Hamilton Fonte II

Coletando dados de memória de uma máquina em nuvem para análise forense

São Paulo, Brasil

2016, v-0.1

Hamilton Fonte II

Coletando dados de memória de uma máquina em nuvem para análise forense

Projeto de pesquisa para a disciplina Metodolodia de Pesquisa Científica em Engenharia de Computação.

Universidade de São Paulo – USP

Escola Politécnica - Engenharia de Computação

Programa de Pós-Graduação em Engenharia Elétrica

São Paulo, Brasil

2016, v-0.1

Sumário

1 Introdução

Os crescentes avanços tecnilógicos que têm ajudado a vida do ser humano também trouxeram diversos novos tipos de crimes relacionados a tecnologia da informação. (citação) Quando do evento de um crime, há a necessidade de preservar as evidências de modo que apoiem processos investigativos e legais mas também para que possamos compreender a sequência de eventos envolvidos no ataque de modo que possamos evitar que estas vulnerabilidades sejam exploradas novamente.

Ciência forense digital é uma ferramenta importante para a solução de crimes cometidos com um computador pela sua capacidade de reconstruir a cena do crime a partir das evidências digitais deixadas por um ataque. Com o crescente uso de ferramentas online, virtualização e hospedagem em nuvem, o volume de dados gerado por esses sistemas que já era uma preocupação da comunidade forense em 2008 (citação), hoje começou a inviabilizar algumas de suas práticas. (citação)

Coma funcionalidade da elasticidade de carga ofertada pelos provedores de nuvem, por meio da qual infraestrutura pode ser alocada e desalocada dinamicamente, veio à tona o problema da volatilidade dos dados nas máquinas virtuais. Com algumas ameaças que não deixam evidências em disco(citação), a memória de uma máquina despejada de um pool seria para sempre perdida. Com a máquina mais poderosa hoje ofertada pela Amazon tendo 240Gb de memória (citação), o ferramental forense disponível hoje esta pouco adaptado a desafios trazidos pela núvem (citação).

2 Justificativa

A tecnologia hoje é parte de nossas vidas e também é parte da vida dos criminosos. O último crime registrado na America do Norte que não envolveu uma evidência digital data de 2011 (citação), no Brasil só em 2015 houve um aumento de 87% no registro de notas relacionadas a abusos ou crimes digitais (citação), forense digital é uma disciplina que precisa avançar para ajudar na resposta da lei a esses delitos.

Do ponto de vista forense, praticantes e pesquisadores concordam que aspectos legais e o crescente volume de dados figuram entre as principais dificuldades trazidas pela computação em nuvem (citação). As técnicas forenses atuais são da época pré-nuvem onde o controle da evidência é um de seus principais pilares (citação). No processo de coleta de evidências, remove-se o hardware relacionado ao caso e o coloca sob custódia. Com a nuvem, o aspecto multi inquilino impede esta prática pois a mídia é compartilhada com outros usários, removê-la seria uma violação da privacidade de usuários não relacionados a investigação. Outro aspecto da implementação da nuvem é o carater distribuído, a evidência pode estar localizada em um país diferente daquele em que o crime foi cometido dificultando a obtenção da mesma (citação). O crescente volume de dados das aplicações operando em nuvem caminha para inviabilizar a forense digital. Investigadores forenses hoje estão com 6 a 12 meses de backlog de dados para investigar (citação), download de terabytes de dados para análise tem levado horas para ser realizado e requer colaboração dos operadores de nuvem (citaçã. Mudar o paradigma de coleta de evidência tem sido proposto por pesquisadores e praticantes há alguns anos (citação), porém esta prática precisa submeter a legislação pois em algum momento a evidência será usada em um processo legal.

Por fim, a criatividade dos criminosos para explorar vulnerabilidades trouxe a tona ataques que não deixam evidências em disco, toda a operação ocorre em memória (citação). Com o caráter elástico das soluções em nuvem, uma maquina despejada de um pool e cujos recursos foram reutilizados não pode mais prover as evidências necessárias para investigação criminal e assim o criminoso fica impune. Coletar a memória de máquinas em núvem de modo que sejam usadas com sucesso em um processo penal, sem sobrecarregar ainda mais os investigadores é a principal justificativa desta pesquisa.

3 Objetivos

Declarar e explicar as 3 hipõteses do trabalho, associa-los ao objetivo principal e os 3 sub-objetivos

4 Plano de Trabalho

Não faço ideia de como faremos isso mas estou muito interessado em saber... :)

5 Material e Métodos

Implementação de virtualização de mercado. rede laboratorio

6 Análise dos Resultados

Nao faço a mais remota ideia de como fazer isso

7 Considerações finais

considerei finalmente que estamos gastando mais tempo formatando o documento do que realmente escrevendo seu conteúdo.

Referências