TRAIRA: Tratamento de Incidentes de Rede Automatizado

Italo Valcy[1], **Jerônimo Bezerra**[1]

[1]Centro de Processamento de Dados – Universidade Federal da Bahia (UFBA)
Av. Adhemar de Barros, s/n – Campus Ondina – Salvador, BA – Brasil

{italovalcy, jab}@ufba.br

Resumo. *O crescimento atual da Internet tem alavancado o número de incidentes de segurança da informação. Devido aos prejuízos causados por tais incidentes e sua dificuldade de prevenção, é necessário estabelecer políticas e mecanismos eficientes de tratamento e resposta a incidentes de segurança. Entretanto, um dos entraves à correta identificação de equipamentos comprometidos ou participantes em um incidente de segurança consiste na ampla existência de redes que utilizam técnicas como NAT ou DHCP, que ocultam a identificação precisa dos hosts internos. Este trabalho descreve o projeto, a implementação e avaliação da ferramenta TRAIRA, a qual automatiza o procedimento de detecção, identificação e isolamento dos dispositivos geradores de incidentes de segurança em redes locais. A ferramenta desenvolvida foi avaliada em um ambiente real, na Universidade Federal da Bahia (UFBA), sendo utilizada como base do processo de tratamento de incidentes de segurança gerados pela instituição. O baixo custo de execução e implantação da ferramenta indica, assim, a viabilidade de sua aplicação prática em ambientes corporativos.*

1. Introdução

O crescimento atual da Internet tem alavancado o número de incidentes de segurança da informação. Segundo dados do *Grupo de Resposta a Incidentes de Segurança da Bahia/Brasil* (CERT.Bahia), de Janeiro à Outubro de 2010 já foram reportados mais de 1500 incidentes de segurança às instituições de ensino e pesquisa monitoradas na Bahia [CERT.Bahia 2010].

Devido aos prejuízos causados por tais incidentes e sua dificuldade de prevenção [Scarfone et al. 2008], é necessário estabelecer políticas e mecanismos eficientes de tratamento e resposta a incidentes de segurança. Entretanto, um dos entraves à correta identificação de equipamentos comprometidos ou participantes em um incidente de segurança consiste na ampla existência de redes que utilizam equipamentos para traduzir ou mapear os endereços dos *hosts* internos à rede via NAT ou DHCP. O emprego dessas técnicas oculta a identificação precisa dos *hosts* internos, o que dificulta o tratamento adequado de incidentes. Outro complicador desse processo é o volume de notificações recebidas e a heterogeneidade da rede. Mesmo as grandes instituições, geralmente, não possuem uma equipe e ferramentas de segurança necessárias para tratar todos os incidentes.

Além disso, a maior parte dos incidentes, aqueles relacionados às máquinas infectadas com *vírus/worm* [CERT.Bahia 2010], são causados por ferramentas que comprometem a máquina de forma automatizada. Certamente, a infecção automatizada de

máquinas com software malicioso não pode ser tratada manualmente. Uma alternativa é tornar o processo de tratamento desses incidentes o mais automatizado possível. Por exemplo, usando ferramentas para detectar e isolar as máquinas comprometidas de forma automatizada e contando com o apoio de uma equipe de apoio (*helpdesk*) para trabalhar na desinfecção das máquinas. Dessa maneira, reserva-se os analistas de segurança (cujo custo de contratação é comumente alto) para o tratamento de incidentes mais importantes ou complexos, e para as outras atividades de segurança da instituição.

Este trabalho descreve o desenvolvimento de uma ferramenta que automatiza parte do processo de tratamento de incidentes de segurança, o *TRAIRA* (Tratamento de Incidentes de Rede Automatizado). Em sua primeira versão, o TRAIRA atua nas duas primeiras fases do tratamento de incidentes [Scarfone et al. 2008] (*preparação* e *detecção e análise*) de forma que a detecção da máquina interna que gerou o incidente, etapa trabalhosa do processo, é totalmente automatizada. A arquitetura da ferramenta prevê ainda uma atuação na etapa de *isolamento* das máquinas comprometidas. Neste trabalho será apresentado as principais dificuldades que norteiam o tratamento de incidentes, a ferramenta TRAIRA e alguns resultados alcançados com sua utilização.

2. Principais dificuldades do tratamento de incidentes

Segundo [Scarfone et al. 2008], o processo de resposta a incidentes é composto principalmente de quatro fases: *Preparação*, que envolve o estabelecimento e treinamento de um grupo de resposta a incidentes, aquisição de ferramentas e recursos necessários, armazenamento dos registos de atividades dos sistemas para futuras auditorias, etc.; *Detecção e Análise*, onde deve-se detectar ou identificar de fato a existência de um incidente; *Contenção, Mitigação e Recuperação*, fundamental para evitar que o incidente se propague ou afete outros recursos da rede, e para restaurar o funcionamento normal dos serviços afetados; *Ações Pós-Incidente*, que consiste em avaliar o processo de tratamento de incidentes e verificar a eficácia das soluções adotadas.

Cada uma destas fases requer ações específicas de mitigação ou controle. Por exemplo, na fase de detecção e análise, deve-se listar quais os recursos que foram afetados (no caso de incidentes contra a organização) ou qual foi a origem do incidente (no caso de incidentes originados na organização); na fase de contenção e mitigação deve-se isolar os sistemas diretamente relacionados ao incidente e efetuar o tratamento do recurso em questão (desinfecção de uma máquina contaminada com *vírus/worm*, remoção de um artefato malicioso, recuperação de uma página web modificada, etc). No entanto, alguns serviços importantes de rede, como NAT e DHCP, podem dificultar a execução dessas ações.

A técnica de *Tradução de Endereços de Rede* (NAT), tem como ideia básica permitir que, com um único IP roteável na Internet, ou um pequeno conjunto deles, vários *hosts* possam trafegar na Internet. Em outras palavras, com o NAT é possível "esconder" as máquinas da rede interna, ocultando a topologia. No que tange ao tratamento de incidentes de segurança, a principal dificuldade com o NAT está em determinar com precisão o endereço IP interno que foi traduzido no endereço IP externo, uma vez que as notificações de incidentes contêm apenas o endereço IP externo.

Outro agravante é o *Protocolo de Configuração Dinâmica de Hosts* (DHCP), que permite a um *host* obter endereço IP automaticamente, além de outros parâmetros de

configuração da rede. Com o DHCP é possível que um mesmo dispositivo possua diferentes endereços IP ao longo do dia, da semana ou do mês, a depender do tempo de concessão (*lease time*). Com isso, para o tratamento de incidentes, pode não ser suficiente saber o IP interno que gerou a notificação. Faz-se necessário um endereço que identifique unicamente o *host* em questão na rede. Esse identificador será o endereço *MAC* (Media Access Control).

Um terceiro desafio para o tratamento de incidentes é a falta de gerenciamento dos registros de atividades (*logs*) de dispositivos. Esses registros são de grande valor quando um incidente ocorre, pois auxiliam na auditoria dos sistemas afetados. Não obstante, a quantidade, volume e variedade dos *logs* de segurança dos sistemas têm crescido bastante, atrapalhando e até inviabilizando, por exemplo, a investigação de incidentes de segurança gerados por uma instituição. Essa investigação consiste em efetuar buscas nos *logs* do dispositivo de NAT por uma ocorrência do IP e porta listados na notificação e cuja data e hora estejam em concordância com os dados. Vale salientar que, considerando os entraves supracitados, o processo de tratamento de incidentes de segurança em muitos casos é interrompido nessa etapa. Portanto, considera-se que essa é uma etapa passível de automatização.

3. TRAIRA: uma ferramenta para Tratamento de Incidentes de Rede Automatizado

O TRAIRA (*Tratamento de Incidentes de Rede Automatizado*) é um software que atua nas duas primeiras fases do tratamento de incidentes de segurança [Scarfone et al. 2008], a saber, na fase de *preparação* e na fase de *detecção e análise*, de forma a automatizar as atividades trabalhosas que são executadas nessas fases. Na fase de preparação destacam-se duas principais recomendações de boas práticas: i) a configuração do serviço de *logging* remoto do equipamento de NAT e ii) a utilização de um sistema de registro sobre a atribuição de IPs, associando-os aos endereços físicos dos dispositivos de rede: os endereços MAC.

Já na fase de detecção e análise, o TRAIRA utiliza os recursos configurados anteriormente para automaticamente extrair as informações relevantes de uma notificação; buscar por evidências nos *logs* do dispositivo de NAT que informem o(s) IP(s) interno(s) responsável(veis) pela notificação recebida; associar o endereço IP interno à um endereço MAC da máquina, de forma que sua identificação seja única; gerar relatórios e estatísticas sobre os incidentes recebidos; e responder à organização que reportou o incidente. Ainda, sua arquitetura de funcionamento prevê uma extensão desse processo até a fase de contenção, pois permite que a máquina (representada pelo seu endereço MAC) seja bloqueada no *switch* gerenciável (ou roteador) mais próximo. Ao final do tratamento de uma notificação, o TRAIRA gera uma resposta automática à organização que reportou o incidente e também um relatório detalhado para a equipe de apoio a fim de que as medidas cabíveis possam ser aplicadas.

Durante seu desenvolvimento, o TRAIRA foi idealizado para integrar-se a alguma ferramenta que já fosse utilizada nas instituições, ao invés de ser mais um software e um serviço a ser mantido (evitando todas as implicações que isso traz – sistema de autenticação, backup, segurança da própria aplicação, atualização, etc). Obviamente, é muito difícil encontrar uma ferramenta que seja comumente utilizada pelas instituições

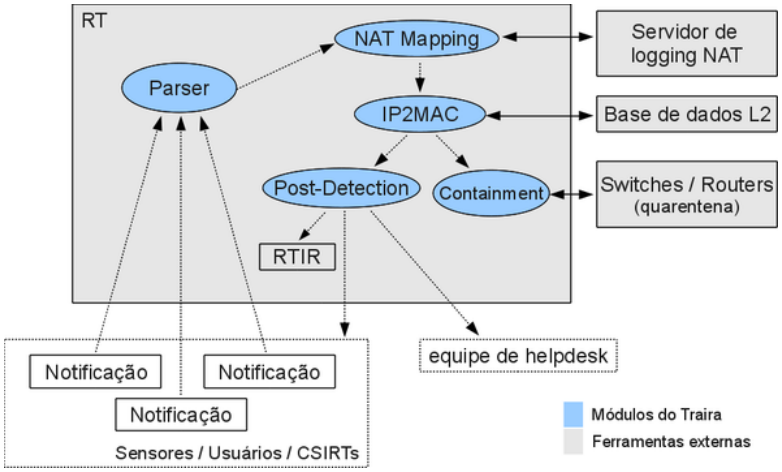

Figure 1. Visão geral da arquitetura do TRAIRA

e ainda permita a integração com um sistema externo, como o TRAIRA. No caso das instituições de ensino e pesquisa clientes da RNP, uma ferramenta bastante utilizada é o *Request Tracker* (RT), como sistema de *helpdesk*. O RT permite a adição de novas funcionalidades através de *extensões*, disponibilizando, inclusive, uma extensão para o gerenciamento dos incidentes de segurança, o *Request Tracker for Incident Response* (RTIR).

Na subseção seguinte, a arquitetura de funcionamento do TRAIRA será apresentada em maiores detalhes.

3.1. Arquitetura do TRAIRA

A arquitetura do TRAIRA é apresentada na Figura 1. Nessa figura, os componentes em formato de elipse (na cor azul) representam os módulos que foram desenvolvidos como parte do TRAIRA e os componentes em formato de retângulo (na cor cinza) representam softwares ou recursos externos necessários ao funcionamento do TRAIRA. O software é desenvolvido como uma extensão do RT, permitindo que o tratamento dos incidentes de segurança seja feito tanto pela interface web, onde o usuário fornece manualmente a notificação do incidente, quanto via e-mail quando a organização que reporta o incidente envia uma mensagem para um endereço de e-mail especialmente designado para este fim. A linguagem de programação utilizada é o *Perl*, com a qual o próprio RT é escrito. Em sua primeira versão, possui aproximadamente 2.500 linhas de código entre interfaces de usuário, núcleo da aplicação, módulos de interface com recursos externos (*logs*, tabela de endereços MAC, etc) e demais componentes. O TRAIRA é distribuído sob a licença GPLv2 ou superior[1] e encontra-se disponível para download em [TRAIRA 2010].

O TRAIRA é composto por cinco módulos (objetos em formato de elipse com preenchimento azul na Figura 1), conforme listado abaixo:

- *Parser:* é o módulo responsável pelo recebimento da notificação e pela extração das informações essenciais ao tratamento do incidente: endereço IP e porta de origem, data e horário.

[1]GPL é uma sigla usada para *GNU Public License*, uma licença de software livre especificada pela *Free Software Foundation*.

- *NAT Mapping:* este módulo utiliza as informações extraídas pelo *parser* e realiza uma busca nos *logs* do dispositivo de NAT para associar a tupla `<data, hora, IP, porta>` a um endereço IP interno, responsável de fato pelo incidente.
- *IP2MAC:* aqui é feita a associação do IP interno ao endereço MAC da máquina. Esse passo é importante em instituições que utilizam o DHCP, pois um IP pode ter sido usado por mais de uma máquina ao longo do tempo.
- *Post-Detection:* Este módulo é responsável pela extração de dados da notificação e do tratamento realizado a fim de gerar estatísticas sobre os incidentes, gerar relatórios à equipe de *helpdesk* (para, por exemplo, efetuar o isolamento e desinfecção da máquina) e responder à instituição que reportou o incidente.
- *Containment:* Neste módulo é feito o isolamento do *host* que causou o incidente para evitar que ele continue com a atividade maliciosa na rede ou afete outros recursos.

Dessa forma, o tratamento de incidentes que podem ser automatizados pelo TRAIRA segue o seguinte fluxo de trabalho:

1. Uma entidade submete uma notificação ao TRAIRA reportando um problema de segurança. Essa notificação deve conter evidências suficientes para comprovar a atividade maliciosa, incluindo, no mínimo, o endereço IP e porta de origem, data e hora que ocorreu o incidente (além do *timezone*). A entidade que reporta incidentes pode ser materializada nos CSIRTs (CAIS, CERT.Bahia, CERT.br, etc), em sensores de monitoramento de atividades maliciosas (IDSs, *honeypots*, etc) ou até mesmo em usuários que submetem incidentes através da interface web;
2. O TRAIRA verifica se existe um *parser* definido para aquela notificação e, caso exista, extrai os dados importantes da notificação e passa para a etapa de detecção da máquina interna. Caso não exista um *parser* definido, a notificação permanecerá em aberto no RT aguardando pelo tratamento manual da equipe de segurança;
3. Usando os dados extraídos da notificação (tupla `<data, hora, IP, porta>`) é feita uma busca nos *logs* do dispositivo de NAT para determinar qual o IP interno utilizou o IP e porta reportados;
4. Uma nova busca é feita; agora para mapear o IP interno em um endereço MAC da máquina que causou o incidente;
5. De posse do endereço MAC, o TRAIRA notifica a equipe de *helpdesk* para que possa tomar as medidas cabíveis;
6. Uma resposta automática é enviada à instituição que reportou o incidente informando que a máquina foi detectada e que os procedimentos de desinfecção já foram iniciados (no caso de máquinas infectadas com *vírus/worm*, por exemplo).

Como se pode perceber, o TRAIRA automatiza todo o processo inicial de tratamento de incidentes de segurança. Não obstante, o tratamento de um incidente ainda não está completo com os passos acima, e o TRAIRA deixa a cargo do administrador definir a próxima providência a ser tomada (por exemplo, desinfectar uma máquina contaminada com *vírus/worm* ou aplicar as medidas administrativas cabíveis à uma violação de *copyright*). Vale destacar, no entanto, que, dado o volume de notificações que uma instituição recebe e a falta de equipe suficiente para responder às notificações, essa etapa de detecção muitas vezes nem chega a ser iniciada. Assim, o TRAIRA proporciona uma importante

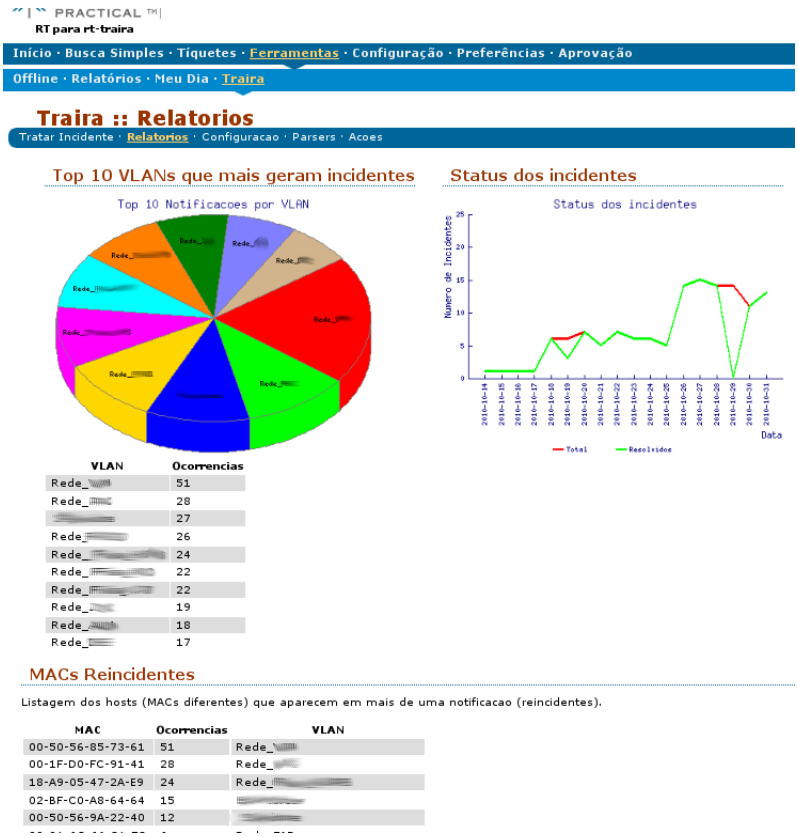

Figure 2. Tela do TRAIRA para exibição de relatórios/estatísticas

contribuição para o processo de tratamento e resposta aos incidentes de segurança de uma instituição.

As etapas descritas acima são executadas de forma *on-line*, ou seja, assim que um incidente é reportado ao TRAIRA, o tratamento é iniciado. A duração do tratamento vai depender da capacidade computacional (processador e acesso a disco) do servidor em que o TRAIRA esteja instalado.

3.2. Geração de estatísticas

Um recurso fundamental aos grupos de resposta a incidentes de segurança (CSIRTs) são as estatísticas [Arvidsson et al. 2001]. Elas ajudam os CSIRTs a detectar tendências, prever futuros ataques em grande escala, direcionar atividades, dentre outros.

A implementação atual do TRAIRA fornece algumas estatísticas geradas automaticamente a partir de informações retiradas da notificação recebida e do tratamento efetuado. A Figura 2 mostra a tela do TRAIRA para exibição de estatísticas (relatórios), baseadas em dados experimentais. Naquela figura tem-se as seguintes estatísticas:

- *Gráfico de incidentes por VLAN.* Esse gráfico ressalta as VLANs que mais impactam na geração de incidentes de segurança, o que permite direcionar medidas de prevenção específicas;
- *Quantidade de incidentes por dia.* Esse é um gráfico quantitativo que pode ser usado para medir a efetividade do tratamento de incidentes de segurança na instituição. Ele lista os incidentes que são reportados *versus* aqueles que foram

resolvidos. O esperado é que a linha de incidentes resolvidos se aproxime da linha dos incidentes reportados e elas tendam a cair (a menos que haja implantação de novos sensores);

- *MACs reincidentes.* Esta estatística pode ser usada como indicador qualitativo do tratamento de incidentes, quando observa-se reincidência na geração de incidentes em determinado *host*. A interpretação desse dado pode levar a uma série de hipóteses, por exemplo: a fase de isolamento e desinfecção não está sendo eficaz; no caso dos incidentes de *vírus/worm* pode indicar inexperiência do usuário no uso do recurso, propiciando novas infecções com facilidade; dentre outros.

4. Resultados Alcançados

Desde a implantação do TRAIRA na UFBA, todos as notificações de incidentes de segurança recebidas pela equipe (sejam aquelas enviadas por ferramentas de monitoramento interno, tais como *honeypots*, IDSs, ou as enviadas pelos grupos de segurança, tais como CAIS, CERT.Bahia, CERT.br) tem sido tratados automaticamente. Por exemplo, as notificações de incidente relacionadas ao projeto Honeypot.BR do CERT.br [Honeynet.BR 2010], do qual a UFBA participa, correspondem a uma média diária de 5 a 10 notificações, e cada notificação contém cerca de 20 incidentes. Tendo em vista que a rede da UFBA conta mais de 10.000 computadores, o tratamento de todas essas notificações era extremamente custoso, do ponto de vista de alocação de pessoal qualificado. Somente em 2010, foram mais de 1200 notificações recebidas na UFBA, e a grande maioria delas foi tratada automaticamente pelo TRAIRA. Com a automatização proporcionada pelo TRAIRA, a equipe de *helpdesk* apenas recebe o endereço MAC dos dispositivos suspeitos identificados pelo sistema e realiza o tratamento das máquinas. A resposta às notificações é praticamente instantânea, comparado à abordagem manual em que cada incidente tomava cerca de 30 minutos para ser tratado, resultando inclusive no não tratamento de algumas notificações.

Outro resultado direto alcançado com o TRAIRA, a partir da análise de suas estatísticas, foi a identificação de quais sub-redes da UFBA mais geram incidentes. Com base nesse resultado, pôde-se iniciar um trabalho específico e direcionado àquelas sub-redes (associadas à unidades acadêmicas) visando identificar o motivo da atividade maliciosa e implantar estratégias de controle e mitigação.

5. Conclusões

Este trabalho apresentou uma ferramenta para automatizar o processo de tratamento de incidentes de segurança, o TRAIRA (um acrônimo para *Tratamento de Incidentes de Rede Automatizado*), que atua nas etapas de detecção e isolamento da origem do incidente, deixando a cargo da equipe de segurança apenas as próximas medidas a serem tomadas. Com a utilização do TRAIRA, reserva-se o time de segurança da instituição (cujo custo de contratação é comumente alto) para o tratamento de incidentes mais importantes ou complexos e para as outras atividades de segurança, como atividades preventivas, por exemplo.

Desenvolvido como extensão do RT, o TRAIRA permite integração com outras ferramentas de resposta a incidentes, especialmente o RTIR (extensão do RT para Resposta a Incidentes), permitindo uma gerência completa sobre um incidente de segurança.

Os requisitos para implantação e execução da ferramenta são simples, indicando, assim, a viabilidade de sua aplicação prática em ambientes complexos e heterogêneos, realidade das instituições acadêmicas de ensino e pesquisa brasileiras.

Atualmente, o TRAIRA encontra-se em produção na Universidade Federal da Bahia (UFBA), sendo usado como base no tratamento de incidentes de segurança para todas as notificações recebidas pela instituição. Além disso, outras instituições de pesquisa e ensino da Bahia já demonstraram interesse em incluir o TRAIRA em seus respectivos processos de tratamento de incidentes, iniciando parcerias com o CERT.Bahia e a UFBA para implantação da ferramenta e treinamento.

References

Arvidsson, J., Cormack, A., Demchenko, Y., and Meijer, J. (2001). TERENA'S Incident Object Description and Exchange Format Requirements. RFC 3067 (Informational).

CERT.Bahia (2010). Estatísticas do CERT.Bahia. Disponível em: http://www.certbahia.pop-ba.rnp.br/Estatisticas. Último acesso em 03 de Dezembro de 2010.

Honeynet.BR (2010). Brazilian Honeypots Alliance. Disponível em: http://www.honeypots-alliance.org.br/. Último acesso em 03 de Dezembro de 2010.

Scarfone, K., Grance, T., and Masone, K. (2008). Computer Security Incident Handling Guide. *NIST Special Publication*, 800–61.

TRAIRA (2010). TRAIRA – Tratamento de Incidentes de Rede Automatizado. Disponível em: http://www.pop-ba.rnp.br/~arquivos/RT-Extension-Traira.tgz. Último acesso em 03 de Dezembro de 2010.