Más de un millón de dominios son vulnerables a ser tomados por actores maliciosos mediante lo que se conoce como un ataque de Patos Sentados.

Este potente vector de ataque, que explota vulnerabilidades en el sistema de nombres de dominio (DNS), está siendo utilizado por más de una docena de ciberdelincuentes con vínculos rusos para secuestrar dominios de manera furtiva, según un análisis conjunto publicado por Infoblox y Eclypsium.

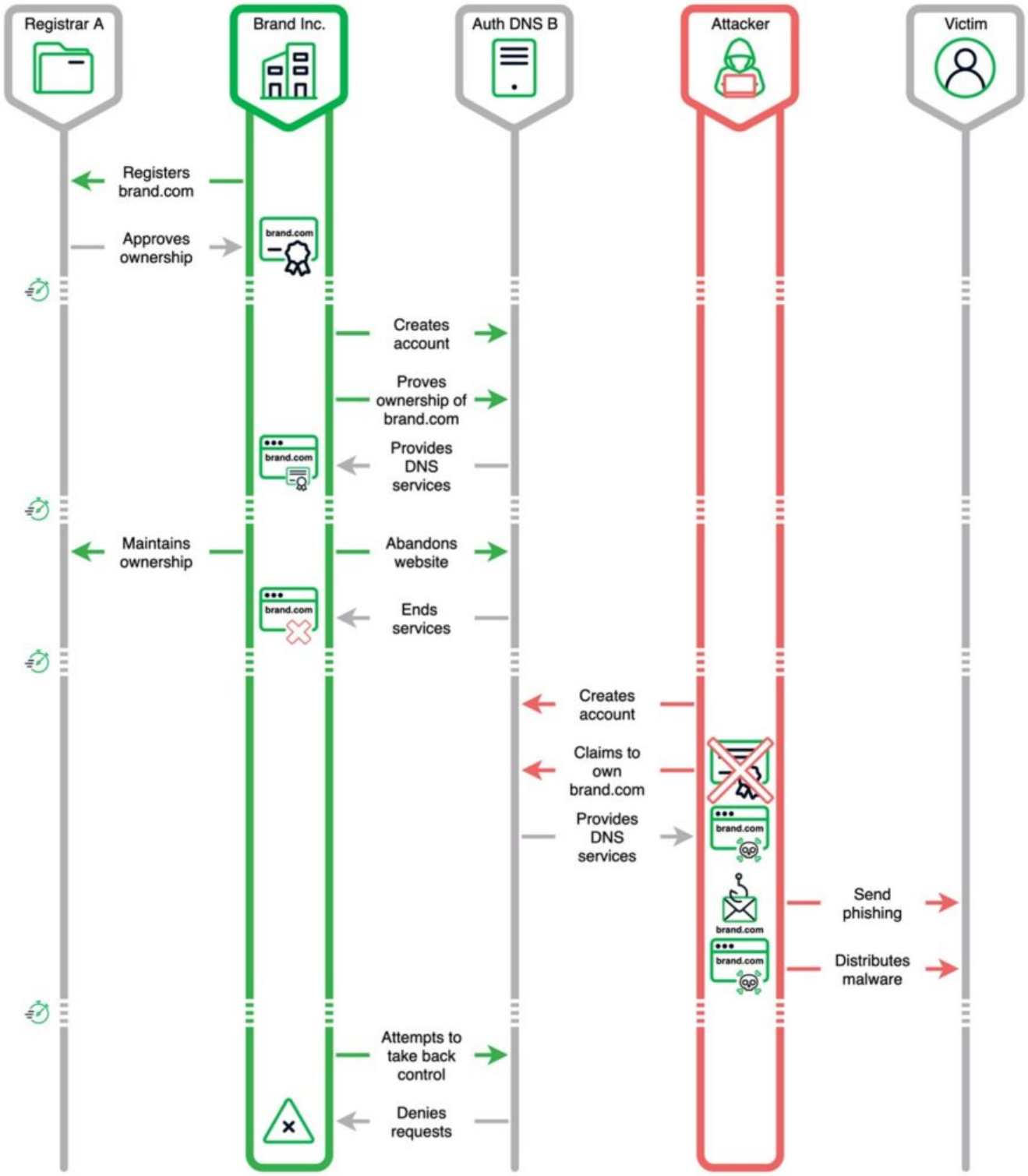
> *«En un ataque de Patos Sentados, el atacante toma control de un dominio registrado en un servicio DNS autoritativo o proveedor de alojamiento web sin acceder a la cuenta del verdadero propietario en el proveedor de DNS o registrador,»* explicaron los investigadores.
>
> *«Patos Sentados es más fácil de ejecutar, más probable de tener éxito y más difícil de detectar que otros vectores de ataque de secuestro de dominios ampliamente conocidos, como los CNAMEs colgantes.»*

Una vez que un dominio ha sido tomado por el atacante, podría ser utilizado para diversas actividades maliciosas, como servir malware y realizar spam, aprovechando la confianza asociada con el propietario legítimo.

Los detalles de esta técnica de ataque «perniciosa» fueron documentados por primera vez por The Hacker Blog en 2016, aunque sigue siendo en gran parte desconocida y no resuelta hasta hoy. Se estima que más de 35,000 dominios han sido secuestrados desde 2018.

«Es un misterio para nosotros. Frecuentemente recibimos preguntas de clientes potenciales sobre ataques de CNAMEs colgantes, que también implican el secuestro de registros olvidados, pero nunca hemos recibido una pregunta sobre un secuestro de Patos Sentados», dijo la Dra. Renee Burton, vicepresidenta de inteligencia de amenazas en Infoblox.

El problema radica en la configuración incorrecta en el registrador de dominios y el proveedor de DNS autoritativo, además del hecho de que el servidor de nombres no puede responder autoritativamente para un dominio que está designado para servir (es decir, delegación defectuosa).


Registrar A
Brand Inc.
Auth DNS B
Attacker
Victim
Registers brand.com
Approves ownership
brand.com
Creates account
Proves ownership of brand.com
Provides DNS services
Maintains ownership
Abandons website
Ends services
Creates account
Claims to own brand.com
Provides DNS services
Send phishing
Distributes malware
Attempts to take back control
Denies requests

También se requiere que el proveedor de DNS autoritativo sea vulnerable, permitiendo al atacante reclamar la propiedad del dominio en el proveedor de DNS autoritativo delegado sin tener acceso a la cuenta del propietario legítimo en el registrador de dominios.

En tal escenario, si el servicio DNS autoritativo para el dominio expira, el atacante podría crear una cuenta con el proveedor y reclamar la propiedad del dominio, suplantando a la marca detrás del dominio para distribuir malware.

> *«Hay muchas variaciones, incluyendo cuando un dominio ha sido registrado, delegado, pero no configurado en el proveedor,»* dijo Burton.

El ataque de Patos Sentados ha sido utilizado por diversos actores de amenazas, con los dominios robados utilizados para alimentar múltiples sistemas de distribución de tráfico (TDSes) como 404 TDS (también conocido como Vacant Viper) y VexTrio Viper. También se ha utilizado para propagar falsas amenazas de bomba y estafas de sextorsión.

> *«Las organizaciones deberían revisar los dominios que poseen para ver si alguno está defectuoso y deberían usar proveedores de DNS que tengan protección contra Patos Sentados,»* recomendó Burton.