Cenário de Ameaças e Contexto de Segurança em TI para o setor de Educação

Gustavo Leite

Sales Manager - Symantec

Visão geral

Symantec.

Symantec.

Figure G.1

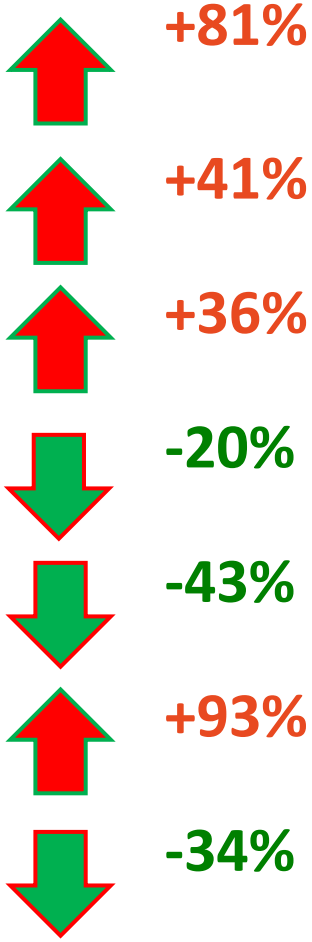
Malicious Activity By Source: Americas Rankings, 2011

Geography	2011 Region Rank	2011 World Rank	Region 2011 Malicious Code Rank	Region 2011 Spam Zombies Rank	Region 2011 Phishing Hosts Rank	Region 2011 Bots Rank	Region 2011 Network Attacking Geography Rank	Region 2011 Web Attacking Geography Rank
Brazil	1	4	1	1	1	1	1	1
Argentina	2	22	5	2	3	2	2	4
Colombia	3	28	3	5	2	7	5	5
Mexico	4	29	2	7	5	6	3	2
Chile	5	34	4	4	4	4	4	3
Peru	6	41	7	3	10	3	7	11
Venezuela	7	52	6	9	9	9	6	6
Dominican Rep.	8	54	9	6	25	5	9	15
Uruguay	9	61	20	8	15	13	8	9
Puerto Rico	10	73	11	17	20	8	10	13
Italy	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Indonesia	10		2.4%	28		0.7%	+1.7%	

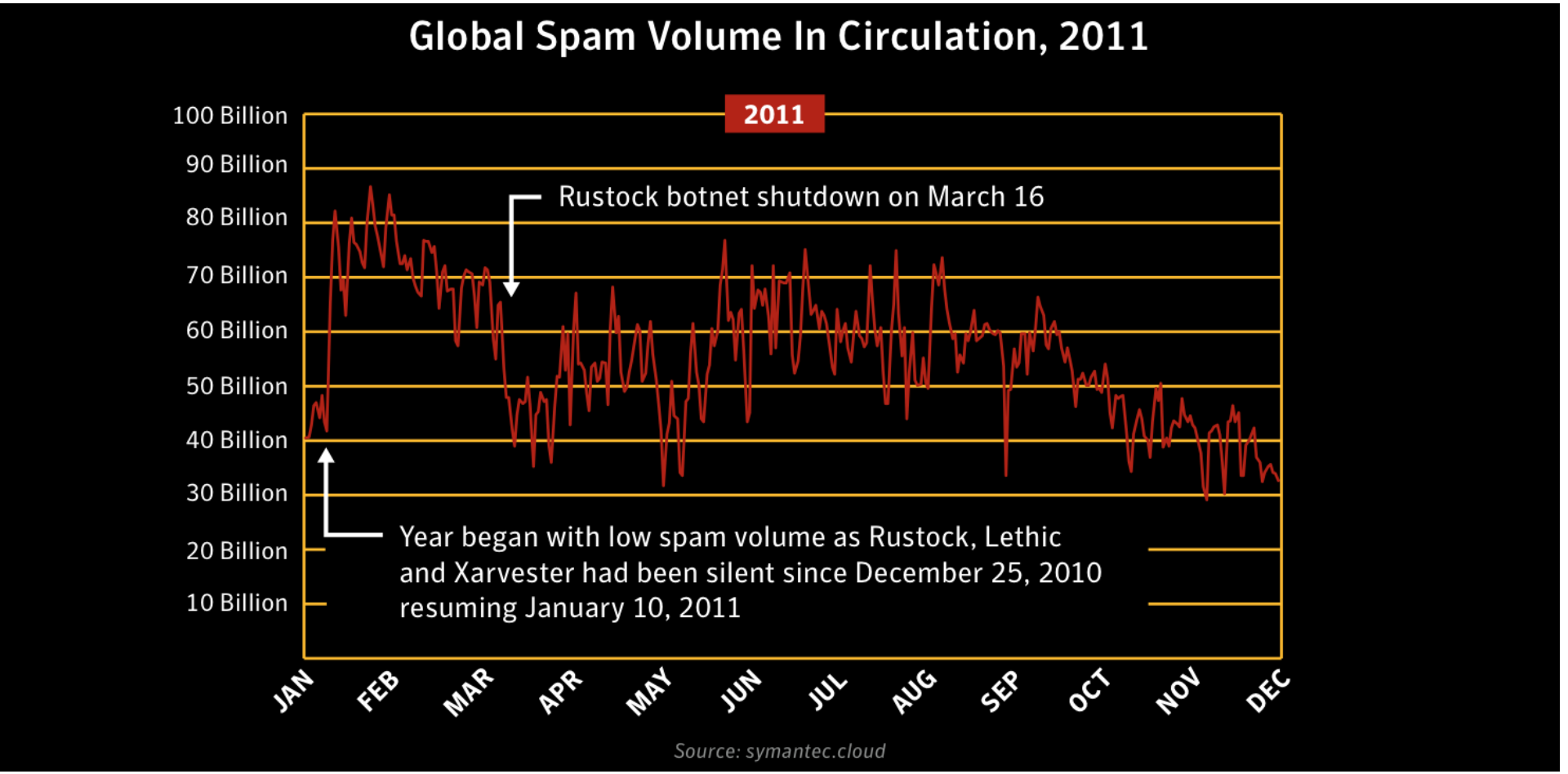
Source: Symantec

Números importantes de 2011

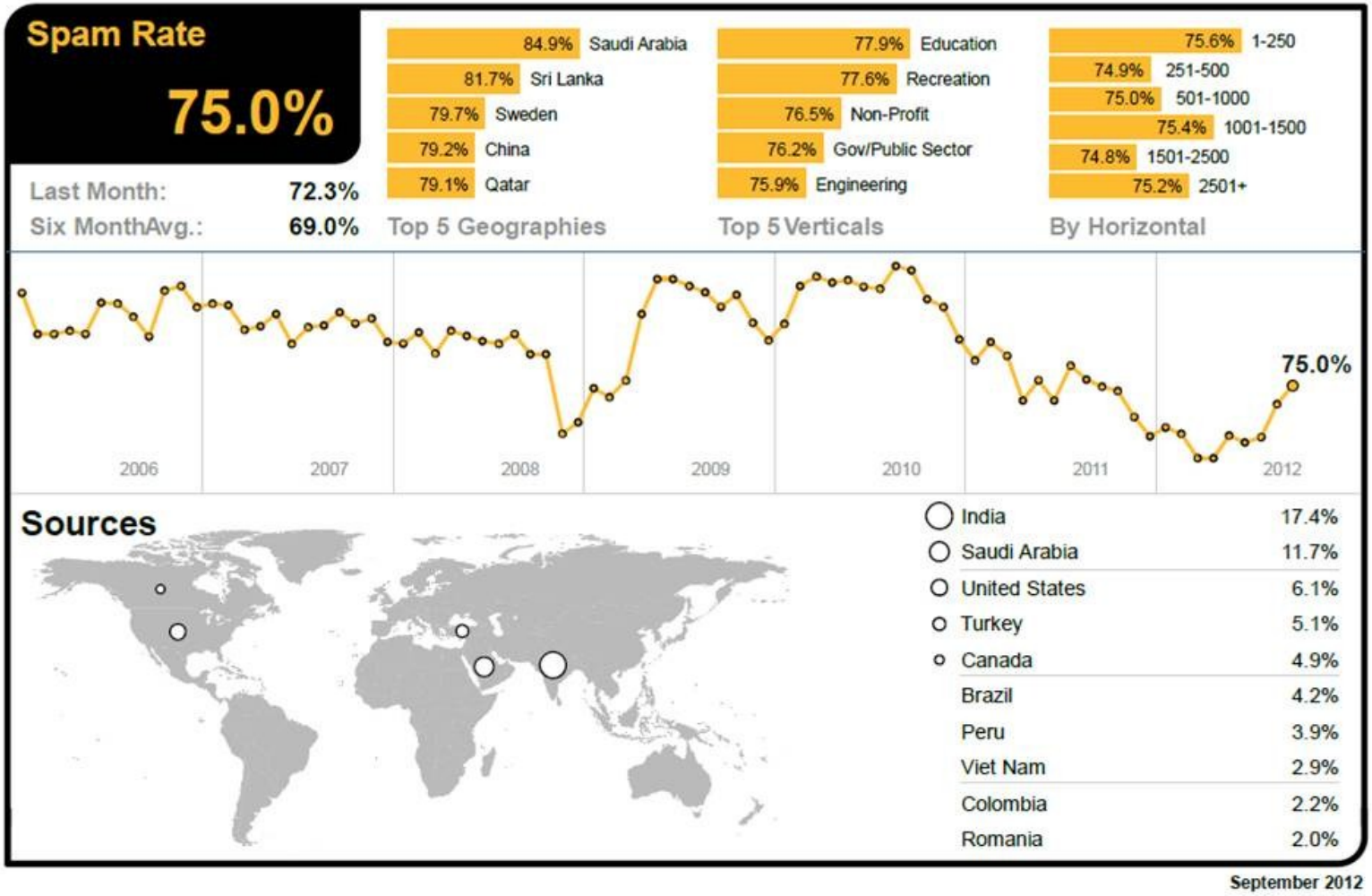
5,5B	Ataques bloqueados pela Symantec	+81%
403M	Variantes exclusivas de malware	+41%
4.597	Ataques Web por dia	+36%
4.989	Novas vulnerabilidades	-20%
8	Vulnerabilidades Zero-Day	-43%
315	Novas vulnerabilidades móveis	+93%
75%	Taxa de spam	-34%



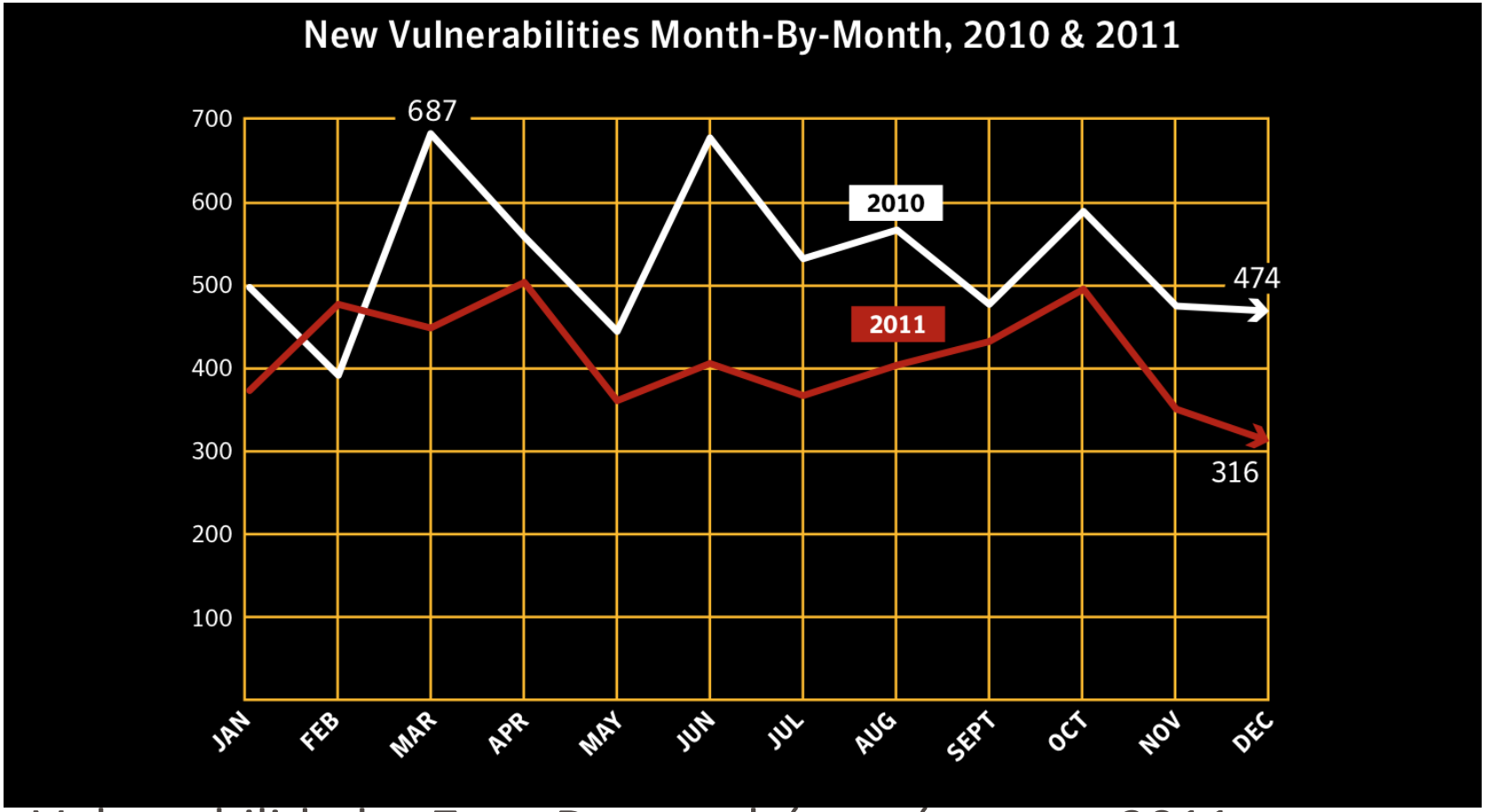
Spam ainda é eficaz, mas há mudanças em curso



O setor de educação é um dos que mais sofrem com SPAM



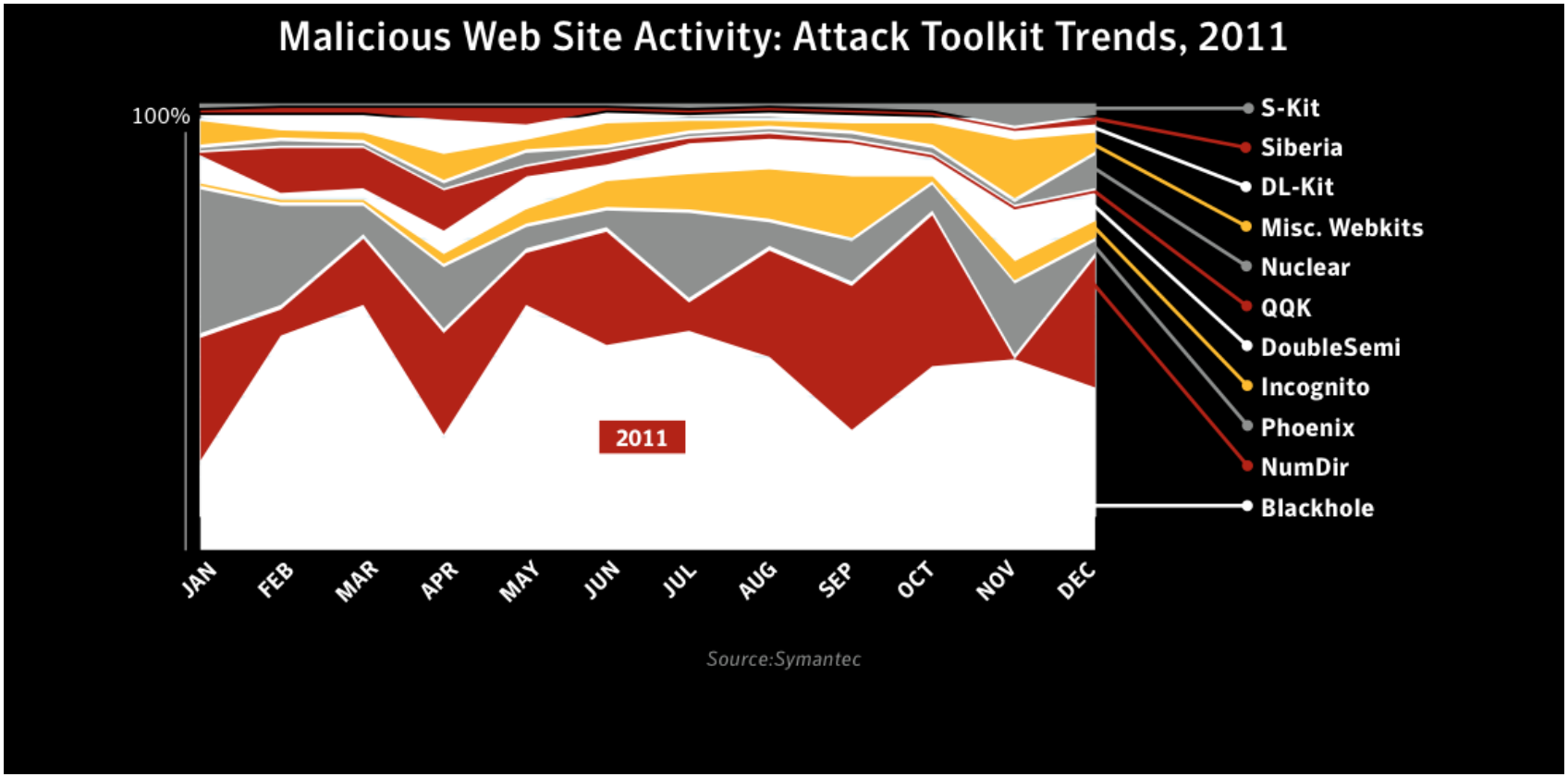
Vulnerabilidades não estão sendo descobertas à mesma taxa anterior



- Vulnerabilidades Zero-Day também caíram em 2011

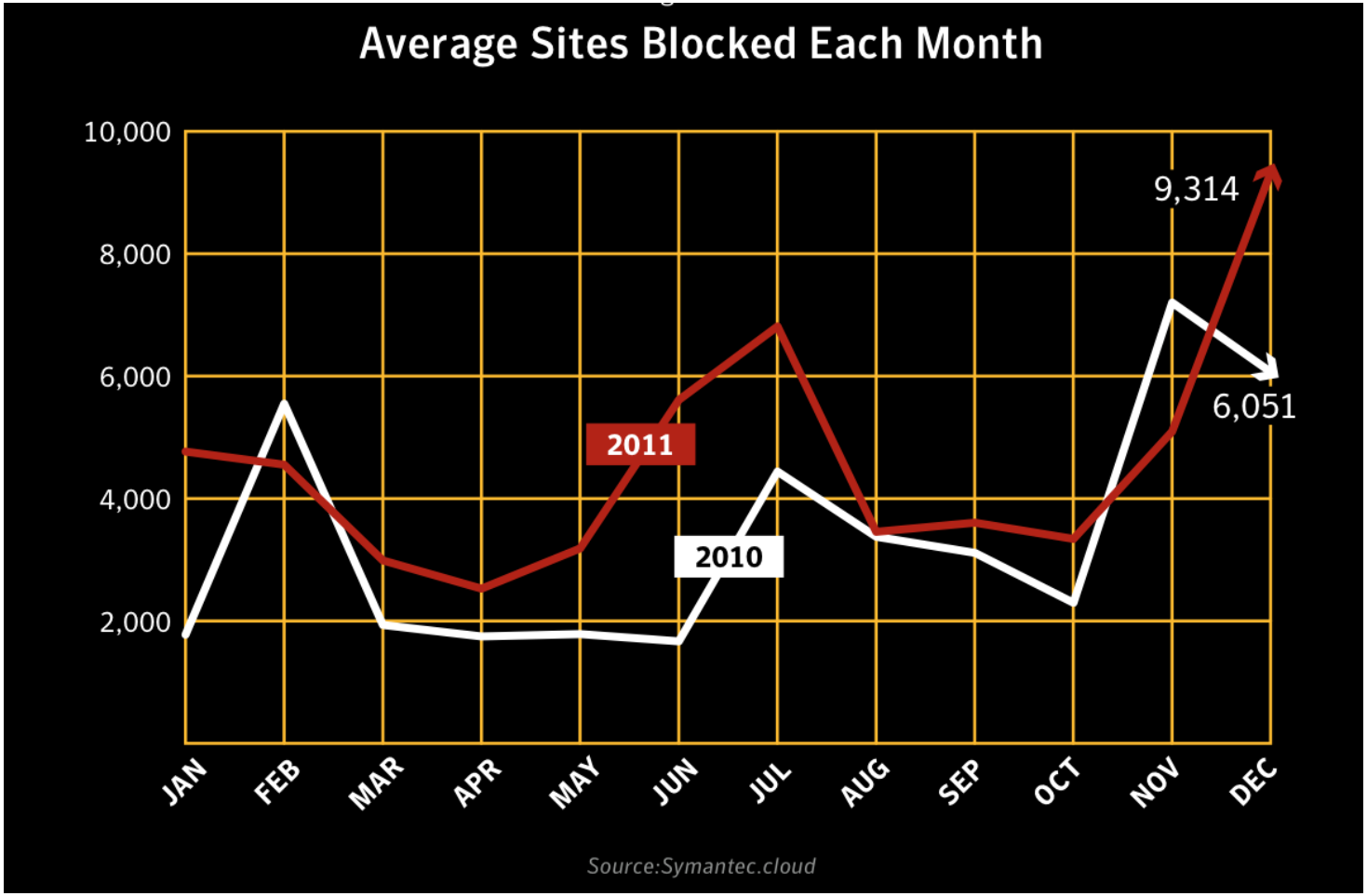
Por que malware continua crescendo?

- Continuam surgindo toolkits para ataques
- Maior eficácia para vulnerabilidades conhecidas



Por que malware continua crescendo?

- Ataques Web estão crescendo



Sites mais prejudiciais por categoria

Malicious Web Activity:
Malicious Code By Number Of Infections Per Site, 2011

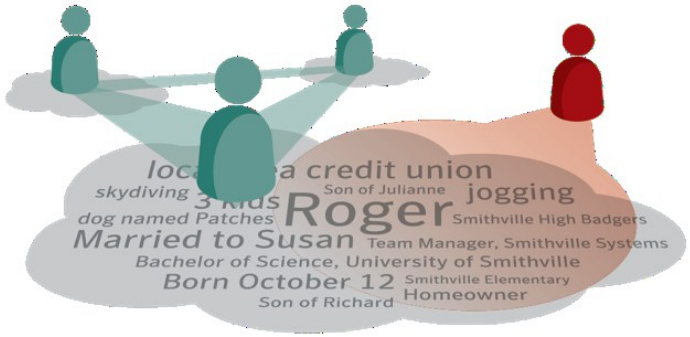
Rank	Categories Of Web Sites	Average Number Of Threats Found On Infected Web Sites	Major Threat Type Detected
1	**Religion/ Ideologies**	115	Fake Antivirus: 82%
2	**Hosting/ Personal hosted sites**	39	Trojans: 43%
3	**Pornography**	25	Trojans: 44%
4	**Entertainment and Music**	21	Fake Antivirus: 42%
5	**Business/ Economy**	17	Fake Antivirus: 62%
6	**Technology/ Computer and Internet**	17	Fake Antivirus: 54%
7	**Travel**	16	Fake Antivirus: 46%
8	**Sports**	13	Fake Antivirus: 69%
9	**Automotive**	11	Fake Antivirus: 41%
10	**Shopping**	9	Fake Antivirus: 63%

Source: Symantec

- Sites com baixo nível de segurança são alvos fáceis para autores de malware
- Algumas empresas compreendem que os clientes não visitarão sites que os infectam

Por que malware continua crescendo?

- Cibercriminosos estão se aproveitando das mídias sociais
  - Mídia social é viral por natureza – alunos são sociais por natureza
  - As pessoas suspeitam menos de conteúdos de amigos e de colegas



Malicious Web Activity:
Social Networking Attacks By Category, 2011

Rank	Category	# Of Social Network Threats	% Used To Deliver Social Network Attacks
1	**Blogs / Web Communications**	25,022	53%
2	**Hosting/ Personal hosted sites**	20,830	44%

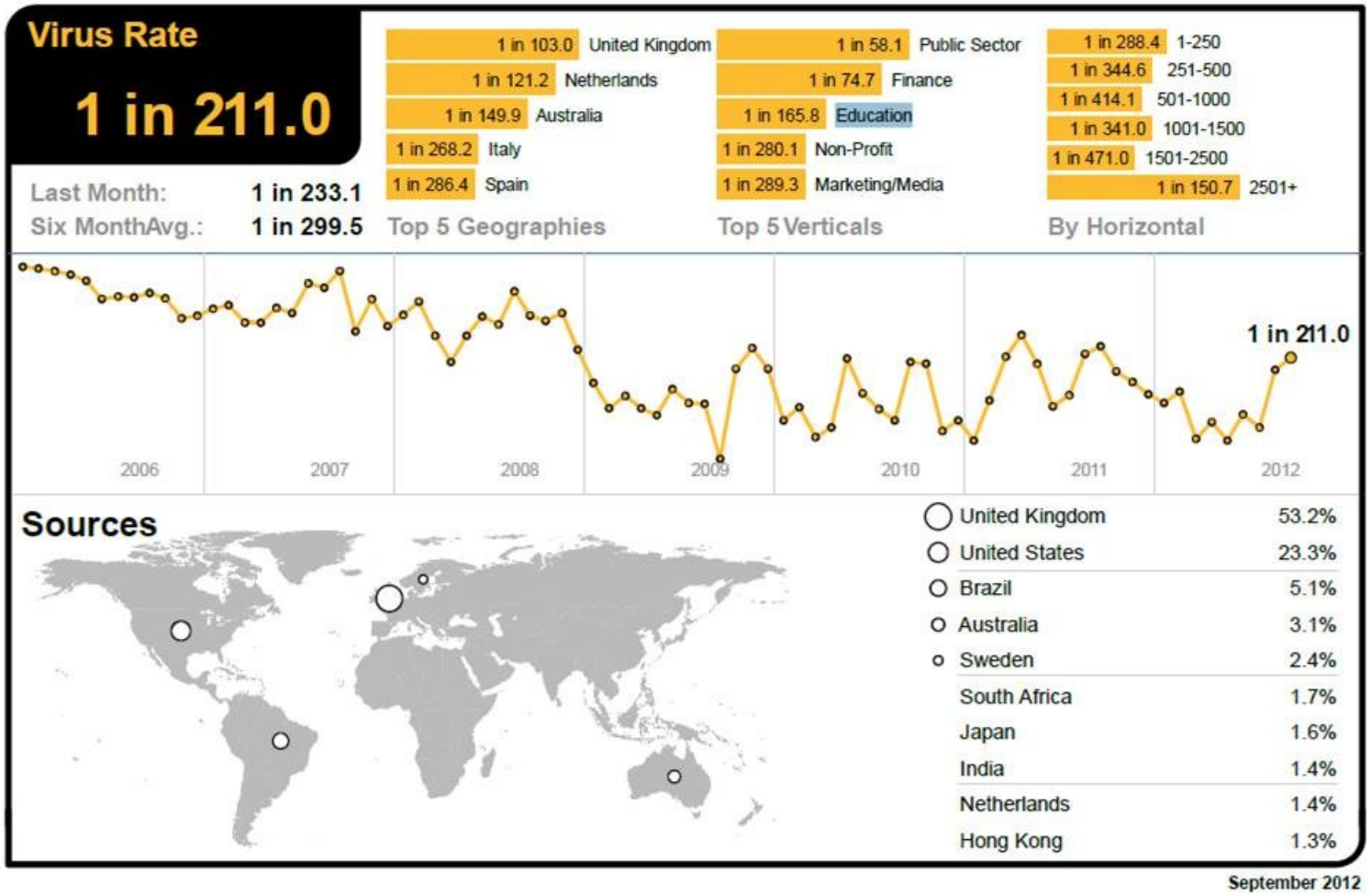
Source: Symantec

Engenharia social é eficaz nas mídias sociais

- Colegas dispostos a ajudar acabam se infectando

Ameaças por virus

O Setor Educacional sofre muito com ataques por virus



Ataques direcionados se expandiram

Ameaças direcionadas avançadas

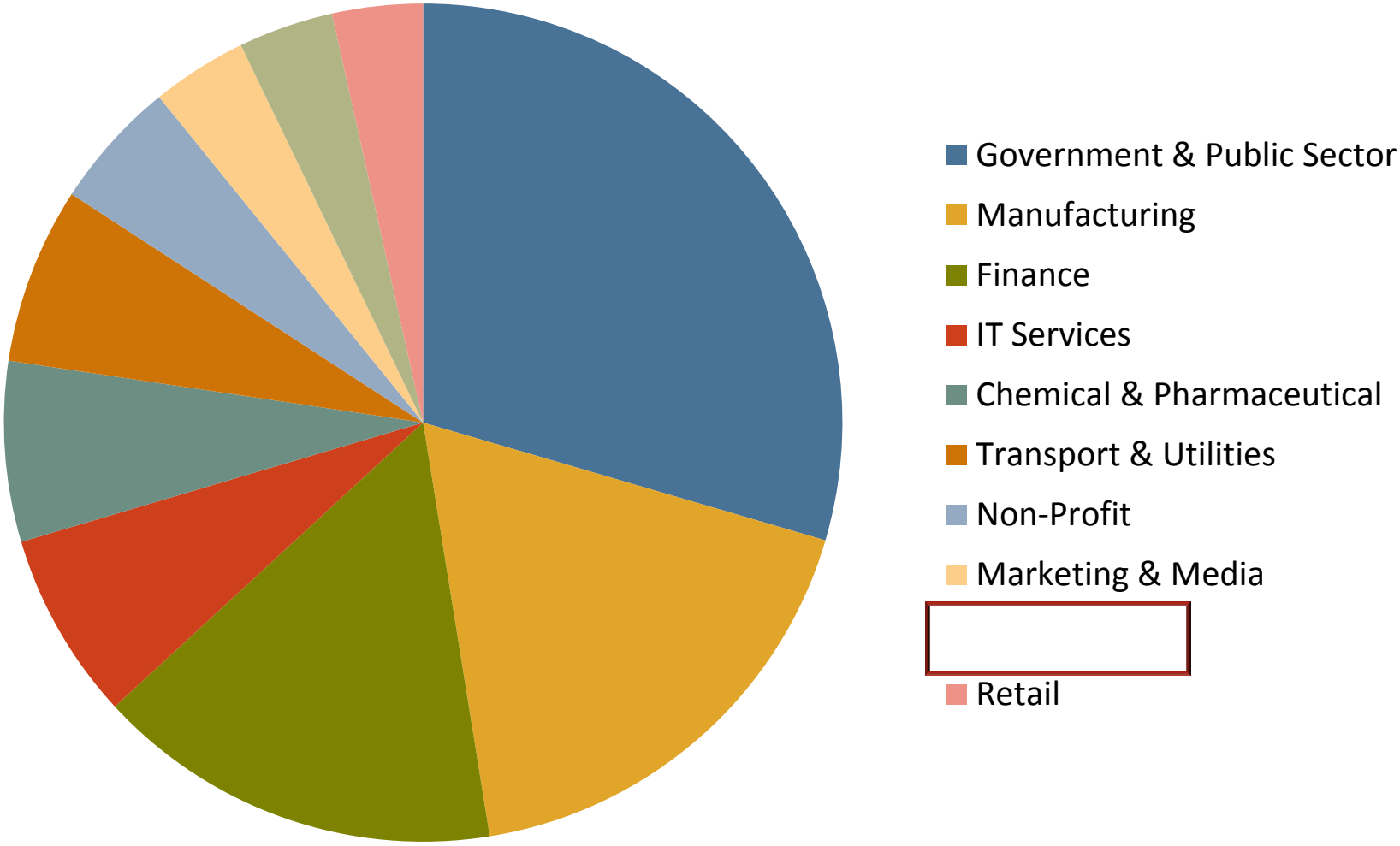
Suas suposições estão erradas

Suposição #1

Somente grandes corporações, governos e setor da defesa estão sendo alvos dos ataques.

Organizações de todos os portes correm o risco de ataques direcionados

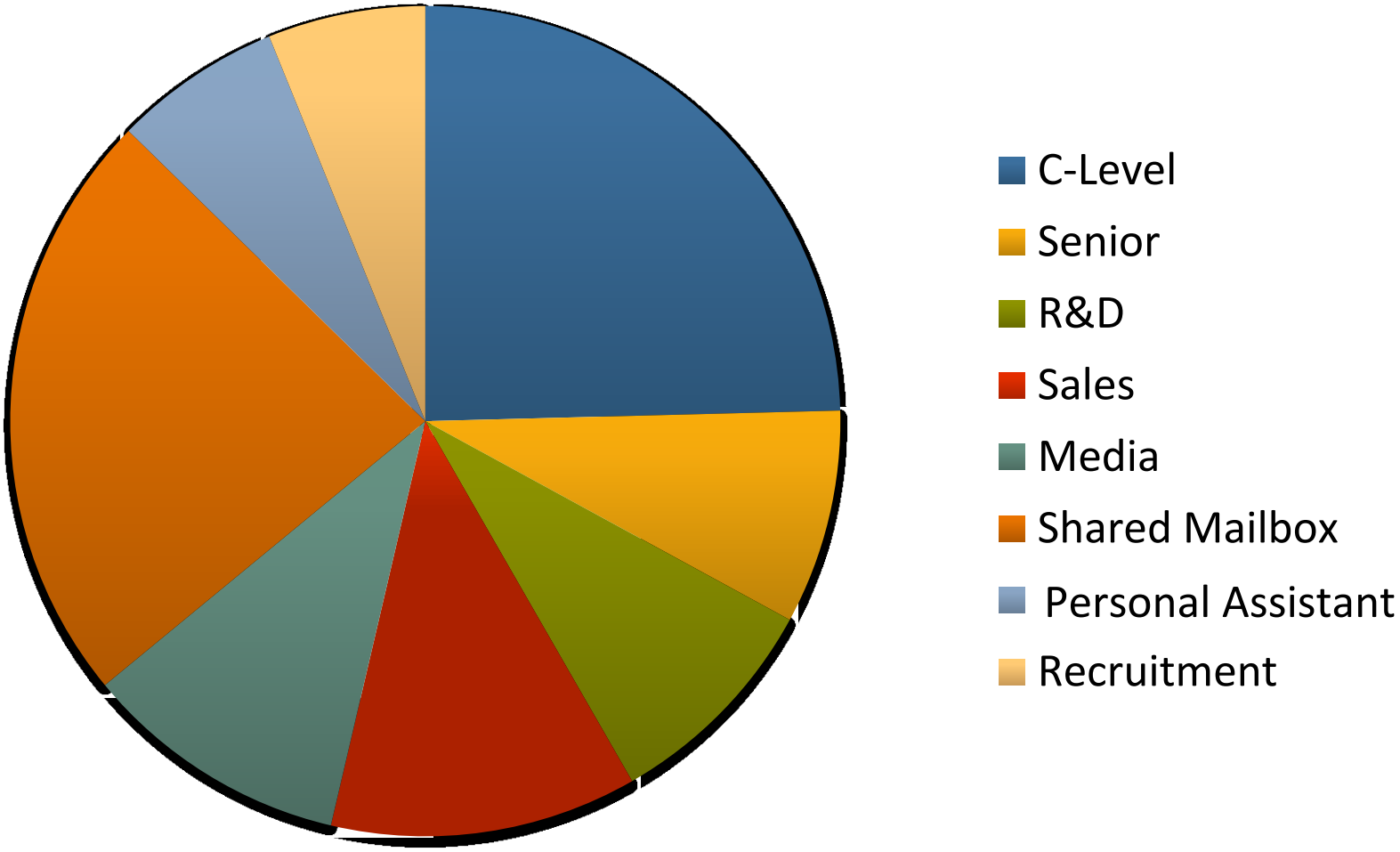
Ataques direcionados por setor



Suposição #2

Apenas CEOs e Gerentes Senior são alvos.

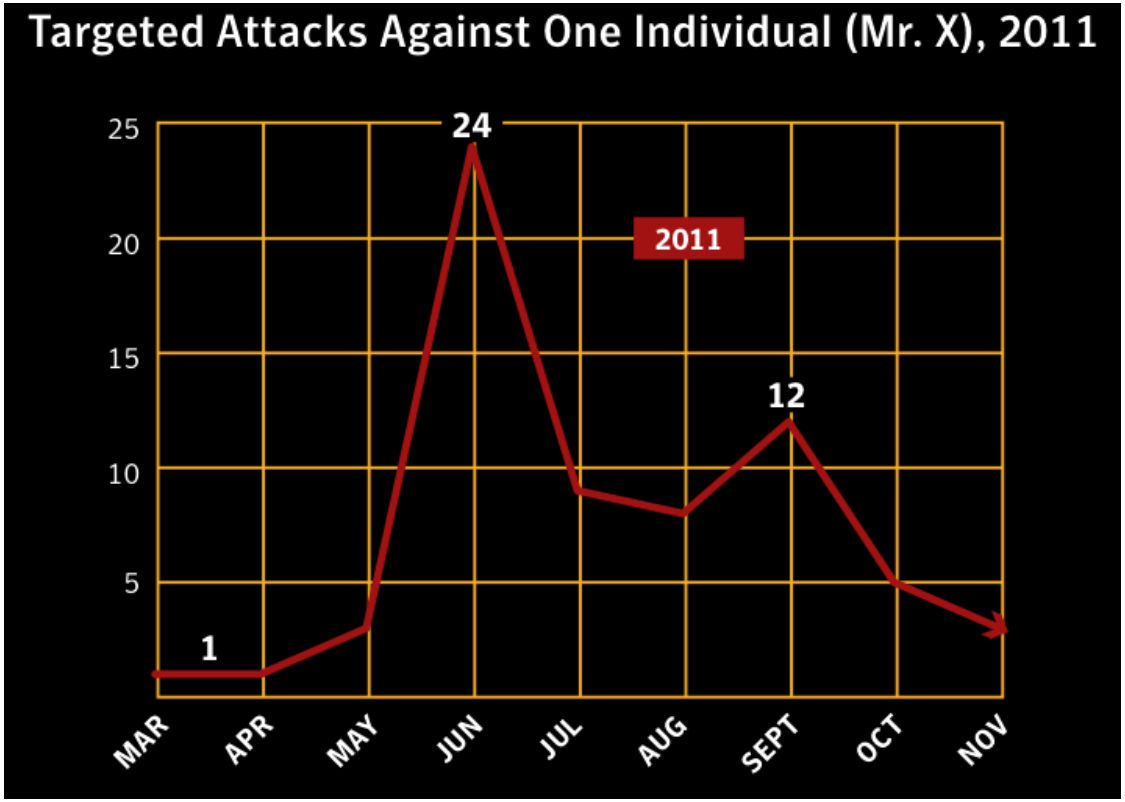
Ataques direcionados por função



Suposição #3

O ataque direcionado é um ataque único.

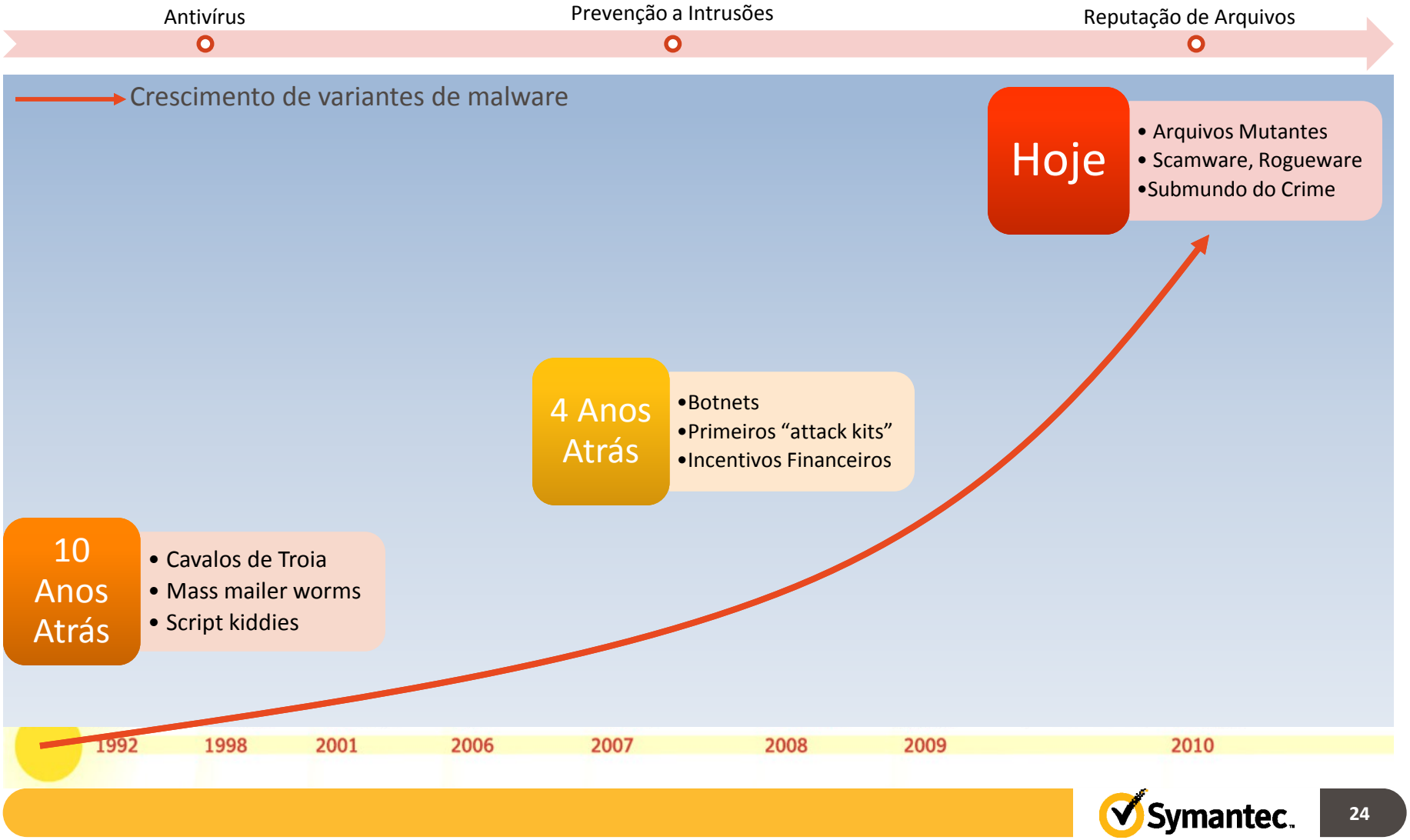
Estudo de caso: Taidoor



- Um alvo foi atacado por 9 meses seguidos
- Em junho, os ataques ocorreram praticamente uma vez por dia

É necessário um novo tipo de proteção...

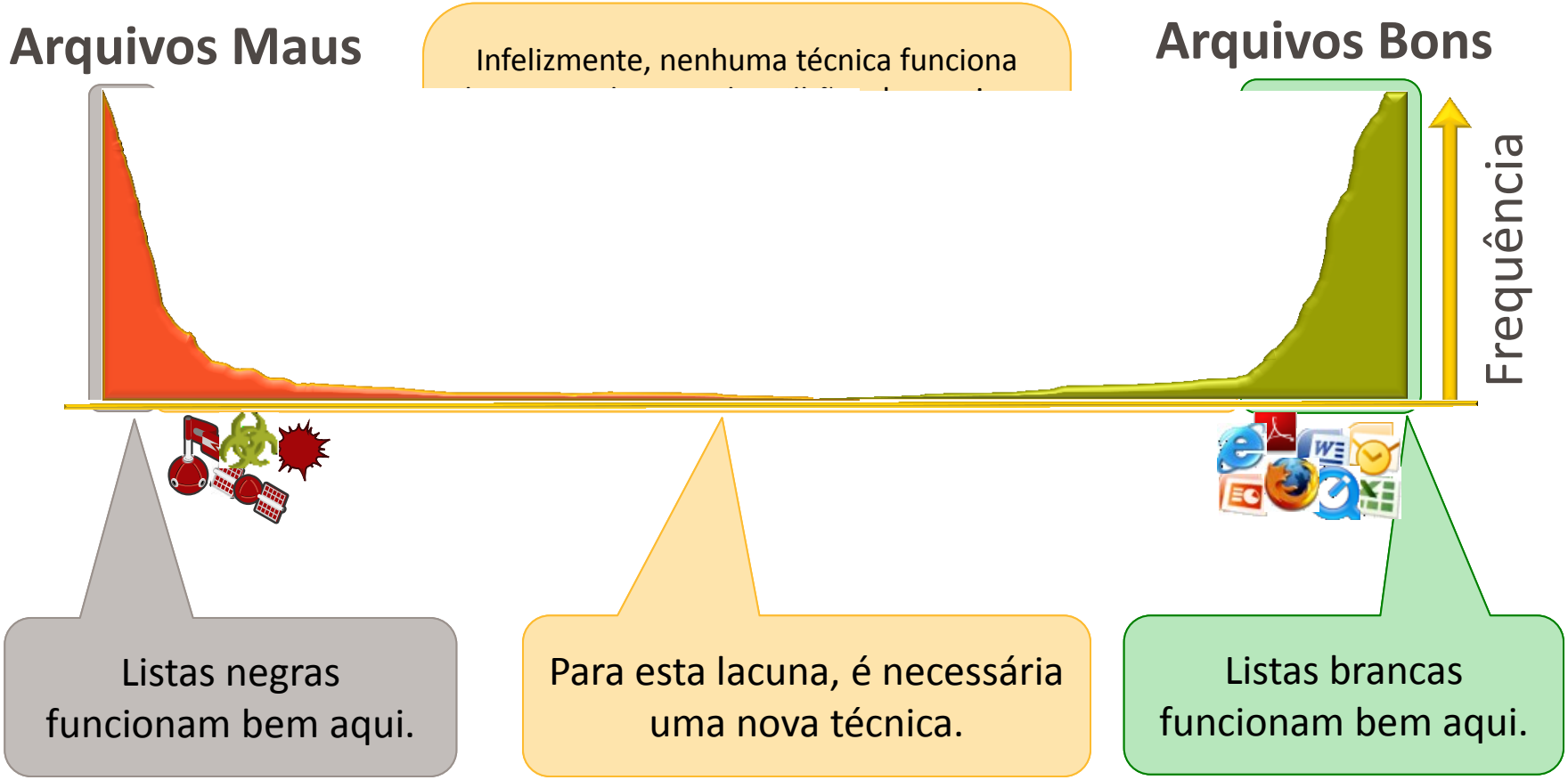
Hoje em dia, 75% dos malwares afetam menos de 50 usuários



*Amostras de preços em fóruns do underground

Proteção Baseada em Reputação...

Nenhuma proteção atual soluciona a chamada “Long Tail”



Um exemplo de Tecnologia que Inova: Proteção Baseada em Reputação

Proteção Baseada em Reputação

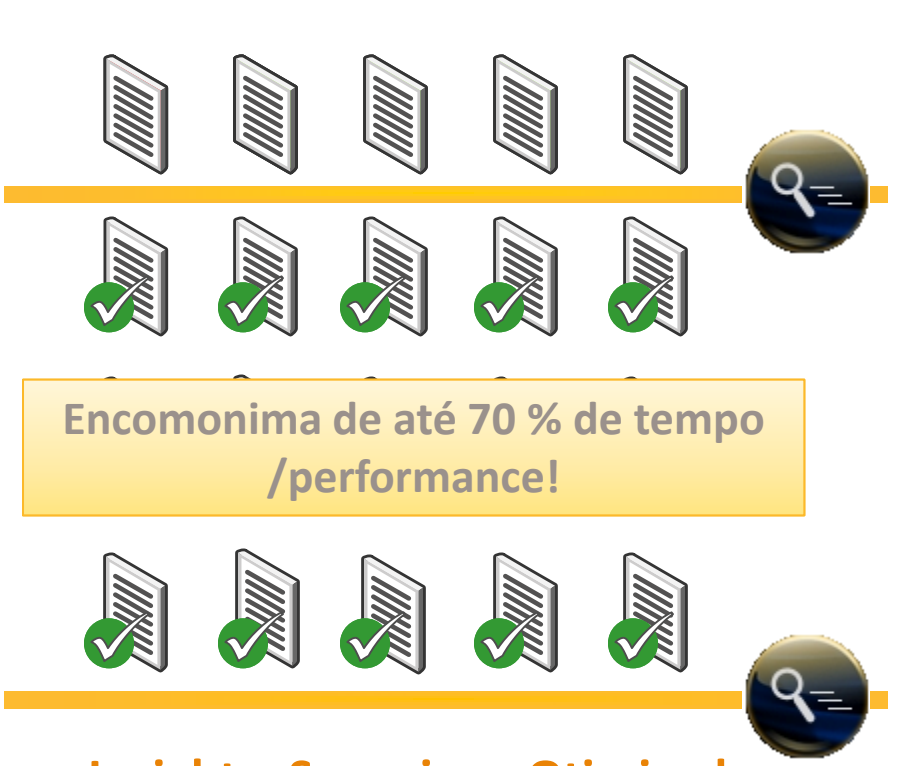
- Uma tecnologia revolucionária que oferece **proteção proativa** contra ameaças novas e direcionadas, por meio de classificações de segurança alimentadas por uma comunidade de mais de **175 milhões** de endpoints.
- Proteção Baseada em Reputação é a tecnologia incorporada ao Symantec Endpoint Protection que permite identificar uma possível ameaça por sua “reputação”.
- Utilizada em todo o produto
  - Download Insight
  - ScanLess
  - Monitoramento de comportamento de aplicações SONAR
  - Heurística e Corroboração durante a detecção

Como Funciona

Mais Rápida – “Powered by” Proteção Baseada em Reputação

Scanning Tradicional

Precisa scanear todos os arquivos



Insight – Scanning - Otimizado

Pula os arquivos com boa reputação, consequentemente scan mais rápido

‘Até agora vimos como manter as ameaças fora das empresas, passamos agora a analisar como garantir que as informações boas mantenham-se nas empresas’’

Complementando a Proteção

- Duas disciplinas que complementam a proteção do Endpoint
  - Prevenção contra vazamento de informação – DLP “Data Loss Prevention”
  - Criptografia de “Endpoint”

Proteção de Dados e **Vazamento de Dados** é um dos top 3 investimentos na área de segurança em 11.

- Deloitte Global Security Survey

380 **milhões de registros** foram roubados em 2011, mais do que a soma dos 3 anos anteriores

- PrivacyRights.org

O faturamento do Cyber-Crime ultrapassou o do narcotráfico em 2011.

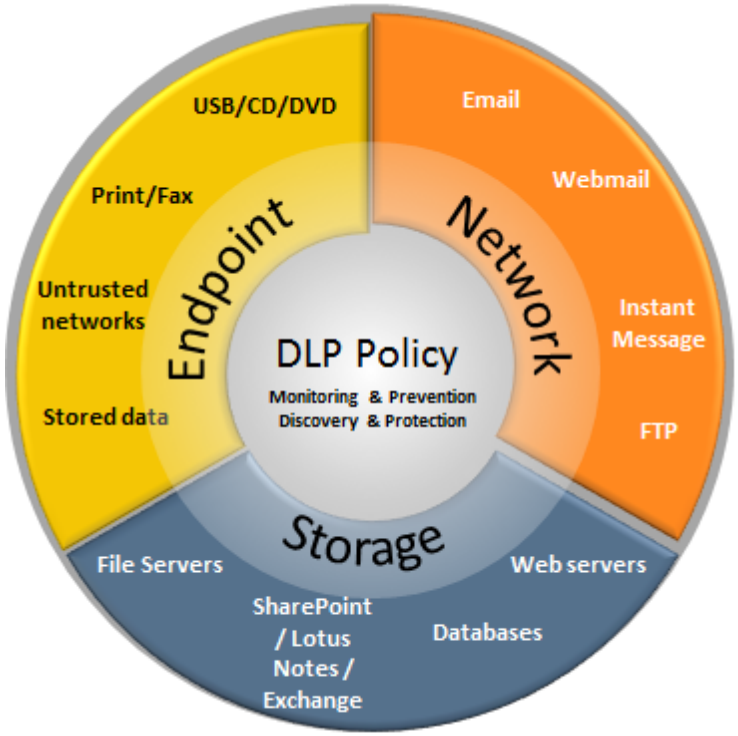
O Problema com os Dados

Dados estão por toda parte e são portáteis:

- Desktops e Laptops
- HDs de Computadores
- Dispositivos de armazenamento móvel, tais como CDs ou drives USB

Riscos para as Organizações:

- Perda de Dados e os custos associados



Dados em Risco coloca seu Negócio em Risco

Solução DLP

Você precisa mais do que uma solução de tecnologia.

Onde estão os seus dados confidenciais?

DESCUBRA

Como ele está sendo usado?

MONITORE

Qual a melhor forma para evitar a sua perda?

PROTEJA

Criptografia do “Endpoint”

Redução de Risco

- Protege contra perda , roubo e fins indevidos de computadores
- Reduz os riscos de perda ou roubo de dados confidenciais
- Possibilidade de destruição da máquina de forma remota
- Recursos para recuperação da máquina
  - Localização geográfica
  - Foto automática

Economia de Dinheiro e Tempo

- Reduz tempo e custo de conformidade com privacidade
- Credibilidade a marca
- Propriedade Intelectual protegida

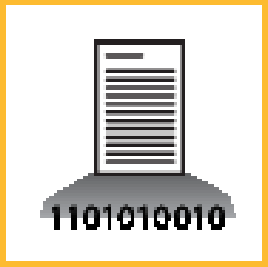
Criptografia + Data Loss Prevention

Network DLP / Email Gateway Encryption

- Cifra automaticamente emails contendo dados sensíveis
- Notifica funcionários em tempo real sobre as políticas de criptografia

Storage DLP / Shared Storage Encryption

- Descobre onde estão os arquivos contendo dados confidenciais e aplica criptografia automaticamente



Endpoint DLP / Endpoint Encryption

- Descobre dados sensíveis na máquina do usuário
- Proteje os dados copiados para dispositivos USB habilitando políticas de criptografia para dados sensíveis

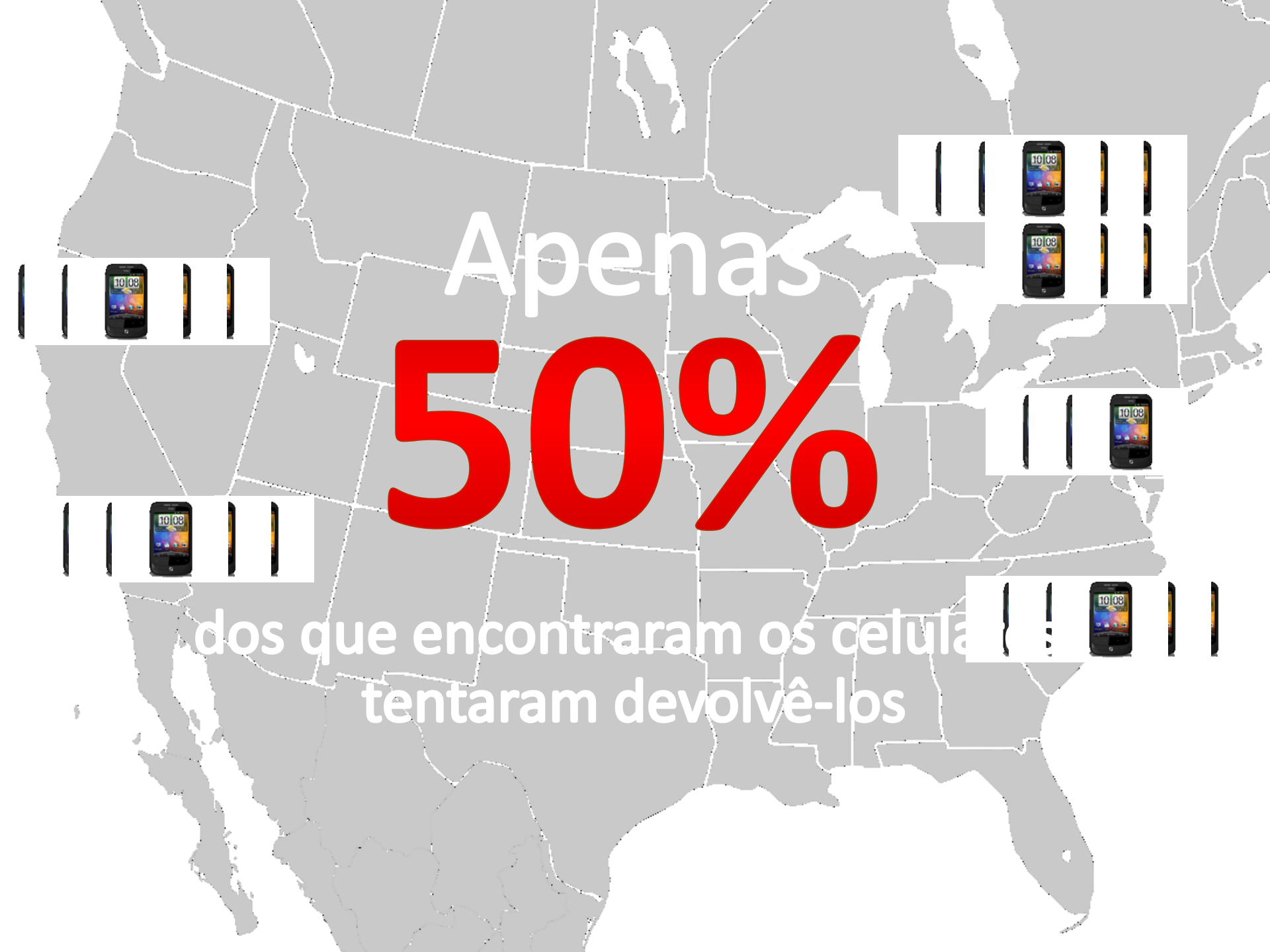
O setor educacional é um grande consumidor de Mobilidade

Celulares: Uma nova fonte de violações de dados

- Dispositivos móveis contêm informações profissionais e pessoais
- Ao contrário do que acontece com um computador de mesa, são facilmente roubados
- … e muitas vezes perdidos

Projeto Honey Stick

- Los Angeles
- São Francisco
- Washington, D. C.
- Nova York
- Ottawa, Canadá


Apenas
50%
dos que encontraram os celula
tentaram devolvê-los

96%

de **todos** os celulares

tiveram aplicações pessoais & profissionais acessadas

Mobile Protection

- Cobertura abrangente
  - E-mail
  - Web
  - Apps
- Aproveita as políticas DLP existentes
- Educa usuários
- Sandbox

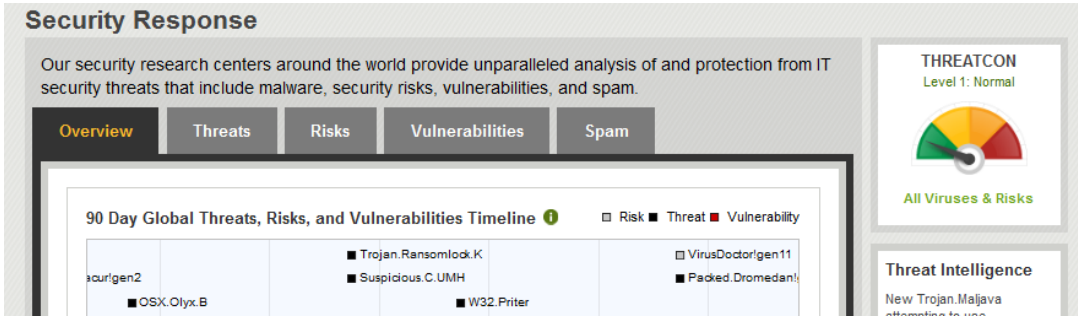
Data Loss Prevention, Criptografia e MDM Integrados

O que vem pela frente em 2012?

- Macs não são imunes a malware
  - O uso de Java em ataques multiplaforma foi discutido na edição 16 do Relatório
- Autores de malware vão capitalizar a mistura de vida profissional e pessoal nos dispositivos móveis
- Computação em nuvem e mobilidade vão forçar a TI a repensar a segurança

Mantenha-se informado

www.symantec.com.br/gin



Site Security Response

twitter

Twitter.com/threatintel

Thank you!

Gustavo Leite

gustavo_leite@Symantec.com