doi :10.3969/j.issn.1671-1122.2011.09.015

浅析云查杀与主动防御

高静峰

（厦门市美亚柏科信息股份有限公司，福建厦门 361000）

摘 要：文章通过介绍杀毒软件病毒防护技术的发展和特点，分析了云查杀技术和主动防御技术，然后针对当前这两种技术进行反思，提出了这两种技术目前存在的一些问题。

关键词：云查杀；主动防御；病毒防护；扫描技术

中图分类号：TP393.08 **文献标识码：**A **文章编号：**1671-1122（2011）09-0047-03

The Discussion of Killing Cloud and Active Defense

GAO Jing-feng

(*Xiamen Meiya Pico Information Co.,Ltd., Fujian Xiamen* 361000, *China*)

Abstract: The paper explains the development and characteristic of the virus protection technology of antivirus software. And it mostly explains the technologies of killing cloud and active defense. Then according to the thinking of the two technologies, the paper brings forward some problems about them.

Key words: killing cloud; active defense; virus protection; scanning technology

1 病毒防护技术的发展

病毒和反病毒软件的对抗最早可以追溯到 20 世纪 70 年代，当时一种名为“爬行者”的病毒出现在了 TENEX 操作系统上，当时 TENEX 操作系统的开发人员发现了这一问题，为了解决这个病毒对操作系统的影响，他们开发了一个名叫“收割者”的软件来专门对付它，这可能就是病毒和反病毒的第一次战争。

随着计算机的普及以及病毒技术的发展，病毒与反病毒技术之间的对抗也日益激烈，二者之间是矛与盾的关系。为了能及时有效地查杀各类病毒，病毒查杀技术也发生了翻天覆地的变化。进入 21 世纪，随着互联网的发展，各类网络应用层出不穷，黑客们为了获取最大的利益，不断研发新病毒和恶意软件，导致每天有大量的网民个人信息被窃取或者电子银行资金被盗窃，同时政府系统的电子政务网的网络安全也面临着极大的威胁[1]。

互联网已经成为病毒制作技术扩散、病毒传播的重要途径，病毒开发者之间已经出现了团队合作的趋势，病毒制作技术也在与黑客技术进行融合，他们对现在的病毒对抗技术提出了挑战。因此，病毒防护技术正在发生重大的变化，概括起来说，就是病毒对抗的理论在做从作品对抗到思想对抗的转变，产品形态在从独立软件产品向操作系统的补丁转变[2]。

1）从作品对抗到思想对抗。 以前，杀毒软件的理论基础是，首先要发现并确认一个病毒，然后再进行防范，它的缺点是，对未知病毒的防范能力弱，我们没有有效的办法对付各种病毒的变形。一般是一种新病毒发作后，大家才能开发出查杀该病毒的软件，用户还需要尽快升级自己的防毒软件，因此，可以说以前的方法就警察找罪犯，在警察没有看到罪犯犯罪，或得到举报前，即使罪犯犯了罪，警察也没有办法，这是一种病毒制造者与安全专家之间在作品层面的竞赛。而新的理论是基于对大量的病毒特征、发作过程、传播变化统计的基础上，建立控制策略数学模型，采取分门别类的方法，有效解决应用同种思想开发出的各种病毒，可以极大提高对新病毒的反应时间。由于这种方法是通过抑制病毒设计思想而实现的，因此，这是一种病毒制造者与安全专家之间在整体思想层面的竞赛。

因此，新的杀毒软件不仅仅是依据病毒数据库中的病毒代码对计算机进行扫描，而是对计算机所运行的各种进程、各种操作进行监控，如果发现某个事件或某项操作存在典型的病毒特征，或是对计算机存在危害，那么这些事件或操作就会被阻止，从而更有效地保护计算机不受新型病毒的入侵。

收稿时间：2011-07-15

作者简介：高静峰（1981-），男，福建，硕士，主要研究方向：网络信息安全、Windows 系统内核及相关 Rootkit 技术。

2）从独立产品到操作系统的补丁。杀毒软件作为一个独立的软件产品，已经存在了很久，但是，由于病毒制造者越来越多地利用操作系统的漏洞和黑客技术，因此，与操作系统的紧密结合成为一种必然：一方面，可以帮助操作系统减少漏洞，另一方面，也可以进一步提高运行效率和软件兼容度。从商业角度上来说，安全技术可以融入各种应用系统，减少应用系统自身的安全漏洞，同时，也可以为用户提供更加个性化的安全服务。

2 杀毒软件病毒查杀技术

随着病毒技术不断地更新发展，病毒种类越来越复杂，杀毒软件技术也急需变革才能对付庞大的病毒群。特别是这几年互联网的发展需求，杀毒软件作为互联网安全的基础保障，正面临着越来越严峻的考验。杀毒软件查杀病毒的技术主要分为以下几类：

1）基于特征码扫描的技术。该技术是杀毒软件采用最长久也最传统的一种病毒查杀技术，该扫描方式是一种静态扫描。这种方法是把分析出来的病毒特征码集中存放于特征库文件中，在扫描的时候将扫描对象与特征代码库比较，如有吻合则判断为染上病毒。特征代码法实现起来简单，对于查传统的文件型病毒特别有效，而且由于已知特征代码，清除病毒十分安全和彻底。但这种方法最大的局限性是过分依赖病毒代码库的升级，因为它对未知病毒和变形病毒没有任何作用。病毒代码库随着病毒数量的增加而不断扩大，搜索庞大的特征代码库会造成查毒速度下降。

2）启发式扫描技术。由于传统的特征码扫描技术存在着先天的不足，于是启发式扫描技术被引入到杀毒软件，其与特征码最大的不同是加入对程序调用相关 API 的评判机制。通常启发式杀毒引擎会内置一套评分机制，当一个未知病毒调用一系列 API 时，通过对这些 API 敏感程度的分析，以及相关 API 调用的相应顺序，对该程序可能的行为进行评分，当达到杀毒软件系统设置的危险等级临界值时，启发式扫描技术就会报警。通常启发级别越高，越容易产生误报。现在使用该技术的杀毒软件也不少，最典型的当属于 Nod32。如何设定评判机制，以及如何减少对具有敏感操作的正常软件的误报率将是该技术应该重点解决的一个问题。

3）文件信誉安全技术。该技术是一门新兴技术，是云安全 2.0 的核心。该技术有点类似我们熟知的黑白名单技术。首先排除了操作系统安全文件（白名单），杀灭已知低信誉的恶意程序（黑名单），在面对无法依靠黑白名单判断的文件时，利用网络上庞大的用户群为该程序的信誉打分，来判断此程序的威胁程度。与启发式判断有相似点，只是判断从打分机制转换为用户人为判断。应用该技术的典型杀毒软件有趋势科技和诺顿网络安全特警。

4）虚拟机查杀技术。虚拟机查杀技术即在电脑中创造一个虚拟 CPU 环境，将病毒在虚拟环境中激活，根据其行为特征，从而判断是否是病毒。有专家认为，所谓虚拟机技术，就是用软件先虚拟一套运行环境，让病毒先在该虚拟环境下运行，从而观察病毒的执行过程。这个技术主要用来应对加壳和加密的病毒，因为这两类病毒在执行时最终还是要自身脱壳和解密的，这样，杀毒软件就可以在其“现出原形”之后通过特征码查毒法对其进行查杀。

5）云查杀技术。“云安全（Cloud Security）”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，获取互联网中恶意程序的最新信息，传送到服务端进行自动分析和处理，再把相关的解决方案分发到每一个客户端。

6）主动防御技术。主动防御技术是近几年才发扬光大起来的实时防御技术，并非传统的文件监控技术。主动防御技术更追求的是智能 + 主动 + 拦截能力，而不需要对程序特征码进行扫描。主动防御技术的发动需要特定的条件，比如目标需要有活动和操作。误报程度和智能拦截能力是体现各产品差距的地方。

以上这些技术是目前杀毒软件常用的技术，每款杀毒软件一般都不会只局限于上面所提到的一种技术，都是集成几种技术的使用。

3 云查杀技术与主动防御技术

3.1 云查杀技术特点

在“云计算”被提出之前，有个很热的概念叫做“网格计算”，就是把大家的计算机联合起来，贡献出一些空闲的计算能力，供大家随时取用。Google 是“网格计算”最早的使用者之一，采用大量联合的廉价 PC 机来取代昂贵的服务器，以提供海量搜索要求的计算能力。其中的技术难点，就在于并行计算、服务器通讯技术。

随着云安全概念广泛地传播，云安全思想被应用到各个领域。在杀毒软件行业中，提出了云查杀概念并把该技术应用到病毒查杀。云查杀技术主要有以下几个特点：

1）海量的客户端（云安全探针）。只有拥有海量的客户端，才能对互联网上出现的病毒、木马、挂马网站等有灵敏的感知能力，及时收集相关病毒的特征码、行为以及恶意网站，上传到云安全中心进行智能分析。因此客户端数量的多少，很大程度决定着云查杀技术的质量和准确性。

2）专业的反病毒技术与经验。采用云查杀技术的杀毒软件，在本地客户端也会带有一个特征病毒库，这就需要拥有专业强大的反病毒技术才能提炼出这样一个特征库，才能在客户端本地及时查杀已被发现的病毒。同时客户端收集到的病毒特征、行为等等上传到云安全中心，在云安全中心也需要有一套智能查杀引擎，及时对上传上来的样本进行智能分析，提取

有效的查杀规则并及时更新到各个客户端。云安全中心样本的分析除了借助程序智能分析外，对于比较复杂的样本也需要配以人工分析，因此，反病毒技术强弱以及经验的丰富程度将影响杀毒软件的病毒查杀能力。

3）大量的技术投入和资金投入。与海量的客户端相对应，云安全中心也需要大量的服务器。这些服务器除了与客户端进行交互，收集客户端提交上来的样本外，还需要对这些样本进行智能分析，下发最新的病毒特征码。随着客户端数量的不断增加以及近几年病毒、恶意软件等呈几何倍数的增长，云安全中心服务器数量必然也要不断增加，同时对于网络带宽的要求也将大大提高，这些都需要投入大量的资金。服务器上的智能查杀引擎技术也需要不断完善，提高分析处理能力，这也需要不断地进行技术投入。

4)开放的系统。云查杀技术如果单单局限于杀毒软件当中，这是远远不够的。随着第三方应用软件大规模的发展，针对第三方软件漏洞的病毒和恶意软件也层出不穷，这让杀毒软件防不胜防。因此基于云查杀的杀毒软件将提供一个开放的平台，让第三方软件加入这个平台共享 " 云安全 " 系统的成果，这也将大大提高 " 云安全 " 系统的覆盖范围。

3.2 主动防御技术特点

主动防御技术主要是通过监视程序的行为来判断程序的危害性。程序运行时会调用各种应用编程接口 (API)，通过监控这些 API 的调用即可了解程序的运行状态，从而可以判断出程序的危害性 [3]。

国内最早提出主动防御概念的是东方微点创始人刘旭。2005 年，他把主动防御的思路发表在《光明日报》上，当时还引起了很大的争议。一些人认为先中毒后杀毒是天经地义的，另外也有人认为主动防御是天方夜谭。当时这个概念的提出引起了杀毒软件业界巨大的轰动，随着这几年的发展，主动防御技术已经被杀毒软件厂商所认同，也逐步应用到杀毒软件产品中。

主动防御是基于程序行为自主分析判断的实时防护技术，不以病毒的特征码作为判断病毒的依据，而是从最原始的病毒定义出发，直接将程序的行为作为判断病毒的依据。主动防御是用软件自动实现了反病毒专家分析判断病毒的过程，解决了杀毒软件无法防杀未知恶意软件和新病毒的弊端。在反病毒与病毒的对抗中，从技术上实现了对木马和病毒的主动防御。主动防御技术具有以下几个特点：

1）创立动态仿真反病毒专家系统。对病毒行为规律分析、归纳、总结，并结合反病毒专家判定病毒的经验，提炼成病毒识别规则知识库。模拟专家发现新病毒的原理，通过对各种程序动作的自动监视，自动分析程序动作之间的逻辑关系，综合应用病毒识别规则知识，实现自动判定新病毒，达到主动防御的目的。

2）自动准确判定新病毒。分布在操作系统的众多探针，动态监视所运行程序调用各种应用编程接口（API）的动作，自动分析程序动作之间的逻辑关系，自动判定程序行为的合法性，实现自动诊断新病毒，明确报告诊断结论；有效克服当前安全技术大多依据单一动作，频繁询问是否允许修改注册表或访问网络，给用户带来困惑以及用户因难以自行判断，导致误判、造成危害产生或正常程序无法运行的缺陷。

3）程序行为监控并举。在全面监视程序运行的同时，自主分析程序行为，发现新病毒后，自动阻止病毒行为并终止病毒程序运行，自动清除病毒，并自动修复注册表。

4）自动提取特征值实现多重防护。在采用动态仿真技术的同时，有效克服特征值扫描技术滞后于病毒出现的缺陷，发现新病毒后自动提取病毒特征值，并自动更新本地未知特征库，实现“捕获、分析、升级”自动化，有利于对此后同一个病毒攻击的快速检测，使用户系统得到安全高效的多重防护。

3.3 反思

云查杀技术和主动防御技术是最近几年炒得非常火的两个技术，它们也分别被各大杀毒软件厂商所采用。现在基本上所有杀毒软件都自称自己使用了主动防御技术和云查杀技术，自称自己的病毒和恶意软件查杀能力有多强，然而情况确实如此吗?

1）主动防御技术。传统的杀毒软件都是使用特征码扫描的方式来查杀病毒和恶意软件的，安装杀毒软件的机器都带有一个庞大的特征库。目前，市面上大部分自称已具有主动防御功能的杀毒软件都还带有特征码扫描功能，其实，这还算不上真正的主动防御，或者说还没真正发挥主动防御技术威力，只能说具有一定的主动防御功能。因为真正采用主动防御技术的杀毒软件应该是依赖于程序的行为来判断，而不需要特征库。当前，市面上真正将主动防御做得还不错的杀毒软件应该算是微点主动防御软件。

主动防御技术能否达到最好效果很大程度上取决于行为监控规则的完善。如何提取有效的行为规则，准确地查杀木马和病毒，这对主动防御技术来说是一大挑战；特别是现在很多合法的应用软件其行为也具有一定的敏感性，那么如何区分这些正常软件，尽可能地减少误报率将是判别该主动防御技术成熟度的一个标准。现在有些杀毒软件使用了主动防御技术，但是涉及到一些恶意软件的行为时，却弹出一些专业的提示窗口（比如：某个 DLL 动态链接库文件尝试注入到某某应用程序）让用户来选择“允许”或者“拒绝”，这就是杀毒软件做得不够智能化、不够专业的表现。用户选择用你这款杀毒软件，就是信赖你，而你把这么专业的提示让用户来选择，这是不合理的。很多用户的电脑水平很一般，不了解这么多专业术语，而杀毒软件却把自己都不能确定的一些恶意软件的行为抛给用户，这是一种责任的转移。因此，如何完善主动防御技术，如何发挥主动防御技术最大的效果，是各个杀毒软件厂商今后还要面对的问题。

2）云查杀技术。云查杀技术一提出来，各大杀毒软件厂

下转第 87 页

页错误，不是这篇论文的内容。可能是排版错误、

试的密码算法套件数目相比，所占比例比较小，这一方面说明 HTTPS 服务器并不需要提供很多密码算法套件就可以保证其服务，另一方面也说明我们所设计的测试工具所支持的密码算法套件是比较全面的。而测试两个服务器所用时间都比较短，表明我们所涉及的测试工具能够较快地完成测试。

4 结束语

本文设计了一种对 HTTPS 服务器密码算法测试的工具，通过该工具进行测试，可以比较充分地了解 HTTPS 服务器所提供的密码算法，也可以了解 HTTPS 服务器的健壮性。作为 HTTPS 服务器安全性能测试的一部分，密码算法测试有其独特的作用，而本文设计的密码算法测试工具，能够较好地完成测试任务，是一种不错的 HTTPS 服务器辅助测试工具。（责编 程斌）

参考文献：

[1] William Stallings 著，孟庆树等译 . 密码编码学与网络安全——原理与实践（第四版）[M]. 北京：电子工业出版社，2006. 377-378.

[2] William Stallings. 网络安全基础——应用与标准（第三版）[M]. 白国强等译 . 北京：清华大学出版社，2007.

[3] IxLoad. 产品介绍 [EB/OL]. http://www.ixiacom.cn/products/applications/ixload, 2011-05-18/2011-07-15.

[4] 王志海，童新海，沈寒辉 . OpenSSL 与网络信息安全——基础、结构和指令 [M]. 北京：清华大学出版社、北京交通大学出版社，2007. 78-79.

[5] 赵春平 . OpenSSL 编程 [EB/OL]. http://read.pudn.com/downloads149/ebook/644677/openssl.pdf.

[6] 国家密码管理局 . SSL VPN 技术规范 [R]. 北京：国家密码管理局，2009.

下面才是正确的内容：

上接第 49 页

商也称自家产品具有云查杀技术，有种怕自己产品没采用云查杀技术会被用户抛弃的感觉。采用云查杀技术的杀毒软件主要有：360 安全卫士、瑞星、趋势科技、金山毒霸等等。然而，云查杀技术真的这么神奇有效吗?

采用云查杀技术的杀毒软件在本地客户端上经常也带有一个特征库，对于已获取特征码的样本直接用病毒库扫描查杀；而没有获取到特征码的样本，客户端把相关样本行为规则提交给云服务器进行判断分析，再把分析结果返回给客户端，让其进行相关行为判断。对于未知病毒木马的判断就完全依赖于云服务器。云查杀技术存在以下几个问题：

1）依赖网络。采用云查杀技术的杀毒软件，客户端和云安全服务端的交互需要网络。如果在断网环境下，那云查杀只能依赖本地特征库，这将大大降低云查杀的效果，或者说得更严重些，云查杀功能就失效了。如果在网络环境不好的情况下，客户端提交的软件恶意行为不能及时传输到云服务器，或者云服务器不能及时地把处理结果返回给客户端，那么查杀效果是可想而知的。

2）本地特征库将急剧膨胀。由于云查杀依赖于庞大的客户端群，且能在短时间内收集大量的样本，因此，服务端通过对这些样本的智能分析也将在短时间内形成大量的特征码下发给客户端，这样客户端本地特征库将不断增大，达到一定程度后将会影响到本地特征码扫描的效率。

3）云服务器智能分析算法有待完善。当客户端数达到一定量时，每天提交的样本数将呈指数级增加，那么服务端如何在最短时间内对客户端提交上来的样本进行分析处理，并把相关处理结果反馈给客户端，这对服务端智能分析算法的要求还是比较高的。如果这块算法使用得不合理，那么云查杀效果将大打折扣。

4）道德约束。使用云查杀技术的杀毒软件会涉及到客户端机器相关信息的收集，必然涉及到网民个人隐私，那么作为杀毒软件厂商对这部分数据如何处理，我们不得而知。然而，在国家还没有出台相关法律法规时，就需要软件厂商恪守道德规范，不能拿用户个人隐私数据谋取非法利益。

5）人力成本和硬件成本。客户端提交上来数量惊人的样本，单单靠机器智能分析是远远不够的。随着木马、病毒的智能化以及专门针对云查杀的特殊手段，更多的是需要人工分析，那么这块的成本也将不断增加，同时云安全服务端机器随着用户群的扩展，投入的硬件成本也将不断增加。

以上提到的这几点是目前云查杀技术存在的一些问题，如果这些问题没有很好的解决方法的话，日后将会对云查杀技术的发展带来一定的瓶颈。

4 结束语

云查杀技术和主动防御技术是目前病毒查杀方面的两个比较主流的技术，也代表当前杀毒软件技术的一个特点。然而纵观这两个技术，从目前杀毒软件的使用情况来看，还有很多不完善的地方，有些技术性的问题还需要攻关解决。两个技术各有优缺点，就是看在今后杀毒软件发展过程中，谁能充分发挥各自技术的优势所在。希望在将来，杀毒软件能给我们带来一个健康安全的网络环境，云查杀的杀毒软件不涉及到个人隐私收集，主动防御不会弹出莫名其妙的窗口让用户来抉择。（责编 杨晨）

参考文献：

[1] 林柏钢 . 网络与信息安全教程 [M]. 北京：机械工业出版社，2004. 287，320，233.

[2] 刘杰 . 反病毒技术及其发展趋势 [EB/OL].http://tech.sina.com.cn/s/s/2004-11-02/1432452445.shtml，2004-11-02/2011-06-02.

[3] 罗晓波，王开建，徐良华 . 基于行为分析的主动防御技术及其脆弱性研究 [J]. 计算机应用与软件，2009，26（07）：269-271.