CTCI 中鼎工程股份有限公司 CTCI Corporation

Notification object			
v	Vendors		
v	Customers		

Info. Security Notice

DATE : 12/Jun/2019
REV. : 0

Subject:

Be aware of fraud/phishing email

1. Description of Risk

CTCI recently received a notification of the security incident from our vendor, they got an email with malware as an attachment and the sender's email address is the same as one of CTCI's colleague. After investigation, it was confirmed that such emails were sent by the hacker to use the email address of the company's colleagues. It lures the recipient to open the file in the email or click on the link, then the malicious code can be executed.

Such an event may cause the user's computer to be controlled by the hacker, it may even cause data loss. In fact, this attack usually spread out through the intranet of one's company and lead heavy impact. To reduce the risk of such information security threats to partners and customers, CTCI publish this notice to remind your company to pay attention.

2. Prevention method

- When receiving an email with a file or link, it is recommended to confirm it before opening. For example, give a phone call to ask

Subject:

Be aware of fraud/phishing email

the sender has sent the email or not.

- Fraud/Phishing emails sent by attacker's hosts are usually blocked by the mail filtering system (SPAM filter). If your company have such a system, you can reduce the possibility of receiving fraud or phishing emails directly.