9-The New York Times-Hacks Raise Fear

Hacks Raise Fear Over N.S.A.’s Hold on Cyberweapons *[Worry]*

Send any friend a story

As a subscriber, you have 10 gift articles to give each month. Anyone can read what you share.

Give this article

281

Read in app

On Wednesday, the calls for the National Security Agency to address its role in the latest hacking attacks grew louder from victims and tech companies. *[Anger, Legal Action]*Credit…Patrick Semansky/Associated Press

By Nicole Perlroth and David E. Sanger

June 28, 2017

Twice in the past month, National Security Agency cyberweapons stolen from its arsenal have been turned against two very different partners of the United States — Britain and Ukraine.

[Disappointment]

The N.S.A. has kept quiet, not acknowledging its role in developing the weapons *[Deny]*. White House officials have deflected many questions, and

responded to others by arguing that the focus should be on the attackers themselves, not the manufacturer of their weapons.

[Deny]

But the silence is wearing thin for victims of the assaults *[Disappointment]*, as a series of escalating attacks using N.S.A. cyberweapons have hit hospitals, a nuclear site and American businesses. Now there is growing concern that United States intelligence agencies have rushed to create digital weapons that they cannot keep safe from adversaries or disable once they fall into the wrong hands.

[Worry]

On Wednesday, the calls for the agency to address its role in the latest attacks grew louder, as victims and technology companies cried foul *[Anger]* . Representative Ted Lieu, a California Democrat and a former Air Force officer who serves on the House Judiciary and Foreign Affairs Committees, urged the N.S.A. to help stop the attacks and to stop hoarding knowledge of the computer vulnerabilities upon which these weapons rely *[Disappointment]*.

In an email on Wednesday evening, Michael Anton, a spokesman for the National Security Council at the White House, noted that the government "employs a disciplined, high-level interagency decision-making process for disclosure of known vulnerabilities" in software, "unlike any other country in the world *[Reinforce]*."

Mr. Anton said the administration "is committed to responsibly balancing national security interests and public safety and security *[Reinforce]*," but declined to comment "on the origin of any of the code making up this malware *[Deny]*."

Beyond that, the government has blamed others *[Deny]*. Two weeks ago, the United States — through the Department of Homeland Security — said it had evidence North Korea was responsible for a wave of attacks in May using ransomware called WannaCry that shut down hospitals, rail traffic and production lines. *[Deny]* The attacks on Tuesday against targets in

Ukraine , which spread worldwide, appeared more likely to be the work of Russian hackers, though no culprit has been formally identified.

Image

“Whether it’s North Korea, Russia, China, Iran or ISIS, almost all of the flash points out there now involve a cyber element,” Leon E. Panetta, the former defense secretary, said in a recent interview.Credit…Paul J. Richards/Agence France-Presse — Getty Images

In both cases, the attackers used hacking tools that exploited vulnerabilities in Microsoft software. The tools were stolen from the N.S.A., and a group called the Shadow Brokers made them public in April. The group first started offering N.S.A. weapons for sale in August, and recently even offered to provide N.S.A. exploits to paid monthly subscribers.

Though the identities of the Shadow Brokers remain a mystery, former intelligence officials say there is no question from where the weapons came: a unit deep within the agency that was until recently called “Tailored Access Operations.”

While the government has remained quiet *[Deny]*, private industry has not. Brad Smith, the president of Microsoft , said outright that the National Security Agency was the source of the “vulnerabilities” now wreaking havoc and called on the agency to “consider the damage to civilians that comes from hoarding these vulnerabilities and the use of these exploits.” *[Anger]*

For the American spy agency, which has invested billions of dollars developing an arsenal of weapons that have been used against the Iranian nuclear program, North Korea’s missile launches and Islamic State militants, what is unfolding across the world amounts to a digital nightmare *[Worry]*. It was as if the Air Force lost some of its most sophisticated missiles and discovered an adversary was launching them against American allies — yet refused to respond, or even to acknowledge that the missiles were built for American use. *[Disappointment]*

Officials fret that the potential damage from the Shadow Brokers leaks could go much further, and the agency's own weaponry could be used to destroy critical infrastructure in allied nations or in the United States.

[Worry]

"Whether it's North Korea, Russia, China, Iran or ISIS, almost all of the flash points out there now involve a cyber element," Leon E. Panetta, the former defense secretary and Central Intelligence Agency chief said in a recent interview, before the weapons were turned against American interests.

"I'm not sure we understand the full capability of what can happen, that these sophisticated viruses can suddenly mutate into other areas you didn't intend, more and more," Mr. Panetta said. "That's the threat we're going to face in the near future."

[Deny]

Using the remnants of American weapons is not entirely new. Elements of Stuxnet, the computer worm that disabled the centrifuges used in Iran's nuclear weapons program seven years ago, have been incorporated in some attacks.

In the past two months, attackers have retrofitted the agency's more recent weapons to steal credentials from American companies. Cybercriminals have used them to pilfer digital currency. North Korean hackers are believed to have used them to obtain badly needed currency from easy hacking targets like hospitals in England and manufacturing plants in Japan.

And on Tuesday, on the eve of Ukraine's Constitution Day — which commemorates the country's first constitution after breaking away from the Soviet Union — attackers used N.S.A.-developed techniques to freeze computers in Ukrainian hospitals, supermarkets, and even the systems for radiation monitoring at the old Chernobyl nuclear plant.

What to Know About Ransomware Attacks

Card 1 of 5

What are ransomware attacks? This form of cybercrime involves hackers breaking into computer networks and locking digital information until the victim pays for its release. Recent high-profile attacks have cast a spotlight on this rapidly expanding criminal industry, which is based primarily in Russia .

Why are they becoming more common? Experts say ransomware is attractive to criminals because the attacks take place mostly anonymously online, minimizing the chances of getting caught. The Treasury Department has estimated that Americans have paid $1.6 billion in ransoms since 2011.

Is there any connection to the rise of cryptocurrencies? The criminal industry's growth has been abetted by cryptocurrencies , like Bitcoin, which allow hackers to transact with victims anonymously, though experts see virtual currency exchanges as a weak point for ransomware gangs.

What is being done about these attacks? The U.S. military has taken offensive measures against ransomware groups, and the Biden administration has taken legal and economic action. Recent attacks have propelled ransomware to the top of President Biden's national security agenda .

Why is the government getting involved? The attacks, which were mostly directed at individuals a few years ago, have dramatically escalated as hackers have begun targeting critical infrastructure in the U.S. , including a major gasoline pipeline and meat processing plants .

The so-called ransomware that gained the most attention in the Ukraine attack is believed to have been a smoke screen for a deeper assault aimed at destroying victims' computers entirely. And while WannaCry had a kill switch that was used to contain it, the attackers hitting Ukraine made sure there was no such mechanism. They also ensured that their code could infect computers that had received software patches intended to protect them.

“You’re seeing a refinement of these capabilities, and it only heads in one direction,” said Robert Silvers, the former assistant secretary of cyber policy at the Department of Homeland Security, now a partner at the law firm Paul Hastings.

Though the original targets of Tuesday’s attacks appear to have been government agencies and businesses in Ukraine, the attacks inflicted enormous collateral damage, taking down some 2,000 global targets in more than 65 countries, including Merck, the American drug giant, Maersk, the Danish shipping company, and Rosneft, the Russian state owned energy giant. The attack so crippled operations at a subsidiary of Federal Express that trading had to be briefly halted for FedEx stock.

“When these viruses fall into the wrong hands, people can use them for financial gain, or whatever incentive they have — and the greatest fear is one of miscalculation, that something unintended can happen,” Mr. Panetta said.

Mr. Panetta was among the officials warning years ago of a “cyber Pearl Harbor” that could bring down the American power grid. But he and others never imagined that those same enemies might use the N.S.A.’s own cyberweapons.

[Worry]

For the past six years, government officials were comforted by the fact that their most fervent adversaries — North Korea, Iran, extremist groups — did not have the skills or digital tools to inflict major damage. The bigger cyberpowers, Russia and China in particular, seemed to exercise some restraint, though Russia’s meddling in the 2016 presidential election added a new, more subtle threat.

But armed with the N.S.A.’s own tools , the limits are gone.

[Worry]

“We now have actors, like North Korea and segments of the Islamic State, who have access to N.S.A. tools who don’t care about economic and other

ties between nation states," said Jon Wellinghoff, the former chairman of the Federal Energy Regulatory Commission.

So long as flaws in computer code exist to create openings for digital weapons and spy tools, security experts say, the N.S.A. is not likely to stop hoarding software vulnerabilities any time soon.

[Disappointment]