Investigadores chinos en ciberseguridad descubrieron otra vulnerabilidad que pone en riesgo 100,000 routers y modifican sus configuraciones de DNS para hackear a los usuarios mediante páginas web con código malicioso, especialmente cambiando vínculos legítimos de sitios bancarios para robar credenciales.

GhostDNS es la campaña que descubrieron los investigadores, que funciona de forma similar al malware DNSChanger, que permite a los atacantes tomar el control del tráfico de Internet de los usuarios para tomar información sensible.

Según el nuevo reporte de la firma de seguridad cibernética, Qihoo 360´s NetLab, al igual que DNSChanger, GhostNDS escanea las direcciones IP de los routers que cuentan o no con contraseña, al acceder a las configuraciones del router, los piratas cambian las DNS por default para controlar el tráfico web.

GhostDNS cuenta con cuatro módulos principales:

1.- DNSChanger Module: Este es el primer módulo del malware diseñado para explotar los objetivos, mediante Shell DNSChanger, Js DNSChanger y PyPhp DNSChanger.

Shell DNSChanger – Escrito en el lenguaje de programación Shell, combina 25 scripts Shell que pueden obtener la contraseña del router mediante fuerza bruta en 21 firmwares de diferentes compañías.

Js DNSChanger – Desarrollado en JavaScript, incluye 10 scripts de ataque diseñados para infectar 6 firmwares.

> *«Esta estructura es funcional principalmente cuando se divide en escáneres, generadores de carga y programas de ataque. El programa Js DNSChanger generalmente se inyecta en sitios web phishing, por lo que funciona acompañado de un sistema web de phishing»,* dicen los investigadores.

PyPhp DNSChanger – Escrito en Python y PHP, contiene 69 scripts de ataque para 47 firmwares de routers diferentes. Este submódulo fue encontrado en más de 100 servidores, entre ellos, Google Cloud. Incluye funcionalidades como Web API y módulo de escaneo y ataque.

Este submódulo es el núcleo de DNSChanger y permite a los atacantes escanear la Internet para encontrar routers vulnerables.

2.- Web Admin Module: Los investigadores aún no tienen mucha información sobre este módulo, pero al parecer imitan el panel de configuración de los routers para que las víctimas ingresen sus credenciales.

3.- Rogue DNS Module: Este módulo es responsable de resolver los nombres de dominio objetivos desde los servidores de control de los atacantes, involucra principalmente servicios bancarios y de alojamiento en la nube, junto a un dominio perteneciente a una empresa de seguridad llamada Avira.

> *«Nosotros no tenemos acceso al Servidor Rogue DNS, por lo que no podemos estar seguros cómo son sustraídos los nombres DNS, pero al consultar al Top 1M de Alexa y a nuestros DNSMon Top 1M contra el servidor DNS falso (139.60.162.188), logramos encontrar un total de 52 dominios que fueron secuestrados»,* afirman investigadores de NetLab.

4.- Phishing Web Module: Cuando un dominio objetivo resuelve satisfactoriamente por medio del módulo de DNS falso, el módulo web de Phishing apunta a servir la versión falsa correcta para el sitio web específico.

Los routers/firmawe que han resultado afectados hasta el momento son:

Según los investigadores, desde el 21 de septiembre al 27 del mismo mes, GhostDNS ha comprometido más de 100 mil routers, de los cuales 87.8% de los dispositivos se encuentran en Brasil, lo que hace suponer que Brasil es el principal objetivo de los piratas informáticos.

> *«Actualmente la campaña se centra en Brasil, donde encontramos más de 100 mil direciones IP de routers, y 70+ router/firmware involucrados, además de 50+ nombres de dominio referentes a grandes bancos de Brasil, por otro lado, Netflix, Citibank.br fueron obejtivos para el robo de credenciales»*, dijeron los investigadores.

Desde que GhostDNS ha logrado escalarse, utiliza diferentes vectores de ataque y ha adoptado procesos automáticos de ataque. Aún así, se ha advertido a los usuarios para proteger sus dispositivos.

Cómo proteger tu router del ataque de hackers

Para evitar ser víctima de un ataque, es recomendable que tu router funcione con la última versión del firmware y asegurarlo con una contraseña de alta seguridad que combine letras, números y caracteres especiales.

Además, es recomendable deshabilitar la administración remota, cambiando la dirección IP por default, y codificar un servidor DNS de confianza en el router o en el sistema operativo.

Los investigadores de NetLab también recomiendan que los fabricantes de routers incrementen la complejidad de la contraseña por default y mejorar el sistema de seguridad de sus productos.