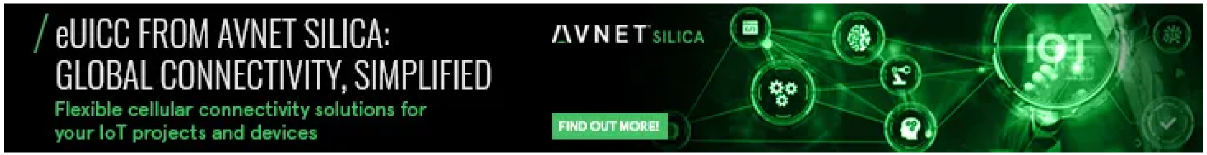


When Refrigerators Attack – How Cyber Criminals Infect Appliances, and How Manufacturers Can Stop Them

An article by Alan Grau, VP of IoT, Embedded Solutions, Sectigo.

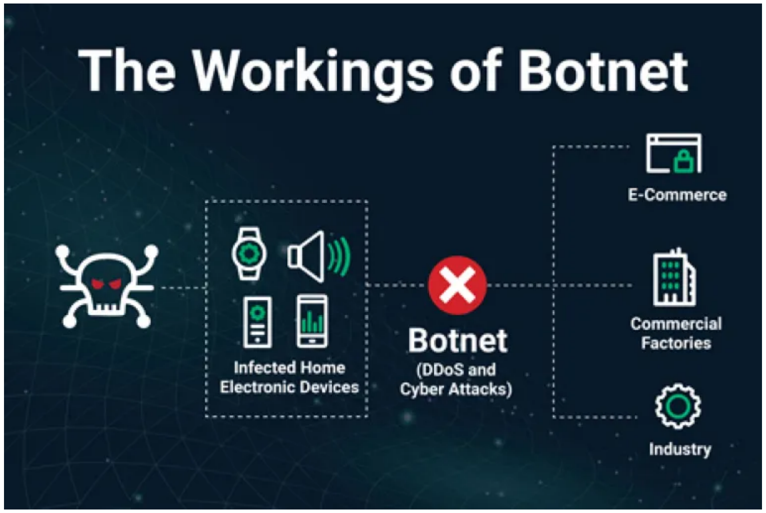
Homes and businesses worldwide are vulnerable to attacks from cyber thieves and other bad actors – and not just through their computer networks. The embedded electronics inside appliances present an easy path of entry.

It's already been happening. According to Business Insider and Proofpoint, one of the first refrigerator incidents occurred in late 2013 when a refrigerator-based botnet was used to attack businesses.

Some of these attacks, such as infecting appliances with botnet malware, don't really have much effect upon a family's security and safety. In fact, if a "smart" refrigerator gets infected by a bot, the homeowner might not even notice anything wrong.

However, connected-appliance based cyberattacks are not limited to just refrigerators – and they are rarely one-off incidents. Almost any type of appliance can be hacked and used to host a botnet that could attack the web. According to Wired Magazine (https://www.wired.com/story/water-heaters-power-grid-hack-blackout/), a botnet of compromised water heaters, space heaters, air conditioners and other big power consuming home appliances, could suddenly turn on simultaneously, creating an immense power draw that could cripple the country's power grid.

A bot, quite simply, is an infected computer. Many cyberattacks, like the Mirai Malware and the Dyn attacks, infect a network of computers, including "smart" connected devices such as home appliances, security cameras, baby monitors, air conditioning/heating controls, televisions, etc., and turn them all into compromised servers. These compromised servers then act as nodes in an attack and together create a botnet. They can participate in a variety of coordinated attacks, infecting other devices and expanding the network of bots, or participating in Denial of Service attacks.



A bad actor or cyber criminal can send infected messages to a home or business network that targets various appliances or machines. Once infected, that machine is under the control of the bad actor and can be used to send out thousands of infected messages to new targets worldwide. The botnets can also send out millions of dummy messages to a single target – overwhelming it and putting it out of service.

Without any apparent symptoms or notice, a criminally enhanced refrigerator could be generating and sending out thousands of attacks every minute. In addition to the homeowner or business manager never realizing what is going on, these attacks may be unstoppable until unless the machine itself is disconnected from its web connection.

Additionally, the infected refrigerator could spread malware from the kitchen to the home's "smart" TVs, to the home's computer networks, to other smart devices in the home, and even to connected smart phones. Every target could be transformed into malicious bots that distribute millions of infected spam messages and cyber-attacks.

So how do we combat this threat?

Unfortunately, end users really have no power to fix this problem. There is probably no way for a homeowner, office manager – or even an experienced refrigerator repair person – to talk to a refrigerator's electronics. No way to get into the appliance's software and middleware to identify and kill an infection. However, if the homeowner suspects an infection, they could disconnect the refrigerator from the its internet connection to make it "dumb" again.

It is up to device manufacturers to protect against these attacks.

So how do manufacturers combat this type of attack? How can they ensure that appliances in homes and offices do not get infected to cause mayhem?

Security starts in the design process for the refrigerator itself, as well as for the appliances' various electronic components and control surfaces. Most appliance manufacturers get their control sub-assemblies from a wide network of smaller manufacturers, sometimes with a worldwide supply chain. These suppliers need to make sure that the chips and sub-assemblies they use are secure from hacks.

Two important security practices can be utilized by appliance makers:

- **Embedded Firewall** with blacklist and whitelist support – Protect appliances and edge devices from attacks by building firewall technology directly into the appliance. An embedded firewall can review incoming messages from the web or over the home network and, via a built in, and regularly updated blacklist, reject any that are not previously approved.

- **Secure Remote Updates and Alerts** – Validate that the firmware inside the device is authenticated and unmodified before permitting installation of any new firmware updates. Updates ensure the incoming software components have not been modified and are authenticated software downloads modules from the appliance manufacturer.

Most consumer and device manufacturers have heard about the potential for attacks on smart devices like door locks, baby monitors, and home thermostats, but this risk awareness needs to expand to types of connected systems – including appliances. An infected refrigerator sending out malware is not just a funny story. These systems have been attacked and used to spread malware. Ensuring the security of these devices is necessary to protect home network, slow the spread of malware and even protect credit card numbers or other personal data stored in smart home devices.

FREE E-NEWS
(https://iotbusinessnews.com/newsletter-signup/)

ADVERTISE
(https://iotbusinessnews.com/advertise/)

IOT NEWS BY CATEGORY

GENERAL IOT NEWS (HTTPS://IOTBUSINESSNEWS.COM/CAT
NEWS/)

IOT MARKET (HTTPS://IOTBUSINESSNEWS.COM/CAT
DATA/)

IOT SOLUTIONS & INNOVATIONS (HTTPS://IOTBUSINESSNEWS.COM/CAT
INNOVATION/)

INDUSTRIAL IOT – IIOT (HTTPS://IOTBUSINESSNEWS.COM/CAT
IOT/)

MONITORING & TRACKING (HTTPS://IOTBUSINESSNEWS.COM/CAT
CONTROL-MONITORING/)

SMART CITIES & SMART HOMES (HTTPS://IOTBUSINESSNEWS.COM/CAT
METERING-SMART-GRID/)

AUTO & TELEMATICS (HTTPS://IOTBUSINESSNEWS.COM/CAT
TELEMATICS/)

FLEET MANAGEMENT (HTTPS://IOTBUSINESSNEWS.COM/CAT
FLEET-MANAGEMENT/)

IOT INSIGHTS

IOT EXPERT OPINIONS (HTTPS://IOTBUSINESSNEWS.COM/CAT
INSIGHTS/)

IOT CALENDAR

BEST IOT EVENTS (HTTPS://IOTBUSINESSNEWS.COM/IOT-
EVENTS/)

RESOURCES

IOT WHITE PAPERS (HTTPS://IOTBUSINESSNEWS.COM/WH
PAPERS/)

IOT BUSINESS NEWS

ABOUT IOT BUSINESS NEWS.COM (HTTPS://IOTBUSINESSNEWS.COM/ABO

TERMS & CONDITIONS (HTTPS://IOTBUSINESSNEWS.COM/SAL

TE

PR

(H

PO

CO

(H

EN

(H

SIGNUP/)

ADVERTISE (HTTPS://IOTBUSINESSNEWS.COM/ADV

CONTACT US (HTTPS://IOTBUSINESSNEWS.COM/CO