**John the Ripper**

Ricardo Rubio

Victor Pineda

Aldair de Gracia

Kevin Aparicio

La empresa Wasser que se dedica al suministro de agua potable es subcontratistas del gobierno, y se encarga de distribuir el vital líquido por el extremo norte de Noruega.  
  
 Se produjo un ataque cibernético el cual inicio cuando la compañía se disponía a aumentar el personal de logística para aumentar el área de cobertura. De esta manera un lunes por la mañana un empleado del sector de recursos humanos recibió un correo que sobre un currículo de una persona solicitando empleo en las instalaciones de la empresa, e incluía una dirección URL que mostraría los proyectos realizados por el aspirante al puesto.   
Dispuesto a evaluar dichos proyectos, abre el link y sin saberlo, se descarga un caballo de Troya que toma control de la computadora y los atacantes encuentran la manera de sobrepasar el firewall y acceder la intranet de la compañía.

Después de tener acceso al equipo, navegan a través de la intranet y toman control de uno de los desarrolladores del sistema interno de contabilidad y usando un programa criptográfico llamado John the ripper el cual aplica fuerza bruta para descifrar contraseñas logran romper el candado digital donde el usuario guardaba las contraseñas de los servidores de desarrollo y producción.

Las contraseñas no era lo suficientemente seguras y el software pudo descifrarlas.

Sabiendo que los operadores no podían eliminar información de la BD. Los atacantes actualizaron los registros de pagos de los clientes a 0.

Cuando el gerente se dirigía a su oficina para realizar un reporte de rutina observo que el promedio mensual de pago era 0 en todos los clientes, desconcertado realizo una llamada urgente a los departamentos sistemas y computación. El daño estaba echo los registros se habían perdidos. La culpa se la echaban en cara jefes de IT. En parte por darle cuentas de administrador en los equipos de trabajo a personas de recursos humanos que generalmente trabajan en ofimática y respondes correos, ellos no deberían tener ese privilegio de instalar software en los equipos. Pero Había que reaccionar rápido. Como eliminar este intruso del sistema

Este programa se dice de fuerza bruta pues prueba múltiples combinaciones de palabras y caracteres entremezclados así también palabras de diccionario ya que las contraseñas de los usuarios generalmente son palabras o nombres de personas.

Por esta razón es importante capacitar a todos los empleados con acceso al sistema sobre algunos aspectos importantes sobre seguridad informática y aplicar el concepto de darle en las maquinas privilegio de administrador solo a aquel que tenga la capacidad de comprender lo que esto significa.

Gracias a que el equipo técnico hacia respaldos semanales y cada dos días pequeños respaldos temporales. se pudo recuperar gran parte de la información. Para recuperar la otra parte de la información hubo que recurrir a los documentos físicos almacenados en la corporación y contactar a los algunos clientes para recuperar datos de vital importancia como números de teléfono.

Se elimino el software malintencionado, cambiaron contraseñas por algunas más seguras y al personal no esencial les asignaron recursos limitados en active directory para que no pudiesen instalar programas o aplicaciones sin el permiso de un operador.