The New York Times https://www.nytimes.com/2016/10/23/us/politics/a-new-era-of-internet-attacks-powered-by-everyday-devices.html

A New Era of Internet Attacks Powered by Everyday Devices

By David E. Sanger and Nicole Perlroth
Oct. 22, 2016

WASHINGTON — When surveillance cameras began popping up in the 1970s and ’80s, they were welcomed as a crime-fighting tool, then as a way to monitor traffic congestion, factory floors and even baby cribs. Later, they were adopted for darker purposes, as authoritarian governments like China’s used them to prevent challenges to power by keeping tabs on protesters and dissidents.

But now those cameras — and many other devices that today are connected to the internet — have been commandeered for an entirely different purpose: as a weapon of mass disruption. The internet slowdown that swept the East Coast on Friday, when many Americans were already jittery about the possibility that hackers could interfere with election systems, offered a glimpse of a new era of vulnerabilities confronting a highly connected society.

The attack on the infrastructure of the internet, which made it all but impossible at times to check Twitter feeds or headlines, was a remarkable reminder about how billions of ordinary web-connected devices — many of them highly insecure — can be turned to vicious purposes. And the threats will continue long after Election Day for a nation that increasingly keeps its data in the cloud and has oftentimes kept its head in the sand.

Remnants of the attack continued to slow some sites on Saturday, though the biggest troubles had abated. Still, to the tech community, Friday’s events were as inevitable as an earthquake along the San Andreas fault. A new kind of malicious software exploits a long-known vulnerability in those cameras and other cheap devices that are now joining up to what has become known as the internet of things.

The advantage of putting every device on the internet is obvious. It means your refrigerator can order you milk when you are running low, and the printer on your home network can tell a retailer that you need more ink. Security cameras can alert your cellphone when someone is walking up the driveway, whether it is a delivery worker or a burglar. When Google and the Detroit automakers get their driverless cars on the road, the internet of things will become your chauffeur.

But hundreds of thousands, and maybe millions, of those security cameras and other devices have been infected with a fairly simple program that guessed at their factory-set passwords — often “admin” or “12345” or even, yes, “password” — and, once inside, turned them into an army of simple robots. Each one was commanded, at a coordinated time, to bombard a small company in Manchester, N.H., called Dyn DNS with messages that overloaded its circuits.

Few have heard of Dyn, but it essentially acts as one of the internet’s giant switchboards. Bring it to a halt, and the problems spread instantly. It did not take long to reduce Twitter, Reddit and Airbnb — as well as the news feeds of The New York Times — to a crawl.

The culprit is unclear, and it may take days or weeks to detect it. In the end, though, the answer probably does not mean much anyway.

The vulnerability the country woke up to on Friday morning can be easily exploited by a nation-state such as Russia, which the Obama administration has blamed for hacking into the Democratic National Committee and the accounts of Hillary Clinton's campaign officials. It could also be exploited by a criminal group, which was the focus of much of the guesswork about Friday's attack, or even by teenagers. The opportunities for copycats are endless.

The starkest warning came in mid-September from Bruce Schneier, an internet security expert, who posted a brief essay titled "Someone Is Learning How to Take Down the Internet." The technique was hardly news: Entities like the North Korean government and extortionists have long used "distributed denial-of-service" attacks to direct a flood of data at sites they do not like.

"If the attacker has a bigger fire hose of data than the defender has," he wrote, "the attacker wins."

But in recent times, hackers have been exploring the vulnerabilities of the companies that make up the backbone of the internet — just as states recently saw examinations of the systems that hold their voter registration rolls. Attacks on the companies escalated, Mr. Schneier wrote, "as if the attack were looking for the exact point of failure." Think of the mighty Maginot Line, tested again and again by the German Army in 1940, until it found the weak point and rolled into Paris.

The difference with the internet is that it is not clear in the United States who is supposed to be protecting it. The network does not belong to the government — or really to anyone. Instead, every organization is responsible for defending its own little piece. Banks, retailers and social media hubs are supposed to invest in protecting their websites, but that does not help much if the connections among them are severed.

The Department of Homeland Security is supposed to provide the baseline of internet defense for the United States, but it is constantly playing catch-up. In recent weeks, it deployed teams to the states to help them find and patch vulnerabilities in their voter registration systems and their networks for reporting results.

What to Know About Ransomware Attacks

What are ransomware attacks? This form of cybercrime involves hackers breaking into computer networks and locking digital information until the victim pays for its release. Recent high-profile attacks have cast a spotlight on this rapidly expanding criminal industry, which is based primarily in Russia.

The F.B.I. investigates breaches, but that takes time — and, in the meantime, people want to bank online and stream television shows. On Nov. 8, Americans will have to look up where they are supposed to vote, and, in a few cases, they will cast their votes on the internet. Yet the voting system is not considered part of the nation's "critical infrastructure."

The head of the National Security Agency, Adm. Michael Rogers, said recently that experts were looking at the problem the wrong way. "We are over-focused on places and things," he said in a talk at Harvard. "We need to focus on the data," and how it flows — or doesn't flow.

That is where the internet of things comes in. Most of the devices have been hooked up to the web over the past few years with little concern for security. Cheap parts, some coming from Chinese suppliers, have weak or no password protections, and it is not obvious how to change those passwords.

And the problem is quickly expanding: Cisco estimates that the number of such devices could reach 50 billion by 2020, from 15 billion today. Intel puts the number at roughly 200 billion devices in the same time frame. (Assuming the global population is around 7.7 billion people in 2020, that would be about six to 26 devices per person.)

Security researchers have been warning of this problem for years, but that caution has largely been written off as hype or fear-mongering. Then Brian Krebs, who runs a popular site on internet security, was struck by a significant attack a few weeks ago. The company protecting him, Akamai, gave up. The malware behind the attack, called Mirai, had a built-in dictionary of common passwords and used them to hijack devices to become attackers.

Chester Wisniewski, a principal computer research scientist at Sophos, a security company, said that attacks like the one on Dyn "might be the beginning of a new era of internet attacks conducted via 'smart' things."

"There are tens of millions more insecure 'smart' things that could cause incredible disruptions, if harnessed," Mr. Wisniewski added in an email.

It is possible, investigators say, that the attack on Dyn was conducted by a criminal group that wanted to extort the company. Or it could have been done by "hacktivists." Or a foreign power that wanted to remind the United States of its vulnerability. The answer may not come by Election Day, but the next wave of attacks very well could.