ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.7, No.11, April 2011,pp.2538-2539

E-mail: info@cccc.net.cn
http://www.dnzs.net.cn
Tel:+86-551-5690963 5690964

浅析杀毒软件中的“云安全”技术

曾德明

(泸州职业技术学院,四川 泸州 646005)

摘要:现阶段,国内和国外的网络厂商和安全专家都提出了“云安全”的概念,在“云安全”的基础上提出计算机安全的解决方法,并把“云安全”和杀毒软件结合在一起。该文主要阐述了对“云安全”技术在杀毒软件中的使用进行简要的分析。

关键词:杀毒软件;云安全;病毒;木马;网络安全

中图分类号:TP393 **文献标识码**:A **文章编号**:1009-3044(2011)11-2538-02

国内外计算机安全厂商及专家为应对计算机安全信息收到的挑战,把计算机从单机防御转变为整个网络防御的层面来对待,对各种资源进行协调,发挥网络资源的优势。从而提出“云安全”的概念及技术。

1 传统杀毒软件

历来都是先有病毒才会有针对性的杀毒,所以,病毒总是先于杀毒软件的,也因此,面对层出不穷的病毒,杀毒软件显得力不从心。究其原因,传统杀毒软件是以捕获新病毒来获取病毒特征,然后升级病毒库代码,然后用对比的办法来判断病毒是否存在。然而新病毒不断的出现,导致病毒库代码越来越多、越来越庞大。根据相关统计,全世界现存的恶意程序超过1100万个,根据分析,整个数据还会出现较大幅度的增长,这就意味着杀毒软件的病毒代码库越来越臃肿,庞大的病毒库代码占据了计算机资源及网络带宽。也就是说传统的升级病毒库的杀毒软件只是一种治标不治本的方法,很难适应计算机技术的发展,杀毒软件的防御能力也会呈现出下降的趋势,主要原因在于,杀毒软件是存在于一个独立的终端计算机中,防御的范围及手段都非常的有限,只能采取不断的更新下载、升级病毒代码库的方式进行防毒杀毒处理,从某种意义上说,这也只是迫不得已的补救措施,必然会导致病毒库越来越膨胀。所以,杀毒软件的现状必须要有一种全新的防御方式来支持或替代现在计算机病毒的威胁。

2 “云安全”概念

按照“计算机就是网络、网络就是计算机”的思维,对于传统的PC基础上的安全防护措施能否替代,构建一个互联网基础上的安全防护措施,把互联网变成一个强大的杀毒软件,让恶意程序无法下手,成为现在计算机安全比较关注的问题。如果有,那么单个的计算机就不会再为安装臃肿的杀毒软件而费心了,也不会因为没有及时更新病毒库导致病毒入侵、系统瘫痪,而造成不必要的损失,所有的防毒杀毒工作有全球范围的杀毒服务器来完成,节约了硬件资源,也降低了病毒威胁的风险。至此,“云安全”的概念被提出来了,它是结合了网格计算、并行处理、未知病毒判断的新兴概念和技术,主要是针对网络中的大量客户端的软件行为异常进行监测,从中获取网络中的病毒、木马及恶意程序的信息,然后传送到云服务器进行分析和处理,然后把病毒、木马和恶意程序的解决方案发送到各个客户端,客户端就成为了病毒的检测者,当然,也是“云安全”的受益者。基于这个思路,国内外各安全厂商也都提出“云安全”的概念,并展示了在“云计算”的基础上的安全方案,第一时间运用到杀毒软件中。截止此时,宣布网络安全“云”时代的到来。

3 “云安全”技术

该技术指的是能有效的防御现阶段网络威胁的一种安全技术。“云安全”技术是在“云计算”的机制上,对互联网上数据的安全程度进行动态的评定,并在云服务器端生成数据库。用户在访问互联网时,安全系统就会自动在云端数据库进行分析比对处理,并组织有威胁的信息进入网络。与传统的代码比对技术相比,“云安全”技术是对潜在的网络威胁进行防御,从防护的时间上提前了,对恶意程序实现了光谱防护。“云安全”技术的核心理念就是,借助分散于全球各地的威胁信息汇总服务器,在安全威胁尚未到达网络终端之前就将其拦截,也就是所谓的零感染防护。“云安全”技术的具体操作构成是:在访问某网页时,请求首先被安装在计算机中的安全系统发送到云端服务器,云端服务器进行分析判断该网页信息的安全级别,对安全级别高的网页自动放行,而对安全级别较低的网页则在用户界面给出风险提示。如果云端服务器没有该网页的数据信息,用户仍可顺利访问此页,同时云端服务器会把网页的信息发布到就近在线服务器,由众多云服务器进行分析综合评定页面风险等级。然后,其他用户在访问该页面时就会得到保护。“云安全”技术理论上对每一个网站都会进行信誉评价,保存在服务器中,这样就提高了用户在访问互联网时的安全性。所以,“云安全”系统在互联网中的建立,给每一个网页都进行信誉度和病毒库的记录,类似于给每台计算机都增加了一个“云安全”的防火墙,完全的阻断了互联网中的一些恶意程序的蔓延。

4 “云安全”技术的应用

4.1 瑞星公司的“云安全”系统

简单的说,“云安全”是一个庞大的系统,是在杀毒软件网络化的具体实现。瑞星“云安全”主要包含三部分内容:数以亿计的客

收稿日期:2011-02-04

户端、与数百家互联网公司合作、指定“云安全”服务器。瑞星卡卡、瑞星 2009 等上网安全工具中集成了“云安全探针”,只要用户的电脑安装有这些软件,那么用户的电脑就成为瑞星“云安全”系统的客户端。瑞星的“云安全”计划则是对其公司旗下的多款软件植入“云安全探针”的功能,电脑只要安装该软件,也就成为瑞星“云安全”的客户端。“云安全探针”可以检测到电脑中的安全信息,比如用户访问带病毒的网页、木马开始运行文件并对注册表关键位置的修改等,“云安全探针”就会把信息直接上传到瑞星“云安全”服务器,然后进行分析,对分析的结果直接加入“云安全”系统中,这样“云安全”的全部用户就可以对这些威胁及时的进行防护。

4.2 金山公司的“云安全”系统

为了解决木马商业化带来的互联网严峻形势,金山公司也推出了“云安全”系统,产生了一种全网防御的安全结构。金山“云安全”系统主要包括:集群式服务端、智能化客户端、和开放平台三个部分,金山“云安全”技术是在原有杀毒防毒技术上的补充和强化,其目的是为了互联网能更全面更快的保护用户的利益。首先,服务端的支持。它是在金山海量的存储中心基础上,智能的分析挖掘技术下的安全分析服务,并与客户端相互协作,提供给用户优质的“云”服务。其次,高效稳定的智能客户端。金山“云安全”客户端既可以是独立的也可以是集群的,;例如金山毒霸 2009 是独立的客户端,而百度安全中心则是金山“云安全”的集群客户端,客户端为“云安全”系统提供了威胁处理和收集样本的功能。最后,金山“云安全”有一个开放性的服务平台,提供给第三方安全合作伙伴一个与病毒对抗的平台。金山“云安全”不仅是提供给第三方一个安全的服务平台,同时也是与第三方相互合作建立全网防御的安全系统,这样,每一个用户都参与到对网络威胁的防御中来。

4.3 趋势科技公司的“云安全”系统

与瑞星“云安全”有所不同的是趋势科技公司推出的“云安全”技术,趋势科技“云”服务器群会对整个互联网的信息自动的进行动态分析,例如分析一个文件就会同时对这个文件的多种属性进行分析,这样就会使任何网络威胁在一出现就会被“云”服务器所共速分析,在进入网络之前,就被拦截,保护了互联网的安全。趋势科技“云安全”技术最大的好处是降低了病毒对下载传染的依赖性,此外,也降低了用户宽带的消耗。现在,趋势科技已经在全球范围建立了 5 个数据中心和几万个在线服务器,可靠性达到99.9999%。现在,每天可以收集 2.5 万个样本、处理 55 亿条查询,请求命中率高达 99%。在“云安全”技术基础上,趋势科技每天可以对 1000 万次的病毒攻击进行阻断。趋势科技“云安全”技术通过动态分析对网络访问信息进行安全等级评估,把隐患消灭在源头,大大提高了网络的安全性。

5 建立“云安全”系统的难点

5.1 需要海量的客户端

对互联网中的木马、病毒最迅速的感知需要海量的客户端。目前瑞星、金山等多家安全厂商已经拥有大量的独立客户端,加之与迅雷、久游等多家合作伙伴组成的集群客户端,“云安全”的覆盖率也在不断的扩大。

5.2 需要专业防毒技术和经验

瑞星、金山等公司自成立以来多年的防毒技术不断的积累,技术力量也达到了一定的水平。瑞星、金山等公司的“云安全”技术目前也能够及时的处理大量的信息,处理信息的结构也在“云”系统中不断被分享。

5.3 开放的系统

瑞星、金山及趋势科技等公司的“云安全”系统都是开放性的系统,其软件的兼容性很强,即使在其他杀毒软件的基础上也能使用该软件,实现了软件的兼容,对“云安全”带来的成果实现共享。

6 结束语

总而言之,“云安全”目前是一个全新的安全概念,同时也是一个全新的安全模式,“云安全”技术的实施还需要安全厂商及用户对其充分的肯定,互相支持与合作,最终把互联网变成一个大型的杀毒软件,保护用户的网络安全。

参考文献:

[1] 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(7).
[2] 游向峰.打造安全的网络环境之“云安全”[J]. 电脑编程技巧与维护.2009(16).
[3] 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].信息技术与信息化.2009(6).
[4] 康斯坦丁.杀毒软件的“云”安全时代[J].信息系统工程.2009(2).

浅析杀毒软件中的"云安全"技术

作者：曾德明
作者单位：泸州职业技术学院,四川,泸州,646005
刊名：电脑知识与技术
英文刊名：COMPUTER KNOWLEDGE AND TECHNOLOGY
年，卷(期)：2011,07(11)
被引用次数：1次

参考文献(4条)

1. 孙红 论"云安全"在杀毒软件中的应用[期刊论文]-信息安全与通信保密 2009(07)

2. 游向峰 打造安全的网络环境之"云安全"[期刊论文]-电脑编程技巧与维护 2009(16)

3. 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[期刊论文]-信息技术与信息化 2009(06)

4. 康斯坦丁 杀毒软件的"云"安全时代[期刊论文]-信息系统工程 2009(02)

本文读者也读过(5条)

1. 祝国辉 云安全:从"杀毒"向"安全防御"转型[期刊论文]-中国制造业信息化2010(24)

2. 蒋国松.金徐伟.陈云志.高永梅.叶青青.JIANG Guo-song.JIN Xu-wei.CHEN Yun-zhi.GAO Yong-mei.YE Qing-qing 互联网病毒新趋势与防治策略研究[期刊论文]-计算机时代2011(3)

3. 张英鹏 如何选择杀毒软件[期刊论文]-职大学报2009(2)

4. 欧阳中辉.张晓瑜.涂帅.顾佼佼.OUYANG Zhong-hui.ZHANG Xiao-yu.TU Shuai.GU Jiao-jiao "云安全"在计算机防病毒应用中的问题研究[期刊论文]-计算机与现代化2010(12)

5. 吕海华.LV Hai-hua 云安全在安全网关中的应用[期刊论文]-沈阳工程学院学报（自然科学版）2011,07(1)

引证文献(1条)

1. 赵鹏.李剑 国内外信息安全发展新趋势[期刊论文]-信息网络安全 2011(7)