https://internationalviewpoint.org/spip.php?article5139

Technology

NSA's Cyberwarfare Blowback

- IV Online magazine - 2017 - IV512 - September 2017 -

Publication date: Thursday 14 September 2017

In May and June, hackers took over thousands of computers around the world, encrypted their contents, and demanded ransom to decrypt them. They used tools developed by the National Security Agency (NSA) to exploit vulnerabilities in the Microsoft Windows operating system.

China suffered most from the May attacks, and Ukraine from the June attacks, but both attacks spread worldwide, including to Russia and the United States.

Some cybersecurity experts thought the May attacks came from North Korea; others thought they were made to look as if they came from North Korea. Why would North Korea target its ally China?

Some thought the June attacks came from Russia. Some thought they came from Iran. Others thought they were made to look as if they came from Russia or Iran.

The motive for the attacks was obscure. The hackers demanded ransom, but they used ineffective methods for collecting it. They may have made a few thousand dollars, but the authorities quickly shut down their public email addresses, making payment in exchange for decryption impossible.

The combination of obvious technological prowess and apparent financial incompetence led to speculation that the hackers' ransom demands were a cover for a deeper operation to obtain credentials for a future attack. Or a dry run for a future attack. Or political disruption. Or simply mischief.

The source of the NSA malware was another mystery. A group calling itself the Shadow Brokers offered the NSA tools for sale last August and posted them for downloading free in April, after Microsoft had belatedly issued a patch to fix the vulnerability. The Shadow Brokers said they would release more NSA tools each month.

Were the Shadow Brokers hackers looking to make money? If so, why did they offer to sell the NSA tools so publicly in August, rather than discreetly seek buyers? Why did they begin giving them away in April? Why did they so publicly declare that they would release more tools each month?

Were they hactivists seeking to expose the NSA's nefarious activities? Were they disillusioned NSA employees or contractors? Or was the attack an NSA operation, a cyberwarfare experiment disguised as a hacker attack?

Whatever the depth of the conspiracies, two facts are clear: 1) The NSA looked for and found vulnerabilities in the Windows operating system and, rather than alert Microsoft and the cybersecurity firms, developed malware âEuros" malicious software âEuros" to exploit the vulnerabilities. 2) The malware escaped the NSA's control and infected computers and networks of governments and corporations that the NSA was supposedly trying to protect.

Cybersecurity, Cyberintelligence and Cyberwarfare

The activities of the so-called "U.S. intelligence community" include cybersecurity, cyberintelligence and

cyberwarfare.

Cbersecurity is defense against cyberattacks by governmental and nongovernmental actors. It involves finding weaknesses in computers and networks and devising ways to fix them and prevent intrusion. Virus protection software and ad-blockers are examples of this.

Cyberintelligence is spying on governments, corporations and people by digital means. It involves finding weaknesses in computers and networks and devising ways to exploit them to gather intelligence.

Edward Snowden revealed that the NSA collects metadata on almost every electronic communication in the United States and a great many in other countries. Metadata in this context is data about who contacts whom, by what means, where, when and for how long.

The NSA has tools to access the content of the communications too, unless they are strongly encrypted. Their doing so is supposedly limited by the requirement of court approval, but "national security" is a watchword that gets past most oversight.

Cyberwarfare is disrupting, damaging or destroying by digital means the military, economic or diplomatic power of an enemy.

The Stuxnet worm was an example of cyberwarfare. The NSA developed it to spread through a network of computers, conceal itself, and on command disrupt software controlling targeted equipment. The United States and Israel used it against Iranian nuclear centrifuges in 2010.

Arrogance

So what happened in the case of the Shadow Brokers ransomware attack? The NSA had identified a weakness, decided to exploit it to create a cyberweapon, and then lost control of the weapon it created. The unintended consequences were the result of arrogance on many levels.

There was military arrogance in thinking that the new weapons could be wielded with impunity. But what goes around comes around. The United States is highly dependent on computers and networks, and others can develop and wield cyberweapons too.

Blowback happens. This has led governments to think twice about the use of biological, chemical and nuclear weapons, targeting civilians, indiscriminate use of land mines, cluster bombs, torture, etc., even if they still too often decide to use them.

There was imperial arrogance in thinking that the weapons could be used with impunity against less powerful countries.

The U.S. government knows that Russia and China can retaliate against U.S. spying and sabotage. Now it must contend with the possibility that North Korea and Iran can retaliate too. In countries around the world hackers are targeting the United States in the service of their governments, for profit, or for fun.

There's capitalist arrogance in thinking that profit justifies all. The tools used in the ransomware attack were developed by the NSA. But they were developed in the culture of Google, Facebook, Twitter, etc, whose business is built on acquiring information about people and selling it for ads or other purposes.

In this culture human intelligence and decency are irrelevant. Money is its only measure. Let the market determine winners and losers.

There's technological arrogance in thinking that development is necessarily beneficial âEuros" because we can develop it, we should.

This concern is particularly pertinent because the software the NSA is developing makes use of artificial intelligence. Once implanted, the malware investigates its environment, adjusts its behavior based on what it finds, tries various courses of action, and adjusts its behavior based on the results.

As with nuclear and many other technologies, the human handlers of the software can't foresee the consequences. They don't know what they don't know.

Social Technology

Technology can be beneficial. The problem is to control and direct it.

Capitalist governments use technology to dominate people. Imperialist governments use it to dominate other countries. Capitalist corporations use it to maximize profits. Researchers, engineers and entrepreneurs shaped by capitalism use it to get rich and famous.

This leads to an unstable world, increasingly dependent on technology but unable to control or direct it. The Shadow Brokers ransomware attack is a warning. Much, much worse will happen, unless human beings regain control of their technology.

Humanity must eliminate the dangers of military arrogance by eliminating militarism and war. This requires eliminating classes and nation-states, as Marxists have said for 170 years.
We must eliminate the dangers of imperial arrogance by eliminating imperialism. Workers of the world, unite; recognize the self-determination of nations; use the combined development of the global economy to eliminate the uneven development which leads to inequality and wars of domination.

We need to eliminate the dangers of capitalist arrogance by eliminating capitalism: Abolish private property in the means of production. Abolish copyrights and patents. Develop science and technology in public institutions run transparently by research workers.

Finally, we have to contain, if not eliminate, the dangers of technological arrogance by openly publishing the results of science, research and development. The achievements of human ingenuity should be common property. Together we can check foolish impulses and correct mistakes.

This is music of the future, of course. But much can be done today:

Join the ongoing fights for civil liberties, privacy protections, restrictions on FBI, CIA and NSA spying, Internet freedom and Net neutrality. Participate in open source software projects, support Wikipedia and other open information projects, and contribute to progressive publications and Internet sites.

Oppose militarism and war, including the development and deployment of cyberweapons. Cut the military budget. Open the secret budget of the security services to public scrutiny.

And in the course of this activity, raise the prospect of a future without the NSA, the CIA and the FBI, and without Google, Facebook, Microsoft, Apple, Amazon, Uber and other corporations which profit from the human need to communicate. Social networks should be truly free, and truly social.

Against the Current

PS:

If you like this article or have found it useful, please consider donating towards the work of International Viewpoint. Simply follow this link: Donate then enter an amount of your choice. One-off donations are very welcome. But regular donations by standing order are also vital to our continuing functioning.