NSA officials worried about the day its potent hacking tool would get loose. Then it did.

Ellen Nakashima, Craig Timberg ⋮ 9-11 minutes ⋮ 5/16/2017

When the National Security Agency began using a new hacking tool called EternalBlue, those entrusted with deploying it marveled at both its uncommon power and the widespread havoc it could wreak if it ever got loose.

Some officials even discussed whether the flaw was so dangerous they should reveal it to Microsoft, the company whose software the government was exploiting, according to former NSA employees who spoke on the condition of anonymity given the sensitivity of the issue.

But for more than five years, the NSA kept using it — through a time period that has seen several serious security breaches — and now the officials' worst fears have been realized. The malicious code at the heart of the WannaCry virus that hit computer systems globally late last week was apparently stolen from the NSA, repackaged by cybercriminals and unleashed on the world for a cyberattack that now ranks as among the most disruptive in history.

The failure to keep EternalBlue out of the hands of criminals and other adversaries casts the NSA's decisions in a harsh new light, prompting critics to question anew whether the agency can be trusted to develop and protect such potent hacking tools.

> If your computer is infected, then a message appears saying all of your files have been encrypted until you pay a ransom. (Video: Gillian Brockell/The Washington Post)

Current and former officials defended the agency's handling of EternalBlue, saying that the NSA must use such volatile tools to fulfill its mission of gathering foreign intelligence. In the case of EternalBlue, the intelligence haul was "unreal," said one former employee.

"It was like fishing with dynamite," said a second.

The NSA did not respond to several requests for comment for this article.

The consequences of the NSA's decision to keep the flaw secret, combined with its failure to keep the tool secure, became clear Friday when reports began spreading of a massive cyberattack in which the WannaCry software encrypted

data on hundreds of thousands of computers and demanded a ransom to decrypt it.

The attack spread virally because the criminal hackers combined EternalBlue's ability to penetrate systems with other code that caused it to spread quickly, like a computer worm, something the NSA never intended. The resulting digital concoction snarled hospitals in Britain, the Interior Ministry in Russia and tax offices in Brazil.

An unlikely combination of voices, ranging from the American Civil Liberties Union to a top Microsoft official to Russian President Vladmir Putin, has singled out the NSA for its role in creating and eventually losing control of computer code.

Microsoft President Brad Smith, in a blog post Sunday, compared the mishap to "the U.S. military having some of its Tomahawk missiles stolen."

Putin, for his part, echoed Microsoft: "They said that the first sources of this virus were the United States intelligence agencies. Russia has absolutely nothing to do with this."

While few critics are saying that the NSA should never develop malicious software — cracking into the computers of surveillance targets is key to its work — the WannaCry incident has revived concerns about internal security at an agency that in 2013 lost massive troves of secret documents to contractor Edward Snowden.

"They've absolutely got to do a better job protecting [the hacking tools]. You can't argue against that," said former NSA director Keith B. Alexander, who ran the agency from 2005 to 2014 but said he was unable to comment on any particular tool. "You had somebody stealing you blind. The government has got to do better at that."

The global backlash to the Snowden revelations added urgency to the government's efforts to revamp rules on when to report flaws to companies and when to use them for surveillance. Alexander said that about 90 percent of discovered flaws are reported to the companies that make the software.

Richard Ledgett, who retired last month as the NSA's deputy director, said disclosing all flaws would amount to "unilateral disarmament." He said the idea that "everything would be just fine" if the NSA disclosed all the vulnerabilities it finds is "nonsense."

In August, a mysterious group calling itself the Shadow Brokers dumped a set of exploits — or hacking tools — online. The exploits are built to take advantage of software flaws.

The agency eventually warned Microsoft after learning about EternalBlue's theft, allowing the company to prepare a software patch issued in March. But the Shadow Brokers did not just release the flaw, which would take time and talent to turn into a tool. They released the exploits, which means even a novice hacker could use them to cause damage.

After fashioning their own tool, WannaCry hackers deployed it last week, causing an immediate outcry. The White House convened an emergency meeting of Cabinet-level heads led by Trump administration homeland security adviser Thomas Bossert.

U.S. systems were mostly spared, but the damage could have been far worse. Since the NSA began using EternalBlue, which targets some versions of Microsoft Windows, the U.S. military and many other institutions have updated software that was especially vulnerable.

The NSA also made upgrades to EternalBlue to address its penchant for crashing targeted computers — a problem that earned it the nickname "EternalBlueScreen" in reference to the eerie blue screen often displayed by computers in distress.

To mitigate its instability in the early days, the NSA hackers were under strict usage rules that required approval from a senior supervisor on a target-by-target basis to use the exploit, the employees recalled.

After a few years, its stability was improved, but NSA was still mindful of the potential for harm if the tool somehow was breached.

"If one of our targets discovered we were using this particular exploit and turned it against the United States, the entire Department of Defense would be vulnerable," the second employee said. "You just have to have a foothold inside the network and you can compromise everything."

The Shadow Brokers' first dump of exploits in August sparked a robust discussion within the Obama administration. "By that point, the intelligence value" of the exploits was "degraded," so it was decided that NSA would alert whatever vendors were affected, a former senior administration official said.

For years, NSA had its own internal process for weighing whether to disclose software flaws to the vendor or to keep them secret so they could be used to build surveillance tools. In the spring of 2014, the Obama administration's National Security Council kicked off a new process to vet vulnerabilities among agencies including the FBI, the NSA, the CIA and Department of Homeland Security.

Some security experts say that the process to debate and disclose vulnerabilities worked in this case but that there was a failure to signal the seriousness of the need to apply fixes.

“NSA identified a risk and communicated it to Microsoft, who put out an immediate patch” in March, said Mike McNerney, a former Pentagon cybersecurity official and a fellow at the Truman National Security Project. The problem, he said, is no senior official took the step of shouting to the world: “This one is very serious and we need to protect ourselves.”

But critics say the government got off easy this time. What if the Shadow Brokers had dumped the exploits in 2014, before the government had begun to upgrade software on its computers? What if they had released them and Microsoft had no ready patch?

Vulnerabilities that are found in widely used software can also provide some of the most valuable intelligence because “they may enable access to a larger number of targets,” said Samir Jain, a former senior White House cyber official. “But the fact that a vulnerability is widely used and therefore the harm could be broad should be a significant factor. At the end of the day, it’s a balancing act.”

Governments around the world will continue using these hacking tools, so the issue is that NSA needs to do a much better job of securing them, current and former officials said.

It is not clear how the Shadow Brokers obtained the hacking tools, which are identical to those breached by former NSA contractor Harold T. Martin III, according to former officials. Martin was arrested in October after the FBI found evidence that he had over the years stolen a massive quantity of classified data from a variety of agencies. The most damaging breach was at the NSA, where Martin allegedly had filched virtually the entire library of hacking tools. Martin has been charged with stealing government property and retaining classified information.

When the breach was discovered last summer, NSA Director Michael S. Rogers told President Obama that he considered himself accountable for it.

“The NSA certainly failed to build an environment that protected these extraordinary secrets that we’ve got,” said a former senior U.S. official. “We’ve got extraordinary capabilities, and it’s a huge responsibility to manage them on behalf of the nation.”

Elizabeth Dwoskin in San Francisco contributed to this report.

Follow The Post’s tech blog, The Switch, where technology and policy connect.