El hacktivista bajo el nombre VandaTheGod, ha sido descubierto por investigadores de seguridad cibernética al dejar rastros de una serie de ataques a sitios web del gobierno desde julio de 2019.

En un informe, investigadores de Check Point afirmaron que lograron mapear la actividad de VandaTheGod a lo largo de los años, y eventualmente reducir la identidad real del atacante a un individuo brasileño de la ciudad de Uberlandia.

La compañía de seguridad cibernética dijo que notificó a las autoridades policiales interesadas sobre sus hallazgos para una acción adicional, y dijo también que las actividades de las redes sociales en los perfiles asociados con el hacker se detuvieron a finales de 2019.

VandaTheGod tiene una gran historia en ataques a sitios web gubernamentales, universidades y proveedores de atención médica. Particularmente, el atacante aseguró haber violado la base de datos de Tu Ora Compass Health, de Nueva Zelanda, ofreciendo los detalles médicos de un millón de pacientes a la venta en Twitter en octubre pasado.

El hacker supuestamente forma parte del *«Ejército Cibernético Brasileño»* (BCA), y también ha comprometido decenas de sitios web para difundir mensajes antigubernamentales, además de mostrar el logotipo de BCA en capturas de pantalla de cuentas y sitios web comprometidos.

> *«Muchos de los mensajes que se dejaron en los sitios web desfigurados implicaron que los ataques fueron motivados por un sentimiento antigubernamental y se llevaron a cabo para combatir las injusticias sociales que el pirata informático creía que eran un resultado directo de la corrupción gubernamental»,* dijeron los investigadores.

Una línea de tiempo de los tweets de VandaTheGod muestra que el pirata informático disfrutó de la atención de los informes de los medios que mencionan los esfuerzos de piratería, hasta el punto de afirmar que *«dejaré de piratear sitios web»* una vez que el total

llegue a 5,000.

> *«VandaTheGod no solo persiguió los sitios web del gobierno, sino que también lanzó ataques contra figuras públicas, universidades e incluso hospitales. En un caso, el atacante afirmó tener acceso a los registros médicos de un millón de pacientes de Nueva Zelanda, que fueron ofrecidos a la venta por 200 dólares»*, dijeron los investigadores.

Según los registros de Zone-H, un portal de seguridad que contiene un archivo de todas las intrusiones en la web, en la actualidad hay 4820 entradas de sitios web pirateados vinculados a VandaTheGod, la mayoría de lo cuales pertenecen a personas y entidades en Estados Unidos, Australia, Países Bajos, Italia, Sudáfrica, Canadá, Reino Unido y Alemania.

Check Point dijo que trabajaron rastreando la información de WHOIS del dominio *«vandathegod.com»*, que los condujo a la dirección de correo electrónico *«fathernazi@gmail.com»*, que se utilizó para registrar otros sitios web, como *«braziliancyberarmy.com»*.

Sin embargo, lo que reveló la verdadera identidad de VandaTheGod fueron unas capturas de pantalla que se cargaron en Twitter, de las cuales los investigadores identificaron un perfil de Facebook que pertenecía al atacante *«Vanda De Assis»*, así como el nombre real de la persona, identificado solo por las iniciales MR.

Con esto, los investigadores afirmaron que lograron identificar una serie de publicaciones cruzadas entre el perfil de Facebook vinculado a MR y el de Vanda de Assis, incluidas fotos de la sala de estar del sujeto, lo que demuestra que tanto las cuentas MR y VandaTheGod estaban controladas por la misma persona.

> *«VandaTheGod logró llevar a cabo muchos ataques de piratería, pero finalmente fracasó desde la perspectiva de OPSEC, ya que dejó muchos rastros que condujeron*

> *a su verdadera identidad, especialmente al comienzo de su carrera de piratería»,* dijeron los investigadores de Check Point
>
> *«Finalmente, pudimos conectar la identidad de VandaTheGod con certeza a un individuo brasileño específico de la ciudad de Uberlandia, y transmitir nuestros hallazgos a las fuerzas del orden público para que pudieran tomar más medidas».*