



¿Tiene la Confianza Digital los pies de barro?

Si el año 2010 estuvo marcado por la liberación de informaciones secretas y confidenciales, o por la asombrosa facilidad de los atacantes para obtener datos personales de millones de suscriptores en sitios web mundialmente conocidos, desde el mes de marzo de este año la novedad es otra y se centra en derribar los bastiones clásicos y aceptados de la autenticación y la identidad digital en Internet.

Primero fue el ataque que permitió sacar de RSA las claves secretas que permiten regenerar todos sus *tokens SecureID*¹, y poco después se produjo lo que se ha dado en denominar el **Comodo Hack**², en el que la víctima es una Agencia de Certificación y su negocio el establecimiento de la "Confianza Digital" en Internet.

La quiebra en la seguridad del sistema OTP³ no solo afecta a RSA, ya que lo que le sucedió a esa compañía muy bien puede haberles pasado ya a otras empresas compitiendo en ese mismo mercado. En todos los casos, el origen del problema está en la posibilidad que ofrecen todas ellas de regenerar los *tokens* que proporcionan las OTPs.

Dada la coincidencia temporal con este escándalo, el incidente de Comodo pasó un tanto desapercibido y los medios lo trataron someramente; después de todo, sólo se emitieron fraudulentamente nueve certificados digitales. Esta fue la situación general del gremio hasta que llegó el pasado mes de agosto.

Después del asalto a Comodo, su autoproclamado

Este 2011 probablemente pase a ser el año en el que se han producido incidentes más serios relacionados con la autenticación y la identidad digital en Internet. Aún siendo la PKI tecnología vetusta diseñada hace décadas, solo es ahora, con los ataques *hackers*, cuando pueda realmente alcanzar la madurez que durante tanto tiempo hemos echado de menos. En este artículo veremos cuáles han sido los acontecimientos y si de ello se puede sacar alguna conclusión o enseñanza.

autor publicó en **pastebin.com** su declaración de Ciberguerra y nadie se tomó en serio la hipótesis de que otras Autoridades de Certificación pudiesen correr riesgo y se consideró el hecho como algo aislado. A pesar de la poca atención que se le dio, el ataque a Comodo fue considerado como un ciberataque

que labó la integridad de una Autoridad de Certificación, cosa hasta entonces nunca vista, ni por muchos imaginada.

Cuatro meses después, salta a los titulares la empresa **DigiNotar** que actuaba como Autoridad de Certificación de **Vasco Data Security Int.**, y cuyas actividades fueron detenidas por orden del gobierno

entró en bancarota. En esta ocasión, el número de certificados indebidamente emitidos ascendió a **531**, y corresponden a dominios muy variados que van desde algunos tan universales en Internet como ***.*.com**, o ***.*.org**, a otros tan específicos como **friends.walla.co.il**.

En este caso el atacante no solo fue capaz de emitir fraudulentamente más de medio millar de **certificados para la firma de código** y el establecimiento de **conexiones seguras SSL**, sino que alardea de haber tenido acceso a otras cuatro compañías en el negocio de la certificación digital. En concreto, el atacante apuntó directamente contra



Las tecnologías de autenticación disponibles y las compañías que las proporcionan son cada día más iguales, prácticamente idénticas, como si el mercado tendiese a un mismo y único modo de hacer las cosas. Este "monocromatismo" en el ámbito de la autenticación e Identidad Digital, sólo puede traer serios problemas en el futuro.

serio que establecía un nuevo récord, pero aún así seguía siendo algo aislado.

La culpa de lo que había pasado se le atribuyó a la escasa atención que se había presentado a la seguridad de las aplicaciones software del *partner* de Comodo que fue atacado. Al final, el objetivo del ataque, que era Google, y las razones políticas del ataque llamaron mucho más la atención del gran público que los procedimientos técnicos utilizados para realizarlo. Sin embargo, se trataba del primer caso en el que se vio-

holandés el 3 de septiembre de 2011. La razón de ello es que se había comprobado que en su seno se habían emitido numerosos certificados digitales "fraudulentos". El gobierno holandés tomó el control de los sistemas de DigiNotar y al final de ese mismo mes la compañía

GlobalSign⁴, del grupo japonés GMO Internet Group, e indirectamente a otras como la israelí **StartCom**⁵; en ambos casos fueron capaces de evitar el ataque **porque su personal humano estaba frente a los terminales del HSM mientras se producía el ataque**⁶. A pesar de no

¹ Ver http://en.wikipedia.org/wiki/RSA_SecureID

² Ver <http://pastebin.com/74KXCaeZ>

³ Ver http://en.wikipedia.org/wiki/One-time_password

⁴ Ver <http://www.globalsign.com/ssl/>

⁵ Ver <http://en.wikipedia.org/wiki/StartCom>

⁶ El hacker de DigiNotar: "GlobalSign, StartCom was lucky enough, I already connected to their HSM, got access to their HSM, sent my request, but lucky Eddy was sitting behind HSM and was doing manual verification."

haber conseguido su objetivo principal, el atacante dice haberse hecho con los correos, las salvaguardias de las bases de datos y datos de los clientes de esas compañías.

La confianza en los certificados de DigiNotar ha sido revocada en todos los navegadores y sistemas operativos del planeta; de forma permanente en todos los productos Mozilla pero **no en los smartphones**⁷, lo que ha tenido serias consecuencias en el programa de PKI del gobierno holandés. En esta ocasión, a la segunda, las aseveraciones del hacker de Comodo disparó el pánico entre los proveedores de certificación que, según algunas fuentes, rondan el medio millar de compañías en todo el mundo.

Sabidamente, el 6 de septiembre, **GlobalSign** decidió como medida de precaución cesar temporalmente en la actividad de emitir certificados⁸, y contrató a la compañía **Fox-IT**⁹ para realizar una auditoría en profundidad de sus sistemas. Esta compañía de seguridad holandesa es la misma que realizó la auditoría a DigiNotar por orden del gobierno holandés. Por su parte, el 7 de septiembre, **Symantec** publicó una nota en la que reafirmó a sus clientes que su infraestructura había sido auditada y que no había sido comprometida. Un anuncio similar lo realizó **Thawte**, que por error había sido acusada por el gobierno holandés de haber sido víctima de otra infiltración. La historia posiblemente no termine aquí ya que el hacker de Comodo promete nuevas filtraciones¹⁰.

De todas las reacciones, la más equilibrada quizás haya sido la de GlobalSign, que ha decidido parar máquinas y considerar "estas declaraciones [las del hacker de Comodo] como un ataque a toda la industria", por lo que propone que "después del ataque a DigiNotar es forzoso repensar el actual modelo de autenticación y la cadena de confianza."

Lo cierto es que las tecnologías de autenticación disponibles y las compañías que las proporcionan son cada día

específico parece ser que permitió a los hackers la "exfiltración" de los certificados generados hacia una "dropbox" externa. Tanto la IP del servidor interno en DigiNotar como la dirección IP del buzón de entrega estaban escritas directamente en el código del software utilizado, por lo que todavía está abierta esa línea de investigación.

Además, se encontró un script escrito en XUDA¹¹ que es una librería utilizada e integrada en algunas infra-

"Janam Fadaye Rahbar", que es la misma que apareció en el incidente de Comodo.

El éxito del ataque indica que la infraestructura de DigiNotar no era suficientemente segura como para evitar este ataque. Según el informe preliminar de Fox-IT "los servidores más críticos contenían software malicioso que normalmente es detectado con software anti-virus" lo cual es sorprendente en el caso de una empresa que quiere ganarse la confianza de todos por su seguridad.



El error que cometió el hacker fue el de generar unos certificados con unos números de serie que no coincidían con la política de secuenciación que estaba establecida y por eso no los reconocía el verificador OCSP. La selección de esos números podría haberse hecho con más tino y los resultados habrían sido del todo "indistinguibles" de los demás certificados legítimos; en ese caso, la indetectabilidad estaría asegurada.

más iguales, prácticamente idénticas, como si el mercado tendiese a un mismo y único modo de hacer las cosas. Este "monocromatismo" en el ámbito de la autenticación e Identidad Digital, sólo puede traer serios problemas en el futuro.

En el escenario del cibercrimen, dentro de las instalaciones de DigiNotar, se encontraron numerosos ejemplos de software malicioso y herramientas *hacking* que iban desde las más comunes como es el caso de la famosa Caín & Abel, y ejemplos de software hecho a la medida para la ocasión.

Parte de ese software

estructuras de clave pública de diferentes productos pero especialmente en el software de la **KEON CA** de **RSA Labs**, que es el que corría en la Autoridad de Certificación atacada. XUDA en origen perteneció a la empresa **Xcert International**, pero ésta fue comprada por **RSA Security Inc.** en el año 2001.

El propósito de los scripts en XUDA fue el de generar firmas con la identidad de la Autoridad de Certificación que estaba ubicada dentro de un HSM y que habían sido solicitadas con anterioridad dentro del sistema. El script contenía un comentario en inglés en el que aparece la firma

Por si eso fuera poco "la separación de los componentes críticos no funcionaba o no se había establecido". Por lo visto, había "claros indicadores de que los servidores de CA, aunque estaban ubicados en sitios muy seguros y dentro de un entorno *Tempest proof*, eran accesibles a través de la red local para funciones de mantenimiento".

Como consecuencia directa de este diseño, la red local fue conquistada por el atacante y, dado que "todos los servidores de CA eran miembros de un mismo dominio *Windows*, esto hizo posible que tuvieran acceso a todos ellos utilizando una única combinación usuario/contraseña". Visto esto, no es de extrañar que "la contraseña no era muy fuerte y podía obtenerse fácilmente mediante ataques de fuerza bruta".

Otras joyas del informe preliminar de Fox-IT indican

⁷ Ver http://www.pcworld.com/businesscenter/article/239607/diginotar_certificates_are_pulled_but_not_on_smartphones.html

⁸ Ver http://www.theregister.co.uk/2011/09/07/globalsign_suspends_ssl_cert_biz/

⁹ Fox-IT es una compañía próxima al gobierno holandés dedicada a la interceptación de datos y a la seguridad IT. La mayoría de los departamentales del gobierno y agencias de seguridad holandesas hacen negocios con dicha compañía. La compañía esta formada por unos 130 trabajadores, todos ellos investigados previamente por el servicio secreto holandés.

¹⁰ Hacker de DigiNotar: "...BUT YOU HAVE TO HEAR SO MUCH MORE! SO MUCH MORE! At least 3 more, AT LEAST!"

¹¹ XUDA (Xcert Universal Database API) es una API que permite a los programadores desarrollar software de PKI aislando su trabajo de las complejidades de esa tecnología. Ver <http://en.wikipedia.org/wiki/Xuda>

que "el software instalado en los servidores web accesibles desde el público era anticuado y no había sido parcheado", "no había protección antivirus presente en los servidores investigados", "había operativo un sistema de detección de intrusiones [IDS]" pero "no está claro por qué no bloqueó algunos de los ataques a los servidores web externos".

Llegados a este punto, uno se pregunta de qué sirven las miríadas de libros, normas, estándares, manuales y recomendaciones de buenas prácticas, etc., si sigue habiendo instalaciones como la descrita en ese informe y que, para mayor ignominia, algunas compañías seguro que la auditaron previamente y le dieron el rango de máxima calificación en cuanto a su seguridad.

Otro aspecto interesante en esta historia es cómo se detectó la existencia de esos "certificados robados". La detección se produjo porque, mientras se estaban utilizando, se recibieron solicitudes de verificación *on-line* mediante el protocolo OCSP, preguntando por **certificados de los que la Autoridad de Certificación no tenía constancia de haber emitido**. La observación de esas solicitudes durante los días en los que se estaba utilizando el certificado *.google.com dio una idea del lugar del mundo en el que el engaño estaba surtiendo efecto.

La primera detección se realiza por casualidad el 27 de agosto y aparece en un foro de Google. En este caso, un usuario iraní informa de que su navegador Chrome, al intentar conectarse a google.com, le dijo que había algo raro en ese certificado; el certificado rechazado había sido emitido el 10 de julio.

Analizando los logs del servidor OCSP de DigiNotar se vio que, a partir del 4 de agosto el número de solici-

tudes de verificación OCSP aumentó rápidamente hasta que ese certificado fue revocado el 29 de agosto a las 19:09 UTC. Hasta entonces se habían recibido solicitudes de **300.000 direcciones IP distintas**, de todas ellas **más de 99% están en Irán**. Las pocas que son de fuera de ese país, corresponden a nodos de salida de la red TOR de anonimato u otros *proxies* o servidores de VPN, pero no a usuarios finales.

Con esa lista de IPs, Google informó a sus usuarios que durante ese periodo de tiempo sus correos electrónicos podrían haber sido

En este incidente no se ha hablado de consecuencias tangibles para las decenas de miles de usuarios iraníes puestos en riesgo, por lo que no se ha tratado públicamente el tema de qué compañía de seguros cubriría las consecuencias de este tipo de ataques en el caso de que alguna autoridad nacional o internacional decidiese poner en marcha esa evaluación. Que ahora no haya habido consecuencias económicas obvias no significa que la próxima vez no vaya a haberlas.

Independientemente de todo lo anterior, no hay que

En este ejemplo se ve como una colección de elementos muy caros como son los *firewalls*, IDSs, HSMs y demás parafernalia de la última década, no sirven de nada "en caliente" y cuando el atacante logra suplantar al agente humano que realmente autoriza la emisión de certificados (en este caso mediante un par usuario/*password* débil). Una mala estructuración de la red, la inexistente separación de funciones y de circuitos de información y una excesiva confianza en los sistemas "automáticos" de seguridad, son los componentes básicos de este fracaso.



Se ha visto como una colección de elementos muy caros como son los firewalls, IDSs, HSMs y demás parafernalia de la última década, no sirven de nada "en caliente" y cuando el atacante logra suplantar al agente humano que realmente autoriza la emisión de certificados. Una mala estructuración de la red, la inexistente separación de funciones y de circuitos de información y una excesiva confianza en los sistemas "automáticos" de seguridad, son los componentes básicos de este fracaso.

interceptados, así como sus *cookies* de acceso. Dicho de otro modo, que sus cuentas en Gmail y por extensión en Google podrían estar en manos de otros. Hay que tener en cuenta que el control de una cuenta en Google afecta a todos los servicios asociados con ella, como son datos de geolocalización, documentos, fotografías, etc. Además, controlando la cuenta de *e-mail*, **se puede tomar control absoluto en todas las redes sociales a las que pertenezca la víctima**, ya que el atacante siempre puede pedir el establecimiento de una nueva a través del correo. El acceso a los perfiles de las redes sociales da una descripción de quién conoce a quién, información muy útil a la hora de avanzar en cualquier tipo de "investigación".

olvidar que también hay muchas aplicaciones que no utilizan la verificación *on-line*, por lo que los datos anteriores no son la totalidad de los casos en los que se pueda haber visto involucrado alguno de los certificados fraudulentos desde el día de su generación y el de revocación universal.

Así pues, el error que cometió el *hacker* fue el de generar unos certificados con unos números de serie que no coincidían con la política de secuenciación que estaba establecida y por eso no los reconocía el verificador OCSP. La selección de esos números podría haberse hecho con más tino y los resultados habrían sido del todo "indistinguibles" de los demás certificados legítimos; en ese caso, **la indetectabilidad estaría asegurada**.

Se pueden montar PKIs que son y serán seguras si se hace bien. Se puede construir la confianza digital basada en certificados aunque no necesariamente deba seguirse la jerarquía original que no es nada adecuada ya que concentra demasiado riesgo en los puntos altos de la misma. Quitando mucha bravuconería que hay en los comunicados del artífice de estos incidentes, lo cierto es que sabe de qué habla y su éxito es el fracaso (remediable) de las empresas que se dedican a la autenticación y la identidad digital. ■

JORGE DÁVILA MURO
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad
de Informática – UPM
jdavila@fi.upm.es