

Cloud inSecurity

TT@chroot.org

Cloud

inSecurity

insecurity 

Block

即時發音

看漢科技提供

釋義

同義字/反義字

變化形

KK: [ˌɪnsɪˈkjʊərəti]

DJ: [ˌɪnsɪˈkjʊərɪti]

n. (名詞 noun)

1. 不安全; 危險
2. 不牢靠; 不穩定
3. 無把握
4. 局促不安, 心神不定

Network Security

Web 2.0 Security

BSD/Linux Kernel

Firewall Internal

Warrior

IPS/IDS

man @ HIT



Antivirus

Programming

Network Access Control

Member

Anti-SPAM

Network Appliance

Sr. Member @



過勞

好人 Orz

苦命工程師

加班

Before the Presentation

This is a trend discussion.

No deep technical issues.

It's about new security model.

Not technology.

AGENDA

Cloud Computing

in

Security World

AGENDA

Vendors are eager to adopt this technology.

Are bad guys scared?

(Or excited 😊)

AGENDA

and ...

What about

Bad guys Own the Cloud.

A photograph of a bright blue sky filled with large, white, fluffy cumulus clouds. The clouds are scattered across the frame, with some appearing more prominent than others. The overall scene is bright and clear.

What is the Cloud Computing?

What is Cloud Computing?

SaaS
(Software as a Service)

In-the-cloud Service

Thin Client

Cloud Computing (SaaS)

Move applications, storages, ...
To Cloud Servers.

Client becomes simple.

Cloud Computing (SaaS)

Still no idea?

Google web applications

Amazon EC2/S3/Simple DB

...

Cloud Computing (SaaS)

No hardware issues,

No software update,

No storage problem, and

You can use it wherever you are.

Cloud Computing (SaaS)

This model is amazing, and really changed our life.

But you may already know, hackers are always ahead of us.

They knows cloud computing very long time ago.

How it works?

Scenario 1

駭客小陳 的 Cloud Computing

~~雲端儲存~~ 肉雞儲存



馬神



後門神



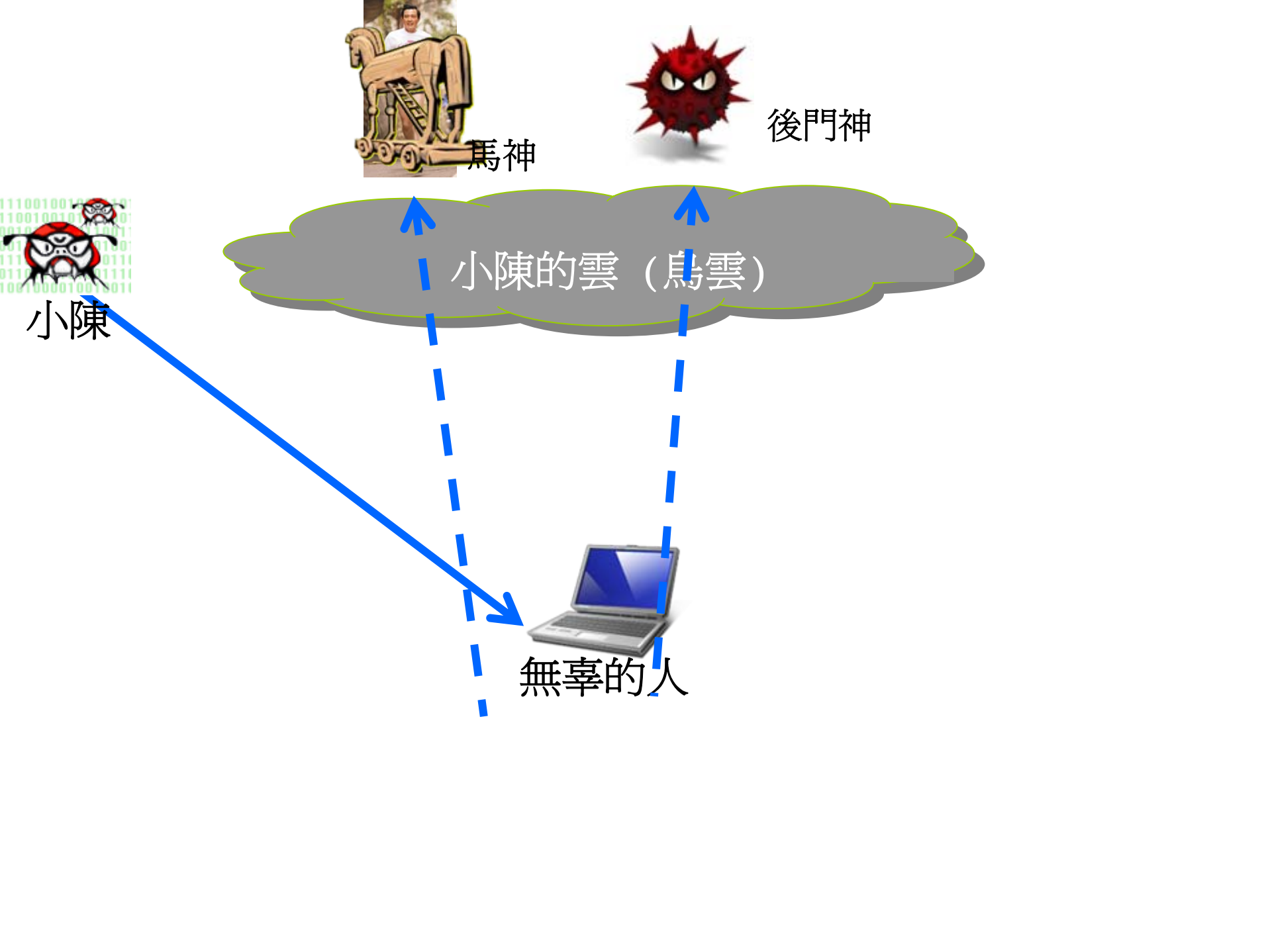
小陳的雲 (烏雲)



小陳



無辜的人



How it works?

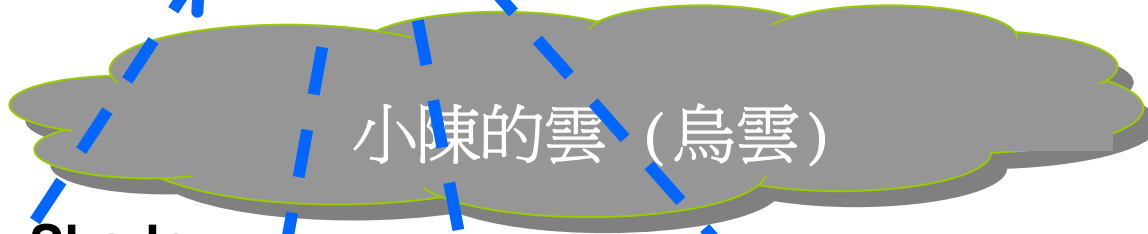
Scenario 2

還是駭客小陳的 Cloud Computing

~~雲端運算~~ 肉雞運算



John 神



小陳的雲 (烏雲)

Shadow
密碼檔



小陳

Grid Computing



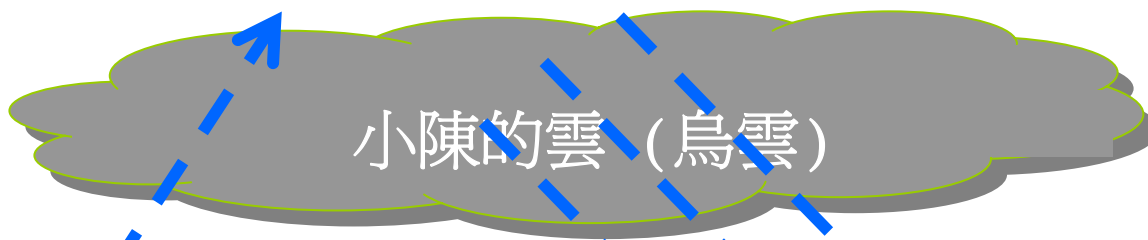
How it works?

Scenario 3

還是駭客小陳的 Cloud Computing

~~雲端運算~~ 肉雞運算

 DDoS 神



召喚



小陳

Bot Net

不爽



MD5 Rainbow Table

本站4T硬盘已经上线,共有md5记录457,354,352,282条，宇宙第一，且还在不断增长中，已包含12位及12位以下数字、8位字母、全部7位及以下字母加数字等组合，并针对国内用户做了大量优化，例如已经包含所有手机号码、全国部分大中城市固定电话号码、百家姓、常用拼音等大量组合，另加入了大型网站真实会员密码数据100万条。本站数据量大，查询速度快，同时支持16位及32位密码查询。通过对10万会员的真实动网论坛样本数据的测试，本站对于动网论坛密码的命中率达到83%。全国独此一家。

Dark Cloud

Malware is software,
software is moving to the cloud,
therefore,
malware is moving to the cloud.

Dark Cloud

Malware as a Service

MaaS

Dark Cloud – Profit Driven

Criminals have adopted the new model too, and are offering “**crimeware** as a service” (CaaS).

Dark Cloud

Cybercrime is now about
making money



CaaS

A few years ago they started selling e-mail addresses, credit-card numbers and other personal information.

CaaS

More recently they have taken to setting up and then **renting out botnets.**

CaaS business model.

CaaS

The operator of the CaaS provides real-time information on the size and availability of the botnets.

CaaS

That can be activated remotely to

flood a website with bogus requests (DDoS)

send **millions** of “spam”

大家好：

我是站長 sega。

在此跟各位報告巴哈姆特此時正遭受的威脅：

27日(日)晚上10:00，機房人員來電通知巴哈首頁伺服器當機，原本以為只是一般的當機，沒想到伺服器重開之後，短短幾秒之內，又再度當機，再次重開之後，情況依舊。

後來經過關閉對外連線後查詢系統 log，發現遭受到來自世界各地的 ip，以極大量的速度對伺服器發出網頁要求試圖癱瘓巴哈首頁，伺服器不堪負荷，因此當機。

直到星期一清晨五點左右，攻勢才逐漸趨緩。

28日(一)下午一點，我們接到了一封信件：

寄件者： wuwebshell <wuwebshell@vip.qq.com>

傳送日期： 2008-4-28 下午 01:00

主旨： 广告联系

昨天发动对贵公司的攻击，在此深表歉意，也说明贵公司的网络安全的当务之急,本人做私人服务器的，能否到贵站发布广告，请速回mail。谢谢

我們終於知道被攻擊的原因。

CaaS

That can be activated remotely to

grab PC owners' online
banking information, or

steal log-in credentials.

So ...

What do security vendors do
against such sophisticated
Maas/CaaS?

Secure Cloud – Anti-Spam

Secure Cloud – Anti-Spam

Anti-spam adopted cloud model
long time ago.

IP black-list

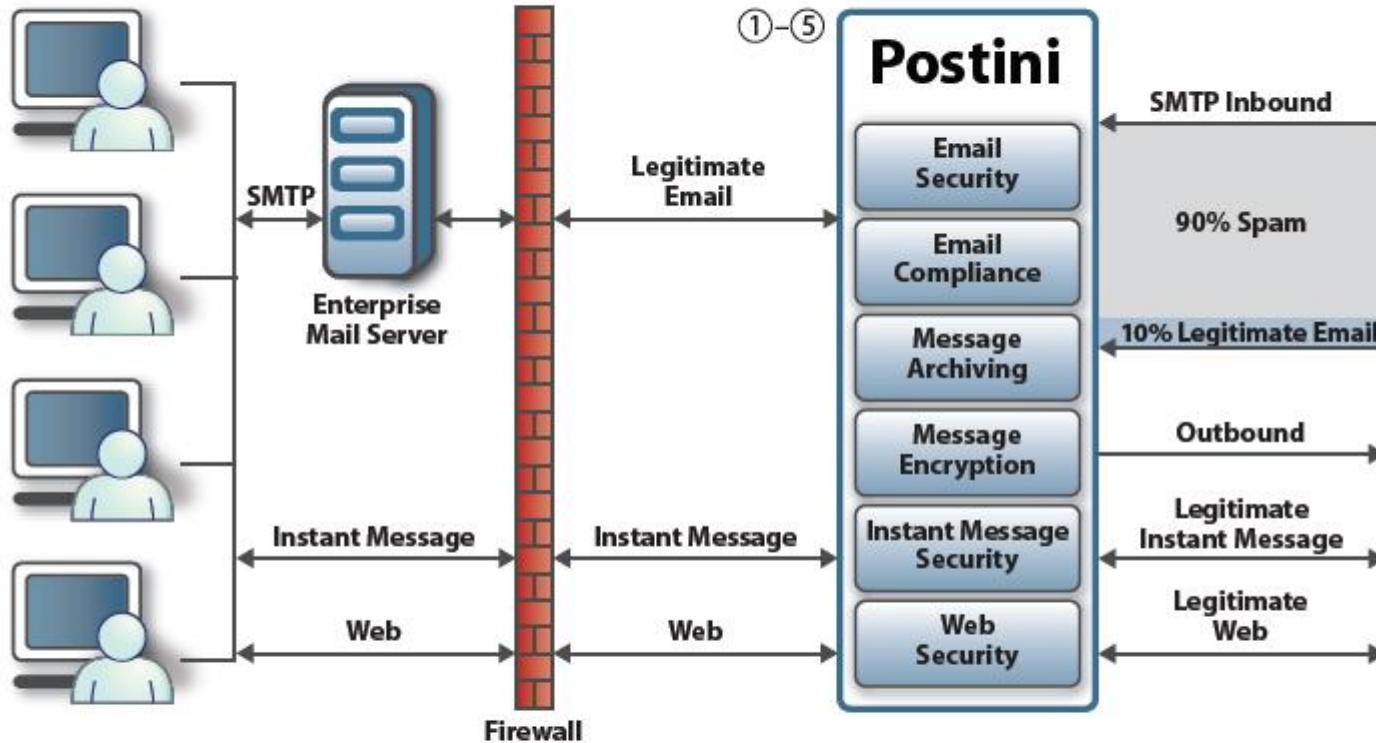
RBL, Spamhaus, SORBS,
DSBL, and ...

Secure Cloud – Anti-Spam

Mail Hosted Service (in the cloud)

Google Postini, Trend Micro
IMHS, and many others

Postini Approach



Postini advantages

1. Hosted solution stops unwanted internet traffic
2. Universal policy management for email, instant message, and web
3. Integrated encryption, compliance, and archiving
4. Built in scale and reliability
5. Easy to manage and use

Secure Cloud – Anti-Spam

Problems:

The growing usage of **zombies** and **botnets** has also made blacklists much less effective in blocking email.

Secure Cloud – URL Filtering

Real-time query for
URL/Domain Name reputation

Black listed model

Problems?

Secure Cloud – URL Filtering

The screenshot shows a Windows Internet Explorer browser window. The title bar reads "IWSVA 3.1 Beta Event (IWSVA-TAIWAN) - Windows Internet Explorer". The address bar contains the URL "http://www.hitcon.org/hit2008". The browser's toolbar includes navigation buttons, a search box with "Google" text, and various utility icons. The main content area displays a large heading "IWSVA 3.1 Beta Event (IWSVA-TAIWAN)". Below this, there is a section titled "IWSVA 3.1 Alert". A prominent message box with a pink header and yellow background states: "URL Blocked. The URL that you are attempting to access is a potential security risk. Trend Micro IWSVA has blocked this URL in keeping with network security policy." Below the message, it lists the URL as "http://www.hitcon.org/hit2008" and the category as "Block Rule: Web Reputation - Very Low". The bottom status bar shows the text "完成" (Complete) on the left, a security icon, the "Internet" label, and a zoom level of "100%" on the right.

IWSVA 3.1 Beta Event (IWSVA-TAIWAN) - Windows Internet Explorer

http://www.hitcon.org/hit2008

IWSVA 3.1 Beta Event (IWSVA-TAIWAN)

IWSVA 3.1 Beta Event (IWSVA-TAIWAN)

IWSVA 3.1 Alert

URL Blocked

The URL that you are attempting to access is a potential security risk. Trend Micro IWSVA has blocked this URL in keeping with network security policy.

URL: http://www.hitcon.org/hit2008
Category: Block Rule: Web Reputation - Very Low

完成 Internet 100%

Secure Cloud – URL Filtering

Web Search Results:

Search Results

Website www.hitcon.org

Category Spyware

Reputation This web site is known to Trend Micro to be a malicious web site.

[SecurityTracker.com Archives - Microsoft Excel STYLE Record Bug ...](#)

4 Jul 2006 ... Excel 2000/XP/2003 Style 0day POC POC <http://www.hitcon.org/Nanika.xls>

Description: A vulnerability has been discovered in Microsoft Excel, ...

www.securitytracker.com/id?1016430 - 18k - [Cached](#) - [Similar pages](#) - [Note this](#)

[SecurityFocus](#)

3 Jul 2006 ... **nanika** chroot.org. Excel 2000/XP/2003 Style 0day POC POC

<http://www.hitcon.org/Nanika.xls> Description: A vulnerability has been discovered ...

www.securityfocus.com/archive/1/archive/1/438963/100/0/threaded - 10k -

[Cached](#) - [Similar pages](#) - [Note this](#)

[SecurityFocus](#)

5 Jul 2006 ... e:file:file:file:file:file:file:file:file:file:file:file:file:file: Attachment: http://hitcon.org/Nanika-desktop_explore_0day.rar ...

www.securityfocus.com/archive/1/439153 - 11k - [Cached](#) - [Similar pages](#) - [Note this](#)

[More results from www.securityfocus.com »](#)

[SecurityReason - Windows Explorer URL File format overflow](#)

http://hitcon.org/Nanika-desktop_explore_0day.rar you can drop in desktop :P

<http://hitcon.org> <http://www.chroot.org>. Feedback : ...

securityreason.com/securityalert/1186 - 23k - [Cached](#) - [Similar pages](#) - [Note this](#)

[Re: Windows Explorer URL File format overflow](#)

On 5 Jul 2006 05:53:52 -0000, **nanika@xxxxxxxxxxxx** <**nanika@xxxxxxxxxxxx**> wrote: ...

Attachment: http://hitcon.org/Nanika-desktop_explore_0day.rar you can drop in ...

archive.cert.uni-stuttgart.de/bugtraq/2006/07/msg00129.html - 7k -

[Cached](#) - [Similar pages](#) - [Note this](#)



TREND MICRO Web Reputation Query - Online System

Trend Micro Web Reputation Query - Online System

Type a website in the field below to:

- Check its reputation ranking/score
- Submit feedback about a certain website

Complete website*:

Only HTTP and HTTPS are supported. (e.g.,
<http://www.trendmicro.com>)

Check Web Site

Submit Feedback



Reported Attack Site!

This web site at bt.icefish.org has been reported as an attack site and has been blocked based on your security preferences.

Attack sites try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack sites intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

[Get me out of here!](#)

[Why was this site blocked?](#)

[Ignore this warning](#)

Warning - visiting this web site may harm your computer!


Suggestions:

- [Return to the previous page](#) and pick another result.
- Try another search to find what you're looking for.

Or you can continue to <http://bt.icefish.org/> at your own risk. For detailed information about the problems we found, visit Google's [Safe Browsing diagnostic page](#) for this site.

For more information about how to protect yourself from harmful software online, you can visit StopBadware.org.

If you are the owner of this web site, you can request a review of your site using Google's [Webmaster Tools](#). More information about the review process is available in Google's [Webmaster Help Center](#).

Advisory provided by 

We test the Web to help keep you safe from spyware, spam, viruses and online scams.

SiteAdvisor's safety ratings help you stay safe online



Loading ...



McAfee VirusScan Plus

[AntiVirus, Firewall, AntiSpyware](#)
[Download Now & Save 50%!](#)



Download SiteAdvisor now
For Internet Explorer

Secure Cloud – Antivirus

Secure Cloud – Antivirus

Wait! What?

Secure Cloud – Antivirus

Antivirus vendors are facing very big challenges.

AV industry in 1998



AV industry in 2008



Secure Cloud – Antivirus

Panda Security TruPrevent - Collective Intelligence 2007

FROM TRADITIONAL
ANTIVIRUS
TO COLLECTIVE
INTELLIGENCE
PANDA'S TECHNOLOGY EVOLUTION

White Paper by **Panda Research**
research.pandasoftware.com

Secure Cloud – Antivirus

TruPrevent - Collective Intelligence

Benefiting from “community” knowledge to proactively protect others.

Automating and enhancing malware collection, classification and remediation.

Gaining knowledge on techniques to improve existing technologies.

Deploying new generation of security services
from the cloud.

Secure Cloud – Antivirus

McAfee Artemis

McAfee Avert® Labs Artemis

What is Artemis?

Project “Artemis” will enable McAfee to provide our customers using windows-based McAfee Anti-virus products with the most up-to-date detections for certain malware. Artemis will be looking for suspicious programs and dlls running on Windows endpoints protected by McAfee products, including VirusScan Enterprise, ToPS SB V4.5, and VirusScan. When suspicious programs are found, Artemis will send a request to a central database server hosted by McAfee Avert Labs. The database server is continually updated by the McAfee Avert Labs Research teams whenever new malware is found. When the database receives the request from Artemis enabled end-point, it will determine if this program is malicious and will respond.

Secure Cloud – Antivirus

McAfee Artemis

Provide customers with the most up-to-date detections for certain malware.

Looking for suspicious programs and dlls

Send a request to a central database server hosted by McAfee Avert Labs

Server will determine if this program is malicious and will respond

Secure Cloud – Antivirus



Anti-Virus Comparative

Technology Preview Report

McAfee Artemis

Date: February 2008

Last revision: 3rd June 2008

Secure Cloud – Antivirus

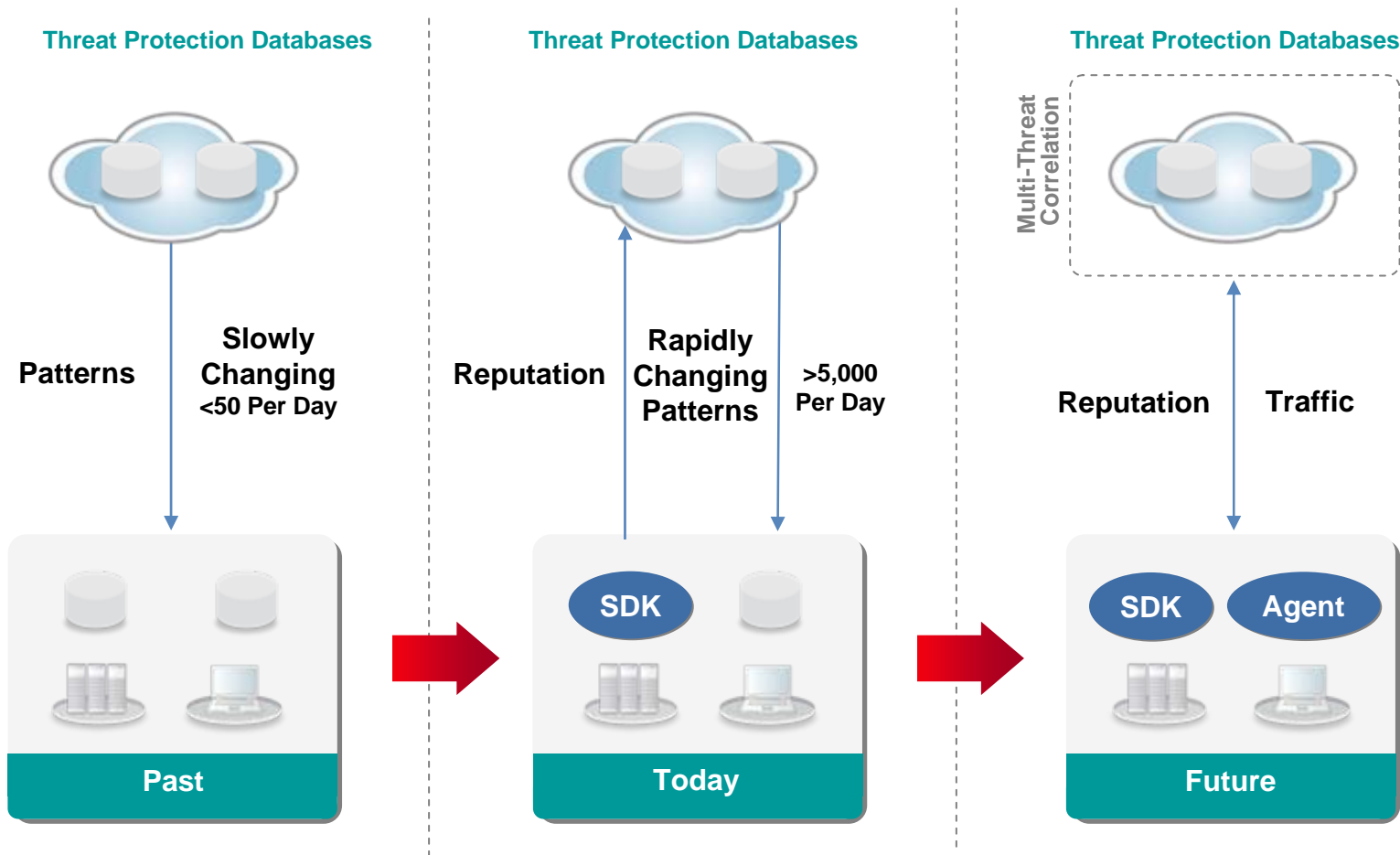
<i>Company</i>		McAfee		McAfee	
<i>Product</i>		McAfee VirusScan+		McAfee VirusScan+	
<i>Program version</i>		12.0.176		12.0.176	
<i>Engine / signature version</i>		5200.2160 / 5222		5200.2160 / 5222	
<i>Number of virus records</i>		371.817		371.817	
				with Artemis	
Windows viruses	149.202	147.115	98,6%	148.326	99,4%
Macro viruses	95.059	95.056	~100%	95.056	~100%
Script viruses	14.284	12.855	90,0%	12.855	90,0%
Worms	190.952	188.318	98,6%	190.816	99,9%
Backdoors/Bots	400.986	383.059	95,5%	398.850	99,5%
Trojans	817.043	757.305	92,7%	808.359	98,9%
other malware	15.838	14.370	90,7%	15.412	97,3%
TOTAL	1.683.364	1.598.078	94,9%	1.669.674	99,2%

During our tests over our clean set of files we found Artemis producing very many false alarms (over 500), but it has to be considered that this technology is still not fully tested and was an internal beta at time of testing.

Secure Cloud – Antivirus

**Trend Micro
File Reputation Service
and
Smart Protection Network
June, 2008**

Secure Cloud – Antivirus



Secure Cloud – Antivirus

Secure Cloud – Antivirus

Trend Micro FRS

Minimal endpoint pattern updates.

Significantly reduce endpoint memory consumption

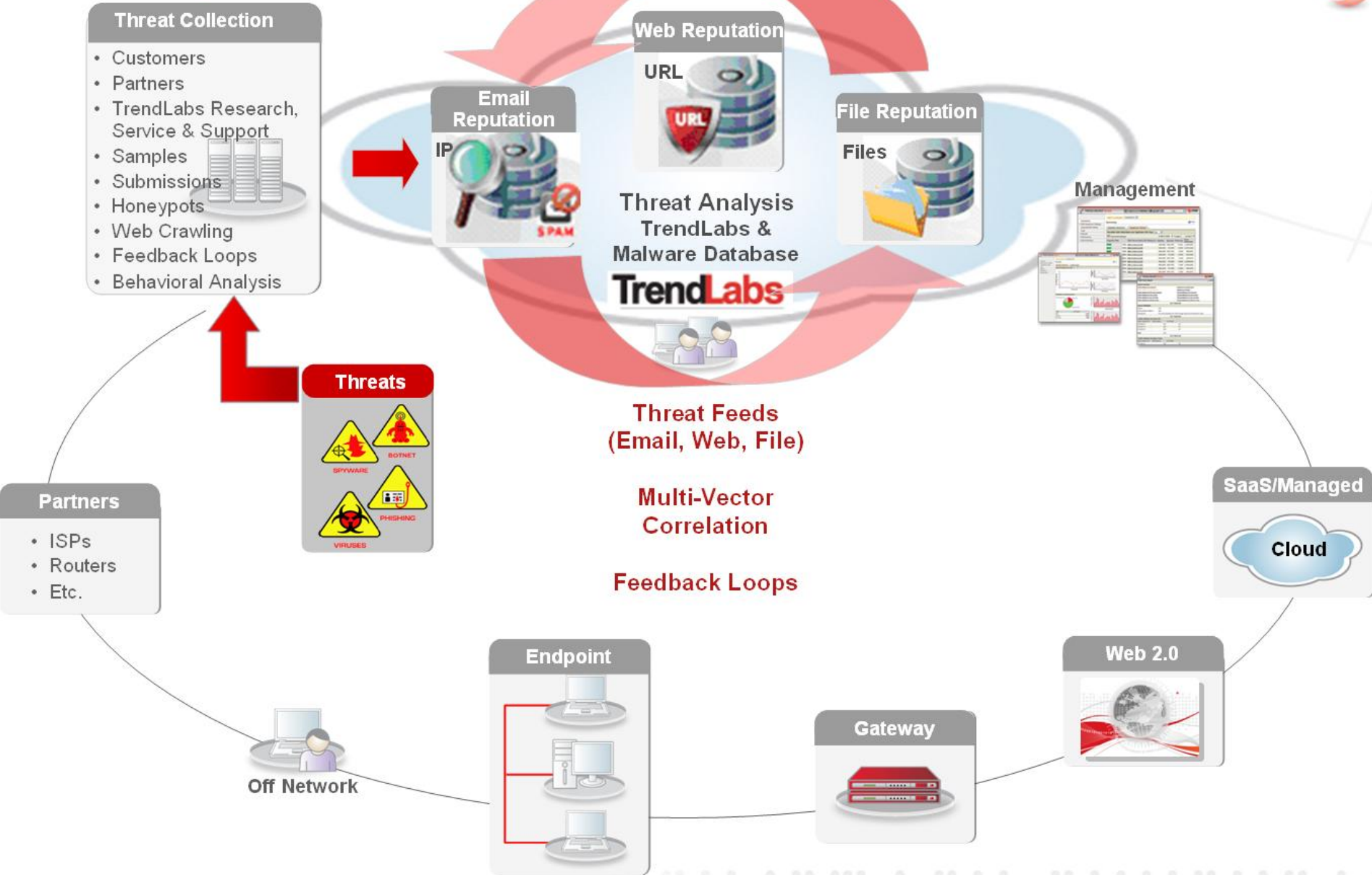
Protect in real time

Reduce the need for pattern updates

Trend Micro Smart Protection Network

Securing Your Web World

Security Made Smarter



Secure Cloud - Benefits

Effectiveness

Flexibility

Ease of Deployment and Use

No admin and setup overhead

Low total cost of Ownership

Scalability and Reliability

Secure Cloud - Benefits

It hopes the shift in architecture will help to speed its reaction to zero-day threats and improve the performance of end users' PCs.

Secure Cloud – Challenge - Technical

Must be

**Stable and
Internet Connected**

Secure Cloud – Challenge - Technical

DNS becomes very critical.

DNS hijacking risks.

DNS must be stable as well.

Secure Cloud – Challenge - Technical Antivirus ‘in the cloud’ problems

Easier to be bypassed?
(Cache attack)

It is still pattern based scanning.
(against dark cloud packer)

<http://meatchicken.com/packer.pl?file=trojan.exe>

Overestimated forensics engine

Secure Cloud – Challenge - Technical

Are they all “hacker safe” ;-)

It makes total sense but they don't mention what will happen if they get hacked

What you send is not what is received?

Cloud becomes critical.
(once hacked, all hacked.)

Secure Cloud – Challenge – non Technical

Privacy Issue.

When someone else hosts and processes your data, how can you tell if it is "secure?"

If you haven't noticed yet, everything is pushed into the cloud, not only your social life but your personal data and now even your health records thanks to Google.

Secure Cloud – Challenge – non Technical

Cost

the cost of shifting away from
their existing deployment.

Secure Cloud – Challenge – non Technical

Enterprise Concerns

IT against.

New model introduced new
vulnerabilities.

Billing model changed.

Secure Cloud – Challenge

SaaS infrastructures are
definitely more attractive to
attackers. :)

Secure Cloud – Challenge

Are you cloud services used
by normal user or bad guys?

Leverage existing cloud
services

(Hacking - power by Google
cpu/bandwidth/...)

Discussion

Discussion

White list

VS

Black list

Discussion

Behavior / heuristic analysis

vs

Signature based protection

Discussion

Is it just a white or black listed
filtering model.

No, the most valuable thing is
collaboration

Discussion

Correlation technology with behavioral analysis.

Feedback loops contributing

Conclusion

It is still worth to try for
security vendors
(as well as for hackers)

Behind the Cloud



Who is watching you?