Security Soft Skills Scenario

**Send a machine for operating system reinstallation due to a serious malware infection.**

Contoso CIRT team provides remote security support for whole global company Contoso Ltd. An automated alert is generated for one of Contoso computers indicating presence of a malware. The incident takes place on a different continent in a time zone shifted by 6 hours, which makes direct communication with host owner (Natasha Romanoff) difficult.

Company security policy requires the host be completely reinstalled and any passwords are changed if a malware infection is detected. It means the user has to schedule an appointment with a member of local support IT staff and wait between one and two days for data backup and system reinstall. Generally, since malware infections are uncommon, users are not familiar with the process and CIRT is expected to provide instructions for them in the initial incident message.

It’s not surprising that the end user doesn’t want to spend up to two days of her daily work without a laptop/desktop. Usually, she attempts to mitigate the infection on her own with antivirus SW or by following recommendations found on Google. In this particular case, it is not the way the infection can be reliably removed, because the malware is known to use sophisticated rootkit techniques.

Infections are usually not end user’s fault and Contoso CIRT team understands that. Still, users often go to great lengths to make sure that no guilt is associated with them, even to the point of deliberately hiding relevant information or even providing false information to investigating security analysts.

Questions:

* Brainstorming – what information should be included in the initial message?
* If the user declines the proposal in the initial message (see reply from Natasha), what arguments and message style should be used for the subsequent response? How should be Natasha convinced to continue with reinstallation?
* When user’s manager intervenes, what arguments and message style should be used for the subsequent response to him?

Sample initial message:

*From: CIRT@contoso.com  
To: Natasha Romanoff  
Sent: Tuesday, May 20, 2014 9:30:18 AM GMT  
Subject: Cyber Incident Notification #007 on your host  
  
Security Operations Center has identified one or more security risks involving your system.*

*Natasha,*

*We have identified your system to be infected with a malicious software/virus, communicating with other infected systems over Internet.*

*Please contact your local IT support to have a technician perform all of the actions listed below. Please inform the technician that this request is coming from Contoso CIRT.*

* *Re-install the operating system using approved Contoso standard image.*
* *Update Windows and standard software (such as Java and Adobe Reader)*
* *Change all passwords used on the system, including personal passwords such as banking and web-mail.*

*Please notify us as soon as the service request has been completed, so that the incident mitigation can be validated and incident closed.*

*Best regards,*

*CIRT*

As it happens sometimes, user is reluctant to proceed according to the proposed plan, responding with:

*From: Natasha Romanoff   
To: CIRT@contoso.com  
Sent: Tuesday, May 20, 2014 11:24:12 AM GMT +2  
Subject: Re: Cyber Incident Notification #007 on your host*

*Dear Security Team,*

*Thank you for your information. I would like you to close the security incident you reported – my computer has just finished AVG scan. It deleted couple of files and shows no active infection now. I believe that this solution will help me to proceed with my daily work without the interruption you suggested.*

*Best regards,*

*Natasha*

If CIRT team pushes for reinstallation, user may request support from her manager:

*From: Nick Fury   
To: CIRT@contoso.com  
Cc: Natasha Romanoff  
Sent: Tuesday, May 20, 2014 15:14:28 AM GMT +2  
Subject: Re: Cyber Incident Notification #007 on your host*

*Dear Security Team,*

*Natasha is working on an important project that requires her full focus and cannot be interrupted for now. I will make sure that her computer is fixed after the project is closed.*

*Regards,*

*Nick*

CIRTs situation is complicated with long physical distance and user’s initial unwillingness to remediate the intrusion. CIRT members should understand that their request is disrupting for users. Messages from CIRT should always stay firm, but also objective and polite – while on one hand any kind of threats both open and hidden is absolutely unacceptable, on the other hand accepting user’s suggestions is a bad practice from the security point of view. Also, any message that may be interpreted that the user is (partially) responsible for the infection, may trigger a self-defense actions on the user’s side, which would make any future communication much more difficult and also would negatively impact CIRT’s reputation among user’s colleagues.

The strongest argument that CIRT has is that company security policy clearly supports their request. Also, a concise explanation why a simple antivirus scan is insufficient may convince the user to comply. Helpful may be also to objectively point out dangers of working on an infected host, such as data theft, data deletion or further malware spreading through the organization.

Intervening manager may have a position high enough to enforce his will. In such situation, CIRT should clearly communicate risks associated with keeping infected computer in the company network, should push for a clearly defined date when system will be reinstalled and should actively seek if the reinstallation took place. Messages towards management may also be a slightly more polite and descriptive.

And it is never wrong to say “Thank you” and send regards ;-)

Authors’ comment:

Cílem aktivity je opět ukázat, že esenciální skill pro bezpečáka je umět dobře psát maily, aby to user pochopil na první dobrou a neměl tendenci odporovat a celý proces prodlužovat (takových lístku Incident responder řeší třeba 15 denně).

Ukazuje, že user může být (1) v jiné časové zoně, (2) hrozně busy a v hierarchii na mnohem vyšším postu než bezpečák. (3) daleko od nejbližší corporatní site, kde mu to přeinstalují. (4) Jeho manager se za něj postaví. (5) Ten dotyčný se cítí, že trochu IT rozumí a vygooglí si řešení (typicky nějaký cleaner) a pak se s vámi hádá, že si problém vyřešil sám a nechce nechat počítač reinstalovat.

Authors: Václav Lorenz, Vít Bukač, 2017