New American

Written by C. Mitchell Shaw on May 15, 2017

Cyberweapon Used in Ransomware Attack Was Created By NSA

A massive cyberattack on computers around the world on Friday could — and should — have been prevented. The blame for the cyberattack — a "ransomware" attack — rests on the NSA and Microsoft. The NSA developed (and lost control of) the cyberweapon that was used. That cyberweapon works by exploiting unpatched vulnerabilities in Microsoft Windows — vulnerabilities Microsoft was aware of.

Ransomware works by encrypting all of the personal data files on a computer, making them inaccessible to the user unless he has the correct key to decrypt them. In a typical ransomware attack, the first indication the victim has of the attack is a warning that takes over his computer screen telling him that all of his files have been encrypted and that he must pay a ransom to the attacker to get the key. The ransom is only accepted in some type of untraceable currency — usually Bitcoin. It is also common for the attacker to give two deadlines. The first deadline is the day the demanded payment will go up — usually by at least 100 percent. The second deadline is the day the attacker will wipe all of his own files — including the keys to unlock the victim's files — and walk away. After that day, it would be impossible to recover the encrypted files.

While ransomware has been around since 1989, it has really gained notoriety only since about 2005. But even given the long history of ransomware and the large number of attacks over the past decade, this attack — known as "WannaCry" or "WannaCrypt" — has been described by Europol (the European Union police agency) as "unprecedented." It has infected nearly 250,000 computers in more than 150 countries as of this writing. The demands for Bitcoin ransom have been made in 28 languages.

The attack has crippled the computer systems of hospitals and other healthcare providers (including parts of Britain's National Health Service), transportation companies (including Deutsche Bahn and LATAM Airlines), courier delivery services (Including FedEx), telecommunication companies (including Telefónica), automobile manufacturers (including Renault) as well as other types of businesses. The damages are still being estimated, but will likely far exceed those of any attack to date.

The attack was carried out by using the ETERNALBLUE exploit developed by the NSA. ETERNALBLUE was leaked to the web as part of a campaign against the NSA in April by a hacker group calling itself The Shadow Brokers. ETERNALBLUE targets unpatched vulnerabilities in Microsoft Windows. The NSA had developed the cyberweapon and only made Microsoft aware of it in March — after the agency realized the weapon had been stolen.

Microsoft released a patch (MS17-010) for the vulnerability on March 14 — before The Shadow Brokers leaked ETERNALBLUE to the web to be downloaded by any hacker who wanted it. But — since Microsoft made the patch available only to either those using selected versions of Windows or those using other versions who had purchased an extended security agreement plan to provide security updates, the ransomware attack caught hundreds of thousands — if not millions — of victims

unprotected. After the attack, Microsoft released the patch for all Windows users running any version of Windows going back to Windows XP. But the patch is too little, too late; closing the barn door after the horse is out is not security.

This one cyberattack has caused ambulances to be rerouted, surgeries to be rescheduled, patients to be turned away from emergency rooms, manufacturers to halt production, airlines to cancel and reschedule flights, as well as a plethora of other problems involving everything from transportation to communications. And it all started when the NSA developing a cyberweapon to exploit a vulnerability in Microsoft Windows and was allowed to wreak havoc because Microsoft did not make the patch more widely available.

Microsoft's president and chief legal officer, Brad Smith, blames the whole thing on the NSA. In a blog post Sunday, Smith pointed out that the NSA built — and lost — the weapon used in the attack. He wrote, "An equivalent scenario with conventional weapons would be the US military having some of its Tomahawk missiles stolen," adding, "The governments of the world should treat this attack as a wake up call." Smith said that wake up call is a warning to governments and government agencies against hoarding vulnerabilities. He said those governments and agencies have a responsibility to report to manufacturers the vulnerabilities they discover.

And while Smith is correct as far as he goes, the fact remains that Microsoft did know about the vulnerability before the attack. In fact, Microsoft knew about it before the weapon was even leaked to the web. If Microsoft had made the patch available to all Windows users, instead of using patchable security vulnerabilities as selling points to convince users to upgrade to Windows 10, this attack could have been largely avoided.

Moving forward, there is little doubt that the same federal government that created — and lost — the weapon used in this attack will demand more power and authority over the Internet as a result of this attack. After all, it appears that one of their greatest pastimes is creating the poison and the antidote in the same laboratory.

This is a developing story and *The New American* will keep our readers updated as the story progresses.