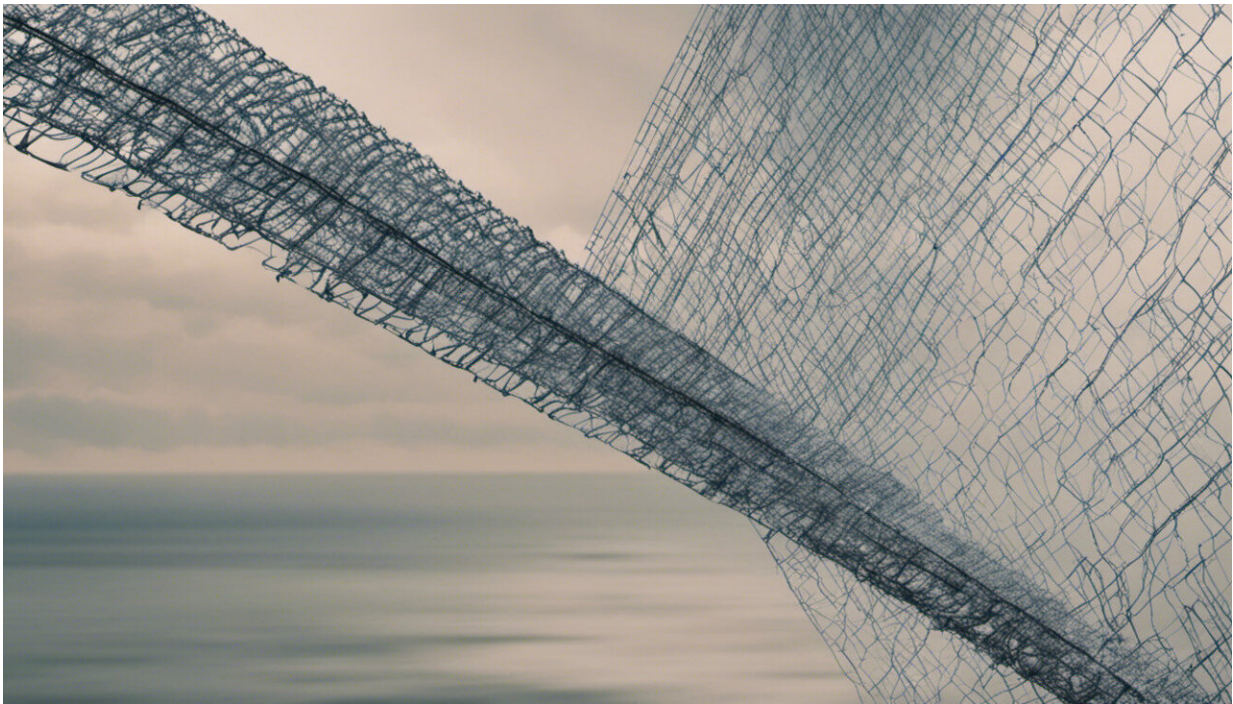


Shadow Brokers threaten release of more NSA hacks to be used against the world

May 17 2017, by David Glance



Credit: AI-generated image ([disclaimer](#))

As if dealing with the continuing drama of the WannaCry global ransomware attack was not enough, the original group behind the leak of National Security Agency ([NSA](#)) hacking tools has [announced](#) it will release more vulnerabilities that could be exploited in the near future.

The ShadowBrokers originally tried to [auction off](#) the NSA hacking tools, which they claimed were from a hacker group tied to the NSA, [Equation Group](#). After failing to get a bidder for the leaked files, the Shadow Brokers released a part of their horde in April 2017, some of which was subsequently incorporated into the WannaCry ransomware.

In the Shadow Broker's latest [posting](#), they have threatened to release even more tools in June. Having failed to get anyone interested in an auction however, the group is starting up what they call something like the "wine of month club": A subscription service where you get new exploits every month.

The exploits that the Shadow Brokers are threatening to pass on include vulnerabilities of browsers, mobile devices and Windows 10, as well as information about compromised banks and Russian, Chinese, Iranian and North Korean nuclear missile programs.

As a final offer, the Shadow Brokers have said that if someone buys the entire horde of data, they will "go dark permanently", having no financial incentive to continue.

Although nobody knows who the Shadow Brokers are, various theories point to either a disgruntled [insider](#) or a group with ties to Russia. In [another post](#), the Shadow Brokers identify themselves as disappointed supporters of US President Donald Trump. The ideals espoused in the post celebrate all that they believed Donald Trump stood for, "anti-globalism, anti-socialism, nationalism, isolationism" and racism.

In any event, it is likely that the exploits they have will find their way into the hands of groups who will in turn unleash them on the global public.

The only mitigating factor in this is that the NSA appears to have been

informing companies about different exploits and so allowing them to fix their products and issue updates to affected software and systems. It is likely that most, if not all of the outstanding exploits held by the Shadow Brokers, have already been fixed by Microsoft, Google, Apple and others.

Despite the availability of fixes, the exploits that the Shadow Brokers still have could lead to even more damage on a global scale. The fact that the WannaCry attack has persisted for so long indicates how many people globally refuse to update and protect their systems, despite the risks.

Part of the blame for this has to be laid at the feet of [people](#) who have advised the public to switch off automatic software updates – advice that has been [condemned](#) by cybersecurity experts.

Security is a balance of risk against cost and updates may seem like a painful ordeal, but the world is moving into an environment where this cost is nothing in comparison to the risks of doing nothing. Vendors do share part of the blame in not making these updates more seamless, but it may simply be impossible to do make updating completely painless for users.

In assessing risk, the public, companies and government are not always in a position to make informed decisions. Experts are still trying to understand the threats themselves without having sufficient time to explain them in simple terms to the public.

The lack of response from governments and security agencies has also not helped, especially in comparison to the involvement of private security companies and individuals trying to battle the attack as it unfolded.

When [22 year olds](#) are the heroes of the anti-cyber attack fight, rather than the agencies tasked to defend countries against these types of threats, it is perhaps time to question what these organisations have been doing all this time?

This article was originally published on [The Conversation](#). Read the [original article](#).

Provided by The Conversation

Citation: Shadow Brokers threaten release of more NSA hacks to be used against the world (2017, May 17) retrieved 18 April 2024 from <https://techxplore.com/news/2017-05-shadow-brokers-threaten-nsa-hacks.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.