Técnicas avanzadas de “phishing” y posibles soluciones

Asociación de Usuarios de Internet

Miguel Pérez Subías

Programa

- **10:30 Bienvenida**
- **10:35 – 11:00 El phishing: estadísticas, efectos y consecuencias**
- **11:00 – 11:45 Técnicas avanzadas de phishing**
- **11:45 – 12:00** *Descanso*
- **12:00 – 12:45 Soluciones disponibles y buenas prácticas para evitar el "phishing"**
- **12:45 – 13:15 Coloquio y debate**

Definición

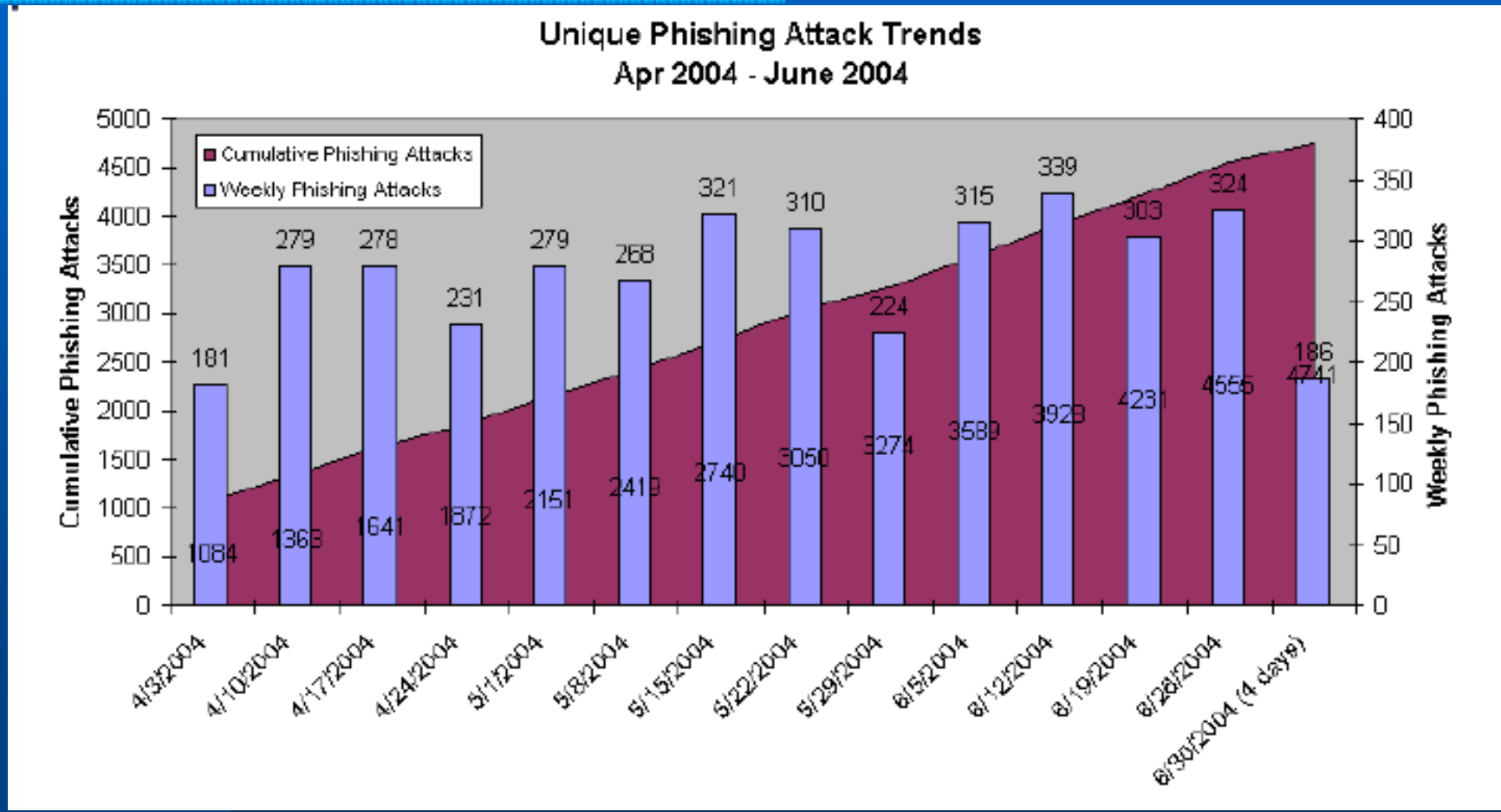
"Phishig, piching, ….

Son ataques que buscan obtener las credenciales (identidad, clave de acceso) de los usuarios de un servicio electrónico las cuales pueden utilizarse posteriormente con fines fraudulentos"

Fines

- Beneficio económico, que se puede obtener directamente realizando transacciones o indirectamente provocando cambios puntuales de cotización.
- Desprestigio de una empresa, entidad u organización.
- Desprestigiar el medio y sus aplicaciones

Una práctica que sigue creciendo



Características del “phishing”

- Combina técnicas de Spam o Spyware con falsificación de webs o el uso de vulnerabilidades
- No le hemos dado hasta ahora la importancia que tiene.
- Es un problema que afecta a cualquier web transacional que exija acreditación: Bancos, Administración Electrónica, Tiendas on-line
- Es un problema global que acaba de despertar y que esta en plena evolución
- Los efectos del phishing son tremendamente costosos y sobre todo dañan y erosionan la confianza de los Usuarios

Evolución tecnológica y social

- Las falsificaciones y los mensajes cada vez se adaptan más a los lenguajes y aplicaciones reales
- Aumentan las posibilidades de manipular los navegadores y las aplicaciones
- Se explotan nuevas vulnerabilidades en las aplicaciones y en los servidores
- Hay una especialización en lo tecnológico y en lo financiero
- El Spyware se esta desarrollando a gran velocidad
- El Spam no encuentra respuestas contundentes que atajen la impunidad económica y legal de quienes lo practican
- La implantación de la firma electrónica avanza despacio

Consejos “erroneos” que se sugieren

- *“No hagas caso de lo que te llega por el correo electrónico”*
- *“Utiliza claves robustas de 8 caracteres alfanumericos o superiores y cambialas con frecuencia”*
- *“ Comprueba que la web es segura https “*
- *“ Comprueba que la dirección de la página es la correcta “*

Evidencias a tener en cuenta

- Internet es un entorno abierto y por tanto la identificación debe de ser mutua entre usuarios y aplicaciones
- Estamos ante un sistema en plena evolución y con cambios continuos
- Los sistemas complejos y complicados acaban por no utilizarse
- La responsabilidad de la Seguridad debe de recaer en las aplicaciones no en los Usuarios
- Los sistemas y aplicaciones en la red deben de reforzarse positivamente.

Es necesaria la cooperación

- Para definir el tamaño y conocer el alcance del problema
- Identificar las tecnologías y las soluciones que pueden ayudar a solucionar o mitigar el problema
- Conseguir que industria, usuarios, reguladores y cuerpos de seguridad trabajemos juntos para dar respuestas rápidas y eficaces
- Coordinar nuestros esfuerzos con otras iniciativas internacionales (www.antiphishing.org)

Necesitamos respuesta urgentes

- Buscando un equilibrio entre eficacia, coste y oportunidad

“ Mejor dar soluciones rápidas ahora que esperar 5 años a tener la solución perfecta “

Nuestro reto

Crear un grupo de trabajo especializado en phishing para:

- Disponer de un inventario actualizado de las amenazas actuales y futuras
- Disponer de un foro común en el que plantear posibles soluciones y propuestas para su discusión y/o evaluación.
- Disponer de un inventario de posibles soluciones
- Conseguir sistemas que permitan obtener alertas tempranas de estos ataques.
- Compartir planes de formación/información y políticas para los responsables de Seguridad de los servicios transacionales.
- Trasladar a la Sociedad el mensaje de que asumimos el reto de superar estas dificultades

Primera etapa el “Día de Internet”

El 25 de Octubre, “**Día de Internet**”

“**Conferencia internacional sobre phishing**”

Con un papel relevante a las soluciones y a las propuestas de Bancos y e-administración

Por qué el "Día de Internet"

Porque disponemos de elementos y de tecnología suficiente para dar respuestas en tiempo.

Algunos ejemplos:

- **Centro de Alerta Temprana Antivirus**
- **Red Sanet de sensores de spam**
- **Pasarelas de seguridad para móviles**
- **Servicios y aplicaciones y consultores del máximo nivel**

Muchas gracias