

<http://www.CLM.com.br>



Ameaças Combinadas
“Combined Threats”
Conceitos Técnicos e Formas
de Proteção

for Internet Professionals
Internet Professionals

<http://www.CLM.com.br>



Duval A. Costa
Diretor de Consultoria
duval.costa@clm.com.br
CLM
Av. Ibirapuera, 2120 - 9º. andar
São Paulo - SP
11-2125-6256

for Internet Professionals
Internet Professionals

Ameaças Combinadas



- **Sumário de Assuntos**
 - Insegurança em Números
 - Exemplos de Ameaças
 - Conceito: Combinação de Ameaças
 - Proteção: Sistemas de Defesa
 - Plano de Ação
 - Algumas Tendências
 - Pontos para Reflexão
 - Referências
 - Perguntas e Respostas

Ameaças Combinadas



- **Insegurança em Números**
 - Incidentes Reportados ao NBSO / CERT. br – Janeiro - Dezembro - Total
 - Estatísticas de (Mau) Uso da Internet
 - Incidência de Ameaças

Incidentes – NBSO / CERT.br



• Incidentes Reportados – Janeiro Dezembro - Total

	2005	2004	2003	2002	2001	2000	1999
Janeiro	4.448	5.886	3.603	1.453	896	424	204
Fevereiro	3.142	6.110	2.948	1.186	1.040	509	172
Março	4.848	6.002	3.255	1.254	1.202	541	203
Abril	5.253	4.763	3.689	1.181	1.444	351	151
Maiο	6.883	5.471	3.393	1.267	1.332	480	145
Junho	5.406	6.502	3.332	1.407	1.109	641	192
Julho	5.146	6.773	3.622	1.900	859	585	208
Agosto	5.718	5.910	4.946	1.716	639	432	385
Setembro	5.361	5.167	5.987	1.964	669	337	264
Outubro	6.316	11.253	6.661	3.783	1.002	468	269
Novembro	7.901	7.149	6.135	4.436	1.171	573	418
Dezembro	7.578	4.736	7.036	3.545	938	656	496
Total	68.000	75.722	54.607	25.092	12.301	5.997	3.107

Insegurança em Números



• Estatísticas de Uso da Internet

- Uso Inadequado de Privilégios de Acesso
- Invasões Internas e Externas
- Uso de Instant Messaging (IM)
- Compartilhamento de Arquivos
- Conteúdo Impróprio
- Código Hostil
- Streaming Media

- *Em resumo: que tipo de tráfego inadequado está passando pela rede corporativa?*

Uso da Internet (1)



- **Uso Inadequado de Privilégios de Acesso (1)**
 - 1/3 do tempo de navegação durante o expediente não é relacionado com trabalho (IDC, 2003)
 - 80% / 59% das organizações reportaram que seus funcionários haviam abusado de seus privilégios de acesso à Internet, por exemplo baixando material pornográfico ou software pirata (CSI/FBI Computer Crime and Security Survey, 2003 / 2004)
 - 64% dos funcionários afirmam usar eventualmente a Internet com fins pessoais durante o expediente (U.S. Dept. of Commerce)
 - 37% dos funcionários afirmam usar constantemente a Internet com fins pessoais durante o expediente (U.S. Dept. of Commerce)

Uso da Internet (2)



- **Uso Inadequado de Privilégios de Acesso (2)**
 - 60% de todas as compras online são feitas durante o horário do expediente de trabalho (IDC Research, 2003)
 - 41% dos funcionários afirmam usar a Internet com fins pessoais durante o expediente de trabalho por mais de três horas por semana (IDC Research, 2003)
 - Em média, os funcionários passam 21 horas por semana online no trabalho, em oposição a apenas 9.5 horas em casa (U.S. Dept. of Commerce)

Uso da Internet (3)



• Invasões Internas e Externas

- 68% / 66% das organizações reportaram acesso não autorizado por usuários internos (CSI/FBI, 2003 / 2004)
- 93% das organizações que perderam acesso aos seus data centers por 10 dias ou mais faliram em um ano, 50% faliram imediatamente (Juniper Networks, 2005)
- O intervalo de tempo entre a descoberta de uma vulnerabilidade e a sua exploração caiu de 288 dias em 1999 para menos de 6 dias em meados de 2004 (Secure Computing Magazine, 2004)

Uso da Internet (4)



• Uso de Instant Messaging (IM-1)

- Aproximadamente 80% do uso de IM nas organizações se dá através de serviços públicos, tais como AOL, MSN e Yahoo, desta forma expondo as organizações a ameaças à sua segurança (Radicati, 2003)
- Há mais de 43 milhões de usuários de IM nas organizações (IDC, 2003)
- Apenas 25% das organizações tem uma política claramente definida quanto ao uso de IM no ambiente de trabalho (Silicon.com, 2003)

Uso da Internet (5)



- **Uso de Instant Messaging (IM-2)**
 - Previsão de 450 milhões de usuários de IM no mundo até 2007 (IDC, Revista TI Inside, nº 11 março de 2006)
 - 85% dos internautas no Brasil usam IM (Ibope Net/Ratings, dezembro de 2005)
 - 25 milhões de usuários de IM no Brasil (Revista TI Inside, nº 11 março de 2006)
 - 80% usam para conversar com parentes e familiares, 66% compartilham fotos e arquivos, 40% usam para obter respostas rápidas sobre assuntos de negócios (Lightspeed Research, pesquisa com usuários ICQ no Brasil, setembro de 2005)

Uso da Internet (6)



- **Compartilhamento de Arquivos**
 - 45% dos arquivos executáveis baixados pelo Kaza contém algum tipo de código hostil (Trusecure, 2004)
 - 73% das buscas por filmes em redes de compartilhamento de arquivos são relacionadas a pornografia (Palisade Systems, 2003)

Uso da Internet (7)



- **Conteúdo Impróprio**

- 70% de todo o material pornográfico é baixado entre 9h00 e 17h00 (SexTracker)
- 37% dos funcionários que acessam a Internet durante o expediente de trabalho visitam sites com conteúdo impróprio (ComScore Networks, 2003)

Uso da Internet (8)



- **Código Hostil**

- **Spyware**

- Existem mais de 7,000 programas do tipo spyware (Aberdeen Group, 2003)

- **Virus**

- Ainda que 99% / 99% das organizações usem antivírus, 82% / 78% delas tiveram problemas com código hostil (CSI/FBI, 2003 / 2004)
- Ainda que 90% das organizações usem antivírus, 66% apontaram vírus como a principal ameaça à Segurança de Informações (Módulo, 2003)

Uso da Internet (9)



- **Streaming Media**

- 77% do uso de “Internet Radio” ocorre entre 5h00 e 17h00 (Arbitron, 2004)
- 44% dos funcionários das organizações usam streaming media todos os dias (Nielsen NetRatings, 2002)

Incidência de Ameaças (1)



- **“Porta Arrombada”**

- 20 minutos é o tempo que um PC conectado à Internet leva para sofrer o primeiro ataque
- 4.496 novos exemplos de código hostil identificados no primeiro semestre de 2004
- 100.000 é o número de pragas virtuais identificadas

(Jornal Folha de S. Paulo, caderno Folha Informática, 29 de setembro de 2004)

Incidência de Ameaças (2)

- **“Mundo das Fraudes”**
 - Pesquisa da KPMG sobre fraude empresarial com 1.000 empresas brasileiras realizada a cada 2 anos desde 2000
 - O índice de respondentes que vivenciaram fraudes em suas organizações foi de 69%
 - Controles internos de clientes permitiram a ocorrência de fraudes para 71%

(Revista Executivos Financeiros, Abril 2005, nº 170)

Incidência de Ameaças (3)

- **“Brasil: Líder em Fraudes nos Bancos”**
 - Somos o terceiro país do mundo em número de fraudes bancárias de “roubo de identidade” (*saques, pagamentos e transferências usando dados pessoais roubados de clientes*), atrás apenas da Inglaterra e EUA, segundo a Unisys Corporation (*estudo realizado em agosto de 2005*)

(Revista TI Inside, no. 9, dezembro de 2005)

Incidência de Ameaças (4)

- **“Fraudes Virtuais Custam Caro a Bancos”**
 - Conforme a Febraban, um prejuízo da ordem de R\$300MM foi causado aos Bancos no Brasil em função de fraudes em canais eletrônicos durante 2005 (*aumento de 20% em relação a 2004*)
(Revista ComputerWorld, no. 447, janeiro de 2006)

Incidência de Ameaças (5)

- **“Internet Fraud Creates Losses in the Brazilian Banking System”**
 - According to the Brazilian daily newspaper Gazeta Mercantil and to local trade sources such as the Brazilian Bank Association (Febraban), losses caused by Internet fraud against Brazilian banks and credit card administrators totaled US \$132 million in 2005.
 - Until 1995, 100 percent of the losses were caused by thefts or kidnappings of people leaving banks.
 - From 1996 to 2000, those types of crime generated 90 percent of the losses, and cloning of credit cards contributed 10 percent.
 - As of 2004, though, 80 percent of the losses originated from Internet fraud, 10 percent from robberies and kidnappings, and 10 percent from cloning credit cards.

Ameaças Combinadas

- **Exemplos de Ameaças**
 - SPAM [SPAM]
 - Código Hostil [CH]
 - Phishing [PHI]
 - Engenharia Social [ES]
 - Roubo de Informações [RI]
 - Conteúdo Impróprio [CI]

Exemplos de Ameaças

- **SPAM (1)**
 - SPiced hAM (presuntada)
 - Lixo eletrônico não solicitado ou mensagens eletrônicas enviadas de forma indiscriminada e em quantidades industriais (mass-mailing)
 - Ontem: primariamente com objetivos comerciais (compre Viagra, Rolex, “Software O&M”, etc.)
 - Hoje: visam roubo de informações (vide Phishing)

Exemplos de Ameaças

- **SPAM (2)**

- **Números da Network World (13/5/2004):**

- E-mails diários: 68,000,000,000 (100%)
- SPAMs diários: 42,840,000,000 (63%)

- **Números da Radicati (empresa de pesquisas - 2006):**

- E-mails diários: 135,000,000,000 (100%)
- SPAMs diários: 90,450,000,000 (67%)

(Revista Security Review, nº 6, Jan/Fev 2006)

Exemplos de Ameaças

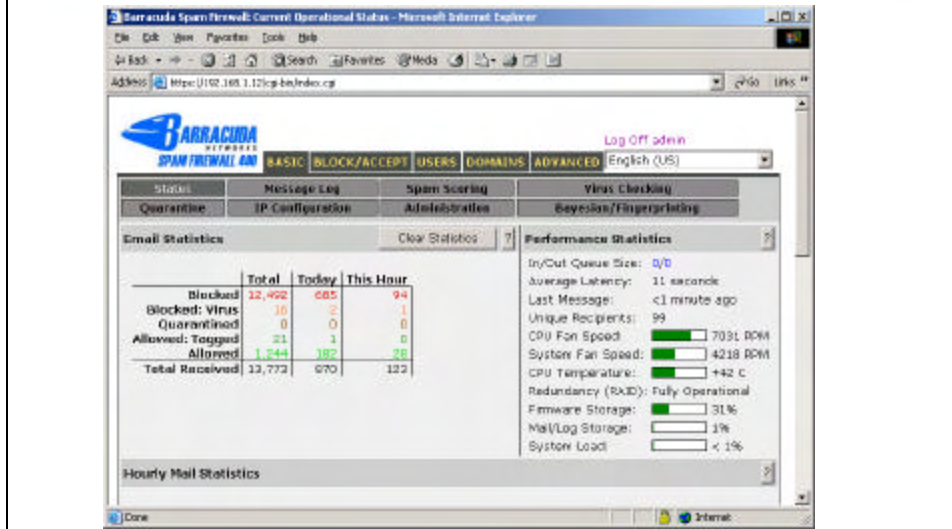
- **SPAM (3)**

- **Meu número:**

- Baseado na implementação de sistemas antispam
- Aproximadamente 80% é SPAM
- Exemplo a seguir

Exemplos de Ameaças CLM

- **SPAM (4)**



Exemplos de Ameaças CLM

- **Código Hostil (1)**

- **CH:** vírus, vermes / worms, cavalos de tróia / trojans e suas variantes – spyware, keyloggers, etc. (hackers automáticos)
- **Ontem:** transmitidos por disquete de boot de 5.25 e apagavam alguns arquivos do seu computador
- **Hoje:** transmitidos por “mass-mailing” e transformam o computador da vítima em um “banheiro público”

Exemplos de Ameaças

- Código Hostil (2)

- Ativos: (WildList, setembro de 2005)

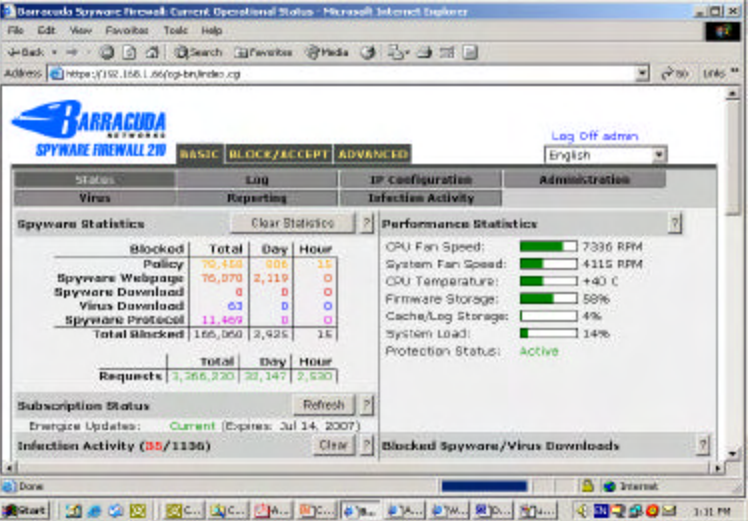
- Reportados por 2 ou mais pesquisadores: 705 (Top List)
 - Reportados por 1 pesquisador: 4182 -705 = 3477 (Supplemental List)

- Total:

- Número varia dependendo do fornecedor
 - Por volta de 80M (~60 a 100M)

Exemplos de Ameaças

- Código Hostil (3)



The screenshot displays the Barracuda Spyware Firewall 210 web interface. The 'BLOCK/RECEIPT' tab is active, showing various statistics. The 'Spyware Statistics' table is as follows:

	Blocked	Total	Day	Hour
Policy	70,123	0	0	11
Spyware Webpage	70,070	2,119	0	0
Spyware Download	0	0	0	0
Virus Download	0	0	0	0
Spyware Protocol	11,459	0	0	0
Total Blocked	165,050	2,425	15	15

The 'Performance Statistics' section shows the following values:

- CPU Fan Speed: 7336 RPM
- System Fan Speed: 4115 RPM
- CPU Temperature: +40 C
- Firmware Storage: 58%
- Cache/Log Storage: 4%
- System Load: 14%
- Protection Status: Active

The 'Infection Activity' section shows 00/1136 infections.

Exemplos de Ameaças

- **Phishing (1)**
 - **Password harvesting fishing**
 - **SPAM especializado no roubo de informações**
 - **Supostamente enviado por organizações sobre as quais não resta a menor dúvida:**
 - Bancos
 - Autoridades governamentais
 - Empresas conhecidas
 - Alguém conhecido

Exemplos de Ameaças

- **Phishing (2)**
 - **Ontem: e-mail com link para um site falso, grosseiramente mal ajambrado**
 - **Hoje: e-mail com executável anexo ou com link para um executável que se instala no computador da vítima e rouba informações e/ou permite o uso remoto do computador da vítima**

Exemplos de Ameaças

- **Engenharia Social (ES)**
 - Uso de técnicas de convencimento com o intuito de iludir ou ludibriar mediante:
 - Ameaça (sabe com quem está falando?)
 - Promessa de recompensa (conto do vigário do bilhete premiado ou da herança do ditador nigeriano)
 - **Ontem**: por telefone, um a um
 - **Hoje**: por e-mail, aos milhares de uma vez

Exemplos de Ameaças

- **Roubo de Informações (RI)**
 - Roubo de Identidade (alguém de posse de seus dados pessoais passa a ser você)
 - **Ontem**: roubo de senha de controle de acesso
 - **Hoje**: roubo de conta(s) bancária(s), user-id(s), senha(s), cartão (ões), PIN(s), etc.

Exemplos de Ameaças

- **Conteúdo Impróprio (CI)**
 - Sites com conteúdo pornográfico, ofensivo, destrutivo ou semelhante
 - Sites cujo conteúdo não diz respeito às atividades profissionais
 - Sites cujo conteúdo não está incluído na Política de Utilização da Internet adotada pela organização
 - **Ontem**: baixa de conteúdo em formato texto
 - **Hoje**: baixa de arquivos executáveis com código hostil

Ameaças Combinadas

- **Conceito: Combinação de Ameaças**
 - O conceito de Ameaças Combinadas / “Combined Threats” está na exposição dos sistemas computacionais a grupos concomitantes de perigos externos que se apresentam simultaneamente e se utilizam de um único vetor ou porta de entrada
 - Formas de exploração de vulnerabilidades (exploits) que conseguem causar dano ou estorvo de múltiplas formas distintas
 - Exemplo ilustrativo a seguir

Combinação de Ameaças

- **Exemplo**

- Atacantes mandam e-mail a milhares de vítimas [SPAM]
- Em português, bem escrito, supostamente de uma empresa conhecida, prometendo um prêmio [ES]
- Link para um site forjado [CI] onde se preenche um formulário com dados pessoais [RI / PHI]
- Com arquivo(s) anexo(s) contendo verme(s) (CH), o(s) qual(is) instala(m) keylogger, servidor de ftp, smtp e backdoor

Combinação de Ameaças

- **Exemplo – cont.**

- Keylogger: grava a digitação em arquivo [RI] e o envia por e-mail ou ftp
- Servidor de ftp: permite acesso ao(s) arquivo(s) [RI]
- Servidor de smtp: permite o envio de mensagens de correio [SPAM / PHI]
- Backdoor: permite o controle remoto da máquina da vítima (zombie) para SPAM, ataques DDoS e outras maldades

Ameaças Combinadas

- **Proteção: Sistemas de Defesa**
 - Soluções Corporativas
 - Soluções SMB
 - *Nota: exemplos dados são sistemas servidores; não esquecer dos desktops, procedimentos, processos, pessoas, treinamento, etc.*

Sistemas de Defesa

- **Soluções Corporativas**
 - Organizações maiores
 - “Best of Breed”
 - Appliances dedicados, independentes e monofunção (exemplos):
 - Firewall
 - IDS / IPS
 - Anti-spam
 - Anti-virus
 - IM server

Soluções Corporativas

- **Firewall (exemplos)**
 - Sistemas de filtro de tráfego entre redes
 - Controlam acesso a servidores e estações na(s) redes(s) protegidas
 - Linha WatchGuard Firebox X Peak
 - X8000, X6000, X5000
 - Até 1.000.000 de sessões concorrentes
 - Até 10 interfaces de rede (4 WAN)

Soluções Corporativas

- **IDS / IPS (exemplos)**
 - Intrusion Detection System / Intrusion Prevention System
 - Auditam o tráfego que passa pelo firewall
 - Linha Sourcefire Intrusion Sensors (IS)
 - IS500 a IS5800-8
 - Performance de 5 Mbps a 8 Gbps
 - Snort-based

- **Anti-spam** (exemplos)
 - Filtro do lixo eletrônico antes deste chegar ao servidor de correio
 - Linha Barracuda SPAM Firewall (BSF)
 - BSF 200 a BSF 900
 - Capacidade nominal de 1 a 15 milhões de mensagens diárias

- **Anti-virus** (exemplos)
 - Filtro do código hostil antes deste entrar na rede
 - Linha Barracuda Spyware Firewall (BYF)
 - BSF 210 a BSF 810
 - Performance de 5 Mbps a 200 Mbps

Soluções Corporativas



- **IM server** (exemplos)
 - Controle do uso de IM
 - Linha Barracuda IM Firewall (BIF)
 - BIF 220 a BIF 820
 - De 200 a 7.000 usuários

Sistemas de Defesa



- **Soluções SME**
 - Organizações menores / filiais de organizações maiores
 - UTMS (Unified Threat Management Systems)
 - Appliances multifunção:
 - Firewall
 - IDS / IPS
 - Anti-spam
 - Anti-virus
 - Filtro de conteúdo

Soluções SME



- **Linha WatchGuard Firebox X Core**
 - X500, X700, X1000
 - De 20.000 a 200.000 sessões concorrentes
 - Até 6 interfaces de rede (normalmente 1 WAN)
 - Serviços adicionais:
 - Gateway AntiVirus for E-mail
 - Gateway AntiVirus/Intrusion Prevention Service
 - WebBlocker Web Content Filtering
 - SpamScreen

Ameaças Combinadas



- **Plano de Ação (1)**
 - 1- **Análise de Ameaças e Vulnerabilidades**
 - Perigos externos a serem evitados / gerenciados
 - Fraquezas internas a serem corrigidas
 - 2 - **Análise de Riscos e Impactos**
 - Ativos sendo arriscados
 - Probabilidade e custo de um Incidente de Segurança

- **Plano de Ação (2)**
 - **3 - Seleção de Ferramentas**
 - Consultas a sites de fornecedores
 - Testes de terceiros
 - Certificações obtidas (ICSA, NSS, NIST/NIAP)
 - TCO e/ou outras medidas financeiras
 - **4 - Projetos – piloto**
 - Test drive das ferramentas candidatas

- **Algumas Tendências**
 - Exércitos de computadores zumbi (zombie armies)
 - Ataques direcionados (spear phishing / special-order spam)
 - Novos temas para spam (exemplo: dicas sobre investimentos com links para sites de spammers)
 - Novos métodos de envio de spam (SMS, IM e blogs ou spam blogs – splogs – blogs com links para sites de spammers)
 - Disseminação do uso de ferramentas de auditoria de tráfego de rede (IDSs, IPSs e App FWs)

Ameaças Combinadas



- **Pontos para Reflexão**

- “There are no victims, only volunteers”
- “Se almejas a paz, prepara-te para a guerra”
- Briga de gato e rato (cat-and-mouse game)
- A eterna disputa entre o canhão e a couraça
- “O preço da segurança é o da eterna vigilância”

Ameaças Combinadas



- **Referências**

- www.antiphishing.org
- www.barracudanetworks.com
- www.cert.br
- www.clm.com.br
- www.modulo.com.br
- www.radicati.com
- www.snort.org
- www.sourcefire.com
- www.gocsi.com
- www.watchguard.com
- www.wildlist.org

<http://www.CLM.com.br>



Ameaças Combinadas

“Combined Threats”

Conceitos Técnicos e Formas de Proteção

for Internet Professionals
Internet Professionals

<http://www.CLM.com.br>



Duval A. Costa

Diretor de Consultoria

duval.costa@clm.com.br

CLM

Av. Ibirapuera, 2120 - 9º. andar

São Paulo - SP

11-2125-6256

for Internet Professionals
Internet Professionals