Contaminação Epidêmica em Redes:

Imunidade Coletiva e Suas Implicações Frente a Atacantes Estratégicos

Vilc Rufino[1,2], Daniel Menasché[2], Ítalo Cunha[3], Cabral Lima[2], Leandro P. de Aguiar[4]

1 2 3 4

UFRJ

Motivação: prevalência de ataques cibernéticos

UOL notícias Tecnologia

ÚLTIMAS CIÊNCIA E SAÚDE ECONOMIA INTER JORNAIS POLÍTICA ELEIÇÕES 2018 UOL C

De olho na segurança

VEJA MAIS DICAS DICAS DE TECNOLOGIA UOL TESTA: CELULARES WHATSAPP

WannaCry: após um ano, ainda não brecaram o maior ciberataque da história COMENTE

Fabiana Uchinaka
Do UOL, em São Paulo 05/05/2018 | 14h13

Ouvir texto Imprimir Comunicar erro

05MAI2018
https://economia.uol.com.br/noticias/efe/2018/06/30/ransomware-torna-se-principal-ciberpesadelo-na-america-latina.htm

Maior cyberataque da história ainda não acabou.

Motivação: prevalência de ataques cibernéticos

threatpost Cloud Security / Malware / Vulnerabilities / Privacy

WannaCry Extortion Fraud Reemerges

Author:
Tara Seals
June 25, 2018 / 4:02 pm
2 minute read
Write a comment

The emails claim that all of the victim's devices have been hacked and infected with the infamous ransomware — and then ask for Bitcoin to "fix" it.

25JUN2018
https://threatpost.com/wannacry-extortion-fraud-reemerges/133062/

Ressurge a ameaça *WannaCry*.

Motivação: prevalência de ataques cibernéticos

UOL economia

ÚLTIMAS | COTAÇÕES | FINANÇAS | EMPREENDEDORISMO | EMPREGOS | IMPOSTO DE RENDA

BOLSAS BOVESPA +1,4% 78.571,29 pts | CÂMBIO DÓLAR COM -1,84% R$ 3,774 | PESO ARG -1,08%

Ransomware torna-se principal "ciberpesadelo" na América Latina

COMENTE

EFE

30/06/2018 | 10h48

Ouvir texto | Imprimir | Comunicar erro

Alejandro Rincón Moreno.

Bogotá, 30 jun (EFE).- O vírus WannaCry conseguiu o que queria: o ransomware, como é conhecido o sequestro de dados, já é a principal causa de "ciberterror" entre as empresas latino-americanas, que dizem temer cada vez menos os vírus informáticos tradicionais.

30JUN2018
https://economia.uol.com.br/noticias/efe/2018/06/30/ransomware-torna-se-principal-ciberpesadelo-na-america-latina.htm

Malware que sequestra dados afeta economia, e já é a principal causa de **cyberterrorismo**.

Motivação: prevalência de ataques cibernéticos

Maior ransomware da história, WannaCry completa 1 ano

Da Redação Siga @idgnow 11/05/2018 - 18h39

Flip Imprima

Companhias atingidas tiveram de parar operações, como foi o caso de montadoras e hospitais; Empresas e órgãos públicos no Brasil também foram afetados

Na sexta-feira, 12 de maio de 2017, a comunidade global testemunhou o início da maior infecção de ransomware da história. Este ataque conseguiu afetar mais de 200 mil sistemas em 150 países. A montadora Renault teve de fechar sua maior fábrica na França e os hospitais do Reino Unido tiveram que rejeitar pacientes. Já no Brasil, o ataque causou a interrupção do

ÚLTIMAS NOTÍCIAS

- Novo recurso do WhatsApp alerta usuários sobre links suspeitos
- O que esperar do próximo Android P, segundo o próprio Google
- Como deletar o histórico de séries e filmes assistidos na Netflix
- Nasa pode montar base na Lua para astronautas na próxima década
- Google fecha acordo para oferecer Internet no Quênia com balões
- 10 habilidades que todo profissional de TI precisa desenvolver

11MAI2018
http://idgnow.com.br/internet/2018/05/11/maior-ransomware-da-historia-wannacry-completa-1-ano/

11/maio/2018: um ano do ataque WannaCry, +200 mil computadores atingidos, 150 países.

Motivação: prevalência de ataques cibernéticos

BUSCAR

tecmundo

NOTÍCIAS COMPARAR CELULARES VOXEL TECMUNDO TV CUPONS DE DESC

No final do ano passado, quase um milhão de usuários da web ficaram sem conexão na Alemanha por conta de um ataque da botnet Mirai. E a ameaça, baseada na Internet das Coisas, volta ainda mais poderosa nesta temporada: seus operadores conseguiram recrutar silenciosamente uma armada de 100 mil novos roteadores, que podem ser usados para uma ofensiva a qualquer momento.

"O malware consegue agir em ambientes bem protegidos e até com o gerenciamento remoto desligado"

Desde que o código da Mirai veio a público, as variantes vem apresentando poucas modificações e falhas amadoras. Contudo, desta vez é diferente. Essa versão pode tirar vantagem de uma brecha de segurança de dois aparelhos da Huwaei, o EchoLife Home Gateway e o Huwaei Home Gateway, amplamente utilizados em residências e pequenos escritórios. E o pior é que o malware consegue agir mesmo em ambientes protegidos por senhas complexas e com a administração remota completamente desligada.

05DEZ2017
https://www.tecmundo.com.br/seguranca/124921-botnet-mirai-atacar-100-mil-roteadores-qualquer-momento.htm

Malware que causou o maior ataque DDOS, afetou 1 milhão de usuários, em 2016 na Alemanha; ainda possui 100 mil bots.

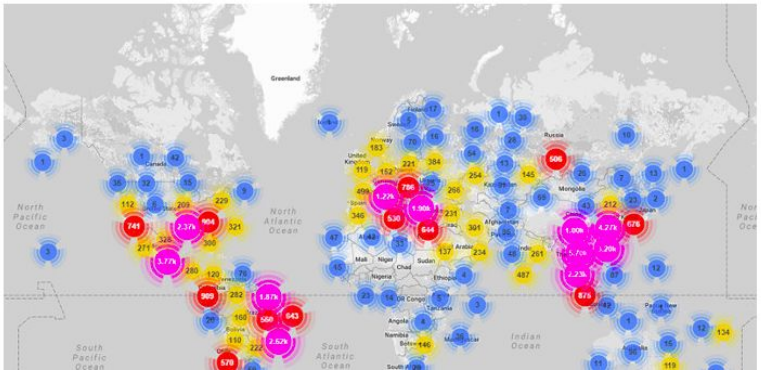
Motivação: prevalência de ataques cibernéticos

MENU G1 SEGURANÇA DIGITAL

Brasil é o 2º país mais contaminado por vírus que ataca câmeras

Números divulgados pela empresa de segurança Imperva apontam que o Brasil é um dos países mais atacados pelo vírus Mirai, que contamina câmeras de segurança IP e gravadores digitais de vídeo (DVRs). A Imperva estimou que 11,8% dos dispositivos infectados pelo vírus estão no Brasil, uma fatia só menor que a do Vietnã, que é de 12,8%. Os números foram publicados pela Imperva nesta segunda-feira (10).

O "top 5" também é composto pelos Estados Unidos (10,9%), China (8,8%) e México (8,4%). Pesquisadores estimam que o número total de países com infecções do Mirai passa de 160 e o número total de sistemas contaminados é de aproximadamente 150 mil.



12OUT2016
http://g1.globo.com/tecnologia/blog/seguranca-digital/post/brasil-e-o-2-pais-mais-contaminado-por-virus-que-ataca-cameras.html

Brasil revela uma cultura de insegurança, só não é pior que Vietnã.

Motivação: prevalência de ataques cibernéticos

SECURITY INFORMATION NEWS

O seu BLOG sobre noticias e dicas sobre Segurança da Informação

NOTICIAS

Malware do tipo Mirai atinge alvos brasileiros

21ABR2018
https://securityinformationnews.com/2018/04/21/malware-do-tipo-mirai-atinge-alvos-brasileiros/

Também somos vítimas.

Motivação: prevalência de ataques cibernéticos

TIME

These Are Some of the Devices Vulnerable to Mirai

By ALEX FITZPATRICK October 27, 2016

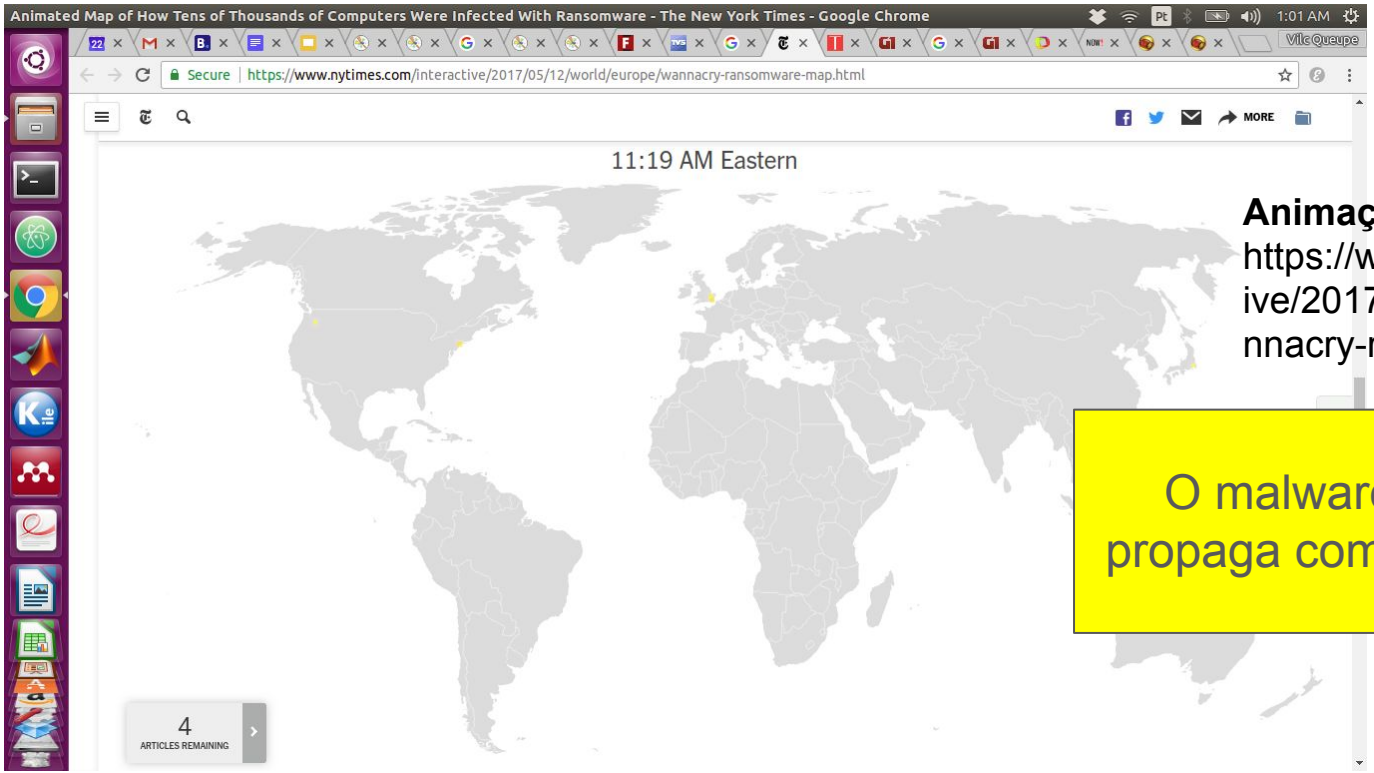
Internet users across the eastern seaboard found their connections interrupted Oct. 21 during a massive cyberattack. The attack was in part fueled by Mirai, a virus that gives hackers access to unsecured webcams and similar devices. (The hackers commandeer the devices and use them to send bogus traffic to a target server in hopes of overloading it and knocking it down.)

How can you tell if your gadgets are infected with Mirai? A good place to start is this list compiled by security researcher Brian Krebs, who analyzed Mirai's publicly available source code to see which devices it's been targeting.

27OUT2016
http://time.com/4543132/these-are-some-of-the-devices-vulnerable-to-mirai/

Até os mais fortes podem ser vítimas.
Quem são os próximos?

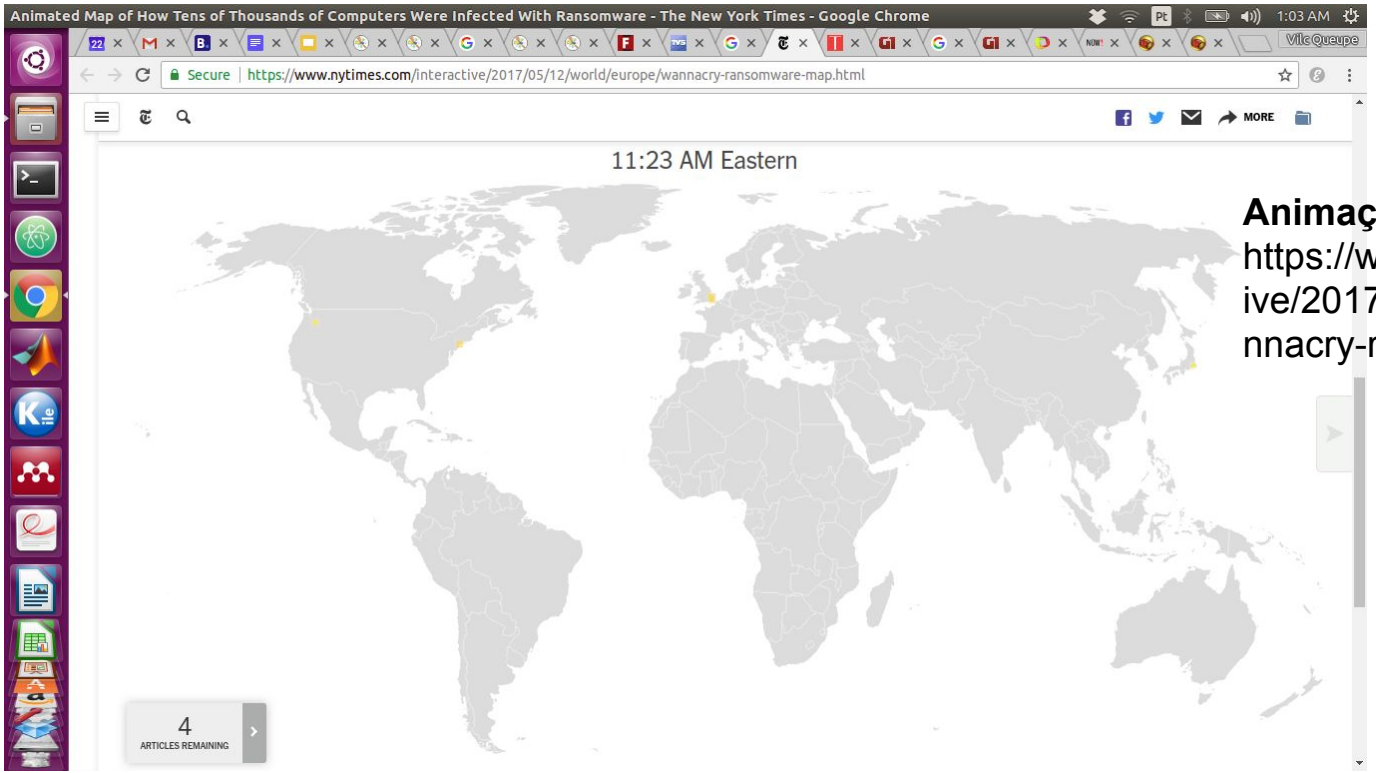
Motivação: prevalência de ataques cibernéticos



Animação disponível em:
https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html

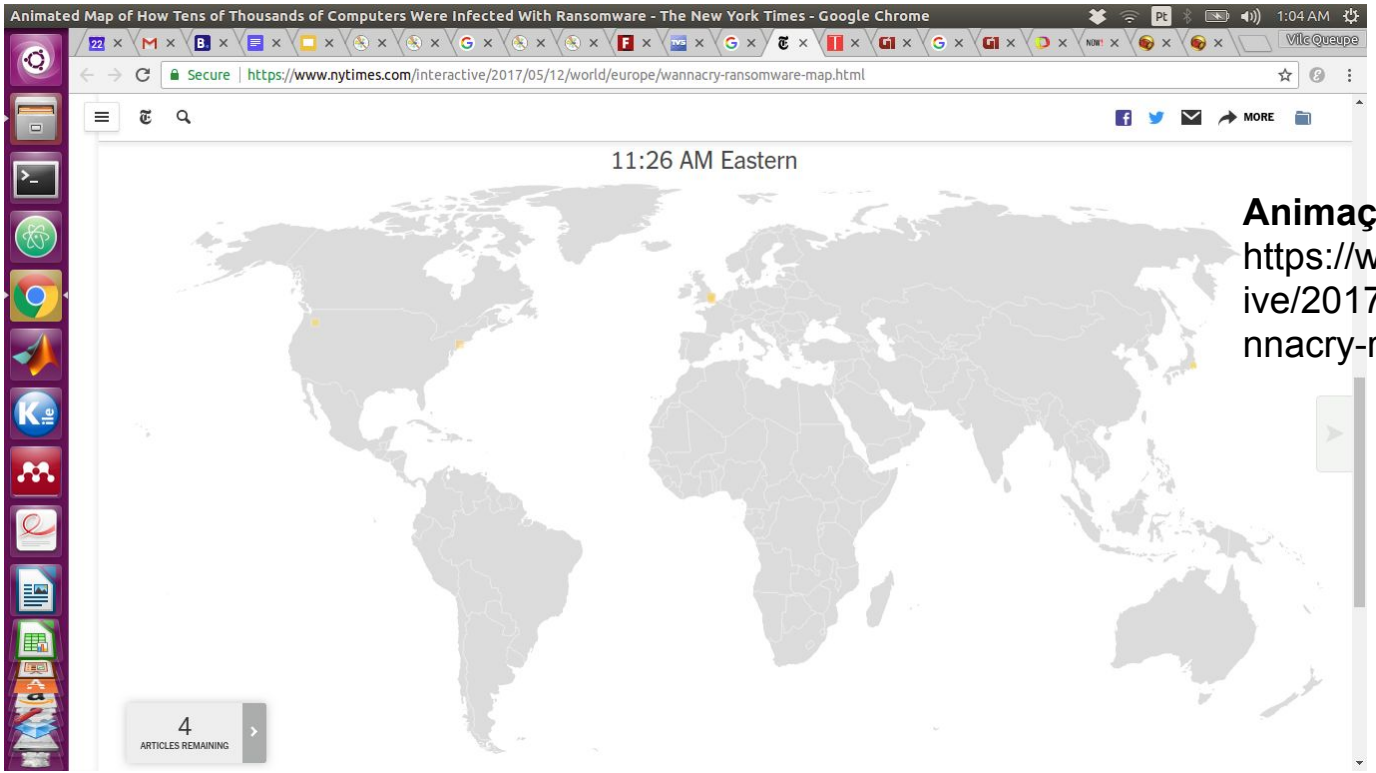
O malware de computador se propaga como o vírus biológico???

Motivação: prevalência de ataques cibernéticos



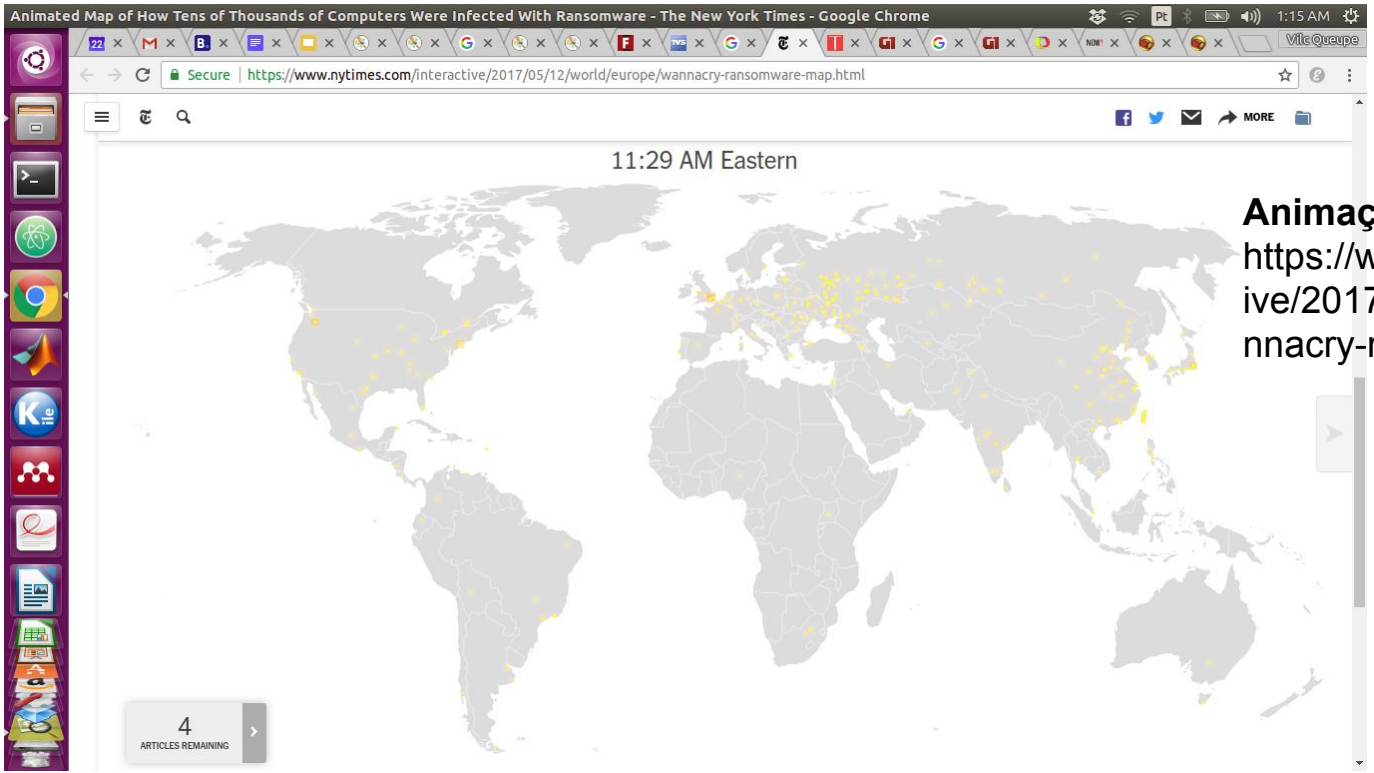
Animação disponível em:
https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html

Motivação: prevalência de ataques cibernéticos



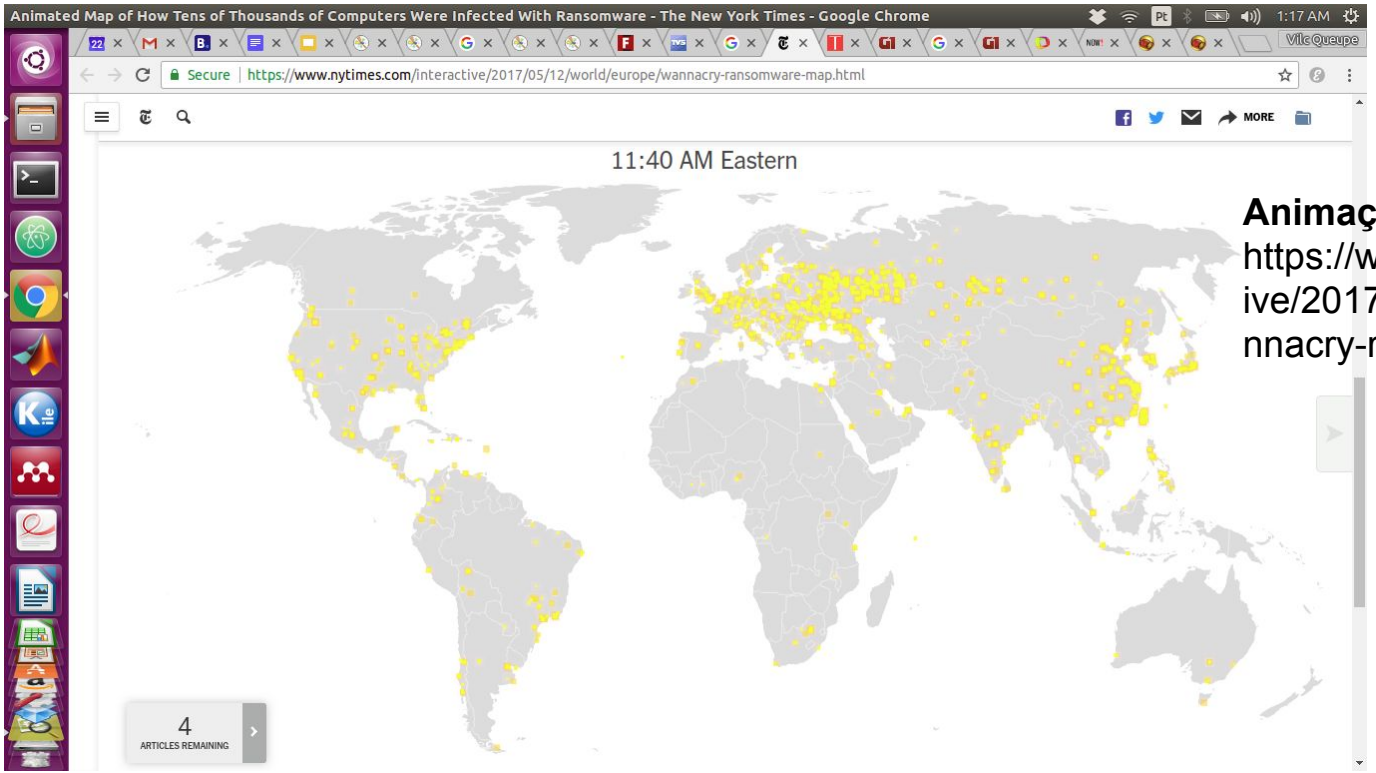
Animação disponível em:
https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html

Motivação: prevalência de ataques cibernéticos



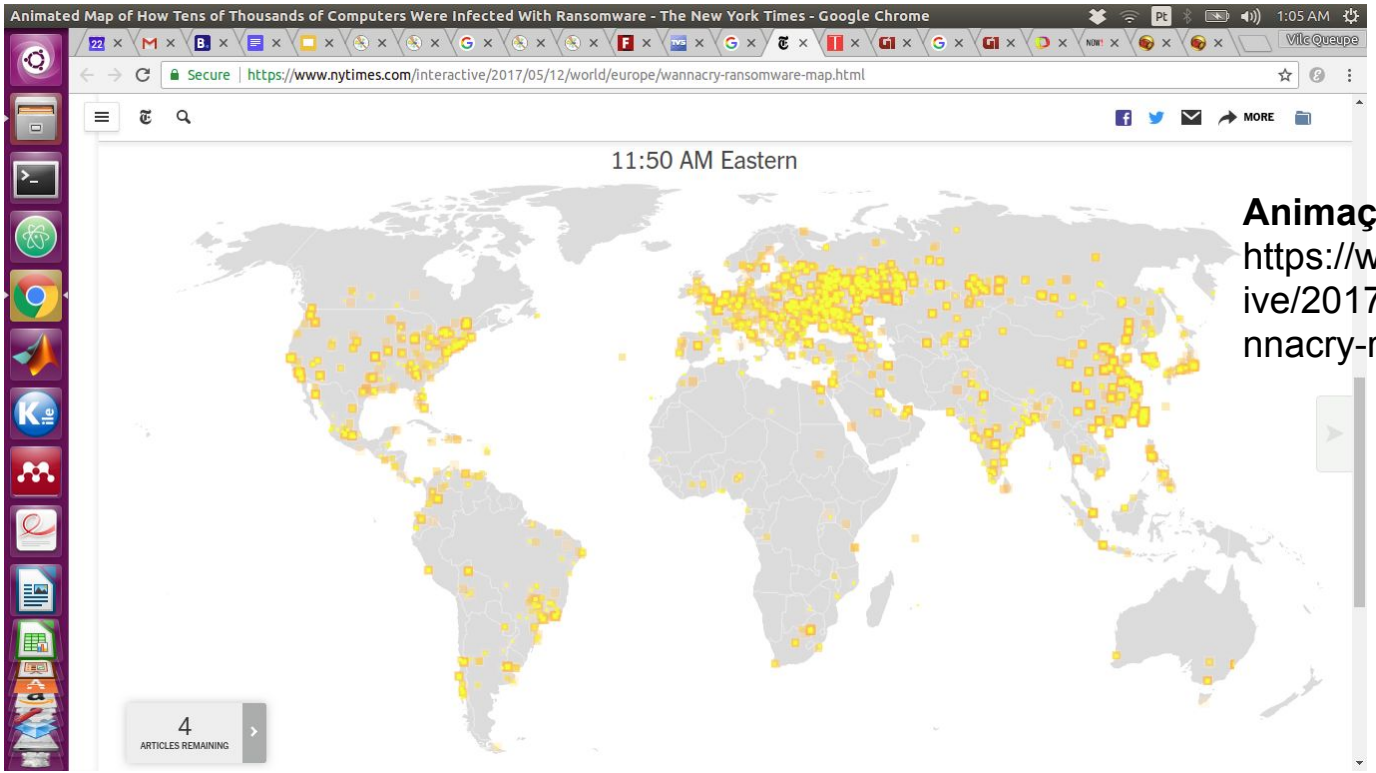
Animação disponível em:
https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html

Motivação: prevalência de ataques cibernéticos



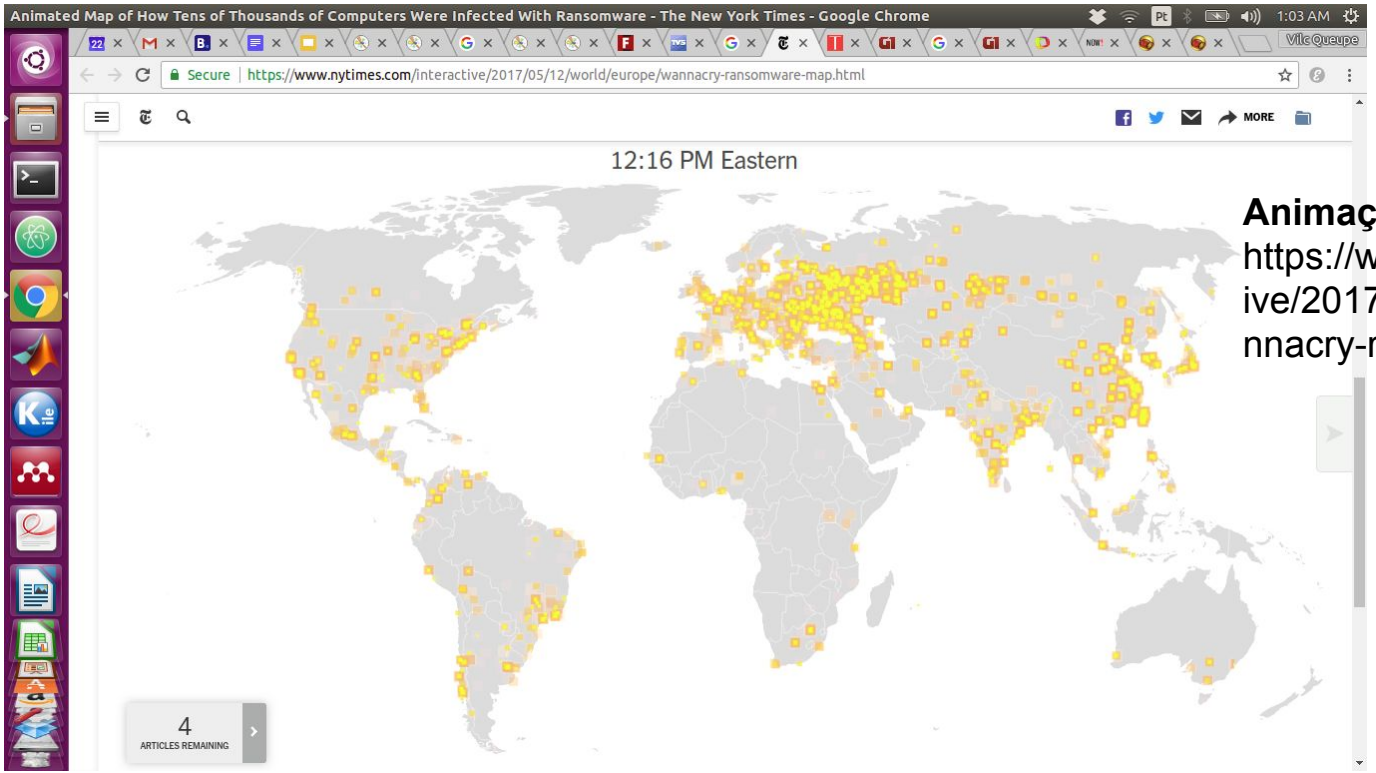
Animação disponível em:
https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html

Motivação: prevalência de ataques cibernéticos



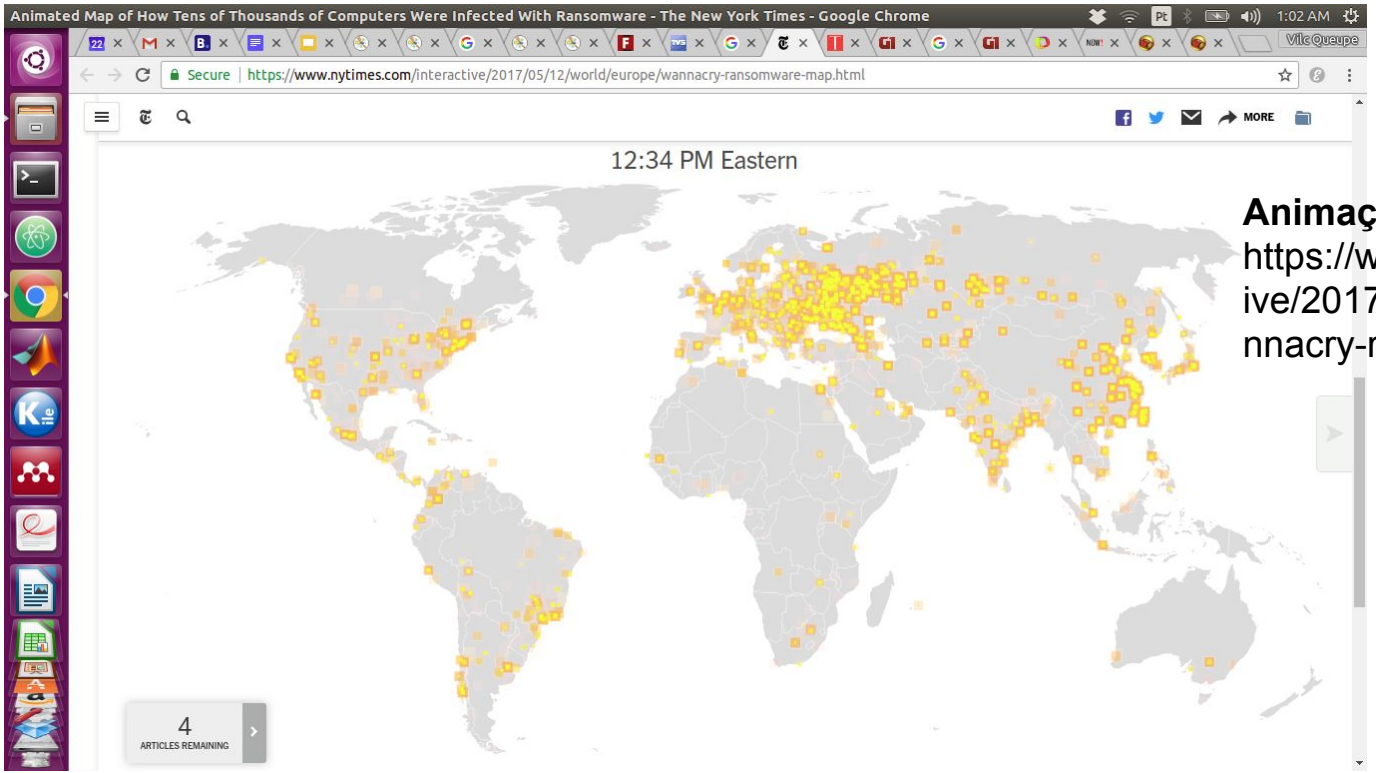
Animação disponível em:
https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html

Motivação: prevalência de ataques cibernéticos



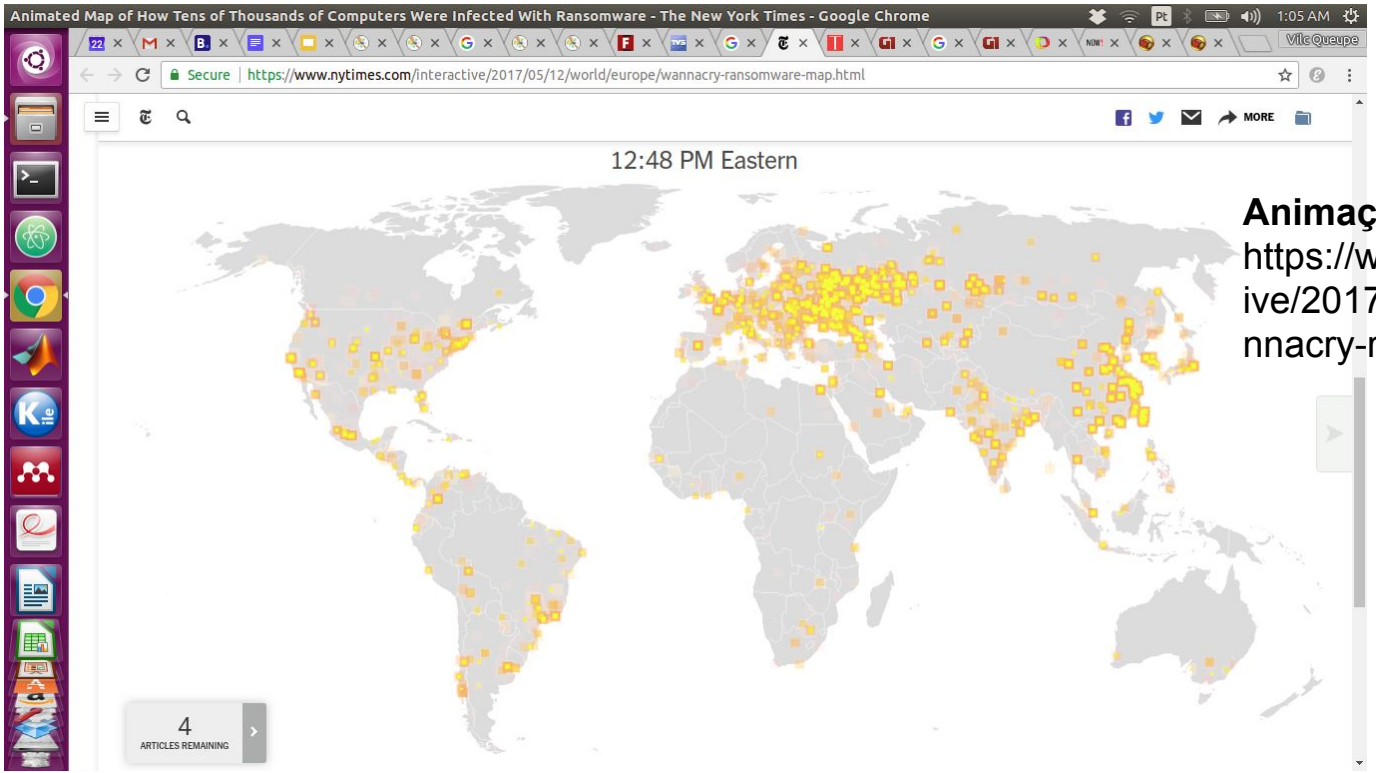
Animação disponível em:
https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html

Motivação: prevalência de ataques cibernéticos



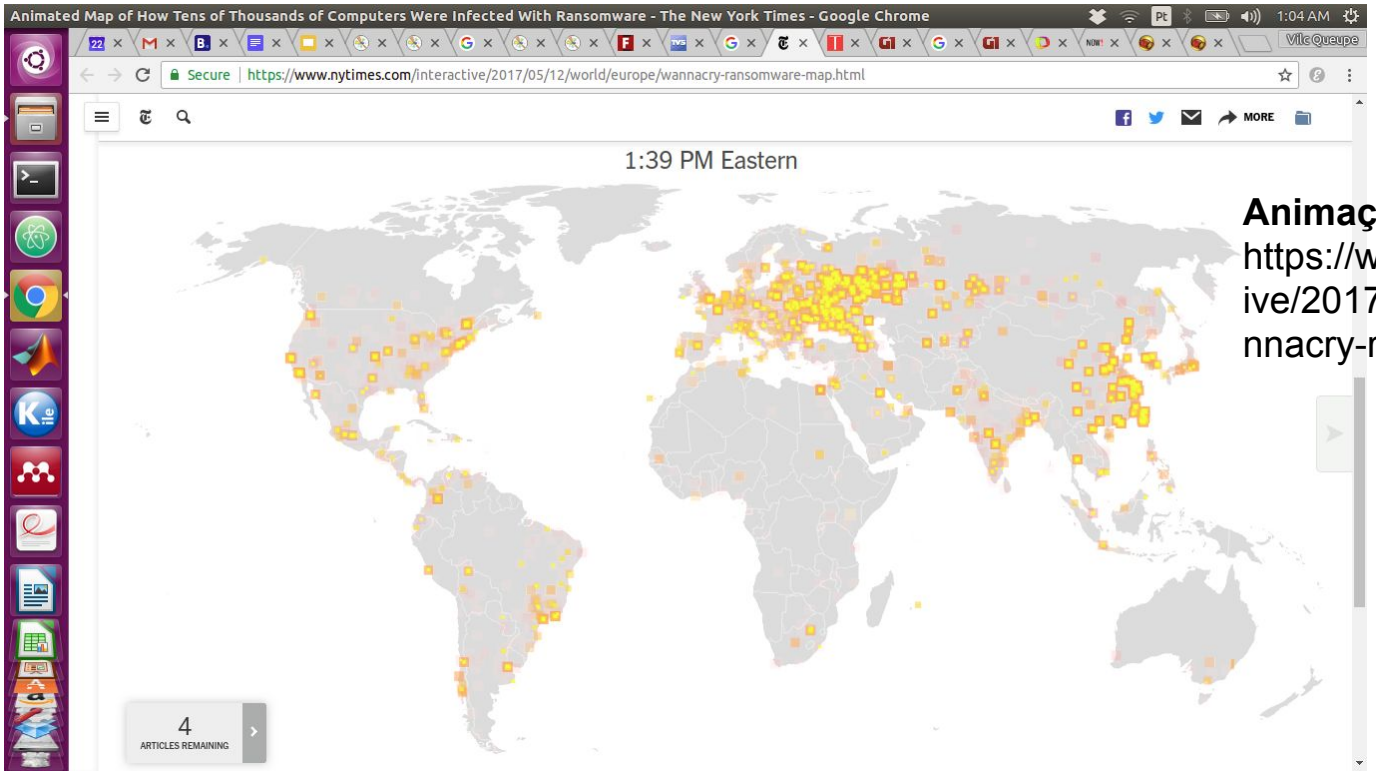
Animação disponível em:
https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html

Motivação: prevalência de ataques cibernéticos



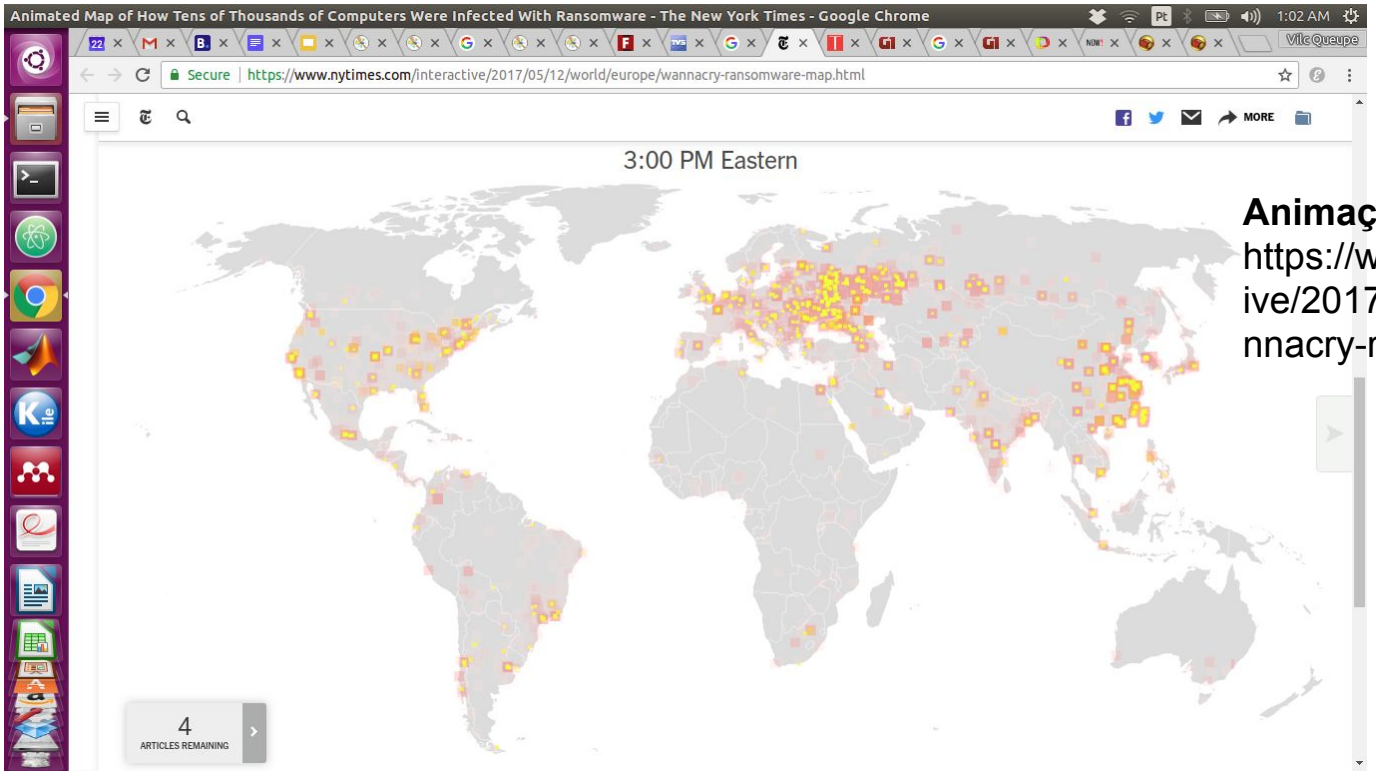
Animação disponível em:
https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html

Motivação: prevalência de ataques cibernéticos



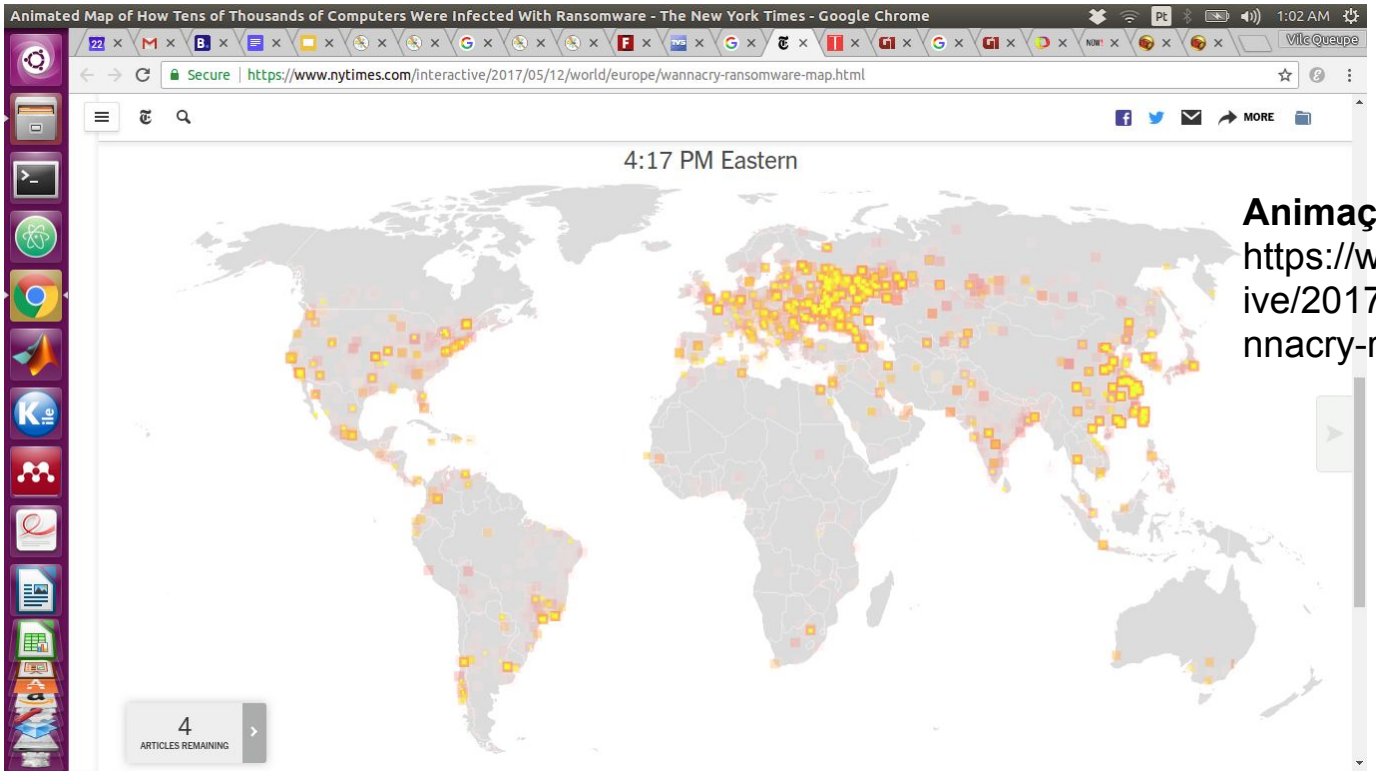
Animação disponível em:
https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html

Motivação: prevalência de ataques cibernéticos



Animação disponível em:
https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html

Motivação: prevalência de ataques cibernéticos



Animação disponível em:
https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html

Motivação: prevalência de ataques cibernéticos

Animação disponível em:
https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html

É importante entender como os malwares se propagam

Imunidade coletiva (*herd immunity*)

Propagação de vírus: problema chave enfrentado pela sociedade

1. Modelos epidemiológicos: desde década de 1920*
2. Hipótese chave: vírus se espalha entre vizinhos
3. Imunidade coletiva: para proteger vizinhos, vacine-se!

* Kermack & McKendrick (1927) e Reed & Frost (1928)

Imunidade coletiva (*herd immunity*)

Propagação de vírus: problema chave enfrentado pela sociedade

1. Modelos epidemiológicos: desde década de 1920*
2. Hipótese chave: vírus se espalha entre vizinhos
3. Imunidade coletiva: para proteger vizinhos, vacine-se!

Entretanto...

1. *Sistemas computacionais diferentes de sistemas biológicos*
2. *Atacante pode infectar qualquer nó da Internet*
3. *Qual o papel da imunidade coletiva em sistemas computacionais?*

Estado da arte e nossa contribuição

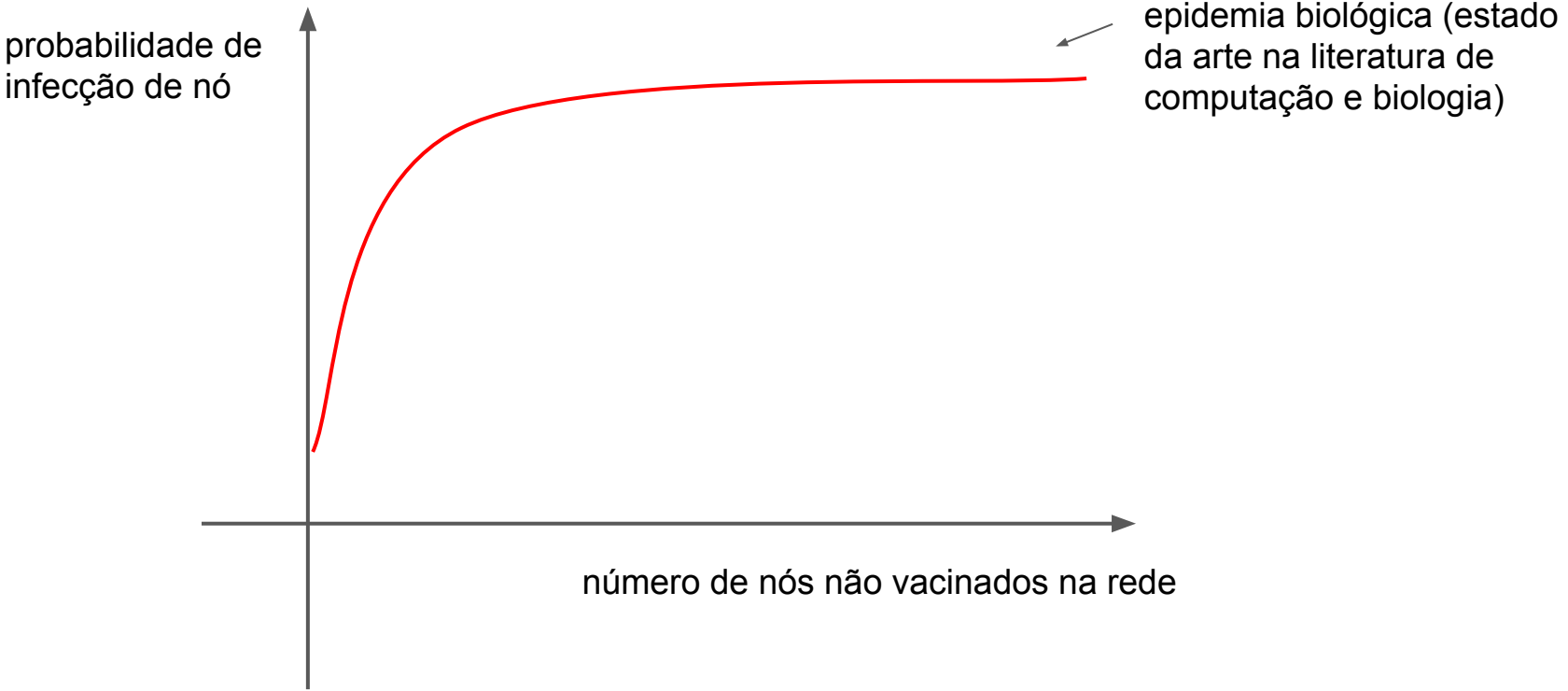
Estado da arte: epidemias estudadas usando modelos biológicos

- atacantes "tolos" (vírus biológicos, para modelar sistemas computacionais!)

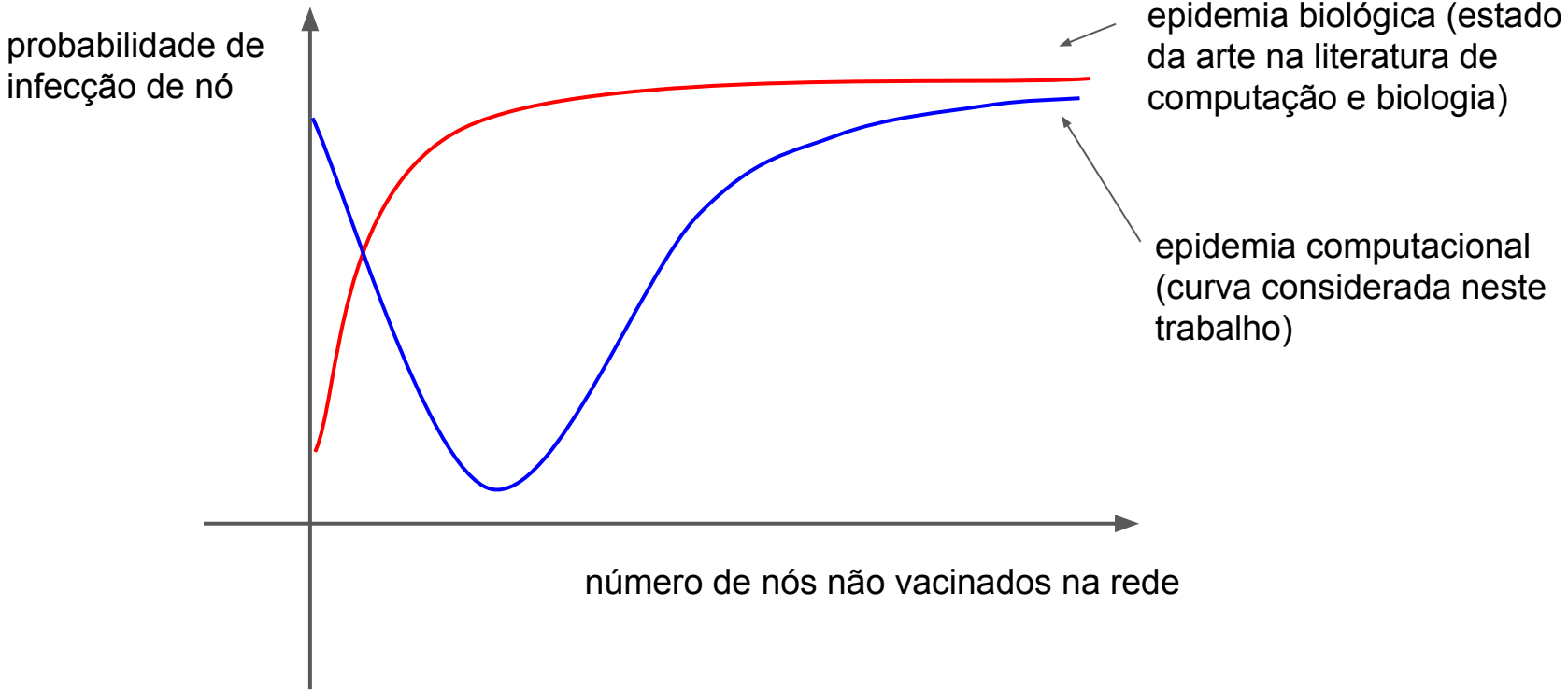
Neste trabalho: consideramos atacantes estratégicos híbridos (e.g., Mirai)

	biologia	computação
atacante	tolo	tolo e estratégico
propagação endógena (entre vizinhos)	sim	sim
propagação exógena (varredura da rede na busca por alvos)	não	sim (e.g., usando ZMap [Durumeric 2013])

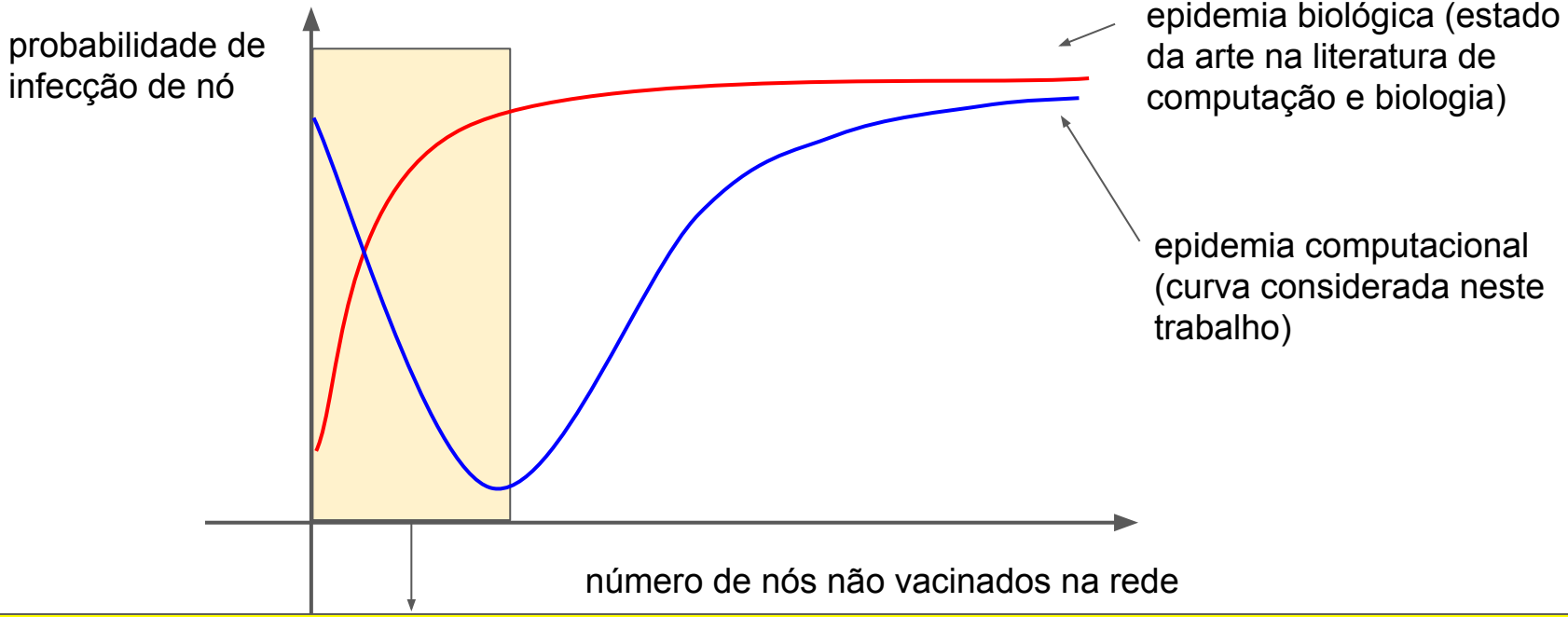
Comparando epidemia biológica e computacional



Comparando epidemia biológica e computacional



Comparando epidemia biológica e computacional



Regime inicial: aumento de nós não vacinados diminui risco individual

Desafios e objetivos

- Propagação estratégica versus epidêmica
  - Estratégica: atacante escaneia rede na busca por vulnerabilidades
  - Epidêmica: vírus se espalha por vizinhos
- Trabalhos anteriores: focaram na propagação epidêmica

- Objetivo
  - Determinar qual a melhor estratégia de defesa: contramedidas
  - Levar em conta custos e benefícios destas contramedidas

Neste trabalho: estudo de propagação estratégica e epidêmica

Contribuições

1. Identificação do comportamento de usuários reais
    a. Os usuários seguem ou evitam a multidão?
2. Modelo analítico para capturar evolução de *malware*
    a. Tradeoffs: custos e benefícios de vacinação
    b. Modelo completo intratável
    c. Modelo simplificado e fórmulas fechadas para custos
3. Análise dos pontos de equilíbrio
    a. Qual a fração da população imunizada no longo prazo?
    b. Identificamos equilíbrios estáveis e instáveis para o sistema

Roteiro

1. **Introdução ao sistema**
    a. **Como um malware se propaga na rede?**
    b. Poder do atacante
    c. Possíveis contramedidas
    d. O dilema da atualização: evitar ou seguir a multidão?
2. Identificação do comportamento de usuários reais
    a. Os usuários no mundo real seguem ou evitam a multidão?
3. Modelo analítico para capturar evolução de *malware*
    a. Apresentação do modelo
    b. Tradeoffs: custos e benefícios de vacinação e equilíbrios subjacentes
    c. Modelo simplificado e fórmulas fechadas para probabilidade de infecção
4. Conclusão

Como *malware* se propaga?

1. **WannaCry**
   a. Alta taxa de contaminação entre vizinhos (**contaminação endógena**);
   b. Espalhamento para outras redes, via e-mails (**contaminação exógena**).
2. **Mirai**
   a. Rede de bots, com localização descentralizada de agentes suscetíveis;
   b. Atacante estratégico: o envio da infecção é centralizado, servidor carregador (*loader*) (**contaminação exógena**)
   c. Capacidade de ataque limitada pelos recursos do loader (**poder do atacante**).

Roteiro

1. Introdução ao sistema
    a. Como um malware se propaga na rede?
    b. Poder do atacante
    c. Possíveis contramedidas
    d. O dilema da atualização: evitar ou seguir a multidão?
2. Identificação do comportamento de usuários reais
    a. Os usuários no mundo real seguem ou evitam a multidão?
3. Modelo analítico para capturar evolução de *malware*
    a. Apresentação do modelo
    b. Tradeoffs: custos e benefícios de vacinação e equilíbrios subjacentes
    c. Modelo simplificado e fórmulas fechadas para probabilidade de infecção
4. Conclusão

Poder do atacante

1. **Capacidade limitada**: Λ infecções por unidade de tempo
2. **Divisão uniforme** pelos nós não vacinados:

   cada nó atacado de forma exógena sob taxa $\lambda(N) = \Lambda / N$

Quanto maior o número de nós não-vacinados, menor a chance de um nó ser atacado diretamente pelo atacante

Roteiro

1. Introdução ao sistema
    a. Como um malware se propaga na rede?
    b. Poder do atacante
    c. Possíveis contramedidas
    d. O dilema da atualização: evitar ou seguir a multidão?
2. Identificação do comportamento de usuários reais
    a. Os usuários no mundo real seguem ou evitam a multidão?
3. Modelo analítico para capturar evolução de *malware*
    a. Apresentação do modelo
    b. Tradeoffs: custos e benefícios de vacinação e equilíbrios subjacentes
    c. Modelo simplificado e fórmulas fechadas para probabilidade de infecção
4. Conclusão

Contramedidas

1. **Moderadas:** atualizações de sistemas e antivírus baseados em assinaturas
   a. atualizações constantes;
   b. evolução dos códigos maliciosos, por meio do despistamento;
   c. neste trabalho: agentes com contramedidas moderadas caracterizados endemicamente pelo modelo SIS (Susceptible-Infected-Susceptible).
2. **Rigorosas:** desconexão, substituição do sistema por mais moderno e antivírus de efeito total
   a. mais eficientes;
   b. maior custo de execução;
   c. neste trabalho: agentes com contramedidas rigorosa são sempre imunes.

Roteiro

1. Introdução ao sistema
   a. Como um malware se propaga na rede?
   b. Poder do atacante
   c. Possíveis contramedidas
   d. O dilema da atualização: evitar ou seguir a multidão?
2. Identificação do comportamento de usuários reais
   a. Os usuários no mundo real seguem ou evitam a multidão?
3. Modelo analítico para capturar evolução de *malware*
   a. Apresentação do modelo
   b. Tradeoffs: custos e benefícios de vacinação e equilíbrios subjacentes
   c. Modelo simplificado e fórmulas fechadas para probabilidade de infecção
4. Conclusão

Introdução ao sistema: dilema da atualização

1. **Gerenciamento de atualizações (*patch management*):** aplicação contramedidas possui custo
2. **Modelos de epidemias:** podem auxiliar na escolha das contramedidas.

Posso postergar a aplicação de um *patch*? neste trabalho focamos no impacto da decisão de um agente sobre a decisão dos demais.

Introdução ao sistema: evitar ou seguir a multidão

1. **Evitando a multidão (*avoid the crowd*)**
   a. abordagem clássica = modelo biológico;
   b. se a maioria dos indivíduos forem vacinados, para que vacinar?
   c. **se todo mundo vacinar, a vacina não é mais tão necessária!** (e.g., vacina de febre amarela, anos sem ser aplicada)
2. **Seguindo a multidão (*follow the crowd*)**
   a. reconhece adversário estratégico;
   b. se a maioria dos indivíduos forem vacinados, o risco de contaminação aumenta;
   c. se todo mundo vacinar, vacine-se!

Roteiro

1. Introdução ao sistema
    a. Como um malware se propaga na rede?
    b. Poder do atacante
    c. Possíveis contramedidas
    d. O dilema da atualização: evitar ou seguir a multidão?
2. **Identificação do comportamento de usuários reais**
    a. Os usuários no mundo real seguem ou evitam a multidão?
3. Modelo analítico para capturar evolução de *malware*
    a. Apresentação do modelo
    b. Tradeoffs: custos e benefícios de vacinação e equilíbrios subjacentes
    c. Modelo simplificado e fórmulas fechadas para probabilidade de infecção
4. Conclusão

Identificação de comportamentos no mundo real

Existem evidências de que usuários da Internet às vezes seguem e às vezes evitam a multidão?

Identificação de comportamentos no mundo real

Existem evidências de que usuários da Internet às vezes seguem e às vezes evitam a multidão?

Vamos verificar usando o Shodan!

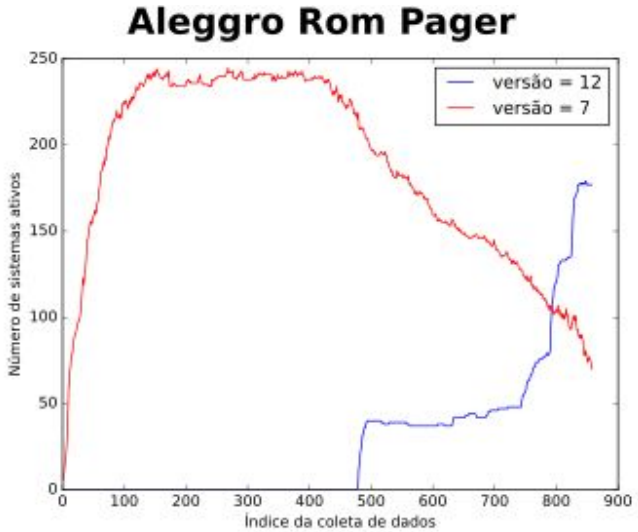
https://www.shodan.io/

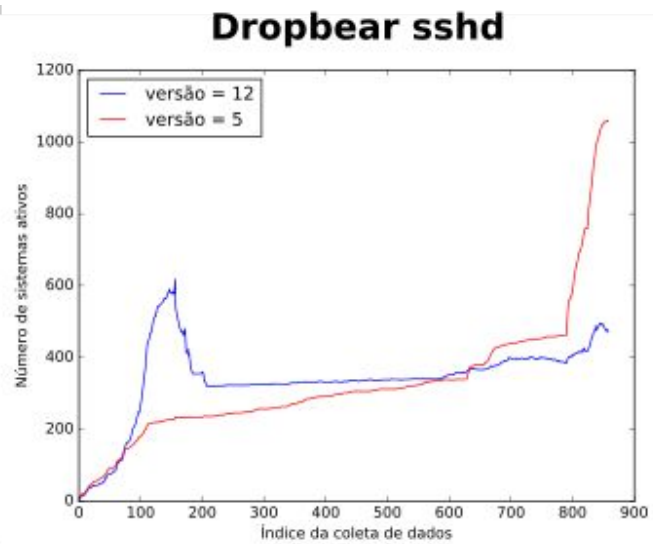
Identificação de comportamentos no mundo real

Evidências no Shodan de dispositivos industriais (críticos!) nos quais usuários

i. "**seguem a multidão**": usam últimas versões do software
[seguir = adotar contramedidas rigorosas (patching)]

ii. "**evitam a multidão**": versões antigas do software mantidas quando novas disponíveis
[evitar = não adotar contramedidas rigorosas (não patching)]



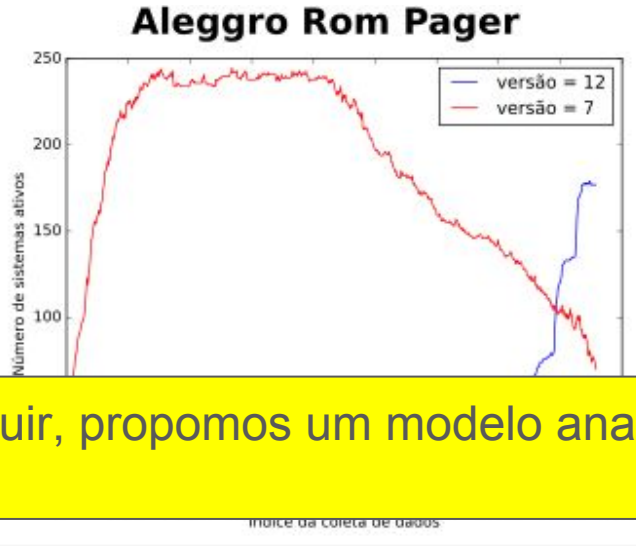


Identificação de comportamentos no mundo real

Evidências no Shodan de dispositivos industriais (críticos!) nos quais usuários

i. "**seguem a multidão**": usam últimas versões do software
[seguir = adotar contramedidas rigorosas (patching)]

ii. "**evitam a multidão**": versões antigas do software mantidas quando novas disponíveis
[evitar = não adotar contramedidas rigorosas (não patching)]



A seguir, propomos um modelo analítico inspirado em tais comportamentos.

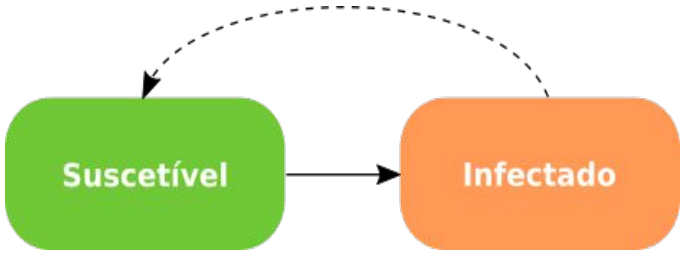
Roteiro

1. Introdução ao sistema
    a. Como um malware se propaga na rede?
    b. Poder do atacante
    c. Possíveis contramedidas
    d. O dilema da atualização: evitar ou seguir a multidão?
2. Identificação do comportamento de usuários reais
    a. Os usuários no mundo real seguem ou evitam a multidão?
3. **Modelo analítico para capturar evolução de *malware***
    a. **Apresentação do modelo**
    b. Tradeoffs: custos e benefícios de vacinação e equilíbrios subjacentes
    c. Modelo simplificado e fórmulas fechadas para probabilidade de infecção
4. Conclusão

Modelo: parâmetros e métricas de interesse

Estado do sistema:

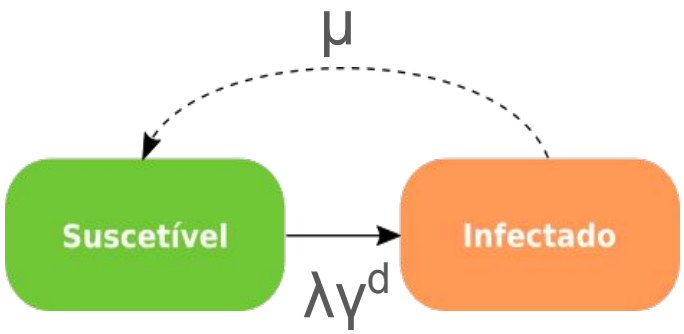
1. Nó aplicando contra-medida rigorosa: sempre imune
2. Nó aplicando contra-medida moderada: alterna entre dois estados,
   a. Suscetível ou
   b. Infectado:
3. Decisão de aplicação de contramedida rigorosa: tomada em escala de tempo grossa



Topologia: rede totalmente conectada (grafo completo)

Modelo: parâmetros e métricas de interesse

termo	descrição
N	nós na rede (aplicando contra-medidas moderadas)
Λ	poder do atacante (taxa de infecção exógena)
$\lambda(N) = \Lambda / N$	taxa de infecção exógena por nó
γ	taxa de infecção endógena
d	# vizinhos infectados
μ	taxa de recuperação

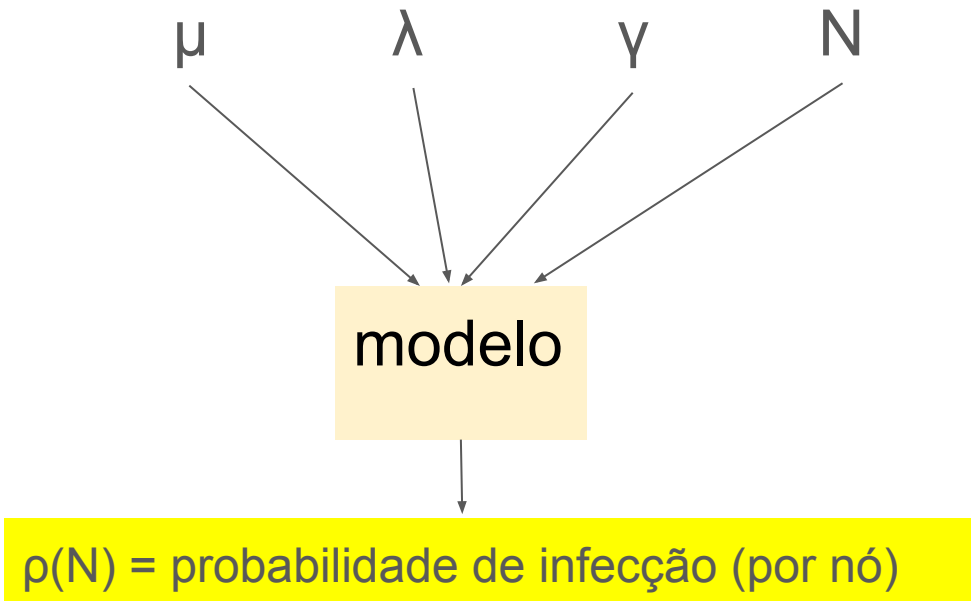


taxa de infecção por nó = $\lambda\gamma^d$

modelo multiplicativo

Modelo: parâmetros e métricas de interesse

termo	descrição
N	nós na rede (aplicando contra-medidas moderadas)
Λ	poder do atacante (taxa de infecção exógena)
$\lambda(N) = \Lambda / N$	taxa de infecção exógena por nó
γ	taxa de infecção endógena
d	# vizinhos infectados
μ	taxa de recuperação

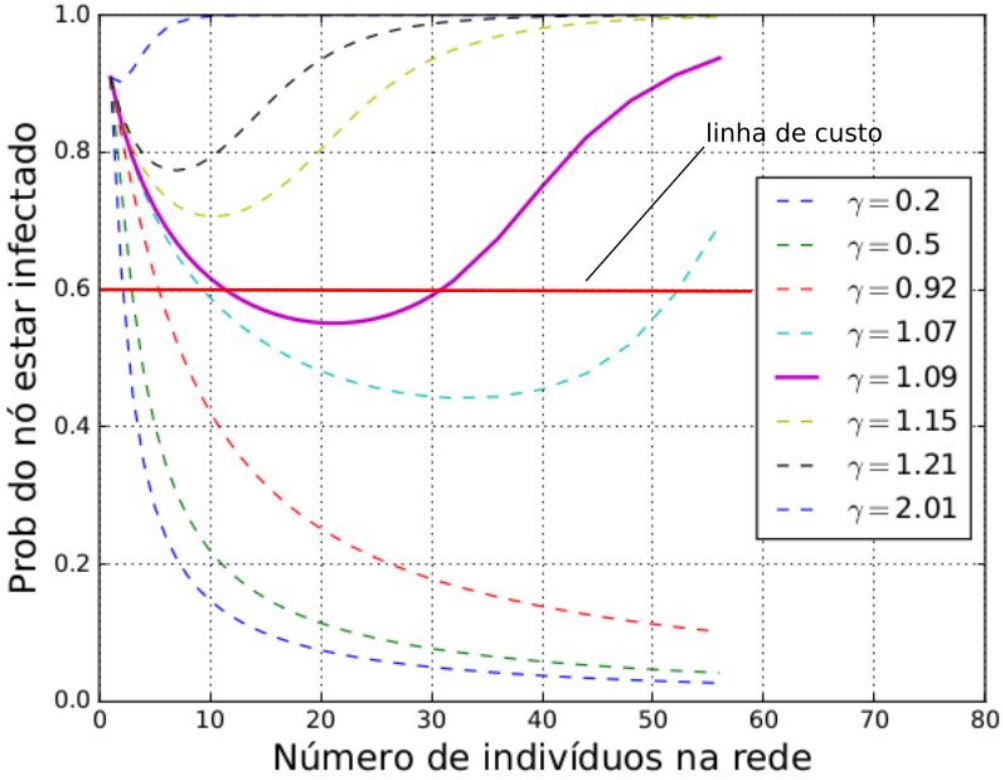


Roteiro

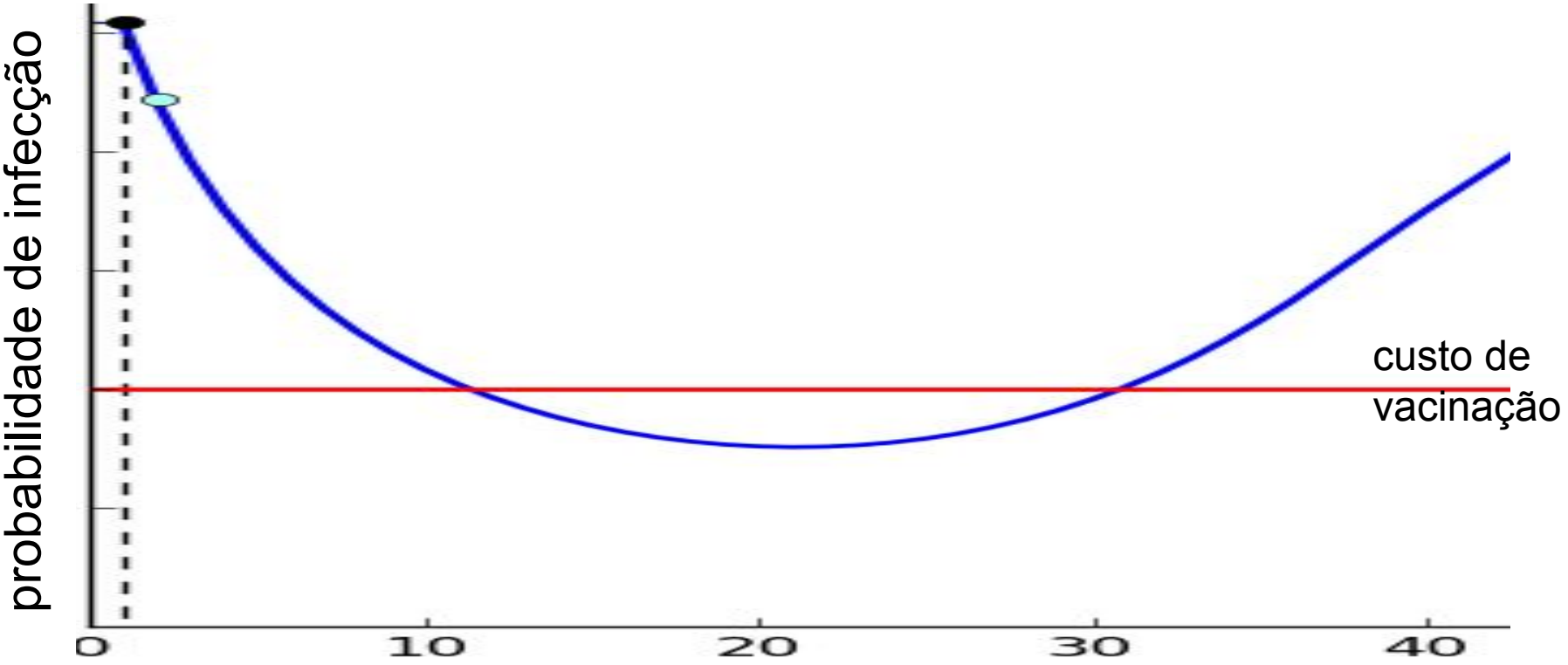
1. Introdução ao sistema
    a. Como um malware se propaga na rede?
    b. Poder do atacante
    c. Possíveis contramedidas
    d. O dilema da atualização: evitar ou seguir a multidão?
2. Identificação do comportamento de usuários reais
    a. Os usuários no mundo real seguem ou evitam a multidão?
3. **Modelo analítico para capturar evolução de *malware***
    a. Apresentação do modelo
    b. Tradeoffs: custos e benefícios de vacinação e equilíbrios subjacentes
    c. Modelo simplificado e fórmulas fechadas para probabilidade de infecção
4. Conclusão

Modelo: benefícios e custos de vacinação

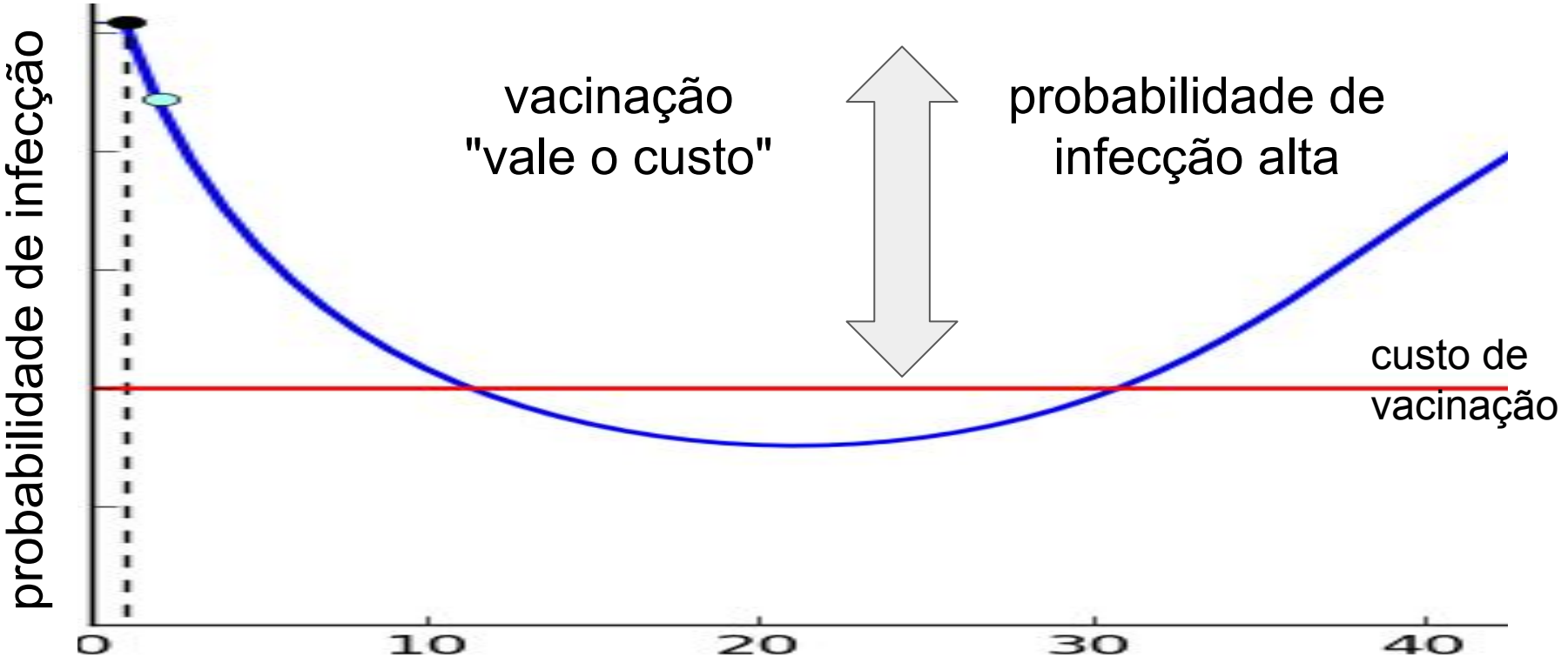
1. Parâmetros
   a. Taxa de infecção exógena: λ(N) = 10/N
   b. Taxa de cura: μ = 1
   c. Custo de vacinação: 0,6
2. Variamos taxa de infecção endógena
   a. Alta: modelo biológico
   b. Média: modelo híbrido
   c. Baixa: modelo estratégico



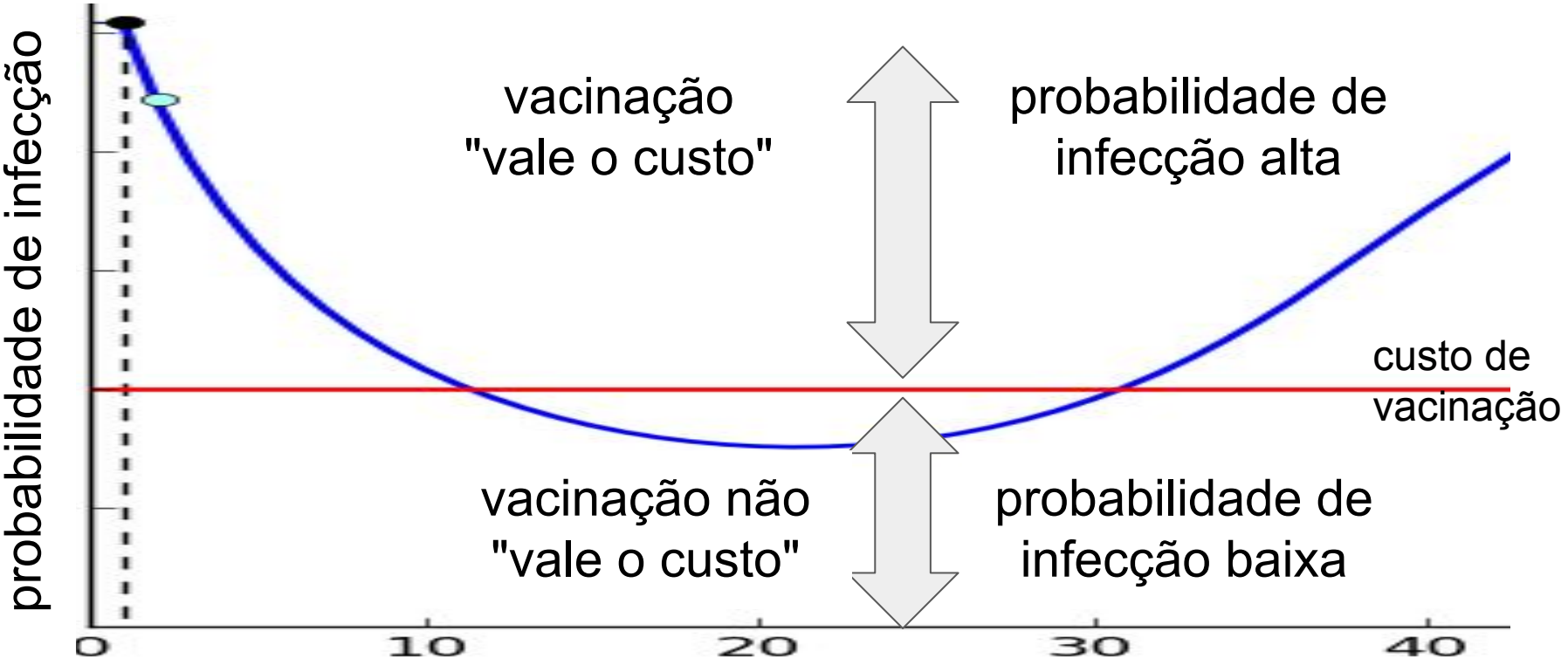
Vacinar vale a pena? Custos e benefícios



Vacinar vale a pena? Custos e benefícios

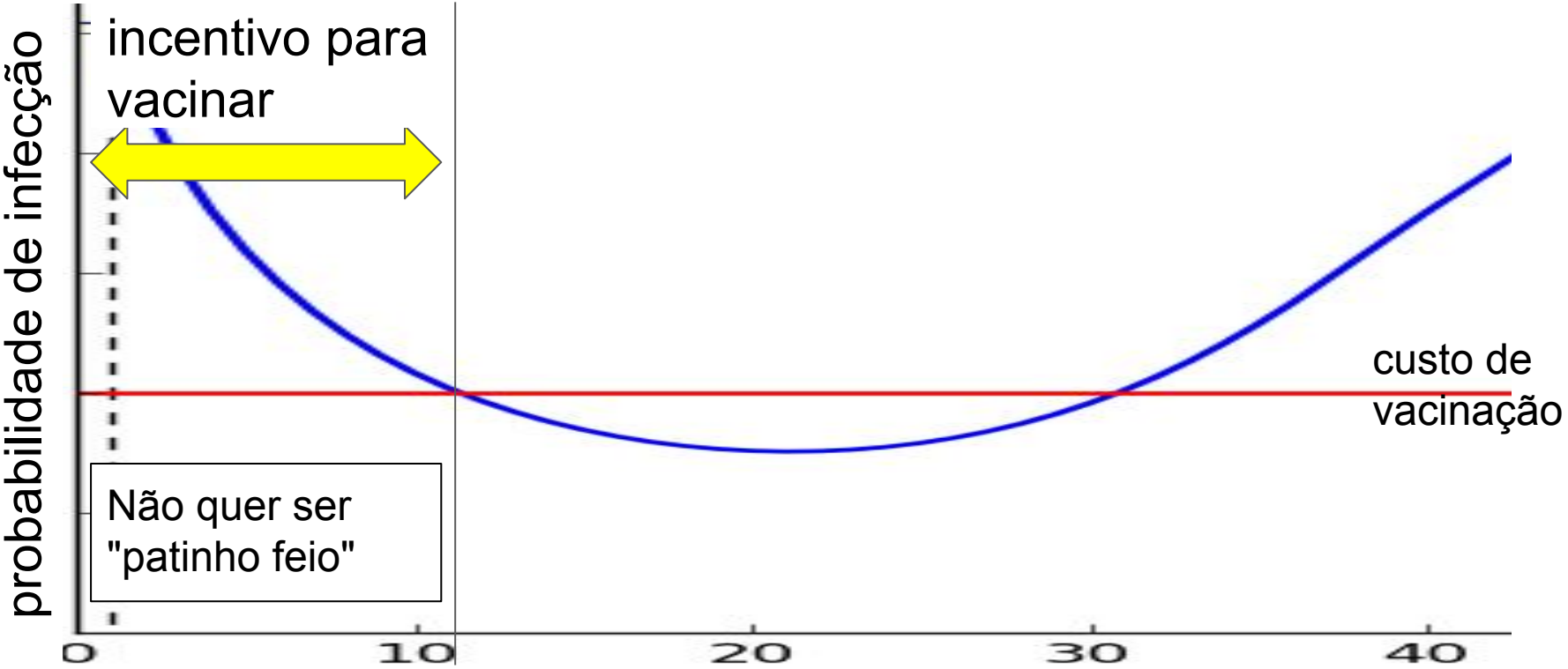


Vacinar vale a pena? Custos e benefícios

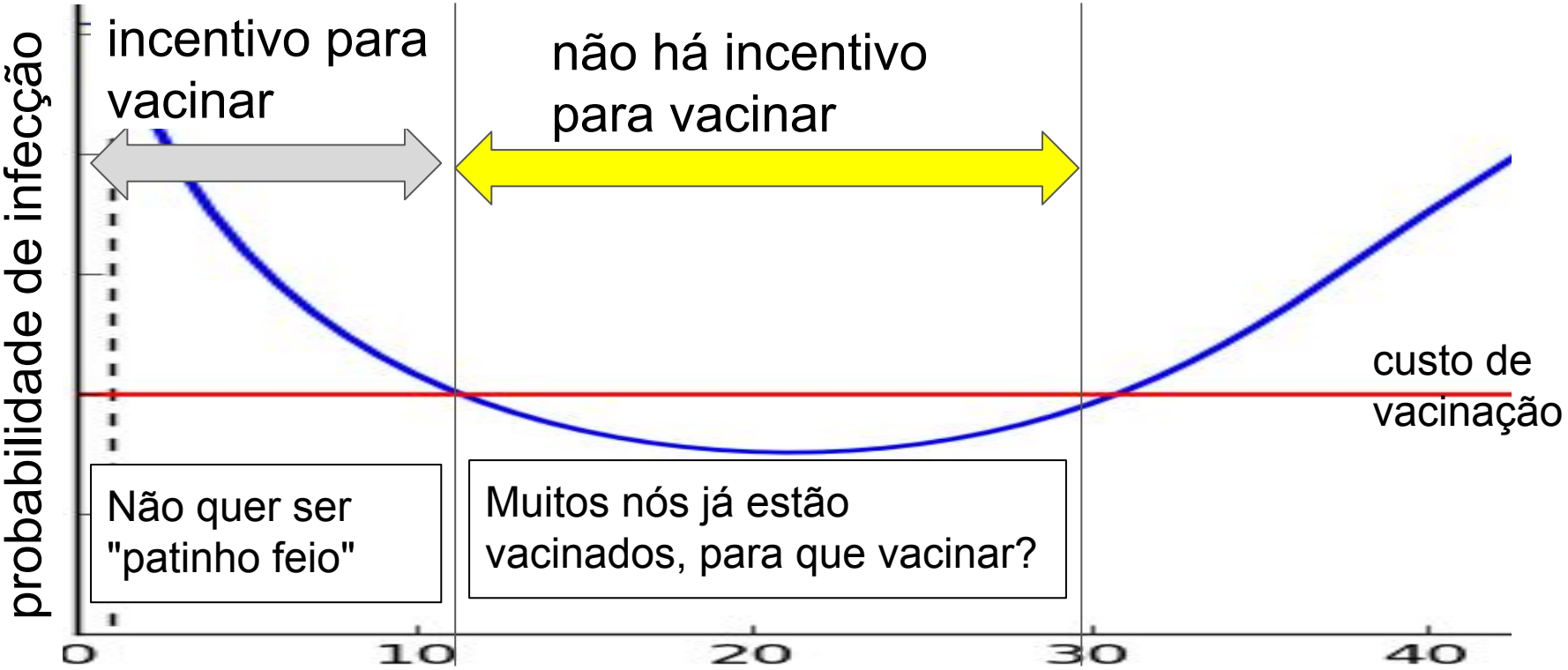


número de nós na rede (aplicando contramedidas moderadas)

Regime de operação 1: não ser "patinho feio"

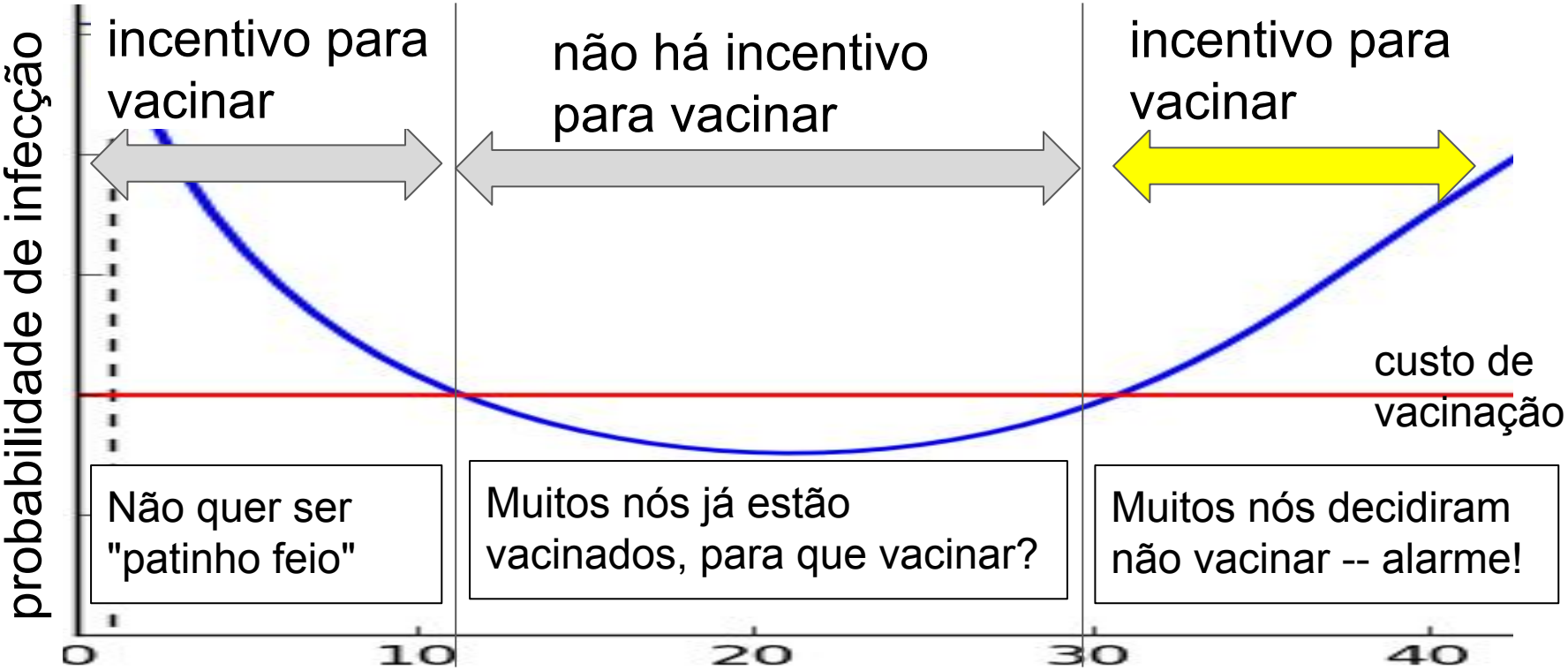


Regime de operação 2: economizar com vacina



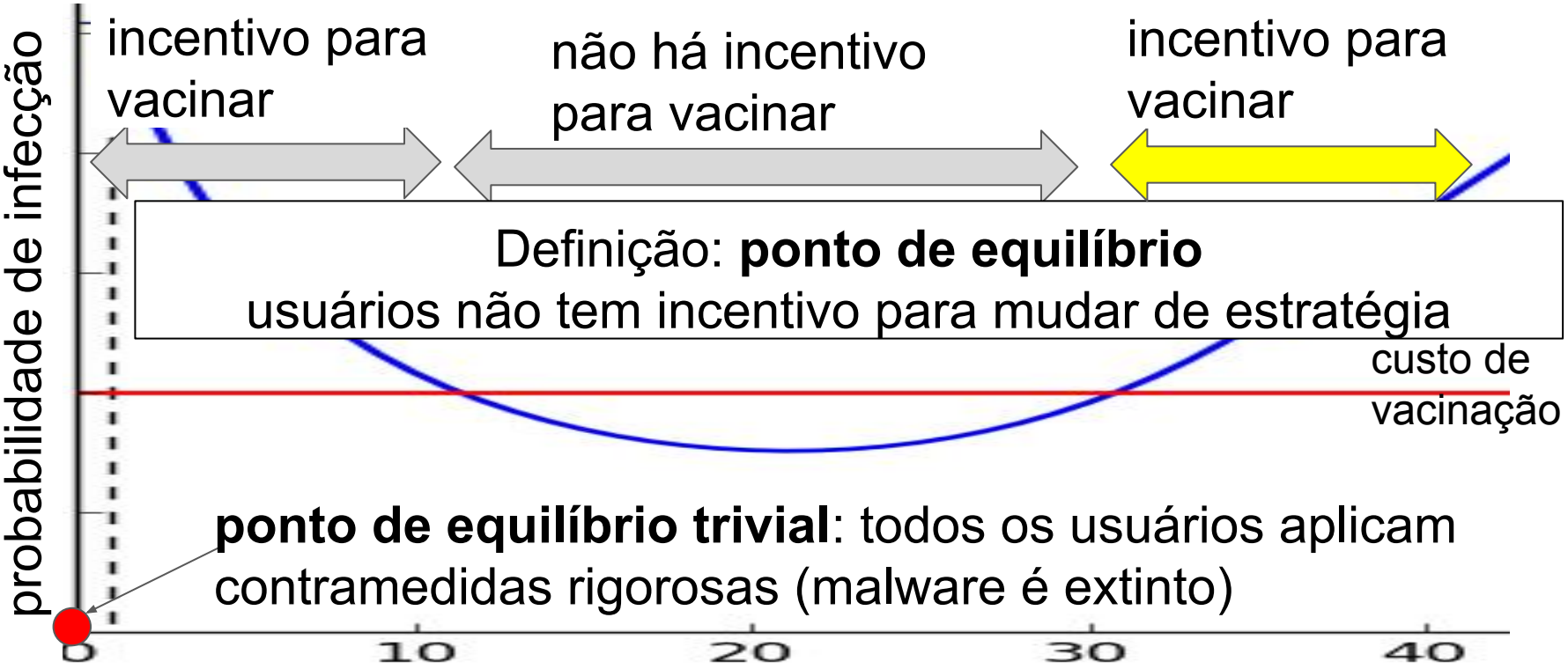
número de nós na rede (aplicando contramedidas moderadas)

Regime de operação 3: vacinar é preciso

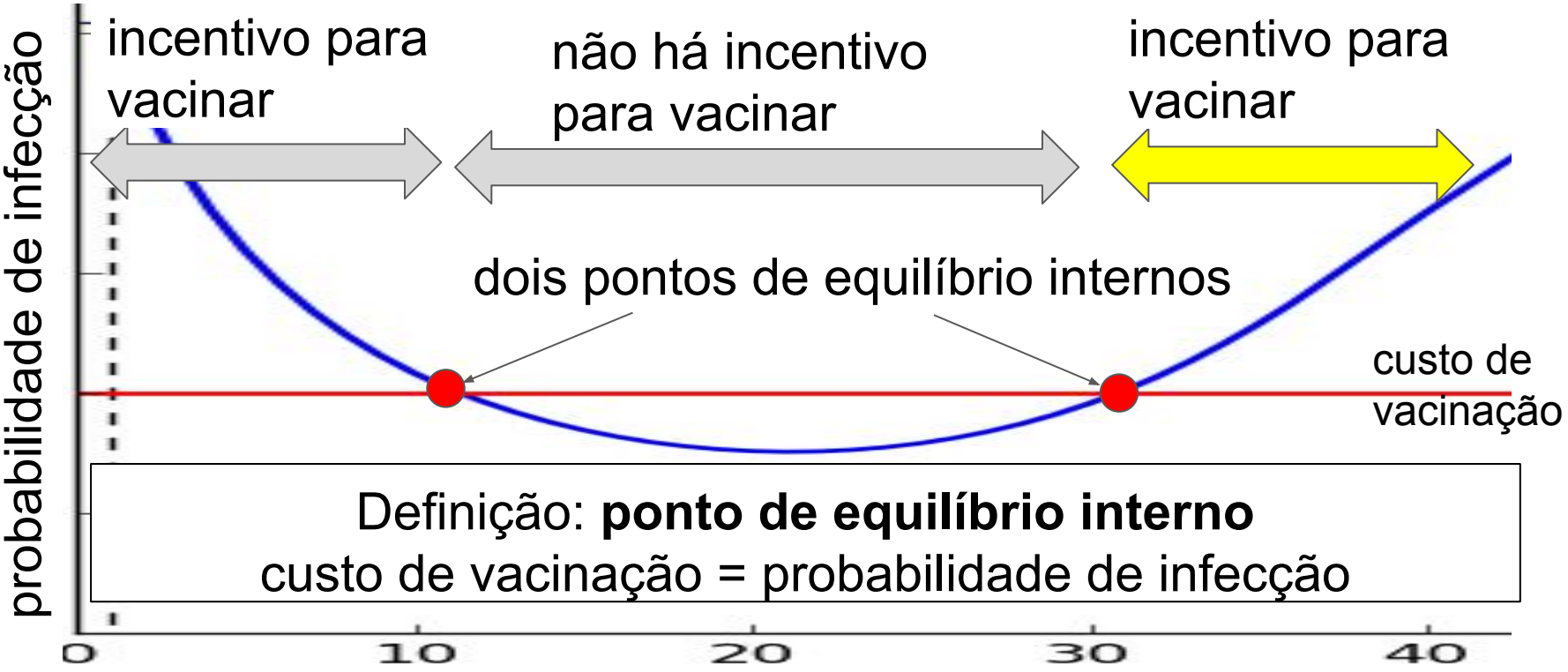


número de nós na rede (aplicando contramedidas moderadas)

Ponto de equilíbrio: definição



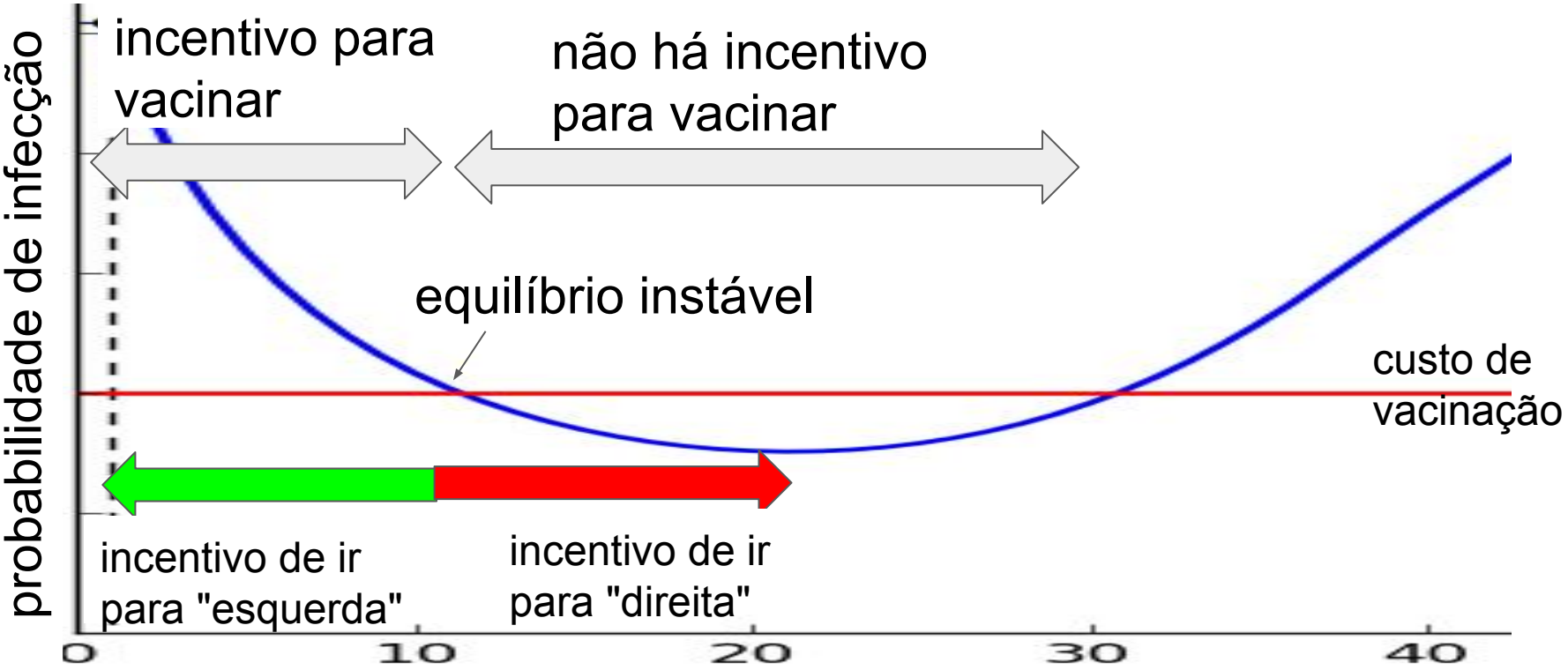
Ponto de equilíbrio: definição



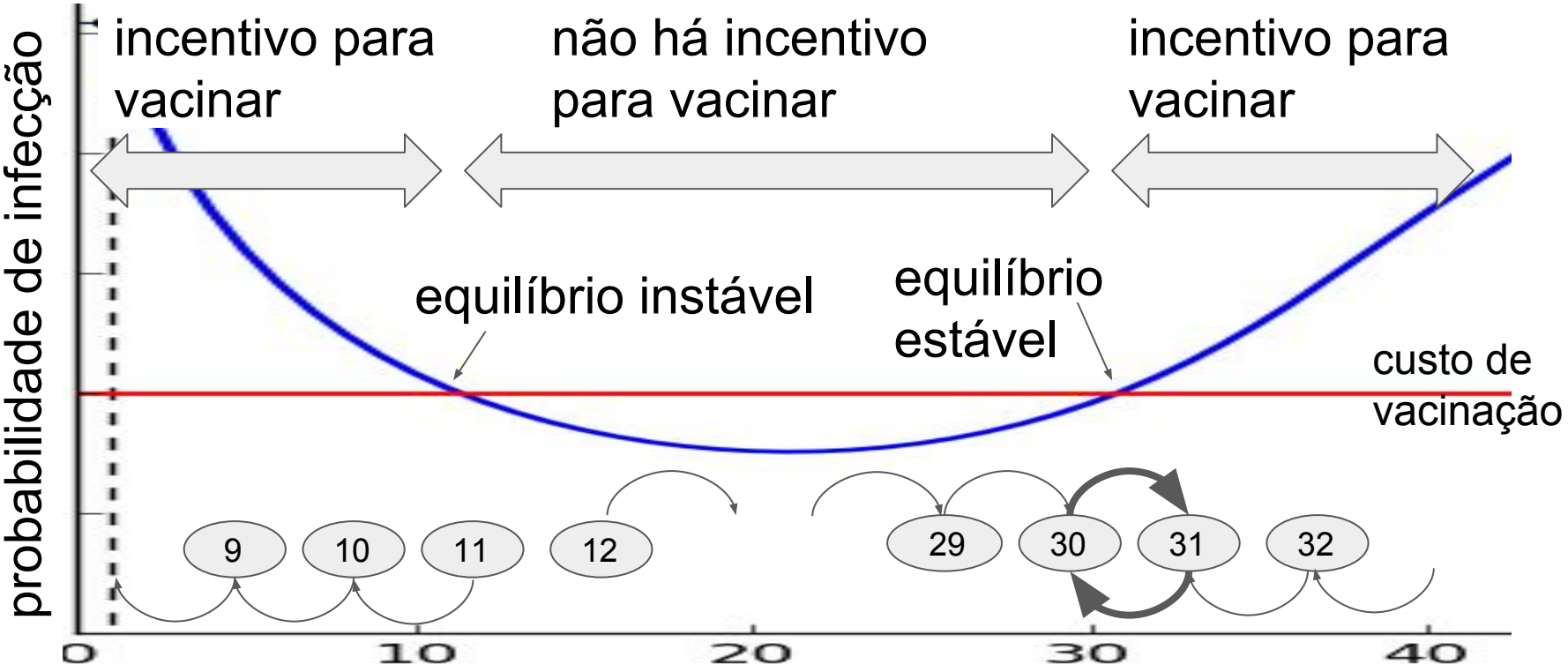
Definição: **ponto de equilíbrio interno**
custo de vacinação = probabilidade de infecção

número de nós na rede (aplicando contramedidas moderadas)

Equilíbrios da população: equilíbrio instável



Equilíbrios da população: equilíbrio estável



Roteiro

1. Introdução ao sistema
    a. Como um malware se propaga na rede?
    b. Poder do atacante
    c. Possíveis contramedidas
    d. O dilema da atualização: evitar ou seguir a multidão?
2. Identificação do comportamento de usuários reais
    a. Os usuários no mundo real seguem ou evitam a multidão?
3. **Modelo analítico para capturar evolução de *malware***
    a. Apresentação do modelo
    b. Tradeoffs: custos e benefícios de vacinação e equilíbrios subjacentes
    c. Modelo simplificado e fórmulas fechadas para probabilidade de infecção
4. Conclusão

Modelo: questionamentos analíticos

1. Como expressar a probabilidade de infecção em fórmula fechada simples?
2. Quantos equilíbrios admite o sistema?

Modelo: simplificação e resultados

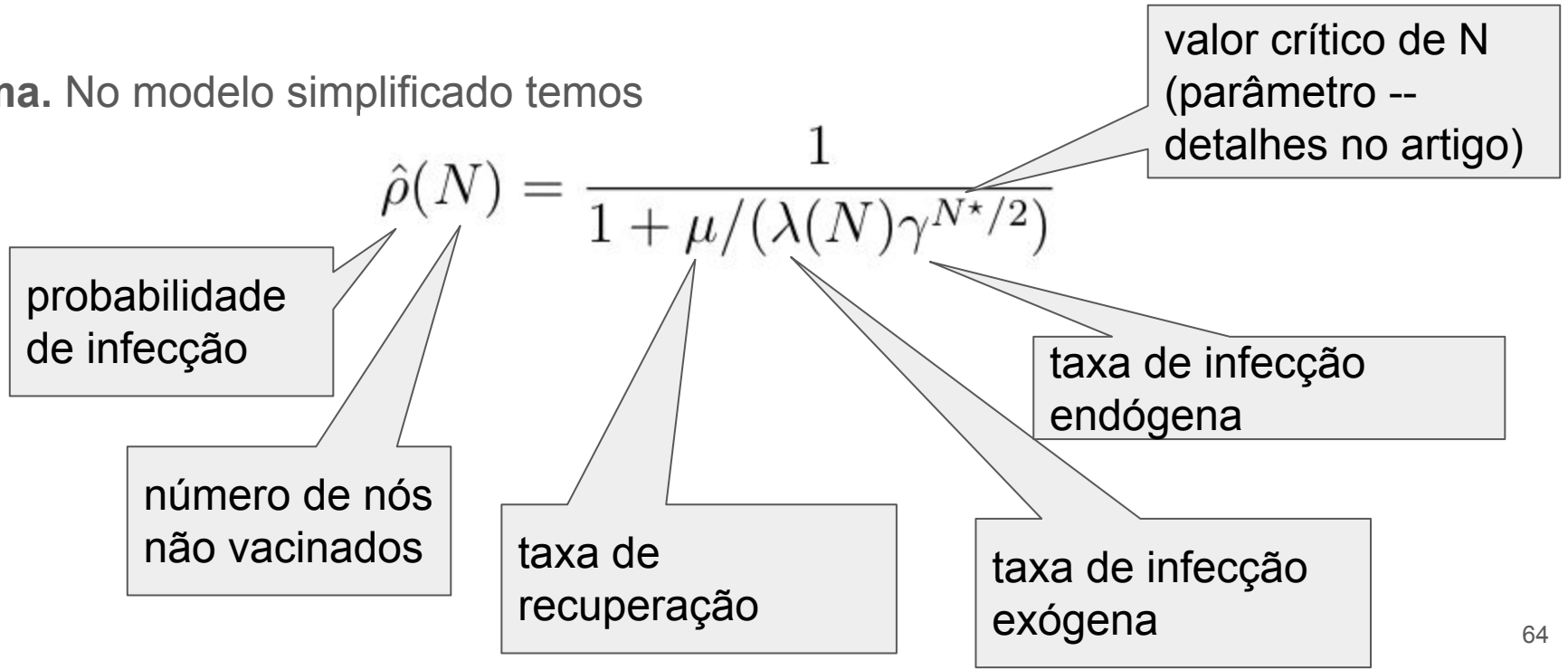
1. Como expressar a probabilidade de infecção em fórmula fechada simples?
2. Quantos equilíbrios admite o sistema?

Para responder estas perguntas, consideramos uma **simplificação do analítico analítico** (detalhes no artigo)

Modelo: resultados em fórmula fechada

Como expressar a probabilidade de infecção em fórmula fechada simples?

Lema. No modelo simplificado temos

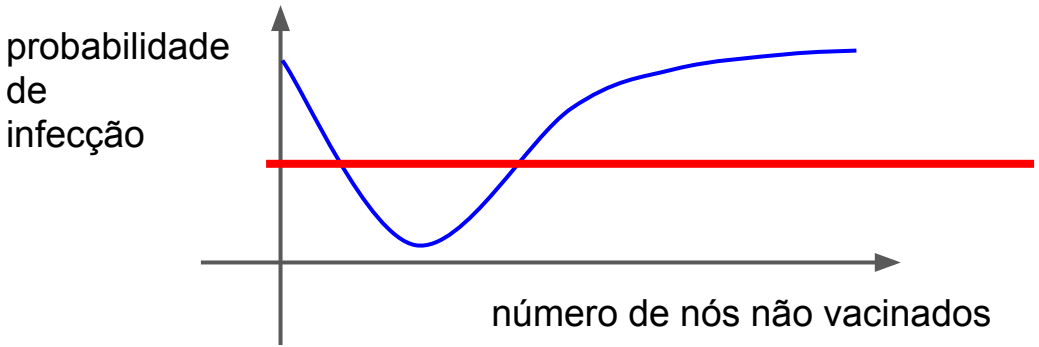


Modelo: número de equilíbrios

Quantos equilíbrios admite o sistema?

Teorema. O modelo simplificado admite no **máximo dois equilíbrios** além do equilíbrio trivial.*

Prova: mostramos que curvas abaixo cruzam em no máximo dois pontos



máximo 2
pontos de
interseção

* para condições, vide artigo

Contribuições e conclusão

1. Identificação do comportamento de usuários reais
   a. Os usuários seguem ou evitam a multidão?
2. Modelo analítico para capturar evolução de *malware*
   a. Tradeoffs: custos e benefícios de vacinação
   b. Modelo simplificado admite fórmulas fechadas para custos
3. Análise dos pontos de equilíbrio
   a. Qual a fração da população imunizada no longo prazo?
   b. Identificamos equilíbrios estáveis e instáveis para o sistema

Obrigado! [contato: queupe@gmail.com]