Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

José Henrique Pereira Branco

O ANO DE 2007 E AS PERSPECTIVAS TECNOLÓGICAS NO CENÁRIO GLOBAL DA SEGURANÇA DA INFORMAÇÃO

Rio de Janeiro

2009

José Henrique Pereira Branco

O ANO DE 2007 E AS PERSPECTIVAS TECNOLÓGICAS NO CENÁRIO GLOBAL DA SEGURANÇA DA INFORMAÇÃO

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Prof. Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil

Rio de Janeiro

2009

José Henrique Pereira Branco

O ANO DE 2007 E AS PERSPECTIVAS TECNOLÓGICAS NO CENÁRIO GLOBAL DA SEGURANÇA DA INFORMAÇÃO

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovado em Dezembro de 2009.

Prof. Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil

Rio de Janeiro

2009

AGRADECIMENTOS

Meus agradecimentos a todos que nas últimas décadas contribuíram para o desenvolvimento da tecnologia da informação e a utilização dessa no caminho de um mundo mais justo e igualitário.

RESUMO

BRANCO, José Henrique Pereira. **O ANO DE 2007 E AS PERSPECTIVAS TECNOLÓGICAS NO CENÁRIO GLOBAL DA SEGURANÇA DA INFORMAÇÃO.** Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2009.

Esse trabalho de pesquisa busca entender o fenômeno ocorrido no cenário global da Segurança da Informação em 2007 e entender as perspectivas tecnológicas dessa indústria, dado a crescente quantidade e qualidade de novas ameaças e comportamento dos ofensores ocorridos naquele ano. Através de pesquisas em organizações independentes e principais fabricantes de tecnologia de segurança da informação, analisamos o cenário global de ameaças em 2007, principais técnicas de defesa existentes, suas limitações, vantagens, desvantagens, como essas tecnologias e o mercado de segurança da informação estão tecnologicamente adaptando seus produtos e tecnologias frente às mudanças ocorridas em 2007. A pesquisa é descritiva e bibliográfica. Esse estudo não é definitivo, dado o aspecto evolutivo dos ambientes e sistemas de computadores. Assim sendo o objetivo secundário da pesquisa é incentivar outros estudiosos do tema a estender essa pesquisa, divulgar e compartilhar resultados para que o objetivo primário seja por sua vez amplamente satisfeito.

ABSTRACT

BRANCO, José Henrique Pereira. **THE 2007 YEAR AND TECHNOLOGICAL PERSPECTIVES OF THE GLOBAL IT SECURITY LANDSCAPE.** Monograph (Internet Technologies and Computer Networks Management Specialization). Núcleo de Computação Eletrônica, Federal University of Rio de Janeiro. Rio de Janeiro, 2009.

This research looks for to understand what happened in the global IT security scenery during 2007 year and the technologies perspectives of this industry due to the new attacker behavior, fast growing amount and quality of new threats. Trough a extensive research based on independent organizations and most important vendors of IT security we analyzed the 2007's global IT security threat landscape, current most important defense technologies, it's limitations, advantages and disadvantages, how those technologies and the IT security market are adapting their products and technologies to all changes happened during 2007. This research is descriptive and bibliographic. This research is not final by itself due to the fast changing and evolutionary environment of computer systems. Once this said, the secondary objective of this research is to encourage others to extend this research, broadcast and share its results, so the primary objective will be extensively reached.

LISTA DE FIGURAS

Página

LISTA DE QUADROS

Página

LISTA DE ABREVIATURAS E SIGLAS

B2B	Business to business, comunicação entre empresas via rede de dados
B2C	Business to customers, comunicação entre empresas e clientes via rede de dados
Firewall	Sistema de segurança de redes para controle da comunicação entre sub-redes
IPS	Intrusion Prevention System, sistema de segurança que bloqueia ataques detectados
IDS	Intrusion Detection System, sistema de segurança que detecta ataques, sem bloqueio
Logs	Arquivos ou base de dados que armazenam informações diversas sobre sistemas
Nessus	Sistema de IDS/IPS open source
Nagios	Sistema de inventário de computadores open source
OSI	Open System Interconnection, modelo de referência para protocolos de rede de dados
Payload	Carga útil do pacote, ou seja, o dado gerado pela aplicação ou serviço fim-a-fim. Que deve ser movimentado da origem para o destino e vice-versa
TCP/IP	Transmission Protocol / Internet Protocol, protocolo de comunicação para redes de dados
WEB	Programa de computador criado por Donald Knut, muito utilizado na internet

SUMÁRIO

Página

1 INTRODUÇÃO

Ataques a sistemas de computadores hoje estão entre as principais formas de violação a políticas de privacidade e fuga de informações corporativas bem como de indisponibilidade dos sistemas, causando prejuízos e danos tangíveis (ex: operacionais) e intangíveis (ex: imagem e reputação da empresa) muitas vezes incalculáveis às corporações alvo de tais ataques. [1]

A quantidade e qualidade de novas ameaças digitais é cada vez maior e melhor ano após ano, o que certamente impacta a detecção dos ataques [26,14]. Esse impacto certamente é refletido nas tecnologias que são utilizadas para detectar, alertar e até mesmo impedir tais ataques.

2007 foi um marco na história da segurança da informação [18]. Nunca foram identificadas tantas ameaças [14, 28]. O comportamento dos ofensores mudou definitivamente. Grandes redes de crimes cibernéticos foram identificadas e são realidade no cenário global [18 ,23, 28]. A criação de um mercado de software que vende produtos para desenvolvimento de código malicioso também virou realidade. Esse mercado vende seus produtos com suporte técnico, atualização de produtos, módulos de diversos níveis e tipos para escritas variadas de códigos [18].

As métricas utilizadas para demonstrar o fenômeno ocorrido no ano de 2007 são descritas no Referencial Teórico. As principais métricas utilizadas são: a quantidade de novas ameaças detectadas nesse ano e análise da mudança de perfil ou comportamento dos ofensores, ambas fornecidas pelos principais fornecedores de produtos para o mercado de segurança da informação e organizações internacionais independentes que estudam esse mercado.

Ainda no Referencial Teórico, do ponto de vista tecnológico, mostramos como as principais técnicas, de defesa e detecção de ameaças, comportam-se frente às mudanças dos ataques ocorridas em 2007.

Outra análise realizada é avaliar as atuais tecnologias e produtos frente ao ocorrido em 2007, que mudanças foram e serão realizadas nas tecnologias existentes e que novidades tecnológicas emergem. Buscamos com isso avaliar a perspectiva tecnológica em função do fenômeno ocorrido em 2007.

Esse trabalho de pesquisa busca entender o fenômeno ocorrido no cenário global da Segurança da Informação em 2007 e entender as perspectivas tecnológicas dessa indústria, dado a crescente quantidade e qualidade de novas ameaças e comportamento dos ofensores ocorridos naquele ano. Através de pesquisas em organizações independentes e principais fabricantes de tecnologia de segurança da informação, analisamos o cenário global de ameaças em 2007, analisamos as principais técnicas de defesa existentes, suas limitações, vantagens, desvantagens. Como essas tecnologias e o mercado de segurança da informação estão tecnologicamente adaptando seus produtos e tecnologias frente às mudanças ocorridas em 2007.

Não buscamos a causa raiz do fenômeno, buscamos somente entender suas características.

Esse estudo não é definitivo dado o aspecto evolutivo dos ambientes e sistemas de computadores. Assim sendo o objetivo secundário da pesquisa é incentivar outros estudiosos do tema a estender essa pesquisa, divulgar e compartilhar resultados para que o objetivo primário seja por sua vez amplamente satisfeito.

1.1 MOTIVAÇÃO

Estamos vivendo um momento sem precedentes na história da segurança da informação. A quantidade de novas ameaças utilizadas pelos ofensores (hacker) para invadir sistemas tem crescido substancialmente nos últimos anos e tende a continuar com esse mesmo comportamento. Além disso, significativas mudanças no perfil dos ofensores são também observadas [7, 8, 12, 15, 23, 24, 25, 26].

A principal motivação dessa pesquisa é verificar o que realmente ocorreu em 2007 no campo da segurança digital, suas características. Buscamos também entender, caso o fenômeno seja comprovado, como as atuais tecnologias e produtos do mercado de segurança da informação se comportam frente a esse novo cenário, bem como tecnologias que emergem frente a essa nova realidade global.

1.2 OBJETIVO

Saber se foi real o fenômeno já descrito, e caso esse seja confirmado, conhecer os desafios tecnológicos impostos pelo novo cenário mundial da segurança da informação, as mudanças das tecnologias existentes e novas tecnologias de segurança da informação que despontam frente a esse novo ambiente, e como a indústria da segurança da informação está endereçando tais mudanças para o presente e futuro próximo, consistem nos principais objetivos desse trabalho.

1.3 RELEVÂNCIA

Empresas de grande porte nos EUA perdem em média US$ 31 Milhões/ano com perda de receita e produtividade em função de ataques a sistemas [21], mantendo as devidas proporções, o resto do mundo também sofre tal impacto. Hoje vivemos um momento sem precedentes na história da segurança da informação, dada a grande quantidade de novas ameaças identificadas por ano, além da mudança de comportamento dos ofensores.

Entender como se defender no cenário acima descrito é de grande importância para as empresas e instituições mundo a fora. Tal entendimento leva a indústria de TI, universidades, pesquisadores e instituições afins a elaborar pesquisas, novas tecnologias e produtos que visam endereçar as necessidades tecnológicas necessárias ao momento atual e futuro próximo.

1.4 METODOLOGIA DE PESQUISA

A metodologia de pesquisa sugerida foi a que melhor encontramos para ter sucesso no estudo mesmo tendo ciência de suas limitações e dificuldades em função da forte característica evolutiva dessa área. Em função disso, esperamos que novos estudantes e profissionais da área se interessem pelo tema e aprofundem sua análise.

1.4.1 Tipo de Pesquisa

Em vias de estudar esse novo momento da segurança da informação adotamos o tipo de pesquisa descritiva. Descrevemos, portanto, as características do fenômeno e estabelecemos as relações entre as variáveis de tal fenômeno. Por meios bibliográficos procedemos com extensa coleta

de dados de fontes publica e internacionalmente reconhecidas e com forte expressão no segmento de segurança da informação.

1.4.2 Seleção dos Sujeitos

Os sujeitos dessa pesquisa são todos diretamente ligados na área da segurança da informação como: consultorias independentes, principais fabricantes de tecnologia para segurança digital, pesquisadores e escritores.

Muitos documentos foram consultados, muitas publicações avaliadas e após uma seleção de documentos, artigos e fontes de informação diversas, as fontes utilizadas nessa pesquisa foram aquelas que tratam diretamente dos objetivos desse trabalho, sem qualquer restrição a opiniões congruentes ou adversas.

Inclui nessa pesquisa as opiniões e visões das maiores consultorias independentes no segmento : Gartner Research, IDC, SANS Institute, Infonetics Research, SecurityFocus e Opus Consulting Group; maiores fabricantes de tecnologia na área da segurança da informação: CISCO, Juniper Networks, McAfee, Trend Micro, Symantec, Ironport, F-Secure; bem como escritores atuantes na área como : Leonardo Scudere, Joel Scambray, Elisabeth Zwick, Sandro Melo. A importância de tal abrangente pesquisa é reduzir a probabilidade de erro, confrontar opiniões e buscar trazer aquilo que realmente afeta a análise do escopo do trabalho.

1.4.3 Coleta e Análise de Dados

A coleta e análise dos dados foram realizadas por documentação indireta. Coletei dados das fontes já mencionadas que tratam o período de 2006 à

primeira metade de 2009, referente ao objeto da pesquisa. A exceção, contudo, são os documentos que esclarecem tecnologias já utilizadas no período anterior ao mencionado e que persistem em utilização até a data atual.

A interpretação dos dados é objetiva e direta. O fenômeno tratado ocorreu em 2007. Coletamos dados desse período, ou sobre esse período, para validarmos o fenômeno, verificarmos se foi isolado, e também apontarmos a perspectiva da indústria de segurança da informação caso comprovada a existência real do fenômeno.

1.4.4 Limitações do Método

Limitamos a pesquisa ao entendimento do fenômeno ocorrido em 2007, suas características, sem buscar a causa raiz desse fenômeno. Limitamos a análise de tecnologias e tipos de produtos aos diretamente impactados pelas mudanças detectadas no fenômeno citado, e que também são amplamente utilizados no mercado (padrão de mercado).

2**REFERENCIAL TEÓRICO**

2.1 O CENÁRIO GLOBAL DE AMEAÇAS DIGITAIS ATÉ 2007

Segundo a F-Secure, "Foram produzidos em 2007 tantos malwares quanto nos 20 (vinte) anos anteriores."[14]

"A proximidade do final de 2007 é um bom momento para refletir sobre o panorama atual de ameaças. Os últimos 12 meses compreenderam um ano recorde.", diz a McAfee. [23]

A figura 1 totaliza por ano, desde 2002 até 2007, as vulnerabilidades VoIP globalmente encontradas e documentadas pelo National Vulnerability Database do NIST (National Institute of Standards and Technology - USA). Observe como o gráfico dá indícios do fenômeno que estudamos. Compare 2007 com os anos anteriores e veja a expectativa do NIST para o ano seguinte, 2008.

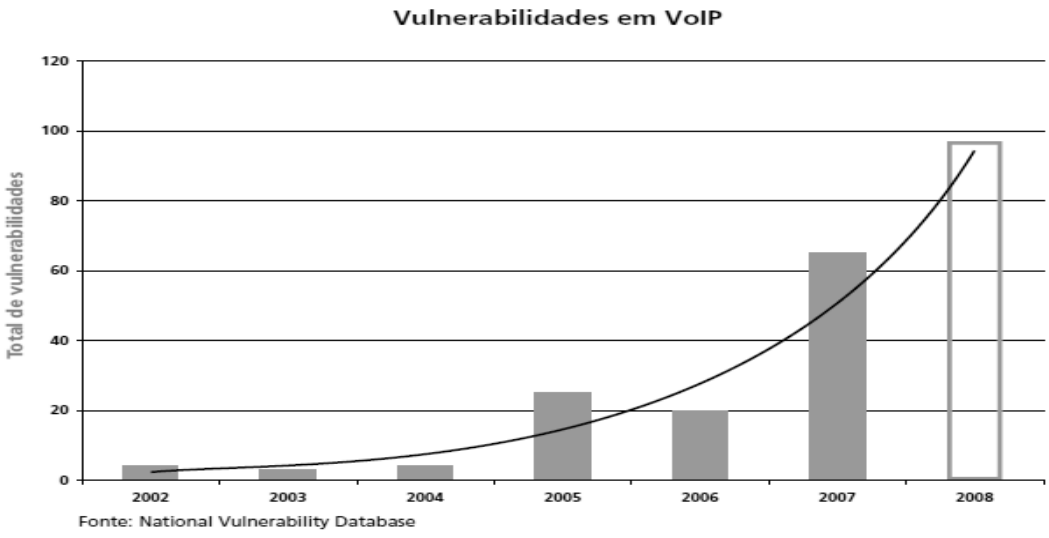

Figura 1 – Vulnerabilidades em VoIP (McAfee)

A figura 2 totaliza por ano, desde 1999 até 2007, vulnerabilidades em ambiente VMware globalmente encontradas e documentadas pelo National Vulnerability Database do NIST (National Institute of Standards and Technology – USA). Observe como o gráfico dá indícios do fenômeno que estudamos. Compare 2007 com os anos anteriores.

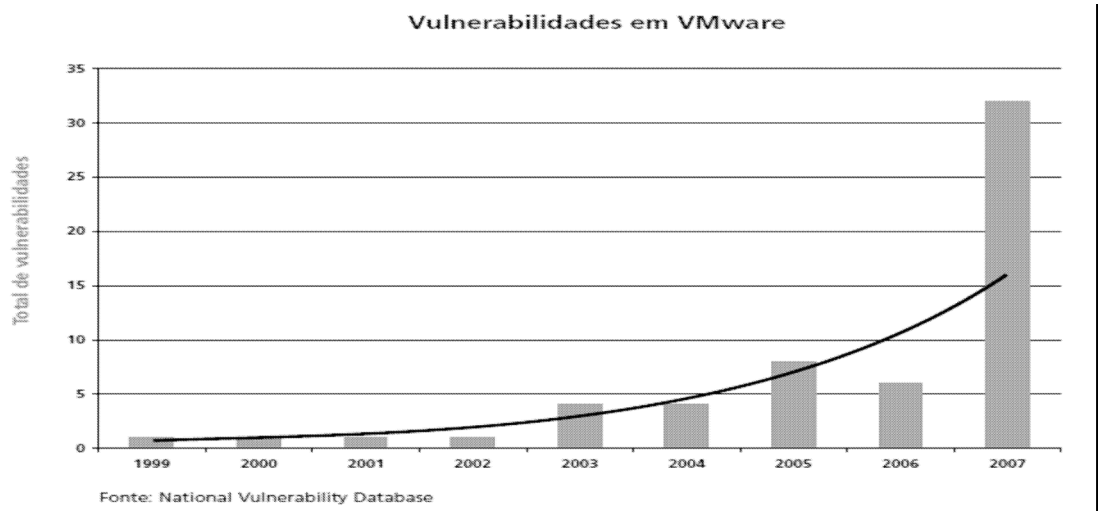

Figura 2 – Vulnerabilidades em VMware (McAfee)

A figura 3 totaliza por ano, desde 2005 até 2007, vulnerabilidades em ambientes de Mensagens Instantâneas globalmente encontradas e documentadas pelo National Vulnerability Database do NIST (National Institute of Standards and Technology – USA).

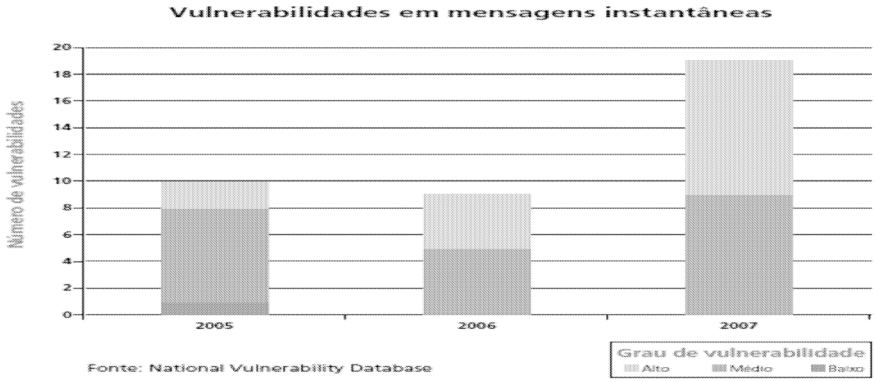

Figura 3 – Vulnerabilidades em Mensagens Instantâneas (McAfee)

"711.912 novas ameaças foram produzidas em 2007, 468% mais ameaças que em 2006. Isso significa que aproximadamente 2/3 de todos os códigos maliciosos atualmente detectados pela Symantec foram produzidos em 2007." [28]

A figura 4 totaliza por semestre, de 2002 até 2007, todas as ameaças globalmente encontradas e documentadas pela Symantec (maior fabricante mundial de segurança da informação). Mais de 65% das ameaças documentadas pela Symantec foram observadas em 2007.

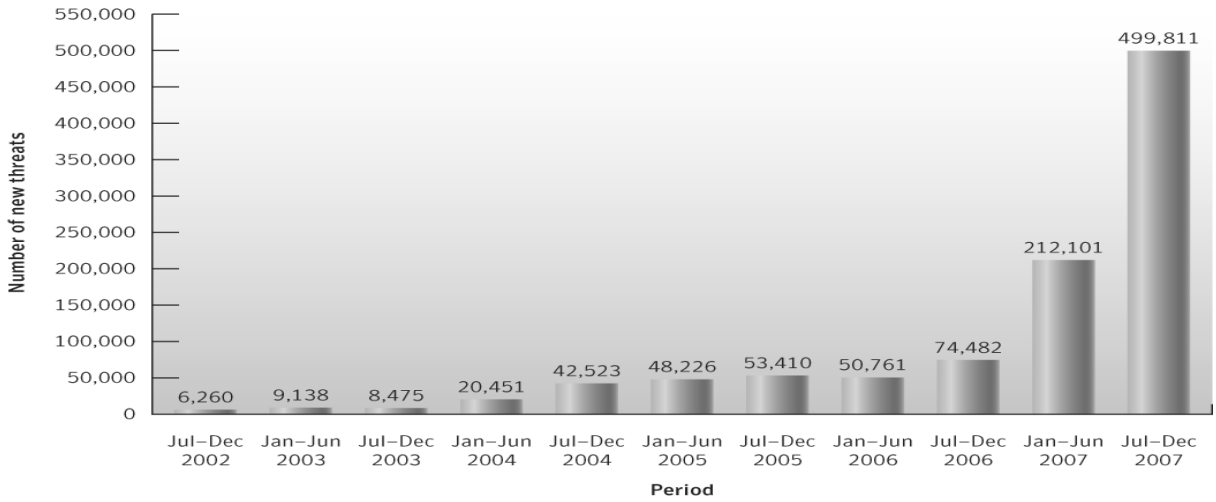

Figura 4 – Novas ameaças descobertas até o ano de 2007

"Em face às verdadeiras melhorias na segurança de redes e sistemas, atacantes têm agora dois principais alvos que os permitem invadir firewalls, antivírus e sistemas de prevenção de intrusão: usuários que são facilmente enganados e aplicações customizadas (aplicações internas das empresas). Essa é a maior mudança comparando aos anos anteriores em que os atacantes limitavam a maior parte dos seus destinos a falhas de softwares comumente usados.", diz o SANS Institute no ano de 2007. [25]

"A natureza dos ataques mais prejudiciais aos negócios mudou. Atacantes motivados por dinheiro não vão mais atrás de somente computadores sem patches; esses aumentos estão focando malwares que requerem mais do que simples detecção baseada em assinaturas."[8]

"Atacantes serão muito mais seletivos quanto ao alvo e a forma do ataque.". Disse o diretor de Pesquisa do Gartner em 2007 fazendo previsões sobre os próximos 12 a 18 meses.

O prejuízo anual por perda de produtividade e receita em função de falhas na segurança da informação para grandes empresas dos EUA em 2007 foi de aproximadamente US$30 milhões. Diz o relatório do Infonetic Research sobre ataques a empresas americanas em 2007.

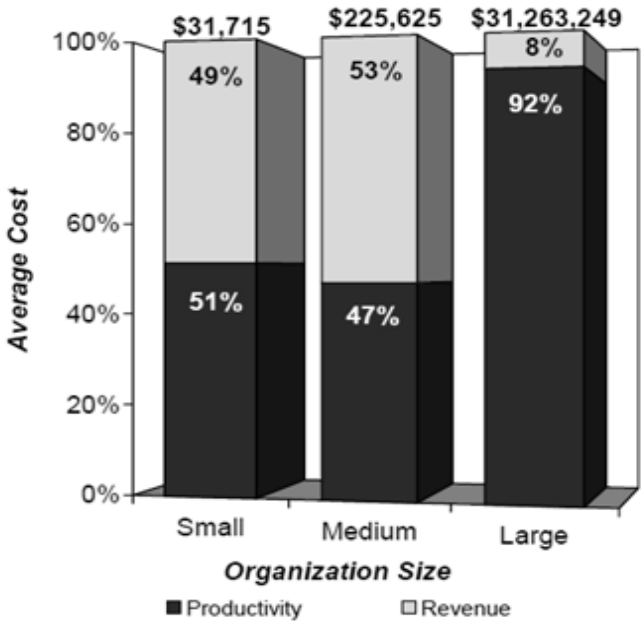

Figura 5 – Prejuízo anual por perda de produtividade e receita

"Nos anos anteriores os ofensores eram garotos que queriam ficar famosos atacando sistemas, derrubar esses sistemas, tudo para virar notícia. Agora o que se quer é dinheiro, porque há muito dinheiro na internet.". Disse Richard

Archdeacon, Diretor de Serviços Globais da Symantec, em entrevista para a Globo News em 2007.

"2007 é um marco. O tempo dos amadores acabou.". Diz o relatório da CISCO sobre Tendência de Segurança para Internet. [18]

Em 2007 um novo fenômeno ocorreu, nunca foram produzidos tantos códigos maliciosos, tantos malwares, tantos ataques sofisticados. Outro fenômeno foi a mudança do comportamento dos ofensores: dada a melhoria da segurança das redes e sistemas, eles estão mais precisos e focando em alvos mais específicos.

Todas as instituições e empresas que formaram a base para coleta e análise de dados desse trabalho são claras quanto às grandes mudanças no cenário global de segurança da informação que iniciou após 2007. Sistemas e técnicas de detecção e prevenção de ataques terão que se adaptar para proteger seus clientes e usuários, outras técnicas já são emergentes.

Mas o que efetivamente aconteceu em 2007?

Veja abaixo o que as instituições e empresas disseram durante ou após o fenômeno de 2007:

<u>Gartner</u>

"Mesmo o melhor banco de dados de assinatura pode não detectar ameaças relativamente novas a uma taxa de 2 a 10% e a maioria tem menos de 50% de chances de pegar ameaças totalmente novas.".[7]

"Detecção baseada em assinaturas são extremamente ineficientes contra ataques precisos (botnets) e ameaças do tipo zero-day."[7] [30]

No relatório do final do ano de 2006, sobre o mercado de IPS, o Gartner nem mencionou a necessidade de técnicas de detecção para ataques do tipo zero-day. No relatório de 2008 citou a mudança de comportamento dos ofensores e as ameaças zero-day bem como as focadas em alvos específicos.

"Tojans em função da web 2.0 serão muito normais" [12]

IDC

"A janela para aplicar patches em sistemas vulneráveis antes de surgir um exploit é cada vez menor e nós temos visto uma quantidade cada vez maior de ataques zero-day nos últimos 2 anos."[15]

McAfee

"Registramos mais de 100.000 novos vírus e cavalos de tróia. Phishing e zero-days também cresceram."[23]

"Redes de bots peer-to-peer certamente continuarão crescendo, como houve a explosão em 2007"[23]

"A adoção de novas tecnologias como VoIP, Virtualização e web2.0 fez também crescer o número de ameaças" [23]

"O Storm Worm cresceu e se transformou na maior rede de bots P2P da história, enquanto o cavalo de tróia TJ Max revelou a maior vulnerabilidade de dados da história."[23]

SANS

" Nós vimos crescimento significativo no número de vulnerabilidades nas aplicações do endpoint...e estão sendo massivamente exploradas em

estágio ainda selvagem, frequentemente pelo recrutamento de botnets."[25]

No ano anterior (2006) em seu relatório sobre as tendências sobre segurança para 2007 o SANS disse: "Vulnerabilidades zero-day irão resultar nas maiores epidemias em milhares de computadores infectados pelo mundo."[24]

"Aplicações web assim como aplicações domésticas das empresas foram responsáveis por quase a metade das vulnerabilidades descobertas no ano de 2007"

CISCO

"Proteção a Zero-Day vírus é uma camada essencial de proteção contra esses ataques que mudam rapidamente. Como observado em 2007."[18]

"As mudanças de 2007 podem ser ilustradas pela descoberta de self-defending : redes de bot e malware desenhados para serem reutilizados." [18]

"Em 2007 foi observado um crescimento significativo no número de epidemias que se espalharam por URLs ao invés do tradicional attachment no email. Um aumento de 253% sobre 206 essas epidemias por URL respresentam a tendência dos ataques que hoje procuram múltiplas formas de infectar o cliente. Normalmente essas URLs apontam para web servers infectados." [18]

"83% dos Spams de 2007 contém URL". No parágrafo seguinte o relatório da CISCO informa que ataques coordenados, com pequenas mensagens de spam, irão apontar o browser do usuário para outra máquina já infectada

que acabou de levantar um web Server. E então aquela estará infectada também com um Storm Trojan, aumentando assim a rede botnet. [18]

"Estudo do Google, liberado em Maio de 2007, analisou a presença de malware através de todas as paginas indexadas pelo Google. Foi reportado que 1(uma) em cada 10 (dez) páginas estão infectadas com código malicioso e que 70% (setenta por cento) das páginas infectadas encontradas, são web sites legítimos" [18]

"Virus não mais estão no cabeçalho dos relatórios, porque escritores de vírus evoluíram, vírus estão muito mais polimórfico e tipicamente associado com a proliferação de botnets bastante sofisticadas..."[18]

O relatório anual ainda informa que storm, feebs and clagger são as variantes de vírus com maior número de epidemias em 2007. E logo depois classifica feebs como worm.

"Vender malware ou exploits não é novidade, mas prover serviços e suporte é sem precedentes. MPack e o Dream Coders Team criaram um mercado provendo vendas de add-ons e oferecendo suporte para produtos que geram códigos maliciosos que eles vendem." [18]

Symantec

"A continuação do aumento de ameaças nesse período (2007) é principalmente atribuida ao continuado aumento de novos Trojans." [28]

"O significante aumento das novas ameaças do último ano (2007) é também indicativo da crescente profissionalização dos códigos maliciosos e a existência de organizações que empregam programadores dedicados na produção dessas ameaças" [28]. Leia-se: botnets.

"58% das vulnerabilidades documentadas na segunda metade de 2007 são relacionadas a aplicações web, na primeira metade representaram 61%" [28]

F-Secure

"Transações finaceiras continuam sendo o alvo preferido pelos criminosos. A quantidade de phishing continua a crescer, mas como os clientes dos bancos estão cada vez mais cientes desse tipo de crime, os criminosos começaram a utilizar novas técnicas mais sofisticadas. Um exemplo disso são trojans que utilizam métodos para se injetar diretamente nos browsers." [14]

"Enquanto nenhum malware verdadeiramente novo foi visto, os existentes foram refinados e adaptados para ter eficiência muito maior...Um exemplo de refinamento tecnológico foi a "Storm Worm" botnet." [14]

Trend Micro

"2007 realmente girou em volta das ameaças na web. Muitos ataques em organizações online, via web, sites comprometidos....A expansão e recente atividades do Nuwar botnet nos mostrou que as ameaças botnet cresceram seu tamanho, aumentando o risco de alvos potenciais."[29]

"O perfil dos autores de malware de fato mudou de tediosos jovens para criminosos empreendedores." [29]

Os relatórios não são precisos e nem sempre é possível confrontar seus números, mas principalmente os sumários e conclusões apontam para as seguintes grandes mudanças ocorridas no ano de 2007:

- O número de novas ameaças detectadas foi realmente muito fora da curva normal de crescimento. Foi histórico.

- Os ofensores não são somente mais aqueles jovens querendo brincar de derrubar sistemas, pichar páginas web e roubar os números de alguns cartões de crédito. Os ofensores de hoje são criminosos organizados, profissionais, com ataques precisos, ameaças de difícil detecção e estão atrás de muito dinheiro.

- O grande número de ameaças desse ano se deu em função de trojans e worms com ligação direta às botnets. A maioria das infecções iniciou por spams e páginas web comprometidas.

- Novas tecnologias como VoIP, Web 2.0 e ambientes virtuais ajudaram a aumentar o número de vulnerabilidades descobertas, mas grande parte das ameaças continuam sendo encontradas em antigos sistemas e aplicações, principalmente web.

Esse novo cenário mostra o definitivo surgimento de desenvolvedores profissionais de códigos maliciosos e o expressivo aumento desses, que por sua vez fazem códigos de mais difícil detecção, demandando por tanto uma adaptação ou melhoria das técnicas de detecção e prevenção de ataques.

Técnicas com base em assinaturas não mais são definitivos para proteger os computadores [7]. Técnicas de análise comportamental e utilização de diversas tecnologias de detecção são fundamentais. [15]

Após avaliarmos as perspectivas do cenário global de ameaças digitais para os anos seguintes, iremos verificar como a indústria de TI está se movimentando frente a esse novo cenário.

2.2PERSPECTIVAS DO NOVO CENÁRIO GLOBAL (2008)

Conforme a figura 6, podemos observar que o fenômeno ocorrido em 2007 continua a refletir nas estatísticas de 2008, e provavelmente terá o mesmo comportamento nos anos seguintes.

A Symantec detectava em média 5 novas ameaças/dia no ano 2000. E permaneceu com crescimento padrão até 2007, quando passou a detectar em média de 1430 novas ameaças/dia por todo o globo. Em 2008 a Symantec reporta em seu Symantec Internet Threat Report XIV, taxas de detecção de 12.000 novas ameaças/dia. [31]

A Symantec criou cerca de 800.000 assinaturas em 2007 e cerca de 1.700.00 novas assinaturas em 2008. [31]

Se o que aconteceu em 2007, em termos de novas ameaças, representou mais que o somatório dos 20 anos anteriores da história da segurança da informação, em 2008 não foi muito diferente. Somente para a Symantec, 60% das novas ameaças detectadas em sua base dados foram detectadas em 2008.

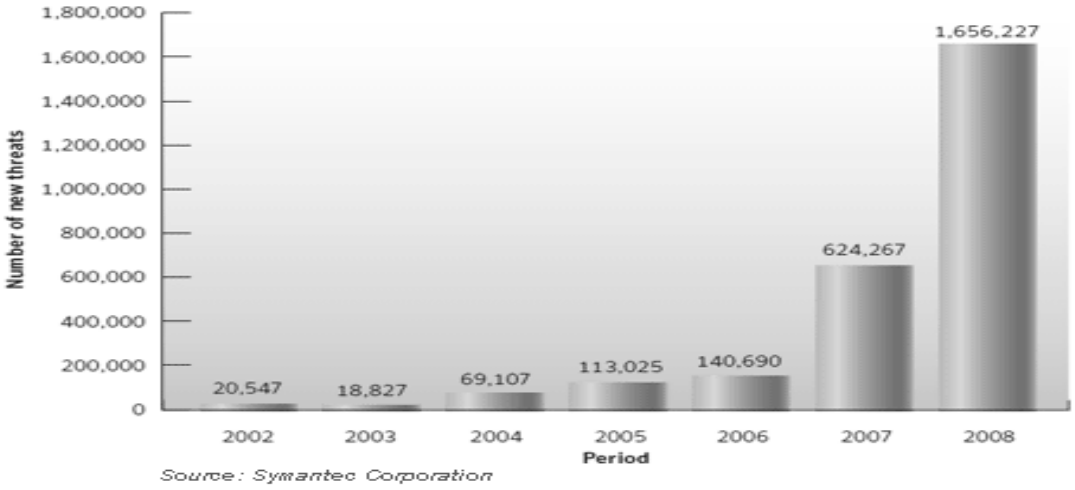

Figura 6 – Novas ameaças descobertas até o ano de 2008

Para reforçar, a McAfee diz em seu relatório sobre 2008 e previsões para 2009, que apesar de ter identificado somente em 2007 quase 40% dos códigos maliciosos que identificou nos últimos 15 anos (exceto 2008), apenas no primeiro trimestre de 2008 já havia identificado a mesma quantidade de todo o ano de 2007. [32]

O mesmo relatório da McAfee também diz que os códigos maliciosos ainda têm o mesmo padrão de 2007: eles são difíceis de identificar (stealthy), escritos com propósitos bem definidos, e a grande parte busca formas de fazer seu dono ganhar dinheiro. O relatório afirma que 90% dos códigos maliciosos escritos hoje são trojans e downloaders com o único objetivo de roubo de dados. Confirmando outra mudança na característica do ofensor, conforme identificado em 2007, de escritor de vírus para criminoso cybernético. [32]

Ainda segundo o relatório, em 2008, os ofensores continuam basicamente com o mesmo comportamento da mudança de perfil observado em 2007. Suas táticas, focos e formas de ataques seguiram, com pouca variação, as mudanças observadas em 2007. Um exemplo claro disso é a Figura 7, que mostra os principais alvos da indústria para ataques de roubo de dados.

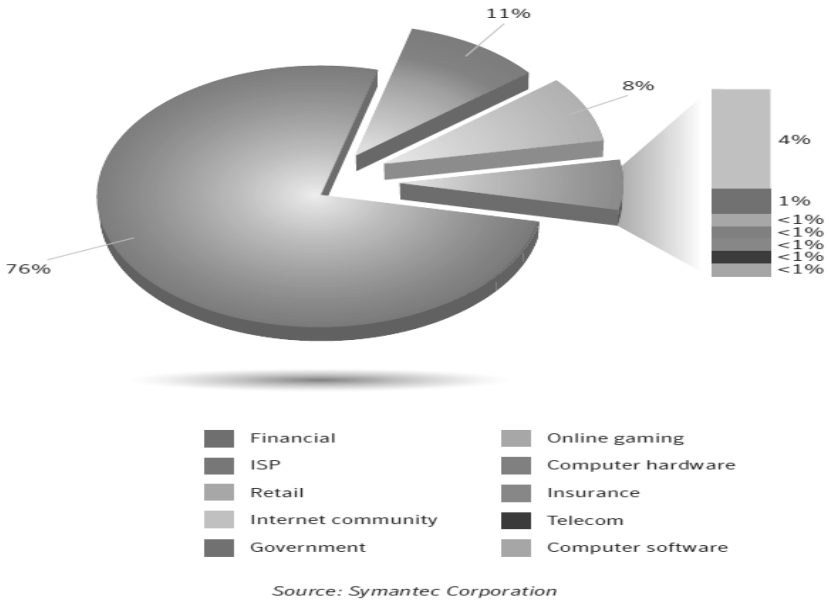

Figura 7 – Principais setores atacados em 2008

Outro grande fator que levou ao fenômeno de 2007 voltou a ocorrer em 2008: o crescimento das redes de crimes cibernéticos (underground economy). Com poucas mudanças em seus interesses, como retrata o quadro de preços de compra desse mercado. Nesse mesmo quadro podemos ver os itens que mais interessavam ao ofensor em 2007 e em 2008. [31]

Quadro 1 – Preços dos itens a venda no underground e seus principais interesses

2008 Rank	2007 Rank	Item	2008 Percentage	2007 Percentage	Range of Prices
1	1	Credit card information	32%	21%	$0.06–$30
2	2	Bank account credentials	19%	17%	$10–$1000
3	9	Email accounts	5%	4%	$0.10–$100
4	3	Email addresses	5%	6%	$0.33/MB–$100/MB
5	12	Proxies	4%	3%	$0.16–$20
6	4	Full identities	4%	6%	$0.70–$60
7	6	Mailers	3%	5%	$2–$40
8	5	Cash out services	3%	5%	8%–50% or flat rate of $200–$2000 per item
9	17	Shell scripts	3%	2%	$2–$20
10	8	Scams	3%	5%	$3–$40/week for hosting, $2–$20 design

Goods and services available for sale on underground economy servers
Source: Symantec

A Symantec ainda encontrou uma média de 75.000 computadores infectados por bot-nets por dia em 2008. Um aumento de 31% comparado a 2007. As bot-nets foram um dos principais fatores apontados no fenômeno de 2007.

As maiores quantidade de ameaças em 2008 continuaram a endereçar serviços web, novas tecnologias e legados.

Com base nessas informações podemos prever que 2009 não será muito diferente. As mudanças ocorridas no cenário global de ameaças digitais repercutiram por 2008 e devem afetar também as estatísticas de 2009.

Agora vamos avaliar como a indústria de TI está se movimentando frente a esse novo cenário.

2.3 ATUAIS MÉTODOS DE DETECÇÃO

As atuais tecnologias de proteção contra ataques basicamente trabalham em quatro níveis: nível de pacotes, nível de sessão, nível de aplicação e nível de arquivo. São basicamente 4 (quatro) as principais tecnologias que utilizamos para nos defendermos de ataques: ACL, Firewall, IPS e Anti-vírus. Vamos verificar como essas tecnologias se comportam frente ao novo ambiente já descrito

Quadro 2 – Comparação das categorias de tecnologias de segurança

	Proteção ao nível de Pacotes	**Proteção ao nível de Sessão**	**Proteção ao nível de Aplicação**	**Proteção ao Nível de Arquivo**
Exemplo	Filtro de Pacote (ACL de Router ou "stateless" firewall)	"Statefull Inspection" Firewall	(Host) IPS e (Personal) firewalls	Antivirus
Mecanismo	Examina o header do pacote	Examina o header do pacote e campos de controle	Examina os campos e comportamento da aplicação	Examina os arquivos dentro do tráfego da aplicação
Cobertura de protocolo e aplicação	Não há - Trabalha a nível de pacotes	Grande	Médio	Pequeno (email, web e transferências de arquivo)
Proteção fornecida	cliente-servidor e servidor-cliente	cliente-servidor e servidor-cliente	Na maior parte cliente-servidor	Na maior parte servidor-cliente
Performance	Alta	Alta	Média	Baixa

As atuais tecnologias de proteção contra ataques basicamente trabalham em quatro níveis: nível de pacotes, nível de sessão, nível de aplicação e nível de arquivo. São basicamente 4 (quatro) as principais tecnologias que utilizamos para nos defendermos de ataques: ACL, Firewall, IPS e Anti-vírus. Vamos verificar como essas tecnologias se comportam frente ao novo ambiente já descrito.

2.4 LIMITAÇÕES E TENDÊNCIAS DOS ATUAIS MÉTODOS DE DETECÇÃO

Os novos tipos de ameaça compartilham as seguintes principais características:

- Mutantes : variam seu código e forma muito rapidamente
- Invisíveis: não buscam chamar muita atenção, sem variar significativamente o comportamento de utilização dos computadores e redes
- Únicos: o algoritmo de mutação não é distribuído com o malware
- Reutilizáveis: podem ter diversos tipos de ação

Parte dos trojans e worms que invadem computadores são únicos, Um exemplo é o Zlob que instala um trojan com identificador (MD5 hash) diferente para em cada visitante de sua página e o algoritmo de mutação não é distribuído juntamente com o malware.

Além disso, os desenvolvedores geram dia-a-dia um novo formato de malwares com diferentes funções. No passado os malwares executavam basicamente uma função, Os malwares de hoje podem executar diversas funções de forma programada para não chamar a atenção do usuário e dos administradores de rede.

No quadro 3, pode-se observar que nenhuma das tecnologias de proteção tem total eficácia na proteção contra os novos ataques. A que melhor está posicionada é a proteção ao nível de aplicação que controla o comportamento da aplicação.

A tendência de utilização de diversas soluções de segurança combinadas é por sua vez uma tendência que todas as fontes pesquisadas indicaram.

Quadro 3 – Comparação das categorias de tecnologias de segurança e sua eficácia contra os novos malwares

	Proteção ao nível de pacotes	**Proteção ao nível de sessão**	**Proteção ao nível de Aplicação**	**Proteção ao Nível de Arquivo**
Exemplo	Filtro de Pacote (ACL de Router ou "stateless" firewall)	"Statefull Inspection" Firewall	(Host) IPS e (Personal) firewalls	Antivirus de Gateway
Mecanismo	Examina o header do pacote	Examina o header do pacote e campos de controle	Examina os campos e comportamento da aplicação	Examina os arquivos dentro do tráfego da aplicação
Eficácia frente os novos malwares	Baixa	Média	Média-alta	Baixa

Outra grande tendência é a utilização de análises comportamentais para detecção de novos malwares, ou essa combinada com as tecnologias já conhecidas para detecção de ataques.

A Cisco afirma em seu relatório anual, que analisa o ano de 2007, que mesmo sua tecnologia de reputação (análise comportamental dos sites web e emissores de email) não deve mais ser utilizada sozinha e que técnicas de detecção de malwares não conhecidos devem também ser aplicadas em conjunto [18]

O Gartner sugere a convergência de tecnologias para se defender das novas ameaças [7]. Para o Gartner essas tecnologias devem prover além das técnicas atuais de detecção:

- Detecção de anomalias de protocolo
- Deep-packet inspection
- Simulação de potenciais códigos maliciosos antes da execução desses, usando análise estatística e simulação em sandbox ou máquinas virtuais.
- Análise heurística genérica para detecção de variações dos malwares
- Grande controle de buffer overflow
- Controle de execução de aplicações
- Controle do comportamento da aplicação
- Auditoria e proteções para garantir que as políticas de proteção estão ativas
- Log de eventos detalhados
- Uso coordenado do firewall em conjunto com outras tecnologias de detecção de malware para prover rápida defesa de vulnerabilidades não corrigidas

"O IDC espera cada vez mais a convergência de anti-vírus,firewall,antispyware, host intrusion prevention system (HIPS), application control e device control. Pois as ameaças convergentes estão se tornando cada vez maiores e precisarão de várias tecnologias para detectá-las."[15]

Outra grande tendência é a integração dos Firewalls de rede com os IPS de rede, criando o que já está sendo chamado de NGF (new generation firewall), Alguns fabricantes como a checkpoint já fizeram essa fusão. Mas de qualquer forma, a utilização de IPS de rede separado do firewall de rede continua em crescimento.

Todos os grandes fabricantes de produtos para proteção contra ataques já iniciaram, e muitos até mesmo já concluíram, a integração dessas soluções.

A Symantec, ainda em 2007, lançou seu conjunto de proteção de endpoints que congrega: antivírus, antispyware, firewall, detecção de intrusão, controle de aplicações e dispositivos removíveis, e controle de acesso à rede (NAC).

A Symantec também vem evoluindo suas soluções de controle de comportamento das aplicações que, basicamente, coloca a aplicação em containers e monitora seu comportamento. O funcionamento se dá com base na premissa "Eu não sei exatamente o que você faz, mas eu sei o que você nunca deveria fazer." [26]

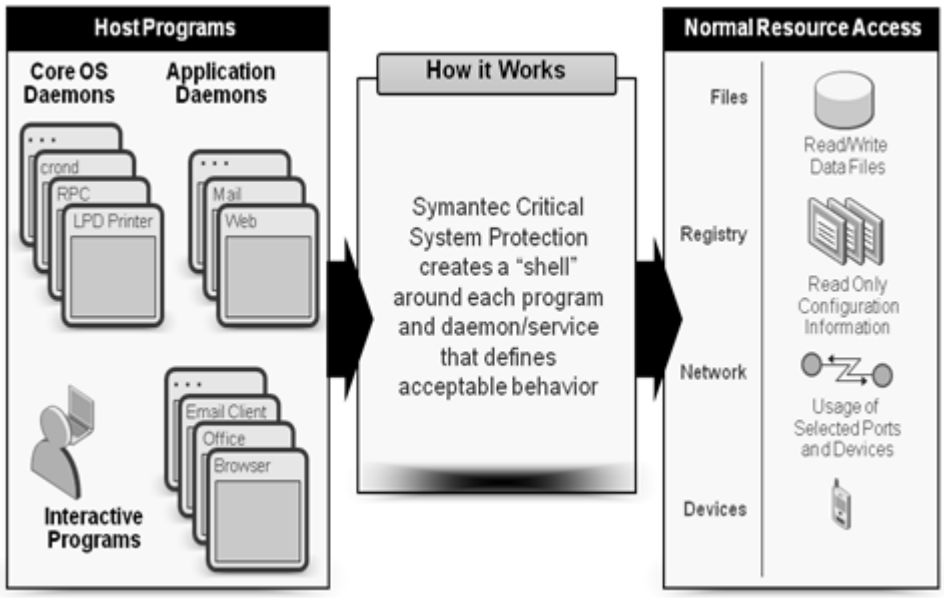

Figura 8 – Controle de comportamento da aplicação da Symantec

2.5NOVAS TECNOLOGIAS DE DETECÇÃO DE AMEAÇAS E ATAQUES

Dado as novas características das ameaças e ofensores, mesmo as novas tecnologias e suas integrações certamente não evitarão que atacantes consigam invadir sistemas e aplicações. Como o atual objetivo dos ofensores não é mais simplesmente a indisponibilidade de sistemas, mas sim

as informações e dados sensíveis contidos nos destinos dos ataques, novas tecnologias estão surgindo.

A tecnologia de DLP (Data Loss Prevention) é a mais nova lançada e, apesar de ainda estar em fase de amadurecimento, promete complementar ainda mais as técnicas de defesa contra ataques. As soluções de DLP evitam que informações sensíveis sejam enviadas a destinos não desejáveis, esteja essa informação no email, no endpoint ou qualquer outro meio de armazenamento.

Não é feito o controle do arquivo ou o controle da aplicação em dispositivos, mas sim a análise do conteúdo e o destino desejado de sua transferência. Não importa se o conteúdo está em uma planilha Excel ou em um arquivo texto ou em arquivo compactado. Através da identificação de conteúdos sensíveis, a indexação do mesmo em uma base de dados, ou até mesmo o padrão (formato) daquele conteúdo, é monitorado por todos os pontos que podem acessá-lo. Políticas de utilização, acesso e transferência do mesmo são então criadas e aplicadas naqueles pontos de acesso.

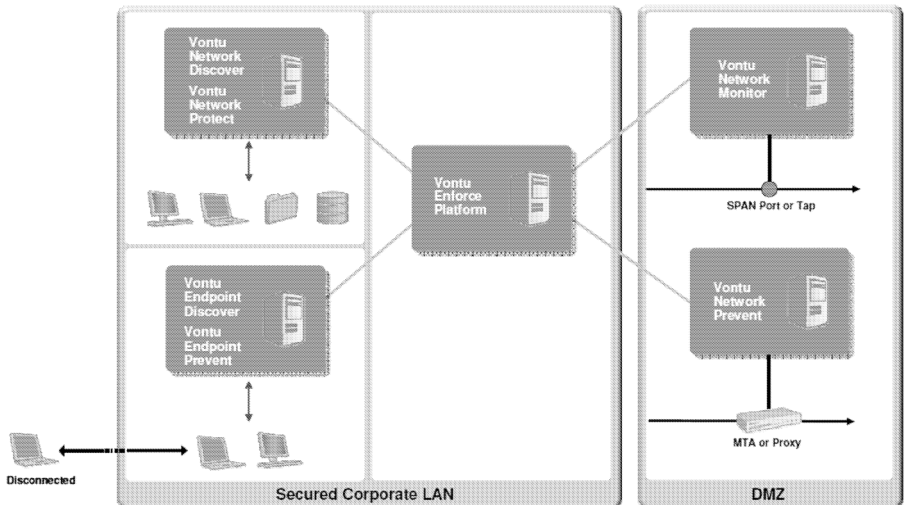

Figura 9 – arquitetura da solução de DLP da Vontu

Na figura 9 podemos ver a arquitetura utilizada por soluções de DLP para fazer o controle do acesso e utilização do conteúdo. Algumas soluções fazem inclusive controle de imagens e também de impressão, incluindo print-screen.

Quando as políticas de acesso e utilização do conteúdo são violadas, incidentes podem ser criados e até mesmo ações automáticas, como bloqueio do conteúdo ou remoção do conteúdo. Além disso, incidentes para simples monitoração do acesso ao conteúdo são práticas normais na implementação de Soluções de DLP.

As soluções de DLP também tendem a integrar-se totalmente aos IPS, Firewall e soluções de proteção de endpoints. Esse movimento já está existindo ainda que esteja em fase muito inicial.

A inteligência para entender o comportamento dos ataques também moveu a indústria de segurança da informação para a criação de tecnologias de correlação de eventos, SIEM (Security Information Event Management).

Essas soluções analisam dados geradas por fontes diversas (IPS, Firewall, Proxy, Sistemas operacionais, aplicações de servidores e desktops, Syslogs, dispositivos de rede,etc.) e as correlacionam objetivando encontrar padrão de comportamento que sinalize uma violação à política de segurança da informação.

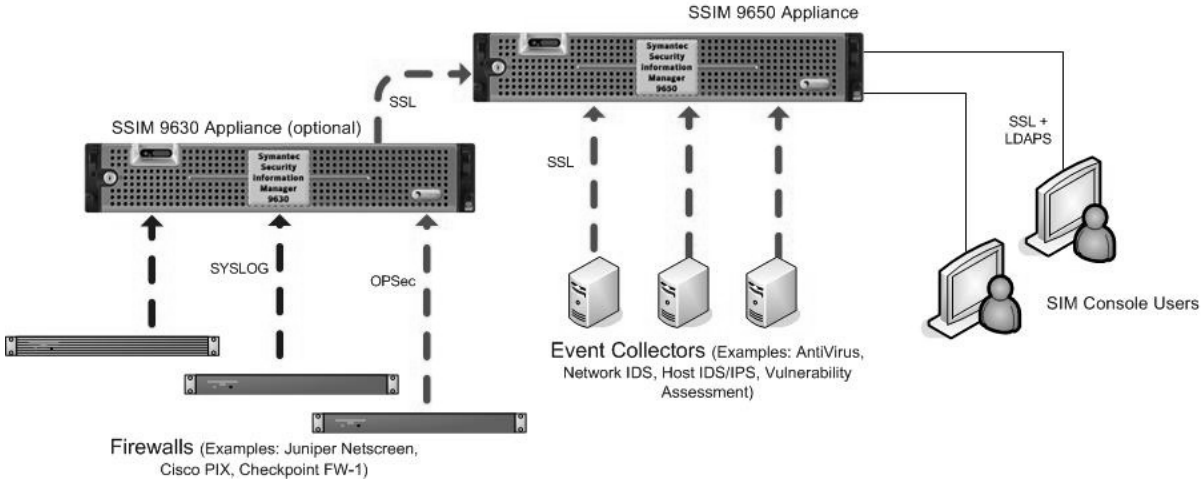

Figura 10 – arquitetura da solução de SIEM da Symantec

Tal tecnologia ajuda os profissionais de segurança da informação a identificar e ter foco em incidentes críticos, pois reduzem dramaticamente o número de incidentes falso-positvos, uma vez que milhares de eventos de segurança gerados nas fontes coletadas são reduzidos a centenas ou até mesmo dezenas de incidentes quando os dados são correlacionados. (conforme figura 11).

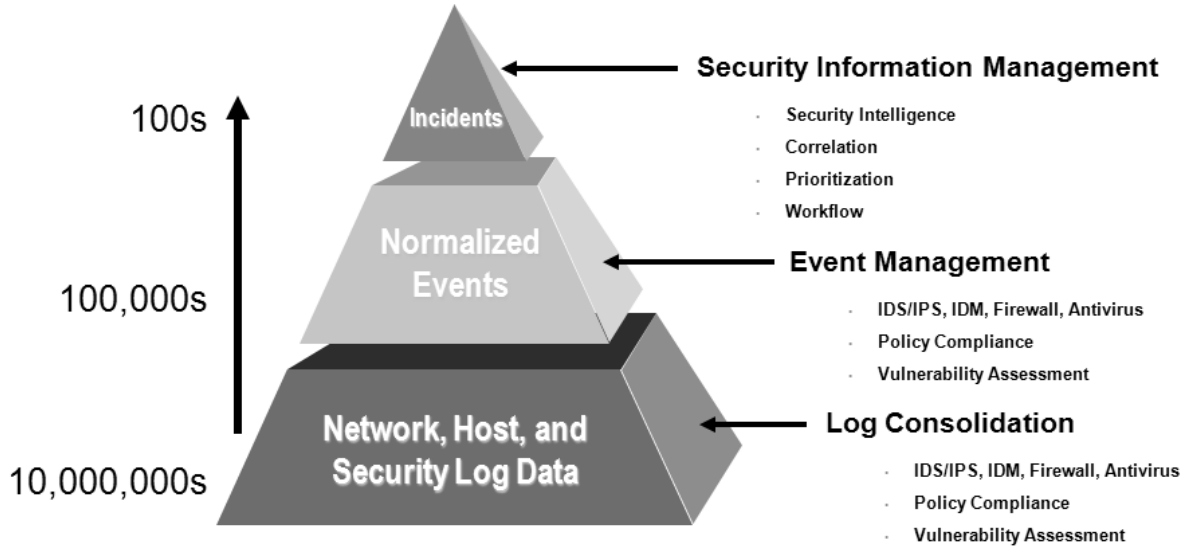

Figura 11 – SIEM, consolidação de eventos em Incidentes

No quadro 4 são apresentados alguns exemplos que caracterizam a relação eventos/incidentes dia, por tipo de dispositivo, em empresas de grande porte.

Quadro 4 – SIEM, relação eventos/incidentes por ativos

Tipo de Dispositivo	Eventos/Dia por Ativo	Eventos por Incidente
Desktop/Server AV	20	100
Client Firewall	75	150
Network Firewall	3,000,000	100
Network IDS/IPS	20	10
Host IDS/IPS	-	10
Vulnerability Assessment	-	2
Policy Compliance	25	100
Syslog	300	1
Windows Event Log	2,000,000	100
Mail Security	-	10
Roteadores	3,5	10
Active Directory	300	10
Banco de Dados	50	10

3CONCLUSÃO

O Ano de 2007 realmente foi um marco na indústria de segurança da informação. As mudanças aqui apresentadas já vinham sendo sentidas e muitas vezes foi anunciada sua breve chegada. Mas efetivamente em 2007 elas ocorreram, e as tecnologias de defesa já estão mudando para atender as atuais necessidades. As tradicionais e mais amplamente adotadas técnicas de detecção de ameaças digitais somente nos protegem contra adolescentes aventureiros, mas agora a luta não é contra os amadores. Por isso temos que lançar mão de novas tecnologias e abordagens.

As principais características do fenômeno ocorrido em 2007 são:

- Aumento expressivamente fora do normal no número de ameaças identificadas
- Mudança na forma e comportamento dos ofensores

Em função disso o mercado de segurança da informação respondeu da seguinte forma:

- Maior integração das tecnologias de detecção e bloqueio de ataques
- Foco em tecnologias que analisam o comportamento dos fluxo de dados,conteúdo, sistemas e aplicações

Novas tecnologias estão sendo criadas, as atuais estão sendo aprimoradas, todas tendem a trabalhar de forma bem integrada. É como um exército, se não lutar de forma coordenada, em harmonia e com inteligência, todas as guerras serão perdidas.

As previsões para os anos seguintes são de repetição do ocorrido em 2007. Mais um sinal de que essa guerra não acabará nunca.

7REFERÊNCIAS BIBLIOGRÁFICAS

[1] **Scudere, Leonardo** ; Risco Digital; Elsevier 2007

[2] **Scambray, Joel** ; Hackers Expostos ; Makron Books 2001

[3] **Zwicky, Elizabeth D**.; Contruindo Firewalls para Internet; Campus 2000

[4] **Melo, Sandro**; Exploração de Vulnerabilidades ; Alta Books 2005

[5] **Tanenbaum, Andrew** ; Redes de Computadores; Campus 1994

[6] **Martin, Murhammer** ; TCP/IP Tutorial e Técnico; Makron Books 2000

[7] **Firstbook, Peter**; Magic Quadrant for Endpoint Protection Plataform; Garnter RAS Core Research Dezembro 2007

[8] **Young, Greg** ; Magic Quadrant for Network Intrusion Prevention Systems; Garnter RAS Core Research Fevereiro 2008

[9] **Oullet, E.** ;Magic Quadrant for Content Monitoring and Filtering and Data loss Prevention; Garnter RAS Core Research Junho 2008

[10] **Nicolle, Mark** ; Magic Quadrant for Security Information and Event Management; Garnter RAS Core Research Maio 2008

[11] **Young, Greg** ; Deconfusicating Network Intrusion Prevention; Garnter 2007

[12] **Firstbook, Peter; Genes Raimund** ; Securing your Business from the New Web Threats; Trend Micro Inc and Gartner 2007

[13] **Young, Greg** ; Magic Quadrant for Network Intrusion Prevention Systems; Garnter RAS Core Research Dezembro 2006

[14] **Hypponen, Mikko**; F-Secure Reports 2007; F-secure Dezembro 2007

[15] **Hanson, Andrew**; IDC Analyst Connection – Endpoint Security: Combating Today's Threats and Planning for Tomorrow's; IDC Julho 2008

[16] **Dearborn, Rob** ; The cost of Network Security Attacks:North America 2007; Infonetics Research Inc.

[17] Ironport Email Security Appliance Overview – White Paper; IronPort Systems Inc 2006

[18] **Chambers, John**; 2008 Internet Security Trends ; CISCO 2008

[19] Juniper Networks; Accurate Attack Protection; Juniper Networks Inc 2005

[20] **Pereira, Juan Pablo**; Comparison of Firewall, Intrusion Prevention and Antivirus technologies ; Juniper Networks 2006

[21] **Snyder, Joel** ; Six Integral Steps to Selecting the Right IPS for your Network; Opus Consulting Group Ltd. 2007

[22] **Dubrawsky, Ido** ; Firewall Evolution – Deep Packet Inspection; SecurityFocus 2003

[23] Avert Labs, McAfee; As 10 maiores previsões de ameaças para 2008; McAfee Inc. 2007

[24] **NorthCutt, Stephen** ; The tem most Important Security Trends of the Coming Year ; SANS Technology Institute 2006

[25] SANS Institute; SANS top 20 Internet Security Risk of 2007; SANS Technology Institute 2007

[26] **Waggoner, Jim** ; Symantec's Endpoint Security Overview; Symantec Corporation 2008

[27] **Engels, John**; Symantec Critical System Protection Overview; Symantec 2008

[28] Symantec Global Internet Threat Report – Trends for July-december 2007; Symantec Corporation 2008

[29] Yaneza, Jaime Lyndon ; 2007 Threat Report | 2008 Threat and Technology Forecast ; Trend Micro Inc. 2008

[30] **Pescatore, John**; Early Detection of PCs that have been Compromissed via botnet clients; Gartner RAS Core Research 2008

[31] **Fossi, Marc**; Symantec Internet Security Threat Report XIV; Symantec Corporation , abril 2009.

[32] Avert Labs, McAfee; 2009 Treath Predictions; McAfee Inc. 2009