Networking

How to crash the Internet

By Steven J. Vaughan-Nichols | February 13, 2011, 10:39am PST

We know you can take down Web sites with Distributed Denial of Service (DDoS) attacks. We know that a country, like Egypt, can knock down a country's entire Internet infrastructure. And, we thought we knew that you couldn't take down the entire Internet. It turns out we could be wrong.

In a report from New Scientist, Max Schuchard a computer science graduate student and his buddies claim they've found a way to launch DDoS attacks on Border Gateway Protocol (BGP) network routers that could crash the Internet.

BGP is an essential Internet protocol. It's the routing protocol used to exchange routing information across the Internet. Without it ISPs couldn't connect to each other and you couldn't connect Web sites and services outside of your local intranet. Because network connections and routers are constantly changing, BGP routers and switches are constantly working to keep current route maps of the Internet. In short, you don't want to mess it.

In an Association for Computing Machinery (ACM) paper, *Losing control of the Internet: using the data plane to attack the control plane*, Schuchard describes the theoretical assault as "the Coordinated Cross Plane Session Termination, or CXPST, attack, a distributed denial of service attack that attacks the control plane of the Internet. CXPST extends previous work that demonstrates a vulnerability in routers that allows an adversary to disconnect a pair of routers using only data plane traffic. By carefully choosing BGP sessions to terminate, CXPST generates a surge of BGP updates that are seen by nearly all core routers on the Internet. This surge of updates surpasses the computational capacity of affected routers, crippling their ability to make routing decisions"

Here's how it would work. The CXPST attack would use approximately 250,000 PCs in a botnet to launch the attack. Does that sound unreasonably large number of computers to you? It shouldn't. Thanks to Windows' built-in insecurity, its easy to create huge Windows botnets. We know for a fact that the Mariposa botnet alone was made up of 12.7-Million Windows PCs. The 250,000 PCs that a CXPST-style attack would require is *nothing* in botnet terms.

Once a CXPST botnet was set-up, it would use what Schuchard calls, ZMW, after its authors, Zhang, Mao and Wang. This trio of researchers described their attack in the paper: *A Low-Rate TCP-Targeted DoS Attack Disrupts Internet Routing* (PDF Link).

They found that "BGP routing sessions on the current commercial routers are susceptible to such low-rate attacks launched remotely, leading to session resets and delayed routing convergence, seriously impacting routing stability and network reachability." They also discovered that "low-rate TCP attacks can severely degrade TCP throughput by sending pulses of traffic leading to repeated TCP retransmission timeout." So far, this was just a new, but rather ordinary, DDoS technique.

The researchers also found though that "Aside from the potential impact is whether such attacks are powerful enough to reset BGP's routing session as a result of a sufficiently large number of consecutive packet drops. If the session is reset, it can have serious impact on the Internet in the form of routing in- stability, unreachable destinations, and traffic performance degradation." OK, now we were officially into "this is bad news" territory. Such an attack would be hard to spot and if could easily knock out a corporate, school, or even a national intranet.

Page 2: [Breaking the Internet] »

Steven J. Vaughan-Nichols, aka sjvn, has been writing about technology and the business of technology since CP/M-80 was the cutting edge, PC operating system

Disclosure

Steven J. Vaughan-Nichols is a freelance writer. He does not own stocks or other investments in any technology company.

Biography

Steven J. Vaughan-Nichols, aka sjvn, has been writing about technology and the business of technology since CP/M-80 was the cutting edge, PC operating system; 300bps was a fast Internet connection; WordStar was the state of the art word processor; and we liked it!

His work has been published in everything from highly technical publications (IEEE Computer, ACM NetWorker, Byte) to business publications (eWEEK, InformationWeek, ZDNet) to popular technology (Computer Shopper, PC Magazine, PC World) to the mainstream press (Washington Post, San Francisco Chronicle, BusinessWeek).