ESTADO DE SANTA CATARINA

MUNICÍPIO DE JABORÁ

SECRETARIA MUNICIPAL DE EDUCAÇÃO E DESPORTO

ESCOLA BÁSICA MUNICIPAL ALBERTO BORDIN

PROFESSOR: ORIDES PARIZOTTO

ALUNO: _____8º ANO_____

7ª ETAPA DE ATIVIDADES PEDAGÓGICAS NÃO PRESENCIAIS E/OU PRESENCIAIS DO ENSINO FUNDAMENTAL, DE INFORMÁTICA.

DATA: 17/05/2021 Á 28/05/2021

VÍRUS ELETRÔNICO DE COMPUTADOR

Em informática, um vírus de computador é um software malicioso que é desenvolvido por programadores geralmente inescrupulosos. Tal como um vírus biológico, o programa infecta o sistema, faz cópias de si e tenta se espalhar para outros computadores e dispositivos de informática.

A maioria das contaminações ocorre por ação do usuário. Um exemplo muito comum se dá por meio do download de arquivos infectados que são recebidos em anexos de e-mails. A contaminação também pode ocorrer de outras formas: acessando sites de procedência duvidosa ou ainda por meio de arquivos infectados em pen drives, CDs, DVDs ou qualquer outro tipo dispositivo de armazenamento de dados. Uma outra maneira de ter um dispositivo contaminado, seria por meio de um Sistema Operacional desatualizado, sem as devidas correções de segurança que visam barrar o acesso indevido destes softwares maliciosos que tentam entrar nas máquinas via Internet.

Existem vários tipos de vírus, alguns assim que alojados na máquina, que agem instantaneamente. Outros procuram por informações específicas e ainda há outros que permanecem ocultos em determinadas horas ou até mesmo por dia. Estes, geralmente, entram em execução em horas ou datas específicas.

Crackers e hackers

Nos anos 90 eram aficionados em informática, conheciam muitas linguagens de programação e quase sempre jovens, que criavam seus vírus, para muitas vezes, saber o quanto eles poderiam se propagar. Atualmente é completamente diferente; são pessoas que atacam outras máquinas com fins criminosos com um objetivo traçado: capturar senhas bancárias, números de conta e informações privilegiadas que lhes despertem a atenção.

Há quem diga que cracker e hacker são a mesma coisa, mas tecnicamente há diferenças:

Hacker

São os que quebram senhas, códigos e sistemas de segurança por puro prazer em achar tais falhas. Preocupam-se em conhecer o funcionamento mais íntimo de um sistema computacional, ou seja, sem intenção de prejudicar ou invadir sistemas operacionais ou banco de dados.

Em geral um hacker não gosta de ser confundido com um cracker. Nesta polêmica, o termo hacker é recuperado por programadores de computador que argumentam que alguém que invade computadores é chamado de cracker.

Cracker

É o criminoso virtual que extorque pessoas usando seus conhecimentos, usando as mais variadas estratégias. Seu interesse é basicamente o vandalismo.

Porém, já se criou um verdadeiro mercado negro de vírus de computador, onde certos sites, principalmente russos, disponibilizam downloads de vírus e kits para qualquer um que puder pagar, virar um Cracker, o que é chamado de terceirização da "atividade".

Principais tipos de vírus de computadores

Vírus de Boot

Um dos primeiros tipos de vírus conhecido, o vírus de boot infecta a parte de inicialização do sistema operacional. Assim, ele é ativado quando o disco rígido é ligado e o Sistema Operacional é carregado.

Time Bomb

Os vírus do tipo "bomba-relógio" são programados para se ativarem em determinados momentos, definidos pelo seu criador. Uma vez infectando um determinado sistema, o vírus somente se tornará ativo e causará algum tipo de dano no dia ou momento previamente definido. Alguns vírus se tornaram famosos, como o "Sexta-Feira 13", "Michelangelo", "Eros" e o "1º de Abril (Conficker)".

Minhocas, worm ou vermes

Como o interesse de fazer um vírus é ele se espalhar da forma mais abrangente possível, os seus criadores por vezes, deixaram de lado o desejo de danificar o sistema dos usuários infectados e passaram a programar seus vírus de forma que apenas se repliquem, sem o objetivo de causar graves danos ao sistema. Desta forma, os seus autores visam a tornar suas criações mais conhecidas na Internet. Este tipo de vírus passou a ser chamada de verme ou worm. Eles estão mais aperfeiçoados, já há uma versão que ao atacar a máquina hospedeira, não só se replica, mas também se propaga pela INTERNET, pelos e-mails que estão registrados no cliente de e-mail, infectando as máquinas que abrirem aquele e-mail, reiniciando o ciclo .

Cavalos de Troia (Trojans)

Certos vírus trazem em seu bojo um código a parte, que permite a um estranho acessar o micro infectado ou coletar dados e enviá-los pela Internet para um desconhecido, sem notificar o usuário. Estes códigos são denominados de Trojans ou Cavalos de Troia. Apesar de popularmente costumar-se denominar “vírus” qualquer ataque à segurança do computador, de acordo com o CERT.br (2012, p. 113), o vírus e o Cavalo de Troia são tipos distintos de código malicioso (malware), sendo este o termo correto aplicável a qualquer software desenvolvido com a finalidade de causar dano ao computador.

Inicialmente, os Cavalos de Troia permitiam que o micro infectado pudesse receber comandos externos, sem o conhecimento do usuário. Desta forma o invasor poderia ler, copiar, apagar e alterar dados do sistema. Atualmente os Cavalos de Troia procuram roubar dados confidenciais do usuário, como senhas bancárias.

Os vírus eram, no passado, os maiores responsáveis pela instalação dos Cavalos de Troia como parte de sua ação, pois eles não têm a capacidade de se replicar.

Atualmente, os Cavalos de Troia não mais chegam exclusivamente transportados por vírus, mas instalados quando o usuário baixa um arquivo da internet e o executa. Prática eficaz devido a enorme quantidade de e-mails fraudulentos que chegam nas caixas postais dos usuários. Tais e-mails contém um endereço na Web para a vítima baixar o Cavalo de Troia, ao invés do arquivo que a mensagem diz ser. Esta prática se denomina phishing, expressão derivada do verbo to fish, "pescar" em inglês. Atualmente, a maioria dos Cavalos de Troia visam a sites bancários, "pescando" a senha digitada pelos usuários dos micros infectados. Há também Cavalos de Troia que ao serem baixados da Internet vêm "guardados" em falsos programas ou em anexos de e-mail, encriptografam os dados e os comprimem no formato "zip", "rar" ou de outro tipo de compactação de arquivos. Um arquivo .txt dá as "regras do jogo": os dados "sequestrados" só serão "libertados" mediante pagamento em dinheiro para uma determinada conta bancária, quando será fornecido o código restaurador.

Hijackers

Hijackers são programas ou scripts que "sequestram" navegadores de Internet. Quando isso ocorre, o hijacker altera a página inicial do browser e impede o usuário de mudá-la, exibe propagandas em pop-ups ou janelas novas, instala barras de ferramentas no navegador e podem impedir acesso a determinados sites (como sites de software antivírus, por exemplo).

Estado Zombie

O estado zombie em um computador ocorre quando é infectado e está sendo controlado por terceiros. Podem usá-lo para disseminar, vírus, keyloggers, e procedimentos invasivos em geral. Usualmente esta situação ocorre pelo fato da máquina estar com seu Firewall e ou Sistema Operacional desatualizados. Segundo estudos na área, um computador que está na internet nessas condições tem quase 50% de chance de se tornar uma máquina zumbi, que dependendo de quem está controlando, quase sempre com fins criminosos, como acontece vez ou outra, quando crackers são presos por formar exércitos zombies para roubar dinheiro das contas correntes e extorquir

Vírus de Macro

Os vírus de macro (ou macro vírus) vinculam suas macros a modelos de documentos gabaritos e a outros arquivos de modo que, quando um aplicativo carrega o arquivo e executa as instruções nele contidas, as primeiras instruções executadas serão as do vírus.

Vírus de macro são parecidos com outros vírus em vários aspectos: são códigos escritos para que, sob certas condições, este código se "reproduz", fazendo uma cópia dele mesmo. Como outros vírus, eles podem ser escritos para causar danos, apresentar uma mensagem ou fazer qualquer coisa que um programa possa fazer.

Bugs

Os bugs, falhas no código do software, não são um tipo de malware, mas erros cometidos pelo programador. Eles podem ter efeitos prejudiciais sobre o computador, como travamento, falhas ou redução do desempenho. Os bugs de segurança, por outro lado, são vias fáceis para os invasores burlarem sua defesa e infectar a máquina. Melhorar o controle de segurança por parte do desenvolvedor ajuda a eliminar bugs, mas também é fundamental aplicar as correções de software para resolver bugs específicos em campo.

Exercícios:

1. O que é um vírus eletrônico de computador?

_____
_____
_____

2. Como ocorre a maiorias das contaminações dos computadores por vírus?

_____
_____
_____
_____

3. O que é um Hacker?

_____
_____
_____

4. O que é um Cracker?

_____
_____
_____

5. Assinale a alternativa correta quanto ao texto. Um dos primeiros tipos de vírus conhecido, infecta a parte de inicialização do sistema operacional. Assim, ele é ativado quando o disco rígido é ligado e o Sistema Operacional é carregado.
   a) Cavalos de Troia b) Vírus de Boot c) Worms ou vermes

6. Assinale a alternativa correta, são programas ou scripts que "sequestram" navegadores de Internet. Quando ocorre o ataque, o vírus altera a página inicial do browser e impede o usuário de mudá-la, exibe propagandas em pop-ups ou janelas novas, instala barras de ferramentas no navegador e podem impedir acesso a determinados sites (como sites de software antivírus, por exemplo).
   a) Cavalos de Troia b) Vírus de Boot c) Hijackers

7. Assinale a alternativa correta, vinculam seus modelos de documentos gabaritos e a outros arquivos de modo que, quando um aplicativo carrega o arquivo e executa as instruções nele contidas, as primeiras instruções executadas serão as do vírus.
   a) Cavalos de Troia b) Vírus de macro c) Hijackers

8. O que são os bugs de software?

_____
_____
_____

9. Assinale, Spywares são programas instalados em computadores pessoais, capazes de identificar e remover determinados vírus, como, por exemplo, Hoax e Trojan.
   a) Certo
   b) Errado