Electronic Design

WILLIAM WONG | Technology Editor

Beware BrickerBot, the IoT Killer

BrickerBot is designed to attack IoT devices, disabling or "bricking" them. It attacks devices that are open to attack due to poor configuration or design.

IoT security (or the lack thereof) seems to pop up in the news a lot these days. Our Embedded Revolution reader survey and whitepaper highlights what developers think about this topic (Fig. 1).

IoT devices and PCs are often compromised to employ these "bots" in a massive, distributed denial of service (DDoS) attack. Of course, a compromised device can also be used for other nefarious means. The problem is many fold from the starting point of a bad design to the inability users to take corrective measures, as vendors are often the only ones that can provide relief from these attacks.

Enter BrickerBot, which was exposed by the security firm Radware (see "BrickerBot Results In PDoS Attack"). BrickerBot is a form of malware that is designed to disable or "brick" an IoT device that it can compromise. Essentially a bricked device is about as useful as a real brick. Devices normally require replacement or more advanced update techniques like direct JTAG connections. This permanent denial-of-service (PDoS) is supposed to be "good" for the community since—in theory, and according to the author—it removes the device from the internet and prevents it from being used in a DDoS attack or for other unwanted purposes, from spying with cameras to capturing security information.

Of course, BrickerBot works like existing malware. It hides itself and uses distributed means to hide itself and its management servers. The author is unknown and any alternative use of the compromised devices is unknown, although they appear to be bricked.

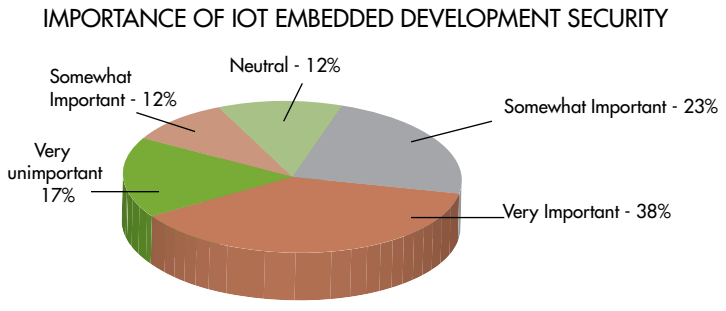
So, is this variant on Robin Hood, Zorro, or Batman? A vigilante who remains hidden, but does good?

In a sense, removing a device in this fashion may protect some from possible future attacks by another piece malware running on the device, or from having the device used for other means. Unfortunately, it would actually be very difficult to notify the owner of the device by means other than bricking it. Likewise, the owner of the device cannot know that it was bricked. The device will just stop working, usually to be replaced by another of the same type (and most likely with the same problems.

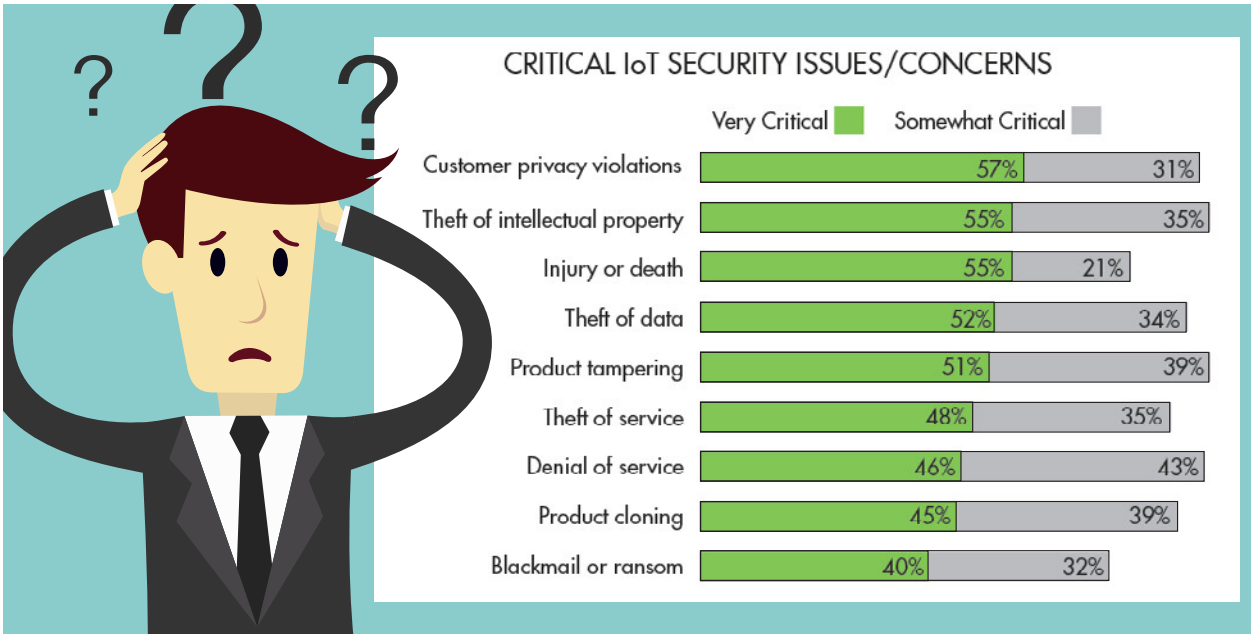
We in the embedded community may know what's going on, but the general public is unlikely to associate their disabled devices with a BrickerBot attack. Of course, they wouldn't know if their device was compromised by another piece of malware.

Attacking a device is against the law. So is trespassing in a building to lock the front door. On the other hand, this type of attack would be more like filling a building with concrete to prevent it from being used.

There is also the issue of what such an attack is actually doing. From one side, it is just preventing others from compromising the device by making it unusable. That is only annoying for something like a wireless speaker or smart lightbulb, but it could be devastating for a security system that all of a sudden loses all its cameras. I won't even get into medical or other safety-related devices. In theory, these attacks will be looking at what kinds of devices they are bricking but that only holds if the device is easily identifiable, or if the programmer actually takes the time to discern the device and its importance. The likelihood of severe consequences like death are low at this point, but



1. Security is important to the majority of IoT developers, but this chart still shows a significant lack of concern for security.



2. Those that are concerned about security are placing safety and privacy concerns at the top of their list. Protecting intellectual property and the products themselves is key, as well.

grow as the number of IoT devices and their uses increase.

This malware does bring up the issue of controlling IoT devices, and whether they should be required to have alternate means of updates. Most are locked down by the vendor, but there is no requirement to support updates. Most rarely provide them past a short device half-life. Some never provide updates even though they are possible.

PDOS is only another in a string of attacks on an ever-growing attack surface of IoT devices. Those movie scenarios where the villain takes over a city grid will look just as bad if a PDOS attack shuts down all the stoplights.