

'Petya' ransomware attack goes global, targets Merck in US

Published time: 27 Jun, 2017 16:42 Edited time: 27 Jun, 2017 18:36

link: <https://www.rt.com/usa/394294-ransomware-attack-petya-merck/>

The US-based division of the global pharmaceutical giant Merck has been hit by the 'Petya' ransomware attack that has crippled computer systems across the world on Tuesday.

"We confirm our company's computer network was compromised today as part of global hack," Merck said in a statement on Tuesday. "Other organizations have also been affected. We are investigating the matter and will provide additional information as we learn more."

We confirm our company's computer network was compromised today as part of global hack. Other organizations have also been affected (1 of 2)

— Merck (@Merck) June 27, 2017

"The company is currently experiencing a hostile ransomware attack on its network systems," said an internal Merck memo quoted by the Philadelphia Inquirer. *"While IT risk management and global security respond to this threat please remain calm."*

Merck employees were instructed to disconnect all mobile devices from the company network and advised not to speak to reporters or post messages on social media accounts.

Computers at Merck facilities in Pennsylvania and New Jersey locked up Tuesday morning around 8am local time, according to the Inquirer.

The ransomware attack reportedly began in Ukraine, but has since spread to corporate systems across the world, affecting the Russian state oil giant Rosneft, the international shipping and energy conglomerate Maersk, and the UK-based advertising and public relations company WPP, among others.

"We can confirm that Maersk IT systems are down across multiple sites and business units. We are currently asserting the situation," the company said. pic.twitter.com/iixDbTkfP5

— Maersk (@Maersk) June 27, 2017

Group IB, a Moscow-based cyber security company, said that hackers used a cryptolocker called "Petya," which blocks access to computers and displays a message demanding a \$300 ransom payable in bitcoin.

#Petya uses long #sleep functions: if infected you have 30-40 mins to turn off your computer to save it from ransom. #infosec#WannaCryp [pic.twitter.com/BNG7Nthhbt](https://twitter.com/BNG7Nthhbt)

— Group-IB (@GroupIB_GIB) June 27, 2017

The ransomware is similar in impact to "WannaCry," a code derived from the US National Security Agency (NSA) and posted online by the hacker group ShadowBrokers. A WannaCry ransomware attack shut down over 200,000 computers globally in May.

Just talked with Group IB expert in cybercrime who said there's no evidence yet that Petya hack used leaked NSA tools.

— Andrew Roth (@ARothWP) June 27, 2017

No one has claimed responsibility for this latest attack.