

Nuevo objetivo del fraude online: el control de dominios

David Barroso Berrueta
R&D CTO S21sec

La situación actual respecto al fraude online, nos permite desde S21sec detectar y prevenir, en numerosos casos, los ataques de fraude que se van produciendo, muchas veces incluso en las fases de preparación. Se ha comentado en varias ocasiones la capacidad actual de los troyanos existentes en Internet del robo de credenciales de acceso a las páginas web de las entidades financieras, actividad que realizan mediante diversas técnicas cada día más sofisticadas (BHO, inyección en procesos o man-in-the-middle) y en este artículo vamos a exponer un nuevo uso observado de los mismos.

El escenario más frecuente con el que nos encontramos suele estar compuesto por tres elementos muy bien diferenciados:

1. Un *exploit* que aprovecha una vulnerabilidad en un navegador generalmente introducido como un *iframe* dentro de páginas legítimas (**el método de infección**).
2. Código malicioso que es descargado una vez explotado el punto anterior (**el troyano**).
3. Una aplicación web donde se almacenan los datos robados en el ordenador infectado y se pueden posteriormente consultar (**el panel de control**).

Dentro de este escenario, las combinaciones son múltiples: utilización de varios sitios web, de diferentes troyanos, *exploits* para Internet Explorer, Firefox u Opera. Las posibilidades son casi infinitas.

Dentro de la tríada anterior, para obtener el mayor número de ordenadores infectados, es necesario que el método de contagio esté presente en la mayor cantidad de sitios web posibles, y por supuesto, en sitios web de masiva afluencia. La forma de 'infectar' páginas totalmente legítimas suele basarse en alguna vulnerabilidad existente en el portal web (SSI, SQL Injection), una práctica bastante efectiva que puede ser utilizada masivamente debido a malas configuraciones o a la escasa actualización del software utilizado en estos portales.

Una vez que el ordenador está infectado, el código malicioso obtiene control total sobre el mismo y comienza a capturar toda la información que se envía a través de Internet, como por ejemplo los usuarios y contraseñas de acceso a portales. Otras veces, redirige al usuario a páginas de phishing para intentar convencer al usuario que introduzca todas sus credenciales.

La situación descrita hasta ahora no ofrece nada nuevo que no se haya comentado con anterioridad. La diferencia que encontramos ahora está relacionada con la existencia de nuevos factores con los que antes no contábamos y que suponen un riesgo mayor a

todas las organizaciones. El factor principal del que estamos hablando es el control de los dominios de Internet.

Un ejemplo de panel de control como el que se aprecia debajo, muestra el número de ordenadores infectados dentro de España, 68684:

Top 10 Countries			Top 10 new countries today			Top 10 Countries order by bot's reports		
Country	Rating		Country	Rating		Country	Rating	
United States	82636 20%		United States	90 30%		United States	3870126 40%	
Spain	68684 17%		France	50 17%		Spain	1019367 11%	
Peru	41545 10%		Spain	42 14%		Australia	408507 4%	
China	39698 10%		Peru	40 13%		Peru	361388 4%	
Turkey	26367 6%		Turkey	11 4%		Russia	355136 4%	
France	24399 6%		Germany	10 3%		Brazil	307113 3%	
Germany	17727 4%		Russia	6 2%		France	283249 3%	
Russia	12082 3%		Macedonia	5 2%		United Kingdom	280295 3%	
Egypt	10719 3%		Slovakia	5 2%		Mexico	256798 3%	
Mexico	10636 3%		Venezuela	4 1%		Turkey	235749 2%	
Totally: 115			totaly: 300			Totally bot's reports: 9636334		

Generalmente, en los paneles de control se suelen filtrar los datos robados a los ordenadores infectados buscando portales que tengan alguna relación con algún medio económico: entidades financieras, subastas, pagos *online*. Sin embargo, en los últimos casos se ha podido comprobar que también interesan los datos de acceso para la alta/modificación/baja de dominios de Internet (las credenciales de acceso para el mantenimiento de estos dominios).

Con estos datos un atacante es capaz de gestionar:

- Denegaciones totales de servicio redirigiendo su dominio principal de Internet (www.miempresa.com) a una dirección IP inexistente.
- Ataques de phishing realizando el mismo método que en el punto anterior pero redirigiendo todo el tráfico a una dirección IP maliciosa (www.miempresa.com resuelve a w.x.y.z)
- Venta/Transferencia de dominios de forma no autorizada (transferencia del su dominio miempresa.com)
- Cambio de datos de contacto de su dominio
- Redirigir todo el tráfico de correo de su dominio (el registro MX) a un servidor de correo malicioso para obtener todo su correo electrónico.
- Creación de subdominios (ej: infector.miempresa.com) utilizados posteriormente de forma maliciosa (como por ejemplo de métodos de infección)

En los últimos casos detectados por S21sec, son varias las empresas encargadas de mantenimiento de dominios involucradas en el robo de credenciales y en el último caso detectado, existen más de 400 usuarios y contraseñas de acceso a la administración de dominios de Internet. Teniendo en cuenta que estos usuarios generalmente gestionan

varios dominios de Internet, obtenemos una cifra de varios miles de dominios de Internet que pueden ser utilizados de diferentes fines.

En resumen, las actividades ilegales relacionadas con el fraude en Internet utilizan nuevas técnicas para delinquir. La gestión de los dominios de Internet es una actividad que rara vez se considera como un proceso a evaluar en un análisis de riesgos. Sin embargo, está claramente demostrado que la amenaza del robo de las credenciales de acceso está bien presente y tenemos que tenerla en cuenta.

Algunas prácticas seguras que pueden ayudar a protegerse de este tipo de amenazas son:

- Cumplir la política de usuarios y contraseñas en las credenciales de gestión de dominios (generalmente en portales externos)
- No utilizar usuarios genéricos
- No utilizar estas credenciales en ordenadores que no sean de confianza
- Si es posible, utilizar doble autenticación
- Contratar servicios de detección y prevención de robos de credenciales