Imprimir

Glossário do Mal: conheça os diferentes tipos de ataque ao computador

Por Renan Hamann
Fonte: www.tecmundo.com.br/8284-Glossario-do-Mal-conheca-os-diferentes-tipos-de-ataque-ao-computador.htm

Sexta-Feira 4 de Fevereiro de 2011

Snooping, Adware, Denial of Service... O que é isso? Saiba o que significam os termos mais utilizados por hackers e crackers de todo o mundo.

O sucesso do site WikiLeaks reacendeu algumas discussões acerca de um tipo de usuário muito controverso no mundo da tecnologia: os hackers. Amados por muitos, odiados por outros tantos, eles podem ser considerados os heróis da resistência tecnológica, mas há quem diga que são apenas usuários mal-intencionados e loucos para encontrar portas abertas para invasões.

Estes últimos são também conhecidos como crackers e são responsáveis por boa parte da má fama da classe. Mas estes termos (hacker e cracker) são apenas a ponta do iceberg gigantesco que é o universo dos invasores.

Acompanhe agora o glossário que o Baixaki preparou para explicar cada termo designado para os ataques e técnicas realizados por usuários deste gênero. Também não podemos nos esquecer de muitos outros termos relacionados aos aplicativos e arquivos que são apenas um peso para os computadores, aqueles que nem deveriam ter sido lançados, mas incomodam a vida de todos.

A

Adware: este tipo de arquivo malicioso nem sempre é baixado por acidente para o seu computador. Alguns programas carregados de propagandas que só as eliminam após a aquisição de uma licença também são considerados adwares. Em suma, um adware é um aplicativo que baixa ou exibe, sem exigir autorização, anúncios na tela do computador.

Application-Layer Attack: os “ataques na camada de aplicação” podem ser feitos tanto em servidores remotos quanto em servidores de rede interna. São ataques nas comunicações dos aplicativos, o que pode gerar permissões de acesso aos crackers em computadores infectados. Aplicativos que utilizam base de dados online (como Adobe Reader) também podem ser atingidos.

B

Backdoor: traduzindo literalmente, “porta dos fundos”. São falhas de segurança no sistema operacional ou em aplicativos, que permitem que usuários acessem as informações dos computadores sem que sejam detectados por firewalls ou antivírus. Muitos crackers aproveitam-se destas falhas para instalar vírus ou aplicativos de controle sobre máquinas remotas.

Black Hat: o mesmo que “Cracker”. São os usuários que utilizam os conhecimentos de programação para causar danos em computadores alheios.

Bloatware: os “softwares bolha” não são considerados aplicativos de invasão. Na verdade, são programas que causam perda de espaço livre nos computadores por serem muito maiores do que deveriam ser. Ou possuem muitas funções, mas poucas que são realmente funcionais. Alguns dos softwares considerados Bloatwares são iTunes, Windows Vista e Nero.

Bluebugging: é o tipo de invasão que ocorre por meio de falhas de segurança em dispositivos Bluetooth. Com equipamentos de captura de sinal Bluetooth e aplicativos de modificação sem autorização, crackers podem roubar dados e senhas de aparelhos celulares ou notebooks que possuam a tecnologia habilitada.

Botnet: são computadores “zumbis”. Em suma, são computadores invadidos por um determinado cracker, que os transforma em um replicador de informações. Dessa forma torna-se mais difícil o rastreamento de computadores que geram spams e aumentam o alcance das mensagens propagadas ilegalmente.

C

Crapware: sabe quando você compra um computador pré-montado e ele chega à sua casa com algumas dúzias de aplicativos que você não faz ideia da funcionalidade? Eles são chamados de *crapware* (em português: software porcaria) e são considerados um “bônus” pelas fabricantes, mas para os usuários são poucos os aplicativos interessantes.

Compromised-Key Attack: são ataques realizados para determinadas chaves de registro do sistema operacional.

Quando o cracker consegue ter acesso às chaves escolhidas, pode gerar logs com a decodificação de senhas criptografadas e invadir contas e serviços cadastrados.

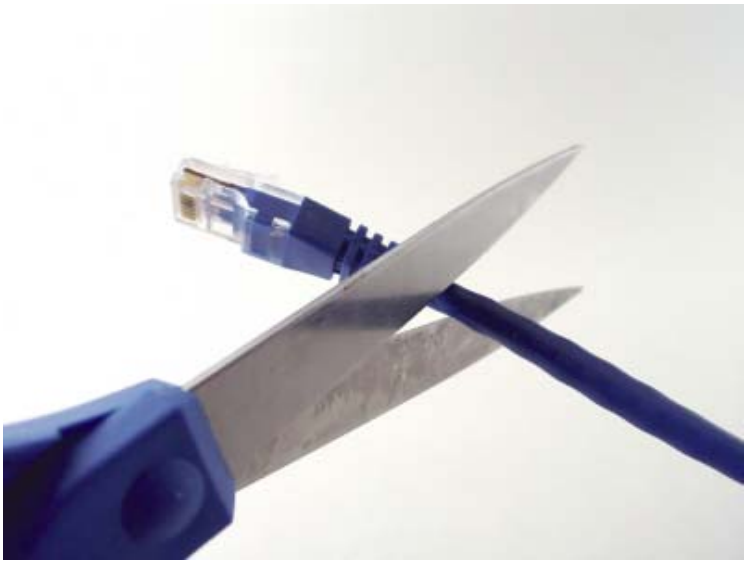
D

Data Modification: alteração de dados. O invasor pode decodificar os pacotes capturados e modificar as informações contidas neles antes de permitir que cheguem até o destinatário pré-definido.

Denial of Service (DoS): "Ataque de negação de serviços" é uma forma de ataque que pretende impedir o acesso dos usuários a determinados serviços. Alvos mais frequentes são servidores web, pois os crackers visam deixar páginas indisponíveis. As consequências mais comuns neste caso são: consumo excessivo de recursos e falhas na comunicação entre sistema e usuário.

Distributed Denial of Service (DDoS): o mesmo que DoS, mas realizado a partir de vários computadores. É um DoS distribuído.

DNS poisoning: "envenenamento do DSN" pode gerar alguns problemas graves para os usuários infectados. Quando ataques deste tipo ocorrem, os usuários atingidos conseguem navegar normalmente pela internet, mas seus dados são todos enviados para um computador invasor que fica como intermediário.



"Drive by Java": aplicativos maliciosos "Drive-by-download" são arquivos danosos que invadem os computadores quando os usuários clicam sobre alguns anúncios ou acessam sites que direcionam downloads sem autorização. O "Drive-by-Java" funciona da mesma maneira, mas em vez de ser por downloads, ocorre devido à contaminação de aplicativos Java.

H

Hacker: são usuários mais curiosos do que a maioria. Eles utilizam essa curiosidade para buscar brechas e falhas de segurança em sistemas já criados. Com esse processo, conseguem muito aprendizado e desenvolvem capacidades de

programação bastante empíricas. Quando utilizam estes conhecimentos para causar danos passam a ser chamados de crackers.

I

ICMP Attack: ataques gerados nos protocolos de controle de mensagens de erro na internet. Um computador com o IP alterado para o endereço de outro usuário pode enviar centenas ou milhares de mensagens de erro para servidores remotos, que irão enviar respostas para o endereço com a mesma intensidade. Isso pode causar travamentos e quedas de conexão no computador vitimado.

ICMP Tunneling: podem ser criados túneis de verificação em computadores invadidos, por meio da emissão de mensagens de erro e sobrecarga da conexão. Com isso, arquivos maliciosos podem passar sem interceptações de firewalls do computador invadido, passando por esses “túneis” de maneira invisível.

IP Spoofing: é uma técnica utilizada por crackers para mascarar o IP do computador. Utilizando endereços falsos, os crackers podem atacar servidores ou computadores domésticos sem medo de serem rastreados, pois o endereço que é enviado para os destinatários é falso.

K

Keylogging: é uma prática muito utilizada por ladrões de contas bancárias. Aplicativos ocultos instalados no computador invadido geram relatórios completos de tudo o que é digitado na máquina. Assim, podem ser capturados senhas e nomes de acesso de contas de email, serviços online e até mesmo *Internet Banking*.

L

Lammer: é o termo utilizado por hackers mais experientes para depreciar crackers inexperientes que utilizam o trabalho de outros para realizar suas invasões. Não se limitam a invadir sites, quando o fazem modificam toda a estrutura e até assinam as “obras” em busca de fama na comunidade.

Logic Bomb: este termo pode ser empregado em dois casos. O primeiro refere-se a programas que expiram após alguma data e então deixam de apresentar algumas de suas funcionalidades. O segundo, mais grave, é utilizado em casos de empresas que utilizam aplicativos de terceiros e quando os contratos são rompidos, estes softwares ativam funções danosas nos computadores em que estavam instalados.

M

Malware: qualquer aplicativo que acessa informações do sistema ou de documentos alocados no disco rígido, sem a autorização do administrador ou usuário, é considerado um malware. Isso inclui vírus, trojans, worms, rootkits e vários outros arquivos maliciosos.

Man-in-the-Middle-Atack: este tipo de ataque ocorre quando um computador intercepta conexões de dois outros. Cliente e servidor trocam informações com o invasor, que se esconde com as máscaras de ambos. Em termos mais simples: pode ser um interceptador de uma conversa de MSN, que passa a falar com os dois usuários como se fosse o outro.

P

Password-based Attacks: é o tipo de ataque gerado por programas criados no intuito de tentar senhas repetidas vezes em curtos intervalos de tempo. Criando instabilidades na verificação do logon referido, podem ser geradas duplicatas de senhas ou logons válidos.

Ping of Death: um invasor realiza constantes *Pings* na máquina invadida para causar travamentos na banda e até mesmo para travar o computador. É um tipo de ataque *Denial of Service*.

Phishing: mensagens de email enviadas por spammers são criadas com interfaces e nomes que fazem referência a empresas famosas e conhecidas, como bancos. Nestas mensagens são colocados links disfarçados, que dizem ser prêmios ou informações sobre a empresa em questão, mas na verdade são arquivos maliciosos.

Phreaker: os hackers de telefonia. São responsáveis pelo roubo de sinal de outros aparelhos e também por desbloquear aparelhos famosos, como é o caso dos especializados em desbloqueio do iPhone.

Pod Slurping: é o nome atribuído às práticas de roubo de informações por meio de dispositivos portáteis pré-configurados para a atividade. Podem ser utilizados pendrives, iPods e muitos outros aparelhos de armazenamento portátil. Há ataques diretos desta maneira e também ataques que apenas abrem portas dos computadores para invasões.

Port Scanning: atividade realizada por *Port scanners*. É a varredura de servidores em busca de portas vulneráveis para a invasão posterior.

R

Repudiation Attacks: quando aplicativos ou sistemas não são criados com os comandos corretos de rastreamento de logs, crackers podem utilizar isso para remodelar os envios de comandos. Assim, podem ser modificados os dados de endereçamento das informações, que são enviadas diretamente para servidores maliciosos.

Rootkit: tipo de malware que se esconde nas bases do sistema operacional, em localidades que não podem ser encontradas por antivírus comuns. São utilizados para interceptar solicitações do sistema operacional e alterar os resultados.

S

Scareware: malwares que são acessados pelos usuários mais desavisados, pois ficam escondidos sobre banners maliciosos. Podem ser percebidos em páginas da web que mostram informações do tipo: “Você está infectado, clique aqui para limpar sua máquina”.

Session hijacking: roubo de sessão. Ocorre quando um usuário malicioso intercepta cookies com dados do início da sessão da vítima em algum serviço online. Assim, o cracker consegue acessar a página do serviço como se fosse a vítima e realizar todos os roubos de informações e modificações que desejar.

Scanners: são softwares que varrem computadores e sites em busca de vulnerabilidades.

Script Kiddy: o mesmo que *Lammer.*

Server Spoofing: o mesmo que *IP Spoofing*, mas direcionado a servidores VPN.

Sidejacking: prática relacionada ao *Session hijacking*, mas geralmente com o invasor e a vítima em uma mesma rede. Muito frequentes os ataques deste tipo em *hotspots* Wi-Fi sem segurança habilitada.

Shovelware: é o tipo de aplicativo que se destaca mais pela quantidade de funcionalidades do que pela qualidade das

mesmas. Muitos conversores multimídia fazem parte deste conceito de *shovelware.*

SMiShing: similar a phishing, mas destinado a celulares (SMS).

Smurf: o mesmo que ICMP Attack.

Sniffer Attack: tipo de ataque realizado por softwares que capturam pacotes de informações trocados em uma rede. Se os dados não forem criptografados, os ofensores podem ter acesso às conversas e outros logs registrados no computador atacado.

Snooping: invasões sem fins lucrativos, apenas para “bisbilhotar” as informações alheias.

Social Engineering (Engenharia Social): é o ato de manipular pessoas para conseguir informações confidenciais sobre brechas de segurança ou mesmo sobre senhas de acesso a dados importantes.

Spam: mensagens enviadas em massa para listas conseguidas de maneira ilegal. Geralmente carregam propagandas sobre pirataria de medicamentos. Também podem conter atalhos para páginas maliciosas que roubam listas de contatos e aumentam o poder de ataque dos spammers.

Spoof: mascarar informações para evitar rastreamento.

Spyware: são aplicativos (*malwares*) instalados sem o consentimento dos usuários. Eles são utilizados para capturar informações de utilização e navegação, enviando os logs para os invasores. *Keyloggers* fazem parte desta denominação.

T

TCP Syn / TCP ACk Attack: ataques realizados nas comunicações entre servidor e cliente. Sendo enviadas mais requisições do que as máquinas podem aguentar, a vítima é derrubada dos servidores e perde a conexão estabelecida. Podem ocorrer travamentos dos computadores atingidos.

TCP Sequence Number Attack: tentativas de previsão da sequência numérica utilizada para identificar os pacotes de dados enviados e recebidos em uma conexão. Quando é terminada com sucesso, pode emular um servidor falso para receber todas as informações do computador invadido.

TCP Hijacking: roubo de sessão TCP entre duas máquinas para interferir e capturar as informações trocadas entre elas.

Teardrop: uma forma de ataque *Denial of Service.* Usuários ofensores utilizam IPs inválidos para criar fragmentos e sobrecarregar os computadores vitimados. Computadores mais antigos podiam travar facilmente com estes ataques.

Trojan: tipo de *malware* que é baixado pelo usuário sem que ele saiba. São geralmente aplicativos simples que escondem funcionalidades maliciosas e alteram o sistema para permitir ataques posteriores.

V

Vírus: assim como os vírus da biologia, os vírus de computador não podem agir sozinhos. Anexam-se a outros arquivos para que possam ser disseminados e infectar mais computadores. São códigos que forçam a duplicação automática para aumentar o poder de ataque e, assim, criar mais estrago.

W

White Hat: hackers éticos.

Worm: funcionam de maneira similar aos vírus, mas não precisam de outros arquivos hospedeiros para serem duplicados. São arquivos maliciosos que podem replicar-se automaticamente e criar brechas nos computadores invadidos. Disseminam-se por meio de redes sem segurança.

.....

Assim termina o glossário de termos que são considerados maliciosos. O Baixaki espera que todos tenham gostado destas informações e que, principalmente, elas tenham sido úteis para o esclarecimento de cada um. Agora deixe um comentário para nos contar se já conhecia todos estes termos e qual achou mais interessante.