Volume 4, número 1, ano 2021
REVISTA DE TECNOLOGIA INVEST

Artigo 4

UM ESTUDO SOBRE TÉCNICAS E MÉTODOS USADOS NA INVESTIGAÇÃO DE CRIMES VIRTUAIS

Ed Wilson Rodrigues Silva Júnior[1]
Jully Endyane dos Santos Guimarães[2]

RESUMO: Em tempos de pandemia não só no Brasil mas como no mundo, grande parte da sociedade tiveram que se adaptar e adotar home office, onde funcionários acessam a rede através da VPN e acesso remoto online para dar continuidade de seus afazeres já que não é possível atendimento presencial, com isso, muitas empresas sofreram ataques cibernéticos devido à falta de segurança em seus web services. O presente artigo tem como objetivo analisar os tipos de crimes cibernéticos que organizações e pessoas físicas sofrem durante a pandemia, ressaltar sobre os ataques contra a segurança da informação utilizando como metodologia a pesquisa bibliográfica e apresentar ferramentas que auxiliam na prevenção desses tipos de crimes.

Palavras-chave: Crimes cibernéticos, segurança da informação, softwares forenses.

ABSTRACT: In times of pandemic not only in Brazil but as in the world, much of society had to adapt and adopt home office, where employees access the network through VPN and remote access online to continue their business as it is not possible to face-to-face, with this, many companies have suffered cyber attacks due to the lack of security in their web services. This article aims to analyze the types of cybercrimes that organizations and individuals suffer during

[1] Doutorando em Computação Aplicada pela Universidade do Vale do Rio dos Sinos (Unisinos); Mestre em ensino de linguagens e seus códigos pelo Programa de Pós-Graduação Stricto Sensu em associação ampla entre a Universidade de Cuiabá-UNIC e o Instituto Federal de Educação, Ciência e Tecnologia do Estado de Mato Grosso-IFMT. Possui graduação em Sistemas de Informação pelo Centro Universitário de Várzea Grande, licenciatura em computação pelo Claretiano Centro Universitário e especialização em tecnologias na educação pela Universidade do Oeste Paulista. Tem experiência na área de ciência da computação, com ênfase em sistemas de computação, na educação profissionalizante e superior voltada para a área de tecnologia da informação e pesquisas em inovação, criatividade e metodologias de aprendizagem.
[2] Bacharel em Ciência da Computação pela Faculdade Invest de Ciências e Tecnologia.

the pandemic, highlight attacks against information security using bibliographic research as methodology and also present tools that help prevent these types of crimes.

Keywords: Cybercrime, information security, forensics softwares.

1. INTRODUÇÃO

A pandemia que se deu início no final de 2019 na China, causou milhares de mortes no Brasil e no mundo todo, o Coronavírus (Covid-19) tem assustado pessoas do mundo todo, porque é um vírus desconhecido com alta taxa de mortes, e é um momento muito delicado e desafiador para história da saúde pública.

Diante deste cenário, pessoas de má índole se aproveitam da situação para aplicar golpes nas redes sociais, enviando e-mails falsos, mensagens enganosas, links contaminados que após um clique pode causar um estrago muito grande, como perda de informações pessoais e para empresas podem até perder acesso aos seus sistemas.

Este artigo tem o objetivo de apresentar um estudo sobre os métodos e técnicas utilizadas nas investigações de crimes virtuais, utilizando como metodologia a pesquisa Bibliográfica obtida em livros, revistas, artigos científicos. E também tem como objetivo mostrar as organizações formas de prevenção contra os crimes virtuais e auxiliar usuários que devido a pandemia tiveram que adotar o home office.

2. REFERENCIAL TEÓRICO

2.1.TÉCNICAS E MÉTODOS USADOS NA INVESTIGAÇÃO DE CRIMES VIRTUAIS

Os crimes cibernéticos vêm crescendo a cada ano, e com a pandemia os crimes aumentaram muito. Ataques cibernéticos são aqueles praticados por qualquer dispositivo que tenha acesso a uma rede de internet. Alguns dos motivos são para roubo de informações, roubo de dados pessoais, de contas digitais, senhas e até mesmo passam falsa informação utilizando a engenharia social e a pessoa acaba acreditando e assim caindo em um típico golpe conhecido como crime virtual.

Os crimes virtuais conhecidos como o perigo da internet abrangem toda e qualquer atividade ilegal realizada com o uso da tecnologia, são realizados através de qualquer dispositivo que tenha acesso a uma rede de internet, praticados por cracker[3] com objetivo de roubo, pedofilia, assédio, crime contra a honra e injúria.

São crimes organizados, onde passam dias pensando em como aplicar o golpe e com quem ele irão aplicar, maioria de suas vítimas são idosos, os mais vulneráveis a cair nestes tipos de crimes, pois são pessoas com baixo nível de entendimento da tecnologia e por isto acabam clicando em links maliciosos, ofertas que aparecem com um designer cativante, sites que criam

[3] Cracker - Individuo com muito conhecimento e usa para cometer crimes digitais.

para simular outros sites de vendas, aplicam ofertas com preço em conta e assim chamam atenção das pessoas e acabando caindo em um crime virtual.

A vulnerabilidade não está somente em empresas, mais em todo o lugar. Aquele que não tiver um bom antivírus está apto a qualquer momento cair em um tipo de crime virtual através dos links maliciosos, a porta de entradas dos Adware e worms. Segundo Telles (2020, p.2):

> A vulnerabilidade das empresas ficou ainda maior devido ao acesso remoto dos sistemas via home office. As pessoas, muitas vezes, trabalham com um computador e também compartilham o uso do aparelho com outras pessoas da casa. Todo esse movimento se torna um risco para as redes das organizações.

Nestes casos, as falhas de privacidade se tornam uma grande fragilidade para os usuários, podendo colocar em risco sistemas inteiros de suas empresas. Estes problemas são provenientes, principalmente, de autenticação através de contas em redes sociais em sites não confiáveis, e navegação e fornecimento de dados a sistemas com padrões de segurança de fácil quebra, por exemplo.

Correções nestas falhas devem vir, principalmente, da preocupação de gestores em prover segurança cibernética para seus funcionários. Estruturação de redes confiáveis, uso de aparelhos dedicados ao trabalho e outros pontos viabilizam o trabalho remoto sem riscos aos envolvidos.

2.2.ATAQUES CIBERNÉTICOS: FUNCIONAMENTO E PROTEÇÃO

Os ataques de crackers vêm crescendo muito nos últimos anos e, sobretudo depois da pandemia, estão se tornando cada vez mais comuns. Segundo a Zscaler, só nas primeiras semanas de março, houve crescimento de 20% de golpes em relação a fevereiro, grande parte delas usando termos relacionados à COVID-19. Isso mostra que o novo Corona vírus não está apenas gerando ameaça para os sistemas de saúde de todo o mundo, mas também para os computadores e dispositivos de muitos usuários. (SANTOS, 2020).

A COVID-19 não está se apresentando somente com uma ameaça para os sistemas de saúde de todo o mundo, mas também para os computadores e dispositivos dos usuários. Segundo empresas de cibersegurança, criminosos estão se aproveitando da desinformação e temor com a doença para fazer vítimas em golpes. (WAKKA, 2020, p. 1)

Além de invasões em sistemas, mensagens falsas são disseminadas via e- mails, SMS ou WhatsApp tentando atrair vítimas por meio de promoções, descontos, ofertas ou prêmios, agora entra nessa soma pessoas mal-intencionadas que estão usando um assunto recorrente e de uma importância sem precedentes, para aplicar ataques.

Dentre as formas de ataque, o phishing[4] golpe que usa mecanismos tecnológicos, geralmente baseados em mensagens pode ser considerada a maneira mais eficaz que um criminoso tem de conseguir acesso a uma empresa, uma vez que o objetivo é enganar por e-

[4] Phishing – é a tentativa fraudulenta de obter informações confidenciais.

mail o destinatário, o fazendo acreditar que a mensagem é algo que ele deseja ou precisa, inserindo um link para acesso ou um arquivo para fazer download. O cracker dedica seu tempo pesquisando a fundo funcionários e a empresa que será seu alvo – quanto mais informações em mãos, maiores são as chances de sucesso.

De acordo com Santos (2020) existem duas formas de golpes deste tipo. O primeiro é o em massa ou, no qual todos são passíveis de serem alvo de um atacante, pois são mais genéricos e o foco é obter a maior quantidade de vítimas. São utilizadas promoções chamativas, oportunidades como cartão de crédito sem limites ou anuidade, alguma oportunidade de trabalho dos sonhos ou outras maneiras, porém todas partindo do princípio de instigar a curiosidade.

O segundo é o ataque direcionado, no qual o alvo costuma ser algum funcionário ou departamento específico. Nesse caso, o assunto descrito no material, seja e-mail, SMS ou por voz, tem como principal objetivo atrair e chegar até seu alvo, portanto os conteúdos geralmente são relevantes à área que se deseja obter informações. (SANTOS, 2020). Existem também formas de prevenção contra o crime virtual, alguns exemplos são:

- Não baixar nada de fonte desconhecida.
- Não clicar em links de e-mails recebidos de pessoas que você não conhece.
- Não fornecer senhas ou dados pessoais para pessoas estranhas ou até mesmo conhecida pois são confidenciais.
- Ter um antivírus poderoso para escanear seu sistema e remover arquivos perigosos como vírus, spyware[5], ransomware[6], entre outros.

Devemos, portanto, adotar hábitos seguros durante a navegação na internet evitar também sites não confiáveis.

2.3.SEGURANÇA DA INFORMAÇÃO APLICADA NO HOME OFFICE

Com a pandemia da COVID-19 empresas de vários segmentos de diversas partes do mundo têm adotado o home office como modelo de trabalho, porém é necessário realizar este processo de maneira segura para o ponto de vista empresarial.

Desse modo, estão sendo tomadas várias medidas, dentre elas, a essencial é a utilização de VPN (Virtual Private Network) a qual é uma das medidas fundamentais para as operações da empresa neste novo cenário. Pelo fato de impactar e influenciar em questões relacionadas com a segurança e disponibilidade segura das informações. (RODRIGUES, 2020).

Sempre há a possibilidade de vazamento de informações delicadas da empresa, por meio de vírus ou ataques no computador doméstico onde é realizado o trabalho e que, muitas vezes, conta com uma segurança menor que um sistema corporativo. Isso também pode se estender ao

[5]Spyware - é um tipo de programa automático intruso destinado a infiltrar-se em um sistema de computadores.
[6]Ransomware - é um tipo de software nocivo que restringe o acesso ao sistema infectado com uma espécie de bloqueio e cobra um resgate em criptomoedas para que o acesso possa ser restabelecido.

mundo físico se houver a perda ou furto de dispositivos com dados importantes, como pen drive e smartphones. (KENOBY, 2020).

E para prevenir um possível ataque ou invasão a rede é necessário seguir um protocolo de segurança que a empresa disponibiliza tais como:

- Não disponibilizar seu login de acesso à rede para desconhecido nem para qualquer outra pessoa, pois é de uso pessoal, após estar conectada à rede através da VPN (Virtual Private Network).
- Não acessar site de carácter duvidoso.
- Não baixar arquivos estranhos.
- Não clicar em mensagem ou links de phishing.
- Adotar alertas de novos logins para todos os serviços ativos.
- Quando for possível, ter um gerenciador de senhas para auxiliar na utilização de senhas não repetidas entre serviços.
- Não conectar pen drive ou HD's externos estes podem ser porta de entrada de infecções e devem ser evitados.
- Ter um bom antivírus na sua estação de trabalho auxilia a barrar a entrada desses invasores, evitando danos à rede virtual da sua empresa e até da sua própria residência.
- O usuário precisa estar atento ao incluir senhas para participação em sorteios, prêmios, bonificação de valores financeiros, vagas de emprego e temas relacionados ao corona vírus, pois nem sempre são confiáveis

2.4.TIPOS DE CRIMES CIBERNÉTICOS

Crime cibernético é uma atividade criminosa que tem como alvo ou faz uso de um computador, uma rede de computadores ou um dispositivo conectado em rede. Não todos, mas a maioria dos crimes cibernéticos é cometida por cibercriminosos ou crackers que querem ganhar dinheiro.

O crime cibernético é realizado por pessoas ou organizações. Alguns cibercriminosos são organizados, usam técnicas avançadas e são altamente capacitados em termos técnicos. Outros são crackers novatos. Raramente o crime cibernético visa danificar os computadores por outros motivos que não o lucro. Nesses casos, os motivos podem ser pessoais ou políticos. (KASPERSKY, 2020).

Podemos definir como ataque cibernético o uso de técnicas e sistemas voltados para o roubo de dados e a invasão de sistemas. Eles são direcionados tanto para empresas quanto para usuários domésticos, e podem causar vários tipos de prejuízos. Entre os mais comuns, podemos apontar:

- Fraude por e-mail e pela Internet conhecido como phishing.
- Fraude de identidades, quando informações pessoais são roubadas e usadas.
- Roubo de dados financeiros ou relacionados a pagamento de cartões.
- Roubo e venda de dados corporativos.
- Extorsão cibernética, que exige dinheiro para impedir o ataque ameaçado.
- Ataques de ransomware, um tipo de extorsão cibernética.

- Espionagem cibernética, quando crackers acessam dados do governo ou de uma empresa.
- A perda de informações privadas;
- O roubo de dados sigilosos;
- A alteração não autorizada de registros digitais;
- A indisponibilidade de sistemas e equipamentos tecnológicos.

Como se pode verificar nas descrições acima, esses são alguns exemplos de crimes cibernéticos.

2.5.TIPIFICAÇÃO DOS CRIMES CIBERNÉTICOS

Os crimes cibernéticos são tipificados por todos aqueles que são cometidos por meio da internet, são crimes que aumentaram a partir dos avanços tecnológicos que ocorrem na sociedade, uma vez que podem ser cometidos através de qualquer dispositivo que tenha acesso à internet (SILVA, p.8, 2019).

O crime virtual engloba todas as atividades criminosas realizadas por meio de computadores ou da internet. Podem ser empregados diversos métodos e ferramentas, tais como phishing, vírus, spyware, ransomware e engenharia social, geralmente com o objetivo de roubar dados pessoais ou praticar fraudes GLOBAL NETWORKS, (2020).

2.6.OS TIPOS MAIS COMUNS DE ATAQUES CIBERNÉTICOS:

De acordo com a Intnet (2019), - cujas informações foram a seguir transcritas na íntegra -, todo usuário de serviços web pode ser atingido por um ataque cibernético, os tipos mais comuns de ataques são:

- **Malware** - O malware, também chamado de vírus, é um tipo de software de computador malicioso. Ele pode ser criado para prejudicar a performance do aparelho ou executar operações não solicitadas pelo usuário.

Essa é a forma de ataque mais tradicional existente. Malwares podem ser propagados por meio de programas ilegais, documentos infectados ou e-mails falsos. Uma vez instalado, ele se ocultará no aparelho do usuário. Desse modo, poderá manter-se ativo sem que uma ferramenta de segurança o detecte.

- **Ransomwares** - O ransomware ganhou popularidade e destaque nos últimos anos. Esse tipo de ameaça digital pode causar um grande prejuízo ao usuário. Isso ocorre, pois, os danos ocasionados por esse tipo de ataque cibernético vão da interrupção de rotinas de trabalho à perda de informações estratégicas.

Esse tipo de ataque criptografa todos os dados do aparelho. O acesso passará a ser liberado apenas após o pagamento de um resgate. Caso contrário, o usuário não terá como ler e modificar os seus principais arquivos.

- **Phishing** - O phishing é a forma mais tradicional de roubo de dados. Nesse caso, o usuário é direcionado a uma página falsa. Ela tem como objetivo roubar informações como senhas de e-mail e contas de bancos.

Geralmente esse tipo de ataque é feito com direcionamento para o seu alvo. A partir de técnicas de engenharia social, se buscará identificar a melhor forma de direcionar o usuário para uma página falsa. Assim, as chances de roubar as informações serão muito maiores.

- **Ataque DDOS** - Distributed Denial of Service (ou negação de serviço distribuída, em português), o DDoS é um ataque que pode prejudicar o acesso a vários serviços web de uma única vez. Ele geralmente é direcionado às páginas grandes, por exemplo, a de serviços de streaming, como a Netflix, ou mesmo de jogos digitais. Porém, não raro o DDoS também atinge (indiretamente e diretamente) serviços web pequenos.

Esse tipo de ataque cibernético utiliza de um grande número de aparelhos infectados por um malware para direcionar um fluxo elevado de pacotes de dados para um único IP. Desse modo, o servidor ficará sobrecarregado e inacessível pelo prazo em que o ataque acontecer: incapaz de identificar quais são os pacotes legítimos ou não, o servidor não atenderá às requisições existentes. (INTNET, 2020).

3. RESULTADOS E DISCUSSÕES

Os números de crimes cibernéticos cresceram tanto do início do ano, devido ao isolamento social o consumo da internet cresceu muito e com isso milhares de brasileiros teve algum tipo de problema como ataques cibernéticos, e nesta época de pandemia, quando muitas pessoas estão usando a internet para realizar operações bancárias, trabalhar e fazer compras, todo cuidado é pouco. Segundo Santos (2020, p.2):

> Todo cuidado é pouco. O ser humano é o elo mais fraco da segurança da informação e é preciso ter muita cautela com qualquer tipo de comunicação oriundas de sites, grupos de conversas e redes sociais. A dica de ouro que sempre costumo dar é: sempre desconfie de tudo!

A implementação de home office nas empresas pode e deve deixar lições valiosas para o futuro. Entre elas, sem dúvida, está o uso da tecnologia para um trabalho mais colaborativo, inteligente e produtivo, sem perder de vista a qualidade e segurança do serviço entregue. É hora de aprender com o momento e aplicar as lições mais importantes para evoluirmos rapidamente. As empresas podem e devem continuar na ativa, mas sempre priorizando a seguridade dos negócios e, claro, das pessoas. (ARAUJO, 2020).

Esperamos que a mensagem principal presente nesse artigo possa atingir um número grande de pessoas que possuem baixo nível de conhecimento da internet, para que possam auxiliá-las a não cair nesses tipos de golpes e crimes virtuais, sabendo que o aumento deles durante a pandemia foi gigantesco e também seguir os protocolos de segurança da informação para evitar esse tipo de ataques.

3.1.SOFTWARES FORENSES QUE AUXILIAM NA INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS.

No processo de investigação forense existem diferentes tipos de tarefas de realização essencial. Além das ações de confeccionar cópias de segurança de evidências, documentação, pesquisa e outros processos como esses, o investigador precisa de softwares[7] específicos para realizar tarefas forenses. Como requisitos destas ferramentas podem ser citadas a garantia de acesso a informações que possam ter sido excluídas ou possam estar escondidas, além do manejo de arquivos criptografados e armazenados em espaços não-alocados (LAWRENCE, 2009).

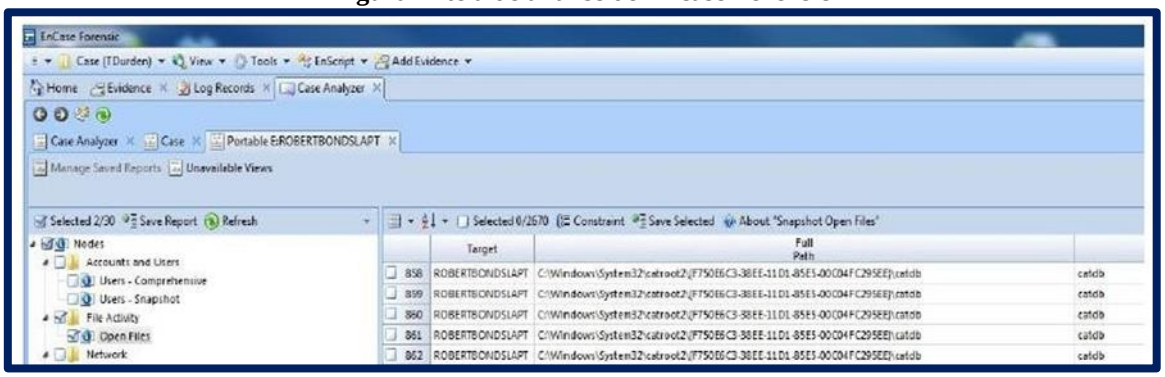
A procura por softwares de exclusão de rastros tem crescido ao longo dos anos. Muitos softwares disponíveis são capazes de zerar e sobrescrever arquivos de dados. Sendo assim, essas ferramentas utilizam múltiplos processos de escritas e consequentemente qualquer tentativa de recuperação se torna impraticável ou até impossível de ser realizada (KESLER, 2007).

Entretanto, os softwares utilizados pelos criminosos para limpar seus rastros não são perfeitos e podem criar uma trilha de vestígios adicionais (CARVEY, 2007). Além disso, muitas destas ferramentas não cumprem tudo o que prometem fazer e frequentemente deixam para trás rastros como nome e tamanho do arquivo, data de criação e exclusão dos arquivos.

3.2.ENCASE FORENSIC

EnCase Forensic é uma das ferramentas mais utilizadas pelos peritos forenses na busca por evidências em um ato criminoso. A ferramenta tem a capacidade de realizar análise simultânea de múltiplas máquinas em uma rede LAN/WAN em nível de disco e memória, analisar múltiplas plataformas, identificar dlls (Dynamic-Link Library) injetadas no sistema, identificar processos ocultos entre outros.

Figura 1- tela de análise do Encase Forensic



Fonte: Guidance Software ([199-] e).

A ferramenta EnCase é uma das mais completas da perícia forense computacional porque ela tem a padronização de laudos periciais, organização do banco de dados ligado as evidências, fornece senha ou as quebras e também recupera arquivos excluídos, Sendo possível a realização de análise de evidências através do Encase Forensic, pode-se determinar se um

[7]Software -Termo técnico para representar conteúdos, produtos ou aplicações em formato digital.

crime pode ou não ter sido cometido. Alguns recursos do processador de evidências do Encase Forensic:

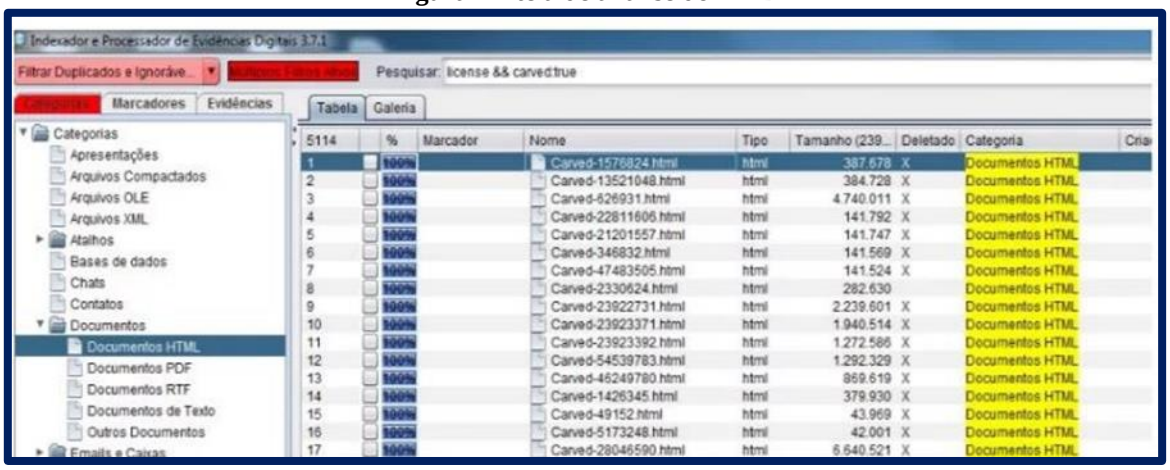
- Realiza análise de arquivos protegidos utilizando-se de um módulo analisador de criptografia, detecta automaticamente informações do sistema operacional; possui um módulo que analisa os arquivos da lixeira, arquivos de log e transações MFT (Master File Table), Possui um localizador e analisador de conversas de bate-papo na internet registradas no sistema, possui um analisador de logs de eventos e informações de login.

- A ferramenta oferece ainda ao usuário, principalmente, uma análise avançada dos dados, visualização de fotos e vídeos em diversos formatos, juntada de provas para uma análise mais rápida e permite que o usuário tenha acesso ao que realmente aconteceu no sistema operacional do computador, podendo assim, fornecer relatórios consistentes. (GUIDANCE SOFTWARE [199-]c).

3.3.SISTEMA IPED

É um sistema para indexação e processamento de evidências digitais, que busca e organiza dados de interesse em arquivos visíveis, ocultos, apagados e fragmentados que estejam em dispositivos como discos rígidos, pendrives, cartões de memória, SSDs, CDs, DVDs e outros tipos de mídias de armazenamento.

Figura 2 – tela de análise do IPED



Fonte: TI forense

Ao organizar os dados, o IPED permite que sejam feitas buscas instantâneas por palavras chave e a classificação e visualização rápida de conteúdos de imagens e vídeos, além de recuperação de mensagens de chats, de redes sociais e de e-mail que tenham sido gravados no dispositivo, ainda que temporariamente.

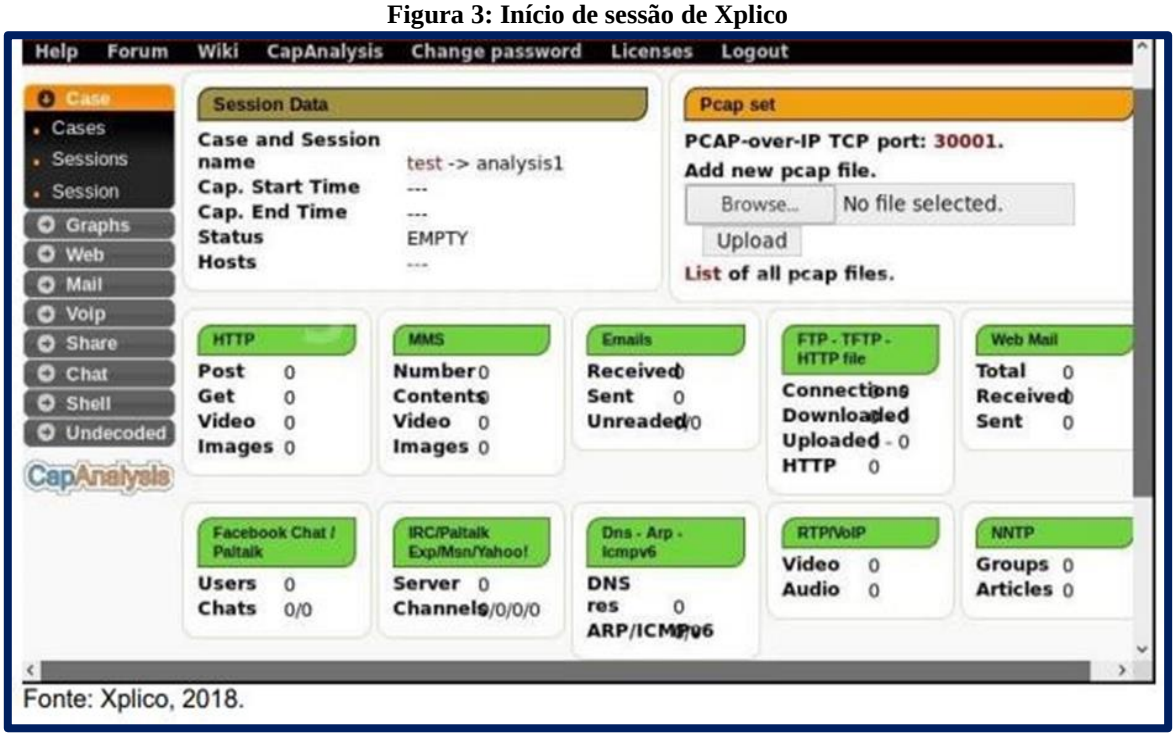
Este software computacional forense foi desenvolvimento na linguagem de programação Java. Possui uma interface simples, intuitiva e integrada para análises e exames periciais detalhados dos dados armazenados em diferentes mídias, como: computadores, pendrives, cartões de memória, CD's, DVD's, entre outros dispositivos. Software utilizado na investigação da Operação Lava Jato.

3.4.XPLICO

O Xplico é capaz de extrair e reconstruir todas as páginas e conteúdo da Web imagens, arquivos, cookies. Da mesma forma, o Xplico é capaz de reconstruir os e-mails trocados com os protocolos IMAP, POP e SMTP.

O objetivo do Xplico é capturar o tráfego de rede e dados de aplicativos. O Xplico trabalha, por exemplo, a partir de um arquivo .pcap (arquivo de dados, que contém dados de pacotes de rede) o Xplico extrai de cada e-mail (POP, IMAP e SMTP), todo o conteúdo HTTP, cada chamada VoIP (SIP), FTP, TFTP, e assim por diante (XPLICO, 2018).

Figura 3: Início de sessão de Xplico



Fonte: Xplico, 2018.

Algumas das características mais importantes deste software são listadas a seguir:

- Protocolos suportados: HTTP, SIP, IMAP, POP, SMTP, TCP, UDP, IPv6, entre outros;
- Porta Independente Protocolo de Identificação (PiPi) para cada protocolo de aplicação;
- Saída de dados e informações em banco de dados SQLite ou banco de dados MySQL e/ou arquivos;
- TCP ACK remontagem com a verificação de qualquer pacote;
- A consulta reversa do DNS dos pacotes DNS contidas nos arquivos de entradas (CPPE), não do servidor DNS externo;
- Não há limite de tamanho para entrada de dados ou o número de arquivos de entrada (o único limite é o tamanho HD);
- Suporte a IPv4 e IPv6;
- Modularidade. Cada componente Xplico é modular. A interface de entrada, o decodificador do protocolo e a interface de saída (dispatcher) são todos os módulos.

4. CONSIDERAÇÕES FINAIS

Podemos ressaltar que, os crimes virtuais são tipificados em todos aqueles que são praticados por meio de qualquer dispositivo que tenha acesso a internet, nos dias atuais devemos ficar mais atentos a qualquer anúncio, notícias, ou até links que possam estar contaminados por phishing, criminosos que utilizam a engenharia social para obter informações sigilosas, causando um grande caos para as organizações e sociedade.

Foram sanadas todas as perguntas propostas no trabalho, as pesquisas realizadas foram bem sucedidas e além de obter mais conhecimento, pode-se compartilhar com todos aqueles interessados em como prevenir-se de um crime virtual em tempos de pandemia, pois aumentou o consumo de internet, mais a segurança estava baixa, então foi proposto formas de segurança da informação, evitando assim perda de dados confidenciais e também as empresas que utilizam as VPN (rede privada virtual) para que seus funcionários possam trabalhar via home office de forma segura.

Há várias formas de se prevenir destes tipos de crimes virtuais que foram citados nos tópicos acima, depende de nós seguirmos as normas de segurança da informação para evitarmos que ocorra estes tipos de situações.

REFERÊNCIAS

ARAUJO, Guilherme. Home Office e a segurança de rede das empresas. (2020). Disponível em:<https://securityinformationnews.com/2020/04/21/home-office-e-a-seguranca-de-rededas-empresas/> Acesso em: 08 de Out. 2020.

BURKE, P. CRAIGER, P; Avaliando vestígios de evidências deixados por programas de exclusão segura, em avanços na perícia digital II, M. Olivier e S. Shenoi (Eds.), Springer, New York, pp. 185-195, 2006.

CARVEY, H. Windows Forensic Analysis. DVD Tolkit. Syngress Publishing, Inc, 2007.

CYBERNEWS. Os dados sugerem um interesse sem precedentes em hackers e crimes cibernéticos durante a pandemia. 2020. Disponível em: <https://cybernews.com/security/data-suggests-unprecedented-interest-in-cybercrime- during-pandemic/ > Acesso em: 30 de Set. 2020.

FORENSE TI, Site. IPED – Indexador e Processador de Evidências Digitais – DPF. Disponível em: <https://www.tiforense.com.br/iped-indexador-e-processador-de-evidencias-digitais-dpf/>. Acesso em: 16 Set 2020.

GUIDANCE SOFTWARE. EnCase Forensic: Process. [199-]a. Disponível em: <https://www.guidancesoftware.com/products/Pages/EnCase-Forensic/Process.aspx>. Acesso em: 18 Set. 2020.

IPOG, Blog, Conheça as principais funcionalidades do software utilizado na investigação da operação lava jato. (2018) Disponivel em: <https://blog.ipog.edu.br/tecnologia/sistema-iped-software-usado-pela-policia-federal/> Acesso em: 08 de Set. de 2020.

INTNET, Blog. Os tipos de ataques cibernéticos e a importância da proteção. (2019): Disponivel em: <https://blog.intnet.com.br/os-tipos-de-ataques-ciberneticos-e- importancia-da-protecao/> Acesso em: 02 de Set. 2020.

JUNIOR, Ed Wilson e BRAVO, Higor e FRANÇA, Alinni - Artigo - Ameaças, desafios e oportunidades da Inteligência Artificial e Cibersegurança na crise da Covid-19 (2020). Disponívelem:<https://mail.google.com/mail/u/0/#label/%5BImap%5D%2FSent%2FARTIGO+TCC/ KtbxLvgpsZWRdTxplGqjckrJGZMrwZwRDB?projector=1&messagePartId=0.2> Acesso em: 24 de Ago. de 2020.

JUNQUEIRA Daniel. Olhar Digital (2020). Falhas de privacidade são o foco de ciberataques durante a pandemia. Disponível em: <https://olhardigital.com.br/fique_seguro/noticia/falhas-de-privacidade-sao-o-foco-de- ciberataques-durante-a-pandemia/107278> Acesso em: 23 Set. 2020

KENOBY, Blog - Home office: o que você precisa saber sobre esse modelo está aqui, 2020. Disponível em: https://kenoby.com/blog/home-office/. Acesso em: 25 de Ago de 2020.

KASPERSKY, Ao Lab. Blog. Dicas de como se proteger contra crimes cibernéticos. 2020. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/what-is- cybercrime>: Acesso em: 26 de Ago de 2020.

KESSLER, G. Anti-Forensics and the Digital Investigator. Disponível em: http://scissec.scis.ecu.edu.au/ conference_proceedings 2007/forensics/01_Kessler_Anti-Forensics.pdf. Acesso em: 02 de Set. 2020.

LAWRENCE, K. R. Tools for Computer Forensics: A Review and Future Works. Proceedings of the 47th Annual Southeast Regional Conference, 2009. Acesso em: 02 de Set. 2020.

NETWORK, Global. Blog - crimes Cibernéticos 2020. Disponível em: <https://hello.global.ntt/en-us/insights/2020-global-network-insights-report> Acesso em: 26 de agosto de 2020.

RODRIGUES, A. Home office e a segurança de rede das empresas. security information news, 2020. Disponível em: <https://securityinformationnews.com/2020/04/21/home- office-e-a-seguranca-de-rede-das-empresas/>. Acesso em: 25 de Ago. de 2020.

RED HAT, Website - O que é malware? (2020): Disponível em: <https://www.redhat.com/pt-br/topics/security/what-is-malware> Acesso em: 02 de Set. 2020.

SANTOS, Daniel Oliveira - Artigo - Ataques cibernéticos: como funciona e como se proteger (2020) - Disponível em: <https://tiinside.com.br/21/08/2020/ataques- ciberneticos-como-funciona-e-como-se-proteger> Acesso em: 25 de Ago. de 2020.

SILVA, Gleice Kelly paixão. Infiltração virtual de agentes policiais no combate aos crimescibernéticos na Deep web e Dark web (2019):Disponível em: <http://repositorio.anhanguera.edu.br:8080/bitstream/123456789/227/1/TCC%20CAP.%201%2c%202%20E%203%20GLEICE.pdf> Acesso em: 28 de Ago. 2020.

SZCALER, Blog - Ataques durante a pandemia covid-19 Disponível em: < https://www.zscaler.com/blogs/research/covidlock-android-ransomware-walkthrough- and-unlocking-routine> Acesso em 28 de Ago. de 2020.

Telles, Caio. Redação. Olhar Digital (2020). Falhas de privacidade são o foco de ciberataques durante a pandemia. Disponível em: <https://olhardigital.com.br/fique_seguro/noticia/falhas-de-privacidade-sao-o-foco-de- ciberataques-durante-a-pandemia/107278> Acesso em: 23 Set. 2020

WAKKA, wagner. Matéria - Ataques hackers crescem à medida que pandemia da COVID-19 se alastra. 2020. Disponível em:<https://canaltech.com.br/hacker/ataques- hackers-crescem-a-medida-que-pandemia-da-covid-19-se-alastra-162080/> Acesso em: 28 de Ago. de 2020.

XPLICO. Xplico, a Open Source Network Forensic Analysis Tool (NFAT). Disponível em: <https://www.xplico.org/>. Acesso em: 16 Set 2020.