Issued 4/12/17

A Malware Outbreak Is Bricking Insecure Internet Connected Devices

The Mirai botnet ripped through the Internet of Things last year, turning scores of improperly secured devices into a an electronic army capable of launching powerful DDoS attacks. Now there's a new malware strain targeting those devices, but its aim is not to enslave them. It wants to knock them offline for good.

This new malware is called BrickerBot, and it scours the Internet looking for a poorly-secured database of default usernames and passwords. If it finds one exposed and manages to log in, then it's game over. The device's connectivity is disrupted, its processing power limited, and finally its storage is scrambled and wiped, leaving it more or less useless.

Researchers refer to the kind of attacks it's carrying out as a PDoS, which stands for permanent denial of service. Experts aren't certain why BrickerBot does what it does just yet, but one theory is that it's the work of a vigilante. In order to stop the spread of Mirai and other Mirai-based malware, someone may have crafted BrickerBot to shut vulnerable devices down before they wind up infected and causing more disruption and chaos.

Cybersecurity company Radware recently observed nearly 2,000 PDoS attempts in a four-day span. They're seeing two separate BrickerBot strains at work right now. They could prove difficult to disrupt, too, because they're

using the TOR network to obfuscate their activity. It's really not that hard for owners of vulnerable devices to keep BrickerBot at bay, however. All they have to do is change default passwords and shut down external access to telnet and their wireless access points, security cameras, and high-tech toasters should be fine.