The global ransomware attack and the crimes of the US spy agencies

Andre Damon
16 May 2017

Over the past four days, some 350,000 computers have been infected by the so-called "WannaCry" malware, including 70,000 devices such as MRI scanners, blood storage refrigerators and operating equipment used by Britain's National Health Service. As a result of the attack, the NHS was forced to turn away emergency room patients and divert ambulances, potentially resulting in serious illnesses and even fatalities.

The worm is a piece of "ransomware" that encrypts users' data until the creators receive a payment. It uses "exploits" developed by the US National Security Agency as just a small part of the NSA's catalog of hacking tools.

When NSA researchers discovered the vulnerability in the Windows operating system targeted by "WannaCry," they refused to inform Microsoft. The company found out about the existence of the vulnerability only shortly before the general public, when it was leaked by the Shadow Brokers hacker group on April 14 of this year.

On Saturday, Microsoft President Brad Smith, in a tersely worded blog post, faulted the NSA for failing to share its knowledge of the exploit. "This attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem," he wrote, adding that "this most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats in the world today—nation-state action and organized criminal action."

He concluded, "We need governments to consider the damage to civilians that comes from hoarding these vulnerabilities and the use of these exploits."

Microsoft is far from blameless when it comes to the NSA's operations. It has established a standing practice of reporting bugs to the US government before they are repaired and publicly acknowledged, allowing the NSA to use these vulnerabilities to break into systems.

Regardless, Smith's statement represents a stinging indictment of the operations of the US intelligence apparatus, implying that its actions are only once removed from those of criminals.

The hacking tools used in the "WannaCry" malware serve an even more malevolent purpose than any ransomware: illegal spying on the population of the whole world as part of a systematic practice of subversion and cyber aggression.

In May 2013, NSA contractor Edward Snowden revealed that the US intelligence apparatus collects, processes, reads and catalogs a vast quantity of private communications, both in the United States and internationally. Snowden explained that the stated aim of the NSA, the "signals intelligence" arm of the US intelligence apparatus, is unfettered access to all private information. Its mottos are, according to a leaked internal presentation, "Collect it All," "Process it All," "Exploit it All, "Sniff it All" and "Know it All."

Illegal domestic surveillance operations authorized by the Bush administration after 9/11 resulted in the vastly expanded scale of government spying that was exposed by Snowden. With the collaboration, both voluntary and coerced, of the major telecommunications companies, the US government was able to vacuum up nearly all phone conversations, email and chat messages exchanged on digital devices.

In subsequent years, common communications platforms substantially improved their security capabilities, with nearly all Internet communication systems enabling encryption by default. These developments prompted US intelligence officials to complain of the Internet "going dark" to the NSA and

CIA, prompting repeated calls by politicians, including Democratic presidential candidate Hillary Clinton, to criminalize the use of encryption.

The NSA responded by vastly expanding its use of "Tailored Access Operations," the arm of the NSA devoted to "computer network exploitation," commonly known as hacking. The agency adopted the slogan, "Your data is our data, your equipment is our equipment—anytime, any place."

The NSA worked to build up a catalog of cyber weapons, known as "exploits," which allow it to easily break into almost any Internet-connected device. One internal NSA document from 2012 claimed that the NSA worked with the largest telecommunications and technology companies in the world to "insert vulnerabilities into commercial encryption systems, IT systems, networks and endpoint communications devices used by targets."

The NSA's massive team of security researchers—the largest in the world—also worked to discover and exploit vulnerabilities within existing products, keeping these bugs a secret from manufacturers in order to allow the NSA to exploit them to gain access to computers, networks and Internet-connected devices before other researchers could discover them and recommend fixes to manufacturers.

In addition to using these tools to carry out mass surveillance, the NSA weaponized them in order to carry out cyberattacks against Washington's geopolitical adversaries. The most notorious of these efforts was the release of the Stuxnet worm in 2010, which ruined some 1,000 Iranian nuclear centrifuges. The cyberattack was coordinated with a series of car bomb murders, attributed by the media to the US and Israel, which killed at least three Iranian nuclear physicists.

The fact that over 70 percent of the initially reported "WannaCry" infections took place in Russia raises the very real possibility that the current disaster is the result of a Stuxnet-like cyberattack by the United States. The other country disproportionately affected was China.

Speaking in Beijing on Monday, Russian President Vladimir Putin said, "As for the source of these threats, Microsoft's leadership stated this directly. They said the source of the virus was the special services of the United States."

White House Homeland Security adviser Tom Bossert declared that finding those responsible for cyberattacks is "something that sometimes eludes us. Attribution can be difficult here."

Bossert's statement contrasts sharply with the declaration by the director of national intelligence in October 2016 that the US spy agencies were "confident that the Russian Government directed… recent compromises" of emails related to the Clinton campaign.

That declaration was part of a vast campaign by the Democratic Party, the media and much of the political establishment aimed at demonizing Russia by claiming it had "hacked" the 2016 US elections. As part of that campaign, media outlets, led by the *New York Times*, sought to present Russia as a global hacking powerhouse, subverting the spotless US electoral system.

One can only imagine what would have happened if, instead of the current malware attack mainly affecting Russia and largely bypassing the US in its initial stages, the situation had been reversed. The media would be up in arms about Russian "hackers," with demands that the Trump administration retaliate with sanctions, cyberattacks and more menacing military moves. The Democrats would be in the forefront of calls for new war-mongering resolutions in Congress.

An examination of the facts exposed by the "WannaCry" attack, however, show that the world's biggest band of cyber criminals by far is headquartered in Washington, D.C.