CENTRO PAULA SOUZA

ETEC PROFESSOR MASSUYUKI KAWANO

Técnico Em Redes De Computadores

Abner Nathan De Godoy Dias

Antonio Carlos Berengue

Everton Torres Da Costa

João Pedro Bêss Vicente

Luiz Davi Santos Oliveira

SEGURANÇA DA INFORMAÇÃO: Estratégias para proteger computadores de ataques maliciosos

Tupã - SP

2018

Abner Nathan de Godoy Dias

Antonio Carlos Berengue

Everton Torres da Costa

João Pedro Bêss Vicente

Luiz Davi Santos Oliveira

SEGURANÇA DA INFORMAÇÃO: Estratégias para proteger computadores de ataques maliciosos

Trabalho de Conclusão de Curso apresentado ao curso Técnico em Redes de Computadores da ETEC Prof. Massuyuki Kawano, orientado pelo Prof. Anderson Tukiyama Berengue e Paula R. Garcia Zanini como requisito parcial para obtenção do título de Técnico em Redes de Computadores.

Tupã - SP

2018

RESUMO

Abner Nathan de Godoy Dias, Antonio Carlos Berengue, Everton Torres da Costa, João Pedro Bêss Vicente, Luiz Davi Santos Oliveira
Orientadores: Anderson Tukiyama Berengue, Paula R. Garcia Zanini

A tecnologia vive uma expansão contínua originando ameaças que evoluem no mesmo ritmo, levando à necessidade de aprimorar as técnicas utilizadas na segurança da informação, sendo estas consideradas importantes e sigilosas, portanto devem ser protegidas. No âmbito empresarial, a segurança é de suma importância. Portanto, funcionários mal treinados e máquinas desatualizadas, aumentam as chances de uma quebra de segurança, colocando em risco a rede e a organização em si. Um servidor bem estruturado é necessário, pois controla e gerencia a rede, além de proteger de vários tipos de vírus presentes na internet e inúmeros métodos que podem infectar computadores. Este trabalho tem como objetivo, criar estratégias para proteger as informações de ataques maliciosos e de má fé, apresentando os tipos de ataques mais comuns bem como as precauções e soluções para evitá-los além de demonstrar a execução do *ransomware* e seus efeitos colaterais.
.

Palavras Chave: Tecnologias, redes, computadores, servidores, server, ataques, defesa, *ransomware*, Linux, Windows.

SUMÁRIO

1. Introdução

A tecnologia vive uma expansão continua trazendo as ameaças que evoluem no mesmo ritmo, levando a necessidade de aprimorar técnicas utilizadas na segurança de suas informações sendo estas consideradas importantes e sigilosas, portanto devem ser protegidas.

No âmbito empresarial a segurança é de suma importância e com funcionários mal treinados e máquinas desatualizadas aumentam o perigo de uma quebra de segurança colocando em risco as informações e a organização em si, um servidor bem estruturado é necessário, pois controla e gerencia a rede, além de proteger contra vários tipos de vírus presente na internet e inúmeros métodos que podem infectar computadores.

Seguido dessas informações o uso de máquinas com sistema *Linux Server* ou *Windows Server*, atualmente é a melhor opção, pois o desempenho da segurança, estabilidade e aplicabilidade agregados com um excelente *firewall* e criptografia resultam no difícil acesso às ameaças externas. Dessa forma essas informações são armazenadas em servidores, máquinas com aplicações específicas para o monitoramento e gravação de grandes volumes de dados, bem como responsável pelo gerenciamento de usuários da rede, controlando diretamente o acesso aos periféricos e arquivos compartilhados com impressoras, modens ou discos.

As empresas atuais necessitam não apenas de segurança física, mas também da virtual, com o avanço da tecnologia os documentos considerados “importantes” foram transferidos para computadores tornando difícil a segurança física dos dados no servidor. Pensando nisso, ocorreram formas de dificultar o acesso às informações sigilosas.

2. Segurança da Informação

A Segurança da Informação está sofrendo muitas vulnerabilidades nas empresas brasileiras de pequeno e médio porte. Sabendo-se que estamos vivenciando a era digital, temos poucos investimentos significativos na área. Mas por um lado, o aumento de pessoas interessadas na tecnologia só cresce, fazendo com que empresas e órgãos ligados ao tema, busquem meios de manter a vasta conexão *web* (Security 2016).

Pode-se dizer que segurança da informação tem o objetivo de proteção a um conjunto de dados, com a finalidade de guardar o valor que possuem para uma organização.

Com essas características, levantou-se alguns aspectos que devem ser seguidos para um ótimo desempenho, como: confidencialidade, integridade e disponibilidade; não girando em torno apenas de sistemas operacionais, informações eletrônicas ou sistemas de armazenamentos.

A confidencialidade é o ato que faz informações sigilosas só serem acessadas por pessoas autorizadas.

Integridade tem o pensamento que dados não devem ser alterados ou excluídos de maneira não programada ou autorizada, ou seja, garantia de que os dados estarão íntegros.

Disponibilidade, o serviço ou acesso a informação deve estar sempre disponível para quem possui autorização (SEGURANÇA DA INFORMAÇÃO EM REDES CORPORATIVAS,2011).

Segundo o “Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil ocorreram mais de 722 mil incidentes de segurança na Internet em 2015” (ALERTA SECURITY, 2016), os 5 maiores causadores desse levantamento são: *scan*, fraudes, ataques a servidores *web*, *worms* e Denegação de serviço (Denial of Service - DOS).

3. Conceitos de servidores

Alguns tipos de servidores que serão abordados neste trabalho, de acordo com o Serviço Nacional de Aprendizagem Comercial (SENAC) do Rio Grande do Sul (Projeto e Implantação de Servidores,2014):

3.1- Servidor de Arquivos:

É uma máquina com memória ou vários HDs de grande capacidade onde arquivos ou aplicativos estão gravados e disponíveis para o ambiente de rede permitindo que o armazenamento centralizado de arquivos proporcione alto grau de segurança de dados para toda a organização.

3.2- Servidor de Banco de dados:

Tem a responsabilidade de servir a uma aplicação (software). Os dados armazenados nele, além de possuir uma ferramenta gerenciadora de banco de dados, permitindo a leitura e Alteração dos dados.

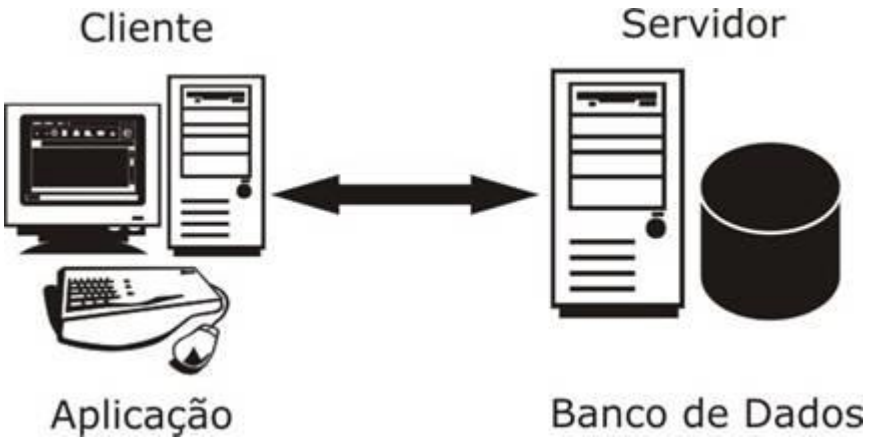

Figura 1 - Representação da comunicação entre cliente e servidor
Fonte : www.juliobattisti.com.br/artigos/livrodelphibd/capitulo1/01.asp

3.3- Servidor Linux:

O Linux é um sistema operacional que foi desenvolvido pelo finlandês, Linux Torvalds, onde seu código fonte é aberto sobre a licença GPL (*General Public License*) com disponibilidade para que qualquer pessoa possa utilizar e estudar, modificar, distribuir livremente conforme está no acordo dos termos de licença (MORIMOTO, 2006).

O sistema Linux é conhecido por sua capacidade de funcionar anos sem falhas, isso é positivo para uma pequena e média empresa, nas quais estes erros no sistema possam causar problemas significativos, o sistema Linux também trabalha com grande número de processos simultâneos, de uma forma melhor que o Windows.

Além disso o Linux é nativamente mais seguro, seja em servidores, desktop ou ambientes embarcados, se comparado ao Windows. O sistema também sofre menos ataques, pois estas vulnerabilidades tendem a serem descobertas rapidamente e corrigidas (NOYES,2010).

Sendo um sistema leve e flexível a necessidade dos usuários, tornando suas adaptações e “correções”, muito mais rápidas. Funcionando praticamente em qualquer computador, pode ser instalado e executado em diversos processadores e arquiteturas (Arm e Titanium). Sendo assim poderá estabelecer parâmetros para incluir apenas os serviços que serão necessários no determinado momento para a

determinada empresa, reduzindo memória, melhorando o desempenho e mantendo o funcionamento simples e contínuo.

.

Figura 2 - Tux, mascote do Linux

Fonte : Vivaoliux.com.br

3.4- Servidor Windows:

Uma opção de uso de servidor é o software desenvolvido pela Microsoft que possui muitas funções no ambiente do sistema, entre usuário e servidor. Os servidores são configurados para fornecer autenticação, executar aplicativos e comunicação dos usuários com outros servidores e recursos da rede.

Em abril de 2003, foi lançado o Windows Server 2003 que teve como base o Windows 2000 Server. Com o Windows Server 2003 a Microsoft realizou melhorias em seu serviço de rede e ao Active *Directory* (PROCÓPIO,2008). *Active Directory* é um serviço de diretórios usados em Windows Server, é um identificador de recursos disponíveis na rede, e disponibiliza informações a usuários e administrador. O Windows Server 2003 tem outras versões: *Standard edition, web edition, enterprise edition, x64-bit edition.*

Alguns dos serviços prestados em ambiente *Windows* são: *FIREWALL, PROXY, DNS, DHCP, FTP, E-MAIL, WEB,* banco de dados, acesso remoto. Podem ser instalados e configurados de acordo com as necessidades.

Mais tarde, foi lançado o *Windows Server* 2008 que teve como objetivo ser o sucessor do *Windows Server* 2003. Oferecendo um melhor desempenho seja em aplicações de infraestrutura de redes mais seguras e uma melhor organização. Também possui quatro versões de seu sistema operacional: *Windows Server 2008 standard edition, Windows enterprise edition, Windows server 2008 datacenter edition e Windows web server 2008.*

Logo, veio ao mercado *o Windows Server 2012* e o mais atual *Windows Server 2016* sendo os mais populares, junto ao *Windows Server 2008*.

No mundo da tecnologia onde os computadores contêm informações valiosas, o sistema de servers da Microsoft são os que mais sofrem ataques de hacker por ser de fácil acesso por conta de um vírus por exemplo.

Ainda assim o Windows Server tem algumas vantagens por possuir uma excelente interface gráfica com diversas opções ao usuário complementado por uma grande facilidade de operação. Entretanto, há desvantagens em relação ao preço exorbitante de uma licença vendida pela Microsoft, além da segurança que não é 100% confiável havendo falhas que "criminosos virtuais" aproveitam.

Existem os softwares de proteção, antivírus próprios para servidores que são pagos e oferecem um bom serviço, contando sempre com o bom firewall atualizado. Manter o sistema sempre atualizado e gerenciado, evita que sofram com ataques e prejuízos para empresa.

Figura 3 – Logo do Windows Server 2012 e suas versões

Fonte: https://infrashared.wordpress.com/2014/06/05/windows-server-2012-diferenca-entre-versoes/

4- Tipos de ataques

Os tipos de ataques mais conhecidos e comumente utilizado na internet são a *Denial of Service* (DOS), *Distributed Denial of Service* (DDOS), Cavalo de troia, *toolbars*, *Backdoor*, *Port scanning, Ransomware, Worm* (Teotônio,2012).

4.1-Trojan Horse (Cavalo de Troia)

São vírus que se apresentam como um programa normal desejável e não maliciosos. Instalam-se e executam sem serem percebidos por programas de antivírus, mas isso não acontece sozinho é necessário a “vítima” executar o vírus. Visto que ao ser acionado causa a perda ou roubo de dados. São muito conhecidos por criarem a *backdoor*, ou porta de fundos de um computador, que fornece o acesso ao sistema e a informações confidenciais ou pessoais. O cavalo de troia diferente de outros vírus não infecta outros arquivos e nem se autorreplica na rede.

4.2- Rootkit.

Definidos como *malwares* que muitas vezes não são detectados por *softwares* de segurança, como os antivírus, pois se escondem e ocultam suas chaves de registro, funciona interceptando ações do próprio sistema operacional e alterando seus resultados. Sendo assim, com tal capacidade permite que este tipo de *malware* fique no sistema da vítima por meses, e até anos, sem mesmo ser percebido. Isso permite ao *hacker* uma porta livre de entrada e saída chamada *backdoor*. O *rootkit* pode infectar tanto o sistema *Linux* quanto o *Windows*. No *Linux* ele substitui um programa de listagem de arquivos. Assim ele mesmo exibira a lista, e não ficara visível. No *Windows* ele infecta os processos de memória, anulando pedidos do programa que está infectado enganando e forçando acreditar que o arquivo malicioso não existe, provocando mensagens de erro.

Para evitar é bom saber por onde eles se proliferam como a maioria dos vírus, trojans e várias outras pragas digitais, os *rootkits* se espalham em e-mails e sites maliciosos. Ao clicar em um deles você pode dar acesso a uma *backdoor*, um caminho para roubar suas informações pessoais. Sempre tenha ao seu dispor um bom antivírus e um *firewall* atualizado. Com alguns anti*malwares* que garantem uma maior proteção, com um *scan* regularmente.

4.3- Worm

São pragas semelhantes aos vírus, se defendem pela sua capacidade de se autorreplicar sem a necessidade de infectar outros arquivos. A ideia é criar cópias funcionais e buscar maneiras de infectar outros computadores através conexões de rede locais, *internet*, anexos de e-mail e *drivers* USB.

Além de disso, o *worm* pode tornar o computador infectado vulnerável a outros ataques e provocar danos apenas com o tráfego de rede gerado pela sua reprodução.

4.4- DOS e DDOS

O tipo DOS, ataque de negação de serviço (*Denial Of Service*, em inglês), tem como objetivo sobrecarregar um servidor ou um computador comum, fazendo com que os recursos do sistema fiquem esgotados. O atacante envia simultaneamente pacotes para o alvo, deixando o sobrecarregado impossibilitando de responder qualquer pedido de pacote.

Os servidores *web* são os que mais sofrem com este tipo de ataque pois, *hacker* ou *cracker* tenta tornar as páginas hospedadas indisponíveis na *Web*. Esse ataque não se caracteriza como uma invasão do sistema visto que ele realiza apenas a invalidação por meio de sobrecarga.

Os ataques DOS envolvem apenas um atacante, sendo um único computador a enviar pedidos de pacotes. Desta forma apenas é possível derrubar servidores fracos e computadores comuns com pouca banda e com baixas especificações técnicas.

DDoS tem a mesma função do DOS, sendo a única diferença na qual se caracteriza, por ter uma máquina mestre que pode gerenciar até milhões de computadores, chamados de zumbis. Por meio destas máquinas "Zumbis", o computador mestre manda comandos que fazem todas elas acessarem um recurso em um determinado servidor ao mesmo tempo provocando travamento e sobre carregamento de tráfego de pacotes no alvo.

É sempre bom estar atento ao tráfego da rede no qual o seu computador ou servidor está conectado. Caso o computador estiver enviando pacotes sem que o usuário esteja acessando algum serviço na internet, pode ser um indício de que a máquina é um zumbi

4.5- Ransomware

É um tipo de *malware* que tem como intuito bloquear ou “sequestrar" o computador e os arquivos da vítima. Forçando um resgate via pagamento. Geralmente por *bitcoins* que torna quase impossível o rastreamento do criminoso. Os *ransomwares* agem codificando dados do sistema operacional de forma com que os usuários não tenham mais acesso.

A propagação deste *malware* não é diferente do modo de disseminação de outros vírus: e-mails, redes sociais, sites falsos, entre outros.

4.6- Backdoor

Um computador infectado por um *malware* que contenha *backdoor* será vulnerável a um ataque externo onde o dono do *malware* pode controlar os arquivos livremente através de uma porta.

A forma mais comum de infectar o computador está na substituição de um serviço por outro diferente, se a nova versão for adulterada o *malware* irá infectar o sistema deixando-o controlável pelo invasor. Outra forma é através de cavalo de troia que vem em alguns programas que o administrador instala.

4.7- Spoofing

É um tipo de falsificação tecnológica que procura enganar uma rede ou uma pessoa fazendo-a acreditar que a fonte de uma informação é confiável, quando a realidade é bem diferente. Por exemplo, hackers podem fazer um *spoofing* de e-mail, enviando a você mensagens que pareçam vir de alguém em quem você confia como forma de fazê-lo fornecer dados sigilosos. Ou então eles podem realizar o *spoofing* de IP e DNS para tentar fazer com que sua rede direcione você para sites fraudulentos que vão infectar seu computador.

4.8- Cache Poisining

Ocorre quando o servidor armazena informações incorretas de um domínio, toda vez que for solicitado esse domínio ele irá responder incorretamente, o servidor aceitara o domínio sem uma checagem de veracidade. Assim o cache infectado alcança as informações armazenadas e podendo ser alteradas pelo invasor.

4.9- Port Scanning Attack

É uma técnica utilizada para averiguar se as portas do sistema estão abertas tornando-as vulneráveis a invasões de softwares perigosos, essa técnica é extensamente utilizada tanto por potenciais invasores como também pelo responsável da segurança do sistema.

O ataque é simples, uma mensagem é enviada para uma porta e após isso espera pela resposta, a partir da resposta é possível indicar a situação da porta e se ela é suscetível a uma invasão ou não.

4.10- Ataques de Força Bruta

Consiste em atacar o alvo com todas as combinações de senhas possíveis através do método de tentativa e erro onde o atacante tenta combinações de senhas até conseguir encontrar a senha correta (Paula,2014).

4.11- Phishing

Consiste em uma ação para tentar conseguir informações pessoais como usuário e senhas de bancos, redes sociais, número do RG, CPF, cartões bancários entre outros. Esse tipo de ataque ocorre em maior frequência em web sites e em e-mail aparentemente reais pedindo para a vítima digitar essas informações (Pedro Silveira).

5- Desenvolvimento

O principal motivo de ataque aos servidores é a falta de conhecimento do usuário na utilização da máquina assim como não respeitar as normas de segurança de empresas acessando locais indevidos com alto índice de vírus.

Um ataque que teve grande notoriedade nos últimos anos é o *ransomware* que foi utilizado por criminosos como um meio de ganhar dinheiro, pois pedem uma quantia em moeda geralmente na forma de *bitcoin*, tipo de moeda virtual que não tem como ser rastreada no mercado financeiro, para a recuperação de seus arquivos, segundo o FBI, o *ransomware* é uma ‘indústria’ emergente a qual faturou aproximadamente US$ 1 bilhão em 2016 (RIBEIRO,2017)

O *Ransomware* que causou um dos maiores prejuízos é o *WannaCry* que em 2017 infectou diversos computadores pelo mundo, tornando-se uma preocupação

para empresas que dependem do uso de computadores, criptografando seus dados em geral.

O surto sem precedentes ficou conhecido mundialmente por volta de maio de 2017, afetando usuários domésticos e empresas. Sendo reconhecido como o primeiro *ransomworm* da história, ou seja, um *ransomware* com função de um *worm*.(SITE PROOF,2017)

Desenvolvido pelo grupo de hackers The Shadow *brokers*, o ataque utilizava uma falha *EternalBlue* que explorava vulnerabilidades do Microsoft Windows, no módulo de compartilhamento de arquivos o *Server Message Block* (SMB), que permitia execução de código remoto.

O Ataque deu início dia 12 de maio de 2017, logo nas primeiras horas o vírus conseguiu se disseminar por 11 países entre eles o Brasil. Em um período de 3 dias, foi identificado mais de 250 mil sistemas no mundo em mais de 150 países infectados, em 5 dias o número passou de 345 mil. Presumindo que 97% dessas máquinas tiveram seus dados criptografados.

Figura 4 – calendário do ataque Wannacry
Fonte : https://www.proof.com.br/blog/wannacry-ransomworm/

5.1- Como ser vítima do RANSOMWARE:

- Baixando programas que dizem ser um utilizável como crack (*software*);
- Baixando imagens que podem conter o *malware*;
- Links de *download* anexados em e-mails falsos;
- Não possuir antivírus ou deixa-lo desatualizado;
- Acessar sites duvidosos;
- Falta de treinamento básico para utilização do computador.

5.2- Como evitar o RANSOMWARE:

- Ter um antivírus atualizado;
- Verificar atualizações do sistema operacional;
- Ter cópias dos arquivos em mais de um lugar (backup);
- Verificar a veracidade de e-mails antes de clicar nos arquivos anexados;
- Não acessar sites duvidosos;
- Evitar fazer downloads pessoais nas máquinas da empresa;
- Tomar cuidado ao utilizar pendrives e cartões de memórias (Evitar de usar fora do ambiente de trabalho);
- Ter máquinas com senha para evitar que qualquer pessoa consiga acessá-la;
- Seguir a política de segurança da empresa;
- Não instalar programas duvidosos nos computadores;
- Não abrir ícones com extensão .bat ou.cmd.

5.3- Caso contraia o vírus devemos.

- Se o usuário conseguir utilizar o computador mesmo com as informações criptografadas, restaurando o Windows a um ponto anterior a execução do *ransomware* consiga ter acesso ao seus arquivos e documentos, contudo se não conseguir utilizar essa ferramenta, a formatação do computador e a utilização do backup é a saída.
- Mais viável se os arquivos que foram infectados forem de suma importância pagar o 'resgate' seria a maneira mais fácil de tentar recuperar a senha com os hackers, mas não é garantido que eles vão liberar a senha para você recuperar os arquivos isso deve ser o último recurso a ser usado.
- O ideal é ter sempre um backup atualizado em mídias fora do computador como pen drives, hd externos, nuvem para ser utilizado nesses casos.

6- Considerações finais

A principal forma de se prevenir contra *malwares* na rede é respeitar as diretrizes da empresa quanto a segurança no manuseio das máquinas e utilização da internet. Para evitar que o servidor e as máquinas sejam infectados, é imprescindível que a empresa mantenha um sistema de segurança atualizado (firewall, antivírus, sistema operacional, servidores) evitando com isso que sua rede seja infectada.

Assim como fazer o backup de arquivos, bloquear sites que não sejam utilizados no ambiente de trabalho da empresa, não baixar conteúdo duvidoso e não utilizar o servidor diretamente preferindo assim as máquinas clientes.

7- **Referências**

LEÃO, Marcelo. Borland Delphi 7 cursos completo. Editora Axcel Books, 1ª Edição, 2003. Acesso em 22/02/2018

PEREIRA, Paulo Roberto Alves. Desenvolvendo aplicações orientadas a objetos com Borland Delphi. Web Publicação de 2002. Disponível em http://www2.fateb.br/ftp/apostilas/Delphi/OO-Delphi.pdf. Acesso em 19/03/2014.

Ana Paula Muniz; Diogo Rocha Ferreira de Menezes. Artigo Evolução da linguagem Delphi – Web Publicação em 13/08/ 2014. Disponível em http://pt.slideshare.net/diogorochamenezes/evoluo-da-linguagem-delphi-artigo. Acesso em 26/04/2015

ANSELMO, Fernando Antonio F. Desvendando o Caminho das Pedras. Web Publicação de 1995-97. Disponível em http://www.greantoniobraga.seed.pr.gov.br/redeescola/escolas/13/870/10/arquivos/File/Adenildo/Biblia-Delphi-7-PtBr.pdf. Acesso em 27/04/2015

ALERTA SECURITY. Política de segurança da informação: entenda a sua importância. Publicado em 20 dez. 2016. Disponível em:< https://alertasecurity.com.br/blog/183-politica-de-seguranca-da-informacao-entenda-a-sua-importancia. Acesso em 20 mai. 2018.

PROFF; Wannacry-ransomworm; disponível em https://www.proof.com.br/blog/wannacry-ransomworm/; acesso em 06/06/2018

MORIMOTO, Carlos E. Guia Completo de Redes; web publicação; https://www.hardware.com.br/. Acesso em 10/04/2018;

NOYES, Katherine; Cinco motivos que colocam o Linux à frente do Windows em servidores; web publicação 2010; disponível em http://idgnow.com.br/ti-corporativa/2010/08/31/cinco-motivos-que-colocam-o-linux-a-frente-do-windows-em-servidores/; acesso em 04/06/2018

TEOTÔNIO, Ítalo Diego; Ameaças Virtuais – Conheça algumas delas e suas principais características; web publicação 2010; disponível em https://www.profissionaisti.com.br/2012/07/ameacas-virtuais-conheca-algumas-delas-e-suas-principais-caracteristicas/; acesso 04/06/2018

PRADO, Jean. Como se proteger contra o *ransomware* que atacou empresas de todo o mundo https://tecnoblog.net/214637/ransomware-wannacry-windows-smb-remover/. Acesso em 16/05/2017

SILVEIRA, Pedro. Tudo que você precisa saber para não cair no phishing; Web publicação 2017; disponível em https://canaltech.com.br/seguranca/tudo-que-voce-precisa-saber-para-nao-cair-no-phishing-89514/; Acesso em 11/06/2018

8- Bibliografia

LEÃO, Marcelo. Borland Delphi 7curso completo. Editora Axcel Books, 1ª Edição, 2003. Acesso em 22/02/2018

PEREIRA, Paulo Roberto Alves. Desenvolvendo aplicações orientadas a objetos com Borland Delphi. Web Publicação de 2002. Disponível em http://www2.fateb.br/ftp/apostilas/Delphi/OO-Delphi.pdf. Acesso em 19/03/2014.

ANA PAULA MUNIZ; Diogo Rocha Ferreira De Menezes. Artigo Evolução da linguagem Delphi – Web Publicação em 13/08/ 2014. Disponível em http://pt.slideshare.net/diogorochamenezes/evoluo-da-linguagem-delphi-artigo. Acesso em 26/04/2015

ANSELMO, Fernando Antonio F. Desvendando o Caminho das Pedras. Web Publicação de 1995-97. Disponível em http://www.greantoniobraga.seed.pr.gov.br/redeescola/escolas/13/870/10/arquivos/File/Adenildo/Biblia-Delphi-7-PtBr.pdf. Acesso em 27/04/2015

YAMAZACK, WESLEY. Recursos de Compilação no Delphi. Web Publicação. http://www.devmedia.com.br/recursos-de-compilacao-no-delphi/16964. Acesso em 25/01/2016

SZYMANSKI, THIAGO. Os 4 ataques hackers mais comuns da web. Web Publicação.

https://www.tecmundo.com.br/ataque-hacker/19600-os-4-ataques-hackers-mais-comuns-da-web.htm. Acesso em 20/02/2012

NOVAES, RAFAEL. Botnet x Backdoor: o que são e como se prevenir

http://www.psafe.com/blog/botnet-x-backdoor-sao-como-prevenir/. Acesso em 18/09/2014

FERREIRA, MARCOS. Ransomware: O Que é e Como Recuperar Seus Arquivo

http://labs.siteblindado.com/2015/05/ransomware-o-que-e-e-como-recuperar.html. Acesso em 23/09/2016.

MEYRELLES, THIAGO. Peguei um Ransomware, o que devo fazer?

http://www.migalhas.com.br/dePeso/16,MI257412,31047-Peguei+um+Ransomware+o+que+devo+fazer. Acesso em 18/04/2017

RIBEIRO, HENRIQUE. O que fazer após um ataque de ransomware?

https://canaltech.com.br/infra/o-que-fazer-apos-um-ataque-de-ransomware-96210/. Acesso em 28/06/2017.

PEGUEI UM RANSOMWARE, O QUE DEVO FAZER? https://www.penso.com.br/peguei-um-ransomware-e-agora-o-que-devo-fazer/

WESTPHALEN, FREDERICO. Segurança da Informação aplicada a servidores utilizando técnicas de Hardening. Brasil 2013

SOUSA, RIBAMAR FERREIRA DE. Administração de Servidores Linux, Passo-a-passo - Fortaleza: Clube de Autores, 2012

ABREU, YGOR. Guia Completo Ubuntu https://ubunteiro.wordpress.com/ . Acesso em 16/05/2018

NASCIMENTO, EDMAR JOSÉ DO. Introdução às Redes de Computadores http://www.univasf.edu.br Acesso em 10/04/2018.

BOTELHO, ELIZAR SEVERINO. INSTALAÇÃO E CONFIGURAÇÃO DE SERVIDORES LINUX. Acesso em 27/03/2018.

https://support.microsoft.com/pt-br/help/129972/how-to-prevent-and-remove-viruses-and-other-malware

https://www.cisco.com/c/dam/r/pt/br/internet-of-everything-ioe/assets/pdfs/whitepaper_c11-733367_PTBR.pdf

https://www.mcafee.com/br/resources/solution-briefs/sb-quarterly-threats-jun-2017-1.pdf

http://187.7.106.13/vanessa/TURMA%20IV/Material%20de%20Servidores%20PDF.pdf

Anexo 1

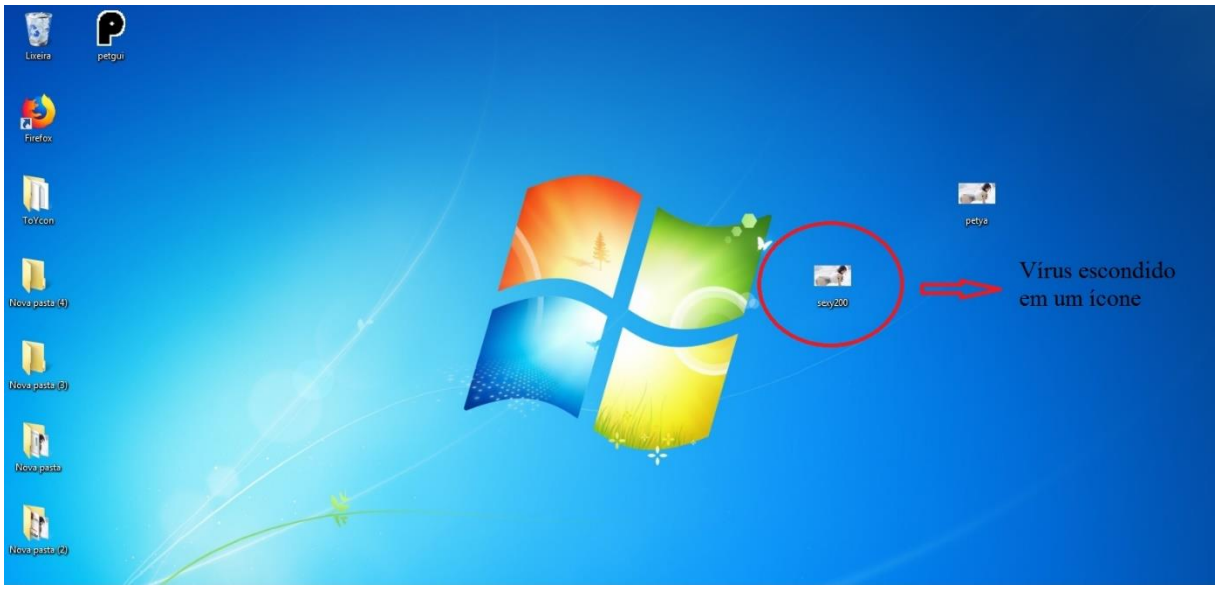

Figura 1 – Vírus escondido em um ícone
Fonte : Autoria própria

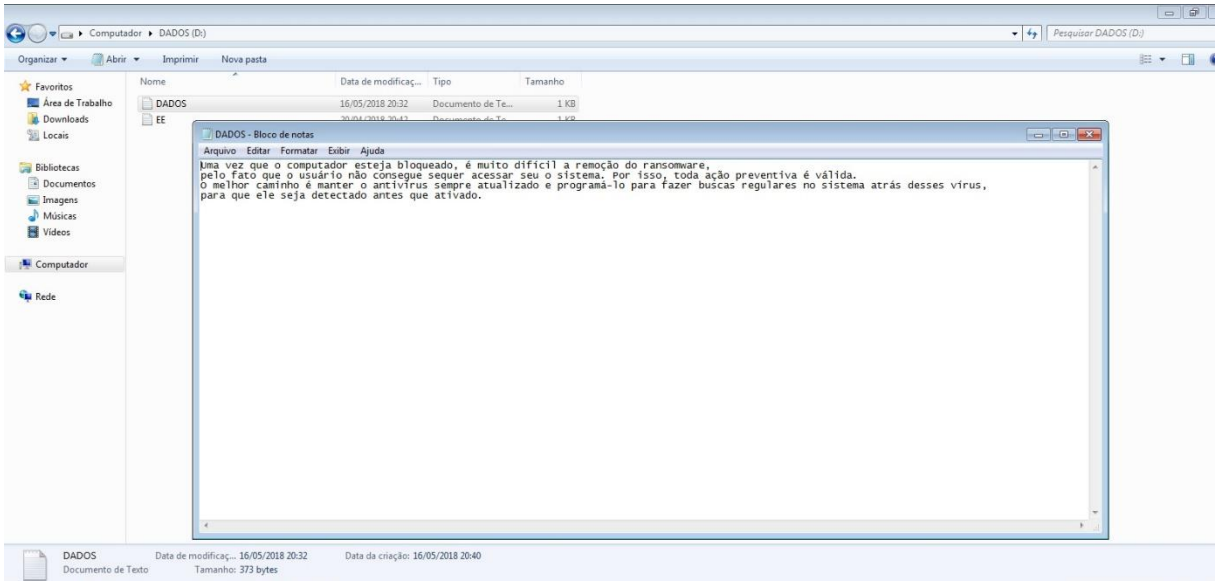

Figura 2 – Demonstração de um arquivo de texto com informações dentro
Fonte – Autoria própria

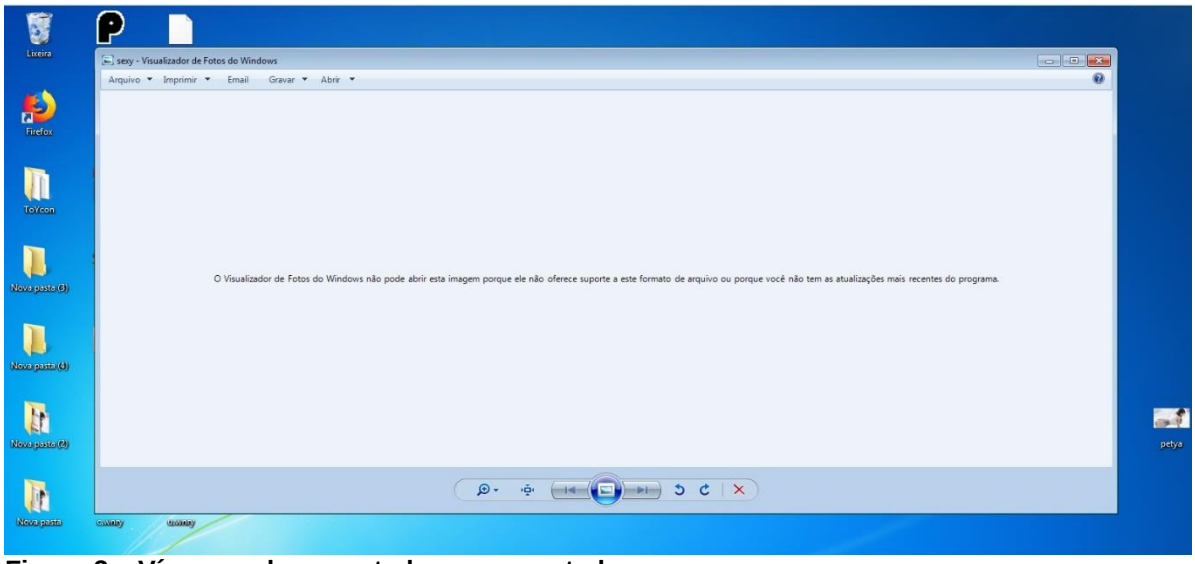

Figura 3 – Vírus sendo executado no computador
Fonte – Autoria própria

Figura 5 – Layout do vírus em execução
Fonte – Autoria própria

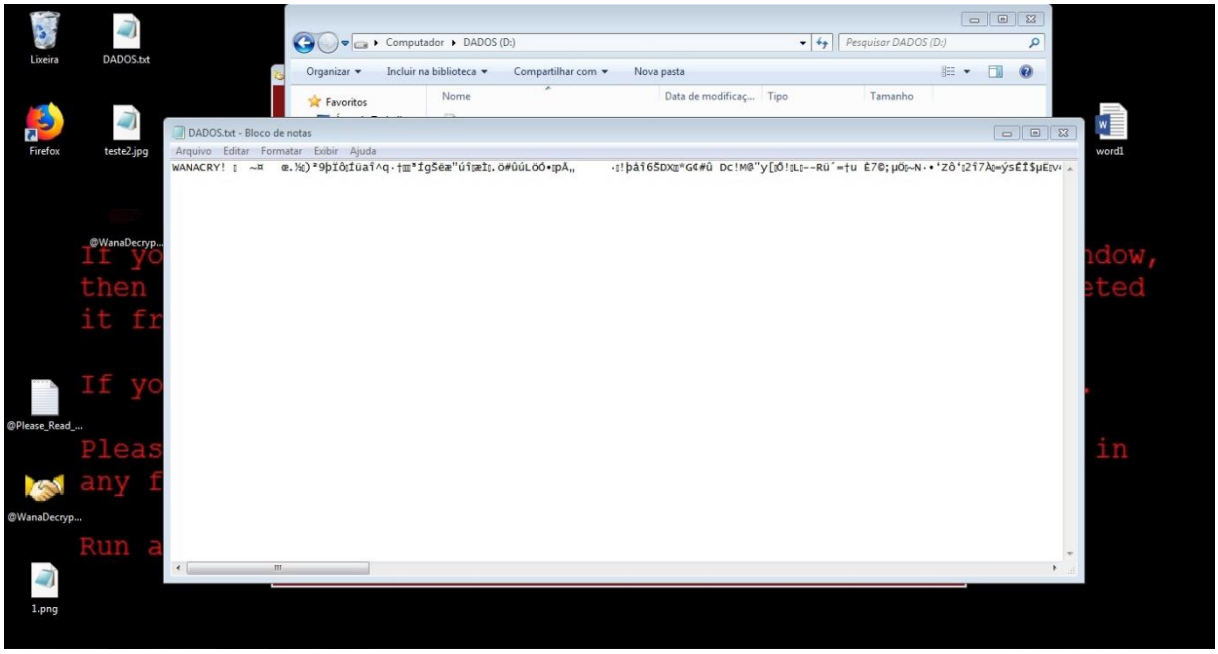

Figura 6 – Demonstração dos arquivos criptografados
Fonte – Autoria própria