Dangerous malicious code, capable of self-mutating, attacking the vaccine manufacturing industry

A dangerous type of malicious code, capable of mutating itself to avoid security software, is attacking vaccine manufacturing and supply companies globally.

This type of malware, targeting computers using the Windows operating system, was discovered by security researchers from the Information Sharing and Analysis Center (ISAC), a non-profit organization specializing in detecting and detecting report network security threats and threats.

ISAC named this malicious code Tardigrade (water bear), referring to its ability to survive long-term by mutating itself to bypass security software, similar to water bears, microorganisms capable of ability to live in extremely harsh environments and even in a vacuum.

Many security experts are concerned that malicious code can attack and disrupt the global production and supply chain of Covid-19 vaccines (Artwork: WHO).

Security experts warn that Tardigrade can be spread through phishing emails, infecting via USB, external storage devices . after infecting computers, this type of malicious code can secretly take over the right to control the system to steal the data contained on it or encrypt, change the content of the data.

ISAC first discovered Tardigrade earlier this year, when this malicious code attacked BioBright, a biotech company based in Massachusetts (USA). ISAC then continuously monitored this malicious code and noticed signs that Tardigrade was targeting biotech companies and companies that manufacture and supply vaccines globally.

Currently, ISAC has not been able to identify the culprit behind this dangerous malware, but based on the sophisticated and dangerous way of operating, this organization believes that it is likely that the Tardigrade malware has government backing. a certain country.

To prevent the infection of Tardigrade malware, ISAC security experts call on biotech companies and companies in the supply chain, producing vaccines - which are the targets of this malicious code. targeted, should use security software capable of identifying viruses through analysis of malware behavior; At the same time, prevent attacks via phishing emails to avoid infection with this dangerous code.

Many security experts are concerned that malicious code attacking the vaccine production and supply chain could disrupt the production and supply of vaccines, thereby affecting the fight against the Covid-19 pandemic. Currently, vaccines are still considered the most important "weapon" to repel the pandemic.