TECH INTERNET

How Web Cams Helped Bring Down the Internet, Briefly

7 MINUTE READ

Getty Images

BY HALEY SWEETLAND EDWARDS

OCTOBER 25, 2016 3:07 PM EDT

In a world where we increasingly live and work in giant webs of internet connectivity—our computers and phones, not to mention cameras, thermostats, garage door openers, kitchen appliances and baby monitors are all now connected to the web, often by default—we find ourselves facing an uncomfortable new reality: How secure is the so-called Internet-of-Things?

That question is front and center in the wake of a massive cyber attack Oct. 21 that left millions of internet users unable to access roughly 1,200 websites, including Twitter, Reddit and Netflix for the better part of a day.

While the attack did cause some economic damage, cybersecurity experts say the bigger issue is the way in which the hackers were able to pull off such a feat. They did it not only by co-opting zombie computers—the typical way that hackers push servers off-line—but by leveraging "tens of millions" of addresses on insecure, internet-connected devices that had been infected with malicious software code, according to Kyle York, the chief strategy officer at Dynamic Network Services Inc., the company that came under attack.

"The obvious point that we learned from last week's attack is that the Internet of Things has made the threat of a denial-of-service attack more potent than

ever before," Timothy Edgar, a director of law and policy at Brown University's cybersecurity program, told TIME.

Here's how it worked.

On Friday morning, hackers launched a massive distributed denial-of-service, or DDOS, attack on a domain-name system called Dynamic Network Services Inc., or Dyn., which serves a crucial role in the Internet infrastructure. A domain name system translates what you type into a URL—"Twitter.com," say—into the appropriate, numerical IP address and directs you to where you want to go.

In a typical DDOS attack, hackers take over virus-infected computers, known collectively as a "botnet," and command them to send large numbers of requests, or "garbage packets," to a server with the intention of overwhelming it—making it impossible for legitimate users to access it as needed.

What made the attack on Friday exceptional, and exceptionally scary for cyber researchers, is that the hackers used not only virus-infected computers, but hundreds of tens or hundreds of internet-connected devices—namely, certain types of security cameras and DVR players—that we don't really think of as "computers" in the first place. XiongMai Technologies, a Chinese company that manufactures some of the webcams used in the attack, announced Monday that it would recall some of its products.

But such recalls aren't going to do much at a time when literally millions of new, internet-connected devices are being connected every day, Edgar said. "There are millions and millions of cameras out there on the shelves and in people's homes and there's no security on them," he said. "Going back and making sure that each of these cameras have better security isn't really possible—it's a depressing thought."

According to a 2015 report by the information technology research company Gartner, there are now roughly 6.4 billion internet-connected things worldwide, from smart watches to smart refrigerators to smart web cams. By 2020, Gartner expects that number to bounce to 20.8 billion. That means that

even if a relatively small portion of those devices are infected with malware and commandeered in a DDOS attack like the one Friday, hackers could an extraordinary amount of damage either the U.S. economy or, potentially, to national security.

"This particular attack disrupted key services that are a part of people's daily lives, but no lives were lost," Chris Petersen, a co-founder of the security analytics firm LogRhythm, told TIME. But, he added, it's not hard to imagine a scenario in which hackers utilized this same army of devices to disrupt other key services, like hospitals or physical infrastructure projects. "This attack just proves that an attack of this nature could be easily realized," he said.

Just two weeks before Election Day, cybersecurity experts have, for example, raised the specter that hackers, possible operating on behalf of a nation state, like Russia or China, could plan a similar attack to compromise state and county election websites, which voters rely on to access information about their registration or where their polling places are. Since no voting machines in the U.S. are connected to the internet, it would be extremely difficult for hackers to undermine the actual act of voting, but they could fairly easily succeed in creating the impression that the election had been compromised in some way.

"The possibility of hacking the vote-counting process is quite difficult," said Edgar. "But the goal is causing chaos on Election Day? That's pretty simple."

A large part of the problem is that internet-connected device makers currently do almost nothing to protect their products from cybersecurity threats, Mike Raggo, the chief research officer at the security firm ZeroFOX, which focuses on social media platforms, told TIME. "Manufacturers want you to be able to plug it in and it's ready to go," he said. "So most of these devices have a default password, default configuration, default login." That makes it easy to plug-and-play, but it also makes these devices very vulnerable to attack.

According to Network World, the hackers on Friday used only about 10 to 20% of all the 500,000 or so devices known to be infected with a particular malicious code, known as Mirai, which means that the DDOS attack could easily have

been five to ten times larger than what it actually was. “There’s a lot of dry gunpowder left in terms of compromised IoT devices,” Petersen warned.

Consumers can protect themselves to some degree by keeping the software on their devices up to date, changing the default password if its possible, or—for the more sophisticated consumer—hardening up other parts of a home network, said Scott Radcliffe, a former military officer and vice president at FleishmanHillard, where he works on cybersecurity issues. “But it’s a problem of getting the message out. It’s just not intuitive that we have to worry about security on all of these new things.”

On Monday, Homeland Security Secretary Jeh Johnson told Politico that his department is working with law enforcement officials and the private sector to produce a strategic plan “in the coming weeks” to guard against similar attacks in the future.

There are currently no state or federal regulations in the U.S. that require even basic cybersecurity protocols on internet-connected devices and appliances. It’s a scenario that creates a vacuum of responsibility, Edgar said.

“You can say, let’s hold manufacturers liable for damaged caused by insecure IoT devices, but how would you do that?” he said, explaining that DDOS attacks can involve hundreds of thousands or millions of devices made by dozens of different manufacturers. “If you’re looking at it from the point of the view of a law firm, how do you define the damage, find plaintiffs and defendants?”

Edgar and others suggest that perhaps the time has come for the government to step in. “There’s a big fear in the high tech community that government regulation is going to kill the goose that laid the golden egg by telling tech companies how to make their devices,” he said, but added that regulations can establish security benchmarks without being prescriptive.

“Look, I’m an entrepreneur,” said Petersen. “I am certainly not someone who wants to see more regulation from a business standpoint. But when I put on my cybersecurity hat and I look at the realities of what is going to protect our

nation from devastating cyber security attacks, I don't see much of an alternative except to regulate."

MORE MUST-READS FROM TIME

- **Cybersecurity Experts** Are Sounding the Alarm on DOGE
- Meet the **2025 Women of the Year**
- The Harsh Truth About **Disability Inclusion**
- Why Do More **Young Adults Have Cancer?**
- **Colman Domingo** Leads With Radical Love
- How to Get Better at **Doing Things Alone**
- **Michelle Zauner** Stares Down the Darkness

WRITE TO HALEY SWEETLAND EDWARDS AT HALEY.EDWARDS@TIME.COM