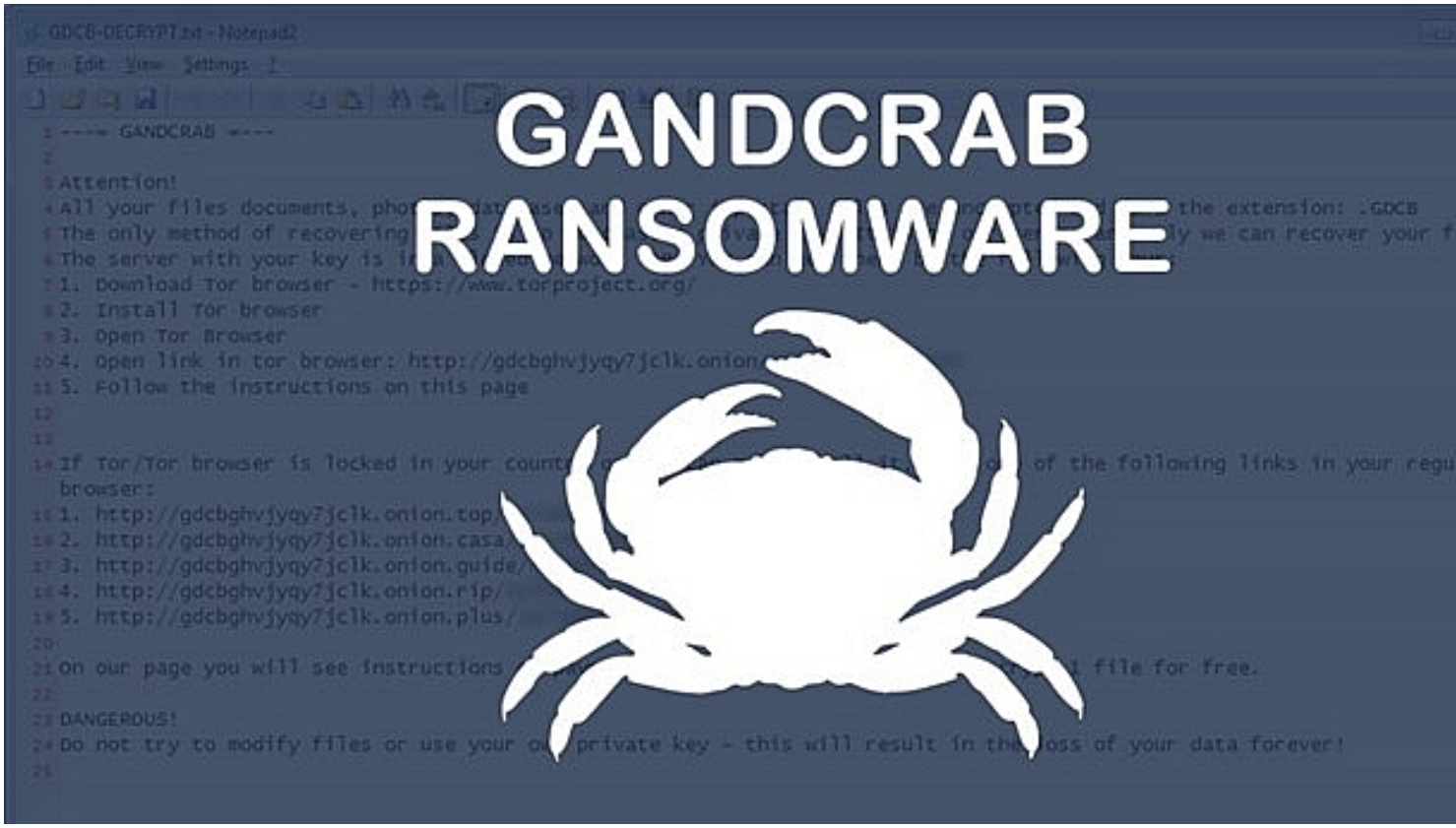
A large number of Vietnamese businesses are in distress after ransomware GandCrab attacked their computers, demanding a ransom of $400-1,000.



Ransomware GandCrab requires victims pay money for decrypted data

On April 5, the Vietnam Computer Emergency Responses Teams (VNCERT) sent a document to many telecom, internet, electric power, aviation, transport, and financial enterprises, about the spread of a ransomware virus called GandCrab. The malicious software has been detected in many countries, including Vietnam, and has been designated as more dangerous than the previous WannaCry virus.

In the morning of April 6, Kim Ngoc, an employee of an IT company in Ho Chi Minh City's District 4, confirmed that she received VNCERT's announcement from the company's IT

department.

“This alarm is very important to our company, which is specialised in resolving data. Previously, thanks to being notified of WannaCry in time, the company suffered no damages,” Ngoc said.

GandCrab is a ransomware-type virus distributed using RigEK toolkit. Once inside the system, it encrypts most stored data and adds the “.GDCB” extension to the name of each compromised file. From this point, files become unusable. Immediately after the encryption, GandCrab generates a “GDCB-DECRYPT.txt” and places a copy in every existing folder to seize victims attention.

According to this .txt file, to decrypt data, victims have to pay $400-1,000 by e-currency Dash (similar to Bitcoin). However, according to independent security expert Pham Duc Hung, payment of the ransom may not ensure getting victims’ data back.

According to the recommendation, users should not open and click links or email attachments with extensions of “.doc,” “.pdf,” or “.zip” sent by strangers or acquaintances that include messages of illegible or unusual messages.

After receiving such an e-mail, individuals should report to the technical departments of their companies and organisations to prevent the virus from spreading to other computers and accessing protected systems such as IDS/IPS or the Firewall.

GandCrab was detected in late January this year and spread speedily through advertisements linking to websites hosting the malicious code and through emails.

According to newswire Bitdefender, GandCrab has spread to over 50 million computers globally. Currently, various antivirus software have been developed against this ransomware-type virus.

At the latest seminar titled “Security World 2018” on April 5, director of the Ministry of Public Security (MoPS)’s Internet Security Department, Hoang Phuoc Thuan, affirmed that ransomware viruses are becoming common in Vietnam, according to vnexpress.net.

“Hackers do not stop at small-scale attacks, but also organise large-scale and systematic campaigns,” said Thuan.

In May last year, ransomware-type viruses became a global obsession, especially after WannaCry spread to over 150 countries, including Vietnam. This virus attacked over 250 businesses and over 1,900 computers in Vietnam.

Source: **VietNamNet**