Ataques a sitios web gubernamentales en Argentina y su relación con la ciberdefensa

Federico Pacheco

Universidad Tecnológica Nacional, Facultad Regional Buenos Aires

federico.pacheco@gmail.com

***Abstract*—Every government protect their digital assets against different kinds of threats. Whereas cyber defense strategies involve protection against external threats and cybersecurity strategies involve protection against internal threats, it is not obvious in advance what field hacking government websites belongs. In this paper we analyze the hacking attacks suffered on government websites in Argentina in the last 6 years, and its relationship with national cyber defense and cyber security strategies.**

***Resumen*—Todo gobierno protege sus activos digitales contra distintos tipos de amenazas. Considerando que las estrategias de ciberdefensa suponen la protección contra amenazas externas y las estrategias de ciberseguridad suponen la protección contra amenazas internas, no es obvio a priori a qué terreno pertenece el hackeo de sitios web gubernamentales. En este trabajo se analizan los hackeos sufridos sobre los sitios web gubernamentales de Argentina en los últimos 6 años, y su vinculación con las estrategias de ciberdefensa y ciberseguridad nacional.**

I. Introduction

El concepto de ciberdefensa implica el conjunto de acciones de defensa activas pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición [1]. En el presente trabajo se estudia la efectividad de las medidas de ciberdefensa nacional a la luz de los ataques recibidos sobre sitios web gubernamentales, como parámetro representativo de los resultados visibles que pudieren ser de interés para la población.

La Ley de Defensa Nacional Argentina y su decreto reglamentario establecen que la misión de las Fuerzas Armadas es conjurar y repeler una agresión militar estatal externa. Para el caso de la ciberdefensa, la identificación del origen, límites y alcances, por tratarse del ciberespacio, no es evidente sin suficiente capacidad técnica y humana.

En 2006 y según la Oficina Nacional de Tecnologías de la Información (ONTI) se constituyó en el Ministerio de Defensa el primer comité de seguridad de la información. En septiembre de 2013 se creó la Unidad de Coordinación de Ciberdefensa, que recogió las iniciativas desarrolladas por las tres fuerzas y el área civil del ministerio, que luego elaboró una propuesta orgánica que permitió la creación de un Comando Conjunto de Ciberdefensa, una Dirección General de Ciberdefensa (marzo de 2015) y una instrucción para desarrollar la capacidad de ciberdefensa en cada una de las Fuerzas Armadas y el Estado Mayor Conjunto. Esto dio entidad formal al ciberespacio como ámbito y objetivo militar.

En base a lo antedicho, es de esperarse que se exista a nivel nacional una serie de acciones orientadas a verificar y reforzar la seguridad de la infraestructura gubernamental relacionada con el ciberespacio, entre lo cual se encuentran los sitios web pertenecientes a organismos de la administración pública nacional.

II. Tipos de ataque

No existe una taxonomía estricta y universalmente aceptada de los objetivos de ataque en términos de ciberdefensa, pero podemos suponer a priori que todo aquello que de alguna forma se encuentre online, puede ser un objetivo válido. Esto incluye principalmente:

- Dispositivos conectables a Internet (Internet de las cosas).
- Sistemas accesibles desde Internet.
- Sitios web gubernamentales.

En cuanto a los dispositivos conectables, se estima que un 70% de los productos de mercado poseen vulnerabilidades [2] que no pueden ser reparadas (ya que requerirían de un sistema de actualizaciones). No obstante, la cantidad de dispositivos pertenecientes al sector gubernamental aún no pareciera ser representativo como para ser una vía de ataque preferencial. Esto no implica que no puedan explotarse en sí dichas vulnerabilidades, sino que deben tomarse en consideración con el tiempo.

Con respecto a los sistemas accesibles a través de Internet, pueden ser sistemas de control industrial del tipo SCADA, o cualquier tipo de software que permita ser administrado de manera remota que sirva a los fines de algún conjunto de tareas relacionadas con el estado nacional. Dichos sistemas no están incluidos en el alcance de este estudio debido a que el mero testeo de seguridad de los mismos sin autorización explícita implicaría la violación de la Ley 26.388 (Ley de Delitos Informáticos).

Por parte de los sitios web gubernamentales, estos constituyen la mayor superficie de ataque expuesta, debido a la cantidad de servidores y páginas en existencia. En este sentido, si bien existen estándares técnicos para su instalación y puesta en producción, se torna dificultoso mantener dichos estándares en todo el país, debido a que muchos sitios pertenecen a organismos menores, o de distintas provincias, que no siempre cuentan con los recursos técnicos y humanos adecuados.

El impacto de un ataque a un sitio web gubernamental suele ser bajo en términos de información obtenida por parte de un atacante, es decir que evaluando los 3 aspectos primordiales de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad) la que se suele ver menos afectada es la confidencialidad, salvo casos excepcionales donde los servidores afectados contengan

bases de datos o sistemas sensibles. De esta forma, puede deducirse que el aspecto más riesgoso de un ataque a una web de gobierno, más allá de la información en sí misma, es el daño a la imagen pública que dicho ataque deja en la población y la comunidad internacional. Esto empeora cuanto más importante (o visitado) sea el sitio, o cuando se producen coyunturas que lo ponen en primera plana, como ser por ejemplo, un organismo que está siendo protagonista de noticias locales y en tiempos cercanos es atacado pese a no ser particularmente relevante fuera de ese momento.

III. Obtención de información

A los fines del análisis de los ataques se ha utilizado información obtenida del procesamiento de las bases de datos públicas de la organización Zone-H (www.zone-h.org) que cuenta conl un sitio web de fuentes abiertas que desde el año 2002 recoge los resultados visibles que producen de los ataques a los sitios web de distintos países del mundo. Dichas acciones son denominadas comúnmente *defacements* por su significado en inglés de "cambio de cara", que en muchas ocasiones es el resultado visible de un ataque (la alteración de un contenido o página).

La cantidad de registros obtenidos para análisis se limita en este estudio a los últimos 6 años completos (2010 a 2015) según permite consultar la base de datos en cuestión.

Los registros que pueden encontrarse incluyen tanto sitios de la antigua terminación de sitios web gubernamentales (.gov.ar) como de la nueva terminación adoptada por el gobierno nacional (.gob.ar). Según datos oficiales provistos por la autoridad nacional de registro de dominios (http://nic.ar) actuante bajo la Dirección Nacional del Registro de Dominios de Internet, que depende de la Secretaria Legal y Técnica de la Presidencia de la Nación, existen más de 4300 dominios registrados activos, dato que debe considerarse aproximado ya que cada semana se dan de alta nuevos dominios y se eliminan otros.

No obstante, la información proporcionada por el buscador Google solo arroja una cifra superior a los 600 resultados significativos, utilizando el siguiente criterio de búsqueda: site:gov.ar OR site:gob.ar. Esto permite estimar un escenario de cantidad de páginas expuestas, lo que define el tamaño de la llamada "superficie de ataque".

IV. Hallazgos significativos

El principal elemento a ser analizado es la cantidad de sitios web gubernamentales que han sido atacados "con éxito" en cada año. Tomando los últimos 6 años, el pico máximo se encuentra en el año 2013, con 677 sitios y desciende hasta los 175 en 2015. Considerando que la registración de los dominios en cuestión ha crecido en los últimos años, el descenso de los ataques exitosos pareciera indicar una mejora en las medidas adoptadas para protección.

Muchas veces los ataques parten de escaneos masivos de ciertas vulnerabilidades conocidas que se logran explotar de forma automatizada mediante software creado específicamente para tal fin. En otros casos veces se trata de las llamadas amenazas persistentes avanzadas o APT (Advanced Persistent Threats) que buscan de forma específica tomar control de un determinado sitio[3].

La protección y defensa contra ataques de esta naturaleza se realiza mediante la adecuada aplicación de procesos de desarrollo seguro de software y sitios web, que además de las técnicas de programación segura y aplicación de medidas preventivas, debe incluir la realización de pruebas de penetración (penetration tests) y evaluación de vulnerabilidades (vulnerbility asessments) en el marco del proceso de incremento proactivo de la seguridad que se conoce como Ethical Hacking[4].

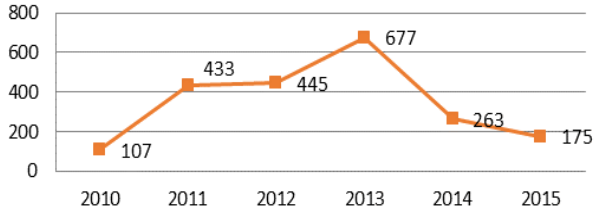

Figura 1. Cantidad de ataques por año (2010 a 2015).

Un parámetro de importancia al analizar los ataques lo constituye la página en particular que se haya logrado modificar en el ataque. En este aspecto, se distingue entre la página principal (*homepage*) y cualquier otra página que esté disponible mediante la navegación interna en el sitio.

Resulta lógico que el ataque se perciba como más grave en el caso de haber sido vulnerada una página principal por ser la que indefectiblemente es accedida por los usuarios al iniciar la navegación por el sitio. Los datos arrojan que un 59% de los sitios fueron afectados en su página principal.

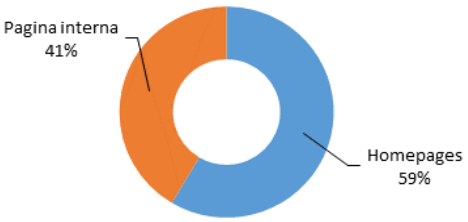

Figura 2. Ataques a páginas principales vs. páginas internas

Otro parámetro de interés es el tipo de ataque según su alcance individual o masivo. Esto implica que ciertos ataques son realizados de forma específica contra un sitio, buscando afectar alguna vulnerabilidad que permita tomar control sobre la página en cuestión, y otros son atacados de forma masiva, afectando a servidores que contienen una gran cantidad de sitios, y por tanto vulnerar el servidor implica tomar control sobre todos los sitios allí alojados.

En términos de la protección contra ataques masivos, la solución tradicional consiste en mantener una correcta política de gestión de vulnerabilidades, que incluya el ciclo de actualizaciones de sistemas y software de los servidores.

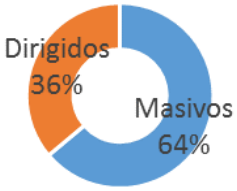

Figura 3: Ataques dirigidos y masivos

Adicionalmente, sin que represente un parámetro particular de riesgo, y solo mencionándolo a título de información adicional es posible determinar el sistema operativo de los sitios vulnerados. No debe realizarse ninguna deducción sobre la seguridad del sitio en cuestión en relación a que haya sido vulnerado, debido a que la mayor parte de los incidentes en sitios web proviene de otros vectores de ataque como las fallas en configuraciones o las aplicaciones instaladas.

Cabe destacar que en general el sistema operativo Linux es el más utilizado a nivel mundial en Internet para alojamiento de sitios web, por lo que es de esperar su mayor presencia. También vale destacar que el uso de sistemas propietarios (como es el caso de servidores Windows) no deberían encontrarse presentes en el ámbito de la administración pública nacional, ya que el software libre es considerado política de estado desde el año 2011 a partir de la Resolución 754/2011 de la Jefatura de Gabinete de Ministros.

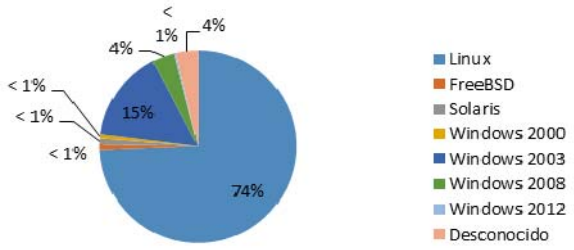

Figura 4. Sistemas operativos afectados.

En cuanto a la frecuencia de los ataques, la obtención detallada de ataques por día sería poco confiable en términos estadísticos, ya que en general los informes de ataque se reportan por cantidades y no de forma individual por cada uno. Si tomamos un alcance semanal, aún queda enmascarado el dato por los informes que se reciben cada varios días, con lo que la mejor estimación pareciera ser la que toma un período mensual, para que los datos sean más representativos. Así, puede calcularse que cada mes se reciben un promedio de 31,6 ataques como los analizados, no siendo correcto deducir de aquí que se realiza aproximadamente un ataque por día.

V. Origen de los ataques

La defensa nacional implica actividades políticas que desarrollan los estados-nación para hacer frente a los ataques militares que pudieren realizar otros estados-nación, lo cual sugiere por definición la existencia de un potencial enemigo externo. Esto bien podría ampliarse análogamente al terreno de la ciberdefensa nacional, donde los atacantes potenciales provendrían (o serían en sí mismos) de otros países.

La deducción del origen real de los ataques en términos de los objetivos analizados aquí no es posible sino por medio de suposiciones y asunciones técnicas. Esto es así dado que la fuente de datos arroja solamente nombres de fantasía a los que se les atribuye cada ataque (*defacement*) los cuales pueden ser falsificados sin mayor problema al momento de ser reportados, y que además en muchos casos son reportados por los propios atacantes.

Adicionalmente, la naturaleza misma de un ataque de estas características tiende a ser técnicamente anónima en origen, ya que los atacantes toman medidas de ocultamiento de direcciones de Internet y anonimización mediante el uso de servicios de VPN (Virtual Private Networks) o proxies anónimos. En este sentido, la fuente de datos también arroja el país de origen del ataque según la dirección IP reportada, lo cual no es indicador directo del origen real, en base a lo antedicho, aunque puede correlacionarse con el nombre de fantasía o sobrenombre (*nickname*) reportado para obtener conclusiones.

De cualquier forma, asumiendo que existe cierto marco de realidad, donde además se pone en juego la necesidad psicológica de los atacantes de ser en algún punto "reconocidos", y asumiéndolo de forma estadística, se puede hallar entre los nombres, información relacionada con la proveniencia del ataque. En este sentido, pueden encontrarse más de 200 nombres diferentes, entre los que se detectan referencias a una nacionalidad, idioma o ideología. Por ejemplo, es posible encontrar nombres como "*Hacked by X*" donde X es sencillamente el sobrenombre con el que desea ser identificado el individuo. Dichos nombres se repiten múltiples veces entre distintos casos, lo que indica que el atacante no está particularmente orientado a una institución u objetivo solamente.

En otros casos se encuentran 28 nombres de los llamados grupos de hackers (*hacking teams*) no vinculados de forma directa a países en base a su nombre, como ser "Ashiyane Digital Security Team" o "Fallaga Team". Estos conforman 391 registros de ataque, lo cual implica un 17% del total de los ataques, atribuidos a grupos o equipos. También pueden darse entre las atribuciones algunas referencias a nacionalidades, encontrándose así nombres como "Afghan Exploiters", "Turkish Energy" o "Brazil hack team" aunque solo podría ser concluyente el origen en estos casos cuando los ataques provengan de direcciones IP del país referenciado. En la mayoría de los eventos, en efecto, los ataques provienen de direcciones argentinas, que son utilizadas como pivot para alcanzar los sitios objetivo.

En cuanto a lo que puede analizarse de los nombres de fantasía, probablemente lo más llamativo es que pueden encontrarse referencias a equipos y personas que son del propio país (Argentina) lo que, aunque constituye una minoría de los registros (menos del 10%) obliga a descartar la idea de que los incidentes siempre son perpetrados por atacantes externos. Dicha situación aparece en muchas ocasiones cuando se trata de casos de corte político, donde por cuestiones ideológicas o de bandera política, se realizan también ataques dirigidos, práctica que se denominada *hacktivismo*, por síntesis de hacking y activismo[5]. Como

dato adicional, cabe destacar que, en la mayoría de los casos, los atacantes que por sus sobrenombres parecieran ser ciudadanos argentinos, no siempre ocultan su dirección de IP desde la cual realizan el ataque, ya que puede verse que la misma coincide con direcciones del espacio de asignación nacional.

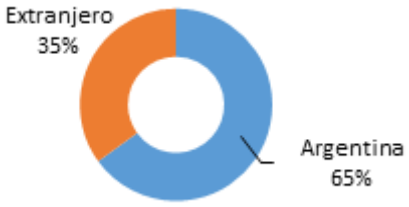

Figura 5. Orígenes de los ataques según dirección IP.

VI. Conclusiones

Si bien para evaluar una estrategia de ciberdefensa se requiere de información específica que apunte a la resolución de potenciales conflictos y problemas en el corto y largo plazo, no puede dejarse de lado la muestra más visible de la infraestructura online nacional, que lo constituyen los sitios web gubernamentales.

Tanto en un aspecto técnico como en el sentido del daño a la imagen pública que provocan los ataques a dicho tipo de dominios, es necesario tomar medidas preventivas, detectivas y correctivas, que se orienten a garantizar que los activos informáticos del estado nacional están suficientemente protegidos ante las distintas amenazas existentes.

Dependiendo del tipo de ataque pueden considerarse violados los principios de confidencialidad (materializado por ejemplo en el robo o acceso no autorizado a información sensible) integridad y disponibilidad, con lo que los pilares de la seguridad podrían quedar totalmente comprometidos según el caso.

Es importante mencionar que las medidas de control y prevención aplicables están largamente estudiadas en el ámbito de la seguridad informática y de la información, por lo que las soluciones y acciones a tomar parecieran estar más limitadas por cuestiones políticas y de gestión que por cuestiones técnicas.

Reconocimientos

A Arturo Busleiman, por la información provista y el conocimiento aportado.

Referencias

[1] Consejo Argentino para las Relaciones Internacionales, Ciberdefensa-Ciberseguridad, Riesgos y Amenazas, 2013.

[2] "Internet of things research study," Hewlett-Packard Enterprise Development LP, Palo Alto, California, Estados Unidos, 2015.

[3] C. Tankard, "Advanced Persistent threats and how to monitor and deter them," Network security, vol. 8, pp. 16-19, Agosto 2011.

[4] B. Smith, W. Yurcik, & Doss, D. "Ethical hacking: the security justification redux," In Technology and Society, 2002.(ISTAS'02). 2002 International Symposium on, pp. 374-379.

[5] T. Jordan, "Online direct action: Hacktivism and radical democracy," InRadical democracy and the internet, Palgrave Macmillan UK, 2007, pp. 73-88.