ATAQUES A LINKS INTERNET

JULHO/2004

Ataques Silenciosos

Este documento traz de forma sintética os resultados da análise de tentativas não autorizadas de acesso (ataques) via Internet a um conjunto de redes corporativas gerenciadas pela i.web.

Nenhuma das redes analisadas teve sua segurança comprometida, entretanto devido ao volume e as características dos ataques, justifica-se atenção especial ao quesito segurança de redes. A divulgação deste documento visa fornecer uma idéia do volume de "ataques" a que suas redes são submetidas no dia a dia, evidenciando a necessidade ou até mesmo justificando o investimento em infra-estrutura de forma a garantir a segurança de suas redes de computadores.

Observações e agradecimentos

Visando garantir a privacidade de nossos clientes, todos os dados que possibilitariam a sua identificação foram omitidos e as informações aqui contidas não oferecem qualquer risco quanto à segurança de suas instalações.

Os clientes que utilizam nosso contrato de monitoramento 24x7, deverão receber o relatório com o estudo detalhado de suas redes e um comparativo com as demais redes analisadas até o final de julho. Para os demais clientes, os relatórios serão fornecidos apenas sob demanda.

Agradecemos a todos os clientes que nos autorizaram a utilizar as informações que resultaram neste estudo e esperamos que este relatório lhes seja útil.

Metodologia

A análise baseou-se nos dados coletados no período de abril a junho de 2004 e foi dividida primeiramente pelo tipo de link e posteriormente pela data e horário da ocorrência, tipo de protocolo, porta de acesso e conteúdo.

Neste documento, limitamo-nos a apresentar os dados diferenciados por tipo de link, ou seja, uma separação no primeiro nível de análise, deixando a análise detalhada para relatórios específicos de cada cliente.

Divisão de links	Participação
Frame relay	21.73%
ADSL	63.68%
Rádio	14.59%

Tabela 1 – Participação de cada tipo de link em relação ao total

Resultados

Dentre os links, verificou-se que os de rádio mostraram-se extremamente visados para ataques, detendo quase 70% dos mesmos, volume este que corresponde a quase 4 vezes o volume de ataques em relação aos links ADSL (Gráficos 1 e 2). Por sua vez, os links ADSL, os mais populares entre as empresas pequenas e médias, apresentaram um comportamento anômalo: o número de ataques por IP varia muito, indo de 30.000 a 230.000 tentativas por mês (Gráfico 3). O frame relay mostrou-se o link menos visado para ataques, talvez nem tanto por esses links serem considerados seguros, mas em virtude dos links ADSL e rádio serem considerados mais vulneráveis.

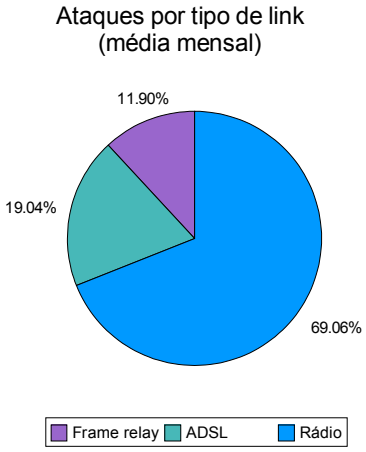

Gráfico 1 – Ataques por tipo de link

Apesar de a maioria dos ataques ser simples e de fácil controle, o volume é grande, atingindo valores médios alarmantes, como mostra a Tabela 2.

Médias por tipo de link	Ataques / Hora	Ataques / Minuto
Frame relay	93.9	1.6
ADSL	150.3	2.5
Rádio	545.2	9.1

Tabela 2 – Ataques por tipo de link

Isto signfica um ataque a cada 24 segundos para os links ADSL e um ataque a cada 6.6 segundos no caso dos links de rádio. Mesmo não obtendo êxito em invadir a rede, este volume de tráfego causa danos ao tráfego dos pacotes autênticos, provocando lentidão no

tráfego de dados através da Internet, diminuindo a performance das VPNs, websites, sistemas de correio, navegação na Internet, etc.

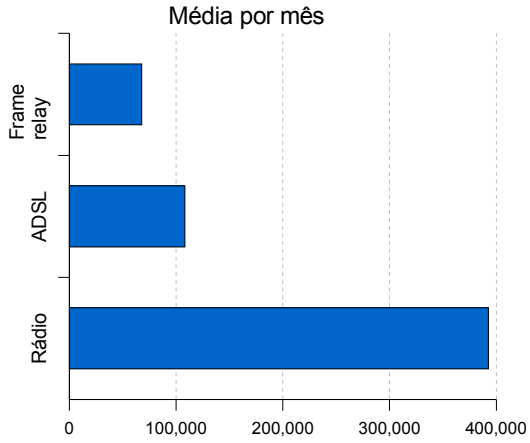

Gráfico 2 – Médias mensais

Foram detectados ataques contra as plataformas Windows, Unix e Netware. Entretanto, os exploits para a plataforma Windows (servidores web IIS, servidores Windows e servidores de correio Exchange, bem como backdoors abertas por vírus) foram os mais utilizados.
Tanto no caso do Windows quando do Unix, as técnicas utilizadas exploravam as vulnerabilidades de segurança destas plataformas. Caso os sistemas não estivessem devidamente atualizados, diversos ataques teriam sido bem sucedidos.
Detectamos que uma parcela considerável dos ataques originaram-se fora do Brasil, principalmente a partir da Ásia, Leste Europeu e América do Norte.

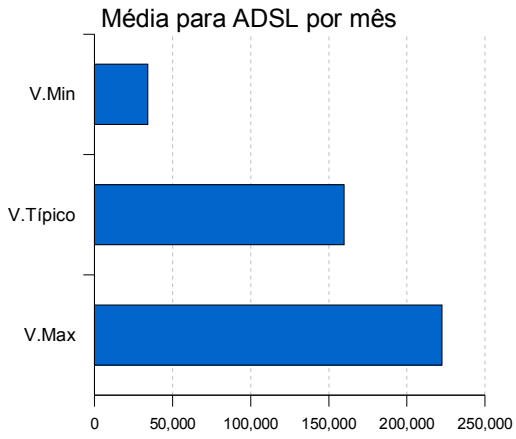

Gráfico 3 – Ataques a links ADSL

A análise ainda mostra que os ataques contra links ADSL, em sua maioria, visam obter acesso às máquinas com o objetivo de utilizá-las como open relay (e consequentemente utilizá-las para o envio de SPAM). Já os ataques contra links de rádio visam "coletar" dados que eventualmente trafeguem sem criptografia. Finalmente, os ataques contra redes frame relay são os mais sofisticados, embora em menor número.

Segurança
Embora a maioria dos ataques não tenha como alvo a empresa em si e sim o IP, ou seja, tratam-se de ataques contra as redes, sem que o atacante necessariamente conheça a empresa sob ataque ou tenha algum interesse específico em atingir uma determinada empresa, diversas empresas sofreram tentativas de acesso indevido a partir de concorrentes.

Contra-ataque
Grande parte das redes analisadas contavam com ferramentas de IDS (Intrusion Detection System) além do firewall, o que torna mais fácil detectar um ataque e principalmente reagir rapidamente evitando que o mesmo tenha sucesso. O monitoramento 24x7 mostrou-se valioso, uma vez que os ataques são bem distribuídos ao longo das 24 horas do dia e também durante os finais de semana.

Conclusão
Embora a maioria dos usuários tenha a impressão que instalando-se um firewall em suas redes, elas automaticamente estarão protegidas, este estudo demonstra a necessidade de manter uma estrutura de constante vigilância, visando não apenas manter o sistema operacional e o software de firewall atualizados, mas principalmente em manter ou adotar um eficiente sistema de detecção de intrusão e, quando necessário, de reação efetiva contra o invasor.