INCIDENT RESPONSE METHODOLOGY

IRM #15 TRADEMARK INFRINGEMENT INCIDENT RESPONSE

Guidelines to handle and respond to trademark infringement 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

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.

- Maintain a list of all legitimate trademarks belonging to your company and its subsidiaries. This will help in assessing the situation at hand and prevent you from starting an infringement procedure on an outdated trademark, an unrelated legitimate website or social network account.
- Establish a thorough, evidence-based information list related to your trademarks to support your legal rights:
  - Name(s), legitimate domain names and social media accounts used by your company and its subsidiaries
  - Your trademarked words, symbols, taglines, graphics, etc.
  - Trademark registration numbers if applicable
  - International and federal/local trademark registration offices (USPTO, INPI, etc.) where registered trademarks have been labelled as such if applicable
  - Any other document establishing clearly that a trademark belongs to your company
- Prepare trademark infringement e-mail forms. You will use them for every trademark infringement case, if possible in several languages. This will help speed up things when trying to reach out the registrar, service provider and any other relevant party during the procedure.
- Promote a central domain management system using normalized WHOIS fields.
- Promote an ethical online advertisement to avoid appearing in parked domain names.
- Prepare takedown processes and templates with the legal team.
- Have process, experts, and technologies in place to manage the brand portfolio.
- Have a centralize process or repository to manage applicable brand names, IPs, domains, PII's, keywords, etc.

Internal contacts

- Maintain a list of all people involved in trademark registration in the company especially those part of the legal and PR departments.
- Maintain a list of all people accredited to take decisions on trademarks and eventual actions regarding trademark infringement. If possible, obtain a written agreement that gives you the ability to take this kind of decisions.

External contacts

- Establish and maintain a list of external contacts within registrars and service providers involved in trademark issues.

IDENTIFICATION

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

Trademark infringement Detection

- Deploy active monitoring of domain names registration through registries' zones updates whenever possible or brand alert services.

- Set up feeds to monitor usernames, pages and groups on social networks.
- Analyze HTTP referrers in website logs to identify fraudulent content downloads and fraudulent mirroring of your websites.
- Set up brand name monitoring with specialized search engines.
- Leverage automation whenever possible to trigger alarms and improve reaction times.
- Collect and analyze alerts from trusted partners.

Involve appropriate parties

- As soon as an infringement is detected, contact the people in your company who are accredited to take a decision if you haven't been empowered to do so on your own.

The decision to act on the fraudulent domain name, group or user account must be taken as soon as possible.

Collect evidence

- Collect evidence of infringing domain names, websites, specific URLs (e.g., Facebook vanity URL), pages, groups or account details.
- Make a time-stamped copy of the infringing material (page, group, blog, forum, micro-blogging timeline, etc.) and take screenshots if possible.

CONTAINMENT

OBJECTIVE: MITIGATE THE INFRINGEMENT EFFECTS ON THE TARGETED ENVIRONMENT.

Evaluate the impact of the trademark infringement:

- Can it be used for traffic redirection (cybersquatting, typosquatting, SEO)?
- Can it be used for spoofing, counterfeiting or scamming (cybersquatting with redirect to the corporate website)?
- Can it be used to slander the brand?
- Evaluate the visibility of the infringing component:
  - Website visibility (ranking).
  - Number of fans or followers on social medias.
- Monitor the dormant, infringing domain for signs of fraudulent activities.

Refer to IRM-13-Phishing and IRM-14-Scam for more information.

REMEDIATION

OBJECTIVE: TAKE ACTIONS TO STOP THE TRADEMARK INFRINGEMENT.

In most trademark issues, monitoring is usually sufficient. Remediation must be started only if there's an impact on your company or its subsidiaries.

Domain name

- Contact the domain name owner and hosting service provider to notify them of the trademark infringement and ask them to remove the fraudulent content.
- Contact the domain name registrar to notify them of the trademark infringement and ask them to deactivate the associated domain name or to transfer it to you.
- Ask the domain name owner or registrar to redirect all DNS requests to your name servers if possible.
- If neither the domain name owner nor the registrar complies with your requests, initiate a Uniform Domain-Name Dispute-Resolution Policy (UDRP) procedure if you are empowered to do so or ask the internal contacts to conduct it.

Social network account

- Contact the service provider of the infringing page, group or account to notify them of any violation of their Trademark Policies or Terms of Service and ask them to deactivate the infringing account.
- Ask the service provider to transfer the trademarked account to an existing company account if possible.

In both cases, send e-mails to the contact addresses of the registrar or service provider. There's generally an e-mail address to report abuse, legal or copyright issues.

Fill out a trademark or abuse complain form if available.

RECOVERY

OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.

Assess the end of the infringement case

- Ensure that the infringing domain name, page, group or account are down or redirected to your company.
- Keep monitoring the infringing domain name, page, group or account. Sometimes a website can reappear later.
- Consider acquiring the infringing domain name if available.

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.