INCIDENT RESPONSE METHODOLOGY

IRM #16
PHISHING

Guidelines to handle and respond to phishing targeting collaborators

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

C'EST VOUS L'AVENIR

SOCIETE GENERALE

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.

- Prepare a communication, ready to be published anytime, to warn your collaborators about an ongoing phishing attack. Prepare and test a clear deployment procedure as well.
- Deploy DKIM, DMARC and SPF to all mail chain.
- Implement multi-factor authentication mechanisms.
- 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

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

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.

- Run periodic awareness phishing campaigns.

- Deploy a technical solution allowing collaborators to easily report email to security teams.
- Establish specific procedures for attachment and URL analysis.

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 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.

Phishing attack scoping

- Determine the number of targeted users.
- Search for exploited compromised accounts and identify related malicious activities.

Analyze the phishing

Remember to follow established analysis procedures

- Determine:
  - If it is a credential harvesting campaign or a malware spreading campaign
  - If it is a targeted campaign or not
- Inspect message subject and body.
- Use sandbox environment to analyse malicious attachments and extract IOCs.
- Analyse links, domain and hostnames with threat intelligence services.
- Check the source-code of the phishing website.
- Investigate email headers for interesting artifacts: originated server and sender information for example.

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.

If the phishing campaign is distributing a malware, you should refer to IRM 7 WindowsMalwareDetection.

CONTAINMENT

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

- Block network IOCs discovered via the attachment / URL analysis on DNS, firewalls, or proxies.
- Block the phishing campaign based on senders, subjects, or other email artifacts via email gateway.
- Try to delete phishing emails from inbox.
- Apply DNS Sinkhole on the suspicious URL (optional depending on DNS architecture).
- Communicate with your collaborators.
- Deploy the alert/warning page with information about the current phishing attack.

REMEDIATION

OBJECTIVE: TAKE ACTIONS TO STOP THE PHISHING CAMPAIGN.

- Change and/or block temporarily login credentials of compromised accounts.

If the phishing campaign was targeted, consider contacting law enforcement and regulators.
You may consider contacting your local CERT.

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