Incident handling: A suspicious e-mail communication

Exercise information

This exercise is based on the real work of incident handlers in IT corporations. The names, addresses, and other revealing details have been changed to preserve anonymity; however, the underlying nature of the assignment is realistic. A professional should handle this within 15 minutes; for others, it can take two to three times as much. You don't need any specialized tools, just critical analytical thinking.

Background and context

You are an incident handler, a member of a Computer Security Incident Response Team (CSIRT) in a major industrial software corporation called Big Company International, Inc. The company creates commercial and customer software products. It has more than 100,000 employees and a similar number of computers all over the world. You are one of 10 members of the incident handling team, which has to manually address 80 incidents daily, including antivirus alerts, IDS alerts, phishing reports, or suspicious e-mail conversations. All these incidents reported to the handlers are already processed by automated tools and evaluated as requiring human attention.

Bear in mind that regular employees and users are not security experts and have little understanding of what you do. Moreover, as the users are often in different time zones, it can take hours before they answer -- and they might not answer at all. Solving a single incident would then prolong from minutes to days. As a result, asking the user is not an option.

The task

Your colleague Peter Wilson forwarded the e-mail conversation below to you. It includes a PDF scan of the printed e-mail conversation between Irene Gonzales, who seems to be the employee of our company, and Li Zhang, who seems to be our business partner representative.

(Note: Yes, this actually happened. The business partner printed the e-mail conversation, scanned it, and sent it to your company to check it. So, forget about e-mail headers or anything you might extract from it.)

Another incident handler, Jack, scanned the PDF attachment for malware, examined the e-mail headers in the exchange between Peter and the business partner, and checked names of the people involved, and reported that everything seems fine. Jack is certain that Big Company International has an employee in the credit department named Irene Gonzales. However, neither him nor you are sure whether Li Zhang really is a business partner of yours and there is no quick way to find out.

Can you have a look at the e-mail and its PDF attachment to see if you smell something fishy? Or is this just a false alarm?

From: Peter Wilson <peter.wilson@bigcompany.com>
To: You <incident.response@bigcompany.com>
Sent: Friday, July 27, 2018 11:38 AM
Subject: FWD: [External] RE: Contact information

Hello,

Our business partner received the attached email and believed it was fraudulent.

Is this the normal form that goes out now?

Thanks

Peter

From: IT Partner <itpartnerco@gmail.com>
To: Peter Wilson <peter.wilson@bigcompany.com>
Sent: Friday, July 27, 2018 11:04 AM
Subject: [External] Re: Contact information

Dear Peter,

Please see attached email with irregularities.

Best regards,

Li Zhang

IT Partner Company

TEL: 123-456-7890

On Fri, Jul 27, 2018 at 8:27 AM, Peter Wilson <peter.wilson@bigcompany.com> wrote:

Hello,

Please send me the email you received from our accounting.

Thank you.

Peter Wilson
Sales Manager

Big Company International, Inc.
Phone 098-765-4321

peter.wilson@bigcompany.com