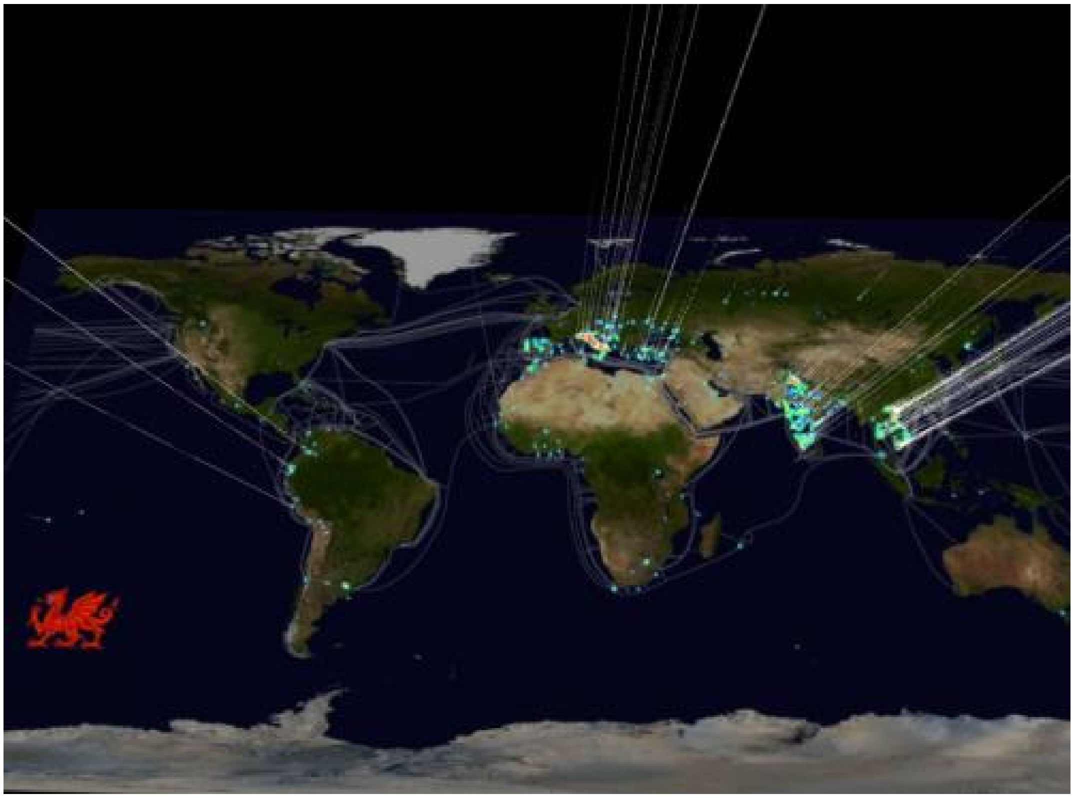
TechXplore

Security firm finds 300,000 home routers hacked

March 4 2014, by Bob Yirka



Affected'router'distribution'heatmap'visualization

(Phys.org) —Nonprofit American security firm Team Cymru (Celtic world for Wales) has announced that they have uncovered a hacking scheme that has impacted at least 300,000 routers used by people in their homes. Reps for the firm say that while the hack appears ominous, there is no evidence as yet to suggest that the hack was used for whatever purpose it was designed.

Hacker attacks on home routers generally take two approaches, though both rely on the same strategy—namely, accessing the router and changing a table to redirect domain name server (DNS) queries. DNS servers are the machines that convert native language web names, to IP addresses. What this means, for example, is that a user accessing a compromised router might use the link on their browser's "favorites" bar, to access their bank account. But instead of being routed to their bank, they are instead routed to a web page on a fake server that looks just like the real one. When the user types in their login information, it is stolen by the hackers, who use it to drain the account. That's the first approach (and the one used in the infamous attack carried out in Poland recently). Since it takes a great deal of effort to pull off, most hackers seem to instead prefer to redirect users to their expected site, but replace ads with their own, or add code that runs on user computers when they visit certain sites.

Reps for Team Cymru report that the hacked routers were mostly in Vietnam and other countries where many people are still using older, less well protected routers. They also note that it doesn't appear that the hackers actually misrouted users, thus, the hack is a mystery still. Interestingly, they note that the hacked routers all used just two IP addresses, both UK based. The companies that hold those two addresses have been notified regarding the hacking activity as have all the companies that make the routers that were hacked. Team Cymru suggests users take added precautions to safeguard their routers, such as being sure to password protect it (with a good password) and to occasionally check to see if unknown entities show up on their network.

More information: Report PDF: www.team-cymru.com/ReadingRoom … ymruSOHOPharming.pdf

Citation: Security firm finds 300,000 home routers hacked (2014, March 4) retrieved 5 May 2024 from https://techxplore.com/news/2014-03-firm-home-routers-hacked.html