12º **ENTEC – Encontro de Tecnologia: 16 de outubro a 29 de novembro de 2018**

MÉTODOS DE INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS

Lucas de Paiva Santos[1]; Paulo Ribeiro da Silva Junior[2]; Vinícius de Freitas Silva[3]; José Roberto de Almeida[4]
[1,2,3,4]*Universidade de Uberaba - UNIUBE, Uberaba - Minas Gerais*
lukkas202@gmail.com; jose.almeida@uniube.br

Resumo

A internet está presente praticamente no mundo todo e o que torna o seu uso importante é a informação disponível em toda sua “biblioteca”. Informações que geralmente são uteis e outras que são dispensáveis, pois não trazem nada de valor na vida de muitas pessoas.

Os crimes cibernéticos podem acontecer em rede pública, doméstica e até mesmo privada. O ponto mais importante para prevenir é tomar cuidados em aplicativos, *download* de documentos e a forma com que são usados. Por exemplo, acessar *a Internet Banking*em uma rede aberta, o risco é muito maior que em uma rede privada. Com isso, o ladrão pode conseguir acesso a sua conta e acabar se beneficiando do uso do dinheiro da mesma e, com isso, o usuário pode se tornar uma vítima de um crime cibernético.

E para investigação de todo esse crime, hoje há inúmeros estudos e técnicas que são aprofundados pela perícia forense. Atualmente esta área está crescendo muito no Brasil e no mundo, pois a cada vez que a *internet* cresce, a tendência dos crimes é aumentar. Logo, podemos deduzir que essa é uma área que vai precisar de muitos profissionais futuramente.

Com isso, devemos tomar alguns cuidados no que fazemos na internet. E, caso sejamos uma vítima, devemos procurar o órgão da Policia Federal para investigar o caso junto com a Perícia Forense.

Palavras-chave: Internet. Usuários. Informações. Perícia. Computador.

1 Introdução

Os crimes cibernéticos parecem não ser muito explorados. Mas acontece que eles estão, cada vez mais, presentes no mundo da *internet*.

Esses crimes podem acontecer em rede pública, privada ou doméstica, sendo que pode atingir apenas um usuário ou milhares.

Alguns exemplos que estão mais presentes nos noticiários de todo pais, como o ato de praticar *bullying*, chantagem, espionagem, plágios, entre outros. Mas temos outros que acontecem de forma mais oculta como envio de e-mails com vírus, roubo de informações confidenciais. Isso tudo resulta em crimes cibernéticos.

Em 2012 entraram em vigor as Leis 12.735 e 12.737 que têm como aplicação penal de normas específicas sobre os crimes digitais próprios, aqueles cometidos contra dados, informações ou sistemas, ao revés dos crimes digitais impróprios, quando os sistemas de informação apenas servem como meio para se praticar o delito (GAZETA DO POVO, 2013).

De acordo com o último relatório da *Norton Cyber Security* de 2017, o Brasil ocupa a segunda posição com maior número de crimes cibernéticos, perdendo apenas para a Austrália. Cerca de 62 milhões de brasileiros foram vítimas de *cibercrime*, e as perdas totalizaram um valor aproximado de 22 bilhões de dólares.

Mas o que devemos saber, são as atitudes das pessoas que acabam abrindo as portas para os bandidos praticarem esses crimes. Segundo o relatório, temos que:

- 59% dos usuários compartilham as senhas;
- 34% escrevem a informação em um pedaço de papel;
- 24% usam a mesma senha para todas as contas.

Com isso, devemos tomar mais cuidados com nossas informações para não sermos mais uma vítima desse crime.

2 Materiais e Métodos

Nos tempos atuais e, em uma visão globalizada, parte do mundo está em uma área intangível, porém acessada a todo instante por bilhões de pessoas espalhadas por todo o planeta. Com o passar dos anos, cada vez mais pessoas conseguem adquirir um computador ou algum outro dispositivo capaz de conectar em rede. Com isso, aumenta o número de usuários inexperientes e/ou inocentes sobre os possíveis atos criminais na área da informática, e surgem mais usuários a fim de cometer tais atos delituosos, visto as oportunidades que perduram ou até surgem a cada instante.

Faz-se necessário o desenvolvimento de uma área capaz de analisar com detalhes os métodos e mecanismos utilizados pelos criminosos, com o intuito de rastreá-los após cometerem tais atos, surgindo então a Perícia Computacional Forense. Segundo Freitas (2006, p.1), a perícia Forense utiliza de métodos científicos para identificar, preservar, analisar e documentar evidências localizadas em computadores e outros dispositivos eletrônicos.

A perícia é composta de quatro etapas básicas, as quais se complementam e trazem uma maior veracidade nas provas que serão posteriormente apresentadas pelo perito.

Inicialmente é feita a identificação das provas, variando o tipo de objeto de busca a ser analisado, pois cada crime possui suas especificidades e áreas onde ficam os rastros do delito, podendo variar entre imagens armazenadas no computador, histórico de navegação na *internet* ou arquivos que registram os processos em um servidor ou sistema operacional, chamados de "*log*". A complexidade da análise de cada tipo de prova também varia. Um exemplo é quando a perícia deverá ser feita em uma memória permanente de um computador (discos rígidos, *pen drives*, cartões de memória, entre outros), onde os dados podem ser deletados a qualquer momento pelo usuário. Sempre que um dado é armazenado em algum destes dispositivos, um rastro é deixado em partes inferiores da memória e não desaparece por completo, sendo apenas sobrescrito por outros arquivos com o tempo. O trabalho do perito, nesse caso, é buscar essas informações remanescentes. Porém, a dificuldade desse processo pode variar. Fatores como o tempo que esses dados foram deletados pelo suspeito, ou pelo tipo de sistema operacional instalado na máquina (alguns possuem particularidades perante o tratamento de alocação ou reciclagem de memória) são agravantes.

Após a identificação das provas, assim como em qualquer investigação, a preservação do material encontrado deve ser feita de maneira que não haja comprometimento sobre sua veracidade. Etiquetar todos os cabos e componentes do computador ou do dispositivo eletrônico, criar imagens do sistema investigado e guardar as evidências em sacos plásticos etiquetados (em casos de serem discos rígidos, devem ser usados sacos anti-estática para não comprometer os dados), entre outros métodos, as

maneiras de evitar que haja qualquer tipo de distúrbio na análise posterior. Assim previnem que haja uma substituição ou perda dos dados enquanto o material é manuseado ou transportado. De acordo com Queiroz e Vargas (2010, p.1), o perito deve tratar esse procedimento de forma rigorosa e com cuidado, não deixando que haja um comprometimento do caso, com a documentação de todo o processo de forma cronológica, aumentando mais ainda a sua veracidade e autenticidade ao apresentar no tribunal.

Por fim, o perito analisa tudo o que foi obtido previamente, dando um foco no material que mais condiz com o tipo da investigação, assim como foi relacionado nos parágrafos anteriores. Alguns tópicos podem ser facilmente respondidos após o processo, tais como qual sistema operacional o suspeito usava, quem estava utilizando o mesmo na hora do ato criminal ou quais arquivos foram excluídos por exemplo. As provas devem ser exatas e completas, não podendo haver brechas ou inconsistências, pois serão usadas na próxima e última etapa.

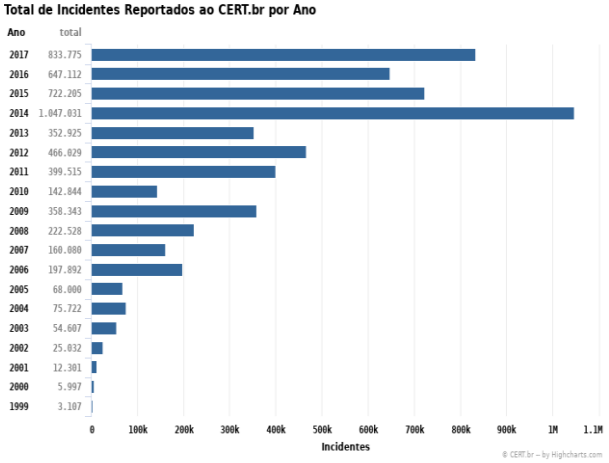
A apresentação da análise é a etapa final de um processo forense, na qual é apresentado um laudo pericial, apresentando um relatório técnico sobre todas as etapas anteriores, juntamente com um resultado. Montado de forma concisa, bem estruturado e detalhado, sem nenhum tipo de ambiguidade ou brecha para haver algum tipo de dúvida ou confusão. O relatório contém apenas os fatos que podem ser comprovados, pois será apresentado depois para a justiça, onde decidirão sobre o caso.

3 Resultados

Como citado anteriormente, o acesso a aparelhos com conexão com a *internet* está cada vez mais fácil. O número de usuários crescente faz com que aumente também em uma proporção diretamente proporcional é o número de possíveis vítimas de crimes nesse ambiente virtual. A profissão de Perícia Digital se mostra cada vez mais importante nos tempos atuais.

O Brasil, por exemplo, de acordo com dados recentes, ocupa o segundo lugar no ranking mundial de países com maiores números de crimes virtuais. De acordo com o portal “Centro de Estudos, Resposta e Tratamentos de Incidentes de Segurança no Brasil”, os números têm uma tendência a aumentar todos os anos, como pode ser notado na Figura 1.

Figura 1: Número de Crimes Virtuais Anualmente



Fonte: CETR.br (2018)

4 Discussão

No ano de 2017 houve mais de oitocentos mil incidentes virtuais, ou seja, um número grande para a atualidade tendo em vista que as empresas sempre tentam aumentar os níveis de segurança de seus produtos. De acordo com dados presentes em pesquisas recentes, o número de profissionais ativos nessa área, mesmo com sua existência passando os quarenta anos, ainda é baixo e isso é um fator preocupante.

Um fator agravante é o possível aumento na demanda dos profissionais, devido ao maior contato dos criminosos

com ferramentas antiforenses, que estão se tornando mais populares e de fácil obtenção, dificultando o trabalho de perícia, podendo até mesmo torná-lo impossível.

5 Conclusão

Por fim, nota-se a atual importância da especialização de profissionais na área de investigação digital, pois ela está sempre passando por um crescimento tanto no seu número de usuários, como também de dispositivos e de possíveis métodos que podem ser utilizados pelos criminosos. É de extrema importância que as empresas e o governo se voltem mais para esta área, investindo mais na profissionalização e ajudando afinal seus usuários.

Referências

2017 NORTON CYBER SECURITY INSIGHTS REPORT. **Symantec**, 20 jan. 2018. Disponível em: <https://us.norton.com/cyber-security-insights-2017/>. Acesso em 25 out. 2018.

A NOVA LEI DE CRIMES DIGITAIS. **Gazeta Do Povo**, 14 abr. 2013. Disponível em: < https://www.gazetadopovo.com.br/vida-publica/justica-direito/artigos/a-nova-lei-de-crimes-digitais-evf935c0vqjw7rh9b4cq75tfy/>. Acesso em 25 out. 2018.

FREITAS, Andrey Rodrigues. **Perícia forense aplicada à informática**. Rio de Janeiro: Brasport, 2006.

QUEIROZ, Claudemir & VARGAS, Raffael. **Investigação e Perícia forense computacional: certificações,**

Leis processuais e estudos de caso. Rio de Janeiro: Brasport, 2010.