

# Games, Metrics, and Emergent Threats

Adam J. O'Donnell, Ph.D.

Cloudmark, Inc.

[adam@cloudmark.com](mailto:adam@cloudmark.com)

[adam.j.odonnell@gmail.com](mailto:adam.j.odonnell@gmail.com)

<http://np-incomplete.com>

When will attackers move  
from target *X* to target *Y*?



- Windows malware: around 250k samples by the end of 2006, 500k by the end of 2007, I'm may have been already hit.
- Macintosh Malware: under 100, including pre-OSX

1. Mac users are just fundamentally more intelligent than PC users
2. Macs are harder to attack, and therefore less malware exists
3. Mac market share is too small to be of interest to malware writers

1. ~~Mac users are just fundamentally more intelligent than PC users~~
2. Macs are harder to attack, and therefore less malware exists
3. Mac market share is too small to be of interest to malware writers

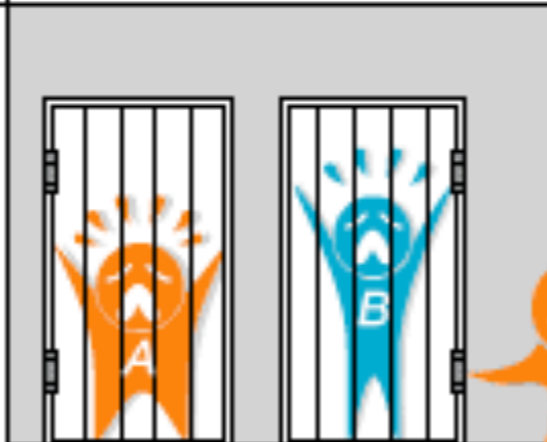



1. ~~Mac users are just fundamentally more intelligent than PC users~~
2. ~~Macs are harder to attack, and therefore less malware exists~~
3. Mac market share is too small to be of interest to malware writers

**If not now, when?**



# Game Theory!

# Prisoners' dilemma

		prisoner B			
		confess		remain silent	
prisoner A	confess	 5 years    5 years	 0 year    20 years		
	remain silent	 20 years    0 year	 1 year    1 year		

# Dr. Strangelove

Or:  
How  
I Learned  
To  
Stop  
Worrying  
And  
Love  
The  
Bomb





- **Players:** *Users* and *Attackers*
- **Strategies:** *Users* can either defend *A* or *B*; *Attackers* can either attack *A* or *B*
- **Payoffs:** Zero-Sum game; *Attackers* compromise all systems if they are undefended, but only fraction if they are defended

$f$	Market size of majority systems
$p$	Accuracy of security mechanisms
$v$	Value of a compromised host

# Normal Form

		Defend	
		A	B
Attack	A	$(1-p)fv$	$fv$
	B	$(1-f)v$	$(1-p)(1-f)v$

# Normal Form

		Defend	
		A	B
Attack	A	$(1-p)fv$	$fv$
	B	$(1-f)v$	$(1-p)(1-f)v$



- If the ratio  $f/(1-f)$  is greater than  $1/(1-p)$ , then there is no rational point to attacking system  $B$ .

- Translation: Protection methods have to have effectiveness rates around the same level as the market penetration of *A* to make attacking *B* viable.

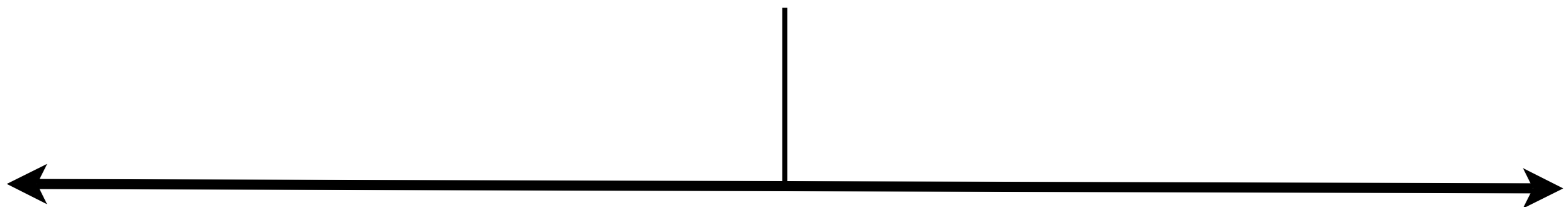
- Translation: Protection methods have to have effectiveness rates approximately the same level as the market penetration of PC to make attacking Macs viable.

# Given AV Accuracy...

- At 95% effectiveness rates, Macs will be attacked at 4.8% market share.
- At 80% effectiveness rates, Macs will be attacked at 16.7%

# Bottom Line?

I expect relatively wide-spread, monetized Mac malware when we see around 12-16% of the Internet population using Macs.



More likely...

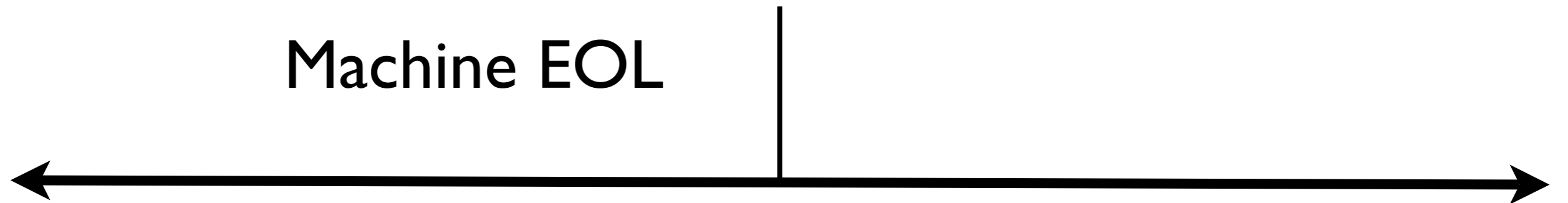
Less likely...

Cleanup Services

More Macs      Better AV

Competitive Malware

Machine EOL



More likely...

Less likely...

Cleanup Services

Efficient  
Malware Market

More Macs      Better AV

Recession

Competitive Malware

Targeted & Zero  
Day Attack  
Effectiveness

Machine EOL



More likely...

Less likely...



# Predicting Emerging Threats

		Defend	
		A	B
Attack	A	$(1-p)fv$	$fv$
	B	$(1-f)v$	$(1-p)(1-f)v$

		Defend	
		E-Mail	Social Networks
Attack	E-Mail	$(1-p)fv$	$fv$
	Social Networks	$(1-f)v$	$(1-p)(1-f)v$

		Defend	
		E-Mail	SMS
Attack	E-Mail	$(1-p)fv$	$fv$
	SMS	$(1-f)v$	$(1-p)(1-f)v$

		Defend	
		MySpace	Facebook
Attack	MySpace	$(1-p)fv$	$fv$
	Facebook	$(1-f)v$	$(1-p)(1-f)v$

		Defend	
		Twitter	Qwigibo
Attack	Twitter	$(1-p)fv$	$fv$
	Qwidgibo	$(1-f)v$	$(1-p)(1-f)v$

		Defend	
		Twitter	Qwigibo
Attack	Twitter	$(1-p)fv$	$fv$
	Qwidgibo	$(1-f)v$	$(1-p)(1-f)v$

# What is “v”?

The value of a given target is defined by how much value an attacker can extract over time.



“v” defined by...

# “v” defined by...

User response rate

Message generation rate

# “v” defined by...

User response rate

Message generation rate

Cost of account creation

Target market

# “v” defined by...

Network size

User response rate

Message generation rate

Cost of account creation

Target market

Number of contactable users

**Can we enumerate all of these factors and measure them, thereby to predict who will be attacked next?**

**Can we model when the metrics  
are acceptable to business growth  
but not highly “attackable”?**

# Games, Metrics, and Emergent Threats

Adam J. O'Donnell, Ph.D.

Cloudmark, Inc.

[adam@cloudmark.com](mailto:adam@cloudmark.com)

[adam.j.odonnell@gmail.com](mailto:adam.j.odonnell@gmail.com)

<http://np-incomplete.com>