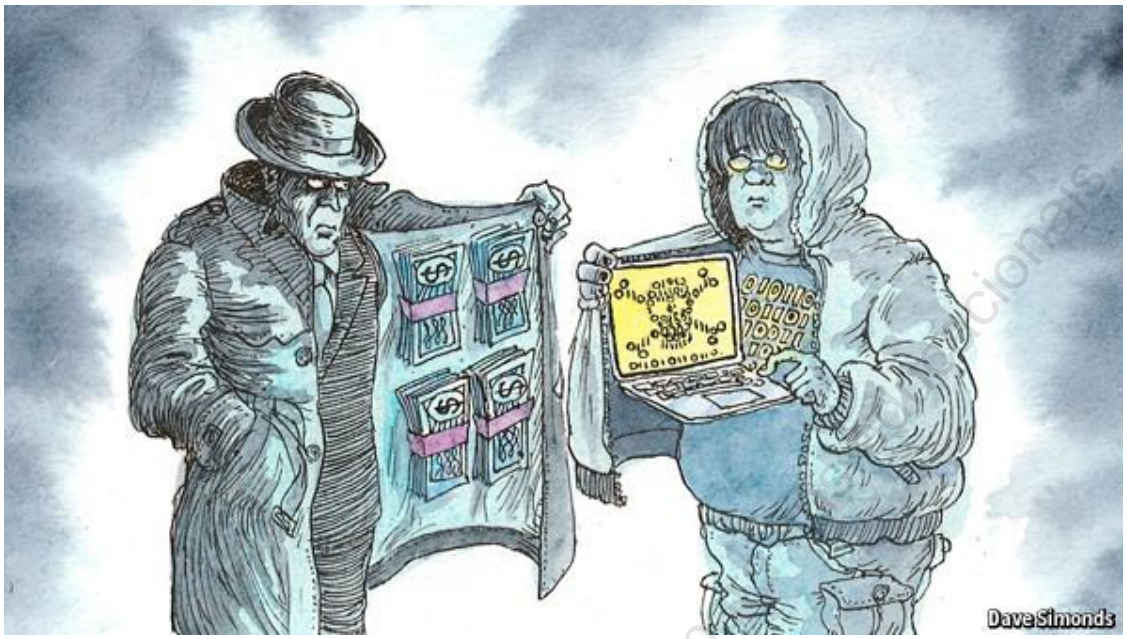
The digital arms trade

The market for software that helps hackers penetrate computer systems



IT IS a type of software sometimes described as “absolute power” or “God”. Small wonder its sales are growing. Packets of computer code, known as “exploits”, allow hackers to infiltrate or even control computers running software in which a design flaw, called a “vulnerability”, has been discovered. Criminal and, to a lesser extent, terror groups purchase exploits on more than two dozen illicit online forums or through at least a dozen clandestine brokers, says Venkatramana Subrahmanian, a University of Maryland expert in these black markets. He likens the transactions to “selling a gun to a criminal”.

Just a dozen years ago the buying and selling of illicit exploits was so rare that India’s Central Bureau of Investigation had not yet identified any criminal syndicates involved in the trade, says R.K. Raghavan, a former director of the bureau. Underground markets are now widespread, he says. Exploits empower criminals to steal data and money. Worse still, they provide cyber-firepower to hostile governments that would otherwise lack the expertise to attack an advanced country’s computer systems, worries Colonel John Adams, head of the Marine Corps’ Intelligence Integration Division in Quantico, Virginia.

Exploits themselves are generally legal. Several legitimate businesses sell them. A Massachusetts firm called Netragard last year sold more than 50 exploits to businesses and government agencies in America for prices ranging from $20,000 to more than $250,000. Adriel Desautels, Netragard’s founder, describes some of the exploits sold as “weaponised”. The firm buys a lot from three dozen independent hackers who, like clients, are carefully screened to make sure they are not selling code to anyone else, and especially not to a criminal group or unfriendly government.

More than half of exploits sold are now bought from bona fide firms rather than from freelance hackers, says Roy Lindelauf, a researcher at the Netherlands Defence Academy. He declines to say if Dutch army or intelligence agencies buy exploits, noting that his government is still figuring out “what we’re allowed to do offensively”.

Laws to ban the trade in exploits are being mooted. Marietje Schaake, a Dutch member of the European Parliament, is spearheading an effort to pass export-control laws for exploits. It is gathering support, she says, because they can be used as “digital weapons” by despotic regimes. For example, they could be used to monitor traffic on a dissident’s smartphone. However, for a handful of reasons, new laws are unlikely to be effective.

Exploits are a form of knowledge, expressed in computer code. Attempting to stop people from generating and spreading knowledge is futile, says Dave Aitel, a former computer scientist at America's National Security Agency (NSA) who went on to found Immunity, a computer-security firm in Florida. He says that legal systems would not even agree on which code is good and which is bad. Many legal experts say code should be protected by free-speech laws—it is, after all, language expressed as strings of zeros and ones.

Moreover, tracking down exploits is hard. Hackers keep them secret so that the intended victim doesn't identify and fix the vulnerability, thereby rendering the exploit worthless. As a French exploit developer puts it, those liable to be rapidly detected are about as useful as a "disposable gun" that can be fired just once. Secrecy surrounding the design, sale and use of exploits makes protecting computer networks from them akin to finding "unknown unknowns", says Kenneth Geers, a cyber-security specialist at America's Naval Criminal Investigative Service.

Several governments want firms to develop exploits. In 2010 a computer worm called Stuxnet was revealed to have attacked Iran's nuclear kit. It used four main exploits to get in; at least one appears to have been bought rather than developed in-house by the government that launched the attack (presumably America or Israel), says David Lindahl, an IT expert at the Swedish Defence Research Agency, a government body in Stockholm. An unprecedented weapon, Stuxnet remained undetected for years by quietly erasing its tracks after "planting sabotage charges at exactly the right place" in Iran's uranium-enrichment centrifuges, Mr Lindahl says.

Nearly all well-financed intelligence agencies buy exploits, says Eric Filiol, a lieutenant-colonel in computer intelligence for France's army until 2009. Computer experts who years ago would reveal software vulnerabilities for mere prestige have realised that they were treating "diamonds as pebbles", says Mr Filiol, now head of the Operational Cryptography and Computer Virology Lab in Laval. His lab is partly financed by France's defence ministry to provide it with exploits.

Finding holes in the firewall

The price of exploits has risen more than fivefold since 2004, Mr Filiol says, referring to a confidential document. They vary greatly, depending on three main factors: how hard the exploit is to develop; the number of computers to which it provides access; and the value of those computers. An exploit that can stealthily provide administrator privileges to a distant computer running Windows XP, a no-longer-fashionable operating system, costs only about $40,000. An exploit for Internet Explorer, a popular browser, can cost as much as $500,000 (see chart).

Software firms also buy exploits to identify and repair vulnerabilities in their products before others take advantage of them. A small Vancouver firm called Tarsnap, for example, has paid 30 people who pointed out flaws in its encryption software for online PC backups. To develop better defences for its clients' computer systems, HP, an American giant, has spent more than $7m since 2005 buying hundreds of "zero days", as undiscovered exploits are also known in hacker slang. (Once discovered, an exploit's days are numbered, literally: it becomes a "one day", then a "two day", and so on until the vulnerability it exploits is patched.)

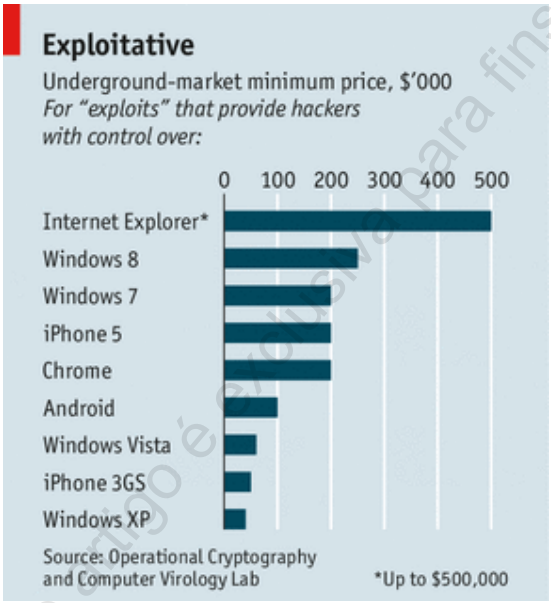
Such "bug bounty" schemes, however, will struggle to compete with buyers who want to exploit rather than seal vulnerabilities. Tarsnap's biggest payout was just $500. Last year Google offered Vupen, a French firm, $60,000 for an exploit that burrowed into its Chrome browser. Vupen's boss, Chaouki Bekrar, balked, noting that he could get more elsewhere.

Other reputable customers, such as Western intelligence agencies, often pay higher prices. Mr Lindelauf reckons that America's spies spend the most on exploits. Vupen and other exploit vendors decline to name their clients. However, brisk sales are partly driven by demand from defence contractors that see cyberspace as a "new battle domain", says Matt Georgy, head of

technology at Endgame, a Maryland firm that sells most of its best exploits for between $100,000 and $200,000. He laments a rise in sales by unscrupulous vendors to dangerous groups.

On March 12th the head of the Pentagon's Cyber Command, General Keith Alexander, warned the Senate Armed Services Committee that state-sponsored groups are stepping up efforts to steal and destroy data using "cybertools" purchased in illicit online markets. As an American military-intelligence official points out, governments that buy exploits are "building the black market", thereby bankrolling dangerous R&D. For this reason, governments appear increasingly keen to develop exploits in-house. Paulo Shakarian, a cyberwar expert at West Point, an American military academy, says China appears to be moving in this direction.

Developing exploits in-house reduces the risk that a double-dealing vendor will resell code meant to be exclusive. Even so, the trade isn't likely to fade away. When developers work out a trick that gives them control over the targeted software, they like to yell out a celebratory "who's your daddy?" notes Pierre Roberge, boss of Arc4dia, a Quebec firm that sells exploits to spy agencies. Exploit trading will continue as long as people pay big money for the opportunity to utter the same joke—this time at the expense of a victim who has been hacked.



Fonte: The Economist, London, v. 406, n. 8828, p. 65-66, 23 a 29 Mar. 2013.