Hacker Lexicon: What Are CNE and CNA?

Author: Kim Zetter.Kim Zetter Security
WIRED | 2016-07-06

For years, the US government's offensive hacking operations were kept in dark shadows, neither acknowledged nor discussed. That changed with the discovery of Stuxnet in 2010—a computer sabotage operation reportedly conducted by the US and Israel to destroy machines used in Iran's once-illicit nuclear program.

Stuxnet was the first US digital sabotage operation to be exposed, but it's not the first government hacking operation ever conducted. Documents leaked by Edward Snowden in 2013 shone a light on a vast underground operation conducted by the NSA's Tailored Access Operations team (TAO), responsible for what the government refers to as computer network exploitation and computer network attacks. Those may sound similar, but there are important differences between them.

Computer network exploitation, or CNE, refers to espionage and reconnaissance operations. These are conducted to steal data from a system or simply to obtain intelligence about networks, to understand how they work and are configured. Examples of CNE include Flame, a massive spy tool used to gather intelligence from Iran and other targets, and Regin, which was used to hack the European Commission and Belgium's partially state-owned telecom Belgacom. The Regin operations have been attributed to the UK spy agency GCHQ.

A catalog of custom NSA hacking tools leaked to reporters in 2013 shows the vast capabilities available to TAO hackers. The tools, with names like PICASSO, IRATEMONKEY, COTTONMOUTH, and WATERWITCH, can subvert firewalls, servers, and routers, or impersonate GSM base stations to intercept mobile phone calls or siphon data from wireless networks. There are also bugging devices the TAO hackers plant in targeted computers to siphon data, via radio waves, to listening stations, sometimes located up to eight miles away from a victim's machine.

In 2011, the NSA launched 231 offensive computer operations, according to Snowden documents. This included placing covert implants in more than 80,000 machines around the world.

If you think of CNE as the *Ocean's Eleven* of cyberattacks, CNA is more like *Die Hard*.

CNA operations are designed to damage, destroy, or disrupt computers—or operations controlled by computers—such as the Stuxnet attack that targeted centrifuges used by Iran to enrich uranium hexafluoride gas. Another CNA operation attributed to nation states is the air-to-ground hack conducted by Israel in 2007 against Syria's air defense system. That hack, launched from Israeli planes, was designed to prevent Syria's automated air-defense system from seeing bomber jets flying in to conduct an air strike against the Al-Kibar complex, believed to be an illicit nuclear reactor Syria was building.

The recent hack of power distribution plants in Ukraine was a CNA, as was the Wiper attack that targeted Iran's oil industry in 2012. That attack wiped data from machines belonging to the Iranian Oil Ministry and the National Iranian Oil Company. The hack of Sony, attributed to North Korea, would also be considered a CNA operation since the hackers didn't just siphon data from the company's network, they also destroyed data and systems on their way out the door.

Although CNE and CNA operations might seem to be technically distinct—since one involves espionage and the other destruction or disruption—they aren't necessarily. Many CNA attacks begin as CNE operations, since attacks designed to cause destruction often

require digital reconnaissance and intelligence collection first. The gang of hackers that launched Stuxnet, for example, also designed several spy tools, some of which are believed to have been used to gain intelligence about the computers controlling Iran's centrifuges that was then used to design the malicious code that destroyed the centrifuges.

Because some tools can be used for both CNE and CNA attacks—for example zero days are used to install both espionage tools and attack tools on targeted systems—it can be difficult for victims who find such malware on their machines to know whether the operation is a spy mission or an attack mission; at least, that is, until their systems get destroyed.

Go Back to Top. Skip To: Start of Article.

read:https://www.wired.com/2016/07/hacker-lexicon-cne-cna/