TECH CORNER

20/06/2014

CIBERINTELIGÊNCIA: afinal, quem precisa dela?

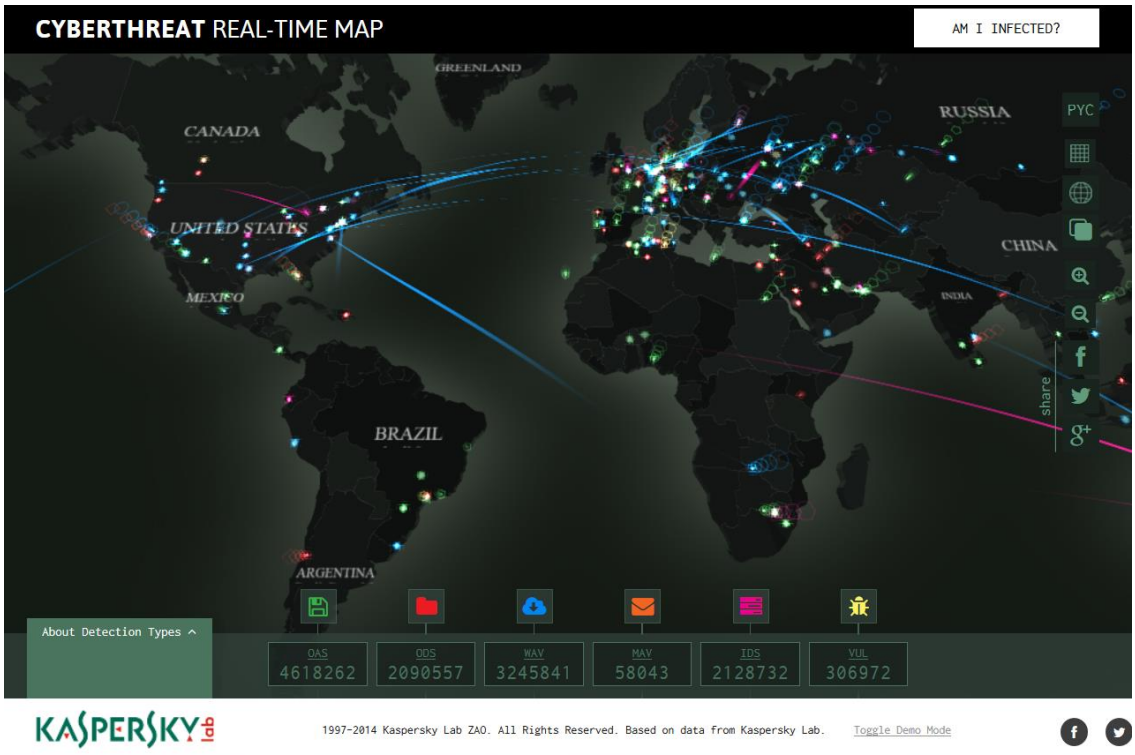
Adriano Mauro Cansian
Unesp (Universidade Estadual Paulista) e
ACME! - Laboratório de Pesquisa em Cibersegurança
André Ricardo Abed Grégio
Unicamp (Universidade Estadual de Campinas) e
CTI (Centro de Tecnologia da Informação Renato Archer)

Como pesquisadores de segurança cibernética, infelizmente temos constatado que, contra um panorama atual de ameaças mutantes cada vez mais complexas e cibercriminosos ou ciberterroristas cada vez mais especializados, os profissionais da área estão se tornando desarmados e ultrapassados. Uma batalha contra o tempo é travada diariamente. A estratégia tradicional de esperar por um alerta e, em seguida, responder a um evento, tem se mostrado ineficiente contra ameaças que se propagam e se sofisticam rapidamente. Respostas tardias a eventos que envolvem segurança da informação, colocando em risco os ativos tangíveis e intangíveis de uma organização, representam um grave problema para as instituições.

Durante o ano de 2013 e este início de 2014, nossas pesquisas sobre o cenário brasileiro apontam que os ataques direcionados e coordenados, associados a exemplares de malware artesanalmente preparados, estão aumentando em número e em sofisticação técnica, ao passo que nossas capacidades de detecção e de resposta estão se tornando inadequadas. Ameaças avançadas persistentes (APTs - Advanced Persistent Threats), espionagem organizacional e de Estado, crimes eletrônicos e financeiros, roubo de propriedade intelectual e ataques de negação de serviço tornaram-se muito mais frequentes, complexos e orquestrados. Isso tem exigido dos analistas de segurança da informação a defesa proativa de suas redes e dados, além de uma elevada capacidade de atualização, somada a instrumentos, técnicas e conhecimentos para lidar com as ameaças.

Assim, temos proposto que deve-se aplicar conceitos de inteligência cibernética como um meio de combate eficiente e eficaz contra ameaças atuais. Dados coletados tanto em sistemas de detecção de ataques como em analisadores de malware desenvolvidos no âmbito de nossas pesquisas nos permitem afirmar que, sem mecanismos de inteligência cibernética e de análise de ameaças eficientes, não teremos mais condições de nos proteger adequadamente. Dentro de uma janela de tempo aceitável, nós teremos dificuldades em compreender e avaliar variáveis importantes para a defesa cibernética, entre elas: as motivações e os métodos dos atacantes, as deficiências e vulnerabilidades existentes interna e externamente, os mecanismos de execução e ativação de malwares, por quanto tempo o oponente tem transpassado ou estado dentro de nossas linhas de defesa, ou até mesmo os vetores de ataque que levam às ameaças propriamente ditas.

A Rede ANSP é um projeto de infraestrutura de apoio à pesquisa, financiado pela FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo), por meio do processo nº 13/11711-5. O coordenador científico é o Prof. Dr. Luis Fernandez Lopez, docente da Faculdade de Medicina da Universidade de São Paulo. Av. Dr. Arnaldo, 455, 2º - CEP 01246-903 - São Paulo – SP –tel.: 55-11-3061-8600.



Mapa de Ciberameaças produzido em tempo real pelo Laboratório Kaspersky. (Instantâneo obtido em 22/07/2014, às 18h15, horário de Brasília, Brasil). Fonte: http://cybermap.kaspersky.com/

Os sistemas integrados para defesa de redes agregam diversas tecnologias de proteção, incluindo sistemas de prevenção e detecção de intrusos, firewall, bloqueio de spam, antivírus aplicado ao tráfego de rede e arquivos em trânsito, controle de acesso a documentos, filtragem de conteúdo na camada de aplicação, armazenamento e análise de logs, e mecanismos para tratamento de tentativas de negação de serviço. Entretanto, a mera implantação de um sistema desse tipo, robusto e com uma ampla gama de mecanismos de segurança, não garante a proteção da rede. Esses sistemas integrados dependem de configuração especializada e detalhada, atualização constante dos subsistemas, assinaturas e heurísticas de detecção, bem como da análise dos dados coletados, (logs, alertas, estatísticas, arquivos em quarentena) e tomada de contramedidas.

Para tanto, é preciso promover a formação de profissionais conscientes e altamente capacitados que possam atuar onde a máquina não pode. É neste ponto que os conceitos de ciberinteligência devem ser aplicados. Afinal, um sistema de contra ameaças é tão bom quanto o classificador que foi desenvolvido e treinado para tal fim; sistemas de detecção de ataques e antivírus são tão eficazes quanto as assinaturas conhecidas e heurísticas desenvolvidas; anti-malware só é efetivo em relação aos exemplares conhecidos; anti-spam é tão eficiente quanto a configuração de segurança do servidor de e-mail e a qualidade das listas de bloqueio utilizadas; um log é tão informativo quanto a capacidade e abrangência de se registrar eventos para auditoria. Todos esses dados, advindos de fontes distintas e com diferentes tipos de informação e possibilidades de correlação, são tão úteis

quanto a expertise do profissional de segurança que se beneficia de sua análise para defesa cibernética e proteção dos sistemas sob sua responsabilidade. Sem recursos humanos, não há análise de ameaças. Sem análise de ameaças é impossível prover segurança adequada.

Atualmente todos os sistemas mais avançados de segurança utilizam a análise de ameaça cibernéticas como parte fundamental de seus mecanismos. Ainda existem poucas instituições mundiais atuando e fornecendo dados públicos ou privados sobre análise de ameaças e ciberinteligência. Nós advogamos que é imperativo que exista no Brasil pelo menos um centro de análises de ameaças cibernéticas, com capacidade para fornecer informações sobre conhecimento das vulnerabilidades internas e externas relacionadas com ataques cibernéticos do mundo real. Ciberinteligência, afinal, nós realmente precisamos dela.

---

http://www.acmesecurity.org (ACME!)

São Paulo, 20 de junho de 2014.