



Anchiva 威胁防御白皮书

目录

- ◆ 概览-----1
- ◆ 安启华威胁防御系统-----1—2
- ◆ 智能模式识别技术-----3—5
- ◆ Malicious Sites 过滤技术-----6
- ◆ 启发式行为关联分析技术—6—7
- ◆ Web 入侵防护技术-----7
- ◆ 网络应用或内容的分析管控技术-----7

Wildlist 介绍

Wildlist Organization，全球主要防病毒信息的提供者，让防病毒业界所有成员快速而安全地分享最紧急的病毒样本。为了确保 Wildlist 里的病毒真正流行于现实网络世界，Wildlist Organization 对病毒的收录采取非常严谨的态度，首先必须有两位或两位以上的病毒专家向该机构报告发现该款病毒，该报告亦必须附有病毒的样例，才能列入主要清单中，这样可确保所有收录病毒都是确实存在并具有破坏性，而不是单纯而无意义的统计数字。

多种途径的 Internet 应用威胁防御

概览

成立于 2005 年的安启华 RapidRx 安全实验室是全球重要的病毒、恶意威胁和漏洞研究机构，其研究人员来自全球各地的最顶级研究员，从事世界级的恶意代码研究、恶意入侵及漏洞防护研究。

经 RapidRx 安全实验室的持续观察分析，网络威胁具有多变性和多态性特点，并且出现了爆炸性增长的趋势；面对日益复杂和严峻的网络威胁防御任务，安启华 RapidRx 安全实验室在 2005 年创建了威胁防御系统，并陆续研究开发了智能模式识别技术、Malicious Sites 过滤技术、启发式行为关联分析技术，并且为了提供全方位的 Internet 应用安全服务，安启华还提供了网络应用或内容的分析管控技术和 Web 入侵防护技术，从而打造了多种途径的 Internet 应用威胁防御方案，不但能够高效预防已知和未知网络威胁，还能对零日攻击提供有效的防御手段和服务。

安启华威胁防御系统

安启华威胁防御服务中一个重要的部分就是安启华的威胁防御系统，能够为客户提供联网式、整合式的网络威胁服务，它由三部分组成：威胁采集网络、威胁处理中心、ASDN 升级服务网络。

安启华威胁采集网络主要有下图 1 所示 6 部分的采集渠道，安启华 RapidRx 安全实验室是世界反病毒组织 Wildlist 成员，上报 malware 样本到 Wildlist 的同时也享受其他众多成员的研究成果，用于加强自身的威胁数据库，这样的行业交换渠道使安启华能够及时获得全球最新的 malware 样本；除此之外，安启华还有自己的用户反馈系统、honeynet、WebCrawler 系统、恶意站点监测系统和可疑文件监控网，实时不断的采集、监测 Internet 上的威胁信息。

安启华威胁采集网络汇总Malware信息到RapidRx Database后，安启华威胁处理中心的Malware智能分析处理系统，可自动化处理 90%以上的malware, 剩余不到 10%的一小部分智能分析处理系统不能处理的Malware会交付安全专家进行分析；通过Malware智能分析处理系统和安全专家分析后，最终形成Anchiva Malware特征库和Anchiva Malicious Sites数据库，同时这 2 大数据库经过安启华的自动测试系统的严格测试以后，会通过安启华的ASDN升级服务网络为安启华的web安全网关进行统一的升级分发。

ASDN (Anchiva Service Distribution Network) 为安启华服务分发网络，是由安启华分布在全球的升级服务器组成，保证了 Malware、Malicious Sites、网络应用管控等各种特征库能够及时可靠地分发到安启华Web 安全网关中去，为客户提供可靠的升级服务保障。

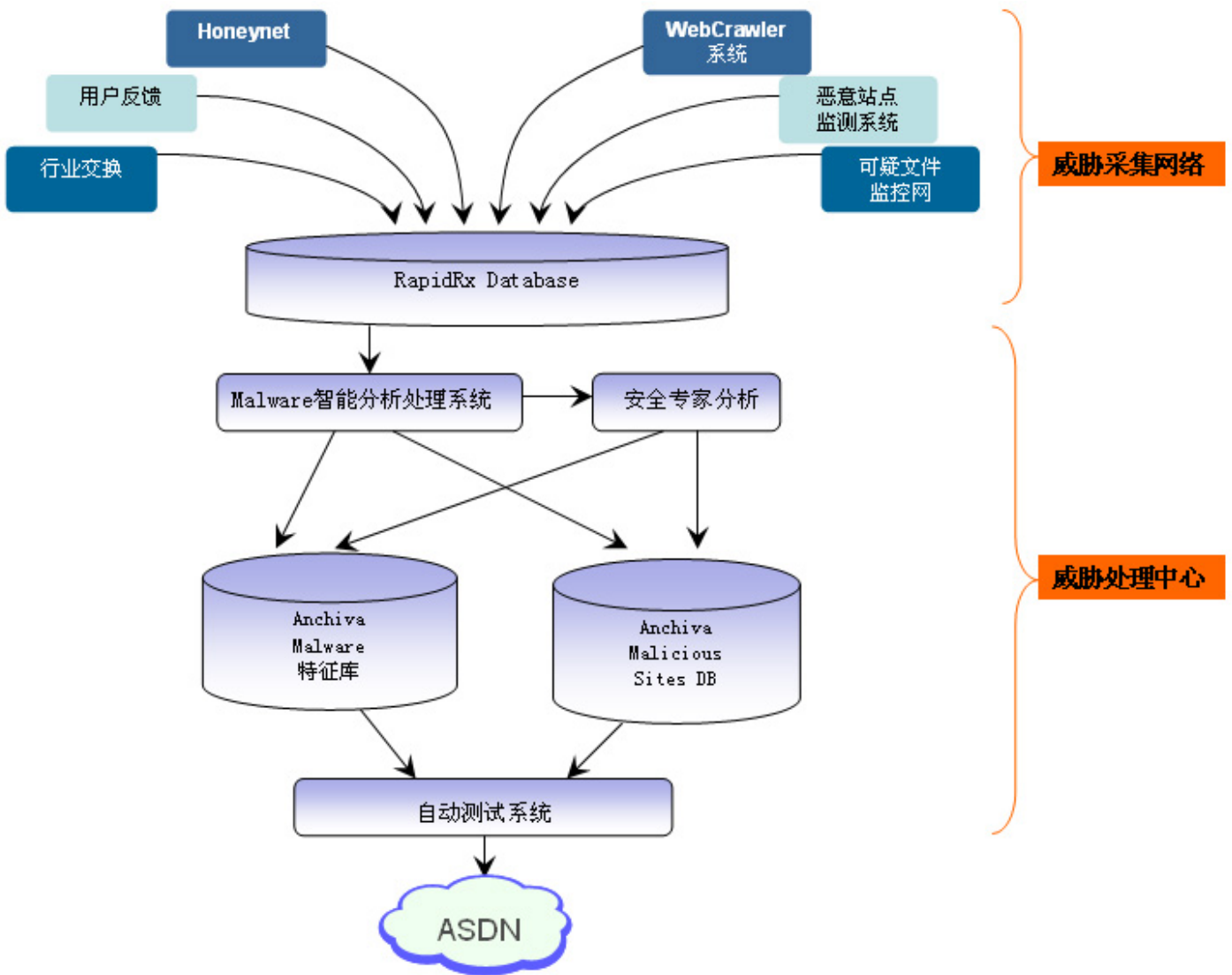


图 1: Anchiva 威胁防御系统

智能模式识别技术

在经济利益的驱动之下，木马，间谍软件等恶意软件已经成为某些人的赚钱工具，各类木马，间谍软件的自动生成机也已经出现，而为了逃避杀毒软件的检测，恶意软件的更新周期越来越短，变种也越来越多。

传统 Malware 特征识别，人工创建模式生产方式，人均每天 20 个左右，生产效率低，面对爆炸性增长的 Malware 总是落后一步，常常面临特征尚未发布，而恶意软件已经自动更新到更新变种的现实。



图 2: 传统 malware 特征

弊端：人工创建 malware 特征，生产效率低，总是比 Malware 爆发晚一步，适用性差。

为了解决传统 malware 特征的弊端，高效应对爆炸性增长的 Malware，提高特征库的适应性，Anchiva RapidRx 安全实验室在对大量的恶意软件的程序入口、程序结构、文件头、文件内容、行为特征以及规避技术等进行研究并通过 Malware 智能分析系统分析以后，根据相似度分别建立程序结构建模库、应用行为建模库和规避技术建模库，并通过对这 3 个建模库进行关联分析建立安启华 malware 特征库。由于采用自动化的处理系统，每天可生产上万条 Malware 特征，不仅能够高效应对爆炸性增长的 Malware，而且由于安启华 malware 特征库建立在对大量 Malware 的程序入口、程序结构、文件头、文件内容、行为特征以及规避技术综合分析的基础上，不仅能够检测已知的大量恶意软件，还能够检测到这些恶意软件将来出现的相关变种，为客户提供零日防护。

大量Malware元素

程序入口
程序结构
文件头
文件内容
行为特征
规避技术

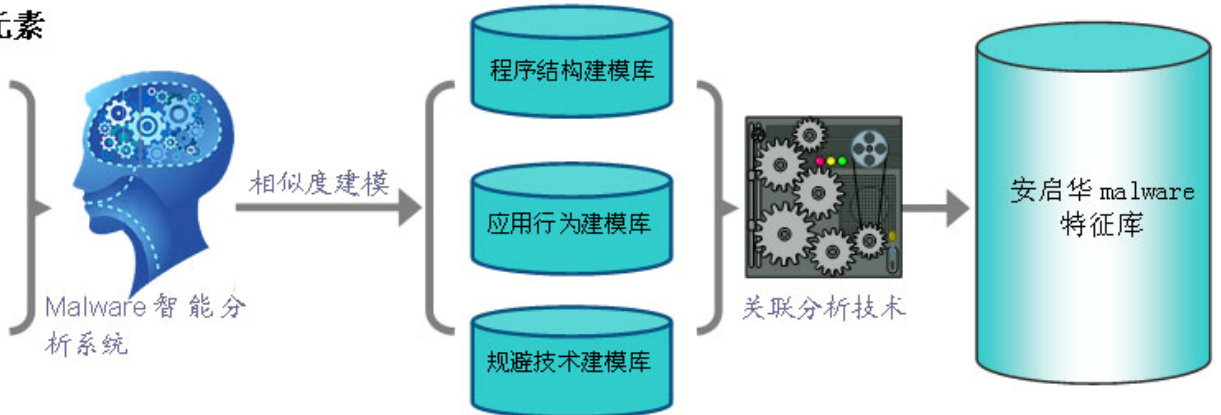


图 3: 安启华 malware 特征

优点:

- ◆ 应对 malware 爆炸性增长趋势
- ◆ 检测未知 Malware 及其变种
- ◆ 提供零日防护

在 Wildlist 每月公布的当月最新流行 Malware 中,相当一部分会被 Anchiva 智能模式识别技术检测到,这说明这些新 Malware 第一次出现时就会被 Anchiva 的设备拦截到。

下表为 wildlist 列出的 2008 年 11 月部分新 malware,这些新 malware 均被 Anchiva 的 malware 特征 Trojan/XPack.gen 检测到,其它两个 AV 厂商均需要使用多个不同的新特征来检测这些 Malware。

wildlist sample	AV Vendor1	AV Vendor2	Anchvia 检测结果
ITW#66	Trojan.Win32.Vaklik.ced	TROJ_VAKLIK.GY	Trojan/XPack.gen
ITW#65	Trojan.Win32.Vaklik.cce	TROJ_VAKLIK.HU	Trojan/XPack.gen
ITW#64	Trojan.Win32.Vaklik.bop	WORM_ONLINEG.EWO	Trojan/XPack.gen
ITW#63	Trojan.Win32.Vaklik.bwc	WORM_TATERF.AF	Trojan/XPack.gen
ITW#606	Trojan-GameThief.Win32.OnLineGames.tob	WORM_LINEAGE.AZ	Trojan/XPack.gen
ITW#605	Trojan-PSW.Win32.OnLineGames.aptk	WORM_GAMMIMA.T	Trojan/XPack.gen
ITW#604	Trojan-GameThief.Win32.OnLineGames.sbo	Mal_NSAnti-1	Trojan/XPack.gen
ITW#602	Trojan-PSW.Win32.OnLineGames.ahvd	TSPY_ONLINEG.QYI	Trojan/XPack.gen
ITW#600	Trojan-GameThief.Win32.OnLineGames.sbwk	TROJ_GAMETHI.ER	Trojan/XPack.gen
ITW#597	Trojan.Win32.Vaklik.cms	TSPY_ONLINEG.PPX	Trojan/XPack.gen
ITW#596	Trojan.Win32.Vaklik.asm	WORM_ONLINEG.EWH	Trojan/XPack.gen
ITW#499	Worm.Win32.AutoRun.elj	WORM_AUTORUN.BEN	Trojan/XPack.gen
ITW#498	Worm.Win32.AutoRun.ekz	WORM_AUTORUN.AAF	Trojan/XPack.gen
ITW#487	Worm.Win32.AutoRun.dki	WORM_ONLINEG.EVW	Trojan/XPack.gen
ITW#442	Trojan-PSW.Win32.OnLineGames.adsy	WORM_AUTORUN.BZH	Trojan/XPack.gen
ITW#437	Trojan.Win32.Vaklik.ajx	WORM_ONLINEG.EWJ	Trojan/XPack.gen
ITW#361	Trojan-PSW.Win32.OnLineGames.acgu	WORM_ONLINEG.SYM	Trojan/XPack.gen
ITW#336	Trojan-GameThief.Win32.OnLineGames.zex	TSPY_ONLINEG.KTP	Trojan/XPack.gen
ITW#279	Trojan-GameThief.Win32.OnLineGames.ywy	TSPY_ONLINEG.MI	Trojan/XPack.gen
ITW#260	Worm.Win32.AutoRun.clb	WORM_ONLINEG.EVT	Trojan/XPack.gen
ITW#259	Trojan-GameThief.Win32.OnLineGames.zll	WORM_ONLINEG.SAY	Trojan/XPack.gen
ITW#253	Trojan-PSW.Win32.OnLineGames.acdy	TSPY_ONLINEG.IQR	Trojan/XPack.gen
ITW#243	Trojan-PSW.Win32.OnLineGames.acas	TSPY_ONLINEG.THF	Trojan/XPack.gen
ITW#167	Packed.Win32.PolyCrypt.h	WORM_ONLINEG.EWD	Trojan/XPack.gen
ITW#149	Trojan-GameThief.Win32.OnLineGames.ubg	WORM_ONLINEG.EWM	Trojan/XPack.gen

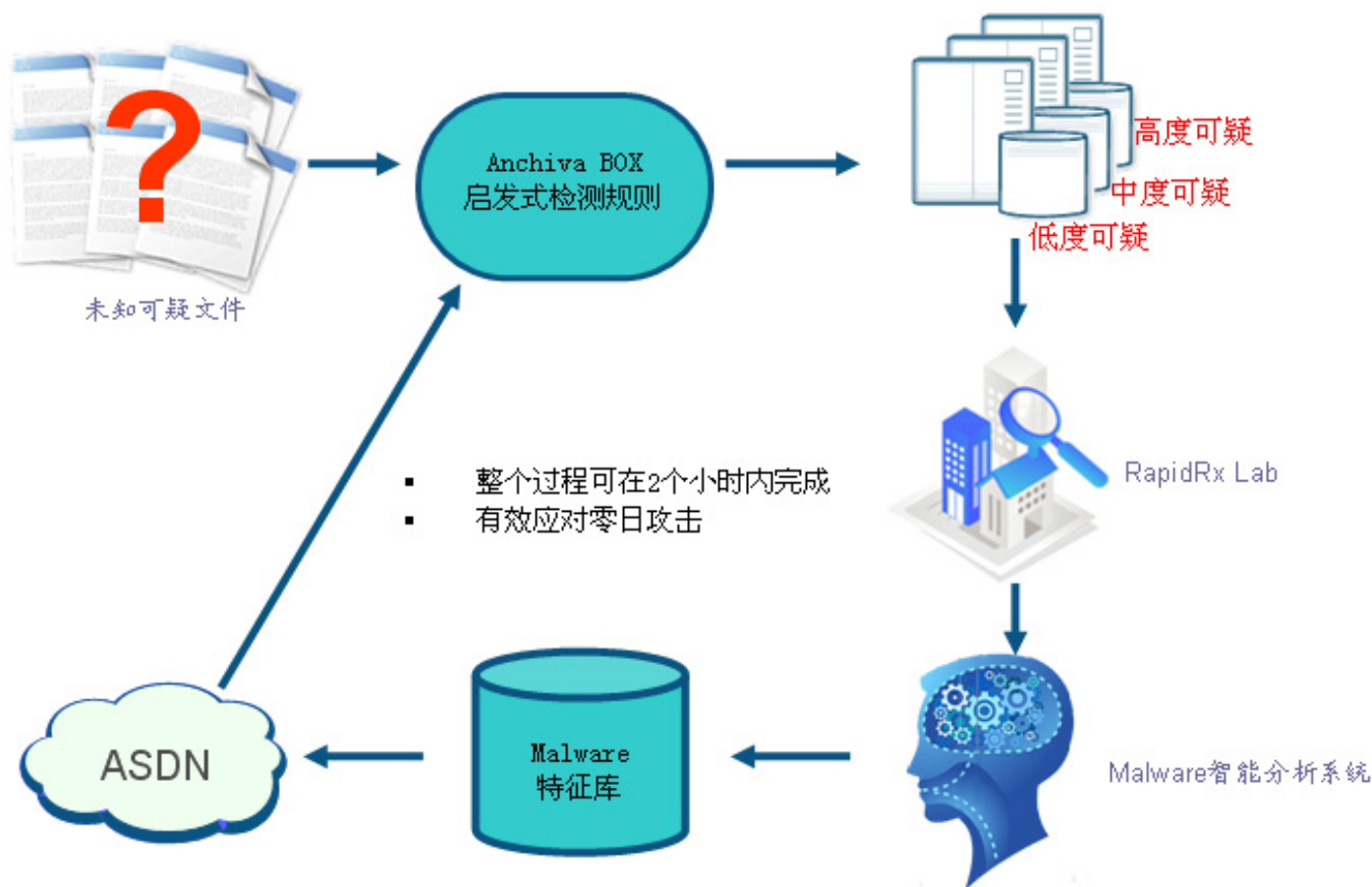


图 5：启发式行为关联防护模型

Web 入侵防御技术

攻击者可以通过 SQL 注入、跨站点脚本攻击等入侵手段，通过对正常网站的恶意访问，来达到窃取网站信息、修改网站内容，入侵控制网站等目的。安启华针对这类攻击提供了专门的防护技术：针对访问者的访问请求进行实时安全监测，来识别访问者的访问请求是否包含有恶意攻击，并进行实时阻止，从而保护网络中 Web 服务器的安全。

网络应用或内容的分析管控技术

经安启华 RapidRx 安全实验室的长期分析研究，对于员工的网络应用完全不加控制的企业，其爆发安全事件的比例要比严格加以控制的企业高 3-4 倍。因此安启华率先在 Web 安全网关上实现了 Application Control 和 Web Filtering 功能，在对 Internet 应用或内容分析的基础上，实现基于用户和用户组的控制策略，最大程度的掌控 Internet 应用威胁的各个环节，进一步降低企业的网络安全风险。