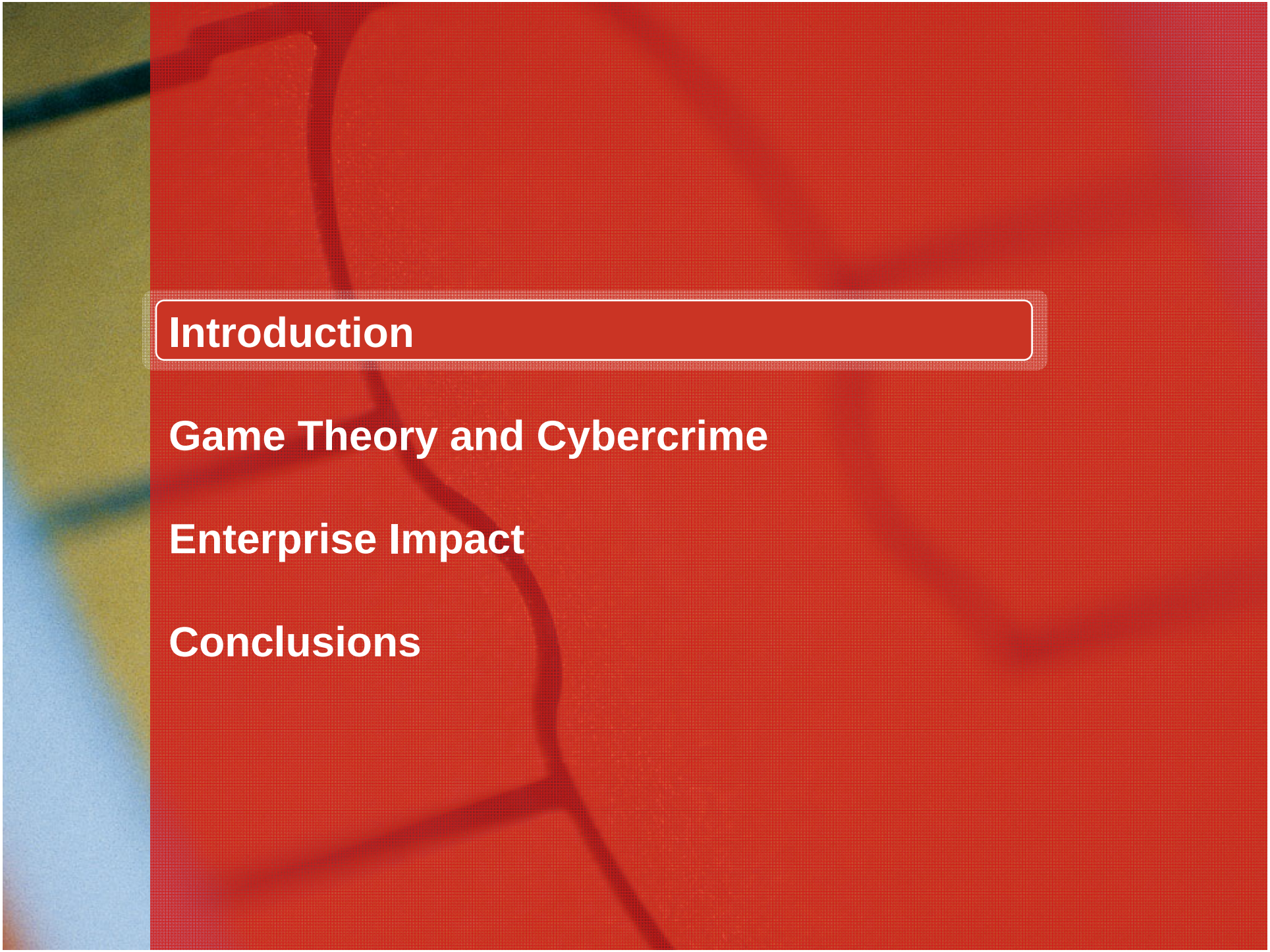
The Economics of Cybercrime (and rationale for optimal risk reduction)

Sam Curry

Chief Technologist, RSA, The Security Division of EMC

October 2010

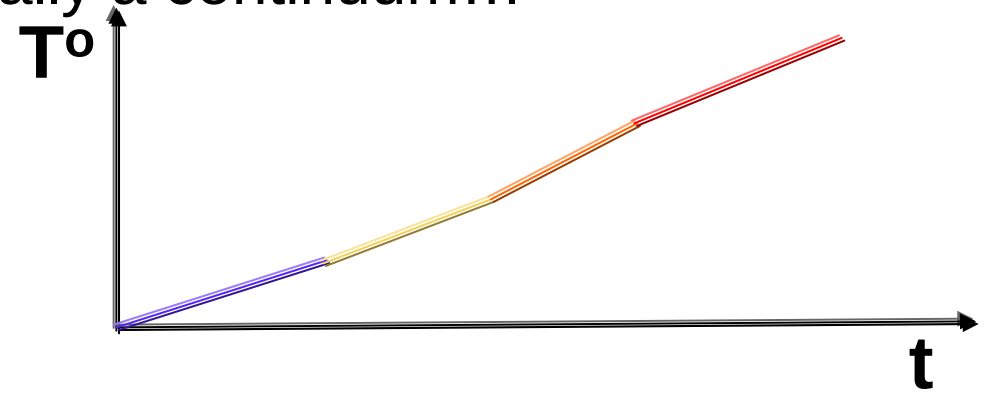

Introduction
Game Theory and Cybercrime
Enterprise Impact
Conclusions


FUD
“from a national security perspective, other than a weapon of mass destruction or a bomb in one of our major cities the threat to our infrastructure, the threat to our intelligence, the threat to our computer network is the most critical threat we face.”
Shawn Henry, Assistant Director of the FBI Cyber Division
NOTE: FUD is an English acronym for FEAR, UNCERTAINTY and DOUBT


Cybercrime economy is massive!
FUD
"Last year was the first year that proceeds from cybercrime were greater than proceeds from the sale of illegal drugs"
Valerie McNiven, who advises the US Treasury on cybercrime

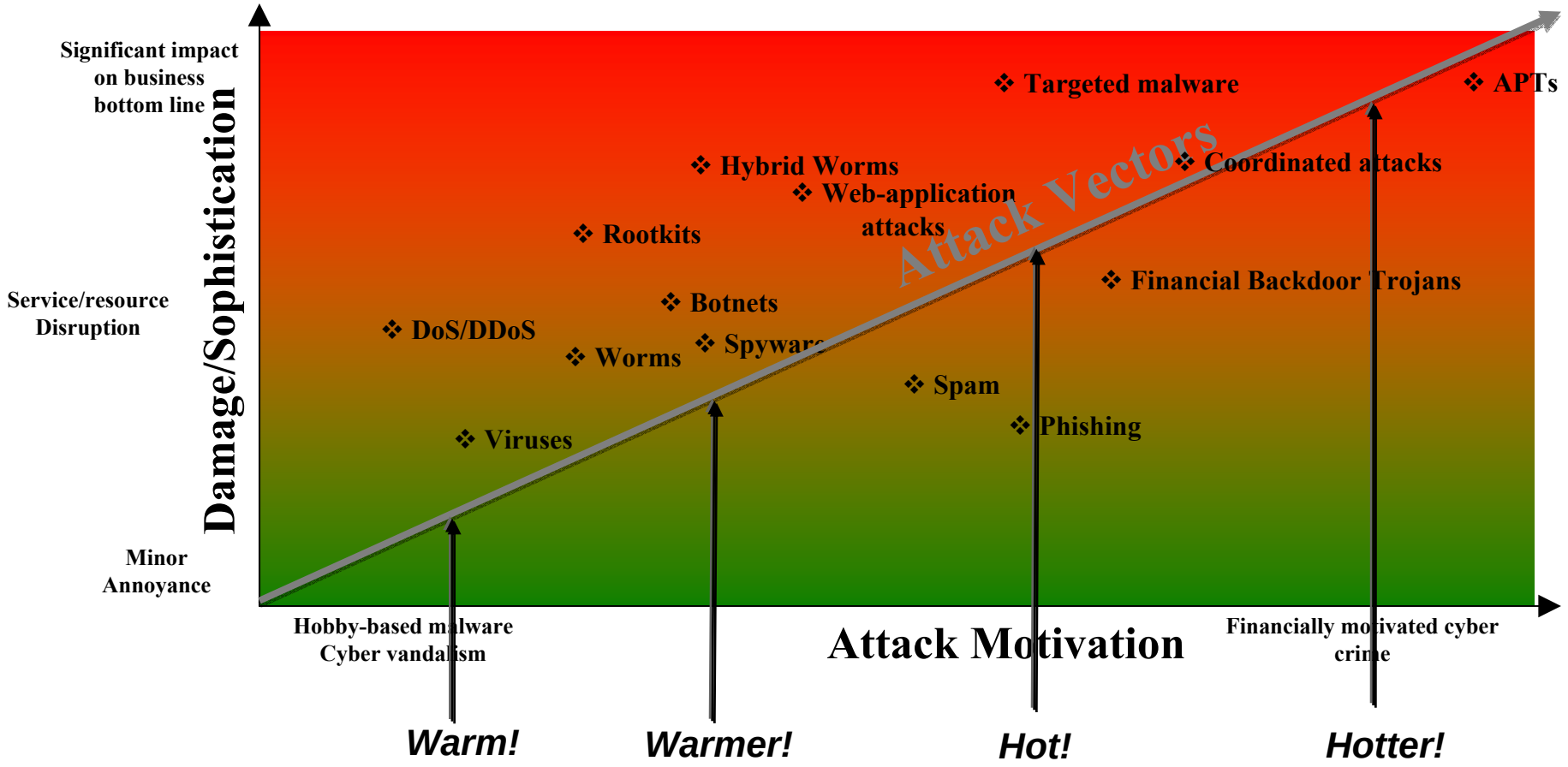
The Frog

- Famous story: frog in gradually heating water…eventually boils to death
- Reality:
  - The frog jumps out before the end but gets scalded as the water heats
  - The frog actually notices the water warming as several separate hot moments before leaping out
- It's actually a continuum…



Source: http://en.wikipedia.org/wiki/Boiling_frog

Changing Threat Environment

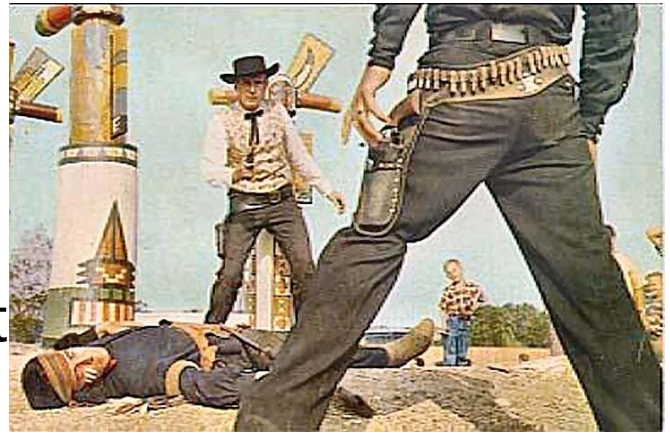


- **Critical point: this isn't 4 things…it's one continuum**
- **What's changing is damage and the sophistication / speed of the opponent!**

RSA
The Security Division of EMC

Content Race

- No one woke up one day and set out to build a massive, unmanage-able technology that is always racing
- Who wins in this picture
- It's all about decision loops
  - OODA
  - Command-and-control
- We have an intelligent opponent
  - They adapt and change
  - They improve / we improve

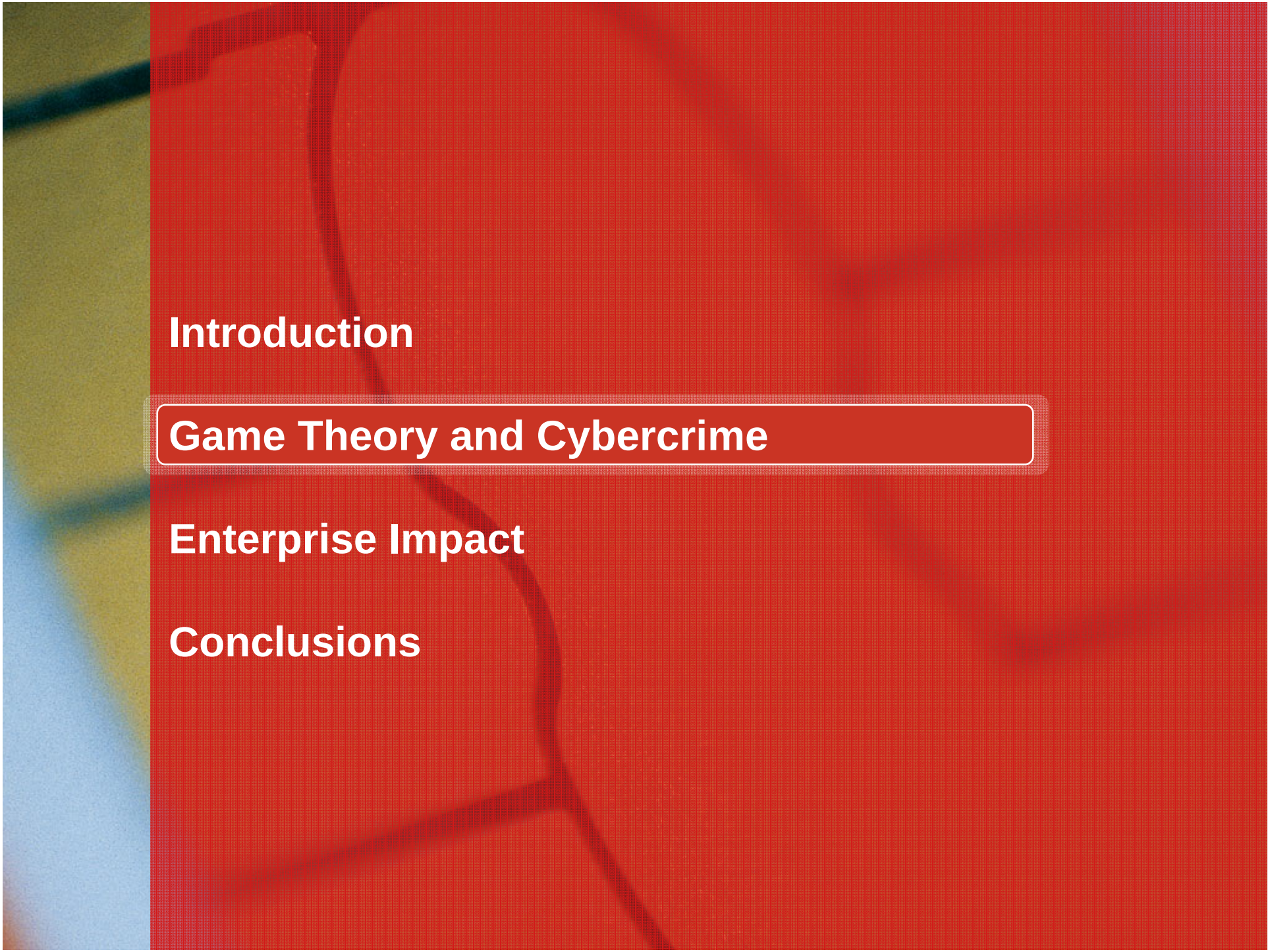


- Conclusion: It always winds up a content race
- Our challenge is to *create an industry and approach that always breaks out of the content race*

The Dark Side of the Cloud

Who's the Big Dog of Cloud Offerings?

Provider	Systems	CPUs	Bandwidth


Introduction
Game Theory and Cybercrime
Enterprise Impact
Conclusions

Cybercrime Dilemma

- Operation Aurora / Google-China incident…
  - In the days of CodeRed, the “private sector” used “public sector” developed tools “Hacked by Chinese”
  - Now…it’s the reverse: “public sector” using “private sector” developed tools
- We are dealing with intelligent, financial motivated opponents
- The main way to describe media and market attention is FUD
- A “War on Cybercrime” doesn’t make sense
  - A study of the *behavior* of online criminals does make sense
  - As with fighting any intelligent opponent, the goal must be…
    - To analyze
    - To act
    - To achieve measurable *reductions* in fraud
      - Make it expensive to do in systematic ways
      - Coordinate better and improve defenses
    - To adapt
    - To repeat the above
- Victory is not found in destroying the opponent, it is found in reducing him (or her)

The Reality

"You know, you can do this just as easily online."

There is an Underground Economy…

Asset	Going-rate
Pay-out for each unique adware installation	30 cents in the United States, 20 cents in Canada, 10 cents in the UK, 2 cents elsewhere
Malware package, basic version	$1,000 – $2,000
Malware package with add-on services	Varying prices starting at $20
Exploit kit rental – 1 hour	$0.99 to $1
Exploit kit rental – 2.5 hours	$1.60 to $2
Exploit kit rental – 5 hours	$4, may vary
Undetected copy of a certain information-stealing Trojan	$80, may vary
Distributed Denial of Service attack	$100 per day
10,000 compromised PCs	1,000 $
Stolen bank account credentials	Varying prices starting at $50
1 million freshly-harvested emails (unverified)	$8 up, depending on quality

Sample data from research on the underground digital economy in 2007

RSA
The Security Division of EMC

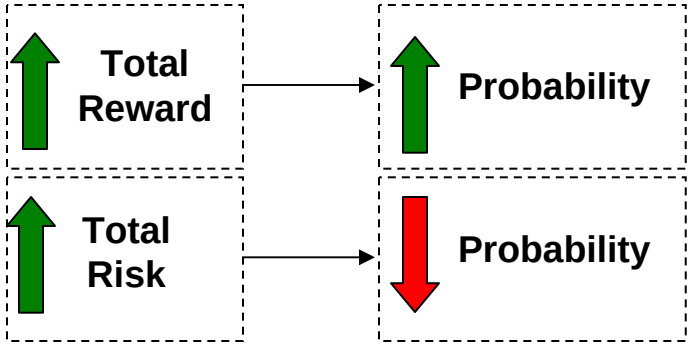
The "Law" of Malware Probability

- When you are dealing with an intelligent opponent and quantifiable gains (reward) and losses (risks), you can apply Game Theory

- You can determine to some level of accuracy the relative probability of a set of attack types with respect to one another

- You can use this information to implement stronger controls against a dynamic and increasingly hostile threat environment

- You can use this outlook to examine the effects of world events and small changes in "State of the Art" or even the introduction of disruptive technologies



Therefore

$$\text{Probability} \propto \frac{\text{Total Reward}}{\text{Total Risk}}$$

Or…

$$P_V \propto \frac{A_V}{D_V * R_V}$$

RSA
The Security Division of EMC

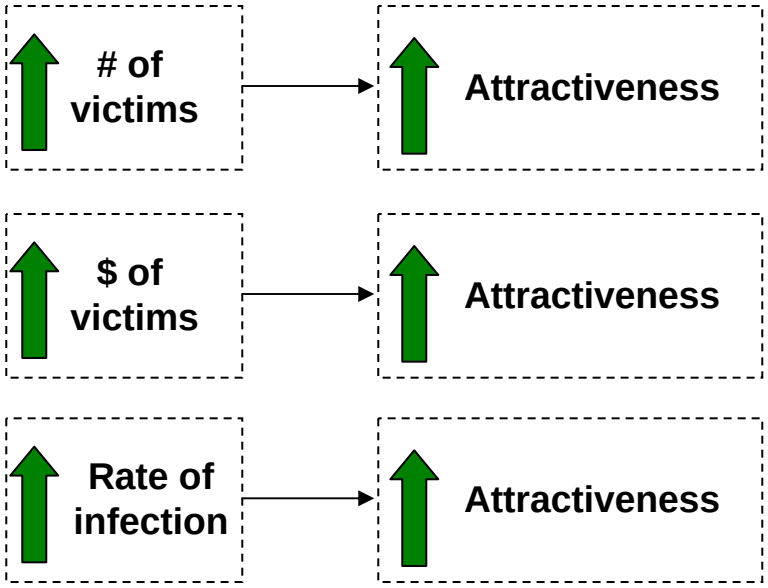
Target's Attractiveness

- Attractiveness is related to several factors
  - Number of victims (unit-less)
    i.e. more victims is more attractive
  - Yield: effectiveness of cash out mechanism
  - Value per victim
    i.e. more money per victim is more attractive
  - Rate of infection among victims (this can be measured with a cash analog or as a weighting factor such as "0.3" for a low rate or "1.0" for a high rate)
    i.e. Cash is King – getting to the victim means getting to the case faster

- Maturity of cash out mechanism is an important factor – related to the criminal "networks" sophistication

Note: for mathematical simplicity, everything should be measured in a currency (e.g. $ € £ ¥ etc.) – this also has interesting implications on a geographic basis, especially with cost (q.v.)

$$P_V \propto \frac{A_V}{D_V * R_V}$$



$$A_V \propto \#_V * Y_V * V_V * R_V$$

Difficulty (raw cost) of a Vector

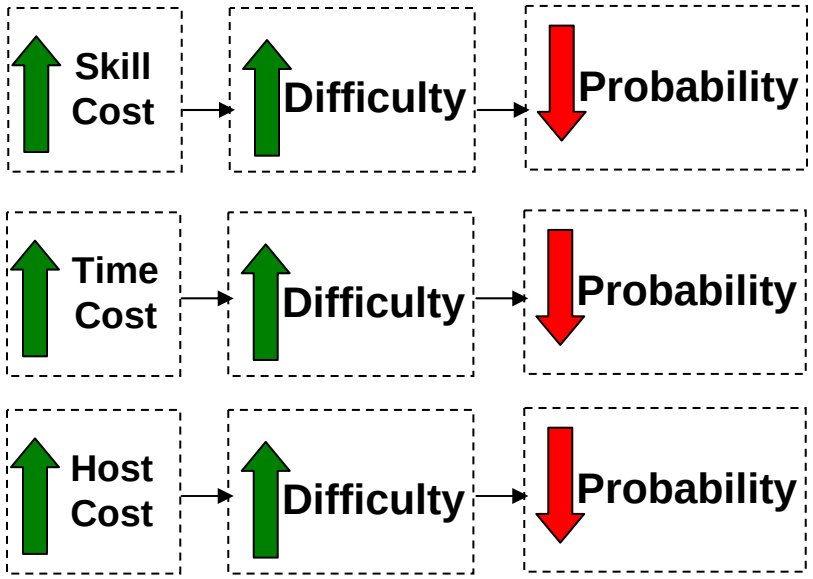
- Attractiveness is related to several factors
  - Scarcity of Skill set
    i.e. Finding and hiring specialists is expensive – that's bad!
  - Yield (effectiveness of Antivirus)
  - Time to execute matters – that costs
    i.e. Cash is King! Fast exploits to build mean $$$
  - Cost to "host" or execute (e.g. hardware)
    i.e. A legacy infrastructure or exploiting others's resources is good!

- Over time cost always comes down!

- Breakthrough technologies, improvements in infrastructure (especially in the developing world) regional or global advances in programming, increases in a populations skill sets make a big difference, bringing down cost…

Note: for mathematical simplicity, everything should be measured in a currency (e.g. $ € £ ¥ etc.) – this also has interesting implications on a geographic basis, especially with cost (q.v.)

$$P_V \propto \frac{A_V}{D_V * R_V}$$



$$D_V \propto S_V * Y_V * T_V * H_V$$

“Risk” to the Attacker

- Attractiveness is related to several factors
  - Penalty
    i.e. Severe penalties drive down the chance of any vector being used (compare physical robbery with online for instance)
  - Chance of being caught
    i.e. If penalties have a chance of being enforced, they are more effective

- This is where careful collaboration and international efforts can bear fruit

- Crime is fluid and will move to the “best reward for least risk” – meaning no measure will “solve” the attack problem…it will merely move it elsewhere

Note: for mathematical simplicity, everything should be measured in a currency (e.g. $ € £ ¥ etc.) – this also has interesting implications on a geographic basis, especially with cost (q.v.)

$$P_V \propto \frac{A_V}{D_V * R_V}$$

$$R_V \propto P_V * \%C_V$$

RSA
The Security Division of EMC

Example of a Comparison

Formula Factors⇒	V	N	I	D	E	T	L	P	ρ
Cyber CrimeTypes ⇓									
Wireless Malware	3	6	4	6	5	6	2	5	0.42
PC Malware (Low)	5	7	5	3	4	4	2	5	1.59
Spam	1	7	1	1	3	3	1	5	0.20
Phishing	5	7	5	6	5	6	1	5	2.06
Mail Fraud	2	7	1	1	3	3	7	8	0.04

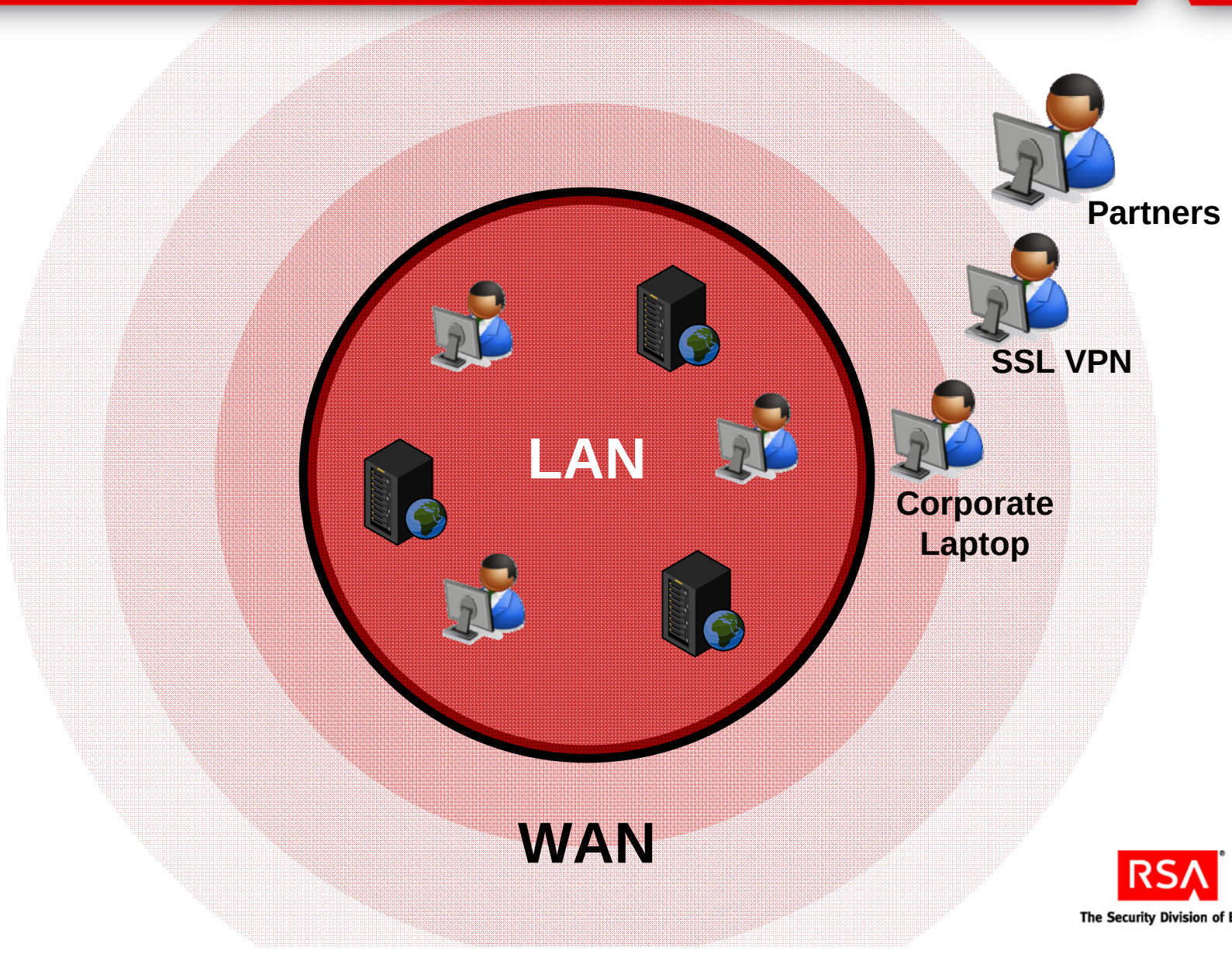
Introduction

Game Theory and Cybercrime

Enterprise Impact

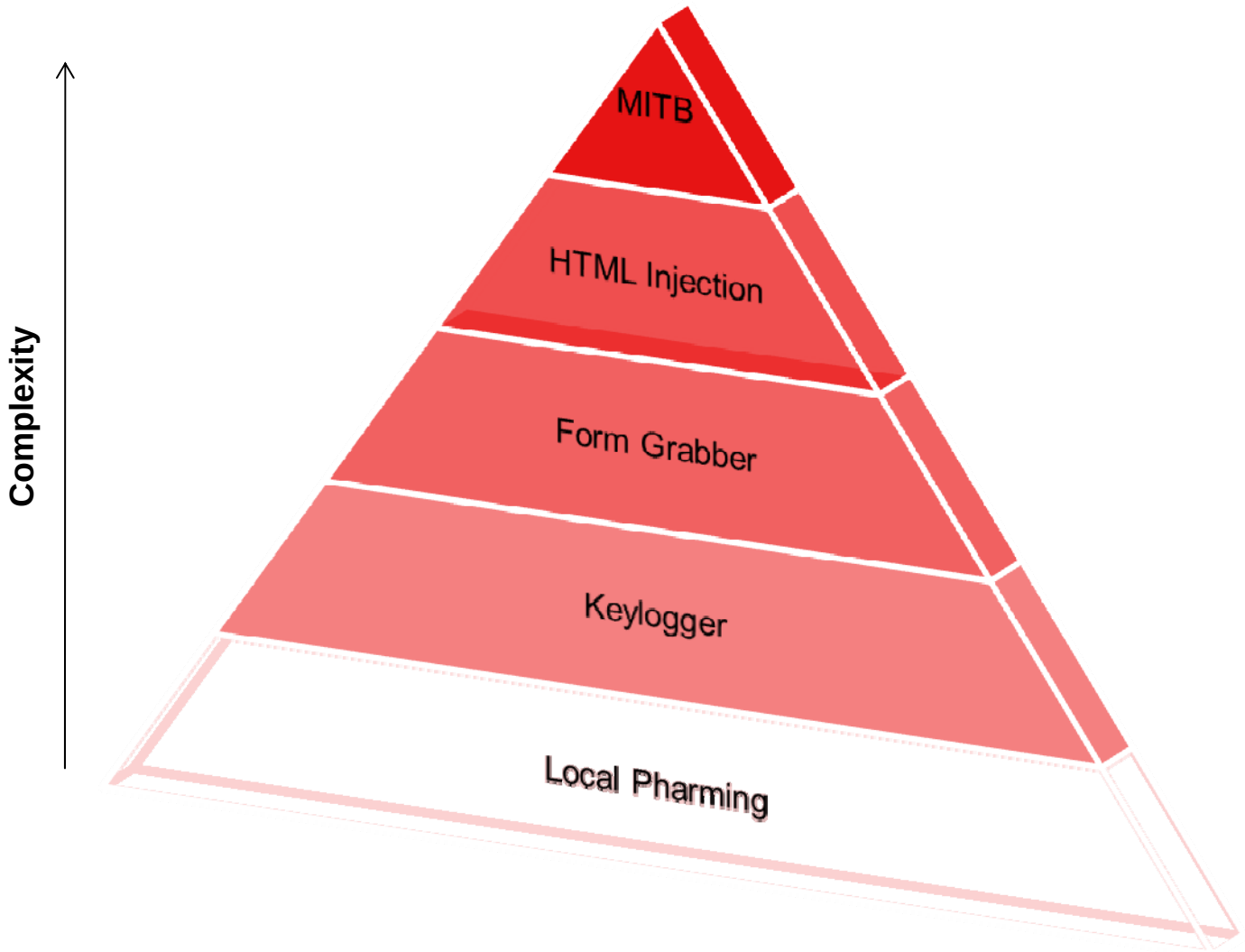
Conclusions

Sphere of Security Awareness



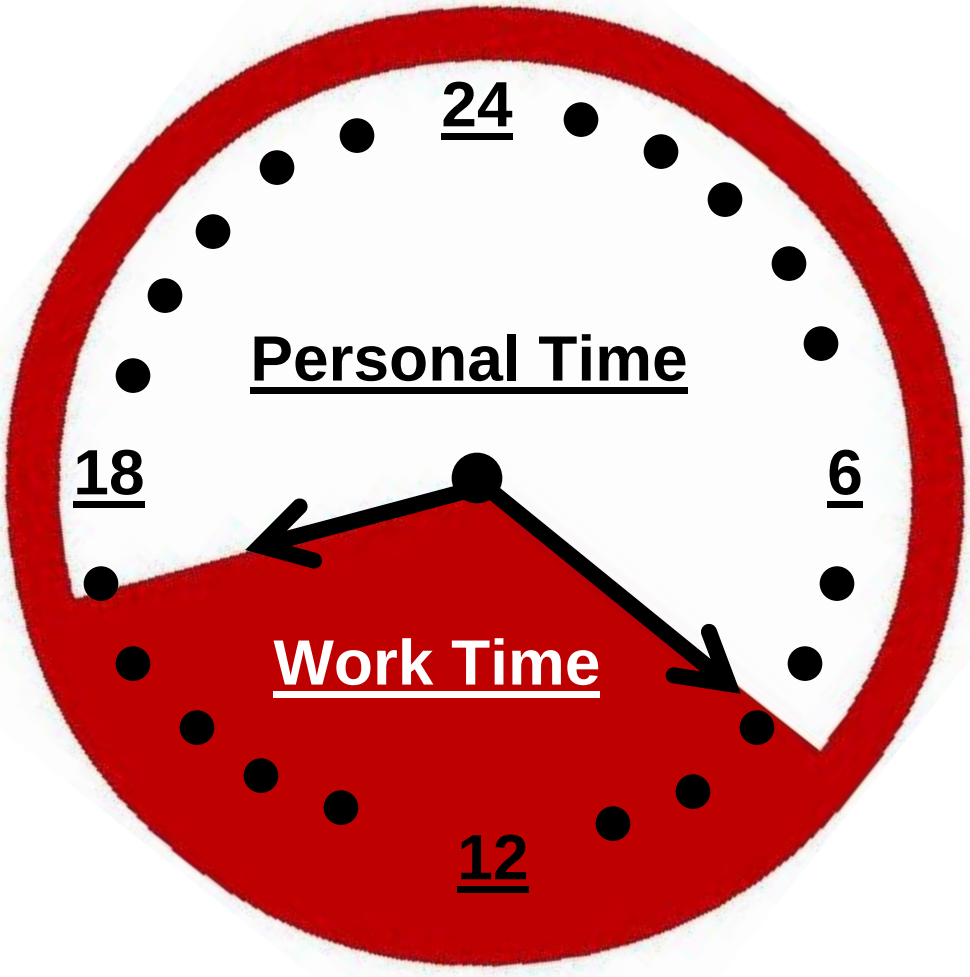
RSA
The Security Division of EMC

Trojan Progression



The 24-Hour Computer

Employee personal time with corporate resources is 2/3 of the day

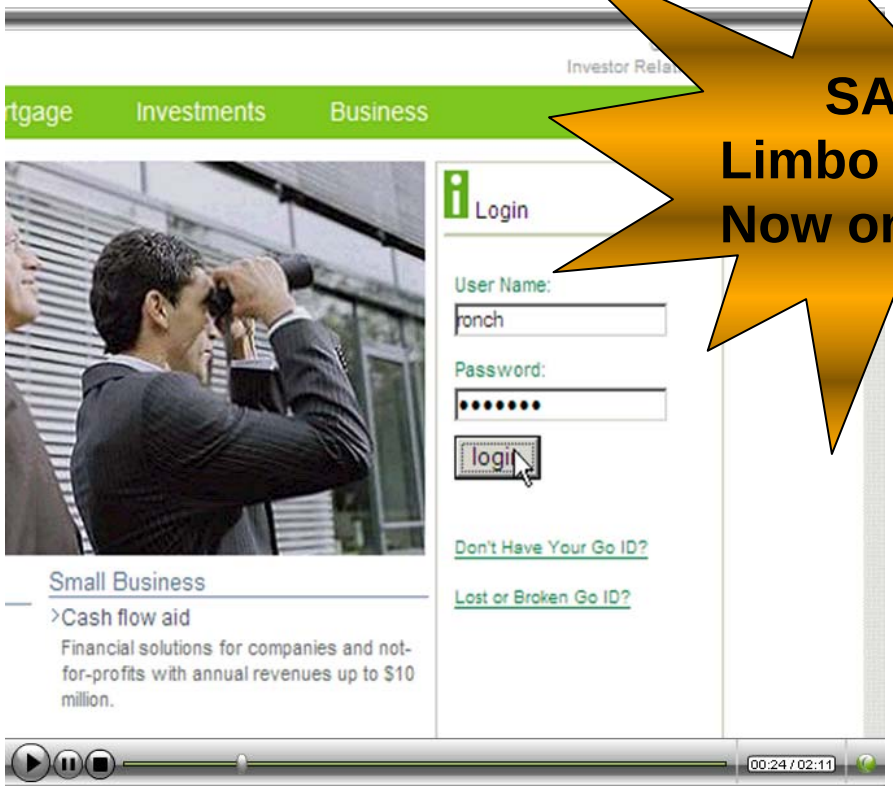


RSA
The Security Division of EMC

A Basic Trojan Attack

Username / Password Stolen

HTML Injection Trojan



SALE!
Limbo Trojan:
Now only $350

RSA
The Security Division of EMC

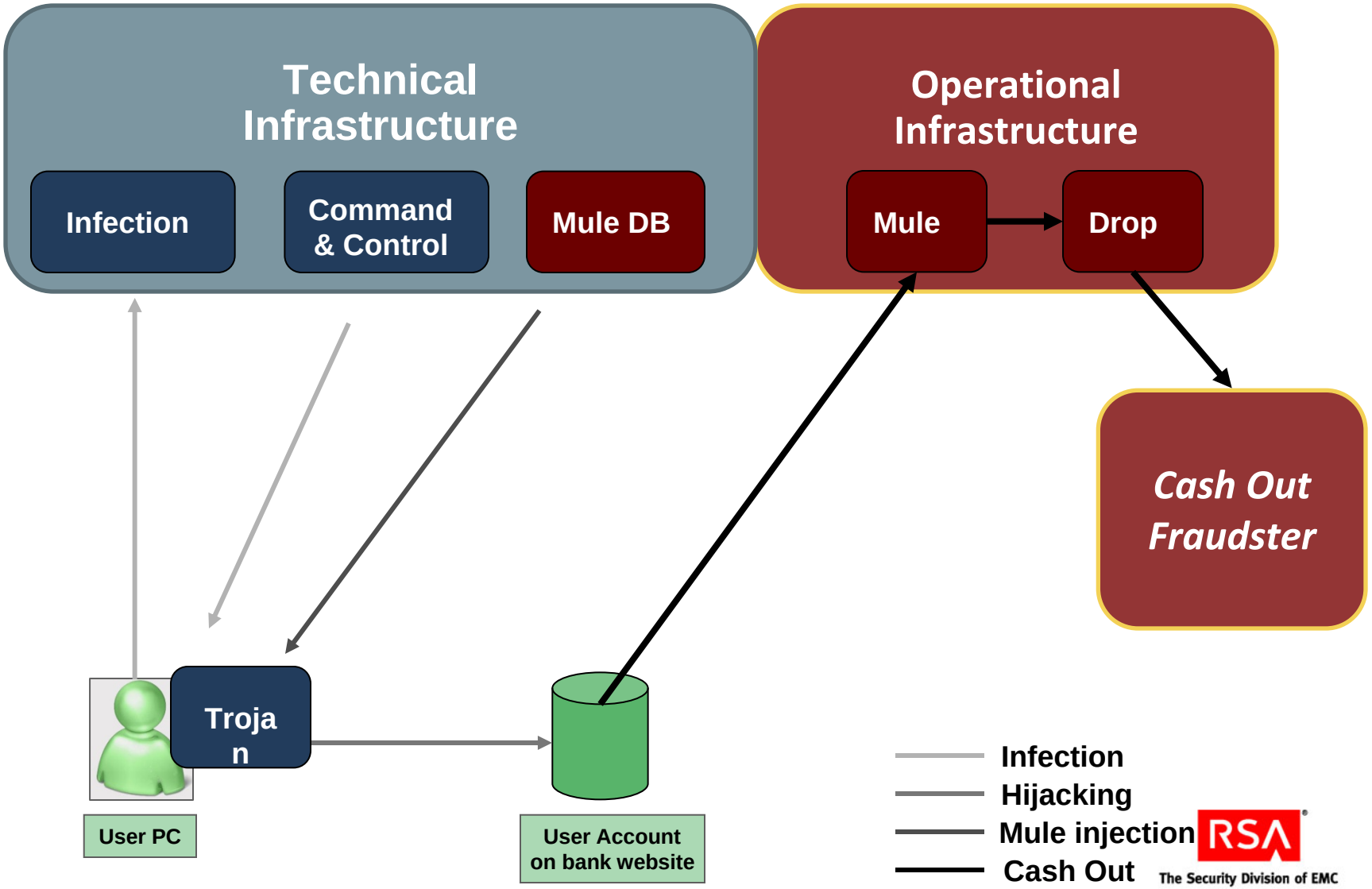
Man-in-the-Browser Trojans

1. A consumer gets infected with a Trojan, capable of MITB attacks
2. During online banking transaction the Trojan is triggered into action
3. The consumer passes login authentication stages
4. Trojan hijacks session
5. Trojan retrieves mule, triggers money transfer invisible to user
6. In some cases, using social engineering, user tricked to provide any 2-factor / transaction signing information needed

Mule Account 72345 in Bank C

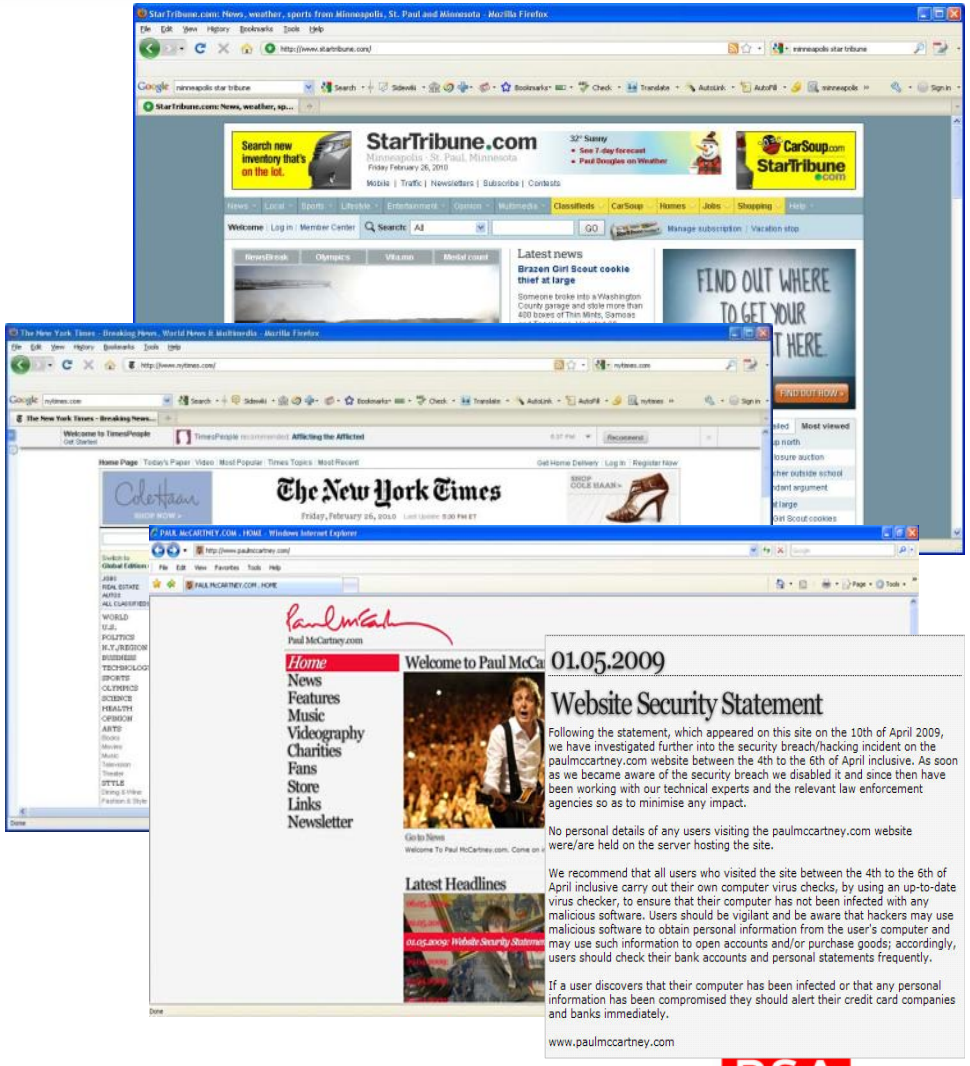
RSA
The Security Division of EMC

Fraud Supply Chain for MITB



The Challenge with Employee Behaviors

- Bad things can occur outside of the usual suspects (porn, gambling, pharma, etc.)
  - NY Times
  - Minneapolis Star Tribune
  - paulmccartney.com



RSA
The Security Division of EMC

The Theft of Corporate Information

==========

Timestamp:26.08.20** 19:07:02

[https://crm.emc.com/OA_HTML/AppsLocalLogin.jsp?requestUrl=APPSHOMEPAGE

username=KEYLOGGED:<EMC-ID> KEYSREAD:<EMC-ID>

[https://crm.emc.com/OA_HTML/fndvald.jsp]

Login

username=<EMC-ID>

password=xxxxxxx

langCode=US

requestUrl=APPSHOMEPA

[https://crm.emc.com/OA_HTML/OA.jsp?page=/oracle/a

bui/TcActivitiesPG%26_ri=809%26retainAM=Y%26Actio

A265N1display=KEYLOGGED:v KEYSREAD:P

[https://crm.emc.com/OA_HTML/OA.jsp?page=/oracle/apps/hxc/selfservice/timecard/we

bui/TcActivitiesPG%26_ri=809%26retainAM=Y%26Action=Update%26Timecard_id=29$

Time Entry: <First Name>, <Last Name>, <EMC-ID>

==========

EMC Data

Corporate data Can & Is captured in Trojan log files

RSA

The Security Division of EMC

The Infection of Corporate Resources

Infected resources identifiable by captured information

Trojan Family: Zeus (version 2)
MD5: 4b19e74a48b73345abf32f17fbd12a2e
https://www.google.com/accounts/ServiceLoginAuth?service=orkut
time_system: 7/1[redacted] PM
ipv4: *.33.49.251**
country: US

RSA
The Security Division of EMC

The Infection of Corporate Resources

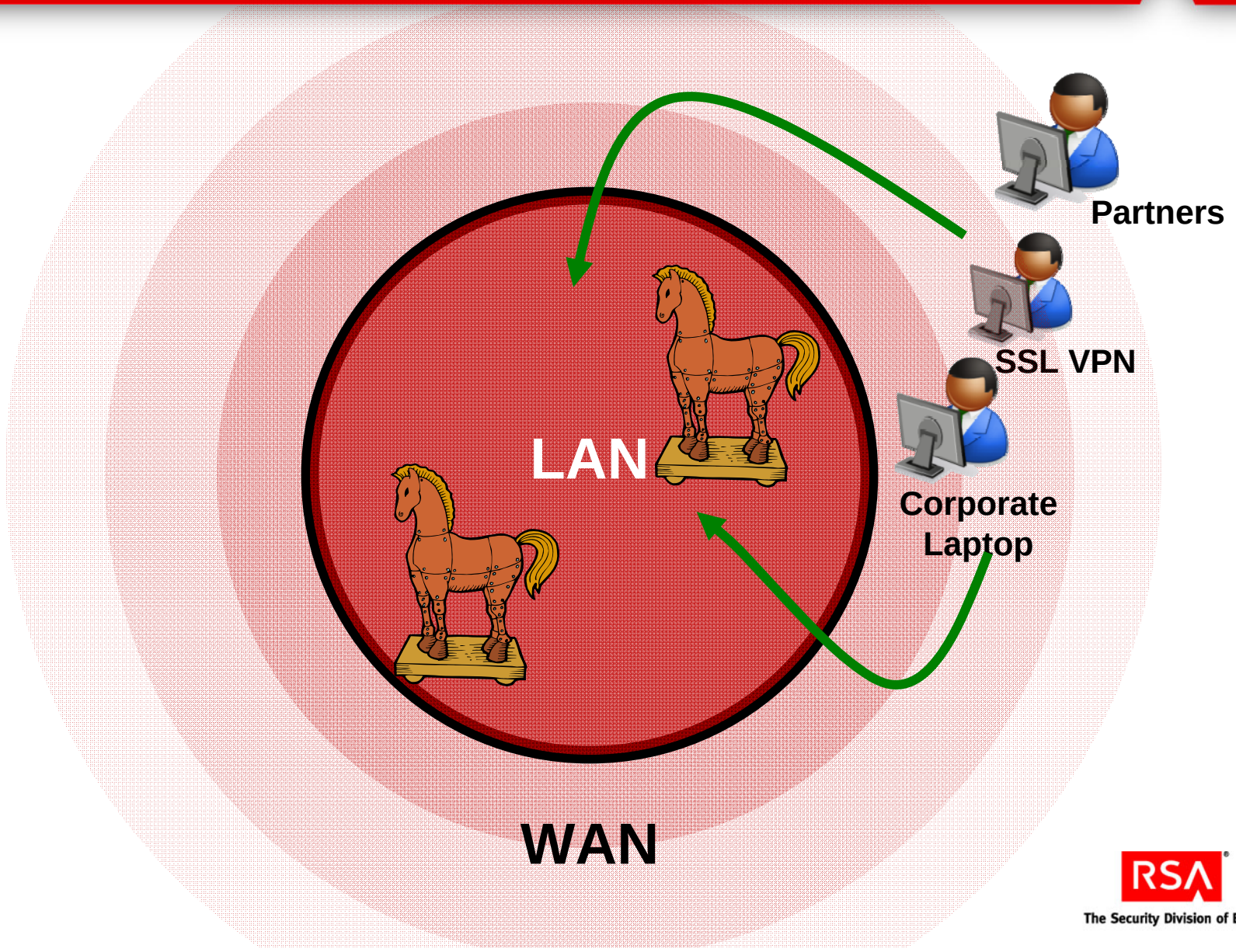
```
OrgName:
OrgID:
Address:      3039 Cornwallis Road
City:         Research Triangle Park
StateProv:    NC
PostalCode:   27709-2195
Country:      US

NetRange:     [redacted].33.0.0 - [redacted].33.255.255
CIDR:         [redacted].33.0.0/16
NetName:      NET-9-0-0-0-1
NetHandle:    NET-129-33-0-0-1
Parent:       NET-129-0-0-0-0
NetType:      Direct Assignment
NameServer:   RTPUSSXDNSB03.RALEIGH.MEBS[redacted].COM
NameServer:   RTPUSSXDNSB04.RALEIGH.MEBS[redacted].COM
NameServer:   BLDUSWXDNSB01.BOULDER.MEBS[redacted].COM
NameServer:   BLDUSWXDNSB02.BOULDER.MEBS[redacted].COM
Comment:
RegDate:      1989-06-22
Updated:      2006-09-27

RAbuseHandle: ORGAB-ARIN
RAbuseName:   Org Abuse
RAbusePhone:  +1-630-568-[redacted]
RAbuseEmail:  [redacted]

OrgTechHandle: RAIN-ARIN
OrgTechName:   Registrar Authority, Internet numbers
OrgTechPhone:  +1-800-426-[redacted]
OrgTechEmail:  [redacted]
```

*****.33.49.251**

This is an infected machine located at a Fortune 100

RSA
The Security Division of EMC

External Corruption of Internal Resources



RSA
The Security Division of EMC

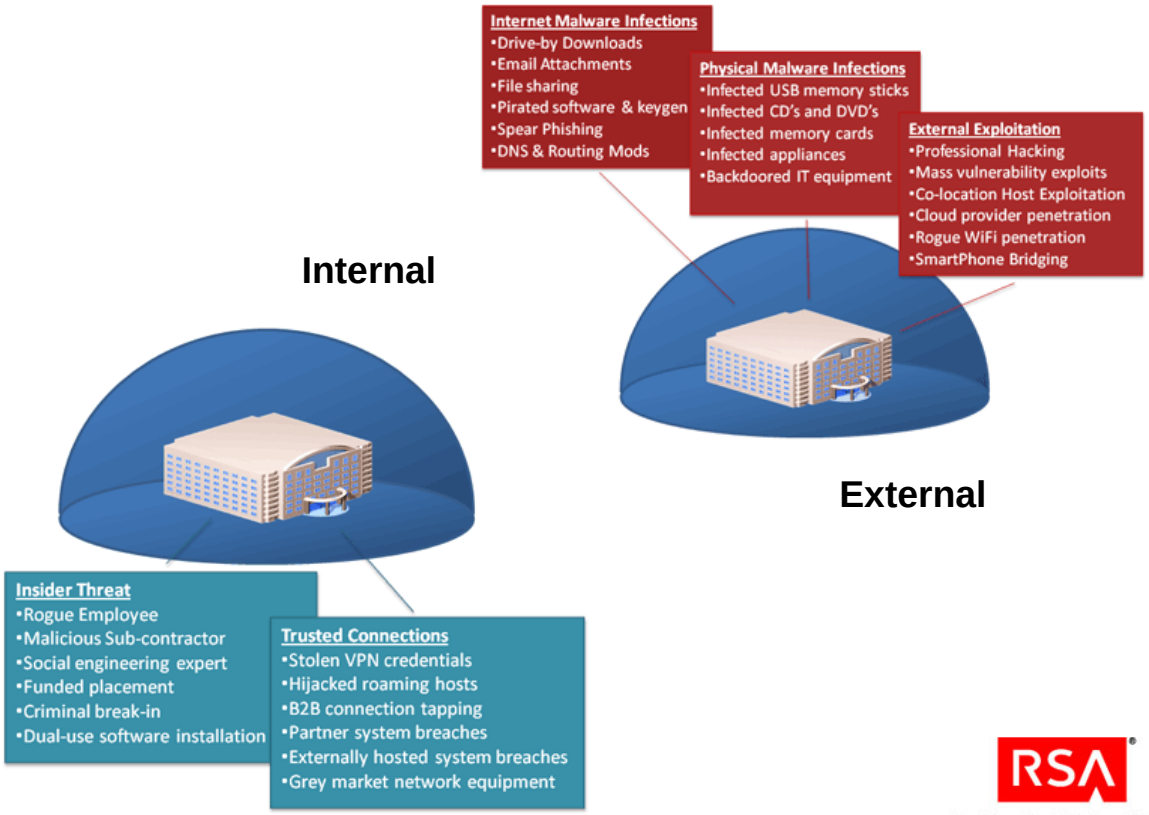
Crimeware in the Enterprise- Infection

RSA
The Security Division of EMC

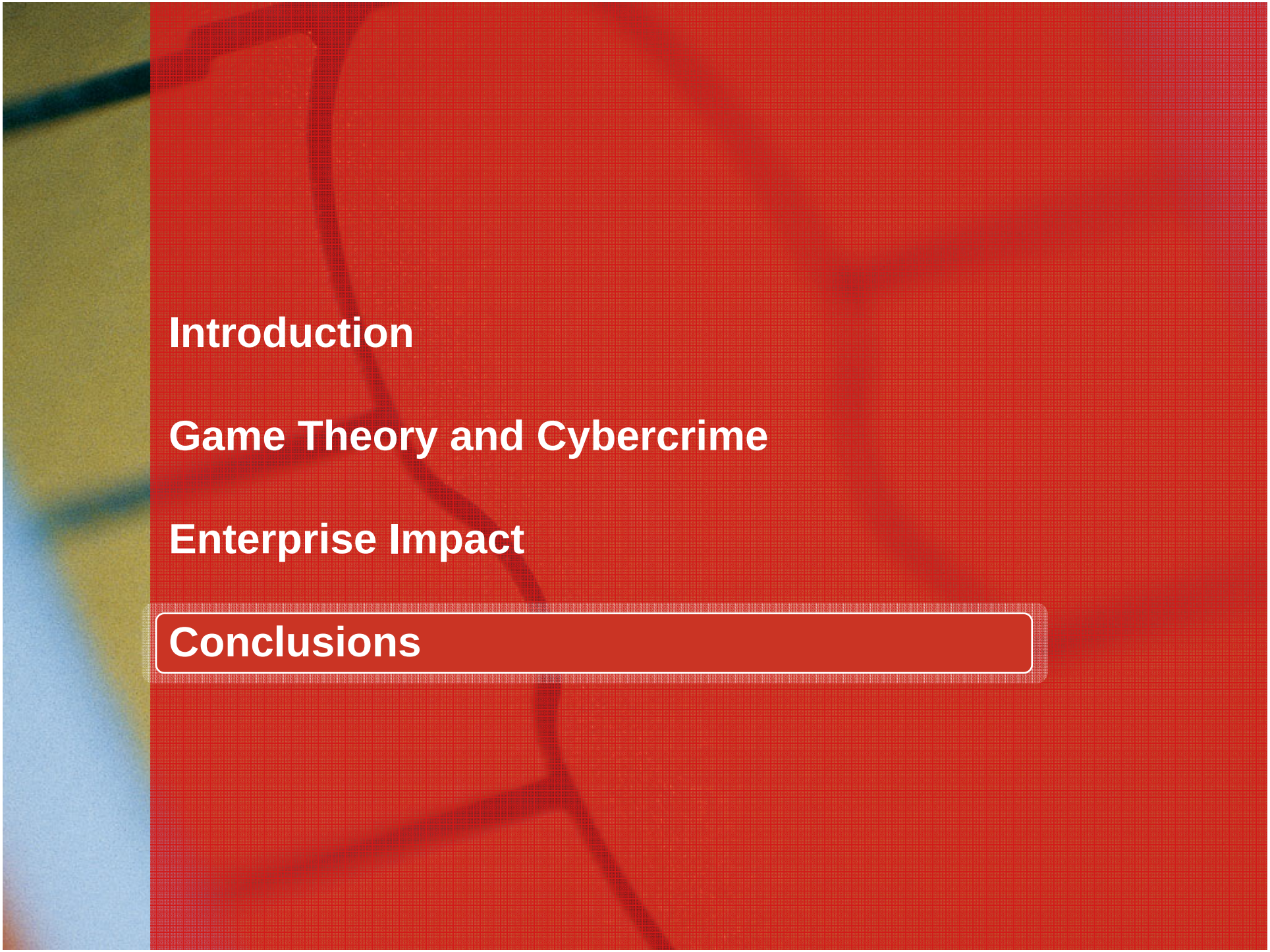
Advanced Persistent Threats (APTs)

- New generation of cyber threats
- Leverage a high degree of stealthiness over a prolonged duration
- Attack objectives typically extend beyond immediate financial gain
- Compromised systems continue to be of service even after key systems have been breached and initial goals reached

- Utilizes the full spectrum of computer intrusion technologies and techniques
- Combines multiple attack methodologies and tools in order to reach and compromise their target
- Requires a holistic view of environment to detect and defeat



RSA
The Security Division of EMC


Introduction
Game Theory and Cybercrime
Enterprise Impact
Conclusions

Perimeter v. Information (transaction) centric

- The perimeter is going away
  - We all know it and have heard it
  - We all sense there's something right about this
- It's better to say that it's shrinking
- Ultimately, it's about the data

Truth: you should be perimeter aware and information and transaction centric

http://www.primrosecottageholidays.co.uk/custom/kent_dover_castle.jpg

Attack Focus v. Context

- So you want to commit a murder…
  - Locard's principle: there is always an exchange of physical evidence between the criminal and the scene (this is why we have CSI labs)
  - You have two options
    - Clean up all traces (duck tape / spandex / etc.)
    - Spread around a lot of false trace
- The Internet is seeing a huge amount of "noise"
  - Background noise covers tracks
  - Don't focus on the attacks

Some personal items of Mr Sherlock Holmes

Truth: Focus on the context of events and intelligence

Static v. Dynamic

- There is an intelligent opponent
- Therefore, if you build a wall, the opponent will…
  - Go around it
  - Go over it
  - Go under it
- The right way to deal with the situation is to build walls (don't let anyone tell you that's a bad idea)
- It's a bad idea to rely on the wall as the primary means of defense

Truth: rely on dynamic, adapting technologies and seek architectural breakthroughs (whose boundaries you know)

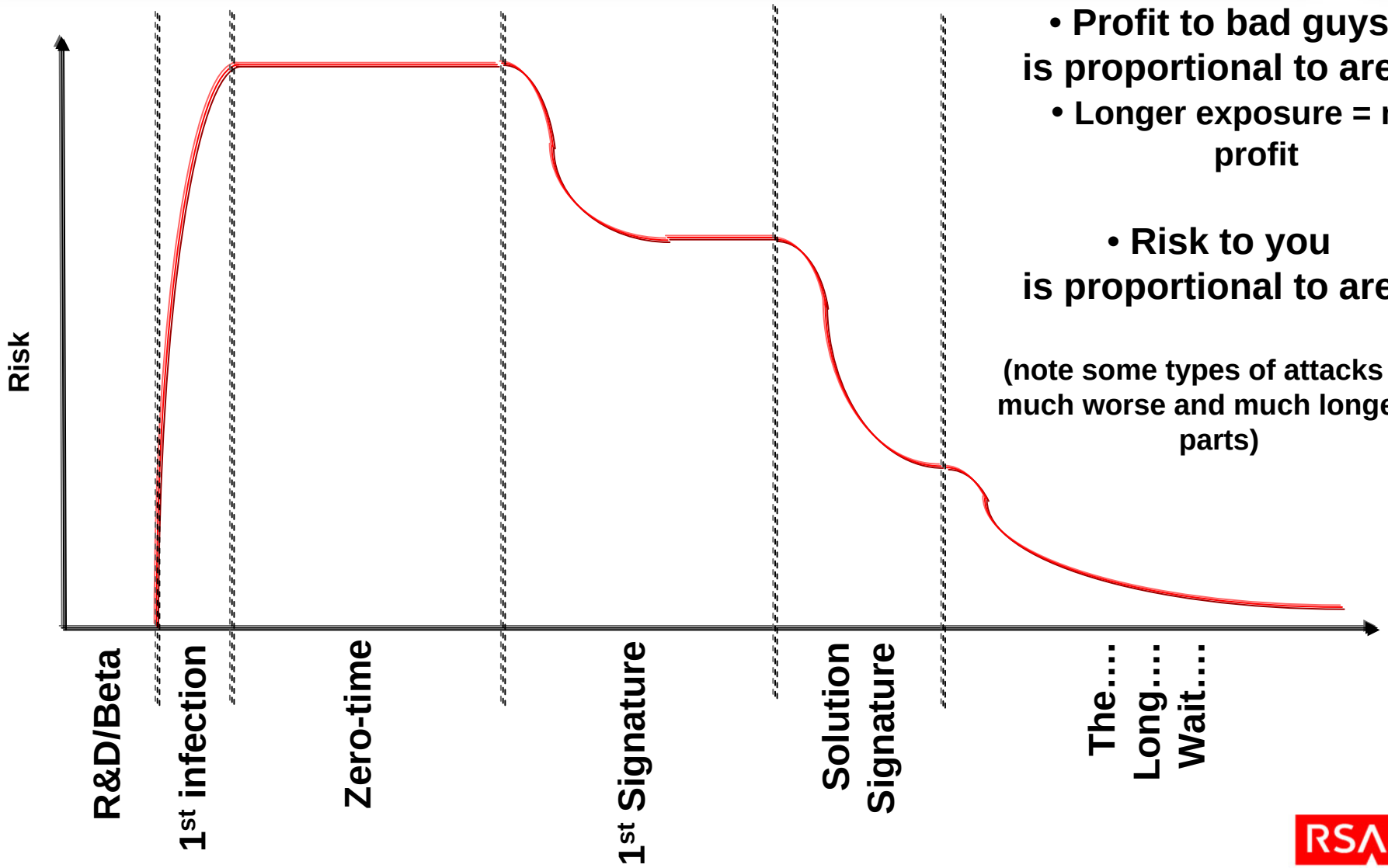
Update Dependent v. Self-Learning

- There is nothing to be ashamed of in a content race
- We still need updates
- All breakthroughs will wind up in a race
- However, systems that can learn how to run the race better are the best solution

Truth: focus on self-learning and greater intelligence in your breakthroughs instead of relying on the content updates

RSA
The Security Division of EMC

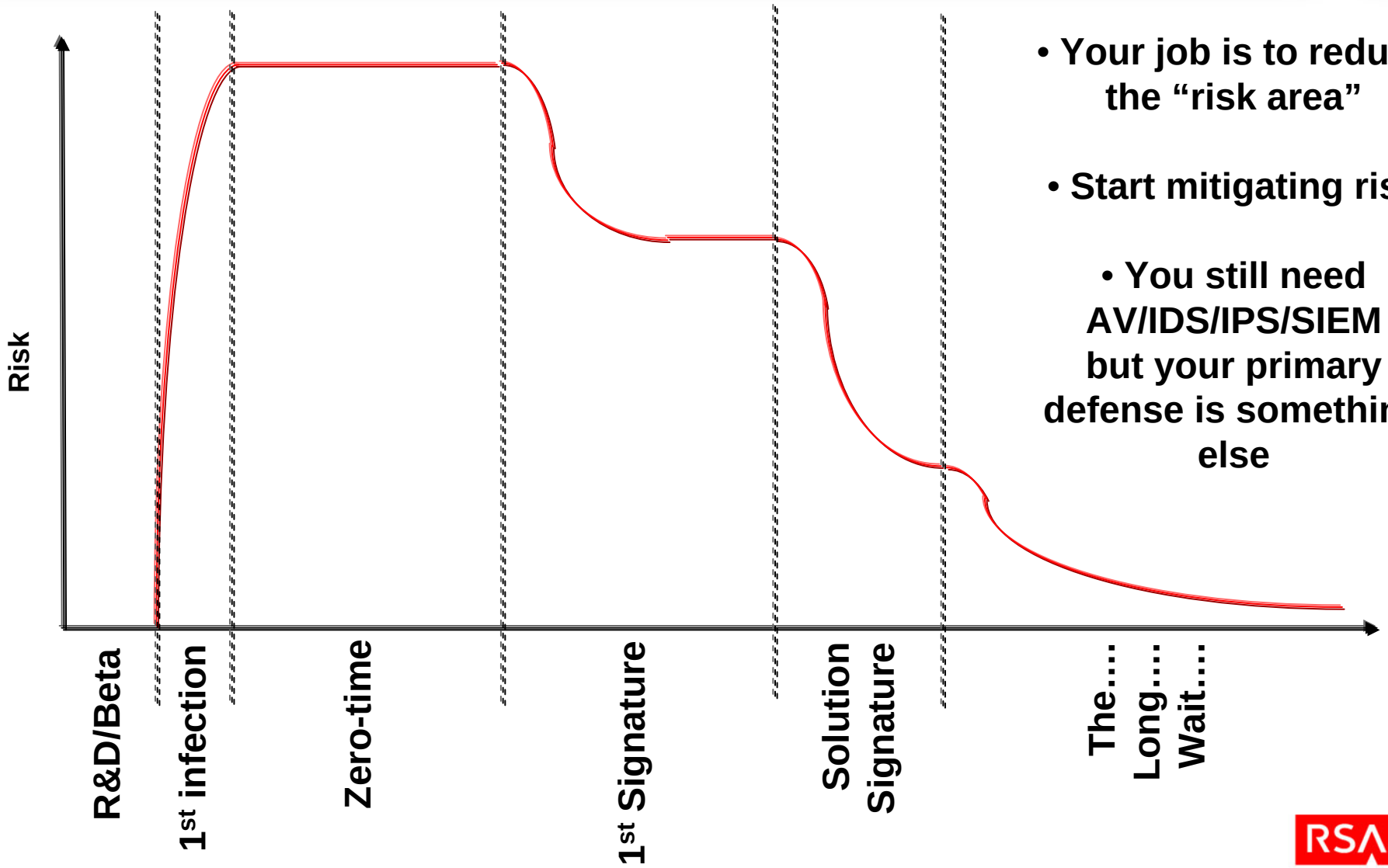
What Does the Risk Curve Look Like?



- **Profit to bad guys is proportional to area**
  - **Longer exposure = more profit**
- **Risk to you is proportional to area**

(note some types of attacks are much worse and much longer in parts)

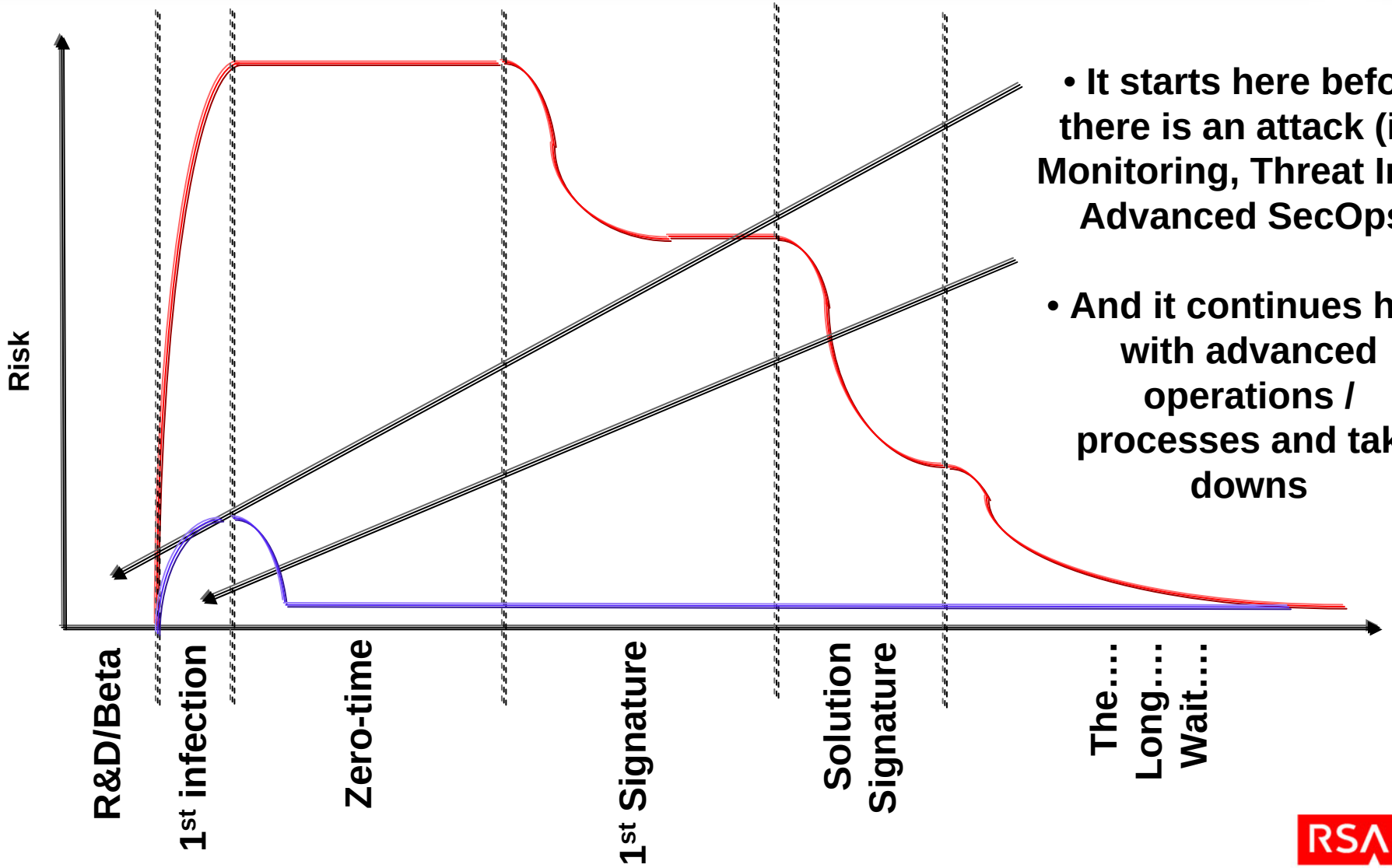
What Should Security Do in this Case?



- **Your job is to reduce the "risk area"**
- **Start mitigating risk**
- **You still need AV/IDS/IPS/SIEM but your primary defense is something else**

Standards Security Controls Are Only Partially Effective

How Do You Change the Risk Curve?



- **It starts here before there is an attack (i.e. Monitoring, Threat Intel, Advanced SecOps)**
- **And it continues here with advanced operations / processes and take downs**

A Note on Offensive Strategies

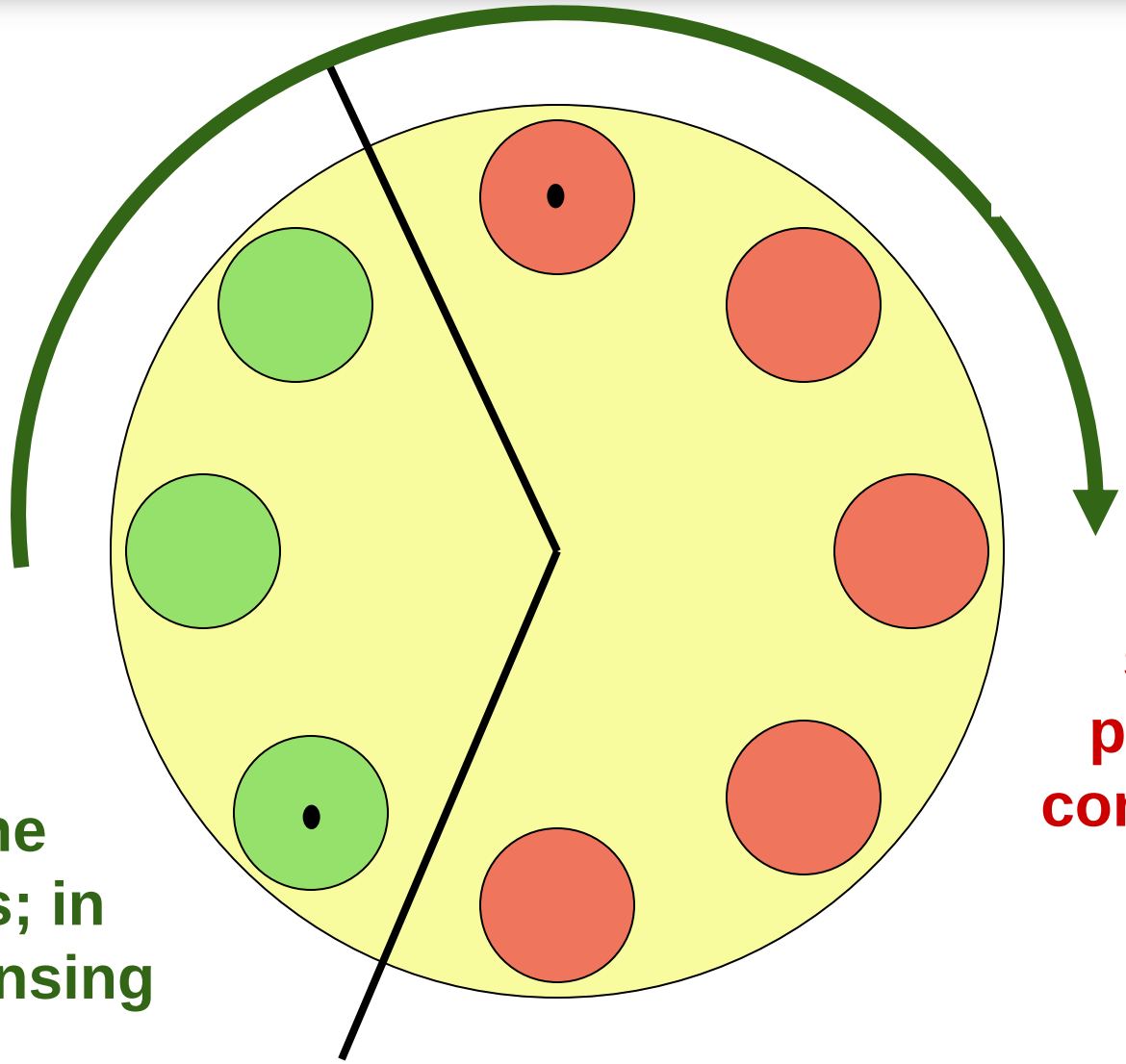
- Offense is not a very effective strategy
  - Enemy is too distributed and difficult to identify
  - They leverage 'innocent bystander' resources
    - e.g. compromised hosts in botnet
  - Huge potential for collateral damage
- Limited offense is possible
  - Identify servers/sites and work with local LEOs to shut them down
  - Identify attackers and work with LEOs to arrest/convict
  - Still a reactive offense (offensive defense?)
  - Difficult to get inside your opponents decision cycle
- Strategic defense, tactical offense

Changing the Game
Self-Cleansing Intrusion Tolerance (SCIT)

- SCIT focuses on minimizing the exposure window of an attack
  - Shorter exposure = minimal potential damage
- Leverages virtualization technology to rotate servers to a known good state at regular intervals
  - Any infections are cleansed at each rotation
- Supports session persistence but does not migrate state
  - Applicable for web servers, DNS servers, SSO, database, etc.
- Started as a research project at George Mason University
  - Tested & deployed by Lockheed Martin, Northrop Grumman, Raytheon

SCIT in Action

Servers
-Virtual
-Physical

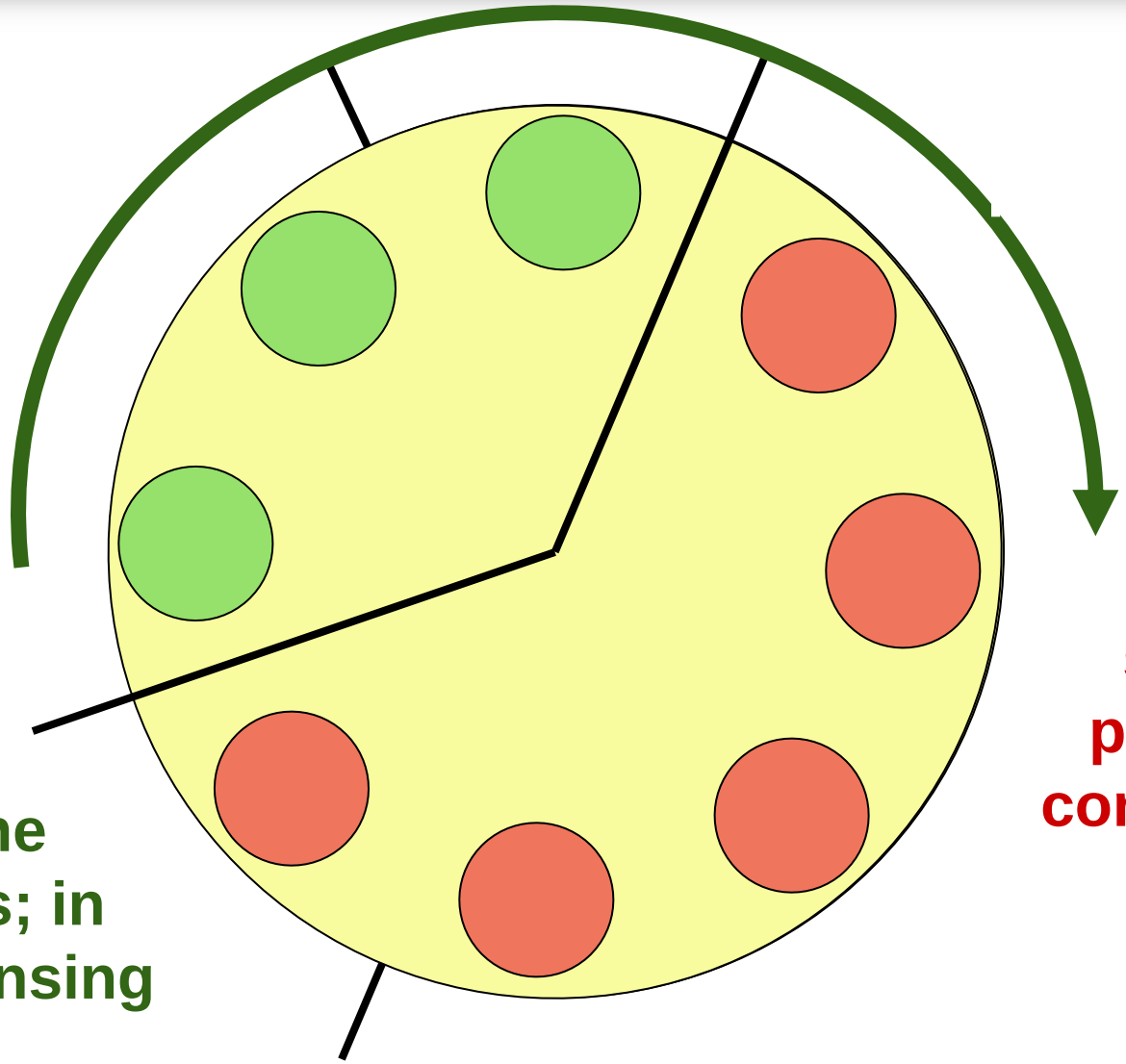


Online servers; potentially compromised

Offline servers; in self-cleansing

SCIT in Action

Servers
-Virtual
-Physical

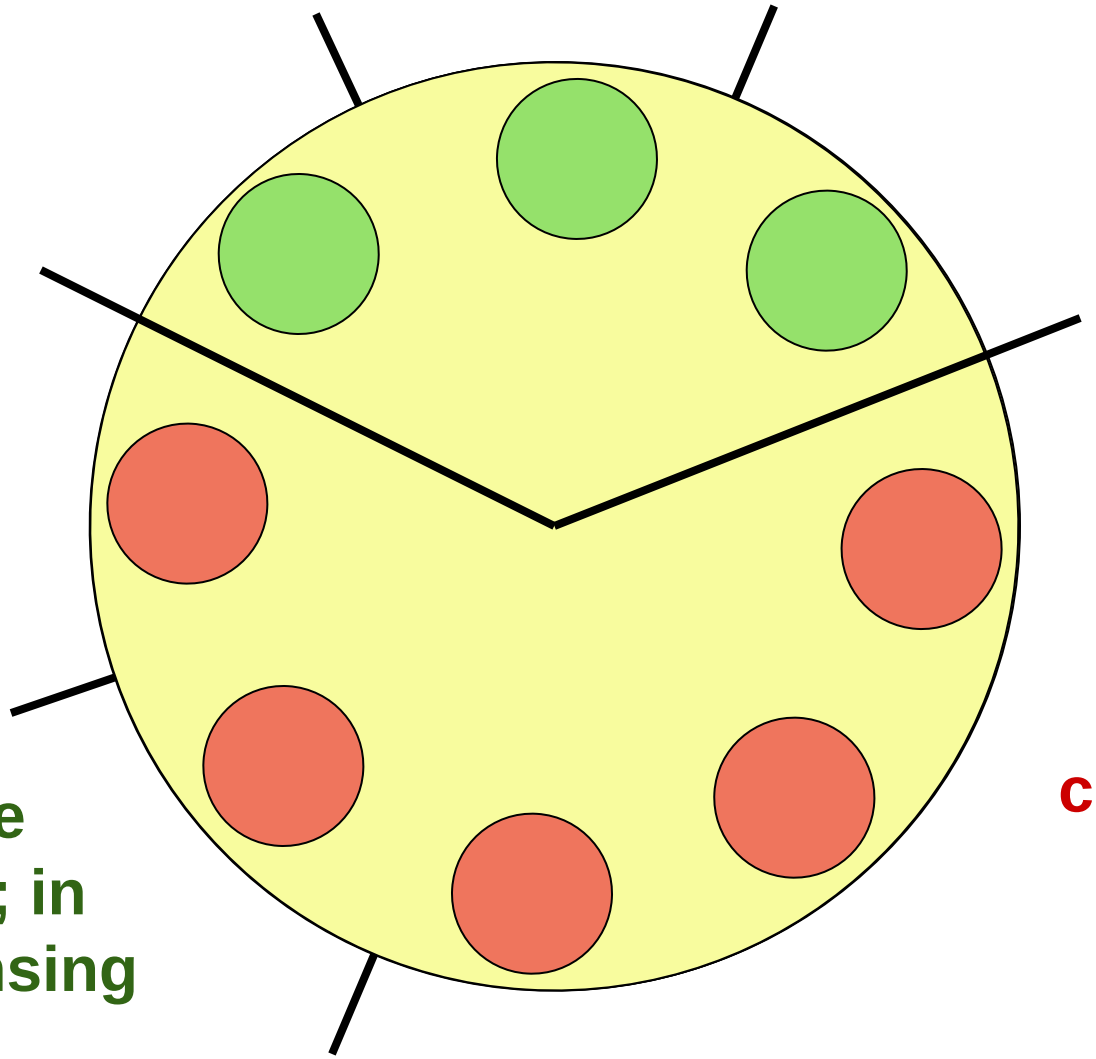


Online servers; potentially compromised

Offline servers; in self-cleansing

SCIT in Action

Servers
-Virtual
-Physical



Online servers; potentially compromised

Offline servers; in self-cleansing

Wrap-up

- The basics
  - There is nothing special about the malware with “APTs” – it’s about the people and economics
  - The bad guys generally are out to make money – profit!
  - The “greatest reaction mass” is in the private sector
  - There is a “Consumerization of IT” wave coming (more risk!)
- The bad guys will keep getting worse: we have an intelligent opponent!
  - Expect a bleed v. butcher approach in malware
  - Expect “benefits” to be introduced concurrent with malware
  - Expect the Dark Cloud to continue to flourish
- We can apply game theory to predict changes
- Enteprises can improve security with some simple principles, but ultimately we have to coordinate internationally and attack the criminals (i.e. the people) to slow down and to limit the expansion of malware!
- The Cloud…
  - The “bad guys” have no blocks to using cloud computing!
  - On the corporate side…
    - Expect SMBs to go to the Public Cloud first
    - Expect innovation to happen in Private / Hybrid Clouds
    - Expect large enterprises to reject the Public Cloud (require safety in the cloud)

The Security Division of EMC

Thank you!