INCIDENT RESPONSE METHODOLOGY

IRM #13 CUSTOMER PHISHING INCIDENT RESPONSE

Guidelines to handle customer phishing 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/cert-advens/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 an ongoing phishing attack. Prepare and test a clear deployment procedure as well.
- Prepare takedown e-mail forms. You will use them for every phishing case, if possible, in several languages. This will speed up things when trying to reach the hosting company etc. during the takedown process.
- Deploy DKIM, DMARC and SPF to all mail chain.
- Monitor cybersquatted domains and content posted on them. Gather contact and abuse information to be prepared in the case you need to use them.

Internal contacts

- Maintain a list of all people involved in domain names registration in the company.
- Maintain a list of all people accredited to take decisions on cybercrime and eventual actions regarding phishing. If possible, have a contract mentioning you can take decisions.

External contacts

- 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
- Establish and maintain a list of takedown contacts in:
  - Hosting companies
  - Registry companies
  - E-Mail providers
- Establish and maintain contacts in CERTs worldwide, they will probably always be able to help if needed.

PREPARATION

Raise customer awareness

Don’t wait for phishing incidents to communicate with your customers. Raise awareness about phishing fraud, explain what phishing is and make sure your customers know you won’t ever ask them for credentials/banking information by e-mail or on the phone.

Raise business line awareness

People in business lines must be aware of phishing problems and consider security as a priority. Therefore, they should apply good practices such as avoid sending links (URL) to customers and use a signature stating that the company will never ask them for credential/banking information online.

IDENTIFICATION

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

Phishing Detection

- Monitor all your points of contact closely (e-mail, web forms, etc.).
- Deploy spam traps and try to gather spam from partners/third-parties.
- Deploy active monitoring of phishing repositories, like PhishTank and Google Safe Browsing for example.
- Monitor any specialized mailing-list you can have access to, or any RSS/Twitter feed, which could be reporting phishing cases.
- Use automated monitoring systems on all of these sources, so that every detection triggers an alarm for instant reaction.
- Monitor your web logs. Check there is no suspicious referrer bringing people to your website. This is often the case when the phishing websites brings the user to the legitimate website after he's been cheated.

Involve appropriate parties

As soon as a phishing website 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 website/e-mail address must be taken as soon as possible, within minutes.

Collect evidence

Make a time-stamped copy of the phishing web pages. Use an efficient tool to do that, like HTTrack for example. Don't forget to take every page of the phishing scheme, not just the first one if there are several. If needed, take screenshots of the pages.

Check the source-code of the phishing website:

- See where the data is exported: either to another web content you cannot access (a PHP script usually), sent by e-mail to the fraudster or using an application API (like Telegram for example).
- Gather information about the phishing-actor which may be available in URI, source code and credential dropping system (email addresses, Telegram bots, etc).
- Do the graphics come from one of your legitimate websites, or are they stored locally?

If possible, in case the graphics are taken from one of your own websites, you could change the graphics to display a "PHISHING WEBSITE" logo on the fraudster's page.

CONTAINMENT

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

Spread the URL of the attack in case of a phishing website:

Use every way you have to spread the fraudulent URL on every web browser: use the options of Internet Explorer, Chrome, Safari, Firefox, Netcraft toolbar, Phishing-Initiative, etc.

This will prevent the users from accessing the website while you work on the remediation phase.

Spread the fraudulent e-mail content on spam-reporting websites/partners.

Communicate with your customers:

Deploy the alert/warning page with information about the current phishing attack.

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

REMEDIATION

OBJECTIVE: TAKE ACTIONS TO STOP THE PHISHING CAMPAIGN.

- In case the fraudulent phishing pages are 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, 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 accounts which receive the stolen credentials or credit card information (Either on an “e-mail only” phishing case or on a usual one, if you managed to get the destination e-mail address).
- In case there is a redirection (the link contained in the e-mail often goes to a redirecting URL) also **take down the redirection** by contacting the company responsible for the service.
- In case you get no answer, or no action is taken, don’t hesitate to **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.

RECOVERY

OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.

Assess the end of the phishing case

- Ensure that the fraudulent pages and/or e-mail address are down.
- Keep monitoring the fraudulent URL. Sometimes a phishing website can reappear some hours later. In case a redirection is used and not taken down, monitor it very closely.
- At the end of a phishing 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

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.
- Collaborate with legal teams if a legal action is required.