AI时代移动安全需要AI技术来解决

任宇驰：360企业安全华南基地副总

360企业安全 安全第一™

360企业安全集团

中国政企网络安全市场的领军者

2005 公司成立

2008 安全卫士市场占有率第一

2009 推出免费杀毒

2010 人工智能杀毒引擎

2011 美国上市

2015 业务分拆

360企业安全集团

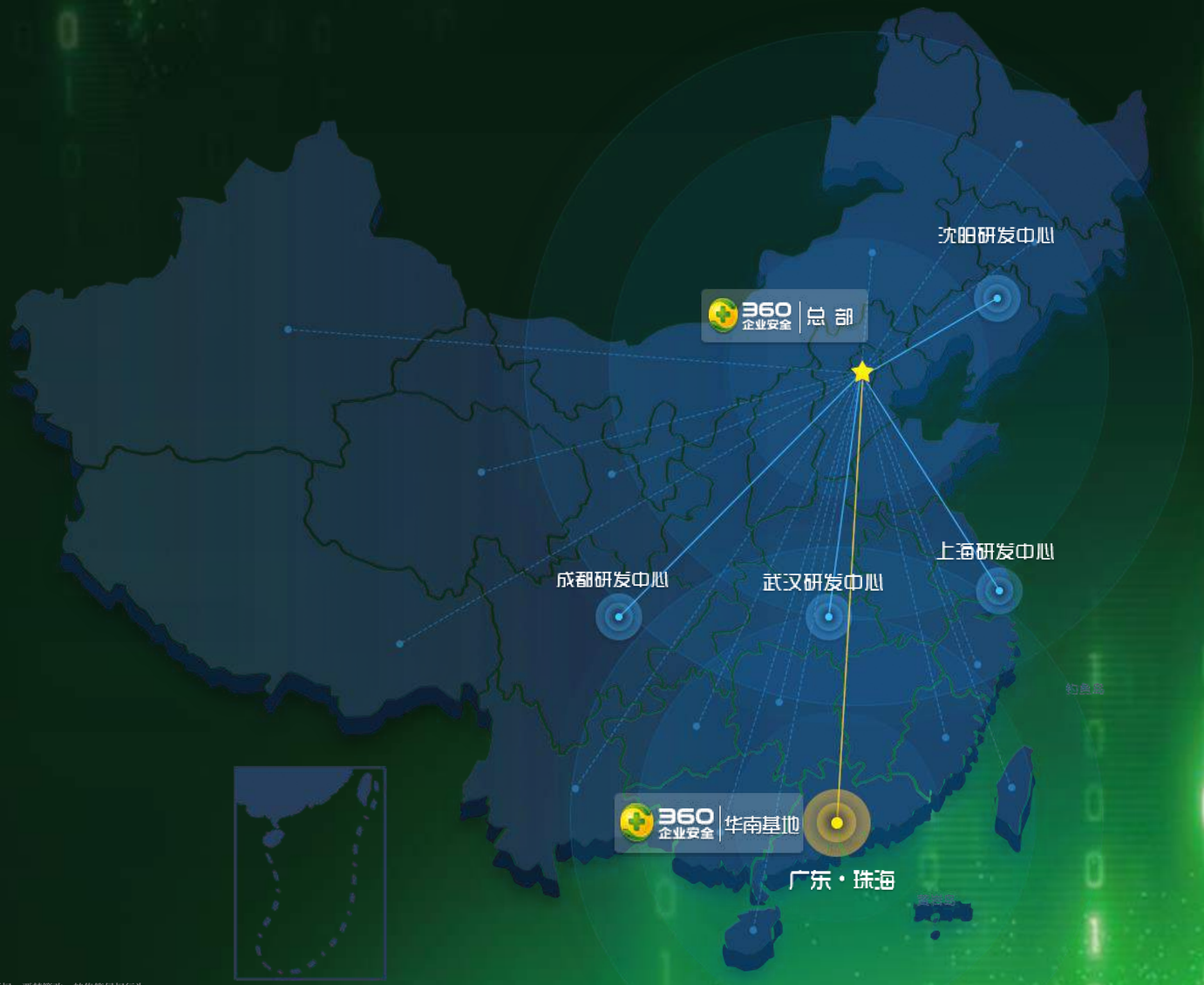
专注政企安全业务

专注个人消费者业务

360集团

- 亚太地区最大的安全创新中心
- 16支安全研究团队
- 3大安全研究院
- 9大实验室
- 1200名核心安全专家

360企业安全集团.华南基地



华南基地

360企业安全集团华南总部基地，为全职能、全建制编制。

作为集团的“安全能力中心、新产品新业务中心、服务支持中心”将为集团提供强力的安全能力支持，为华南区域的政企客户提供优质高效的技术服务支持。

目录

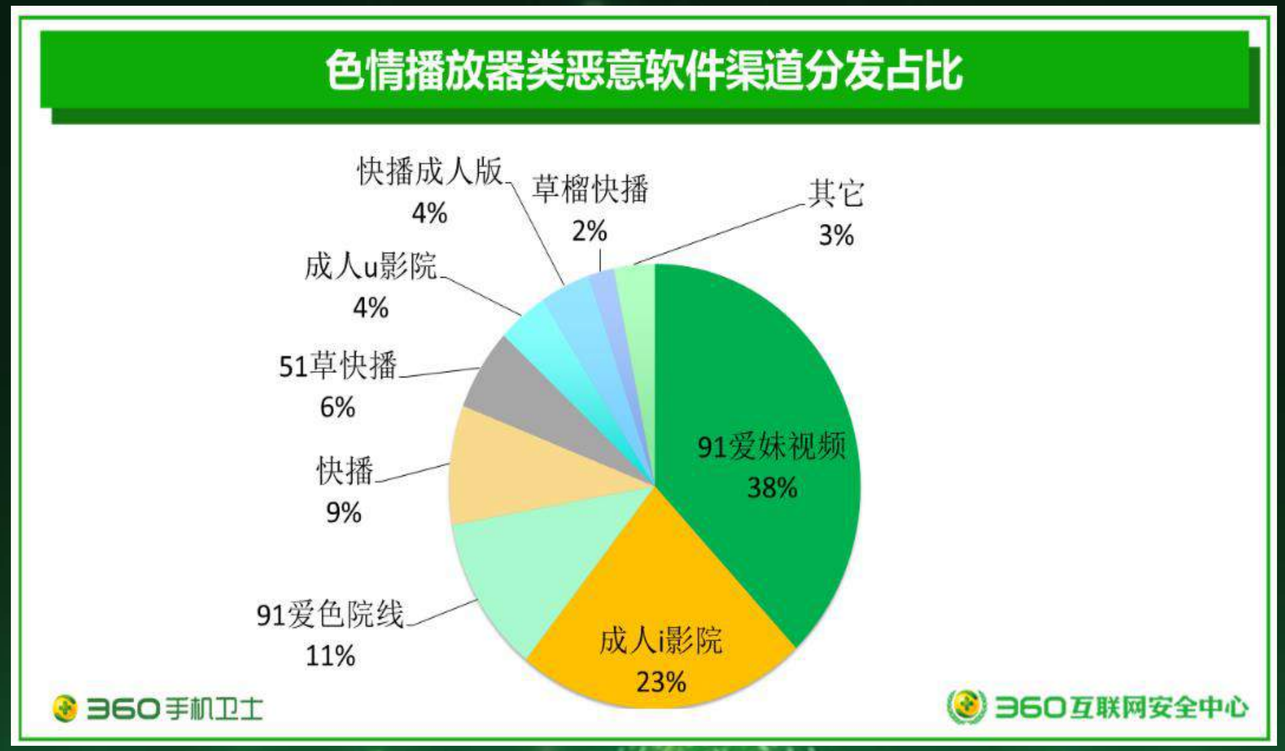
烈性病毒大量传播

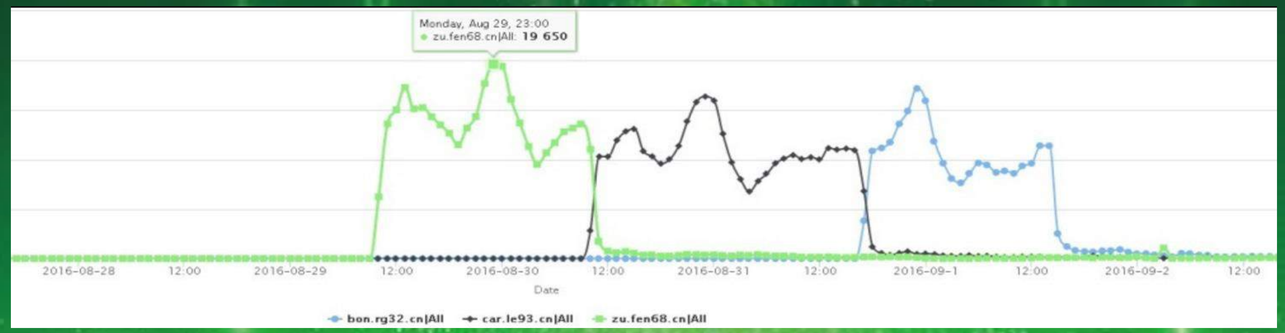
大规模烈性病毒

Root用户手机，替换系统文件，监控用户短信/位置等。

此类病毒称之为烈性病毒。

黑产人员针对人性底层需求开发的色情视频类恶意软件，是烈性病毒的主要载体，该类样本隐蔽性强，具有周期性特点





目录

安全防护面临的技术问题

混淆、加固让传统安全无助

通过各种混淆、加固等对抗手段，对抗传统特征检测机制。

软件名称	包名	版本	签名信息
色色影院	com.ekwdox.lxcilacz	8608598	CN=arlbwvavbfwp, OU=arlbwvavbfwp, O=arlbwvavbfwp, L=arlbwvavbfwp, ST=arlbwvavbfwp, C=99
色色影院	com.cvgnvr.lrgycgrw	7069258	CN=revaryboachi, OU=revaryboachi, O=revaryboachi, L=revaryboachi, ST=revaryboachi, C=48
色色影院	com.wiwbsx.uwgydbop	3023490	CN=ypeisofjkhdn, OU=ypeisofjkhdn, O=ypeisofjkhdn, L=ypeisofjkhdn, ST=ypeisofjkhdn, C=36
色色影院	com.ugwjkd.vfvgijxq	4219413	CN=qajbuptcghlh, OU=qajbuptcghlh, O=qajbuptcghlh, L=qajbuptcghlh, ST=qajbuptcghlh, C=17
色色影院	com.dxmmeu.tpnlpzby	4484101	CN=kkuogebuhgsg, OU=kkuogebuhgsg, O=kkuogebuhgsg, L=kkuogebuhgsg, ST=kkuogebuhgsg, C=38
色色影院	com.vrhxox.qppldgyr	1010162	CN=wqudmskpvttu, OU=wqudmskpvttu, O=wqudmskpvttu, L=wqudmskpvttu, ST=wqudmskpvttu, C=66
色色影院	com.nlhjfm.npsnoxfg	7816018	CN=aeoqddubfpsv, OU=aeoqddubfpsv, O=aeoqddubfpsv, L=aeoqddubfpsv, ST=aeoqddubfpsv, C=59
色色影院	com.merkmf.lrimgzcd	5702539	CN=aevnzgnkeect, OU=aevnzgnkeect, O=aevnzgnkeect, L=aevnzgnkeect, ST=aevnzgnkeect, C=36
色色影院	com.ysjija.xcdvpdwq	6392941	CN=nhjkxnjgubet, OU=nhjkxnjgubet, O=nhjkxnjgubet, L=nhjkxnjgubet, ST=nhjkxnjgubet, C=09
色色影院	com.hrltqc.bouvdtod	2860215	CN=ymdfwnkwkkuu, OU=ymdfwnkwkkuu, O=ymdfwnkwkkuu, L=ymdfwnkwkkuu, ST=ymdfwnkwkkuu, C=06
色色影院	com.dfjoaa.vzmasxuy	58131	CN=etzaycnsxsfg, OU=etzaycnsxsfg, O=etzaycnsxsfg, L=etzaycnsxsfg, ST=etzaycnsxsfg, C=98
色色影院	com.vbbwyf.belqevyz	8084750	CN=vhmmxdkzndzm, OU=vhmmxdkzndzm, O=vhmmxdkzndzm, L=vhmmxdkzndzm, ST=vhmmxdkzndzm, C=21
色色影院	com.mgicqy.tfnfxvze	3353303	CN=bqocsigaeuwp, OU=bqocsigaeuwp, O=bqocsigaeuwp, L=bqocsigaeuwp, ST=bqocsigaeuwp, C=55
色色影院	com.juvytv.iloccxpi	805390	CN=vyryoqlutzrs, OU=vyryoqlutzrs, O=vyryoqlutzrs, L=vyryoqlutzrs, ST=vyryoqlutzrs, C=34
色色影院	com.mhkjzt.pigtxphv	7824618	CN=itqaisderrut, OU=itqaisderrut, O=itqaisderrut, L=itqaisderrut, ST=itqaisderrut, C=60

目录

天生的克星，AI技术检测

为什么可以用人工智能

从人的视角看该案例，我们可以一眼辨别出来，它们是同一类。因为：
名称一样、包名都已Com开头，签名信息长度一样，等等。

软件名称	包名	版本	签名信息
色色影院	com.ekwdox.lxcilacz	8608598	CN=arlbwvavbfwp, OU=arlbwvavbfwp, O=arlbwvavbfwp, L=arlbwvavbfwp, ST=arlbwvavbfwp, C=99
色色影院	com.cvgnvr.lrgycgrw	7069258	CN=revaryboachi, OU=revaryboachi, O=revaryboachi, L=revaryboachi, ST=revaryboachi, C=48
色色影院	com.wiwbsx.uwgydbop	3023490	CN=ypeisofjkhdn, OU=ypeisofjkhdn, O=ypeisofjkhdn, L=ypeisofjkhdn, ST=ypeisofjkhdn, C=36
色色影院	com.ugwjkd.vfvgijxq	4219413	CN=qajbuptcghlh, OU=qajbuptcghlh, O=qajbuptcghlh, L=qajbuptcghlh, ST=qajbuptcghlh, C=17
色色影院	com.dxmmeu.tpnlpzby	4484101	CN=kkuogebuhgsg, OU=kkuogebuhgsg, O=kkuogebuhgsg, L=kkuogebuhgsg, ST=kkuogebuhgsg, C=38
色色影院	com.vrhxox.qppldgyr	1010162	CN=wqudmskpvttu, OU=wqudmskpvttu, O=wqudmskpvttu, L=wqudmskpvttu, ST=wqudmskpvttu, C=66
色色影院	com.nlhjfm.npsnoxfg	7816018	CN=aeoqddubfpsv, OU=aeoqddubfpsv, O=aeoqddubfpsv, L=aeoqddubfpsv, ST=aeoqddubfpsv, C=59
色色影院	com.merkmf.lrimgzcd	5702539	CN=aevnzgnkeect, OU=aevnzgnkeect, O=aevnzgnkeect, L=aevnzgnkeect, ST=aevnzgnkeect, C=36
色色影院	com.ysjija.xcdvpdwq	6392941	CN=nhjkxnjgubet, OU=nhjkxnjgubet, O=nhjkxnjgubet, L=nhjkxnjgubet, ST=nhjkxnjgubet, C=09
色色影院	com.hrltqc.bouvdtod	2860215	CN=ymdfwnkwkkuu, OU=ymdfwnkwkkuu, O=ymdfwnkwkkuu, L=ymdfwnkwkkuu, ST=ymdfwnkwkkuu, C=06
色色影院	com.dfjoaa.vzmasxuy	58131	CN=etzaycnsxsfg, OU=etzaycnsxsfg, O=etzaycnsxsfg, L=etzaycnsxsfg, ST=etzaycnsxsfg, C=98
色色影院	com.vbbwyf.belqevyz	8084750	CN=vhmmxdkzndzm, OU=vhmmxdkzndzm, O=vhmmxdkzndzm, L=vhmmxdkzndzm, ST=vhmmxdkzndzm, C=21
色色影院	com.mgicqy.tfnfxvze	3353303	CN=bqocsigaeuwp, OU=bqocsigaeuwp, O=bqocsigaeuwp, L=bqocsigaeuwp, ST=bqocsigaeuwp, C=55
色色影院	com.juvytv.iloccxpi	805390	CN=vyryoqlutzrs, OU=vyryoqlutzrs, O=vyryoqlutzrs, L=vyryoqlutzrs, ST=vyryoqlutzrs, C=34
色色影院	com.mhkjzt.pigtxphv	7824618	CN=itqaisderrut, OU=itqaisderrut, O=itqaisderrut, L=itqaisderrut, ST=itqaisderrut, C=60

相似度举例

软件名称	包名	版本	签名信息
快播影音	com.meiriyougou.cn	98139075	CN=leishen, OU=feeker15, O=fee15, L=beijing, ST=chaoyang, C=1
快播影音	com.meiriyougou.cn	11708509	CN=leishen, OU=feeker15, O=fee15, L=beijing, ST=chaoyang, C=1
快播影音	com.meiriyougou.cn	20915778	CN=leishen, OU=feeker15, O=fee15, L=beijing, ST=chaoyang, C=1
快播影音	com.meiriyougou.cn	78334213	CN=leishen, OU=feeker15, O=fee15, L=beijing, ST=chaoyang, C=1

软件名称	包名	版本	签名信息
色色影院	com.ekwdox.lxcilacz	8608598	CN=arlbwvavbfwp, OU=arlbwvavbfwp, O=arlbwvavbfwp, L=arlbwvavbfwp, ST=arlbwvavbfwp, C=99
色色影院	com.cvgnvr.lrgycgrw	7069258	CN=revaryboachi, OU=revaryboachi, O=revaryboachi, L=revaryboachi, ST=revaryboachi, C=48
色色影院	com.wiwbsx.uwgydbop	3023490	CN=ypeisofjkhdn, OU=ypeisofjkhdn, O=ypeisofjkhdn, L=ypeisofjkhdn, ST=ypeisofjkhdn, C=36
色色影院	com.ugwjkd.vfvgijxq	4219413	CN=qajbuptcghlh, OU=qajbuptcghlh, O=qajbuptcghlh, L=qajbuptcghlh, ST=qajbuptcghlh, C=17

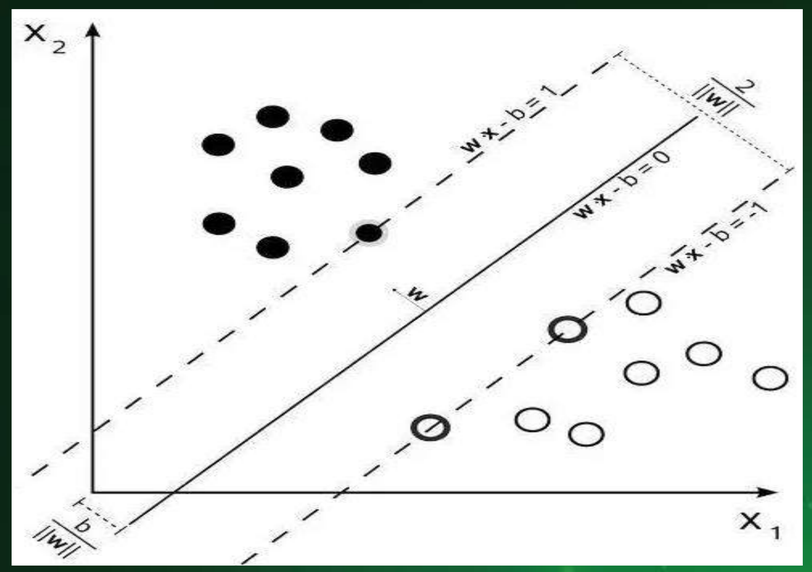
- 软件名称相同
- 包名都是com.开头
- 包名以点号分开，都可以分为三段，且对应每段长度一样
- 包名中都是纯字符串

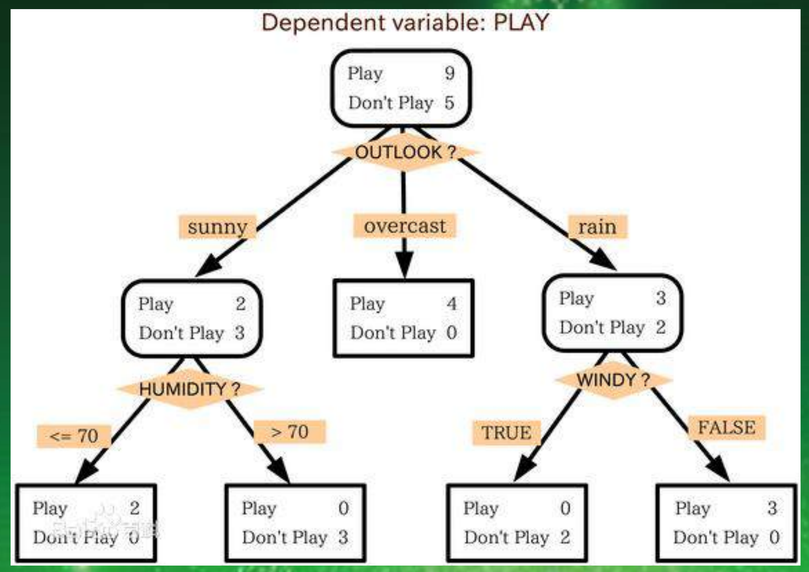
- 整个包名长度一样
- 签名信息长度一样
- 每个签名信息前四段等号后面都相同，且是小写字符串
- 签名信息最后一段等号后面是数字，且只有两位

所以我们人为判断第一部分（快播影音）的四个样本，不仅相互相似，而且与另外一类(色色影院)相似度概率大约在90%以上

机器学习算法

- 支持向量机（Support Vector Machine）
- 决策树（Decision Tree）
- 集成学习（ Ensemble Learning ）





目录

AI技术在APK检测领域的应用

AI技术步骤闭环

效果

- 对新样本的识别率大幅提升
- 模型大小逐渐减低
- 不断自我进化能力
- 极大降低人工成本

目录

APK程序检测分析系统

AI时代移动安全的保障

APK程序检测系统特点

- 静态、动态相结合（静态扫描引擎、动态沙箱系统）
- 传统技术、AI技术相结合（特征码引擎、AI智能引擎）
- 模拟用户操作，自动诱发恶意行为
- 安全告警与修复建议详细报告
- 支持大流量高并发检测，支持横向扩展
- 业内手机安全类产品市场占有率第一（62%市场占有率、71.5%最常使用率）

注：数据来自本次大会官方推荐数据机构：艾媒咨询

THANKS