Computer says no

Denial of service attacks over the internet are growing easier and more powerful. Their perpetrators are more cunning, too

"Tick tock tick tock", tweeted Anonymous Africa, a group of computer hackers, on June 14th. Minutes later a website of the African National Congress (ANC), South Africa's ruling party, went offline: another victim of the oldest and crudest form of cyber-assault, a distributed denial of service (DDoS) attack. Arbor Networks, an American security firm, counts 2,800 each day. Unlike some forms of internet mischief DDoS attacks generally are not clever or complex. They consist of floods of nuisance traffic, which slows or crashes the victims' websites, leaving them offline, unable to send e-mail, process orders, make bank transactions or (for governments) run the country.

Teenage pranksters in the 1990s used DDoS attacks to boot enemies from internet chat rooms. Youthful mischief still accounts for many. Matthew Prince of CloudFlare, a networking firm, says attacks spike in the summer holidays. Politics and religion often fuel them too. The ANC's attackers cited its support for Zimbabwe's Robert Mugabe. Arab hackers who clobbered American banks between September and May wanted "The Innocence of Muslims", a controversial video, removed from the web. Iranian military hackers may have helped—though the attacks also resembled those carried out in 2010 against PayPal, Visa and MasterCard, which had stopped processing donations to WikiLeaks, a whistle-blowing group.

Now DDoS is maturing. Extortion is thriving: pay up, or your site stays offline. Rival businesses may use them during peak sales periods or while bidding for big contracts. They are useful as part of other crimes, distracting attention, for example, during the theft in 2011 of more than 100m customer records from Sony, a media and electronics giant. Mt Gox, the largest exchange for Bitcoin, a digital currency, said market manipulators used DDoS attacks to drive down prices in April. In last year's Russian election, attacks hit news sites and election observers. In 2012 a South Korean politician's aide was jailed for an attack aimed at stopping opposition voters from finding the right polling stations.

An underground economy makes ordering such attacks easy. Gwapo is one of several firms that openly advertises DDoS services on YouTube. It charges $5 an hour to disable small sites and up to $100 for big ones. Payment is in Bitcoin or by other anonymous means. A plethora of tiny firms claims to help test defences, but they rarely check who runs the sites they target.

For the technologically adept, DDoS software is available free. The Low Orbit Ion Cannon is named after a weapon in “Command and Conquer”, a video game. Other tools let sympathisers join in by using their internet browsers. The attacks are growing more powerful (see chart). In March CloudFlare helped Spamhaus, a spam-fighting charity, against nuisance traffic which flooded in at an unprecedented 300 gigabits per second, almost 200 times faster than an average assault.

As well as roping in collaborators, most attackers use botnets: vast networks of virus-infected computers that obey secret commands from a faraway “bot-herder”. These are getting beefier. A typical botnet in the past comprised infected single computers, mostly in emerging countries. Now the bot-herders have learned to commandeer huge corporate or public-sector computers in America. These have more processing power and better internet connections. Whereas big attacks once used tens of thousands of zombie computers, this year’s assaults on American banks employed only about 2,500.

Attackers are also getting better at exploiting flaws in the internet’s design. Deep in its architecture are computers known as domain name system (DNS) servers. These help direct genuine traffic around the network. But they can be tricked into firing data at their victims. Many thousands of DNS servers helped batter Spamhaus; geeks think concerted attackers could rope in 20m.

Better-targeted attacks need less muscle to do more damage. Instead of congesting the connections between the victim and the internet, hackers increasingly target internal weaknesses on the targeted website. They identify functions that use a lot of processing power—such as search boxes or login scripts—then pummel them until the whole site freezes. These now make up about a quarter of all large attacks. They are fiddlier to arrange, but hard to counter, says Dan Holden of Arbor Networks.

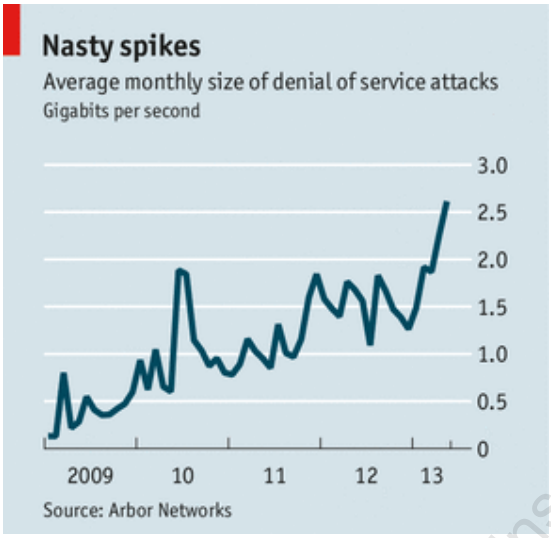
The technical means of blocking DDoS attacks are growing. The legal screws are tightening too. Such attacks have been illegal in Britain since 2006, and for longer in America (where some culprits face up to 15 years in jail). In May a judge in London handed down jail terms of 24 to 32 months to three members of Lulzsec, a short-lived gang which crashed the site of Britain’s Serious Organised Crime Agency in 2011. A month earlier police investigating the Spamhaus attack arrested Sven Kamphuis, a Dutchman who praised the assault on Russian television. Supposedly in hiding, he failed to conceal his real-world whereabouts. A battered orange van, laden with satellite equipment, drew attention to his flat near Barcelona; so did his name on the letter box.

Hapless cyber-vandals are easier to nab than sophisticated cyber-criminals. But some free-speech activists think automatic criminalisation of DDoS attacks is unfair. They liken the tactic to civil protests such as sit-ins. Hackers think “technology actions” should be protected like free speech, explains Vanessa Barnett, a lawyer.

Jay Leiderman, a Californian lawyer, thinks sentences are “hysterically unjust”. He defended Christopher Doyon, a hacker better known as Commander X, who fled to Canada last year while awaiting trial for an 18-minute attack on the Santa Cruz County website, in protest at rules that outlaw sleeping in parks. Mr Leiderman wants American laws to tolerate “limited and constrained” DDoS campaigns.

Foreign precedents may help. In 2006 a German court overturned the conviction of a campaigner who attacked the site of the airline Lufthansa because it let its planes be used to deport asylum-seekers. But in January an American petition demanding the decriminalisation of DDoS failed to force an official response. Recent efforts to rewrite America’s aged computer-crime law are bogged down. “I worry we’ve taught bored teenagers that with ten lines of code they can scare the internet and make the front page of the New York Times,” says Mr Prince. As denial of service becomes a destructive, sophisticated and lucrative criminal industry, pranksters can expect less tolerance, not more.

Correction: An earlier version of this article stated that the attack on Spamhaus reached 300 gigabytes per second. It should have said 300 gigabits. Sorry.



Fonte: The Economist, London, v. 407, n. 8841, p. 63-64, 22 a 28 Jun. 2013.