C□nh báo! Chi□n d□ch botnet có tên GhostDNS đang chi□m quy□n ki□m soát hơn 100000 router

Những nhà nghiên cứu b□o mật tại công ty an ninh mạng NetLab c□a Qihoo 360 mới đây vừa phát hiện ra một chi□n dịch mã độc có tên là GhostDNS đã chi□m quy□n đi□u khi□n c□a hơn 100 ngàn router □ các gia đình, thay đ□i thi□t lập DNS và dùng những trang web độc hại đ□ ăn c□p thông tin người dùng.

Tương tự mã độc DNSChanger n□i ti□ng, GhostDNS hoạt động bằng cách thay đ□i thi□t lập DNS c□a các thi□t bị chịu □nh hư□ng. Sau đó, k□ t□n công sẽ đi□u hướng truy cập Internet c□a người dùng qua các máy ch□ nguy hại và ăn c□p các thông tin nhạy c□m như tài kho□n ngân hàng… c□a người dùng.

Theo NetLab, hệ th□ng GhostDNS s□ dụng r□t nhi□u đoạn mã khác nhau đ□ dò tìm mật kh□u c□a các router từ 21 nhà s□n xu□t khác nhau. Thậm chí, họ còn phát hiện □ hơn 100 server, h□u h□t là trên Google Cloud có c□ những đoạn mã t□n công được thi□t k□ riêng dành cho các router hoặc firmware c□a router bị □nh hư□ng

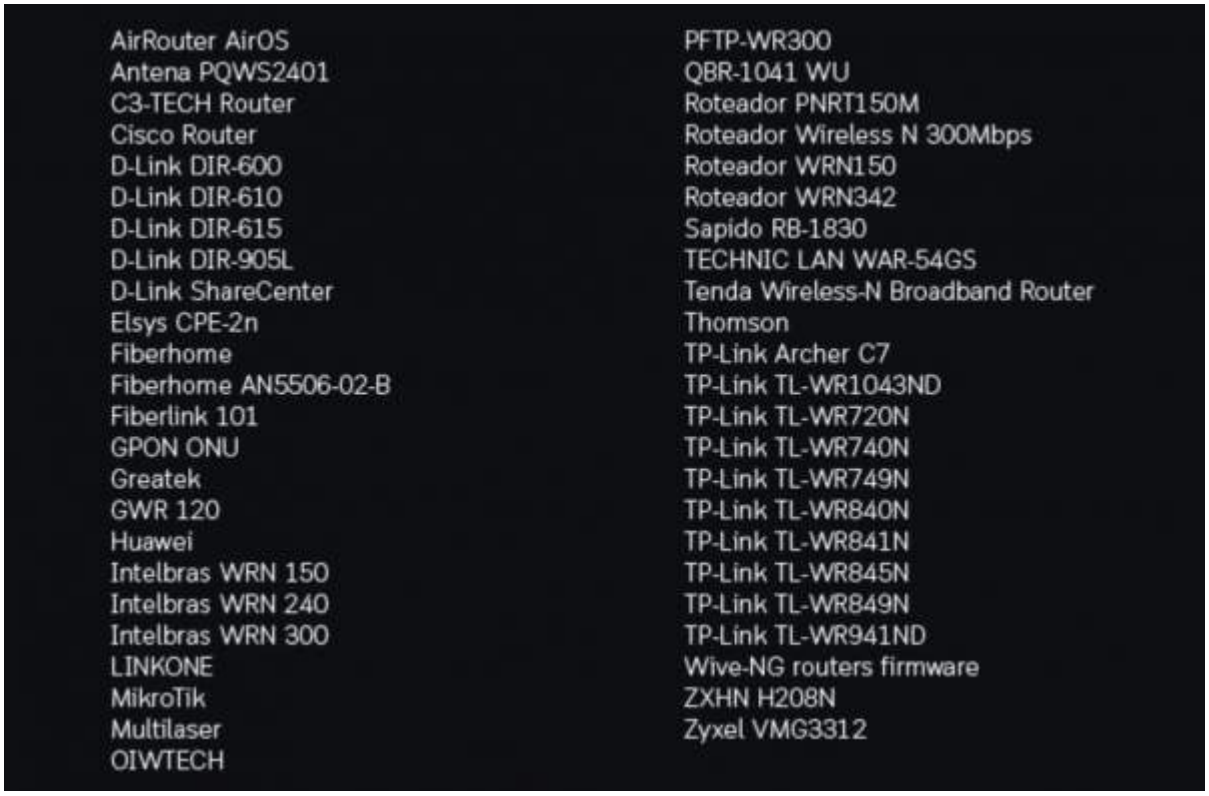
Ngoài ra, GhostDNS còn có hàng loạt các module phụ trợ đ□ quét trên Internet và tìm ra các router nằm trong nhóm bị □nh hư□ng và có th□ khai thác. Đặc biệt, có một module DNS gi□ mạo chuyên phân gi□i tên mi□n mục tiêu từ các máy ch□ web do k□ t□n công ki□m soát,

Chưa h□t, GhostDNS còn có hàng loạt các module phụ trợ đ□ k□ t□n công có th□ quét trên Internet và tìm ra các router nằm trong nhóm bị □nh hư□ng và có th□ khai thác. Đáng chú ý là một module DNS gi□ mạo chịu trách nhiệm phân gi□i tên mi□n mục tiêu từ các máy ch□ web do k□ t□n công ki□m soát.

Theo các chuyên gia b□o mật, ch□ từ 21/9 đ□n 27/9, hơn 100 ngàn router (kho□ng hơn 87% là các thi□t bị tại Brazil) đã bị GhostDNS thao túng. Đáng lưu ý là các m□u router c□a D-Link và TP-Link, được khá nhi□u người dùng trong nước s□ dụng cũng nằm trong danh sách các router bị □nh hư□ng. Thậm chí các thi□t bị

do Huawei sản xuất, đang được nhiều nhà mạng cung cấp cho người dùng theo hợp đồng Internet cũng nằm trong danh sách này.

Dưới đây là danh sách các router/firmware bị ảnh hưởng bởi GhostDNS.



Chiến dịch GhostDNS là một mối nguy hiểm thật sự cho người dùng bởi nó có quy mô lớn, quá trình tấn công tự động với nhiều phương pháp tấn công khác nhau.

Theo khuyến cáo của các nhà nghiên cứu, người dùng nên chủ động bảo vệ router tại gia đình của họ bằng cách cập nhật firmware mới nhất, đổi mật khẩu mạnh và phức tạp, thay đổi các địa chỉ IP mặc định trong mạng nội bộ, dùng tắt tính năng quản trị từ xa (remote administration), và chỉ sử dụng các DNS đáng tin cậy cho router hoặc hệ điều hành.