Angler Exploit Kit Usa Camuflaje Para No Ser Detectado

Angler Exploit Kit se ha convertido en el más avanzado, más potente y el mejor kit exploit disponible en el mercado, superando al perverso **BlackHole exploit kit**, con una serie de hazañas incluyendo vulnerabilidades de tipo «Zero Day» y una nueva técnica agregada al kit.

Angler Exploit tiene una reciente técnica en el Kit, la cual es llamada «**Domain Shadowing**» o Camuflaje de Dominio; la cual se considera que es la próxima evolución de la delincuencia en línea. *Domain Shadowing*, apareció por primera vez en 2011, es el proceso de utilización de los inicios de sesión de registro de dominios a los usuarios al **crear subdominios**.

¿Qué Es Domain Shadowing?

Con la ayuda de la técnica de Camuflaje de Dominio utilizado en una campaña Angler reciente, los atacantes están robando las credenciales de dominio del registrante para crear decenas de miles de subdominios que se utilizan en los ataques de estilo hit-and-run con el fin de reorientar las víctimas, ya sea a los sitios de ataque.

El investigador de seguridad Nick Biasini de equipo de inteligencia Talos de Cisco analiza la campaña y dijo que la campaña de ataque ha sido masiva y continua en los últimos tres meses.

> *«Domain Shadowing usa credenciales del registrante comprometido, ha sido la técnica más eficaz hasta el momento, difícil de parar. Las cuentas son en gran medida al azar lo que no hay manera de rastrear cual será el siguiente dominio*

*a atacar», dijo **Nick Biasini**.*

¿Cómo Lo Hacen Los Hackers?

En los recientes ataques, los ciberdelincuentes están aprovechando el hecho de que la mayoría de los propietarios de dominio no monitorean regularmente sus cuentas de resgistro, las cuales están comprometidas típicamente a través de **ataques de phishing**. Esto es aprovechado por los atacantes para crear un suministro interminable de subdominios que se utilizará en futuros ataques.

Una nueva técnica llamada Fast Flux permite a los piratas informáticos cambiar la dirección IP asociada a un dominio para evadir la detección y técnicas de listas negras. A diferencia del camuflaje de dominio, el cual cambia subdominios asociados a un único dominio o pequeño grupo de direcciones IP, Fast Flux gira rápidamente una sola entrada de dominio o DNS a una gran lista de direcciones IP.

Cuentas De GoDaddy En Riesgo

Cisco ha encontrado hasta 10.000 sub-dominios maliciosos en las cuentas, la mayoría de ellos relacionados con los **clientes de GoDaddy**, aunque los investigadores de seguridad señalaron que este no fue el resultado de cualquier violación de datos, pero esto es debido a que el GoDaddy controla un tercio de los dominios en la Internet.

Medio De Ataque

Hay varios niveles al ataque, con diferentes subdominios maliciosos que se crean para las diferentes etapas enumeradas a continuación:

- Los usuarios usan anuncios maliciosos en el navegador

web.

- El anuncio malicioso redirige al usuario a la primera fila de subdominios conocidos como «puerta».
- El primer nivel es responsable de la redirección de las víctimas a una página de destino que aloja el Angler Exploit Kit, el cual usa un Adobe Flash o Microsoft Silverlight.
- Esta página final está siendo girado en gran medida y, a veces, esas páginas están activos sólo para una cuestión de minutos.