# UMA ANÁLISE SOBRE MALWARES E ESTRATÉGIAS DE PREVENÇÃO

JAQUES, Gabriel[1]; BARASUOL, Joao Breno[2]; CHICON, Patricia Mariotto Mozzaquatro[3]

**Palavras-Chave:** Malware. Vírus. Aplicação. Invasor.

## INTRODUÇÃO

Com o passar dos anos, a tecnologia da informação tem mudado as nossas vidas, as informações estão ficando cada vez mais digitais e de fácil acesso no dia a dia. É exorbitante o número de informação que circula hoje em nossos computadores, celulares, tablets, etc.

Como o número de informação cresce cada vez mais, a tecnologia vai se multiplicando e se tornando cada vez melhor, mas quanto mais a tecnologia avança, mais brechas em sistemas aparecem. Quando isso acontece, é preciso somente um clique para infestar um sistema com um *malware*, que nada mais é um programa malicioso que tem como objetivo causar dano ao seu sistema.

Um exemplo de *malware* seria o vírus, em alguns casos, é capaz de roubar seus dados pessoais e até mesmo informações extremamente sigilosas de uma empresa.

## HISTÓRIA DOS MALWARES

Segundo o artigo publicado no site da Tecmundo (TECMUNDO, 2011), o primeiro malware foi um vírus para computadores que nasceu em 1971, chamado de “The Creeper”. Foi criado por Bob Thomas e era apenas um programa experimental e foi testado infectando um PDP-10, um computador de grande porte.

Basicamente, o vírus invadia a máquina e apresentava no monitor uma mensagem dizendo: “Im the creeper, catch me if you can!” (1Eu sou assustador, pegue-me se for capaz!). Após o recado aparecer em uma máquina, ele saltava de sistema em sistema repetindo a mensagem diversas vezes. Contudo, foi criado um antivírus chamado “The Reaper” que era capaz de eliminar a aplicação e manter o sistema seguro do vírus.

[1] Discente do Curso de Ciência da Computação. Unicruz. E-mail: gabrielnjaques@gmail.com
[2] Discente do Curso de Ciência da Computação. Unicruz. E-mail: joaobrenobarasuol@hotmail.com
[3] Professora, UNICRUZ. E-mail: pmozzaquatro@unicruz.edu.br

No início da era da informática, não haviam intenções de infectar ou roubar informações de usuários com tais aplicações, existiam apenas intenções de irritar usuários e colegas de trabalho. Com o passar das décadas de apenas um vírus em 1971, estimava-se mais de 1.300 vírus na década de 1990. Atualmente não há um número exato, mas estima-se que existam mais de 200 milhões de tipos de vírus diferentes e espalhados de diversas maneiras.

## TIPOS DE VIRUS/APLICAÇÕES

Existem alguns *malwares* que não têm o objetivo de provocar danos ao computado. Um exemplo seria vírus benignos**,** os quais têm a intenção de apenas mostrar uma mensagem no sistema em determinado dia lembrando uma atualização ou algum programa que não está sendo executado (BARROS,2003).

Em oposição, existem os vírus malignos que infligem danos ao sistema. Segundo o artigo publicado pela UOL (UOL, 2013) um vírus maligno pode deixar o sistema lento, tendo a necessidade de uma formatação, pode causar também vulnerabilidade ou roubo informações.

## CLASSIFICAÇÃO DOS MALWARES

Segundo o artigo publicado no site da Cartilha**,** alguns tipos de malwares são:

Spam e Phishing**:** O termo spam é utilizado para referenciar o recebimento de uma mensagem não solicitada, que geralmente tem o caráter de fazer propaganda de algum produto ou assunto não desejado. (MELO et al. 2001, p.4). Esses *malwares* normalmente são utilizados para pescar informações de usuários da Internet, constituindo-se um ataque que tem como objetivo efetuar algum ilícito através do envio de mensagem não solicitada.

Backdoor: Aparecem escondidos em arquivos baixados ou em E-mails. Quando o usuário executa o arquivo, ele libera o vírus, que abre uma porta para o invasor e desse modo ele pode controlar a máquina infectada.

Keylogger**:** Tem como principal objetivo capturar todas as informações que são digitas no computador pelo usuário. Ele faz uma coleta de dados e as informações são enviadas diretamente ao invasor, assim, é possível que ele colete dados pessoais como senhas de redes sociais, e-mail e cartões de crédito (MELO et al., 2001).

Ramsomware: Bastante conhecido por ser um dos piores tipos de vírus da atualidade, o ataque executado por essa aplicação pode causar grandes prejuízos a empresas que podem ir de perda de dados a valores financeiros (MELO et al., 2001).

Trojan: Bastante conhecido também como Cavalo de Tróia, é listado entre as ameaças mais perigosas da rede de computadores. São geralmente aplicativos simples que escondem funcionalidades maliciosas e alteram o sistema para permitir ataques posteriores.

**PREVENÇÃO**

O que deve ser feito para se prevenir dos vírus é sempre uma questão importante a ser abordada. Mesmo com a utilização de um antivírus no sistema, ainda é possível um vírus infectar a sua máquina e dar uma imensa dor de cabeça , existem algumas formas de se prevenir, tais como, conforme a Cartilha de Segurança para a Internet.

Fazer downloads em sites confiáveis: O ideal é sempre fazer downloads em sites confiáveis que já possuem uma equipe para testar programas e verificar a existência de vírus (BARROS, 2003).

Mantendo o Sistema Operacional e programas atualizados: Muitos programas de computador, inclusive o Sistema Operacional possuem falhas que a cada atualização elas aplicam uma correção, e ao manter o sistema desatualizado o usuário abre brecha para programas se aproveitarem da falta de atualizações e infectarem o sistema.

Cuidado ao conectar PenDrives: Vírus também são espalhados via PenDrive, que, quando a pessoa coloca seu PenDrive lá, certamente será infectado e essa pode ser a brecha que o invasor precisa para ter acesso ao sistema.

Utilizando um Antivírus: Existem vários tipos de Antivírus no mercado e todos eles têm a mesma funcionalidade, a utilização de um antivírus é um dos principais passos para quem deseja proteger a sua máquina.

**METODOLOGIA**

Esse estudo tem como carácter ser explicativo, pois há o esclarecimento sobre alguns conceitos de *malware*. Conforme Gil (2002, p.42) as pesquisas explicativas: "[...]têm como preocupação central identificar os fatores que determinam ou que contribuem para a ocorrência dos fenômenos. Sendo assim houve uma pesquisa para realizar esse estudo, que tem por finalidade informar as pessoas sobre os variados tipos *malwares* que estão circulando atualmente e ajudá-las a entender e se prevenir de ataques.

## CONSIDERAÇÕES FINAIS

Este resumo é parte integrante de um trabalho em andamento cujo o objetivo é a conscientização da existência de diversos malwares e aplicações que podem danificar um sistema e até mesmo prejudicar um usuário de inúmeras maneiras, seja elas financeiramente quanto socialmente, assim o usuário terá conhecimento sobre aplicações danosas e formas de prevenção a serem usadas no seu dia a dia.

## REFERÊNCIAS

BARROS, Élvio Américo, Arruda. **Vírus de computadores: uma abordagem histórica e prática,** 2003.

**Cartilha de Segurança para Internet.** Disponível em: https://cartilha.cert.br/malware

Acessado em 16 de abril de 2018.

GIL, Antonio Carlos. **Como Elaborar Projetos de Pesquisa.** 4. ed. São Paulo: Atlas, 2002. 176 p.

MELO, Laerte Peotta et al. **Análise de Malware: Investigação de Códigos Maliciosos Através de uma Abordagem Prática**, 2011. Disponível em: http://www.peotta.com/sbseg2011/resources/downloads/minicursos/90650.pdf. Acessado em 10 de abril de 2018.

OSÓRIO, Livio Gomes, Tito. **Política de Rede computacional**, 2004.

TECMUNDO, 2011. Disponível em: https://www.tecmundo.com.br/virus/9184-primeiro-virus-de-computador-completa-40-anos.htm. Acessado em 10 de abril de 2018.