文章编号: 1006-2475(2010)12-0072-04

“云安全”在计算机防病毒应用中的问题研究

欧阳中辉[1], 张晓瑜[2], 涂 帅[2], 顾佼佼[2]

(1.海军航空工程学院兵器科学与技术系, 山东 烟台 264001; 2.海军航空工程学院研究生管理大队, 山东 烟台 264001)

摘要: 针对目前“云安全”在杀毒软件中的广泛应用, 分析以趋势科技和瑞星两种主流代表的“云安全”系统的优缺点, 然后对“云安全”在计算机病毒防护应用中面临的困难和存在的问题进行论述, 最后提出解决方案和发展方向。

关键词: 云安全; 病毒防范; 隐私安全
中图分类号: TP391 文献标识码: A **doi** 10.3969/j.issn.1006-2475.2010.12.021

Research on Problem of Application of “Cloud Security” in Computer Anti-virus

OUYANG Zhong-hui[1], ZHANG Xiao-yu[2], TU Shuai[2], GU Jiao-jiao[2]

(1.Department of Ordnance Science and Technology, Naval Aeronautical and Astronautical University, Yantai 264001, China; 2.Graduate Students' Brigade, Naval Aeronautical and Astronautical University, Yantai 264001, China)

Abstract: Aiming at the broad application of “Cloud Security” in computer anti-virus, this paper analyzes the virtues and disadvantage of the representative “Cloud Security” system, the companies of The Trend of IT and Rising and the difficulties of “Cloud Security” are discussed, as well as the existed problems, finally, proposes the solution and development

Key words: cloud security; anti-virus; privacy security

0 引 言

“云安全”计划是网络时代信息安全的最新体现,它融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念,通过网状的大量客户端对网络中软件行为的异常监测,获取互联网中木马、恶意程序的最新信息,传送到服务器端进行自动分析和处理,再把病毒和木马的解决方案分发到每一个客户端[1]。

“云安全”最大的特点是实现了计算机资源的高效整合与快速处理病毒的能力,而实现形式则是防病毒的互联网化。这种互联网化首先体现在资源的互联上,通过成千上万的服务器互联,可以大大提高反病毒的处理能力与响应时间;其次是信息的互联,利用海量客户端收集并获取最新病毒信息,将最终解决方案实现共享。因此,对于客户端用户来说,既是推动反病毒技术发展的贡献者,也是受益者。正是看到“云安全”的互联网化给反病毒企业带来的全新反病毒思路和给用户全新的应用体验,该模式一经推出,就得到了包括瑞星、趋势科技、SYMANTEC等国内外诸多反病毒厂商关注,并根据自身的理解,推出了相应的“云安全”解决方案。但是,无论是“云安全”厂商,还是使用“云安全”的用户,安全问题都是第一大问题。对安全厂商来说,如何保证“云端”服务自身的安全性?对用户来说,如何才能相信提供商能保证自己的隐私不被窃取?这些都是“云安全”应用急需解决的问题。

1 主流反病毒软件“云安全”架构

当前已经出现的“云安全”实现原理大概可以分为两种[2-5]:

(1)趋势科技。

趋势科技的“云安全”主要用于企业级产品当中,以Web信誉服务(WRS)、邮件信誉服务(ERS)和文件信誉服务(FRS)为基础架构的云客户端安全架

收稿日期: 2010-08-04

作者简介: 欧阳中辉(1966-),男,湖南永州人,海军航空工程学院兵器科学与技术系教授,硕士生导师,研究方向:计算机网络;张晓瑜(1983-),男,河南南阳人,海军航空工程学院研究生管理大队硕士研究生,研究方向:计算机网络,网络安全;涂帅(1986-),男,湖南岳阳人,硕士研究生,研究方向:计算机网络;顾佼佼(1985-),男,山东青岛人,硕士研究生,研究方向:计算机网络。

构,把病毒特征码文件保存到互联网云数据库中,令其在端点处保持最低数量用于验证。趋势科技“云安全”技术基于其拥有庞大的服务器群和并行处理能力,构建一个庞大的黑白名单服务器群,用于客户端查询,在 W eb威胁到达最终用户或公司之前即对其予以拦截。

在趋势的“云安全”概念中,趋势的服务器组成一个大“云”。因此,趋势“云安全”必须建立在大量服务器基础上。趋势“云安全”存在的缺陷是,它主要是对外来威胁进行组合、判断和拦截,无法对已经存在于本地计算机上的未知威胁进行有效感知。

(2)瑞星。

瑞星“云安全”主要是通过网状的大量客户端监测网络中软件行为的异常,截获互联网中的木马、恶意程序的最新信息,然后推送到服务器端进行自动分析和处理,最后把病毒和木马的解决方案分发到每一个客户端。

瑞星的“云安全”的实质是一个样本收集处理机制。实现瑞星“云安全”需要有大量的客户端,才能组成真正意义上的“云”。瑞星的“云安全”也有自己的缺陷,它虽然能感知用户计算机上已经存在的未知病毒,但却不具备在未知病毒入侵计算机前对其进行拦截的能力。

2　面临的困难

“云安全”概念的提出,对于网络安全来说是很有意义的,但是要想建立“云安全”系统,并使之正常运行,需要解决以下几个方面的问题[6-7, 12]:

(1)需要海量的客户端(“云安全”探针)、足够的服务器群以及海量数据处理能力。只有拥有海量的客户端,才能对互联网上出现的恶意程序、危险网站有最灵敏的感知能力。而庞大的数据中心,大量的服务器是实现“云安全”的基本前提。

(2)要求能够准确收集、上报病毒,并对其进行快速有效的分析和处理。完成这些需要程序未知行为判断、虚拟机脱壳、人工智能等一些前沿的反病毒和网络安全技术。而这些技术难题,在解决上是比较复杂的,需要专业的反病毒技术和经验。

(3)需要大量的资金和技术投入。“云安全”系统在服务器、带宽等硬件方面需要极大的投入,同时要求安全厂商应当具有相应的顶尖技术团队、持续的研究经费。

(4)可以是开放的系统,允许合作伙伴的加入(不涉及用户隐私的情况下或征得用户同意)。“云安全”可以是个开放性的系统,其“探针”应当与其它软件相兼容。

3　存在的问题

3 1 用户的隐私安全不能得到确保

信任问题是“云安全”发展过程中的大障碍。虽然安全厂商宣称其只是“从用户机上发现可疑文件并自动上传”,但谁又能保证机器上的个人隐私,甚至公司商业机密也被当作“可疑文件”被上传了呢?在“云安全”模式中,谁能保证收集主机信息的合法性呢?又有谁能够对此进行监督呢[8]?在 SYMANTEC的服务条款中很清楚的写道, SYMANTEC不会将 Norton CommunityW atch中存储的数据与 SYMANTEC为了促销目的而收集的任何数据、联系人列表或订阅信息进行汇总。如果法律要求或许可,或者根据传讯或其它执法过程要求,执法人员要求公布收集的信息, SYMANTEC此时可能会公布此信息。也就是说,到底收集了用户什么样的信息,收集后怎么处理,必要时会不会交给安全部门,用户是完全没法知道的。这样的隐私保护政策,极易引起用户更大的恐慌。

更让人担心的是,“云时代”让国家、民族之间的界限变得越来越模糊,任何一个处于其中的国家都很难保持自身“云系统”的独立性。一旦国际形势突变,国外的云服务提供商与政府、军方合作,那么受“云安全”系统保护的重要单位将处于严重的危险之中。

3 2 自动分析的准确性不足

“云安全”的最大的优势就是快速捕获样本提交到安全厂商进行分析,可是面对海量的可疑文件,自动分析和人工分析如何结合起来?“云安全”又如何解决误报问题?

目前“云安全”的实际价值仅体现在厂商处理互联网威胁能力增强,响应时间缩短,但依然无法实现全自动检测、预警及分发,整个过程都需要人或多或少的干预。相对普通的应用,安全厂商对新型的病毒及攻击行为的分析,更多的是依据人工分析,如何缩短响应时间成为关键。其次,如何加强自动分析的准确性,也是安全厂商亟待解决的问题。曾经轰动全国

的诺顿误杀事件就是一个例子。虽然病毒样本自动搜集和处理系统必然会大大提高杀毒软件的病毒库样本搜集数量和升级速度,但每天从终端用户搜集上来的可疑文件多数可能并非病毒,如果自动搜集系统自动提交特征并加入病毒库的话可能会引起误报误杀的问题。

3.3 “云安全”服务器安全隐患影响巨大

“云计算”是建立在一个巨大的网络基础之上,“云计算”无法得到大规模应用,网络无疑是最重要的因素之一。对于“云安全”来说,这种局限表现得更加明显。网络安全服务完全转移到“云”上,那么用户将不得不接受这样的风险:一旦用户的网络发生状况或者遭受网络攻击导致用户无法连接到“云端”,那么这时的用户无疑是很脆弱的,遭受网络攻击的可能性也将大大增加[9]。去年发生的全国十多个省、市断网事件证明了这种风险存在的可能性。

从最近几年的安全形势来看,针对杀毒软件自身的攻击明显增多,很难想象的是,一旦在“云时代”安全服务被移到“云端”,那么这些杀毒软件如何确保自身安全都会成为一个难题。一旦“云安全”探针和“云安全”服务器自身出现安全漏洞,那么整个“云安全”的体系会经受严重挑战,甚至变成助纣为虐。

3.4 “云安全”技术标准不统一

“云安全”目前在业界产生如此大的争议和分歧,并让很多人感到迷惑,一个重要原因在于,虽然都被称为“云安全”,但每个厂商对“云安全”的理解都不一样,因此,所采用的技术手段和商业模式也完全不同。现在业内并没有统一的标准,各个厂商仍在各自为战,各有各的标准,客户端可能会得到不同的判定结果,这对未来的“云安全”统一是非常不利的。不仅标准混乱,各个厂商的云端服务器也没有做到统一,都是各自收集客户端信息,这样难免会造成收集信息不全的情况,导致最终的保护也不够完善。

4 解决的办法

4.1 建立统一标准的“云端”服务器

“云安全”需要一个开放性的安全服务平台作为基础,它为第三方安全合作伙伴提供与病毒对抗的平台支持,使得缺乏技术储备与设备支持的第三方合作伙伴,也可以参与到反病毒的阵线中来,摆脱目前反病毒厂商孤军奋战的局面[11,13]。政府应组织所有的杀毒厂商建立一个联盟,订立一个通用的协议,统一的恶意代码检测规则、安全事件处理、恶意网站识别规则和可疑文件搜集,共建一个“安全云”。这个“安全云”就是一个病毒库的提供商,无疑会成为世界上最大的病毒库,所有的安全厂商都可以通过接口连接到“云端”进行安全检测。各个安全厂商可以将精力和资金用在保护客户端安全的研发上,听取用户的意见使得产品功能更完善,而不用紧盯着病毒代码的发现。以互联网为例,除了技术上大家共同遵循的 RFC(请求注解)开放标准以外,在服务上则是百花齐放。

4.2 多种自动分析技术与人工分析结合

自动分析识别判定的依据主要有两个,一个是程序自身的行为分析权值分析完毕相加后是否符合将其界定为一种新出现的恶意程序的标准,另一个则是用海量客户端提交的数目来做判断。因此,为了节省时间和效率,并提高智能分析服务器平台的机动灵活性,可以将第二种判别机制上升为最高优先级。另外,“云安全”服务端采用多种鉴定方法,包括虚拟机、启发式分析、沙盒技术、动态行为分析、API序列分析等,新的分析方法不断改进和增加。多种分析方法并行、相互纠错,这些鉴定方法对病毒作者来说,是完全不可见的,他们无法知道“云安全”服务器端是用何种手段在对付病毒木马,也就无法拿出针对性的绕过或反制手段。

自动分析系统需要病毒分析员不断总结对程序的判断经验,通过这些相关的恶意程序进行分析,可以不断地更新自动判断逻辑,以提高自动分析系统判断的准确性,以及它识别恶意程序的能力。并且通过监控这些恶意程序的相关变化,分析人员可以为“云安全”客户端提供防御策略以及启发特征、行为特征,以提高云安全客户端的防御能力。

4.3 “云安全”与传统防病毒结合

“云网络”的健壮性和自我安全性是厂家服务网络的一部分,这是一个基础组成部分,是一个前提。每一个厂家都应该在构建“云网络”时就应该同步部署其健壮保护体系,作为服务网络,这是不可分割的。当前还没有专门针对“云环境”的安全威胁,对于云的保护,主要是对于“云端”服务器而言,保障这部分安全主要依靠传统的网关、防火墙、容灾备份和为云设置监控系统等措施。

“云安全”对传统杀毒模式的影响也不会在一朝

一夕就能完成。虽然传统的病毒防范模式具有一定局限性,但是优点也很突出,就是准确度和处理质量都很高。对于局限性,目前很多安全厂商也已通过添加其他的安全模块,如:启发式分析、主动防御、IDP系统(Intrusion Detection & Prevention System,入侵侦测防御系统)等进行了有效的提升。“云安全”仍然不足以也没有必要使安全产品完全脱离传统模式,应该将两者有机地结合起来,既能对目前通过挂马、移动存储介质等渠道进入计算机的未知威胁进行拦截,又能对通过其它渠道或手段已经进入到用户计算机中的未知威胁进行感知,同时也能保证用户即使在断网的情况下仍能享受到安全的保护。

4.4 防毒与杀毒齐头并进

当前众多挂马网站已经超越移动存储成为病毒木马的集散地和发源地,潜伏在网站里的众多病毒木马借用户访问网站之机渗入个人计算机。虽然各安全厂商的“云安全”大大提高了用户对病毒木马的防御能力,但其效果毕竟是有限的。因为他们忽视了作为病毒木马“毒源”的网站的安全,这些挂马网站即使被安全软件拦截并弹出警告,仍有不少用户选择继续浏览。

而“用户——网站——安全厂商”三位一体式的“云安全”系统,可以有效解决作为病毒木马“毒源”的众多中小网站安全问题[14]。一旦服务器被植入木马,安全厂商应立刻通知网站管理员,帮助网管实时监控自己的网站安全状况,并去除植入的恶意代码、木马等,而不单单仅是将网站放入黑名单。同时应该通知服务商、搜索引擎等合作伙伴,此时合作厂商应对其源地址进行屏蔽,让其无法在网络中感染,只有这样才能达到真正的互联网化的“云安全”。如图 1所示。

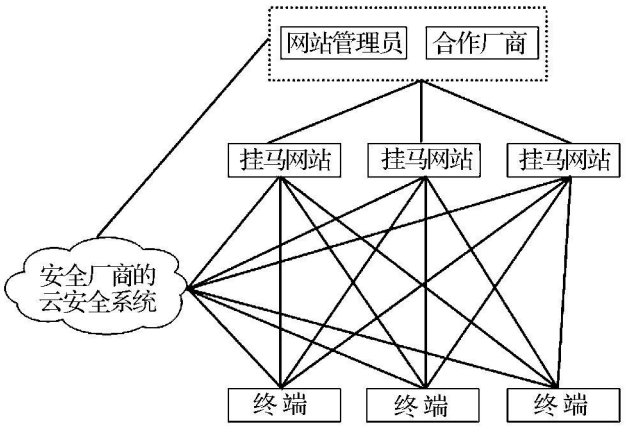

图 1 “三位一体”的“云安全”联动系统

5 结束语

由上可见,“云安全”并不是一种纯粹的反病毒技术,可以将其理解为一种反病毒理念,一种安全互联网化的思路,一个互联网化的安全防御体系,也就是杀毒软件的互联网化。

云安全技术仍处在发展阶段,标准化和规范化的统一需要大家共同的努力,在各大安全厂商技术不断创新的发展趋势下,云安全会随着用户的需求而发展变化。未来的云安全系统应为每一个电脑用户提供个性化的可疑文件识别、安全检查等服务。

参考文献:

[1] 游向峰. 打造安全的网络环境之“云安全”[J]. 计算机安全技术, 2009, 15(10): 97-98.

[2] 付江. 解读两种云安全模式 2009年迈向 2.0时代[EB/OL]. http://news.csdn.net/n/20090306/123835.html, 2009-03-06.

[3] ZDNet China 云安全技术架构不完全报告[EB/OL]. http://security.zdnet.com.cn/security_zone/2008/0723/1006514.shtml, 2008-07-23.

[4] 胡伟俭. 浅谈云计算在反病毒软件中的应用[J]. 牡丹江教育学报, 2009, 10(4): 101-102.

[5] 孙红. 论“云安全”在杀毒软件中的应用[J]. 信息安全与通信保密, 2009, 20(7): 56-58.

[6] Rising 有关云安全的五大问题和解答[EB/OL]. http://it.rising.com.cn/new2008/Safety/NewsInfo/2008-12-15/12293228222d50859.shtml, 2008-12-15.

[7] 姚远耀, 张予民. 云计算在网络安全领域中的应用[J]. 科技广场, 2009, 25(7): 86-88.

[8] 张琦. 云安全能否实现“全民防毒”? [J]. 信息系统工程, 2009, 16(1): 26.

[9] 赵鹏, 齐文泉, 时长江. 下一代计算机病毒防范技术“云安全”架构与原理[J]. 网络与通信, 2009, 10(6): 67-71.

[10] 王力, 解林冬, 王军委, 等. 病毒武器与网路战争[M]. 北京: 军事谊文出版社, 2001.

[11] 刘炯. 站在“云”端看安全[N]. 中国计算机用户, 2009-03-23(62).

[12] 吴珍. 漫步云端一探秘云安全[J]. 信息安全与通信保密, 2008, 9(11): 16-18.

[13] 胡晓荷. “云安全”将给用户带来什么[J]. 信息安全与通信保密, 2008, 9(12): 75.

[14] 苏熠渊. 瑞星“云安全网站联盟”:网站跨入“云安全”时代[EB/OL]. http://news.newhua.com/news1/safe_industry/2009/97/099713174524ECJH6DBE4GKI6DJA4IBJ6E4I3BDJ703G9I990D3F502K.html, 2009-09-07.