The Internet of Things Is a Cyber War Nightmare

But we can still prevent our household appliances from becoming an army of malicious computer zombies out to destroy the web.

BY JAMES STAVRIDIS, DAVE WEINSTEIN  NOVEMBER 3, 2016

The world got a glimpse of the future last month when a large-scale cyberattack prevented access to hundreds of key websites, including Twitter, the online New York Times, and Amazon. The “distributed denial of service” attack against the New Hampshire-based DNS provider Dyn, which blocked access to major online services for users as far away as Europe, fulfilled the direst predictions of technologists and security researchers alike.

The attack exposed the clear reasons for concern about the coming age of an Internet of Things, in which more household devices are connected to the web. What’s less immediately clear is what should be done to ensure the internet’s most likely future iteration remains safe.

Trending Articles

Mon Dieu, François Hollande’s Approval Rating Is at 4...
Ç’est mal. The French people are very displeased with their president.
To date, the vast majority of disruptive and even destructive cyberattacks have been the work of militaries, foreign intelligence services, or other state-sponsored hackers. These actors are usually operating under some degree of political direction and interests and tend to moderate their use of malicious code for disruptive or destructive purposes.

But according to America’s top intelligence official, Director of National Intelligence James Clapper, last month’s attack was “likely” the work of a nonstate actor, and his assessment has been backed up by reports from the private cybersecurity firm Flashpoint. This marks an important shift. The barriers to entry are becoming low enough that hackers no longer need the backing of a government to carry out crimes or even acts of warfare in cyberspace. These nonstate actors are especially destabilizing because they are not subject to traditional means of diplomacy or law enforcement. They operate beyond legal jurisdictions and without regard for geographic political boundaries, so the instruments of deterrence that have largely kept nation-states from projecting disruptive or destructive cyberforce are increasingly obsolete.

The first factor driving these low barriers to entry is the internet’s rapidly expanding digital real estate, which nonstate hackers view as their battlefield. The rapidly expanding Internet of Things consists of normal household devices like surveillance cameras, thermostats, baby monitors, televisions, and refrigerators to which an IP address has been affixed and that can communicate with one another and other devices. It is already massive and is expected to more than triple in size by 2020 to nearly 21 billion devices. For a cyber-defender, this means that hackers will not only have three times as many targets — they will also have three times as many vectors from which to attack any given target. This creates vast new challenges for network security and complicates the already murky legal and technical landscape for attributing who is responsible for an attack.

The second factor bolstering this threat is the ubiquity of the tools used to conduct such attacks. The Mirai malware that was used last month to compromise 50,000 internet-connected devices is a powerful new threat. Botnets, or armies of zombie computers infected with malware, are not a new phenomenon; what is new, however, is the act of transforming the Internet of Things into a distributed zombie network — an Internet of Botnets. But the source code for Mirai is not secured in a government vault, but rather shared in forums on deep, dark corners of the web for sympathetic, force-multiplying hackers to copy and deploy with the stroke of a key.
Finally, last month’s attack demonstrated our need for a more redundant internet. Dyn, which is akin to a large digital phonebook, is one of many companies that connect a web address typed in a browser to a website’s IP address. By flooding its servers in New Hampshire with dummy traffic from random devices, amateurs effectively shut down popular online services like Twitter and Netflix for millions of their customers. Ultimately, the effects of that attack were quite limited. The effects, however, of a similar style attack directed against more critical services during a local, regional, or national emergency could be catastrophic.

Such hypotheticals are entirely reasonable to contemplate. They will also undoubtedly encourage a chorus of criticism about the viability of the Internet of Things. Technology skeptics will ask, “Why does my refrigerator need an internet connection?” But that’s the wrong question. There are too many benefits to linking our world together to slow that process down. The real question is: How can we prevent such attacks?

First, we need to require higher levels of security in any device that will be connected to the web. Some of this will be done because manufacturers are self-incentivized to do so. For example, last week, Chinese camera manufacturer Hangzhou Xiongmai was quick to recall millions of its products sold in the United States that were vulnerable to the Mirai malware. More will follow voluntarily to avoid legal liability in the event of an attack.

Second, we need better technology to manage in real time the vulnerability of Internet of Things devices. Just as technology vendors (or at least the more reliable ones) deploy software patches when a bug is discovered, Internet of Things manufacturers should include device-based auto-updates as a standard security measure in their new products. And there are plenty of other viable low-cost solutions for these devices — after all, we’re not talking about nuclear weapons. An entire secondary cybersecurity market to protect relatively simple devices attached to the Internet of Things is already gaining speed.

And third, we all have to recognize that we have a broad responsibility to protect the internet as consumers of it. While it’s easy to place blame on device manufacturers, in the end, perhaps the more appropriate culprit is the user. Think about how we fully embrace our responsibilities to prevent the spread of the flu: We take shots, wash our hands, cover our mouths when we cough, and stay home and self-isolate when we are sick (at least most of us do). That same mentality must be inculcated in the public when it comes to the web. When we attach a device to the internet, we need to change the password, allow security updates, and monitor for trouble. Technology can help, but in the end we own the internet — all of us — and it’s our job to keep it safe and secure.
In October, the United States observed National Cybersecurity Awareness Month. How appropriate that the largest single attack on the internet came rolling through it like a line of squalls. It neatly demonstrated the basic facts of our present cybersecurity state: Everything is hackable, and in the digital age of nonstate threats, cybersecurity is a collective responsibility. Now we need to heed those facts.

Photo credit: MICHAEL BOCCHIERI/Getty Images

YOU MAY LIKE

THESE INVISIBLE HEARING AIDS ARE SECRETLY SWEEPING PHOENIX
HEAR.COM

30 EPIC BRIDES YOU CAN'T MISS
VIRALWALRUS

28 LADIES WHO ARE DOING YOGA RIGHT
BUZZBEAGLE

YOU'RE IN FOR A BIG SURPRISE IN 2016 IF YOU OWN A HOME IN ARIZONA
COMPARISONS.ORG QUOTES

MORE FROM FOREIGN POLICY

THIS MAP SHOWS CHINA'S HILARIOUS STEREOTYPES OF EUROPE

5 THINGS THE PENTAGON ISN'T TELLING US ABOUT THE CHINESE MILITARY
WHAT RUSSIA COULD LOOK LIKE IN 2035, IF PUTIN GETS HIS WISH

THE DANGERS OF READING FOREIGN POLICY?: ARMY TOSSES INFANTRY BDE COMMANDER

THE WORLD'S OLDEST WORDS?

IRAN: DEATH TO PORNOPGRAPHERS