black hat® EUROPE

March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

HELDHAFTIG VASTBERADEN BARMHARTIG

An Attacker's Day into Human Virology

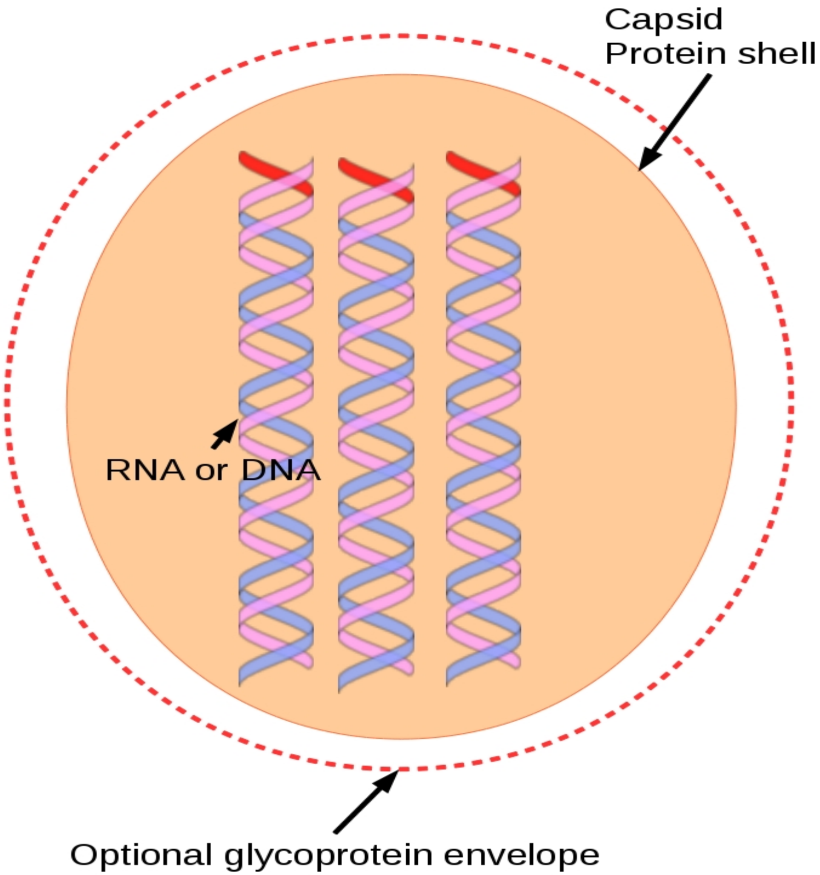
Guillaume Lovet, Axelle Apvrille
Fortinet

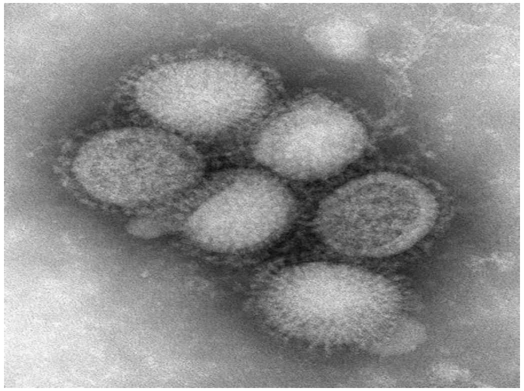
black hat® EUROPE

March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

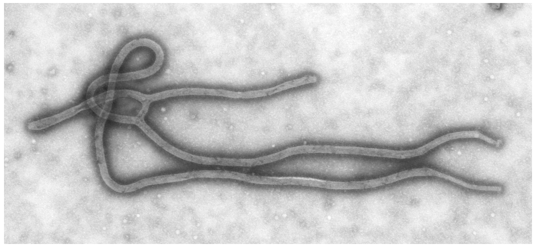
HELDHAFTIG VASTBERADEN BARMHARTIG

What is a Virus ?

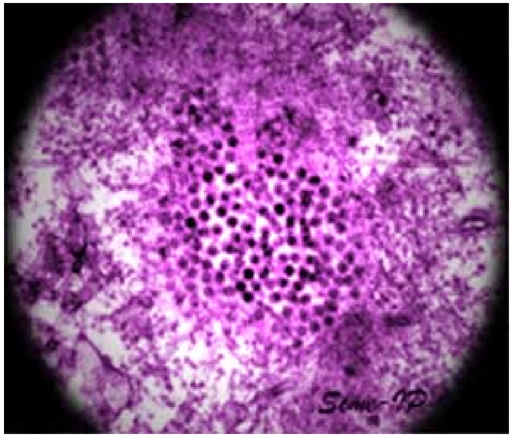




H1N1 Flu



Ebola

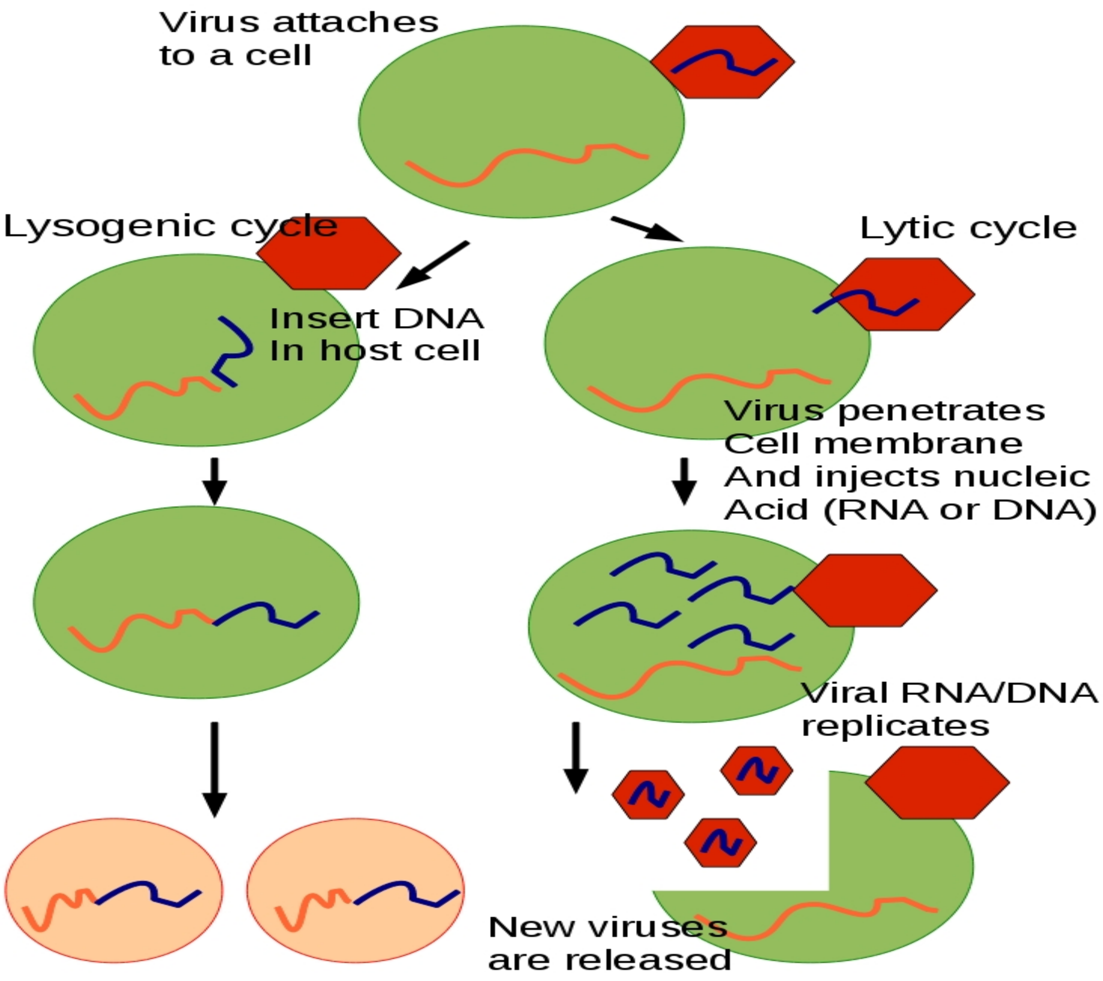


West Nile Virus

black hat EUROPE
March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

Photo credits: CDC, NIH

Virus Replication



Virus attaches to a cell

Lysogenic cycle

Insert DNA In host cell

Lytic cycle

Virus penetrates Cell membrane And injects nucleic Acid (RNA or DNA)

Viral RNA/DNA replicates

New viruses are released

The Immune System

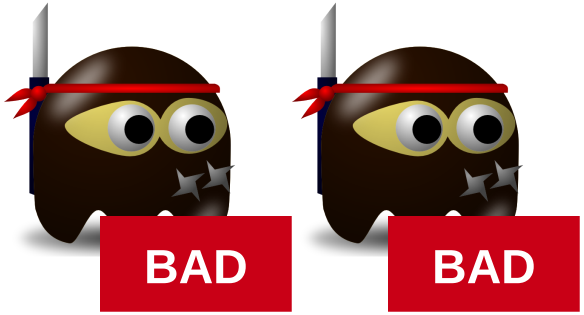
Innate

- Non-specific response
  - Generic
- Contents
  - Complement system
  - Phagocytes
  - NK cells
  - ...

Adaptive

- Specific response
  - Immunity via memory mechanisms
- Contents
  - Helper T cells
  - Killer T cells
  - B cells

The Complement System

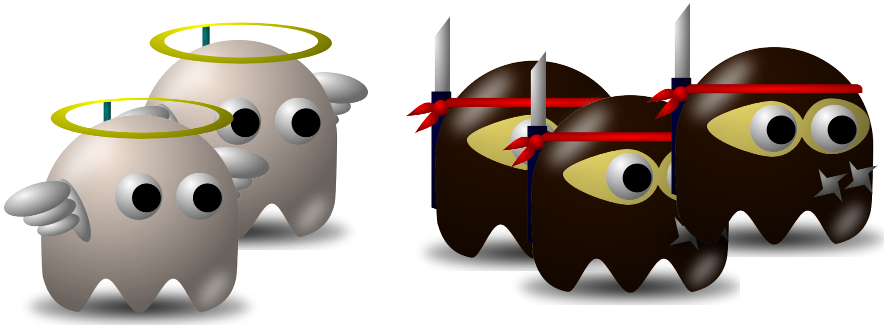


Mark intruder to have
Then eaten up

OPSONIZATION

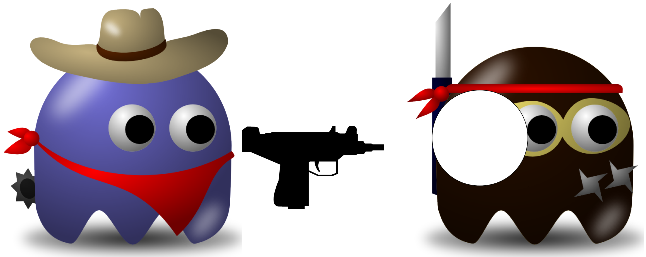
Attract macrophages

CHEMOTAXIS



Group intruders

CLUMPING

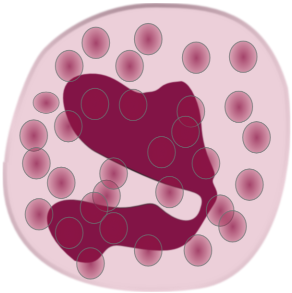


Make a hole into

MEMBRANE ATTACK COMPLEX

black hat EUROPE
March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

Phagocytes



Granulocytes aka polymorphonuclear leukocytes

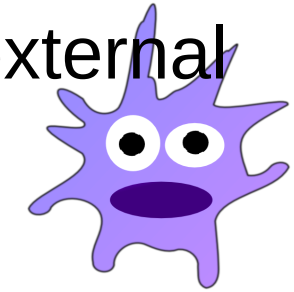
- Fast to react
- Small appetite
- Release toxic material to eat

Macrophages

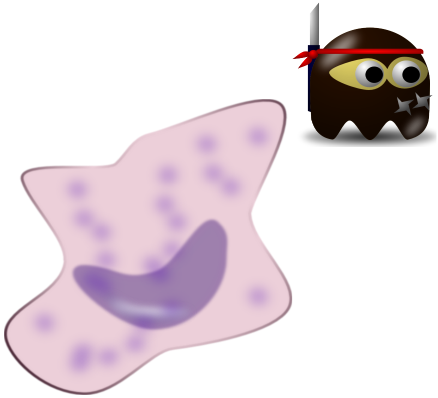
- Big appetite
- Slow to react
- Release cytokines → helps NK cells

Dendritic cells

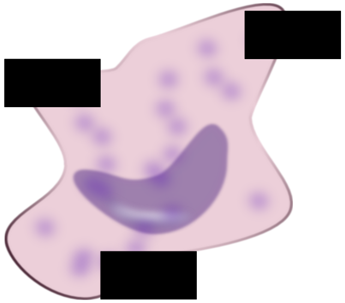
- Contact with external env.



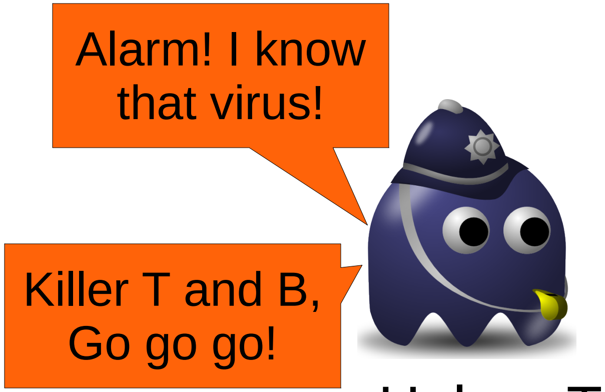
Helper T cells



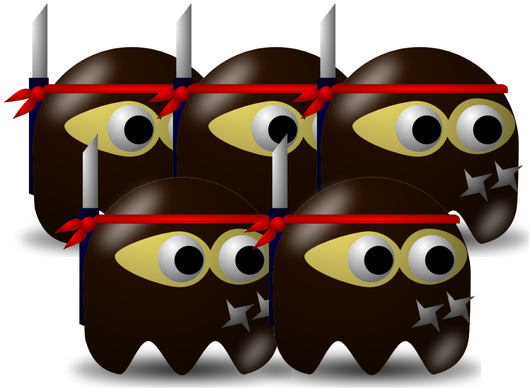
MM... YUMMY!



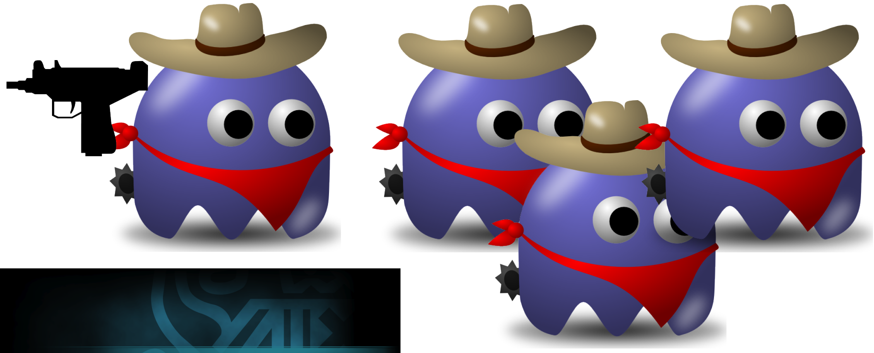
Antigen presentation



Helper T cell activation



Viruses



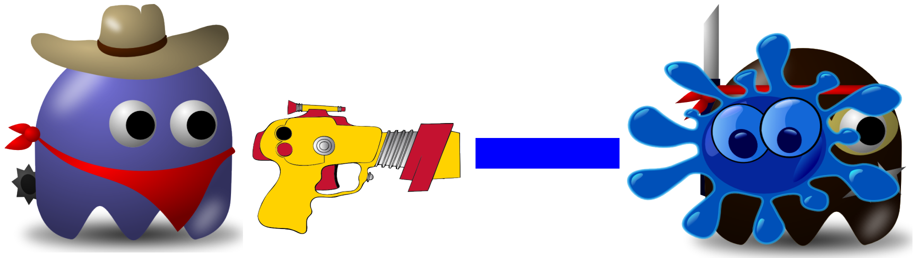
Killer T and B cells

Killer T cells, and B cells

Killer T cells

Like NK cells, but

Dedicated to a virus



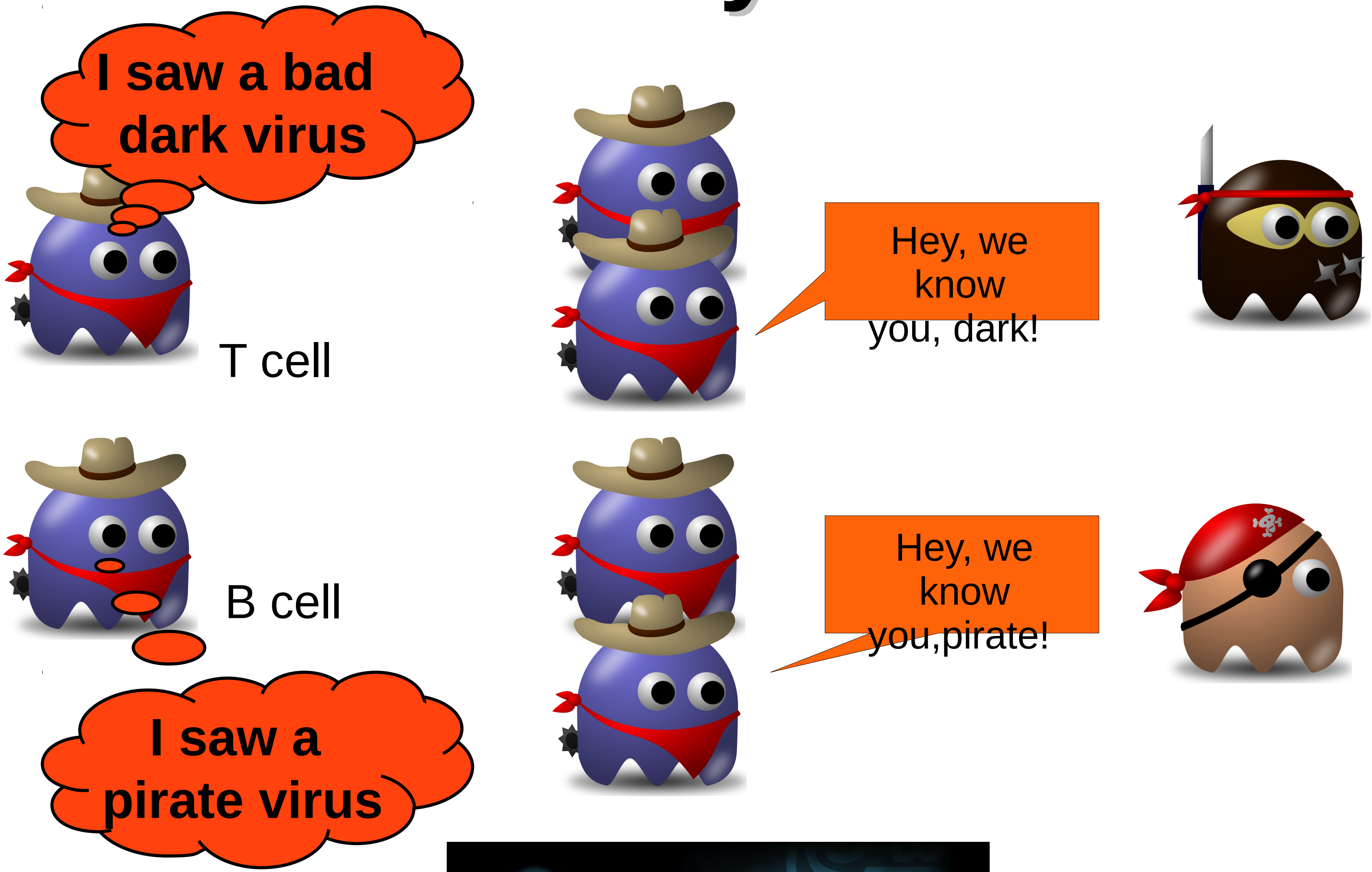
B cells

Mark viruses

with antibodies

→ easy to spot for phagocytes

Memory cells



I saw a bad dark virus

T cell

Hey, we know you, dark!

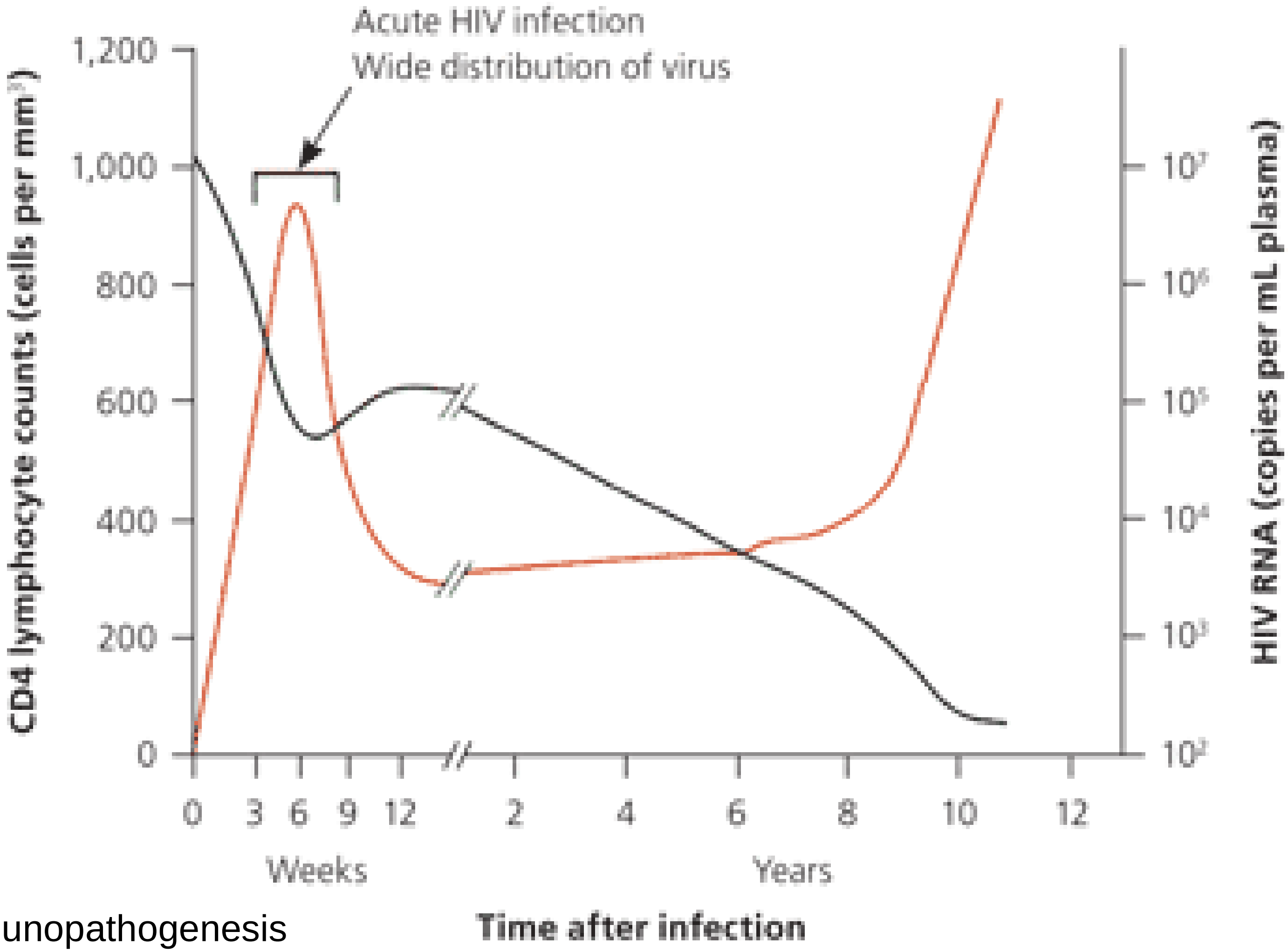
I saw a pirate virus

B cell

Hey, we know you,pirate!

Outnumbering defenses

1 million of HIV virus per ml of blood

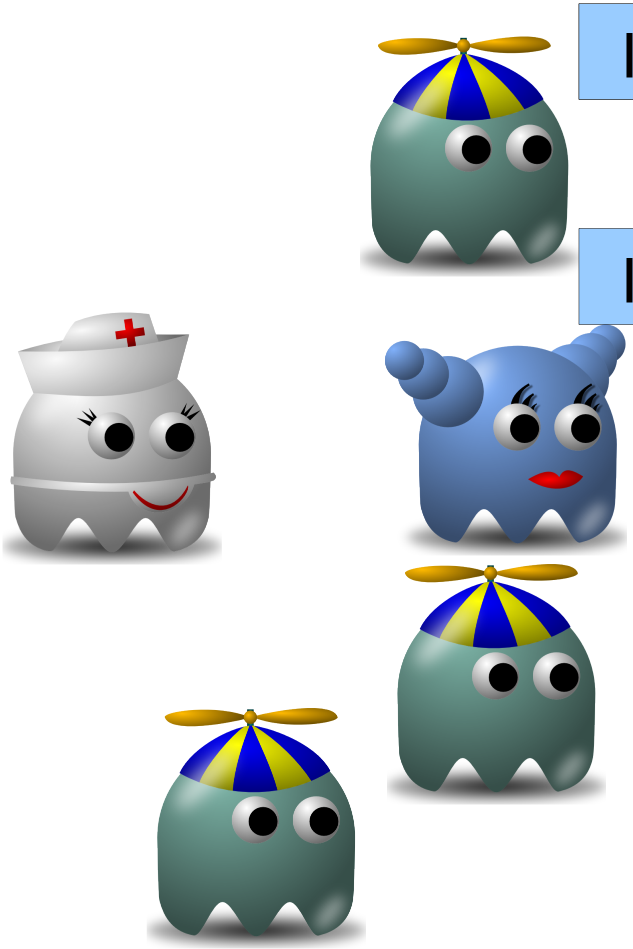


Source: AS. Fauci et al
New concepts in the immunopathogenesis
Of human immunodeficiency virus infection

Outnumbering defenses

- No use to massively infect a host
  - Infection indicators
- Propagate to other victims
  - Conficker: > 8 million infected hosts
  - Slammer: 90% of vulnerable hosts in 10 min
  - ZeuS: 3.6 million bots in USA

Waiting Room

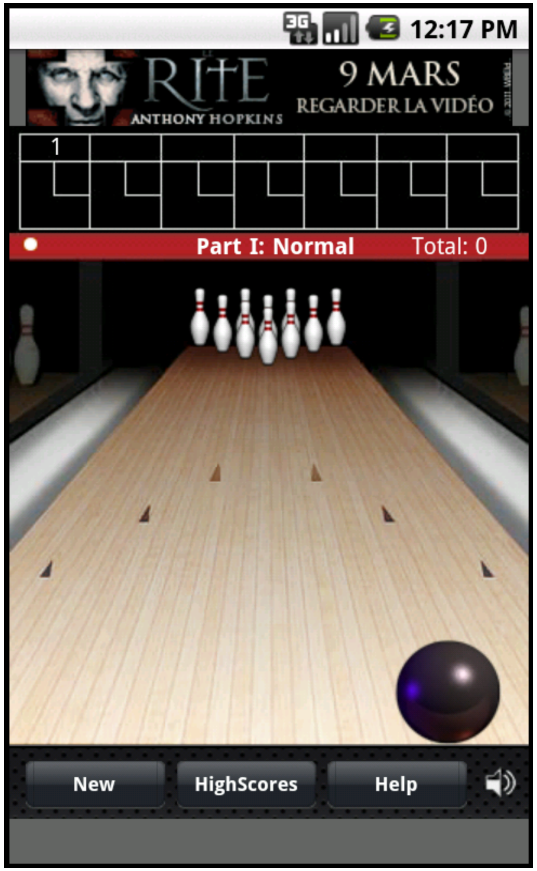


I've got the flu

I've got the flu

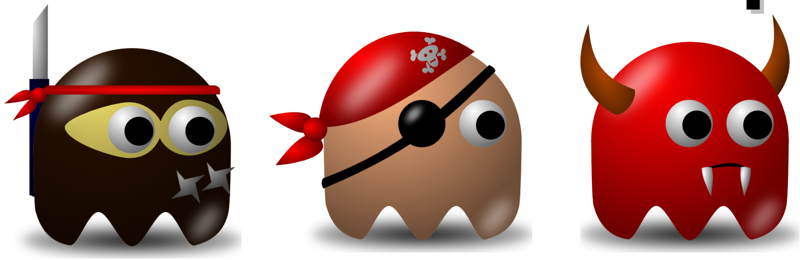
I haven't got
The flu yet,
But soon will :(

I've got the flu



**Android/DrdDream
Shortly available on
The Android Market
> 250,000 infections**

Computer viruses did not invent polymorphism

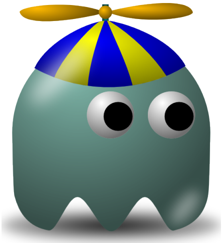


- Influenza: omit the replication error checking protein
- HIV: 1 substitution per genome per round

- Xpaj
- Sality
- Mabezat
- Koobface
- ...

Virus Mixing

I've got flu A



I've also got flu B (unlucky, huh?)

I'm gonna replicate Hybrid flu C!!!

Infected with MyDoom

Infected with Virut

Propagating “MyVirut”!!!

Attacking the AV engine

W32/Sality:

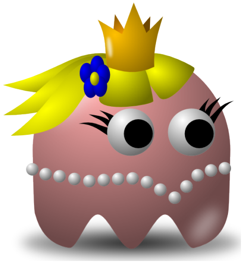
- Terminates anti-virus programs
- Bypasses Microsoft's firewall `HKLM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\Authorized Application List`

- **HIV** replicates in helper T cells, macrophages, dendritic cells → immuno-deficiency
- **Flavivirus** targets lymph nodes & dendritic cells

Targets: Random or Not?

- Rotavirus → small intestine
- Poliovirus → motor neurons
- Rhinovirus → nasopharynx

- W32/Expiro → FileZilla, Internet Explorer, Windows Protected Storage
- iPhoneOS/Eeki → check default password on jailbroken iPhones.



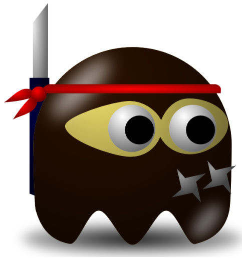
Sleeping beauty

Incubation

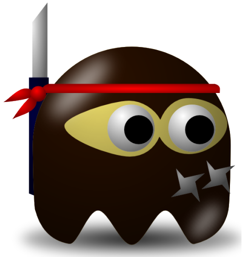
- Chicken pox: 2 weeks
- Flu: 2-3 days
- Measles: 6-19 days
- Ebola: 2-21 days
- Rabies: 2-12 weeks

No real utility for malware authors?

- Time bombs
- Michelangelo (1991) → March 6th
- CodeRed (2001) → 1st - 19th of each month
- Conficker: fake date (April 1st)



Remaining Infected



- **HIV** infects memory T cells

→ replicates without detection

- **TDL4**: infecting the MBR
- **ZeuS** bots: frequent updates

Who's the inventor?

- Brute-forcing
- Polymorphism
- Attack the AV engine
- Find vulnerable hosts
- Time bombs
- Remain infected
- Anti-debugging tricks

Human Virology

Computer virology

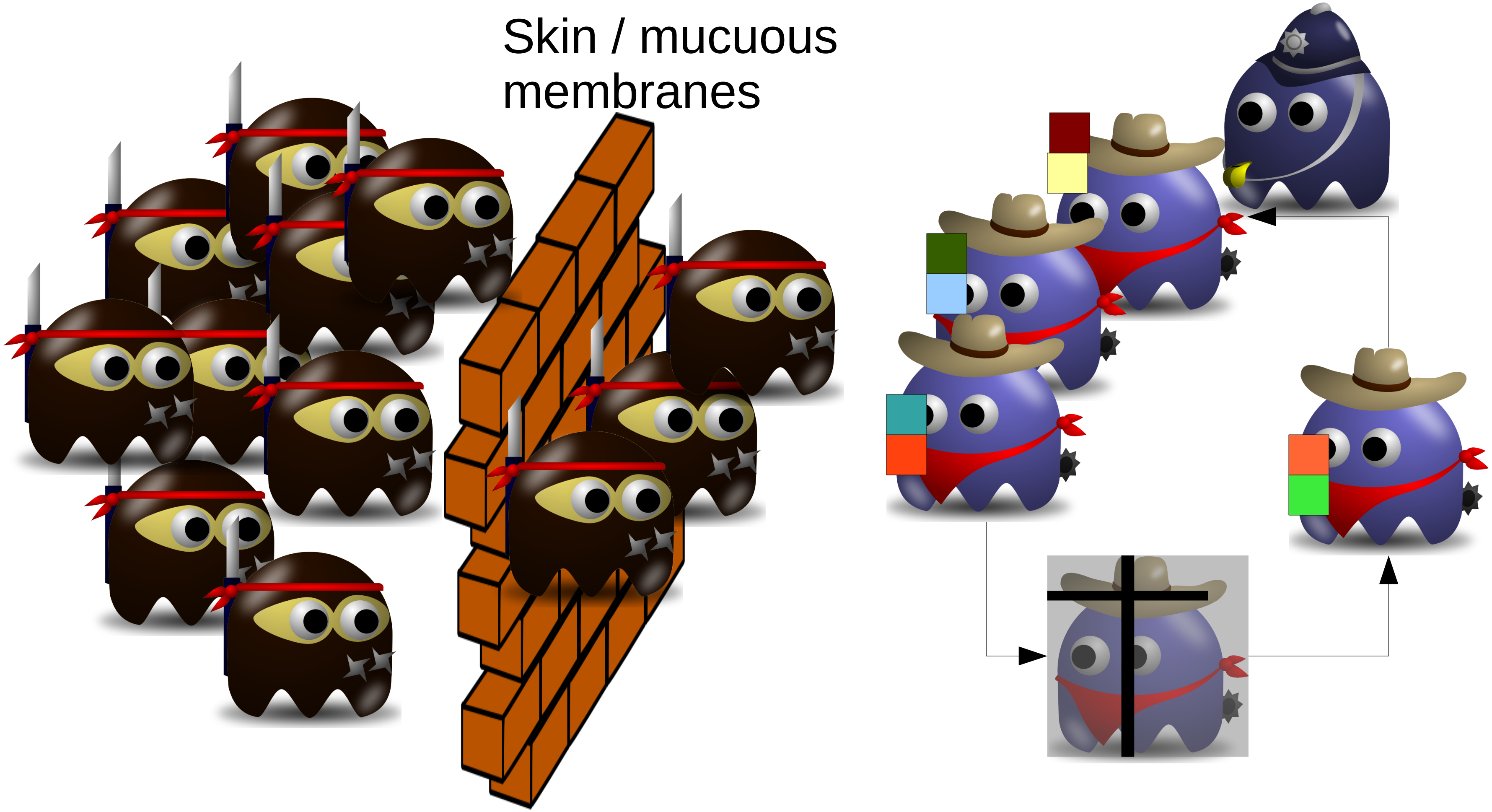
Computer inventions

- URL redirection (especially AV websites): W32/DNSChanger
- Detecting reverse engineering tools (IDA Pro etc)
- Detecting debuggers
- Detecting virtual machines
- Complex code vs Influenza = 22KB

Cures

- Humans able to work when already infected
  - Kill infected cells
  - Post exposure treatments (e.g Rabies)
- Detecting viruses
  - Body uses whitelisting!
  - Adaptive immune system ~ Generic signatures
  - Vaccines: detect non-variable elements

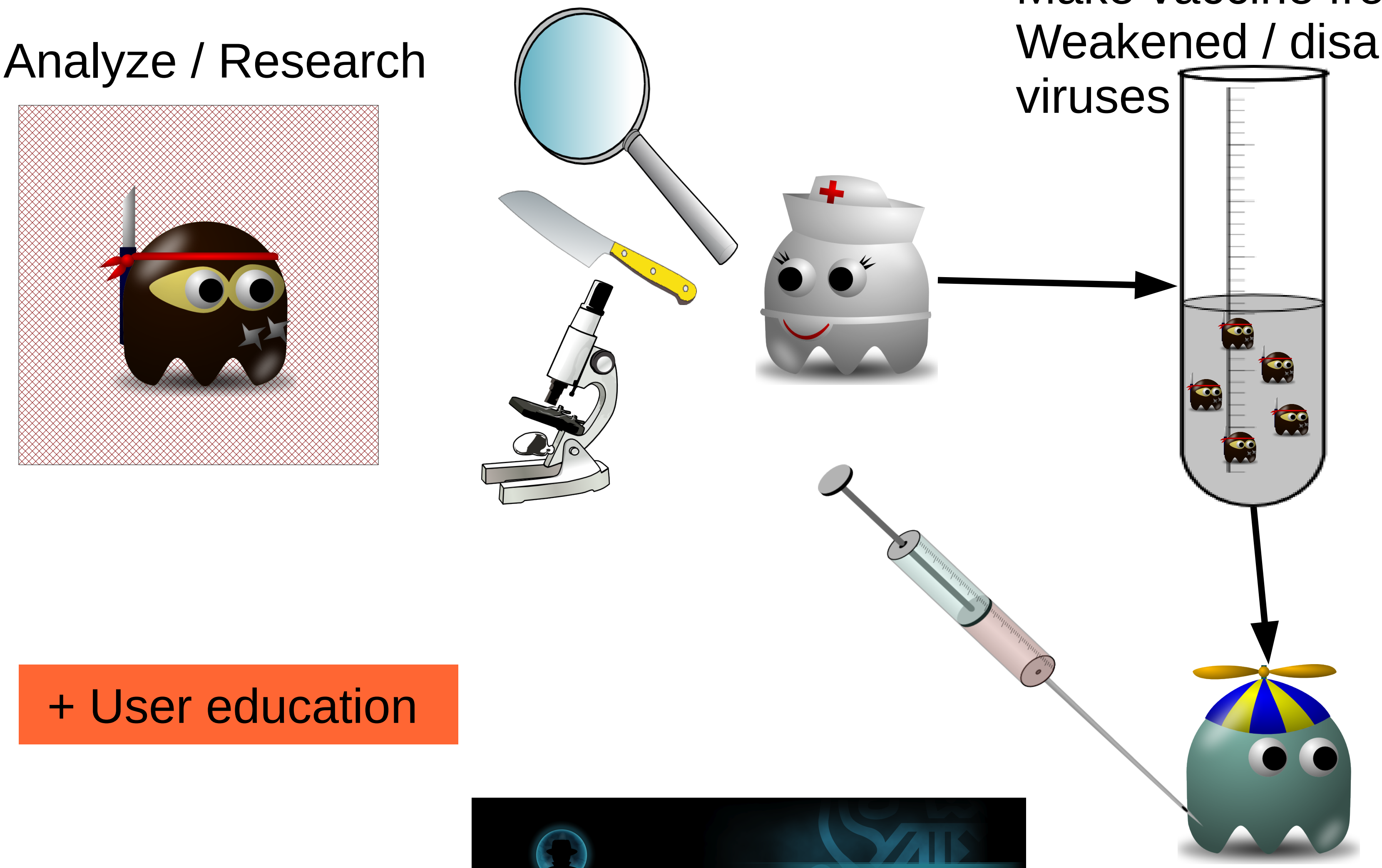
Handling unknown viruses



10^16

10^8

Prevention



Analyze / Research

Make vaccine from Weakened / disabled viruses

(Ouch, that hurts)

+ User education

black hat EUROPE
March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

Convergence and Futuristic Threats

- Essence
- Purpose
- Crossing the frontier?

Essence of a Virus

- Biological: DNA strand
  - info in base 4 (A, G, C, T)
  - Coding proteins => behavior

- Computer: Binary code
  - info in base 2 (0, 1)
  - Coding instructions => behavior

Both = information coding for a parasitic, replicative behavior

Purpose of a Virus

- Computer
  - Key: Designed by a conscious intelligence
  - Money, espionnage, destruction...
- Biological
  - Key: Fruit of random mutations (Darwin)
  - No “purpose”

Switching Realms

=> Designed Biological Viruses

=> Darwinian Computer Viruses

Designed Biological Virus

- Pop Culture: AIDS, SARS, St Mary
- Synthetic Viruses: Polio (2002), SARS (2008)
- Bio Weapons?

Darwinian Computer Virus

- Evolvable Malware with genetic algo
- Spontaneous virus?
- Pop Culture: Ghost in the Shell
  - 15 Petabytes of new info daily
  - Smallest virus: 8 chars

Convergence

- Same Essence
- Info materialized differently
- Virus crossing to the other realm
    - a fool's question?

Blurring the Frontier

- Cybernetic Device = Computers
- PoC: Implanted RFID chip (2010)
- Evolution of “living organism” definition

Crossing the Frontier

- 2010: Bacteria Synthesized
- Genes are modified for applications, daily
- Info that codes for synth DNA stored where..?
- Sequencing DNA involves Software...

black hat® EUROPE
March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

Thank You!

Please fill your feedback survey form!

Contact:

glovet (at) fortinet.com
aapvrille (at) fortinet.com
Twitter: @FortiGuardLabs