INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

LUCIANDERSON ALVES GOMES

O USO DE MALWARES EM GUERRAS CIBERNÉTICAS

NATAL – RN

2015

LUCIANDERSON ALVES GOMES

O USO DE MALWARES EM GUERRAS CIBERNÉTICAS

Trabalho de Conclusão de Curso apresentado ao curso de Tecnologia em Redes de Computadores, do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, em cumprimento às exigências legais como requisito parcial à obtenção do título de Tecnólogo em Redes de Computadores.

Orientadora: Prof.ª Dra. Joêmia Leilane Gomes de Medeiros.
Coorientador: Prof. Dr. Rodrigo Siqueira Martins.

NATAL – RN

2015

Gomes, Lucianderson Alves.
G633u O uso de malwares em guerras cibernéticas / Lucianderson Alves Gomes. – Natal, 2015.
62 f. : il. Color.

Trabalho de Conclusão de Curso (Tecnólogo em Redes de Computadores) – Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte. Natal, 2021.
Orientadora: Prof.ª Dra. Joêmia Leilane Gomes de Medeiros.
Coorientador: Prof. Dr. Rodrigo Siqueira Martins.

1. Redes de computadores. 2. Segurança da informação. 3. Ameaças cibernéticas. 4. Guerras cibernéticas. 5. Malwares – Código malicioso. I. Medeiros, Joêmia Leilane Gomes de. II. Martins, Rodrigo Siqueira. III. Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte. IV. Título.

CDU: 004.7

Catalogação na Publicação elaborada pelo Bibliotecário Joel de Albuquerque Melo Neto – CRB-15/320
Biblioteca Central Sebastião Fernandes (BCSF) – IFRN

LUCIANDERSON ALVES GOMES

O USO DE MALWARES EM GUERRAS CIBERNÉTICAS

Trabalho de Conclusão de Curso apresentado ao curso de Tecnologia em Redes de Computadores, do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, em cumprimento às exigências legais como requisito parcial à obtenção do título de Tecnólogo em Redes de Computadores.

Trabalho de Conclusão de Curso avaliado e aprovado em: 16/03/2015, pela seguinte Banca Examinadora:

Joêmia Leilane Gomes de Medeiros Martins

Prof.ª Dra. Joêmia Leilane Gomes de Medeiros Martins – Presidente

Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte

Rodrigo Siqueira

Prof. Dr. Rodrigo Siqueira Martins – Membro Interno

Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte

Ronaldo Maia

Prof. Msc. Ronaldo Maia de Medeiros – Membro Interno

Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte

Dedico este trabalho aos meus pais, que com seus esforços e sua ajuda, concederam-me a oportunidade de chegar até aqui. Sem esses eu não teria conseguido.

AGRADECIMENTOS

Primeiramente, agradeço a Deus, que é dono de toda sabedoria, por ter me permitido chegar até aqui.

Aos meus pais, Francisco e Suely, pela base familiar e educacional que me concederam.

À Luiza pela paciência e apoio constante durante a minha trajetória no curso.

Às minhas irmãs, Aline e Andresa, pelos momentos de distração, permitindo alívio mental para uma posterior retomada ao trabalho.

Aos meus avós, Antônio, Lúcia e José, que sempre demonstraram apoio e incentivo pela minha busca intelectual, além de sempre elogiarem a minha capacidade.

Aos meus demais familiares pelo reconhecimento e incentivo aos estudos.

Aos meus amigos que com suas provocações e com seu apoio me incentivaram a continuar e nunca desistir.

Aos meus orientadores, Rodrigo e Leilane, que me apoiaram e incentivaram a concluir o curso.

A todos os professores que tive a honra de poder ser aluno e me passaram o conhecimento que precisei.

Aos demais colegas que me apoiaram e me acompanharam mostrando que sempre se pode ir mais além.

A habilidade suprema não consiste em ganhar cem batalhas, mas sim em vencer o inimigo sem combater. Sun Tzu (2011, p.41).

A verdadeira lei da guerra consiste em conquistar tudo de modo intato, sem esgotar as forças. Sun Tzu (2011, p.42).

RESUMO

Graças aos grandes avanços tecnológicos, o dia a dia das pessoas ficou repleto de facilidades. A tecnologia está presente nas mais diversas áreas como na indústria, no comércio e na área acadêmica. A sua existência traz facilidade, melhorias e agilidade aos processos de trabalho. Mas nem tudo que a tecnologia oferece é benéfico, ela é uma ferramenta neutra que pode ser utilizada para o bem ou para o mal. Existem aqueles que a utilizam para se beneficiarem de forma ilícita, para se aproveitar e causar danos aos outros. Baseado no pensamento da sua utilização para todos e quaisquer fins, surge a preocupação dela ser usada como um objeto de ataque ou estar sendo transformada em uma arma. Diante disso, surge a necessidade, também, de tê-la como um objeto de defesa ou escudo. Por conseguinte, torna-se preocupante o uso das tecnologias como ferramentas bélicas, aparecendo, assim, o contexto de Guerra Cibernética. Este trabalho vem, sobretudo, contextualizar que a Guerra Cibernética é uma realidade, na qual as ferramentas tecnológicas podem funcionar como armas. O trabalho exemplifica o *Malware* (código malicioso) como uma destas ferramentas de ataque, mostrando o seu potencial catastrófico em uma guerra, uma vez que ele pode ser inserido em um sistema e começar a danificá-lo sem ser notado ou se percebido, o ser tardiamente; possuindo o poder de devastar e aterrorizar em segundos. Sendo assim, ele é um perigo que deve ser combatido.

Palavras-chave: tecnologia; guerra cibernética; malware.

ABSTRACT

Thanks to great technological advances, people's daily lives are full of ease. Technology is present in the most diverse areas such as industry, commerce and academic area. Its existence brings ease, improvements and agility to work processes. But not everything technology offers is beneficial; it is a neutral tool that can be used for better or for worse. There are those who use it to benefit themselves illegally, to take advantage of and harm others. Based on the thought of its use for any and all purposes, concerns arise that it is being used as an object of attack or being turned into a weapon. Therefore, the need also arises to have it as an object of defense or shield. Therefore, the use of technologies as war tools becomes worrisome, thus appearing the context of Cyber Warfare. This work comes, above all, to contextualize that Cyber War is a reality, in which technological tools can function as weapons. The work exemplifies Malware as one of these attack tools, showing its catastrophic potential in a war, since it can be inserted into a system and start to damage it without being noticed or if noticed, the being belatedly; possessing the power to devastate and terrify in seconds. As such, itis a danger that must be fought.

Keywords: technology; cyberwar; malware.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CGI.br	Comitê Gestor da Internet no Brasil
DOS	*Denial of Service*
DDOS	*Distributed Denial of Service*
DLL	*Dynamic-Link Library*
EUA	Estados Unidos da América
GCS	*Ground Control Station*
IPEA	Instituto de Pesquisa Econômica Aplicada
IFRN	Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
IDS	*Intrusion Detection System*
IP	*Internet Protocol*
CRYSYS	*Laboratory of Cryptography and System Security*
PLC	*Programmable Logic Controller*
SGSI	Sistema de Gestão de Segurança da Informação
SCADA	*Supervisory Control And Data Acquisition*
TIC	Tecnologia da Informação e Comunicação
TCC	Trabalho de Conclusão de Curso
USB	*Universal Serial Bus*
VANT	Veículos Aéreos Não Tripulados

SUMÁRIO

1 INTRODUÇÃO

No século XXI, tanto as pessoas como as empresas, organizações e o Estado estão dependentes da Tecnologia da Informação e Comunicação (TIC). Os sistemas de informação e comunicação se tornaram a base do desenvolvimento econômico, social e intelectual da humanidade. A tecnologia, com seu uso globalizado, traz consigo a otimização do processo de trabalho. O que antes era feito em dias, hoje pode ser feito em horas ou até mesmo em minutos. Com a automatização de processos, não é mais necessário a presença constante de uma pessoa durante a execução de uma determinada tarefa. Essa melhoria de produtividade que atraiu as empresas também atraiu o governo. As nações vêm utilizando as tecnologias para armazenar dados, operar, gerenciar e até mesmo controlar seus serviços. Os dados são de grande valor para as pessoas. Então, é notória a sua importância para uma nação.

Cada dado que é gerado, cada informação sobre estratégias militares, sobre combate ao crime, desenvolvimento econômico, pesquisas acadêmicas, entre outros está armazenado em computadores. Computadores que por sua vez trocam informações entre si, ou seja, essas informações trafegam todos os dias pelas redes internas (Intranets) e podem estar ligadas à grande *World Wide Web* (Internet). Portanto, ter segurança em TIC é fundamental.

Desde o começo da humanidade, as nações se opõem umas às outras pelos mais diversos motivos: políticos, religiosos, territoriais, étnicos; gerando assim, enormes conflitos e guerras. Graças ao rápido e crescente avanço tecnológico, esses conflitos vêm mudando de perspectiva. Hoje a guerra é multidimensional, não se concentra somente na terra, na água e no ar; ela tem novos campos de batalha. O combate se estende para o espaço, para o espectro eletromagnético e para o ciberespaço.

É nesse contexto que a guerra cibernética se enquadra, onde as Tecnologias de Informação e Comunicação são usadas como armas. De acordo com Mandarino e Canongia (2010), a segurança cibernética, desafio do século XXI, vem se destacando como função estratégica de Estado, sendo essencial à manutenção das infraestruturas críticas de um país, tais como energia, defesa, transporte, telecomunicações, finanças, da própria informação, dentre outras.

A guerra cibernética é uma realidade nos dias de hoje. A prova disso é o investimento em massa das nações em sistemas informatizados de ataque e defesa. Este trabalho apresentará exemplos de como o *Malware* pode ser utilizado como arma em ataques cibernéticos.

1.1 OBJETIVOS

O presente trabalho objetiva fazer um estudo sobre a importância da infraestrutura de tecnologia da informação e comunicação para uma nação e o uso de *Malwares* em uma guerra cibernética, separando o tema abordado em dois grupos:

a) o primeiro grupo visa introduzir a importância da segurança no ambiente de TIC, atentando sobre segurança cibernética de uma nação e os efeitos ocasionados caso haja falha;
b) no segundo, procura-se aprofundar o conhecimento sobre *Malwares*, exemplificando o seu potencial como arma em guerras cibernéticas e citando os problemas causados por seu uso, como também definindo até que ponto uma guerra cibernética pode ocasionar uma guerra física.

1.2 METODOLOGIA

Neste documento será utilizado um método de pesquisa bibliográfica sistematizada de conceitos que permite criar um estado da arte do tema proposto. Ela trará conceitos de segurança da informação, segurança cibernética, *Malware* e guerra cibernética que são estudados na literatura. Os conceitos serão analisados e contextualizados em um cenário de guerra cibernética mostrando os riscos desta realidade.

1.3 ESTRUTURA DO TRABALHO

No primeiro capítulo deste trabalho, intitulado Segurança da Informação, são definidos os conceitos básicos sobre segurança da informação e sua importância, assim, como conceitos fundamentais sobre segurança cibernética; mostrando a segurança da informação focada no âmbito de segurança nacional e a definição de defesa cibernética. No segundo capítulo, Ameaças Cibernéticas, define-se os conceitos sobre o tema e sobre ataques cibernéticos e exemplificam-se alguns tipos destes ataques. No terceiro capítulo *Malwares*, é definido o conceito de *Malware*, como também seus tipos, seu modo de infecção e propagação e suas aplicações. No quarto capítulo, Guerra Cibernética, define-se esse tipo de guerra e como ela acontece. No quinto capítulo, *Malwares* em Guerra Cibernética, será apresentado como os *Malwares* vêm sendo utilizados em guerras cibernéticas, porque essa disseminação e como essa guerra terá efeitos no mundo físico. Finalizando será exibida uma verificação de *Malware* e uma simulação de um ataque.

2 SEGURANÇA DA INFORMAÇÃO

Com o avanço tecnológico, o computador e os dispositivos semelhantes vêm se transformando em ferramentas fundamentais no cotidiano das pessoas. Cada informação que antes era anotada em incontáveis folhas de papel está sendo armazenada nos computadores. O que também é notório é que os dados agregam cada vez mais valor e com essa valorização, prezar pela segurança deles vem se tornando cada vez mais importante. A partir desta necessidade é que surge o conceito de segurança da informação.

De acordo com Tanenbaum (2003), em sua forma mais simples, a segurança se preocupa em garantir que pessoas mal-intencionadas não leiam ou, pior ainda, modifiquem secretamente mensagens enviadas a outros destinatários.

Os computadores estão conectados através de diversos dispositivos, formando assim uma rede, e estas podem ser interligadas com outras redes. Esta interligação permite a troca constante de dados e informações, formando a Internet.

Com a enorme quantidade de conexão, existe uma disseminação de informações importantes, muitas delas confidenciais e cruciais, trafegando pela rede global de computadores. Preservar a segurança em redes de computadores é outro ponto da segurança da informação, pois com o crescente valor agregado a cada informação, cresce o número de pessoas ou entidades interessadas em manipular e/ou se apropriar delas.

Segundo Carissimi, Rochol e Granville (2009), a área de segurança tornou-se um ponto fundamental em redes de computadores em nossa atualidade. Pelo amplo aspecto dos problemas de segurança, diz-se que eles são alvo de estudo e implementação do que genericamente se denomina segurança da informação.

Uma conexão com a internet é uma via de mão dupla, ou seja, se um computador A pode acessar dados fora de sua rede, um computador B, de uma rede externa, pode obter acesso à rede do computador A e ter acesso aos dados do computador A. Partindo dessa exemplificação, percebe-se o quanto é vital que se priorize a segurança da informação e o quanto se tem que torná-la eficaz.

A segurança em Tecnologia da Informação e Comunicação tem o objetivo de inibir o acesso a informações e fornecer acesso seguro a quem tem o devido direito. Para isso a segurança em TIC preza por conceitos/pilares básicos, tais como: a confidencialidade, a integridade, a disponibilidade, a autenticidade e o não repúdio ou irretratabilidade. A Figura 1 ilustra a ideia dos pilares da segurança da informação.

Figura 1 – Pilares da Segurança da Informação

Fonte: Elaboração própria em 2015.

a) Disponibilidade

A disponibilidade está ligada ao contexto de que quando um serviço for posto em funcionamento ele esteja disponível a quem é de direito, no momento ao qual se for necessário/solicitado, além de estar no estado adequado para a sua utilização.

b) Integridade

Na integridade, garante-se que a informação não sofreu modificação/alteração, ou seja, mantém-se em seu estado original desde o momento em que foi salva. Ela garante que o dado não foi comprometido.

c) Confidencialidade

A confidencialidade é a propriedade que assegura o acesso da informação somente a pessoas ou órgãos estritamente autorizados.

d) Autenticidade

A autenticidade faz valer os itens anteriores, fazendo com que para o acesso seja necessária autenticação, garantia de que o conteúdo confidencial é permitido a determinado usuário/grupo.

e) Não repúdio ou Irretratabilidade

O não repúdio ou irretratabilidade, é a garantia de que uma pessoa ou órgão assuma a responsabilidade pelo envio ou assinatura de uma determinada informação, não podendo negar sua autoria.

> A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos (ISO/IEC 27002, 2005).

Para um bom funcionamento da segurança da informação, a organização deve trabalhar juntamente com seus funcionários, além de um investimento e atualização contínuos. Podem-se destacar entre as várias técnicas que mantém um SGSI as políticas de segurança da informação, as quais são um conjunto de regras e definições com base na política, nas normas da instituição e nas leis vigentes para assegurar as boas práticas da segurança da informação; e nas ferramentas de controle de acesso, podendo ser físicas (restrição de acesso ao ambiente computacional como portas, segurança, cartão de acesso, entre outros) e lógicas/virtual (uso de usuário e senha, *firewall*, IDS, antivírus, criptografia, entre outros).

> A informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Definir, alcançar, manter e melhorar a segurança da informação podem ser atividades essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado (ISO/IEC 27002, 2005).

2.1 SEGURANÇA CIBERNÉTICA

A segurança cibernética é a proteção e a garantia de se poder utilizar os ativos computacionais que se encontram disponíveis. Ela tem o objetivo de eliminar ou reduzir as vulnerabilidades do espaço cibernético.

> Segurança Cibernética é o conjunto de ferramentas, políticas, conceitos, medidas, orientações, abordagens de gerenciamento de riscos, ações, treinamento, boas práticas, garantias e tecnologias que podem ser usadas para proteger o ambiente cibernético e os ativos das organizações e dos utilizadores (ITU X.1205, 2008, tradução nossa).[1]

[1]Texto original: Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets

A ideia principal sobre a segurança cibernética é a de garantir que as redes de comunicação estejam disponíveis para serem utilizadas, os ativos mantenedores da infraestrutura crítica estejam sempre operantes e caso ocorra uma falha na disponibilidade, ela seja trazida a normalidade quase instantaneamente.

Segundo Mandarino e Canongia (2009), a segurança cibernética é entendida como a arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no espaço cibernético, seus ativos de informação e suas infraestruturas críticas. É, portanto, maior que segurança em TI, pois envolve pessoas e processos.

Tendo em vista a importância da segurança em TI para uma empresa, nada é mais lógico do que se imaginar a segurança cibernética vital para uma nação. É na segurança cibernética que o país protege sua infraestrutura, garantido a soberania nacional.

Ainda de acordo com Mandarino e Canongia (2010), a segurança cibernética, portanto, vem se caracterizando cada vez mais como uma função estratégica do Estado, e essencial à manutenção e preservação das infraestruturas críticas de um país, tais como energia, transporte, telecomunicações, águas, finanças, informação, dentre outras.

2.1.1 Defesa cibernética

Defesa cibernética é compreendida como a parte da segurança cibernética que é voltada para a proteção ofensiva do espaço cibernético de uma nação.

De acordo com Mandarino (2011), entende-se, portanto, que segurança cibernética incorpora as ações de prevenção (incidentes) e repressão, enquanto a defesa cibernética abrange ações ofensivas e defensivas.

A nação deve utilizar de estratégias, medidas, equipamento e planos para que, assim que se torne necessária, a defesa cibernética entre em ação, garantindo assim a preservação da integridade das estruturas do país. A defesa cibernética pode ser mais bem interpretada como a reação a qualquer ameaça oriunda do espaço cibernético que se caracterize como agressão ou ameaça. Também cabe ao escopo da defesa cibernética a coleta de informação para inteligência militar, uma vez que ela é capaz de prever ataques e causar danos aos inimigos.

3 AMEAÇAS CIBERNÉTICAS

Em ambientes computacionais existem diversas ameaças com as mais distintas finalidades. Elas são a ocorrência de algo que tem o potencial de infringir/violar os pilares da

segurança da informação. Ameaça é definida pela ISO/IEC 13335-1 (COMITÊ GESTOR DA INTERNET NO BRASIL, 2004) como causa potencial de um incidente indesejado, a qual pode resultar em dano para um sistema ou organização.

> As organizações, seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Danos causados por código malicioso, *Hackers* e ataques de *Denial of service* estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados (ISO/IEC 27002, 2005).

Segundo Hagel (2013), às ameaças cibernéticas representam um perigo "discreto, furtivo e traiçoeiro" para os EUA e outros países, ele defendeu a criação de "regras de trânsito" para orientar os comportamentos e evitar conflitos nas redes digitais globais.

As ameaças cibernéticas apresentam perigos e riscos de quantidades imensuráveis que podem ser divididos em quatro níveis:

1) Crime de baixo-nível/individual (*Hacking*): composta por indivíduos que detêm determinado conhecimento sobre tecnologia, mas depende de ferramentas pré-compiladas de terceiros. Utilizam-se de scripts para realizar suas tarefas. Não tendo algum objetivo concreto. A invasão é somente o que necessitam.
2) Criminalidade grave e organizada: um fator que infelizmente segue em evolução é a criminalidade. Na área tecnológica não é diferente. Caracteriza-se aqui como a “modernização do crime organizado”, é a migração ou apoio tático do crime tradicional. Encontra-se aqui lavagem de dinheiro, roubo, estelionato, entre outros.
3) Extremismo político e ideológico: esses grupos usam os recursos da internet para comunicação, treinamento, geração de fundos, recrutamento, planejamento de ataques, entre outros. Usam recursos como criptografias e esteganografia para permaneceram no anonimato.
4) Patrocinados pelo Estado: nela o Estado utiliza a recursos computacionais para espionar, roubar informações e até mesmo atacar alvos que sejam considerados ofensivos à segurança nacional ou aos interesses econômicos da nação.

De acordo com Mandarino Junior e Canongia (2010), às emergentes ameaças cibernéticas mostram o quanto é preciso incrementar tanto a segurança da informação quanto a cooperação internacional no sentido de evitar ou reduzir efeitos negativos de operações cibernéticas antagônicas. O tema ameaça cibernética deve ser resolvido em escala mundial,

envolvendo o maior número de partes, de leis e de agências de todas as nações. Convenções têm de ser reescritas uma vez que a guerra cibernética confunde princípios como os da proporcionalidade, neutralidade e distinção. As regras cibernéticas necessitam ser melhor discutidas.

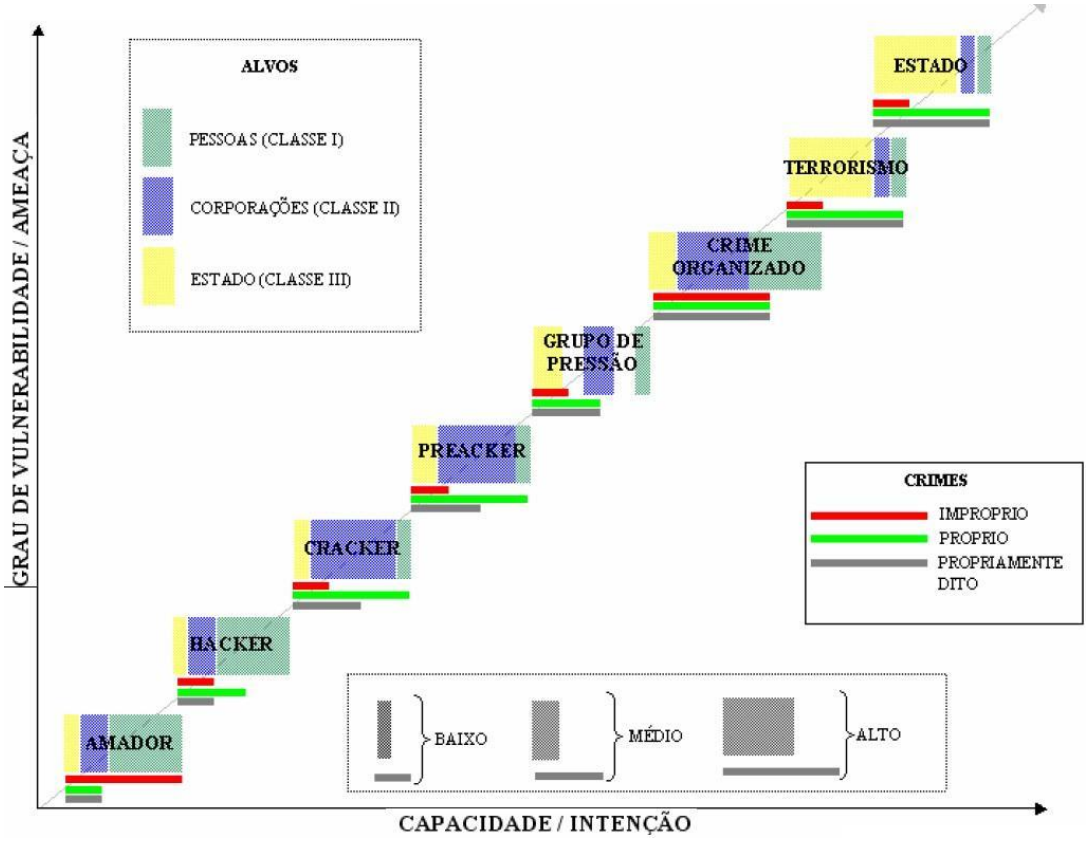
3.1 ATAQUES CIBERNÉTICOS

Ataque cibernético é a execução de uma ação ofensiva, por meio de recursos de TIC, com a finalidade de capturar, interromper, penetrar, adulterar, degradar e/ou destruir sistemas e/ou redes de computadores. É a ameaça em execução.

Ataques costumam ocorrer na internet com diversos objetivos, visando diferentes alvos e usando variadas técnicas. Qualquer serviço, computador ou rede que seja acessível via internet pode ser alvo de um ataque, assim como qualquer computador com acesso à internet pode participar de um ataque (COMITÊ GESTOR DA INTERNET NO BRASIL, 2012).

Os ataques, dependendo do seu nível, podem ter investimento e impactos maiores ou menores, além de terem as mais variadas intenções. A Figura 2 mostra uma relação de ameaça e intenção. Na vertical vê-se que quanto mais baixo se encontra o atacante, significa que ele possui menos conhecimento sobre vulnerabilidades, possui menos recursos e representa menor ameaça para o seu alvo; enquanto que na linha horizontal mostra que quanto mais longe do centro do gráfico, maior deve ser o investimento em recurso, conhecimento e tecnologia e maior será o tempo gasto com pesquisa para o alvo ser atingido com sucesso. Assim, quanto mais alto na figura e mais à direita, maior ameaça o atacante apresenta; e quanto maior o nível se encontra o atacante, mais dano ele pode causar.

Figura 2 – Relação investimento capacidade de ataque cibernético



Fonte: Mandarino Junior (2009).

Na Figura 2, também é demonstrado, através de linhas coloridas abaixo de cada tipo de atacante, uma tipificação criminal baseada na utilização de tecnologia pelos atacantes. A cor vermelha ilustra os crimes impróprios, crimes esses que não necessariamente precisam de um meio cibernético para existir, no qual a tecnologia é uma variação do crime, por exemplo, a pornografia infantil. Na cor verde encontram-se os crimes próprios, crimes que são realizados somente por meio virtual, como o acesso indevido a uma base de dados. Representado pela cor cinza estão os crimes em que o objetivo é o próprio computador ou o ambiente computacional, intitulados crimes propriamente ditos, exemplo deste é o terrorismo cibernético.

Esta mesma figura traz três classes de alvos: Classe I – Pessoas, Classe II – Corporações e Classe III – Estado. À medida que o atacante cresce em capacidade, o alvo sofre variação. A Classe I está mais vulnerável ao ataque dos atacantes com menor capacidade e recursos, mas também está incluída na lista de interesse do crime organizado. A Classe II está mais vulnerável a atacantes com capacidade um pouco maior e com um pouco mais de recursos, o que inclui também o crime organizado. Para atacar a Classe III é necessário a maior capacidade do gráfico e os maiores recursos.

Para realizar ataque, o atacante utiliza diversas técnicas e ferramentas buscando por vulnerabilidades, que nada mais são do que falhas no hardware e/ou software dos dispositivos. O atacante pode entrar na rede do seu alvo e assim obter a informação que deseja ou pode "derrubar" a rede, tornando o serviço indisponível. Entre as técnicas podem ser citadas a Engenharia Social (técnica que o atacante usa para persuadir o alvo), na qual uma pessoa é levada a dar informações que o atacante pode usar para invadir o sistema; o *Exploit* (programa que faz varredura à procura de vulnerabilidades), na qual o atacante descobre onde estão as falhas de segurança e assim escolhe os melhores métodos para se infiltrar; *Distributed Denial of Service* (DDoS) e o *Denial of Service* (DoS) – são ataques de negação de serviço – com eles pode-se parar a disponibilidade de um determinado serviço – o que muda entre os dois é basicamente a dimensão do ataque; *Sniffers* (programa de captura de tráfego), no qual pode-se analisar e capturar o tráfego de rede e, a partir dos dados capturados, ter acesso a rede; *Scan* (varredura de rede), na qual verifica-se na rede quais dispositivos possuem serviços e portas abertas; e os *Malwares* (programas que rodam em *Background* causando ações danosas no sistema), nesta técnica existem vários tipos e formas de se realizar o ataque, geralmente, por um descuido do usuário do sistema, esses softwares são instalados e começam a agir.

No setor privado, as empresas, bancos, bolsas de valores e indústrias mantêm a relação com seus clientes e fornecedores dependentes das TICs. Elas realizam as transações bancárias, onde circulam milhares, milhões e até bilhões, através dos sistemas computadorizados. Quando uma empresa sofre um ataque, tende a mostrar fragilidade, recebe a desconfiança dos clientes e negócios de milhões podem ser desfeitos.

No setor público, o governo, a cada dia mais, gere os serviços de atenção básica a população com a tecnologia. Além dos sistemas de defesa da nação estarem conectados por redes de dados sigilosos. Um ataque cibernético causa um negativismo sobre a soberania do Estado e compromete a segurança da população.

Para Júnior César Da Cruz (2013), na medida em que o bem-estar e a segurança da sociedade passam a depender da segurança cibernética, ela se torna um dever do Estado e não apenas mais uma questão de maior ou menor prioridade de um governo.

4 MALWARES

Os *Malwares* (abreviação de *Malicious software)* ou códigos maliciosos, são softwares que em seus códigos contém instruções que após executadas causam ações danosas em

equipamentos computacionais. Diz-se que quando foi consolidado o primeiro sistema computacional, também se passou a criar o código malicioso.

De acordo com o Comitê Gestor da Internet do Brasil (2012), após infectar o seu computador, o código malicioso pode executar ações como se fosse você, como acessar informações, apagar arquivos, conectar-se à internet, enviar mensagens e ainda instalar outros códigos maliciosos.

São encontrados diversos tipos de *Malwares* com diferentes finalidades e formas de propagação. Eles possuem as mais variadas formas de serem obtidos: via correio eletrônico, redes sociais, dispositivos infectados; como também se alocam em dispositivos os deixando vulneráveis ao atacante podendo se propagar por toda a rede.

Na Figura 3, mostra-se uma comparação entre os tipos *Malwares*. Tomando o vírus como exemplo, pode-se concluir que esse tipo de código malicioso pode infectar o sistema vindo de seis fontes diferentes, ele é instalado a partir da execução de um arquivo infectado, faz cópias de si para se propagar e como ações ele altera e/ou remove arquivos e procura se manter escondido, ou seja, ele procura maneiras de não ser detectado pelo usuário, sistema operacional e pelos programas.

Figura 3– Comparação de Malware

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	✓				✓	✓	✓

Fonte: Comitê Gestor da Internet no Brasil (2015).

A seguir são apresentados os *Malwares* mais comuns e suas definições de acordo com a Cartilha de Segurança para Internet do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br):

a) vírus: é um programa ou parte de um programa de computador, normalmente, malicioso, o qual se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. Para que possa se tornar ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para o seu computador ser infectado é preciso que um programa já infectado seja executado.
b) *worm*: é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. *Worms* são notadamente responsáveis por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costumam propagar e, como consequência, podem afetar o desempenho de redes e a utilização de computadores.
c) *bot*: é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do *Worm*, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.
d) *spyware*: é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas.
e) *keylogger:* capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de *Internet banking*.
f) *screenlogger:* similar ao *Keylogger*, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado ou a região que circunda a posição onde ocorre o clique. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em sites de *Internet banking*.
g) *adware*: projetado especificamente para apresentar propagandas. Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito.

h) *backdoor*: é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.
i) cavalo de tróia, *trojan* ou *trojan-horse*: é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente, maliciosas e sem o conhecimento do usuário.

Dentre os tipos de *Malwares* citados o vírus se tornou o mais conhecido e faz-se o uso de seu nome para generalizar os códigos maliciosos. Isso se deve ao fato dele ter seu nome baseado em seu correspondente biológico que afeta os seres humanos desde o início do surgimento da humanidade.

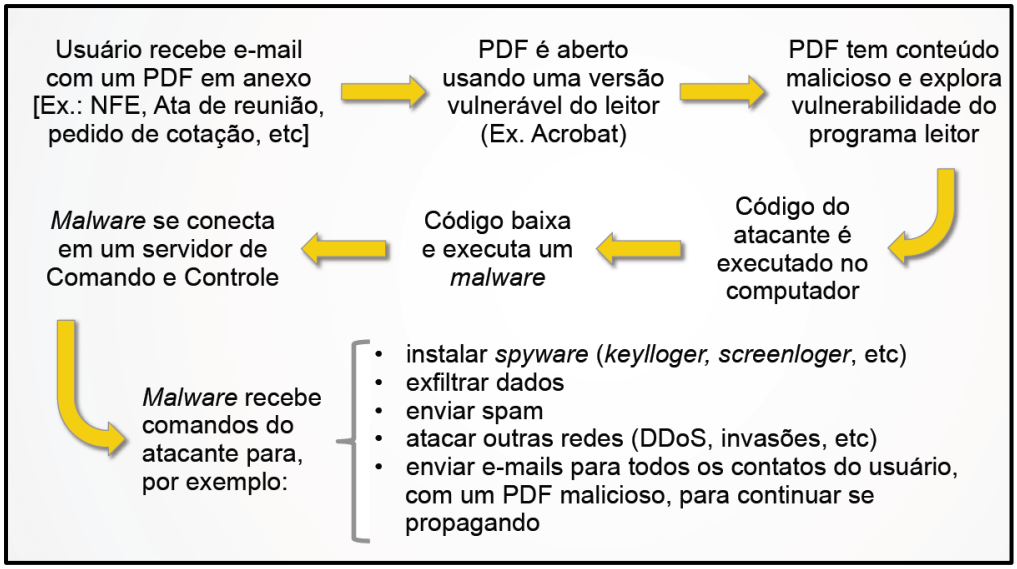
Segundo Yuri Diogenes (2013), o primeiro vírus criado era chamado de *Creeper*, sendo a forma experimental de criar um programa que se auto multiplicava. Este vírus foi criado por Bob Thomas em 1971 e este infectou computadores '*Digital Equipment Corporation'* (DEC) PDP-10 executando sistemas operacional TENEX. Estes computadores eram interligados via ARPANET, conhecida como predecessora da atual internet, e ao ser executada nos computadores exibia a seguinte mensagem "Eu sou '*Creeper'*, pegue-me se puder!". Um outro programa chamado *Reaper* foi criado para remover o "*Creeper*"; seguindo a mesma linha de pensamento podemos assim dizer que o *Reaper* foi o primeiro antivírus.

Após o código malicioso estar instalado e em execução, o atacante terá acesso ao sistema alheio e poderá moldá-lo a maneira que desejar até que a vulnerabilidade seja descoberta e solucionada, o que em inúmeras vezes é tardio.

O *Malware* é distribuído pelo atacante na internet, ficando à espera de infectar um computador. Para realizar a infecção, o atacante desfruta de inúmeras técnicas, como foi visto na Tabela 1, entre elas o spam.

O spam caracteriza-se pelo envio em massa de e-mails para incontáveis destinatários, após receber um e-mail, o usuário executa alguma operação, por exemplo, o download e o computador é infectado. A Figura 4 relata um exemplo de propagação de código malicioso.

Figura 4 – Distribuição de Malware



Fonte: Hoepers e Steding-Jessen (2015).

Outra forma em que o *Malware* é distribuído é através de sites não confiáveis. Uma determinada pessoa, a qual não detém um bom conhecimento de informática, acessa um site desconhecido e inseguro para baixar um software ao qual ela precisa. Ao realizar o download, juntamente com o programa desejado ou até ao invés dele, o código malicioso é instalado. Muitas vezes não é necessário estar buscando um programa, o site informa que para continuar acessando-o é necessário fazer o download e instalação de um software e este contém o *Malware.*

De acordo com Emerson Wendt (2011), uma ação no ciberespaço, em grande escala e bem planejada, pode fazer com que cavalos de tróia, vírus, *Worms* etc. possam ser espalhados pela rede através de páginas web, de e-mails (*Phishing scam*), de comunicadores instantâneos (*Windows Live Messenger*, *Pidgin*, *GTalk* etc.) e de redes sociais (*Orkut*, *Twitter*, *Facebook* etc.), entre outras formas possíveis.

Os *Malwares* têm um enorme potencial para serem usados como armas cibernéticas, sejam por quadrilhas de crime organizadas, por “curiosos” ou por nações.

De acordo com Clarke (2015), os países já estão se infiltrando nas redes uns dos outros e instalando *Backdoors* para terem acesso rápido a essas redes quando precisarem. É a partir deste ponto de vista que se pode falar sobre guerra cibernética.

5 GUERRA CIBERNÉTICA

O surgimento da Internet e sua evolução desde a ARPANET, vide detalhamento na Figura 5, tem seus laços no militarismo, uma vez que ela foi desenvolvida com o objetivo de interligar os computadores do governo americano pela Agência de Projetos de Pesquisas Avançadas do Departamento de Defesa dos EUA (*Department of Defense Advanced Research Projects Agency* (DARPA)).

Segundo Tanenbaum (2011), as primeiras redes de computadores tiveram início no final da década de 1950. No auge da Guerra Fria, o Departamento de Defesa dos Estados Unidos queria uma rede de controle e comando capaz de sobreviver a uma guerra nuclear. Nessa época, todas as comunicações militares passavam pela rede pública de telefonia, considerada vulnerável.

Figura 5 – Cronologia da Internet

Ano	Evento
1969	ARPANET autorizada pelo DOD
1970	ARPANET adota o *Network Control Protocol* (NCP)
1971	23 hosts na ARPANET
1972	Especificação do *Telnet*
1973	Especificação do *File Transfer Protocol* (FTP)
1974	Especificação do *Transmission Control Protocol* (TCP)
1975	Primeiro *mailing list* da ARPANET (MsgGroup)
1978	TCP subdividido em TCP e IP
1981	Publicação do Standard *Internet Protocol* (IP)
1982	TCP e IP definidos como *suite* pela ARPA e DCA
1983	Substituição do NCT pelo TCP/IP (flag day)
1984	Surgimento do DNS1986: Criação da NFSNet
1986	Criação da IETF e da IRTF pela IAB
1987	10.000 hosts na NFSNet
1989	100.000 hosts na NFSNet
1990	ARPANET deixa de existir
	Brasil se conecta à NFSNet
1992	Criação da ISOC
1993	Criação do InterNIC
1994	Início do uso comercial da Internet no Brasil
1996	Guerra dos browsers: Microsoft x Netscape
1999	60.000.000 de hosts na Internet

Fonte: Palma e Prates (2000).

Para Theiler (2011), nos últimos vinte anos, a informática desenvolveu-se muito, de ferramenta administrativa cujo objetivo era otimizar os processos administrativos, tornou-se um instrumento estratégico para a indústria, a administração e as forças armadas.

A cada dia que se passa a humanidade vem procurando desenvolver projetos com maior velocidade, com maior eficiência e precisão. Esta busca por melhores resultados gera uma competividade. Isso não é diferente entre as nações. Desenvolver uma melhor tecnologia de infraestrutura, defesa e ataque vem sendo um dos objetivos dos países na atualidade.

Como relata Araújo (2011), a guerra cibernética nada mais é que a evolução do modo de batalha que a humanidade vem aprimorando com o decorrer do tempo. Esta nova batalha se destaca pelo aparato tecnológico, na qual o objetivo principal da nação envolvida é dominar, controlar ou destruir a força do inimigo, por meio da invasão de seus sistemas de controle informatizados.

Iniciou-se uma "nova corrida espacial", onde desta vez o objetivo não é mais criar uma tecnologia que permita à humanidade viajar ao espaço, trata-se do desenvolvimento de um equipamento bélico que possa atuar sozinho ou aliado aos armamentos tradicionais, destacando-se pelo menor esforço físico possível.

Vale a pena salientar que na era da informação existe uma situação semelhante à Guerra Fria. Onde antes se demonstrava a grandeza, autonomia e soberania militar de um país através do desenvolvimento de caças mais velozes, tanques mais sofisticados, mísseis mais destrutivos, entre outros; hoje, desenvolver métodos informatizados de controlar e/ou extrair informações dos equipamentos do inimigo torna visível o poder de uma nação. A guerra, que antes só poderia se encontrar na terra, no ar, na água e/ou no espaço; hoje, tem o quinto domínio: o ciberespaço. É no ciberespaço que a guerra cibernética vai ser travada.

Segundo Carvalho (2011), em tempos mais recentes, com o advento da Era da Informação e sua sucedânea, a Era do Conhecimento, a informação foi alçada à categoria de ativo estratégico para organizações e Estados-Nação, conferindo àqueles que a detém e dela se utilizam, efetiva e oportunamente, uma inquestionável vantagem no ambiente competitivo e nos contenciosos internacionais.

A guerra cibernética tornou os combates entre os países menos sangrentos, embora não torne extinto o derramamento de sangue, mas o simples fato de uma ameaça poder ser feita a quilômetros de distância, sem a necessidade de sacrificar um soldado em campo de batalha, já é uma grande mudança. A tecnologia se tornou uma arma que ao se pressionar um botão pode se iniciar uma guerra. Conforme vemos em BRASIL (2012, p.53): "só existe soberania de fato

com defesa forte, isto é, com Forças Armadas adequadamente equipadas e adestradas, em condições de atuar de forma conjunta em quaisquer cenários, especialmente ante os cenários de ameaças cada vez mais difusas".

O uso do espaço cibernético para ataques às nações vem se tornando a cada dia uma realidade, cada vez mais a tecnologia vem sendo usada como arma, casos vêm aparecendo na mídia com mais frequência. Abaixo vermos alguns casos que tiveram grande repercussão na mídia, os quais foram tratados por João Roberto de Oliveira no livro Desafios Estratégicos Para Segurança e Defesa Cibernética (2011, p.114):

> a) De 2003 a 2006: nesse período, diversas instalações estratégicas dos Estados Unidos da América (EUA), como laboratórios de pesquisa voltados a inovações tecnológicas, foram alvos de tentativas de penetração em seus sistemas informatizados, provavelmente com o intuito de apropriar-se de conhecimento sensível.
>
> b) Abril/maio de 2007: ocorrências de ataques massivos a redes estratégicas da Estônia, causando degeneração no seu funcionamento. Esse episódio ocasionou a instalação de um Centro de Defesa Cibernética, pela Organização do Tratado do Atlântico Norte (Otan), no território estoniano.
>
> c) Setembro de 2007: suposta ação de "apropriação" do controle do sistema de defesa aérea da Síria, antecedendo ao bombardeio aéreo israelense contra instalações em construção naquele país, que seriam destinadas a apoiar o processo de produção de armas nucleares (CLARKE, 2010, p. 1-9).
>
> d) Agosto de 2008: ocorrências de ataques massivos a redes estratégicas da Geórgia, inclusive de Defesa, antecedendo a ação de tropas russas no território da Ossétia do Sul.
>
> e) Julho de 2009: ataques a sítios eletrônicos importantes dos EUA e da Coreia do Sul e suposta tentativa de penetração no sistema de controle de fornecimento de energia elétrica norte-americano.
>
> f) Setembro/outubro de 2010: ataques aos sistemas de controle de infraestruturas nucleares do Irã e a sistemas estratégicos de outros países, utilizando o sofisticado software (*Worm*) denominado *Stuxnet.*

De acordo com Braquinho (2012), os ataques cibernéticos estão cada vez mais poderosos e perigosos. É só imaginarmos que a água que bebemos, a eletricidade que chega às nossas casas, a sinalização dos transportes de massa (inclusive aéreos), o controle de usinas hidroelétricas e nucleares são controlados por sistemas de computação que podem ser potenciais alvos de *Hackers* do mundo inteiro.

O crescente aumento das ameaças cibernéticas vem ocasionando iniciativas de desenvolvimento de sistemas de proteção a ataques cibernéticos, a defesa cibernética. A preocupação com a defesa cibernética é um fator que vem fazendo países como os Estados Unidos, a Correia do Sul, a China, a Rússia, a Inglaterra, a Índia e o Brasil criarem leis e centros especializados em defesa cibernética. As ações militares estão cada vez mais dependentes do aparato tecnológico, diante isso, buscar medidas para neutralizar o desenvolvimento do inimigo tornou-se uma grande preocupação.

Segundo Bernardo Wahl (2012), assim como um submarino nuclear ou um avião de combate invisível podem atacar e desaparecer sem deixar rastros, da mesma forma, pode agir um agressor cibernético.

Por esse motivo as armas cibernéticas estão entrando em cena, elas podem causar uma catástrofe equivalente às armas convencionais sem ter a necessidade de locomover toda uma tropa de soldados, com os mais variados tipos de armamentos, com os mais variados tipos de veículos e sem todo o custo e tempo inerentes a isso.

De acordo com Bernardo Wahl (2012), a principal diferença é que apenas os países mais desenvolvidos têm condições de produzir um submarino nuclear e/ou um avião de combate invisível, enquanto as armas cibernéticas, cada vez mais poderosas e invisíveis, estão ao alcance de atores não-estatais.

Na guerra cibernética deixa-se claro o pensamento dos Estados-Nação no século XXI, o qual é explorar ao máximo a imensidão do espaço cibernético abandonando, na medida do possível, a ideia do “super soldado”, ou seja, começa-se a investir na capacidade mental do indivíduo e não mais em sua força física.

De acordo com Clarke (2015), não precisamos de soldados atléticos que consigam correr 8 km carregando uma mochila, precisamos de pessoas que consigam derrubar uma rede elétrica.

Vale salientar que ainda há nações que, seja por motivos religiosos, tradição ou falta de recursos, não têm uma infraestrutura tecnológica, elas ainda detêm, na grande maioria, de seus recursos baseados na manufatura, sendo assim, uma guerra cibernética é ineficaz contra esses inimigos.

Segundo Steed (2011), se o "poder" é a capacidade de A fazer com que B faça algo que B não faria de outra maneira, o poder cibernético é apenas o poder na medida em que a outra pessoa está em rede. O que isto significa é que o poder cibernético para coagir um inimigo para cumprir sua vontade é diretamente proporcional à forma como ele se encontra em rede, quanto mais ele estiver em rede, maior a relevância estratégica e capacidade de pressionar o inimigo

com o poder cibernético. Se ele não está em rede, o poder cibernético não é uma ferramenta significativa de estratégia no caso deste inimigo.

6 *MALWARES* EM GUERRA CIBERNÉTICA

Os *Malwares* vêm tendo participação significativa na guerra cibernética, justamente pelo fato de conseguir se infiltrar sorrateiramente nos dispositivos, tornando sua identificação tardia ou até mesmo imperceptível. Casos como o *Stuxnet*, o *Duqu* e o *Flame* vêm surgindo na mídia neste século.

Foi graças aos *Malwares* citados anteriormente, principalmente, ao *Stuxnet*, que se começou a acreditar em um ataque cibernético de alta escala e deixou-se de ignorar casos como o do Irã, no qual aproximadamente 30 mil sistemas foram atacados pelo *Stuxnet*, demonstrando assim o potencial das armas cibernéticas. Logo após este ataque, a Suíça criou um grupo para responder a possíveis ataques que o país possa sofrer, usando recursos computacionais.

6.1 STUXNET

O exemplo mais falado foi o do *Stuxnet* em 2010, o qual demonstrou o risco potencial de um *Malware* afetar os sistemas informáticos críticos de uma nação, mas acredita-se que ele tenha sido desenvolvido e posto em execução bem antes. O quadro abaixo mostra a linha do tempo de algumas detecções do *Malware*.

Quadro de linha do tempo *Stuxnet*

(continua)

Data	Evento
20/11/2008	Trojan.Zlob variante encontrada utiliza a vulnerabilidade LNK só mais tarde identificado no *Stuxnet*.
04/2009	Revista Segurança Hakin9 libera detalhes de uma vulnerabilidade de execução remota de código no serviço *Spooler* de impressora. Mais tarde identificado como MS10-061.
06/2009	Primeira amostra *Stuxnet* vista. Não explora MS10-046. Não tem arquivos de *Driver* assinados.

Quadro de linha do tempo *Stuxnet*

(continua)

Data	Evento
02/01/2010	*Driver* do *Stuxnet* assinado com um certificado válido que pertence ao *Realtek Semiconductor Corps*.
03/2010	Primeira variante *Stuxnet* para explorar MS10-046.
17/06/2010	VirusBlokAda relata W32.Stuxnet (RootkitTmphider nomeado). Relatos de que ele está usando uma vulnerabilidade no processamento de atalhos/arquivos .lnk, a fim de propagar (mais tarde identificado como MS10-046).
13/07/2010	*Symantec* acrescenta detecção como W32.Temphid (previamente detectado como cavalo de troia).
16/07/2010	*Microsoft Security Advisory* emite para "Vulnerabilidade no *Windows Shell* pode permitir a execução remota de código (2286198)" que cobre a vulnerabilidade no processamento de atalhos/arquivos .lnk. *Verisign* revoga certificado *Realtek Semiconductor Corps*.
17/07/2010	*ESET* identifica um novo *Driver Stuxnet,* desta vez assinado com um certificado da *JMicron Technology Corp*.
19/07/2010	Relatório *Siemens* que estão investigando relatos de *Malware* que infectam os sistemas SCADA Siemens WinCC. *Symantec* renomeia detecção de W32.Stuxnet.
20/07/2010	*Symantec* monitora o tráfego *Stuxnet* com Servidor de Comando e Controle.
22/07/2010	*Verisign* revoga o certificado *JMicron Tecnologia Corps*.
02/08/2010	*Microsoft* emite MS10-046, que corrige a vulnerabilidade de atalho do *Windows Shell*.
06/08/2010	*Symantec* relata como *Stuxnet* pode injetar e esconder código em um PLC afetando os sistemas de controle industrial.

Quadro de linha do tempo *Stuxnet*

(conclusão)

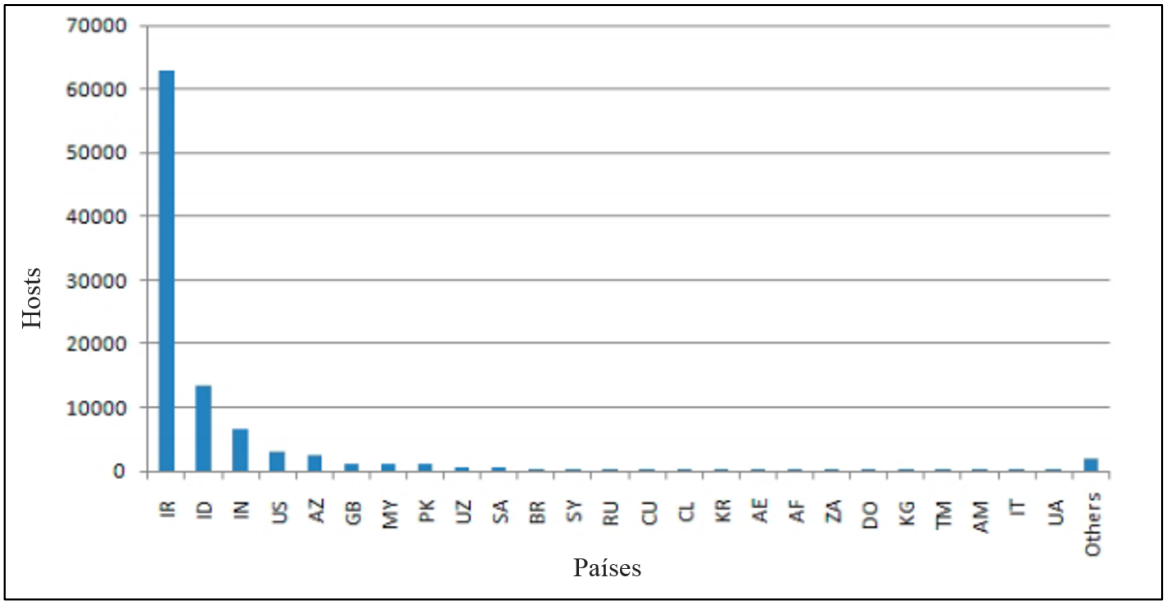
14/09/2010	*Microsoft* libera MS10-061 para corrigir a vulnerabilidade de *Spooler* de impressão identificado pela *Symantec* em agosto. *Microsoft* relata duas outras vulnerabilidades de elevação de privilégios identificados pela *Symantec* em agosto.
30/09/2010	*Symantec* apresenta pelo *Virus Bulletin* e libera análise abrangente do *Stuxnet.*

Fonte: Adaptado de Falliere, Murchu e Chien (2011).

O *Stuxnet* é um *Malware* projetado para atacar sistemas de controle industrial, mais especificamente o software SCADA, da empresa *Siemens*. Mas de acordo com Matrosov *et al*. (2010), no entanto, ele também tem como alvo Controladores Lógicos Programáveis (PLCs). em redes que utilizam sistemas SIMATIC WinCC Siemens ou STEP 7 SCADA (*Supervisory Control* e Aquisição de Dados).

O SCADA é um software responsável por supervisionar equipamentos em ambientes industriais. Acredita-se que o alvo do *Stuxnet* eram as usinas nucleares Iranianas, pois foi o país que mais foi afetado pelo *Malware*, como pode ser visto na Figura 6, a qual mostra o número de *Hosts* infectados por país. Em 2010, o *Stuxnet* foi responsável por inutilizar 1000 centrífugas na Usina Nuclear de Natanz, no Irã.

Figura 6 – Infecção do Stuxnet

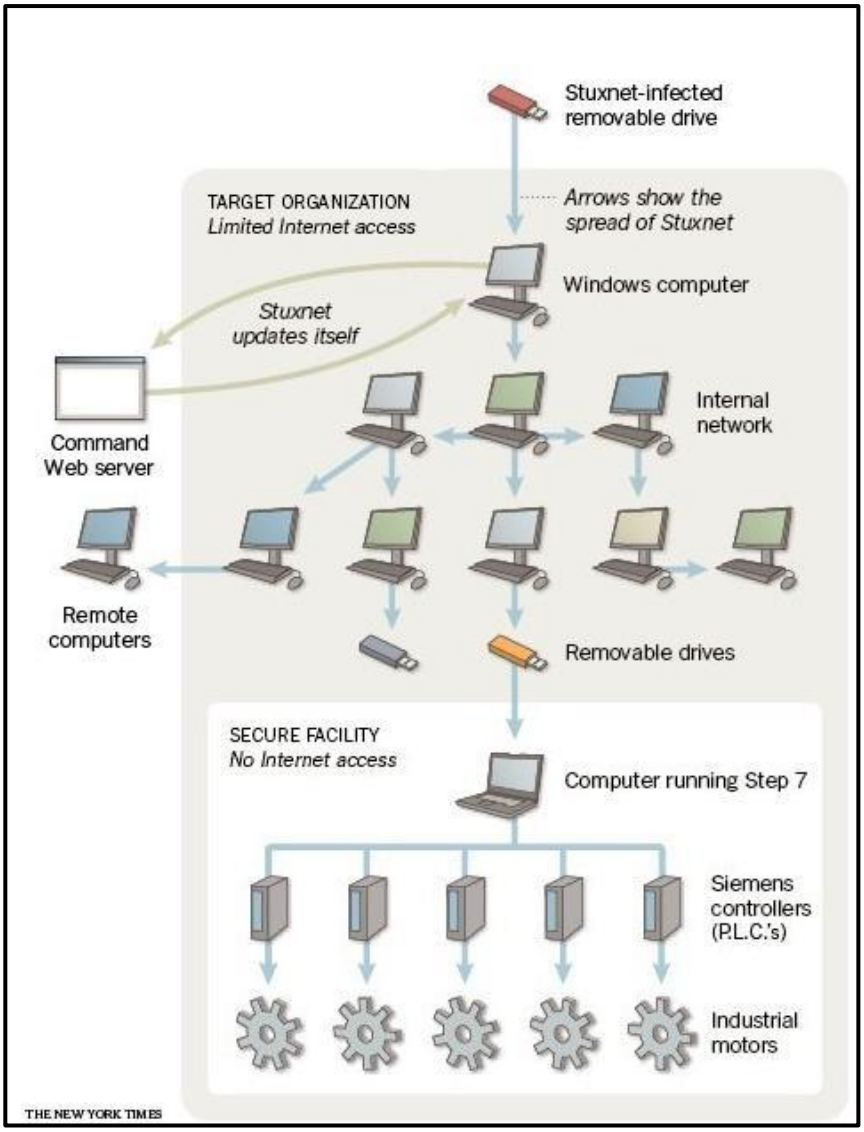


Fonte: Falliere, Murchu e Chien (2011).

Ele explora quatro vulnerabilidades "*Zero-day*" (falha de segurança que o fabricante não tem conhecimento, não está documentada e não há correção), em sistemas *Microsoft*, para entrar e infectar o sistema. Para não ser identificado ele usa dois certificados digitais válidos roubados da *Realtek* e da *JMicron*.

Esse *Worm* se propaga através de pen drives procurando por computadores com o software SCADA, após identificá-lo ele se instala no sistema e se propaga pela rede infectando outros computadores, bem como quaisquer *Drives* removíveis conectados ao computador infectado, a Figura 07 demonstra esse procedimento.

Figura 7 – Propagação Stuxnet



Fonte: Adaptado de BROAD, William J., MARKOFF, John; SANGER, David E. (2011).

De acordo com Randy Abrams (2010), a assinatura digital em um arquivo diz que o arquivo não foi adulterado ou corrompido. Se um vírus infecta um arquivo depois dele ter sido assinado digitalmente, ele quebra a assinatura digital e o *Windows* não irá executar o arquivo. Agora se um arquivo está infectado e, em seguida, é assinado digitalmente, isso significa que você tem um *Malware* funcional em um programa que tem uma assinatura digital válida.

Ao infectar um computador, ele passa por um período de stand by e fica escondido por vários dias. Após este período, ele procura o software usado para programar os controladores *Siemens* e começa a moldá-lo da maneira que lhe é pré-programado, assim, ele regula os motores de centrífugas e outras máquinas. O *Stuxnet* passa a acelerar e desacelerar os motores

para danificar ou destruir as máquinas. Enquanto faz a modificação na rotação das centrífugas, ele envia falsos sinais para o sistema, dizendo que está tudo funcionando normalmente.

Se o *Worm* identificar que o computador hospedeiro tem acesso à Internet, ele verifica se há atualizações de sua versão e tenta baixá-las e instalá-las.

O código do *Stuxnet* é complexo. Ele contém um arquivo com extensão .dll (*Dynamic-Link Library*) e contém blocos criptografados. Seu código é altamente modular, o qual analisa a melhor maneira de se infiltrar no sistema e pode variar essa infiltração. Além disso, o *Malware* analisa qual é a versão do sistema operacional e o nível de hierarquia do usuário conectado ao computador durante a infecção, caso não seja o administrador, ele executa um código para subir o nível de privilégios.

Segundo a *Microsoft* (2007), um arquivo de biblioteca de vínculo dinâmico (DLL) é um arquivo executável que permite que os programas de compartilhamento de código e outros recursos necessários executem determinadas tarefas. O *Microsoft Windows* fornece arquivos .dll que contêm funções e recursos que permitem que os programas baseados no *Windows* operem no ambiente *Windows*.

6.1.1 Vulnerabilidades Exploradas

O *Stuxnet* usa as seguintes vulnerabilidades no *Windows*: MS08-067, a qual se espalha pela rede da mesma forma que o DOWNAD/Conficker fez; MS10-46, a qual permite que ele se espalhe por meio de unidades removíveis mesmo se o *Autorun* estiver desabilitado; MS10-061, a qual se espalha por meio de redes, se um sistema compartilhar uma impressora na rede; e a MS10-073, a qual escala o nível de privilégio até o administrador do sistema, permitindo que ele realize qualquer tarefa que desejar na máquina local. Ele as utiliza para se infiltrar, instalar-se e se propagar no ambiente alvo. Atingindo com sucesso essas vulnerabilidades, ele garante sua permanência e execução no sistema.

6.1.1.1 MS08-067

Essa falha permite a execução remota no *Windows*. De acordo com a *Microsoft* (2008), o invasor que explorar com êxito essa vulnerabilidade poderá assumir o controle total de um sistema afetado.

O *Stuxnet* explora essa falha e consegue acessar remotamente uma máquina que não está com a falha corrigida, a qual está desatualizada. A partir daí ele faz uma cópia de si mesmo para a máquina, faz sua instalação e continua sua propagação.

De acordo com Falliere, Murchu e Chien (2011), o *Stuxnet* irá verificar as seguintes condições antes de explorar MS08-67: a data atual deve ser antes de 1 de janeiro de 2030; as definições de antivírus para uma variedade de produtos antivírus deve ser datado antes de 01 de janeiro de 2009 e o Kernel32.dll e Netapi32.dll timestamps após 12 outubro de 2008 (antes do dia patch).

6.1.1.2 MS10-046

Esta é uma falha no tratamento de atalhos. O *Windows* interpreta errado, deixando-o vulnerável.

De acordo com a *Microsoft* (2010), a vulnerabilidade existe porque o *Windows* analisa atalhos incorretamente de maneira que seja possível executar um código mal-intencionado quando o sistema operacional exibir o ícone de atalho deste arquivo.

Esta falha permite que um código malicioso crie um atalho para um acesso, outro *Malware,* entre outros. O dispositivo pode ser infectado através da navegação pelo *Windows Explorer* acessando uma unidade removível ou por compartilhamento de rede.

De acordo com por Massod, Ghazia e Anwar (2011), como arquivos de atalho apontam para o local original do recurso, *Stuxnet* usa essa funcionalidade para redirecionar arquivos de atalho para a sua DLL maliciosa.

A MS10-046 é conhecida como vulnerabilidade de arquivo .LNK (arquivos de atalho), tem grande aplicabilidade devido ao fato que todo software que é instalado gera um atalho, substituí-lo da maneira correta, fará com que o atacante consiga êxito.

Segundo Matrosov *et al.* (2010), poucos dias após o debate público sobre o código de exploração PoC (do inglês *Proof-of-Concept*) disponível para a vulnerabilidade .LNK, o *Metasploit Framework* lançou um código incluindo a implementação do *Exploit*, a fim de permitir ataques remotos.

6.1.1.3 MS10-061

Essa vulnerabilidade permite que através de uma brecha no *Spooler* de impressão, usuários não autenticados possam acessar as configurações remotamente e aumentar o nível de permissão dos usuários. De acordo com a *Microsoft* (2010), um invasor poderá instalar programas, visualizar, alterar ou excluir dados, ou ainda criar novas contas.

6.1.1.4 MS10-073

Essa vulnerabilidade é mais uma de elevação de privilégios, mas dessa vez uma falha no agendador de tarefa, onde captura e se utiliza de um ponteiro, substituindo seu valor, injetando uma parte do código do *Malware*.

Segundo a *Microsoft* (2010), existe uma vulnerabilidade de elevação de privilégio devido à maneira como os *Drivers* do modo do *Kernel* do *Windows* mantêm a contagem de referência para um objeto.

De acordo com Falliere, Murchu e Chien (2011), a vulnerabilidade reside no código que chama uma função em uma tabela ponteiro de função; no entanto, o índice da tabela não é validado, permitindo corretamente que o código seja chamado de fora da tabela de funções.

6.2 DUQU

Em 14 de outubro de 2011, o Laboratório de Criptografia e Segurança de Sistema (*Laboratory of Cryptography and System Security* (CrySyS)) da Universidade de Tecnologia e Economia de Budapeste, Hungria, publicou um documento que alertava para outro *Malware*, o Duqu.

O Duqu é um *Troja*n que tem como objetivo ser um *Backdoor* que irá facilitar o acesso ao sistema e, assim, o furto de informação, mas também pode roubar informações contidas nos computadores infectados. Ele recebeu este nome por criar arquivos que começam com "~DQ". O Duqu contém três arquivos: um arquivo *Driver*, um arquivo DLL e um arquivo criptografado.

O *Trojan* se utiliza de um certificado digital válido da empresa C-Média. Ele possui em seu código uma configuração que o mantém operando por trinta dias, por padrão, decorrido esse período o *Malware* se remove automaticamente. Isso faz com que sua detecção seja dificultada.

De acordo com a *Symantec* (2011), em um dos casos, os atacantes usaram um e-mail contendo um documento do *Microsoft Word* especificamente criado para a infecção. O documento do *Word* continha um *Exploit* com uma *Zero-day*, não conhecida, que afetava o *Kernel* do sistema; sendo, assim, capaz de instalar o Duqu.

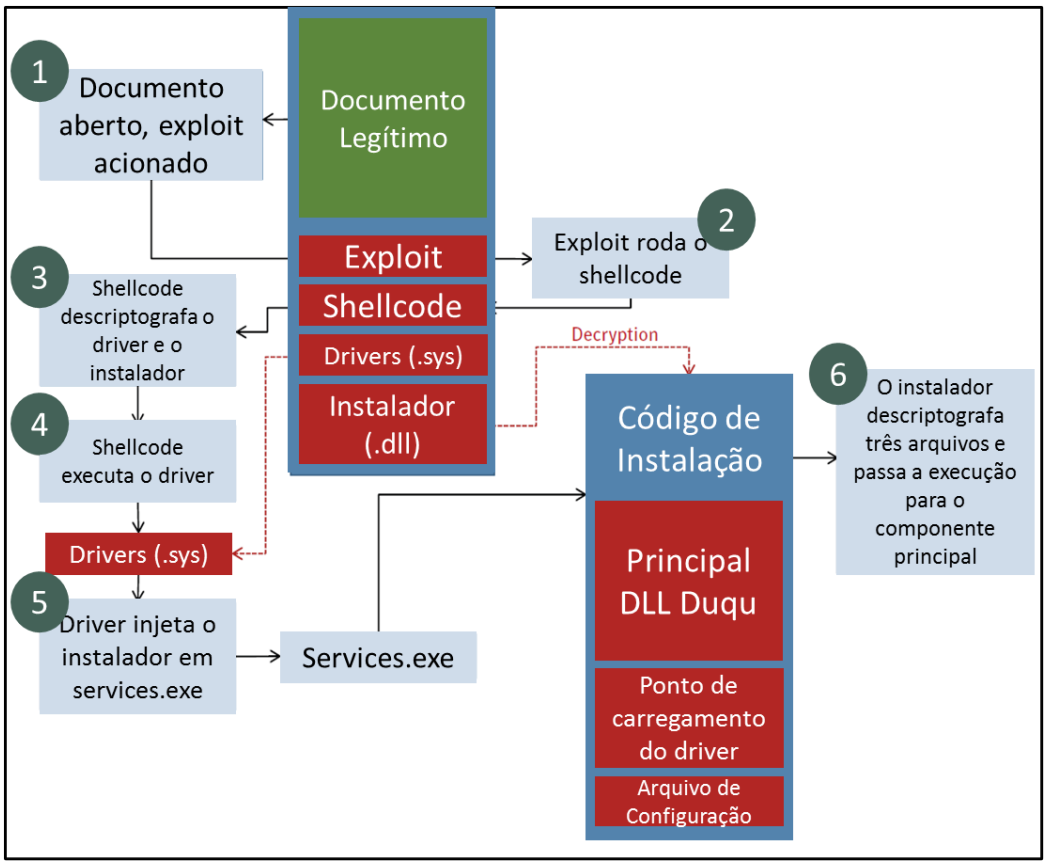
O processo de infiltração e instalação do Duqu, como mostra a Figura 8, é da seguinte forma: quando o documento *Word* é aberto é explorada a vulnerabilidade no *Kernel* que, por sua vez, permite a execução dos códigos maliciosos (1). Quando o arquivo infectado é executado, o *Exploit* realiza uma varredura nos registros do *Windows* (2) para verificar se o computador já se encontra infectado, caso já tenha ocorrido a infecção a operação é abortada, caso não, ele executa o arquivo *Driver* (3 - 4) que injeta códigos no arquivo *services.exe* (5); em seguida, executa um instalador DLL e limpa a memória. O instalador DLL descriptografa o outro arquivo e extrai de dentro dele mais três arquivos: *Main dll*, *Driver* e um arquivo de configuração do instalador (6). O arquivo *Driver* será o responsável por iniciar o Duqu quando

o sistema inicializar. O arquivo de configuração do instalador possui um cronômetro que analisa o tempo de instalação do *Malware*, caso ele não seja instalado no prazo, a instalação é cancelada. O *Main dll* irá se copiar para %Windir%\infz e será inicializado com o sistema.

O Duqu pode ser visto como uma ferramenta que coleta as informações necessárias do sistema ao qual quer atacar, permitindo o acesso e o teste de vulnerabilidade. Após essa coleta, o criador do *Trojan* desenvolve um *Malware* para um ataque específico. Pode-se afirmar que o *Stuxnet* foi desenvolvido após um software semelhante ou até uma versão anterior do Duqu que não foi detectada, ter feito a varredura do sistema do alvo.

Foi relatado que o *Stuxnet* e o *Duqu* têm diversas semelhanças, desde o designer do código até técnicas de infiltração. Muitos estudiosos dos dois *Malwares* acreditam que eles devem ter sido desenvolvidos pela mesma equipe ou no mínimo que elas tenham compartilhado informações.

Figura 8 – Instalação do Duqu



Fonte: Falliere, Murchu e Chien (2011).

6.3 FLAME (OU SKYWIPER)

Entre os *Malwares* que apareceram neste início de guerra cibernética, encontra-se o *Flame*, um *Malware* que pode ser considerado uma arma cibernética de espionagem. Programado em linguagem LUA, consegue capturar o teclado, a tela, os sons captados pelo microfone, dispositivos de armazenamento, rede, WiFi, Bluetooth, USB e enviá-los ao seu desenvolvedor.

Após o sistema estar infectado, ele cria arquivos temporários, como mostra o quadro abaixo, executa seus módulos (um após o outro com uma diferença de tempo de dois minutos, aproximadamente) e seus *Scripts* desenvolvidos em linguagem de programação LUA.

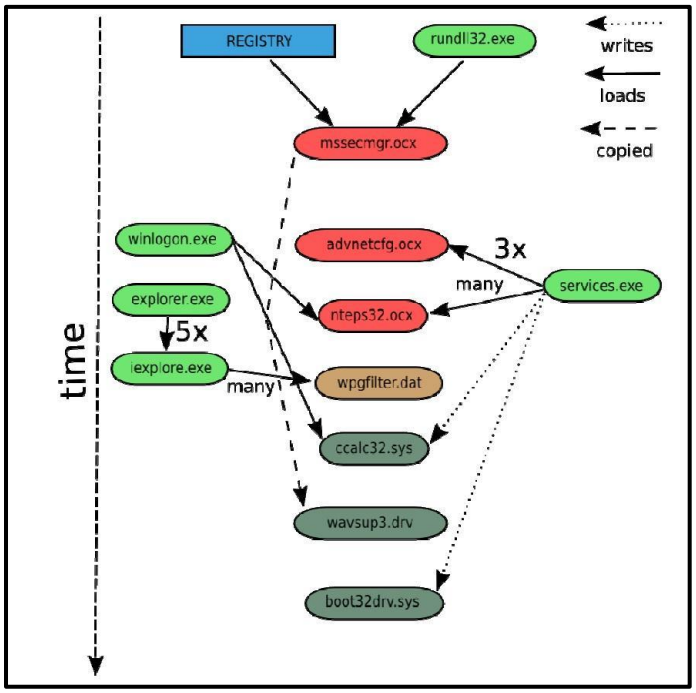
Quadro de Arquivos temporários do *Flame*

Nome do Arquivo	Função
~DEB93D.tmp	Arquivo criptografado contendo banco de dados SQLite de pesquisas de bloqueadores neuromusculares.
~HLV084.tmp	Partes comprimidas contém informações sobre os processos em execução.
~HLV294.tmp	Finalidade desconhecida. Este e 4 ou 5 arquivos semelhantes, muitas vezes aparecem em sistemas infectados.
~KWI<>	Peças comprimidas contém informações sobre os processos em execução.
~rf<number>.tmp	Contém o arquivo completo com listagem do computador infectado em SQLite 3 formado de base de dados e criptografados.

Fonte: Adaptado pelo autor de Skywiper Analysis Team (2012).

A Figura 9 mostra a sequência de inicialização dos módulos do *Flame*, a qual será explicada em seguida.

Figura 9 – Inicialização do Flame



Fonte: Skywiper Analysis Team (2012).

Na inicialização do sistema é carregado o módulo principal, o mssegmgr.ocx, ele é carregado como se fosse um pacote de autenticação local do *Windows*, ou seja, um (LSA) *Local Security Authority*. Cerca de 2 minutos depois advnetcfg.ocx é carregado por services.exe. Esse processo é repetido a cada 2 a 3 minutos, 3 vezes no total. Cerca de 2 minutos depois, o services.exe carrega o nteps32.ocx de mssecmgr.ocx e, em seguida, o winlogon.exe também carrega o nteps32.ocx. Este arquivo é carregado várias vezes. Enquanto isso, explorer.exe inicia 5 processos iexplore que subsequentemente criam wpgfilter.dat. Novamente, 2 minutos depois, o ccalc32.sys é escrito por services.exe e, em 1 minuto, o winlogon.exe o carrega. Em seguida, o mssecmgr.ocx é copiado para wavsup3.drv. Depois, o boot32drv.sys é carregado por services.exe.

O *Flame* tem métodos de proteção contra programas anti-*Malwares*. Ele detecta o programa de segurança que está instalado e modifica as extensões de seus arquivos para não ser detectado. Dentre outros motivos, essa mutação deve ser uma das causas do *Flame* ter se espalhado grandemente em alguns países do Oriente Médio, conforme pode ser observado na Figura 10, suspeita-se que o ataque tem como motivação atacar o programa nuclear iraniano e foi comandado pelos Estados Unidos e por Israel.

Figura 10 – Propagação do Flame

Fonte: THE FLAME (2012).

6.4 MALWARES: DA GUERRA CIBERNÉTICA À GUERRA

Como visto anteriormente, a guerra cibernética é uma guerra no mundo digital, que pode ser levada ao mundo real. O código malicioso pode ser a porta pela qual essa transição pode ocorrer. O uso dos *Malwares* como armas cibernéticas pode desencadear uma guerra real.

Existem três cenários de guerra cibernética que são, segundo Anchises (2011), uma guerra tradicional usando recursos digitais. Um *Cyber* ataque causando um *Cyber* conflito é um *Cyber* ataque causando uma resposta convencional (guerra tradicional).

6.4.1 Cenários possíveis

Baseando-se no que disse Anchises (2011), pode-se exemplificar cenários da guerra em situações que realmente podem acontecer.

No primeiro caso, a guerra tradicional usando recursos da guerra cibernética, pode ser exemplificado da seguinte maneira: uma das nações invade o sistema do inimigo e interrompe as comunicações do quartel general com os pelotões que se encontram na frente da batalha.

Sendo assim, sem as devidas informações/ordens, a nação atacada não saberá onde e/ou quando agir, ou até mesmo pode ser induzida por uma mensagem falsa a "cair" em uma armadilha.

Um caso real desse cenário foi na Guerra Russo-Georgiano, onde enquanto as tropas russas invadiam a Geórgia, os sistemas de comunicação da Geórgia foram derrubados por DDOS feito pelos russos. De acordo com Vianna (2013), o ataque cibernético coincidiu com ações de combate em terra, no mar e no ar desferida por um país contra o outro.

Já no caso de *Cyber* ataque causando um *Cyber* conflito é ilustrado pelo fato de ao receber um ataque cibernético, o país atacado revida com outro ataque cibernético.

Para finalizar, tem o cenário de um ataque cibernético causar uma guerra tradicional, para muitos é a possibilidade mais real e que mais se teme. Nesse cenário o país, ao identificar um ataque ou espionagem cibernética, responde pondo os soldados em campo de batalha, invadindo outro país, disparando mísseis, entre outros.

Após analisar esses três cenários, pode-se enxergar que uma nação pode infiltrar um código malicioso no sistema de outra e derrubar o sistema financeiro, a bolsa de valores, os bancos, os meios de comunicação, os sistemas de aeroportos e atacar os sites das forças armadas. A partir daí poderiam tomar conta do lançamento de mísseis e dizimar o país com suas próprias armas ou até mesmo "sequestrar" um VANT e atacar uma terceira nação e culpar outro país.

De acordo com Santos Júnior (2013), a Revista *Wired* reportou que um vírus tinha infectado um sistema de controle de VANT norte-americano, capturando o que era digitado nas cabines de pilotagem dos drones na Base Aérea de Creech, em Nevada.

As ameaças baseadas em *Malwares* são possíveis devido ao fato de os sistemas dos veículos aéreos não tripulados poderem utilizar redes baseadas em protocolos TCP/IP (pilha de protocolos bastante usado na Internet) para que as GCS se conectem com centros de controle, de onde são enviadas as informações para atacar ou não certo alvo, por exemplo, confirmando dados ou obtendo informações sigilosas. O que torna um risco elevado a operação dessas aeronaves, pois caso seja criada uma *Advanced Persistent Threat* (APT) – em português Ameaça Avançada Persistente – com a finalidade de atacar este sistema propriamente dito, é difícil saber a proporção dos prejuízos que podem acontecer (SANTOS JÚNIOR, 2013).

7 AMBIENTE DE TESTE E ANÁLISES

Para o desenvolvimento deste trabalho serão apresentados estudos sobre a detecção de dois dos *Malwares* já apresentados neste trabalho, o *Stuxnet* e o *Flame*, os quais foram escolhidos por estarem em grande destaque devido a sua utilização para atacar vários países nos últimos anos. Para esta análise foi utilizada a ferramenta online Virus Total, por se tratar de um serviço online e gratuito, o qual faz a análise de arquivos e URLs e possibilita a identificação de conteúdo malicioso detectável pelos antivírus.

A Virus Total é uma subsidiária do Google. Ela permite a identificação de vírus, *Worms*, *Trojans* e outros tipos de conteúdos maliciosos detectados por vários mecanismos de antivírus e scanners. Ao mesmo tempo, ele pode ser utilizado como um meio para detectar os falsos positivos, ou seja, os recursos inócuos detectados como maliciosos por um ou mais scanners (VIRUS TOTAL, 2015, tradução nossa).[2]

Também será feita uma ambientação do funcionamento do *Stuxnet.* Será montado um ambiente virtualizado reproduzindo um ambiente similar ao que é apresentado no artigo *SWAM Stuxnet Worm Analysis in Metasploit* (MASSOD; GHAZIA; ANWAR, 2011).

7.1 VÍRUS TOTAL

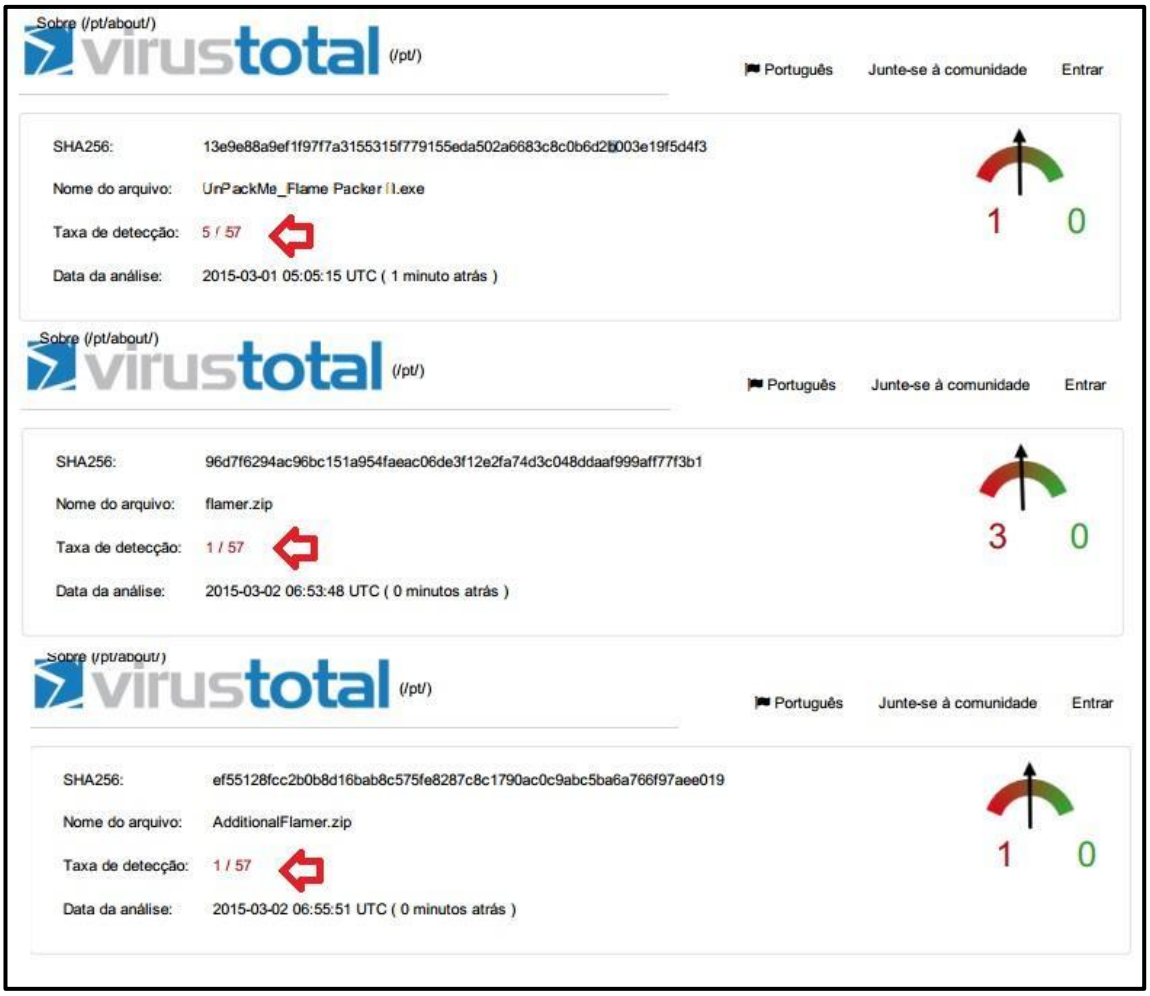
Após baixar os arquivos do *Stuxnet* e do *Flame* eles foram submetidos ao site do *Virus Total* que, por sua vez, informou a taxa de detecção dos *Malwares* pelos antivírus encontrados no mercado atualmente, como o *McAfee*, *Malware Protection* e o *Avast*! *Antivirus.*

Para o *Flame* foram usadas três amostras diferentes: UnPackMe_Flame Packer II.exe, flamer.zip e AdditionalFlamer. A análise encontrou dois resultados diferentes, os quais são explicados abaixo.

A ferramenta *Virus Total* analisou as três amostras do *Flame* e demostrou que para a amostra *UnPackMe_Flame Packer II.exe* a taxa de detecção foi 5/57, isso quer dizer que a ferramenta submeteu o arquivo a cinquenta e sete antivírus e somente cinco deles identificaram o arquivo como uma ameaça. Para o arquivo *flamer.zip* a taxa de detecção foi 1/57 e para o arquivo *AdditionalFlamer* a taxa foi a mesma, 1/57. Na Figura 11, pode-se observar os resultados obtidos.

[2] Texto original: VirusTotal, a subsidiary of Google, is a free online service that analyzes files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners. At the same time, it may be used as a means to detect false positives, i.e. innocuous resources detected as malicious by one or more scanners.

Figura 11 – Identificação do *Flame*



Fonte: Elaboração própria em 2015.

Para o *Stuxnet* também foram utilizadas três amostras: *malware.exe*, *Stuxnet-Sourcecode.rar* e *Stuxnet.rar*. No arquivo *malware.exe*, a taxa de detecção foi 53/57, ou seja, a ferramenta submeteu o arquivo a cinquenta e sete antivírus e somente cinquenta e três deles identificaram o arquivo como uma ameaça; para o arquivo *Stuxnet-Sourcecode.rar* a taxa de detecção foi 0/57, ou seja, nenhum antivírus conseguiu identificar o arquivo como uma ameaça; e para a amostra *Stuxnet.rar* a taxa de detecção foi 0/56, conforme mostra a Figura 12.

Figura 12 – Identificação do *Stuxnet*

Fonte: Elaboração própria em 2015.

Diante do que foi relatado pela ferramenta, pode-se afirmar que todos os dois códigos maliciosos ainda têm chance de causar danos nos dispositivos, uma vez que passam despercebidos pela maioria dos antivírus encontrados no mercado. O que não deveria acontecer, já que é notório o grau de periculosidade dos mesmos e também o fato de terem sidos descobertos há muito tempo, ou seja, não são ameaças recentes, portanto, já houve tempo suficiente para os antivírus serem atualizados e, consequentemente, conseguirem identificá-los e removê-los. São essas fragilidades de atualização, entre outras, que fazem com que o *Malware* se torne uma arma silenciosa.

7.2 SIMULAÇÃO

A simulação será realizada somente com o *Stuxnet,* ficando a simulação do *Flame* para estudos futuros.

O *Stuxnet* foi desenvolvido para se propagar até encontrar uma rede industrial com a presença de PLCs e softwares específicos, como o SCADA, e se instalar. Após a instalação, ele danifica o sistema.

Tendo em vista a dificuldade de se conseguir tal ambiente, será reproduzido neste trabalho um cenário semelhante a simulação feita por Massod, Ghazia e Anwar em 2011, na qual os autores reproduziram um cenário em ambiente virtualizado que explora falhas *Zero-day* no sistema operacional *Windows* que o *Stuxnet* se utiliza para infectar e se propagar.

Eles simularam três vulnerabilidades de *Worm Stuxnet* através do *Metasploit Framework*, o qual é um *Hacking framework* de código aberto escrito em linguagem Ruby. Ele é usado para explorar, executar e escrever o código para vulnerabilidades e também pode ser usado para configurar a construção de *Exploits* e seus *Payloads*, os quais são úteis para a análise. Ele tem outras utilizações para os *Hackers*, como testes de penetração, quebra de senha e muito mais.

O *Stuxnet* infecta uma máquina inicialmente por um dispositivo USB. Após a infecção, ele busca se propagar pela rede explorando as falhas citadas anteriormente. Para simular isso será usado o *Metasploit Framework* versão 4.11.1, através desta ferramenta será feita o acesso às máquinas da rede.

O laboratório montado consiste em ambiente virtualizado utilizando o software VM VirtualBox, versão 4.2.16 r86992, da empresa *Oracle*. Com o VM VirtualBox pode-se instalar vários sistemas operacionais distintos, os quais funcionaram hospedados em um sistema operacional ligado direto ao hardware e as máquinas virtualizadas podem se comunicar em rede interna e com a internet.

As máquinas virtualizadas para este trabalho possuíam o sistema operacional Kali Linux ver 1.0 e o sistema operacional *Kali Linux*, no papel de atacante; e a alvo, o sistema operacional *Microsoft Windows XP service Pack 3* versão 2002.

7.2.1 Acesso Remoto e Propagação

Será explorada a falha MS08-067 para demonstrar que por essa falha o *Stuxnet* pode acessar o sistema, no caso o *Windows XP*, e se propagar pela rede, uma vez que esta vulnerabilidade permite que ele se espalhe pela rede. Para isso a máquina *Linux Kali* terá instalada a ferramenta *Metasploit framework*, o qual facilita os testes de penetração.

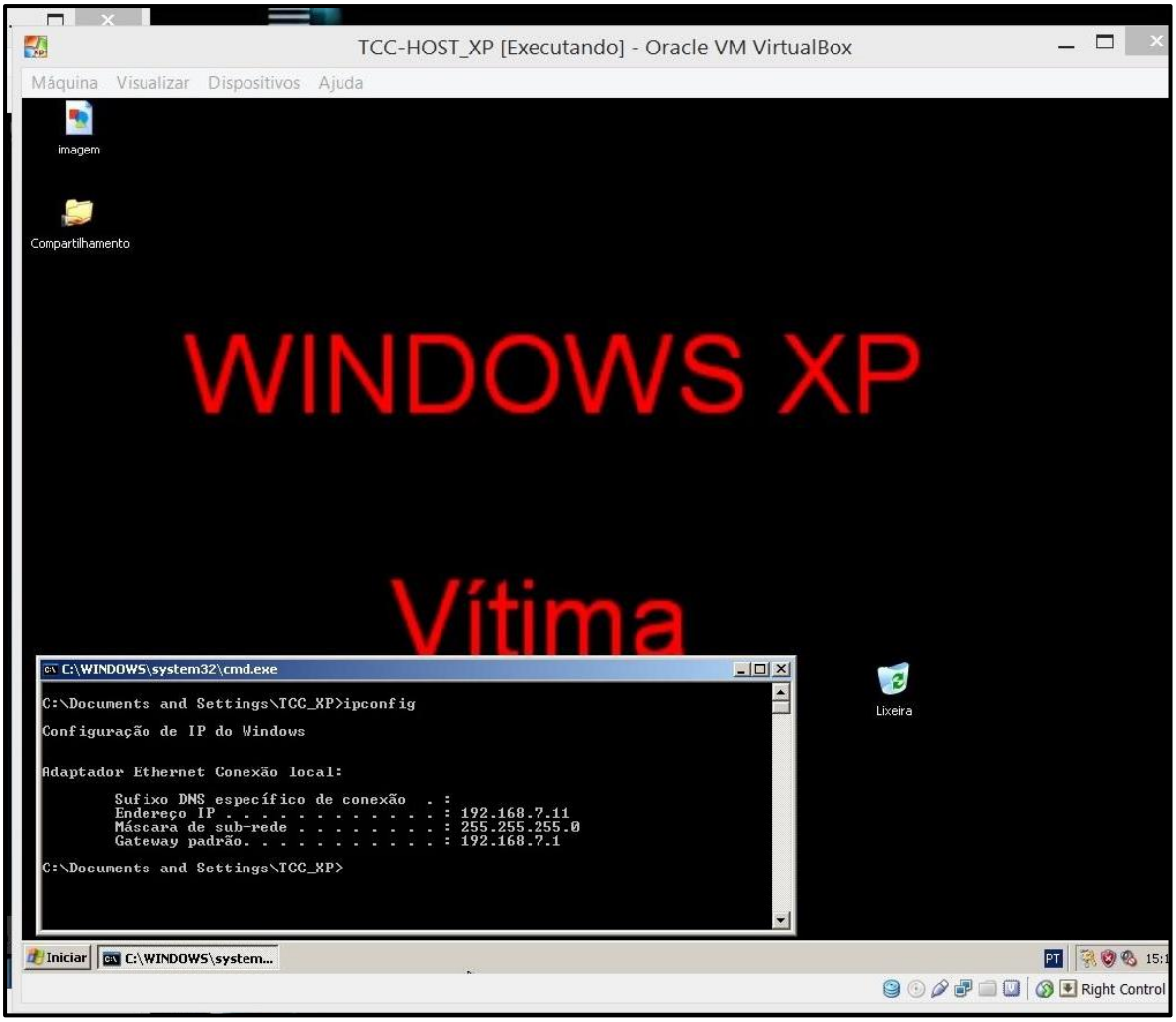
Para simular o ataque, primeiramente, será necessário saber os IPs de cada máquina, como pode ser observado na Figura 13, a qual faz a identificação do IP da máquina atacante; e

na Figura 14, a qual faz a identificação do IP da máquina alvo; visto que o comando usado no *Metasploit framework* faz uso da identificação dos endereços para o ataque.

Figura 13 – Identificação de IP da máquina atacante

Fonte: Elaboração própria em 2015.

Figura 14 – Identificação de IP da máquina alvo



Fonte: Elaboração própria em 2015.

Quadro de Identificação de IP

Identificação de IP	
Máquina	Endereço IP
Máquina Alvo	192.168.7.11
Máquina Atacante	192.168.7.14

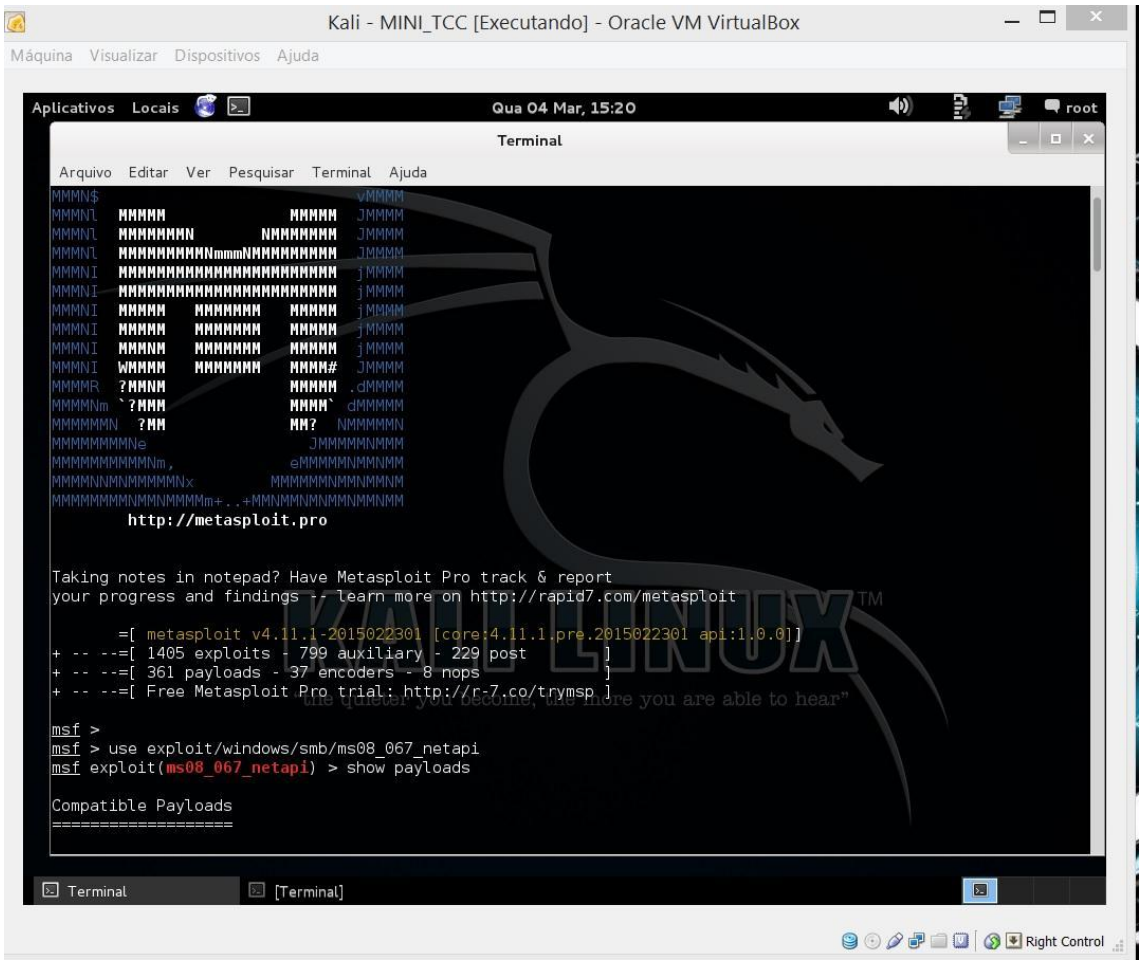
Fonte: Elaboração própria em 2015.

Depois de identificar os endereços IPs de cada máquina, será iniciada a ferramenta *Metasploit framework*. Após iniciá-la, será indicada qual vulnerabilidade será atacada, no caso a MS08-067, para isso é digitado o comando "*use exploit/windows/smb/ms08_067_netapi*", conforme mostra a Figura 15. Em seguida, é carregado o *Payload*, arquivo que contém o código

para explorar a vulnerabilidade. Com o comando "*show payload*" será exibida uma lista de códigos que se pode usar.

Com o comando "*set PAYLOAD windows/meterpreter/reverse_tcp*" é carregado o *Payload* que será utilizado. Agora serão identificados os IPs das máquinas envolvidas na simulação.

Figura 15 – Iniciando Metasploit

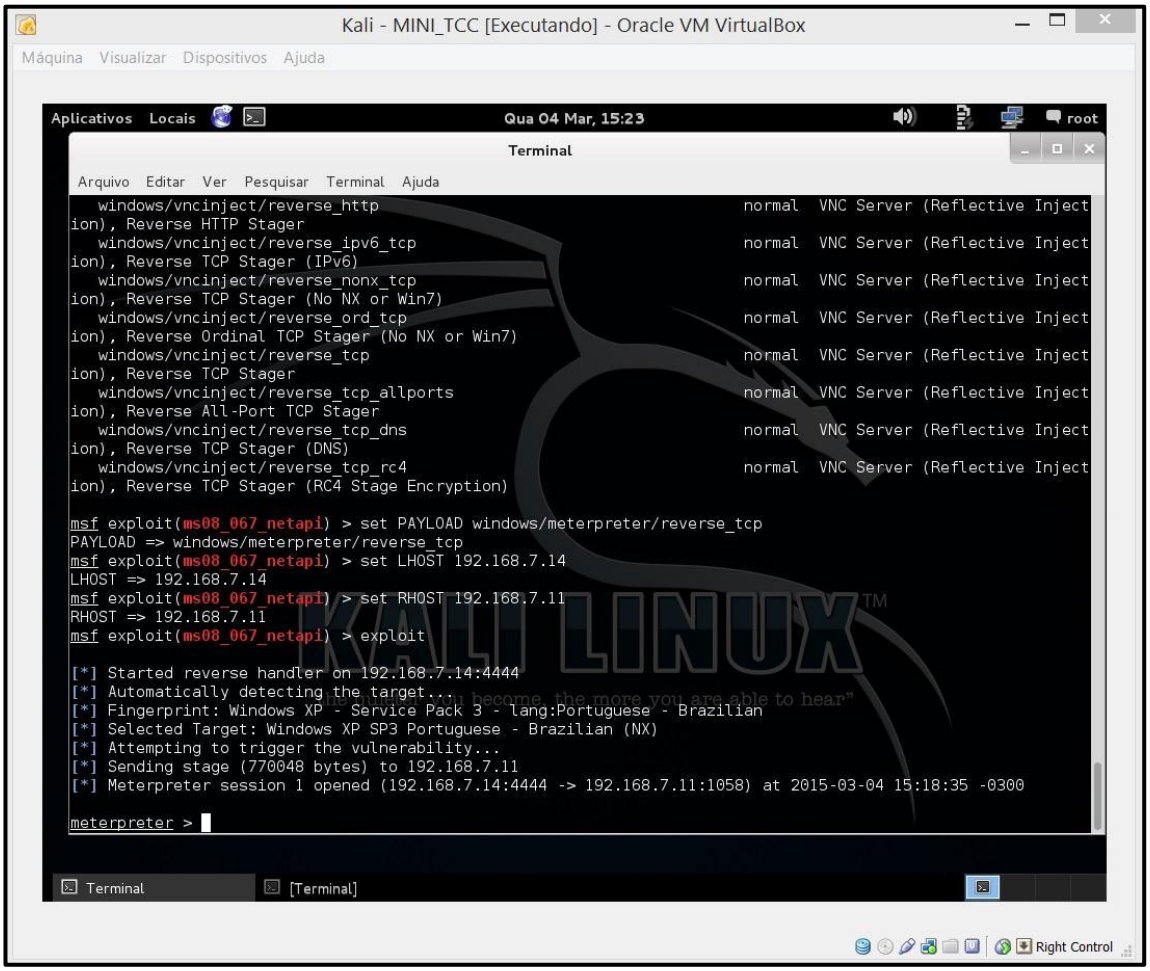


Fonte: Elaboração própria em 2015.

Para identificar a máquina do atacante, também chamada de LHOST, é digitado o comando "*set LHOST 192.168.7.14*". Para identificar a máquina alvo/vítima, também conhecida como RHOST, é digitado "*set RHOST 192.168.7.11*". Com essas configurações realizadas basta digitar o comando "*exploit*". Ao aparecer na tela "*Meterpreter session 1 opened (192.168.7.14:4444 -> 192.168.7.11:1058) at 2015-03-04 15:18:35 – 0300*", significa que foi

aberta uma seção da máquina 192.168.7.14 (atacante) para a máquina 192.168.7.11 (alvo). Feito isso, o atacante tem acesso à máquina alvo, conforme mostra a Figura 16.

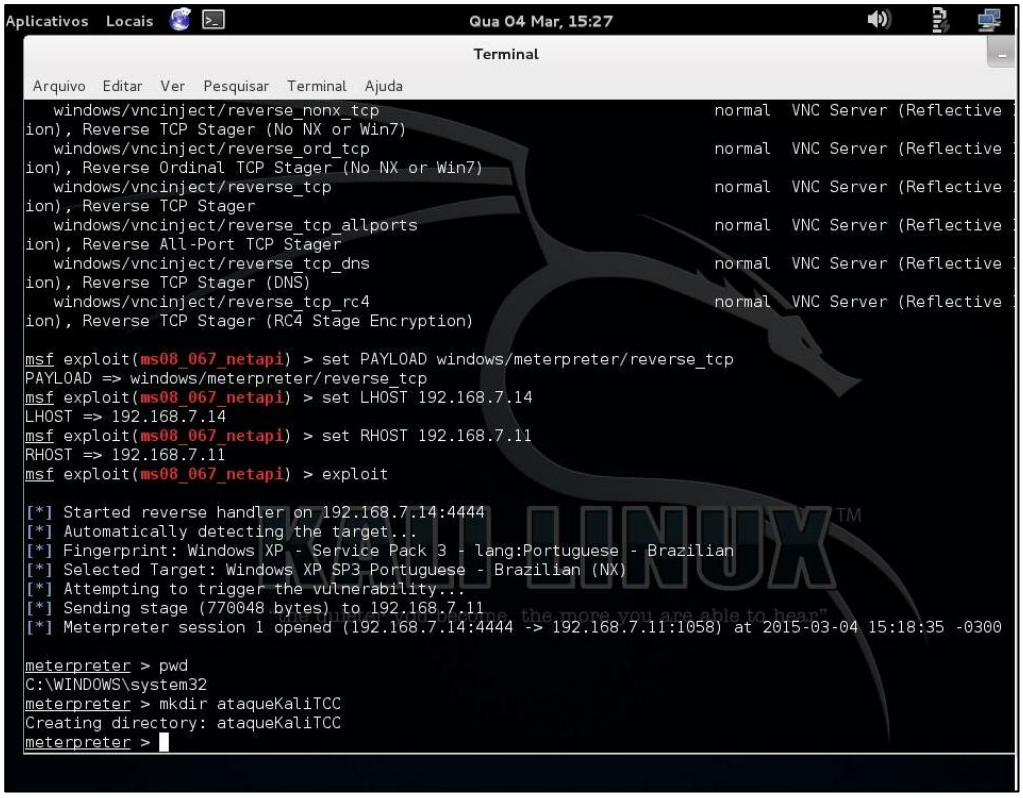
Figura 16 – Configurando *Metasploit*



Fonte: Elaboração própria em 2015.

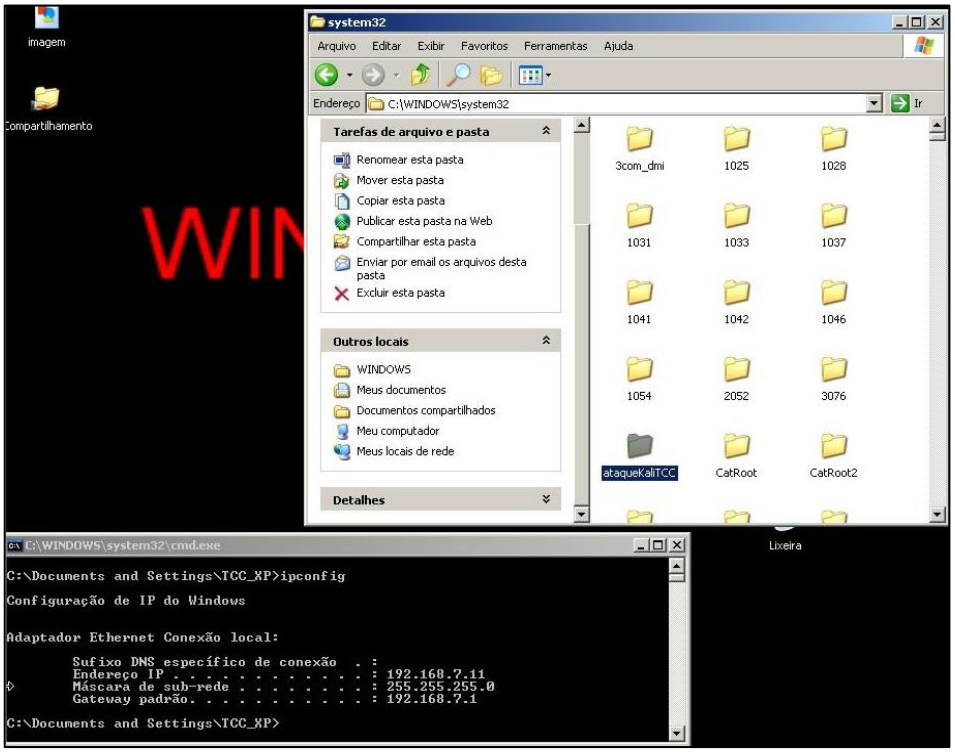
Com acesso à máquina o atacante pode navegar pelos diretórios livremente, podendo roubar o conteúdo de pastas, modificar arquivos e criar pastas, como se fosse o usuário da máquina, assim como mostram a Figura 17 e a Figura 18. Também existe a possibilidade do atacante ter acesso às funções do sistema, verificando processos abertos e explorando outras vulnerabilidades.

Figura 17 – Criando pasta remotamente



Fonte: Elaboração própria em 2015.

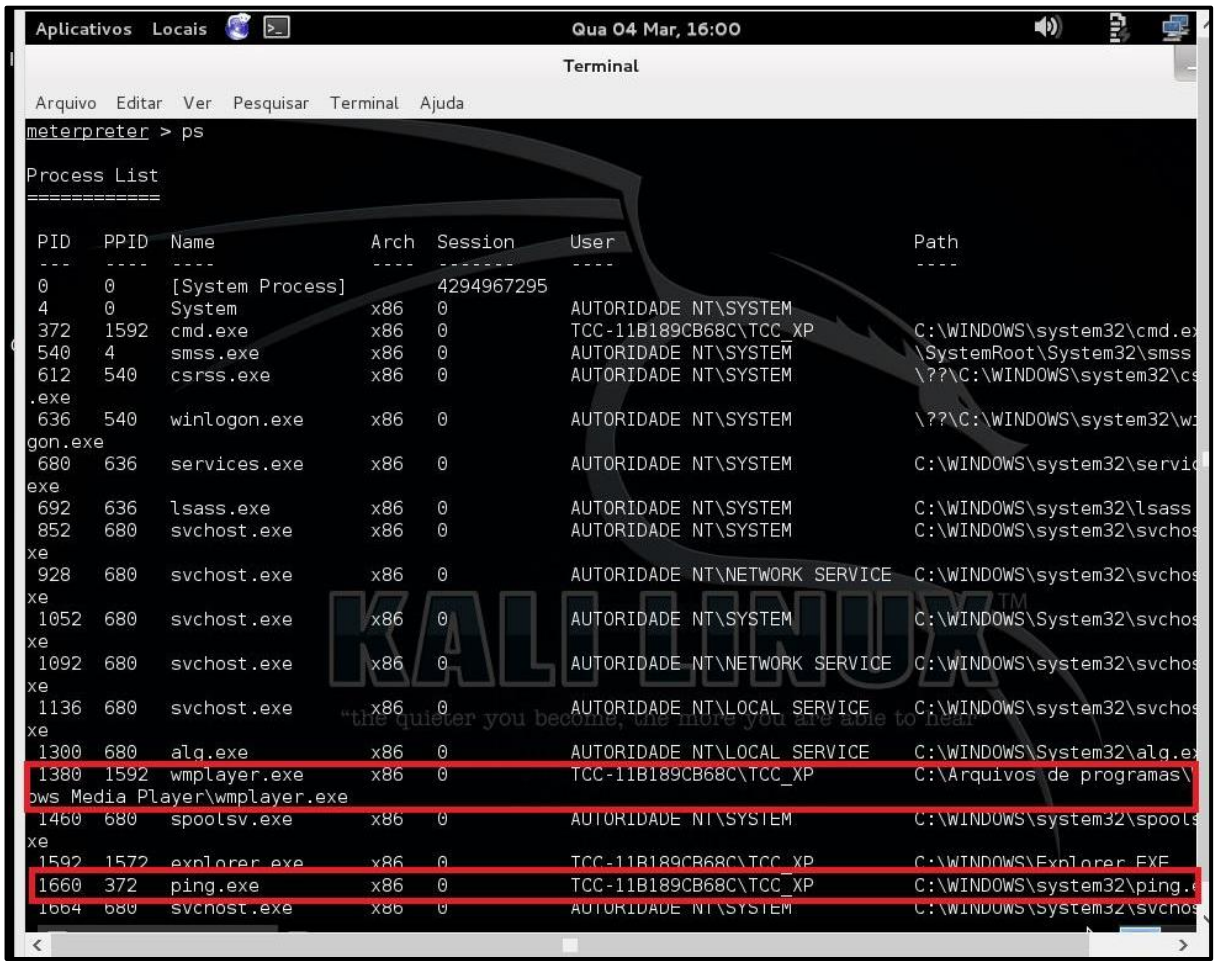
Figura 18 – Pasta criada remotamente



Fonte: Elaboração própria em 2015.

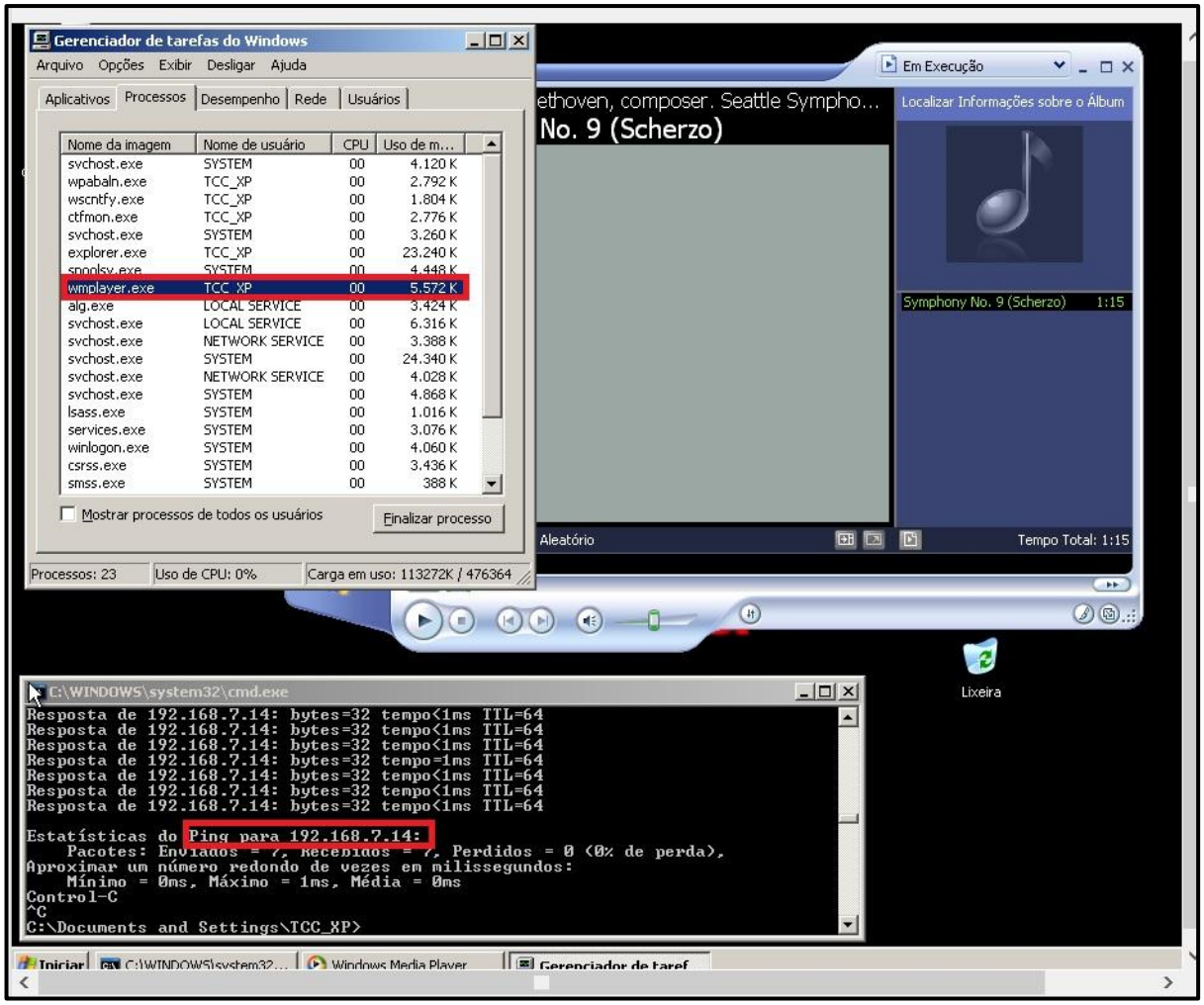
A Figura 19 e a Figura 20 mostram que ao executar o comando “PS” são listados os processos em execução e, neste caso, dentre eles estão listados o *ping* e o *media player*.

Figura 19 – Execução do comando “PS”



Fonte: Elaboração própria em 2015.

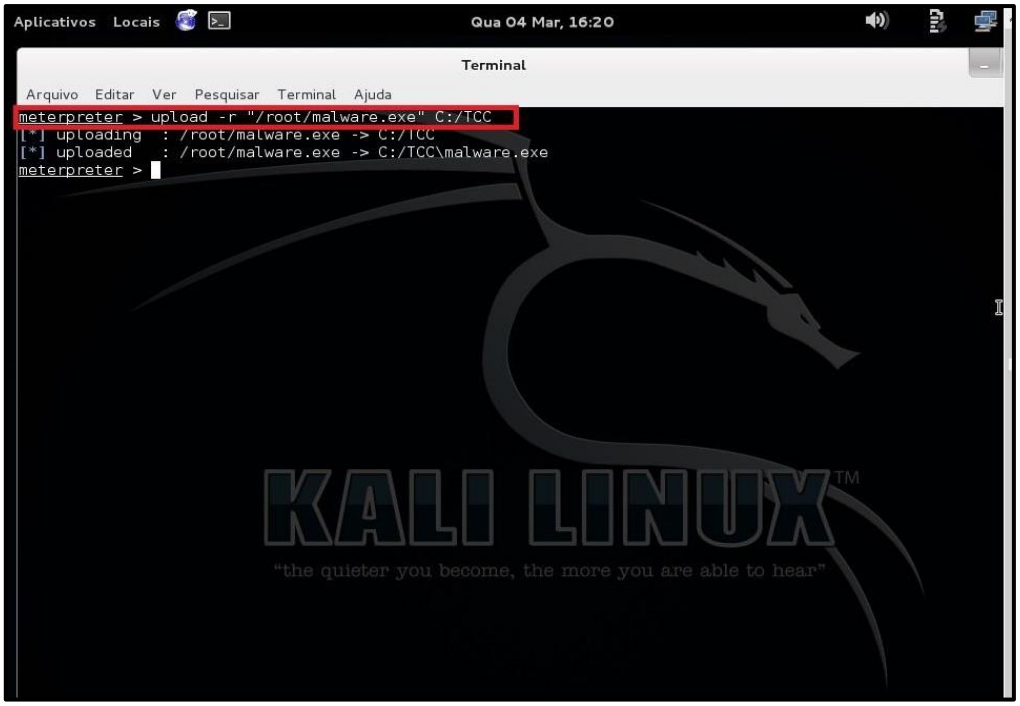
Figura 20 – Processos sendo executados



Fonte: Elaboração própria em 2015.

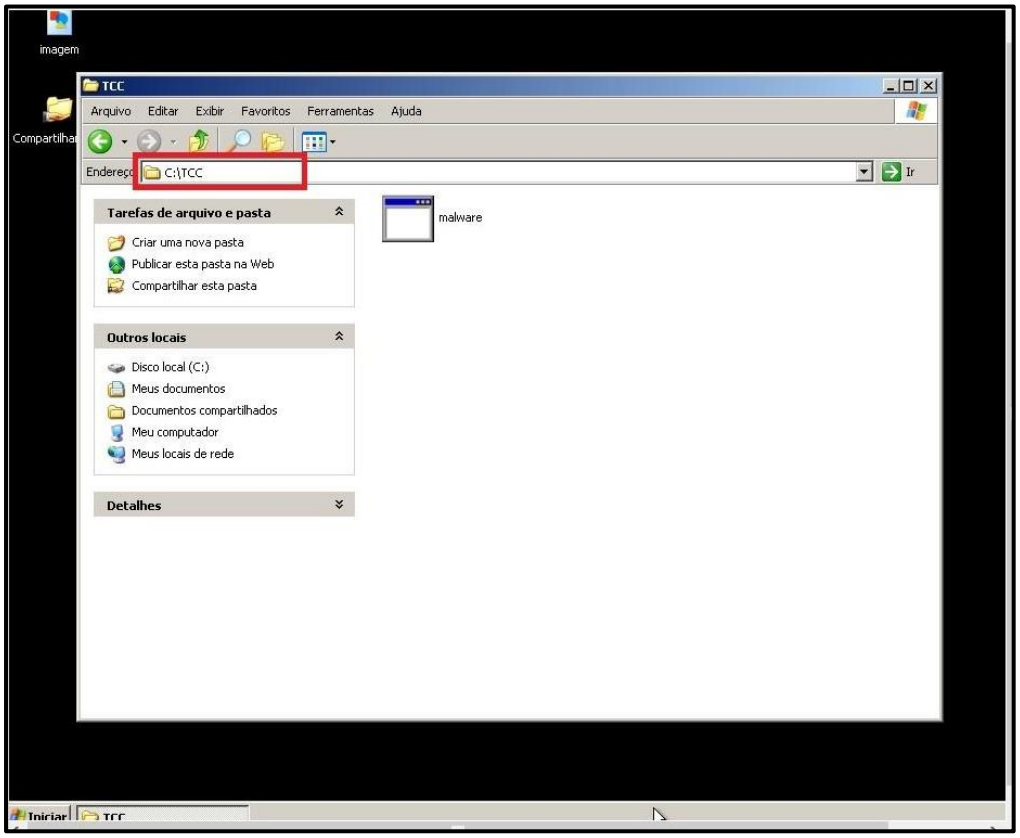
Levando para o lado do *Stuxnet*, com essa vulnerabilidade o *Malware* conseguiu acessar máquinas na rede e identificar processos abertos. Ele também conseguiu identificar se a máquina já estava infectada e caso não estivesse, faria uma cópia do código, conforme a Figura 21 e a Figura 22.

Figura 21 – Transferindo Malware



Fonte: Elaboração própria em 2015.

Figura 22 – Malware Transferido



Fonte: Elaboração própria em 2015.

8 RESULTADOS

A partir da análise realizada no Virus Total do *Stuxnet* e do *Flame* para saber a taxa de detecção dos *Malwares* pelos antivírus encontrados no mercado atualmente, pode-se observar que o mercado não consegue se atualizar ao mesmo tempo que os avanços tecnológicos acontecem e nem na mesma velocidade que surgem novas tecnologias e novas ameaças.

Por meio da simulação realizada foi possível acompanhar o passo a passo realizado pelos invasores e, assim, perceber o poder de destruição que os *Malwares* possuem. Diante disso, têm-se a necessidade de traçar estratégias de defesa para responder a estes ataques.

É de fundamental importância os países construírem uma infraestrutura de tecnologia da informação e comunicação para a sua defesa em um possível ataque cibernético ou uma guerra cibernética.

Com o estudo e a simulação apresentados neste trabalho foi possível conhecer a importância da segurança no ambiente de TIC, atentando sobre a segurança cibernética de uma nação, os efeitos ocasionados caso haja uma falha na proteção dos dados do país. Também foi possível aprofundar o conhecimento sobre *Malwares* e exemplificar o seu potencial como uma arma em guerras cibernéticas e os problemas causados por seu uso.

9 CONCLUSÃO

A guerra cibernética é a mais pura realidade. As nações já estão se preparando com treinamento, capacitação e desenvolvimento para uma guerra cibernética. Por ser uma arma silenciosa, que permite ocultação dos passos e a não identificação do seu responsável, o *Malware* é uma maneira apta e precisa de ataque em uma guerra cibernética. Ele mostra ser um tipo de ataque efetivo, de poder destrutivo e de ampla escala.

A tendência é que a cada dia mais o número de casos de ataques cibernético patrocinados por nações venha surgir. Cada um com mais sofisticação, mais inteligência, maior maleabilidade e com alvos cada vez mais específicos.

Logo, este trabalho traz como contribuição o conhecimento do passo a passo de uma invasão para a obtenção de dados sigilosos e, assim, identificar as principais vulnerabilidades dos sistemas para que possam ser corrigidas, diminuindo, assim, o poder de destruição dos ataques.

Uma vez conhecidas as vulnerabilidades, é possível corrigi-las e tornar o sistema mais seguro, diminuindo, assim, a entrada do invasor nele.

É de fundamental importância conhecer os tipos de *Malwares* existentes e a forma como estes conseguem entrar nos sistemas e roubar os seus dados. Diante disso, têm-se a necessidade de que haja um grande investimento na área de segurança da informação para que seja possível se atualizar na mesma velocidade que surgem novas ameaças e ser capaz de combatê-las a tempo.

Como sugestão de trabalhos futuros, propõe-se a simulação de ataques com o *Flame* e com outros *Malwares* existentes, para que seja possível conhecer as suas formas de ataques aos sistemas e de quais vulnerabilidades eles se utilizam.

REFERÊNCIAS

ABOUT us. VirusTotal. Disponível em: https://support.virustotal.com/hc/en-us/categories/360000160117-About-us. Acesso em: 5 feve. 2015.

ABRAMS, Randy. **Why steal digital certificates?** 2010. Disponível em: http://www.welivesecurity.com/2010/07/22/why-steal-digital-certificates/. Acesso em: 4 mar. 2015.

ALEXANDRE, Paulo. **Especialista afirma que a guerra cibernética já começou**. 2011. Disponível em: https://www.youtube.com/watch?v=kKBsCdtkshQ. Acesso em: 10 ago. 2014.

AMEAÇA cibernética é traiçoeira, dizem EUA. **Exame**, São Paulo, 2013. Disponível em: http://info.abril.com.br/noticias/seguranca/ameaca-cibernetica-e-trai.shl. Acesso em: 25 out. 2014.

ARAÚJO, Paulo Sérgio de. **O uso da tecnologia da informação como arma de ataque**. São Paulo: Faculdade de Tecnologia de Ourinhos, 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISSO/IEC 27002**. Rio de Janeiro: ABNT, 2005. 120 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISSO/IEC 13335-1**. Rio de Janeiro: ABNT, 2004. 120 p.

BRAQUINHO, Marcelo. A guerra cibernética bate à nossa porta. **Admin Redes & Segurança**, São Paulo, n. 6, p. 52, jun. 2012.

BRASIL. **Livro Branco de Defesa Nacional**. Brasília, DF: [*s. n.*], 2012. 273 p. Disponível em: https://redectidc.com.br/assets/files/2010%20-%20Livro%20Verde%20-%20Seguran%C3%A7a%20Cibern%C3%A9tica%20no%20Brasil.pdf. Acesso em: 30 jun 2014.

BROAD, William J., MARKOFF, John; SANGER, David E. **Israeli test on worm called crucial in Iran nuclear delay**. [*S. l.*]: The New York Times, 2011. Disponível em: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&_r=0 –. Acesso em: 2 ago. 2014.

CANONGIA, Cláudia; MANDARINO JUNIOR, Raphael. **Segurança cibernética**: o desafio da nova sociedade da informação. **Parcerias Estratégicas**, Brasília, DF, v. 14, n. 29, p. 21-46, jul./dez. 2009. Disponível em: www.cgee.org.br/atividades/redirKori/6000. Acesso em: 19 fev. 2015.

CARISSIMI, Alexandre da Silva; ROCHOL, Juergen; GRANVILLE, Lisandro Zambenedetti. **Redes de computadores**. Porto Alegre: Bookman, 2009. 391 p. (Livros Didáticos).

CARVALHO, Paulo Sergio Melo de. Conferência de abertura: o setor cibernético nas forças armadas brasileiras. *In*: BARROS, Ótavio Santana Rêgo; GOMES, Ulisses de Mesquita;

COMITÊ GESTOR DA INTERNET NO BRASIL. Núcleo de Informação e Coordenação do Ponto Br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de Segurança para Internet**: versão 4.0. São Paulo: CERT.br, 2012. Disponível em: https://cartilha.cert.br/malware/. Acesso em: 23 fev. 2015.

CHIEN, Eric; MURCHU, Liam O.; FALLIERE, Nicolas. **W32.Duqu**: the precursor to the next stuxnet. [*S. l.*: *s. n.*], 2011. Disponível em: https://www.usenix.org/system/files/conference/leet12/leet12-final11.pdf. Acesso em: 22 de agosto de 2014.

CLARKE, Richard; KNAKE, Robert. **Cyber war**. New York, USA: CCCO, 2010. 290p.

CLARKE, Richard A; KNAKE, Robert K. **Guerra cibernética: a próxima ameaça à segurança e o que fazer a respeito**. Rio de Janeiro: Brasport, 2015. 240 p.

DEFINIMOS e explicamos um arquivo DLL. [*S. l.*]: Microsoft. Disponível em: http://support.microsoft.com/kb/87934/pt-br. Acesso em: 23 fev. 2015.

DUVILLARD, Laureline. **Suíça se arma contra guerra cibernética**. [*S. l.*]: Swissinfo.ch, 2011. Disponível em: https://www.swissinfo.ch/por/su%C3%AD%C3%A7a-se-arma-contra-guerra-cibern%C3%A9tica/29202304. Acesso em: 18 fev. 2015.

FALLIERE, Nicolas; MURCHU, Liam O.; CHIEN, Eric. **W32.Stuxnet Dossier**. [*S. l.*]: Symantec Security Response, 2011. Disponível em: https://www.wired.com/images_blogs/threatlevel/2011/02/Symantec-Stuxnet-Update-Feb-2011.pdf. Acesso em: 22 ago. 2014.

FINKLE, Jim. **Poderosa cyber-arma "Flame" é descoberta no Irã**. [*S. l.*]: G1 Mundo, 2012. Disponível em: http://g1.globo.com/mundo/noticia/2012/05/poderosa-cyber-arma-flame-e-descoberta-no-ira.html. Acesso em: 22 jan. 2015.

FREITAS, Whitney Lacerda de. **Desafios estratégicos para segurança e defesa cibernética**. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. p. 37-48.

HOEPERS, Cristine; STEDING-JESSEN, Klaus. **Fundamentos de Segurança da Informação**. [*S. l.*]: Escola de Governança da Internet no Brasil, 2014. (Slides de aula). Disponível em: https://pt.slideshare.net/egibr/fundamentos-de-segurana-da-informao-51815158. Acesso em: 27 fev. 2015.

INTERNATIONAL TELECOMMUNICATION UNION. Recommendation X.1205 (ITU X.1205). Geneva, Switzerland: [*s. n.*], 2008.

Jorge Pontual entrevista especialista americano em segurança. 2011. 1 vídeo (22 min). Publicado pelo canal Worldnewsbrasil. Disponível em: https://www.youtube.com/watch?v=qvxwptqt564. Acesso em: 10 ago. 2014.

JORGE, Bernardo Wahl G. de Araújo. **Das "guerras cibernética"**. Rio de Janeiro:[s. n.] 2012. Disponível em:

http://www.eceme.ensino.eb.br/ciclodeestudosestrategicos/index.php/CEE/XICEE/paper/viewFile/29/50. Acesso em: 27 fev. 2015.

JÚNIOR CÉSAR DA CRUZ, Samuel (org.). **Nota Técnica nº 11**: tecnologias e riscos: armas cibernéticas. Brasília, DF: Ipea, 2013.

MANDARINO JUNIOR, Raphael. Reflexões sobre segurança e defesa cibernética. *In*: BARROS, Ótavio Santana Rêgo; GOMES, Ulisses de Mesquita; FREITAS, Whitney Lacerda de (org.). **Desafios estratégicos para segurança e defesa cibernética**. Brasília, DF: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. p. 37-48.

MANDARINO JUNIOR, Raphael; CANONGIA, Claudia (org). **Livro Verde: segurança cibernética no Brasil**. Brasília, DF: Gabinete de Segurança Institucional da Presidência da República; Secretaria Executiva; Departamento de Segurança da Informação e Comunicações, 2010. 63 p. Disponível em: https://redectidc.com.br/assets/files/2010%20-%20Livro%20Verde%20-%20Seguran%C3%A7a%20Cibern%C3%A9tica%20no%20Brasil.pdf. Acesso em: 11 out. 2021.

MANDARINO JUNIOR, Raphael. **Um estudo sobre a segurança e a defesa do espaço cibernético brasileiro**. 2009. Monografia (Especialização em Gestão da Segurança da Informação e Comunicações) – Universidade de Brasília, Brasília, DF, 2009. Disponível em: http://dsic.planalto.gov.br/cegsic/83-monografias-da-1o-turma-do-cegsic . Acesso em: 15 maio 2014.

MASOOD, Rahat; GHAZIA, Um-e; ANWAR, Zahid. Swan: suxnet worm analysis metasploit. *In*: INTERNATIONAL CONFERENCE ON FRONTIERS OF INFORMATION TECHNOLOGY, 9., 2011, Islamabad, Paquistão. **Proceedings** […]. Islamabad, Paquistão: IEEE Computer Society, 2011. Disponível em: https://ieeexplore.ieee.org/document/6137135. Acesso em: 25 fev. 2013.

MATROSOV, Aleksandr *et al*. **Stuxnet Under the Microscope**. 2010. Disponível em: http://www.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf. Acesso em: 23 fev. 2015.

MINISTRO de Israel defende uso do vírus 'Flame' contra o Irã. [*S. l.*]: G1 Tecnologia e Games, 2012. Disponível em: http://g1.globo.com/tecnologia/noticia/2012/05/ministro-de-israel-justifica-uso-do-virus-flame-contra-o-ira.html. Acesso em: 22 jan. 2015.

NARAINE, Ryan. **Stuxnet attackers used 4 Windows zero-day exploits**. [*S. l.*]: ZADNet, 2010. Disponível em: https://www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/. Acesso em: 29 jan. 2015.

NOVA versão do vírus Flame é detectada no Irã e Líbano. **Exame**, São Paulo, 2012. Disponível em: https://exame.com/tecnologia/nova-versao-de-virus-e-detectada-no-ira-e-libano/. Acesso em: 23 jan. 2015.

PALMAS, Luciano; PRATES, Rubens. **TCP/IP**: guia de consulta rápida. São Paulo: Novatec, 2000.

PAULA, Anchises Morais G. de. **Guerra cibernética e hacktivismo**. 2011. (Slides). Disponível em: http://pt.slideshare.net/SegInfo-Workshop-Blog/a-guerra-ciberntica-e-o-novo-hacktivismo-por-anchises-m-g-de-paula. Acesso em: 3 fev. 2015.

SANTOS JÚNIOR, Carlos Eduardo de Barros. **Análise de vulnerabilidades e ataques a veículos aéreos não tripulados (Vant)**. 2013. 83 f. Monografia (Redes de Computadores) – Instituto Federal de Educação Ciência e Tecnologia do Rio Grande do Norte, Natal, 2013.

SKYWIPER ANALYSIS TEAM. **sKyWIper (a.k.a. Flame a.k.a. Flamer**): a complex malware for targeted attacks. 2012. Disponível em: https://www.crysys.hu/publications/files/skywiper.pdf. Acesso em: 3 fev. 2015.

STEED, Danny. Cyber power and strategy – so what? **Infinity Journal**, n. 2, p. 21-24, 2011. Disponível em: https://www.militarystrategymagazine.com/article/cyber-power-and-strategy-so-what/. Acesso em: 12 ou 2014.

TANENBAUM, Andrew S. **Redes de computadores**. Tradução: Vandenberg D. de Souza. Revisão: Edgard Jamhour. Rio de Janeiro: Elsevier, 2003. 945 p.

TANENBAUM, Andrew S.; WETHERALL, David J. **Redes de computadores**. 5. ed. São Paulo: Pearson, 2011. 600 p.

TECHCENTER DE SEGURANÇA. **Microsoft Security Bulletin MS08-067 – Crítica**. 2008. Disponível em: https://technet.microsoft.com/pt-br/library/security/ms08-067.aspx. Acesso em: 18 fev. 2015.

TECHCENTER DE SEGURANÇA. **Microsoft Security Bulletin MS08-073 – Importante**. 2010. Disponível em: https://technet.microsoft.com/library/security/ms10-073. Acesso em: 18 fev. 2015.

TECHCENTER DE SEGURANÇA. **Microsoft Security Bulletin MS10-046 – Crítica**. 2010. Disponível em: https://technet.microsoft.com/library/security/ms10-046. Acesso em: 18 fev. 2015.

TECHCENTER DE SEGURANÇA. **Microsoft Security Bulletin MS18-061 – Crítica**. 2010. Disponível em: https://technet.microsoft.com/library/security/ms10-061. Acesso em: 18 fev. 2015.

THE FLAME: questions and answers. [*S. l.*]: Securelist, 2012. Disponível em: https://securelist.com/the-flame-questions-and-answers/34344/. Acesso em: 4 mar. 2015.

THEILER, Olaf. Novas ameaças: a dimensão cibernética. **Revista da Nato**, set. 2011. Disponível em: http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/PT/index.htm. Acesso em: 2 ago. 2014.

TZU, Sun. A arte da guerra. Tradução: André da Silva Bueno. São Paulo: Jardim dos Livros, 2011. 129 p.

VELUZ, Danielle. **STUXNET malware targets SCADA systems**. [*S. l.*]: Trend Micro, 2010. Disponível em: https://www.trendmicro.com/vinfo/au/threat-encyclopedia/web-attack/54/stuxnet-malware-targets-scada-systems. Acesso em: 3 ago. 2014.

VIANNA, Nilson Rocha. **A defesa cibernética na visão da MB**. Disponível em: http://www.eceme.ensino.eb.br/meiramattos/index.php/RMM/article/viewFile/218/187. Acesso em: 5 mar. 2015.

WENDT, Emerson. Ciberguerra, inteligência cibernética e segurança virtual: alguns aspectos. **Revista Brasileira de Inteligência**, Brasília, DF, n. 6, p. 15-25, abr. 2011. Disponível em: https://rbi.enap.gov.br/index.php/RBI/article/view/80/63. Acesso em: 21 out 2014.

W32.DUQU: the precursor to the next Stuxnet. 2011. Disponível em: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf. Acesso em: 27 jan. 2015.