**An NSA cyber weapon is reportedly being used against American cities by the very adversaries it was meant to target**

By Jared Keller, May 25, 2019

In less than three years after the National Security Agency found itself subject to an unprecedentedly catastrophic hacking episode, one of the agency's most powerful cyber weapons is reportedly being turned against American cities with alarming frequency by the very foreign hackers it was once intended to counter.

An explosive New York Times story published Saturday detailing how the NSA's Tailored Access Operations lost control of its so-called 'EternalBlue' malware tool to a cadre of hackers known as the Shadow Brokers, which subsequently publicized the agency's software exploits on the internet and passed them along to hackers associated with Russia, China, and North Korea

The Shadow Brokers' disclosure reportedly came thanks to a 54-year-old former contractor Harold Martin III, who plead guilty in March 2019 for, among other things, taking classified documents and electronic devices home with him for more than 20 years in what government officials characterized as the biggest leak of classified information in U.S. history.

The New York Times story comes in the midst of an ongoing cyberattack on the city government of Baltimore that has paralyzed critical infrastructure and halted daily important transactions from home sales to utility payments. But apparently, the NSA connection wasn't publicly known before Saturday — and the first four paragraphs of the Times story will absolutely make your blood boil:

*For nearly three weeks, Baltimore has struggled with a cyberattack by digital extortionists that has frozen thousands of computers, shut down email and disrupted real estate sales, water bills, health alerts and many other services.*

*But here is what frustrated city employees and residents do not know: A key component of the malware that cybercriminals used in the attack was developed at taxpayer expense a short drive down the Baltimore-Washington Parkway at the National Security Agency, according to security experts briefed on the case.*

*Since 2017, when the N.S.A. lost control of the tool, EternalBlue, it has been picked up by state hackers in North Korea, Russia and, more recently, China, to cut a path of destruction around the world, leaving billions of dollars in damage. But over the past year, the cyber weapon has boomeranged back and is now showing up in the N.S.A.'s own backyard.*

*It is not just in Baltimore. Security experts say EternalBlue attacks have reached a high, and cybercriminals are zeroing in on vulnerable American towns and cities, from Pennsylvania to Texas, paralyzing local governments and driving up costs.*

To be clear: the NSA built a malware tool capable of disabling the computer systems that control everything from payroll to power grids, lost it, and then

basically kept its mouth shut as its own tool was turned against them by the *very enemies they were meant to target in the first place*.

This is basically the cyber equivalent of the GBU-43/B Massive Ordnance Air Blast bomb falling into the hands of ISIS fighters in Nangarhar because some personnel assigned to U.S. Forces Afghanistan delivered the schematics by hand.

Even worse, it casts a major shadow over the aggressive cyber defense plan that the Pentagon rolled out last year to "[defend] forward to intercept and halt cyber threats."

It's also worth noting that Martin's 2016 arrest and the Shadow Broker's subsequent leak of NSA hacking tools occurred just over three years after Edward Snowden pulled back the curtain on the agency's vast domestic surveillance apparatus.

But while a narrow majority of Americans tended to support the NSA's domestic surveillance missteps in the aftermath of the Snowden disclosures, they may not be so forgiving when their light start going out.

SEE ALSO: When Does A Cyber Attack Constitute An Act Of War? We Still Don't Know
WATCH NEXT: The Navy's 'Sky Penis' Incident (A Dramatic Reading)

The Navy's "Sky Penis" Incident (A Dramatic Reading)

The transcript reveals the pilots approached their dick-drawing with calm, precise professionalism.