Classificação de Malware e sua Identificação na Perícia Digital

Yuri Euflauzino da Silva – euflauzino@paranapericias.com
Computação Forense e Perícia Digital
Instituto de Pós-Graduação - IPOG
Curitiba, PR, 27 de novembro de 2018

Resumo

O presente trabalho demonstra as técnicas utilizadas por peritos em informática, utilizadas para identificação de malwares e sua classificação na indústria, conceitos de computação forense e sua reelevancia como metodo científico na elaboração de provas utilizadas em processos judiciais,

***Palavras-chave**: Malware, Computação Forense, Pericia em informática.*

1. Introdução

Começamos a perceber que a informação é o maior bem empresarial atualmente, segundo Sandro Melo (2009) o ativo mais compettitivo e que pode definir a trajetória ao sucesso de uma empresa é a informação, para Mitnick e Simon (2006), a informação sempre foi um ativo importante para as empresas e para as pessoas em geral, com avanços tecnologicos e a rápida mudança de tendencia de mercado, o uso da internet elimina as barreias geográficas.

Atualmente não é possível pensar em projetos de segurança sem pensar em segurança digital, ainda mesmo que por mais seguro que seja um firewall ou sistema de segurança os equipamentos computacionais sempre estao sucetiveis a falhas, nao podendo afirmar que um sistema seja invunerável. (Sandro Melo, 2009).

Além de assumir que um sistema de segurança não seja suficiente e não poder garantir que sistemas computacionais sejam invulneráveis, de acordo com uma pesquisa da IBM e do Ponemon Institute (2016), em 74% dos incidentes, a falha do usuário desempenhou um papel decisivo no vazamento de dados e se tratando de uma rede corporativa, um cavalo de troia pode congestionar o trafego dos dados, enviar spam, efetuar mineração de dados além de destruir ou vazar dados críticos para os negócios (Karspersky, 2018).

Para o usuário comum, a infecção por Malware pode acarretar perda de dados que não sao tão importantes além de dados que podem ser usados para fins ilicitos por

criminosos como roubo de contas bancárias.

Todos esses problemas são causados por aplicações denominadas malware, e cabe a computação forense a apuração de vestigios digitais, facilitando a constatação da invasão, quais medidas tomar, além da manipulação, preservação e elaboração das provas digitais para uso judicial se necessário, neste ultimo caso é importante manter a boa prática da coleta, preservação, extração e análise assim como a interpretação do harware e software quanto ao ocorrido pois mantem a integridade das provas digitais e a sua usuabilidade para fins jurídicos, esses vestigios se encontram no equipamento invadido, nos servidores, na internet, nos ativos da rede, e em estações de trabalho (Sandro Melo, 2009).

2. Definição de Computação Forense

A computação forense pode ser definida como aplicação de metodos cientificos, para a identificação, coleta, armazenamento e preservação de dados que podem ser utilizados na área judicial (MERCURI, 2005). Uma outra variação da definição encontrada na literatura, é a do professor Sandro Melo (2009, p. 13) o qual afirma uma ramificada da computação forense;

> "[...] A Computação Forense pode ser definida como uma área da Ciência da Computação que se desenvolve gradualmente para atender à demanda oriunda da Criminalística, e também como uma parte da Criminalística que se apropria de fundamentos da Ciência da Computação."

Ilustrando essa ramificação, segue abaixo a figura que unifica a ciência da computação e a criminalistica mostrando o espaço em que a computação forense ocupa:

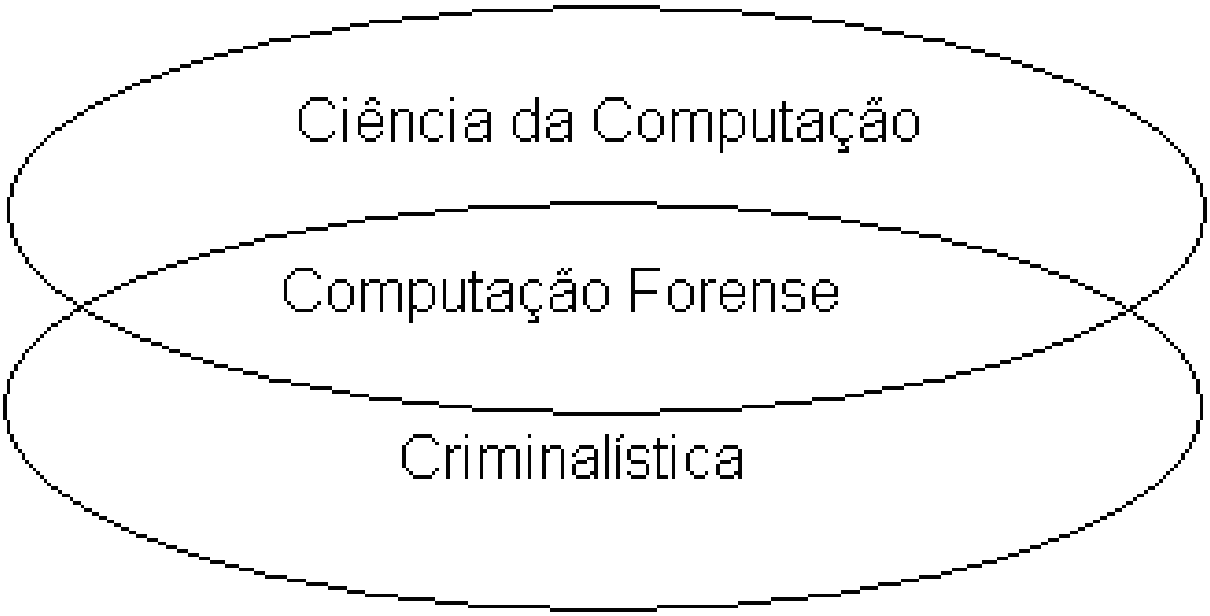

Figura 1 - Relação Ciência da Computação, Criminalística e Computação Forense.
Fonte: MELO, 2009, p. 2

Araujo (2010), esclarece que as provas coletadas no inquerito policial, devem ser preservadas para utilização no meio judicial, isso significa que deve ser empregado um metodo ciêntifico para sua aquisição, preservação e armazenamento, porém é sabido que "[...] Não há padrões internacionais para o tratamento de dados periciais, embora existam documentos de boas práticas dedicados a classifcar respostas a incidentes de segurança.

A realização de uma perícia forense, é a forma Técnico-Científica que elucida os fatos do ocorrido, não há necessidade de seguir normas rígidas, independente da área que for necessário, cada caso é tratado de uma forma diferente e de acordo com a necessidade, contudo é indicado que haja uma sequência de cuidados para alcançar esse objetivo, sugere-se assim que a perícia siga um processo forense composto por quatro etapas: coleta, extração, análise e apresentação (Kent et al, 2006).

A Figura 1 ilustra as etapas do processo forense Kent et al., (2006) em um contexto computacional:

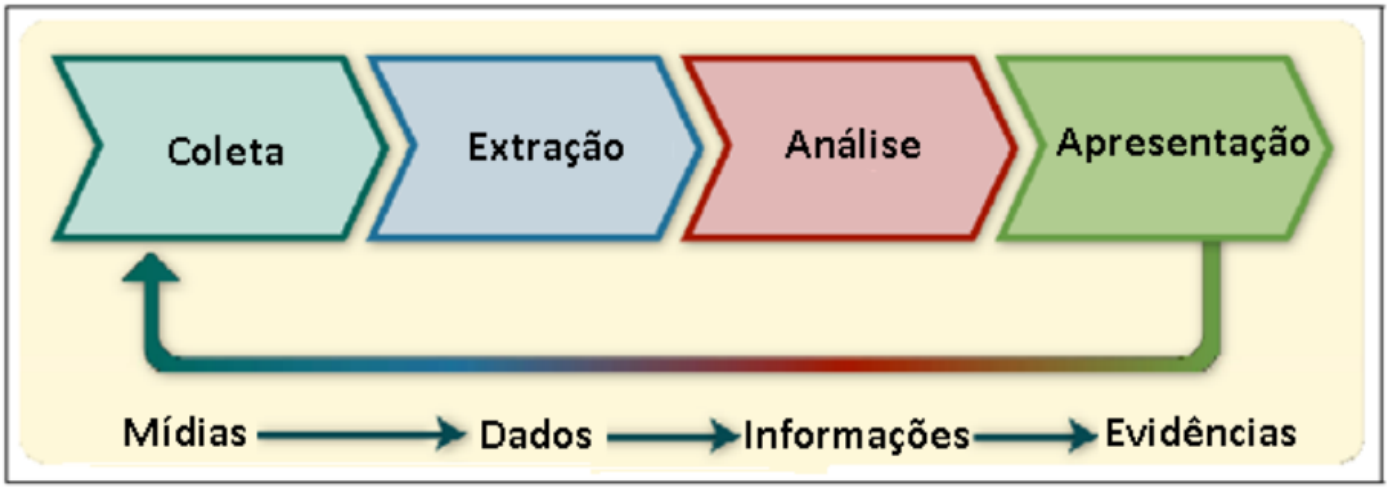

Figura 2 - Etapas do processo forense
Fonte: Adaptado de Kent et al., 2006.

a) **Coleta**: Na primeira etapa, identifica, isola e registra os dados e componentes físicos que tem relação com o incidente que esta sendo investigado.
b) **Extração**: Nesta etapa, o perito averigua e extrai informações dos equipamentos, com o amparo de ferramentas e tecnicas forenses adequadas para cada caso, mantendo assim a integridade dos dados.
c) **Análise**: Efim a análise é feita nos dados obtidos da extração para que possam ser respondidos os quesitos feitos ao perito.
d) **Apresentação:** Decorrido a sequencia das etapas anteriores, o perito elabora seu laudo de forma a encontrar relevancia para caso sendo de conclusão imparcial clara e concisa além de expor os metodos utilizados na pericia, além de ser de fácil interpretação por pesoa comum ou de conhecimento médio.

3. Definição de Malware e sua classificação na indústria

Chamados de códigos maliciosos, malware são todas as aplicações criadas com a intenção de alterar, acessar dados ou criam funcionalidades nas aplicações ou sistema operacional, sem consentimento do usuário (AYCOCK, 2006). Eles podem ser projetados em scripts, traços infiltrados no código de aplicações, e executáveis, esse conceito é subdividido em categorias que incluim os vírus, rootkill, ransomware, cavalos de troia entre outras (SIKORSKI; HONIG, 2012).

Casos de proliferação de malware vem sendo notados por empresas de informática já a anos, exemplo como o da empresa Microsoft (MICROSOFT, 2005) relata que em seu

sistema operacional foram encontrados rootkills que vieram em cds fornecidos oficialmente pela Sony que maniúlavam dados dos usuários sem o seu consentimento, essas informações eram capturadas de falhas do sistema operacional, dos navegadores ou plugins como o java.

Há uma classificação genérica na industria de antívirus, demontra-se isso na figura 3 onde alguns antivirus submeteram trechos de códigos maliciosos a ferramenta VIRUSTOTAL, cada um com um nome e classificação diferente.

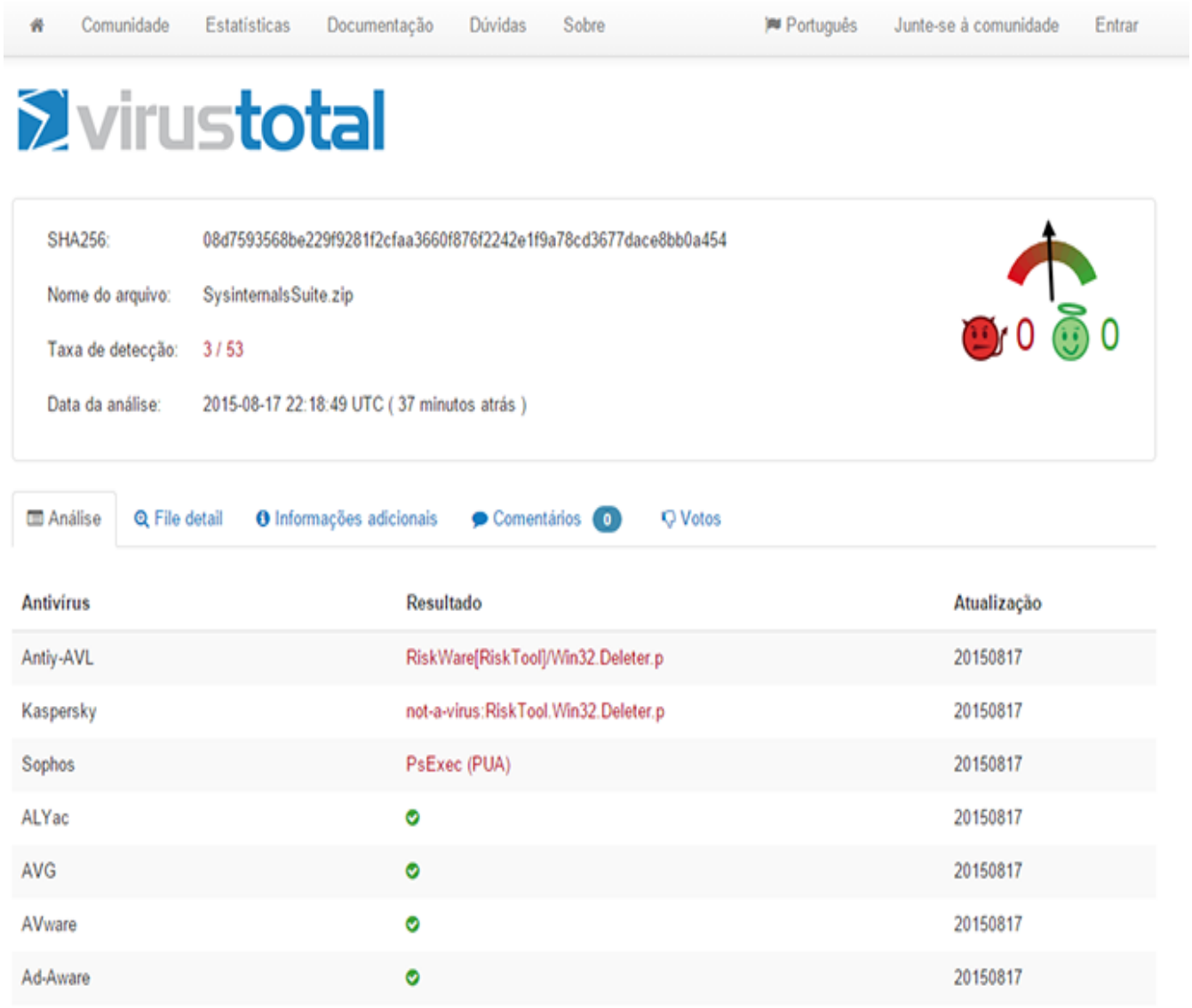

Figura 3 – Discrepância virustotal.com

Fonte: Alarmes falsos e as falhas nos sistemas de análise de malware (2018)

Estudos e pesquisas sobre malwares é desenvolvida anualmente pelo CARO (Computer Antivirus Research Organization) fundada em 1990 porém, não existe consenso em classificação entre as empresas. Abaixo exemplo de classificação de Malware no website da empresa Kaspersky (KASPERSKY, 2018);

Classe	Definição
Virus	Programas que infectam outros programas adicionando-lhes um código de vírus ao seu processo de inicialização. Esta definição simples revela a ação principal de um vírus: infecção. A velocidade de propagação dos vírus é menor do que a dos worms.
Worm	Este tipo de Malware usa recursos de rede para propagação. Esta classe foi chamada de worm por causa de sua peculiar característica de "fluência" de computador para computador usando a rede, e-mails e outros canais informativos. Graças à essa fluência a velocidade de espalhamento de worms é muito alta. Worms invadem seu computador, calculam endereços de rede de outros computadores e enviam para esses endereços suas cópias. Além dos endereços de rede, os dados dos catálogos de endereços dos clientes de correio também são usados. Os representantes deste tipo de Malware às vezes criam arquivos em discos do sistema, mas não usam outros recursos do computador (exceto a memória operacional).
Trojan	Programas que executam em computadores infectados sem autorização por ações do usuário. Dependendo das condições podem deletar informações no disco, congelar o sistema, roubar informações, etc. Este tipo de malware não é um virus na definição tradicional, ou seja, não infecta outros programas ou dados. Os cavalos de Tróia não podem invadir o PC por si mesmos, são difundidos por violadores como software útil e necessário. E ainda, danos causados por Trojans são maiores do que os causado por um ataque de vírus tradicional.
Spyware	Software que permite coletar dados sobre um usuário ou organização específica, que não estão cientes disso. Você talvez nem saiba que está infectado por um spyware em seu computador. Como regra geral, o objetivo de um spyware é: Rastrear as ações do usuário no computador. Coletar informações sobre o conteúdo do disco rígido; Muitas vezes significa digitalizar algumas pastas e registros do sistema para fazer uma lista de softwares instalados no computador. Coletar informações sobre a qualidade da conexão, modo de conexão, velocidade do modem, etc. Coletar informações não é a principal função desses programas, eles também ameaçam a segurança. No mínimo dois programas conhecidos - Ga-

	tor e eZula – permitem ao violador não só coletar informações, mas também controlar o computador. Outro exemplo de spyware são programas incorporados no navegador instalado no computador para retransferir o tráfego. Você definitivamente já se deparou com esses programas, se ao acessar um endereço de um website, outro website foi aberto. Um dos spywares é o phishing-delivery.
Phishing	São e-mails cujo objetivo é obter informações confidenciais do usuário, como regra geral. O Phishing é uma forma de engenharia social, caracterizada por tentativas fraudulentas de adquirir informações sensíveis, como senhas e detalhes de cartão de crédito, mascarando-se como uma pessoa ou negócio confiável em uma comunicação eletrônica aparentemente oficial, como um e-mail ou uma mensagem instantânea. As mensagens contêm um link para um website deliberadamente falso onde o usuário é instruído a inserir o número do seu cartão de crédito e outras informações confidenciais.
Riskware	Este software não é um vírus, mas representa uma ameaça em potencial. Por algumas condições a presença de tais riskware no seu PC coloca seus dados em risco. Estão incluídos nesta classe de software utilitários de administração remota, programas que usam conexão discada, e alguns outros que se conectam com websites da internet que oferecem servios de pay-per-minute.
Jokes	Software que não prejudica o computador, mas exibe mensagens de que dano já foi causado ou que será causado em algumas condições. Este software frequentemente adverte o utilizador sobre perigo não existente, por exemplo, exibe mensagens sobre formatação de disco rígido (embora nenhuma formatação esteja realmente acontecendo), detectar vírus em arquivos não infectados e etc.
Rootkit	São utilitários usados para ocultar atividades maliciosas. Eles disfarçam o Malware, para evitar que sejam detectados pelos aplicativos antivírus. Os rootkits também podem modificar o sistema operacional no computador e substituir suas principais funções para disfarçar sua presença e ações que o violador faz no computador infecta-

	do.
Spam	Mensagems de e-mail anônimas e em massa, de caráter indesejável. O spam pode ser propaganda política, comercial, ou e-mails que pedem para ajuda para alguém. Outra categoria de spam são mensagens que sugerem que você invista uma grande soma de dinheiro, ou convidando você para pirâmides financeiras, e-mails que roubam senhas e número de cartão de crédito, mensagens sugerindo para enviá-los para seus amigos (mensagens de felicidade), etc. Spam sobrecarrega servidores de correio e aumenta o risco de perder informações importantes para o usuário.
Outros	Outros programas diferentes que foram desenvolvidos para criar outros Malware, organizando ataques DoS em servidores remotos, invadindo computadores, etc. Hack Tools, construtores de vírus e outros referem-se a tais programas.

Tabela 1 – Classificação Kaspersky

Fonte: Adaptado de Kaspersky (2018)

Já a empresa F-Secure (F-SECURE, 2018) subdivide Malware da seguinte forma:

Classe	**Definição**
Virus	Integra seu próprio código em programas ou arquivos de dados e se espalha integrando-se em mais arquivos cada vez que um arquivo afetado é executado.
Worm	Usa recursos de computador ou de rede para fazer cópias completas de si mesmo e distribuí-las para outras vítimas. Pode incluir código ou outro malware para danificar tanto o sistema quanto a rede. Worms também podem ser desenvolvidos mais especificamente com base no tipo de rede que eles usam para se espalhar: • Net-Worm: através de uma rede local ou da Internet • Email-Worm: via e-mails, contidos no próprio e-mail ou como anexos de arquivo

	• P2P-Worm: em arquivos enviados por redes peer-to-peer (redes P2P) • IM-Worm: sobre redes de mensagens instantâneas • (IM)IRC-Worm: através de canais de conversa por internet (IRC) • Bluetooth-Worm: difusão via Bluetooth
Rootkit	Esconde a si mesmo, ou outros arquivos, dos programas de segurança do dispositivo. Pode ser usado por usuários remotos para manipular o dispositivo.
Backdoor	Permite que usuários remotos manipulem um programa, computador ou rede.
Trojan	Permite que usuários remotos manipulem um programa, computador ou rede. Cavalos de Tróia utilizam desorientação, desinformação, omissão ou fraude para enganar o usuário na instalação ou execução, para que ele possa executar ações potencialmente indesejadas / prejudiciais. Não se reproduz. Trojans podem ser desenvolvidos mais especificamente com base no tipo de ações que desejam executar: • Trojan-Spy: instala programas de espionagem como keyloggers • Trojan-PWS: rouba senhas e outras informações confidenciais • Trojan-Downloader: baixa programas de um servidor remoto, instala e executa • Trojan-Dropper: carrega pelo menos um programa, que instala e executa • Trojan-Proxy: permite que usuários remotos conectem o sistema infectado a um servidor proxy anonimamente • Trojan-Dialer: conecta-se à Internet através de linhas telefônicas premium. Também pode levar a websites não solicitados ou inapropriados.
Rogue	Utiliza mensagens de alta gravidade, mensagens enganosas ou fraudes diretas para pressionar os usuários a comprarem software antivírus que podem não funcionar conforme informado.
Exploit	Aproveita-se de uma vulnerabilidade em um programa ou sistema operaci-

	onal para obter acesso ou executar ações além do que é normalmente permitido.
Packed	Compactado para um tamanho menor usando um programa packer, co- nhecido por ser usado por outros malwares.
Construtor	Um programa utilitário usado para construir malware.

Tabela 2 - malware F-Secure.

Fonte: Adaptado de (F-SECURE, 2018)

Entram nessa classe, os virus, rootkill, worm definidos como podendo ser prejudicial para o usuário ou para o sistema, roubando dados e até manipúlar dispositivos sem a autorização do usuário (F-SECURE, 2018).

Já na classificação de Spywares estao os programas que coletam dados particulares do usuário, exemplo; a solicitação de acesso a midia, agenda de contatos, camera e bluetooth do celular quando é instalado e executado pela primeira vez (F-SECURE, 2018).

Abaixo tabela da classe spyware da empresa -Secure (F-SECURE, 2018):

Classe	**Definição**
Spyware	Coleta informações sobre o comportamento de navegação na web do usuário ou aplicativos preferenciais. Os dados coletados podem ser armazenados localmente ou enviados.
Trackware	Permite que um terceiro identifique o usuário ou seu dispositivo, geral- mente com um identificador exclusivo. O trackware mais comum é o rastreamento de co- okies.
Adware	Fornece conteúdo publicitário, no navegador da Web, no Desktop de um PC ou em um aplicativo.

Tabela 3 - spyware F-Secure.

Fonte: Adaptado de (F-SECURE, 2018) .

Já na classificação de riskware entram as ferramentas seguras que se utilizadas adequadamente não apresentam perigo, porém se utilizada por um invasor ela pode causar danos exemplo como aplicativos de análise de trafego como wireshark, keyloger utilizado

por administradores de redes para controle de dados além das ferramentas de análise de navegação na internet para controle de acesso de funcionários entram nessa categoria conforme tabela abaixo:

Classe	Definição
Monitoring-Tool	Monitora e registra ações de um usuário em um dispositivo
Hack-Tool	Ignora as restrições de acesso ou mecanismos de segurança para dar acesso aos usuários ou a capacidade de executar ações além do que é normalmente permitido
Application	Introduz um risco de segurança se usado de forma errada ou maliciosa

Tabela 4 - riskware F-Secure.

Fonte: Adaptado de (F-SECURE, 2018)

Observando as duas empresas (KASPERSKY e F-SECURE) percebe-se uma discrepancia entre a forma de classificação delas. A primeira sugere que malware são em geral formadas por virus, spam, rotkil spyware entre outros, já a segunda sugere uma divisão em malware, spyware e riskware dando tambem uma subdivisão para cada uma delas.

Além destas duas empresas, tabelas em sites de antivirus como (PANDA SECURITY, 2018), (AVG, 2018), (AVAST, 2018), constata-se discrepancia na hora da classificação dos malwares .

4. tipos de análise de artefatos

Exite três tipos de análise que podem ser feitas no artefatos questionados, *a Live analysis*, *Network Analysis e Post Mortem Analysis* cada uma contem particularidades, sendo a ultima (*Post Mortem Analysis*) a mais londa e honerosa ao perito.

4.1 Live Analysis

Quando o equipamento é encontrado ligado, ou não é possivel desliga-lo por ele depender de outros equipamentos conectados para funcionar, é feito uma análise denominada *live analysis,* que segundo Sandro Melo (2009) afirma a posiblidade de coleta de informações, tanto na maquina (memoria principal, *cpu*, periférios, dispositivos de armazenamento) além de coleta como na rede, podendo contribuir para a identificação de atividades de malwares no equipamento, essa análise e identificação de dispositivos na redę.pode ser feita através de um *sniffer*, programa que captura dados na rede, dados como portas e endereços utilizados pela maquina, endereços de ip, trafego de dados e requisições

de páginas *web* (Sandro Melo, 2009) Ainda de acordo com o autor, esses dados coletados na fase de *live analysis,* poderão ser utilizadas na fase denominada *Post mortem analysis* que é a análise feita após o desligamento do equipamento e a cópia bit a bit do dispositivo.

A *Live Analysis* pode resgatar dados que após desligado o equipamento se perdem com facilidade, porem o risco a fazer este tipo de análise, esta justamente em quebrar um dos principios de boa prática, trata-se da preservação da evidencia, por isso quando possivel, a pericia é feita apenas na *post mortem analysis* na cópia forense da evidencia, porém devidamente fundamentada a prova pericial feita de forma *live analysis* é aceita.

Conclui-se entao, sobre a *Live Analysis* a extrema impoprtancia da preservação da memória principal. também por sua volatilidade que respeitando ordem de risco de perda de dados do equipamento da mais volatil para a menos volatil, endende-se que o procedimento padrão seria a coleta do cache e dos registro, alem de se encontrar dados das ultimas aplicaçõe acessadas pelo usuário, esse tipo de análise é excelente quando se trata de dados criptografados no disco, pois uma vez na memoria eles nao estao protegidos por criptografia.

Além de outros casos como a presença de malware, trechos de arquivos ou conversas de chats que ainda nao foram armazenadas no disco local, justificam a preservação da memória principal ao encontrar o equipamento ligado, atenta se para o autor Tiago Souza (2008) que nos deixa a ressalva que se deve observar no critério de não alteração de dados, isso ocorre por que uma vez que esse tipo de análise é geralmente feita com um pen drive externo, ao se conectar na maquina examinada, ele altera os dados da maquina em pelo menos cinco locais quando se tratando do sistema operacional windows;

São eles;

1. A chave USBSTOR localizada em SYSTEM (SYSTEM/CurrentControlSet/Enum/USBSTOR)
2. A chave MountedDevices (SYSTEM/MountedDevices)
3. A chave MountPoints2 localizado em (Software/Microsoft/WindowsCurrentVersion/Explorer/MountPoints2)
4. A chave USB localizada em SYSTEM (SYSTEM/CurrentControlSet/Enum/USB)
5. O arquivo de log setupapi (Windows/inf/setupapi.dev.log para Windows Vista/7/8 e Windows/setupapi.log para Windows XP)

Ainda conforme o autor, para contornar esse problema de alteraçao do artefato no ambiente “controlado”, bastaria registrar os dados do pen drive, e relatar a necessidade e alteração no sistema no laudo pericial, pois as vantagens dessa coleta são maiores do que a

não alteração no “ambiente controlado”.

Alguns exemplos de ferramentas com licença livre utilizados na *Live Analysis* são a *FTK IMAGER* e a *Belkasoft Live RAM Capturer.*

4.2 *Network Analysis*

Na *Network Analysis* é a técnica de obtenção de “dados dos demais ativos de rede envolvidos em um incidente desegurança” (SANDRO MELO, 2009) o autor também menciona algumas técnicas de obtenção de dados, como *footprint*, *fingerprint* e *port scanner*; estas podem gerar a confirmação de invasão ou malware automatizado; a forma que um serviço foi utilizado para realizar a invasão; as vulnerabilidades que esse malware explorou; definição da origem da ameaça; tipo de usuário que realizou o ataque;possíveis falhas de segurança; instalação de *backdoors* ou *rootkits*; e tentativasde eliminação de rastros (Sandro Melo, 2009), todas estas evidencias coletadas na *Network Analysis* são posteriormente confrontadas com a coleta feita na live analysis de forma que ajuda a elucidar e formar a conclusão do perito quanto a invasão do dispositivo.

Ainda segundo o autor a *Network Analysis* pode ocorrer em dois momentos. No primeiro momento, ocorre na procura de comunicação da estação com outros dispositivos na rede ou fora dela, o segundo é a coleta e mapeamento dos ativos de redes, como servidores switches e roteadores.

Já segundo Tiago Souza (2017) a *Network Analysis* é uma variação da computação forense, que esta relacionada ao monitoramento e análise do trafego de uma rede, afim de coletar informações, evidencias e detectar intrusões, além diferir das outras áreas forense digital no que tange a volatilidade dos dados e a parte dinamica, pois o trafego é transmitido e depois perdido de forma que a *Network Analysis* é muitas vezes proativa, exemplos do autor de ferramentas de código livre como o Wireshark e o Xplico, volta sua análise a pacote capturado do trafego da rede que depois de coletado pode-se extrair e-mail, todos os conteúdos HTTP, e ligações provenientes de protocolos de comunicação como *VoIP (SIP), FTP, TFTP*.

4.3. ***Post Mortem Analysis***

Segundo Vaine Luiz Barreira (2018) a análise Post Mortem geralmente é feita quando o equipamento encontra-se desligado, ou não haja necessidade de manter o equipamento ligado pelos dados não serem voláteis (geralmente hdds, pen drive e discos). De acordo com Eleutério Machado (2018) essa etapa começa com a cópia bit a bit do objeto questionado e ainda conforme Eleutério Machado (2018) esse procedimento é o mais longo

e cansativo uma vez que qualquer hdd de tamanho pequeno pode contem milhares de arquivos.

Para exemplo de tipos de arquivos e diretórios analisados peor peritos em informática Reis (2003) demonstra em uma tabela as principais fontes de informações que peritos em computação forense utilizam para coleta de evidencias no sistema GNU/LINUX;

Arquivos e diretórios de usuários	Arquivos de texto, mensagens de correio eletrônico, imagens, entre outros tipos de dados que podem conter informações úteis relacionadas ao perito.
Arquivos de Log	Os arquivos de Log são muito importantes, pois podem registrar as atividades dos usuários, dos processos, do sistema das atividades de rede e Informações específicas de aplicativos e serviços.
Executáveis e bibliotecas	Arquivos executáveis e bibliotecas são alterados pelo usuário/atacante para esconder sua presença.
Arquivos e diretórios escondidos ou não usuais	Arquivos e diretórios ocultos ou com nomes incomuns são freqüentemente usadas por atacantes para camuflar-los..
Diretório de arquivo de dispositivos	Com exceção de alguns arquivos especiais, o diretório /dev deverá conter apenas os arquivos de dispositivo.
Diretório temporário	Os diretórios temporários /tmp e/usr/tmp servem como diretórios de “rascunho” para todo o sistema. Como eles são apagados periodicamente, acabam se tornando locais muito utilizado para armazenar dados que não serão usados com freqüência.
Arquivos de configuração	O sistema GNU/Linux possui certos arquivos de configuração comumente acessados ou alterados pelos usuários, são scripts de inicialização, senhas e permissões de usuários.e configurações.

O esquema de pesquisa pode mudar de acordo com o sistema operacional, por exemplo, no caso de um sistema Windows 7 a pesquisa é feita em cima das chaves de

registro da máquina, segundo Marcelo Osvaldo aranha (2015) o registro do Windows alem de conter *log* das atividades do sistema fornece dados de configurações.

Na Análise de Malware, as seguintes chaves podem ser utilizadas para iniciá-lo e conter dados que podem ser evidencias da existência do software malicioso.

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_USERS\SID\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_USERS\SID\Software\Microsoft\Windows\CurrentVersion\RunOnce

C:\Users\username\AppData\Roaming\Microsoft\Windows\Menu Iniciar\Programas\Inicializar
ou

C:\Users\username\AppData\Roaming\Microsoft\Windows\Start Menu

Ainda conforme Marcelo Osvaldo Aranha (2015) várias chaves do sistema operacional Windows podem ser exploradas pelo perito, chaves que contem os programas mais utilizados, atalhos, seleções, configurações de rede, acesso remoto entre outras funcionalidades acessadas no sistema.

5. ***Conclusão***

O trabalho exclarece a questão da do que é um *malware*, onde se nota uma discrepancia no meio da industria quanto sua classificação, denominação e nomes onde a unica concordancia encontrada esta apenas na sua definição central, que é a de se tratar de um softaware mal intencionado, mesmo havendo organizações que tratam das pesquisas sobre o tema, não foi possivel localizar textos na literatura que sirvam como classificação predominante.

Também ficou claro que com a atual mudança no cenário corporativo e particular onde os dados são um bem sensivel, e importante para as empresas e usuários comuns, os dados devem ser manipulados com tecnicas adequadas, softwares e demais precauções a fim de mante-las preservadas caso seja necessário para utilização judicial ou extajudicial,

assim abrindo campo para a ciência denominada computação forense.

Referências

ELEUTÉRIO, P. M. S.; MACHADO, M. P. **Desvendando a computação forense**. São Paulo: Novatec, 2011

Kent, K. et al**. Guide to integrating forensic techniques into incident response: recomendations of the National Institute of Standards and Technology. Special publication**. Gaithersburg: NIST, 2006.

REIS, Marcelo Abdalla dos. **Forense computacional e sua aplicação em segurança imunológica**. Universidade.2003. Dissertação de Mestrado.Universidade de Campinas. Campinas,SP

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

Marcelo osvaldo Aranha, **o Sr. Perito tratar sobre arquivos de registro do Windows – Parte 02** acesso em 30 de janeiro de 2019 https://qperito.wordpress.com/2015/04/08/queira-o-sr-perito-tratar-sobre-arquivos-de-registro-do-windows-parte-02/

Vaine Luiz Barreira, **Termos e Definições** acesso em 30 de janeiro de 2019 http://www.ciberforense.com.br/termos-e-definicoes/

Tiago Souza, **Como analisar arquivos pcap** acesso em 30 de janeiro de 2019 https://tiagosouza.com/como-analisar-arquivos-pcap-xplico-network-forensic-analysis-tool/

Kaspersky, **Roubo e perda de dados** acesso em 28 de janeiro de 2019 https://www.kaspersky.com.br/resource-center/threats/data-theft