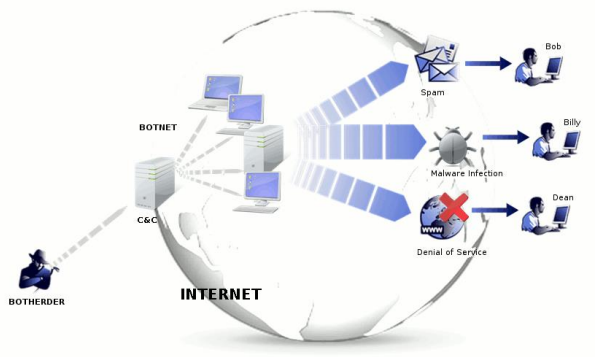
Proteja seu Computador das Botnets, as “Redes Zumbis”

Todos os anos, milhões de máquinas são atingidas pelas botnets; a sua pode ser uma delas. Nunca ouviu falar? Então entenda como funcionam esses ataques e como recuperar o seu computador caso ele tenha sido capturado. O nome botnet vem das paavras em inglês, robot e network, ou seja, rede robô. As botnes também conhecidas como redes de PCs zumbis são malhas de computadores infectados por malwares que podem ser controlados remotamente por cybecriminosos. O termo zumbi existe porque essas máquinas ficam aguardando para responder aos comandos.

Entender como as botnets funcionam parece simples, mas o maior problema é que se a sua máquina realmente estiver sob o domínio das redes zumbis, pode ser que você sequer perceba. As botnets podem ser utilizadas como forma de distribuição de spam, vírus, ou até mesmo para cibe ataques de negação de serviços, DDOs. É quando milhões de PCs tentam acessar um único servidor, invalidando por sobrecarga, uma página de web.

Os prejuízos causados pelas botnets vão além. Segundo uma pesquisa feita por essas empresa em parceria com o FBI, divulgada no início deste mês de Setembro, a infecção por botnets em geral atinge 500 milhões de máquinas por ano, representado perdas de 110 bilhões de dólares no mundo todo. É brincadeira? ***Não***



Se antes as botnets eram poucas conhecidas, hoje, viram negócios profissionalizados em nível mundial. Entenda como funciona essa cadeia?

No primeiro plano, uma hacker desenvolve um software malicioso capaz de invadir máquinas sem ser notado. Ele testa em todos os antivírus, passando por todos os softwares de proteção. Em segundo momento, alguém que possua uma botnets distribui os malwares para diversas máquinas. Aliás, as redes botnets podem se “alugadas” exploradas por qualquer pessoa. O terceiro passo é quando o espião que está dentro do computador, rouba as informações, como informações do seu PC sem ser notado, passando por diversos endereços em diferentes países, assim não se acha o responsável pelo roubo.

No próximo passo uma máquina especializada vai acessar a sua conta e tirar o dinheiro vivo, sem ser preso.

Se você descobriu que seu computador faz parte de uma botnets, uma antivírus eficiente é capaz de remover estres bots. Mas, vale lembrar, que mesmo utilizando algumas medidas básicas de segurança, os computadores podem continuar infectados. Em alguns casos, o estrago é tão grande, que a única saída é formatar a máquina.

Para Evitar os Ataques das Redes Zumbis, Algumas Dicas São Válidas

- Tenham um bom antivírus e um firewall instalados.
- Mantenha versões atualizadas e qualquer tipo de aplicações em seu computador. Versões antigas podem conter brechas de segurança e funcionar como uma porta de entrada para software maliciosos;
- Seja cuidadoso ao instalar aplicativos de desenvolvedores desconhecidos;
- Não saia clicando em tudo o que vê pela frente;
- Nunca é demais lembrar que e mails com assuntos suspeitos, devem ir diretamente para o lixo;
- Atenção redobrada para links enviados, até mesmo por conhecidos: as infecções são grandes através das redes sociais ou e-mails;
- Cuidado ao fazer login em qualquer site.