Jornada sobre ciberseguretat

Exploits d'un Troià Legal

Ruth Sala Ordóñez – Lletrada -

Objectiu de la ponència:

És la de fer veure als presents que el que sembla una solució pràctica en les investigacions policials, com és la possible existència d'un eina de Registre de Suport Informàtic de manera remota, no és processalment viable donat que té / tindrà moltes carències des de el punt de vista tècnic.

No es podrà garantir la cadena de custòdia de proves i fer servir els troians com a registre remot no garantirà que es puguin obtenir proves de càrrec per fer una imputació a un possible delinqüent.

1. Què és un Exploit?

Entenem per un "exploit" com aquell programa o codi que s'aprofita d'un forat de seguretat (vulnerabilitat) en una aplicació o sistema de manera que un atacant podria fer-la servir en el seu benefici.

Són generalment creats per investigadors de seguretat informàtica per a demostrar que existeix una vulnerabilitat.

No estem parlant d'un malware, si no que parlem de la clau per tal que els codis maliciosos accedeixin als nostres sistemes. Cada dia poden aparèixer nous exploits de manera que també apareixen cada dia noves vulnerabilitats que aquests tracten d'aprofitar.

http://www.welivesecurity.com/la-es/2014/10/09/exploits-que-son-como-funcionan/

2. Què és un Troià?

Un Troià és un programa maliciós que realitza accions no autoritzades per l'usuari. Els Troians es poden classificar en funció de les accions que poden realitzar en un ordinador. Aquestes accions poden incloure:

- Eliminació de dades
- Bloqueig de dades
- Modificació de dades
- Còpia de dades
- Interrupció del rendiment de l'ordinador o xarxes d'ordinadors

A diferencia dels virus o cucs informàtics, els troians no poden multiplicar-se.

La diferència amb un virus informàtic és que els troians, un cop s'han executat, donen el control remot de l'equip infectat sense ser advertit i sens, mentre que l'objectiu del virus informàtic és la de ser hoste destructiu. Contràriament, el Troià no té cap objectiu destructiu.

Donada la discreció amb la que es poden mantenir dins de l'ordinador dels usuaris, és possible que aquests troians puguin mantenir-se dins de l'ordinador sense que l'usuari se'n assabenti.

La única manera de poder-nos introduir en un ordinador és fer que l'usuari accepti una instal·lació, o que accepti la actualització d'una aplicació o es pugui aprofitar la vulnerabilitat d'una pàgina web per tal que quedi instal·lat a l'ordinador de l'usuari.

3. **Què és el malware**?

Virus. Un virus s'activa en executar un programa i a més d'ntentar reproduïr-se dur a terme activitats com l'esborat d'arxius, per exemple.

Cuc o *worm*. Anàleg al virus però es transmet de manera automática per la xarxa, aprofitant una vulnerabilitat.

Aquests tipus de programes tenen en comú la capacitat d'autoreplicar-se, és a dir, poden contaminar amb còpies de si mateixos que en algunes ocasions ja han mutat. La diferència entre un cuc i un virus informàtic radica en què el cuc opera de forma més o menys independent als altres arxius, mentre que el virus depèn d'un portador per a poder replicar-se

Altres tipus de malware són:

- Spyware
- *Adware*
- *Scareware*
- Backdoors
- *Rootkits*

Aquesta classificació és una orientació donat que molt sovint no hi ha una distinció clara davant un virus, un cuc i un troià per exemple, o pot pasar que un programa maliciós tingui característiques de diferents tipus de malware.

4. La Reforma de la Llei de Enjudiciament Criminal

En data de 5 de desembre de 2014 el Consell de Ministres feia aprovació de l'Avantprojecte de Llei d'Enjudiciament Criminal on es dedica una part a la regulació de les mesures d'investigació tecnològica.

Fiscalia emet un informe en data de 23 de gener de 2015 on es fa una valoració sobre la Reforma. En quant a l'apartat dedicat als Registres Remots sobre equips informàtics es crea el Títol III, del Llibre II amb el nou Capítol VII. L'article 588 sexies a., segons Fiscalia, exigeix autorització judicial a la vista que es tracta d'una mesura molt invasiva i una exigència indispensable. Es fa limitació a la comissió de delictes en el sí de:

- Organitzacions criminals
- Terrorisme

- Menors / persones amb capacitat modificada judicialment

- Delictes contra la Constitució, de traïció i relatius a la defensa nacional

Fan referència a que s'hauria d'atendre a criteris de necessitat, adequació i proporcionalitat en funció de la naturalesa i les característiques del fet investigat.

Fiscalia recomana que es pogués autoritzar la recuperació de dades esborrades. Fan reclamació que l'òrgan judicial es pronuncii sobre les característiques i les funcionalitats del software que ha de ser utilitzat en la pràctica de la diligència, és a dir, sobre la seva potencialitat per tal de tenir accés a les dades buscades i la manera en que s'ha de dur a terme.

En prevenció d'un possible esborrat de les dades per part dels delinqüents , Fiscalia proposa efectuar un bloqueig de les dades. En cas de considerar-se que les dades puguin estar en altra suport, es podrà fer una petició al Jutge per fer una ampliatòria a l'ordre de registre remot.

En quant a l'objecte o instrument que com a tal ha d'efectuar l'accés, Fiscalia opta per no pronunciar-se ni fer-ne delimitació donada la gran velocitat amb la que evolucionen les noves tecnologies de manera que, podria ser que definir l'eina limités les possibilitats futures.

En quant als serveis de *cloud computing* o plataformes al núvol, i concretant en casos de pornografia infantil on els arxius siguin emmagatzemats en plataformes cloud, Fiscalia recomana que les autoritats judicials espanyoles puguin accedir-ne al contingut inclús quan la plataforma sigui d'un altra país, però l'imputat o la persona investigada tingui accés al material des de territori espanyol on la Justícia Espanyola en seria competent.

Es proposa aquesta formula per tal d'evitar els dilatats tràmits que suposa la petició de cooperació judicial internacional.

5. Opinió del Jutge Eloy Velasco de la Audiència Nacional

Segons publica europa press: **“Velasco recuerda que "el 65% de la delincuencia informática sigue vinculada a estafas y fraudes" Europapress 16 / 01 / 2015**

http://www.europapress.es/la-rioja/noticia-eloy-velasco-recuerda-65-delincuencia-informatica-sigue-vinculada-estafas-fraudes-internet-20150116172422.html

(…)
FRONTERA ENTRE "SEGURIDAD Y LIBERTAD" En otro orden de asuntos, para Velasco es "fundamental" respetar siempre "la frontera entre la seguridad y la libertad". Por ello, ha recordado, "usamos textos encriptados para que nadie se meta en nuestros negocios pero si los utiliza un terrorista no sabemos lo que dice y eso nos dificulta el trabajo". Por ello, ha reiterado, encontrar ese límite "es un trabajo muy difícil el que tiene el legislador de autorizarnos y darnos herramientas pero a la vez “son eficaces para acabar con los problemas de seguridad y evitar que nos desmonten los sistemas de libertad que tantos siglos nos ha costado conseguir”

6. Apreciacions des de el punt de vista pràctic i tècnic

6.1.El Troià

Quin desenvolupament tindrà?

El Troià com a eina d’entrada i registre és un desenvolupament informàtic al qual se li hauran de donar una sèrie de INPUTS i OUTPUTS, és adir, si es compleixen una sèrie de paràmetres el Troià haurà d’executar l’objectiu pel qual ha estat dissenyat. Parlem del que s’anomena “taules de decisió” sobre un munt d’INPUTS.

Un Troià es pot desenvolupar en un dia, però un Troià que pugui preveure totes les possibilitats d'aquesta taula de decisió té un elevat cost i suposa tenir molts més recursos.

Imaginem que un Troià el deixem "latent" dins d'un disc dur i és previst una activació amb el sistema operatiu Windows però l'investigat fa la instal·lació d'Ubuntu(Sistema Operatiu Linux) i el Troià té comportaments "no previstos" provocant danys.

- De qui és la responsabilitat? Del desenvolupador? De qui ha fixat els paràmetres de INPUT?

Un Troià "respectuós" és aquell que queda latent fins que s'activa per unes circumstàncies concretes i molt ben programades per no incòrrer en irresponsabilitats. Juga en contra del Troià "respectuós" el temps que permetria un Jutge que es produís la investigació remota.

En cas que se li incloguin els paràmetres de còpia de documents amb extensió **.doc** i l'investigat resultés que tingués la documentació encriptada, ens trobarem dins del servidor un munt de brossa amb uns grans costos en la analítica de dades. Ho podem assumir? Tenim el personal per fer-ho?

Més qüestions:

Cada CFSE tindrà la seva eina?

N'hi haurà alguna d'estandaritzada?

Qui la desenvoluparà?

Qui marcarà la pauta de quines funcionalitats ha de tenir?

Quin és el seu cost? Qui ho pagarà? Cada Cos Policial el seu?

Qui la farà servir?

Personal autoritzat? Amb qualificació formativa? Amb només patrons d'autoaprenentatge dins del Cos?

6.2.L'Ordre d'entrada i registre: La redacció de la ordre d'entrada i registre. Diferències entre la analógica i la tecnológica.

a.En una petició d'Ordre d'entrada i registre en recinte tancat no accessible al públic, s'hauria de fer la descripció de tots aquells elements de convicció que han portat a l'investigador a fer una suma d'indicis que faci que prengui la decisió concloent d'haver d'entrar en un recinte tancat on és molt segur que s'hi puguin trobar les proves de càrrec que puguin imputar a un investigat.

b.En un cas on s'hi afegeixen elements tecnològics com el delicte mitjançant elements tecnològics, la investigació tecnològica pot dur a la conclusió mitjançant una adreça IP que l'autor del delicte pugui ser localitzat en un domicili determinat, de manera que l'investigador farà sol·licitud d'Ordre de Registre de recinte tancat per trobar moltes més proves incriminatòries.

c. Per fer sol·licitud d'una Ordre de Registre Remota s'haurà de "ser" com a observador en algun punt des de on es pugui fer una captació de paquets de dades i que sigui una xarxa pública i oberta. Sobre una captació "casual" de dades i una investigació mitjançant la captació de les mateixes, s'haurà de raonar per què fem la sol·licitud de registre remot d'un suport, de persona determinada.

Si he procedit a un procés de seguiment físic per "deduïr" que en aquell domicili hi pot haver informació valuosa i qualificada com a prova de càrrec, així ho haig de fer veure al Jutge per tal que em doni la Ordre d'entrada i Registre remota.

6.3. A qui o a quin suport dirigir el Troia? Com entrar? Què fer dins? Hi ha garanties dels continguts que entren? I dels que surten?

a. Imaginem un supòsit en que l'investigador ha arribat a la conclusió de que una determinada IP va enviaments i obre material de pornografia infantil. Però tampoc podem assegurar qui n'és l'autor donat que la IP és associada a una vivenda o despatx en el qual hi treballen 20 persones.

En aquest cas, algú amb una IP privada, associada a una MAC (tarja de Xarxa de l'ordinador) fa una petició que ha de passar pel router, que, en rebre la petició, crearà el que s'anomena taules de peticions per transformar aquell paquet en informació que surti des de la IP que el mateix router té assignada.

D'aquesta manera, en tornar la petició, es distribuirà internament a la IP privada inicial que en va fer la sol·licitud.

Conclusió: en un espai on hi treballen més de 20 persones, des de fora no és possible quina de les persones és la que està fent els enviaments. Amb l'agravant de que, en cas que fos un advocat, estarem vulnerant el secret professional que l'empara.

b. Imaginem que tenim localitzat a l'autor. Com podem entrar?

- Fent-li enviament d'un mail amb un enllaç
- Fent servir una vulnerabilitat d'un navegador que no sigui actualitzat i introduïr-ne el troià sense que el mateix navegador l'avisi.
- Fer servir també vulnerabilitats de pàgines web.

Respecte al què fer dins, podríem plantejar:

- Com garantim que el Troià no "deixa" en l'ordinador de l'investigat cap tipus d'informació que no li pertany?
- Es pot documentar d'alguna manera que l'actuació s'ha fet dins dels límits jurídics?
- Podriem fer servir un Tercer de Confiança per tal que ves "d'observador" de la operació i en garantís tots els moviments? Què són els Tercers de Confiança? Son els que anomenem Prestadors de Servei de Certificació i que, sent autoritzats pel Ministeri d'Indústria espanyol, faciliten la funció de garantir tots els actes i processos que s'efectuen dins la xarxa. Són com un "observador" que no és part de la relació i que garanteix tot el tràfic de dades donant fe de la seva autenticitat.

Tenint en compte que els advocats el primer que aniran a comprovar és la cadena de custòdia sobre les evidències electròniques, com es poden garantir? Quan s'extreuen? Quan es bloquegen? ...

Haurem de pensar en si estem també preparats per assumir la responsabilitat d'una fallida en la nostra "estada" dins del suport de l'investigat, sobre tot, si en pateix danys i perjudicis econòmics.

Conclusió: Estem / Estem preparats?