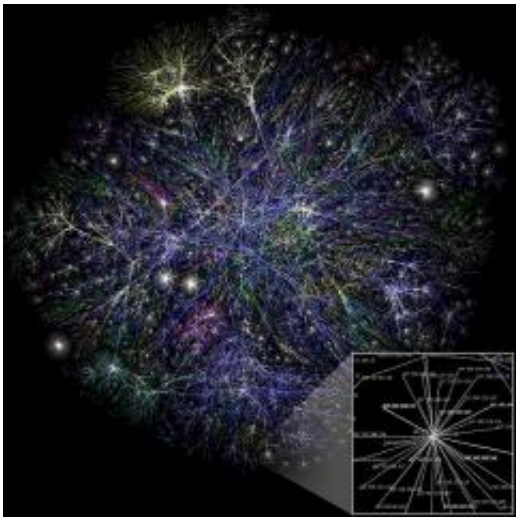
Peculiar traffic routes suggest hijacking headaches

December 8 2013, by Nancy Owano



Partial map of the Internet based on the January 15, 2005 data found on opte.org. Each line is drawn between two nodes, representing two IP addresses. Image: Wikimedia Commons.

(Phys.org) —Findings from Internet intelligence company Renesys sound an alert to a hijacking practice in the form of traffic misdirection on the Internet. A November 19 blog on the Renesys site has since caught the attention of a wider press: "Who is sending Internet traffic on long, strange trips?" asked a headline in *The Christian Science Monitor* earlier this month. The Renesys blog author, Jim Cowie, Chief Technology Officer, said that "We have actually observed live Man-In-the-Middle (MITM) hijacks on more than 60 days so far this year." He

said about 1,500 individual IP blocks have been hijacked in events lasting from minutes to days by attackers working from various countries. Simply put, data to and from finance firms, net phone services and governments was re-routed in several attacks this year. As Michael Mimoso of *Theatpost* noted, "Attackers are accessing routers running on the border gateway protocol (BGP) and injecting additional hops that redirect large blocks of Internet traffic to locations where it can be monitored and even manipulated before being sent to its intended destination."

As a result of the BGP routes hijacked, a portion of Internet traffic was misdirected to flow through Belarus and Iceland. The nature of this type of traffic crime is that it can happen again and again without the victim taking any notice. The traffic would just keep flowing. A user may log on each morning and work thinking nothing is unusual while it would be possible that the same traffic was being inspected and then released right back into the Internet and on its way to the user's desired destination. "It's possible to drag specific Internet traffic halfway around the world, inspect it, modify it if desired, and send it on its way," he said.

In February this year, security watchers at Renesys found that global traffic was being rerouted to Belarus. The Belarus traffic diversions stopped in March. They restarted briefly in May. Traffic diversions to Iceland were also seen this year. What's not known is the exact mechanism, motivation, or actors during these events, said Cowie. "These Belarusian and Icelandic examples represent just two of a series of MITM attack sequences that we've observed playing out in the last 12 months, launched from these and other countries around the world." MITM refers to "man-in-the-middle" attack.

Cowie said large global carriers, bank and credit card processing companies, and government agencies should be monitoring the global routing of their advertised IP prefixes. Not that this kind of warning is

entirely new. In 2008, two security researchers at the DefCon hacker conference demonstrated a security vulnerability where Internet traffic could be intercepted with the use of a tactic that exploits the Border Gateway Protocol. (Renesys, in explaining on its site what the BGP contributes to the life of the Internet, notes that the BGP routers' role "is to exchange routing information messages with one another so that they can properly direct traffic, hop by hop from one AS [Autonomous System] to another, until it reaches its final destination. Without such a global routing infrastructure, there simply would be no Internet as we know it.")

More information: www.csmonitor.com/World/Securi … n-long-strange-trips
www.renesys.com/2013/11/mitm-internet-hijacking/
www.renesys.com/bgp-routing/

Citation: Peculiar traffic routes suggest hijacking headaches (2013, December 8) retrieved 17 July 2024 from https://phys.org/news/2013-12-peculiar-traffic-routes-hijacking-headaches.html