EOAS Help Desk

Mirai Botnet denial of service attack

2016-10-26 - Burner EOAS - 0 Comments - in Security

As you may be aware, there was a recent denial of service (DDoS) attack that targeted DNS services offered by DynDNS (dyn.com), which resulted in sites and services interrupted for large companies including Paypal, Netflix, and Airbnb. According to press information, the botnet behind the attack leveraged flaws in a brand of smart cameras and DVRs (arstechnica.com/information-technology/2016/10/inside-the-machine-uprising-how-cameras-dvrs-took-down-parts-of-the-internet/).

The code used to exploit the flaw is now in the public domain. UBC and other institutions and companies are experiencing an increase of malicious traffic. The malicious traffic is targeting the University's DNS servers and our networks are being scanned for insecure devices on port 23/TCP and 2323/TCP. In response, on **November 2, 2016**, the University will be blocking inbound traffic specific to ports 23 and 2323 for all UBC networks. Port 23/TCP is used by the application telnet (www.packetu.com/2012/04/17/whats-wrong-with-telnet/), and port 2323/TCP is designated as part of the 3d-nfsd protocol, however many vendors use that port as an alternative to port 23/TCP. I don't expect this change will impact anyone in our department. If you use telnet or port 2323/TCP to access services on campus from an off campus location, you will need to start using UBC's myVPN service.

If you are not sure how to use UBC's myVPN service, please contact helpdesk@eoas.ubc.ca or come drop-in to EOAS Main 113 and we can talk about what needs to be done.