O que são vírus?

Um vírus é a forma mais antiga de malware e é de longe o mais conhecido por todos. Mas o que é um vírus? O que separa um vírus de outras formas de malwares? Como um vírus é criado, e como ele ataca sua vítima?

O primeiro código que poderia ser classificado como um vírus chegou por volta de 1970 na forma do projeto Creeper. Este projeto implementou capacidades como a replicação e a capacidade de infectar um sistema. O projeto também gerou outro vírus conhecido como o reaper, que removeu o Creeper de qualquer sistema infectado com o código.

A vida e os tempos de um vírus

Vamos explorar o que significa ser um vírus antes de ir adiante. Simplificando, um vírus é um aplicativo auto-replicante que se anexa a outros programas executáveis. Muitos vírus infectam o host assim que são executados; Outros permanecem em espera, adormecidos, até um evento ou tempo predeterminado, antes de executar suas instruções. O que o vírus faz então? Muitas ações potenciais podem ocorrer, como estas:

- Alteração de dados
- Infectar outros programas
- Replicar-se
- Criptografar-se
- Transformando-se em outra forma
- Alteração de configurações
- Destruir dados
- Corromper ou destruir hardware

Os vírus não se restringem às ações listadas aqui e podem facilmente realizar uma ampla gama de atividades em potencial. Os autores de malware estão constantemente desenvolvendo e

melhorando a sua arte, por isso você deve estar sempre alerta, a fim de pegar as novas variações.

O processo de desenvolvimento de um vírus é muito metódico. O autor está preocupado com a criação de um vírus eficaz que pode ser facilmente difundido. O processo ocorre em seis etapas:

1. **Design** – O autor prevê e cria o vírus. O autor pode optar por criar o vírus completamente a partir do zero ou usar um dos muitos kits de construção que estão disponíveis para criar o vírus de sua escolha;
2. **Replicação** – Uma vez implantado, o novo vírus se espalha através da replicação: multiplicando e, em seguida, se espalhando para diferentes sistemas. Como este processo ocorre depende da intenção original do autor, mas o processo pode ser muito rápido, com novos sistemas infectados em curto prazo;
3. **Lançamento** – O vírus começa a fazer seu trabalho sujo executando a tarefa para a qual foi criado (como destruir dados ou alterar as configurações de um sistema). Uma vez que o vírus se ativa através de uma ação do usuário ou outra ação predeterminada, a infecção começa;
4. **Detecção** – O vírus é reconhecido como tal após infectar sistemas durante algum período de tempo. Durante esta fase, a natureza da infecção é tipicamente relatada a fabricantes de antivírus, que iniciam suas pesquisas iniciais sobre como o software funciona e como erradicá-lo;
5. **Incorporação** – Os fabricantes de antivírus determinam uma maneira de identificar o vírus e incorporar o processo em seus produtos através de atualizações. Normalmente, o malware recém-identificado é incorporado em arquivos de assinatura, que são baixados e instalados pelo antivírus;
6. **Eliminação** – Os usuários dos produtos antivírus

incorporam as atualizações em seus sistemas e eliminam o vírus.

É importante perceber que esse processo não é linear: é um loop ou ciclo. Quando a etapa 6 é atingida, todo o processo começa na etapa 1 com outra rodada de desenvolvimento de vírus.

Por que as pessoas criam vírus? Há uma série de razões, tais como curiosidade, hacktivismo, mostrando, e muitos outros que podem ou não fazer sentido para alguém fora do processo. Como um pentester, você pode achar que a criação de um vírus é algo que você precisa fazer a fim de testar adequadamente sistemas defensivos.

Todos os vírus não são criados iguais. Cada um pode ser criado, implantado e ativado de diferentes maneiras, com objetivos diferentes em mente, por exemplo:

- Em meados da década de 1970, um novo recurso foi introduzido no vírus Wabbit. Este vírus representou uma mudança nas táticas e demonstrou uma das características associadas aos vírus modernos: a replicação. O vírus replicado no mesmo computador repetidamente até que o sistema foi invadido e eventualmente caiu;
- Em 1982, o primeiro vírus visto fora da academia estreou na forma do vírus Elk Cloner. Este pedaço de malware estreou outro recurso de vírus mais tarde – a capacidade de se espalhar rapidamente e permanecer na memória do computador para causar mais infecção. Uma vez residente na memória, ele infectava disquetes colocados no sistema, como muitos vírus mais tarde fariam. Hoje em dia, este vírus seria espalhado através de dispositivos USB, como flash drives;
- Quatro anos mais tarde, o primeiro vírus compatível com PC estreou. Os vírus anteriores a este ponto foram concebidos para o Apple II ou para redes de pesquisas específicas. Em 1986, o primeiro vírus boot-

sector estreou, demonstrando uma técnica mais tarde visto em uma escala muito mais ampla. Esse tipo de vírus infectou o setor de inicialização de uma unidade e espalhou sua infecção quando o sistema estava passando por seu processo de inicialização;

- A primeira bomba lógica estreou em 1987: o vírus de Jerusalém. Este vírus foi concebido para causar danos apenas numa determinada data: sexta-feira 13. O vírus foi assim chamado por causa de sua descoberta inicial em Jerusalém;
- Os vírus multipartidos apareceram em 1989 no vírus Ghostball. Este vírus foi projetado para causar danos usando múltiplos métodos e componentes, todos os quais tinham de ser neutralizados e removidos para limpar o vírus de forma eficaz;
- Os vírus polimórficos apareceram pela primeira vez em 1992 como uma forma de evadir as técnicas precoces de detecção de vírus. Os vírus polimórficos são projetados para alterar seu código e forma para evitar a detecção por antivirus, que procuram um código de vírus específico e não a nova versão. Os vírus polimórficos empregam uma série de técnicas para mudar ou mutar, incluindo o seguinte:
    - Motor polimórfico – altera ou altera o design do dispositivo, mantendo intacto a carga útil (a parte que causa os danos);
    - Criptografia – Usado para embaralhar ou ocultar o payload prejudicial, evitando que os mecanismos de antivírus detectem;

      Quando implantado, esse tipo de vírus muda cada vez que é executado e pode resultar em até 90% de alteração no código, tornando-o praticamente não identificável por um antivírus.
- Os vírus metamórficos reescrevem-se completamente em cada infecção. A complexidade desses vírus é imensa, com até 90% de seu código dedicado ao processo de mudança e reescrita da carga. Em essência, este tipo de vírus

possui a capacidade de se reprogramar. Através deste processo, tais vírus podem evitar a detecção por aplicações antivírus;
- Mocmex – Em 2008, ele foi enviado em molduras de fotos digitais fabricados na China. Quando o vírus infectou um sistema, o firewall do sistema e o software antivírus foram desativados; Então o vírus tentou roubar senhas de jogos online.

Tipos de vírus

Os vírus modernos vêm em muitas variedades:

- Um sistema ou vírus de setor de inicialização (boot sector) é projetado para infectar e colocar seu próprio código no registro mestre de inicialização (MBR) de um sistema. Uma vez que essa infecção ocorre, a sequência de inicialização do sistema é efetivamente alterada, o que significa que o vírus ou outro código pode ser carregado antes do próprio sistema. Os sintomas pós-infecção, como problemas de inicialização, problemas com a recuperação de dados, instabilidade no desempenho do computador e incapacidade de localizar discos rígidos são problemas que podem surgir;
- Os vírus de macro entraram em vigor em 2000. Apropriam-se das linguagens incorporadas, como o Visual Basic for Applications (VBA). Em aplicações como o Microsoft Excel e Word, estas linguagens de macros são concebidas para automatizar funções e criar novos processos. O problema com estas línguas é que elas se prestam muito eficazmente ao abuso; Além disso, eles podem ser facilmente incorporados em arquivos de modelo e arquivos de documentos comuns. Uma vez que a macro é executada no sistema de uma vítima, ela pode fazer todos os tipos de coisas, como alterar uma configuração do sistema para diminuir a segurança ou ler o catálogo de endereços de um usuário e enviar e-mails para outros (o que aconteceu

em alguns casos iniciais). Um excelente exemplo desse tipo de vírus é o vírus Melissa do final da década de 1990;

- Os vírus de cluster são outra variação da árvore genealógica que realiza seu trabalho sujo de uma outra forma original. Esse vírus altera as tabelas de alocação de arquivos em um dispositivo de armazenamento, fazendo com que as entradas de arquivo apontem para o vírus em vez do arquivo real. Na prática, isso significa que quando um usuário executa um determinado aplicativo, o vírus é executado antes que o sistema execute o arquivo real. Tornar esse tipo de vírus ainda mais perigoso é o fato de que os utilitários de reparo de unidade infectados causam problemas de uma variedade ainda mais difundida. Utilitários como o ScanDisk podem até mesmo destruir seções da unidade ou eliminar arquivos;
- Um vírus stealth ou tunneling é projetado para empregar vários mecanismos para fugir dos sistemas de detecção. Os vírus furtivos empregam técnicas específicas, incluindo interceptar chamadas do sistema operacional e retornar respostas falsas ou inválidas que são projetadas para engana;
- Os vírus de criptografia são um recém-chegado à cena. Eles podem se misturar para evitar a detecção. Este vírus muda seu código de programa, tornando quase impossível detectar usando meios normais. Ele usa um algoritmo de criptografia para criptografar e descriptografar o vírus várias vezes como ele replica e infecta. Cada vez que o processo de infecção ocorre, uma nova seqüência de criptografia ocorre com configurações diferentes, tornando difícil para o software antivírus detectar o problema;
- Os vírus de cavidade ou de sobrescrita de arquivos se escondem em um arquivo do host sem alterar a aparência do arquivo do host, de modo que a detecção torna-se difícil. Muitos vírus que fazem isso também implementar técnicas furtivas, para que você não ver o aumento no

tamanho do arquivo quando o código do vírus está ativo na memória;

- Sparse-virus infector evita a detecção, realizando suas ações infecciosas apenas esporadicamente, como a cada 10 ou 25 ativações. Um vírus pode até ser configurado para infectar apenas arquivos de um determinado tamanho ou tipo ou que comecem com uma determinada letra;
- Um companheiro ou vírus camuflagem compromete um recurso dos sistemas operacionais que permite que o software com o mesmo nome, mas de diferentes extensões, operem com prioridades diferentes. Por exemplo, você pode ter program.exe em seu computador, e o vírus pode criar um arquivo chamado program.com. Quando o computador executa o program.exe, o vírus executa o programa antes de executar o program.exe. Em muitos casos, o programa real é executado, de modo que os usuários acreditam que o sistema está funcionando normalmente e não estão cientes de que um vírus foi executado no sistema;
- Uma bomba lógica é projetada para esperar até que um evento ou ação predeterminada ocorra. Quando este evento ocorre, a bomba ou carga útil detona e executa a ação pretendida ou projetada. Bombas lógicas têm sido notoriamente difíceis de detectar porque não parecem prejudiciais até que sejam ativadas – e até lá, pode ser tarde demais. Em muitos casos, a bomba é separada em duas partes: o payload e o gatilho. Não parece ser perigoso até que o evento predeterminado ocorra;
- Os vírus de arquivo ou multipartite infectam sistemas de várias maneiras usando múltiplos vetores de ataque, daí o termo multipartite. Os alvos de ataque incluem o setor de inicialização e os arquivos executáveis no disco rígido. O que torna esses vírus perigosos e armas poderosas é que para detê-los, você deve remover todas as suas partes. Se qualquer parte do vírus não é erradicada do sistema infectado, ele pode reinfectar o sistema;
- Os vírus Shell são outro tipo de vírus onde o software

infecta o aplicativo alvo e o altera. O vírus torna o programa infectado em uma sub-rotina que é executada depois que o próprio vírus é executado;
- Os criptovírus buscam arquivos ou certos tipos de dados em um sistema e depois os criptografam. Em seguida, a vítima é instruída a entrar em contato com o criador do vírus através de um endereço de e-mail especial ou outros meios e pagar uma quantidade específica (resgate) para a chave para desbloquear os arquivos;

Um hoax não é um vírus como as outras formas que vimos aqui, mas é importante saber que um hoax pode ser tão poderoso e devastador quanto um vírus. Os hoaxes são projetados fazer o usuário tomar uma ação mesmo que nenhuma infecção ou ameaça exista.

Como criar um vírus

Criar um vírus é um processo que pode ser muito complicado ou algo que acontece com alguns cliques de botão. Programadores avançados podem optar por codificar o malware a partir do zero. Os menos experientes ou experientes podem ter que usar outras opções, como a contratação de alguém para escrever o vírus, compra de código ou usar um virus-maker “subterrâneo” ou do “mercado negro”.

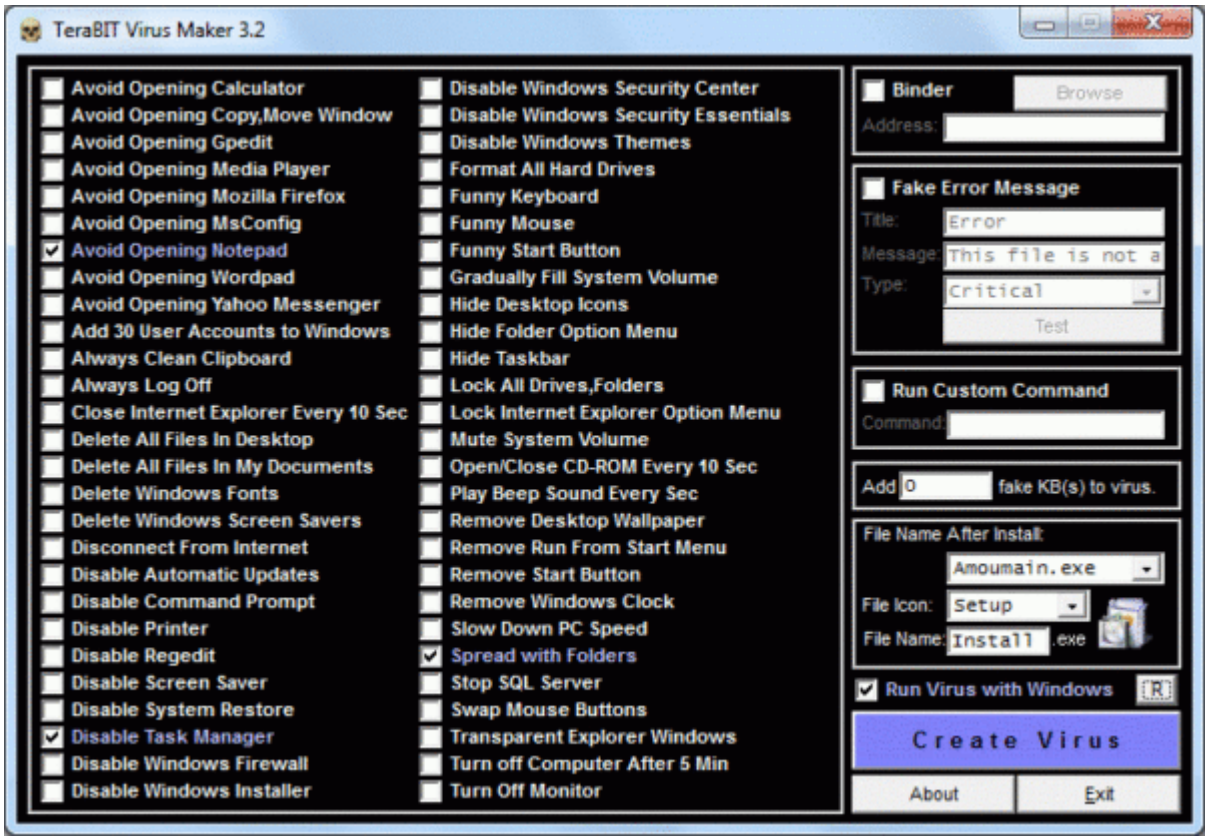
Criando um vírus simples

Então, vamos escrever um vírus simples. Você precisa acessar o Bloco de Notas e bat2com (você pode encontrar na Internet).

Antes de começar, aqui está um aviso: Não execute este vírus. Este exercício pretende ser uma prova de conceito e apenas para fins ilustrativos. Executar este código em seu sistema pode resultar em danos ao seu sistema que podem exigir tempo e habilidade para corrigir corretamente. Com isto dito, seguem as etapas para criar um vírus:

1. Crie um arquivo batch chamado *virus.bat* usando o Bloco de Notas do Windows.
2. Insira as seguintes linhas de código:
   @echo off
   Del c:\windows\system32*.*
   Del c:\windows*.*
3. Salve o arquivo virus.bat.
4. No prompt de comando, use bat2com para converter virus.bat em virus.com.

Outra forma de criar um vírus é usar um utilitário como o "JPS Virus Maker". É um utilitário simples no qual você escolhe opções de uma interface e então escolhe criar um novo arquivo executável que pode ser usado para infectar um host. A imagem abaixo mostra a interface do JPS Virus Maker.



Pesquisando vírus

Existem muitas técnicas defensivas para combater o malware, mas o que dizer da pesquisa de novos malwares? Se você precisa

investigar e analisar malware, além de defender contra ele, você deve saber sobre um mecanismo conhecido como um *sheep-dip system*. Um *sheep-dip system* é um computador que é configurado especificamente para analisar arquivos. O sistema normalmente é simples, sem muitos recursos e inclui apenas os serviços e aplicativos necessários para testar o software para verificar se é seguro.

Fora da computação, o termo *sheep-dip* refere-se à prática dos fazendeiros de mergulhar os carneiros em fungicidas especiais e outros medicamentos para evitar que parasitas e infecções se espalhem através do rebanho, tanto como um pedaço de software é analisado antes de ser introduzido na rede, a fim de evitar uma infecção em massa do sistemas.

Sugestões de livros: