下一代计算机病毒防范技术“云安全”架构与原理

The Next Generation of Computer Virus Prevention Technology “Cloud security” Framework and Principle

赵 鹏* 齐文泉 时长江

ZHAO Peng QI Wen-quan SHI Chang-jiang

doi:10.3969/j.issn.1672-9528.2009.06.014

摘 要 云安全网络防护解决方案是杀毒软件的一种全新理念,是未来杀软技术发展的必然趋势,和传统方式相比,它可以在最新威胁到达用户计算机或公司网络之前对其予以拦截,从而让安全变得更加智能。山东出入境检验检疫局一直采用三层架构的计算机网络防病毒体系,有效阻挡查杀了各类恶意代码近十万余种。本文对云安全技术进行了详细研究与分析,目的是为山东检验检疫局构造全新的防病毒体系,从源头切断病毒的传播途径,从而保证各种业务系统更加安全稳定运行。

关键词 云计算 云安全 分布处理 并行处理 网格计算 信誉评估

Abstract Cloud security solutions for network protection is a new antivirus software philosophy, which was the next to kill soft inevitable trend of technological development, and the more traditional method, which can arrive in the latest threat to a user's computer or corporate network to be intercepted before it, thereby so that security becomes more intelligent Shandong Exit Inspection and Quarantine has been using a three-tier computer network anti-virus system, effectively blocking all types of malicious code has been killing hundreds of thousands more than the past In this paper, cloud security technology research and analysis in detail for the purpose of Construction Inspection and Quarantine Bureau of Shandong new anti-virus system, cut off from the source route of transmission of the virus, thus ensuring a variety of business systems more safe and stable operation.

Keywords Cloud computing Cloud security Distributed computing Parallel computing Grid computing

前言

在云计算、云存储大热的今天,云安全也出现了,而云安全的核心在于超越了客户端拦截 Web威胁的传统方法,转而借助威胁信息汇总的全球网络。云计算由网络技术,网格技术,并行分布式计算等技术发展而来,并发、分布是“云计算”的关键,而云安全也是由云计算演变而来。

“云安全”,顾名思义,就是借助“云计算”的理念应用在安全领域,综合国内外各家防病毒软件厂商对云安全的解释,可以理解为将用户和杀毒厂商技术平台通过互联网紧密相连,组成一个庞大的恶意代码监测、查杀、追踪网络,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,通过动态对被访问信息的安全等级进行评估,在恶意代码侵入网络之前,在源端直接将其阻止,再把恶意代码的解决方案分发到每一个客户端。从而达到零接触、零感染的防护价值,每个用户都为“云安全”计划贡献一份力量,同时分享其他所有用户的安全成果。“云安全”一句话描述,互联网就是一个巨大的“杀毒软件”,参与者越多,每个参与者就越安全,整个互联网就会更安全,云安全是下一代安全技术架构,是网络时代信息安全的最新体现,甚至是安全发展的必然出路,它将随着云计算的发展而进一步被推动,并最终为用户的互联网安全带来益处。

1 恶意代码现状分析

今天的网络威胁频繁地把大量看似无害的恶意程序组合在一起以形成感染链。例如,经常被网络威胁利用的单个下载器程序可能看似无害,但是当它们用来把恶意代码下载到一个毫无防备的用户的计算机上时,该程序就会变成恶意程序,基于文件的启发式扫描对此将无能为力。网络威胁经常会把这种技术扩大到多层、多协议的协调式攻击,以避免被传统安全方式发现[1]。例如,网络犯罪分子在电子邮件或即时信息中嵌入 URL链接,如果用户点击了某个被网络犯罪分子于几天或几小时之前攻击的合法URL的链接,则 ActiveX控件将测试用户浏览器的漏洞,如果发现了漏洞,恶意代码就会发起攻击。如果没有,则会下载一个文件,测试其它漏洞,或者再下载其它文件,不断重复测试。每个单独的部分均看似无害,但是联合起来就变成了协同攻击。单一的安全解

*山东出入境检验检疫局科技处信息中心 266001

决方案不再能囊括网络威胁的方方面面,这种攻击是目前市场所有防病毒软件无法解决的。

一组数据足以说明利用传统代码比对技术的防病毒软件所面临的窘境:今年第一季度相比 2005年第一季度,Web威胁增长了 1731%;据 AV - Test org的最新统计,全球恶意程序总数更是超过 1100万个。因此,单靠传统的扫描安全解决方案将不再能够针对恶意 Web威胁提供有效的保护,现在需要的是多层、多组件的灵活的可适应技术来应对当今高度复杂的序列式混合威胁。传统安全技术正面临一次新的革命,今天的信息安全正处在一个关键的转折点上,而云安全正是在这一种背景下诞生。

2 “云安全”的工作原理

纵观防毒技术二十年的发展,就会发现传统的代码比对技术多年来一直走的是解毒路线,即只有当部分用户中毒并反馈后,杀毒企业才能解码防护。但是在 Web威胁成为真正主要的安全隐患之后,大量且具有针对性的隐秘式攻击使得解毒的方式防不胜防,同时,特征码的激增大大影响了客户端的负载。而云安全的核心在于超越了客户端拦截 Web威胁的传统方法,转而借助威胁信息汇总的全球网络,在 Web威胁到达网络或计算机之前即可对其予以拦截,真正做到了防毒而非解毒。[2]

其实说到云 in - the - Cloud,是必定与主动防御 Proactive联系在一起的,大家去搜索这两个单词一定会大有斩获。主动防御和云安全其实是一回事。大家都在 Internet中,就好像在一团云中,目前防病毒采用的是被动打补丁的方式,也就是说发现了什么特征码,防病毒厂商就把它加入特征库,然后你的杀软就自动下载了。主动防护不需要在客户端安装特征码,但会有一个类似监控和报告的终端软件,随时从中央数据库获得和发送信息。比如你要浏览雅虎,你的客户端会先请示服务器,服务器认为雅虎安全,你就可以访问了,反过来,某天雅虎被人挂马,那么总有第一个访问它并中毒受害的人,此受害人的客户端随即向服务器发出警告,那么第二个请求访问雅虎的人即被提示告警信息。这样客户端就不用忙于下载各种特征库了,云结构就是一个大型的 CS架构。

云安全通过把大多数特征码文件保存到互联网云数据库中,并令其在客户端保持最低数量,使得在 Web威胁、电子邮件威胁和文件威胁到达最终用户或公司网络之前对其予以拦截。通过推出在云中的快速实时安全状态“检测”,这种方式降低了对端点上下载传统特征码文件的依赖性,同时减少了与在公司范围内部署特征码有关的成本和管理费用。如图 1。

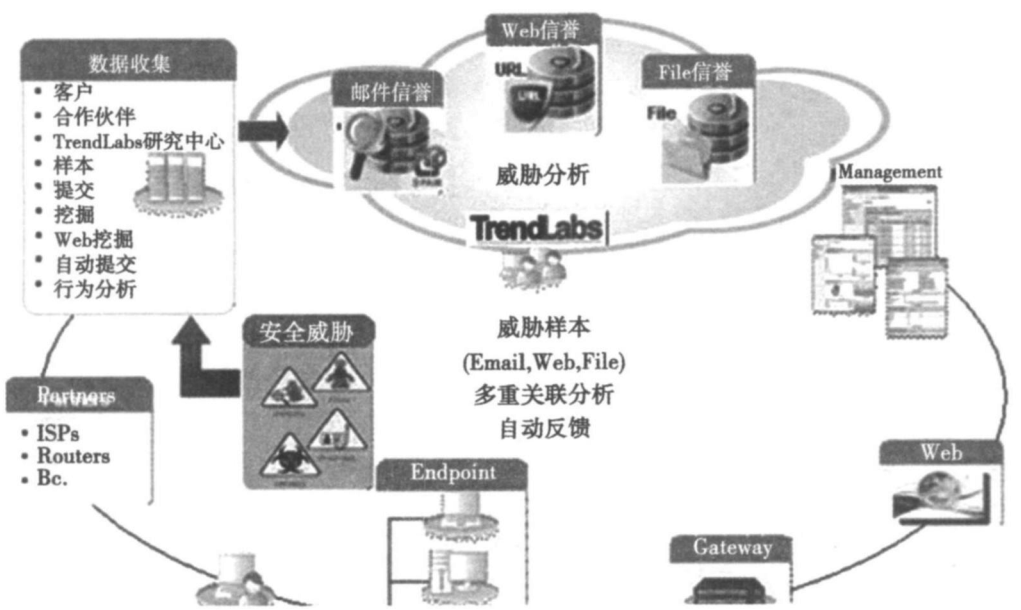

图 1 趋势科技云安全技术架构图

3 云安全核心要素

3.1 Web信誉服务

借助全球信誉数据库,云安全可以按照恶意软件行为分析所发现的网站页面、历史位置变化和可疑活动迹象等因素来指定信誉分数,从而追踪网页的可信度。然后将通过该技术继续扫描网站并防止用户访问被感染的网站。为了提高准确性、降低误

报率,安全厂商还为网站的特定网页或链接指定了信誉分值,而不是对整个网站进行分类或拦截,因为通常合法网站只有一部分受到攻击,而信誉可以随时间而不断变化。

通过信誉分值的比对,就可以知道某个网站潜在的风险级别。当用户访问具有潜在风险的网站时,就可以及时获得系统提醒或阻止,从而帮助用户快速地确认目标网站的安全性。通过 Web信誉服务,可以防范恶意程序源头。由于对零日攻击的防范是基于网站的可信程度而不是真正的内容,因此能有效预防恶意软件的初始下载,用户进入网络前就能够获得防护能力。

3.2 电子邮件信誉服务

电子邮件信誉服务按照已知垃圾邮件来源的信誉数据库检查 IP地址,同时利用可以实时评估电子邮件发送者信誉的动态服务对 IP地址进行验证。信誉评分通过对 IP地址的"行为"、"活动范围"以及以前的历史进行不断的分析而加以细化。按照发送者的 IP地址,恶意电子邮件在云中即被拦截,从而防止僵尸或僵尸网络等 Web威胁到达网络或用户的计算机。

3.3 文件信誉服务

文件信誉服务技术,它可以检查位于端点、服务器或网关处的每个文件的信誉。检查的依据包括已知的良性文件清单和已知的恶性文件清单,即现在所谓的防病毒特征码。高性能的内容分发网络和本地缓冲服务器将确保在检查过程中使延迟时间降到最低。由于恶意信息被保存在云中,因此可以立即到达网络中的所有用户。而且,和占用端点空间的传统防病毒特征码文件下载相比,这种方法降低了端点内存和系统消耗。

3.4 行为关联分析技术

通过行为分析的"相关性技术"可以把威胁活动综合联系起来,确定其是否属于恶意行为。Web威胁的单一活动似乎没有什么害处,但是如果同时进行多项活动,那么就可能会导致恶意结果。因此需要按照启发式观点来判断是否实际存在威胁,可以检查潜在威胁不同组件之间的相互关系。通过把威胁的不同部分关联起来并不断更新其威胁数据库,即能够实时做出响应,针对电子邮件和 Web威胁提供及时、自动的保护。

3.5 自动反馈机制

云安全的另一个重要组件就是自动反馈机制,以双向更新流方式在威胁研究中心和技术人员之间实现不间断通信。通过检查单个客户的路由信誉来确定各种新型威胁[3]。例如:趋势科技的全球自动反馈机制的功能很像现在很多社区采用的"邻里监督"方式,实现实时探测和及时的"共同智能"保护,将有助于确立全面的最新威胁指数。单个客户常规信誉检查发现的每种新威胁都会自动更新趋势科技位于全球各地的所有威胁数据库,防止以后的客户遇到已经发现的威胁。

由于威胁资料将按照通信源的信誉而非具体的通信内容收集,因此不存在延迟问题,而客户的个人或商业信息的私密性也得到保护。

3.6 威胁信息汇总

安全公司综合应用各种技术和数据收集方式——包括"蜜罐"、网络爬行器、客户和合作伙伴内容提交、反馈回路。通过云安全中的恶意软件数据库、服务和支持中心对威胁数据进行分析。7×24小时的全天候威胁监控和攻击防御,以探测、预防并清除攻击。

3.7 白名单技术

作为一种核心技术,白名单与黑名单(病毒特征码技术实际上采用的是黑名单技术思路)并无多大区别,区别仅在于规模不同。AVTest org的近期恶意样本(Bad Files,坏文件)包括了约 1200万种不同的样本。即使近期该数量显著增加,但坏文件的数量也仍然少于好文件(Good Files)。商业白名单的样本超过 1亿,有些人预计这一数字高达 5亿。因此要逐一追踪现在全球存在的所有好文件无疑是一项巨大的工作,可能无法由一个公司独立完成。

作为一种核心技术,现在的白名单主要被用于降低误报率。例如,黑名单中也许存在着实际上并无恶意的特征码。因此防病毒特征数据库将会按照内部或商用白名单进行定期检查,趋势科技和熊猫目前也是定期执行这项工作。

4 云安全工作步骤

假如您收到了一封含有网络链接的恶意电子邮件,云安全将根据以下步骤进行分析查杀:

a、首先,"云安全"将截取该邮件,采用邮件信誉服务数据库检查其发送源 IP地址;

b、如果其地址属于垃圾邮件发送源,那么该电子邮件将在连接层被阻止;

c、接下来,"云安全"将采用 Web信誉服务数据库检查邮件中的链接,保证用户不能随意打开恶意链接;

d、除此之外,网页中的组件和相关的重定向网页也会被自动下载并对其加以分析;

e、链接中的 IP信息也会被提取并分析;

f、结果会被立即添加到基于互联网的交互式威胁数据库中;

5 目前业内杀软"云安全"技术比较分析

现在各个杀毒软件厂商都在热炒"云安全"概念,其中炒的最响的是瑞星和趋势。

第一阵营:趋势科技

趋势科技的"云安全 Secure Cloud"主要用于企业级产品当中,强调的是对复合式攻击的拦截和轻客户端策略,最终目的是让威胁在到达用户计算机或公司网络之前就对其予以拦截。

趋势的云安全可以概括为基于互联网数据库的轻客户端程序,也就是构架一个庞大的黑白名单服务器群,用于客户端的查询。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,无法对已经存在本地计算机上的未知威胁进行感知。从趋势的"云安全"概念中可以看到,其主要是对外来威胁进行组合、判断、拦截。但一旦有未知病毒或威胁通过其它渠道入侵到用户的计算机当中,趋势是无法对已经在本机的安全威胁有效感知的。

第二阵营:瑞星

瑞星"云安全"官方给出的定义:通过网状的大量客户端对网络中软件行为的异常监测,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,然后再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"和趋势的"云安全"讲述的并不是同一个概念。趋势"云安全"中的"云"是趋势的服务器群,而瑞星的"云"则是大量用户。在瑞星的云安全当中,瑞星的服务器反倒成了一个 Client端。通过各个客户端对用户计算机进行扫描,然后提取可能是病毒的文件上报,经过瑞星的处理后,升级杀毒软件或卡再推送给用户。

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,另外需要有对病毒的快速分析处理能力。在瑞星云安全里,由于客户端才是云的组成部分,所以不需要架设那么多服务器。瑞星的云安全特点是能够感知用户计算机上已经存在的未知病毒,思路还是好的,但瑞星是否有能力真正的达到云安全设想的目标,就需要用时间去检验了。

瑞星的云安全也有自己致命的缺陷,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,可以说是"事后诸葛"。

6 总结

从上面的分析我们可以看出,趋势和瑞星都提出了"云安全"概念,但两者所指并不是同一个东西。趋势的云安全强调阻止外来威胁,需要大量的服务器(厂商);瑞星的云安全则强调对用户计算机上已经存在的未知威胁进行感知,需要有大量的客户端(用户)。它们代表了两大阵营,许多厂商也都在迅速跟进。但两者目前都存在缺陷,趋势忽略了对本机未知威胁的感知、收集,而瑞星则只能被动防守,不能在未知威胁进入到电脑前进行拦截。而且云安全还存在以下问题:

第一,互联网瘫痪了怎么办;

第二,云端服务器的安全性怎么保障;

第三,有些病毒通过在线查杀的方式是无法彻底清除的;

第四、杀毒的滞后性,病毒的解决方案是在病毒出现后才开发出来,那么对于还未开发出杀毒代码的新病毒则无能为力。

综合看来,云安全目前还处于一种概念状态,只是传统的病毒防范模式在病毒样本搜集方面的进步,将以前的手动分析更新病毒样本改为系统自动更新升级,将人工分析改为系统自动分析的缺点就是可能会产生严重的误报误杀问题,因此,再智能化的东西可能也存在误差,"云安全"离开人工干预和完善的测试环节,可能带来不安全隐患。离开人工干预的"云安全"并不适用于企业,企业用户更加注重系统的可持续运行和业务的不间断,而完全自动的"云安全"目前并不能让人放心。

我们到底需要什么样的云安全?我个人认为,"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,应该将两者有机的结合起来,即能对目前通过挂马、优盘等渠道进入计算机的未知威胁进行拦截,也要对通过其它渠道(手段)已经进入到用户计算机中的未知威胁进行感知。

目前山东出入境检验检疫局防病毒体系采用趋势科技网关 IWSA、网络层 NVW,终端 OSCE8.0立体防范技术,所有软硬件已具备强大的病毒扫描引

车辆与通讯

Vehicle and Communication

初国新* 刘 悦 李宝珠

CHU GuoXin LIU Yue LI Bao-zhu

doi:10.3969/j.issn.1672-9528.2009.06.015

摘 要 随着社会的发展和经济的提高,车辆已经成为生活中不可缺少的交通工具,但是过多的车辆也会带来许多新的问题,如交通阻塞,交通事故等,这些问题吸引了大量的研究,其中的车辆自组织通讯网络 VANET(Vehicular Ad hoc Network)的提出成为了当前研究的热点,文章就 VANET相关研究进行分类,并且提出了一种新的基于网络负载的路由策略,文章最后提出了车辆相关技术的发展方向。

关键词 自组织 网络负载 路由 策略

Abstract With the social development and economic improvement, vehicle has become an indispensable tool in daily life, but so-many vehicles also bring lots of new problems, such as traffic congestion, traffic accidents. These problems have attracted a lot of research, in which the presentation of VANET (Vehicular Ad hoc Network) turns into current top research. Paper not only provides the classification of related research on VANET, but proposes a new network-load based routing strategy, finally paper puts forward future development of related technology.

Keywords Ad hoc Nnetwork load Routing Strategy

1 引言

随着车辆的智能化,越来越多的车辆和公路边的基础设施都开始装备通信设备,如不久的将来,车辆需要能够在一个暂时的、自组织的、快速变化的无线移动网络中进行通信;同时,这些车辆还应能访问公路边的网络设施。因此,诞生了车辆网络[1](vehicular network)这个新概念。这种车辆网络也被称为车辆 Ad-hoc网络(VANET),它作为“智能交通系统(intelligent transportation system)”的重要组成部分,以及无线移动网(MANET)的一种特殊应用,已经得到越来越多的重视。其最重要的特点是能进行车与车之间(IVC)和车与路之间(RVC)之间的信息交换,从而达到车辆与车辆之间、车辆与路边的基础设施之间的实时通信,利用这些信息来实现道路交通的安全与高效,VANET的发展依赖社会经济和科技水平,VANET在许多发达国家已经得到了广泛的应用。

2 研究分类

车辆网络技术的发展分为硬件和软件协议方面。其中硬件是研究的基础,而软件协议则是要在硬件的基础上进行重组和优化。

2.1 软件

软件方面主要是通讯协议的发展,近年许多国家都致力于协议标准的研究。其中,欧洲多国合作开展的 Fleenet[2]项目,美国加利福尼亚大学等部门联合开发的 PATH[3]项目,此外还有德国的“Network on Wheels”[4]都是致力于 VANET的工程项目,而协议标准的研究也主要分为两类:网络层和 MAC层。

2.1.1 网络层

VANET的拓扑结构的快速变化给路由协议的设计带来了很大的挑战,而由于定位技术的提高使

*济南大学信息科学与工程学院 济南 250022

擎和病毒码对比技术,对已知各类恶意代码的查杀高达 99%,下一步再全面融合趋势科技的云安全技术,必将会为山东出入境检验检疫局打造更为安全健康的网络环境。

参考文献:

[1] 程胜利. 计算机病毒及其防治技术. 清华大学出版社, 2004.

[2] 新型病毒与新的反病毒策略. 2005.

[3] 喻凯. 病毒发展趋势及对策. 2005.

[作者简介] 赵鹏,山东出入境检验检疫局科技处信息中心网络安全工程师,思科 CCNA、趋势科技 TCSE,主要研究领域计算机网络信息安全、病毒防范、网站防篡改等。

(收稿日期:2009-05-05)