China Cloud Computing Conference
第三届中国云计算大会
2011年5月18-20日 北京国家会议中心

基于云计算模式的创新网络信息安全服务

奇虎360
石晓虹

目 录

- 安全是互联网基础需求
- 互联网时代的网络安全趋势
- 传统网络安全技术的困境
- 基于云计算模式的网络安全防护体系

安全是互联网的基础需求

- 随着互联网与人们生活的结合日益紧密，用户在使用任何互联网应用时都可能遭遇到安全威胁。用户终端及网络的安全已成为互联网的基础服务需求。


网络浏览


搜索


即时通信


电子邮件


下载安装软件

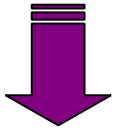
网络游戏


影音播放


网上购物


网上银行/证券

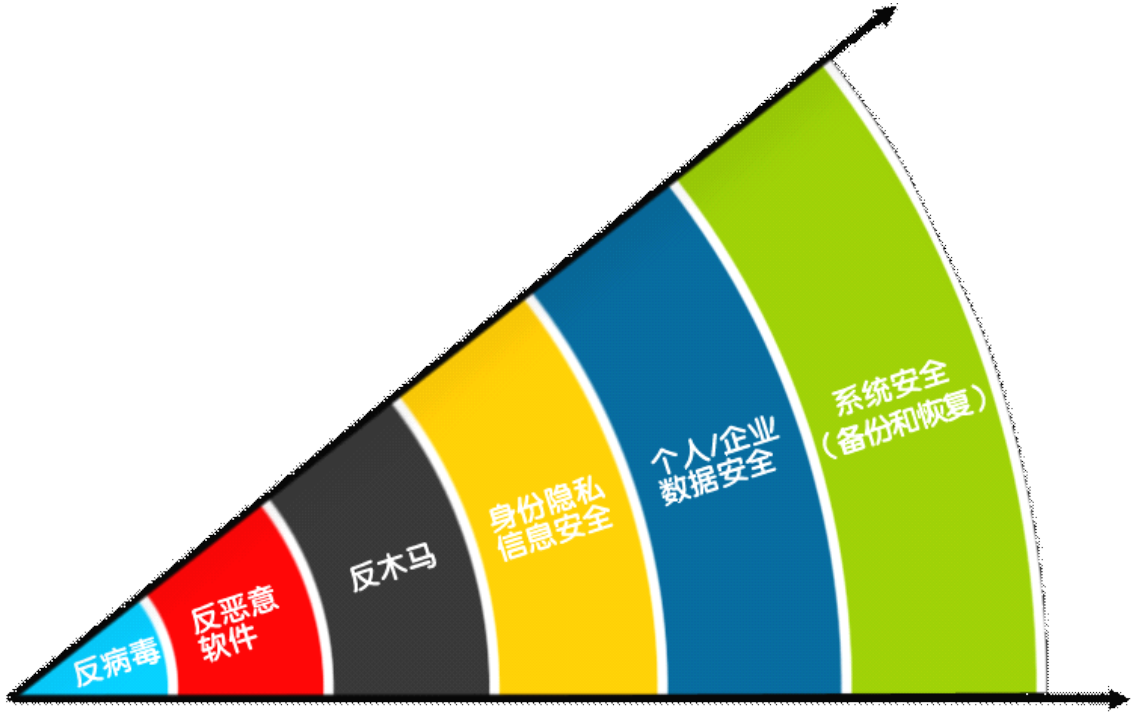
.....



安全成为互联网的基础服务需求（Infrastructure）

从杀毒到泛安全

- 用户的安全需求已不仅仅是传统的反病毒，而是扩展到了反恶意软件、反木马、浏览安全、隐私安全、个人数据安全等泛安全领域：



终端安全从反病毒扩展到更多的泛安全领域

目 录

- 安全是互联网基础需求
- 互联网时代的网络安全趋势
- 传统网络安全技术的困境
- 基于云计算模式的网络安全防护体系

木马：互联网安全的主要威胁

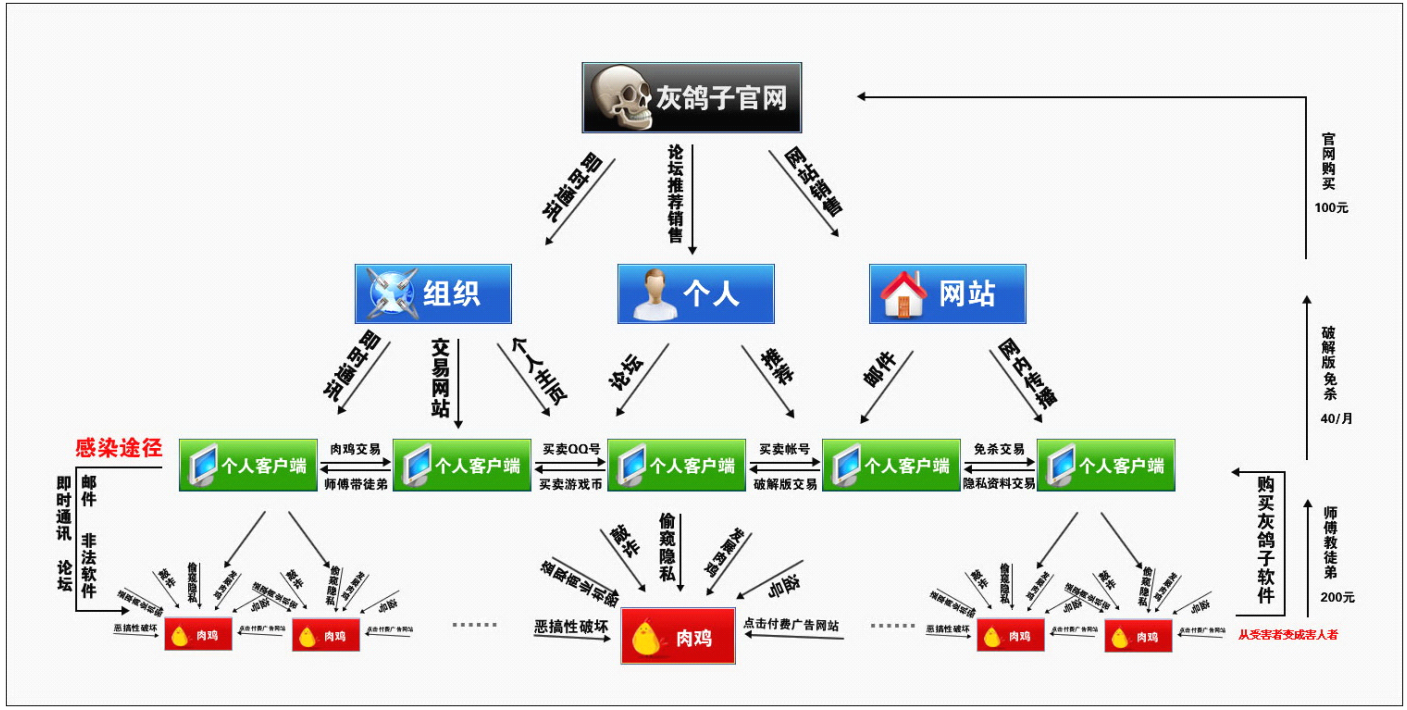
- 单机系统时代，病毒是电脑安全的主要威胁：
  - 传播介质：磁盘等移动介质
  - 传播方式：交叉感染
  - 传播目的：破坏电脑系统
- 互联网时代，木马是电脑安全的主要威胁：
  - 传播介质：互联网络
  - 传播方式：网格状交叉模式
  - 传播目的：非法获取财产

木马侵犯用户财产的方式多种多样

- 木马形式多样，角色各异
  - 盗号木马：盗取虚拟财产
  - 僵尸网络：对网站等攻击、勒索
  - 肉鸡木马：在用户的电脑中弹出广告
  - 间谍木马：窃取隐私和商业机密

木马已形成上百亿元的灰色产业链

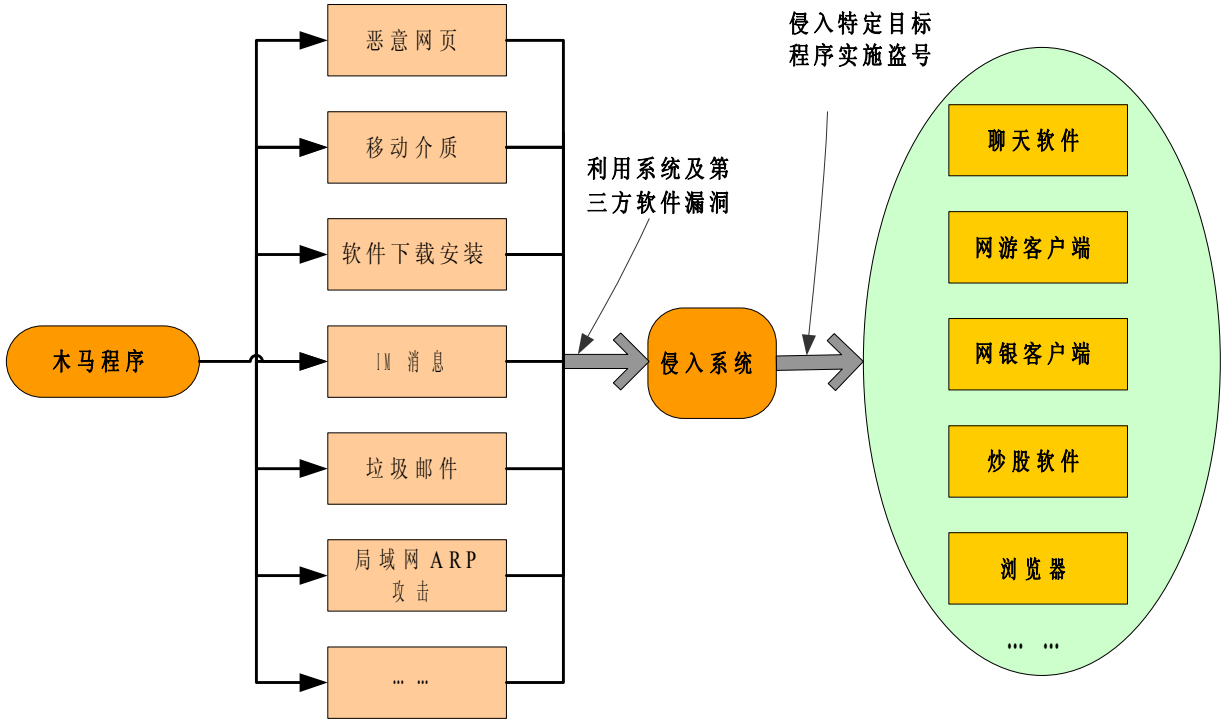
- 木马已经形成了造马、改马、卖马、买马、发马、挂马、盗号、销赃等分工明确的灰色产业链，从业人数以十万计：



灰鸽子木马产业链示意图

互联网时代木马传播方式日益多样化

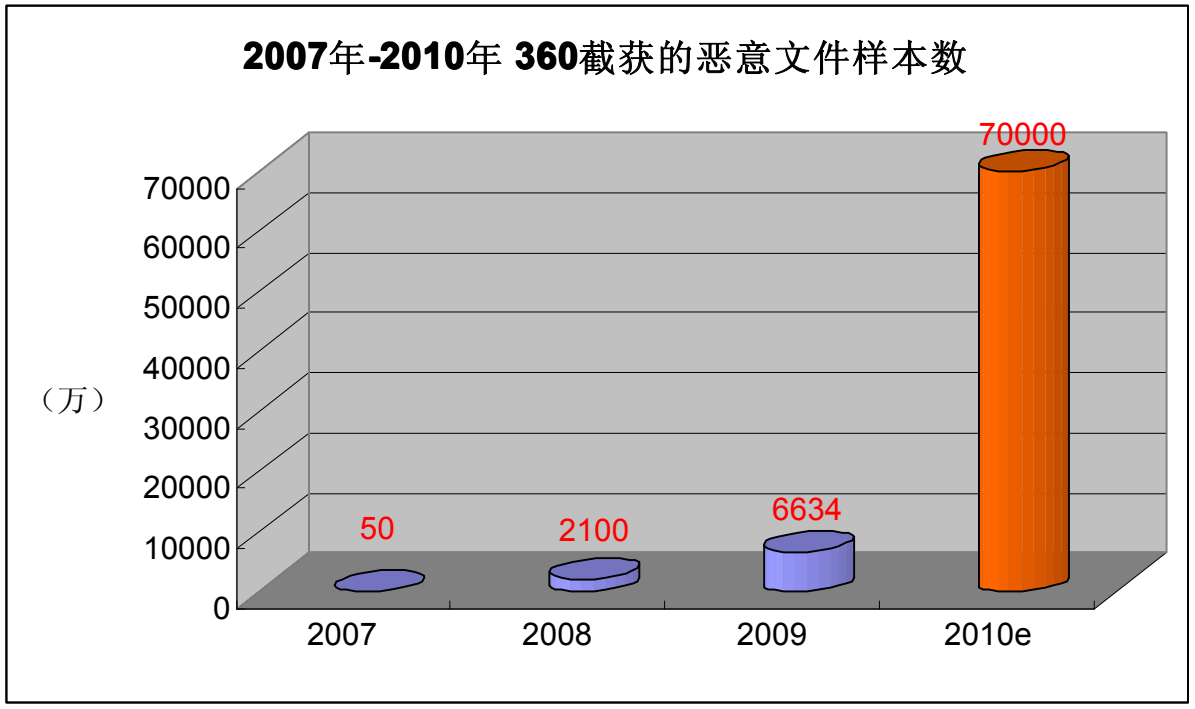
- 互联网为木马提供了多样化的传播途径，使之无需像病毒那样依靠感染即可大规模传播：



多样化的木马传播途径

结果：恶意软件的“摩尔定律”

- 木马灰色产业链的形成，使得恶意软件制作、传播的门槛大大降低，由此导致恶意软件数量的爆炸性增长：



恶意软件的“摩尔定律”：新增木马数每年增加十倍

目 录

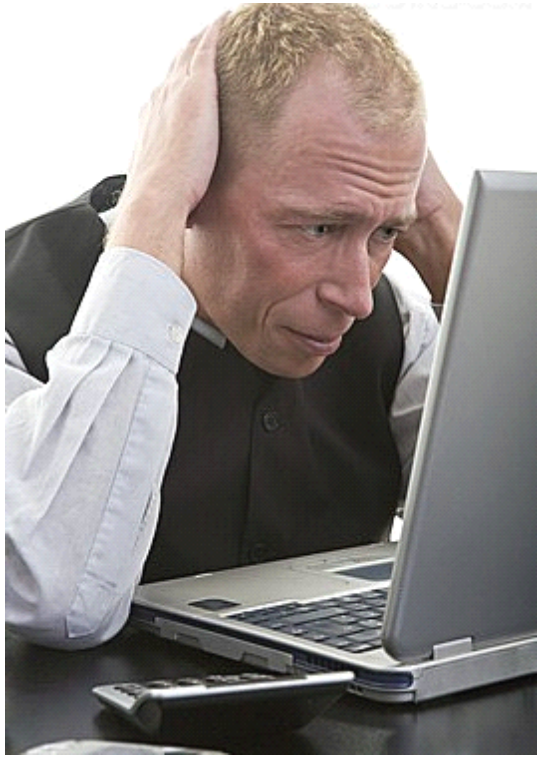
- 安全是互联网基础需求
- 互联网时代的网络安全趋势
- 传统网络安全技术的困境
- 基于云计算模式的网络安全防护体系

传统反病毒技术的问题

- 每日**500**万新增木马样本给传统杀毒软件带来如下问题：
  - 大量样本由人工分析提取其特征码，工作量巨大；
  - 恶意软件借助互联网的传播速度极快，迫使杀毒软件不断缩小病毒库升级时间间隔；
  - 即使如此，杀毒软件病毒库的更新速度亦远远滞后于恶意软件的变化速度，导致杀毒软件沦为“马后炮”；
  - 大量恶意软件是针对性的“多品种，小批量”未知木马，并经过免杀处理，杀毒软件防不住；
  - 病毒库的不断升级导致用户电脑资源耗尽，机器变“卡”；

传统杀毒软件面临的问题

卡

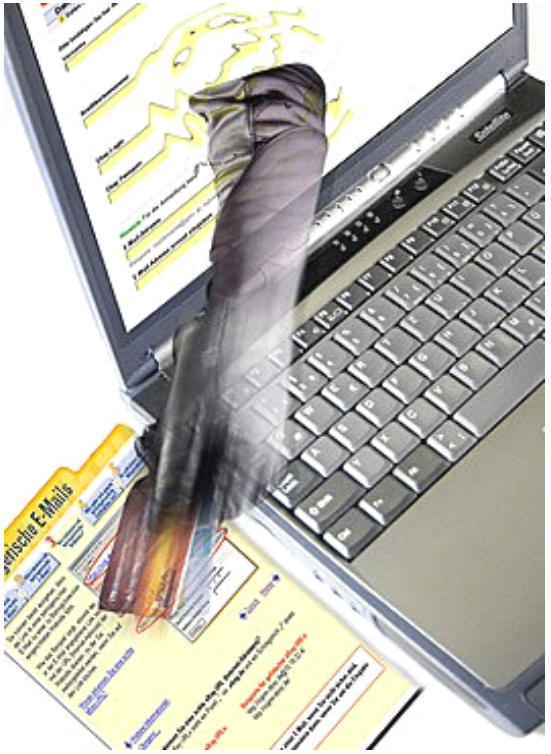


庞大的资源占用造成卡机

慢

扫描慢
木马特征库更新慢

效果差



轻松被免杀
跟不上木马病毒的变化速度

目 录

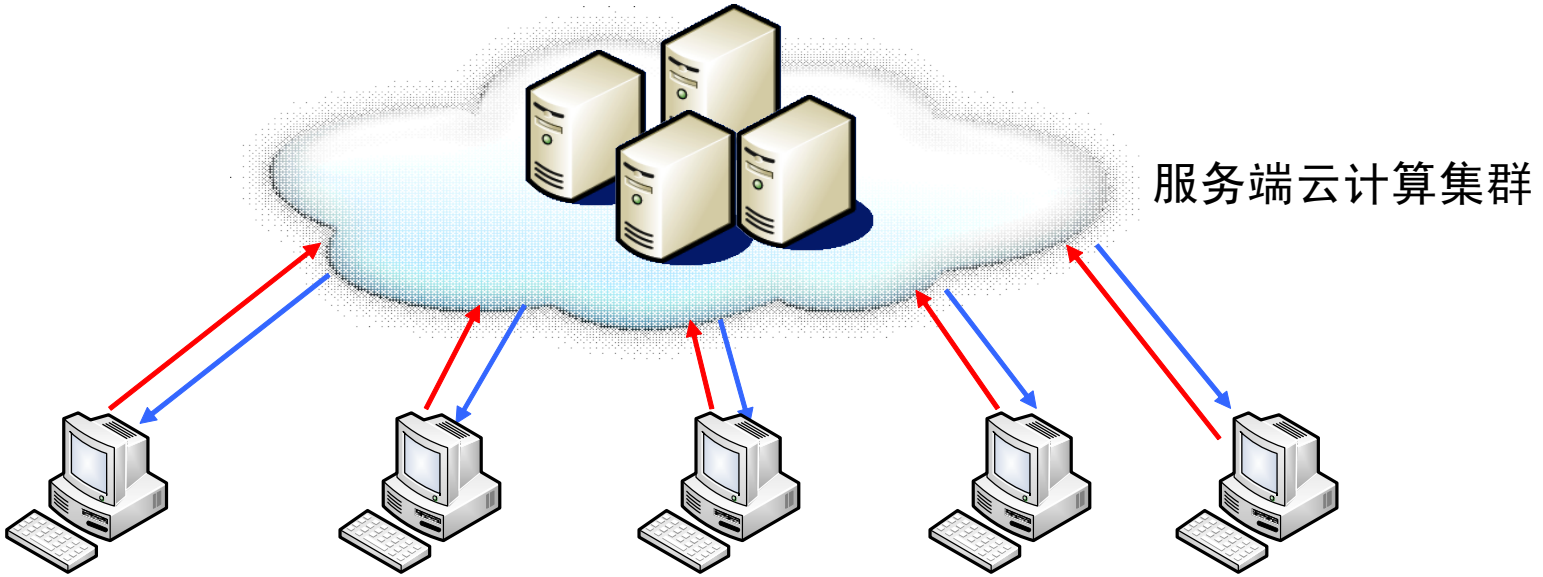
- 安全是互联网基础需求
- 互联网时代的网络安全趋势
- 传统网络安全技术的困境
- 基于云计算模式的网络安全防护体系

基于云计算模式的安全原理

采集： 从上亿用户终端电脑中采集可疑行为程序样本及其行为特征

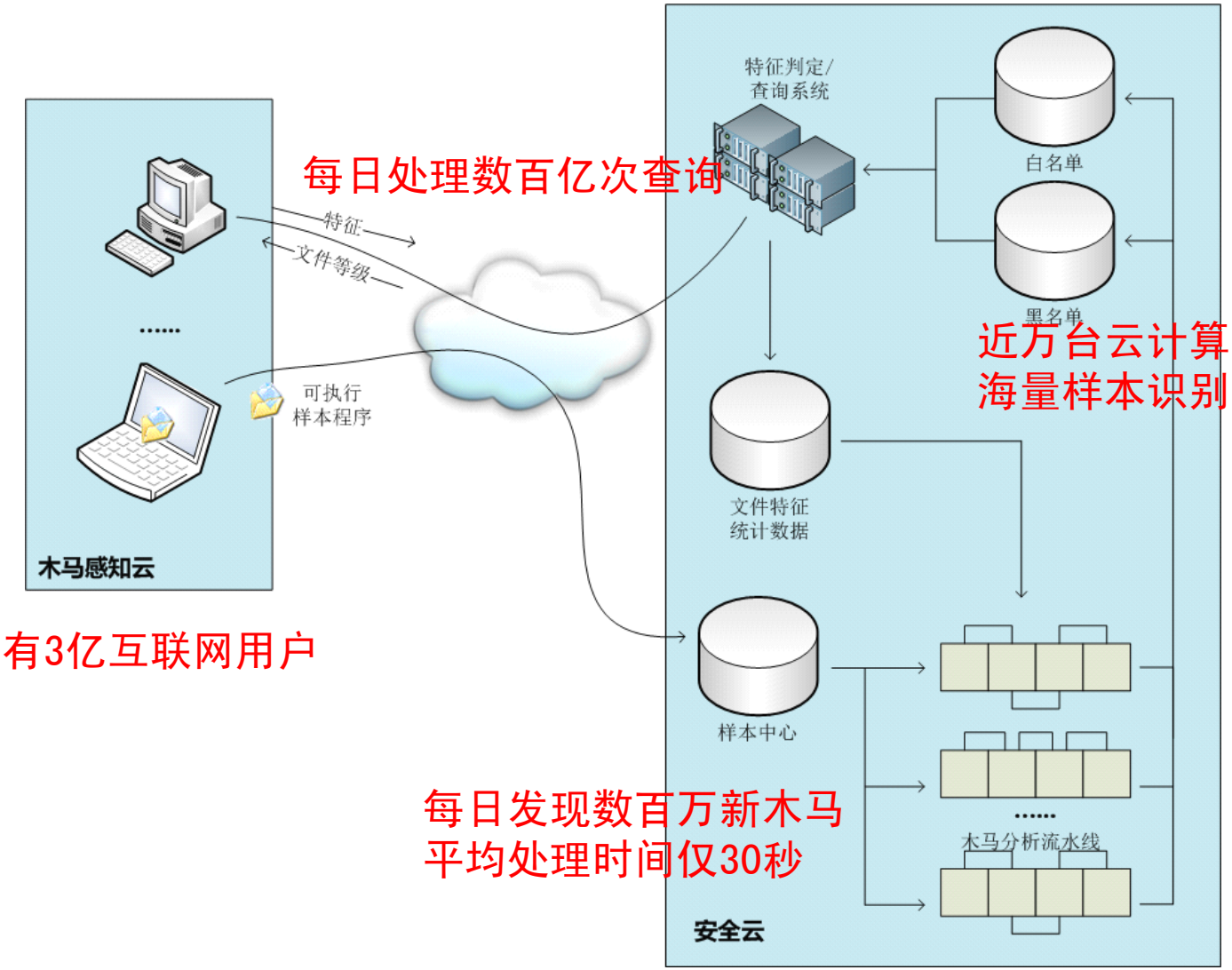
分析： 经过服务端集群自动分析处理，形成对恶意程序处置的指导规则

处置： 恶意程序判定指导规则反馈回客户端进行处置



云安全的基本原理： 云计算中心对从用户电脑采集到的可疑程序样本依据其代码特征、行为特征、生存周期、传播趋势进行数据挖掘和智能分析，进而判定恶意程序及其传播规律，在恶意软件传播初期予以查杀。

360云安全技术体系示意



云安全需要解决的三大问题

1. 云端文件知识库的完备性

2. 云查询的快速实时响应

3. 对未知恶意文件/网页的实时分析处理

云端文件知识库的三大要素

白名单的完备性
- 云安全中最大的难点
- 360白名单已经覆盖98%的合法程序

黑名单的积累
- 每日发现200万以上的新增木马病毒

新程序的收集能力
- 搜索引擎的蜘蛛技术
- 3亿用户保证即时发现、不遗漏
- 360软件认证服务
- 手工收集和人工甄别

日收集新程序样本：1000万

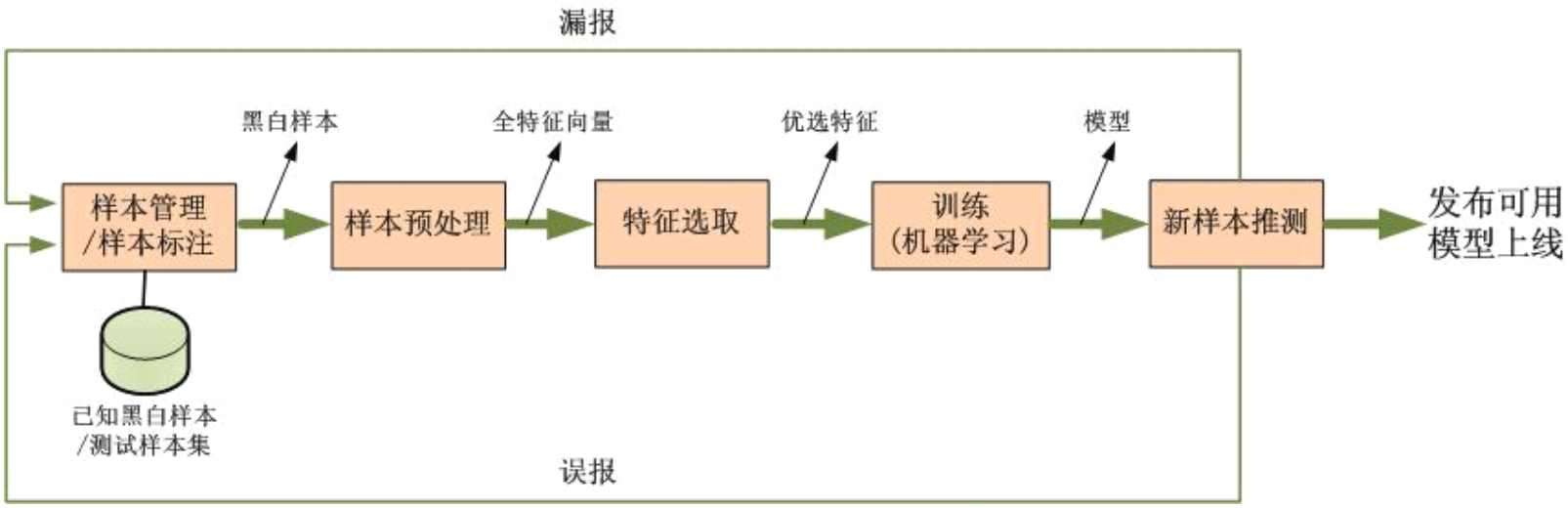
高性能云查询响应能力

- 基于强大的搜索引擎等服务器端技术
- 千亿规模下高性能查询：
  - 单机存储10亿条文件安全信息
  - 单机QPS ＞ 10000
- 高可靠性、高稳定性

未知文件/网页的自动分析处理

- 未知文件/网页的自动分析技术
  - 文件特征、行为特征、智能启发、统计分类……
- 未知文件/网页的海量分析性能
  - 日均处理 > 8000万样本
  - 样本平均处理时间 < 30秒

人工智能识别引擎QVM：实现对海量恶意文件的自动识别



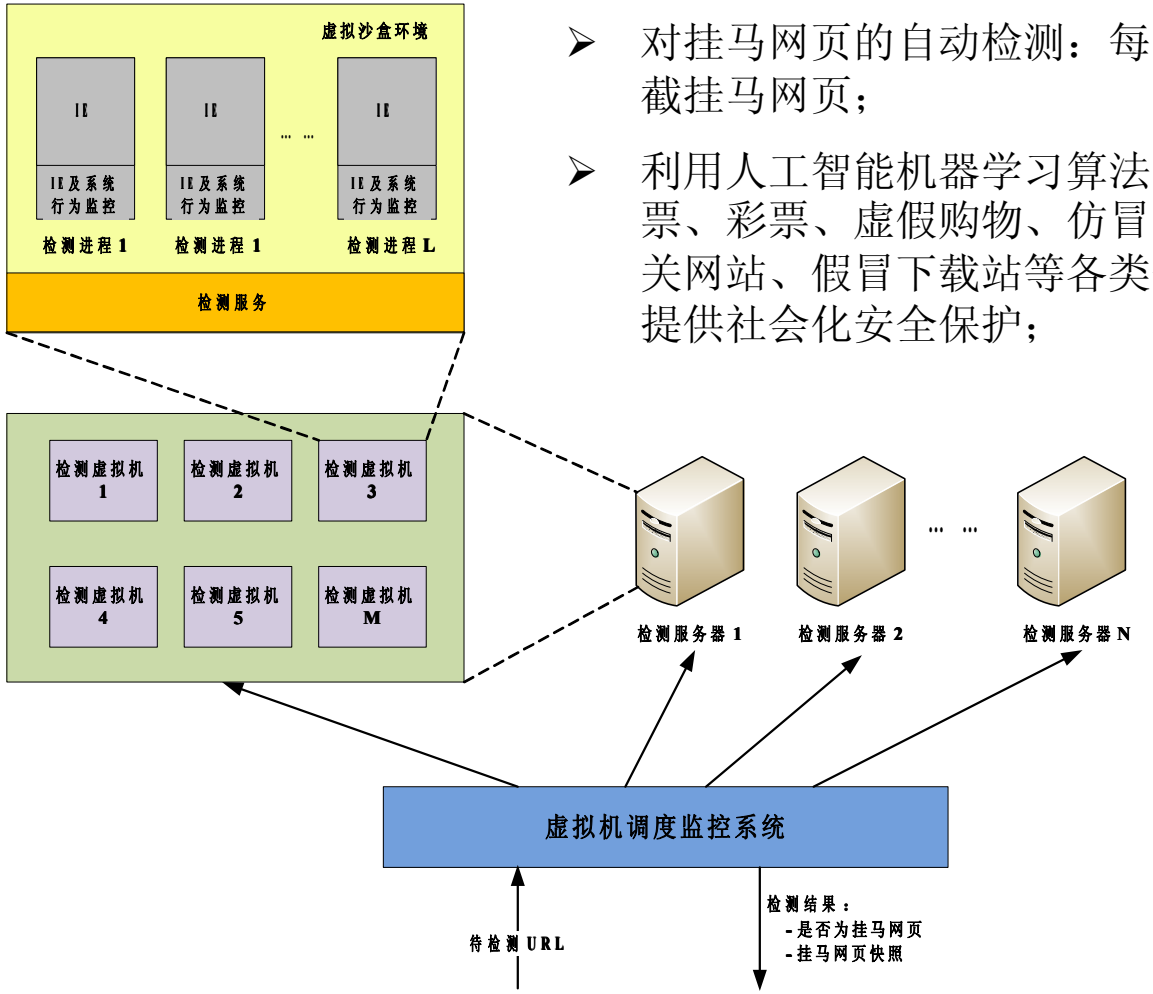
- 基于云端海量黑白文件样本的训练，采用人工智能机器学习方法，实现对未知二进制文件的自动识别；
- 对未知新木马的检出率高达74.88%，远高于其他启发式扫描技术；
- 无需更新，对恶意软件变化具有极强的适应能力；

QVM与流行杀毒引擎的启发式检测能力对比：

检测产品	样本总数	侦测样本数	侦测率
奇虎360杀毒QVM引擎	1218	912	74.88%
对比产品 A	1218	686	56.32%
对比产品 B	1218	533	43.76%
对比产品 C	1218	321	26.35%
对比产品 D	1218	704	57.80%
对比产品 E	1218	460	37.77%

- 数据来源： AMTSO认证检测机构PCSL 于11月28日的测试结果；
- 评测对象：选取中国市场占有率排名前十的杀毒软件与QVM对比；
- 检测方法：冻结病毒库，测试对新流行病毒的检测能力；

云端恶意网页自动监测系统



- 对挂马网页的自动检测：每日检测50亿网页访问并拦截挂马网页；
- 利用人工智能机器学习算法，智能检测虚假中奖、股票、彩票、虚假购物、仿冒网站、虚假医疗/药品相关网站、假冒下载站等各类钓鱼、欺诈网站，向网民提供社会化安全保护；

360云安全系统主要指标

- 每日采集新程序样本数 > **1000**万
- 日均样本分析能力 > **8000**万
- 样本平均分析时间 < **30**秒
- 累计黑白名单库 > **20**亿
- 白名单覆盖率 > **98%**
- 日均云安全查询数 > **500**亿次
- 日均查杀恶意软件数 > **5000**万
- 日均拦截恶意网页 > **6100**万次

全球应用规模最大的云安全系统

云安全需要的核心技术

- 大规模分布式并行计算技术
- 海量数据存储技术
- 海量数据自动分析和挖掘技术
- 未知恶意软件的自动分析识别技术
- 未知恶意软件的行为监控和审计技术
- 海量恶意网页自动检测
- 海量白名单采集及自动更新
- 高性能并发查询引擎

云安全技术的重要意义

- 云安全对保护基础信息网络和重要信息系统的安全稳定运行具有重大的意义：
  - 遏制安全事件于萌芽状态

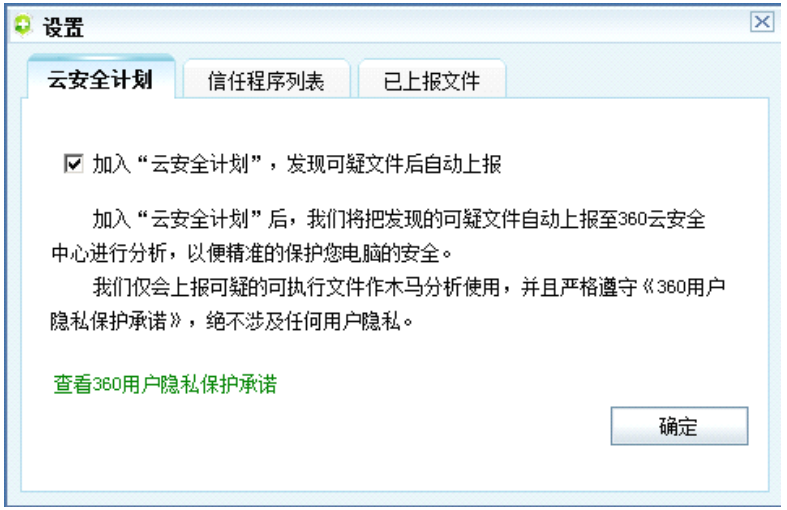
    大多数安全事件都是来自于终端恶意软件的攻击。云安全技术可以克服传统病毒查杀技术的缺点，零时差地实现对恶意软件的判定、查杀更，从而将安全事件扼杀在萌芽状态。
  - 应急预警与漏洞消控

    云安全体系可监测整个中国互联网的恶意软件和恶意网页，可在第一时间发现新的漏洞利用0day漏洞以及定向攻击，为国家重要信息系统提供安全事件的应急预警和漏洞消控服务；
  - 奠定国家可信软件管理基础

    海量白名单技术将为实现国家可控的可信软件配置管理奠定基础；

云安全的用户隐私保护

- 隐私承诺
- 文件上传明确声明
- 仅上传可执行程序
- 源代码托管
- 加入**IAPP**隐私保护协会



China Cloud Computing Conference

第三届中国云计算大会

2011年5月18-20日 北京国家会议中心

Thank you