9º Foro ABUSES

Fecha 20 y 21 de Octubre
Lugar: Edificio Caisanova (LA Coruña)

Asistencia

Asistieron unas 33 personas el primer dia (dia abierto) y 25 el Segundo (dia cerrado solo para miembros). Abajo del mensaje os incluyo la relación de instituciones que asistieron. Agradecer la asistencia de todos pero si podría destacar la de:

- Cristobal Lopez (gerente de Espanix)
- Luis Maria Uriarte (Fiscalía Provincial de Pontevedra, Miembro del Servicio de Criminalidad Informática (SCI)
- Manuel Vazquez López Comisario Jefe de la B.I.T. (Brigada de Investigación Tecnologica)
- Juan Salom (Grupo Delitos Telemáticos de la Guardia Civil)

Organización.

Foro ABUSES es una grupo sin intereses comerciales (gratuito) y sin esponsorización (nunca han sido aceptados los comerciales). Las reuniones se organizan fundamentalmente en salones de universidad que es donde tenemos mas contactos. La asistencia media son 30-40 personas dependiendo del lugar (Madrid tiene mas asistencia). Tiene un enfoque mas cercano al grupo de trabajo y debate que a presentaciones magistrales. Los cafes (2 por Jornada) los paga quien lo organiza y hasta ahora en un 80% de ocasiones los viene pagando RedIRIS. Las 2 comidas y 1 cenas se pagan a tocateja.

En esta ocasión todo ha sido diferente. Lo ha organizado el ISP gallego con un nombre tan corto como "R" dejándonos un magnifico salón de actos en un edificio de Caixanova en el centro de la ciudad. El caso es que han estado sobresaliente, no solo pagado los cafés, sino que nos han obsequiado con unos detalles (paraguas, camisetas, bolis etc) y sobre todo nos invitaron a cenar en un sitio especial y reservado los restaurantes de la comidas. Quiero resaltar la amabilidad de Abel y su buen hacer en "R" pero en general de todos sus compañeros y directores. Han dejado el listón demasiado alto para lo que

estamos acostumbrados en el Foro ABUSES.

Desarrollo

La estrella de esta convocatoria fue una mesa redonda muy completa sobre el estado del arte en intercambio de incidentes entre juzgados, policía (comisarias), guardia civil e ISPs. Para esta sesión asistieron un fiscal, un comisario (policia) y un Guardia civil, moderado por un ISP: Telefonica. Con lo cual coloqué todos los eslabones en una sola mesa. El tema es muy complejo, las cosas no funcionan como a todos nos gustaría pero se va avanzado pasito a pasito. Me resulta difícil hacer un resumen de lo tratado en esta sesión que duró desde las 10.30h hasta las 14.00h. Se sacaron conclusiones y una linea de trabajo que os comentaré en el apartado de conclusiones.

Por la tarde hubo una serie de presentaciones técnicas spam, botnets, plataformas de correo etc) de diversos ISPs y la presentaciónde un nuevo servicio de INTECO (http://osi.gob.es). Tambien se presentó un nuevo miembro: **Dinahosting** y un ISP de León (**Argored**) interesados en ser miembros de ABUSES.

Al dia siguiente hubo una presentación sobre una magnifica herramienta desplegada por Euskaltel para el cumplimiento de la Ley de retención de datos. Luego se trataron temas propios del Foro ABUSES: spamtraps, botnets, intercambio de incidentes, nuevos miembros

Conclusiones

La oportunidad que tuvimos de contar con miembros de la fiscalía y los cuerpos de seguridad ha dado lugar a una iniciativa para mantener una sección dentro del las páginas de información del foro abuses (www.abuses.es), dedicada a informar de los aspectos a tener en cuenta a la hora de solicitar información a un ISP dentro de una investigación (* Basicamente hay muchos problemas y lentitud algunas veces o desconocimiento, de forma solicitando al proveedor equivocado determinada información (por ejemplo exigir a un proveedor de alojamiento que identifique al usuario de una dirección IP, etc, la idea es mantener este sitio "centralizado" con la información que se puede solicitar y como, y a quien), de forma que se pueda ir mejorando esta comunicación.

Así mismo se decidió mantener el canal de comunicacion (lista de correo electrónico), mantenido en RedIRIS entre la fiscalia y los miembros del Foro (ISP, CERT, Policia), para tratar los aspectos y dudas que puedan ir surgiendo.

A nivel de aspectos operativos entre los diversos operadores , se ha seguido avanzando en un formato, adaptado del empleado en RediRIS, para compartir entre diversos operadores la información de listas de reputación que permita complementar el servicio de Listas blancas .

Se acordó estudiar la compartición de información de controladores de Botnets entre los diversos operadores para así mitigar un poco los problemas de seguridad existentes.

En las reuniones se intenta acordar la temática principal de la siguiente, centrada sobre todo en la coordinación con las entidades financieras, no sollamente como mitigación de los problemas de seguridad, sino también los problemas de uso incorrecto de SPF, campañas publicitarias , etc que muchas veces ocasionan problemas los operadores.

Asistentes

ISPs:

Arsys Internet.(1)
Abansys & Hostytec, S.L.(1)
Infortelecom Hosting (1)
R Cable y Telecomunicaciones (4)
Sarenet(1)
Argo Redes y Servicios Telemáticos, S.A.(1)
EUSKALTEL, S.A. (1)
Hostalia/ACENS (1)
Telefonica de España (5 personas)
RedIRIS (3 personas)
Dinahosting (1)

Certs

INTECO (2 personas)
CCN-cert (1)

CESICAT (1)

Cuerpos de Seguridad del Estado

BIT (2 personas)
Guardia Civil ciberterrorismo (3 personas)
Guardia Civil delitos telematicos (1)

No miembros

Argored (3)

Especiales

Espanix (1)
Fiscalia Pontevedra (1)