ANAMARIS

ANálisis de Actividad MAliciosa y Respuesta a IncidenteS

Carles Fragoso i Mariscal
Centre de Supercomputació de Catalunya

IRIS-CERT - RTIRIS-19

26 de Mayo del 2005

Un día cualquiera en la vida de un profesional de la seguridad...

- ✓ Una serie de alarmas en el sistema de detección de intrusos perimetral llama nuestra atención:
  - ¿Qué es este tráfico tan extraño?
  - ¿Habrá alguien más que lo esté recibiendo?
  - ¿Puedo confiar en alguien ajeno a mi institución para correlar esta actividad?
  - ¿Qué herramientas y técnicas de monitorización están utilizando los demás?
  - ¿Cómo puedo contener el problema?

¿estoy solo en este mundo?

¿A quién llamarás?

Análisis de Actividad Maliciosa y Respuesta a IncidenteS

- ✓ **ANAMARIS:** iniciativa para la creación de un foro técnico especializado integrado por técnicos en seguridad informática con el objetivo de fomentar el análisis de actividad maliciosa y dar respuesta a incidentes de forma coordinada en la comunidad RedIRIS
- ✓ Objetivos:
  - Mejorar la detección temprana de actividad maliciosa
  - Analizar nuevas amenazas y estudiar sus contramedidas
  - Respuesta coordinada a incidentes
  - Correlación de actividad maliciosa
  - Intercambio de técnicas, herramientas y scripts
  - Transferencia de conocimiento al resto de comunidad RedIRIS

Los personajes aquí expuestos son propiedad de © Columbia Tristar

ANálisis de Actividad Maliciosa y Respuesta a IncidenteS

- ✓ Coordinación:
  - Carles Fragoso i Mariscal (CESCA)
  - IRIS-CERT
- ✓ Participantes:
  - Administradores habituales de seguridad perimetral: ids, cortafuegos, etc.
    - Nota: deben ser autorizados por su correspondiente PER
- ✓ Recursos:
  - Lista electrónica de correo
  - Repositorio de herramientas, “scripts”, etc.
  - Base de datos de conocimiento
- ✓ Proyectos:
  - Sondas de monitorización de espacio IP oscuro
  - Herramientas de correlación de alertas
  - Recogida automática de código malicioso

ISC/DShield

NSP-SEC

ANAMARIS

ANálisis de Actividad MAliciosa y Respuesta a IncidenteS

¡¡¡Gracias por tu atención!!!

mynetwatchman

malware collect alliance

Honeynet Project Alliance

http://www.rediris.es/cert/proyectos/anamaris.es.html