iCoaching

#iRes® 4 le ocurrió a un amigo

Christian Javier Vila

CTO - ISec Global Inc

una historia real que cuenta sobre:

abogado estafador & un hacker

y un final feliz!... (para el hacker)

resulta que un día un amigo mío tuvo en accidente en motocicleta…

si así quedó la moto (imaginen mi amigo!)

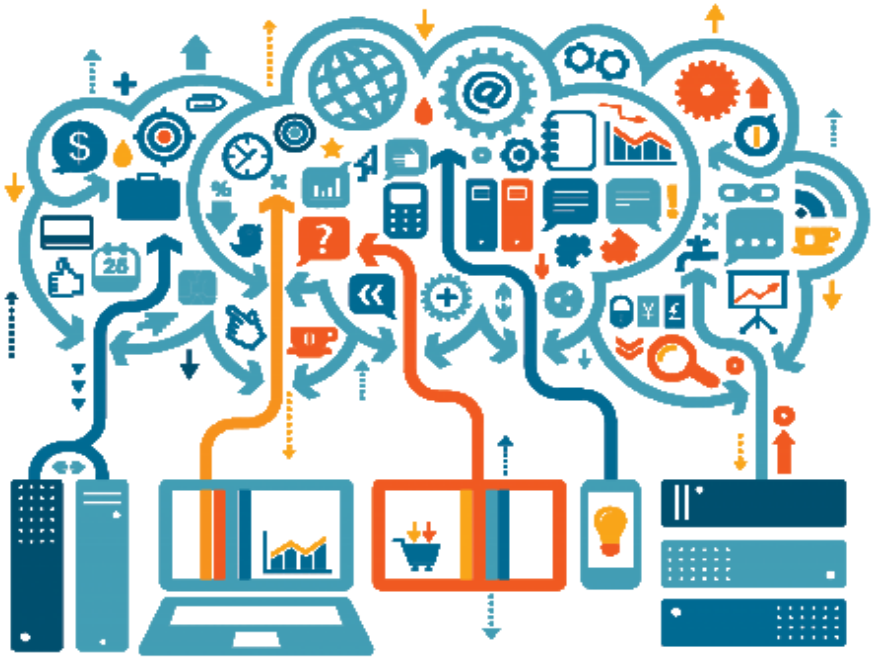
- hospital + 4 operaciones + rehabilitación + prótesis…
- prótesis generó una deuda de $15mil
- y a los 2 meses…
- llamado de abogado diciendo que su deuda de 15mil se transformó en 15mil+100%intereses+100%honorarios
- *y que después de 48 horas iban a ser 5%semanal*
- mi amigo pensó: **[habrá que salir a mojarse los pies!!!]**

y en 48 horas…

Copyright © 2017 ISEC GLOBAL inc. Todos los derechos reservados - www.isec-global.com

en 48 horas… 1) data mining

buscó algo de data del estafador:



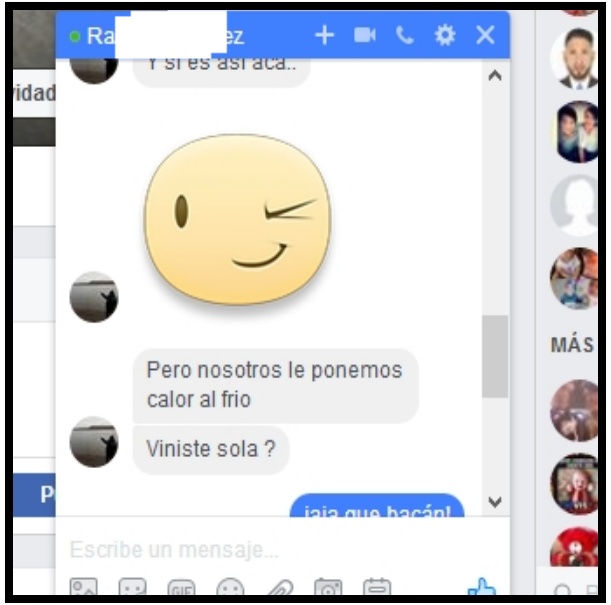
REDES_SOCIALES
GEOLOCALIZACIÓN
INFO_ENTORNO_LABORAL
APLICACIONES_QUE_USA
DEBILIDADES_EXPLOTABLES
PRESENCIA_EN_INTERNET
INFO_ENTORNO_SOCIAL
NÚMERO_CELULAR
DIRECCIONES

Copyright © 2017 ISEC GLOBAL inc. Todos los derechos reservados - www.isec-global.com

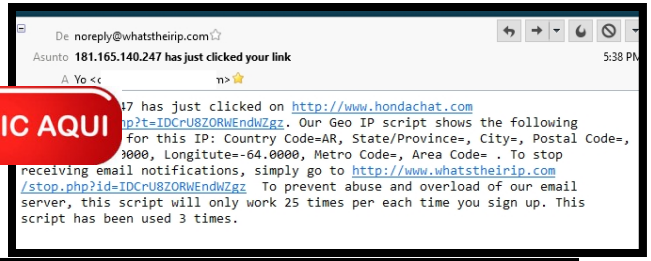
en 48 horas… 2) exploiting - ingeniería social

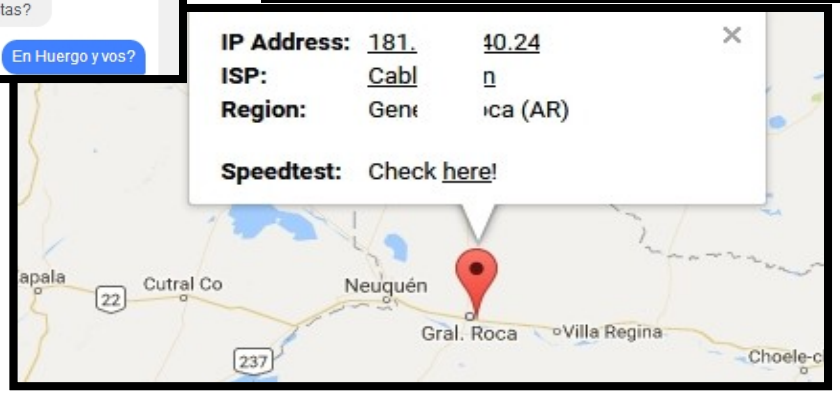
explotó algunas de esas debilidades y lo ubicó geográficamente

(ing social & geolocalización)



HAZ CLIC AQUI





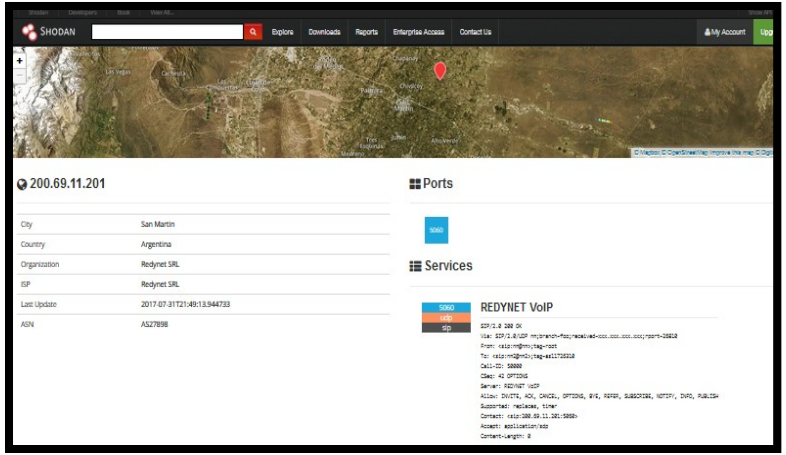
Copyright © 2017 ISEC GLOBAL inc. Todos los derechos reservados - www.isec-global.com

en 48 horas… 2) exploiting - OSInt

y siguió explotando debilidades

- **geoposición** a través de twitter logró las cuentas de todo su entorno social

- **app´s vulnerables**: descubrió que tenía un telefono ip vulnerable; (https://www.shodan.io/search?query=country%3Aar+VoIP+city%3A%22San+Martin%22)

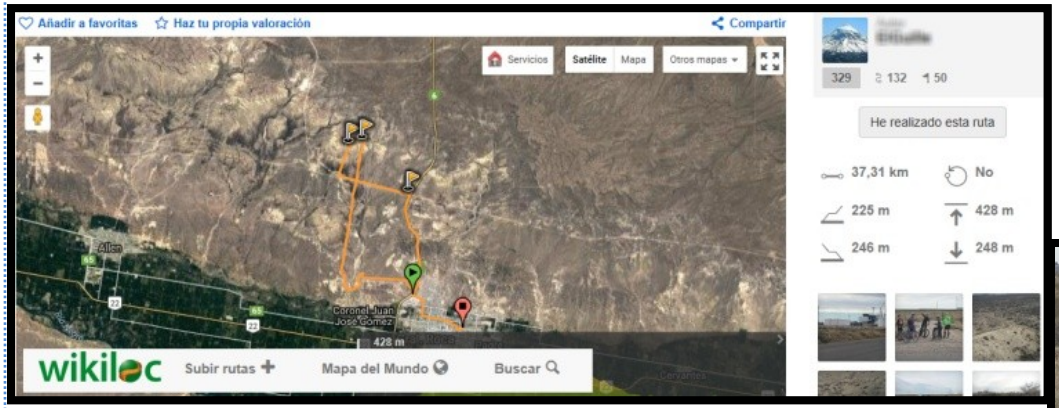


Copyright © 2017 ISEC GLOBAL inc. Todos los derechos reservados - www.isec-global.com

en 48 horas… 2) exploiting - wereables vulnerables

y siguió explotando esas debilidades

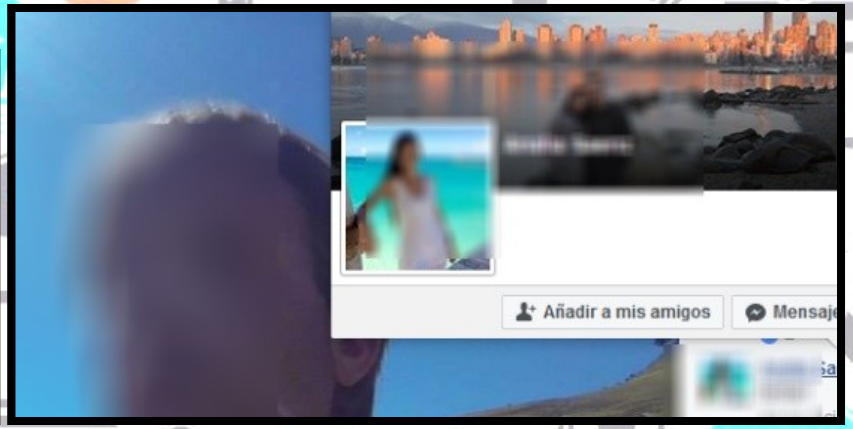
- app vulnerables: https://es.wikiloc.com/wikiloc/user.do?id=496386



Copyright © 2017 ISEC GLOBAL inc. Todos los derechos reservados - www.isec-global.com

en 48 horas… 3) ataque

- **OSInt**: interrelaciones de perfiles
- la esposa del extorsionador contenta **acepta una solicitud de amistad de la amante del extorsionador** (por recomendación de un face falso)



Copyright © 2017 ISEC GLOBAL inc. Todos los derechos reservados - www.isec-global.com

en 48 horas… 3) más ataque

- **hacking invoice mobile**: se tomó control de la casilla de mensajes de voz de celular del estafador & su esposa (por las dudas..) **claves default**
- **guardó los mensajes de citas y demás con su amante**

Copyright © 2017 ISEC GLOBAL inc. Todos los derechos reservados - www.isec-global.com

en 48 horas… 4) evidencias y anonimato

dejó un rastro para evidencia y comenzó a negociar:

- el extorsionador **recibe todas las capturas** de pantalla **del chat hot con su** nueva amiga (la del face falso que quería conquistar)
- también recibe todos **los recorridos en bicicleta** junto a su amante…
- tambien **recibe todos los mensajes de voz de su propio celular** dejados por su amante…

para tener en cuenta: todo fue enviado desde el mail **loqueDiosmanda@xx.com** a través de un onion de tor

Copyright © 2017 ISEC GLOBAL inc. Todos los derechos reservados - www.isec-global.com

y las 48 horas terminaron…

resultado: negoció el valor real de la deuda; le pidió amablemente que le cobre sólo

“lo que Dios manda”

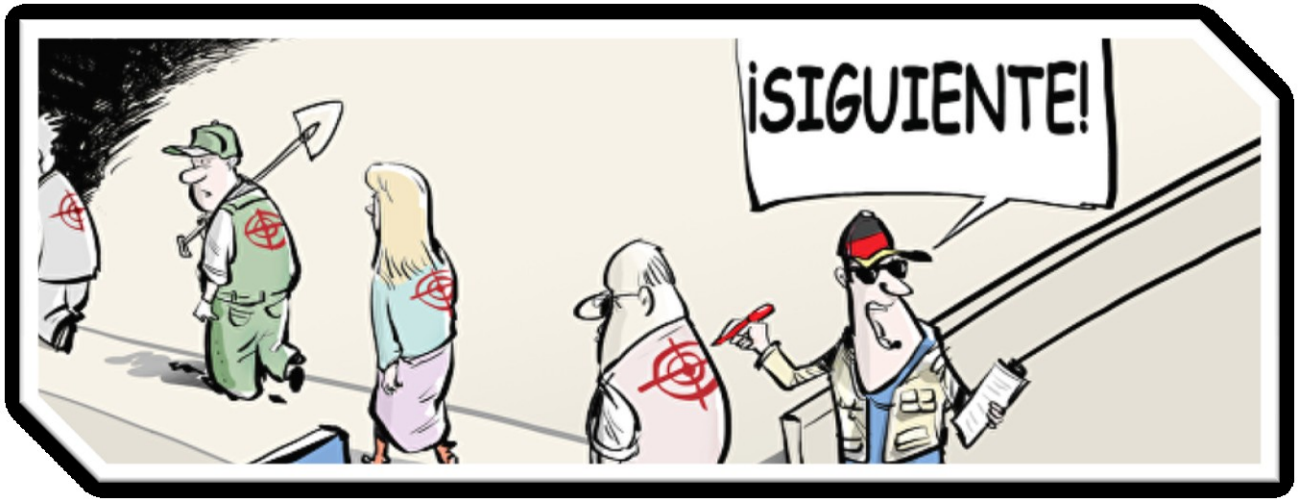
¿cuanto cobró? ¿cobró honorarios?

5) **borrado de rastros (última etapa):** las cuentas falsas y mail loque… (todo red tor) y devolvió las casillas de voz a sus dueños!

Copyright © 2017 ISEC GLOBAL inc. Todos los derechos reservados - www.isec-global.com

#iRes® 4 le ocurrió a un amigo ∴ conclusión

mejor que ser un **blanco fácil…**



…es ser un **“negro difícil”**

Copyright © 2017 ISEC GLOBAL inc. Todos los derechos reservados - www.isec-global.com

EOF - GRACIAS!!!

#iRes® 4 le ocurrió a un amigo

Christian Javier Vila

CTO - ISec Global Inc

tw: @infosecurityvip

christian.vila@isec-global.com

http://www.isec-global.com/icoach/