Proposta de Piloto

Grupo de Trabalho Segunda Fase

GT-EWS: Mecanismos para um Sistema de Alerta Antecipado

Daniel Macêdo Batista

1/9/2015

1. Concepção

1.1. Resumo

O GT-EWS teve como principal objetivo alcançado na Fase 1 a entrega do protótipo de um sistema de alerta antecipado (EWS – *Early Warning System*) que antecipa eventos e incidentes de segurança contra a rede e contra os sistemas computacionais da RNP. A antecipação é realizada por meio de um sistema web, coletores de mensagens em redes sociais e sensores de rede. Mesmo durante a fase de protótipo a ferramenta auxiliou o Centro de Atendimento a Incidentes de Segurança (CAIS) da RNP na detecção e resposta a alguns incidentes de segurança envolvendo instituições clientes da RNP. Observou-se uma detecção mais rápida do que se o protótipo não

fosse utilizado. De forma mais detalhada, na Fase 1 confirmou-se que o Twitter e o Facebook são fontes relevantes de informações para um EWS antecipar alertas de vazamentos de dados, orquestrações de ataques e desfigurações de páginas web no escopo da RNP. Outros objetivos secundários alcançados foram a confirmação da viabilidade de realizar correlação entre as várias fontes de dados utilizadas e a confirmação da viabilidade de utilizar firewall, logs, honeypots e informações de redes definidas por software como fontes de dados. O protótipo pode ser acessado em http://gtews.cm.utfpr.edu.br/ews[1] . Para a Fase 2 pretende-se entregar um piloto do EWS a ser utilizado pelo CAIS da RNP como um serviço que auxiliará nas atividades de detecção e respostas a incidentes. O piloto será testado na UFBA, USP, Polícia Federal, além do próprio CAIS, e terá sua interface web focada em fornecer para o analista uma pré-análise dos alertas, acelerando as tomadas de decisão.

1.2. Abstract

The main achievement of GT-EWS in Phase 1 was the delivery of the prototype of an Early Warning System (EWS) that anticipates security events and incidents against network and computer systems located at RNP. The anticipation is realized by means of a web system, message collectors in social networks and network sensors. Even during the prototype phase, the EWS assisted the Service Center for Security Incidents (CAIS) at RNP in detecting and responding to some security incidents involving client institutions from RNP. There was a more rapid detection than if the prototype was not used. In more detail, in Phase 1 it was confirmed that Twitter and Facebook are relevant sources of information for a EWS to anticipate alerts about data leaks, attack orchestrations and defacements of web pages on the scope of RNP. Some secondary achievements were the confirmation of the feasibility of conducting correlation between the various data sources used and the confirmation of the feasibility of using firewall, logs, honeypots and information from software defined networks as data sources. The prototype can be accessed at http://gtews.cm.utfpr.edu.br/ews . For Phase 2 the GTEWS intends to deliver a EWS to be used by CAIS as a service which will assist in the detection and incident response activities. The pilot will be tested at UFBA, USP, Federal Police, in addition to CAIS itself, and will have its web interface focused on providing a pre-analysis of alerts, speeding up decision-making to the security analyst.

1.3. Descrição do produto/serviço

O piloto do EWS proposto na segunda fase do GT-EWS será um sistema de software capaz de antecipar a detecção de orquestrações de ataques, de vazamentos de dados, de desfigurações de páginas web e de vulnerabilidades em software no escopo da RNP. As principais fontes de informação para o EWS serão as redes sociais Twitter e Facebook.

A proposta do GT-EWS é que o EWS seja utilizado como um serviço interno da RNP, pelo CAIS, de modo a reduzir o tempo de resposta a incidentes de segurança envolvendo as instituições clientes da RNP. Idealmente, espera-se que o sistema detecte incidentes antes mesmo deles acontecerem, possibilitando assim medidas que evitem o sucesso de um ataque cibernético. Durante o desenvolvimento do protótipo alguns incidentes de segurança foram detectados e eles servem para ilustrar como o

1 Usuário: RNP Senha: 12345RNP

sistema poderia ser utilizado pelo CAIS. O primeiro exemplo, ilustrado na Figura 1.1, mostra a detecção, feita pelo protótipo do sistema, de um alerta envolvendo a desfiguração de uma página web do MEC no dia 8 de Agosto de 2015.

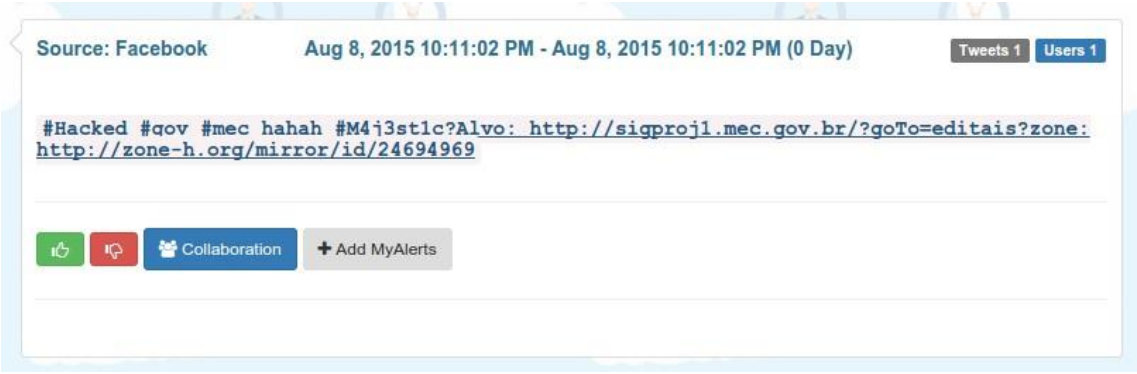

Figura 1.1: Captura de tela do protótipo com alerta sobre desfiguração de página web no domínio do MEC.

A Figura 1.2 mostra que de fato a página foi modificada. Nesse caso específico o CAIS foi avisado e tomou as providências para que os responsáveis no MEC fossem informados a cerca da desfiguração e pudessem retornar o conteúdo anterior da página o mais breve possível (Sem o protótipo, o CAIS seria informado pelo sistema de alertas do zone-h [1] mas tal sistema só envia 1 mensagem diária e bem depois do alerta detectado pelo protótipo).

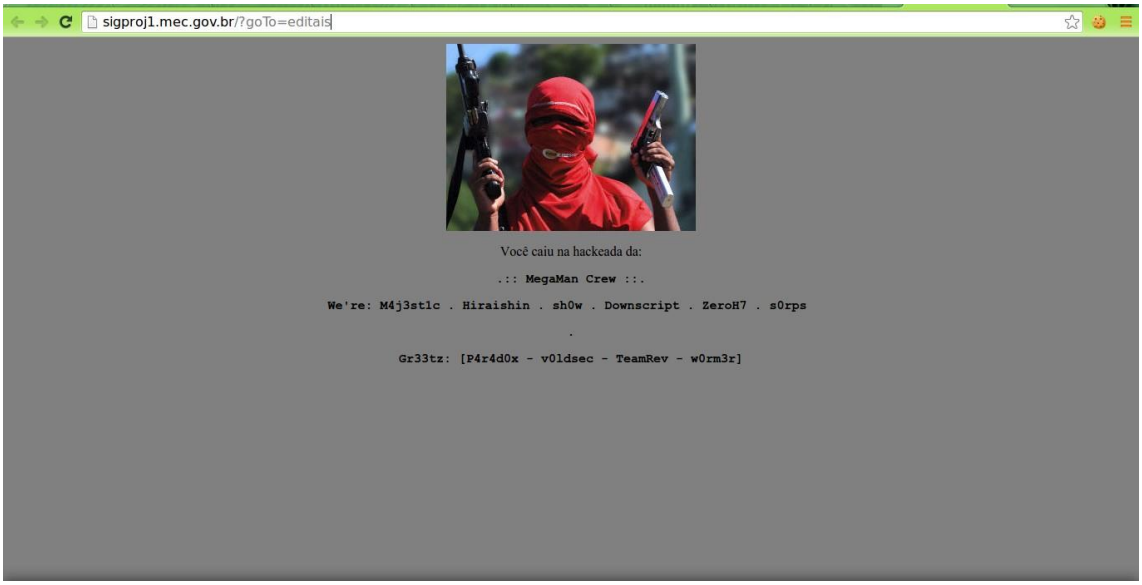

Figura 1.2: Captura de tela de desfiguração de página web no domínio do MEC.

O segundo exemplo, ilustrado na Figura 1.3, mostra a orquestração de um ataque realizada via Facebook.

Figura 1.3: Captura de tela de página no Facebook com mensagens sobre orquestração de ataque.

Os atacantes perguntam qual seria o próximo alvo de um ataque e alguns minutos depois a página de um dos órgãos considerados como alvo foi desfigurada (Figura 1.4). Se alguma instituição cliente da RNP fosse citada nessa mensagem, o CAIS poderia entrar em contato com a instituição instruindo a mesma a verificar se houve acessos indevidos nos últimos dias e também para atualizar os seus servidores. Uma possível opção seria ainda manter a página fora do ar por alguns dias a fim de reduzir o interesse dos atacantes no ataque, já que com a página fora do ar, o status obtido com a desfiguração deixaria de existir.

Um sistema como o que será entregue como resultado da Fase 2 do GT-EWS é importante para reduzir os incidentes de segurança contra a rede da RNP e das suas instituições clientes, reduzindo, consequentemente, (i) possíveis perdas financeiras, que ocorreriam em casos de vazamento de dados sensíveis, (ii) a má reputação das instituições atacadas, que ocorreria em casos de desfiguração de páginas web e (iii) tarefas inesperadas de reconfiguração de sistemas, que ocorreriam em casos de ataques por conta de vulnerabilidades em software.

Do ponto de vista do usuário do sistema, que seriam os analistas do CAIS, espera-se que o sistema facilite os seus trabalhos, acelerando as tomadas de decisão a partir do momento que um alerta for gerado no sistema. Pretende-se que o sistema se integre ao Sistema de Gestão de Incidentes de Segurança (SGIS) do CAIS agindo como mais uma fonte de dados do mesmo. Do ponto de vista dos usuários da rede da RNP, espera-se que o sistema, por intermédio do CAIS, leve a melhorias na percepção de segurança que o usuário tem de todo o ambiente computacional e de comunicação da rede.

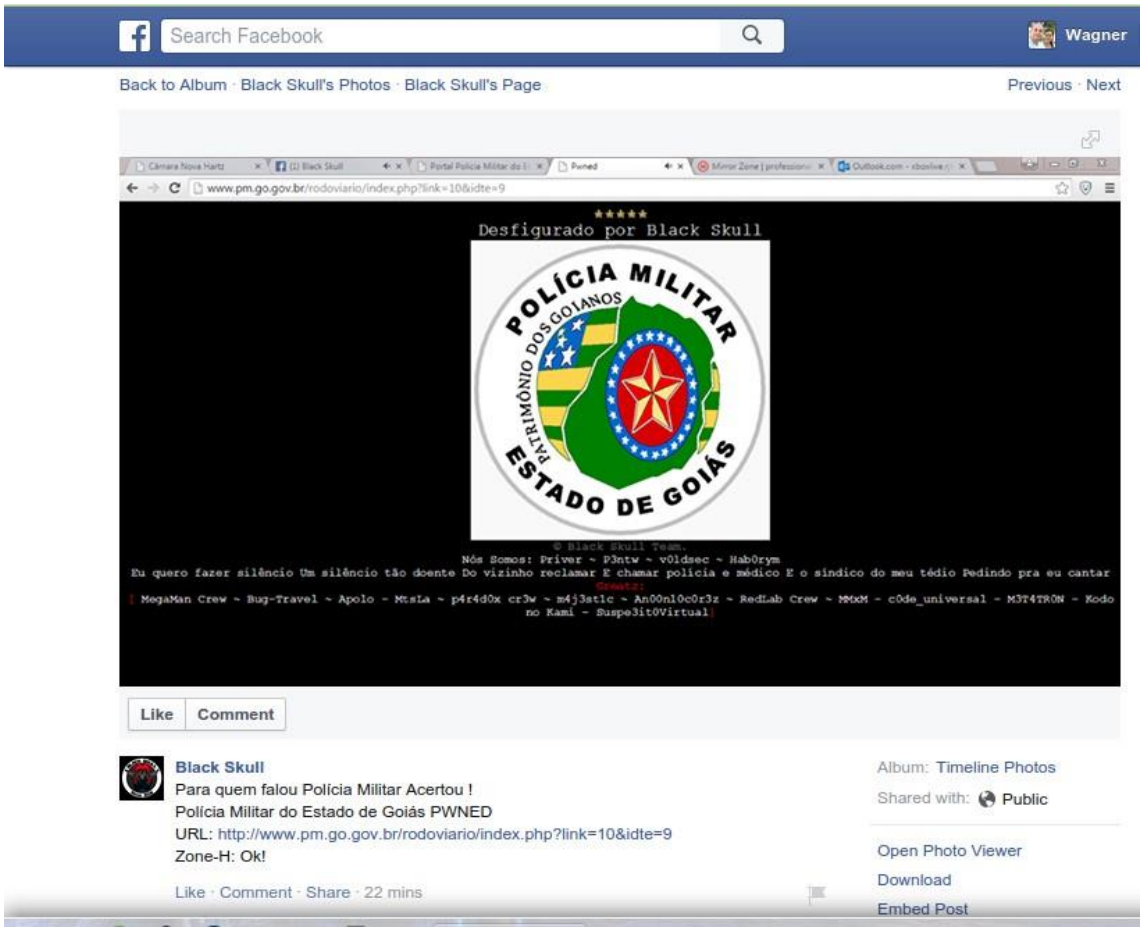

Figura 1.4: Captura de tela de desfiguração de página web no domínio da Polícia Militar de Goiás.

1.4. Identificação do público alvo

O sistema será desenvolvido com o objetivo de ser de uso interno da própria RNP, mais especificamente, pelo CAIS. Dado que o CAIS é o órgão da RNP responsável pela segurança no backbone da rede, é natural que esse órgão seja o principal usuário do sistema. Dentro da rotina de operação do CAIS, o EWS seria mais um sistema a ser usado em conjunto com o SGIS, sistema que centraliza incidentes de segurança enviados por diversas ferramentas. Embora tenha como usuário final o CAIS, todas as entregas de novas versões dos módulos de software que compõe o sistema serão empacotadas de modo a serem facilmente configuradas, personalizadas e instaladas por qualquer instituição. Por exemplo, uma instituição que seja cliente da RNP pode ter interesse em instalar o sistema para monitorar alertas relacionados com palavraschave bem específicas para aquela instituição. De fato os demais parceiros que usarão o piloto provavelmente terão interesses de monitoramento diversos, o que justifica a entrega de todos os softwares independente da utilização pelo CAIS.

2. Definição do piloto

2.1. Arquitetura do piloto

O piloto consistirá de um sistema de software composto por uma interface web, na qual o analista de segurança acessará o sistema tanto para configurá-lo quanto para obter os alertas, por um conjunto de coletores de dados, que monitorarão as redes

sociais Twitter e Facebook em busca de mensagens que antecipem a detecção de vazamentos de dados, orquestrações de ataques, desfigurações de páginas web e vulnerabilidades em software no escopo da RNP, e por uma arquitetura de plugins que permitirá a inserção de novas fontes ao sistema. O EWS será entregue como um pacote de software que poderá ser configurado e personalizado por qualquer instituição, apesar dele ser desenvolvido tendo em vista a utilização pelo CAIS da RNP. O sistema empregará mecanismos de agrupamento por similaridade, para evitar uma enxurrada de informações desnecessárias para o analista de segurança e uma pré-análise dos alertas, acelerando as tomadas de decisão por meio de classificação dos alertas em pelo menos 5 categorias:

- Desfiguração de página;
- Orquestração de ataque;
- Vulnerabilidades encontradas em sistemas operacionais;
- Vulnerabilidades encontradas em serviços de rede;
- Vazamento de dados.

Além da interface web, o usuário do sistema terá a opção de receber alguns alertas por e-mail. A Figura 2.1 ilustra a arquitetura do protótipo integrado ao ambiente do CAIS (a região delimitada pela linha pontilhada no canto direito da figura representa a utilização do SGIS no CAIS. O piloto se acoplará a essa rotina do CAIS).

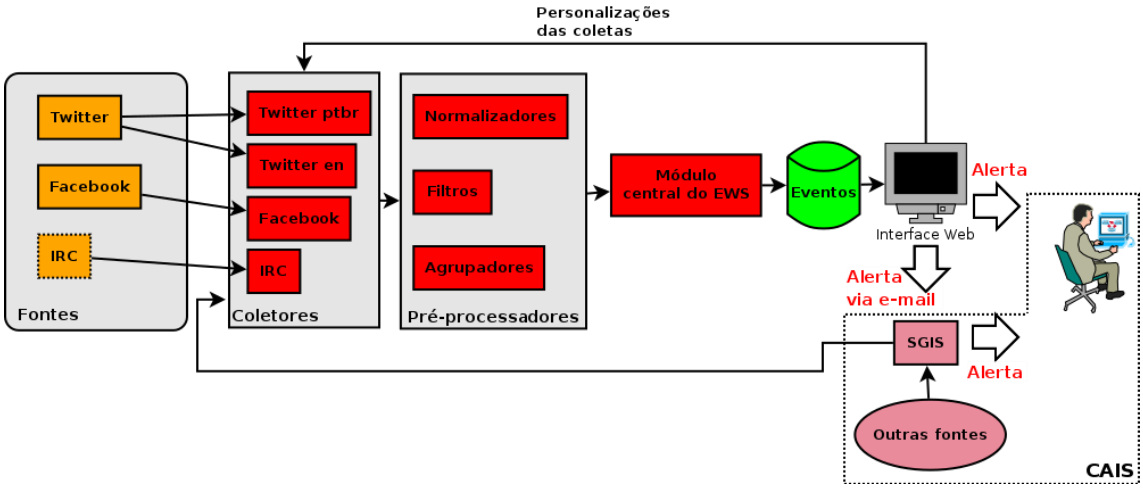

Figura 2.1: Arquitetura do piloto a ser executado no CAIS da RNP

Com exceção da área delimitada pela linha pontilhada no canto direito da Figura 2.1, todos os outros módulos exibidos representam softwares que serão entregues como parte do piloto. Seguindo o fluxo principal de dados a partir da esquerda, mensagens postadas no Twitter e no Facebook são coletadas levando em consideração prioridades e palavras-chave especificadas pelo usuário do sistema. Pretendemos adicionar uma nova fonte de dados que seria o IRC, motivados por resultados recentes que alguns integrantes do GT obtiveram [2].

Os dados coletados passam por uma arquitetura baseada em serviços e módulos acopláveis (plugins), adicionada ao sistema para evitar a necessidade de modificações no núcleo do código caso hajam mudanças nas APIs de acesso às redes sociais. Os módulos acopláveis possibilitam adicionar novos algoritmos para normalização, filtragem e agrupamento. Também possibilitam no módulo central do EWS modificar

os algoritmos para a detecção e correlação de alertas. Módulos acopláveis possibilitam preparar e enviar notificações para diferentes destinos, como por exemplo, para a interface Web ou para o SGIS.

O monitoramento de cada fonte de dados necessita da instanciação de um serviço de coleta (coletor) específico para a fonte. Na arquitetura proposta também é possível a instanciação de serviços independentes para monitorar a mesma fonte. Isso provê um meio de atender monitoramentos específicos ou sazonais sem modificar a configuração dos coletores em execução. Outra vantagem é a possibilidade de distribuir remotamente esses coletores, evitando pontos de falhas e provendo maior disponibilidade por meio da duplicação de monitoramento.

Os plugins de normalização, filtros e agrupamento possibilitam implementar novos algoritmos e carregá-los no sistema sem a necessidade de modificação do códigofonte original. Em geral, são implementados para atender um serviço de coleta específico, mas há situações que um mesmo módulo pode ser carregado para processar informações de serviços de coleta diferentes.

Os dados, intermediados pelos plugins, chegam no módulo central do EWS que é a parte do sistema que tem o papel de correlacionar e priorizar eventos relacionados com incidentes de segurança. Nessa etapa os eventos são também categorizados para antecipar ao analista do que se trata. Por fim, os eventos são mantidos em uma base de dados e exibidos em uma interface web para o usuário. Configurações referentes às coletas nas redes sociais poderão ser feitas também pela interface web.

Além dos alertas serem exibidos na interface web, o usuário tem a opção de recebêlos via e-mail. No caso específico do CAIS, o objetivo é que esses e-mails sejam direcionados para o SGIS e a partir daí cheguem ao analista de segurança. Esse SGIS, que concentra informações de diversas outras fontes de dados, pode inclusive servir também como uma quarta fonte de dados para o EWS. Outras fontes de dados relevantes do CAIS, como listas de URLs utilizadas para phishing, podem também ser usadas no sistema para alimentar as buscas nas redes sociais.

Com relação a equipamentos, o CAIS, a UFBA e a Polícia Federal utilizarão seus próprios equipamentos para instalar e usar o piloto. Em particular, a UFBA utilizará o servidor adquirido com o financiamento da RNP na Fase 1 do GT. A instalação do piloto na USP será realizada em um servidor que está sendo solicitado para essa Fase 2. Outros equipamentos também serão utilizados para manter uma quinta instalação do sistema na UTFPR. Essa instalação será usada para testes antes de novas versões do sistema serem enviadas para os parceiros.

2.2. Instituições participantes

O piloto proposto será implantado nas 4 instituições listadas a seguir. O contato em cada instituição é informado.

- Universidade de São Paulo: O Superintendente da STI da USP, o Professor Dr.

  João Eduardo Ferreira está ciente do projeto e deu o aval para o Professor Daniel Batista, coordenador deste GT, manter um piloto do EWS em funcionamento na STI da USP monitorando atividades suspeitas em redes sociais que indiquem possíveis ataques contra a rede da universidade;

- Universidade Federal da Bahia: O analista de segurança de TI da UFBA, Italo Valcy, participou da Fase 1 do GT como voluntário e mostrou interesse em ter um piloto do EWS em funcionamento na STI da UFBA monitorando atividades suspeitas em redes sociais que indiquem possíveis ataques contra a rede da universidade;
- Polícia Federal: O perito criminal federal da Polícia Federal, Ivo Peixinho, mostrou interesse no projeto, participando inclusive como convidado no workshop de transferência de conhecimento da Fase 1 do GT-EWS, e teve o aval da sua chefia para manter um piloto do EWS em funcionamento na Polícia Federal em Brasília monitorando diversas atividades suspeitas na Internet. A participação da Polícia Federal poderá ser ampliada no futuro a depender dos resultados obtidos com a utilização do piloto em Brasília;
- CAIS da RNP: O analista de segurança Alan Wanderley dos Santos tem mantido contato com os participantes do GT-EWS pois está na lista de discussão do projeto desde a Fase 1. Vários alertas detectados pelo protótipo foram repassados para ele e ele mostrou interesse de agora, na fase de piloto, ter uma versão do sistema para testes e aprimoramentos no CAIS. No CAIS o sistema será usado como mais uma fonte de dados do SGIS.

2.3. Refinamento do protótipo

O feedback dos participantes do workshop de transferência de conhecimento da Fase 1 do GT-EWS foi útil para definirmos diversos refinamentos que precisam ser realizados durante a Fase 2 do GT-EWS. Esses refinamentos são:

1. Mudança do layout da interface de modo a facilitar a visualização para o analista de segurança. Ao invés de separar as fontes de dados por diversas abas, a nova versão deve manter os dados em uma única aba principal. Além disso, os alertas não devem ser mostrados 1 a 1 sem prévia classificação e de forma “crua”. Eles devem ser classificados pelo menos em 5 categorias: Desfiguração de página, orquestração de ataque, vulnerabilidades encontradas em sistemas operacionais, vulnerabilidades encontradas em serviços de rede e vazamento de dados e um único alerta deve ser gerado para todas as mensagens similares. Outras classificações podem ser feitas utilizando *tags* nos alertas. Essa pré-classificação facilitará o processo de tomada de decisão do analista. As informações “cruas” deverão ser mantidas no sistemas mas em uma segunda visão opcional que pode ser escolhida pelo analista. No caso de desfigurações de páginas, um screenshot deverá ser exibido. A interface do splunk [3] e de outros softwares serão estudados e comparados com a interface proposta para o piloto. Se for o caso, a interface atual será descontinuada e alguma interface já bem aceita na comunidade de segurança será utilizada para acesso ao EWS;
2. Integração do EWS com o SGIS do CAIS por meio de envio de e-mails padronizados;
3. Empacotamento e documentação de todo o sistema de modo a permitir a replicação da instalação por todos os parceiros;

4. Definição de uma interface para plugins que facilite a inserção de novas fontes de dados ao EWS, além de servir para facilitar a manutenção nos casos em que ocorram mudanças nas APIs de terceiros. Essa tarefa já vem sendo realizada desde a Fase 1 com a personalização de normalizadores e filtros;
5. Mudança da interface web para permitir que as configurações de palavraschave (e outras configurações) sejam feitas diretamente pela interface;
6. Redução de falsos positivos por meio da implementação de mais técnicas de classificação;
7. Avaliação de possíveis ganhos com a inclusão do IRC como fonte de dados;
8. Melhorar a apresentação das informações georeferenciadas;
9. Integração com a CAFeExpresso para autenticação de usuários na ferramenta. Pode ser útil para instituições cliente que queiram ter uma versão própria do sistema em execução. Como o piloto inicialmente será usado por poucas instituições, essa tarefa será realizada no fim do projeto;
10. Eventual proposta de uma arquitetura para colaboração entre os parceiros baseada na anonimização e compartilhamento de informações;
11. Eventual mudança na arquitetura de modo a centralizar algumas tarefas do EWS, que consumam muitos recursos, na UTFPR ao invés de replicá-las de forma desnecessária por todos os parceiros. Por exemplo, buscas por vulnerabilidades informadas nas redes sociais usando o idioma inglês tendem a retornar sempre os mesmos resultados. Essa busca poderia ser feita na UTFPR e os resultados serem enviados para todos os parceiros.

2.4. Ferramentas de suporte à operação (para propostas de serviço)

Na etapa final do GT, o acesso autenticado ao piloto será realizado por meio da CAFeExpresso. Estudos preliminares para a inclusão desse suporte já foram realizados na Fase 1 e serão finalizadas na Fase 2. Sobre os parâmetros de busca das mensagens relevantes em redes sociais, é necessário um conjunto de palavraschave relevantes, além de listas de URLs de interesse. Ambas informações devem ser usadas na configuração do piloto. Desde o início da Fase 1 o CAIS tem mantido o pessoal do GT atualizado a cerca dessas listas. Esse processo de atualização tem sido feito por meio de arquivos mas será melhorado na Fase 2 para ser realizado por meio da própria interface web do sistema.

3. Cronograma

A Tabela 1 apresentada a seguir lista as tarefas que foram apresentadas na Subseção 2.3 de acordo com o período em que elas serão realizadas.

Atividades	Nov/ 15	Dez/ 15	Jan/ 16	Fev/16	Mar/16	Abr/ 16	Mai/ 16	Jun/ 16	Jul/ 16	Ago/ 16	Set/ 16	Out/ 16	Nov/ 16	Dez/ 16
1	x	x	x	x	x	x	x	x	x	x				
2		x												

3		x			x		x	x					x	x
4			x	x										
5			x	x	x									
6			x	x	x	x	x	x	x	x				
7	x	x	x											
8							x	x						
9												x	x	
10										x	x			
11										x	x	x		

Tabela 1: Atividades

4. Recursos financeiros

4.1. Equipamentos e softwares

A Tabela 2 lista os equipamentos e softwares necessários para a Fase 2 do GT.

Descrição	**Quantidade**
Servidor s/ monitor	1
Desktop s/ monitor	1
Nobreak	1
Módulo de 16GB de memória RAM	3
Disco de 2TB	1
Acesso à VPN	1
Acesso à uma sala no mconf	1

Tabela 2: Equipamentos e software

O servidor s/ monitor será mantido na USP para operação do piloto que será executado na STI da universidade. O desktop s/ monitor juntamente com o acesso à VPN serão usados na UTFPR para monitoramento de salas do IRC. O acesso vai ser feito via VPN para que os endereços IP da universidade não sejam vistos externamente. O nobreak será usado para proteção dos equipamentos na UTFPR. Os módulos de memória e o disco serão utilizados para upgrade do servidor que foi adquirido na Fase 1 e que se encontra na UTFPR. Esse servidor será usado tanto para executar a versão mais recente do sistema quanto para testes da próxima versão.

Por conta do GT possuir integrantes de diversos lugares do país, as reuniões regulares serão realizadas via Internet e para isso a sugestão é que o GT possua uma sala fixa no mconf da RNP.

Boa parte da equipe do projeto já foi definida. O Professor Doutor Daniel Macêdo Batista da USP será o coordenador geral do projeto. Os coordenadores adjuntos serão

o Professor Rodrigo Campiolo e o Professor Luiz Arthur Feitosa dos Santos da UTFPR. O Professor Rodrigo e o Professor Luiz são orientandos de doutorado do Professor Daniel pelo Programa de Pós-Graduação em Ciência da Computação da USP. O Assistente 1 será o Wagner Aparecido Monteverde da UTFPR. Todos esses integrantes fizeram parte da Fase 1 do GT-EWS desde o início do mesmo. O Assistente 3 será selecionado posteriormente.

Por conta do foco intensivo em desenvolvimento nesta segunda fase, dois novos integrantes com experiência prévia em desenvolvimento farão parte do projeto na função de Assistente 2: Thiago Lima Vieira da UFSCAR e Marlon Fernandes Antonio, ex-aluno de graduação da UTFPR.

5. REFERÊNCIAS

[1] Zone-H.org - Unrestricted information. Dispon ível em https://www.zone-h.org/ . Último acesso em 2 de Setembro de 2015.

[2] BATISTA, D. M. ; CAMPIOLO, R. . Análise de mensagens associadas àcibersegurança em redes IRC. In: XV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSEG15), 2015 (Aceito para publicação)

[3] Operational Intelligence, Log Management, Application Management, EnterpriseSecurity and Compliance | Splunk. Disponível em http://www.splunk.com/ . Último acesso em 2 de Setembro de 2015.