OVERCOMING BOTNETS, ZOMBIES AND IOT SECURITY BREACHES

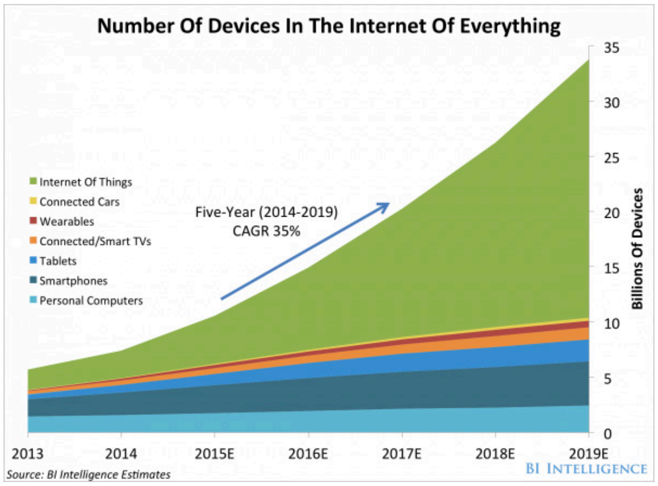
Deep Thoughts by Deepinder Singh: Part 5

A series on the future of cloud computing, big data and buildings

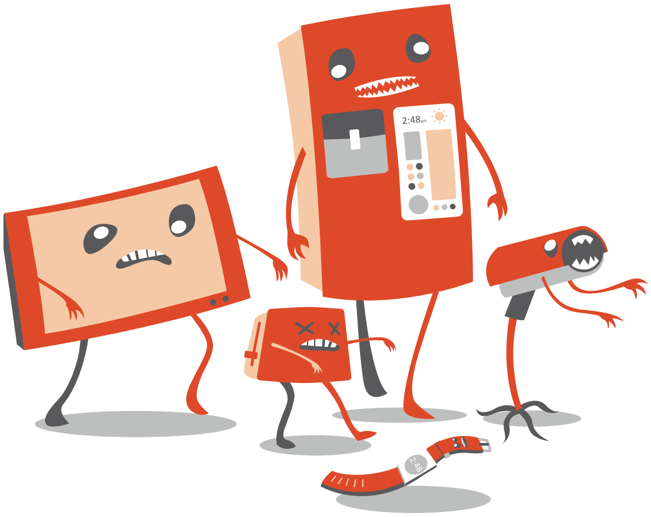
OVERCOMING SECURITY BREACHES

In an era of growing botnets, zombies and security breaches, IoT systems in particular, need to keep safety a top priority at all times. A bot (short for robot), is a script or software application that performs tasks on command. Evil bots complete malicious tasks and install intrusive software including computer viruses, trojan horses, spyware, adware and other malevolent programs. This invasive software allows attackers to take remote control over any infected computer that's connected to the internet. Known also as web robots, bots are usually part of a network of infected machines, known as a botnet. Botnets are often created from victim machines that stretch across the globe, unbeknownst to the owners and can be used to spread spam and perpetuate scams. The infected machines are also referred to as zombies.

IoT is the next revolution in the explosion of devices everywhere and hackers are turning to IoT devices to grow their botnet armies. In this ubiquitous presence lies the opportunity to subvert them to be a part of a botnet. Gartner estimates there will be 6.4 billion IoT devices connected to the internet in 2016 and that number is expected to reach an impressive 21 billion by just 2020. The sheer number of devices in existence makes fertile ground for skillful hackers.



Source: ironpaper.com/webintel/articles/internet-things-market-statistics-2015



IoT devices are vulnerable to IoT viruses because most don't have a UI (user interface). This means that to configure an IoT device requires some sort of access over the network via a web interface or app using TCP/UDP sockets. The issue is that access methodology needs to be common across each device. So even if the device is protected with a password, it is the same default across all devices. Consumers are jaded from having to remember their regular passwords, from banking to online grocery shopping. Therefore, it's easy to leave the password set to the default, meaning that simple brute force for well-known default passwords gives an attacker easy access.

The very fact that IoT devices don't have a UI means we don't regularly interact with them, making it easy to ignore their presence. Once set up, we tend to forget that these devices are connected to the internet, leaving them vulnerable to attack.

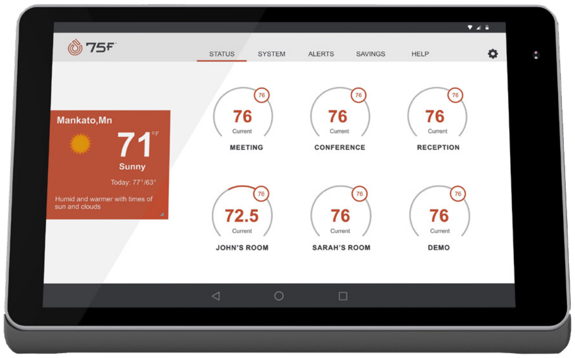
By design, IoT devices have limited computational capabilities and no concept of firewalls or diagnostic tools. The cumbersome access methods, like using a web browser or app to specifically log into each device makes it unlikely that anyone will use them. When was the last time somebody logged into their light bulbs to do a tcpdump to check if there were rogue packets?

One key mistake manufacturers are making is they're pushing their devices to connect directly to the internet over Wi-Fi. The right thing to do would be to use a simpler protocol like ZigBee within the premise and then have an aggregated feed through a secure gateway. The gateway could have more compute resources and hence a greater chance of running tools that would secure it. For that to happen however, the IoT model must mature. Equally as importantly, the industry needs to unite around standards. Right now, every manufacturer from Amazon and Wink to Nest think they hold the golden key to gateway standards and yet no one truly does.

The other issue is that we have been lulled into accepting automatic remote updates to devices over the air. At the heart of this, manufacturers want to ship out product before its fully featured and thoroughly tested. This is partially because as consumers, we welcome upgrades because of the exciting new features they bring. From a hacker's perspective, however, this quick to market product ignites a wealth of opportunity, since the underlying framework to push malicious updates comes built in with each device. The cross checks to prevent this (if any), are rudimentary and easily overcome for these simple devices.

PREVENTING IOT BOTNETS

Dealing with the rising threat of IoT botnets is not only important, but doable. As Smokey the bear says, "Care will prevent 9 out of 10 fires." If you're connecting a device to the internet, change the default password! Even if you must write it down and stick it to the device itself, don't overlook this crucial step. Now if people are coming into your house to steal your refrigerator's password for ordering groceries, you have other things to worry about. Get behind a good firewalling router and turn the firewall function on. Unsurprisingly, the firewall works much better when it's enabled.



Touch screen interface allows for direct access to our devices, removing the need for risky open TCP ports.

75F specifically adheres to the model of having a secure gateway that protects all on premises devices. Ours is based on a hardened version of android. From a software standpoint, we make a strong distinction between having a kernel that is not remotely upgradeable and an application that is limited to only the permissions it needs to function. We chose to provide an actual user experience (UX) on our devices for configuration (touch screen on our gateway and buttons/LCD on room modules), so there are no open TCP ports. We also enforce the creation of a distinct account password as part of our setup process for all remote access.

Our end devices (wireless room modules and smart dampers) communicate back to the gateway over a hardware encrypted mesh network.

A hardware encrypted mesh network allows our devices to communicate as securely as possible.

These devices are thoroughly field tested and for our production deployments we don't allow firmware updates over the internet. Having spent the time to understand client requirements upfront and having them well sorted out in the beginning, means we don't have to add device features necessitating firmware updates. Another key component is that we are reporting any unidentified packets back to our cloud hosted servers. There, they are analyzed by our central alarming infrastructure, which promotes identification.

The key to killing off IoT botnets lies in the very things that make them vulnerable. Their limited compute power may make it difficult to put tools to firewall. But it also means that an attacker with a compromised device has fewer resources to mount a Distributed Denial of Service (DDOS) attack. So IoT botnets are really only useful if there are literally thousands of compromised devices as part of a coordinated attack. To make it worth their while, attackers must get more compute or network leverage from the IoT device than the effort of hacking it. Doing simple things like changing the default password might make it unappealing enough to a potential hacker.

In short, take the time to change default passwords, invest in a strong firewalling router and ensure the firewall function is enabled. When it comes to IoT devices, do your research. Until the Internet of Things industry unites to create uniform standards, it will ultimately be up to the consumer to ensure their devices are safe and secure. Lastly, be conscious about your devices connecting directly to the internet over Wi-Fi. That can lead to a hacker's paradise and a consumer's nightmare, complete with botnets and zombies.

ABOUT THE AUTHOR

Deepinder Singh founded 75F in 2012 after he designed some of the world's fastest core networks for Tier 1 service providers like AT&T, NTT and Verizon. With almost 25 years experience in electronics and computing, he's brought a wealth of embedded products to the market. His key goal in every endeavor is to simplify operational complexity and make products intuitive.

That's why he created 75F, an intelligent building solution that utilizes the Internet of Things and the latest in cloud computing to create systems that predict, monitor and manage the needs of light commercial buildings.