iNSS The Institute for National Security Studies
Strategic, Innovative, Policy-Oriented Research

INSS Insight No. 867, November 7, 2016

The Threat of Connected Devices to the Internet

Gabi Siboni and Tal Koren

At least three consecutive waves of complex online attacks were directed at Domain Name System (DNS) servers operated by Dyn, a US internet infrastructure provider. The attack on October 21, 2016 consisted of a Distributed Denial of Service (DDoS) attack, and blocked access to thousands of websites, including Netflix, Amazon, Twitter, Airbnb, the *New York Times*, PayPal, and more. Immediately, suspicions centered on Russia and China as having both the motivation and the ability to plan and execute such an attack. Yet as of this writing, it is not at all clear if the attack was state-motivated. After the attack, it was reported that the Chinese and Russian hacker group known as New World Hackers assumed responsibility and claimed it was a sophisticated attack using botnets at higher-speed traffic than ever know before – 1.2 terabytes per second (Tbps).

The attack exploited vast numbers of connected devices (in an announcement to the media, Dyn stated that some 100,000 devices were involved). These devices, also known as the Internet of Things (IoT), include webcams, alarm systems, baby monitors, internet-based security cameras, DVRs, printers, and routers – all connected to the internet. The attackers managed to plant a software component in these devices that could receive commands from a control server so that the masses of devices all sought out the target in a synchronized manner and paralyzed the attacked servers' ability to function by flooding it with traffic. The vast majority of these devices lack any kind of significant defenses; access to most of the systems is ensured through default usernames and passwords installed by the manufacturer. In fact, there is no current effective concept to respond to this type of threat.

The threat inherent in the swarm of connected devices is not new. As early as 2013, Symantec reported the existence of a worm called Linux.Darlloz that according to estimates, infected some 50,000 IoT connected devices, such as routers and Set Top Box devices or computers based on Intel's X86 architecture. The goal was to install software allowing attackers to mine crypto currencies. In 2015, Symantec issued a detailed report about simplifications that make it possible to break into 50 different kinds of smart home devices. In its April 2016 report, the company

Dr. Gabi Siboni is a senior research fellow and head of the Cyber Security Program at INSS.
Dr. Tal Koren is a researcher in the Cyber Security Program at INSS.

stated that medical devices (such as insulin pumps, X-ray systems, and CT scanners) are also exposed to attack, as well as smart TV systems and dozens of other devices of all types.

Even though the ability to penetrate these devices and carry out extensive DDoS attacks through them was not surprising, the intensity of the attacks demonstrated the destructive capability of using a large number of synchronized simple devices. The attack broke the record for the largest DDoS attack ever, which occurred in September 2016, targeting the French company OVH, at a scope of 1 Tbps; it used bots (software agents) that exploited the widespread CCTV cameras. In many respects, this is a dangerous escalation and sets a new threshold for a cyber threat that on a few levels so far has no satisfactory response.

The first aspect is connected to the proliferation of these devices. In the US, there are about 25 connected devices per every 100 people, and this is just the beginning of the trend. Gartner Inc. estimates that in 2016 the world will have 6.4 billion connected devices, and that by 2020 that number will approach 21 billion. Such a vast number of devices creates a significant weakness for the web and allows attackers of various sorts to use them for any number of goals. The new twist in the most recent attack was the simplicity with which it was carried out. Millions of devices can serve as the potential means for DDoS cyberattacks whose execution is relatively simple, because the devices create new entrance points to the internet, making the scope of the threat enormous. The threat grows even greater because end devices, such as smartphones and computers, are used to control the connected devices.

The second aspect concerns the weakness of the defense. Most IoT devices lack appropriate means of security, making it easy for attacks to exploit the weaknesses of the systems operating the devices. The majority of manufacturers have yet to adopt a framework of standards and security; they generally use publicly available open code to make it possible for their devices to communicate with other similar devices in the area, and this itself generates severe security soft spots. Important corrective steps have been initiated in the United States, as security companies, manufacturer associations, and even government agencies have begun to cooperate, but these steps are far from constituting a sufficient defensive response.

The third aspect regards the scope and depth of the damage. The attack on Dyn was a clear warning sign: while the offensive capabilities displayed in the attacks did not require anything particularly sophisticated, the impact was significant. The fact that the malicious code was made public prepared the ground for other attacks that will make use of this or similar code, and raises the specter that the writers of the code already possess an improved version. Thus the use of similar methods of attack will presumably be seen again, perhaps even in more powerful versions.

Finally, there is privacy. One of the key problems with connected devices is securing user privacy. Connected devices are constantly collecting information about their users' parameters, at home and in the office, including the nature of use of equipment and electrical appliances as well as wearable devices, whose use is becoming more widespread. The inherent defensive weaknesses of these devices means that all that information could be available to various attackers intent on subversion.

The weakness shown in the last attack is not the burden of the private sector alone. The use of armies of connected devices is a challenge for the state, because it has the capability to harm the routine performance of governments and, worse still, disrupt performance during emergencies and in wartime. Because the risk is real, defending connected devices is an enormous challenge. In response to the attack on Dyn, the United States government was called on to enact regulation on the security of IoT products. Indeed, this seems precisely where efforts should be focused, with measures similar to the steps taken in the financial sector. Although the problem is global, Israeli entities charged with cyber security must fully understand the risk of exposure to such attacks and take action by partnering with international efforts on the issue, while at the same time taking steps to enhance the relevant defensive mechanisms and their continued performance in order to cope with this type of attack.