The dark destiny of safety

By Max Rowe & Jose Trejos

Originally published November 3, 2016

Image: Arielinson via Wikimedia Commons, licensed CC-BY-SA

Most people imagine hacking to be an exceedingly complex crime, requiring an understanding of computing systems that goes far beyond that of average, functionally literate PC users. While there are sophisticated hacking techniques which do fit this description, many forms of hacking require little more than the ability to install basic programs on a computer. Perhaps the simplest of all forms of hacking is DDoS, or denial of service attack. DDoS is a simple brute-force method that spams a server with millions of identical simple requests, which can cause sites and providers to be overloaded and temporarily shut down.

Users can simply band together and use their combined computing power to take down a target, as notable attacks on Donald Trump's and even the CIA's websites have illustrated. More sophisticated DDoS attacks have employed "Trojans" or other viruses to take control of the computers of virtual bystanders and used them to perpetrate these types of attacks unawares. While DDoS usually fails to permanently bring down websites, it is also almost impossible to stop completely, since simple request-overload is not something most normal programs guard against.

The DDoS hacking technique has been around for so long that many controversial websites see them as a regular part of business. But developed countries' increasing dependence on connective technology could make these attacks exponentially more dangerous than they ever have been. Economists have long predicted an "Internet of Things", in which an ever-growing network of interconnected appliances work together to gather information and personalize their performance for different users. In an oft-mentioned example, groceries may one day order and replenish themselves, as an electronic pantry scans the used items and orders replacements autonomously.

The Internet of Things is increasingly becoming a reality, and while it has its benefits, it has also resulted in a massive increase of appliances connected to the internet that are virtually defenseless. Hackers find it laughably easy to hack a refrigerator that is programmed to automatically share its information. In fact, it is not difficult to make programs that can infect entire networks of such interconnected appliances in an automated process. Although each individual unit has low processing power, these networks can be incredibly powerful when directed toward a single goal. DDoS attacks are a natural application.

The attack on Brian Krebs just a month ago displayed the terrifying power of these repurposed networks. Mr Krebs is a journalist specializing in cybersecurity; in the course of his reporting he has naturally run afoul of multiple hacking groups. Mr. Krebs, aware of his status as a high-level target among these groups, preemptively purchased powerful DDoS protection from internet providers in an effort guard against these type of attacks. It proved to be of no avail. In September, when a coordinated strike against Mr. Krebs reached almost 700 gigabits per second – enough to interrupt connections between entire countries – Mr. Krebs was cut loose by the desperate companies. This incident may seem fairly insignificant to those who do not follow journalists like Mr Krebs, but it has terrifying implications: If a hacking group is determined to stop a journalist, these networks have given hackers power to completely censor them from the internet.

A far more publicized attack took place a little over a week ago, bringing down large swaths of the United States' connections altogether. This attack fulfilled what had long been a terror of cybersecurity experts, but had never been seriously attempted due to the sheer computational power required: an attack on DNS servers. Domain Name System services, or DNS, serve as the internet's directory; DNS is what converts names such as "google.com" into directions that allow a computer to connect to a website. Without access to DNS, the entire internet could be temporarily shut down. Using Mirai, a large network that took advantage of poorly secured appliances like those heralded by the Internet of Things, a hacking group attacked DNS servers and reached a record-breaking trillion gigabits per second. The group managed to completely take down the domains of some of the **world's largest companies** for several hours, including Airbnb, Twitter, Vox, Spotify, Netflix, and Reddit. A larger attack could take down the internet in an entire country for a much longer period of time.

In a world where the internet is already nearly omnipresent, DDoS attacks are now an enormous threat to national security. Perhaps the biggest underlying issue is that fact that users, and therefore the market, face little incentive to program any form of serious cybersecurity into simple appliances. While many live in fear of a computer hacking revealing personal secrets, the thought of a security breach revealing refrigerator temperatures is far less frightening. World governments need to pass regulations controlling these devices, demand strong security standards, and dedicate far more resources to improving cybersecurity. If they do not, it may not be long before entire countries lose their access to the connective fabric of modern society.

References

Beal, V. (n.d.). DDoS attack – Distributed Denial of Service. *Webopedia*. http://www.webopedia.com/TERM/D/DDoS_attack.html Archived at https://perma.cc/5LJN-TUL5

Keane, J. (2016). Brian Krebs is back online following a DDOS attack thanks to Google's Project Shield. *Digital Trends*. https://www.digitaltrends.com/computing/brian-krebs-project-shield/ Archived at https://perma.cc/NG9M-HZFW

Klein, A.G. (2016). How anonymous hacked Donald Trump. *The New Republic*. https://newrepublic.com/article/132283/anonymous-hacked-donald-trump Archived at https://perma.cc/3Y78-DDHC

Krebs, B. (2016). DDoS on Dyn impacts Twitter, Spotify, Reddit. *Krebs on Security*. https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/ Archived at https://perma.cc/KA8U-TE8A

Morgan, J. (2014). A simple explanation of ‘the Internet of Things’. *Forbes*. https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#28b97bc71d09 Archived at https://perma.cc/P8YJ-7CXV

O’Brien, S.A. (2016). Widespread cyberattack takes down sites worldwide. *CNN Tech*. http://money.cnn.com/2016/10/21/technology/ddos-attack-popular-sites/ Archived at https://perma.cc/MB69-SGPV

The Economist. (2016). The internet of strings. http://www.economist.com/news/science-and-technology/21708220-electronic-tsunami-crashes-down-solitary-journalist-internet Archived at https://perma.cc/8GG8-W4X4