LEARNING MALWARE IN CLOUD AND VIRTUALIZATION AGE

Zhao Wei
KnownSec

Who am I?
Who are we?

About This Presentation

1. Part One: Malware industry in China
2. Part Two: What we learned from malware
3. Part Three: Our “Steam” and Virtualization System

Underground Malware Industry

Underground Malware Industry

Now

China is not only the world’s factory,
but also the world’s *malware* factory

They totally changed our life

1. My parents’ computer!☹
2. Changed how people are using the network/internet
3. Maybe they are more cloud than us☹

Underground Malware Industry

4 tech waves

1. Server Side Wave 1998-2003
   1) IIS, Serv-U, Apache, Samba, Jabberd etc
2. Client Side Trend 2002-2007
   1) Image format: ANI, JPG, BMP etc
   2) Windows Office doc, ppt etc
   3) IE: ActiveX, HTML parser, XML parser
3. 3rd party applications attacking 2006-NOW, this done only for profit
4. 0day, Anti-Anti-Virus and underground industry

Underground Malware Industry

Trend

1. From 06-07 they started using 3rd party vulns， Why?
   1) Very big local market and huge amount of users
   2) Users know more about security now (patch system, using anti-virus etc.)
   3) Some local security vendors supply patch service to users of pirated Windows (They all love it☺)
   4) Windows 0days really expensive now
   5) Local application vendors are totally lame (sell them Fortify!)
2. They use 0days in massive attacks, I’d never seen this before 2006, definitely a phenomenon
3. More 0days?
   1) RealPlayer
   2) Flash
   3) XunLei*
   4) UUSee
   5) Sina

Underground Malware Industry

Technique Trend

1. They like exploiting logic bugs

   1) Baidu Toolbar

   2) Snapshot

2. *Anti* Anti-Virus

   Detect if Anti-virus exists

3. Bypass anti-virus: they charge money to make your malware bypass:

   1) Kaspersky

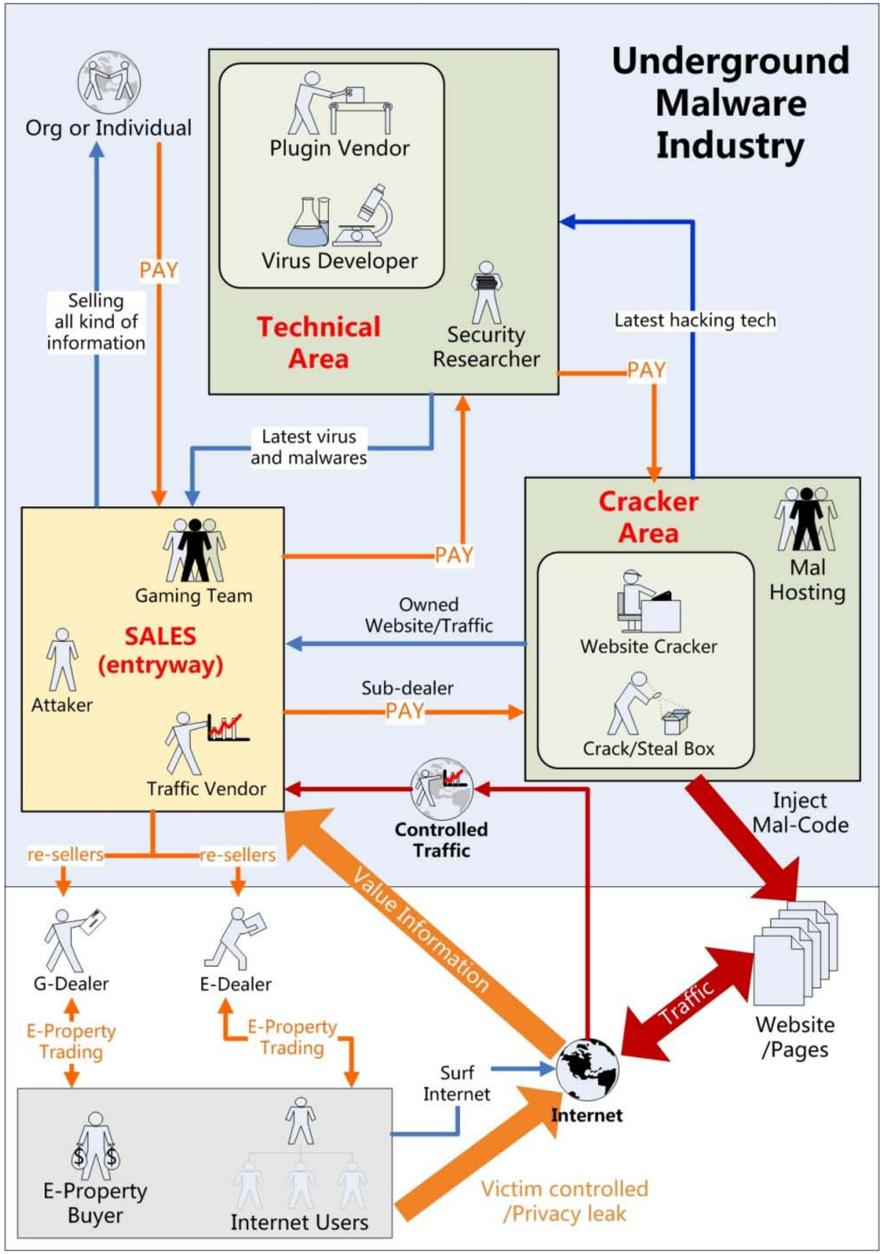
   2) Nod32

   3) Rising

   4) Kingsoft

Underground Malware Industry

Map



Underground Malware Industry

Next?

- Web 2.0? SNS worm☹
  - At Xkungfoo(xcon) 2008 we talked about SNS worm plus drive-by download attacks http://hi.baidu.com/ycosxhack/blog/item/c28fed54d7d0a35fd0090636.html
  - This year something real
    - QQ zone worm http://forum.eviloctal.com/viewthread.php?tid=35024
- Interactive web malware
  - Interacts with user to make *anti* anti-virus
  - Authentication
  - Flash AS
  - Silverlight?

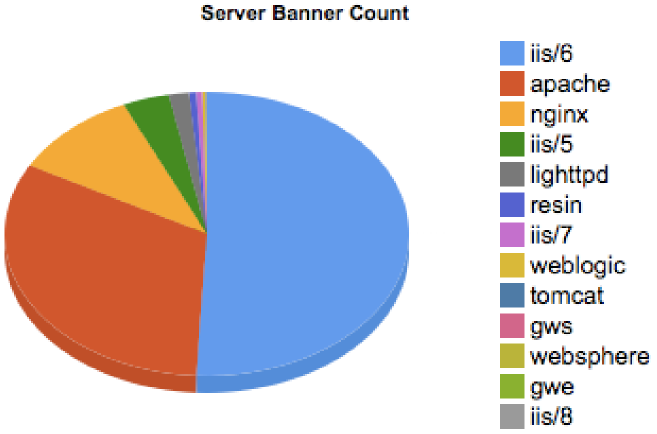
What We Learned

What we learned

The Root

- What make of China web?
  - Half of it is IIS6
  - And Apache
  - SQL injection and application

  Vulnerabilities
- The root problem of China malware
  - Poor web security☹
  - Web sites injected drive-by download attacks
  - We need find them all(How to do that?)



What we learned

Our System ScanW

- We need find all these websites
- Started in 2006
- We learned from:
  - *Google* safe browsing
  - Microsoft HoneyMonkey
  - McAfee SiteAdvisor
- We are based on:
  - Vmware Server 2.0
  - Python 2.5
  - Django 1.0
  - C
- We try to move these things to:
  - Google APP engine (GFW?)
  - Or using Hadoop (Java)?

What we learned

Our System ScanW

- We are not Google☺
  - Lacking enough bandwidth
  - Not enough servers (just mist/water vapor rather than a cloud ☺)
- So these make our sandbox different
  - The main idea is not to get infected
  - Lightweight, faster
  - Behavior basis (APIs)
  - Suitable for China

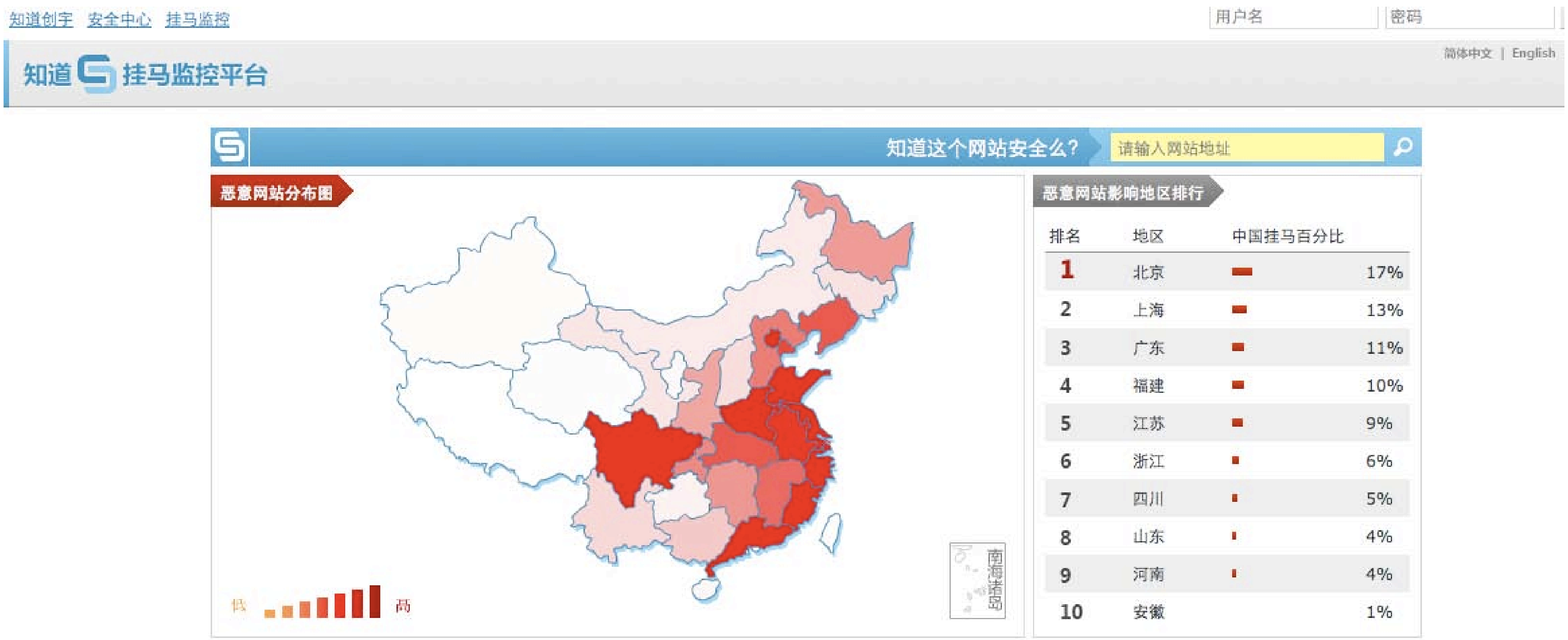
What we learned

Malware

- The problems:
  - 80-90% victims get infected from the web
  - Poor web application security
  - Vulnerabilities in Internet Explorer and 3rd party vulnerabilities
  - 0day world! Using 0days to attack people
- What we can do for users?
  - Make a safer IE?
  - Make a clean/trustworthy web?

What we learned

Top 10 Malware Areas



知道创宇 安全中心 挂马监控

用户名 密码

简体中文 | English

知道 挂马监控平台

知道这个网站安全么? 请输入网站地址

恶意网站分布图

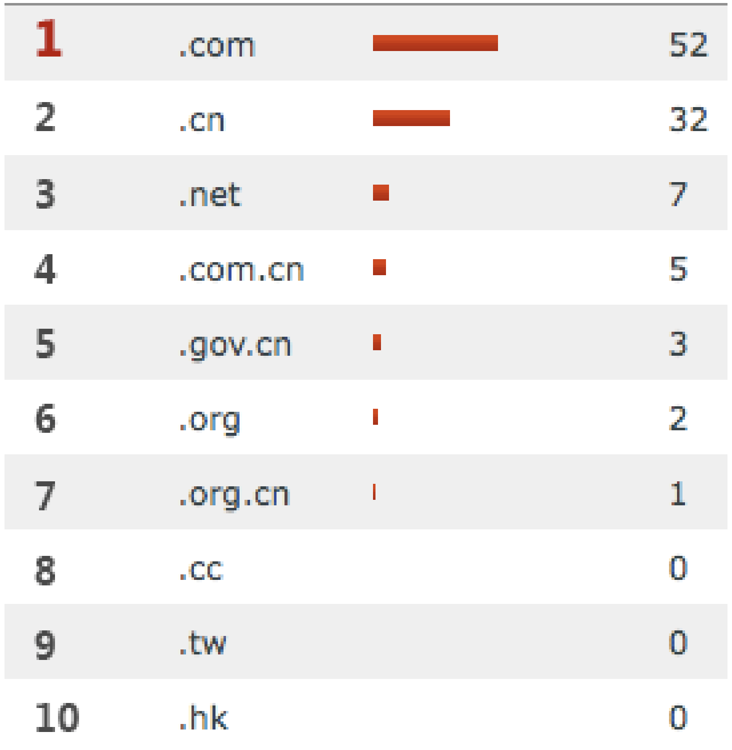
恶意网站影响地区排行

排名	地区	中国挂马百分比	
1	北京	▬	17%
2	上海	▬	13%
3	广东	▬	11%
4	福建	▬	10%
5	江苏	▬	9%
6	浙江	▪	6%
7	四川	▪	5%
8	山东	▪	4%
9	河南	▪	4%
10	安徽		1%

What we learned

Top 10 Domains

1. We monitor **4,071,927** websites every day
2. Around 0.3% of them are malicious per day
3. Found **89073** websites were malicious at least once (2.2%)



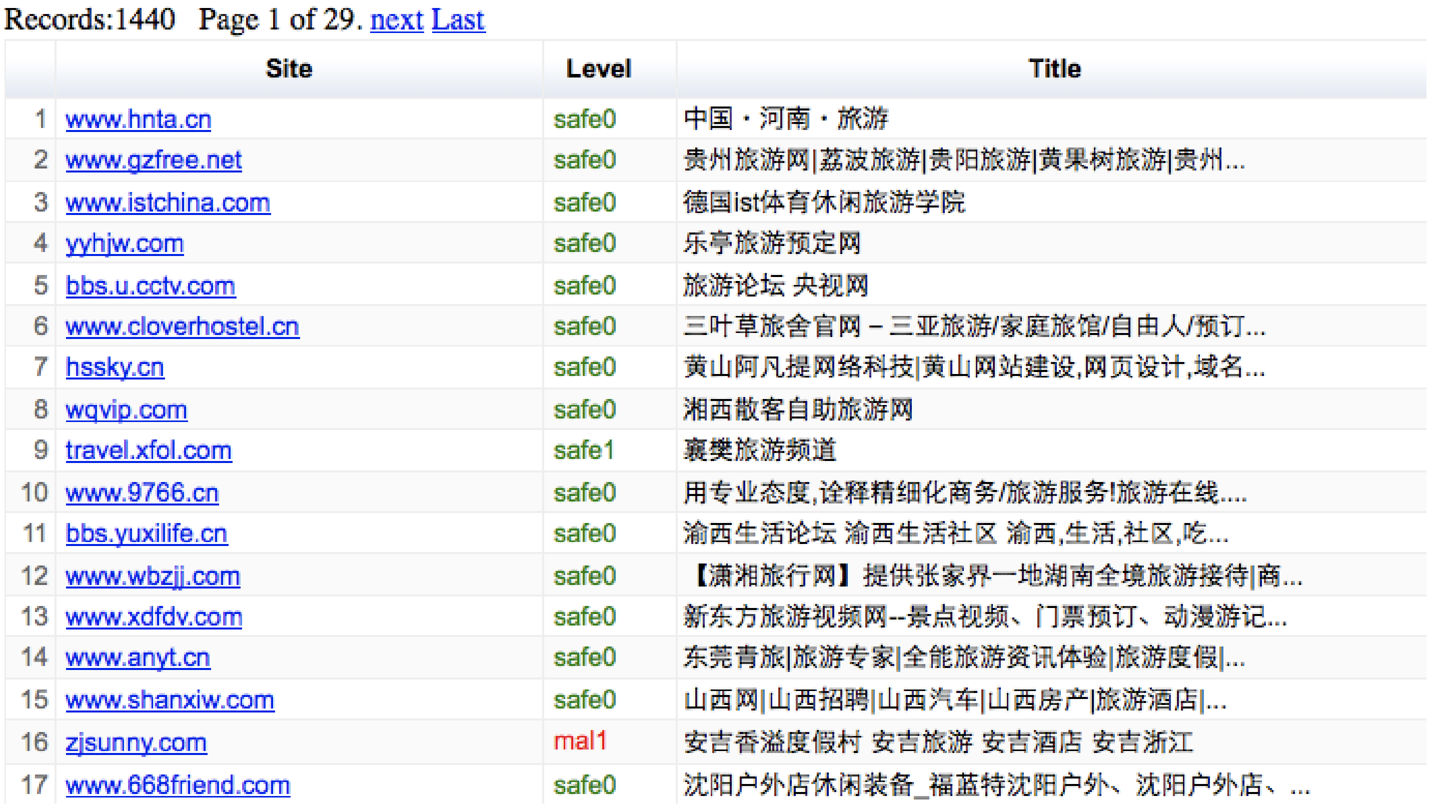
1	.com	52
2	.cn	32
3	.net	7
4	.com.cn	5
5	.gov.cn	3
6	.org	2
7	.org.cn	1
8	.cc	0
9	.tw	0
10	.hk	0

Title Include: Bank,
insurance,
网站数目:9465 这些网站
中出现过挂马的数目:
318 比例:3.4%

What we learned

Target Attack + Mass Attack

1. They are using some popular keywords
2. Title Including Bank, Insurance, Securities 318 of 9465 are malicious
3. Tile Including travel when there is a holiday.

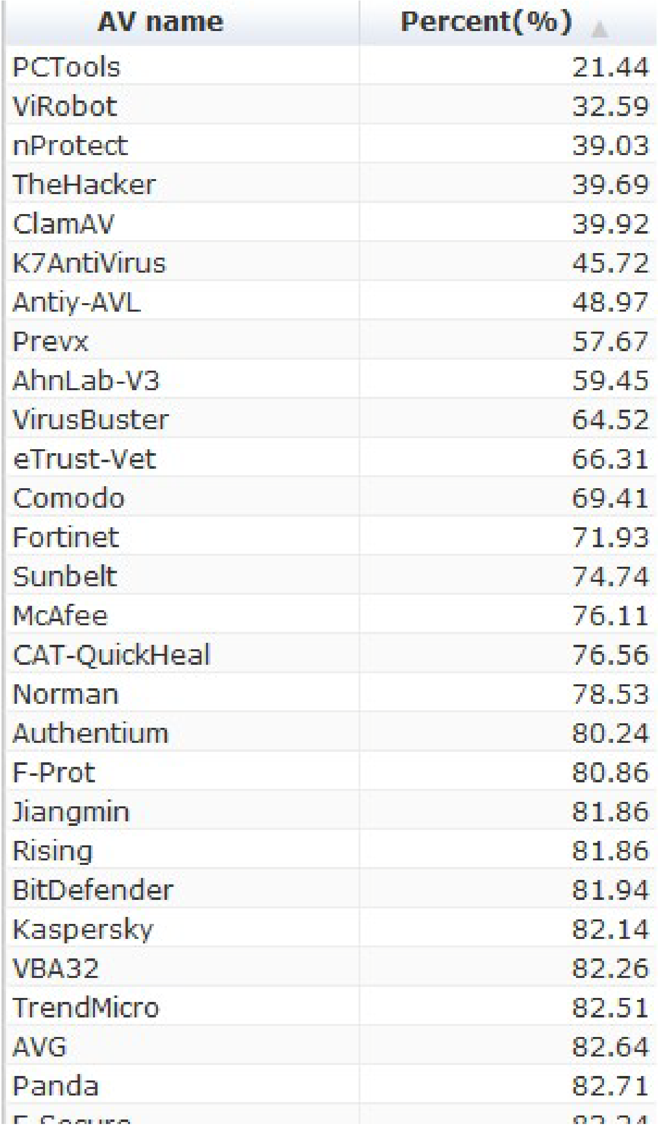


Records:1440 Page 1 of 29. next Last

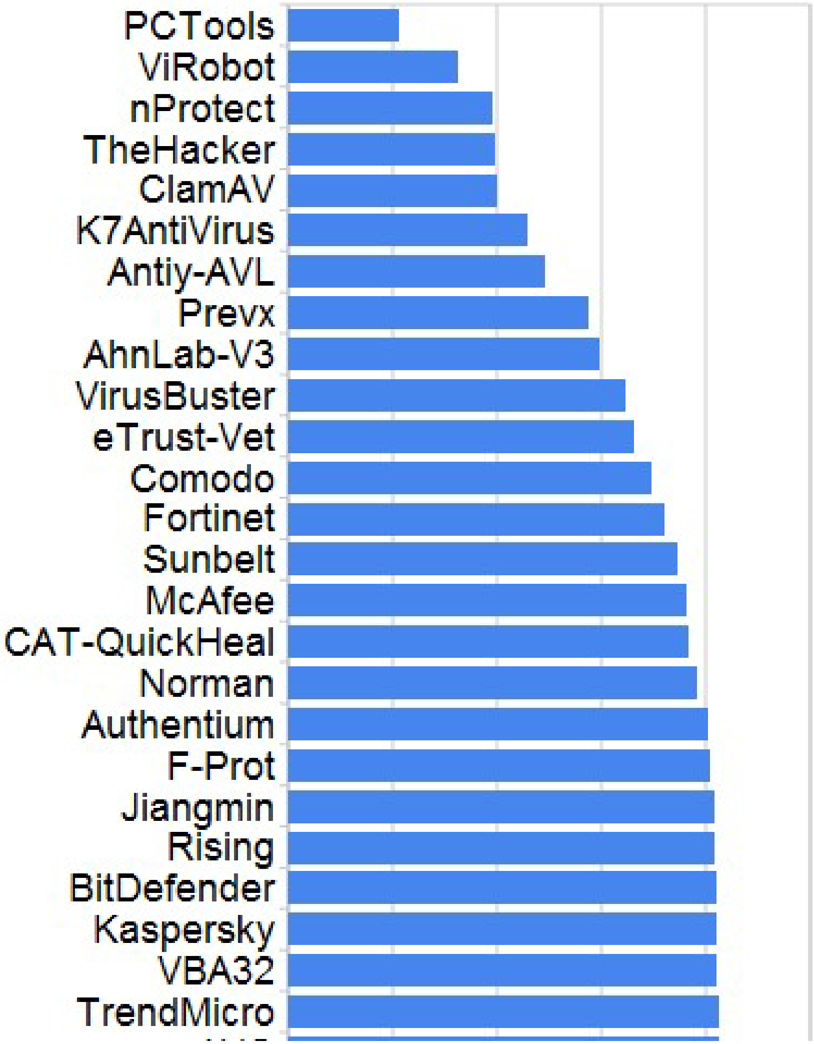
	Site	Level	Title
1	www.hnta.cn	safe0	中国・河南・旅游
2	www.gzfree.net	safe0	贵州旅游网|荔波旅游|贵阳旅游|黄果树旅游|贵州...
3	www.istchina.com	safe0	德国ist体育休闲旅游学院
4	yyhjw.com	safe0	乐亭旅游预定网
5	bbs.u.cctv.com	safe0	旅游论坛 央视网
6	www.cloverhostel.cn	safe0	三叶草旅舍官网－三亚旅游/家庭旅馆/自由人/预订...
7	hssky.cn	safe0	黄山阿凡提网络科技|黄山网站建设,网页设计,域名...
8	wqvip.com	safe0	湘西散客自助旅游网
9	travel.xfol.com	safe1	襄樊旅游频道
10	www.9766.cn	safe0	用专业态度,诠释精细化商务/旅游服务!旅游在线....
11	bbs.yuxilife.cn	safe0	渝西生活论坛 渝西生活社区 渝西,生活,社区,吃...
12	www.wbzjj.com	safe0	【潇湘旅行网】提供张家界一地湖南全境旅游接待|商...
13	www.xdfdv.com	safe0	新东方旅游视频网--景点视频、门票预订、动漫游记...
14	www.anyt.cn	safe0	东莞青旅|旅游专家|全能旅游资讯体验|旅游度假|...
15	www.shanxiw.com	safe0	山西网|山西招聘|山西汽车|山西房产|旅游酒店|...
16	zjsunny.com	mal1	安吉香溢度假村 安吉旅游 安吉酒店 安吉浙江
17	www.668friend.com	safe0	沈阳户外店休闲装备_福蓝特沈阳户外、沈阳户外店、...

What we learned

Top AV Engines



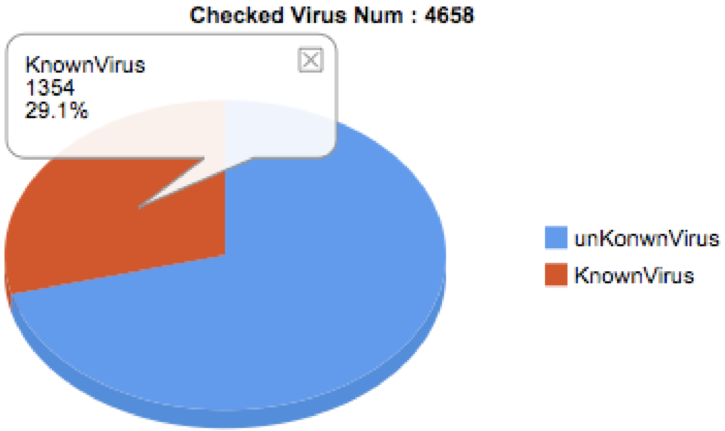
AV name	Percent(%) ▲
PCTools	21.44
ViRobot	32.59
nProtect	39.03
TheHacker	39.69
ClamAV	39.92
K7AntiVirus	45.72
Antiy-AVL	48.97
Prevx	57.67
AhnLab-V3	59.45
VirusBuster	64.52
eTrust-Vet	66.31
Comodo	69.41
Fortinet	71.93
Sunbelt	74.74
McAfee	76.11
CAT-QuickHeal	76.56
Norman	78.53
Authentium	80.24
F-Prot	80.86
Jiangmin	81.86
Rising	81.86
BitDefender	81.94
Kaspersky	82.14
VBA32	82.26
TrendMicro	82.51
AVG	82.64
Panda	82.71
F-Secure	83.24

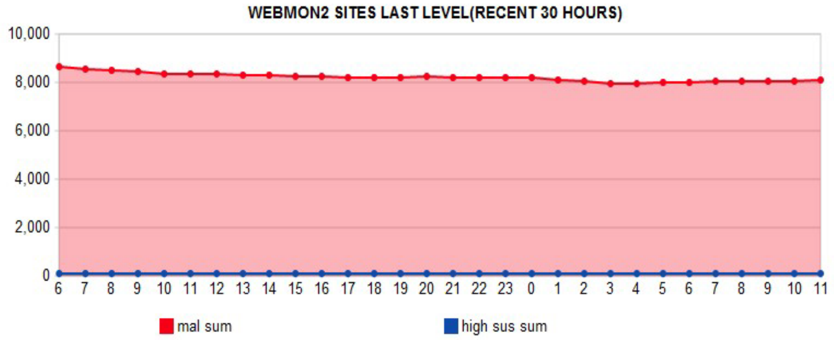


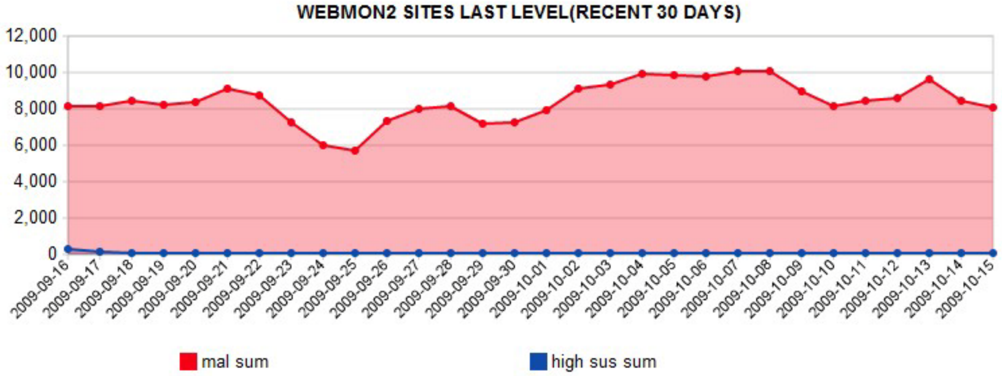
What we learned

What we found

1. Malware market is busy
    1. They do a lot of things to anti anti-virus
    2. They heavily depend on downloaders
2. We capture all kinds of downloaders
    1. 858 downloaders per day
    2. Around 16% are new
3. We check them on VirusTotal, we found:
    1. 71% of them are new to VT
    2. Average detection rate is around 60%(already on VT)







How to find them?

Webmon Open APIs and Malware URL Data Feed

- Webmon Open APIs
  - Why: We believe our information is useful and we also need your help☺
  - What: We share malware and malicious websites information
  - How: http json apis
- Malware Urls Data Feed
  - FTP download
  - Email real time feed

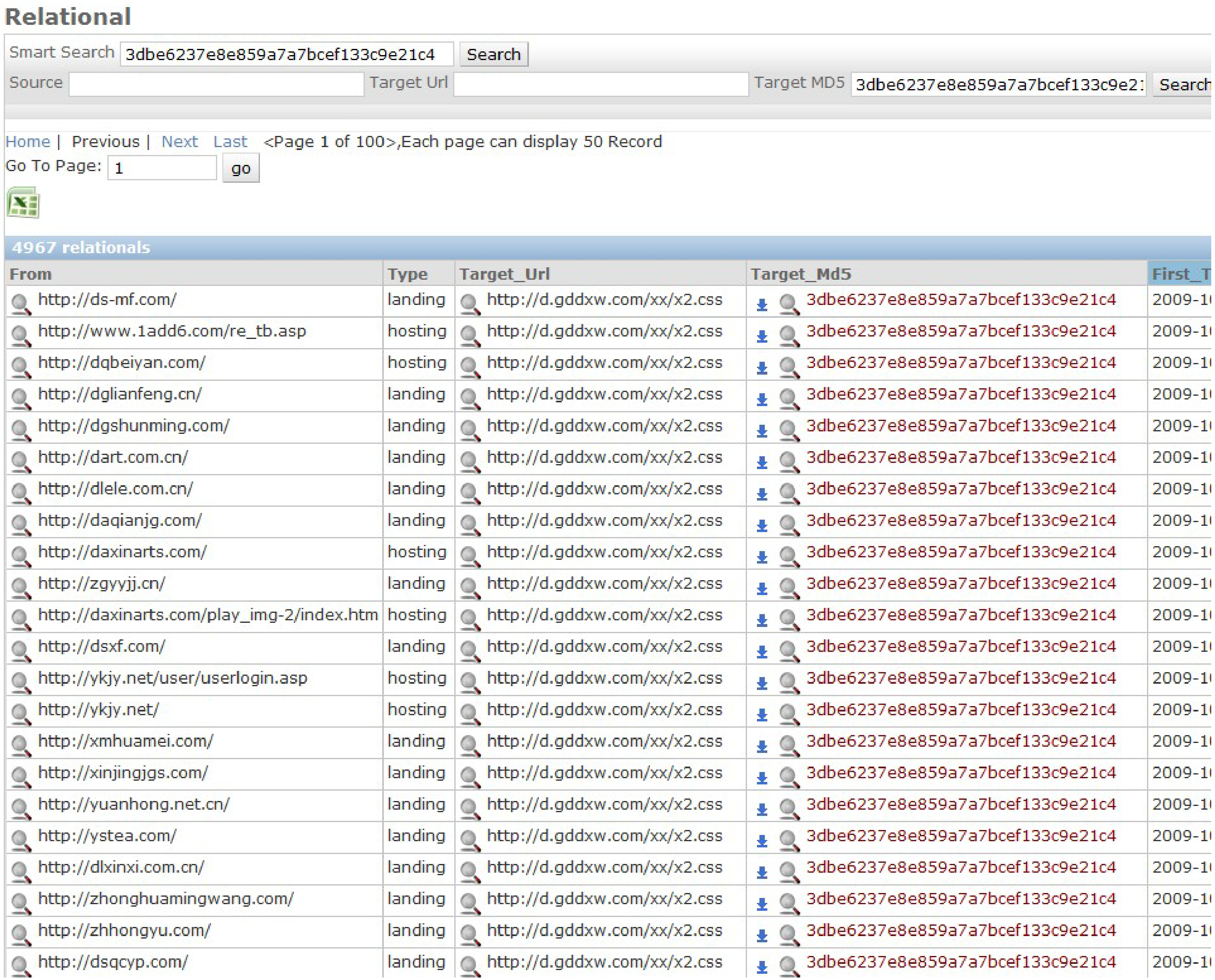
How to find them?

Webmon Open APIs

- Website reputation api☺
  - Function: Checking the history of websites we monitoring
  - Format: https://webmon.knownsec.com/apis/open_query?site=www.yoursite.com&type=[text|json]
- Website scan api
  - Function: Behavior-based real-time check
  - Format: https://webmon.knownsec.com/apis/scan?urls=url1, url2,..,urln&key=secret-key
- Beta testing invitation mail: sec@knownsec.com

How to find them?

Knownsec Intelligence Portal



Relational

Smart Search 3dbe6237e8e859a7a7bcef133c9e21c4 Search

Source Target Url Target MD5 3dbe6237e8e859a7a7bcef133c9e2 Search

Home | Previous | Next Last <Page 1 of 100>,Each page can display 50 Record

Go To Page: 1 go

4967 relationals

From	Type	Target_Url	Target_Md5	First_T
http://ds-mf.com/	landing	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1
http://www.1add6.com/re_tb.asp	hosting	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1
http://dqbeiyan.com/	hosting	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1
http://dglianfeng.cn/	landing	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1
http://dgshunming.com/	landing	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1
http://dart.com.cn/	landing	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1
http://dlele.com.cn/	landing	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1
http://daqianjg.com/	landing	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1
http://daxinarts.com/	hosting	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1
http://zgyyjj.cn/	landing	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1
http://daxinarts.com/play_img-2/index.htm	hosting	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1
http://dsxf.com/	landing	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1
http://ykjy.net/user/userlogin.asp	hosting	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1
http://ykjy.net/	hosting	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1
http://xmhuamei.com/	landing	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1
http://xinjingjgs.com/	landing	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1
http://yuanhong.net.cn/	landing	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1
http://ystea.com/	landing	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1
http://dlxinxi.com.cn/	landing	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1
http://zhonghuamingwang.com/	landing	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1
http://zhhongyu.com/	landing	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1
http://dsqcyp.com/	landing	http://d.gddxw.com/xx/x2.css	3dbe6237e8e859a7a7bcef133c9e21c4	2009-1

Demo

Our “Steam” and Virtualization System

What we are facing

The Root

- Using 0day and logic vulnerabilities attack
- 3rd party applications' vulnerabilities
- Aggressive Anti-Anti-Virus Tech
- More attack beyond signature detection
- Poor web security problem in China
- Our resource is limited
  - A "Steam" system☺
  - A virtualization system

What we are facing

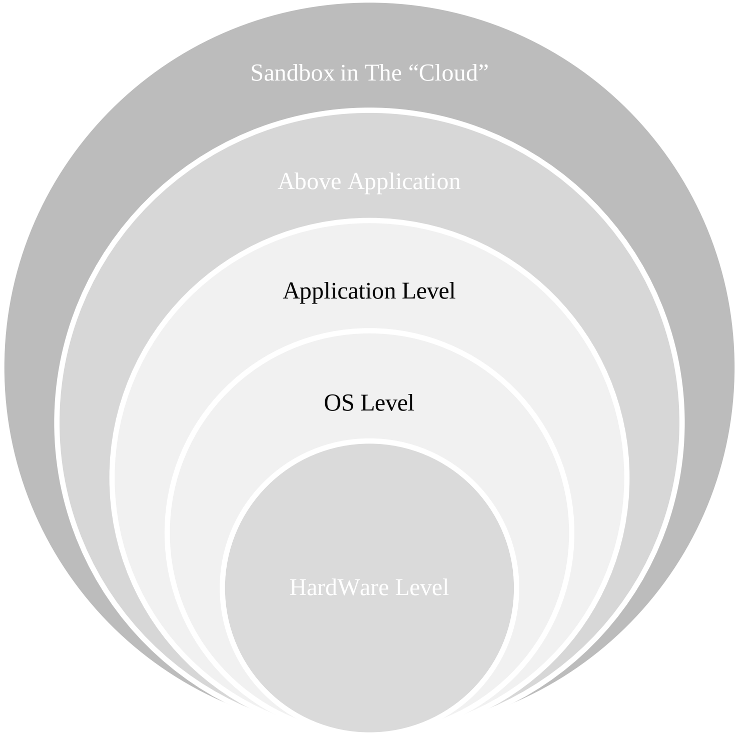
how to solve these problems

- Our virtualization philosophy for detecting malware
- We tested 4 system:
  - Signature
  - Behavior
  - Virtualization
  - Virtualization + Behavior
- Our conclusion
  - Don’t use signature to detect them!
  - Virtualization + Behavior and put it to a cloud is the best system

What we are facing

The Cloud System

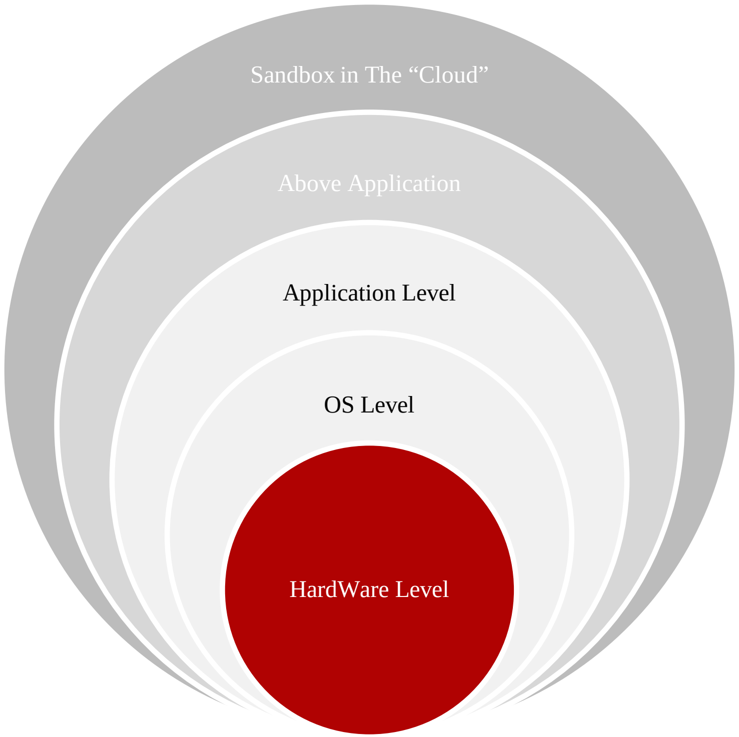
- Client type cloud system
  - We build a IE plugin
  - More sensitive
  - Many FPs
- Server type cloud system
  - More control
  - Need more resource
  - A platform of virtualization



We try to solve this by virtualization

The Root

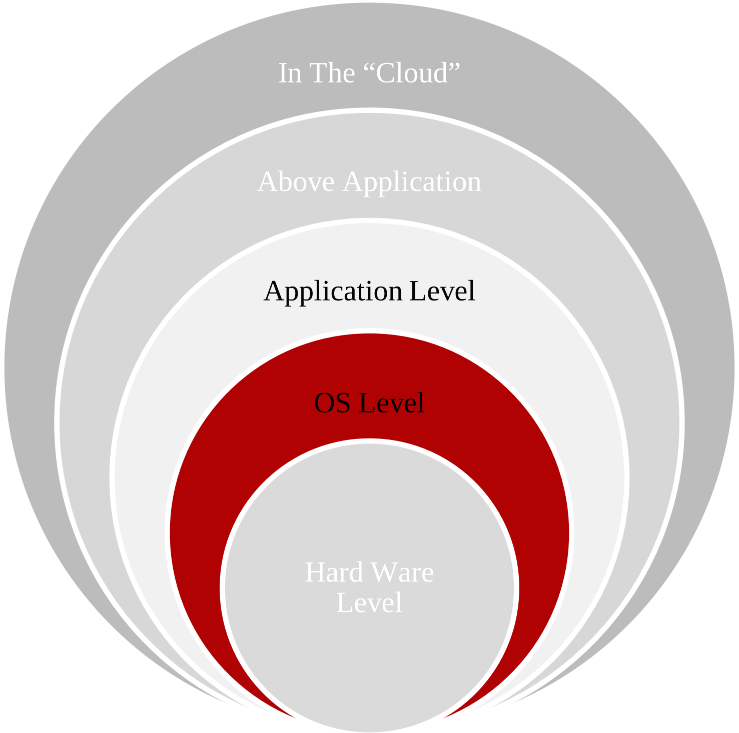
- HW level: Vmware Server
  - Free!☺
  - VIX APIs
  - Object:
    - Managing the guest OS
    - Base of the “Cloud”



We try to solve this by virtualization

The Root

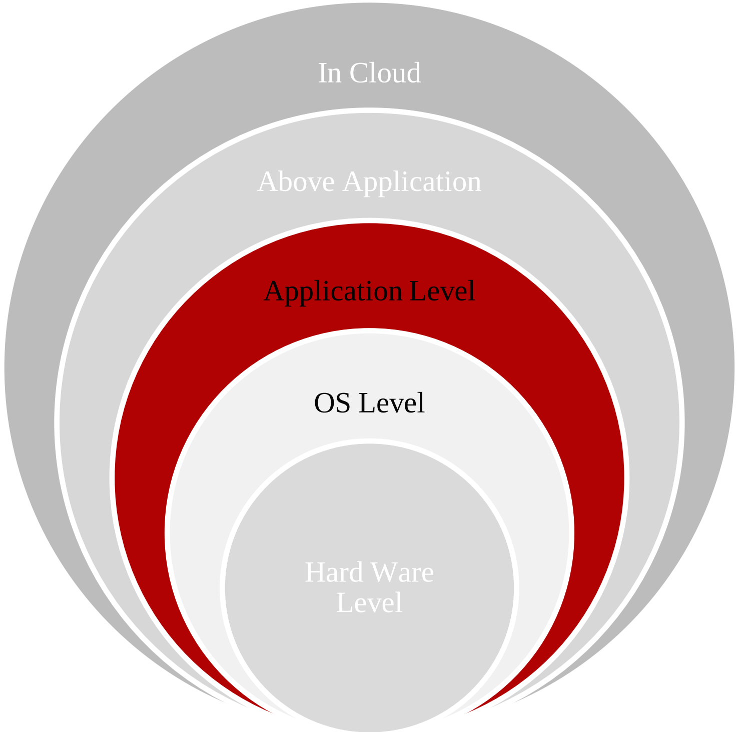
- OS level:
  - Our main idea is not get infected
  - Like a small HIPS but monitoring
    - File system, Register, APIs etc.
  - Objects:
    - Protecting OS from 0day attacks



We try to solve this by virtualization

The Root

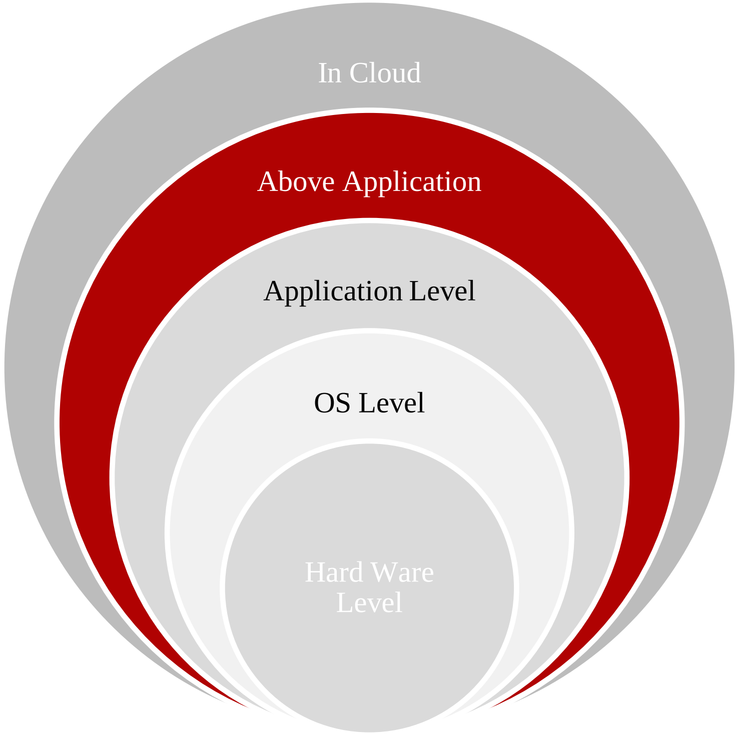
- App Level:
  - Browser virtualization
    - IE based
  - 3rd party application virtualization
  - Objects:
    - Detecting IE, 3rd app vulnerability attack
    - Anti-Anti-Anti-Virus☺



We try to solve this by virtualization

The Root

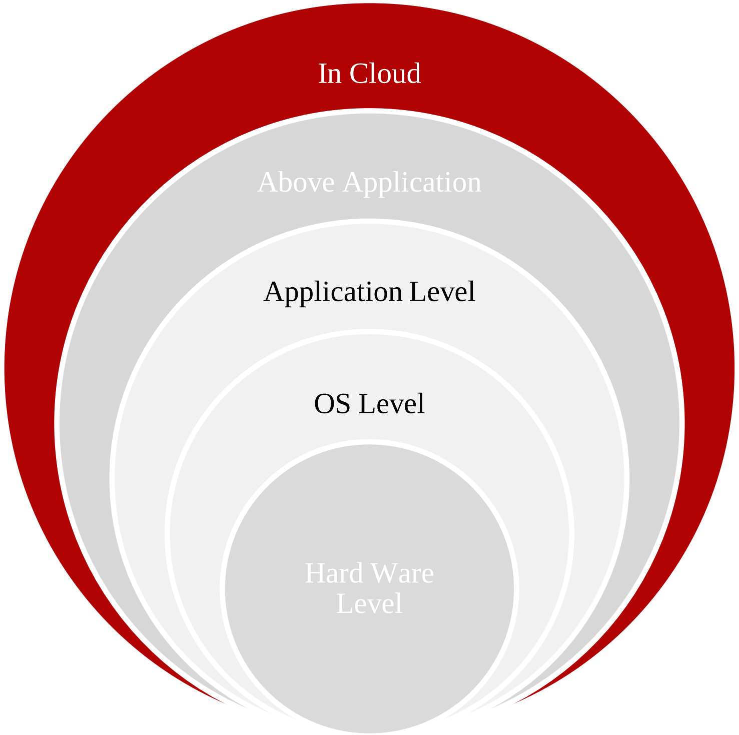
- Above App Level:
  - Javascript, Vbscript virtualization
    - Monitoring
    - Recording
  - Objects:
    - Anti-Anti-Anti-Virus☺
    - Detecting any script related behavior



We try to solve this by virtualization

The Root

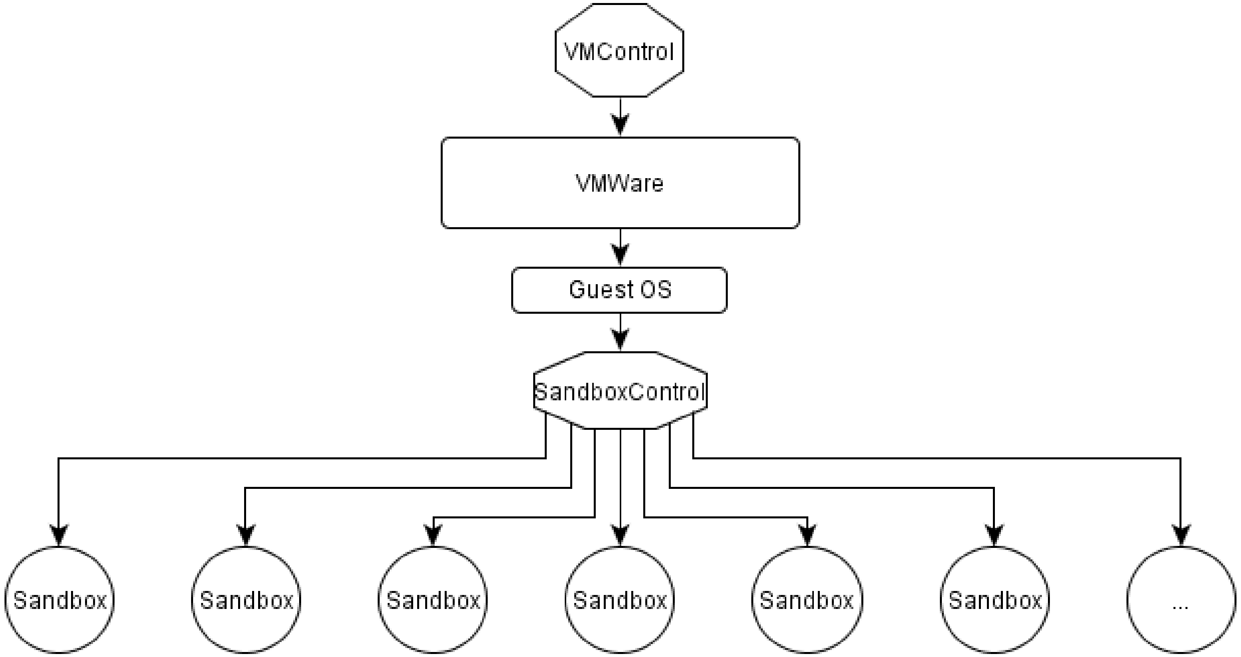
- The “Steam”
  - Our own web crawler
  - Sandbox idea
  - Distributed system



We try to solve this by virtualization

The Root

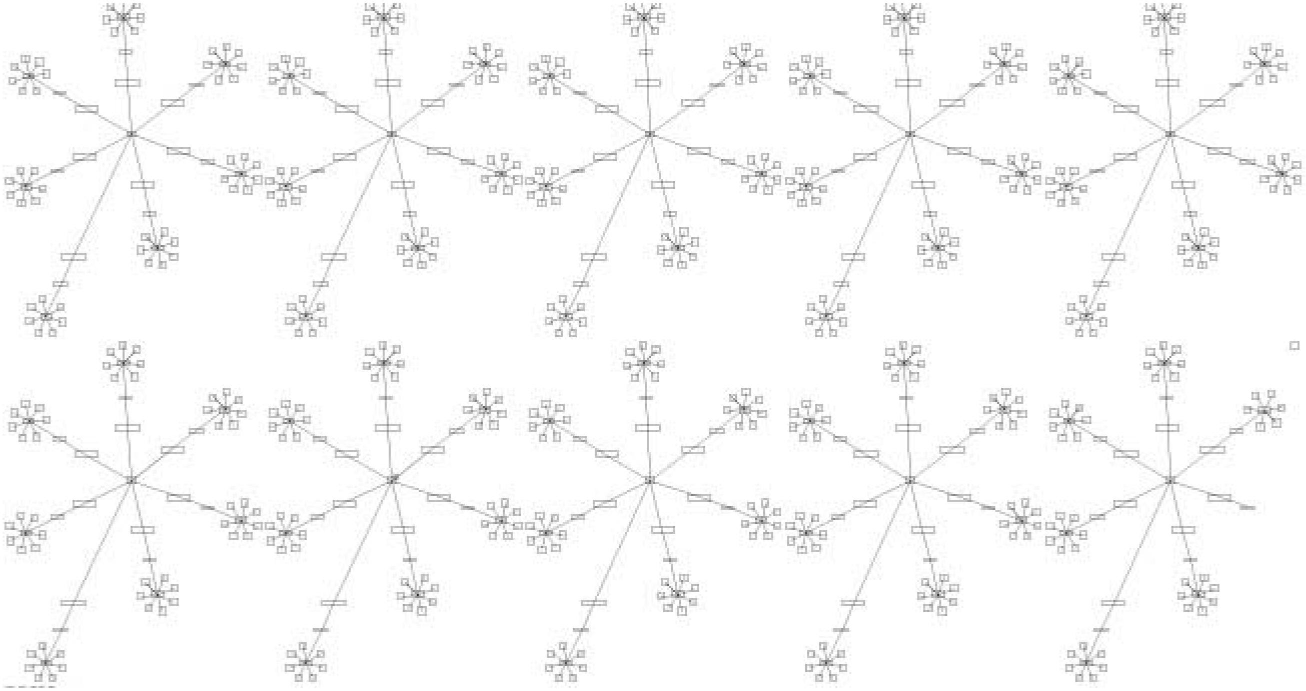
- The “Steam”
  - Our own web crawler
  - Sandbox idea
  - Distributed system



We try to solve this by virtualization

The Root

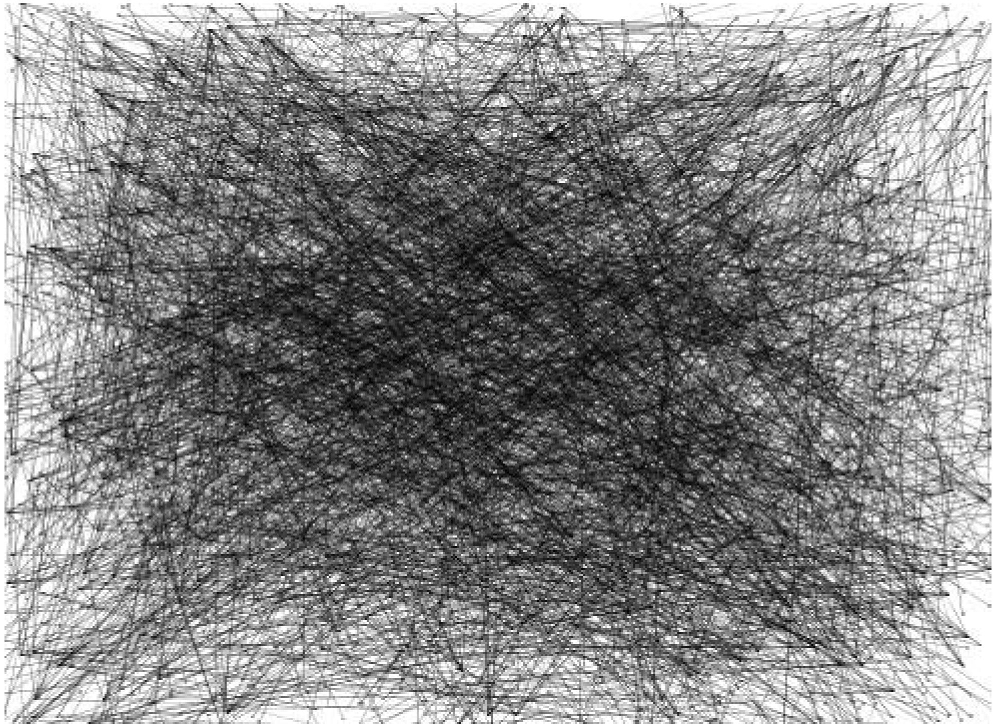
- The “Steam”
  - Our own web crawler
  - Sandbox idea
  - Distributed system



We try to solve this by virtualization

The Root

- The “Steam”
  - Our own web crawler
  - Sandbox idea
  - Distributed system



Q/A

Thank You!

ic@knownsec.com