EXPERIMENTAL

EWS - Mecanismos para um Sistema de Alerta Antecipado
Hórus CEWS

EQUIPE

Coordenadores:
Daniel Macêdo Batista (IME-USP)
Rodrigo Campiolo (UTFPR-CM)
Luiz Arthur F. Santos (UTPFR-CM)

Desenvolvedores:
Marlon F. Antônio (UTFPR-CM)
Eder S. Ferreira (UTFPR-CM)
Thiago L. Vieira (UFSCAR)

Parceiros:
CAIS
USP
UTFPR

Gerente de projeto:
Wagner Ap. Monteverde (UTFPR)

SITE
gtews.ime.usp.br

CONTATO
Gerência do Programa de GT-RNP: ggt@rnp.br

DESCRIÇÃO

O Hórus CEWS – *Cybersecurity Early Warning System* – é um sistema de *software* para a detecção antecipada de orquestrações de ataques, vazamentos de dados, desfigurações de páginas *web*, vulnerabilidades de *software*, novas ameaças, como ferramentas, códigos de exploração, entre outros, por meio do monitoramento de fontes de dados não estruturadas, em especial, as mídias sociais.

O sistema foi implantado como piloto no Centro de Atendimento a Incidentes de Segurança (CAIS) da RNP, na detecção e resposta a alguns incidentes de segurança envolvendo instituições clientes da RNP, e integrado com sucesso ao SGIS, sistema interno para gestão de incidentes utilizado pelo CAIS. Atualmente, está em implantação definitiva no CAIS como um serviço para a detecção antecipada ou premente de incidentes de segurança.

A arquitetura do Hórus é orientada a serviços, conforme ilustrado na Figura 1.

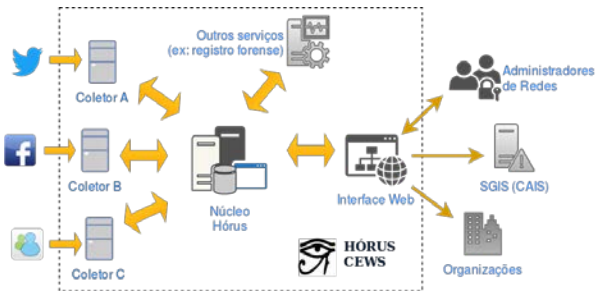

Figura 1: Arquitetura do sistema Hórus CEWS.

Os coletores monitoram mídias sociais e enviam para o núcleo Hórus as informações coletadas e pré-processadas, em um formato estruturado por um canal de comunicação criptografado. Também enviam periodicamente informações do estado de operação. O núcleo Hórus interage com os coletores ao prover autenticação e configurações para o monitoramento e módulos dos coletores. A interface *web* acessa periodicamente o núcleo Hórus, para atualizar os alertas e acessar informações sobre o estado do sistema. Também possibilita a notificação de alertas por outros meios, como correspondência eletrônica. Serviços podem ser acoplados ao núcleo Hórus para

prover novas funcionalidades ou realizar processamentos específicos. Por exemplo, o serviço de registro forense realiza a cópia de sítios desfigurados, códigos de exploração e vazamento de informações. Administradores podem colaborar com o sistema, confirmando alertas e evidenciando notificações importantes.

As principais funcionalidades disponibilizadas pelo sistema Hórus são: (i) monitorar potenciais alertas/incidentes publicados em mídias sociais (Twitter, Facebook e IRC); (ii) classificar os alertas em diversas classes para facilitar o trabalho dos administradores; (iii) fornecer informações importantes para a investigação de ataques, como capturas de telas de páginas desfiguradas; (iv) gerenciar os sensores pela própria interface *web* do sistema; (v) produzir uma linha do tempo dos alertas; (vi) calcular o índice de risco de diferentes instituições a partir dos alertas capturados; (vii) permitir a categorização manual dos alertas, à medida que eles vão sendo analisados pelo administrador; (viii) exibir informações georreferenciadas a respeito dos alertas capturados; (ix) gerenciar várias configurações do núcleo do sistema na própria interface *web*.

A Figura 2 apresenta o menu principal do sistema e a tela de detalhamento de alerta. Observa-se um alerta que foi classificado como uma desfiguração (*deface*) e o grau de confiança da notificação é de 97%. Além da informação da desfiguração, o alerta notifica sobre uma futura ameaça a sítios do Governo. A classificação do alerta e a extração de entidades pelo Hórus é realizada via modelos gerados para a língua portuguesa usando técnicas de processamento de linguagem natural.

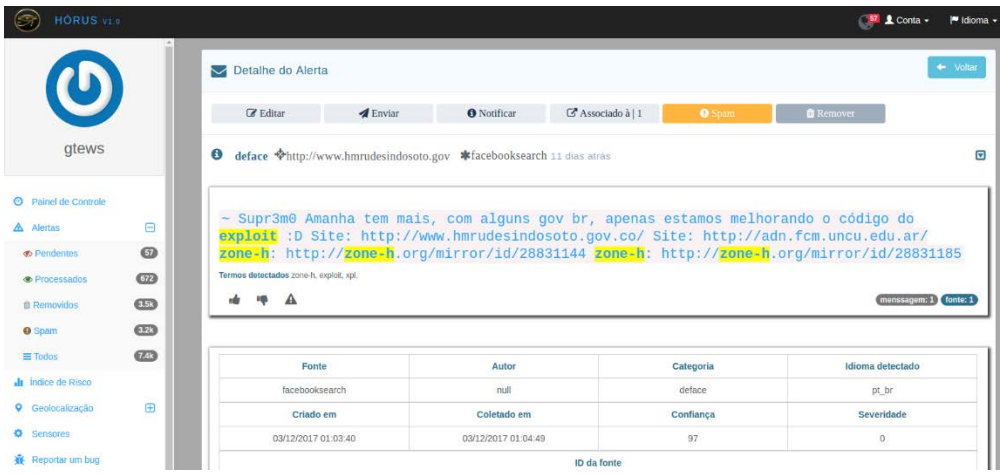

Figura 2: Exibição detalhada de alerta no Hórus.

O Hórus CEWS visa antecipar ou reagir rapidamente aos incidentes de segurança contra a rede da RNP e das suas instituições clientes, consequentemente reduzindo (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.

O sistema foi desenvolvido considerando aspectos de facilidade de uso e adição de novos módulos, como de coleta, normalização, filtros e processamento. Como consequência, pode ser adaptado para atender necessidades específicas de clientes que precisam monitorar mídias sociais visando identificar ameaças ou ataques contra organizações ou indivíduos.