FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Luiz Felipe Zerbetto Masson

Trojans, Spams e Vírus: Prevenções

Americana, SP

2014

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Luiz Felipe Zerbetto Masson

Trojans, Spams e Vírus: prevenções

Trabalho monográfico, desenvolvido em cumprimento á exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec Americana.

Área de concentração: Infraestrutura de Sistemas Computacionais.

ICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS

Dados Internacionais de Catalogação-na-fonte

Masson, Luiz Felipe Zerbetto

M 372t — Trojans, spams e vírus: prevenções. / Luiz Fernado Zerbetto Masson. – Americana: 2014.

38f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.

Orientador: Prof. Dr. Maria Cristina Aranda

1. Segurança em sistemas de informação I. Aranda, Maria Cristina II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5

Luiz Felipe Zerbetto Masson

Trojans, *Spams* e Vírus: Prevenções

Trabalho de conclusão de Curso apresentado à Faculdade de Tecnologia de Americana como parte dos requisitos para obtenção do título de Tecnólogo em Segurança da Informação

Área de Concentração: Infraestrutura de Sistemas Computacionais.

Americana, 04 de Dezembro de 2014.

Banca examinadora:

Maria Cristina Aranda.
Doutora
Faculdade de Tecnologia – Fatec Americana

Alexandre Mello Ferreira
Doutor
Faculdade de Tecnologia- Fatec American

Maria Cristina Luz Fraga Moreira Aranha
Mestre
Faculdade de Tecnologia- Fatec American

AGRADECIMENTOS

Em primeiro lugar gostaria de agradecer a Deus por essa vida maravilhosa que levo. À meus pais que me deram uma boa criação e estudos. À meus colegas de faculdade pela ajuda que me prestaram em momentos de necessidade e aos professores da Fatec Americana pelo conhecimento que esses me passaram.

Resumo

Este trabalho apresenta um estudo bibliográfico atual sobre as ameaças encontradas na Internet e uma aplicação real de políticas de segurança da informação, focando vírus, *spam* e *trojans*. No trabalho é abordada uma descrição desses tipos de ataque, principais características, modos de atuação e indicação de casos polêmicos envolvendo essas ameaças. Também são apresentados métodos de defesa e indicações de melhores práticas contra eles. Esse estudo foi aplicado e testado na área de Tecnologia da Informação de uma escola pública da cidade de Americana. Apresenta-se no trabalho a estrutura de rede da organização e um relatório dos problemas encontrados na instituição de ensino onde foi desenvolvido o estudo de caso. O trabalho resultou na criação de políticas de segurança voltadas à prevenção e controle de situações que envolvem vírus, *spam* e *trojans*, as quais já foram implantadas e avaliadas pela escola aqui tratada como instituição educacional a pedido da mesma.

Palavras-chaves: Vírus, politicas, prevenção.

ABSTRACT

This work introduces a modern case study about the threat that is in the Internet and a real explanation of data security politics, focusing on virus, spam and Trojan. In the work will be aboard discretion of this kind of attacks, mainly character, ways of operation and indication of polemic cases involve these threats. Also showing methods of defense and indication of best practices against them. This study was applied and test on the Technology of Information area of a public school of Americana. Showing in this work the web structure of the organization and a report of the problems found on the education institution where the case was developed. The work resulted on the creation of security politics turn to the prevention and control of situations involving virus, spam and Trojan, which already been implemented and availed by the school here treated as educational institution the request thereof.

Keywords: virus, policies, prevention.

SUMÁRIO

Lista de Figuras e Tabelas

1. INTRODUÇÃO

Entre os anos 40, o governo dos Estados Unidos da América (EUA) começou a desenvolver um projeto especial de processamento e transmissão de dados entre pontos distintos em função da 2º Guerra Mundial. Esse projeto foi acelerado para fins bélicos, resultando nos radares, que tiveram um papel importante para a defesa dos Aliados (Estados Unidos, Império Britânico, União Soviética), assim como as máquinas de criptografia de códigos. Com o término da Guerra o uso dessa ferramenta foi voltado para a comunicação entre as universidades, as quais se responsabilizaram pela continuidade do projeto, resultando num dos meios de comunicação mais eficazes desenvolvidos pelo homem, possibilitando o envio e recebimento de informações, por milhões de pessoas através da Internet em qualquer lugar do planeta.

A Internet tornou-se um dos grandes adventos da época moderna. Nunca antes as pessoas tiveram acesso a tantos dados e conhecimento com tanta facilidade. Segundo Magalhães (2002) seus serviços abrangem o mundo dos negócios, como os negócios *online* conhecidos por *e-commerce*, na ampliação a distribuição de conhecimento através de sites educativos ou informativos e até para o lazer, com jogos, vídeos de qualquer gênero e sites de bate-papo.

Com o aumento de uso da Internet surgiu um novo tipo de ameaça cuja propagação seria minimizada sem a Internet, os vírus de computador. Esses vírus são programas maliciosos criados das mais diversas maneiras que começaram a surgir por volta dos anos 80, no auge do uso descuidado da Internet. O intuito principal desses vírus é roubar ou destruir informações e sistemas indefesos. Essa “infecção” ocorre por razões diversas, desde motivações politicas até por puro prazer de destruir, chegando até mesmo a causar grandes estragos em um número significativo de PC’s (*Personal Computer;* Computador Pessoal) ou em sistemas de empresas e de governos.

O maior problema está relacionado à falta de conhecimento e de atenção com que as pessoas tratam essas ameaças, levadas pelo pensamento, “isso nunca vai acontecer comigo”. Esse tipo de atitude é o que causa as vulnerabilidades nos sistemas de segurança das empresas, redes domiciliares ou computadores pessoais, onde os vírus costumam atacar.

Como mitigar as ações de um vírus através de melhores práticas de uso da Tecnologia da Informação (TI) e como utilizá-las para que possam preparar o ambiente para evitar novas infecções? Essa é uma pergunta feita por vários usuários de redes por todo o mundo, principalmente aqueles que já sofreram algum tipo de ataque e que sabem o quão trabalhosa e danosa uma situação dessas pode ser. As maiorias das empresas que sofrem infestações de programas maliciosos optam por não divulgar o ocorrido com o intuito de não perder prestígio e confiança perante seus clientes. Sendo assim, as técnicas utilizadas pelos responsáveis de TI para combater essas ameaças permanecem ocultas da maioria das pessoas.

É preciso lembrar que existe uma grande variedade de vírus de computador e outros tipos de software mal intencionados que podem causar um grande estrago.

Este trabalho visa uma análise desses programas, seus tipos e meios de ataque, assim como métodos que podem ser usados para preveni-los de explorar falhas no sistema, tanto lógicas como humanas e físicas. Esse trabalho realiza um levantamento bibliográfico sobre esses programas e outras ameaças comuns em potencial aos computadores e redes de informação, abordando também exemplos de ataques já ocorridos e visando detalhar seus danos as redes e as máquinas, mensurando os descuidos dos usuários em relação vírus de computador.

Através de pesquisas e estudos, um conjunto de regras e boas práticas foram colocadas em uso em um ambiente de informática de uma organização que por sigilo profissional optou-se por não revelar o nome sendo tratada aqui como Organização Educacional. O desempenho desses procedimentos implementados na referida organização foram acompanhados antes, durante e

depois da adoção das políticas de segurança demonstrando os benefícios que uma boa gerência dos recursos de TI possa trazer, além da efetiva diminuição de incidentes relacionados a vírus e da mitigação dos danos que possam ocorrer com os dados ou com a estrutura de empresa no caso de uma efetiva infestação do sistema.

As práticas apresentadas neste trabalho visam ajudar na percepção, defesas, especificamente de vírus, *trojan*, *spam* tipos de ataques a redes que causam problemas, maior comoção e custo à organização, por seu período prolongado de ataque, sendo que um vírus pode ficar dormente por vários dias em um PC antes de agir, e da perda de informações valiosas nos ataques.

2. Pesquisa Bibliográfica

Os computadores, máquinas que possuem dentro de si instruções lógicas para agir em cada situação conhecidos como Sistemas Operacionais (SO), que consistem em um conjunto de regras e códigos que definem como a máquina se comporta em determinadas situações para seu efetivo funcionamento. Nos últimos anos o processamento desses Sistemas Operacionais está mais rápido do que nunca, visando melhorar o desempenho nas tarefas solicitadas.

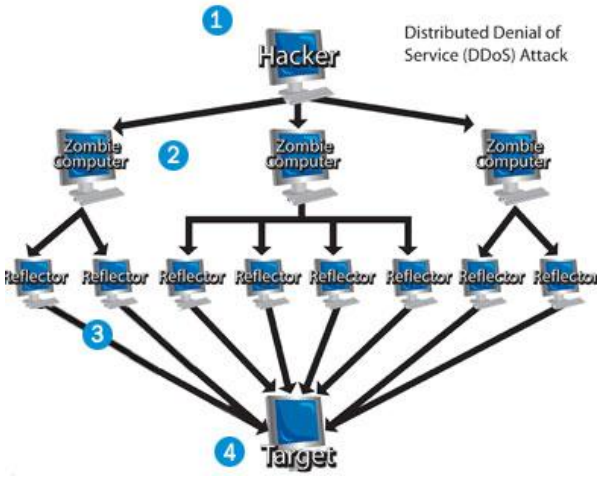
Garantir que nenhum dano irá acontecer nos computadores está entre os grandes desafios para os desenvolvedores da área de Tecnologia da Informação. Gonçalves (2003) afirma que se de um lado um Hacker utiliza um novo programa ou lógica para detectar e corrigir um defeito na segurança dos SO das máquinas e dos aplicativos usados por elas, por outro lado existem cerca de outras vinte pessoas buscando novos defeitos e fraquezas para explorar. Esses seriam os Crackers, definição em inglês de Gonçalves (2003); para usuários de computador com fins maliciosos e/ou destrutivos; programadores habilidosos e gênios da informática que por motivos políticos, pessoais ou por pura necessidade de fazer algo destrutivo, realizam ataques a outros usuários. Esses ataques podem ser classificados em grupos distintos por suas diferenças na forma de afetar a vitima e efeitos, imediato ou de longo prazo, consequentes de um ataque bem sucedido.

Segundo Duarte (2008) os ataques que buscam saber que computadores existem em uma rede alvo e suas fraquezas, pertencem à classificação de ataques por reconhecimento. Um exemplo desse tipo de ataque é a Pesquisa Vertical de portas onde um Cracker utiliza programas como o *NMAP* para escanear as portas do computador, que são as entradas e saídas dos programas/serviços que interagem com o sistema, pedindo vários serviços nessas mesmas portas com intuito, não de invasão, mas de mapear as entradas de serviço e assim conhecendo as portas usadas na rede para um futuro ataque, pois só esse conhecimento sobre seu alvo ajuda o Cacker definir ideias de com que tipo de sistema operacional está lidando e quais seriam ataques mais eficientes.

Outros ataques são mais danosos, como o *Denial of Serviçe* (DoS) ou o *Distributed Denial of Service* (DDoS) que procuram impedir que servidores consigam realizar seus serviços adequadamente aos clientes, realizando um grande número de pedidos para sobrecarregar os sistemas responsáveis pela prestação de serviço do alvo. São classificados como ataques de negação.

Duarte (2008) descreve algumas das técnicas utilizadas no DoS, como o *ping of deah* (ping da morte), o qual através de programas como o sPing envia diversas mensagens de teste de conexão de 65.536 bytes. Os *pings* enviados possuem uma quantidade de bytes acima do normal, fazendo o sistema travar em função da quantidade de dados ser maior que a usada normalmente no tipo de serviço que utiliza os *pings* para averiguar as conexões. Para tal é utilizado o protocolo ICMP (*Internet Control Message Protocol*). Essa categoria de ataque é muito eficiente pelo fato de não haver um programa intruso diretamente na rede alvo, mas sim em máquinas zumbis, máquinas infectadas por vírus que estão sobre o controle de Crackers como nos usados nos ataques DDoS exemplificados na Figura 1. O ataque em si é apenas uma quantidade de pedidos ao servidor em uma escala maior do que os provedores podem suportam, não havendo maneira ainda conhecida de diferenciar um pedido de conexão real de um pedido falso, citando o já falado “ping da morte”.

Figura 1 - Estrutura de Ataque de DDoS



Fonte: Mestre dos Sites[1]

[1] Disponível em: <mestredossites.com.br>. Acesso em: 20 de out. 2014.

Apesar dos tipos de ataque de DoS serem muito difíceis de impedir com a capacidade da tecnologia atual de reconhecer quando uma máquina está sendo usada por seu dono legitimo portanto é o criminoso, ou como um zumbi por um Cracker, sendo a máquina atacante só mais uma vitima, e os ataques por reconhecimento não afetarem de fato a máquina durante seu reconhecimento de rede e portanto não serem detectados durante o escaneamento das máquinas atingidas, são os ataques do terceiro grupo, ataques por obtenção de controle, que causam maior dano em maior tempo que serão apresentados a seguir. Como dito por Duarte (2008) esses ataques visam conceder controle sobre a máquina e apagar dados importantes impedindo o funcionamento da mesma ou transferir o domínio de sua vitima para seu Cracker, garantindo que ele possa fazer o que quiser com as máquinas com mínima chance de ser notado pelo usuário leigo. Esses ataques vêm de maneiras mais variadas, pois seus meios de infiltração mudam não só por causa dos diferentes tipos de tecnologia, mas também pela astúcia de quem os criam e disseminam nas mais variadas formas. Algumas das técnicas e programas maliciosos desenvolvidos por Crackers que se encaixam nessa categoria segundo CERT (2012) seriam os *worm* (verme), *bot, spyware*, *rootkit*, vírus e *trojan*.

Esse tipo de programa criado para consumir os recursos do Sistema Operacional infectado ou da rede a qual pertence através do envio de cópias de si mesmo uma vez que adentra no alvo. O *worm* é problemático pelo fato de não afetar diretamente os programas do computador como um vírus, que será explicado mais detalhadamente à frente no trabalho, mas agirem com seu próprio programa para aumentar sua lista de infectados, o que pode levar a baixo desempenho da rede ou do computador infectado. O *bot* é extremamente semelhante ao *worm* segundo CERT (2012). Porém ele visa não uma grande propagação e sim o controle da máquina para seu criador através do estabelecimento de uma via de conexão. *Spyware* é um *malware* de espionagem, feito para monitorar as atividades do alvo e enviar dados alheios, ou programados, para o seu Cracker. Apesar de seu grande uso indevido ele pode ser usado como técnica de proteção de um computador, monitorando qualquer atividade dentro da máquina em que é instalada para o dono. Já o *rootkit* não é um ataque em si, esse nome é dado a um conjunto e regras

desenvolvidas pelos Cracker para ocultar seus *malwares* nas máquinas alvos. A maioria das regras é usada em conjunto com ataques de obtenção de controle que envolve programas dentro das redes e máquinas afetadas, porém elas visam à continuação desses ataques e não seu sucesso. O vírus é um programa criado pelo Cracker que pode se inserir dentro de outros programas para afetar sua função. Esta entre o tipo de ataque mais variado dentre os outros quanto a sua maneira de infectar o alvo. *Trojan* e *backdoor* são programas disfarçados, entram nas máquinas como outros programas, ou presos a eles, e afetam as defesas do alvo para permitir a entrada de outros *malwares* no sistema.

Entre as mais famosas e letais técnicas de obtenção de controle, mostradas na Tabela 1 e descritas anteriormente àquelas que foram encontradas no estudo de caso serão aqui apresentadas detalhadamente para um melhor conhecimento de seus perigos e possíveis soluções baseadas no próprio estudo de caso.

Tabela 1 - Códigos Maliciosos

	Vírus	***Worm***	***Bot***	***Trojan***	***Spyware***	***Backdoor***	***Rootkit***
Como é obtido:							
Recebido automaticamente pela rede		✔	✔				
Recebido por *e-mail*	✔	✔	✔	✔	✔		
Baixado de *sites* na Internet	✔	✔	✔	✔	✔		
Compartilhamento de arquivos	✔	✔	✔	✔	✔		
Uso de mídias removíveis infectadas	✔	✔	✔	✔	✔		
Redes sociais	✔	✔	✔	✔	✔		
Mensagens instantâneas	✔	✔	✔	✔	✔		
Inserido por um invasor		✔	✔	✔	✔	✔	✔
Ação de outro código malicioso		✔	✔	✔	✔	✔	✔
Como ocorre a instalação:							
Execução de um arquivo infectado	✔						
Execução explícita do código malicioso		✔	✔	✔	✔		
Via execução de outro código malicioso						✔	✔
Exploração de vulnerabilidades		✔	✔			✔	✔
Como se propaga:							
Insere cópia de si próprio em arquivos	✔						

Envia cópia de si próprio automaticamente pela rede		✔	✔				
Envia cópia de si próprio automaticamente por *e-mail*		✔	✔				
Não se propaga				✔	✔	✔	✔
Ações maliciosas mais comuns:							
Altera e/ou remove arquivos	✔			✔			✔
Consome grande quantidade de recursos		✔	✔				
Furta informações sensíveis			✔	✔	✔		
Instala outros códigos maliciosos		✔	✔	✔			✔
Possibilita o retorno do invasor						✔	✔
Envia *spam* e *phishing*			✔				
Desfere ataques na Internet		✔	✔				
Procura se manter escondido	✔				✔	✔	✔

2.1. Vírus

O termo vírus é usado como um sinônimo de algo ruim, principalmente no que diz respeito à Tecnologia da Informação, área esta onde pode existir vários tipos de vírus de computador, sendo uns inofensivos e outros chegando a causar estragos severos a pessoas e até mesmo a países. No século vinte e um esse tipo de ataque se tornou uma característica comum segundo Goulart (2009). No século passado apenas pessoas com elevado conhecimento de programação conseguiam criar um vírus. Atualmente existem programas para criação de vírus favorecendo os usuários comuns, como mostra a Figura 2. Até existem empresas fictícias que lucram com a venda de um serviço de vírus para outras, como exemplo quando uma grande organização deseja roubar o banco de dados de uma rival.

Figura 2 - Programa de Fabricação de vírus

Fonte: Techtastico[2]

Uma das capacidades desses programas maliciosos, também chamados de *malware*, é sua habilidade de infecção espalhando-se por arquivos e setores de inicialização de mídias removíveis e sistemas operacionais. Segundo Alecrim (2011):

> Os vírus recebem esse nome porque possuem características de propagação que lembram os vírus reais, isto é, biológicos: quando um vírus contamina um computador, além de executar a ação para o qual foi programado, tenta também se espalhar para outras máquinas, tal como fazem os vírus biológicos nos organismos que invadem.

Essa infecção pode ser feita de várias maneiras dentre elas Gonçalves (2002) dita que existe a sobregravação, onde o vírus se instala no início do código fonte do programa, quebrando-o e o inutilizando depois para infectar outros programas e arquivos quando o programa for executado pela primeira vez. Outros métodos são a preposição e anexação de arquivos. Preposição é quando o vírus coloca-se diretamente sobre o alvo, ou seja, muda o caminho no computador que deveria ativar o programa desejado para ativar o vírus que infecta o arquivo e o inicia para não levantar suspeitas. Primeiramente é rodado o código do vírus que realiza mais infecções e suas ações maliciosas para então, executar o programa original sem deixar suspeitas. Já o programa de anexação de arquivos instala seu *malware*

[2] Disponível em: <http://techtastico.com/>. Acesso em: 23 de outubro. 2014.

no final do arquivo e adiciona uma marca no início do mesmo para que esse chame o vírus na hora da execução do programa original. Com a chegada da Internet os *malwares* tiveram seu poder de alcance aumentado, pois antes eles precisavam de disquetes para se locomover de uma máquina a outra. Agora existem transmissões através de *e-mails* e de *Downloads*, além dos *bugs* (falhas) existentes nos sistemas operacionais nas primeiras versões de disponibilização dos programas que são amplamente analisadas pelos *hackers*, além de serem divulgadas anonimamente pela Internet.

Segundo Alecrim (2011), existem casos de malwares que causaram tamanhos danos a uma quantidade imensa de máquinas que acabaram entrando para a história, como exemplo o caso do vírus Melissa ocorrido em 1999. Melissa foi criado especialmente para os programas *Word* da *Microsoft*, utilizando o *e-mail* para se propagar e, após infectar a máquina enviava cópias de si mesmo para os 50 primeiros contatos na lista do *e-mail* do usuário. Um ano depois outro *malware* chamado LoverLetter foi liberado nas Filipinas, causando danos de mais de US$ 8,7 bilhões por toda Europa e Estados Unidos, que graças à Internet ele conseguiu em menos de seis horas um total entre 2,5 milhões a 3 milhões de máquinas infectadas. Existe uma grande variedade de vírus no mundo digital. Serão elencados apenas alguns desses vírus e seus modos de ataque. A escolha foi feita em função dos vírus que foram encontrados no estudo de caso, ou seja, na organização aqui apresentada.

O Vírus *Boot* é um dos primeiros tipos de vírus que surgiram no mundo com o nome de Brain, isso na década de 90. Ele pertencia à classe de *malware* e surgiram quando os computadores usavam discos flexíveis, sendo esses disquetes seus alvos principais para infecção e disseminação. Atualmente com o desuso dos disquetes, os novos locais de infecção desses vírus são as unidades de armazenamento como *pendrives* e *hd* externos. Normalmente ficam ocultos em unidades de armazenamento corrompidas segundo Leoop (2011). Ao se utilizarem disquetes, *pendrives* e *hd* que contem o vírus, o vírus se instala na memória Bios (Sistema Básico de Entrada/Saída) que é executado por um computador quando ligado. A Bios é responsável pelo suporte básico de acesso ao hardware, bem como por iniciar a carga do sistema operacional. O *boot* (processo responsável pelo efetivo

carregamento do sistema operacional no computador após a execução da BIOS) é segundo Gonçalves (2002), alterado em sua sequência lógica para se auto-executar cada vez que o computador se reinicia. A partir dai qualquer unidade colocada na máquina passaria a ser infectada com uma cópia do vírus, gerando assim uma grande propagação. Um exemplo desse tipo de vírus é o Vírus Ping-Pong cujo efeito principal é fazer aparecer uma bola na tela do computador que pula seguindo o tic-tac do relógio com o objetivo de afetar o usuário transtornando-o e tirando sua concentração. Esse vírus surgiu no Brasil na época do MS-DOS (sistema operacional criado pela *Microsoft)* na década de 80 e 90.

Outro tipo de vírus encontrado no estudo de caso explora uma das grandes vantagens dos computadores atuais, á automação de atividades que precisam ser realizadas repetidas vezes através da criação de um programa específico para está finalidade, mais conhecido como *macro*. Os *macros* podem ser usados em outros arquivos após seu efetivo salvamento ajudando no desempenho dos sistemas operacionais.

Isso levou esses macros tornarem-se alvos de um tipo especial de vírus, o vírus Macro, que tem como objetivo comprometer seu funcionamento. Segundo Gonçalves (2002) os alvos mais comuns que esse vírus persegue são documentos dos editores de texto MS-Word e da planilha de cálculo MS-Excel. Em especial o arquivo que cuida da configuração do Word, conhecido como NORMAL.DOT, que como é executado várias vezes gera uma maior infecção. Todas as vezes que esses programas infectados são abertos ou usados pelo usuário, entram em ação os macros do vírus, infectando programas bons. Os principais danos feitos por esses *malwares* são alteração de documentos, fragmentação de texto e no pior caso a mudança de arquivos de *lote* (automatizador de tarefa) para apagar partes ou todo o conteúdo do disco rígido do computador. A primeira aparição de um *malware* desse tipo foi em 1995 com o vírus Concept que chegou a fazer mais de 35 mil vitimas. Seu surgimento e poder de infecção abriram caminhos para outros vírus mais fortes como, por exemplo, o vírus Melissa já descrito anteriormente. Apesar disso os vírus *macro* mais comuns podem ser facilmente encontrados nos computadores através de programas conhecidos como antivírus. Daquino (2010) descreve os programas antivírus como ferramentas básicas de segurança de um computador que, apesar de

não ofereceram uma proteção 100% eficiente, costumam melhorar a vida dos usuários por assumirem a responsabilidade de detectar e remover *malwares* dos SOs externos.

2.2. Trojans

Os *trojans* possuem esse nome devido à sua semelhança com a lenda Grega da guerra de Troia. Os gregos derrotaram os troianos usando um gigantesco cavalo feito de madeira, onde esconderam seus soldados e o presentearam para seus inimigos dizendo que era um sinal de que desistiram da guerra. O cavalo foi então levado para dentro da cidade onde acontecia uma grande festa e à noite os soldados escondidos saíram do falso presente e abriram os portões garantindo a entra do exercito grego e sua vitória.

Semelhantemente os *trojans* são programas que dizem fazer um determinado serviço, que podem realizá-lo ou não, mas escondem outra atividade que pode danificar seriamente o computador. Diferentemente dos vírus como os vírus de *boot* e dos *macros*, Gonçalves (2002) diz que os *trojans* não podem fazer uma cópia de si mesmo nem infectar outros programas. No lugar da infecção dos outros *malwares* (programas maliciosos) ele pode se auto executar, ou seja, sem que precisem infectar outros programas para agir realmente. A maneira de ativação varia de acordo com o tipo de *trojan* em questão, mas em geral são usados pelos *Crackers* para assumir controle do PC da vítima e utilizá-lo em outros ataques, segundo Goulart (2009), forçando a máquina a fazer *downloads* de novos vírus como exemplificado na Figura 3.

Figura 3 - Tentativa de acesso à rede por trojan

Fonte: Technize[3]

Segundo Moreira (2011) um exemplo desse tipo de *malware* é o que atende pelo nome de OSX/Tsunami, versão mais nova de um antigo *trojan* que após entrar no computador alvo assume o controle da máquina e a utiliza para realizar ataques do tipo DDS (Distributed Denial of Service), ou seja, atacam mandando várias solicitações de acesso a um site programado como vitima. Em geral sites de prestação de serviço de alguma grande empresa, causando uma sobrecarga no site impedindo seu funcionamento normal. Muitas vezes o site trava por tem sua capacidade de armazenamento e/ou processamento sobrecarregado devido às requisições feitas constantemente pelas máquinas infectadas por esse *trojan*.

Trojan Backdoor é, na definição de CERT (2012), um *trojan* usado principalmente para permitir o retorno de um invasor ao alvo através da criação de programas de acesso ou a modificação de serviços específicos como programas de administração remota, ou seja, programas que permitem a usuários assumir o controle de suas máquinas ou servidores localizados a longa distância para gerenciamento como o BackOrifice*, NetBus ou VNC.* Muitos desses programas de administração foram projetados com intuito financeiro e humanitário, visando ceder aos donos de computadores acesso a suas máquinas, a longa distância, na era digital. Porém acabaram, segundo CERT (2012), sendo usados para a obtenção ilegal de acesso a máquinas alheias, ficando conhecidos pelo nome de *backdoor*. Após sua entrada e instalação no computador, normalmente durante a ação de outro

[3] Disponível em: <www.technize.info>. Acesso em 14 do nov. 2014

malware no alvo o *backdoor* é usado para assegurar o acesso futuro ao computador comprometido, permitindo que ele seja acessado remotamente, sem que haja necessidade de recorrer novamente aos métodos utilizados na realização da invasão ou infecção e, na maioria dos casos, sem que seja notado.

Por ficar escondido em programas normais de computador o *trojan* é um tipo de vírus extremamente preocupante por ser de difícil percepção e remoção do computador após sua entrada. Isso levou à criação de antivírus específicos para cada tipo de Sistema Operacional. Os tipos de ataque DoS ainda não possuem uma resposta realmente eficiente nos dias atuais, chegando a causar grandes danos e prejuízos a todos.

2.3. Spam

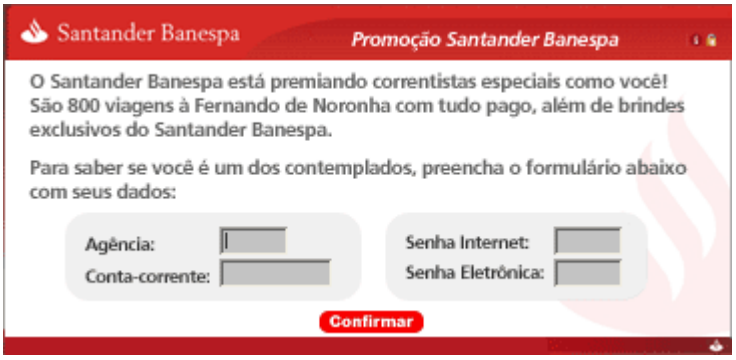
Um tipo de vírus detectado no estudo de caso com uma quantidade alarmante vem causando problemas nos meios de comunicação e propagando ao redor do mundo. O *Spam* não se trata realmente de um vírus de computador como os demais, mas sim de um vírus social na visão de Gonçalves (2002), pois utiliza a Internet apenas como meio de propagação, tendo como alvo principal a ingenuidade e a boa fé dos usuários da rede de Internet.

Segundo Duarte (2008):

> O termo Spam, abreviação em inglês de "spiced ham" (presunto condimentado), é uma mensagem eletrônica não solicitada enviada em massa. O spam é também a designação universal atribuída a correio eletrônico (e-mail), de teor quase sempre comercial, não solicitado. Normalmente é enviado em massa para dezenas, centenas e até milhares de endereços de e-mail em simultâneo, fazendo com que os servidores de e-mail, e linhas de comunicações fiquem sobrecarregados. Pg 13.

Ele é usado por muitos *Crackers* maliciosos devido à facilidade com que pode propagar outros vírus, pois já que se trata de uma mensagem enviada em massa pelo correio eletrônico (*e-mail*), de caráter semelhante ao da Figura 4, a muitos alvos permite uma infecção em massa sem custo. O acréscimo de um *trojan* à mensagem daria ao *Spammer* (quem envia o *spam*) controle sobre quem, que em sua negligência, ativa o *e-mail* para verificar seu conteúdo e acaba, por conseguinte sendo infectado pelo *malware* nele ocultado.

Figura 4 - Exemplo de Spam



Fonte: Santander[4]

Esse tipo de disseminação pode ser usado para diminuir a capacidade de uma rede e/ou conseguir acesso grátis a uma rede paga. Gonçalves (2002) dá como exemplo o envio de *spams* à AOL, uma empresa americana provedora de Internet, pela CyberPromotions com o envio de mais de 1,8 milhões de mensagens ao alvo. O *Spammer* obteve uma conexão grátis para o envio de mensagens no valor comercial de R$ 100,00 por dia e diminuiu a capacidade da empresa alvo de fornecer seu serviço em um total de cinco mil horas diárias com o congestionamento de sua rede pelas mensagens enviadas. Ele afirma também que devido à falta de uma legislação sobre essa prática no Brasil, o governo e as entidades comerciais *online* devem utilizar uma frase especifica no final de sua mensagem, o bordão da empresa, por exemplo, para não serem considerados *Spams* em suas divulgações, além de permitir o desbloqueio pelos clientes e usuários de serviço para novos.

Além dos danos de invasão e perda de tempo de serviço já citados, um *spam* causa outros incômodos como, por exemplo, a quantidade massiva de mensagens recebidas. CERT (2012) relata que em função da quantidade de mensagens na caixa de entrada, um usuário desafortunado pode não conseguir ver a chegada de alguma mensagem realmente importante. Nas empresas atuais o problema se agrava com o controle de tamanho da caixa postal, para controlar o número de *e-mails* recebidos pelos funcionários. Uma meta de quantos *e-mails* por dia cada um pode receber na rede é estabelecida podendo lota-lo com essa prática, deixando o *e-mail* sem possibilidade de receber novos *e-mails* até que seja limpo. Mesmo as redes que se prepararam para esse tipo de ataque também podem ser

[4] Disponível em: < www.santander.com.br>. Acesso em: 20 out. 2014.

afetadas. No exemplo uma rede que possui um filtro com um AntiSpam com regras estabelecidas para classificar certas mensagens como *spam* e descartá-las, feitas incorretamente, causariam o descarte de e-mails reais junto com os *spans*.

Os problemas relatados anteriormente afetam principalmente os usuários de servidores de *e-mail*, mas os próprios servidores alvos de *spam* também têm consequências. Segundo foi descrito por CERT (2012), como uma queda no volume de tráfego na rede devido à elevada quantidade de mensagens juntamente com gasto excessivo dos recursos dos provedores de serviço, como o tempo de processamento de dados e o espaço nos discos rígidos, o que causa uma necessidade de mais investimento em tecnologia de filtragem para evitar novos ataques, gerando custo adicional na entrega do serviço. Dessa forma o Sistema Operacional do servidor pode ficar muito corrompido, ou seja, possuir muitos programas de vírus em seu sistema, e ter seu contato adicionado a listas de bloqueios de outros prestadores de serviço de *e-mail* para evitar contaminação, levando enfim a perda de clientes e contratos.

Esse tipo de vírus atinge grande quantidade de alvos devido às suas técnicas de localizar alvos, usando *e-mails* válidos, através da rede, com métodos bem simples. Uma das técnicas é o “Ataque Dicionário” que consiste na mistura de nome de pessoas com palavras do dicionário combinadas a caracteres alfanuméricos aleatórios para gerar facilmente possíveis endereços. Outra tática de coleta de alvos dos *Spammers* é usar *malwares* com o intuito de checar listas de contato e marcar possíveis novos alvos. Dentre eles existe os “*harvesting*” que consiste na varredura de listas de discussão e sites de bate-papo à procura de qualquer endereço citado.

3. Estudo de Caso

A empresa estudada é uma escola do sistema educacional público brasileiro, localizada no estado de São Paulo, na cidade de Americana. Por motivos tanto políticos como empresariais a instituição decidiu não revelar sua identidade para não prejudicar sua imagem ou violar os direitos de privacidade dos alunos e dos funcionários envolvidos.

Assim como várias outras instituições, essa instituição educacional utiliza a Tecnologia da Informação como apoio educacional, oferecendo um parque computacional a seus alunos, professores e funcionários. Esse parque computacional está todo conectado através de sistemas de redes, gerenciando desde os empréstimos da biblioteca até a disponibilização de impressão. Pelo fato da organização somente usar o computador como ferramenta de trabalho, acaba criando a cultura da mesma não procurar saber muito sobre os perigos que podem afetá-la, como vírus, *spams* e *trojans*. As regras e políticas de segurança foram criadas com o intuito de ajudar organizações que dependem de Tecnologia da Informação a incrementarem segurança em suas redes privadas com baixo custo, criando regras de como agir e usar os recursos de TI sem grandes riscos e minimizando os danos no caso de um ataque bem sucedido.

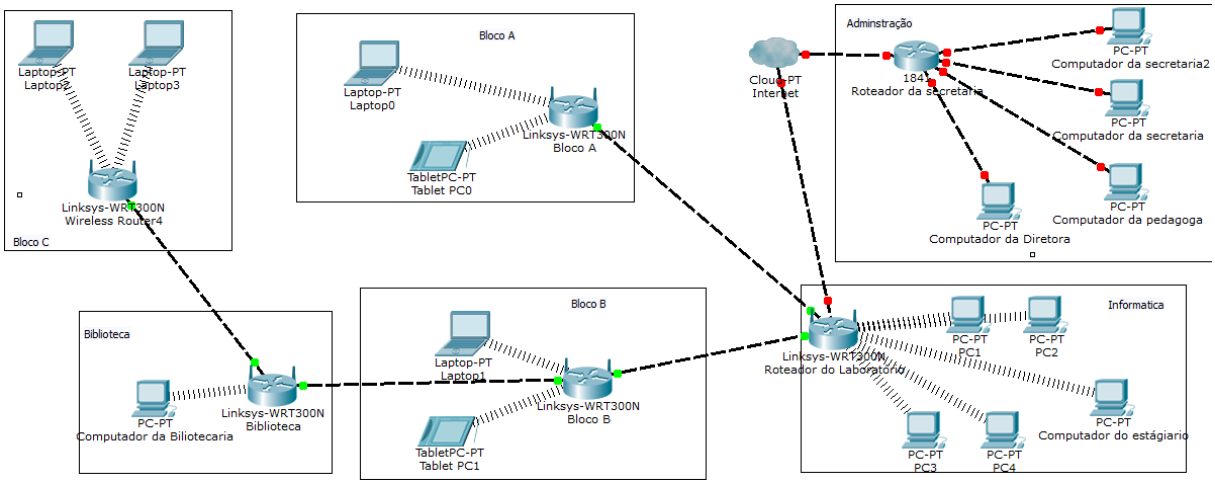
Esse estudo de caso foi divido em descrição da Instituição Educacional e seus recursos de TI, políticas de segurança e sua implementação na organização, seu acompanhamento e desempenho, bem como os efeitos sobre os usuários de TI da Instituição, culminando com uma análise da efetiva diminuição dos casos de ataque por vírus, *spams* e *trojans*.

A Instituição educacional conta atualmente, com uma sala de informática, possuindo nove computadores disponíveis para os alunos com o SO Linux Educacional V.4 instalado, além de um PC para os estagiários de TI com um Windows 8. Na secretaria tem dois PCs e um *notebook* com Windows 7 e XP, respectivamente, para o uso exclusivo de seus funcionários, um PC para a diretora e outro para a pedagoga, sendo o último com o Windows 7 e o outro com XP.

Também está disponibilizado um *notebook* com Windows 7 em cada sala de aula acompanhado de projetor e uma tela interativa, na SAIP (Sala de Apoio e Intervenção Pedagógica) conectado a um computador e um notebook.

Na secretaria existem três impressoras ligadas aos computadores das atendentes e uma impressora *scanner*. A biblioteca da escola também possui uma impressora e um computador. Sobre a responsabilidade da secretaria encontra-se um kit de apresentação (um *notebook*, uma tela e um *Datashow*). A rede interna *wireless* encontra-se dividida entre os Blocos A, B, C, informática e Biblioteca, sendo o ponto de entrada da Internet pela informática, que então utiliza roteadores para distribuir a rede nos outros blocos, como mostrado na Figura 5, que permanecem protegidas por chaves de acesso lógico. A rede de administração que envolve a secretaria, sala da pedagoga e sala da diretora é conectada por cabos por segurança, conectada a rede *wireless* através da Internet. A instituição não possui um técnico de informática que dá suporte aos usuários ou que gerencia sua rede local, por isso conta com a ajuda de estagiários temporários vinculados à prefeitura da cidade. Esse é um dos prováveis motivos de não existir uma política de segurança firme e enraizada, sendo que as normas em vigor dependem do estagiário atuante na Instituição os quais nunca documentaram nada.

Figura 5 - Estrutura da Rede wireless



Fonte: autor

O uso descuidado já causou à Instituição graves prejuízos, como a invasão da rede, em especial por *spammer* vindos de sites acessados pelos funcionários da organização. Esses incidentes diminuíram o tráfego da rede assim como o

desempenho das máquinas e a perda de dados também se mostraram existentes. Com os sistemas desatualizados e a falta de uma política de *backup* nos computadores da área da Administração em comum. Ocorriam com frequência casos de entrada de *trojans* na rede por *e-mails* dos funcionários e sites acessados indevidamente. Por não haver regras que mantinham uma comunicação entre a diretoria e os estagiários, vários computadores encontravam-se com senhas de administradores desconhecidas, impossibilitando a realização de alterações ou atualizações tanto nos sistemas como na rede nesses PCs. Exemplo disso mostrou-se no Bloco C, onde um *notebook* estava programado com um IP (número de identificação do computador na rede) incompatível com a atual infraestrutura da rede desse bloco, bloqueando o acesso à rede por esse dispositivo, como a senha de administrador era desconhecida as reconfigurações necessárias na placa de rede era negada.

Estavam em vigor apenas algumas políticas de segurança criadas pela instituição possibilitando apenas a segurança básica de seus equipamentos. Os *notebooks* localizados na sala permanecem trancados em caixas especiais junto com os controles dos *Datashow* e das lousas interativas, somente o professor responsável pela sala ou pessoal autorizado possui acesso. Ou seja, havia apenas a proteção física do bem.

Os roteadores localizados nos corredores dos Blocos A, B e C estavam posicionados em lugares altos para evitar o acesso físico pelos estudantes ao aparelho. Os que estavam localizados nas salas de Informática e Biblioteca permaneciam sob vigília dos funcionários das respectivas unidades, quando as salas não estavam trancadas.

Apesar do fato da Instituição possuir um sistema de telefones internos conectando os blocos, não havia meios de comunicação dos professores e diretoria com a sala de Informática. Em caso de defeito de alguma máquina ou problemas de comunicação na rede, o processo era lento e muitas vezes os computadores eram conduzidos à sala de informática sem qualquer tipo de registro.

Baseando-se nos estudos realizados, na análise de ocorrências de infecções por virus foram criadas politicas de segurança A seguir serão relatadas as regras desenvolvidas para a Instituição, com o intuito de melhorar o uso dos dispositivos de

TI e evitar, principalmente, ataques de obtenção de serviços já detalhados nesse projeto.

1. Politicas de Acesso Físico

1.1. Somente pessoal autorizado pela diretoria terá acesso à sala de informática.

1.2. O acesso aos computadores da sala de informática só é permitido aos estagiários de informática, ou sobre sua supervisão.

1.3. Todos os *notebooks* usados nas salas de aula devem permanecer guardados com cadeados nas devidas caixas, quando não utilizados pelos professores.

1.4. Em caso de falha nas caixas dos *notebooks* os mesmos ficarão sobre responsabilidade da área de informática até requisitado pelo professor.

1.5. Todo acesso físico, de alunos e visitantes, à escola devem ser feitos pela secretaria.

1.6. Os acessos às salas da diretora e da pedagoga só podem ser feitos com a presença das mesmas ou com a permissão concedida na secretaria.

1.7. Em casos de acesso da equipe de limpeza à sala de informática, da diretora e da pedagoga, a equipe deve informar a secretaria.

1.8. No intervalo, os *notebooks* devem ser desligados e guardados nas respectivas caixas.

1.9. Fora do horário de aula as salas que tem equipamentos devem permanecer fechadas a chave, incluindo as caixas dos *notebooks*.

1.10. Os computadores da sala de informática devem ser desligados ao termino do horário de aula.

1.11. A biblioteca deve permanecer fechada na ausência dos bibliotecários responsáveis.

1.12. O computador da sala da biblioteca é de uso exclusivo dos funcionários da mesma.

1.13. Em caso de empréstimo de livro da biblioteca sem a presença de bibliotecários, um responsável deve acompanhar aluno, visitante ou professor e registrar em papel, o nome e número do livro emprestado para os bibliotecários assim que possível darem entrada no sistema.

1.14. Toda e qualquer pesquisa de Internet solicitada pelos alunos, se efetuadas na instituição, serão realizadas somente na sala de informática, sob a supervisão do professor, quando utilizada como parte da aula, ou com a autorização da diretoria em vista da explicação do motivo da pesquisa pelo aluno.

1.15. Não será permitido acesso aos roteadores localizados nos corredores dos Blocos A B e C por alunos, professores e funcionários.

2. Politicas de Acesso Lógico

2.1. Os acessos às redes dos blocos serão disponibilizados somente aos professores das classes localizadas nos mesmos e aos técnicos de informática.

2.2. O acesso dos funcionários e alunos a rede da Instituição só pode ser feito pelos terminais da sala de informática e pelos computadores localizados na secretaria e biblioteca.

2.3. Todas as cinco redes *wireless*, Bloco A, B, C informática e Biblioteca, devem possuir uma senha de acesso, com características distintas entre si.

2.4. As senhas de acesso às redes *wireless* devem ser de conhecimento somente do estagiário de informática da diretoria.

2.5. Em relação aos aparelhos de acesso *wireless*, como tabletes e *notebooks* pertencentes aos funcionários e professores, serão de responsabilidade somente do estagiário de informática ou um representante da diretoria conectá-los a rede.

2.6. Toda e qualquer tentativa de acesso à rede por dispositivos pessoais deve ser monitorada pelo estagiário de informática ou comunicada à diretoria.

2.7. Em nenhum caso o estagiário tem permissão de entregar a senha de rede a pessoas não autorizadas pela diretoria.

2.8. Todos os *notebooks* devem possuir usuários distintos, um para o professor e outro para o técnico, com senhas distintas.

2.9. O acesso à rede através de cabos só é permitido nos computadores oficiais da Instituição e autorizado pelo técnico de informática.

2.10. Uso de celulares e outros tipos de aparelhos de rede pessoais permitido somente na rede da sala de informática com devida autorização da diretoria.

2.11. Nos computadores utilizados na sala de informática, deve-se manter um usuário para os alunos com permissões de simples usuários e outro para os professores com direitos de administrador. Ambos os usuários criados devem conter senha.

2.12. Todo e qualquer *download* que envolva alterações nos *notebooks* das salas devem ser deixados a cargo do estagiário de informática ou sob supervisão do mesmo.

2.13. Em nenhum momento os alunos da Instituição podem ter acesso a sites com conteúdo para maiores de idade.

2.14. Se houver necessidade de uso de conteúdo adulto nas salas de aula pelo professor, o mesmo deve procurar o técnico e a direção para adquirir permissão de acesso ou de *download* do mesmo.

3. Politicas de *Backup*

3.1. Em todo final de semestre um *backup* deve ser feito nos computadores da diretora, da pedagoga e na secretaria a fim de guardar os dados utilizados no semestre em questão.

3.2. Antes de qualquer alteração nos *notebooks* das salas, por *download* de programas e arquivos pelo técnico de informática, um ponto de retorno deve ser criado.

3.3. Para o funcionamento efetivo dos computadores uma verificação de sistema pelo programa de antivírus deve ser realizada ao inicio e término de seu uso.

3.4. Em caso de infecção de vírus nos sistemas dos equipamentos de tecnologia da informação da secretaria, os mesmos devem ser desabilitados até a devida limpeza e substituídos temporariamente por outros computadores.

3.5. Todo e qualquer computador usado na reposição de outro com defeito deve ser atualizado com os discos de *backup* do substituído.

3.6. O armazenamento de arquivos e dados dos computadores das salas permanece sobre responsabilidade dos professores. Quando esses possuem dispositivos de armazenamento como *pendrives*, ou qualquer outro dispositivo é de responsabilidade do técnico de informática.

3.7. Todos os discos, *pendrives* e outros aparelhos de armazenamento pertencentes à Instituição que contenham dados serão guardados na sala de informática.

3.8. Em caso de infecção nas mídias de *backup* da Instituição, essas devem ser separadas das demais e limpadas no computador do laboratório de informática

usado pelo estagiário, sem que esse esteja conectado a Internet, ou encaminhadas ao suporte da prefeitura.

3.9. Caso uma sala de aula estiver com o *notebook* em reparo e não disponibilizar um substituto temporário, o responsável da sala poderá pedir um empréstimo de um computador em uma sala vizinha, com a ciência do responsável da sala e aprovação do técnico de informática.

3.10. Na falta de substitutos para aparelhos defeituosos o técnico deve informar à direção e comunicar um pedido à secretaria de educação da cidade.

4. Politica de Responsabilidade

4.1. Nenhum professor pode fazer o *download* de um programa pela rede da Instituição sem o conhecimento e aprovação do técnico de informática.

4.2. O funcionamento contínuo da rede e de seus aparelhos de distribuição está sob responsabilidade do técnico de informática.

4.3. Nenhum outro funcionário além do técnico de informática possui permissão de manuseio dos cabos de rede, roteadores, e dispositivos wireless.

4.4. A rotulação adequada dos equipamentos, a separação dos dispositivos defeituosos dos úteis, o descarte dos aparelhos danificados que já foram dados com baixa no patrimônio e a notificação da diretoria da situação do acervo geral de equipamentos de tecnologia da informação disponíveis na instituição é obrigação do estagiário de informática.

4.5. A limpeza das telas e dos projetores nas salas cabe à equipe de limpeza, que deve ser instruída pelo técnico de informática sobre a forma correta de limpeza.

4.6. A limpeza e manutenção dos *notebooks* das salas e dos computadores usados pela equipe da Instituição estão sob a responsabilidade do técnico de informática.

4.7. O uso sensato da rede nas salas é de cuidados dos professores, sendo os mesmos a serem responsabilizados em caso de mau uso.

4.8. A diretora, pedagoga e pessoal da secretaria respondem sobre qualquer uso indevido das máquinas sob seus respectivos cuidados.

4.9. Caso haja uso não permitido das máquinas do instituto, é responsabilidade do estagiário localizar origem e responsáveis e encaminhar relatório à diretoria.

4.10. É de responsabilidade do estagiário de informática a criação e manutenção de um *e-mail* de contatos para atender pedidos de impressão e pesquisa feitas pelos professores.

4.11. É de responsabilidade do estagiário de informática manter no computador da sala de informática uma ferramenta de escaneamento de rede ou politica própria que permita detectar acessos indevidos.

4.12. É de critério do técnico a criação e manutenção de um *e-mail* para contato com os professores e diretoria.

4.13. Qualquer funcionário ou aluno que souber de uso indevido da rede da Instituição deve reportar imediatamente ao técnico de informática.

4.14. É de total reponsabilidade da Diretoria da Instituição a penalização de qualquer individuo pego utilizando indevidamente a Internet e/ou computadores da instituição.

Todas as politicas criadas nesse estudo tiveram o intuito de melhorar a manutenção e uso dos dispositivos eletrônicos e tecnológicos da instituição de ensino, além de ajudar na proteção contra vírus, *spams* e *trojans*.

Essa politica foi focada somente para o manuseio dos aparelhos e da rede sem considerar modelos ou programas em especial, pelo fato da maioria das invasões serem causadas por negligência humana, permitindo a ação dos *malwares*. A partir da implantação dessa política será feito um acompanhamento das regras estabelecidas neste estudo de caso.

Após a criação do manual das politicas de segurança, elas foram apresentadas aos professores e funcionários em uma das reuniões de equipe que acontecem semanalmente. Foram esclarecidas as dúvidas e assegurado aos docentes que os computadores das salas estariam conectados às redes com as senhas criadas pela politica 2.3 do manual gerado, evitando a divulgação das mesmas a pessoas não autorizadas como estipulado na politica 2.4.

O tráfego dos blocos A, B e C melhorou consideravelmente desde a criação das senhas pela diminuição de acessos indevidos. Com o efetivo funcionamento dos escaneamentos nas máquinas para a detecção de intrusos na rede da Informática como descrito na politica 3.3, foram constatados vírus macro nos computadores da secretaria, os quais foram desabilitados para efetiva limpeza e substituídos por outros computadores conforme a politica 3.4. Esses computadores foram atualizados com dados dos antigos computadores por CDs de *backup* permitindo seu uso imediato pelas secretárias seguindo a politica 3.5. O número de pedidos dos professores para o uso da sala de informática aumentou com a criação das senhas, realizando o propósito da política 1.14 do referido manual.

Devido ao mau funcionamento do roteador localizado na biblioteca que permitia a conexão das Redes da Biblioteca, do Bloco B e C com a Internet, as mesmas redes ficaram sem acesso por um período de cinco horas. Para cumprir com a politica 4.2 os técnicos utilizaram de cabos de fibra óptica para conectar o roteador defeituoso com o roteador da sala de Informática e configurando-o para servir de ponto de acesso da rede da Informática e reestabelecer o acesso a Internet nos blocos afetados. Após o furto de um dos *notebooks* do Bloco B que se encontrava fora da caixa de segurança, a diretoria colocou em prática a política 1.9 do manual para assegurar os outros equipamentos. Devido a um defeito no cadeado da sala de onde o *notebook* foi roubado, a secretaria pediu aos técnicos a realização da norma 1.4 durante o período que se seguiu até a reparação da caixa.

Através do acompanhamento do uso do manual de políticas nas situações relatadas confirmou-se uma redução na quantidade de *malwares* encontrados nos escaneamentos das primeiras semanas em relação às antecedentes, além de uma melhoria no desempenho da rede interna da Instituição. Porém vale ressaltar que á pedido dos integrantes do corpo docente, a politica 2.3 foi alterada, mudando de diversas senhas para uma senha única com o propósito de facilitar o uso das cinco redes disponíveis na Instituição. Isso também contrariando a politica de acesso 2.4, pois a nova senha foi disponibilizada aos funcionários.

Isso demonstra a não compreensão das ameaças perante ao uso da rede por usuários não acostumados com a área técnica da informática. Ressaltando o fator humano como principal problema de qualquer rede interna ou externa de uma organização. Entretanto o sucesso das demais políticas nas situações relatadas comprova que esse defeito na segurança pode ser minimizado com a devida gerência e atenção. Criar-se um manual de políticas de segurança para o manuseio de uma organização é um investimento necessário para evitar futuras situações de riscos aos dados trafegados nas redes. Esse trabalho demonstrou que a criação de politicas de segurança de redes é uma tarefa importante na área de segurança de qualquer organização. E disponibiliza um senário para um trabalho que vise acompanhar e analisara evolução da rede e da instituição nos anos seguintes á implementação do manual de regras e políticas.

4. Conclusão

Como estabelecido no inicio deste trabalho, foi realizado uma pesquisa bibliográfica de ameaças encontradas no mundo digital, que foram separadas em três grupos distintos de ameaças para melhor identificação dos pontos fortes e fracos de cada tipo de ataque. Os componentes de cada grupo foram detalhados através de citações de casos já ocorridos com essas mesmas ameaças. Em seguida foi dada uma explicação melhor dos ataques encontrados no estudo de casos contido no trabalho para uma melhor percepção dos riscos e danos que esses mesmos podem ou causaram no sistema de rede estudado.

Após essa explicação dos riscos foi apresentado ao leitor um sistema de rede de informática usado por uma instituição publica não voltada para área de

tecnologia da informação, semelhante a muitas outras organizações, publicas ou privadas, existentes no Brasil. Sua estrutura física e lógica foi relatada e suas fraquezas e vulnerabilidades descobertas durante o estudo. Com a pesquisa já feita sobre as ameaças e a identificação das mesmas no sistema em estudo, um manual contendo um conjunto de boas práticas e regras de manuseio da rede e de seus componentes foi criado e apresentado perante a instituição com o objetivo de ajudar na redução de danos e controle de casos de invasão do sistema de informática da instituição.

Após uma pequena análise e correção pela diretoria da instituição de ensino do estudo de casos as regra do manual de politicas de segurança foram aprovadas e relatadas neste trabalho. A implementação efetiva das mesmas na organização em questão se deu após sua apresentação e explicação aos docentes e funcionários durante uma reunião geral, onde algumas dúvidas foram retiradas. Com os professores devidamente orientados foi dado inicio ao acompanhamento da rede da organização com o uso das regras. A rede teve seu tráfego reduzido e sua velocidade aumentada. Certos computadores pertencentes aos professores tiveram uma melhora em seu desempenho com a remoção de vírus de seu sistema operacional. Casos de acesso a sites indevidos foram controlados e uma comunicação eficiente entre diretoria e área de informática foi estabelecida dentro da instituição, junto com procedimentos de backup para garantir a disponibilidade de dados importantes.

Com as melhorias descritas acima na rede de uma instituição de ensino através da criação de um manual de regras, fica demonstrado que a principal falha explorada pelas ameaças da internet é o fator humano, ou seja, as pessoas. Entretanto, essa vulnerabilidade pode ser combatida pelas organizações dependentes de internet sem um alto gasto, com a criação de regras e boas praticas (dicas) em relação ao manuseio da rede pelos usuários. Sendo que isso pode ser feito por qualquer pessoa com um conhecimento básico de segurança de redes, ou de computação, com uma devida análise de rede e uma rápida pesquisa dos tipos de ataques mais atuais e comuns.

5. Referências

ALECRIM, Emerson. **Vírus de computador e outros malwares:** o que são e como agem. Disponível em: http://www.infowester.com/malwares.php. Acessado em 01 de novembro. 2014

CERT - Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil, **Códigos Maliciosos.** Disponível em: <http://cartilha.cert.br/malware/>. Acessado em: 06 Abr. 2014

DAQUINO, Fernando. **Mito ou verdade: dá pra confiar em antivírus?** Disponível em: http://www.tecmundo.com.br/antivirus/4252-mito-ou-verdade-da-para-confiar-em-antivirus-.htm. Acessado em: 15 de setembro.

Duarte, N. F. L. C. **Segurança Contra Intrusões em Redes Informáticas.** Porto / Portugal/ Instituto Superior de Engenharia do Porto 2008. 224 p.

GONÇALVES, J. C**. O gerenciamento da informação e sua segurança contra ataques de vírus de computador recebidos por meio de correio eletrônico.** Taubaté / SP: UNITAU/Faculdade de Economia, Contabilidade e Administração 2002. 339 p.

Goulart, M. **Vírus de Computador.** Disponível em: http://www.webartigos.com/artigos/virus-de-computador/22108/. Acessado em: 31 de outubro. 2014.

LEOOP. **Trabalho de MTC. Artigo científico.** Disponível em: http://pt.slideshare.net/leopp/artigo-cientfico-anti-vrus. Acessado em: 02 de outubro. 2014.

MAGALHÃES, Marcelo V V. **Segurança de sistemas:** ênfase em redes de computadores**.** Disponível em: http://www.gta.ufrj.br/grad/02_1/seguranca/. Acessado em: 02 de novembro. 2014.

MOREIRA, E. **Novo cavalo de troia usa Mac para atacar websites.** Disponível em: <http://www.techtudo.com.br/noticias/noticia/2011/10/novo-cavalo-de-troia-usa-mac-para-atacar-websites.html>. Acessado em: 20 ago. 2014.

NASCIMENTO, Nelson J. **Vírus de Computador e as Estratégias de Prevenção.** Disponível em: http://www.portaleducacao.com.br/informatica/artigos/50159/virus-de-computador-e-as-estrategias-de-prevencao. Acessado em: 17 de setembro. 2014

STALLINGS, W. **Criptografia e segurança de redes.** 4.ed. São Paulo: Pearson Hall, 2008, 492p.