GlobalResearch
Center for Research on Globalization

NSA Malware: Built Despite Warnings, Used in Global Cyber Attack

Disruptions reported in at least 74 countries, including Russia, Spain, Turkey, and Japan, with some reports of U.S. infiltration as well

By Nadia Prupis
Global Research, May 15, 2017
Common Dreams 12 May 2017

Region: USA
Theme: Intelligence

Apparent National Security Agency (NSA) malware has been used in a global cyber-attack, including on British hospitals, in what whistleblower Edward Snowden described as the repercussion of the NSA's reckless decision to build the tools.

> "Despite warnings, @NSAGov built dangerous attack tools that could target Western software. Today we see the cost," Snowden tweeted Friday.

At least two hospitals in London were forced to shut down and stop admitting patients after being attacked by the malware, which operates by locking out the user, encrypting data, and demanding a ransom to release it. The attacks hit dozens of other hospitals, ambulance operators, and doctors' offices as well.

The *Blackpool Gazette* in the northwest reported that medical staff had resorted to using pen and paper when phone and computer systems shut down. Elsewhere, journalist Ollie Cowan tweeted a photo of ambulances "backed up" at Southport Hospital as the staff attempted to cope with the crisis.

Other disruptions were reported in at least 74 countries, including Russia, Spain, Turkey, and Japan, and the number is "growing fast," according to Kaspersky Lab chief Costin Raiu. Security architect Kevin Beau said it was spreading into the U.S. as well.

The malware, which Microsoft tested briefly earlier this year, was leaked by a group calling itself the Shadow Brokers, which has been releasing NSA hacking tools online since last year, the *New York Times* reports.

Times journalists Dan Bilefsky and Nicole Perlroth wrote:

> Microsoft rolled out a patch for the vulnerability in March, but hackers apparently took advantage of the fact that vulnerable targets—particularly hospitals—had yet to update their systems.
>
> The malware was circulated by email. Targets were sent an encrypted, compressed file that, once loaded, allowed the ransomware to infiltrate its targets.

Reuters reported that the National Health Service (NHS), England's public health system, was warned about possible hacking earlier in the day, but that by then it was already too late.

A Twitter account with the handle @HackerFantastic, the co-founder of the cyber security company Hacker House, tweeted that the firm had

> "warned the NHS with Sky news about vulnerabilities they had last year, this was inevitable and bound to happen at some stage."

> "In light of today's attack, Congress needs to be asking @NSAgov if it knows of any other vulnerabilities in software used in our hospitals," Snowden tweeted. "If @NSAGov had privately disclosed the flaw used to attack hospitals when they *found* it, not when they lost it, this may not have happened."

Disclosing the vulnerability when it was found would have given hospitals years, not months, to update their systems and prepare for an attack, he added.

Twitter user @MalwareTechBlog added,

> "Something like this is incredibly significant, we've not seen P2P spreading on PC via exploits at this scale in nearly a decade."

Patrick Toomey, a staff attorney with the American Civil Liberties Union's (ACLU) National Security Project, said,

> "It would be shocking if the NSA knew about this vulnerability but failed to disclose it to Microsoft until after it was stolen."
>
> "These attacks underscore the fact that vulnerabilities will be exploited not just by our security agencies, but by hackers and criminals around the world," Toomey said. "It is past time for Congress to enhance cybersecurity by passing a law that requires the government to disclose vulnerabilities to companies in a timely manner. Patching security holes immediately, not stockpiling them, is the best way to make everyone's digital life safer."

This work is licensed under a Creative Commons Attribution-Share Alike 3.0 License.

The original source of this article is Common Dreams
Copyright © Nadia Prupis, Common Dreams, 2017

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Nadia Prupis

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca