8-Forbes-NSA

The WannaCry malware locks up victims' files and threatens to delete them unless they receive… [+] Bitcoin payment before time runs out.

Forbes screenshot

After software vulnerabilities exploited and leaked by the NSA were used by cybercriminals to infect as many as 200,000 Windows PCs with ransomware over the last three days, Microsoft has criticized government agencies for hoarding those flaws and keeping them secret. *[Disappointment]*

One particular vulnerability in Windows, leaked by a shady crew called Shadow Brokers, was used by the WannaCry hackers to give their ransomware a worm feature, allowing it to spread between vulnerable PCs silently and at speed. That flaw was exploited by a tool called EternalBlue and was patched by Microsoft in mid-March, but those who didn't apply the update were still open to attack, resulting in the mammoth attack starting Friday that infected 48 UK National Health Service trusts, FedEx, Telefonica, Renault and Nissan car manufacturing plants, U.S. universities, Russian governments and Chinese ATMs, amongst many other systems across 150 countries.

Microsoft president and chief legal officer Brad Smith said by keeping software weaknesses secret, vendors are left in the dark, can't issue updates, and their customers are left vulnerable to attacks *[Disappointment, Worry]*such as the one that exploded this weekend. he compared the leak of NSA exploits to the theft of missiles from the American military, pointing also to the Wikileaks dump of CIA hacking tools.

"An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen. And 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," Smith wrote in a blog post published Sunday.

"The governments of the world should treat this attack as a wake-up call *[Anger]*. They need to take a different approach and adhere in cyberspace to the same rules applied to weapons in the physical worl *[Anger]*d. We need governments to consider the damage to civilians that comes from hoarding these vulnerabilities and the use of these exploits." *[Disappointment, Anger]*

Smith called for a "Digital Geneva Convention" that would include "a new requirement for governments to report vulnerabilities to vendors, rather than stockpile, sell, or exploit them." *[Disappointment]*

Intelligence agencies, private government contractors and criminals all develop hacks for all kinds of software and keep their techniques secret. The legal use of such exploits assists with law enforcement investigations, military operations and securing against such attacks. They've become so valuable an iPhone hack, for instance, can fetch more than $1 million.

Rob Graham, a security expert who will not say if he's previously developed and sold such exploits in a private capacity, said the NSA deserved "a lot of blame for having weaponized the exploit, then allowing it to leak to the internet." *[Anger, Disappointment]*

But, Graham added, it was "stupid" *[Anger]* to believe the NSA would "unilaterally disarm itself" *[Anger]* and that "arms control trying to regulate such things is even stupider." *[Anger]*

"There's no difference between legitimate software we use to test networks and evil software we use to hack into networks. Code is speech — there is no way of 'controlling' software that doesn't also control speech," he added.

"People keep putting 'cyber' in front a real world concept like 'weapon' and believe all the same principles apply. They don't. Cyberweapons are nothing like weapons, anything you derive from the analogy (like cyberarms control) is going to be flawed."

Microsoft fights WannaCry

Though some have criticized Microsoft for not supporting older Windows versions with updates, it's taken the fight to WannaCry in multiple ways. It issued a fix for Windows XP machines, even though it's been out of support since 2014, 12 years after the operating system was released. It also added updates to Windows Defender in an attempt to prevent the malware from spreading further.

Monday could see the launch of fresh attacks of the ransomware, which locked up PCs and demanded $300 from victims or their files would be deleted. Hackers have started to alter the malware's code to ensure that it doesn't contain a killswitch (as the last version did, as one researcher found out to the world's gain) and is less likely to be killed off so easily.

"The new variants appear to have been made by third parties modifying the initial malware. The changes are trivial and some do bypass the so called killswitch," said Craig Williams, senior technical leader and global outreach manager at Cisco Talos. Those new variants are not yet spreading, however.

Many computers also still contain the weaknesses exploited by the ransomware crooks. According to Graham, a scan a week ago revealed as many as 40,000 computers were infected with DoublePulsar, an NSA backdoor that was abused by WannaCry's coders. Earlier in April, researcher Dan Tentler said 1,724,749 were vulnerable to DoublePulsar attacks.

One major concern is that users will enter work with infected systems and spread the ransomware via the EternalBlue vulnerability, launching a fresh wave of attacks.

It's not today, but tomorrow, when people take their notebooks into work, auto connect to wifi, and ask IT to fix them. #wannacry

— Rob Graham٩(●̃̾●̃̾) (@ErrataRob) May 14, 2017

UPDATE Updated at 7.20am ET to note that Robert Graham has no comment on whether he has previously developed and sold exploits in a

private capacity.

Follow me on Twitter . Check out my website . Send me a secure tip .