INCIDENT RESPONSE METHODOLOGY

IRM #14
SCAM INCIDENT RESPONSE

Guidelines to handle fraudulent scam incidents

IRM Author: CERT SG
Contributor: CERT aDvens
IRM version: 2.0
E-Mail: cert.sg@socgen.com
Web: https://cert.societegenerale.com
Twitter: @CertSG

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue.

WHO SHOULD USE IRM SHEETS?

- Administrators
- Security Operation Center
- CISOs and deputies
- CERTs (Computer Emergency Response Team)

Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident Response team or CERT immediately if needed.

→ IRM CERT SG: https://github.com/certsocietegenerale/IRM

→ IRM CERT aDvens (French version): https://github.com/certadvens/IRM

INCIDENT HANDLING STEPS

6 STEPS ARE DEFINED TO HANDLE SECURITY INCIDENTS

1. Preparation: get ready to handle the incident
2. Identification: detect the incident
3. Containment: limit the impact of the incident
4. Remediation: remove the threat
5. Recovery: recover to a normal stage
6. Lessons learned: draw up and improve the process

IRM provides detailed information for each step of the incident response process. The steps come from NIST Computer Security Incident Handling Guide.

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

- Create a list of all legitimate domains belonging to your company. This will help analyzing the situation and prevent you from starting a takedown procedure on a "forgotten" legitimate website.
- Prepare one web page hosted on your infrastructure, ready to be published anytime, to warn your customers about a large ongoing fraudulent scam attack. Prepare and test a clear deployment procedure as well.
- Prepare takedown e-mail forms. You will use them for every fraudulent scam case, if possible, in several languages. This will speed up things when trying to reach Internet operating companies during the takedown process.
- Have several ways to be reached in a timely manner (24/7 if possible):
  - E-Mail address, easy to remember for everyone (ex: security@yourcompany)
  - Web forms on your company's website (location of the form is important, no more than 2 clicks away from the main page)
  - Visible Twitter account
- Deploy DKIM, DMARC and SPF to all mail chain.

Contacts

- Maintain a list of all people accredited to take decisions on cybercrime and eventual actions regarding the topic. If possible, establish a contract with clear processes.
- Establish and maintain a list of takedown contacts in:
  - Hosting companies
  - Registrars
  - Registry companies
  - E-Mail providers
- Establish and maintain contacts in CERTs worldwide, they will probably always be able to help if involved.

Raise customer awareness

Don't wait for scam incidents to communicate with your customers. Raise awareness on several kinds of scamming fraud (lottery scam, 419 scam etc.), explain what it is and make sure your customers know you won't ever contact them for such matters by e-mail.

IDENTIFICATION

OBJECTIVE: DETECT THE INCIDENT, DETERMINE ITS SCOPE, AND INVOLVE APPROPRIATE PARTIES.

Warning: Have a dedicated corporate equipment to identify or exchange with the scammer, do not use your personal equipment.

Fraudulent scam detection

- Monitor all your points of contact closely (e-mail, web forms, etc.).
- Monitor cybersquatted domains and content posted on them. Gather contact and abuse information to be prepared in the case you need to use them.
- Monitor social media accounts usurping your top management or your trademark.
- Deploy spam traps and try to gather spam from partners/third-parties.
- Deploy active monitoring of scam repositories, like 419scam for example.
- Monitor any specialized mailing-list you can have access to, or any RSS/Twitter feed, which could be reporting scam letters.

Use automated monitoring systems on all these sources, so that every detection triggers an alarm for instant reaction.

Involve appropriate parties

- As soon as a scam campaign is detected, contact the people in your company who are accredited to take a decision, if not you.
- The decision to act on the fraudulent e-mail address must be taken as soon as possible, within minutes.

Collect evidence

Get samples of the fraudulent e-mails sent by the fraudsters. Be careful to collect the e-mail headers in addition to the e-mail content. Collect several e-mails, if possible, to check for the real sender's IP address. This will help the investigation, analyzing if the campaign is sent from one machine or from a botnet.

If you feel unsafe about collecting e-mail headers, please check http://spamcop.net/fom-serve/cache/19.html

CONTAINMENT

OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

- Spread the fraudulent e-mail content on spam/fraud reporting websites/partners/tools.
- Communicate with your customers.
- Add the URLs in your Blackhole DNS, proxies and firewall's blocklist.

Deploy the alert/warning page with information about the current scam attack if the brand is impacted.

In case you are impacted several times a week, don't always deploy an alert/warning message but rather a very informative page about scam, to raise awareness.

REMEDIATION

OBJECTIVE: TAKE ACTIONS TO REMOVE THE THREAT AND AVOID FUTURE INCIDENTS.

- In case there is a fraudulent web page related to the fraud, hosted on a compromised website, try to **contact the owner of the website**. Explain clearly the fraud to the owner, so that he takes appropriate actions: remove the fraudulent content, and most of all upgrade the security on it, so that the fraudster cannot come back using the same vulnerability.
- In any case, and specifically if the scam page is hosted on a cybersquatted domain, also **contact the hosting company of the website**. Send e-mails to the contact addresses of the hosting company (generally there is an abuse@hostingcompany) then try to get someone on the phone, to speed things up.
- **Contact the e-mail hosting company** to shut down the fraudulent account of the fraudster. Don't forget to send them a copy of the fraudulent e-mail.
- **Contact social media abuse team** to takedown fraudulent accounts.
- **Block email exchange** with this company or person.

In case you get no answer, or no action is taken, **call back and send e-mails on a regular basis**.

If the takedown is too slow, **contact a local CERT in the involved country**, which could help taking down the fraud, and explain them the difficulties you face.

RECOVERY

OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.

Assess the end of the case

- Ensure that the fraudulent e-mail address has been shut down.
- If there is any fraudulent website associated to the fraud, keep monitoring it.
- At the end of a fraudulent scam campaign, remove the associated warning page from your website.

For more details on authentication and infrastructure recovery, check the Large-scale malware compromise IRMXXX

LESSONS LEARNED

OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

Report

A crisis report should be written and made available to all of the actors of the crisis management cell.

The following themes should be described:

- Initial cause of the infection
- Actions and timelines of every important event
- What went right
- What went wrong
- Incident cost
- Indicators of compromise

Capitalize

- Consider what preparation steps you could have taken to respond to the incident faster or more efficiently.
- Update your contacts-lists and add notes as to what is the most effective way to contact each involved party.
- Consider what relationships inside and outside your organization could help you with future incidents.
- Improve DKIM, SPF and DMARC filters.
- Collaborate with legal teams if a legal action is required.