Realize Innovation of Cyber-Security with Big Data

Qi Xiangdong

I. Initiate the "black-white list" system based on big data

Transform traditional antivirus with big data

In the era of big data, 360 innovatively combines the black list and white list to construct the new “cloud-based antivirus” system, transforming the old antivirus technology.

360 takes a leading role to initiate the “black and white list” system and cloud-based antivirus technology, becoming the model for global Internet security software.

Traditional security vendors		The leading “**cloud-based antivirus**” system of 360
Traditional antivirus Regular upgrade of the virus database	VS	● “Black and white list” system ● Cloud-based antivirus technology and constant upgrade ● QVM AI engine

360 cloud-based antivirus: substantially squeeze the living space of Trojans and virus.

360 deploys over 10 thousand servers in the Cloud Security Center

10T newly added sample data and over 50 billion times of cloud user queries from the Internet each day

360 has the world’s largest database of “black and white list”

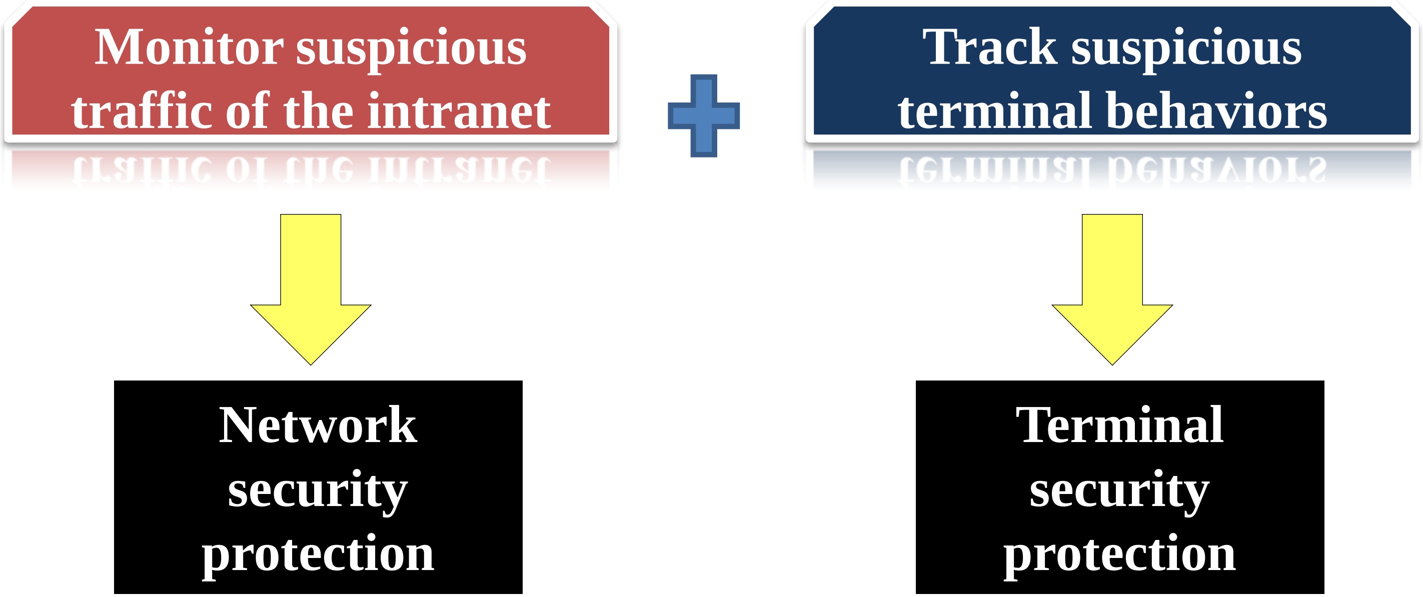
The database of black list contains over 1 billion samples of malicious programs and the database of white list contains around 50 million samples of normal files, covering the operating systems and application software of over 99% Internet users.

360 cloud-based antivirus has dismantled the economic foundation of Trojan industry

360 could realize the “sec-killing” of new Trojans and virus

II. Build the “cloud-based active defense” system with big data

4D active defense system (files, registry, process, and network):



Monitor suspicious traffic of the intranet

+

Track suspicious terminal behaviors

Network security protection

Terminal security protection

Big data provides “gatekeepers” with the analysis and capability to identify malicious attacks.

Timely identify the spread of malware

Identify the different “behaviors” and “trace” of malware and normal software.

◆**Malware: centralized outbreak and surging increase**

◆**Normal software: slow development and curve growth**

Provide criteria for judging network security

Identify intranet attacks through abundant data traffic analysis.

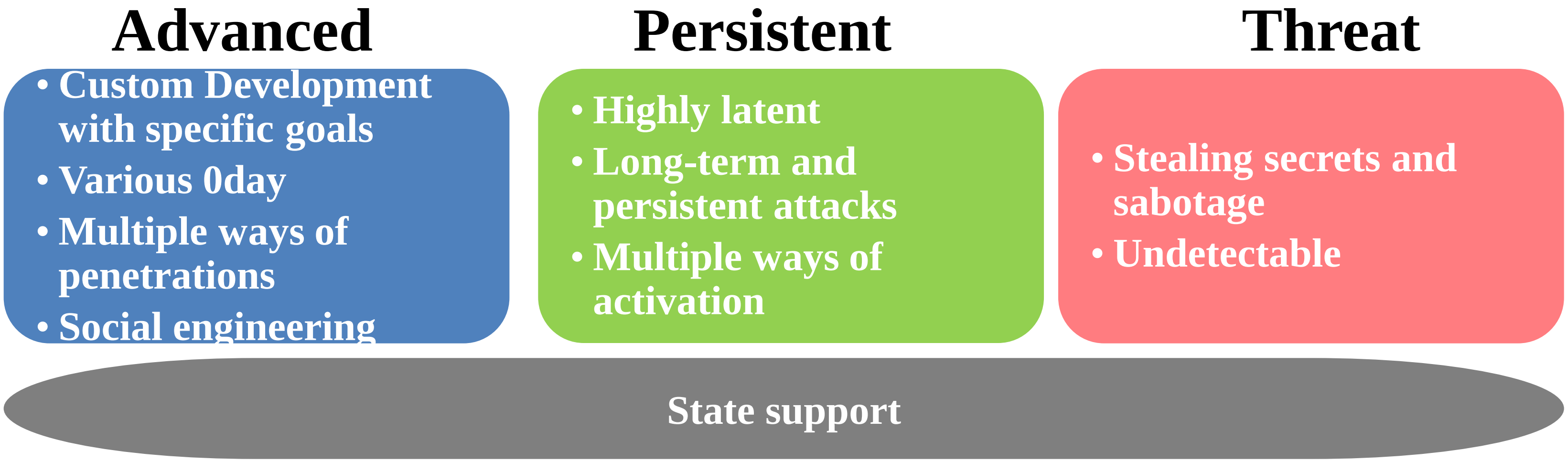
III. Deal with APT attacks based on big data

APT attacks

APT attacks:

Advanced Persistent Threat , APT

It is a advanced, long-term, and persistent attack on specific groups and enterprises by using all loopholes and attack methods. It is generally supported by organizations and states.



Advanced

- **Custom Development with specific goals**
- **Various 0day**
- **Multiple ways of penetrations**
- **Social engineering**

Persistent

- **Highly latent**
- **Long-term and persistent attacks**
- **Multiple ways of activation**

Threat

- **Stealing secrets and sabotage**
- **Undetectable**

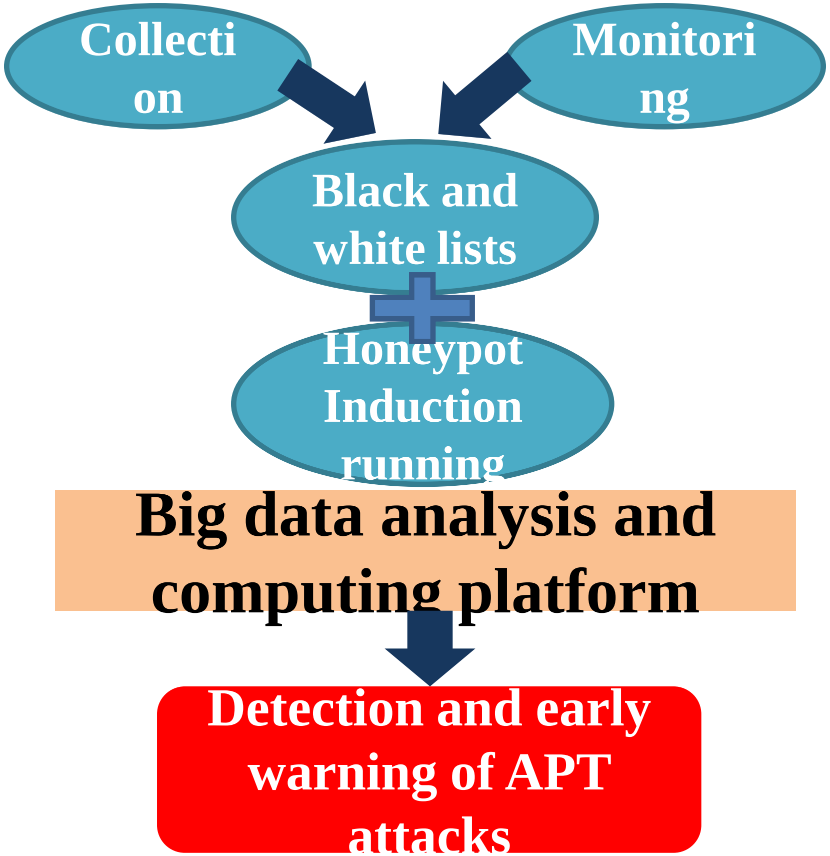
State support

Establish the APT attack detection system based on big data analysis.

Form abundant data resources through sample collection and traffic monitoring

Conduct data mining with cloud storage and cloud computing, and establish the model of software and network behaviors.

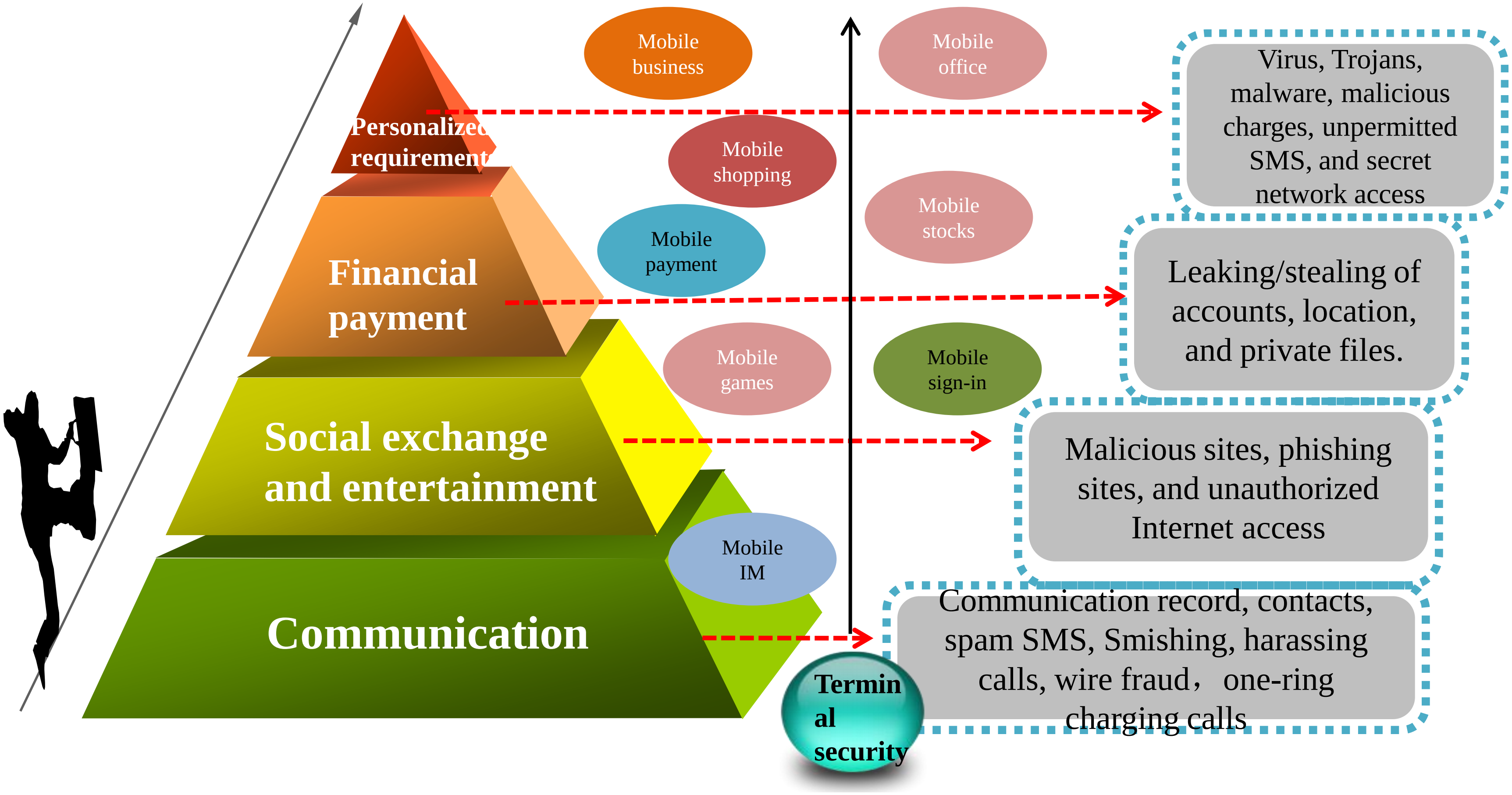
Monitor and prevent abnormal attacks and visits.


Collecti
on
Monitori
ng
Black and white lists
Honeypot Induction running
Big data analysis and computing platform
Detection and early warning of APT attacks

IV. Deal with fraud, harassment, and malware with big data

Network security expands to ubiquitous security

Increasingly serious network security



Virus, Trojans, malware, malicious charges, unpermitted SMS, and secret network access

Leaking/stealing of accounts, location, and private files.

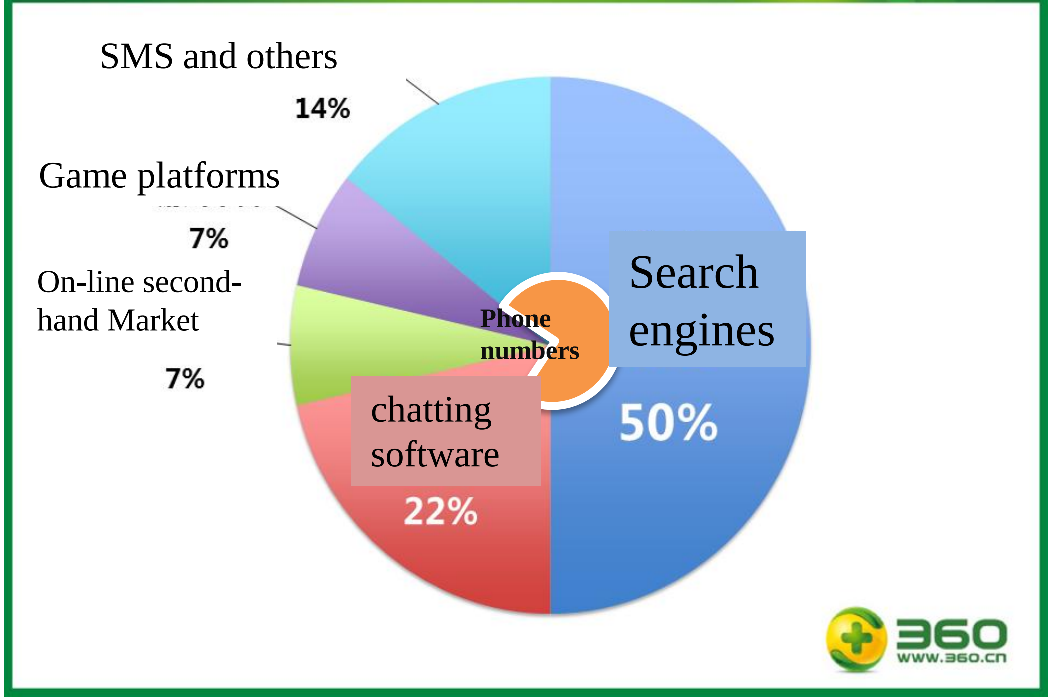
Malicious sites, phishing sites, and unauthorized Internet access

Communication record, contacts, spam SMS, Smishing, harassing calls, wire fraud， one-ring charging calls

Gradual changes of customer needs

Internet fraud

Spreading routes of on-line frauds



Case I:

On April 18, 2014, a university student of Hebei lost around 16000 yuan in a wire fraud by the “fake police” and “fake court”.

国内首例电信诈骗先赔案例诞生
小张莫名接到一个显示为“0335110”的电话
ŋ，赢取安仔和360随身WiFi

Case II:

Cross-provincial wire fraud in Guangdong

Fraudsters cheat users by fake sales of mobile phones and motorcycle through 21 websites, and put their websites in the top page in search sites by 100 yuan per day.
In the investigation, policemen tracked a “133…” mobile phone number and searched key words such as “Apple”, “computer”, and “motorcycle” to eventually uncover the crime

Case III:

In Jun, 2014, movie star Tang Wei lost 210000 yuan in a wire fraud in Shanghai

Harassing phone calls

In the first quarter of 2014, the **newly added** harassing phone call numbers reached **11.86** million;

The number of active harassing phone call numbers nationwide reached over **2.3** million per day;

In the first quarter of 2014, around **80 million** users labelled over **100 million times** of harassing phone calls.

Spam SMS

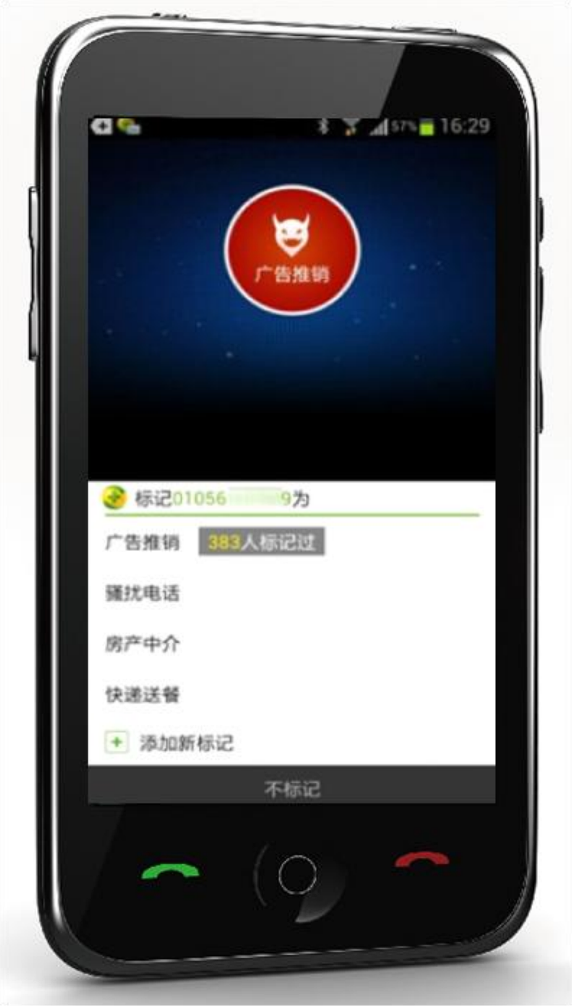
In the first quarter of 2014, 360 Mobile Phone Guard intercepted **20.88 billion** spam SMSs, **232 million** per day in average.

Users report **61.30 million** spam SMSs, **681 thousand** per day in average.

The report & interception rate of 360 Mobile Phone Guard is **0.29%**

360互联网安全中心
360 INTERNET SECURITY CENTER

Inquiry, labeling and report



标记01056[redacted]9为

广告推销 383人标记过

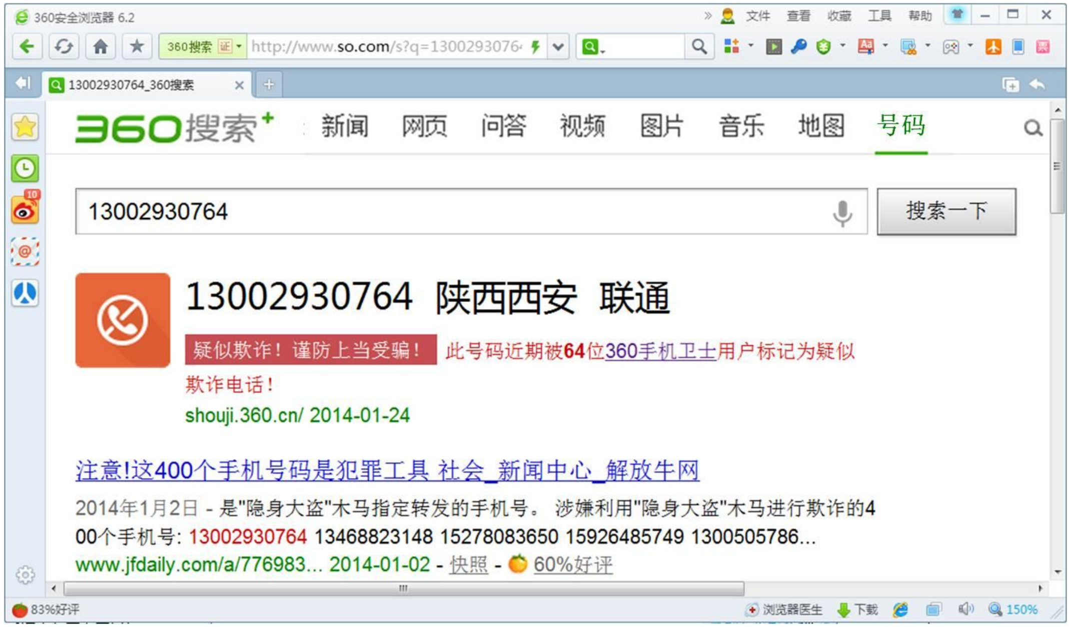
骚扰电话

房产中介

快递送餐

+ 添加新标记

不标记



13002930764

13002930764 陕西西安 联通

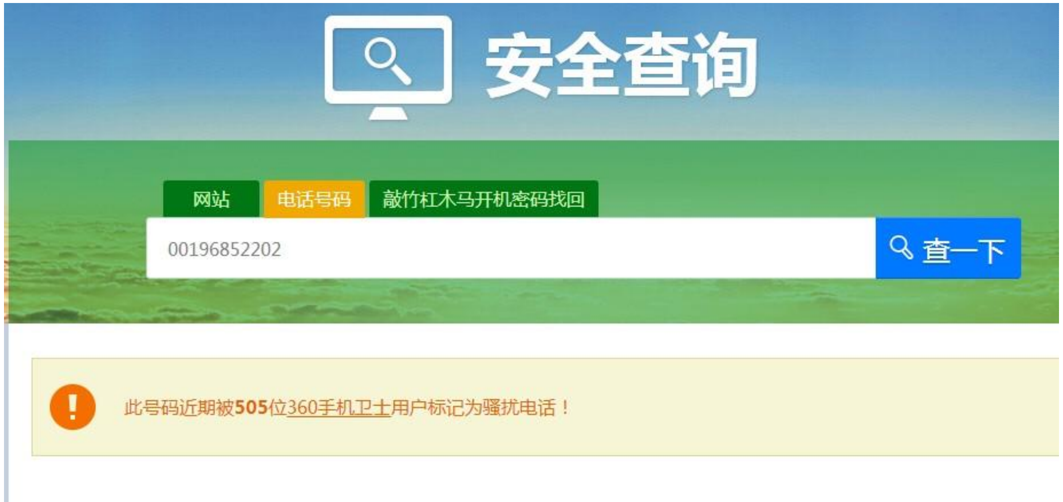
疑似欺诈！谨防上当受骗！ 此号码近期被**64**位360手机卫士用户标记为疑似欺诈电话！

shouji.360.cn/ 2014-01-24

注意!这400个手机号码是犯罪工具 社会_新闻中心_解放牛网

2014年1月2日 - 是"隐身大盗"木马指定转发的手机号。 涉嫌利用"隐身大盗"木马进行欺诈的400个手机号: 13002930764 13468823148 15278083650 15926485749 1300505786...

www.jfdaily.com/a/776983... 2014-01-02 - 快照 - 60%好评

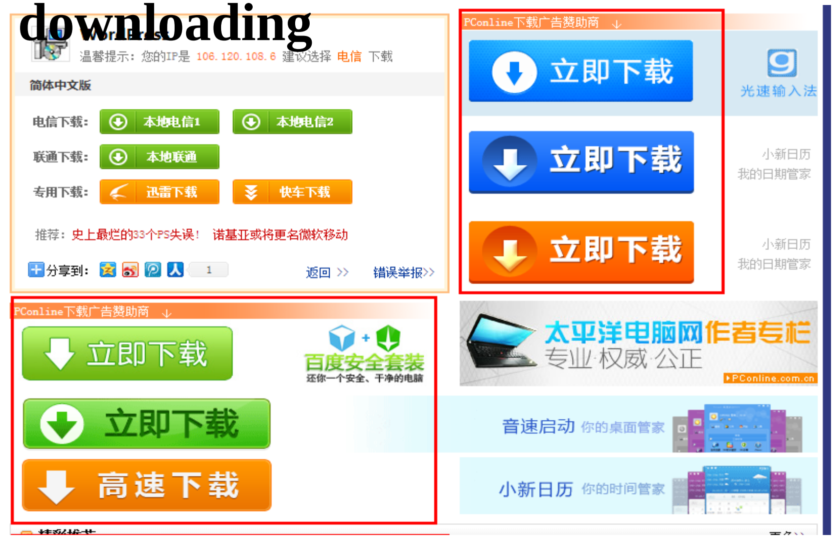


00196852202

此号码近期被**505**位360手机卫士用户标记为骚扰电话！

Growing bundling and harassment

Website popups-cheated downloading



WordPress

温馨提示：您的IP是 106.120.108.6 建议选择 电信 下载

简体中文版

电信下载： 本地电信1 本地电信2

联通下载： 本地联通

专用下载： 迅雷下载 快车下载

推荐：史上最烂的33个PS失误！ 诺基亚或将更名微软移动

分享到： 1 返回 >> 错误举报>>

PConline下载广告赞助商

立即下载

立即下载

立即下载

光速输入法

小新日历 我的日期管家

小新日历 我的日期管家

PConline下载广告赞助商

立即下载

立即下载

高速下载

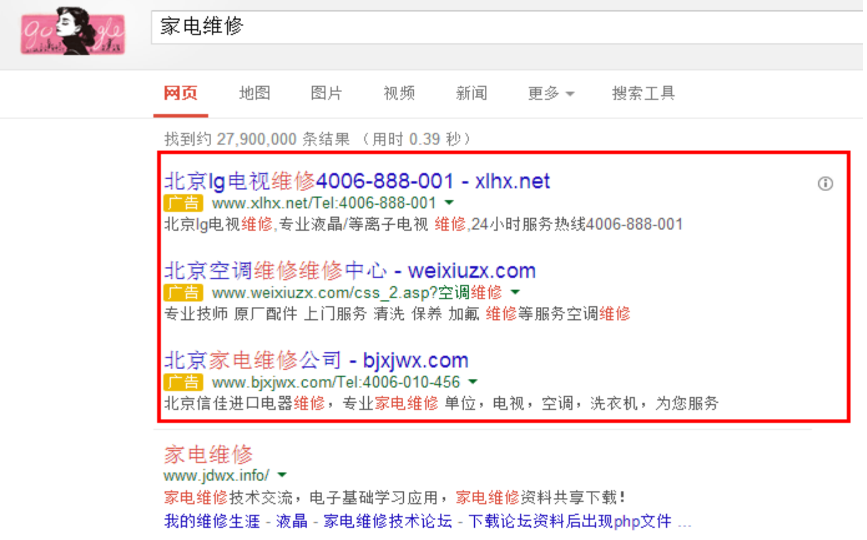
百度安全套装 还你一个安全、干净的电脑

太平洋电脑网作者专栏 专业·权威·公正 PConline.com.cn

音速启动 你的桌面管家

小新日历 你的时间管家

Search engine-fake promotion



家电维修

网页 地图 图片 视频 新闻 更多 搜索工具

找到约 27,900,000 条结果 （用时 0.39 秒）

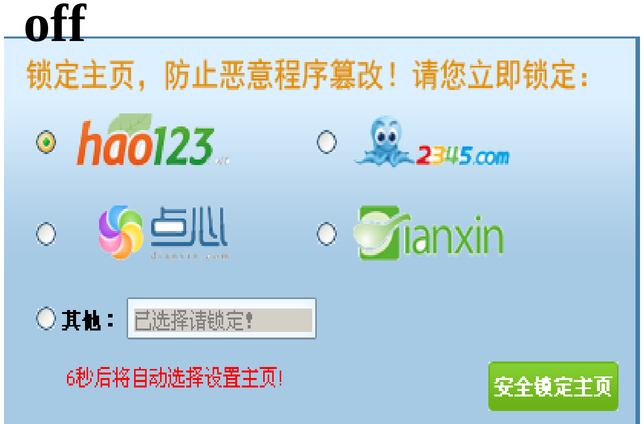
北京lg电视维修4006-888-001 - xlhx.net
广告 www.xlhx.net/Tel:4006-888-001
北京lg电视维修,专业液晶/等离子电视 维修,24小时服务热线4006-888-001

北京空调维修维修中心 - weixiuzx.com
广告 www.weixiuzx.com/css_2.asp?空调维修
专业技师 原厂配件 上门服务 清洗 保养 加氟 维修等服务空调维修

北京家电维修公司 - bjxjwx.com
广告 www.bjxjwx.com/Tel:4006-010-456
北京信佳进口电器维修，专业家电维修 单位，电视，空调，洗衣机，为您服务

家电维修
www.jdwx.info/
家电维修技术交流，电子基础学习应用，家电维修资料共享下载！
我的维修生涯 - 液晶 - 家电维修技术论坛 - 下载论坛资料后出现php文件 ...

Client popups-auto off



锁定主页，防止恶意程序篡改！请您立即锁定：

● hao123 ○ 2345.com

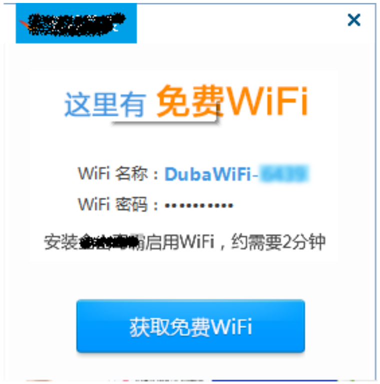
○ 点心 ○ Tianxin

○ 其他： 已选择请锁定!

6秒后将自动选择设置主页!

安全锁定主页

Client popups-traps



[redacted] ×

这里有免费WiFi

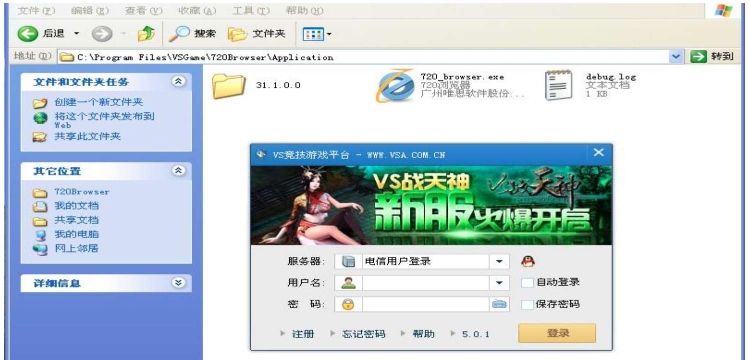
WiFi 名称：DubaWiFi-[redacted]

WiFi 密码：••••••••••

安装[redacted]启用WiFi，约需要2分钟

获取免费WiFi

Client popups-compulsive bundling



文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

后退 搜索 文件夹

地址(D) C:\Program Files\VSGame\720Browser\Application 转到

文件和文件夹任务
创建一个新文件夹
将这个文件夹发布到 Web
共享此文件夹

其它位置
720Browser
我的文档
共享文档
我的电脑
网上邻居

详细信息

31.1.0.0

720_browser.exe
720浏览器
广州唯思软件股份...

debug.log
文本文档
1 KB

VS竞技游戏平台 - WWW.VSA.COM.CN

VS战天神 新服火爆开启

服务器： 电信用户登录

用户名： □ 自动登录

密 码： □ 保存密码

注册 忘记密码 帮助 5.0.1 登录

Boycott: Pre-installation and bundling, and scampish promotion

Intercept ion

Harassing ads and bundled software

Cleaning

Seldom-used and junk software

Warning

Fraud promotion and malicious attacks

Flooding bundled mobile phone and PC software

Vote with mouse. Protect user’s right to know and right of choice.

V. Application of big data

Value and contribution of 360 to users

Driven by the concept of "**free security**" of 360, China becomes the first nation with free security and antivirus service for users.

40 to 80 billion yuan RMB in security software is saved for Internet users each year

Intercept 130 billion spam SMSs each year

Intercept 64 million harassing phone calls each year

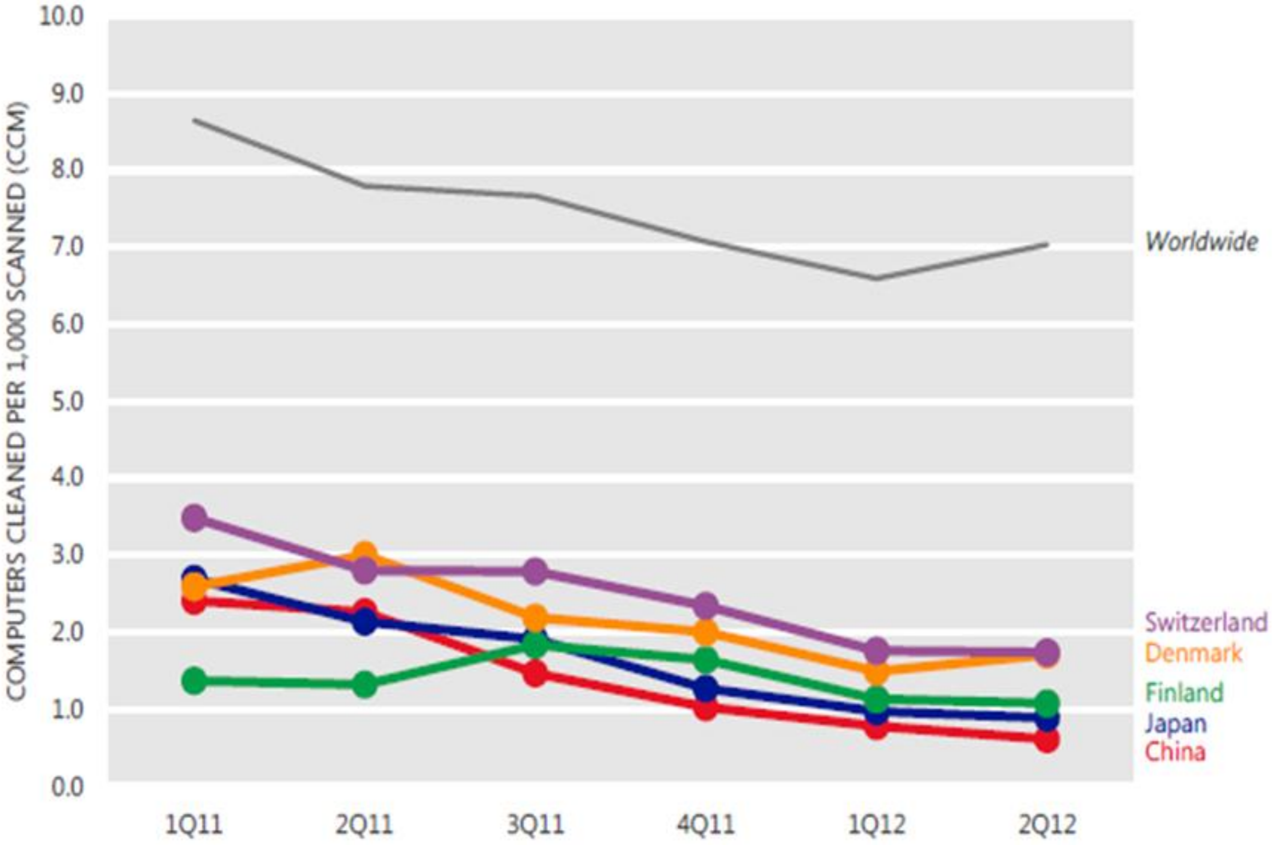
Intercept 2 billion times of bundled software each year

58 billion warnings for phishing and malicious attacks

The success rate of phishing websites is 1% only.

Microsoft: China reports the lowest infection rate in the world

According to the official security report of Microsoft in 2013, the infection rate of malware of Chinese PCs was **0.6‰**, **1/10 of the global average**. It makes China the nation of **lowest infection**.



In recent years, the infection rate of malware in China is decline rapidly. This is because the penetration of **free security software, such as 360,** has played a crucial role in the process. Currently, the penetration of PC security software has reached **99%**.

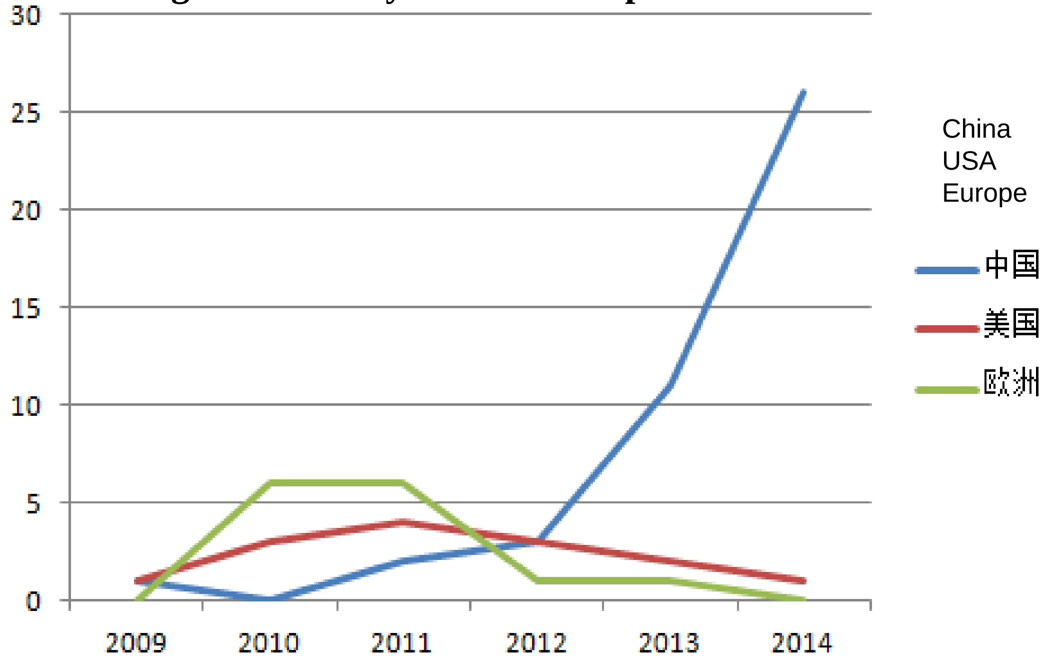
Driven by the concept of "**fee security**" of 360, China becomes the first nation with free security and antivirus service for users.

The Threat Landscape in China: A Paradox

360 Lab against loopholes

——The largest white-hat group of
the Eastern Hemisphere

Discovery of loopholes of Microsoft operating system by global security software companies.



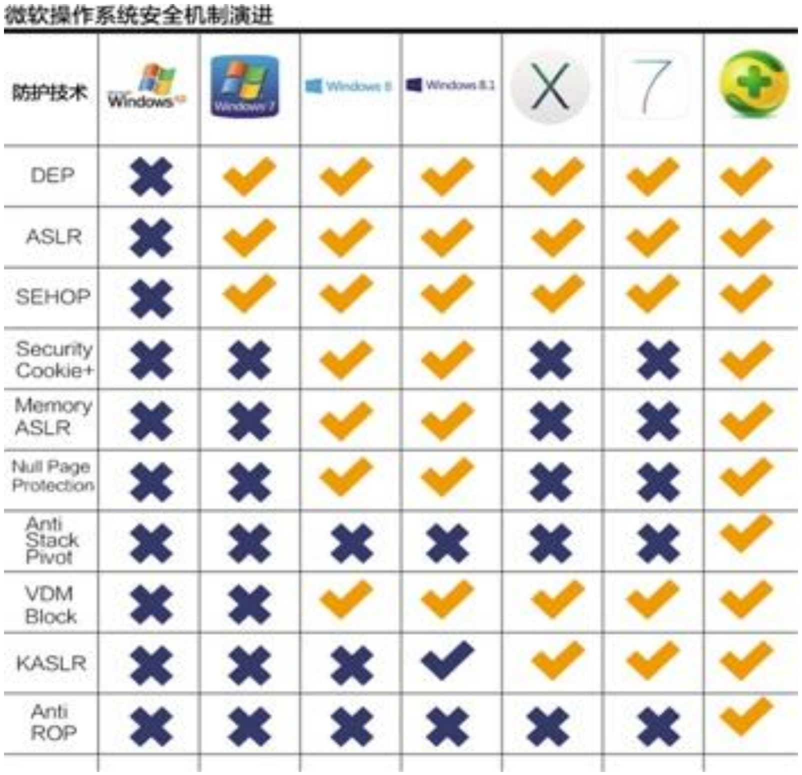
Currently, the number of loopholes reported to Microsoft by 360 ranks first in the world, far ahead of traditional giants as Symantec, McAfee, and Kaspersky.

So far, 360 has received **39** open letters of thanks, and has world-leading technologies in loophole discovery and professional protection.

360 reports 90% of loopholes discovered by Chinese security software companies.

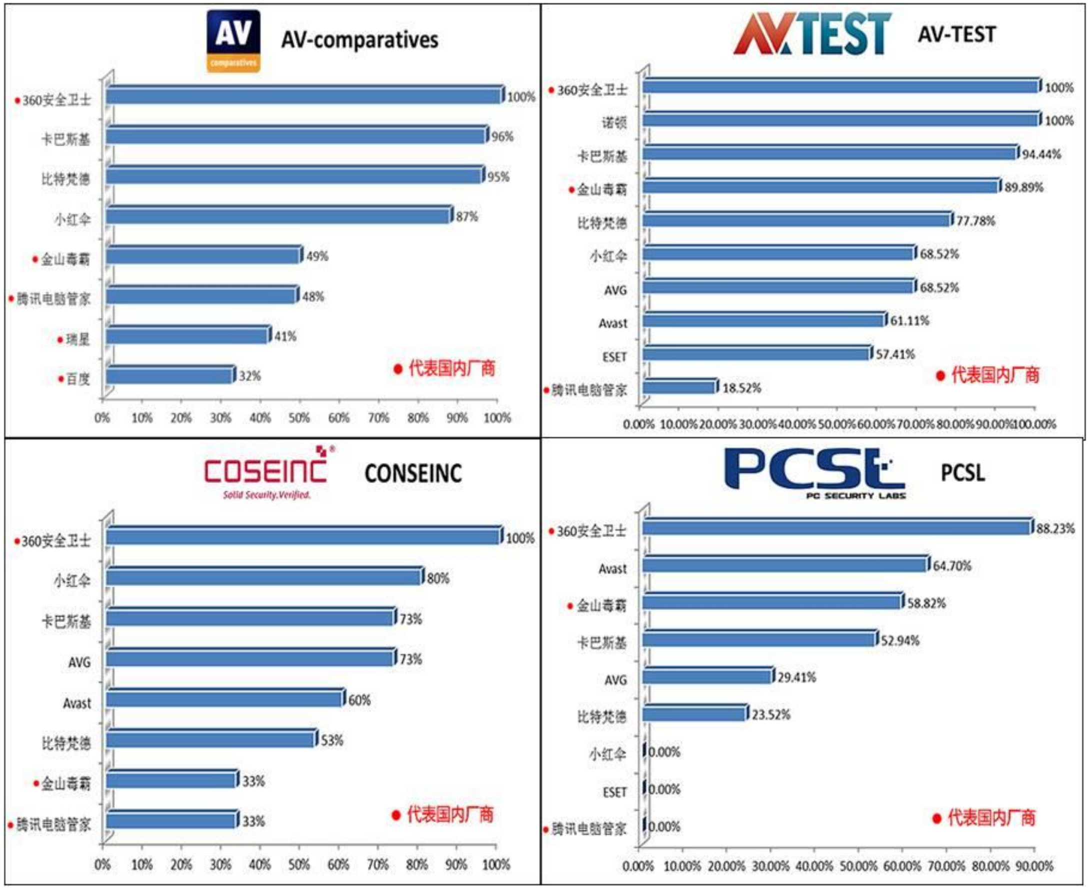
System protection and XP shield

360 initiates system consolidation, isolated protection, and other security technologies. As the only domestic security products of loophole defense, 360 is capable of defending back-door attacks of operating systems.



微软操作系统安全机制演进

防护技术	Windows XP	Windows 7	Windows 8	Windows 8.1	X	7	
DEP	✗	✓	✓	✓	✓	✓	✓
ASLR	✗	✓	✓	✓	✓	✓	✓
SEHOP	✗	✓	✓	✓	✓	✓	✓
Security Cookie+	✗	✗	✓	✓	✗	✗	✓
Memory ASLR	✗	✗	✓	✓	✗	✗	✓
Null Page Protection	✗	✗	✓	✓	✗	✗	✓
Anti Stack Pivot	✗	✗	✗	✗	✗	✗	✓
VDM Block	✗	✗	✓	✓	✓	✓	✓
KASLR	✗	✗	✗	✓	✓	✓	✓
Anti ROP	✗	✗	✗	✗	✗	✗	✓



Four major international tests of XP protection

360 keeps you safe in Internet surfing