



Associação dos Diplomados da Escola Superior de Guerra

Delegacia no Estado de Minas Gerais

“Conhecer o Brasil para melhor servi-lo”



Cyber War – A Nova Guerra

Parte II – As Ações

Por Leonardo SANTOS Silva (022/2007)

1 - Introdução

No primeiro artigo, conhecemos o conceito por trás da cultura dos hackers e vimos suas organizações de acordo com seus ataques. Neste segundo artigo, veremos como geralmente está estruturada uma rede corporativa, como são os ataques que estão ocorrendo no Brasil e como alguns especialistas já consideram que a guerra cibernética já começou.

2 - As redes corporativas

Normalmente, as estruturas das redes corporativas são muito parecidas, no que diz respeito à sua implantação conceitual.

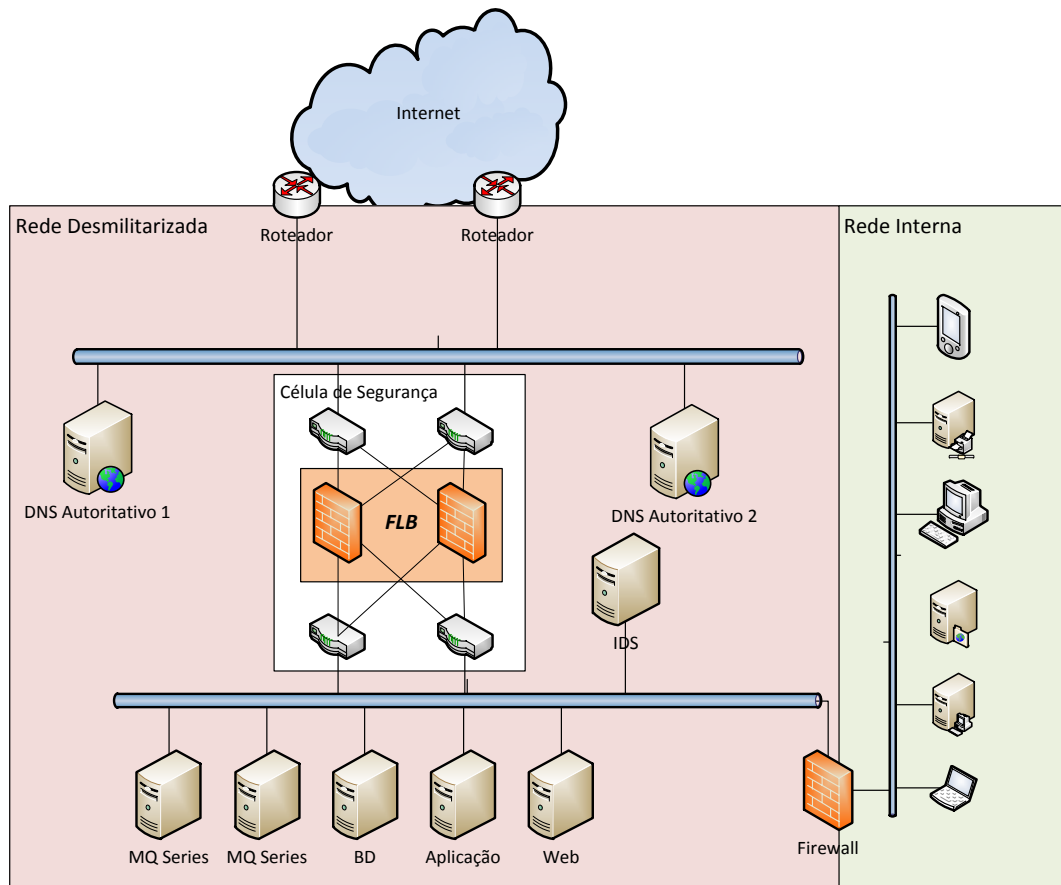


Figura 1 Estrutura típica de segurança em ambientes corporativos

Todo acesso proveniente e destinado à internet passa por uma área chamada Zona Desmilitarizada, ou DMZ. Nesta área o tráfego de dados é analisado por equipamentos como Firewall, Firewall Load Balance (FLB), Detector de Intruso (IDS) e Sistema de Prevenção de Intruso (IPS). Caso os dados de entrada não contenham nenhum comportamento ameaçador, eles são autorizados a seguir para outros servidores ou estações, estejam elas localizadas na DMZ ou na rede interna. Quando existe a necessidade de saída de dados, geralmente verifica-se se o solicitante (usuário ou uma estação) possui privilégios suficientes para que a informação seja enviada para fora da empresa. Caso a autorização exista (geralmente gravada no Firewall), a conexão externa é estabelecida e a comunicação (envio e recebimento de dados) é iniciada.

Dentro da rede interna também existe alguns mecanismos de defesa, geralmente antivírus, firewall nas estações (conhecidos como Firewall de Host) e controles de acesso. Esses componentes, de uma maneira genérica, criam as camadas de proteção que as empresas possuem para se protegerem do mundo externo.

Nesse contexto estão presentes 3 atores que compõem e sustentam os serviços disponibilizados:



Associação dos Diplomados da Escola Superior de Guerra

Delegacia no Estado de Minas Gerais

“Conhecer o Brasil para melhor servi-lo”



- Tecnologia;
- Processos;
- Pessoas.

Qualquer falha em um destes componentes pode levar a um desequilíbrio na balança e provocar prejuízos, sejam eles financeiros, operacionais ou de imagem.

3 - As redes Zumbis e a Preparação do Campo de Batalha – BotNETs

Primeiramente, é necessário definir um termo muito utilizado na área de segurança da informação para descrever a família de programas maliciosos que são criados para causar algum mal nos computadores: Artefatos Maliciosos. Esses artefatos incluem, mas não se limitam a vírus, cavalos de troia, worms (vermes), hoax e discadores. Todos eles realizam tarefas distintas nas máquinas clientes, entre elas, se duplicar, se atualizar, enviar e receber informações, criptografar arquivos, abrir portas para outras invasões, etc.

O grande objetivo dos hackers é infectar o maior número de computadores possível. Diversos meios são usados, entre os mais comuns estão:

- Envio de e-mails com artefatos maliciosos;
- Endereços de internet suspeitos que instalam programas sem a autorização do usuário;
- Duplicação pelas pastas compartilhadas nas redes corporativas;
- Pendrivers, CD's ou DVD's obtidos de maneira suspeita.

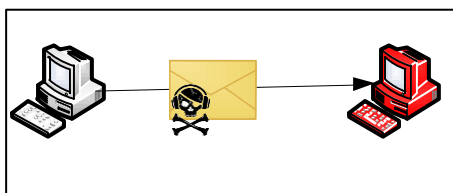


Figura 2 Uma das formas mais comuns de infecção é por e-mails

Uma vez que o artefato malicioso esteja instalado no computador da vítima, várias ações podem ser realizadas, dependendo da característica do programa:

- Roubo de senhas bancárias ou informações pessoais;
- Levantamento do comportamento do usuário;
- Criptografia de arquivos para solicitação de um “resgate” posterior;
- Destruição de dados;
- Criação de uma rede de ataque.



Esse último, a criação de uma rede de ataque, foi a primeira arma que possibilitou o ataque em massa que o Brasil presenciou nos últimos dias.

Um artefato malicioso é instalado na máquina contaminada. Por padrão, essa máquina infectada (chamada de Zumbi) se conecta em um programa de comunicação chamado IRC (Internet Relay Chat), de onde recebe diversas ordens, enviadas por um usuário mestre. As ordens geralmente são:

- attack - Realiza um ataque de negação de serviço (DoS) em um site ou endereço IP específico.
- stop - Para o ataque DoS em um alvo específico.
- stopall - Para o ataque DoS em todos os alvos.
- update - Download e instala uma versão atualizada do artefato malicioso.
- info - Envia as informações do sistema infectado:
 - endereço IP;
 - Nome do computador;
 - Dominio;
 - Nome de Usuário;
 - Sistema Operacional.
- status - Mostra o status do ataque sendo realizado pelo zumbi.

Essas redes de máquinas zumbis infectadas são chamadas de BotNet. Geralmente um grupo controla uma BotNet, com o objetivo de vender os serviços de ataques. Grandes redes chegam a possuir mais de 2.000 máquinas zumbis e seus ataques são vendidos por US\$ 9,00 a hora¹.

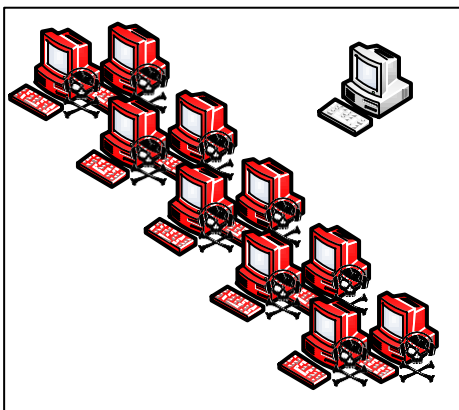


Figura 3 A BotNet sempre recebe as ordens de ataque de um Mestre

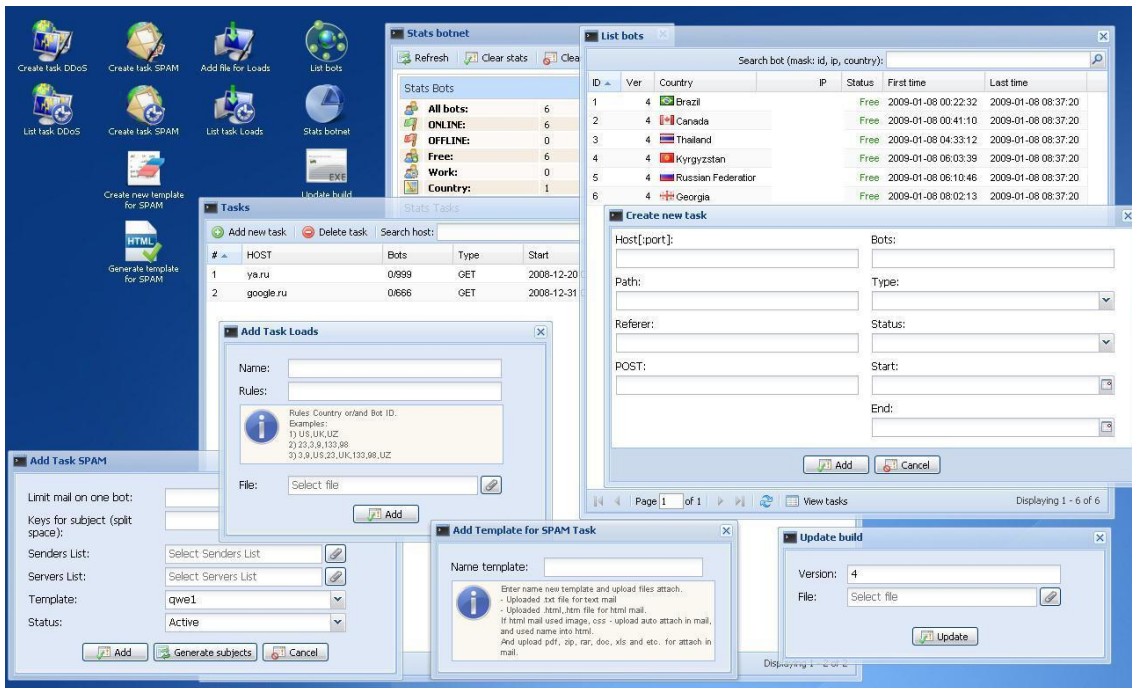


Figura 4 Configuração da BotNet Chimera, que é instalado junto com programas de MP3 gratuitos na Internet

4 - DDoS Atingem os Web Sites do Governo Brasileiro

Os ataques que atingiram algumas páginas da Internet do governo brasileiro e da Petrobrás são conhecidas como Negação de Serviço Distribuído, ou DDoS do inglês (Distributed Denial of Service). Sua característica, como o próprio nome diz, é negar a um usuário a utilização de um serviço. Mas antes de explicar como funciona esse tipo de ataque, é preciso passar algumas noções básicas.

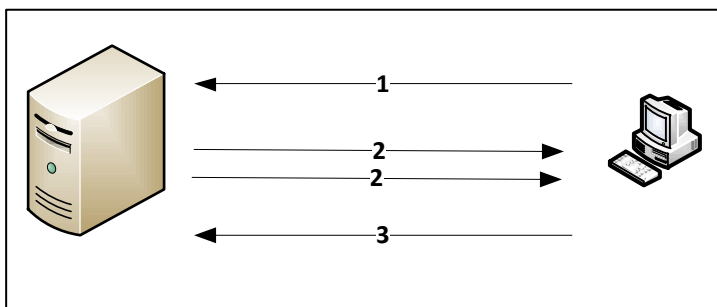


Figura 5 O processo de início de comunicação entre o cliente e o servidor

Quando um computador qualquer faz uma requisição a um servidor (uma página web, um correio eletrônico, etc), três etapas são estabelecidas para que se inicie essa comunicação:

1. O solicitante envia uma mensagem requisitando uma conexão. Algo como um "Olá, sou fulano de Tal; podemos conversar?"
2. O servidor responde a solicitação identificando-se também: "Olá Fulano, sou o Ciclano. Podemos conversar sim". E aguarda a terceira parte da comunicação. Se depois de um



determinado tempo a terceira parte não vier, o servidor envia mais uma requisição, enquanto a conexão está aberta.

3. O solicitante envia uma última mensagem, como se dissesse: “Ok, vamos começar a conversa”. A partir daí, os dados são recebidos e enviados.

Esse é o processo normal de comunicação entre um cliente e um servidor. Mas essa comunicação não ocorre uma vez por cliente, como se fosse em série. Ela acontece com vários clientes simultâneos, já que o Servidor é capaz de “conversar” com vários Clientes ao mesmo tempo.

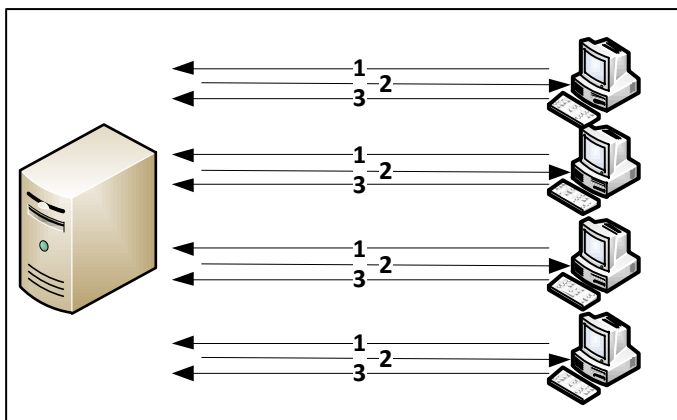


Figura 6 Capacidade do servidor de receber solicitações de comunicação

Entretanto, esse número de clientes que o servidor consegue suportar é limitado. Seja pela capacidade do próprio servidor ou pelo tamanho da banda de internet, chega a um momento em que, vários clientes falando ao mesmo tempo fazem com que o servidor passe a não responder todas as solicitações a ele enviadas, congestionando o canal de comunicação.

Esta situação torna-se perigosamente mais alarmante quando o tráfego que chega aos servidores é proveniente de várias redes BotNet. Essas redes são configuradas para enviar apenas a primeira parte da comunicação com o servidor. Assim, o alvo de um ataque DDoS recebe milhares de milhões de solicitações de “Olá, sou fulano de Tal; podemos conversar?”.

Nesse momento, novas solicitações, sejam elas de redes de ataques BotNet ou usuários autênticos, são ignoradas, pois a fila de espera do servidor para responder é muito longa.

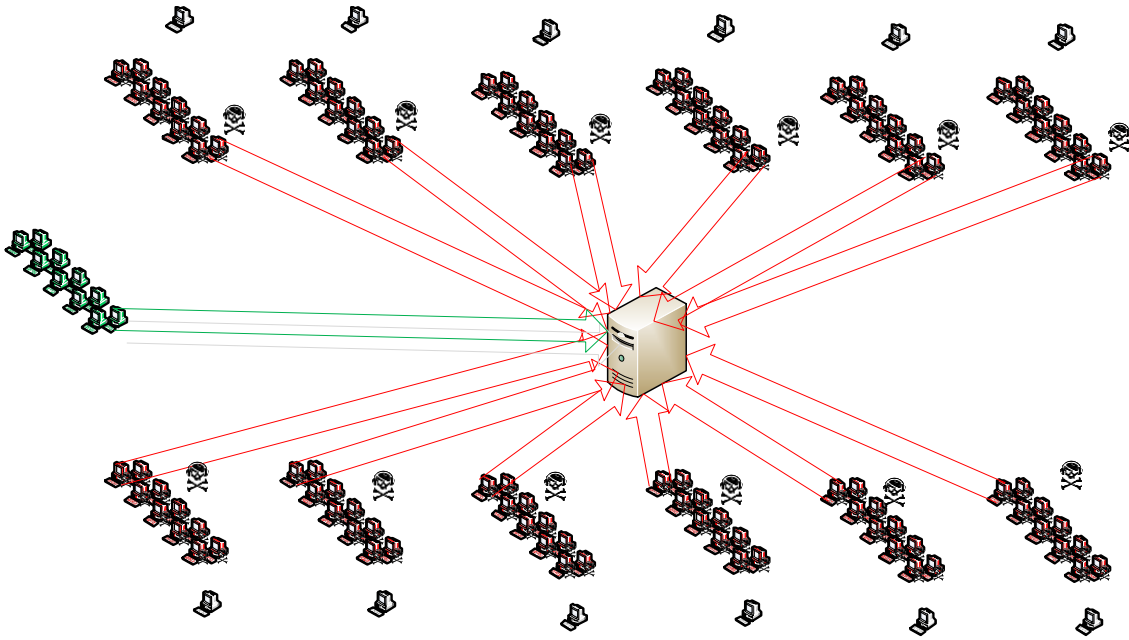


Figura 7 Várias solicitações de comunicação acima da capacidade

Na ilustração acima, podemos imaginar várias redes de ataque a um serviço na Internet (Setas em vermelho), enquanto as requisições autênticas (seta verde) terão as respostas necessárias.

Aparentemente essa é a forma na qual os sites da Presidência da República, do Portal Transparência, da Receita Federal e da Petrobrás foram atingidos. Nenhum dado foi furtado, mas durante a onda de ataque, nenhuma pessoa poderia conseguir as informações necessárias nesses sites.

Uma observação importante é que os atacantes sabiam exatamente onde atacar, pois já haviam feito o mapeamento da rede interna dos sites atacados.

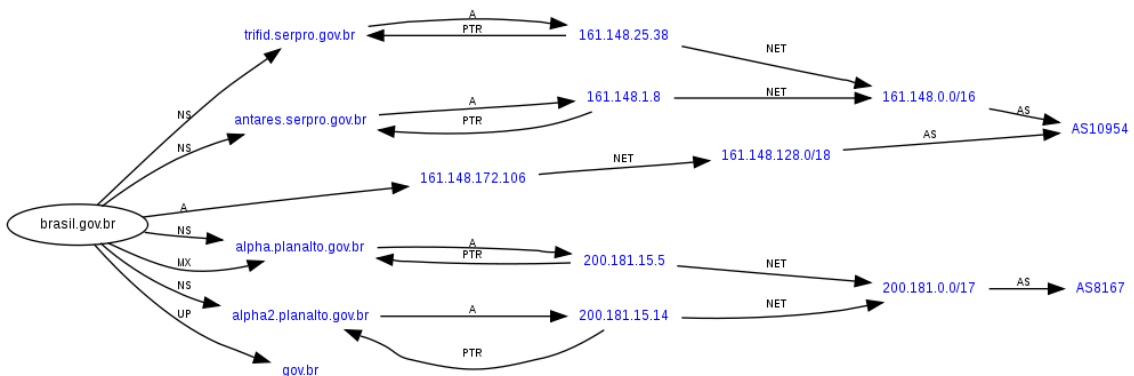


Figura 8 Mapeamento do portal Brasil.gov.br com o endereço dos alvos



Associação dos Diplomados da Escola Superior de Guerra

Delegacia no Estado de Minas Gerais

“Conhecer o Brasil para melhor servi-lo”



A imagem acima foi obtida no endereço “<http://imgpaste.com/i/osxds.png>” e o mapeamento da rede da Petrobrás segue o seguinte endereço: “<http://imgpaste.com/i/ockll.png>”

5 - StuxNET, o Artefato de Guerra

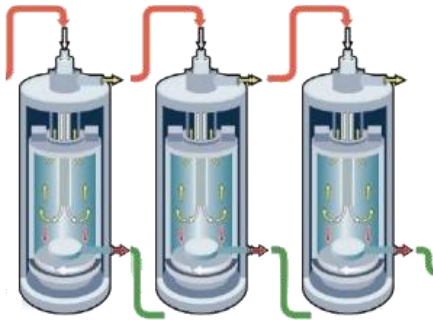
Apesar de acompanharmos casos como o recente ataque a órgãos públicos e privados, no Brasil e no mundo, existe outro tipo de conflito que não é muito explorado, o pelo menos não muito noticiado: quando estados soberanos atacam outros estados.

A Estônia é um país que, como o Brasil, tem grande parte de seus serviços disponíveis na rede. Eleições, sistemas bancários, sistemas do governo, entre outros. Por volta de abril e maio de 2007, este governo do Leste Europeu viveu seus dias de escuridão por causa de um ataque DDoS. A rede central do país foi atacada de tal forma e com tantos pontos de origem que ela simplesmente não conseguia responder a todas as requisições que eram feitas. Com isso, todos os serviços daquele país que necessitavam da rede de computadores para serem executados, ficaram inativos. Supôs-se na época que os ataques foram coordenados por Moscou, uma vez que as instruções de ataque estavam em russoⁱⁱ. Mas se foi um ataque orquestrado pelo Kremlin, ninguém conseguiu provar ao certo.

Mais recentemente, um ataque meticulosamente planejado, acertou as centrífugas nucleares do Irãⁱⁱⁱ, atrasando o projeto de enriquecimento do urânio em pelo menos 10 anos. O que fez deste ataque uma obra prima no meio da segurança da informação foi sua especificidade. Ele foi criado para atacar um componente específico de uma usina nuclear. E tudo isso, ‘personificado’ na figura de um vírus de computador (W32_StuxNet). Apesar de ter sido descoberto em Julho de 2010, investigações mais precisas descobriram que ele estava ativo a pelo menos um ano antes de sua identificação.



Figura 9 O Presidente Iraniano visita as centrífugas, posteriormente danificadas pelo ataque do vírus StuxNet



As centrífugas eram responsáveis pela separação do Urânio 238 do 235 (este último responsável pela produção da energia nuclear). O processo é repetido em várias centrífugas até que o U235 possa ser usado.

Figura 10 Centrífugas de enriquecimento de urânio

A ação do StuxNet é composta de alguns passos que, apesar de parecerem simples, mostram que foi preciso uma equipe especializada em várias matérias para a sua criação:

1. Sua disseminação foi feita por pendrivers 'perdidos' em lugares estratégicos;
2. Quando a pessoa conectava o pendrive no computador, o vírus automaticamente se replicava e infectava o computador;
3. Ele se espalha pela rede através de pastas compartilhadas e do protocolo de impressão para outros computadores;
4. Faz uma série de verificações no computador instalado;
5. Se atualiza com servidores;
6. Se conecta a um Controlador Lógico Programado (PLC) – Somente se esse PLC for um SIEMENS 6ES7-315-2;
7. Altera a programação desses PLC's. Após isso ele entra em um ciclo e execução, de acordo com a figura abaixo.

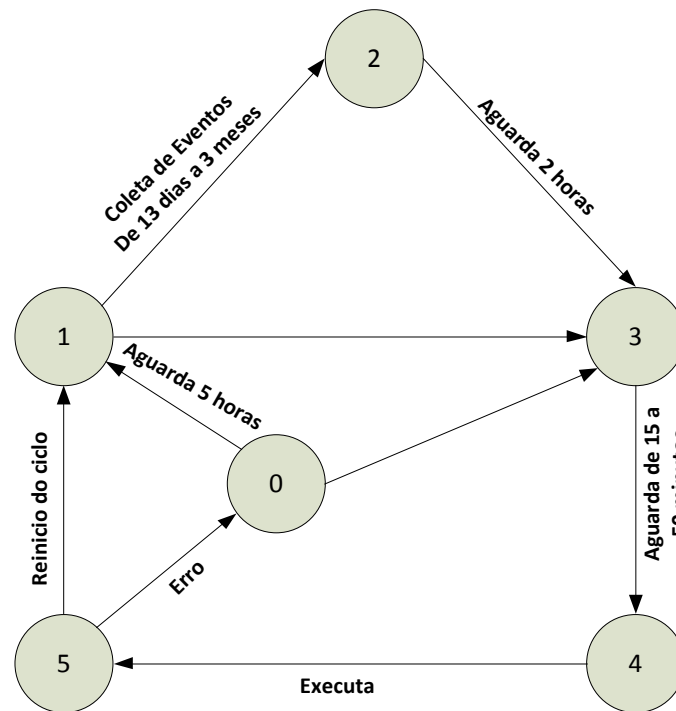


Figura 11 Ciclo de atuação do StuxNet

Assim, o vírus aumentava ou diminuía a velocidade de rotação das centrífugas, fazendo com que a separação do U235 e U238 não funcionasse corretamente.

6 – Mitigação

Existe um ditado na área de segurança da informação que diz que “nenhum sistema é 100% seguro”. Ao levarmos isso em consideração, sempre devemos ficar alertas para os fatos recentes. Ninguém precisa ser um especialista em tecnologia para se manter mais seguro quando acessa a Internet. Algumas pequenas ações ajudam muito na prevenção de incidentes de segurança, entre elas:

- Possua um antivírus confiável e principalmente, atualizado diariamente. A cada dia, novas pragas virtuais são criadas e para identifica-las, o antivírus deve estar atualizado;
- Utilize o Firewall do seu Sistema Operacional ou Antivírus. Normalmente, os sistemas Operacionais (Windows, Linux, Mac OS, etc) em suas versões mais recentes, possuem Firewall nativo. Programas de antivírus mais completos, também possuem um firewall mais completo que as versões dos sistemas operacionais. Esses programas conseguem impedir que atacantes invadam seu computador e que informações sejam roubadas, ou que o computador realize um ataque de DoS;
- Mantenha seu sistema operacional e principais aplicativos atualizados. Os principais fornecedores (Microsoft, diversas distribuições de Linux, Apple) geralmente disponibilizam essas atualizações na internet e de forma gratuita. Até mesmo dentro



do Sistema Operacional, existe a possibilidade de pesquisar quais as atualizações que estão faltando e instala-las automaticamente;

- Desconfie de e-mails enviados de maneira genérica (seu nome consta no nosso cadastro, você foi sorteado, sua mulher está te traindo) e solicitando que você abra um arquivo ou clique em um link específico. Também desconfie de programas gratuitos na internet. Muitos deles incluem artefatos maliciosos escondidos que são instalados sem a sua autorização e consentimento.

São ações pequenas, simples e individuais, mas que garantem uma maior segurança na utilização da Internet.

7 - Conclusão

Há uma guerra sendo travada. Grupos independentes ou patrocinados por estados estão em movimento e já mostraram do que são capazes. Essa nova guerra assemelha-se com o que foi visto no Vietnã quando forças Norte Americanas combateram um exército menos numeroso. O combate era assimétrico e mesmo assim, o governo de Washington sofreu uma de suas maiores derrotas na história. Da mesma forma que o Brasil treina seus combatentes para uma guerra assimétrica na Amazônia (CIGS), o Pentágono e a OTAN já estão há tempos se preparando para um confronto futuro baseado no campo de batalha virtual.

Sobre o Autor



Leonardo Santos Silva (LeoSantos@LeonardoSantos.com.br) é Administrador, com MBA em Gestão Executiva e Adesguiano da turma de 2007. Já atuou em diversas empresas como especialista em Segurança da Informação, possuindo vários certificados na área e realizando análises de risco, criando Plano de Continuidade de Negócios, Política de Segurança da Informação, Infraestrutura de Chaves Públicas, Análises Criptográficas e Defesa em Perímetro.

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

ⁱ <http://www.zdnet.com/blog/security/study-finds-the-average-price-for-renting-a-botnet/6528>

ⁱⁱ <http://info.abril.com.br/aberto/infonews/052007/18052007-4.shl>

ⁱⁱⁱ <http://tecnologia.terra.com.br/noticias/0,,OI4797271-EI12884,00-Virus+Stuxnet+e+ameaca+a+industriaschave+de+todo+o+mundo.html>