



Cảnh báo! Chiến dịch botnet có tên GhostDNS đang chiếm quyền kiểm soát hơn 100000 router

Những nhà nghiên cứu bảo mật tại công ty an ninh mạng NetLab của Qihoo 360 mới đây vừa phát hiện ra một chiến dịch mã độc có tên là GhostDNS đã chiếm quyền điều khiển của hơn 100 ngàn router ở các gia đình, thay đổi thiết lập DNS và dùng những trang web độc hại để ăn cắp thông tin người dùng.

Tương tự mã độc DNSChanger nổi tiếng, GhostDNS hoạt động bằng cách thay đổi thiết lập DNS của các thiết bị chịu ảnh hưởng. Sau đó, kẻ tấn công sẽ điều hướng truy cập Internet của người dùng qua các máy chủ nguy hại và ăn cắp các thông tin nhạy cảm như tài khoản ngân hàng... của người dùng.



GhostDNS

Wi-Fi Router Hacking Malware

Theo NetLab, hệ thống GhostDNS sử dụng rất nhiều đoạn mã khác nhau để dò tìm mật khẩu của các router từ 21 nhà sản xuất khác nhau. Thậm chí, họ còn phát hiện ra hơn 100 server, hầu hết là trên Google Cloud có chứa những đoạn mã tấn công được thiết kế riêng dành cho các router hoặc firmware của router bị ảnh hưởng.

Ngoài ra, GhostDNS còn có hàng loạt các module phụ trợ để quét trên Internet và tìm ra các router nằm trong nhóm bị ảnh hưởng và có thể khai thác. Đặc biệt, có một module DNS giả mạo chuyên phân giải tên miền mục tiêu từ các máy chủ web do kẻ tấn công kiểm soát,

Chưa hết, GhostDNS còn có hàng loạt các module phụ trợ để kẻ tấn công có thể quét trên Internet và tìm ra các router nằm trong nhóm bị ảnh hưởng và có thể khai thác. Đáng chú ý là một module DNS giả mạo chịu trách nhiệm phân giải tên miền mục tiêu từ các máy chủ web do kẻ tấn công kiểm soát.

Theo các chuyên gia bảo mật, chỉ từ 21/9 đến 27/9, hơn 100 ngàn router (khoảng hơn 87% là các thiết bị tại Brazil) đã bị GhostDNS thao túng. Đáng lưu ý là các mẫu router của D-Link và TP-Link, được khá nhiều người dùng trong nước sử dụng cũng nằm trong danh sách các router bị ảnh hưởng. Thậm chí các thiết bị 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.

AirRouter AirOS	PFTP-WR300
Antena PQWS2401	QBR-1041 WU
C3-TECH Router	Roteador PNRT150M
Cisco Router	Roteador Wireless N 300Mbps
D-Link DIR-600	Roteador WRN150
D-Link DIR-610	Roteador WRN342
D-Link DIR-615	Sapido RB-1830
D-Link DIR-905L	TECHNIC LAN WAR-54GS
D-Link ShareCenter	Tenda Wireless-N Broadband Router
Elsys CPE-2n	Thomson
Fiberhome	TP-Link Archer C7
Fiberhome AN5506-02-B	TP-Link TL-WR1043ND
Fiberlink 101	TP-Link TL-WR720N
GPON ONU	TP-Link TL-WR740N
Greatek	TP-Link TL-WR749N
GWR 120	TP-Link TL-WR840N
Huawei	TP-Link TL-WR841N
Intelbras WRN 150	TP-Link TL-WR845N
Intelbras WRN 240	TP-Link TL-WR849N
Intelbras WRN 300	TP-Link TL-WR941ND
LINKONE	Wive-NG routers firmware
MikroTik	ZXHN H208N
Multilaser	Zyxel VMG3312
OIWTECH	

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.