



Is there a lawyer in the lab?

Juraj Malcho
malcho@eset.sk

Malware in current cybercrime

Higher complexity of technology – HW/SW

More faults introduced despite the efforts in security

PoC, exploits, vulnerabilities

Targeted primarily at finding exploits in order to misuse them (and make money of course)

Typical malware of today

Makes use of these and human vulnerabilities, is challenging to detect and is organized into botnets

Botnet = \$\$\$

Trading stolen credentials, renting botnet services: adware push-installations, spam, DDoS

The grey zone – adware, spyware, unwanted...

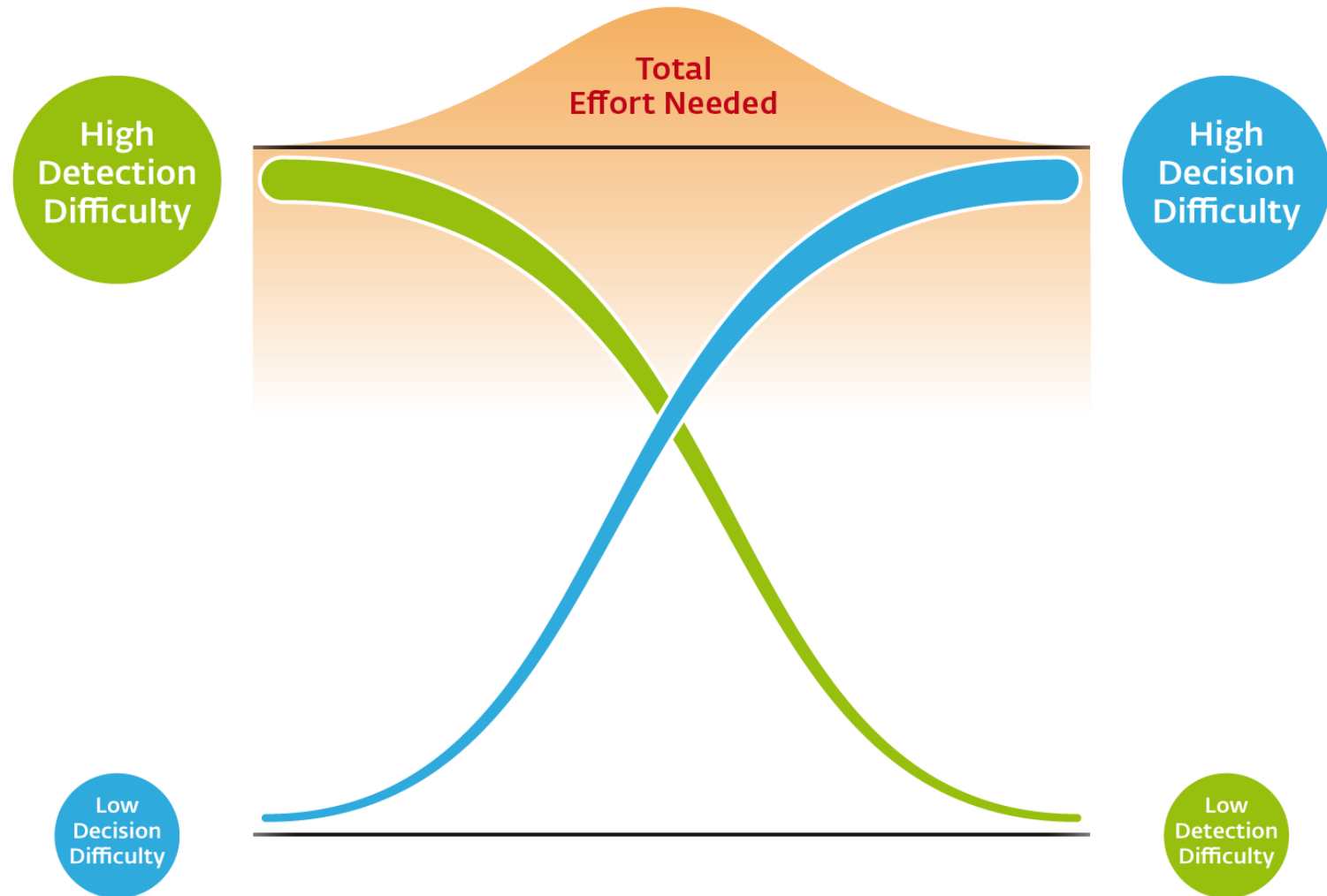
The decision about detection can be troublesome

It can be difficult to give a reason why the software is malicious, unwanted, not useful...

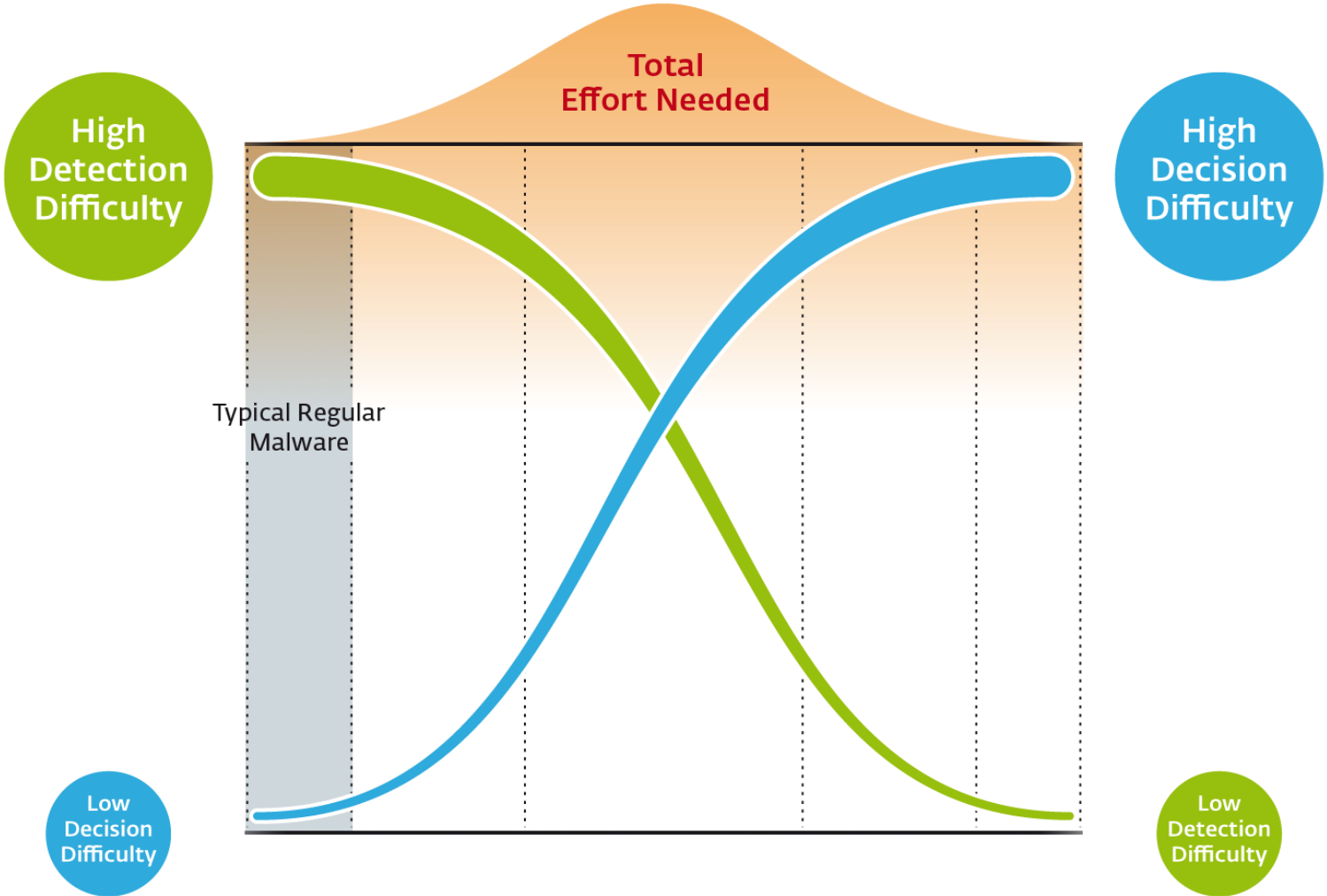
Implementing detection can be rather easy

But there are exceptions to the rule

Detection vs. Decision difficulties



Typical Regular Malware



The grey zone – adware, spyware, unwanted...

Subjectivity enters the decision process

Cooperation needed among AV companies to avoid ambiguous decisions

Initiatives and organizations established

to introduce standards, generally respected rules and best practices – AVPD, ASC, AMTSO...

The grey zone software specifics

What kind of software are we talking about at all?

Completely useless, without providing any real value

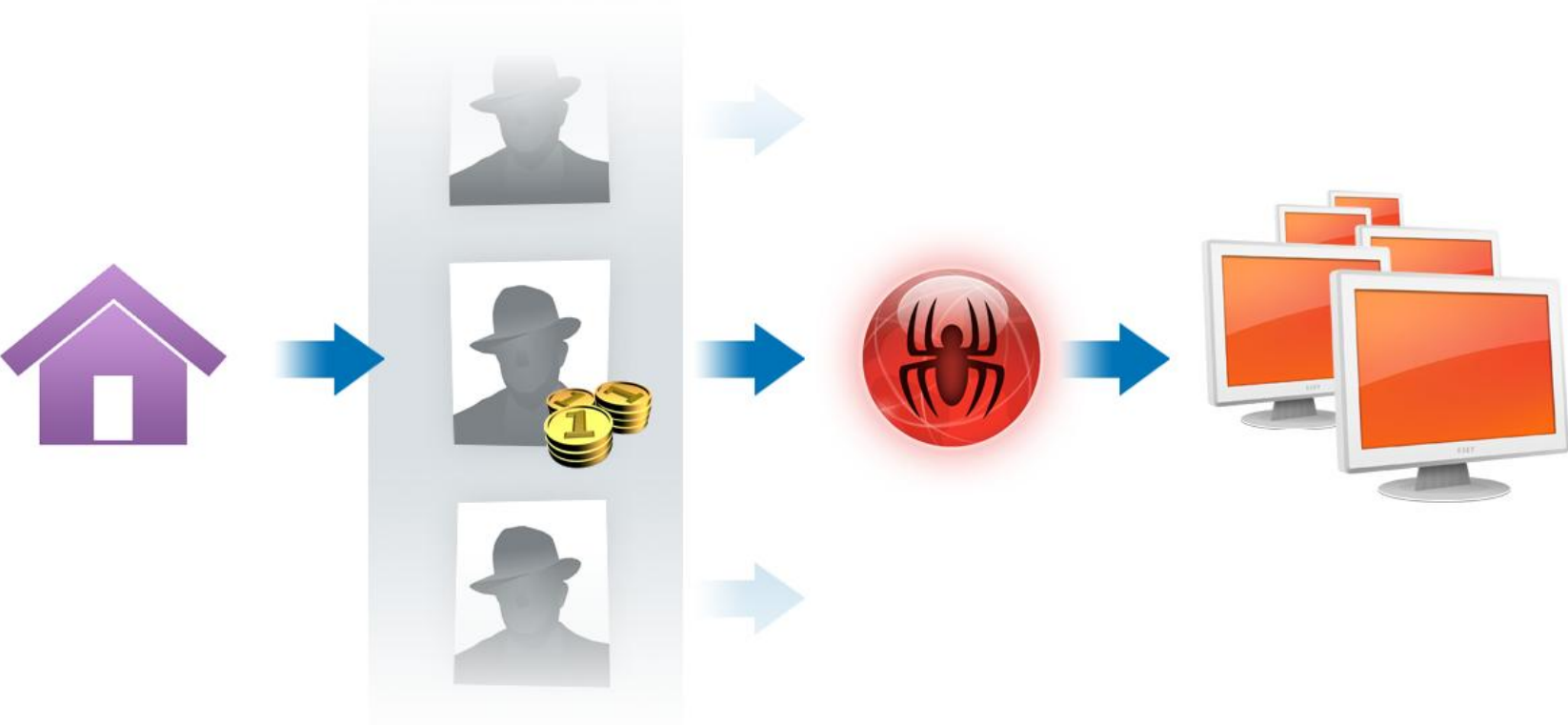
Really? Not any value?

OK, the author/company that develops it gets some money ;)

Collision of interests

Complicated decisions, many factors to take to account: the software code, the user base, the company and the distribution channels

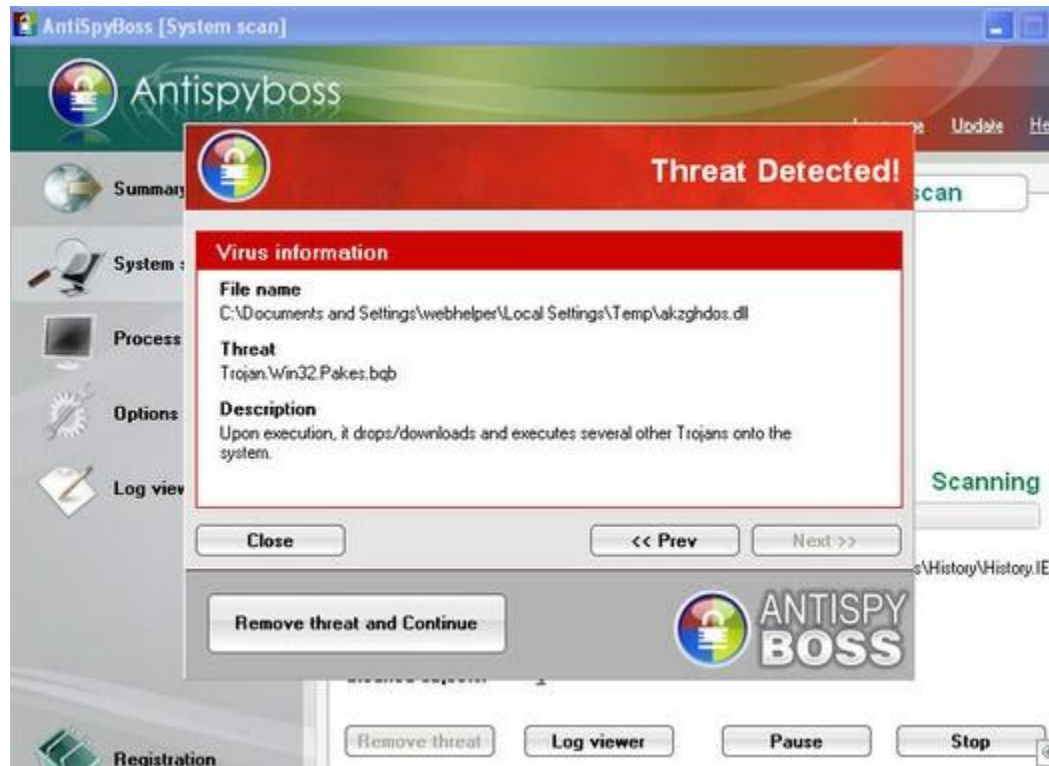
The affiliates distribution model



The grey zone SW specifics

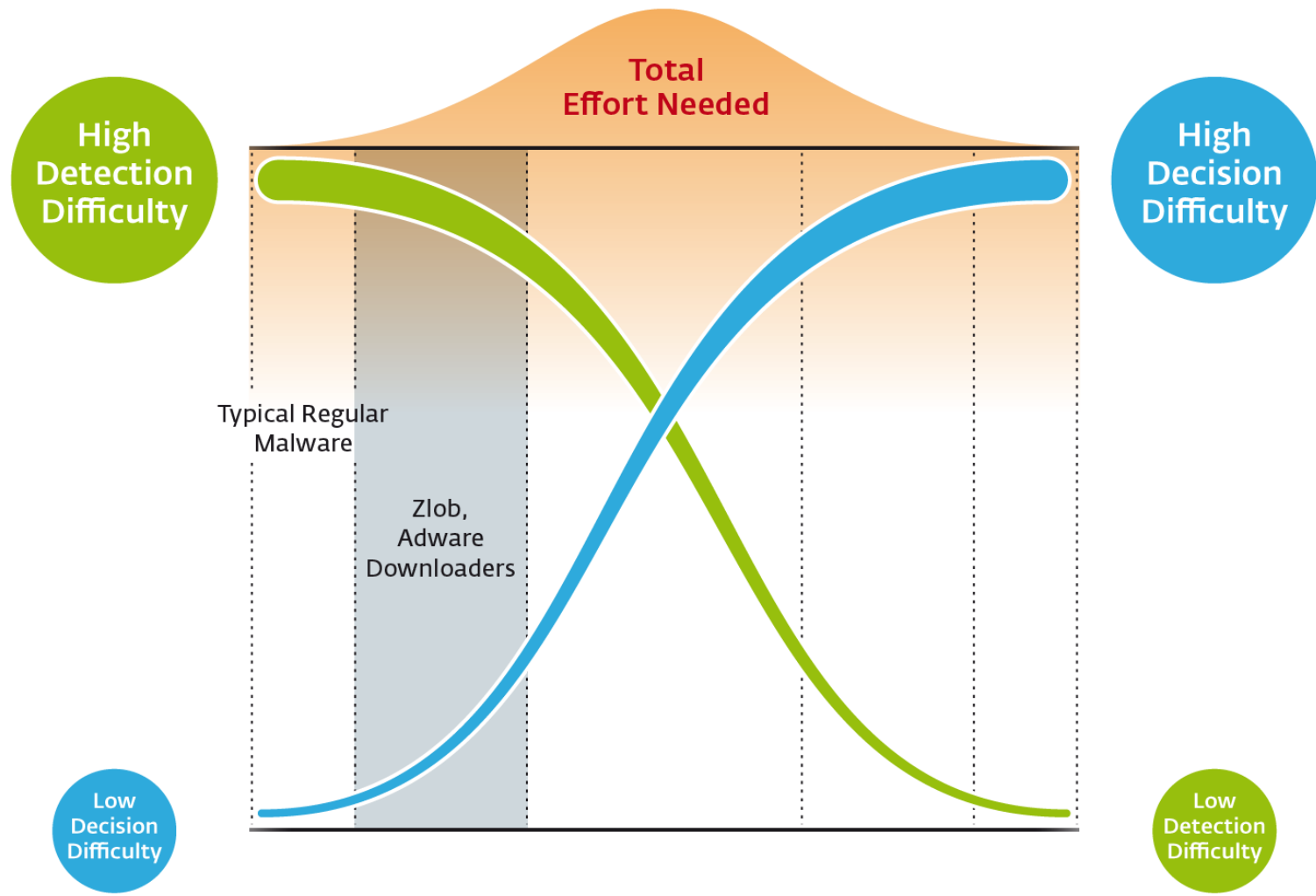
The incentive for detection

Customers' complaints are a good start



The picture courtesy of Sunbelt

Zlob. The easy stuff.



Zlob. The easy stuff.

An adware downloader

Notorious devastator of Windows boxes, since 2005

Financially motivated

Run by a criminal group to make money

A pioneer in detection evading and fine-tuning

Had been systematically updated, evolved over time, provided several updates of their code a day

More was to come...

They started to complain...

From: support [mailto:support@emediacodec.com]

Sent: Wednesday, April 12, 2006 4:28 PM

To: xxx

Subject:

Hello xxx.

We are eMediaCodec support team. we would like to know why your software NOD32 detects our codec as virus "Win32/TrojanDownloader.Zlob.II".

Our emediacodec is provided with Terms and Conditions located at <http://www.emediacodec.com/terms.html> where we describe in details what is the codec itself. We do tell surfers about what being installed on their computers.

We would very appreciate if you remove our eMediaCodec from your virus list.

Thanks

... and they complained some more...

From: xxx [mailto:xxx@pornmagbucks.com]

Sent: Wednesday, July 12, 2006 3:53 PM

To: xxx

Subject: Attn: AV Research Team. Urgent.

Dear Research Team,

I am writing to you on behalf of DIGITAL MEDIA DEVELOPERS.

Why does your AV detect our software as

"Win32/TrojanDownloader.Zlob.UR"? There must be a mistake. Our software has a License Agreement on the very first page of the install wizard, the product itself does not include any trojan or any software to download anything secretly, furthermore all ad components are downloaded with user permission and without any secret. If you have a look at our product more closely, you will find that it can be easily removed from PC with the help of the Add or Remove Programs menu.

Could you please explain your policy on naming and detecting our software as "Trojan"?

Here is the URL of our product

http://www.pornmagpass.com/download/pornmagpass_ver1.107.exe

Best Regards,

xxx



... and finally died (?)

For Windows Defender's Team:

I saw your post in the blog (10-Oct-2008) about my previous message.

Just want to say 'Hello' from Russia.

You are really good guys. It was a surprise for me that Microsoft can respond on threats so fast.

I can't sign here now (he-he, sorry), how it was some years ago for more seriously vulnerability for all Windows ;)

Happy New Year, guys, and good luck!

P.S. BTW, we are closing soon. Not because of your work. :-))

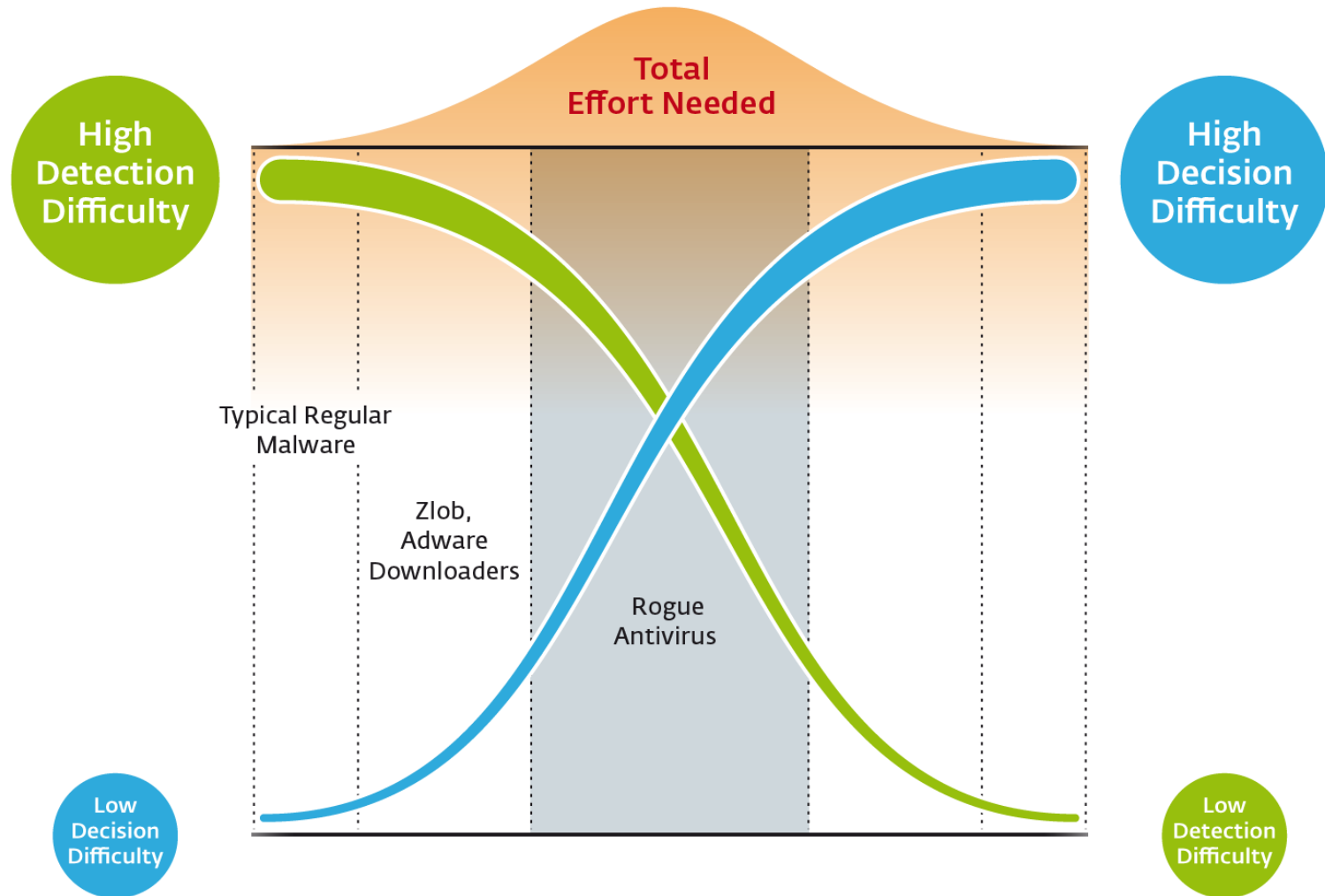
So, you will not see some of my great ;) ideas in that family of software.

Try to search in exploits/shellcodes and rootkits.

Also, it is funny (probably for you), but Microsoft offered me a job to help improve some of Vista's protection.

It's not interesting for me, just a life's irony.

Rogue AV. Things get tricky...



TOP ANTISPYWAREBOSS FEATURES:



- Removes Spyware
- Removes Adware
- Stops Pop-ups
- Clear Cookies
- Block Phishing Attacks
- Kills Browser Hijackers
- Flases History
- FREE Customer Support



EXTEND YOUR ANTISPYWAREBOSS SUBSCRIPTION NOW AND SAVE!

SPECIAL SUBSCRIPTION OFFERS

6 Month: \$38.95 (6.3\$ per month)

Subscription includes new version updates, definition updates, and unlimited customer support for 6 month.

BUY NOW (20% OFF)

1 Year: \$48.95 (Save \$30) - **RECOMMENDED!**

Subscription includes new version updates, definition updates, and unlimited customer support for one year.

BUY NOW (30% OFF)

1 YEAR EXTENDED (+ 2 years free updates): \$68.95 (~0.2\$ monthly!)

Purchase Subscription to AntispyBoss now at a special discount and never worry about Spyware again! This Subscription includes new version updates, definition updates, and unlimited customer support for more then 3 years!

BUY NOW (60% OFF)

Offers only high-quality movies where sexy studs show you their secrets of satisfying experienced mature ladies! Offers only high-quality movies where sexy studs show you their secrets of satisfying experienced mature ladies! Offers only high-quality movies where sexy studs show



ANTISPYWAREBOSS
antispyware pro kit

© 2008 antispywareboss.com



Rogue AV. Things get tricky...

A fraudulent theatre played to scare out some money

Fools users by pretending to find infections and offering their removal by the full PAID version

The trial version pushed onto the PCs via dubious channels

Virtually anything you can think of that botnets have to offer

Eventually the victim pays for a graphical bubble

and also risks his payment card details being compromised

Rogue AV - in case you never saw one

WINDOWS
Protection Suite

Language [English](#)

Home

Windows Protection Suite Yet another lousy Rogue Antivirus suite

Reports fake virus threats

Doesn't provide any protection

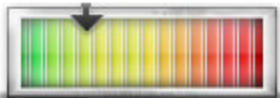
Regularly requests you to buy a new version and spend more money

Trashes the CPU and renders the PC unstable and buggy

[Download Now](#) 

Internet Threats

Online indication of virus activity



Alert Level: **Medium**

[Protect your PC Now](#)

Free Online Scanner

Click "Scan your PC", and you'll see the advantages of this product immediately.



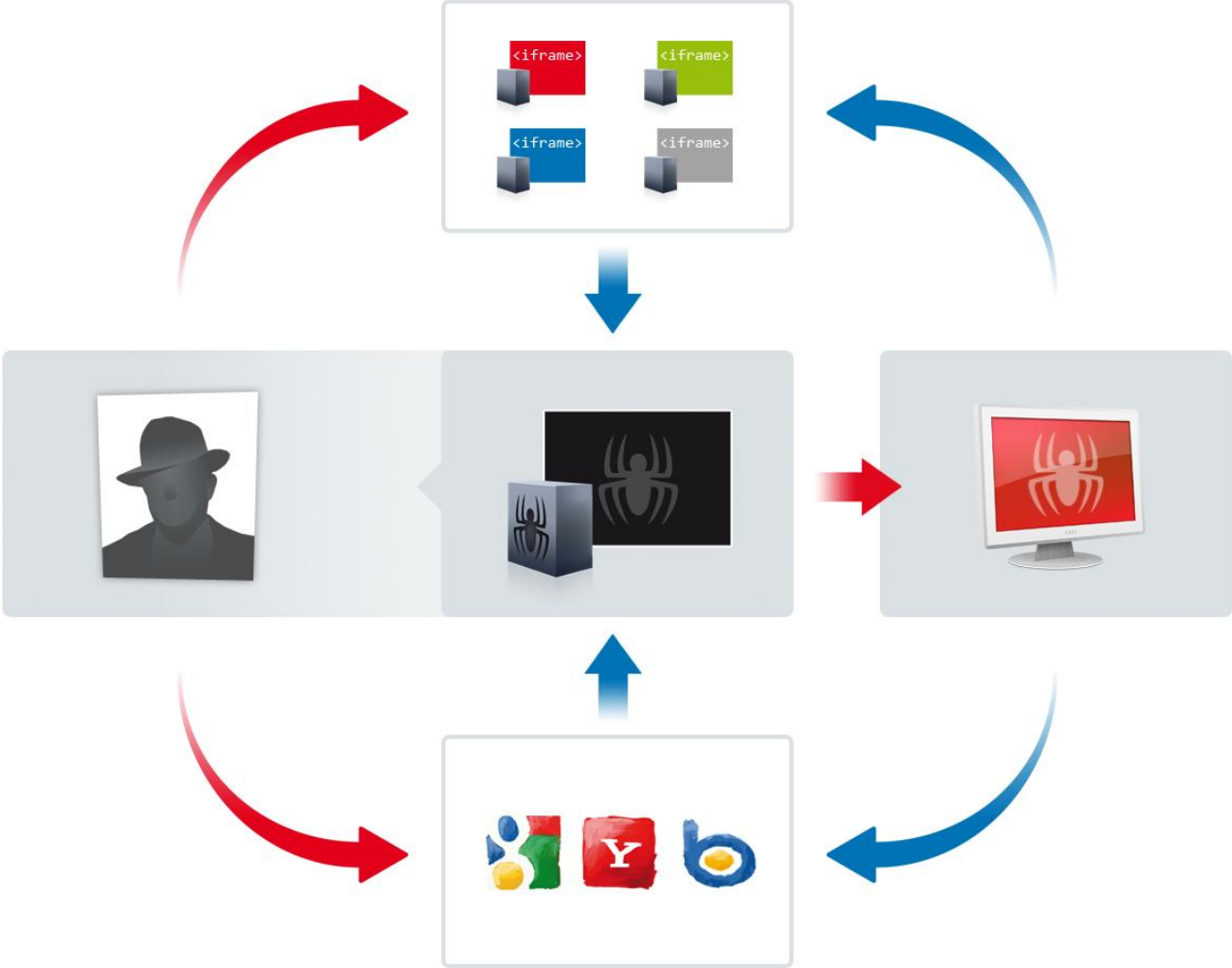
[Scan your PC](#)

It is simple, fast and FREE

Features

- No updates necessary
- Downloads new versions of advanced spyware and adware.
- Self-protection from being modified, stopped or even uninstalled by another application
- High CPU load
- Incompatible with every OS out there

The distribution channels again



Is it a trojan or not?

The trojan downloader

- Uncompromising infection
- Makes use of exploits (packs)
- Unattended, unsolicited installation
- Performs hidden activities (downloads other SW)

The application

- The application itself isn't causing any harm
- EULA – installed with user's consent (?)
- The vendors disclaim involvement with the distribution channels

Attributes to consider

Invasiveness

Impact on system stability, security and integrity

Obfuscation/protection

Detection evading

The distribution model

They don't like being detected

Subject: NOD32 detects our products as malware

Date: 21 Aug 2006 10:21:51 -0500

From: xxx@winsoftware.com

To: xxx

I am contacting you on behalf of WinSoftware Company.

Recently our Quality Assurance Department discovered that parts of our product, WinAntiVirus Pro 2006, were added to your anti-malware database, and are currently being detected as malware.

WinSoftware believes this may have been done inadvertently; nevertheless this has **a big impact on our Company's reputation and on customer satisfaction** level. WinSoftware, therefore, **requests that you remove** these product from your base **no later than fourteen (14) days** from receipt of this notification. Please confirm receipt of this message.

Best regards,

xxx

Senior Vice-President, Legal Compliance
WinSoftware Ltd.



RogueAV: The future is not looking good

Distributed along with malware related to botnets

The same obfuscation technique/protectors, actively trying to evade detection

Pretend to be legitimate and useful – what if they start to be?

Use of CLAM engine, or something else; fix a few small errors in the registry

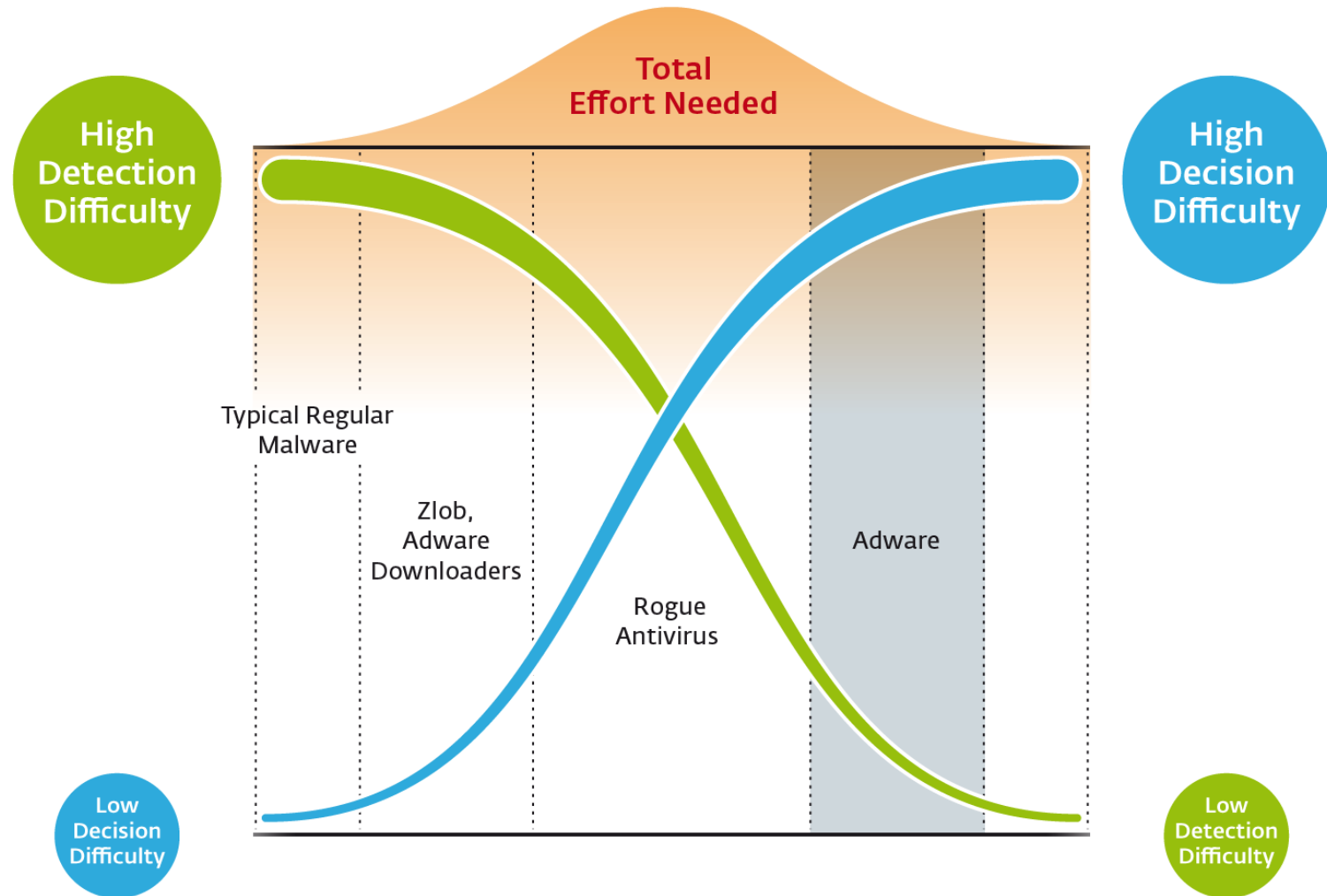
Putting themselves into the position of competitors

What if they hire people to write/buy an amateurish SW and “do the rest”?

What if they get tested in serious tests?

What if they really try but do more damage than good?

Adware



Adware – the easier part

Software primarily specialized on ad delivery

Covers the whole scope from trojans to legitimate applications, often contains a EULA

Generally undesired by end users

People don't want it, it's pesky, annoying, disruptive and useless

Adware – the easier part: Navipromo

Hi,

I am representative of Favorit-Network and I have tried to contact you by mail many times but I have received no reply yet. Actually, several weeks ago, somebody from your company told me that the detection of our applications was due to the fact that SOMEAV was also signing the applications. Now that SOMEAV stopped signing the application you are still doing so.

Here you can find the applications to be downloaded:

`hxxp://some.thing/bad`

I found a report for one of our applications here

<http://someavcompany/en/malware/?Trace.Directory.LivePlayer!A2> and there you clearly state "It is harmful if installed without the knowledge of the user." But it always requires the acceptance of the user! Besides, there is no danger or threat.

Since SOMEAV already removed the signature for these applications, we expect you to do the same.

Regards

Adware – the easier part

Software primarily specialized on ad delivery

Covers the whole scope from trojans to legitimate applications, often EULA

Generally undesired by end users

People don't want it, it's pesky, annoying, disruptive and useless

Problematic decisions and legal issues

Zango vs. Kaspersky case

An interactive computer service provider
(in the context of content filtering)
has the right to block material that he or
his customers consider objectionable

Adware in China

China: problems with piracy, as well as adware

Lots of legitimate applications with some sort of ad-delivery implemented

Green software

Standalone package with (cracked) software that doesn't require installing; generally not considered illegal

Green sites

Offer green SW, custom OS packages, licence keys, serial numbers...

热点推荐

-  **糖果浏览器**
最新崛起的浏览器新宠
-  **阿里通免费网络电话**
免费100分钟手机也能用
-  **ABPlayer**
爱播高清视频播放器
-  **金山毒霸**
2009官方最新免费版
-  **酷我音乐盒**
自带100万首歌的播放器
-  **开屏播放器**
最佳桌面媒体播放器

最新更新

- 博客魔术手_1.0_绿色版_博客好助手[新]
- VSO Inspector_2.0.0.2_绿色英文版[新]
- QQ空间自动留言助手_1.0_免费版 [新]
- Acoo Browser 阿库浏览器_1.96_绿色[新]
- Imagelys Picture Styles_5.1_绿色[新]
- 快车(FlashGet)_3.1.0.1052_简易去[新]
- CAD图纸查看器_9.0_绿色版 [新]
- Groovy Media Player_1.2.0_绿色版[新]
- 电子档案之人事管理系统_V4.3_绿色[新]
- 宏达企业计量信息管理系统_V1.0_绿[新]

Adobe Photoshop CS4 11.0 Extended[绿色版][是基于官方正式版制作]

运行环境: Win9x/NT/2000/XP/2003
文件大小: 83620 K
软件类别: 免装软件
软件语言: 简体中文
软件属性: **热 荐**
授权方式: 免费版
添加时间: 2008-10-19 7:14:04
软件等级: ★★★★★
软件绿化: 佚名
软件添加: 审核:onegreen 录入:admin
下载次数: 日: 2860 总: 292791



Skype

免费网络电话, 全球语音沟通


简介:
Skype可以与全球两亿好友进行免费的文字、语音、视频交流, 拨打长途电话费用只有普通IP电话的10分之1 [立即下载](#)

下载地址:

[高速下载](#)

-  电信服务器下载
-  网通服务器下载

PPF传播快乐: [立即高速下载](#) [迅雷高速下载](#)



Stainless Steel Coils
300 Series, 17-7, stainless strip, sheet, shim stock .002-.035" thick
www.sidecuts.com

Ads by Google

::软件简介:: [PPF传播快乐: 电信高速下载](#) [网通高速下载](#)

=====

Adobe Photoshop CS4 简体中文(汉化)特别版

=====

基于Adobe Photoshop CS4 官方正式版制作
免序列号, 免激活!

特别说明:



>>点击放大观看<<

Green servers are closely monitored not to offer infected content

Safe site = trusted site => more positive reviews => more downloads and page hits => more money from online ads

Hard to tell apart fake from the original

Same issue as with black-market CDs/DVDs => many might be using illegal software unknowingly

The Chinese SW business model

Software is provided for free but vendors are forced to implement ad-delivery mechanisms

Different views of the same thing

China: Adware is regular software

And often there isn't any other version of the software

Rest of the world: Adware??? We hate it!!!

People are allergic to it, demand removal, there are many ad-blockers and filters out there...

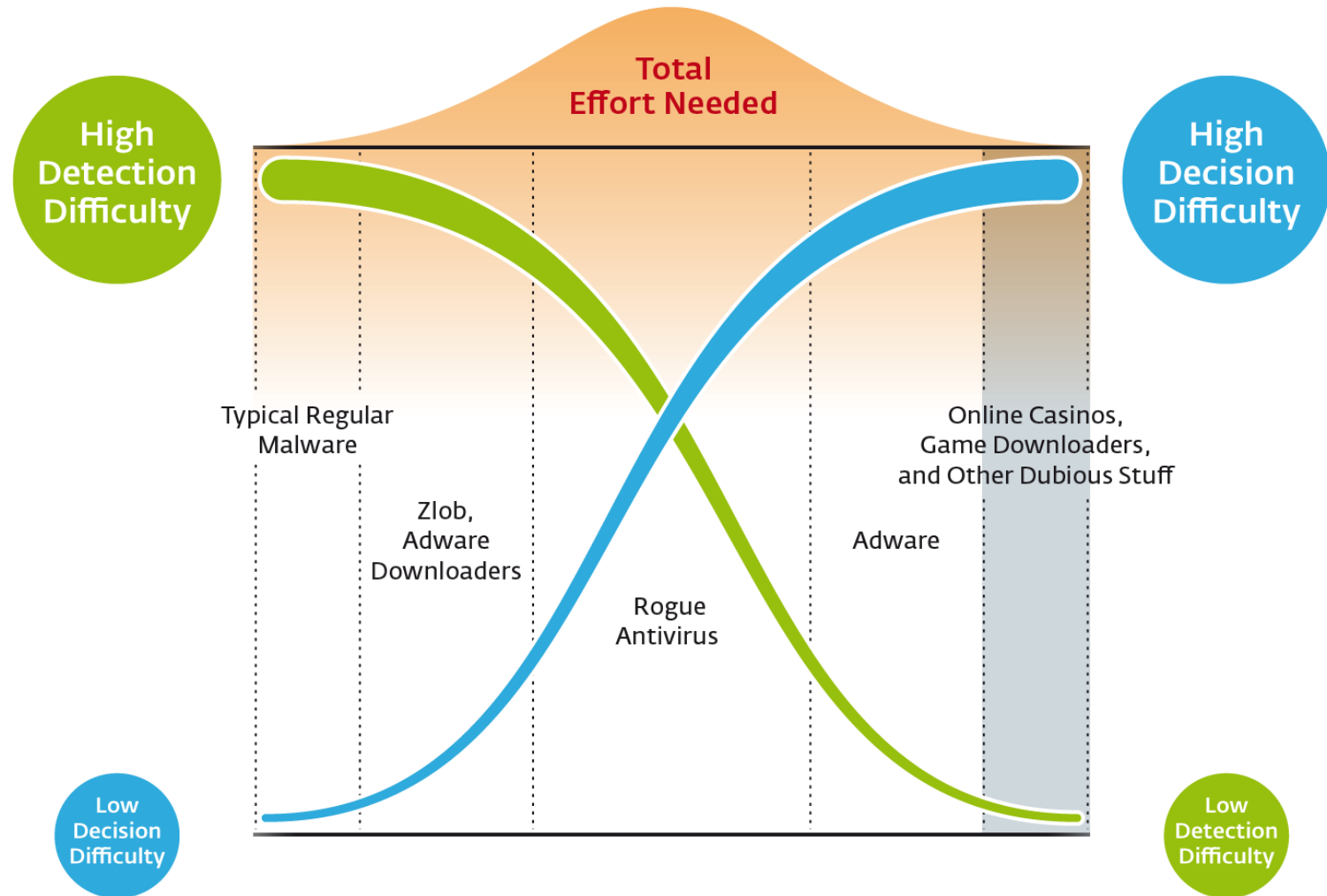
So what exactly is adware?

Does it really matter?

To what extent are common computer users able to tell a good SW from a bad one?

Are we going to end up with double standards?

And we're not done yet



The legally problematic stuff

Applications, developed by (well-established) companies

However, with the affiliate distribution model? Now, in the botnet era?

There are mutual customers

who want to use the software and be protected at the same time

There are other folks

who would never agree to install anything without their consent or something they don't fully trust

HOME | DOWNLOAD | PROMOTIONS

VEGAS CLUB

200% BONUS

DOWNLOAD

VISA MasterCard €\$£

24/7 Live chat support
Tol free: 1-866-866-6945
1-866-546-0445
Int: 1-266-481-2382

BlackJack Slots Craps Roulette

The contents and material within the site are solely controlled by EURO VIP LTD'd Group of Casinos.

JavaScript

<casino88-8.ru>
GET \$400 FREE & DOWNLOAD?

Stop executing scripts on this page

OK Cancel

The implications

Uncontrolled open affiliate distribution model is unfeasible!

Naturally it's misused like everything else and the botnets do their job

We're fighting cybercrime, monitoring the crooks and taking down servers etc...

And here we see a direct sponsorship for these criminal groups

But the SW vendors hate being detected

And they are ready to fight even for the price of a lawsuit

Time to find the lawyer in the lab!



What does all this mean to us?

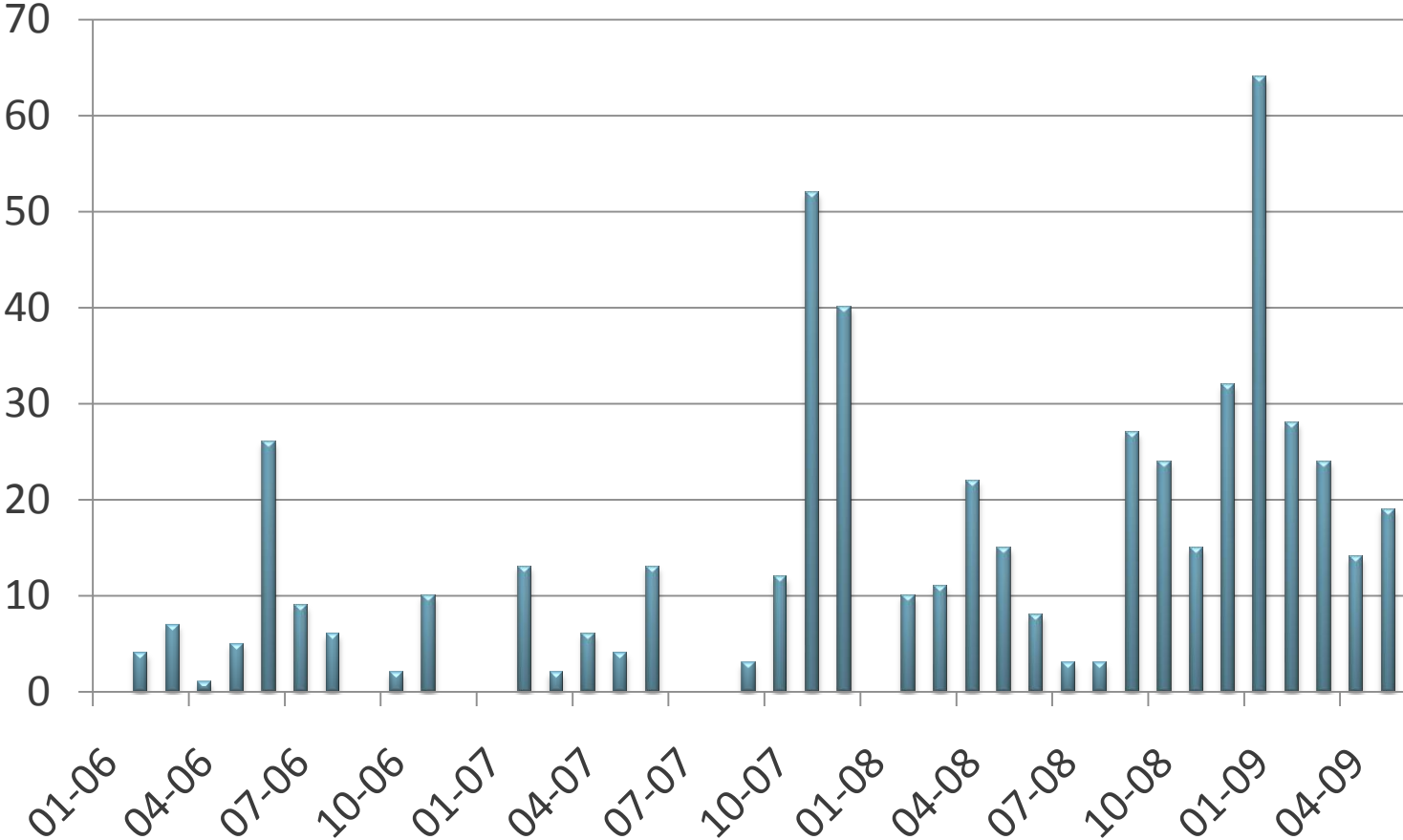


Over the last 3½ years:

- **20+** cases where legal dept. has been involved
- **over 1,150** man-hours and **530** employee interactions
- 2006: 16 man-hours/month, 6 interactions/month
- 2009: 46 man-hours/month, 21 interactions/month

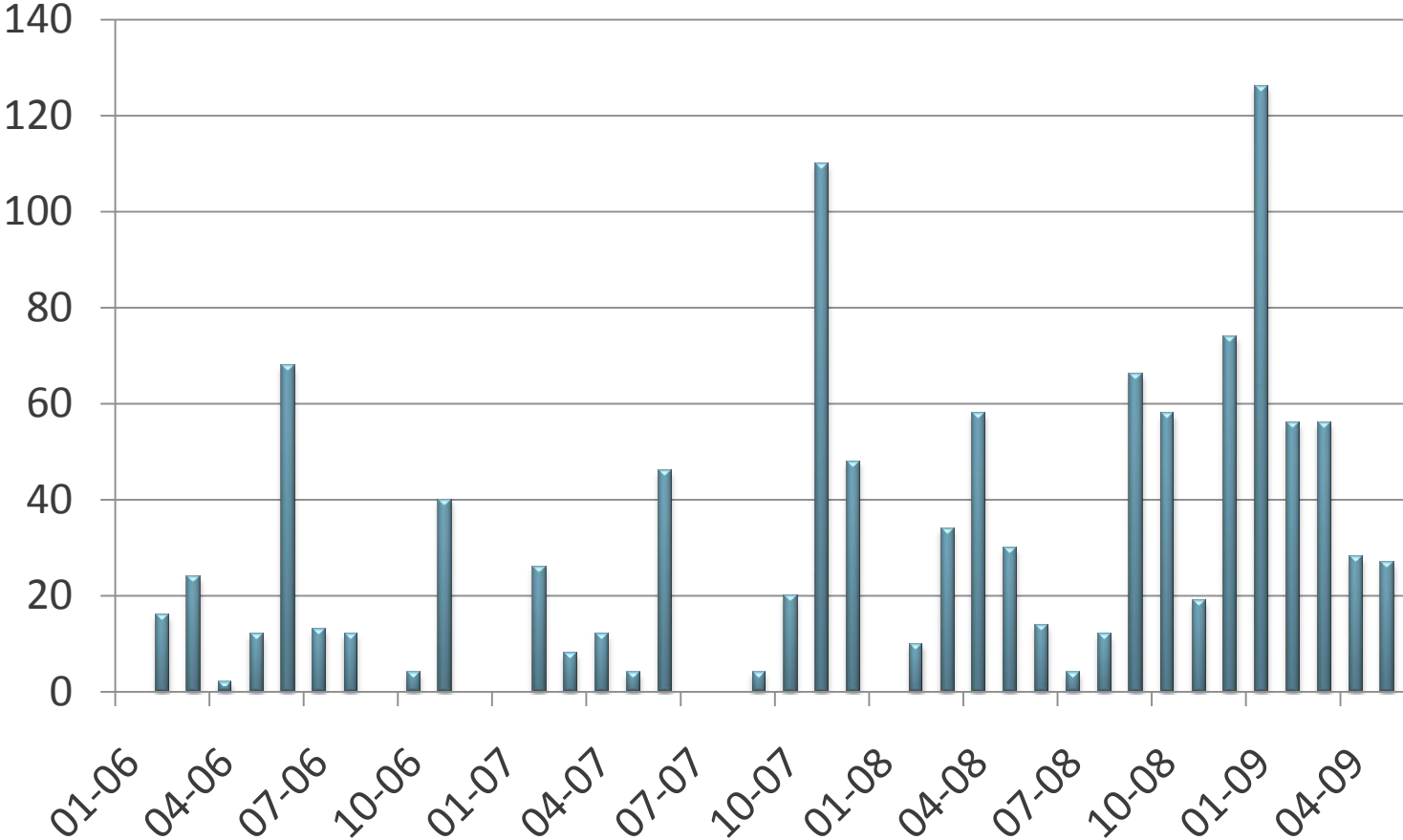
The complaints timeline

The number of employee interactions



The complaints timeline

Man-hours spent on resolving detection complaints





Over the last 3½ years:

- 20+ cases where legal dept. has been involved
- over 1,150 man-hours and 530 employee interactions
- 2006: 16 man-hours/month, 6 interactions/month
- 2009: 46 man-hours/month, 21 interactions/month



Answers?

More questions?

Juraj Malcho, malcho@eset.sk