Pornografia infanto juvenil e invasão há redes de computadores

Marcos de Andrade Sousa Marinho – marcos.masm@live.com

Computação Forense e Pericia Digital

Instituto de Pós-Graduação – IPOG

Brasília, Distrito Federal, 24 de Maio de 2018

Resumo

A tecnologia e os meios de comunicação estão em constante evolução, os usuários podem se comunicar há longas distâncias, enviar fotos, arquivos e conversa com diversas pessoas pelo o mundo. Devido ao surgimento do Whatsapp, Telegram, Skype o objetivo da pesquisa é demonstrar que com a evolução da tecnologia também houve uma evolução dos crimes cibernéticos como: pornografia infanto-juvenil e o roubo de dados de computadores de usuários e de grandes corporações utilizando os malwares para estes fins. Utilizamos a metodologia da descrição utilizando os livros forenses e sites forenses para explicar cada ponto dos crimes cibernéticos estudados na pesquisa. Os malwares que são utilizados para invadir os computadores de usuários e de grandes corporações estão evoluindo também mesmo com a evolução das proteções como firewalls e dispositivos de detecção e prevenção de intrusões. As fontes de pesquisas indicam que a tecnologia deve continuar evoluindo e os cybers crimes também devem acompanhar esta evolução. Os resultados encontrados na pesquisa foram que os crimes cibernéticos estão sendo estudos a verificados e que possível de localizar e identificar os culpados de tais crimes ou até mesmo inocentar quem não cometeu os crimes.

Palavras-chave: **Pornografia. Pedofilia. Malwares. Vírus**.

Introdução

O estudo desse artigo está voltado para área de investigação forense onde podemos identificar crimes cometidos na internet, nos computadores, nos smarthphones, nos HDs externos, e até podemos identificar o autor desses crimes. A área que estuda a Computação Forense, área que busca ou tenta descobrir a verdade para não deixar impune quem comete crimes na área de tecnologia ou inocentar uma pessoa acusada injustamente.

Nesta área investigativa e muito falado de dois crimes: a pornografia infanto juvenil que é muito confundida com o termo pedofilia e o roubo de dados devido ao interesse em trabalhar na área investigativa o artigo foi desenvolvido para aprofundar o conhecimento desses dois crimes. Estamos em tempos de evolução e os crimes de pornografia e invasão e roubo de dados estão seguindo esta linha de evolução. Para entender melhor do que se trata estes crimes foi preciso investigar, analisar, buscar fontes forenses e estudar o que cada crime faz, quais são os seus métodos, características, diferenças, se tem algo especifico que é somente característica desse crime e outro motivo para investigar tais assuntos foram as referências bibliográficas, neste artigo foram utilizados referencias Brasileiras já que estes assuntos no Brasil são pouco falados e estudado e a grande maioria das pesquisas são utilizados referências internacionais. Nas pesquisas utilizadas entendemos como cada crime funciona, quais

são os seus procedimentos, a diferença entre a pornografia infanto juvenil e a pedofilia e como é feito a invasão e roubo de dados.

Um dos fatos importantes para saber se os crimes de pedofilia estão crescentes temos a reportagem do G1 elaborada por Bom dia SP e Globo News onde é reportado que houve várias operações da polícia civil para prender suspeitos por pedofilia em São Paulo e na região metropolitana as operações foram realizadas no dia 20/02/2018 terça feira na capital paulista e na região metropolitana, foram 48 prisões de suspeitos do crime de pedofilia. A operação começou as 04:30 a polícia civil cumpriu 49 mandados de busca e apreensão em 21 cidades da grande São Paulo. Os dados da operação mostram que 36 pessoas foram presas em flagrantes e um dos principais alvos era o funcionário de um buffet infantil. Entretanto o site Rede Brasil Atual no caderno de cidadania, para a reporte Sarah Fernandes, da RBA, com quatro casos de exploração sexual de crianças por hora o Brasil vai debater sobre a prevenção desse crime, o país sustenta um dos primeiros lugares no ranking internacional de casos de exploração sexual de crianças e adolescentes. No site G1 no caderno cidades do Distrito Federal através da matéria registrada por Marília Marques, demonstra através de denúncias e ocorrências que no DF em apenas um ano cresceu os casos de abuso sexual contra crianças e adolescentes e metade das denuncia foram de estupros, e as cidades que com o maior índice são Ceilândia e Samambaia, foram registrado no ano de 2017 um dos maiores números de casos, foram 1.479 casos em que crianças e adolescentes foram vítimas de abuso, 832 foram de estupros de vulnerável um termo para uma vítima menor de 14 anos, Ceilândia e Samambaia registraram juntos 455 casos as duas cidades com o maior índice de casos.

Outro crime que tem crescido de modo acelerado é o de invasão e roubo de dados de usuários e empresas, este tipo de ataque pode causa prejuízos catastróficos principalmente para empresas de pequeno, meio e grande porte algumas podem até ir à falência devido ao prejuízo causado por conta de algum serviço oferecido tenha ficado indisponível por algum tempo. O site Tec Mundo comentou alguns dos maiores roubos de dados da internet, a Playstation teve a sua live indisponível por tempo indeterminado devido a ataques de cracks que conseguiram derruba o serviço devido a uma ação que a Playstation estava movendo contra George Hotz um dos responsáveis de desbloquear o Playstation 3. Na época do ocorrido 77 milhões de usuários ficaram sem acesso a live da Sony e mais de 24 milhões de contas foram roubadas, um prejuízo da Sony que foi de 24 bilhões de dólares. Entretanto, a empresa Visa teve um prejuízo de 68 milhões de dólares devido a um vazamento de informações sigilosa da empresa TJX Companies, um grupo varejista, o ocorrido foi em dezembro de 2006, foram 94 milhões de informações de clientes vazaram nas mãos de desconhecidos em 2007 a empresa Visa calculava que os 68 milhões de dólares eram os prejuízos calculados e cerca de 138 milhões de reais na época. A empresa Google também informou que em dezembro de 2009 foi vítima de um ataque de cracks, o ataque partiu da China não foi somente a Google que reportou este ataque outras empresas como Adobe, Yahoo, Symantec também sofreram este ataque, foi um vazamento de informações e algumas contas de usuários foram acessados pelos os criminosos.

1 - Pedofilia

E uma doença que leva um indivíduo adulto a sentir atração sexual compulsivamente e obsessivamente por crianças e adolescentes. Um pedófilo geralmente tem uma vida comum e normal com emprego e um convívio social. Para ele se torna um criminoso deve usar o corpo da criança ou do adolescente para a sua

satisfação sexual não precisa ter o ato sexual ou a violência física. (CHILDHOOD, 2017).

"Segundo Delton Croce pedofilia e um desvio sexual caracterizado pela atração por crianças ou adolescentes sexualmente imaturos, com quais os portadores dão vazão ao erotismo pela pratica de obscenidades ou de atos libidinosos". (ELEUTÉRIO, MACHADO, 2011:117).

> É comum o uso incorreto do termo pedofilia, por exemplo, dizer que foram encontrados arquivos pedófilos em dispositivo de armazenamento computacional. Não é correto dizer que um arquivo e pedófilo e, o correto seria foram encontrados arquivos contendo pornografia infanto-juvenil ou abuso sexual de crianças/adolescentes. Pedófilo seria a pessoa que tem essa doença (DA SILVA ELEUTÉRIO, MACHADO, 2011:117).

A palavra pedofilia tem origem do grego e originariamente significa "amor por crianças", o termo pedofilia e denominado como um distúrbio de uma pessoa e, portanto, em regra pedofilia não é crime. O pedófilo só se torna criminoso no momento que há o ato sexual com criança ou adolescente para a sua satisfação sexual fazendo uso ou não de violência. Muitos pedófilos sente o desejo por crianças ou adolescentes porem nunca manifestaram este desejo por isso não pode ser considerado crime o desejo por crianças ou adolescentes. O pedófilo não precisa ser considerado um criminoso se não manifestar os seus desejos do mesmo jeito que um abusador de crianças não e necessariamente um pedófilo já que esta pessoa não sofre do distúrbio por crianças ou adolescentes neste caso o termo correto a se tratar é agressor sexual de crianças ou adolescentes. (ELEUTÉRIO, CASTRO POLASTRO, 2016:246).

Podemos mencionar que o termo pedofilia e também tratado como paedophilia erótica ou pedossexualidade e um termo muito antigo que tem pouco tempo incluído no dicionário da língua português. Para ambiente social e considerado um psicanalise na qual a atração sexual de um ente adulto está relacionada ou voltada para crianças ou adolescentes. Na concepção antes de uma pessoa se sentir atraído pelo o sexo oposto e com idade similar ele sente uma compulsão por jovens de idade inferior. (CASTRO, BULAWSKI, 2011: 54).

Para o psicanalista Sandro D' Amato Nogueira, a pedofilia trata- se de um "distúrbio de conduta sexual" que uma pessoa adulta nos termos da lei brasileira acima dos 18 anos sente uma grande atração por crianças ou adolescentes de caráter homossexual quando a envolvimentos com meninos ou heterossexual quando a envolvimentos com meninas que são crianças ou adolescentes. Para o médico Jim Hopper pesquisador da Faculdade de Medicina da universidade de Boston o termo pedofilia e uma doença que sofre uma variação de abuso sexual de menores, desde os homossexuais que procuram os meninos em locais como ruas, no lar familiar, escolas. (CASTRO, BULAWSKI, 2011: 55).

Existe outras definições que foge um pouco da divergência entre médicos e psicanalistas. Com base na Organização Mundial da Saúde pedofilia e uma preferência sexual por crianças, do gênero masculino ou feminino ou de crianças do sexo oposto ou igual que geralmente são pré-puberes ou não. (CASTRO, BULAWSKI, 2011: 56).

Como foi apresentado até o momento podemos entender que pedofilia não pertence ao termo jurídico, e sim um termo médico que é determinado por um distúrbio de comportamento a ser diagnosticado no caso concreto. Para a medicina e uma doença em espécie do gênero parafilia ou uma perversão para a psicanalise são transtornos para

uma estrutura psicopatológica que são os desvios do caráter para finalidades sexuais. (CASTRO, BULAWSKI, 2011: 57).

> Deve-se notar que não há necessidade da presença do ato sexual entre pedófilo e criança, eis que uma pessoa poderá, perfeitamente, ser considerada clinicamente como pedófila apenas pela presença de fantasias ou desejos sexuais em sua mente, desde que preenchidos certos criterios. Pelo que se pode extrair dos conceitos tecidos acima, busca-se organizar alguns critérios para o fim de que, assim, se possa amoldar determinado agente produtor de uma conduta ao conceito de pedófilo. Todavia, tal tarefa não é nada simples, haja vista que a pessoa portadora dessa perturbação sexual, frequentemente, não admite que seu comportamento fica alheio aos padrões normais da sociedade. Em grande parte das vezes, os sujeitos taxados como portadores de tal perversão negam veementemente este rótulo, relatam não estarem cometendo qualquer ilícito e alegam que, se praticaram algum ato, foi por motivação advinda da criança. (DE CASTRO, BULAWSKI, 2011: 57).

1.1- Diferença entre o termo exploração sexual infanto-juvenil e abuso sexual infanto-juvenil

Existe outros dois termos muito usados pela a sociedade, mas de maneira errada que seria a exploração sexual infanto-juvenil e o abuso sexual infanto-juvenil a diferença entre eles que a exploração sexual trata – se de um comercio onde temos o interesse financeiro, ou seja, crianças e adolescentes são utilizados em atividades exploradas comercialmente, e cada uma delas se tonar a mercadoria ou meio a uma troca. Neste ramo de exploração geralmente envolve muitas pessoas como o aliciador, o intermediário que comercializa o ato, além do próprio agressor, neste caso de exploração não podemos dizer que há uma prostituição infanto-juvenil já que a criança não detém do certo ou errado, sendo que as crianças e os adolescentes se torne as vítimas do crime. Outros meios de exploração sexual infanto-juvenil seriam com o turismo sexual, tráfico de pessoas e pornografia. (ELEUTÉRIO, POLASTRO, 2016:24)

O abuso sexual já um pouco diferente porque consiste em uma relação sexual com a criança ou adolescente com ou sem consentimento dela. Nos casos de abuso e comum acontece no âmbito familiar depois vem no âmbito extrafamiliar. (ELEUTÉRIO, POLASTRO, 2016:246).

> A violência sexual contra crianças talvez tenha permeado a humanidade, mas ganhou um grande impulso nas últimas décadas com o avanço da tecnologia principalmente com a internet, com a popularização dos equipamentos de caturra de imagens e também com a modernização dos equipamentos de captura de imagens e também com a modernização dos meios de comunicação. A internet permite o fácil acesso a pessoas de todo o mundo sem a necessidade de sair de casa, utilizando-se ferramentas de comunicação com possibilidade de “anonimato”, sendo fatores tentadores para o agressor. Além disso, com o avanço das comeras fotográficas, filmadoras e dos telefones celulares (smartphones), a obtenção de fotos e vídeos relacionado a pornografia infanto-juvenil se tornou cada vez mais fácil. Novas modalidades de violência sexual surgiram com o avanço da tecnologia como o groomong (assédio sexual pela internet) e o sexting (troca de fotos e vídeos de nudez, eróticas ou pornográficas pela internet). (ELEUTÉRIO, POLASTRO, 2016:247).

1.2- Modos de abordagem tradicional ou virtual

Antes da evolução das tecnologias, comunicações, internet, celulares, vídeo conferencias, e-mails os abusadores tinham um certo limite de regiões, o abusador geralmente se limitava a uma única região. A estratégia do abusador e tentar uma aproximação com a vítima a partir de presentes e doces, com isso ganhar a confiança da vítima, ou seja, da criança ou do adolescente, esta tática e mais usadas com pessoas que não tem parentesco com a vítima que não pertença ao ambiente familiar. Esta aproximação que e denominada de "Abordagem Tradicional" que levar dias, semanas, meses ou até mesmo anos, o abusador após começar a adquirir a confiança da vítima usa da estratégia de ser um "Amigo Secreto", que seriam aqueles que a vítima jamais deve contar e um segredo. Para a criança isso para ser normal, pode ser também uma brincadeira, uma aventura, uma liberdade de expressão, geralmente estas abordagens acontece nos shoppings, parquinhos resumindo em locais públicos para que a criança sinta – se confiante e até segura de conversa com o amigo secreto. Nas escolas também eram feitas estas abordagens porem devido a constante vigilância em relação a drogas e o álcool de alguma forma dificulta esta abordagem também. (ELEUTÉRIO, POLASTRO, 2016:249).

Nos casos onde os abusadores pertencem ao ambiente familiar, ou seja, são os parentes como tios, padrastos, primos, irmãos, esta aproximação a muito mais fácil já dentro deste ambiente a confiança e algo bem simples de conseguir devido à criança ter o convívio de que ele e seu parente mais velho e deve respeita – ló e obedecer. O abusador depois de ter adquirido a confiança da vítima o seu próximo passo e preparar um local para ficar sozinho com a vítima e este local vai se torna o ambiente ideal para os abusos. O abusador vai tentar manter o máximo possível os encontros com a vítima e cada encontro o abusador sempre vai presentear a vítima para manter o local em segredo, com o passar do tempo a criança vai adquirindo confiança do local e o abusador irar manter registro dos encontros como fotos e vídeos isso para eles e como se fosse troféus que futuramente iram ser postados nas redes sociais para que outros abusadores sexuais possam ver e admirar estes abusos. (ELEUTÉRIO, POLASTRO, 2016:249).

No começo desse século com a evolução das tecnologias como os computadores, Notebooks, Smartphones, Tabletes, a evolução dos softwares como WhatsApp, Skype, Telegran, SMS, MMS etc. Isso facilitou e abriu um novo meio dos abusadores sexuais terem uma aproximação das suas vítimas. Este tipo de aproximação e mais fácil para pessoas que o abusador não tem nem um contato não pode esquecer que a internet, as salas de bate papo, o Orkut que já está morto e o atual Facebook que possui um aplicativo de bate papo o "Facebook Messenger" possibilitam o anonimato ou até mesmo o abusador se esconder através de um perfil falso. Esta abordagem que foi denominada como "Abordagem Virtual" aqui o abusador irar se tornar o "amigo virtual", o abusador passar a enviar mensagens com algum conteúdo erótico para se identificar e também solicitar fotos e vídeos já na tentativa de estabelecer confiança e com o intuito de começar a marca os primeiros encontros pessoais, o abusador neste momento está usando uma serei de tecnologias principalmente as de comunicação online para atrair e ganhar confiança das suas vítimas. (ELEUTÉRIO, POLASTRO, 2016:249).

Um dos meios de comunicação mais comuns para as crianças e os adolescentes eram as salas de bate – papo logo os abusadores se espalhavam por essas salas em busca das vítimas perfeitas com o intuito de adquirir a confiança e muita das vezes os abusadores usam nomes falsos, perfis falsos, idades falsas para assim conquistar a

vítima e ter uma conversa mais privada no passar do tempo. Nos tempos atuais o meio mais comum de conversa com alguém e através de aplicativos fornecidos nos smartphones, aparelhos que hoje e muito comum crianças e adolescentes terem acesso e terem uma privacidade maior os tais aplicativos são o WhatsApp, Telegran e o Facebook Messenger. Estes aplicativos fornecem uma privacidade para os abusadores que se sentem confiantes e seguros para aturem e cometerem os abusos sexuais de forma fácil e agiu. (ELEUTÉRIO, POLASTRO, 2016:250).

Não e somente os aplicativos que facilitam a vida dos abusadores não podemos esquecer das redes sociais o então morto Orkut e o atual que está na moda e o mais utilizado no mundo inteiro o Facebook neles os abusadores podem criar perfis falsos para atrair as suas vítimas, nas redes sócias a vida do abusador geralmente e fácil pois nos perfis das suas vítimas já contém informações pessoais que os abusadores utilizam a seu favor como um meio de aproximação. (ELEUTÉRIO, POLASTRO, 2016:250).

> [...]. Utilizando perfis falsos, os abusadores tentam se aproximar das vítimas por esses meios, sendo que as redes sociais acabam trazendo mais uma grande vantagem ao abusador: o fato do perfil das vítimas conter informações preciosas sobre suas preferencias pessoas, como filmes, comidas e passeios favoritos. Os abusadores utilizam essas informações para se aproximarem das vítimas fingindo possuir gostos em comum. (ELEUTÉRIO, POLASTRO, 2016:250).

Não podemos deixar de mencionar que nem sempre os abusadores virtuais conseguem marca encontros com suas vítimas devido a distância ou alguma dificuldade encontrada no meio da conversa, aí nestes casos as vítimas são induzidas a fazerem fotos ou vídeos pornográficos para enviar aos abusadores que com este material já estão satisfeitos. (ELEUTÉRIO, POLASTRO, 2016:250).

1.3- O negócio de exploração sexual “A pedofilia”

O objetivo desse negócio e obter lucros, ou seja, ganhar o máximo possível de dinheiro com a exploração sexual de crianças muitas pessoas estão enganadas se acham que os abuso de crianças acontecem em isoladamente e independentes, existe muitos casos que os envolvidos não abusão das crianças e sim fazem parte de organizações criminosas que o objetivo e vender vídeos e fotos de abuso contra o menor esta rede está denominada como “Redes de Exploração Sexual de Crianças”. (ELEUTÉRIO, POLASTRO, 2016:251).

Estas redes criminosas estão voltadas para vender e trocar as matérias pornográficos que contém o conteúdo de abuso sexual da criança e do adolescente estes crimes não estão voltados somente aos abusos cometidos, e sim a outros crimes envolvidos alguns exemplos seriam trabalho escravo, sequestro, constrangimento ilegal e lavagem de dinheiro. Muitos abusadores utilizam tecnologia para compartilha este material como a rede (P2P) como o eMule, Kazaa, Shareaza e uTorrent ou eles utilizam as redes privadas como a dark net que está tudo criptografado isso dificulta a investigação e a identificação dos criminosos que se escondem muito bem. (ELEUTÉRIO, POLASTRO, 2016:252).

1.4- Legislação – crime infanto-juvenil

A pratica de possuir arquivos de pornografia envolvendo crianças ou adolescentes não era crime até a data de 25 de novembro de 2008, o exame mais comum na época era a verificação de compartilhamento ou a divulgação dessas matérias via

internet, nesta época era um dos crimes relatados no artigo 241 do Estatuto da Criança e do Adolescente: "Divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente." (ELEUTÉRIO, MACHADO, 2011:118).

Com a Lei 11.829, em 25 de novembro de 2008, conforme consta no artigo 241-B passou a ser crime a posso de arquivos dessa natureza. A Lei 241-B diz: " Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente. " (ELEUTÉRIO, MACHADO, 2011:118).

No Estatuto da Criança e da Adolescente criança são pessoas com idade até doze anos incompletos e adolescente e entre doze e dezoito anos de idade. Para outros países como a Europa e considerado menor de idade até os 18 anos de idade. (ELEUTÉRIO, POLASTRO, 2016:247).

Em meados do século XX o direito penal foi englobando uma diversidade de conceitos, abrangendo a sociologia, a medicina, a psicologia além de utilizar ao seu lado o direito processual e penitenciário. Estas disciplinas têm como oferece uma prevenção ou uma punição para tal crime cometido que o infanto-juvenil, estas prevenções e punições foram certamente acolhidos pela a legislação brasileira que trata a respeito dos direitos da criança e do adolescente e também seus deveres e garantias isso está claro na carta magna com a edição de leis especificas como o ECA (Estatuto da Criança e do Adolescente). (CASTRO, BULAWSKI, 2011: 52).

Com a evolução da proteção da criança e do adolescente as leis foram modificadas para tratar melhor o assunto de crime de pedofilia. Como mencionado no começo desse artigo pedofilia não é um crime e sim uma doença o que as leis brasileiras evoluíram foi colocar o crime de pedofilia associado a outros crimes um indivíduo que cometer o crime de pedofilia ou seja colocar em pratica os atos de abuso não pode alegar inimputabilidade penal de acordo com o artigo 26 da CP já que a pedofilia é uma parafilia e, como tal, denominadas doenças da vontade ou de uma personalidade antissocial. Vamos descrever melhor o que diz a CF (Constituição Federal), ECA (Estatuto da Criança e do Adolescente), CP (Código Penal). (ELEUTÉRIO, POLASTRO, 2016:254).

Para a CF e dever da família, da sociedade e do Estado assegurar os direitos das crianças e dos adolescentes, e a devida proteção de diversos tipos de violência isso e o que diz o art. 227, além disso este artigo diz sobre a lei que punira severamente o abuso a violência e a exploração sexual da criança e do adolescente, mas, a legislação infraconstitucional quem deve tratar a forma de punição para esses crimes. (ELEUTÉRIO, POLASTRO, 2016:254).

No CP trata do assunto estrupo houve uma nova redação dada pela Lei nº 10.015 de 2009 se um homem ou mulher praticar o crime de grave ameaça mediante a violência e a exploração sexual da criança e, ainda, se a vítima possuir entre quatorze e dezoito anos, a pena e aumentada. Se houve uma conjunção carnal, ou seja, uma relação sexual de forma concedida ou não ou qualquer outra forma libidinoso com uma pessoa cujo a idade e igual ou menor de quatorze anos o crime vai se enquadra no art. 217-A o estupro de vulnerável tendo a sua pena aumenta e se a conduta resulta em lesão corporal de natureza grave ou em morte. (ELEUTÉRIO, POLASTRO, 2016:254).

Pela as normas e leis do ECA ele trata diretamente sobre os crimes de pornografia infanto-juvenil seus artigos específicos sobre o assunto são os artigos 240 ao 241-E. No artigo 240 e regulamentado a punição de produção, por qualquer meio, de cenas de sexo explícito que tenha no seu material tenha um menor de idade. Quando dizemos qualquer meio de produção está sendo claro que seria filmes, fotos, qualquer registro que contenha uma criança ou adolescente. (ELEUTÉRIO, POLASTRO, 2016:254).

No artigo 241 do ECA trata da venda ou comercialização de pornografia que contenha criança ou adolescentes. O artigo 241-A trata da distribuição ou oferecer, trocar, distribuir, publicar ou divulgar imagens ou vídeos que contenham relação sexual de crianças ou adolescentes. (ELEUTÉRIO, POLASTRO, 2016:254).

Houve uma atualização da Lei 11.829/2008 que foi a lei 241-B que trata da posse de fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo crianças ou adolescentes. Este dispositivo e de grande importância no combate ao crime de infanto-juvenil antes dessa atualização o criminoso era só preso e processador pelo o crime se vende – se ou se compartilhas – se por qualquer meio o conteúdo ilegal. (ELEUTÉRIO, POLASTRO, 2016:255).

No Art. 241-C trata da simulação de participação de criança ou de adolescente em cenas de sexo explícito ou pornográfico, aqui não a necessidade de que o fato tenha acontecido na vida pois uma simulação já tipifica um crime. “O principal objetivo do legislador e desestimular a produção desse tipo de imagem, de forma a não fluência outras pessoas a buscarem esse tipo de conteúdo. (ELEUTÉRIO, POLASTRO, 2016:255).

O Art. 241-D tratar praticamente das crianças para o ECA e considerado criança com idade até 12 anos e de 12 até os 18 anos e considerado adolescentes. O crime tratado neste artigo e de aliciar, assediar ou constranger uma criança de qualquer forma buscando a pratica do ato de sexo. (ELEUTÉRIO, POLASTRO, 2016:255).

1.5- Como identificar ou caracterizar crime infanto-juvenil

Para caracterizar um crime de infanto-juvenil e preciso examinar as fotos ou vídeos apreendidos pelos os agentes federais no momento da busca e apreensão e identificar que neste material consta a participação de crianças ou adolescentes. Esta tarefa pode se torna um pouco dificultosa devido à grande dificuldade de identificar se aquele adolescente e menor de idade ou não, como os profissionais do sexo da indústria pornográfica se caracterizarem como adolescentes isso identifica uma das dificuldades. Hoje e bem fácil identificar uma criança no meio de material pornográfico, mas um adolescente principalmente do sexo feminino se torna um pouco mais difícil devido estarem mais desenvolvidas de corpo e aparentarem já adultas. (ELEUTÉRIO, MACHADO, 2011:118).

Os autores do livro observam que:

> [...] Na maioria dos exames dessa natureza, é comum existir dezenas ou centenas de arquivos suspeitos. Assim, diversos arquivos envolvendo crianças serão encontrados, e não será necessário se posicionar quanto aos duvidosos, pois a posse de arquivos contendo pornografia infanto-juvenil já foi materializada. Na pratica, se existirem dúvidas sobre a presença de crianças e ou adolescentes em fotos e vídeos, o perito não deve se posicionar. A análise forense deve ser sempre científica e não considerar aspectos subjetivos. Logo, nesses casos, recomenda – se que o laudo mencione e

> disponibilize tais arquivos, pois, com uma investigação mais profunda por parte da autoridade solicitante, talvez seja possível identificar a idade dos envolvidos por outra maneira, e não simplesmente pela análise do material multimídia (fotos e vídeos) encontrado. (DA SILVA ELEUTÉRIO, MACHADO, 2011:118).

1.6- Software de distribuição de arquivos infanto-juvenil

Os principais meios de distribuição e compartilhamento desses arquivos e via Internet, mensagens eletrônicas e programas que utilizam a tecnologia peer-to-peer (P2P). (ELEUTÉRIO, MACHADO, 2011:119).

Segundo Tanenbaum (2003 apud Desvendando a Computação Forense, 2011, p 119) diz que [...]

"[...] A tecnologia peer-to-peer geralmente e utilizada para estabelecer uma rede virtual de nós da rede (peers) têm responsabilidades equivalentes" (ELEUTÉRIO, MACHADO, 2011:119).

Os softwares mais utilizados no Brasil são o Kazaa e o eMule. Nos Estados Unidos o software de grande utilização e o LimeWire que está sendo cada vez mais divulgado no Brasil, mas, devido a uma decisão da justiça norte-americana o software LimeWire teve a sua distribuição foi proibida no dia 26/10/2010. Existe outros softwares como BitComet, Ares, Azureus Vuze, uTorrent que fazem também está distribuição de arquivos via Internet. (ELEUTÉRIO, MACHADO, 2011:119).

O eMule um dos softwares peer-to-peer mais utilizados no Brasil e no mundo quando um perito criminal federal em sua busca e apreensão se depara com este software e fundamental a análise do trafego e do seu compartilhamento. Quando o usuário instala o software eMule e começa a fazer o download dos arquivos automaticamente este mesmo arquivos que está sendo baixado vai ser compartilhado com outros usuários da rede eMule e muitos desses usuários não sabem que esta funcionalidade e automática. (ELEUTÉRIO, MACHADO, 2011:119).

> Para identificar os arquivos automaticamente compartilhados quando da execução do programa, o perito deve observar a configuração do programa. A pasta-padrão de compartilhamento tem o nome "Incoming" e é localizada no diretório de instalação do eMule. As versões mais recentes desse programa permitem o compartilhamento de diversas pastas – configuração que deve ser observada pelos peritos e que também pode ser recuperada a partir dos arquivos shareddir.dat, contido na pasta de configuração "Config" do programa. O eMule também armazena automaticamente os arquivos known.met, localizado na pasta de configuração do programa, um histórico geral sobre o compartilhamento de arquivos. Esse arquivo também deve ser analisado durante os exames forenses, a fim de identificar possíveis compartilhamentos anteriores de arquivos com conteúdo indevido. (DA SILVA ELEUTÉRIO, MACHADO, 2011:120).

O software Kazaa que também e utilizado para compartilhamento de arquivos como o eMule tem uma pasta padrão que já está definido no momento da instalação. Esta pasta pode ser alterada nas configurações pelo o usuário. A pasta padrão do Kazaa e a "My Shared Folder" Este software utiliza arquivos para o seu histórico como o data1024.dbb e data256.dbb e outras extensões.dbb. (ELEUTÉRIO, MACHADO, 2011:121).

O LimeWire era o líder de utilização dos Estados Unidos com seu uso cada vez mais crescendo no Brasil, quando o perito encontra em sua busca este software instalado

deve observar as subpastas *Incomplete, Saved* e *Shared* que por padrão e encontrado no diretório *Meus Documentos\LimeWire* ou algo similar. O perito deve observar também as suas configurações para detectar possíveis pastas e arquivos compartilhados. (ELEUTÉRIO, MACHADO, 2011:121).

Outra forma muito simples de divulgar os arquivos de pornografia infanto-juvenil e através do correio eletrônico (e-mails) que neste podem conter conteúdo em anexo. Assim o perito deve observar e analisar os softwares Microsoft Outlook e o Mozilla Thunderbird que muito usados pelos os usuários. Muitos usuários utilizam os serviços de correio eletrônico da internet como Hotmail, Gmail, Yahoo, e entre outros neste caso o perito deve analisar os arquivos temporários que são armazenados nas telas do WebMail. (ELEUTÉRIO, MACHADO, 2011:122).

1.7- Posse de material pornográfico infanto-juvenil

Muitos materiais de pornografia infanto-juvenil são armazenados em dispositivos tecnológicos como HDs, Pendriver, DVD, Nuvem. Os exames feitos por peritos federais com equipamentos tecnológicos servem para identificar os tais materiais e também identificar o dono desse material que em alguns casos não é própria pessoa que tinha posse desse conteúdo. Estes exames são tão precisos que levam a busca por arquivos ativos que foram enviados para a lixeira e até os apagados e que foram recuperados por técnicas de data carving. (ELEUTÉRIO, POLASTRO, 2016:255).

> [...] Existem casos nos quais foram encontrados arquivos dessa natureza que não foram armazenados nos dispositivos diretamente pelo usuário, como no caso das imagens temporárias dos navegadores de internet. Ou seja, o arquivo está armazenado no dispositivo, mas não foi salvo por ação direta do usuário. Como consequência disso pode surgir a dúvida: ‘ Isso e considerado posse? ’. Como sempre, ou quase sempre, a melhor reposta para essa pergunta e depende. Na verdade, depende principalmente em identificar se houve a intenção de ter acesso a esses arquivos ou não. (ELEUTÉRIO, POLASTRO, 2016:256).

> Vamos imaginar uma situação hipotética que não envolve computadores. Uma pessoa, ao checar a caixa de correio de sua, encontra uma fotografia impressa de pornografia infanto-juvenil. Essa pessoa, sem entender por que essa fotografia foi parar ali, a tasga em diversos pedaços, jogando tudo em sua lixeira. No entanto, um vizinho, sabendo da existência dessa fotografia na caixa de correio avisa a polícia que vai até a casa dessa pessoa e encontra tal fotografia rasgada na lixeira. Agora, imaginando uma situação semelhante no mundo da informática, uma pessoa poderia utilizar um software de compartilhamento P2P para buscar arquivos de pornografia adulta, fazendo o download de diversos arquivos. Ao visualizar tais arquivos, percebe que um deles e de pornografia infanto-juvenil e apaga-o imediatamente. No entanto, dias depois, a polícia vai até a casa dessa pessoa para investigar outro tipo crime e apreende o computador para a perícia em laboratórios. Ao realizar os exames, os peritos recuperam esse arquivo de pornografia infanto-juvenil que ora apagado. (ELEUTÉRIO, POLASTRO, 2016:256).

Na narrativa dos autores a pessoa teve a posse do material de pornografia infanto-juvenil porem não tinham a intenção de buscar ou ficar com elas, ou seja, não demostraram interesse pelo o material e nem intenção de usar o material isso tira a culpabilidade dessas pessoas desses tipos de crimes. A situações que o perito deve analisar se o criminoso tem ou não interesse no material. (ELEUTÉRIO, POLASTRO, 2016:256).

1.8- Pericia digital as técnicas de identificação de arquivos de pornografia infanto-juvenil

Para identificar os arquivos de pornografia infanto-juvenil algumas técnicas da computação forense, técnicas que sempre tende a evoluir para combater este tipo de crime são utilizados técnicas computacionais e ferramentas automatizadas que auxiliem na identificação desse conteúdo pornográfico. As técnicas usadas são: *uso do hash criptográfico, verificação dos nomes dos arquivos, detecção automática de nudez, detecção de vídeos de pornografia a partir da análise de áudio*. (ELEUTÉRIO, POLASTRO, 2016:258).

O hash criptográfico e usado para identificar se dois arquivos que tem o seu conteúdo idêntico são iguais esta técnica de hash permite que seja identificado se um arquivo está em dois dispositivos. Para fazer este tipo de análise e necessário calcular o hash dos dispositivos e compará-los ao original e quase possível afirmar com 100% de certeza que se trata do mesmo arquivo. No mundo tecnológico existem diferentes tipos de hash sendo os mais conhecidos são o MD5, o SHA-1, o SHA-256 e o SHA-512. (ELEUTÉRIO, POLASTRO, 2016:258).

A verificação dos nomes de arquivos e outra técnica utilizada para identificar arquivos de pornografias o que levou a uso dessa técnica seria o compartilhamento dos arquivos de pornografia infanto-juvenil através da internet. Muitos desses arquivos são compartilhados do tipo P2P para que seja encontrar estes arquivos os abusadores usam palavras chaves para efetuarem a busca e fazerem o download que uma vez feito o download o arquivo fica continho na máquina do usuário com os nomes das palavras chaves se não forem renomeados fica mais fácil de encontrar este tipo de arquivo. (ELEUTÉRIO, POLASTRO, 2016:259).

Babyj	Babyshivid	childlover	childporn	childsex	childugga	ddoggprn	Qqaazz	yamad
hassyfan	Kdquality	kidzilla	kingpass	mafiasex	pedo	pedofilia	Raygold	youngvideomodels
pedofilo	Pedoland	pedophile	pedophilia	pedophilie	pthc	ptsc	Reelkiddymov	

Autores: Mateus de Castro Polastro e Pedro Monteiro da Silva Eleutério 26 – expressões e palavras-chave mais utilizadas

Esta técnica e muita utilizada por fazer buscar rápidas isso não envolver operações demoradas com a leitura e disco já que os nomes podem ser obtidos nos sistemas de arquivos. (ELEUTÉRIO, POLASTRO, 2016:260).

Outra técnica utilizada seria a detecção automática de nudez que estuda há muito tempo e antigo a sua área de pesquisa este tema tem vários artigos e trabalhos científicos quem envolver o processamento de imagens principalmente para identificar o conteúdo adulto, são usadas diversas técnicas que envolver analise dos pixels que busca identificar a cor da pele nas imagens analisadas. (ELEUTÉRIO, POLASTRO, 2016:261).

> "[...] Nesse passo, as imagens podem ser trabalhadas nos espaços de cor do padrão RGB, sRGB, HSV, ou CMYK, entro outros. Alguns trabalhos focam no agrupamento dos pixels contendo cor de pele humana, a fim de formar regiões, de forma a identificar as partes do corpo humano. Outros trabalhos combinam as técnicas de geometria computacional para realizar a detecção de nudez humana de uma forma matemática, na tentativa de aprimorar os resultados, aumentando as taxas de detecção. Ainda existem trabalhos que montam histogramas para as imagens, a fim de identificar padrões de nudez.

> Alguns trabalhos utilizam um banco de dados de treinamento, que pode conter milhares de imagens catalogadas. Quando os arquivos a serem examinandos são vídeos, a maioria dos trabalhos de detecção de nudez publicados na leitura realiza a extração dos quadros, transformando os vídeos em uma sequência de imagens, que são trabalhadas com uso das técnicas de detecção desenvolvidas para esse fim. (ELEUTÉRIO, POLASTRO, 2016:261).

A última técnica a ser mencionada e a detecção de vídeos de pornografia a partir de identificação de padrões de movimento e da análise de áudio seriam detecção de movimentos para identificar os vídeos de pornografia. Esta técnica e utilizada para identificar no vídeo analisado os movimentos repetidos, já que numa relação sexual a movimentos repetidos por diversas vezes e também ela se encaixa com a técnica de detecção de áudio que busca melhora a detecção de forma geral assim sendo possível identificar a pornografia. (ELEUTÉRIO, POLASTRO, 2016:262).

> Um trabalho interessante divide o arquivo de vídeo em pequenos segmentos de tempo fixo, cirando vetores de movimento para cada quadro contido nesses segmentos. O algoritmo desenvolvido tenta detecta a repetição de movimentos em uma determinada frequência durante um intervalo de tempo especifico de 16 segundos, A partir dessa análise de repetição, o algoritmo desenvolvido consegue classificar os vídeos como “decente” ou “indecente”. (ELEUTÉRIO, POLASTRO, 2016:262).

> Pesquisadores da Irlanda também utilizam as mesmas estratégias para detecção de vídeos de pornografia, no caso, a segmentação do vídeo, a detecção de movimentos nos vídeos analisados e a posterior criação de vetores de movimentos que, quando analisados são capazes de identificar pornografia. Além disso, esse interessante trabalho também realiza a análise do áudio dos arquivos de vídeos. No caso, está técnica tenta identificar padrões de preterição também nos áudios extraídos dos arquivos de vídeo auxiliam na melhoria das taxas de detecção. (ELEUTÉRIO, POLASTRO, 2016:262).

1.9- Alguns casos de crimes sobre Pornografia infanto-juvenil

Preso homem com o maior material de pedofilia infantil encontrado pela polícia no DF. Homem de 45 anos de idade e preso por pedofilia Alessandro da Silva Santos ex-diretor de escola particular do Distrito Federal, acusado de estuprar crianças e adolescentes e de vender material de pornografia envolvendo menores. (DEBORA, LUCAS, 2017).

As investigações se iniciaram em 2015 quando Alessandro foi preso por receptação de veículos e nesta ação foi apreendido o seu celular pessoal e nele foi encontrado fotos de crianças nuas que levou a polícia civil do DF a começar uma nova investigação. (DEBORA, LUCAS, 2017).

Em maio de 2017 foi pedido a justiça uma busca apreensão na casa de Alessandro onde foi encontrar um HD externo portátil que nele havia material ilegal “fotos e vídeos” de meninos e este mesmo material era vendido para diversas pessoas nos estados do Brasil. Foi preso também um homem de 53 anos no mês de setembro em Belo Horizonte pela a Policia Civil de Minas Gerais ele era um dos compradores de Alessandro. (DEBORA, LUCAS, 2017).

Para conseguir o material Alessandro abordava meninos de classe mais humilde e oferecia dinheiro ou presentes. As crianças geralmente eram abordadas na rua e as convencia a passarem vídeos para ele em troca de lanches ou de dinheiro quantias

de 100 ou 150 reais afirmando o delegado chefe das investigações Rodrigo Viana. (DEBORA, LUCAS, 2017).

No HD externo foram encontradas fotos com datas de 1998, vítimas que hoje já são adultos que confirmaram para a polícia serem os adolescentes mostrados nas cenas, a polícia também tem os depoimentos de dois adolescentes que contaram ter sido estuprados pelo o acusado recentemente. (DEBORA, LUCAS, 2017).

Ação da PF contra pedofilia na web tem 13 presos no DF e 2 em GO

Foram presos pelo menos 15 homens em flagrante no dia 11 de agosto de 2016 pela a polícia federal na operação contra pedofilia infantil na internet. Os suspeitos estavam atualmente armazenado material pornográfico infantil e compartilhando o material pornográfico na web. Um dos suspeitos e servidor da Câmara dos Deputados que guarda mais de 300 HDs em casa. (GABRIEL, 2016).

Devido a iniciativa da PF foi iniciado uma investigação de crimes na web 1 ano antes porem devido à demora da justiça para iniciar a investigação e isso deu tempo suficiente para os suspeitos apagarem provas e mudarem os endereços e outra motivo da demora que a justiça precisava ter certeza que o material envolvido era pornografia infantil. (GABRIEL, 2016). Acesso em: 03 de out de 2017.

Os policiais cumpriram 35 mandados de apreensão, estes eram smartphones, pendrives, computadores e outros aparelhos usados para armazenamento, produção e divulgação de pornografia infantil e dentre dos suspeitos havia um grupo responsável por armazenar e distribuir o material ilício via p2P pela internet. (GABRIEL, 2016). Acesso em: 03 de out de 2017.

Além no estado do DF e de Goiás teve outros estados que a operação ocorreu as investigações iram apontar se os suspeitos tinham ligação com outros grupos de pedofilia, a indícios de que os suspeitos também usavam a "deep web" para anuncia o material.

2- Crime de invasão e roubo de dados

Uma grande quantidade de *vírus, spywares, worms, bots, cavalos de troia e vários outros*, conhecidos como *malwares*, são desenvolvidos todos os anos. A quantidade dessas pragas está aumentando a cada ano, todos os dias inúmeros programas de computador são desenvolvidos com estrita finalidade de buscar e achar uma vulnerabilidade para que ocorra a invasão a um computador ou até mesmo a uma rede completa de uma corporação. (BARÃO, VILAR, 2016:410).

As informações das corporações estão sendo um dos ativos que podem manter ou não a integridade dessas grandes corporações tornando estes ativos mais preocupantes. No passado não muito distante um ambiente de tecnologia da informação mal configurado com uma segurança da informação desfasada representava riscos grandes mesmo sendo confinados dentro dos limites da LAN. (TOLEDO, SOUZA:173).

2.1- Os malwares

Malwares são programas ou softwares maliciosos desenvolvidos com a finalidade de se infiltrar em um sistema computacional e realizar coleta de informações sem autorização podendo até causar dano a vítima. Quando estes *malwares* tem sucesso na invasão a um computador, eles podem ter acesso a diversos arquivos presentes no

computador invadido, ao tráfego de rede, ao teclado, ao microfone e até mesmo à webcam. (BARÃO, VILAR, 2016:410).

Os softwares maliciosos têm este termo genérico que engloba todos os tipos de programa desenvolvidos para executar ações maliciosas em um computador de uma corporação ou residencial, este tipo de software tem vários tipos de propósitos com ameaças reais (TOLEDO, SOUZA:173).

Existe muitos motivos para o desenvolvimento desses *malwares* com por exemplo "*obtenção de recursos financeiros, causas sociais/ideológicas, divulgação de informações confidenciais ou vandalismo também são adotadas por estes atacantes*". Os *malwares* fazem uso de técnicas para infectar os dispositivos com isso dificultando sua detecção por partes dos usuários ou as vítimas. As principais técnicas para efetuarem uma invasão são: (BARÃO, VILAR, 2016:411).

> **Exploração de Vulnerabilidades**: Muitos malwares possuem exploits utilizados para ganhar acesso através de falhas de segurança contidas em programas desatualizados no computador da vítima. (BARÃO, VILAR, 2016:411).
>
> **Auto-execução de mídias externas**: Funções como o autorun do Windows utilizadas por mídias ópticas e dispositivos removíveis como pendrives, são uma grande porta de entrada para software maliciosos, já que executam programas sem o consentimento do usuário e, via de regra, estão habilitadas por padrão. (BARÃO, VILAR, 2016:411).
>
> **Engenharia social**: E a manipulação psicológica empregada pelo atacante para persuadir a vítima e conduzi-la a execução do malware. Técnicas de engenharia social geralmente utilizam meios para despertar a curiosidade da vítima, abusar de sua ambição ou mesmo de sua inocência; (BARÃO, VILAR, 2016:411).
>
> **Execução consciente do usuário**: Em alguns casos, o usuário instala um malware propositalmente com a finalidade de obter informações de acesso sobre outros usuários que compartilham o uso da máquina. (BARÃO, VILAR, 2016:411).

2.2- O que a Lei fala sobre a criação e a distribuição do Malware

E crime com pena que pode chegar de 3 meses a 1 ano de detenção além de multa, conforme exposto no Art. 1º 154-A código que está presente no CP (Código Penal). (BARÃO, VILAR, 2016:411).

Classificação ou classes de malwares

Com a evolução de tempos da modernidade os malwares vem evoluindo também " em um exame pericial, a identificação previa da categoria a qual o malware pertence facilita a busca por vestígios e permite uma análise mais direcionada" com a intuito de evolução alguns malwares podem pertencer a mais de uma classe. Conheça os principais tipos: (BARÃO, VILAR, 2016:411-413).

Spyware: sua finalidade e coletar informações de suas vítimas que estão utilizando o computador sem elas saberem e geralmente este malware enviar as informações colidas para um servidor externo na internet. Adware: sua finalidade e exibir propagandas para os usuários, mas o seu desenvolvimento serve para coletar as

informações da navegação do usuário para que no futuro possa oferecer produtos de acordo com a navegação do usuário.

ScreenLogger: sua finalidade e de captura de telas, este malware monitora a navegação do usuário quando o usuário entra numa página de internet banking ele e ativado assim tentar capturar o login e senha dos usuários.

Keylogger: sua finalidade e de captura as teclas digitas pelo o usuário, depois da captura ele converte em arquivos codificados com o intuito de dificultar uma perícia forense.

Sniffers: sua finalidade e de capturar os dados que são trafegados na placa de rede geralmente estes Sniffers são utilizados por administradores de redes para testar ou corrigir eventuais erros na rede.

Backdoor: sua finalidade server para a pós invasão ou um ataque bem-sucedido, ele serve para garantir o acesso posterior ao invasor, ele permite execução de comandos no sistema local.

Worm: sua finalidade e se propagar ou se espalhar por uma rede, infectando milhares de computadores, ele faz uma exploração atrás de vulnerabilidades presentes em programas ou serviços de rede para ganhar acesso.

Outro estudo diz que Worm e um malware que pode se propagar automaticamente ou seja sozinho por meio de redes de corporações enviando muitas copias de si mesmo a outros computadores conectados a estas redes. Eles exploram as vulnerabilidades para ter acesso aos computadores que estão conectados a esta rede. (TOLEDO, SOUZA:173)

Bot: sua finalidade e receber comandos externos após a infecção nas maquinas ele e muito semelhante ao Worm e o Backdoor. Devido a possibilidade de receber comandos externos o tonar um bot, se um hacker tiver vários bots ao seu comando e gerado um novo ataque que é chamado de DDOS (Negação de Serviço).

Cavalo de troia: sua finalidade e tentar abrir e deixar uma porta aberta para entrada de outros malwares, ele e conhecido também por trojan. Fora esta finalidade as outros são quase inofensivas.

Cavalo de troia segundo Brian, James e George são programas criados para contar a segurança de um computador mais com algum tipo de disfarce como algo bom. O termo cavalo de troia vem de Roma e este malware não pode ser executado sozinho precisa de uma ajuda do usuário para que cumpra o seu destino, na área da computação existe três tipos de cavalos de troias: "*Programa de cavalo de troia, Código-fonte troiano, Binários troianos*". (HATCH, LEE e KURTZ, 2003:194)

Vírus: sua finalidade e de se copiar e espalhar a infecção por vários arquivos ou programas presentes no computador, uma diferença que ele precisa ser ativado para começar a funcionar já que não faz uso de vulnerabilidades no computador da vítima.

Uma outra definição de vírus seria como um binário com uma independência do computador ele pode ser alojar ou não na máquina para ser executado quando alojado

ele infectada os arquivos binários e isso depende do arquivo hospedeiro ou seu meio ele serve como um cliente de correio isso faz com que ele possa voltar e continuar a infecção até o processo esteja terminado. (MELO, 2009:10).

2.3- O que fazer quando há suspeita de software malicioso

Quando há uma suspeita de um software instalado no computador na qual ele possa executar funções secundarias e maliciosas sem conhecimento do usuário o perito que pode ser tanto particular como o oficial tem que buscar evidencias acerca do comportamento do software neste caso deve tentar responder estes 5 procedimentos: (BARÃO, VILAR, 2016:414).

- Analisar: se o software em questão envia informações a ambientes externos não previstos em sua documentação original;
- Averiguar: se o programa realiza download de executáveis ou plug-ins de sites não autorizados na documentação do software.
- Determinar: se as assinaturas dos arquivos binários que compõe o software correspondem as mesmas assinaturas dos arquivos binários após uma nova instalação, pois o software analisado pode executar funções secundarias maliciosas por conta de uma infecção por vírus;
- Verificar: se o programa suspeito registra as teclas digitadas em outras aplicações ou armazena capturas de tela em condições não autorizadas;
- Identificar: a existência de portas TCP/UDP abertas pelo programa que não estão autorizadas

2.4- Os ataques usando os malwares

Quando há um ataque a um computador ou a infraestrutura de redes que envolvam softwares malicioso para obtenção de acesso este ambiente já está comprometido e contaminado pelo o malware, neste momento deve começar um exame em busca de vestígios que determine o objetivo do ataque. Este exame e chamado de "*post-mortem*" que resume a atividade do malware e os efeitos após a execução alguns procedimentos que fazem parte do escopo da análise de malware são (BARÃO, VILAR, 2016:414).

- Identificar o (s) software (s) que possivelmente contribuíram para o sucesso do ataque; (BARÃO, VILAR, 2016:414).
- Verificar se existem portas abertas associadas aos programas em análise no (s) bost (s) ou servidor (es) presentes no ambiente periciado; (BARÃO, VILAR, 2016:414).
- Averiguar a existência de conexões reversas relacionadas aos softwares suspeitos (técnica muito utilizada para burlar elementos de segurança como firewalls, proxies ou IDS). (BARÃO, VILAR, 2016:414).
- Analisar nos logs do sistema operacional em busca de usuários criados pelos programas em análise. (BARÃO, VILAR, 2016:414).
- Determinar quais maquinas e arquivos foram afetados pelo (s) malware (s). (BARÃO, VILAR, 2016:414).

2.5- Os malwares com os elementos secundários para execução

Neste momento o software em si não e mais o principal objetivo da análise ele vai atuar como provedor adicional de informações que não seriam obtidas através dos meios convencionais. Os malwares atuais são muito semelhantes aos spywares que capturam teclas digitadas pelo o usuário e as imagens exibidas no monitor da vítima

com o intuito de coletar as informações valiosas. As atividades executadas para este tipo de análise são: (BARÃO, VILAR, 2016:415).

- “Identificar a presença do malware e o local no qual se encontra armazenado; ” (BARÃO, VILAR, 2016:415).
- “Buscar os arquivos criados pelo malware, decodifica-los e interpreta – los; ” (BARÃO, VILAR, 2016:415).
- “Verificar se o malware não é o elemento responsável pela pratica criminosa presente no dispositivo computacional examinado; ” (BARÃO, VILAR, 2016:415).

2.6- Tipos de análise de malwares

Estudar a evolução de cada malware e uma tarefa muito difícil devido a envolver um grande número de ferramentas e técnicas para descobrir o quais atividades maliciosas e prejudiciais são executadas pelo o software em questão. Existe dois tipos de analise que a literatura especializada usa que seria a análise estática e a análise dinâmica. (BARÃO, VILAR, 2016:415).

2.7- O que é análise estática

Esta analise usa de todas as formas possíveis para obter o maior número de informações sobre o malware, mas sem executá-lo uso da técnica de *strings* do malware ou a identificação de *APIs* são exemplos alguns dos procedimentos adotados por esta análise. Esta analise ainda e subdivida em análise estática básica e análise estática avançada. (BARÃO, VILAR, 2016:415).

Analise estática básica: e o exame com auxílio de ferramentas especificas, mas sem analisar as instruções do código binário. A análise de *binário, strings, PE32* são exemplos de técnicas da análise estática básica, ela pode promover informações de funcionalidades maliciosas do software sendo somente um pouco eficiente em malwares mais complexos. (BARÃO, VILAR, 2016:416).

Analise estática avançada: esta analise usa a engenharia reversa para desmontar o software e assim podendo examinar as instruções pertencentes ao arquivo binário uma vantagem e de examinar as instruções que serão executadas na CPU está analise permite compreender exatamente o que o software faz. Uma desvantagem e a escassez de ferramentas eficientes que automatizem o processo de desopilação isso faz que o software volte a linguagem de alto nível. (BARÃO, VILAR, 2016:416).

2.8- O que é analise dinâmica

Esta analise consistir em analisar o software malicioso em execução, ou seja, ele deve estar rodando em HD, carregado em memória e consumido recursos da CPU aqui são examinados o comportamento do software como as alterações feitas no SO, nos arquivos do HD e da rede. Este tipo de análise deve ser feito em um ambiente controlado devido a importância de analisar as instruções em linguagem de montagem presentes no arquivo binário em tempo real na sua execução com uso de depuradores. Esta análise e dividia também e subdividida em dois níveis. (BARÃO, VILAR, 2016:416).

Analise dinâmica básica: Consiste em observação do software malicioso em um ambiente computacional após a sua execução. O seu foco e mais comportamental, verificando quais alterações serão feitas pelo o malware durante a sua execução na máquina de teste, mas aqui não faz a depuração das instruções de baixo nível em tempo de execução. (BARÃO, VILAR, 2016:416).

Analise dinâmica avançada: é utilizado um depurador para examinar cada instrução aplicada pelo software em tempo de execução e uma análise completa devido a esta técnica e possível colher o maior número de informações possíveis do malware. Se a análise básica não funcionar o próximo passo e fazer a análise avançada. (BARÃO, VILAR, 2016:417).

Sistemas para a prevenção contra a invasão de computadores

Para inibir ou prevenir qualquer tipo de invasão ou contaminação a um computador ou até mesmo uma rede de computadores são usados alguns softwares como firewall, sistemas de detecção de intrusão, antivírus, VPNs etc. (SANTOS, BARCELOS, 2016:376).

Os sistemas de detecção de intrusão são uma combinação de hardware e software com a função de monitorar as atividades relacionadas à rede ou sistema em busca de atividades que não tem a devido autorização ou estão fazendo uma violação das políticas de segurança de uma corporação. (SANTOS, BARCELOS, 2016:376).

Existe um modelo conceitual chamado de CIDF (*Common Intrusion Detection Framework*) que foi proposto para explicar o que seria o IDS (*Instrusion Detection System*): (SANTOS, BARCELOS, 2016:377).

- **Gerador de Eventos (E-boxes)**: cria os eventos a partir do monitoramento do ambiente protegido. (SANTOS, BARCELOS, 2016:377).
- **Analisador de Eventos (A-boxes)**: recebe informações, realiza análise e envia o resultado para outros componentes; (SANTOS, BARCELOS, 2016:377).
- **Base de dados de Eventos (D-boxes)**: armazena os eventos e resultados processados; (SANTOS, BARCELOS, 2016:377).
- **Unidade de Resposta (R-boxes)**: responsável pelas ações, como por exemplo, finalizar um processo, reiniciar uma conexão e realizar notificações. (SANTOS, BARCELOS, 2016:377).

Existe outro modelo desenvolvido para definir uma linguagem de troca de informações entre os componentes, chamado CISL (*Common Intrusion Specification Languagem*), com utilização de autenticação e sistemas criptográficos. (SANTOS, BARCELOS, 2016:377).

Os IDS têm duas principais formas de atuação: baseado em rede e host. Os IDS baseados em rede são colocados estrategicamente para monitorar qualquer padrão incomum no trafego de rede como assinaturas conhecidas e comportamentos esperados, quando a uma identificação de um ataque ou um comportamento anormal e gerado um alerta que e emitido para o administrador da rede ou até mesmo tomadas contramedidas, entretanto de forma reativa. (SANTOS, BARCELOS, 2016:377).

2.9- Diferença entre IDS, firewall e IPS

Os IDS têm como função fazer um monitoramento analisando ou identificando comportamentos inesperados na rede que podem trazer algo prejudicial como ataques, varreduras; com estes comportamentos serão gerados alertas. (SANTOS, BARCELOS, 2016:378).

O *firewall* já atua como um filtro para o acesso a rede através de regras, que vai ajudar a prevenir os ataques que utilizem conexões que por ele podem passar. (SANTOS, BARCELOS, 2016:378).

Os IPSs (*Instrusion Prevention Systems*) já respondem automaticamente as ameaças que estão sendo geradas na rede, fazendo o encerramento de conexões, reprogramando o firewall para que ele possa fazer o bloqueio da ameaça. (SANTOS, BARCELOS, 2016:378).

Conclusão

Devido a evolução da tecnologia e das telecomunicações, há uma facilidade de se comunicar com outras pessoas em diversos lugares do mundo inteiro compartilhar arquivos, fotos, documentos, vídeos etc. Isso facilitou também a evolução dos cyber-crimes facilitando o compartilhamento de conteúdo pornográficos envolvendo crianças e adolescentes, a contaminação e compartilhamento de *malwares* que em milésimos de segundos podem se espalhar e infectar uma grande quantidade de equipamentos de tecnologia, de computadores até mesmo um simples smartphone. As técnicas usadas pelos criminosos estão e uma evolução constante obrigando a partes judiciarias também evoluírem no mesmo ritmo; uma das evoluções foi identificar e explicar a diferença entre pedofilia e os abusadores. Pedofilia é uma doença comprovada cientificamente com várias definições e os abusadores são pessoas que cometem crimes de pornografia infanto-juvenil com crianças e adolescentes e usam como desculpa a pedofilia que é uma doença para justificarem o seu crime. Outra evolução é conseguir recuperar arquivos apagados quando deletados pelos criminosos e analise, classificações dos *malwares* feita pela à justiça com esta evolução de análise é possível saber e identificar o autor o local que foi enviado ou postado o conteúdo.

Referências

BARÃO, Rafael Eduardo; VILAR, Gustavo Pinto. **Tratado de Computação Forense:** Capítulo 12 – Exames em Malwares. Millennium Editora, 2016.

CASTRO, Joelíria Vey; BULAWSKI, Cláudio Maldaner. **O PERFIL DO PEDÓFILO: UMA ABORDAGEM DA REALIDADE BRASILEIRA.** v. 6, 2011. Disponível em: http://www.ibccrim.org.br/site/revistaLiberdades/_pdf/06/integra.pdf#page=52. Acesso em: 12 de dezembro. 2017.

CHILDHOOD, Pela a proteção da infância, 2017. Disponível em: http://www.childhood.org.br/entenda-a-questao/perguntas-mais-frequentes. Acesso em: 09 de outubro. 2017.

ELEUTÉRIO, Pedro Monteiro; MACHADO, Marcio Pereira. **Desvendando a computação forense**. Novatec Editora, 2011.

HATCH, Brian; B. LEE, James; KURTZ, George. **Segurança contra Hackers Linux**. 2. ed. São Paulo: Futura, 2003.

MELO, Sandro. **Computação Forense com Software Livre**: Conceitos, técnicas, ferramentas e estudos de casos. 1. ed. Rio de Janeiro: Alta Books. 2009.

POLASTRO, Mateus; ELEUTÉRIO, Pedro Monteiro. **Tratado de Computação Forense:** Capítulo 7 – Exames Relacionados à Pornografia Infanto-Juvenil. Millennium Editora, 2016.

Referência: CORREIO BRAZILIENSE, Cidades-DF, 2017. Disponível em: http://www.correiobraziliense.com.br/app/noticia/cidades/2017/10/06/interna_cidadesdf,631789/ex-diretor-de-escola-acusado-estupro-e-venda-de-pornografia-infantil.shtml. Acesso em: 09 de out. 2017.

Referência: G1 GLOBO.COM, Distrito Federal, 2016. Disponível em: http://g1.globo.com/distrito-federal/noticia/2016/08/acao-da-pf-contra-pedofilia-na-web-tem-13-presos-no-df-e-2-em-go.html. Acesso em: 09 de outubro de 2017.

Referência: G1 GLOBO.COM, Distrito Federal, 2017. https://g1.globo.com/distrito-federal/noticia/em-um-ano-df-registra-14-mil-casos-de-abuso-sexual-contra-criancas-e-adolescentes.ghtml. Acesso em: 06 de março de 2018.

Referência: G1 GLOBO.COM, São Paulo, Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/operacao-da-policia-civil-prende-suspeitos-por-pedofilia-infantil-na-grande-sp.ghtml. Acesso em: 22 de fevereiro de 2018

Referência: REDE BRASIL ATUAL, Cidadania, 2017. Disponível: http://www.redebrasilatual.com.br/cidadania/2017/05/com-quatro-casos-de-exploracao-sexual-de-criancas-por-hora-brasil-debate-prevencao. Acesso em: 02 de fevereiro de 2018

Referência: TECMUNDO.COM.BR, Noticias, 2012. Disponível em: https://www.tecmundo.com.br/seguranca/26476-os-9-maiores-roubos-de-dados-da-internet.htm. Acesso em: 06 de março de 2018.

SANTOS, Luiz Fernando; BARCELOS, Leandro Bezerra. **Tratado de Computação Forense:** Capítulo 11 – Exames em Detecção de Intrusão. Millennium Editora, 2016.

TOLEDO, Alex Sander de Oliveira; SOUZA, Robert. **Pericia Forense Computacional – Analisa de Malware em Forense computacional utilizando de sistemas operacional GNU/Linux**. Disponível em: http://blog.newtonpaiva.br/pos/wp-content/uploads/2013/04/PDF-E5-SS28.pdf