PCWORLD
TECNOLOGIA+INOVAÇÃO+PRODUTIVIDADE

Now!Digital | IDG Now! | Computerworld | CIO | Macworld | Channelworld | Eventos

Login | Registro | Newsletter Busca: upLexis Search ok

Dicas | Reviews | Downloads | Games | Notícias | Acervo PC World | ShopNow!

Info centers
- Windows
- Notebooks
- Desktops
- Segurança
- Fotografia digital
- Pequenas empresas
- Guia de compras

Twitter

Siga a PCWORLD no twitter

RSS

Acompanhe as novidades do site de PC WORLD em RSS.

RSS Blogs
RSS Reviews
RSS Downloads
RSS Dicas
RSS Mundo Apple
RSS Games
RSS Últimas Notícias

> O que é RSS?

Newsletters

Assine as newsletters do Now!Digital Business. É

[Notícias]

PC WORLD » Notícias » Botnet Kneber: 75 mil computadores corporativos já foram infectados

Botnet Kneber: 75 mil computadores corporativos já foram infectados

Redação da Computerworld/EUA
18-02-2010

Malware rouba credenciais de acesso a e-mails, contas bancárias, redes sociais etc. Mais de 2,5 mil empresas foram afetadas.

E-mail Imprima Comente Erros? a a a Tweet 0 Entre na conversa

Mais de 75 mil computadores corporativos ao redor do mundo foram infectados por um software malicioso, de acordo com a empresa de segurança NetWitness. Ao todo, 2,5 mil companhias foram afetadas, em 196 países.

Segundo a NetWitness, os ataques começaram em 1998, na China e na Europa e recebeu o nome de "botnet Kneber". O propósito do software é roubar senhas para acessar sistemas financeiros online, redes sociais e e-mails, e então transmitir informações para os controladores do sistema.

O botnet conseguiu mais de 68 mil credenciais corporativas, além de acesso a e-mails, contas de banco, Facebook e mais de 2 mil certificados de segurança digital, concluiu a investigação da NetWitness.

A NetWitness afirma que o botnet faz uso sofisticado de um conhecido cavalo de tróia conhecido como ZeuS, famoso por roubar informações de banco.

Quem leu esta matéria também leu:

- Brasil está em 'observação', informa associação antipirataria dos EUA
- Infecção pelo botnet Kneber indica uso de antivírus desatualizado
- Dez tecnologias que precisam urgentemente de padronização

http://pcworld.uol.com.br/noticias/2010/02/18/botnet-kneber-75-mil-computadores-corporativos-ja-foram-infectados/

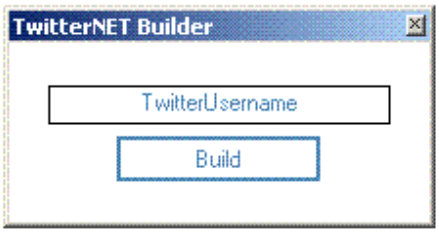
Notícias sobre segurança

Kit de ferramentas de botnet para o Twitter

Thu, 20 May 2010

Os especialistas em segurança de TI da Avira analisaram um kit de ferramentas para um botnet baseado no Twitter e garantiram proteção contra ele

Tettnang, 20 de maio de 2010 – Atualmente, um kit de ferramentas de malware está causando preocupações, pois mesmo os cibercriminosos inexperientes podem usá-lo para produzir um malware, que pode ser distribuído e controlado por meio dos canais do Twitter. As soluções de segurança da Avira garantem proteção contra essa ameaça.



Os especialistas em antivírus da Avira examinaram o kit de ferramentas e os arquivos de malware criados com o kit: com apenas alguns cliques, mesmo sem conhecimento avançado em computadores, cibercriminosos podem criar um malware usando o kit de ferramentas KIT/MSIL.Agent.A.1, que permite a eles criar e controlar um botnet por meio dos canais do Twitter.

A Avira classificou de imediato o drone de botnet como TR/Dropper.Gen com a detecção heurística e agora o identifica como BDS/Twitbot.E. O malware pode iniciar um ataque de negação de serviço distribuído ou fazer download de outros malwares da Internet.

O kit de ferramentas de malware é básico e cria drones de botnet totalmente estáticos. Consequentemente, é fácil detectá-lo e removê-lo de computadores infectados, pois nenhuma função avançada, como rootkits ou autoproteção de processo, é usada.

Entretanto, os usuários não devem subestimar o perigo vindo de drones BDS/Twitbot.E. Se os computadores de usuários inocentes forem infectados com ele, os operadores de botnets criminosos poderão instalar qualquer tipo de malware e causar muito mais danos.

http://row.avira.com/pt-br/noticias_sobre_seguranca/botnet_para_o_twitter.html

Estácio

editorias

Primeira Página
Blogs e Colunas
Brasil
Carros
Ciência e Saúde
Cinema
Concursos e Emprego
Economia e Negócios
Esporte
Mundo
Música
Planeta Bizarro
Política
Pop & Arte
Rio de Janeiro
São Paulo
Tecnologia e Games
VC no G1
Vestibular e Educação
Infográficos
Fotos

03/03/10 - 14h30 - Atualizado em 03/03/10 - 15h26

REUTERS

Estrago de botnet 'Mariposa' poderia ter sido maior, diz polícia

Rede mundial de 'computadores zumbis' é desarticulada na Espanha. 13 milhões de máquinas estavam infectadas em 190 países.

Da Reuters

Tamanho da letra

A- A+

Os administradores da rede que controlava 13 milhões de computadores em 190 países e que foi descoberta pela polícia espanhola não chegaram a aproveitar todo o seu potencial, afirmaram autoridades nesta quarta-feira (3), voltando a defender a necessidade de "navegação responsável" na internet.

"Tivemos sorte por essa 'botnet' com 13 milhões de máquinas estar sob o controle de pessoas que não perceberam as potencialidades que ela oferecia", disse o comandante Juan Salón, chefe da unidade de crimes de computação da Unidade Central de Operações da polícia espanhola, em Madri.

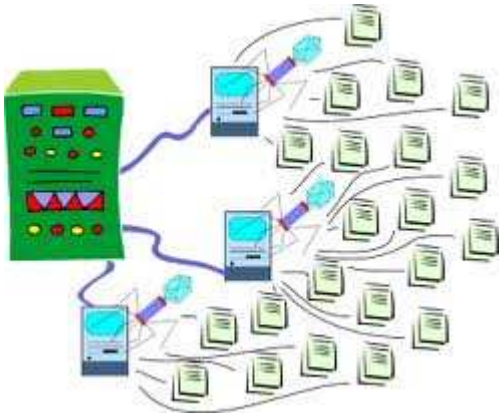
Segundo as autoridades espanholas, a rede descoberta foi a maior já desarticulada até agora pela polícia no mundo. "Temos que nos conscientizar de que a rede pode ser muito positiva, mas é preciso tomar certas medidas básicas. A principal medida de segurança é a navegação responsável", afirmou.

Três jovens espanhois com idades entre 25 e 31 anos foram detidos em Balmaseda, Santiago de Compostela e Molina de Segura, acusados de dirigir uma rede que controlava os computadores depois de infectá-los por meio de um cavalo de troia. A rede permitia aos acusados roubar dados bancários, de correio eletrônico e senhas de milhões de usuários, empresas e até instituições governamentais, ou bloquear suas páginas, segundo as autoridades.

Com essa rede, de acordo com a polícia, poderia ter sido realizado um ataque ciberterrorista muito mais sério do que os executados contra a Estônia ou a Geórgia.

http://g1.globo.com/Noticias/Tecnologia/0,,MUL1513939-6174,00-ESTRAGO+DE+BOTNET+MARIPOSA+PODERIA+TER+SIDO+MAIOR+DIZ+POLICIA.html

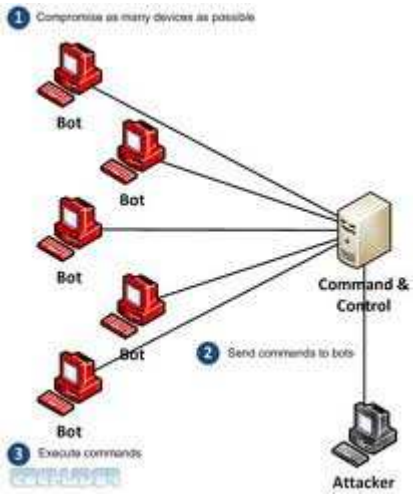
Mas como funciona?



O *bot* é um programa capaz se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador. Ele dispõe de mecanismos de comunicação com o invasor, permitindo que o *bot* seja controlado remotamente.

Obs: não sei se a imagem tem direito autoral, site: http://www.fayerwayer.com.br/tag/botnet/

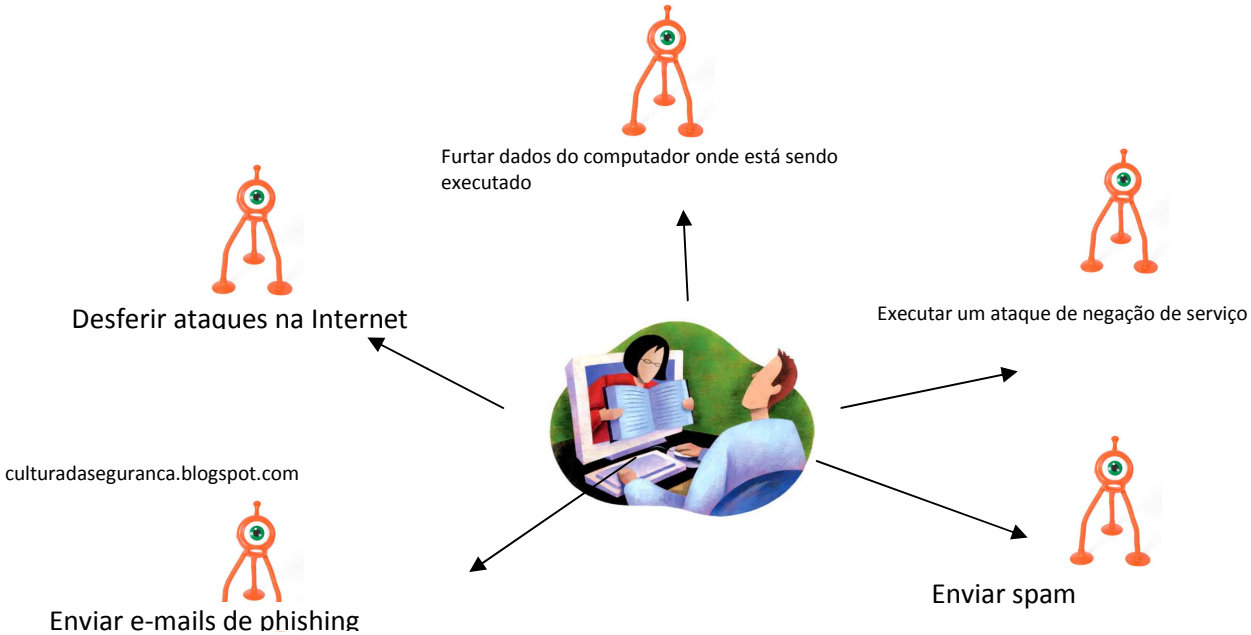
Normalmente, o *bot* se conecta a um servidor de IRC[1] (*Internet Relay Chat*) e entra em um canal (sala) determinado. Então, ele aguarda por instruções do invasor, monitorando as mensagens que estão sendo enviadas para este canal.



O invasor, ao se conectar ao mesmo servidor de IRC e entrar no mesmo canal, envia mensagens compostas por seqüências especiais de caracteres, que são interpretadas pelo *bot*. Estas seqüências de caracteres correspondem a instruções que devem ser executadas pelo *bot*.

[1] **Internet Relay Chat** (**IRC**) é um protocolo de comunicação utilizado na Internet, basicamente como bate-papo (chat) e troca de arquivos, permitindo a conversa em grupo ou privada. Fonte: Wikipédia.

Um invasor, ao se comunicar com um *bot*, pode enviar instruções para que ele realize diversas atividades, tais como:



Para uma melhor compreensão assista ao vídeo : (a defesa) http://www.antispam.br/videos/