Warning, the botnet campaign called GhostDNS is taking over more than 100000 routers

Security researchers at NetLab, a security firm of Qihoo 360, recently discovered a malicious campaign called GhostDNS took over more than 100,000 home routers, changing settings. DNS and use malicious websites to steal user information.

Security researchers at NetLab, a security firm of Qihoo 360, recently discovered a malicious campaign called GhostDNS took over more than 100,000 home routers, changing settings. DNS and use malicious websites to steal user information.

Similar to the famous DNSChanger malware, GhostDNS works by changing the DNS settings of affected devices. The attacker then navigates the user's Internet access through malicious servers and steals sensitive information such as the user's bank account .

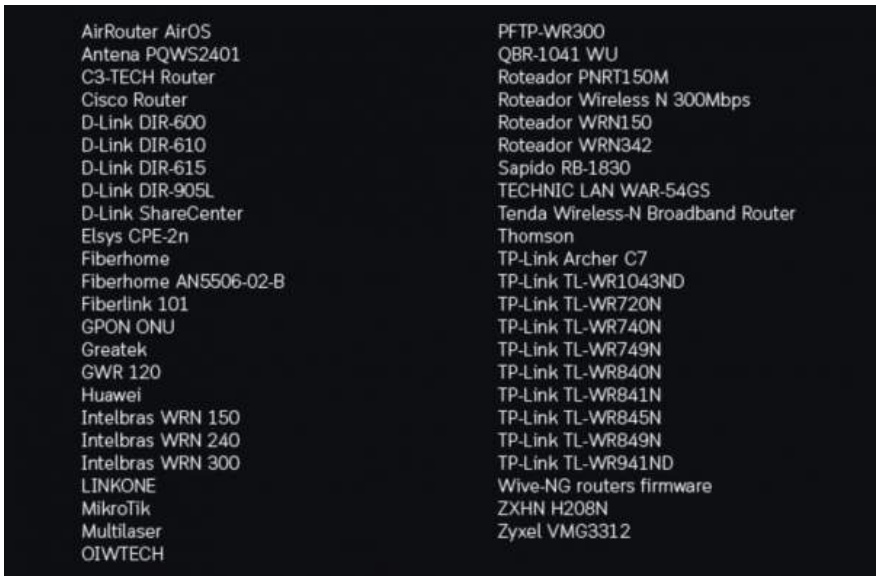
According to NetLab, the GhostDNS system uses a lot of different code to detect the passwords of routers from 21 different manufacturers. They even found in more than 100 servers, mostly on Google Cloud, including attack codes designed specifically for routers or firmware of the affected router.

In addition, GhostDNS has a series of auxiliary modules to scan on the Internet and find out which routers are in the affected group and can exploit. In particular, there is a fake DNS module that resolves target domain names from web servers controlled by attackers.

And yet, GhostDNS has a series of auxiliary modules that an attacker can scan on the Internet and find out which routers are in the affected group and can exploit. It is noteworthy that a fake DNS module is responsible for resolving target domain names from web servers controlled by attackers.

According to security experts, from September 21 to September 27, more than 100,000 routers (about 87% of devices in Brazil) were manipulated by GhostDNS. Notably, D-Link and TP-Link router models, which are used by many domestic users, are also in the list of affected routers. Even devices manufactured by Huawei, which are being provided by many network providers for Internet contract users, are included in this list.

Below is a list of routers / firmware affected by GhostDNS.



GhostDNS campaign is a real danger for users because it is large scale, automatic attack process with many different attack methods.

As recommended by researchers, users should actively protect their home routers by updating the latest firmware, changing strong and complex passwords, and changing the default IP addresses on the local network. , use the remote administration feature (remote administration), and only use trusted DNS for the router or operating system.

See more:

1. How to detect VPNFilter malware before it destroys the router
2. How to change Modem login password and Vigor Draytek Router
3. Instructions to change IP address from Command Prompt