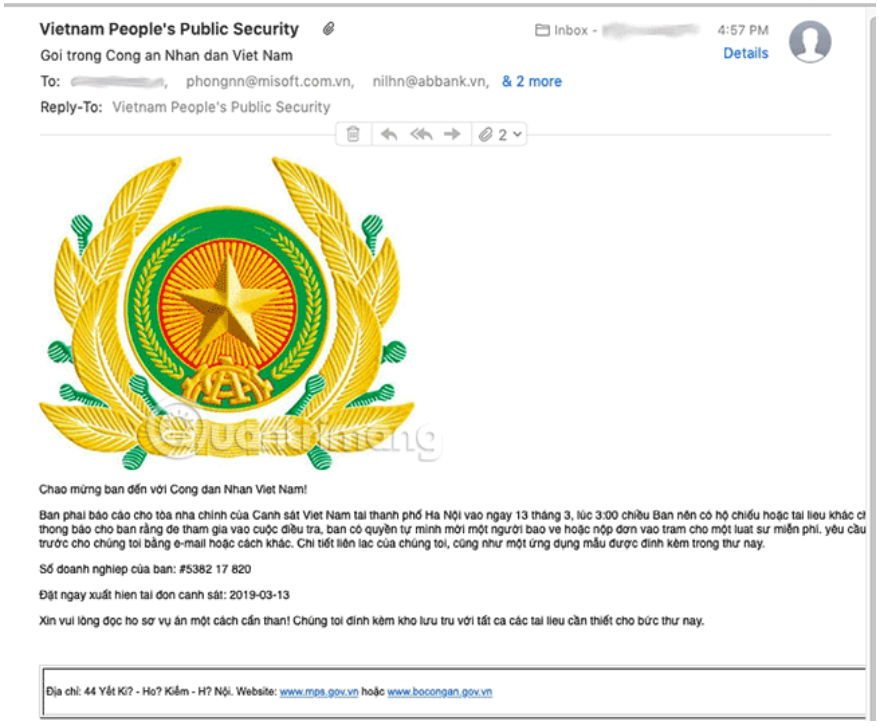
Warning: Detecting a campaign to spread malicious code GandCrab 5.2 into Vietnam via fake email of the Ministry of Public Security

Vietnam Computer Emergency Response Center (VNCERT) has sent a dispatch to member units informing that there is a campaign to distribute malicious code to extort GandCrab 5.2 into Vietnam and Southeast Asian countries. .

Today (March 15), the Vietnam Computer Emergency Response Center (VNCERT) has sent a dispatch to member units to announce that there is a campaign to distribute malicious code GandCrab 5.2. into Vietnam and Southeast Asian countries.

The campaign to spread malicious code GandCrab 5.2 when entering Vietnam spread via phishing email Vietnam Ministry of Public Security with the title 'Go in Vietnam' has attached the file 'documents.rar'.



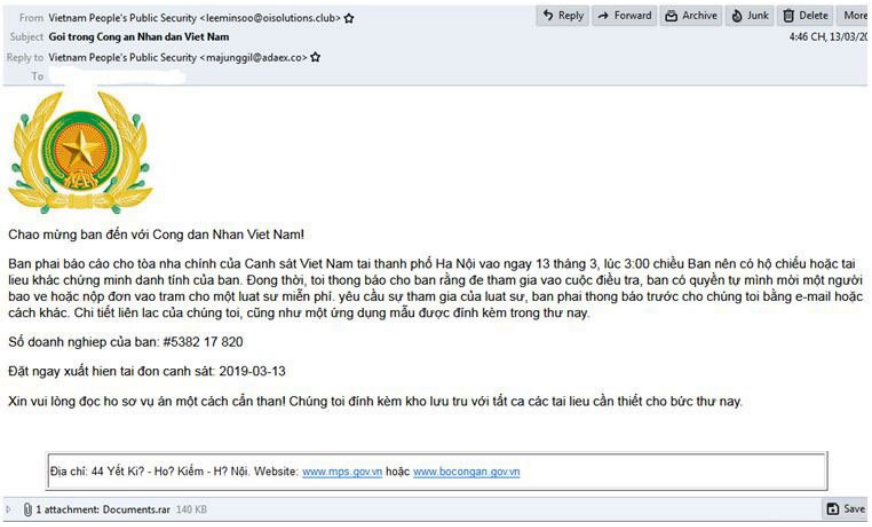
TipsMake.com's email containing the malicious code GandCrab received.

.Rar file attached to the end of the email

For over a year, GandCrab extortion code has spread globally. GandCrab 5.2 is a new version of this dangerous extortion family.

VNCERT once discovered that version 1.0 and 2.0 of malicious code GandCrab attacked Vietnam in April 2018 and issued a command to coordinate requests of agencies, units and enterprises to prevent malicious server connection GandCrab. Currently, VNCERT is still supporting decoding GandCrab version 5.1 and earlier.

If the user opens the mail, unzip and open the malicious attachment that will be activated. It will encrypt the entire user's data and a new file will be generated and instruct the user to pay the ransom to decrypt the data. The ransom is paid via electronic currency and is priced from 400 USD - 1,000 USD.



Malware to extort GandCrab 5.2 is distributed via fake email of the Ministry of Public Security of Vietnam.(Photo: VNCERT).

In the new command of coordinated fire rescue coordination, VNCERT Center requires the management units to monitor and prevent connections to servers that control the extortion of GandCrab malicious code and update the systems. Protection systems such as IDS / IPS, Firewall . according to the identification information in the table below to prevent and prevent the attack of malicious code GandCrab 5.2 in Vietnam.

TT	Địa chỉ C&C	Ghi chú
1	www.kakaocorp.link (IP:107.173.49.208)	Phiên bản 5.2

III. Danh sách mã băm.

	Địa chỉ C&C	Ghi chú
MD5	DDCA6B2B2623904A072A5AF0A9E26267	Phiên bản 5.2
SHA1	E081D35048E2DE07BE34C0EAD3B9FD16F6BADB74	Phiên bản 5.2

List of servers controlling GandCrab 5.2 extortion code and list of hash codes to monitor and prevent connections.

The dispatch also stated that if detected, it is necessary to quickly isolate the detected area / machine.

In order to prevent malicious code GandCrab 5.2, users need to improve their vigilance. Do not open and click links, .doc, .pdf, .zip, rar . attachments in emails sent from strangers or emails with strange titles sent from acquaintances. If detected or in doubt, please notify the system administration department.