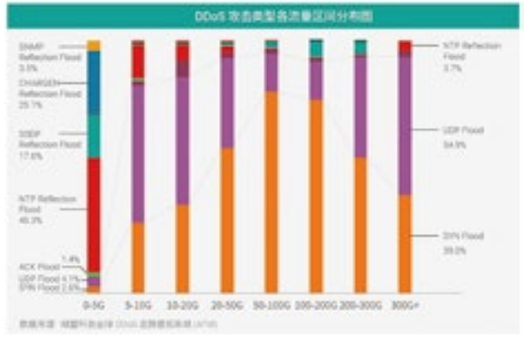


从整体流量来看，在低于 5Gbps 的小流量攻击中包含多种攻击类型，而在大于 5Gbps 的中型、大型、超大型流量攻击中，UDP Flood、SYN Flood 攻击交替占据主流攻击地位。攻击峰值在 50-300Gbps 的大型攻击中，SYN Flood 居多，5-20Gbps 的中型攻击和超过 300Gbps 的超大型攻击中，UDP Flood 居多。

从峰值流量来看，2016 年攻击峰值各区间分布情况如下图所示，小于 5Gbps 的小流量攻击平均占 39.1%，同比去年下降 2 个百分点；5-50Gbps 流量的攻击平均占 47.4%，同比去年下降 0.2 个百分点；大于 50Gbps 的大流量攻击平均占 13.5%，同比去年上升 2.2 个百分点。2016 年小流量攻击占比呈下降趋势，大流量攻击更为流行。

七．类型：大流量攻击 SYN、UDP 是主角 小流量攻击多样化

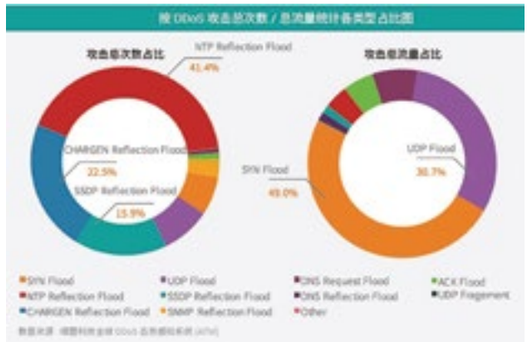
2016 年攻击类型在各流量区间的分布呈现出这样的特点，小流量攻击多样化，大流量 UDP、SYN 作主角，这种现象和去年的分析保持一致。

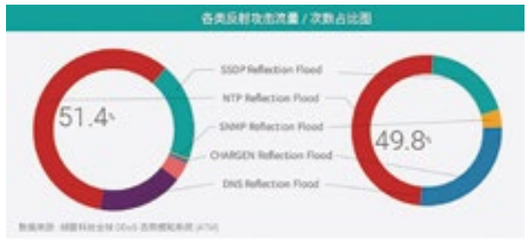


八．混合：复杂攻击门槛降低，混合攻击增多

2016 年混合攻击占全部攻击的 38.7%。

随着 DDoS-for-Hire 服务业的不断发展完善，使得发起复杂攻击的门槛大大降低，只要愿意付一定的价钱，就能得到攻击规模更大、支持攻击种类更多、持续时间更长的攻击服务。





两种至三种攻击类型的组合最为常见，占据混合攻击的 99.7%。

SYN Flood 和 UDP Flood 攻击组合占据全部混合攻击的 34.8%。其次，各类反射攻击的混合也是比较常见的混合方式。

九．反射：反射攻击依然流行 NTP、SSDP Reflection Flood 猖獗

2016 年，全球 Top 3 的 DDoS 攻击均为反射攻击（按攻击次数统计），依次为 NTP、CHARGEN、SSDP 反射，这三种反射攻击合计占比达 80%。从统计的趋势来看，我们认为反射型 DDoS 攻击会存在较长时间。

2016 年 NTP Reflection Flood 攻击次数和攻击流量均占全部反射攻击类型的首位，其次是 SSDP Reflection Flood。

2016 年我们检测到全球的活跃 NTP 反射器（经常参与 DDoS 攻击的 NTP 服务器）52,396 个。在全球分布排名前五位的国家分别为中国、美国、韩国、越南、土耳其，其中中国的反射器个数占全球总数量的 23%。

2016 年我们检测到全球的活跃 SSDP 反射器 795,616 个。我

们观察到 2016 年 Q4 季度活跃的 SSDP 反射器数量激增，中国的活跃 SSDP 反射器数量在各季度均占据首位。

十．国家：最受伤的还是中国

在这些攻击中，中国依然是 DDoS 攻击受控攻击源最多的国家，其次是美、俄，三者占据全球受控攻击源的 72.2%。

受攻击最严重的国家也是中国，攻击占全部被攻击国家的 48.9%，其次是美国，占 20.5%。

2016 年，由国际侧发起的 DDoS 攻击全年合计占 41.1%，互联互通发起的攻击全年合计占 20.9%，电信内发起的攻击全年合计占 38%。与 2015 年相比，电信内发起攻击的占比有所减小，特别是 2016 年 6 月开始，每月电信内部发起的攻击占比同比减小 8-17 个百分点，这也与电信不断出台各种措施治理 DDoS 攻击密不可分。

国际下半年发起的攻击较多，11 月份来自国际的攻击占比高达

54.4%，同比增长 18.7 个百分点，2.4.1 章节分析了攻击源国家，除中国外，其它攻击源国家的合计占比达 44.3%，说明来自国际的威胁总体在上升。

十一．IoT：全球 Mirai 物联网僵尸设备超 200 万 治理 IoT 刻不容缓

DDoS 攻击追求的本质就是尽可能控制更多的、更大规模的僵尸网络。与传统的僵尸网络（Botnet）相比，物联网僵尸网络（IoT Botnet）最显著的特征就是其被感染和被控制的 Bot 端不再是传统的 PC 或 Server，而是物联网设备。由于全球这类物联网设备数量庞大，短期内其安全问题难以解决，且易感染、易控制，基于其的僵尸网络规模将不断扩大，拥有的破坏力也会更加惊人。

以 Mirai 为例，目前我们监测到的 Mirai 控制端就已经达到 57 个，如下表所示。从域名注册和更新时间看，基本都是 2016 年下半年开始活跃。全球感染 Mirai 的物联网设备数量累计已经突破 200 万。Mirai 单个僵尸网络规模庞大，有些僵尸网络 Bot 端的数量多达几十万个。其全球分布情况及 Top 10 国家如下图所示。

我们截取了 2017 年初 1 个多月的 Mirai 扫描数据（其中包含使用最初 Mirai 版本扫描特征的 Bot 日扫描总次数，和未使用该特征的 Bot 日扫描总次数），如下图所示。

自从 Mirai 的源代码在 2016 年 9 月份被公开后，各黑客组织就从未停止过对其功能的改造，Mirai 变种层出不穷。最初版本的 Mirai 使用 23 和 2323 端口进行新感染目标的扫描，且扫描时带有

一些固定特征，到目前已经陆续出现新的扫描端口共 8 个，分别为 Port 7547、6789、5555、32、23231、3777、2222、19058。 部分变种 Mirai 已经不再具备最初的特征。

据 Gartner Inc. 预测，2016 年新的物联网设备将以每天 550 万的速度接入互联网，到 2020 年这个数字将会到达 208 亿。要治理物联网的安全乱象，还需要国家相关主管机构、标准组织、设备生产商、安全厂商等联合协作制定符合物联网行业实情的法律法规、行业安全标准等，以规范物联网的设备生产、管理、运营，构建绿色的网络空间。

我们看到，目前国内外很多相关组织和管理机构开始重视并计划着手应对物联网安全威胁。详情可以参考报告完整版（地址见文首引言）。

十二．云端：14% 的台风 DDoS 控制端位于云端主机上

基于物联网的僵尸网络恶意程序不仅 Mirai，还有 AES.DoS、Luabot、Hajime、台风 DDoS 等。

台风 DDoS（tfddos）这款主要针对中国地区的基于物联网设备的僵尸网络，其 C&C 主控制端已经将近 1000 个，76% 都分布在中国，且江苏、浙江、北京、广东等地分布最密集。

对台风 DDoS 的 C&C 控制端地址进行溯源显示，14% 的 C&C 控制端都位于云端主机上，包括国内多家知名云；30% 位于提供托管服务或服务器租赁的托管公司的主机上，有意思的是，很多这类托管公司都提供 DDoS 清洗服务。

圣诞节的礼物

安全服务交付中心 曹嘉　创新中心 刘文懋
威胁情报与网络安全实验室 赵阳
ROS产品管理团队 卢梁

关键词：智慧安全 2.0 P2SO 云地人机 威胁情报中心 NTI
软件定义安全 SDS 木马攻击 监测与防护体系

摘要：网络安全虽然是一场没有硝烟的战争，但攻守双方的争夺，却如战场一般真实可见。我是一名老兵，这是我的故事。（本文改编自 2008 年 8 月份美国《空军》杂志 AIR FORCE Magazine，原作者是其特约编辑 John T. Correll。故事情节如有雷同，纯属巧合。）

警报 渗透的木马

夜幕下的英吉利海峡，如同神秘的黑洞，既有吞噬一切的气势，又给人无边的恐惧，似乎随时都能跑出一个怪兽。在 Daniel 的身后，是他的家乡——漆黑一团的朴次茅斯。这个昔日十分繁华的港口城市，被德国空军隔三岔五地轰炸了几次，他的父亲、哥哥、嫂子、侄子都在一个月前的轰炸中惨死，相比这城市的满目疮痍，这才是二战以来，朴次茅斯最惨痛的创伤。

还好，今天是万圣节，一群浪漫的年轻人带着各种食物和酒水来朴次茅斯雷达站慰问，搞了一场“万圣节礼物”的假面舞会。送走了这帮人，雷达兵 Daniel 就开始了对发射架的例行检查。不知道为什么，上面来了个神秘的军官，一直都在强调这个事情。

深夜的排查总是枯燥的，Daniel 爬上发射架照章执行。没有发现什么异常，但似乎总是听到哪个地方传来“滴哒”的声音，但又找不到。这个事情让 Daniel 异常烦恼，在回营房的路上腹诽不已。

“什么？你说什么滴答声？”那个讨厌神秘军官 Alarm 听了 Daniel 报告，一把抓住 Daniel 的胳膊，“快带我去看看，只要出事，我们大家都完蛋！”

Alarm 踩着发射架的踏板，爬了四五级，然后取出随身携带的军用手电筒，仔细搜寻。“咦，这是什么？”在踏板与发射架的夹角处，Alarm 发现了一个闹钟、一捆雷管几根电线。“定时炸弹！”Alarm 也只是在培训时见过模型，今天见到了真家伙，一股寒气瞬间从他的脊背扩散到全身。

“警报，炸弹！”一串紧急的哨声响起。

“上尉，难道我们的雷达站里有问题？”Daniel 问 Alarm。“不好说，经历了无数次血与火的考验，我对兄弟们有信心。我怀疑，是那群来慰问的市民里面混进了德国人的木马！”上尉摇了摇头，心里浮现的是那个德军的神秘木马计划。

“木马？是间谍吗？那怎么办，上尉？他们现在都回朴次茅斯去了，麻烦了！”Daniel 叫苦道。

“他们即便是还在这里，我们也很难确定。酒会的时候，大家都带着面具呢。”Alarm 也苦笑，“幸好他们来的时候都做了登记，我们立即把可疑人员资料上报！”

艰难 智慧的决断

深夜，英国皇家空军司令部的战情室中灯火通明。

就在刚才，空军司令接到了朴次茅斯雷达站的急电，立即召集参谋长 Trends 做出布署，几个分管作战参谋也会同参与此次突如其来的会议。

“德国人的轰炸已经快两个月了。雷达站的小伙子们干的不错，让我们的空军击毁敌机一千多架，我军只损失了 500 多架，但三百多个空军的兄弟死在战场上了！”参谋长 Trends 讲述着目前的战场态势，声音有些哽咽。“是啊，人的损失太大了！”空军司令也痛心疾首，飞行员损失的速度太快了。这段时间，战局的胶着以及多少个飞行员家庭的破碎，让他原本乌黑的头发白了一半。

司令的面前是一个十几平方米大的沙盘，沙盘的旁边站着 Trends 和几个中年军官。长达两个月的空战让他们身心俱疲，满眼血丝，但是每个人的身上都透着一股狠戾，显然都是经过尸山血海的历练。

Trends 似乎想说点什么，但是看到司令的话似乎还没说完，他就没打断。

空军司令接着说道：“德国人的轰炸越来越猛烈，我们这点家底可不够他拼的。Churchill 首相说了，如果再以常规的方式和德国人战斗，我们的失败很快就会到来。Trends，你尽快给我拿出一套行之有效的作战方案！”

Trends 沉吟一下，然后清了清嗓子：“这场战役中，目前胶着的情况发生在 4 个方面，1 云，空中战术及战情，2 地，地面补给和后勤保障，3 人，指挥系统及参战人员，4 机，机械化作战系统。从 NTI 回传的情报来看，德军这次 4 个方面的配合相当奏效。但我们也发现他们的弱点——轰炸机。他们再机动，也要让轰炸机过来，这个东西可飞不快。”

空军司令和那几个军官不由得连连点头，知道 Trends 还有话说。

Trends 又说：“其实，二十多年前，我们的富勒将军提出了著名的‘1919 计划’，他提议用飞机和地面坦克部队配合作战，这就相当于我刚才说的云、地、人、机配合。很可惜，当时时机不成熟。而现在，协同作战的条件成熟了。”

一个作战参谋质疑道：“参谋长，咱们的舰艇、装甲车在敦刻尔克大撤退的时候，绝大部分毁于德国人的炮火之下。如你所说的云、地、人、机协同，我们就少了一项，还怎么协同？”

Trends 说道：“无妨，这一次我们依然采用这个方案。不过呢，需要做一点变化。”

大家齐声问道：“参谋长，你要怎么变？”

Trends 向着分管参谋 Albert 使了个眼色，Albert 会意，上前一步：“我建议，即刻成立 4 部协同作战系统 SDS。SDS 有三个使命，第一，在空军和陆军这两个不同兵种之间构建自上而下的紧密沟通渠道，比如，最高司令部、后方机场、和前线部队之间在战时切实保

证迅捷的联系；第二，建议一套独立的通信系统，避免为通信优先权进行无谓的争夺；第三，SDS 下面的特殊任务不仅仅限定给若干作战单位，而且应该分配给战区所有能够调动的战机，打造灵活机动的资源池。”

说到这里，Albert 向着沙盘一指：“既然 NTI 计划已经掌握了敌军的弱点，那我们就应该集结优势力量，寻找战机，来一个云端决战。只要打掉他们的空军有生力量，就能有效遏制敌军横渡英吉利海峡！”

另一个作战参谋提出异议：“我们的飞机及飞行员损耗严重，在这个战机寻找上需要谨慎。”

Albert 又将手指指向了沙盘上的雷达站模型说道：“没错，这就要看我们手里的两张王牌。第一，我们的 51 座雷达阵地及其警戒体系，随时盯着德军的飞机，一旦他们进入一百英里之内，我们的观测队就可以进行追踪，适机迎战，胜算要大得多！第二，那就要看军情五处的了。”

Trends 笑道：“所以，我们这一次的云、地、人、机协同作战，是时候来一场云端决胜了！司令，从长远来看，这是个战略，我们需要给他一个合适的名字！”

“就叫 P2SO 吧！”空军司令笑道。其实这个代号，最高指挥部谋划已久。

Trends 又问道：“将军，这个时候军情五处和朴次茅斯雷达站已经开始行动了吧！”

空军司令点了点头：“我们的 NTI 计划已经收网，一切正朝着我们愿意的方向发展！”

逆转 生死之环

这是朴次茅斯市的一处民宅，无数的断壁残垣，一片凄凉。此时，Trojan 正观察着街上的动静，也在注意在远方的声音。

表面上，Trojan 是一个英国商人，但是他的真实身份是德国盖世太保的一名党卫军人。作为 Hitler 的狂信者，他忠实地执行着总部下达的任何命令。

英国军队敦刻尔克大撤退的时候，Trojan 奉上司的命令，假扮成一个英国籍的破产商人，混进了撤退的人群，来到了朴次茅斯，并在这里潜伏下来。平日里，他借着经商的名义为德军搜集情报，并利用一个小型电报机发送给上司。

一个月前，他接到上司的一个命令，让他无论如何也要想办法把朴次茅斯附近的雷达站给毁掉。虽然只是一个简单的命令，但他也知道，就因为这个雷达站的存在，严重阻碍了德军空军轰炸伦敦的计划。

为了完成这个使命，Trojan 秘密谋划了一个月。他鼓动了一帮浪漫的年轻人，在万圣节这一天来到朴次茅斯雷达站，对那些雷达兵们进行慰问。趁着大家开怀畅饮的时候，他戴着面具来到雷达发射架下，安装了三组定时炸弹。他还给这次的任务取了一个代号——“万圣节的礼物”。

“轰、轰、轰！”大约凌晨三点左右，昏昏欲睡的 Trojan 听到了城外雷达站方向传来了三声间隔极短的三声巨响。他顿时精神大振，立即跑进卧室，把暗藏在墙缝里的小型电报机拿出来，给自己的上司发了一份密电：礼物送达。

电报发送完毕，Trojan 正要把电报机送回原处，忽然听到身后传来“咚”的一声。他回头一看，原来是大门被人踹开，一个身着便衣的陌生男子走了进来。

作为一个受过盖世太保训练的间谍，Trojan 的心理素质十分过硬，只是短暂的慌乱，他就重新镇定，然后冷冷地质问道：“你是什么人？这都后半夜了，你私闯民宅，是何居心？”

那男子笑道：“Trojan，别装了！代号 NTI 就是我。我们两家斗了这么长时间，你还不了解我们吗！”

军情五处的人！Trojan 心里一凉，他知道，今天晚上是别想活着出去了。想到这里，他缓缓地坐到椅子上：“你是怎么找到我的？”

Bob 说道：“我们早就知道了你们的‘木马’。你和一帮人去雷达站慰问，虽然百般伪装，我们还是怀疑上了你。你这段时间的无线电，我们早就解密了。”

Trojan 突然仰天大笑：“现在抓住我已经没有任何意义了。再过一个小时，德意志的飞机就会从朴次茅斯的上空经过，直扑伦敦。我敢说，过了今天，伦敦就会变成一片废墟，你们的女皇、你们的首相、你们的司令部全部都要变成粉尘。你如果不想死的话，不如投靠盖世太保，我可以留你一条命！”

Bob 什么也没说，冷笑着看 Trojan 表演。

Trojan 的声音开始变得有点歇斯底里：“刚才的三声巨响难道你们没有听到吗？那是我用定时炸弹，炸毁了你们的雷达站！没有了雷达，就你们那几架破飞机，凭什么跟我们对抗！我们的飞机一个小时就能到达这里，你们完了！”

Bob 冷冷地打断 Trojan 的话：“你确定只设置了三组定时炸弹？”

Trojan 一愣：“什么意思？我做的东西，难道我不知道？”

Bob 笑道：“很遗憾，你留下的三个‘宝贝’已经被雷达站的人全部查出……”

“骗三岁小孩子呢！你们要是查出来，为什么还要让它爆炸？难道你们还要庆祝已经过去了的万圣节？”

“我们只是为了给你一个错觉！”Bob 笑道，“你只有听到爆炸声，才会向你的上司发报，你们的飞机才会如期而至。而这正是我们所希望的，我们的飞机正好在空中拦截！”

“我不信！”口中说着“不信”，但是 Trojan 已经彻底绝望。

“不管你信不信，都要跟我走！别想逃，外面都是我们的人！”Bob 警告 Trojan。

“德意志万岁！元首万岁……”Trojan 大声叫着，使劲一咬假牙。

Bob 刚刚取出腰间的手铐，就看到 Trojan 的嘴角流出一缕黑血。他明知道抓捕盖世太保基本上会有这样的结果，心中还是有一点小小的遗憾。

终章 云地人机的决战

凌晨四点的英吉利海峡，海面上大雾弥漫，连探照灯的光线都无法穿透。而在高空，却只有片片灰色的云朵。

德国空军第一飞行大队的大队长 Attacker 驾驶着他最心爱的 Me-110 重型战斗机悄然出现在英吉利海峡上偏英国的一方。在他的身后，是二十多个飞行编队，其中有三百多架战斗机，和近七百架轰炸机。

在 Me-110 的下方，就是一团漆黑的朴次茅斯。由此向北，最多

半个小时，就能到达此次行动的目的地——伦敦。

今天晚上的行动，Attacker 也是参与策划了的。他早就知道，盖世太保的人潜入英国，伺机炸毁朴次茅斯雷达站。只要计划成功，他的飞行大队就会不受任何监测，进入英伦三岛如入无人之境。元首的战略如此犀利，让他佩服得五体投地。

“万圣节的礼物虽然晚了一天，但是，我想元首一定会喜欢！”Attacker 强抑着心头的兴奋，他用手轻轻地托起送话器，对他的部下们说道：“全体注意，跟上长机，还有不到半个小时就到伦敦，不许任何人掉队！”

话音刚落，各编队立即作出回应：“收到，绝不掉队！”

Attacker 对部下的迅速回应很满意，可是，就在这时，他的前面突然出现密密麻麻的黑色“蚊子”。

“中计了！”Attacker 的头皮一阵发麻，不由得向他的射手发牢骚，“英国佬怎么会知道我们这个时候来，而且还拦截得这么精准？难道他们的雷达还在？该死的 Trojan 发电报说，已经炸毁了他们的雷达，难道他叛变了？”

Attacker 在发飙的时候，对面的英国飞行大队长 Clouder 也在暗暗惊心：“我的上帝，德国人怎么派来这么多的飞机？起码相当于我们的二倍！”

心惊之余，Clouder 又暗自庆幸：“幸亏我们的雷达站还在，否则，被德国的飞机这么偷袭一次，我们英国皇家空军就要从地球上消失了！Trends 参谋长真是神机妙算，‘P2SO 战略’真是有效。哼哼，别看你们飞机多，这一次我一定要让你们有来无回！”

几乎在同一时间，Clouder 和 Attacker 下达了同样的命令：“开火！”

双方的大队长一声令下，所有的飞机都喷出火苗。防空机枪的子弹在空中像雨点一样任意挥洒。一时间，大围剿开始了。无数的黑色“蚊子”在英吉利海峡物上空翻飞、盘旋，好像在举办一场桑巴舞大赛。跳得好的，都获得掌声。跳不是好的，都被淘汰出局，坠入大海。

唯一不同的是，这些“蚊子”能喷出火焰。对手的舞姿一旦发挥失常，就会被刺上“毒刺”。

二十分钟一过，英德双方高下立判。英军只损失二十架飞机，德国却损失近百架，而且，这近百架飞机中绝大多数都是轰炸机。

Attacker 看得清楚，己方的轰炸机比英国的战斗机重，速度又比战斗机慢，相对来说就笨拙得多，轰炸机中的飞行员一不小心就吃了对方的枪子。于是，他立即下令：“所有的轰炸机向机群内部靠拢，由战斗机负责外围的防御。不要与敌人打胶着战，我们的目标是伦敦！”

Attacker 拎得清，哪怕他把这三百多架战斗机全丢在这儿，只要能带着余下的六百架轰炸机到伦敦走一趟，英国的海、陆、空指挥系统将全部瘫痪，伦敦这个城市也将会被从地球上抹去。

德军飞机的任何一个战术变化，都被地面上的雷达捕捉到，并且迅速通报给了 Clouder。他冷笑一声：“想走，没那么容易！”

于是，Clouder 对着送话器大叫：“全体注意，尽量攻打德军的轰炸机。哪怕放一架轰炸机前往伦敦，我都是大不列颠的罪人！”

Clouder 的命令立即得到回应，十几个飞行编队的队长几乎同时说道：“绝不放过一架德军的飞机前往伦敦！”

“立即采取第二作战方案！”

Clouder 此令一下，英国空军的阵形立即有了变化。十几架战斗机向德军的机群内渗透，集中火力打击德军的轰炸机。

“轰隆、轰隆……”德军轰炸机上因为携带了大量的炸药，每一架轰炸机被击中，都引爆了其内部的炸药，引起震耳欲聋的巨响。

转眼间，英军战斗机就以极小的代价，给德军造成重创。

“我的上帝！”Clouder 正兴奋之际，却看到了他最不想看到的一幕。一架标 033 数字的战斗机在攻击德军轰炸机的时候，被德军的机枪击中，冒着黑烟坠入英吉利海峡。

“队长，我要下去营救！”Clouder 战机旁边的一个编队队长说道。因为他知道，坠海的这个人是他们编队最优秀的飞行员，同时，他还是 Clouder 的儿子 Tom。

Clouder 有一种亲自跳进大海的冲动。但是，下一刻他就冷静下来。他抹了一把眼泪，对着送话器大叫：“全力战斗！”

“全力战斗！”每个英军的飞行员都异口同声地叫道。

不知不觉间，天光大亮。此时的英吉利海峡已经成了一个巨大的绞肉机，海面上到处可见飞机的残骸和飞行员的遗骸。而这些飞机残骸，绝大多数都是德军的。

“各编队立即上报损失！”Attacker 气急败坏地对着送话器大叫。

“一队损失十七架！”

“二队损失二十四架！”

“三队损失三十二架！”

……

二十多个编队共损失超过五百架飞机，也就是说，Attacker 带来的一千架飞机只剩一半了。可是，这还在朴次茅斯，离伦敦还远着呢。就算他们杀出一条血路飞到伦敦，能幸存几架飞机还真难说。而没有了轰炸机，到了伦敦又能怎样？

“立即返航！”Attacker 对着送话器大叫。

德军数百架飞机几乎在同一个时刻转向，远远的看去，倒也十分壮观。

Clouder 依然十分镇定：“德国佬要逃，不要放过他们，争取多打下几架飞机来！”

军令一出，英军飞机上的机枪扫射得更猛烈了。德国人又损失了一百多架飞机之后，被彻底赶出英吉利海峡。

战斗终于结束，地勤人员和海军开始打扫战场。Clouder 在一个勤务兵的引领下来到了他儿子 Tom 的遗骸前。

“Tom，爸爸没有照顾好你！但你的牺牲挽救了更多的生命！”说到这里，Clouder 看着远方的纵深防御阵地，禁不住老泪纵横。

而在海峡另一边的勒阿弗尔机场，Attacker 一下飞机就把自己关进了小黑屋。等在外面的勤务兵听到房间里传来一声枪响，心知不妙，急忙踹开门冲了进去，却看到 Attacker 躺在血泊之中，而他的右手边还有一把勃朗宁手枪。

“我们送给元首的万圣节礼物，元首一定不满……”Attacker 用尽最后一点力气，喃喃地说。

当4G遇上DDoS 实战鹰眼溯源

运营商技术部 罗摇松

关键词：攻击溯源技术 DDoS 攻击 可视化溯源分析 4G 网络

摘要：某运营商出现 4G 防火墙 CPU 异常增高，导致部分用户用 iphone 访问 apple 网站异常缓慢。针对可疑某一业务 IP，运用 BSA 大数据安全分析平台的 IP 业务可视化溯源功能，展开分析下钻，最终成功定位溯源，本文展示了这个实战过程，并提供一些思路。

一．业务分析排障过程

1.1 高速鹰眼：IP 业务可视化溯源

威胁可视化溯源的一个功能为业务流量分析溯源，可以分析网站、DNS、IP 业务。本次采用 IP 业务溯源功能，主要是针对某一业务 IP 或者 IP 段、业务端口和协议，及其对应的分析场景进行分析，包括 IP 业务端口流量流速、IP 业务来源地区流量、IP 业务来源地图、IP 业务流向地图、在线并发 IP、访问持续时间、帕累托图、协议流量溯源和路由器流量溯源。

IP 业务溯源任务模式也分为三种模式内存高速挖掘模式，在线挖掘模式和离线挖掘模式。主要是当前一个小时 8-12 亿数据，需要高速的分析和处理。

• 内存高速挖掘：将挖掘数据存放于内存中，可快速调用，用于反复使用的渐进式查询，优于数据量巨大，非常消耗群集内存，所以 Cache 模式适用于挖掘小数据量 1 天内数据，并且挖掘时建议先由过滤器过滤数据。

• 在线挖掘模式：输入挖掘条件，自动将挖掘条件生成过滤器，直接查询原始 Flow 表，方便快速查看某个分析场景，无需等待创建 Cache，适用于单次且数据范围小于一天的查询。

• 离线挖掘模式：分析较长时间（大于 1 天），预先查询需要数据，再进行数据压缩（合并小文件），新建物理表存于硬盘，后续可以重复且快速使用。由于数据量大，一般需要限定条件，如查询单个 IP 等等。

图 1.2 挖掘出的流量趋势图和统计表

1.2 第一步 分析某业务 IP 上行流量情况

1.2.1 某 IP 的原始上行数据

在业务分析溯源里的“IP 业务”针对业务某 IP 挖掘出相应时间段 3 月 24 号凌晨 1:00 -2:00 数据的数据。这是上行流量分析。

以下是某 IP 相应时间段 3 月 24 号凌晨 1:00 -2:00 的数据，由图中我们能看出流量趋势呈现较小的变化流量算比较平稳的。峰值大概为 2.3M/700B，总值为 3G/1M, 流次数为 1013。原始 Flow 表如右图所示，分别统计了源 IP 地址、目的 IP 地址、源端口、目的端口、流量、数据包、协议等。

图 1.1 挖掘条件图

1.2.2 IP 业务端口流量流速

在业务分析溯源里的“IP 业务”对原始数据进行分析场景分析，点击“IP 业务端口流量流速”分析具体网站端口的流量流速，一个网站有多个端口时候，可以有效分析流量最大或者流量特殊的端口情况。

图 1.3 IP 业务端口流量流速

图 1.3 是某 IP 相应时间段 3 月 24 号凌晨 1:00 -2:00 的 IP 业务端口流量流速数据，由图中我们能看出某 IP 开放的 443 和 769 端口，而且这两个时间段就这么两个端口开放。流量详情统计表如上图所示，分别统计了 IP 地址，协议和协议对应的端口流量的总值和峰值等。

1.2.3 IP TCPFlag 流量流速

在业务分析溯源里的“IP 业务”对原始数据进行分析场景分析，点击“IP TCPFlag 流量流速”分析具体网站的 TCPFlags 常用字段的流量的总值，峰值和流次数等等，还能分析 TCPFlag 各个常用字段的流量占比情况。

图 1.4 TCPFlag 流量流速图

图 1.4 是某 IP 相应时间段 3 月 24 号凌晨 1:00 -2:00IP 的 TCPFlag 流量流速图，由图中我们能看出 ACK 的流量最大峰值为 2M/500B，总值为 1.6G/519K，其次峰值总值最大的为 PSH-ACK 流量，所以响应和 Data 传数据的可能性较多。流量详情统计表如上图所示，分别统计了 TCPFlags 常用字段的流量的总值和峰值等。

1.2.4 在线并发 IP

在业务分析溯源里的“IP 业务”对原始数据进行分析场景分析，点击“在线并发”通过事件序列分析模式，分析在线并发 IP，直观显示 30 秒内消重后 IP 数量，方便用户定位用户突发造成的问题。

图 1.5 在线并发 IP

图 1.5 是某 IP 相应时间段，3 月 24 号凌晨 1:00 -2:00 的在线并发 IP 的趋势图，由图中我们能看出最大峰值为 19 个 IP 同时在线访问该站点，总值为 1001，从图上来看还是算比较正常的访问站点。

1.3 第二步 分析某业务 IP 下行流量情况

1.3.1 某 IP 的原始下行数据

在业务分析溯源里的“IP 业务”针对业务某 IP 挖掘出相应

图 1.6 挖掘出的流量趋势图和统计表

图 1.7 TcpFlag 流量流速图

时间段 3 月 24 号凌晨 1:00 -2:00 数据的数据。这是下行流量分析。

图 1.6 是某 IP 相应时间段，3 月 24 号凌晨 1:00 -2:00 的数据，由图中我们能看出时间段 1:30 -1:35 流量趋势呈现出突增现状。峰值大概为 626.4M/1.1M，总值为 65.1G/102.7M, 流次数为 1427。原始 Flow 表如上图所示，分别统计了源 IP 地址、目的 IP 地址、源端口、目的端口、流量、数据包、协议等。

1.3.2 IP TCPFlag 流量流速

在业务分析溯源里的“IP 业务”对原始数据进行分析场景分析，点击“IP TCPFlag 流量流速”分析具体网站的 TCPFlags 常用字段的流量的总值、峰值和流次数等等。还能分析 TCPflag 各个常用字段的流量占比情况。

图 1.7 是某 IP 相应时间段，3 月 24 号凌晨 1:00 -2:00IP 的 TCPFlay 流量流速图，由图中我们能看出 FIN-ACK 的流量最大峰值为 461.5M/779.5K，总值为 51.4G/86.9M，其次峰值总值最大的为 RST 流量峰值为 8.7G/14.7M，总值为 176.6M/298.3K，所以可能关闭了连接又连接重置。流量详情统计表如上图所示，分别统计了 TCPFlags 常用字段的流量的总值和峰值等。

1.3.3 在线并发 IP

在这种数据突增的情况下，我们可以来分析访问 IP 是不是增多了很多。在业务分析溯源里的“IP 业务”对原始数据进行分析场景分析，点击“在线并发”通过事件序列分析模式，分析在线并发 IP，直观显示 30 秒内消重后 IP 数量，方便用户定位用户突发造成的问题。

图 1.8 是某 IP 相应时间段，3 月 24 号凌晨 1:00 -2:00 的在线并发 IP 的趋势图，由图中我们能看出最大峰值为 21 个 IP 同时在线访问该站点，总值为 1178，从图上来看还是算比较正常的访问站点，

图 1.8 在线并发 IP

没有剧增很明显。

1.3.4 初步结论 --下行流量导致流量突增

得出初步结论，在 1 点 30 分 -35 分，从 apple 网站的返回流量突然从正常的 2Mbps 突增到 600M bps，TCP-Flag 的 FIN-ACK 流量峰值 461.5M bps，RST 流量峰值 176.6M bps。

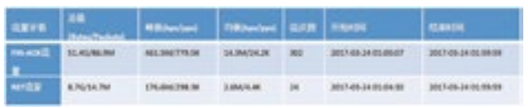


图 1.9 TCP-Flag 表

1.4 第三步 采用时间过滤器下钻到故障 5 分钟

1.4.1 采用可视化拖拽的方式下钻故障时间片

用鼠标拖拽流量突增时间端，会自动建立一个时间过滤器。

1.4.2 分析流量详情

分析流量突增，可以看出更清晰的流量分布。

1.4.3 分析 TCPFlag 流量详情

确认TCP-Flag流量分布，进一步确认fin-ack和rst包是最大的数量。

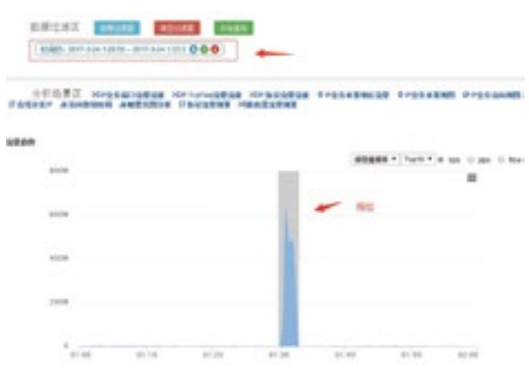


图 1.10 拖拽生成时间过滤器

图 1.11 突增流量详情表

图 1.12 TCP-Flag 突增流量详情表

1.4.4 帕累托特图分析锁定目标，并过滤可疑 IP

在这种数据突增的情况下，我们可以快捷拖拉生成时间过滤器对突增的情况进行更加精准的时间段分析。

在业务分析溯源里的“IP 业务”对原始数据进行分析场景分析，点击“帕累托图”通过采用帕累托图分析，可以支撑严谨定义的帕累托图分析方法，分析师可以定义 flow 的各个要素进行分析。

图 1.12 是某 IP 相应时间段，3 月 24 号凌晨 1:30:4 -1:33:3 的帕累托图，由图中我们能看出源 IP 为某 IP 和目的 IP 为某 IP 占比 Top1 为 99.68%，同样统计表的数据也显示该源目 IP 的总值为最高值 7.5G/101.5M，峰值也是最高值为 132.5M/1.8M，流次数什么的都跟其

图 1.13 帕累托图

他访问差距很大，其他的访问量都很小。

1.4.5 定位目的某 IP 分析

刚刚我们看到异常的目的 IP，现在我们通过“IP TCPFlay 流量流速”对该目的 IP 进行定位分析，所以我们添加该目的 IP 的过滤器。

图 1.14 添加过滤器

图 1.15 流量流速图

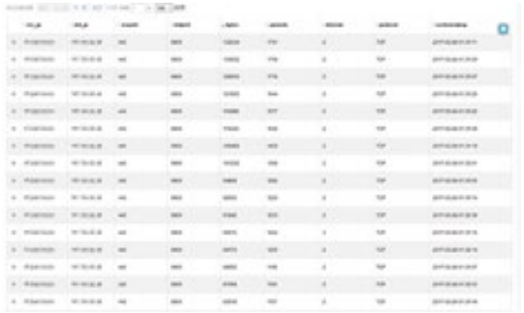


图 1.16 流量流速详情统计表

在业务分析溯源里的 “IP 业务” 对原始数据进行分析场景分析，点击“开始查询”分析过滤器的目的 IP 流量的总值，峰值和流次数等等。

图 1.6 是某 IP 相应时间段，3 月 24 号凌晨 1:30:4 -1:33:3 时间段的流量流速图，由图中我们能看出流量最大峰值为 624.7M/1.1M，总值为 60.1G/101.5M，其次从流量详情统计表中我们还能看到，该源 IP 到目的 IP 全是从 443 端口到 9069 端口，而且还有些包流量较大，基本上能锁定这对源目 IP 可能是业务的问题。

二．该业务故障排障结论

1、某运营商防火墙异常，原因是内网某 IP，访问苹果某 IP 出现异常问题导致。

2、通过某时间段 1:30 -1:35 上下行流量对比分析。可以看出，故障时候内网某 IP，访问苹果某 IP 的上行流量峰值为 21k，但是下行流量高达 624Mbps.

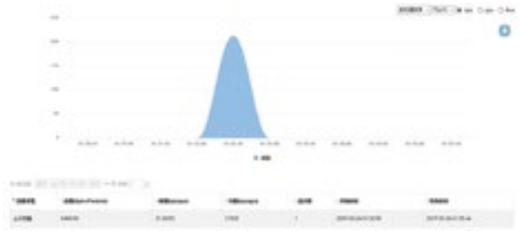


图 2.1 上行流量图

图 2.2 下行流量图

3、发现该源 IP 到目的 IP 在某一时间段很集中，还全是从 apple 源 443 端口到目的 9069 端口，而且还有些包流量较大，基本上能锁定这对源目 IP 可能是业务的问题。

4、在 TCPFlag 流量流速中，上行报文中没有发现 syn。下行报文发现 FIN-ACK 流量峰值 461.5M bps，RST 流量峰值 176.6M bps。

5、从绿盟威胁情报库里面看，这 2 个 IP 都是安全的，没有发生过历史安全事件。

下一步的工作，进一步分析防火墙上某 IP，定位端口 9069 是什么设备，确定设备种类。（运营商有上网日志留存系统。）

金融行业未知威胁检测探知之道

金融技术部 张政祺

关键词：APT 攻击 未知威胁检测 未知威胁防御 威胁态势感知

摘要：对于信息安全而言，建立完善的安全体系和纵深的防御措施是目前主流的安全理念。针对已经存在于系统中的威胁检测，特别是由 APT 攻击带来的未知威胁检测，就显得手段单一，架构模糊，效果也就差强人意。因此，本文针对未知威胁检测探知的思路之前的防护手段做一个简单的梳理。

未知威胁

未知威胁来源

谈到未知威胁，首先还是从 APT 攻击开始谈起。APT（Advanced Persistent Threat）高级持续性威胁，是指隐匿而持久的计算机入侵过程，通常由某些人员或组织精心策划，针对特定的目标。

• Advanced 高级——采用先进的攻击技术和复杂的攻击工具，利用多种 0day 漏洞。

• Persistent 持续性——长期潜伏监或控制特定目标。

• Threat 威胁——人为参与策划的攻击行为。

综上所述，APT 攻击由于利用 0day 漏洞，攻击技术复杂，具有特点：

• **不易发现**

• **渗透性强**

APT 攻击是一个长期的过程，且极其隐蔽，不易被发现，具有特点：

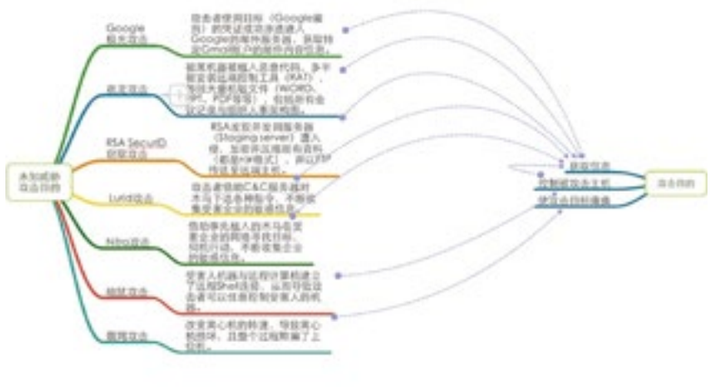
• **潜伏周期长**。

因此在系统中，有别于传统的病毒、蠕虫或各类已知攻击手段，APT 攻击带来的是真正的未知威胁。基于以上特点，未知威胁存在

于网络中的可能性更高，且更隐蔽。

攻击目的

上文中提到“APT 攻击带来的是真正的未知威胁”，那么攻击的最终目的是什么？我们的信息系统中，攻击者最在意的是什么？下图中，列举了几项知名的 APT 攻击事件，通过分析攻击者的攻击行为与攻击结果，总结出 APT 攻击背后的真实意图。



攻击目的总结为三类，获取信息，既攻击者通过数据窃取方式得到敏感信息和关键信息；控制主机，既攻击者取得主机控制权以便监视行为和远程操控，大部分情况下，作为跳板机，目的同样是获取信息；摧毁目标，既破坏物理设备。

从上述 7 个 APT 事件结果来看，其中 6 个都是以获取信息为目的，占比为 85%；仅有 1 项是以破坏物理设备为目的，占 15%。

金融行业未知威胁

未知威胁在金融行业中，数据窃取为目的占比远高于行业平均，也就是几乎所有攻击全都指向关键服务器，目的是获取有用的客户信息（银行和保险）、机密的交易数据（证券和基金），最终通过这些信息获得经济利益。

知名的“证券幽灵”就是典型的针对数据窃取的攻击。长期潜伏在证券业者网络内的未知威胁，慢慢积累大量交易信息，通过这些内幕信息交易获利。

因此，在自己的网络内是否存在此类未知威胁，成为了金融行业信息安全从业人员的一个心病。在建立完善的安全体系扎紧篱笆后，是否存在之前潜伏的未知威胁？该如何去发现它？

未知威胁探知

未知威胁防御

谈未知威胁检测前，简单来介绍下未知威胁的防御之道。

对于未知威胁的防御，传统的安全解决方案，如 IPS、防病毒等基于签名技术的防护手段已经不再有效。目前比较理想的方式是采用沙箱虚拟执行，构造一个可控，可记录的真实模拟环境，运行可疑文件，通过其触发的行为和网络连接状态来判断是否属于未知威胁。

未知威胁检测之殇

目前信息安全技术措施主要落在“防”上，“检”的手段单一，效果欠佳；安全管理理念建好防护体系，没有安全事件发生的网络环境默认安全，忽视“检”的作用。意识形态上检测的不必要性，安全手段上检测能力的差异性，导致安全威胁、未知威胁检测发展步伐缓慢，严重滞后，是整个安全防御体系中的一大短板和隐患。

未知威胁检测探知之道

那么沙箱虚拟执行的防御模式能否应用到未知威胁检测中来呢？答案是否定的。通常需要被检测的网络内设备众多，设备中的文件类型繁杂，数量更是惊人，要完成每个文件的虚拟执行来判别是否为未知威胁是不现实的。

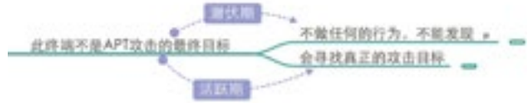
未知威胁检测探知的思路需要从另一个角度展开，以 APT 攻击的目标终端为本，未知威胁的异常行为为导向，通过逆向的思维来推导出如何对未知威胁进行检测。

逆向的第一步是判断终端设备是否为安全的，如果是安全的终端，则不考虑检测方法；如果是不安全的终端则判断其是否为 APT 攻击的最终目标。前文中提到金融行业 APT 攻击目的是数据窃取，因此攻击者需要最终到达关键服务器和存储关键信息的终端设备。所以，未知威胁的检测目标进一步可以细化为跳板机和目标机。

跳板机

跳板机，APT 攻击的非最终目标，通过它作为中转站将未知威胁传送到真正的目标主机。

未知威胁存在于跳板机中有两种状态，一是潜伏期，二是活跃期。



第一种状态暂时对终端设备没有任何威胁，且不易被监测到，因此不考量此状态下的检测手段。

第二种状态下，未知威胁会通过一系列行为向真正的攻击目标转移，在此过程中通过网络、主机层的安全检测手段来进行未知威胁探知。此过程中，通常的攻击行分为两步，判断终端——攻击跳转。

1)APT 攻击在前期准备过程中，会有大量社工行为，充分掌握攻击目标的人员资料、网络情况等等信息，所以通过主机信息可以判断终端是否为最终攻击目标，既关键服务器等。扫描主机的过程会是一个异常的终端行为，因此，对于跳板机的未知威胁检测第一种方式就是针对异常的终端行为日志分析。采用绿盟企业安全平台

ESP 对终端设备日志收集，将大量的日志数据精细化到安全日志，结合其他安全设备日志，达到未知威胁检测的目的。

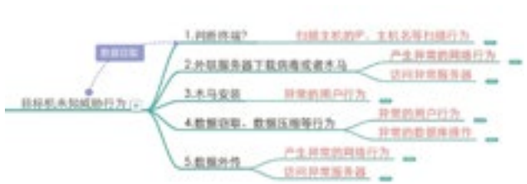
2) 攻击者判断终端为跳板机后，未知威胁必然会通过网络传播，自我复制传输到其他的终端设备。APT 采用较多的水坑式或鱼叉式攻击，针对办公网络，在此类型网络内，使用者网络行为较为固定，因此可以绘制出网络行为白名单作为安全基线。因此，在传输过程中，通过安全基线可以很容易的发现网络中的异常行为，结合绿盟成熟的 NGTP 方案（NIPS+TAC）便可在此阶段检测出未知威胁。

目标机

目标机，APT 攻击的真正目标，窃取此终端上的关键数据。

未知威胁在目标机上的行为模式与绿盟态势感知攻击链模型中的几个阶段相对应。

攻击链模型分为七个阶段：侦查——工具制作——投送——攻击渗透——安装工具——命令控制——恶意活动。



目标机的未知威胁行分为是：判断终端——下载工具——安装工具——数据窃取——数据传输。对应攻击链模型中后四个阶段，覆盖了 APT 攻击整个事中阶段。

1) 与跳板机相同的终端判定，未知威胁的检测方式同上，不予累述。

2) 攻击者判定为目标机后，大部分的 APT 攻击会从 CC 服务器下载病毒、木马或者其他恶意程序，从而产生异常的网络行为，采用 IPS+TAC 组合拳在网络层进行检测防护。同时，绿盟威胁情报中心 NTI 拥有的恶意 IP 情报，能定位出 CC 服务器，结合 IPS 更加准确的抓住网络内的未知威胁。

3) 木马安装和数据窃取阶段产生的异常用户行为，采用用户行为基线结合绿盟 NGTP 方案（NIPS+TAC）便可做到未知威胁检测。

4）当数据存储于数据库中，绿盟 DAS 能对关键数据库操作进行防护检测，判定用户操作行为、操作权限，从而发现可能存在的未知威胁。

5）与行为 2 下载工具阶段的网络数据流向相反，但产生相同的异常用户和网络行为，可以采取上述相同的威胁检测手段。

结束语

未知威胁探知在 APT 攻击的各个阶段采取的手段措施多样，是一个综合性的解决方案。真正要做好对 APT 的防护，未知威胁的检测，还需要用户和安全厂商的共同努力。

在做好“防”的情况下，完成“检”或许才能真正的让用户的信息安全水平得到提升。

工业控制系统安全服务实施方法设计

分销业务线 庞南　产品线ICS产品团队 王晓鹏　工程线安全服务部 胡斌

关键词：工控安全 信息安全服务 工控系统与 IT 系统的差异
ICS 安全服务

摘要：在不同行业客户中，由于行业业务属性存在较大差异，应用场景差异也不小，这就需要尽量贴近行业业务特点，给出有针对性的行业解决方案，同时还应当建立起一套用于规范工控安全服务工程实施的方法论，本文尝试提出一种工控安全服务实施方法的设计思路。

引言

工业控制系统（ICS）在传统上凭借封闭的专有协议，以及与外部其它网络环境相独立，即便与之配套的安全控制机制普遍设计不足，通常意义上也被认为安全风险水平较低，其安全保障并未得到应有的足够重视。

伴随着工业化与信息化的融合，信息技术已经成为工业系统的重要支撑力量，而随之而来的，安全威胁和安全风险显著提高。近年来频繁曝光的与工业控制系统相关的安全事件，其中以 2010 年伊朗核电站 Stuxnet 震网病毒事件在全球范围内引起了对工业控制系统安全的重视，西方国家尤其是美国从 90 年代开始已经开始了针对工业控制系统安全的研究，在各个行业相继出台了标准规范来指导工业控制系统安全的建设。发生在 2015 年的乌克兰电网 Blackenergy 恶意软件事件为工业控制系统安全又一次敲响了警钟，而且由于广泛使用工业控制系统的行业通常是关系到国计民生的重点行业，各国政府也对工业控制系统的安全保障给予越来越高的重视。

我国自 2008 年正式发布标准，推行信息系统安全等级保护政策以来，为适应信息技术和应用的发展趋势，于 2015 年开始组织对等级保护基本要求进行全面修订更新，面向若干新领域和新场景有针对性地提出了安全保护扩展要求，其中就包括了工业控制系统场景。另外相当数量的工业控制系统属于 2016 年 11 月正式颁布的《中华人民共和国网络安全法》中所界定的关键信息基础设施，网络安全法将对关键信息基础设施的安全保障提高到了国家法律的高度，也证明了国家对于工业控制系统的安全保障给予了空前的重视。

公司对工控安全领域进行了持续的技术跟踪和研究积累，产品线在 2016 年正式成立了工控安全产品团队，着力于研究相关标准、设计工控安全解决方案、研发工控安全产品。业务线致力于响应和

挖掘行业客户的工控安全需求，并促成项目落地。我们在了解和接触到的一些工控安全项目机会中，深深感触到工控系统在不同行业客户中的应用场景因为行业业务属性的区别而存在较大差异，为尽量贴近行业业务特点给出有针对性的行业解决方案，不仅需要对不同行业工控系统环境进行深入调研和理解，还应当建立起一套用于规范工控安全服务工程实施的方法论，本文尝试提出一种工控安全服务实施方法的设计思路。

1 信息系统安全保障方法论回顾

首先，我们来回顾一下 IT 信息系统的安全保障思路。我们暂且不去考虑更高层次的周期性安全风险管理过程，以及由被称为最佳实践的安全管理控制措施构成的所谓安全管理体系，仅从信息系统的安全技术保障方面来讲，面向安全域的纵深防御是得到最普遍认可的工程方法，无论是自 1998 年发布并且多次修订更新的信息保障技术框架 IATF，还是在国内广泛实施的信息系统安全等级保护系列标准，这一思想在众多的权威标准规范中都得到了体现。

我们在为一个特定的网络和信息系统设计安全保障技术方案时，通常都会遵循和执行以下的工程步骤：

1、调研信息系统所在的网络环境结构，以及信息系统的构成组件和工作机制，从而能够理解网络拓扑机构、信息系统的软硬件资产构成及其在网络中的部署位置、信息系统不同组件之间的通信机理和数据流转情况。

2、对网络和信息系统进行安全域划分，安全域的划分依据是信息系统及其组件的重要性级别不同，安全域划分的表现形式通常是划分出代表不同安全级别的网络安全域，同一安全域内部分布的信息资产往往具备相同的安全级别，并适用于一致的安全策略。

3、对某一个特定的安全域，需要从边界防护、域内计算环境保护、以及跨越边界的数据安全传输等三方面选择适当的安全技术控制措施，以达成安全保障目标。所选择的安全控制措施不仅要适应 IT 信息系统的层次化特点，全面覆盖物理环境、网络、系统、应用、数据等层面，还应当符合信息保障要求，通常遵循 PDRR 安全模型，兼顾事先预防型（Protection）、事发检测型（Detection）和响应型（Reaction）、事后恢复型（Recovery）等不同类型。选择安全技术控制措施的依据由风险评估的结果决定的安全需求和合规性要求两方面组成，而一些权威性的安全标准规范（例如 NIST SP800-53 和 GB/T 22039 信息系统安全等级保护基本要求）则提供了安全技术控制措施的参考基线，其中包含了大量可供选择的安全控制措施。

4、以确定需要采用的、同时当前系统环境中未部署的安全技术控制措施为基础，编写安全技术设计和实施方案，用于指导后续的安全项目建设。

通过上述步骤我们可以看出，在开始以具体的安全产品或安全系统完成安全项目交付之前，为了能够有效贴合特定网络和信息系统的实际情况，给出有针对性的安全设计方案，需要完成系统调研、风险评估、安全域划分、控制措施选择、甚至安全基线差距分析等一系列工作过程，而这一过程通常是由专业人员以服务的方式完成。

2 工控安全项目推进面临的挑战

在响应行业客户的工控安全需求，推进工控安全项目落地的过程中，当前面临着几个方面的挑战。

2.1 工控系统环境的行业性差异

按照工业企业生产工艺的组织方式，通常将工业企业区分为流程工业和离散制造业两类。

• 流程生产企业的生产方式，主要是通过对原材料进行混合、分离、粉碎、加热等物理或化学方法，使原材料增值。典型的流程生产行业有医药、石油化工、电力、钢铁制造、石油化工、水泥等领域。

• 离散制造企业的生产方式，主要是通过对原材料物理形状的改变、组装，成为产品，使其增值。典型的离散制造行业主要包括机械制造、电子电器、航空制造、汽车制造等行业。

业务线所覆盖的行业客户中，广泛建设和使用工业控制系统的典型行业包括电力（发电与输电）、石油化工、燃气、煤炭、冶金、机械制造、家用电器制造、汽车制造、市政水务处理、轨道交通、港口码头、水利管理、道路交通管理、军工制造等，由于生产的产品类型不同，其工业制造过程在产品结构、工艺流程、作业调度等方面都存在着非常显著的行业化差异，由此所导致的工业控制系统的体系架构、组件构成、应用模式也存在着同行业内相似度较高，不同行业之间差异较大的现状。

出于安全服务于业务的基本原则，为促进工控安全项目的有效推进和落地交付，需要对各个重点行业客户的生产过程和工控系统应用情况进行深入细致的调研，充分理解特定行业客户的生产过程、控制需求以及工控系统的架构组成、部署和使用模式，才能够真正做到理解客户业务，继而有效识别安全缺陷，给出有针对性的安全建议。

因为工业控制系统的行业化差异，决定了不可能有所谓通用的工控安全解决方案，而是必须面向不同的行业业务特点和控制系统应用模式，制定行业化的工控安全解决方案。

2.2 ICS 与 IT 系统的体系架构差异

区别于单纯的 IT 系统，工业控制系统 ICS 因为使用 IT 技术的同时，还涉及对于物理组件的控制，更加接近于德国工业 4.0 和中国制造 2025 等战略规划中“两化融合”的核心概念—信息物理系统 CPS。目前已经有了众多论述涉及 ICS 与 IT 系统的比较和差异，两者在系统性能、通信协议、风险管理、运维模式、事件影响、应急处置、系统生命周期等方面都存在着众多明显的差异。

鉴于以上原因，习惯性使用面向 IT 系统进行安全分析和保障的思路显然并不恰当，必须要从 ICS 系统自身的架构和体系模型出发，或者说从工业控制系统的视角来看待工控安全问题，才能真正做到有的放矢。当务之急是建立工控系统及其安全保障的知识体系，实现从 IT 视角向 ICS 视角的转换。

2.3 服务实施方法论成熟度

一方面由于工控系统安全保障仍属新兴专业领域，另一方面由于工控安全领域的标准规范还在陆续推出，其提供的工程实施方法论也处于完善过程之中，因此工控安全服务方法也需要摸索和总结，才能有效支撑工控安全项目的实施。

3 工控安全服务方法论

按照安全保障 PDCA 过程方法论，在真正开始实施具体的安全

控制措施之前，应当对保障对象及其安全保障的现状调研、与权威安全基线之间的差距分析，继而输出针对特定安全保障对象的安全建议，并对安全建议内容进行合理的规划。因此，特定 ICS 的安全保障项目应该从一个服务过程开始，然后再进入后续的具体安全产品的采购和部署，是一个更加合理的次序。

本文提出的 ICS 安全服务过程的设计，能够提供一种工程方法指导。从服务过程角度，ICS 的安全服务过程与 IT 系统安全服务过程比较类似，但是具体深入到其中的服务步骤中时，由于 ICS 与 IT 系统之间的差异，服务实施的具体方法会存在着显著的不同。

3.1 服务过程

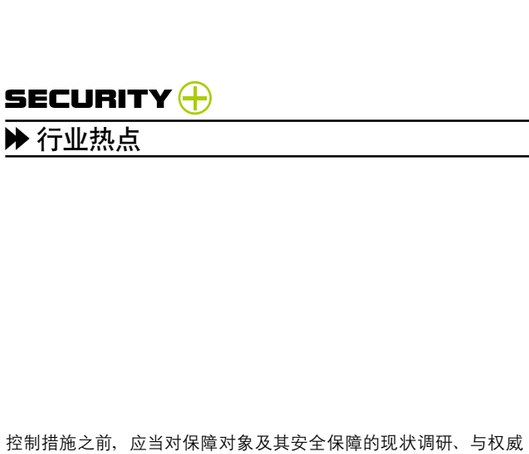


图 1 工控安全服务过程

首先，ICS 的安全服务过程应该优先于 ICS 的安全实施过程。其次，ICS 项目的安全服务过程，一共包括了 ICS 应用调研、安全域划分、安全控制基线构造、差距分析、建设方案编写等 5 个服务步骤。

3.2 任务步骤

3.2.1 ICS 应用调研

对 IT 应用的服务过程中，现状调研步骤的关注重点包括网络拓扑结构、应用类型、支撑应用的软硬件资产在不同的网络区域中的分布、以及部署在网络环境中的安全技术措施等，现状调研步骤的输出物包括了体现了信息资产分布的网络拓扑图、软硬件信息资产清单、以及信息资产的各组件在网络拓扑图中的数据流图等。

ICS 应用与传统的 IT 应用之间的最显著区别在于，虽然两者都会涉及到过程控制，但是 IT 系统通过软件所实现的过程控制，完全是抽象实现于 IT 系统的各组件之间的逻辑过程，而 ICS 应用所实现的过程控制通常都是按照工艺流程，对对物理设施实现的实际控制过程。这点区别决定了，不能够用 IT 应用的视角去看待 ICS，ICS 的架构描述需要从其自身的视角用专门的模型去完成。

IEC 62264 是关于企业控制系统集成的一个标准族，该标准在 2006 年被等同采纳为 GB/T 20720 国家标准，该标准族的第一部分引用了普渡大学的 CIM 参考模型所提供的层次结构模型和功能数据流模型，来描述工业企业生产控制系统的通用架构和工作机制，尤其是其中的层次结构模型，为我们从正确视角看待 ICS 的体系架构提供了重要参考。

新修订的面向工业控制系统的等级保护扩展要求，在 GB/

T20720 标准提供的层次结构模型基础之上，将 ICS 中 SCADA、DCS、PLC 等系统的共性进行了抽象，依次归纳出逐级细化的功能层次模型、功能单元映射模型、和资产组件映射模型，其中前两个模型都包括了 5 个抽象层次，第三个模型只包括 5 个抽象层次的下面四个层次，这是因为第五层企业资源层的系统并非 ICS，而是属于传统 IT 系统的范畴。

在对特定客户的 ICS 应用进行调研时，应当参考功能层次模型，从企业资源层、生产管理层、过程控制层、现场控制层、及现场设备层这 5 个不同层次，对每个层次中的功能单元和支撑功能实现的资产组件进行调查和汇总，最终用功能单元映射模型和资产组件映射模型，来描述这个特定 ICS 的体系架构和资产组件构成。

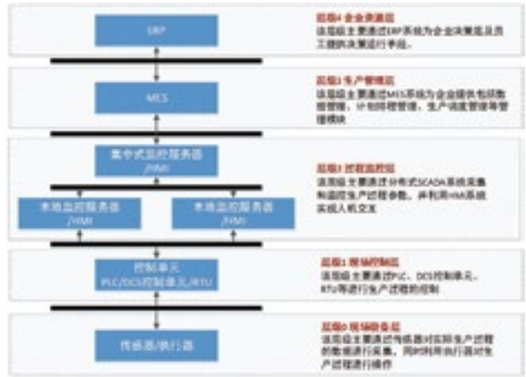


图 3 工业控制功能单元映射模型

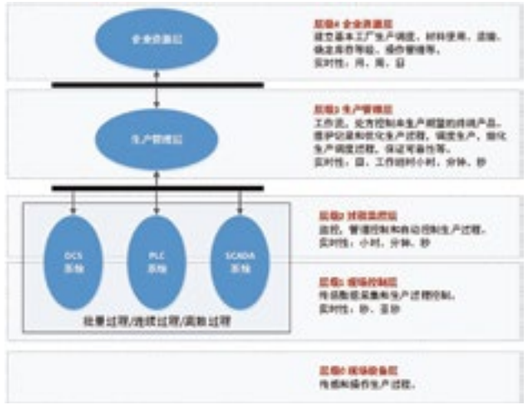


图 2 工业控制功能层次模型

图 4 工业控制资产组件映射模型

- ICS 应用调研步骤的输出结果应当包括：
- 功能单元与资产组件映射详图
- 资产组件清单
- 管理机制描述

3.2.2 安全域划分

虽然描述 IT 系统和 ICS 的架构模型方法、以及资产组件构成不同，但是从安全保障的基本原则和思路方面，两者又是非常类似。几乎所有面向工业控制系统安全保障的权威标准，不论是 NIST SP800-82R2、IEC62443、还是新修订的面向工业控制系统的等级保护扩展要求，都提出了对 ICS 划分安全域，并且按照纵深防御的原则选择适当的安全技术措施对安全域的边界和内部计算环境进行安全防护的整体思路，这一思路与 IT 系统的安全保障思路如出一辙。

IT 网络和系统的安全域划分，通常以网络区域的形式体现，不同的网络区域，代表着不同的安全级别，分布着重要性不同的信息资产，每一个安全域适用于一个统一的安全防护策略。

IEC 62443-1 标准提供了工业通信网络和系统安全的概念和模型，其中给出了安全域的划分方法描述，新修订的面向工业控制系统的等级保护扩展要求引用了 IEC62443-1 的安全域划分方法，并且给出了典型的 DCS 系统和 SCADA 系统的安全域划分示例。

下图为典型的工业化生产企业 DCS 系统结构图，该图将企业内整个网络和系统分为五个层次，包括企业资源层、生产管理层、过程监控层、现场控制层和现场设备层，其中企业资源层和生产管理层为传统的 IT 系统，而过程控制层、现场控制层以及现场设备层为工业控制系统，与 IT 系统有着截然不同的安全需求。一般将企业资源层划分为两个安全域，一个安全域包含的是所有面对互联网提供的公共服务，另一个安全域包含的是所有面对内联网提供的内部服务。在现场层一般会将不同工艺的工业化设备划分为独立的安全域，并通过开放的 opc 服务与上层进行数据交互。

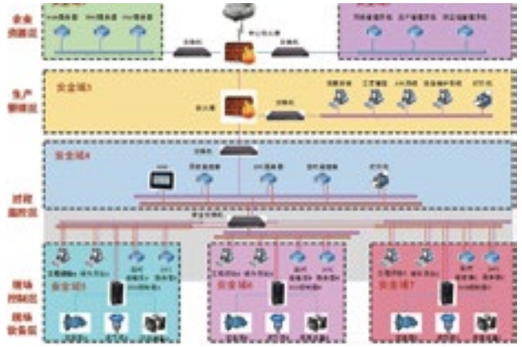


图 4 DCS 系统安全域划分

下图为典型的电力行业调度中心与智能化变电站 SCADA 系统结构图，调度中心与智能变电站通过 IP 认证加密装置进行纵向联系，根据调度中心和智能变电站的功能特点，调度中心被划分为企业资源层和生产管理层，智能变电站被划分为站控层、间隔层和过程层，分别对应到工业化控制企业的过程监控层、现场控制层和现场设备层。在智能变电站内部根据系统的实时性要求不同，又被划分为实时控制区和非实时控制区。

对 ICS 进行安全域划分的结果，可能包含两种情况

• 层内域，即划分出的安全域范围仅涉及 ICS 层次结构模型中的某一层次

• 层间域，即划分出的安全域范围同时包括了 ICS 层级结构模型中的两个或多个层次

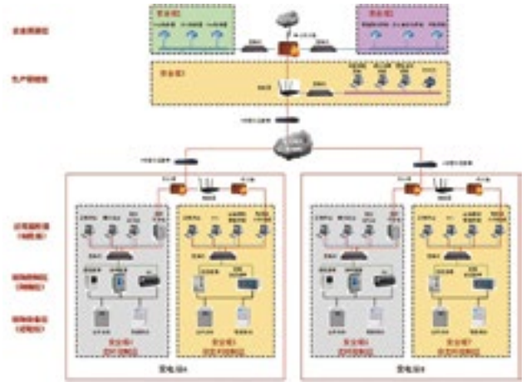


图 5 SCADA 系统安全域划分

以上两种类型的安全域在后续提供安全保障措施时，存在一定的差异，相对于层内域，层间域一方面因为包含了多个层次而减少了需要保障的安全域边界数量，另一方面又因为包含了多个层次结构，而需要在域内环境保护方面，同时考虑对其中每一个特定层次结构的安全控制措施。

ICS 安全域划分步骤的输出成果为建立在资产组件映射图基础上的《ICS 安全域划分示意图》。

3.2.3 安全控制基线构造

• 任何系统的安全保障目标都是通过部署和使用一系列适当的安全控制措施才能达成，ICS 的安全保障也不例外。几乎所有与 ICS 安全保障有关的权威标准、规范和指南，都是面对划分好的安全域，从安全域边界隔离和防护、安全域内部计算环境安全控制等方面，提供了可供使用或者要求具备的安全技术控制措施集合。例如：

• 《NIST SP800-82R2 工业控制系统安全指南》用第五章来专门阐述 ICS 的安全体系架构和推荐的安全控制措施；

• 2016 年发布的《GB/T32919 工业控制系统安全控制应用指南》在第六章阐述了安全控制基线的设计方法，并在附录 B 中用较大的篇幅给出了推荐的共计 18 类安全技术控制措施和安全管理控制措施列表；

• 新修订的《网络安全等级保护基本要求第 5 部分 工业控制系统的等级保护扩展要求》中要求根据定级对象的等级保护级别和划分好的安全域，分别针对安全域可能涉及的工控系统层次结构的下 4 层，给出了安全技术控制措施的扩展要求。

应当对上述的多项标准规范所提供的安全控制措施基线建立深入的理解，并在任何一个特定的 ICS 项目安全服务过程中，根据服务对象的实际情况，为 ICS 建立应有的安全保障控制措施基线，其中所采取的控制措施，一方面是为了符合合规性要求（例如等级保护要求），另一方面是在实践中被证明对控制 ICS 安全风险行之有效的最佳实践经验。

特定的 ICS 项目安全服务过程，在构造安全控制措施基线时，可以分两种模式进行：

• 当 ICS 的安全保障特别注重等级保护合规时，可以直接根据等级保护级别和安全域中的功能层次，从《网络安全等级保护基本要求第 5 部分 工业控制系统的等级保护扩展要求》提供的控制措施基线中选取特定安全域应该具备的安全技术控制措施，一个完整 ICS

的安全保障，体现在对每个安全域的安全保障基础之上。另外，从《网络安全等级保护基本要求》中选择对应等级保护级别的安全管理措施，与确定好的安全技术措施共同组成 ICS 安全基线，需要特别指出的是，安全技术措施是面向组成 ICS 的每个安全域的，而安全管理措施通常是面向整个 ICS 的。

• 当 ICS 的安全保障不以等级保护合规为主要目的，而是要求尽可能全面有效控制 ICS 面对的安全风险，那么可以借鉴《网络安全等级保护基本要求第 5 部分 工业控制系统的等级保护扩展要求》中针对每个安全域的不同功能层次建立安全控制措施的思想，但是在具体的控制措施选择上，不需要局限于等级保护标准，而是同时参考多项安全标准规范，尤其是客户所属行业的工控安全规范，将其中有价值的控制措施识别并合并，提炼出一套融合了多个标准的更加完整的控制措施基线。

本服务步骤的输出成果为面向某特定 ICS 的《安全控制措施基线》。

【说明】本文旨在对 ICS 安全服务过程和主要步骤的工作思路进行整理和归纳，因此未去涉及具体的 ICS 安全控制措施基线的具体分析和详细设计，这部分工作将在后续的技术文章中进行阐述。

3.2.4 差距分析

在本服务步骤中，要将前期对 ICS 应用及其安全保障现状的调研结果与设定好的安全控制措施基线进行逐项比较，从而识别出 ICS 的安全保障现状与基线要求之间的差距。

本服务步骤的工作与 IT 系统安全差距分析的做法非常类似，输出成果为《ICS 安全基线差距分析报告》。

3.2.5 建设方案编写

在本服务步骤中，根据前期工作输出的安全基线差距分析报告，可以识别出当前 ICS 在安全保障方面的不足，所有安全基线中要求的、而当前又不满足的技术措施和管理措施，都应当被合并构成后续的安全建设内容。

需要说明的是，多项安全建设内容可能受限于可投入资源规模，而需要分期建设，因此《ICS 安全建设方案》应该考虑到将建议的建设内容，合理进行规划，给出分步有序的建设路线图建议。

5 小结

本文基于对多个权威标准规范的深入学习理解，并结合 ICS 安全项目经验，介绍 ICS 与 IT 系统在架构方面的差异，分析了在实际工程项目中面临的挑战，然后提出了一种 ICS 安全服务过程的设计方法，对特定 ICS 安全项目的工程实施过程具备参考和指导意义。

参考文献

[1]《GB/T 20720.1-2006/IEC62264.1-2013 企业控制系统集成 第 1 部分 模型和术语》

[2]《NIST SP800-82R2 工业控制系统安全指南》

[3]《GB/T32919-2016 工业控制系统安全控制应用指南》

[4]《网络安全等级保护基本要求第 5 部分 工业控制系统的等级保护扩展要求》

[5]《IEC 62443-1-1 工业通信网络 网络和系统安全 第 1-1 部分 术语、概念和模型》

物联网安全公司及产品介绍

创新中心 张星

关键词：物联网安全需求 物联网安全公司 物联网安全产品

摘要：本文是物联网安全系列文章的最后一篇，通过上期介绍物联网安全技术研究的思路之后，笔者为大家选取了五家公司，在介绍公司产品的同时，也会对其所关注的行业的需求进行一些介绍。在最后，文章对物联网安全可以切入的点，以及可以深入研究的点，进行总结和思考。

一．引言

消费行业的市场处于物联网普及的开端，可穿戴设备、智能家庭产品、照明设备和其他的智能设备正在成为主流。商业和公共部门对于物联网的采用在消费市场之后，Verizon 在 2015 年的物联网报告中预测 2011 年到 2020 年之间的企业对企业（Business-to-Business，B2B）的物联网连接每年将以 28% 的速度增长。工业，如制造型、能源、交通和零售已经采用了物联网 initiatives。埃森哲在其 2015 年的工业物联网市场定位报告中预测，到 2030 年，单纯美国的工业物联网将价值 7.1 万亿美元，将支持效率、安全、生产力和 service provisioning 的增强。

全球的多个城市也正在采用物联网，依赖于从数以千计的按地理位置分布的不同类型的传感器捕获的数据，它们正在往智慧城市的道路上发展。在医疗行业，我们可以看到制造商已经开始在设备中加入网络连接性和智能以探索物联网的应用，例如患者床边设备。我们同样可以看到个人和商业之间的物联网能力的互联性正在开始，智能穿戴设备很快就可以搜集数据，然后将其传输给云中的医疗服务提供商。交通行业是另一个令人振奋的行业，车联网已经萌芽，随着无人驾驶汽车的实验，基于物联网的路边设备对于传感数据的收集和分析的能力将变得越来越重要。在能源行业，集成和互联的系统（如现代变电站综合系统、智能电网系统）趋于增加系统的自动

化和远程访问能力，以在近乎实时的情况下向大范围的用户传输信息以及控制相关的多个任务，以求精简运作和性能。

本章选取了五家公司，在介绍公司产品的同时，也会对其所关注的行业的需求进行一个介绍。赛门铁克提出了一个通用的物联网安全架构。CUJO 是一家智能家庭领域的安全公司，其主打产品为智能防火墙，在智能设备在家庭中日益普及的今天，以智能防火墙作为切入点非常值得关注。Vidder 的技术基础是软件定义边界（Software Defined Perimeter，SDP），其借助于软件定义网络的思想来做访问控制，实现了认证与实际数据访问的分离。NexDefense 是一家工控安全领域的公司，其主打产品 Sophia 是一个工业网络异常检测系统。Intel 发布了关于解决下一代汽车安全和隐私问题的汽车安全最佳实践的白皮书，提出了一种三层纵深汽车安全防御体系。

二．物联网安全公司及其产品介绍

2.1 赛门铁克

由于物联网设备的资源受限，因此并不完全支持传统的安全解决方案。赛门铁克 将物联网安全分为四个部分：通信保护、设备保护、设备管理和理解当前的系统。这几个部分可以结合起来组成一个功能强大的、易于部署的安全架构来移除物联网中的大部分的安全威胁，如 APT 和复杂的威胁。白皮书 “An Internet of Things Reference Architecture” 中对这四部分进行了介绍。

通信保护需要对于设备和远程系统之间的通信进行加密和认证，作为认证机构（CA）的领导者，赛门铁克已经在十亿以上的物联网设备中嵌入了设备证书密钥。

设备保护需要对代码签名以确保所有运行的代码都是经过认证的，以及在运行时防护。运行时防护可以通过基于主机的保护（Host based protections）方法。

设备管理需要提供设备固件安全升级的方法，通常可将 over-the air（OTA）内置在设备中。

理解当前的系统需要对系统进行安全分析以检测出系统中的异常行为。很多已经运行的系统不能轻易被取代，对系统的检测和分析可以作为临时的解决方案进行部署。

下图是赛门铁克对于 PC 时代和物联网时代的安全做法的对比。

图 4.1 赛门铁克对于 PC 时代和物联网时代的安全做法对比

赛门铁克 在工控系统安全方面主要有两类解决方案，一是针对操作者如何保护工厂和基础设施的安全，二是针对设备供应商如何在其产品中增加安全性。

赛门铁克利用分析技术和机器学习对 ICS 网络建模以使用户理解自己的网络，从而检测高级威胁。

Symantec Embedded Security: Critical System Protection（SES CSP）是一个轻量级的安全客户端，通过保护终端和嵌入式设备来保护物联网安全。它在不影响设备性能的情况下向制造商和资产所有者提供 embedded systems robust signatureless, host-based protection in managed and unmanaged scenarios。由于是基于策略的防护，SES CSP 不需要像杀毒软件那样进行安全内容更新。

赛门铁克对汽车安全领域的分析沿用了上文提出的安全框架，同样分为四部分：

(1) 保护所有通信

(2) 保护各传感器，执行器，微控制器（MCU），以及微处理器

(3) 安全和有效地管理整个车辆通过空中下载（OTA）

(4) 减轻高级威胁

图 4.2 汽车安全需要注意的四个点

赛门铁克 嵌入式安全：保护关键系统，保护关键单元和大多数汽车的 IVI 系统。保护 OBD-II 接口设备，包括经销商的诊断设备和 UBI 加密狗。设备认证嵌入式安全证书可以用来认证数据。赛门铁克代码签名证书目前支持全系列代码签名的，包括安全启动签名代码。

嵌入式汽车安全分析用来监测 CAN 总线或 FlexRay 总线。这个软件可轻松部署到单板计算机中，包括用于 IVI 的 SBS。为汽车安全启动设计的代码签名，由赛门铁克全球领先的备份证书机构（CA）和代码签名基础设施支持。嵌入式软件保护同样建立在我们的代码签名证书和 CA 服务的基础上，但是做的并不只是代码签名。在签名之前，嵌入式模糊处理和其他形式保护直接进入代码，使汽车制造商代码可以自己保护自己，甚至在有限的 MCU，例如几十年的老 8 位和 16 位器件。全球物联网安全性分析，从数以百万计的汽车中收集数据进行分析，以抵抗高级威胁。总之，不管你们如何保护每个模块，无论做的多么好，你总是需要一个监测和分析框架，以检测最先进的威胁。

赛门铁克嵌入式安全: 关键系统防护，可配置在许多这些模块中，加强良好代码的白名单，确保它们只能执行提前批准的代码，并控制这些代码的行为。使用白名单和沙盒作为最小特权保护战略的一部分，只允许已知的代码执行已知的功能。赛门铁克公司嵌入式安全: 关键系统保护不仅直接监视应用程序的行为，而且也监视文件，设置，事件和日志，并报告异常行为。特点包括复杂的基于策略的审核和监控；日志整合，便于搜索；先进的事件分析和反应能力。

2.2 CUJO

智能家居（smart home, home automation）是以住宅为平台，利用综合布线技术、网络通信技术、安全防范技术、自动控制技术、音视频技术将家居生活有关的设施集成，构建高效的住宅设施与家庭日程事务的管理系统，提升家居安全性、便利性、舒适性、艺术性，

并实现环保节能的居住环境。但是“便利”向来是把双刃剑，在物联网中传输的数据越多，信息暴露的可能性就越大，存在的安全隐患也因此而剧增。

在智能家庭中，一个很流行的应用是 Nest 公司的智能恒温器，该设备可以控制家庭的温度。但是，由于设备搜集家庭中的人的信息，因此，智能恒温器知道家中什么时候有人，他们的日程安排是什么，他们什么时候起床、什么时候睡觉，他们偏好于多少温度。

许多智能电视带有摄像头，即便电视没有打开，入侵智能电视的攻击者可以使用摄像头来监视你和你的家人。由于缺乏安全标准，攻击者甚至会锁定电视从而达到勒索的目的。

许多智能家庭的用户将车库开门器、门锁、摄像头等安防系统连接到网络上，通过手机 APP 可对其进行控制。攻击者一旦攻破这样的系统很明显会带来问题。比如攻击者在你去度假的时候打开房门，或者在午夜打开车库门等等。

攻击者在获取对于智能家庭中的灯光系统的访问后，除了控制家庭中的灯光外，还可以访问家庭的电力，从而可以增加家庭的电力消耗，导致极大的电费账单。

CUJO 是一个智能防火墙，可以使连接到家庭网络的设备远离网络威胁。CUJO 在本地采样网络流量数据，然后发送元数据到云端用于分析。出于保护用户隐私，并没有发送全部的文件和内容到云端。如果检测到威胁或者受怀疑的活动，CUJO 会下发锁定命令（issue a block），在移动 APP 上也会收到相应的通知。

CUJO 扮演用户设备和与它们相连的网络之间的网关的角色，将数据包头发送到云中用于设备行为分析，通过将流量信息与商业威胁情报源进行对比，以确保未授权的 IP 并没有连接到用户的网络中。

图 4.3 CUJO 与其它产品功能对比

移动 APP 的功能有：

（1）控制和监测用户网络中的所有设备

（2）实时接收威胁通知

（3）控制选定设备的网络访问

2.3 Vidder

Cryptzone 通过问卷调研，对于企业网络访问安全有三个发现：

（1）很多企业使用的是过时的方法，在旧的网络安全模型下，缺乏对于限制授权用户和第三方的访问的解决方案。

（2）大部分的信息安全方面的破坏来自于内部威胁（insider threats）。

（3）一些公司并没有经常回顾访问策略，有的甚至已经几年没有这么做了。当策略制定好后，它们不会或者不去自动实施这些安全策略。

因此，我们需要一个新的安全模型，这个模型可以理解上下文信息，如用户位置，用户使用什么设备来建立连接的，何时建立连接的，以及用户的角色。这些信息可以集成到特定上下文的访问规则中，基于上下文参数的认证检查和对于资源的访问能够提供对于边界内部和外部的威胁的更好的防护。

对于用户的访问控制并不仅仅是在用户访问网络之前对于用户的认证，安全的一个基本方法就是要意识到任何人都可以声称他 / 她是某个人。

Vidder 公司的产品为 PrecisionAccess。PrecisionAccess 使得用户和不同公司、组织、控制区域的应用进行安全连接。PrecisionAccess 基于 SDP。PrecisionAccess 基于预认证（pre-authentication）建立连通性。预认证的意思是在提供应用的可见性和连通性之前首先验证用户的可信和权限。它通过三种方式对抗基于网络的攻击：透明 MFA 可以抵抗证书丢失，服务器隔离可以抵抗服务器利用，TLS 双向认证可以抵抗连接劫持。

PrecisionAccess 的架构如下图所示，由三个组件组成，PA 控制器、PA 网关和 PA 客户端。PA 控制器决定了哪些 PA 客户端可以互相连接。控制器有可能将信息转发到外部的认证服务，比如证实、地理定位、身份服务器等。PA 客户端与 PA 控制器进行通信来请求可连接的主机列表。控制器可以在提供信息之前向 PA 网关之内的主机请求信息，如软硬件清单。初始时，PA 网关之内的主机只与 PA 控制器进行通信，只在控制器的请求下与 PA 客户端建立连接。

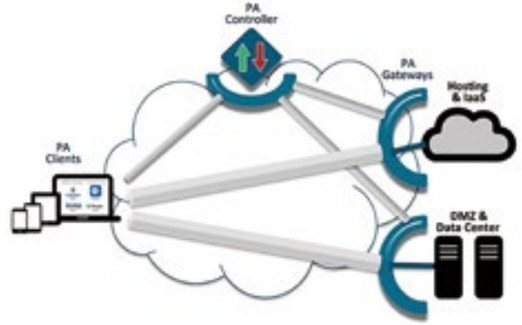


图 4.4 Vidder 架构图

2.4 NexDefense

针对工业控制系统的攻击将导致严重的后果。2010 年 6 月，伊朗布什尔核电站遭到“震网”病毒攻击，1/5 的离心机报废。2014 年，德国的一个钢铁厂，遭受到高级持续性威胁（APT）攻击，攻击者的行为导致工控系统的控制组件和整个生产线被迫停止运转，由于不是正常的关闭炼钢炉，从而给钢厂带来了重大破坏。2014 年，仅仅在美国就发生了 245 起攻击事件。2015 年 12 月，乌克兰电网系统遭受黑客攻击，数百户家庭供电被迫中断。

工业 4.0 驱动制造业、过程控制、基础设施、其他工业控制系统的连通性，对于这些系统的威胁不断上升。

NexDefense 建于 2012 年，致力于实时保护关键基础设施中的系统的完整性，打击复杂的安全威胁。Sophia 是该公司提供的商用安全软件，保持对于威胁的持续洞察和控制，使安全专业人员在不牺牲效率、性能的情况下增加合规性，它能够增加关键基础设施中的工业控制系统的安全性和可靠性。

面向领域：电力、油气、国防。

Sophia 是一个工业网络异常检测系统，由美国能源部、Battelle Energy Alliance 和 Idaho National Laboratory（INL）的网络安全专家协作完成。最初应用于能源和国防组织，用于评估实时威胁和应急协议。它致力于寻找可以降低风险、减少责任（reduce liabilities）和确保自动化和控制系统的完整性的最佳方法和工具。

它可以检测到正常的自动化操作和系统控制操作中的偏差，然后提供预警。Sophia 跟踪网络中的所有设备，知道什么状态是正常的，什么状态是不正常的，对不正常的通信进行报警。

通过对 packet level 数据包级别的监测，来检测网络通信的改变，并对这些改变进行报警。可以提供相应的数据来帮助用户做决定，从而增加 ICS/SCADA 的安全性和可靠性。

它的特点有：

（1）被动（没有对于 ICS/SCADA 的扫描和数据发送）、在线、综合实时通信分析。

（2）在生产环境中可安全使用。

（3）用户在一两天内即可精通。

（4）网络流量 3D 可视化。

（5）对于不在白名单中的非正常 ICS/SCADA 操作进行检测和报警。

（6）支持线下分析。

（7）适用于新的或遗留系统。

（8）支持第三方的离线分析。

2.5 Intel

随着车联网的普及，汽车上的无线技术使用也越来越多，在给人们的生活带来便利的同时，也带来了很多的安全问题。2015 年爆出黑客可以利用美国通用公司 OnStar 系统的漏洞来远程操纵汽车。可见智能汽车安全问题应该得到我们的高度重视。

现代汽车通信与以往有很大不同，目前出现了三种汽车通信方式：

（1）Car-to-Car Communication（V2C）汽车与汽车之间。汽车之间交互信息，相互提醒路上的障碍物或者其它危害。

（2）Car-to-Infrastructure Communication（V2I），汽车和基础设施之间通过无线进行通信，例如交通信号，各种网络节点。

（3）Car-to-X Communication（V2X），汽车和任意物体之间。泛指任意的信息交换，例如汽车与移动电话，或者互联网应用和云服务。

如此广泛的交流方法意味着黑客可利用的方面非常多，因为任何暴漏在网络中的节点都可能遭受到攻击，或者通过被攻击的节点去连接其他的节点。

另一个问题就是汽车平均十几年的时间才换一次，这导致了行驶在道路上的车辆可能有不同的系统和不同的安全等级，相互通信的组件之间也可能会有不同的安全等级，并且对车辆系统和组件之间宽的兼容性的要求可能会增加新的可以利用的点。一个旧的不安全的智能手机连接到一个新的汽车中可能会导致汽车受到攻击。

同时攻击者也可以通过无线的方式利用汽车中的娱乐信息系统，可以侵入“CAN 总线”，向其他设备发送指令。

总结来说，攻击者攻击一辆汽车，要迈过两道重要的“关卡”：

（1）攻破 Wi-Fi 或蜂窝网络进入汽车系统内部；

（2）绕过系统内部的验证机制，对重要设备的发送指令。

Intel 发布了关于解决下一代汽车安全和隐私问题的汽车安全最佳实践的白皮书，文章中提出了一种三层纵深汽车安全防御体系，将在本小节中作重点介绍。

Intel 白皮书中指出：下一代车辆会使用的系统有：

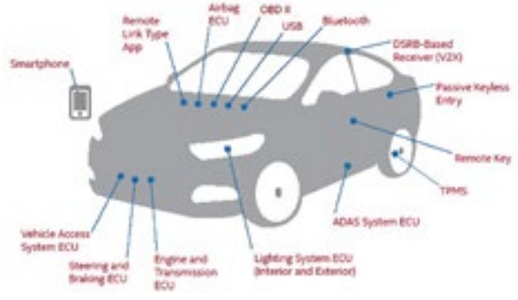


图 4.5 汽车可能被攻击的几个点

（1）Advanced driver assistant systems（ADAS）。智能照明控制、自适应巡航控制、车道偏离警示系统和提车辅助。

（2）Advanced fleet management（车队管理）。实时远程信息处理（车联网），司机疲劳驾驶检测和包裹跟踪

（3）Smart transportation。（Vehicle-to-infrastructure） 车辆和基础设施通信。例如交通灯控制，避免碰撞等。

（4）Autonomous driving 自动驾驶。实现无人驾驶车辆的零事故死亡率或者撞车率。指出了下一代车辆最可能被攻击的几个点：

Intel 提出的安全纵深防御由三层组成 硬件安全模块、硬件安全服务和软件安全服务，如图 4.5 所示。

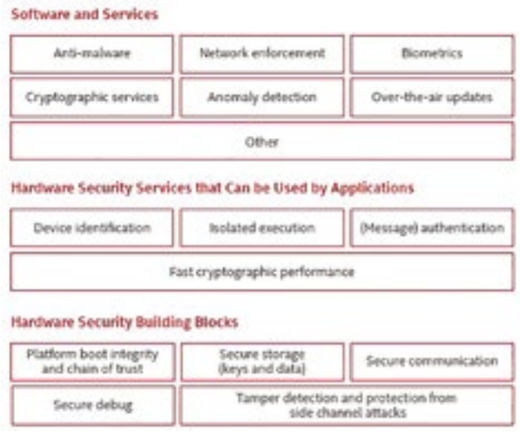


图 4.6 汽车安全纵深防御架构

硬件安全保护：它的主要职责是安全启动，将环境带到可信赖的初始环境状态，安全存储和一个受信任的执行环境。

硬件安全服务：基于硬件安全建造，并提供快速加密性能、永恒不变的设备标识、消息验证和执行隔离。

软件安全服务：在硬件的基础上通过入侵检测和保护服务（IDPS）、防火墙、黑名单 / 白名单。恶意软件检测、加密服务、生物特征识别，over-the-air 更新和其他功能加强安全性。

下面会简要介绍各个层次的主要技术。

（1）硬件安全

硬件安全系统就像汽车的物理保护系统一样，它可以保护汽车的操作组件免受意外或者故意损害。在计算机安全产业有很多硬件安全技术可以用来保护 ECUs 和总线的安全，这些措施包括：

安全启动和软件证明功能：通过检查数字签名和产品秘钥来检测引导加载程序和关键操作系统是否被篡改。不合法的文件将不能运行。

可信执行技术：如可信任的处理器模块：使用密码技术来为每个被批准组件产生唯一标识符，将启动环境中的成分与一个已知的好的代码进行比较，如果代码不匹配则不允许执行。

篡改保护：加密的加密密钥，知识产权，帐户凭证，在编译时其他有价值的信息，并在一个小的执行窗口中解密，防止逆向工程并对消息进行监测，防止消息篡改。

加密加速：优化硬件减少加密工作负载，提高加密性能，并使对称或公钥加密更容易地广泛地应用到应用程序和通信中

主动内存保护：通过在硬件中嵌入 pointerchecking 减少代码漏洞，来防止缓冲区溢出等情况。

设备标识直接在设备上：使制造商能够知道唯一确定每个设备的身份，确保安全识别和防止未经批准的设备访问该制造商的网络或系统。这种技术，集成到芯片，也可以加密身份标识保持匿名。

（2）软件安全

汽车网络和控制单元在硬件架构上被隔离保护，使它们很难受到攻击，但攻击者只要花费足够的时间和金钱依然可以闯入这些系统中。此外更多的 ECUs 通过常规协议连接起来增加了汽车可攻击的点。而且在 ECUs 中增加硬件安全能力是很困难的，所以我们需要基于软件的安全保护措施，保护汽车软件技术包括：

安全启动：与硬件协作，以确保加载的软件组件是有效的，以为其他系统提供信任根。

虚拟化：常用的软件和硬件的结合，使得它可以为单一的 ECU 创建一个防御屏障，分隔面向外部的功能和那些驱动车辆的功能，减少了巩固多个系统到一个单一的 ECU 的复杂性。

软件容器：用于单独系统和应用程序隔离，使之更新或替换单独的功能时，不会影响整体操作或镜像功能，从而实现快速故障转移。

认证：通过一个物理钥匙解锁车门并发动汽车不再是足够的，并正在通过软件增强认证能力，因为汽车提供跨越多种功能和配置文件的个性化服务。汽车需要电子密钥，密码和生物识别来管理和授权访问的个人信息，

允许正确的行为：黑客从一个系统跳到另一个系统或者从一个被

俘获的组件发送信息给一个正常的组件是很常见的。防止这种网络活动是检测和纠正意外或者恶意威胁的关键。

（3）网络安全：

车联网中传输了很多操作和个人信息，包括：位置，导航历史记录，麦克风录音等，为了保护操作安全和用户隐私，保护通信过程中的信息和数据安全十分重要。保护通信的措施主要有：

消息验证：验证消息从被批准的发送源中发送过来，以防欺骗或者重放攻击。

所有系统行为的可预测性：根据预先定义好的征程行为限制网络通信，限制不正常的行为。

防火墙：明确只允许预先批准的系统和传感器之间通信和传递消息，未经批准的和不恰当的信息会被限制，并将这次不合法的尝试发送给安全系统。

（4）云安全服务

车辆安全性是必不可少的，有些额外的安全服务要求实时更新，因此系统需要能够连接到基于云的安全服务，以便于能够及时检测和预防威胁。

与云的安全认证通道：在远程控制，软件更新和其通信过程中，利用硬件辅助的加密实现数数据保护。

车辆活动的远程监控：包括适当的隐私约束以帮助检测异常行为，发现行为异常的车辆，过滤和删除恶意软件。

威胁情报交换：汽车的经销商、制造商甚至政府机构能够合作起来，能够快速将零日漏洞（zero-day exploit）和恶意软件通知相应的车辆。

OTA: 当发现漏洞的时候，可以更新系统，大幅度降低召回成本。

证书管理：联网的车辆组件、车主和司机认证，为用户的配置文件和账户提供安全管理，身份证明以及相关联的加密密钥和服务。证书的安全性是数据隐私的关键。

（5）供应链风险管理

为了保持安全架构的可信和完整性，检测和避免零部件被渗透和污染十分重要，必须要防止攻击者物理地访问车内的硬件。已知的保护供应链的最佳实践包括：

授权分销渠道：用于采购的用来建造和维护车辆的所有硬件和软件。

追踪记录：检测在安全系统中的所有重要部件。

持续的备件和维修部件的供应计划：包括一个长期的部件可用性策略。

（6）数据隐私和匿名。

数据隐私有两个方面　个人数据的机密性和不在用户控制范围内的数据泄露。为了保证数据的机密性，数据在车内或者车外存储和传输的时候都需要进行加密处理。对于数据泄露，需要方法防止非法访问。

其它公司所做的工作，大多在这三层体系中得以体现，如：

（1）Argus

该公司提供了一个独特的入侵检测和预防系统（IDPS），利用正

在申请专利的深度包检测算法识别恶意攻击，扫描所有车载网中的流量，识别不正常的传输，并且实时对威胁做出回应。同时为管理员们提供一个综合性的网络攻击和不合法的行为的概览，使原始设备制造商识别非授权的对 ECU（电子控制单元）调整和改变行为。

因为威胁是动态的，Argus 研究团队持续更新系统，利用 Argus 安全云服务实时通过 Over-The-Air 更新系统。

这种防御方式属于三层中的软件安全服务层，通过入侵检测和保护服务（IDPS）来增强系统安全性。

（2）Karamba

该公司指出完成一个成功的攻击，黑客首先需要找到一种方式进入汽车的控制器局域网（CAN 总线）。虽然有连接到 CAN 总线有过百的 ECU，只有少数有外部通信接口。这些的 ECU 是进入车内入口。检测、并在这些入口处阻止攻击者，那么攻击者渗透到汽车的网络，并破坏汽车的安全操作的风险会显著减少。

Karamba 与系统供应商合作，为每个 ECU 定义出厂设置，生成所有 ECU 允许的程序二进制、程序、脚本、网络行为等的白名单，这一政策被嵌入外部连接的 ECU 内，以确保只有明确允许的策略代码和行为会在其上运行。

该防御方法属于硬件安全服务层，将产品集成在硬件中，提供安全服务，增强系统的安全性。

三．总结及思考

通过前几章的介绍，我们可以了解到：物联网覆盖的范围较为广泛，物联网安全问题所需要关注的方面也非常多，不仅包含传统网络安全问题，还存在着一些物联网特有的安全问题。

本章中我们总结出了物联网安全研究可以切入的三个领域：工业控制、智能汽车和智能家居，然后又列出了六点需要重点关注的方面，公司可以从这些点作为物联网安全研究的切入点。

3.1 物联网安全可以作为切入点的领域

（1）工控安全

针对工业控制系统的攻击将导致严重的后果。工业 4.0 驱动制造业、过程控制、基础设施、其他工业控制系统的连通性，对于这些系统的威胁不断上升。

（2）智能汽车安全

随着特斯拉汽车的推出，以及苹果、谷歌等互联网巨头新的智能汽车系统的成熟，车联网正在从概念变为现实，但是智能汽车一旦遭受黑客攻击，发生安全问题，可能会造成严重的交通事故，威胁人们的生命安全。

（3）智能家居安全

随着物联网技术的迅速发展，智能家居概念颇为火热，但是如果黑客能轻松的利用网络攻破一些智能家用产品的安全防线，如：黑客侵占智能设备（恒温控制器、智能 TV、摄像头），可以获取用户隐私信息，带来安全隐患。

3.2 物联网安全研究点

基于调研，我们总结了物联网安全的六个关注点：

（1）物联网安全网关

物联网设备缺乏认证和授权标准，有些甚至没有相关设计，对于连接到公网的设备，这将导致可通过公网直接对其进行访问。另外，也很难保证设备的认证和授权实现没有问题，所有设备都进行完备的认证未必现实（设备的功耗等），可考虑额外加一层认证环节，只有认证通过，才能够对其进行访问。结合大数据分析提供自适应访问控制。

对于智能家居内部设备（如摄像头）的访问，可将访问视为申请，由网关记录并通知网关 APP，由用户在网关 APP 端进行访问授权。

未来物联网网关可以发展成富应用平台，就像当下的手机一样。一是对于用户体验和交互性来说拥有本地接口和数据存储是非常有用的，二是即使与互联网的连接中断，这些应用也需要持续工作。物理网关对于嵌入式设备可以提供有用的安全保护。低功耗操作和受限的软件支持意味着频繁的固件更新代价太高甚至不可能实现。反而，网关可以主动更新软件（高级防火墙）以保护嵌入式设备免受攻击。实现这些特性需要重新思考运行在网关上的操作系统和其机制。

软件定义边界可以被用来隐藏服务器和服务器与设备的交互，从而最大化地保障安全和运行时间。

细粒度访问控制：研究基于属性的访问控制模型，使设备根据其属性按需细粒度访问内部网络的资源；

自适应访问控制：研究安全设备按需编排模型，对于设备的异常行为进行安全防护，限制恶意用户对于物联网设备的访问。

同时，安全网关还可与云端通信，实现对于设备的 OTA 升级，可以定期对内网设备状态进行检测，并将检测结果上传到云端进行分析等等。

但是，也应意识到安全网关的局限性，安全网关更适用于对于固定场所中外部与内部连接之间的防护，如家庭、企业等，对于一些需要移动的设备的安全，如智能手环等，或者内部使用无线通信的环境，则可能需要使用其他的方式来解决。

（2）应用层的物联网安全服务

应用层的物联网安全服务主要包含两个方面，一是大数据分析驱动的安全，二是对于已有的安全能力的集成。

由于感知层的设备性能所限，并不具备分析海量数据的能力，也不具备关联多种数据发现异常的能力，一种自然的思路是在感知层与网络层的连接处提供一个安全网关，安全网关负责采集数据，

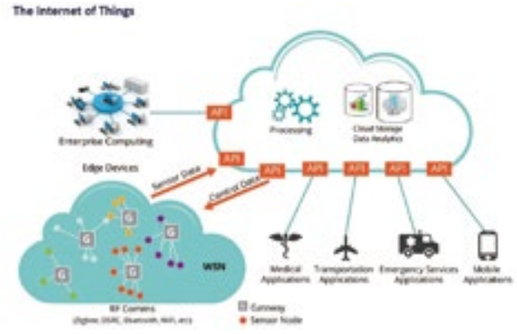


图 5.1 利用云端进行大数据分析

如流量数据、设备状态等等，这些数据上传到应用层，利用应用层的数据分析能力进行分析，根据分析结果，下发相应指令。

传统的 Web 安全中的安全能力，如 URL 信誉服务、IP 信誉服务等等，同样可以集成到物联网环境中，可作为安全服务模块，由用户自行选择。

（3）漏洞挖掘研究

物联网漏洞挖掘主要关注两个方面，一个是网络协议的漏洞挖掘，一个是嵌入式操作系统的漏洞挖掘。分别对应网络层和感知层，应用层大多采用云平台，属于云安全的范畴，可应用已有的云安全防护措施。

在现代的汽车、工控等物联网行业，各种网络协议被广泛使用，这些网络协议带来了大量的安全问题。需要利用一些漏洞挖掘技术对物联网中的协议进行漏洞挖掘，先于攻击者发现并及时修补漏洞，有效减少来自黑客的威胁，提升系统的安全性。

物联网设备多使用嵌入式操作系统，如果这些嵌入式操作系统遭受了攻击，将会对整个设备造成很大的影响。对嵌入式操作系统的漏洞挖掘也是一个重要的物联网安全研究方向。

（4）物联网僵尸网络研究

今年最为有名的物联网僵尸网络便是 Mirai 了，它通过感染网络摄像头等物联网设备进行传播，可发动大规模的 DDoS 攻击，它对 Brian Krebs 个人网站和法国网络服务商 OVH 发动 DDoS 攻击，对于美国 Dyn 公司的攻击 Mirai 也贡献了部分流量。

对于物联网僵尸网络的研究包括传播机理、检测、防护和清除方法。

（5）区块链技术

区块链解决的核心问题是在信息不对称、不确定的环境下，如何建立满足经济活动赖以发生、发展的“信任”生态体系。

在物联网环境中，所有日常家居物件都能自发、自动地与其它物件、或外界世界进行互动，但是必须解决物联网设备之间的信任问题。

传统的中心化系统中，信任机制比较容易建立，存在一个可信的第三方来管理所有的设备的身份信息。但是物联网环境中设备众多，未来可能会达到百亿级别，这会对可信第三方造成很大的压力。

区块链系统网络是典型的 P2P 网络，具有分布式异构特征，而物联网天然具备分布式特征，网中的每一个设备都能管理自己在交互作用中的角色、行为和规则，对建立区块链系统的共识机制具有重要的支持作用。

（6）物联网设备安全设计

物联网设备制造商并没有很强的安全背景，也缺乏标准来说明一个产品是否是安全的。很多安全问题来自于不安全的设计。信息安全厂商可以做三点：一是提供安全的开发规范，进行安全开发培训，指导物联网领域的开发人员进行安全开发，提高产品的安全性；二是将安全模块内置于物联网产品中，比如工控领域对于实时性的要求很高，而且一旦部署可能很多年都不会对其进行替换，这是的安全可能更偏重于安全评估和检测，如果将安全模块融入设备的制造过程，将能显著降低安全模块的开销，对设备提供更好的安全防护；三是对出厂设备进行安全检测，及时发现设备中的漏洞并协助厂商进行修复。

打磨渗透测试人员的利器Kali Linux

华东服务交付部　张百通

关键词：kali linux、办公软件集成、安全服务人员、渗透测试服务

摘要：Kali Linux 是基于 Debian 的 Linux 发行版，专用于数字取证和渗透测试。在其中选择安装一些办公和常用的渗透测试软件，就能形成渗透测试人员的工作利器。本文既是介绍一些安装和调试方法。

前言

为什么要选择 Kali Linux？Kali Linux 是基于 Debian 的 Linux 发行版，设计用于数字取证和渗透测试。由 Offensive Security Ltd 维护和资助。最先由 Offensive Security 的 Mati Aharoni 和 Devon Kearns 通过重写 BackTrack 来完成，BackTrack 是之前写的用于取证的 Linux 发行版 。

Kali Linux 预装了许多渗透测试软件，包括 nmap（端口扫描器）、Wireshark（数据包分析器）、John the Ripper（密码破解器），以及 Aircrack-ng（一应用于对无线局域网进行渗透测试的软件）。另外，Metasploit 的 Metasploit Framework 也支持 Kali Linux。Kali Linux 是一个很容易上手的系统，有助于渗透测试人员熟悉业务并扩展知识面，在硬盘、live CD 或 live USB 上都可以运行 Kali Linux。

Kali Linux 2016.2 为 kali 的滚动版，更新更快，linux 内核版本高，对 Lenovo ThinkPad x260 兼容性好，作为集成安全工具的 linux 系统，有时一句命令能测试一个漏洞，效率极高，在其中选择集成一些办公和常用的渗透测试软件，就能形成渗透测试人员的工作利器。

一．软件集成安装与使用

1.1 必备软件罗列

1. 操作系统：Kali Linux 2016.2

2. 谷歌浏览器：虽然 kali2016.2 已经把 firefox 集成在系统里，谷歌浏览器特点速度快，效率很重要。

3.Flash：看视频必备，谷歌浏览器自带 flash，firefox 没有。

4. 虚拟机：装环境必备。

5.office|WPS：写文档必备。

6. 谷歌 | 搜狗输入法：打字必备。

7. 截图工具 shutter：办公过程需要截图的必备。

8.vpn：PPTP 可拨号进公司 vpn。

9. 邮件 evolution：收发邮件必备。

10. 加密 cryptsetup：加密文件或硬盘

1.2 准备工作

1.2.1 更新源

root@kali:~# leafpad /etc/apt/sources.list，然后将以下源复制进去保存。

阿里云 kali 源

deb http://mirrors.aliyun.com/kali kali-rolling main non-free contrib

deb-src http://mirrors.aliyun.com/kali kali-rolling main non-free contrib

deb http://mirrors.aliyun.com/kali-security kali-rolling/updates main contrib non-free

deb-src http://mirrors.aliyun.com/kali-security kali-rolling/updates main contrib non-free

中科大 kali 源

deb http://mirrors.ustc.edu.cn/kali kali-rolling main non-free contrib

deb-src http://mirrors.ustc.edu.cn/kali kali-rolling main non-free contrib

deb http://mirrors.ustc.edu.cn/kali-security kali-current/updates main contrib non-free

deb-src http://mirrors.ustc.edu.cn/kali-security kali-current/updates main contrib non-free

官方源可自行添加，不过速度比较慢，有可能会造成软件下载失败的问题。

然后更新并安装

root@kali:~# apt-get update && apt-get dist-upgrade

1.2.2 安装内核头（装显卡驱动或者虚拟机增强工具会用到）

root@kali:apt-get install linux-headers-$(uname -r)

注：如果返回错误，可以尝试输入如下命令

aptitude -r install linux-headers-$(uname -r)

1.3 安装必备软件

1.3.1 谷歌浏览器

从官网上下载谷歌浏览器 deb 包，然

图 1 google 浏览器开启命令

后到下载目录安装下，root@kali:dpkg -i google-chrome-stable（具体以实际包的名称为准）。安装完后，执行命令 google-chrome %U --no-sandbox -user-data-dir=chrome 才能运行，该命令是创建一个用户目录，如果没有用户目录，则无法运行。

1.3.2 flash

首先执行，root@kali:apt-get install flashplugin-nonfree

其次执行，root@kali:update-flashplugin-nonfree –install

1.3.3 虚拟机

首先到 VM 官网下载包

https://download3.vmware.com/software/wkst/file/VMware-XXX.bundle

然后赋予修改权限

chmod u+x VMware-Workstation-Full-10.0.2-1744117.i386.bundle

./Mware-Workstation-Full-10.0.2-1744117.i386.bundle

注意：如果 ./vmware 提示 before run vmware xxxxxxxxxxxx

出现这样的问题，就是没有安装对应内核的开发包，在上面的准备工作中有提到。解决方案是使用如下命令：

cd /usr/lib/vmware/modules/source/

tar xf vmmon.tar

mv vmmon.tar vmmon.old.tar

sed -i -e 's/get_user_pages/get_user_pages_remote/g' vmmon-only/linux/hostif.c

tar cf vmmon.tar vmmon-only

rm -r vmmon-only

tar xf vmnet.tar

mv vmnet.tar vmnet.old.tar

sed -i -e 's/get_user_pages/get_user_pages_remote/g' vmnet-only/userif.c

tar cf vmnet.tar vmnet-only

rm -r vmnet-only

大概意思是改了虚拟接口文件的路径，安装成功。执行卸载 vm 命令，方便没配置成功的卸载完再装。

vmware-installer --uninstall-product vmware-workstation

1.3.4 安装 WPS

从 Linux 下可以找到两个办公软件，openoffice 和 WPS。这里选择安装了 WPS。

首选官网下载 deb 包：http://community.wps.cn/download/

其次对应下载位置 dpkg -i 安装下即可。

1.3.5 谷歌 | 搜狗输入法

Kali 自带是不能输入中文的，需要自行安装，这里安装了搜狗输入法和谷歌输入法，具体的使用，看个人习惯了。

apt-get install fcitx

apt-get install fcitx-googlepinyin // 安装谷歌拼音

搜狗打字去官网下载 deb，然后执行如下命令

dpkg -i 安装对应搜狗包 // 安装搜狗拼音

安装好任意输入法需要重启下才能正常打字（ctrl+ 空格）

1.3.6 截图工具 shutter

执行命令 apt-get install shutter

然后配置 ctrl+a 快捷键 命令 shutter -s 开启截图，功能还是很多很方便的，和 QQ 的截图功能差不多。

1.3.7 vpn

默认安装，是没有激活 VPN 的，虽然能看到 VPN 选项，但是不能点击 VPN 连接，需要先执行如下命令

apt-get install -y pptpd network-manager-openvpn network-manager-openvpn-gnome network-manager-pptp network-manager-pptp-gnome network-manager-strongswan network-manager-vpnc network-manager-vpnc-gnome

然后进行 pptp 的配置，就可以拨入 vpn 了。

1.3.8 邮件 evolution

需要执行命令 apt-get install evolution，配置请参照 http://os.51cto.com/art/197001/245284.htm

这里需要注意，发送外网邮件的密码是不一样的，需通过抓包然后 base64 解码才能用！！！

1.3.9 加密 cryptsetup

可以采取如下步骤，对文件进行加密

1、利用文件生成命令生成一个 5G 的文件：

fallocate -l 5G /root/luks.vol

2、对文件进行加密：

ryptsetup --cipher aes-xts-plain64 --key-size 512 --hash sha512 --iter-time 10000 luksFormat /root/luks.vol

3、打开上述的文件容器，xxx 为映射名:

cryptsetup luksOpen /root/luks.vol xxx

4、虚拟磁盘会被映射到 /dev/mapper/xxx

ls /dev/mapper/

5、格式化创建文件系统：

mkfs.ext4 /dev/mapper/xxx

6、挂载文件系统：

mkdir /mnt/xxx

ount /dev/mapper/xxx /mnt/xxx

7、利用 df -hT 就可以看到刚刚挂载的系统了。

1.4 注意事项

如果安装 deb 过程中出现安装失败的情况，很可能就是缺少依赖包，使用 apt-get install -f 试试，会下载相应的依赖包，如遇到网络原因或者源的原因 deb 包无法下载，手动下载 deb 包，然后使用 dpkg -i 安装相应的依赖包。

二．善后

2.1 系统备份

tar cvpzf backup.tgz --exclude=/proc --exclude=/lost+found --exclude=/backup.tgz --exclude=/mnt --exclude=/sys --exclude=/media /

2.2 快捷键

配置快捷键提高工作效率，如：系统》设置》快捷键，可以添加命令，gnome-terminal，然后输入自己习惯的快捷键，我输入的是 CTRL+ALT+T

参考网站：

http://www.freebuf.com/sectool/95167.html

https://communities.vmware.com/thread/536705?start=0&tstart=0

https://program-think.blogspot.com/2015/10/dm-crypt-cryptsetup.html

面对勒索软件的汹汹攻势，你准备好了吗？

ESD产品管理团队 刘弘利

关键词：勒索软件 高级持续性威胁 APT 勒索软件检测防御

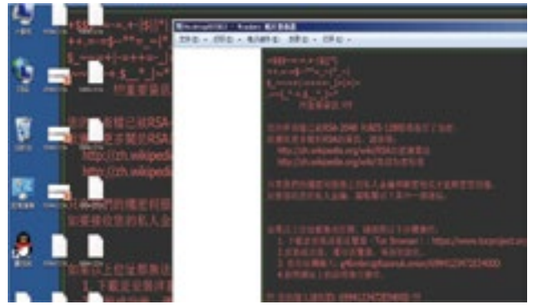
摘要：勒索软件是近年来增长快速的重大威胁。本文通过分析勒索软件的攻击方式、危害、发展趋势，探讨如何应对日益增多勒索软件威胁，重点介绍沙箱技术在勒索软件检测的应用场景。

勒索软件通过加密受害者主机上的文档资料，索要赎金达到勒索的目的。勒索软件利用精心构造“阶段式”攻击方法，层层推进，逐步让受害者中招。

第一步，攻击者一般通过“水坑”或者“鱼叉”攻击，诱骗受害者点击，下载 Launcher，通常是一个下载器，骗过防病毒软件的检测；

第二步，下载器链接黑客控制的服务器，下载真正的恶意文件，绕过防病毒检查，遍历受害者主机的文档，进行加密操作；

第三步，加密完成，在桌面醒目位置留下勒索信息；



1. 勒索软件的危害

1.1 勒索软件的危害

勒索软件危害严重。2016 年 2 月，美国一家医院，遭到勒索软件的入侵，文档被加密，业务系统无法识别，医生无法工作，病人无法接受治疗，医院陷入瘫痪。最后，医院不得以支付高达 1 万 7 千美金，换取文档资料的恢复，为此，医院的 CEO 专门发布了公开信，。

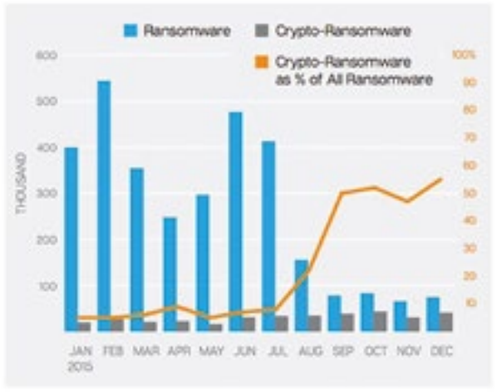
个人用户中了勒索软件，重要的资料，文档和照片等被加密，无法打开。及时按照勒索软件的指示，交纳赎金，依然存在被撕票的风险，严重者找不回来这些重要资料。绿盟科技客服部门，多次接到客户中了勒索软件的求助，咨询解决办法。

以上的案例可以看出，勒索软件对个人和企业，都有严重的影响。轻者如个人用户的资料文档损失，重者则使企业的业务运转停顿，无法持续。

1.2 勒索软件发展趋势

勒索软件在过去几年发展，呈现出这样的发展趋势：勒索软件的数量逐渐增多，富于变化，以及向多个操作系统，大数据平台进行扩散。

1) 勒索软件数量持续增长



勒索软件的数量持续上升。勒索软件的制作者，得到赎金后，尝到甜头，相当于变相激励，制作越来越多的勒索软件；其他黑客组织，也会仿效，成为勒索软件的黑客犯罪团伙。根据赛门铁克 2016 年 Q1 的报告，2015 年加密型勒索软件，占据所有勒索软件的比例越来越高，超过 50%。从下面的图中柱状部分，加密型勒索软件的数量，每个月有数万个活跃的勒索软件。

勒索软件的受害者越来越多。卡巴斯基实验室 2016 年 6 月发布的研究报告，2015 年 4 月至 2016 年 3 月，共有 231 万多人遭到勒索软件的侵害，比上一年提高 17.7%。

2) 勒索软件富于变化

同一个勒索软件家族，有多个变种。有时用 Word 宏感染，有时用 js 脚本的形式进行感染。勒索软件的制作者，处心积虑，时时关注最新

漏洞披露情况，一旦发现可用的漏洞，便更新自己勒索工具。Gartner 的报告显示，有勒索软件，最多使用 15 个漏洞利用进行攻击渗透。

2017 年 4 月份发现的勒索软件 Mole，将这种变化表现得淋漓尽致。据 Palo Alto 对此样本的研究，在短短的 4 天之内，Mole 勒索软件就进行了三次变形。

3) 勒索范围扩大化

勒索软件主要目标在 Windows 用户，逐步向移动设备（安卓），Mac OS X，Linux 操作系统扩展。另外，勒索软件作者，还将 Hadoop 大数据平台，Elastic 等数据分析平台纳入勒索目标，通过锁定数据库等手段进行勒索。

黑客通过一次的勒索行动，可以获利上百万美元，这是他们最大的动力。另外，随着比特币的流行，为黑客的转账行为提供方便。据报道，隐藏在勒索软件背后的黑客组织，在 2015 年，曾经获得了 3 亿多美金的利益。如此巨大利益回报，让黑客犯罪组织铤而走险。

另外，代码平台 github 上有关于勒索软件的开源程序，也为黑客提供了学习便利。更有甚者，暗网平台上，提供勒索软件定制服务，号称 “ransomware as a service”，即勒索软件作为服务，可以制定勒索软件功能，针对杀毒软件的免杀等。勒索软件的制作者和发布者合作分工，加大了勒索软件的传播和感染风险。

勒索软件的发展趋势，深受黑客犯罪团伙利益的驱使。制作更多的勒索软件，攻击方式更精巧，武器更精良（漏洞利用），通过变形躲避终端防病毒的检测，尽可能感染更多的用户，才有可能收到更多的赎金。所谓 “天下熙熙，皆为利来，天下攘攘，皆为利往”，在勒索软件的犯罪组织这里，体现的更加淋漓尽致。

2. 勒索软件与 APT 威胁

APT 高级持续性威胁，是另外一种高级威胁。勒索软件与 APT 威胁，既有相同点，也有不同点。比如，APT 攻击也使用 “水坑攻击” 或者 “鱼叉攻击” 等手法进行入侵。但 APT 威胁，更多的是利用 0Day 漏洞，对抗的等级更高，通过 APT 事件的披露，更多的是国家之间的安全对抗。

比较	内容	勒索软件	APT
相似点	攻击手法	钓鱼邮件	鱼叉攻击 水坑攻击
	攻击过程	下载器 最新的漏洞利用	下载器 最新漏洞利用 0Day 漏洞
不同点	最终目的	勒索比特币	信息窃取
	暴露方式	直接暴露	隐藏
	僵尸网络	单点勒索	CnC 网络

上表是 APT 威胁与勒索软件的异同点对比。在攻击手法和攻击过程上，二者类似。不过勒索软件更多借助垃圾邮件，广撒网，愿者上钩，钓到一个是一个。在攻击过程，都是“阶段式”攻击，如出一辙。APT 威胁，攻击目标更高级，尽量隐藏自己，而勒索软件目的就是赤裸裸的索要赎金，感染加密后，立刻留下勒索信息。

中过勒索软件的企业，如果只是几个终端主机感染，没有造成重大损失，应该感到庆幸。试想，如果这次不是勒索软件，而是一起 APT 攻击，恐怕还有更大的风险在后面。勒索软件为企业敲响了警钟，需要认真对待高级威胁，尽管部署了很多安全产品，制定了安全管理规范，还是存在被入侵的风险。

3. 勒索软件应对之道

勒索软件已成公害，世界范围内的用户和企业深受其苦。对于不慎感染勒索软件的用户，到底应该怎么办? 支付和不支付赎金，这是一个问题。不支付, 重要的文档, 珍贵的图片, 全部损失掉; 对于企业，业务停顿，商业声誉降到最低点。如果支付，有可能解密恢复文件，业务系统恢复正常。但是，这也同时鼓励勒索行为，助长了黑客的气焰，变相提供资金支持。

这个矛盾的选择，网络上引起广泛讨论。如果能够恢复回来，没有人愿意给黑客支付赎金。在没有办法进行恢复的情况下，想要找回文件，恢复业务系统，就像前面提到的医院那样，为了恢复医院正常运营，不得不支付赎金。

3.1 勒索软件公益项目解密工具

各国政府和安全企业，积极参与勒索软件犯罪的打击和治理。欧洲刑警组织，联合卡巴斯基和 Intel 安全，成立了 “no more ransom” 公益项目 ，收集和整理部分勒索软件的解密工具。感染了勒索软件，应该首先浏览这个网站，碰碰运气，看看是否存在解密工具。网站提供了工具，上传两到三个被勒索软件加密的文档后，网站后台进行分析，判断是否有工具可用。笔者粗略浏览，网站提供 30 多个解密工具可用。

虽然有公益组织，提供部分解密工具，不过也只是一小部分；而且，勒索软件犯罪组织，一旦发现有破解方法，也会更新加密算法，让解密工具失效。

3.2 勒索软件应对之道

防范于未然，才是勒索软件的应对之道。安全意识培训，备份和采用高级威胁检测设备，是防范勒索软件的最佳实践。

首先，员工需要进行有效的安全意识培训，点击之前应思考。毕竟, APT 威胁和勒索软件, 都带有社交工程的色彩，诱骗用户点击。员工安全意识足够强，具有基本的分辨能力，不因好奇而点击不明身份的链接和附件，从源头上，遏制对勒索软件的感染风险。

其次, 定期数据备份。一旦勒索软件加密文档, 备份对数据恢复, 业务持续性就显得尤为重要。备份要满足 “3-2-1” 的原则：即 3 份数据拷贝，要分散在 2 个不同的物理地点，并且有一份备份是离线数据备份。数据备份和数据恢复，需要定期演练，模拟发生重大网络安全实践，应急响应团队对数据恢复流程的操作，满足规范，能够在有限的规定时间内完成恢复任务。

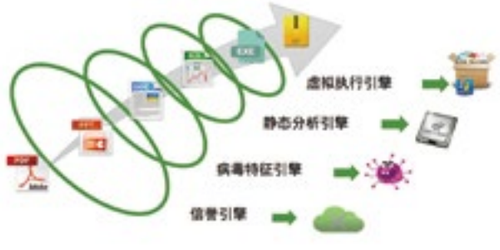
最后，采用具有未知威胁检测能力的安全产品和方案，实时检测和阻断勒索软件的入侵。勒索软件和 APT 威胁，同属于高级威胁，传统的安全手段，防病毒、防火墙、IPS 等缺乏有效检测手段，被勒索软件的 “阶段式” 攻击轻松绕过。因此，需要引入未知威胁能力检测的产品，比如沙箱类安全产品，能够模拟用户终端环境，记录恶意软件的各个阶段的行为，分析这些行为之间的关联关系，判断其是否为勒索软件。

4. 勒索软件检测和防御

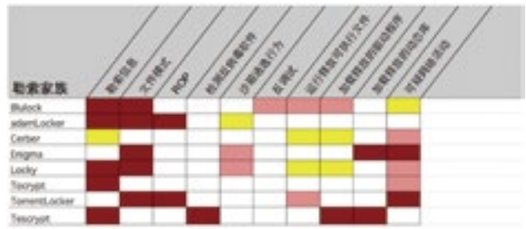
安全意识培训和数据备份，前者是在勒索软件诱骗之前，后者防备勒索中招之后。绿盟科技高级威胁分析产品 TAC，内置多个安全引擎。其中, 安全信誉引擎和防病毒引擎, 对已知勒索软件进行检测。

4.1 勒索软件检测引擎

绿盟科技高级威胁分析产品 TAC，内置多个安全引擎。其中，安全信誉引擎和防病毒引擎，对已知勒索软件进行检测。



静态分析引擎和虚拟执行引擎（即沙箱），对未知的勒索软件进行检测。新的勒索软件，或是最新的变种，在虚拟环境里面运行，TAC 记录和分析可疑文件的行为，根据其程序运行的逻辑，判断是否有勒索行为。



额外的，通过与勒索软件家族的既有行为模式比对，判断其所属的家族。

4.2 勒索软件防护场景

1) 邮件检测和防护场景

绿盟威胁分析系统 TAC 邮件系列型号 (以下简称 TAC-E) 的产品，是专门检测邮件高级威胁的网络沙箱类安全产品。针对邮件的高级威胁，主要有鱼叉 APT 威胁和勒索软件两大类。TAC-E 接收到可疑的邮件，对其中的恶意 URL 和附件进行安全检测。

根据 Osterman 的调研 ， 通过邮件方式感染的勒索软件，占所有感染方式的 60%。邮件高级威胁的检测和隔离，是勒索软件防范重点。如上图所示，TAC-E 与绿盟邮件安全网关 (下称 SEG) 组成

NGTP 解决方案的邮件场景。外部邮件先通过 SEG，过滤掉已知的病毒邮件和垃圾邮件；再经过 TAC-E 设备进行第二层过滤，勒索软件和 APT 威胁被隔离。

2) 网络检测和防护场景

绿盟威胁分析系统 TAC 在线检测系列型号（以下称 TAC-D），专门检测网络上传输的高级威胁产品。TAC-D 既可以独立部署，也可以与网关设备联动，组成 NGTP 解决方案的网络场景。

TAC-D 产品与绿盟网络入侵检测系统（下称 NIPS）联动，NIPS 检测和拦截已知的网络攻击，对于 NIPS 无法检测的可疑威胁，投递到 TAC-D 进行分析。根据分析结果，TAC-D 生成本地安全信誉，与绿盟威胁情报中心（下称 NTI）一道，为 NIPS 提供最及时的安全信誉，检测和阻断最新的高级威胁，最新的勒索软件。

4.3 勒索软件检测案例

某大型制造企业，深受勒索软件之苦。办公网员工，防范意识不够，多次感染勒索软件，文档被加密，影响工作。最严重的一次，领导的笔记本电脑中了勒索软件，对外投资的文档被加密，影响了企业的投资的进展，给合作方留下了负面印象。

客户购买了 TAC 产品，上线第一天，就发现了两起勒索软件。下图为其中一个勒索软件的分析报告。TAC 对勒索软件的检测得到验证。

5. 结语

勒索软件来势凶猛，是近两年增长最为快速的高级威胁。分析勒索软件的发展趋势，可以断言，未来的勒索软件还会持续增长，潜在的受害者也会持续攀升。

勒索软件带来了巨大挑战。防范于未然是勒索软件的应对之道。有效的安全意识培训，定期数据备份，采用高级威胁检测产品和方案，是防御勒索软件的最佳实践。

绿盟威胁分析系统 TAC 产品，配置强大的勒索软件检测引擎，与 SEG，NIPS 等传统安全产品组成 NGTP 解决方案，有效隔离已知和未知勒索软件，保护用户的文档数据安全，保障企业业务持续运行。

CTF夺旗赛经验总结及落地实践

金融事业部 周扬 合作产品部 柴森

关键词：攻防比赛 CTF 比赛规则 信息安全人才培养

摘要：中国是科技人才资源最多的国家之一，但也是人才流失比较严重的国家。世界各国已经把加强人才建设作为抢占网络空间制高点的战略举措。在此背景下，国内外各类 CTF 比赛越来越多，那么怎样一方面准备好比赛，另一方面又怎样才能组织好比赛，小编请两位专家来聊聊。

什么是 CTF 夺旗赛

Capture The Flag（简称 CTF），翻译为“夺旗比赛”，起源于 1996 年举办的 DEF CON 全球黑客大会，最早是交流安全技术的重要途径，发展至今已有 21 年的历史，是目前全球最高技术水平和影响力的 CTF 竞赛，类似于 CTF 赛场中的“世界杯”。

随着安全攻防技术的发展，CTF 比赛也逐渐演变成为信息安全技术竞赛的一种形式，发展成为全球网络安全圈最流行的一种竞赛模式，其比赛形式与内容拥有浓厚的黑客精神和黑客文化。

近年来，CTF 比赛的数量与规模发展迅猛，国内外各类高质量的 CTF 竞赛层出不穷，CTF 已经成为了学习提升信息安全技术，

展现安全能力和水平的绝佳平台。

CTF 基础知识

语言运用：计算机语言可以大致分为机器语言，汇编语言，高级语言，计算机每进行的一次动作，一个步骤，都是按照计算机语言编好的程序来执行。而在 CTF 比赛中，计算机语言的了解与掌握会有事半功倍的效果，进程的动态调试、防护脚本的编写、源代码审计等工作都是建立在对计算机语言有所掌握的基础上进行的。

Web 安全：目前国内大多数 CTF 比赛都以 Web 安全为主，但是 Web 安全涉及的内容非常广泛，就典型的 Web 服务来说，其安全问题可能来自于 Web 服务器、数据库、Web 程序本身与开发语言等。了解一个 Web 应用的组成架构、装载与配置、指令操作及组件缺陷，是参赛者知识储备环节中不可或缺的部分。

安全加固：安全领域的精髓在于攻防，在 CTF 比赛也是同样的道理，比赛成绩不仅取决于在有效的时间内拿下多少 flag，还取决于能抵御多少次外来攻击。有一些比赛队伍不注重或者不善于漏洞加固，即使得到很多分数，但是优势还是会被慢慢的蚕食掉。所以，了解漏洞的产生原因、减小漏洞的影响范围以及行之有效的安全加固也是一个成功队伍的重要能力。

密码算法：参赛者需要了解主流的密码算法，如对称密码、公钥密码、流密码、哈希密码算法等。在不断的攻防对抗中，一些关键信息或者突破口，往往会通过算法的加解密将它们“隐藏”起来增加解题难度。此外还会伴随着弱口令尝试，密码字典的暴力猜解等。

网络取证：对于网络攻击行为的溯源分析、漏洞挖掘过程中的抓包分析往往是很多参赛队伍在攻防对抗中忽略的问题，能够在最短的时间内抓到线索并做出行之有效的响应，这方面的能力也就成为了高手和顶尖高手之间的分水岭，古人常说：“天下大事，必作于细；天下难事，必成于易”，我想应该就是这个道理。

CTF 比赛模式

解题模式：大多数为线上比赛，选手自由组队（人数不受限制），出题者把一些信息安全实战中可能遇到的问题抽象成一个题目，比如一个存在漏洞的网站让选手入侵，一个有漏洞的程序让选手分析来写出漏洞利用程序，一段密文让选手解密，一个图片选手你从里面找出隐藏的线索等等。在完成这些出题的题目后，可以获得一串奇怪的字符串，也就是所谓的 flag，提交它，就能获得这道题目的分数。

攻防模式：大多数为线下比赛，参赛队伍人数有限制（通常为 3 到 5 人不等），参赛队伍保护自己的服务器，攻击其他队伍的服务器，每个队伍的服务器开始拥有相同的配置和缺陷，比如几个有漏洞的二进制程序、有漏洞的 Web 应用、某些权限账户弱口令等等，然后队员需要找出这些漏洞并进行加固，同时利用这些漏洞来攻击别人的服务器，拿到其他队伍的权限后，会获取到相应 flag 后提交，从对方身上赚取相应的分数，每隔一段时间后，可以再次攻击并利用未加固的漏洞获取 flag 并赚取分数。

混合模式：解题模式和攻防模式同时进行，解题模式可能会根据比赛的时间、进度等因素来释放需解答的题目，题目的难度越大，解答完成后获取的分数越高；攻防模式会贯穿整个 CTF 比赛的始终，参赛队伍需不断积累分数，最终参数队伍的名次由两种模式累积的分数总和决定。有些有趣的 CTF 比赛，还会引入一些情景剧情和现场观众的互动，来增加比赛的趣味性。

CTF 比赛经验

交流聆听：CTF 比赛通常强度都很大，少则几小时多则好几天，即使是特别要好的队友，也难免会有意见与思路不统一的时候，这个时候与队友的交流和聆听则显得尤为重要。一句温馨的关怀，一个会心的微笑甚至一个肯定的眼神都会让你的队友倍感温暖，正面的交流与聆听会鼓励大家共同前进，克服困难。

学习能力：CTF 比赛中的题目与攻防手段往往没有特定的规律，因此更看重人临场的快速学习以及把理论付诸实践的能力，而并非大量的知识储备。一定的知识量储备肯定是必要的，但并不能期望完全依靠知识储备来获得胜利。

合作分工：CTF 的成绩主要还是看团队的综合实习。就如学生时代的中考高考一样，考核的总分成绩，往往各个科目都比较好的人才能获得比较高的成绩。如果队伍成员都是只擅长 Web 安全，其他领域涉及很少，就算研究 Web 安全研究的再精通也取得不了好名次，一个团队中既要有攻城拔寨的急先锋，也同样需要留守加固的中流砥柱，需要尽可能的面面俱到。

总结分享：通常专业的 CTF 队伍人员会比较稳定，如果想通过比赛的历练成为顶尖队伍，除了上述几点外，比赛过后以及日常的分享总结也是非常重要的。无论取得怎样的成绩，相信每一个队员心里都会有困惑或者看法，那么赛后队员坐在一起进行讨论、分析、总结不仅可以拉近队员间的感情，提升团队凝聚力，还可以收获更多的经验与心得。

CTF 攻防平台

Facebook CTF 平台

Facebook 的 CTF 平台是一套开源比赛平台，包括游戏地图、团队登记和评分系统。还

可以按需提供逆向工程逆向工程、Web 应用安全、取证、二进制开发和加密等挑战。用户还可以使用 Facebook CTF 平台定制或自定义挑战项目。

挑战分为以下两类：计算机安全方面的小问题，以及漏洞利用和黑客方面的标记问题。标记挑战要求参与者完成一项诸如转储数据库、获取系统外壳或操纵应用程序等任务。

“通过 CTF 平台，你可以学习到常规计算机科学项目中学习不到的技巧。此外，这个平台还帮助你进入安全行业。”Facbook 威胁基础设施团队的软件工程师 Gulshan Singh 说。“在开始找全职工作时，我发现安全职位的面试很像 CTF 挑战，有了后者的经验，我可以更好地展示技能。第一天入职我就让人感觉非同凡响。”

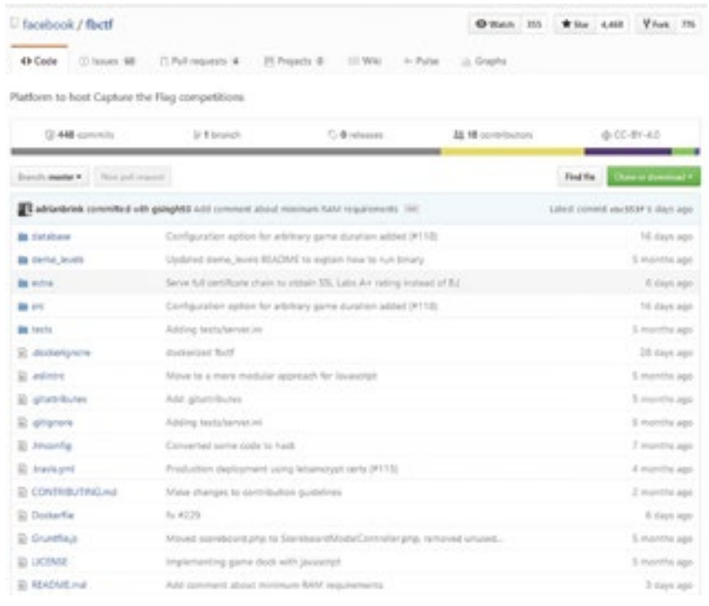
怎么使用 FBCTF

可以组织一场比赛，最少 2 个人，最多数百人。参赛者可以在本地或者在线，或者两种形式均可。按照安装说明来设置平台基础架构，输入 challenges 进入管理界面。

参赛者可以注册为战队，如果是一场封闭的比赛，那么在管理页面，生成并导出令牌，然后分享给核准的团队，然后引导参赛者到注册页。如果是一场开放的比赛，那么直接引导参赛者到注册页面即可。

Facebook CTF 源码下载

CTF 平台可以搭建在运行 Ubuntu 操作系统的系统（物理机或虚拟机）上。Facebook 已提供了关于如何安装和使用平台的说明。下载地址在这里：https://github.com/facebook/fbctf/



绿盟科技 CTF 平台

绿盟科技信息安全攻防实训与竞技产品，包括绿盟科技信息安全实训平台和绿盟科技信息安全竞技平台，如下图所示：

整体框架如上图所示，产品特性说明如下：

• 整体方案采用 B/S 架构对外提供新安全课件培训、实验训练和攻防保障服务。使用人员可以结合自身情况，灵活选取远程在线和线下面对面的实时教学形式。

• 两个平台可以支持进行课件培训、实验训练和攻防保障三大功能。课件培训主要以课件宣讲为主，实现信息安全知识的直接传递；实验训练以安全攻防模拟操作实验为主，使得被培训对象对安全技术的建立直观印象；攻防保则主要为被培训对象提供攻防的虚拟环境，实际检验被培训对象的安全水平。

• IT 支撑基础资源主要包括安操作系统、数据库、中间件、网络设备和安全设备等，通过与虚拟技术相结合，用以保障上层的实训场景和竞技场景。

绿盟信息安全实训系统

ISTS -Information Security Trainning System，为信息安全培训、教学及科研提供一个完整的、一体化的实验教学环境。打造全方位的专业信息安全实验室。主要建设内容包括以下内容：

图 1.1 信息安全实训平台功能框架图

图 1.2 信息安全实训平台选课界面

• 通过各种形式的信息安全意识教育实践、培训及宣传，使得信息安全意识融入到生活工作中，变成一种常态化的工作。

• 以理论学习为基础，结合最全面最专业的实训，增加被培训对象对信息安全诸多领域的深入理解。提供多个方面的实验、实训及工程实践，涵盖多层次的实验操作，以真实环境的真实案例为操作指南，贴近实际岗位能力要求，提供完整的实验教学环境。

由于信息安全属于交叉学科，其中包括：网络安全、系统安全、数据安全等等，信息安全实训平台内置 800 个信息安全实训课程，全面覆盖信息安全各个领域的实训内容。

绿盟信息安全竞技系统

ISCS -Information Security Competition System 是围绕信息安全理论和知识，组建的信息安全对抗技能实战赛。也可以承载信息安全对抗攻防演练项目，考察攻防演练者网络安全理论知识与实际问题处理能力，旨在借助攻防演练培养一批具备信息安全素养的优秀实战专业的安全人员。安全攻防竞赛平的攻防竞赛模式可以分为单兵作战挑战赛、综合靶场及网络混战三种形式。

图 1.3 信息安全攻防竞技平台功能模块图

个人挑战模式

个人挑战模式每个赛题（关卡）是一个单独的靶场，并提供了七大类赛题，WEB、密码学、隐写、溢出、逆向、编程、综合，全面考察参赛选手的安全能力，题目由易到难。

图 1.4 信息安全攻防竞技平台个人挑战功能界面

图 1.5 信息安全攻防竞技平台个人挑战态势展示图

网络混战模式

网络混战模式是多人或者多组互相进行攻击的模式，不仅要加固自己的服务器防止被对手攻陷，同时要尽可能多的攻击对手的服务器以取得更多的得分。

图 1.6 信息安全攻防竞技平台网络混战态势展示

综合靶场模式

综合靶场贴近行业用户业务系统，整个综合靶场由多台漏洞靶机，多层网络架构组成。用户可以有多个攻防入口多种攻防路径选择，让参赛选手在大型真实的行业业务系统中进行挑战，难度较高。

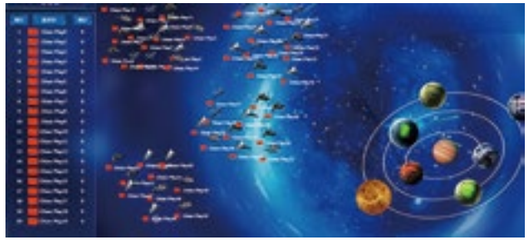


图 1.7 信息安全攻防竞技平台网络靶场势展示

信息安全人才培养，我们在行动

我们认为针对信息安全人才的培养，需要有一套全面而有效的方案。经过多年行业比赛经验积累，绿盟科技推出信息安全人才培养解决方案，本方案由信息安全实训平台 NSFOCUS-ISTS 与信息安全竞技平台 NSFOCUS-ISCS 组成，通过信息安全实训平台建设信息安全人才培养体系，实现网络安全意识培养，实现信息安全实操学习环境。通过信息安全攻防竞技平台进行模拟业务系统安全实践，提高用户信息安全实操能力。同时，通过举办安全技能大赛可进行信息安全能力的检验和信息安全人才的选拔。

信息安全人才培养解决方案已经实际应用到各个行业的多次比赛中，在政府行业支持了 2016 年湖北网络安全技术竞赛，在教育行业支持了全国大学生电子设计竞赛、北理工 ISCC 大赛，在交通运输行业支持了第二届长航局网络与信息安全培训演练，在运营商行业支持了电信系统信息安全大比武、2015-2016 年两届云南省互联网攻防大赛，在金融行业支持了云南银行业首届网络攻防大赛、辽宁省银行业首届网络安全攻防竞赛，在能源行业支持了国家电网信息安全人才选拔赛等等。

信息安全是国家信息化健康发展的基础，是国家安全的重要组成部分，也是一项涉及面广、渗透性强的系统工程，必须培养社会公民的信息安全意识和引导公民参与。国家信息安全的竞争，归根到底是信息安全人才的竞争，再先进的技术、设备也还需要人来掌控，所以人才是信息安全的关键!

你或许不知道SDP 但它能改变IaaS安全现状

创新中心 赵静茹 张星

关键词：软件定义边界 基础架构即服务

摘要：软件定义边界（Software Defined Perimeter，SDP）由云安全联盟（CSA）于 2013 年提出，在 2017 年 2 月，CSA 正式发布《Software Defined Perimeter for Infrastructure as a Service》白皮书。本文对其主要内容进行整理，也结合了我们对于 SDP 的认识，希望读者在读完本文后能够对 SDP 在 IaaS 中的应用有一个较为深入的了解。

IaaS 基本介绍

基础设施即服务（Infrastructure as a Service，IaaS）能够为消费者提供 CPU、内存、存储、网络和其他基础计算资源，在这些资源之上，消费者能够部署和运行任意软件，包括操作系统和应用。消费者不需要关心底层云基础设施，但是可以控制操作系统、存储和部署的应用程序，也可能对特定的网络组件有控制能力。图 1 中展示了一个 IaaS 环境的简化架构图，可以适用于公共云和私有云的部署。

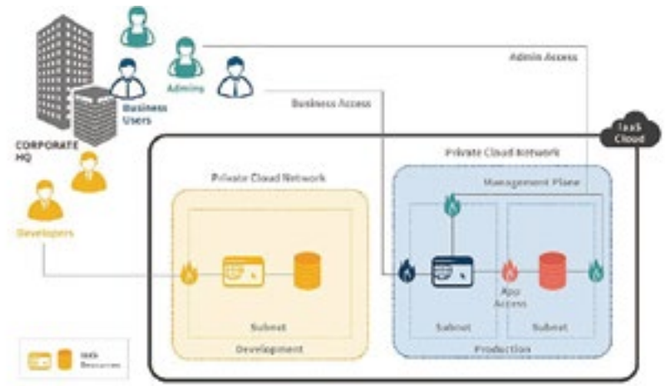


图 1 IaaS 环境的简化架构图

图 1 中展示了一个 IaaS 云环境，这个 IaaS 云环境中有两个私有云网络，每个私有云网络中有一些 IaaS 资源（虚拟机）。从网络访问的角度来看，这些私有云网络能够对应到单独的账户，或者单独的私有云环境区域（例如 AWS 虚拟私有云）。这些私有云网络被防火墙所保护，防火墙控制网络流量进入和走出云环境。在本文档中，省略了路由表、网关等，着重关注管理用户访问的挑战。

IaaS 安全需求新挑战

用户访问场景的变化

位置不再作为网络访问级别的主要标准

不同的开发者可能需要不同类型的网络访问不同的资源。例如，Sally 是数据库管理员，他需要访问运行着数据库的所有服务器的 3306 端口。Joe 坐在 Sally 旁边，管理 Purple 项目的应用程序代码，需要 SSH 到具有应用程序的服务器。Chris 不同于团队的其他成员，需要远程工作，也是 Purple 项目的应用程序开发人员，尽管相隔数百英里，Chris 需要与 Joe 相同的访问权限，

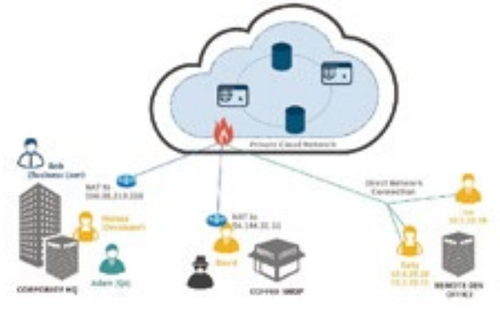
所以位置可能是访问策略过程中需要被考虑到的一个属性，而不再是确定网络访问控制级别的主要因素。

IaaS 环境在不断变化

首先，IaaS 环境中的计算资源是高度动态的，服务器实例需要被不断创建和销毁。手动管理和跟踪对这些服务器实例的访问是几乎不可能的。第二，开发者也是动态的，他们可能在不同的项目中扮演不同的角色，而这不同的角色可能需要同时存在。这种情况在 DevOps 环境中尤为明显，开发，QA，发布和运营的角色在一个团队中混合。

IP 地址问题

不仅用户的 IP 地址定期更改，用户和 IP 地址之间也没有一一对应的关系。下图说明了当访问规则完全由 IP 地址驱动时，即使是简单的环境也是如此复杂：



位置	网络设置	安全隐患
公司总部（HQ）	所有用户都映射到单个 IP 地址	安全组无法区分用户，并且必须授予每个人对所有资源的完全访问权限。这意味着恶意用户、攻击者或恶意软件可以从本地到云网络不受阻碍地穿越。
远程开发办公室	直接网络连接保留每个用户的 IP 地址	IP 地址是动态分配的，并每天更改。用户还可以从多个设备访问云。IT 运营团队不断更新安全组规则（增加业务延迟）或网络完全向云开放（降低安全性）。.
咖啡店	一些用户需要从各个位置远程访问	来自这些位置的网络访问将扩展到同一网络上的任何恶意用户，在同一网络中很难根据用户不断变化的位置和访问需求来手动调整网络访问策略。

IaaS 需要解决两个问题

总体来说 IaaS 安全有两个问题需要解决，A. 安全远程访问；B. 用户访问的可见性和可控性。

安全远程访问

首先，让我们考虑安全的远程访问问题。所有的云用户都是远程访问云的，这意味着到云的通信是通过网络连接发生的。组织通常使用 VPN 解决这一问题，使用 VPN 技术上解决了上述问题 A（安全远程访问），因为它为从用户设备到云网络的网络流量提供了安全的加密隧道。这有一些缺点，特别是如果所有用户流量都需要先到公司网络，然后再去访问云，这将引入额外的延迟，创建单点故障，并可能增加带宽成本和 VPN 许可成本。通过 VPN 直接从每个用户的设备连接到云有助于解决这些问题中的一些，但可能与同时 VPN 连接到公司网络的需要冲突。

Type	Protocol	Port Range	Source
HTTP	TCP	80	173.76.247.254/32
HTTP	TCP	80	50.255.155.113/32
HTTP	TCP	80	73.68.25.221/32
HTTP	TCP	80	98.217.113.192/32
HTTP	TCP	80	209.64.11.88/32
HTTP	TCP	80	172.85.50.162/32
HTTP	TCP	80	68.190.210.117/32
RDP	TCP	3389	173.76.247.254/32
RDP	TCP	3389	110.142.238.207/32
RDP	TCP	3389	50.255.155.113/32
RDP	TCP	3389	73.68.25.221/32
RDP	TCP	3389	98.217.113.192/32
RDP	TCP	3389	209.64.11.88/32

用户访问的可见性和可控性

无论用户如何进入 IaaS 环境（无论是通过 VPN 还是非 VPN），安全团队仍然需要控制（并监控和报告）在 IaaS 环境中哪些用户可以访问的哪些资源。IaaS 平台提供了内置工具来管理这一点，例如 AWS 中的安全组和 Azure 中的网络安全组（在本文中我们称之为 Cloud FIrewall）根据源 IP 地址控制对服务器的访问。

让我们来看一个云防火墙的例子：

这个防火墙配置片断展示了 IaaS 平台提供的简单 IP 地址规则方法。分配给此防火墙组的所有服务器实例将继承此组规则，允许网络访问特定端口。这种方法有几个问题：

- 它提供对此云防火墙中所有服务器的粗粒度访问。
- IP 地址不对应用户。
- 没有策略的概念，也没有解释为什么给定的源 IP 地址在此列表中。
- 此列表是静态的，不能对应用户位置或权限的更改而做出改变。
- 此方法无法考虑任何信任概念（例如身份验证强度，设备配置文件或客户端行为），并相应调整访问权限
- 任何更改都需要对管理员对 IaaS 帐户进行管理访问

o 这将需要集中化，从而延缓生产力，

o 将需要对多个用户设置管理员访问权限，这将导致安全性，合规性和操作问题

对于 IaaS 环境，安全远程访问不再是特殊情况。所有用户都是远离云的，所以安全和网络团队需要关心所有用户是如何访问资源的，而不仅仅是用户的一个子集。也就是说，安全远程访问必须成为一个核心关注点，并且是采用 IaaS 的任何企业的整体安全策略的一部分。

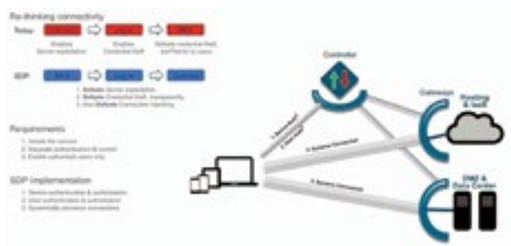
使用软件定义边界解决 IaaS 安全访问问题

软件定义边界简介

软件定义边界（Software Defined Perimeter，SDP）由云安全联盟（CSA）于 2013 年提出，用应用所有者可控的逻辑组件取代了物理设备，只有在设备认证和身份认证之后，SDP 才提供对于应用基础设施的访问。

SDP 改变了传统的网站连接方式。在传统的连接中，首先，客户端需要建立与服务器端的连接，这一步骤使服务端暴露在公网中，若服务端有漏洞，则有可能被利用；其次，用户通过登录页面输入用户名和密码，这一步骤有可能使得用户名和密码被窃取；最后，除用户名和密码外还可使用多因素认证，通过多因素认证，可以抵抗用户名和密码的丢失，但是多因素认证对于用户而言不是很友好。

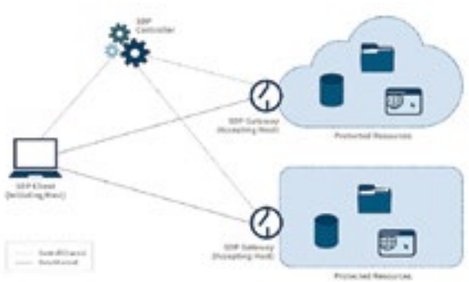
而在 SDP 中，首先，客户端进行多因素认证，认证设备的可靠



性等，这一步对用户而言是透明的。认证通过之后，才进入用户登录阶段。这两步均是客户端与 Controller 进行交互，不涉及对于具体服务的访问。当认证通过后，客户端才能够与可访问的服务建立连接。

因此，SDP 通过三种方式对抗基于网络的攻击：透明多因素认证可以抵抗用户凭据丢失、服务器隔离可以抵抗服务器利用、TLS 双向认证可以抵抗连接劫持。

SDP 包含两部分：SDP 主机和 SDP 控制器。SDP 主机可以创建连接或者接受连接。SDP 控制器（Controller）主要进行主机认证和策略下发。SDP 主机和 SDP 控制器之间通过一个安全的控制信道进行交互。SDP 主机又分为可以创建连接的主机（IH）或者可接受连接的主机（AH）。



SDP 标准 1.0 中所定义的 SDP 工作流程如下：

(1) 一个或多个 SDP 控制器上线，并且和可选的认证和授权服务建立连接；

(2) 一个或多个可接受连接的 SDP 主机上线，这些主机与控制器建立连接并被控制器认证。然而，这些主机并不对其他主机的通信进行应答，也不会响应非预分配的请求；

(3) 每一个发起连接的 SDP 主机上线，它和控制器建立连接并被控制器认证；

(4) 在认证通过后，SDP 控制器确定一个发起连接的主机可以被授权通信的主机列表；

(5)SDP 控制器通过加密信道通知可接受连接的 SDP 主机，以及一些可选的策略；

(6)SDP 控制器将可接受连接的主机的列表和可选的策略发送给发起连接的主机；

(7) 发起连接的 SDP 主机与所有授权的可接受连接的主机之间建立 Mutual TLS 连接，并发送数据。

因为 SDP Controller 和 AH 拒绝无效数据包（大概来自未授权的用户），他们可以防止与未授权用户或设备建立 TCP 连接，从而可以减轻 DDoS 攻击。

SDP 优势

现有技术缺点

(1)VPN 技术

VPN 很好地为远程用户提供对 VLAN 或网段的安全访问，就好像它们实际存在于企业网络上一样。这种技术，特别是当与多因素认证相结合时，对于具有传统边界的企业以及静态用户和服务器资源来说效果很好。但是正如 Gartner 所说，“DMZ 和传统 VPN 是为 20 世纪 90 年代的网络设计的，已经过时，因为它们缺乏保护数字业务所需的敏捷性。

VPN 有两个缺点，使得它们不适合当今的需要。首先，它们对所分配的网络提供非常粗粒度的访问控制，要么全部都可以访问，那么不能访问。尝试配置 VPN 以为不同用户提供不同级别的访问是不现实的。

第二，即使公司对 VPN 提供的控制级别感到满意，VPN 也是一种只能控制远程用户的孤立解决方案。它们不会帮助保护内部用户，这意味着组织需要一组完全不同的技术和策略来控制内部部署用户的访问。这将使协调和对准这两个解决方案所需的工作量增加一倍以上。

Gartner 指出：“到 2021 年，60%的企业将逐步淘汰 VPN，而使用软件定义边界（尽管 2016 年 SDP 的使用量不到 1%）。

(2) 跳板机（Jump Box）

跳板机（Jump Box）是一个服务器，目的是为了使不安全区域的用户访问在更安全区域中运行的服务器或服务。对于本文档，使用 Jump Box 的场景是使用 Jump Box 来代理访问云环境中的服务器。

如上图所示的 Jump Box 的网络访问可以是公开的，通过直接连接可访问，或由 VPN 控制。 访问 Jump Box 桌面本身需要用户认证（多因素）。Jump Boxes 通过对受管理的服务的强制单点访问来控制对云资源的访问。 然而 Jump Boxes 有一些限制，使它们不适合广泛的云资源访问。

- 不是多用户系统，用于单用户访问受保护的服务器
- 设计用于偶尔访问，例如由系统管理员访问，而不是用于不断的进行的访问
- 对跳板机后面的网络上的所有服务器，要么认证通过，所有的服务都可以访问，要么认证不通过，不能访问。
- 如果攻陷了跳板机或可以访问跳转的用户的设备，就可以打开整个网络。
- 难以跟踪用户访问以实现合规性检查

所以跳板机不是云系统访问控制的合适解决方案。

SDP 优势总结

(1) 策略是基于用户的，而不是基于 IP 地址

因为 SDP 系统是以用户为中心的，它在要求任何访问之前都需要对用户和设备进行验证，允许企业根据用户属性创建访问策略，执行最小特权原则，具有更细粒度的访问控制。通过利用目录组成员身份，IAM 分配的属性，角色等方面，公司可以以某种有意义的方式定义和控制对云资源的访问，这对公司业务，安全和合规性很有意义。而传统的网络安全仅基于 IP 地址，根本不考虑用户。

(2) 身份管理

SDP 和 IAM 在几个方面自然互补。

首先，SDP 实现通常被设计为利用已经部署的 IAM 系统进行认

证，从而加速 SDP 的推出。此身份验证可通过 LDAP 或 AD 服务器，或使用标准（如 SAML）进行。

其次，SDP 实现通常使用用户的 IAM 属性——例如目录组成员身份，目录属性或角色——作为 SDP 策略的元素。

最后，SDP 系统也可以包括在由 IAM 系统管理的身份生命周期中。例如，当 IAM 系统创建新帐户时，SDP 系统应同时创建相应的网络权利。

SDP Controller 信任第三方 IAM 系统用于用户身份认证和用户身份生命周期管理。因此，当第三方用户在其 IAM 系统处停用时，用户将自动无法访问受 SDP 保护的资源，因为他们无法再通过联合身份验证。这个联合很好地解决了第三方访问的常见问题。

(3) 预认证和预授权

SDP 依靠预认证和预授权作为其两个基本支柱。在认证和授权之前不会有任何数据包到达服务器，从而可以使云资源对未授权用户完全不可见。这完全消除了许多攻击向量，包括暴力攻击，洪水攻击，以及基于 TLS 漏洞的攻击，如 Heartbleed 和 Poodle。

(4) 运营效率

与实现给定级别的安全通常所需的手动工作相比，由 SDP 执行的自动化策略实施提供了显著的操作益处。

(5) 简化合规性

由于 AH 记录日志和控制所有 IH 的网络流量，所以 SDP 可以提供详细的对每个用户访问的可见性，所以 SDP 能够根据这些信息自动提供合规性报告。

(6) 降低成本

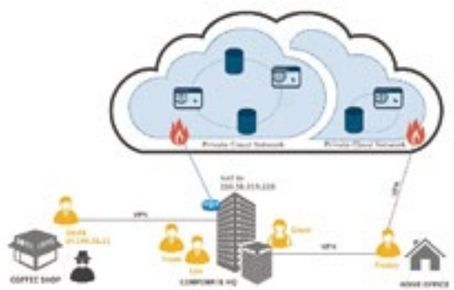
SDP 可以通过几种方式帮助组织降低成本。首先，减少 IT 任务所需的手工劳动量。这将直接降低外包 IT 模式的成本，并减少雇用额外工作人员的需要。第二，精简合规性将减少准备和执行审计所需的时间和精力。这两个活动都需要第三方顾问，每一小时的时间节省是直接的成本节约。最后，SDP 作为其它技术（例如 NAC）的替代还可以帮助组织节省资金。

SDP 在 IaaS 中的应用场景

开发人员安全访问 IaaS 环境

开发人员需要访问 IaaS 资源，以进行开发，测试和部署工作。这些用户需要访问各种各样的端口和协议，以及访问不断变化的 IaaS 资源集。

不使用 SDP 的访问控制



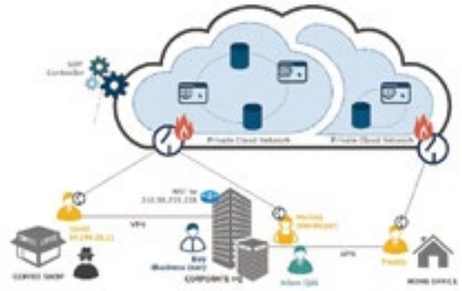
如上图所示，各种开发人员需要访问两个私有云网络环境。这些开发人员具有不同的访问要求，并且在许多不同的位置。Cloud Firewall 是网络流量的唯一控制点，本质上是一个允许连接的简单表，将源 IP 地址映射到目标服务器和端口。

使用 SDP 做访问控制

SDP 部署如下。Controller（如下所示）在所有用户可访问的位置运行（为了清楚起见，连接未在图中示出）。它可能正在云端的公共可访问位置运行，或者可能在公司总部的 DMZ 中运行。对 Controller 的访问受单数据包授权 (SPA) 的保护，因此将其暴露不会增加风险。

在 Controller 正确验证 IH 后，IH 通过 AH 访问私有云网络上的资源。 AH 还受 SPA 保护，所有 IH 流量通过网络上的加密隧道传输。 AH 在每个用户的基础上实施访问策略，实现最小权限的原则。AH 位于每个私有云网络的入口点，并控制所有入站流量。

两种方法的对比



需求	Grace，Lou 和 Frank 在公司总部工作，需要进行协作，并在多个服务器实例上访问端口 22（SSH），443（HTTPS），3306（MySQL）和 3389（RDP）。
挑战	公司总部（HQ）的所有系统都 NAT 到单个 IP 地址 *.*.*.*.

不使用 SDP	使用 SDP
方法：必须将云防火墙配置为允许从 *.*.*.*. 到私有云网络中所有服务器上的所有端口的流量通过。 这些服务器必须分配可公开访问的 IP 地址。	方法：每个用户建立从其设备（IH）到 AH 的相互认证的隧道连接，然后再通过 AH 连接到云中的目标资源。 Cloud Firewall 配置会变得更加简单： • AH 对来自整个互联网的所有流量开放。 因为它只允许通过 SPA 认证的 IH 建立连接，所以它可以在一定程度上减轻 DDoS 攻击或者其它基于 Web 的攻击。 • 受保护资源位于 AH 后面的私有 IP 地址上，无法从 Internet 访问。他们的云防火墙配置为只接受来自 AH IP 地址的访问连接。
影响：公司网络上的所有用户和系统都可以完全访问私有云网络，违反最小权限原则，增加攻击面。 这个云网络可以被扫描，攻击者可以利用漏洞进行攻击。 服务器访问仅通过身份验证保护，而不是在网络级别进行控制。 密钥管理可能成为开发人员的负担。 合规性检查更加困难，因为所有用户都可以访问所有系统。	影响： 因为每个用户到 AH 的连接是单独建立的，并且是经过强认证的，所以 AH 可以细粒度地在每个用户的基础上控制对云资源的访问。企业可以定义与用户，设备和角色相关联的策略。

需求	Freddy 是一位在家庭办公室工作的开发人员，需要访问与团队其他成员分开的私有云网络。这个环境包含敏感信息，所以他设置了一个 VPN 来访问它。他还需要访问 HQ 网络上的开发资源。
挑战	Freddy 的位置不会改变，但他需要持续访问云和 HQ 资源。 出于安全目的，需要安全的网络连接。 但是他不能在同一台机器上同时运行两个 VPN。

不使用 SDP	使用 SDP
方法：Freddy 通过他的开发机器上的不同环境访问这些资源。——他通过 VM 中的 VPN 进入云，通过在其主机操作系统中运行的 VPN 访问 HQ 网络。	方法：Freddy 建立与 AH 的安全连接，以访问受保护的云资源。
意义：这种方法会导致 Freddy 的生产力问题，因为他的一些工具和开发任务需要从同一个系统访问这两个环境。 因为 Freddy 是目前唯一访问此环境的人，所以合规性和审计报告不是问题。但他知道，在几个星期内，随着其他团队成员加入这个项目，他将会面临跟踪和报告这些访问的问题，同时还需要对团队成员的访问进行管理。他应该使办公室中每个人都可以访问云防火墙吗？远程开发人员呢？他应不应该管理大家的 VPN 访问？	启示：他可以同时使用他的 VPN 连接到办公室网络，与访问云资源没有任何冲突，因为 SDP 连接看起来像一个常规的网络连接，而不是 VPN。所以 Freddy 变得更有生产力。 Freddy 可以通过他设计的一套政策，轻松地控制和报告对这些资源的访问。向新用户提供访问权限是编辑其策略或编辑用户属性的简单问题，并且允许他以细粒度的方式控制访问。

需求	David 是一名远程工作的开发人员，并且必须定期从不安全的网络（如咖啡店）访问云系统中的多个服务器。他还需要访问 HQ 网络上的开发资源。这些服务使用多个协议和端口（22，443，3389）
挑战	咖啡店网络 NAT 到单个 IP 地址，*.*.*.*.

不使用 SDP	使用 SDP
方法：不能接受将云防火墙配置成允许整个互联网的连接，或者配置成允许来自 *.*.*.*. 的所有流量都有很大的安全风险，所以 David 首先 VPN 到公司网络，然后再访问云网络。	方法：David 的设备向 Controller 进行验证，只有认证通过了才有对 AH 所保护的资源的访问权限。David 不再需要 VPN 到公司网络，从而，提高网络性能和减少网络带宽使用成本。
影响：David 需要到 HQ 网络的 VPN 连接（他已经需要访问本地资源） 所有流量必须回传到公司网络，然后再从公司网络传出，增加延迟和带宽成本 该解决方案至少要达到上面表格中的要求，即允许公司网络上的所有用户和设备都具有对云网络的完全访问权限。	影响：因为流量是从 David 的设备加密传送到 AH，所以他既使使用公共无线网络或公共互联网也没有太大的风险。云防火墙配置不必更改，AH 对互联网开放（但受 SPA 保护），所以无论他身在何处，David 都可以高效工作。

总结

对于此用例，SDP 为企业提供了强大的优势

- 无论位置如何，都可确保开发者的访问需求
- 通过服务和端口精确控制每个开发人员可以访问的服务
- 简化合规性报告
- 更简单的安全策略配置
- 提高生产率
- 可以同时访问多个地方的资源（如果另外的资源需要 VPN 访问的话）。

主要参考文献

[1] Software Defined Perimeter for Infrastructure as a Service: https://cloudsecurityalliance.org/download/sdp-for-iaas/

[2] SDP Specification v1.0: https://cloudsecurityalliance.org/download/sdp-specification-v1-0/

TAC

阻断渔夫的勒索

我们有王牌！

TAC NSFOCUS

绿盟威胁分析系统

让勒索软件无所遁形

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。

NSFOCUS绿盟科技