# malware.lu CERT

# CSIRT service presentation

## General information

| | |
|---|---|
| **Type** | Standard |
| **Sequence number** | C002 |
| **Version** | 1.2 |
| **State** | Final |
| **Approved by** | C. Harpes |
| **Date** | 27/02/2017 |
| **Classification** | Public |

# Distribution list

Changes to this document are not distributed by a mailing-list, RSS or any other mechanism. Please address any specific questions or remarks to malware.lu CERT e-mail address (see paragraph 1.6).

# Document history

| Version | Date | Modifications |
|---|---|---|
| **0.1 – 0.3** | 27/05/2013 | Document creation & validation |
| **1.0** | 18/06/2013 | Document approval by C. Harpes |
| **1.1** | 02/04/2014 | Document update (Ch. 1.9 - Team members) & validation by M. Morin & C. Harpes |
| **1.1.1** | 03/08/2016 | Document update by N. Kasselouris |
| **1.1.2** | 18/11/2016 | Document update by N. Kasselouris |
| **1.1.3** | 21/12/2016 | Document update by C. Muller, review of itrust consulting look'n'feel |
| **1.1.4** | 18/01/2017 | Document update by T Mouelhi (fixing address and PGP key location) |
| **1.1.5** | 20/02/2017 | Document review by C. Muller |
| **1.1.6** | 21/02/2017 | Document update by T. Mouelhi |
| **1.2** | 27/02/2017 | Validation by C. Harpes |

# Working group

| Name | Organisation |
|---|---|
| C. Muller, N. Kasselouris, T. Mouelhi, C. Harpes | itrust consulting |

# Approbations

| Name | Role | Responsibility | Date | Signature |
|---|---|---|---|---|
| N. Kasselouris | Head of ethical hacking | Content agreement | 27/02/2017 | See printed version managed by CISO |
| C. Muller | CISO | Quality agreement | 27/02/2017 | See printed version managed by CISO |
| C. Harpes | Managing Director | Applicability | 27/02/2017 | See printed version managed by CISO |

# Locations where this document may be found

The current version of this CSIRT description document is available from the malware.lu website; its URL is http://www.malware.lu.

# Acronyms

| Acronym | Definition |
|---|---|
| **CERT** | Computer Emergency Response Team. |
| **CSIRT** | Computer Security Incident Response Team. |
| **PGP** | Pretty Good Privacy. |
| **RSS** | Rich Site Summary. |
| **SMS** | Short Message Service. |

# Table of contents

# 1 Contact information

## 1.1 Name of the team

malware.lu CERT

## 1.2 Address

itrust consulting s.à r.l.
55 rue Gabriel Lippmann
L-6947 Niederanven
Luxembourg

## 1.3 Time zone

Central European Time / Central European Summer Time

## 1.4 Telephone number

+352 26 176 212

## 1.5 Other telecommunication

- Twitter (@malwarelu)
- Internet Relay Chat (server: irc.freenode.net, channel: #malware.lu)

## 1.6 Electronic mail address

Incident reports (including non-incident) related mail should be addressed to cert@malware.lu.

## 1.7 Public keys and other encryption information

malware.lu CERT has a PGP public key, which Key ID is 0xC8F71EEB.

The public key and its signatures can be found at the usual large public key servers, or on malware.lu's website, under:
https://malware.lu/assets/files/pgp/Malware.lu%20CERT%20(Computer%20Emergency%20Response%20Team)(C8F71EEB)pub.asc.

This key signs any communication from malware.lu CERT. It is also used for any confidential communication with malware.lu CERT (incident reports, alerts).

## 1.8 Team members

The team (in alphabetical order) is composed of:

| Name | E-mail | PGP Key-ID |
|---|---|---|
| **Nikolaos Kasselouris** | kasselouris (at) malware.lu | 0x05166C78 |
| **Rémi Chipaux** | chipaux (at) malware.lu | 0x6D35412A |
| **Sam Menghi** | menghi (at) malware.lu | 0x464A7FC7 |
| **Gazmend Ramadani** | ramadani (at) malware.lu | 0x5C1CFC3B |
| **Tejeddine Mouelhi** | mouelhi (at) malware.lu | 0x79E165A6 |
| **Gonzalo Matamala** | matamala (at) malware.lu | 0xD87CC0F0 |
| **Jean Lancrenon** | lancrenon (at) malware.lu | 0xE39C4D44 |
| **Benoit Jager** | jager (at) malware.lu | 0xE0A4E1BD |

## 1.9 Operating hours

malware.lu CERT hours of operation are restricted to: 08:00-18h00 CET Monday to Friday except during Luxembourg's public holidays.

## 1.10 Other information

Any other information about malware.lu CERT can be found at http://www.malware.lu

## 1.11 Points of customer contact

The preferred method for contacting malware.lu CERT is via e-mail at cert@malware.lu. We encourage our constituency (customers) to use PGP encryption when sending any sensitive information to malware.lu CERT.

If it is not possible (or not advisable for security reasons) to use e-mail, malware.lu CERT can be reached by telephone during regular office hours.

# 2 Charter

## 2.1 Mission statement

The missions of malware.lu CERT are to:

- Provide a systematic response facility to ICT-incidents;
- Support national ICT users to recover quickly and efficiently from security incidents;
- Minimise ICT incident-based losses, theft of information and disruption of services at a national level;
- Gather information related to incidents handling to better prepare future incidents management and provide optimised protection for systems and data;
- Coordinate communication among national and international incident response teams during security emergencies and to help prevent future incidents;
- Provide a security related alert and warning system for national ICT users;
- Foster knowledge and awareness exchange in ICT security.

## 2.2 Constituency

malware.lu CERT provides incident response to all kinds of organisations situated in Luxembourg.

## 2.3 Sponsorship and/or affiliation

malware.lu CERT is a private CSIRT. It is a brand and service defined, owned, and operated by itrust consulting s. à r. l.

Authority

malware.lu CERT is officially listed as a trusted introducer since 17 December 2012.

# 3 Policies

## 3.1 Types of incidents and level of support

malware.lu CERT addresses all types of computer security incidents which occur, or threaten to occur, in the constituency networks.

The level of support given by malware.lu CERT will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and malware.lu CERT's available resources. However, in all cases, some response will be made.

Incidents will be prioritised according to their apparent severity and extent.

End users are expected to contact their systems administrator, network administrator, or department head for assistance.

## 3.2 Co-operation, interaction and disclosure of information

malware.lu CERT exchanges all necessary information with other CSIRTs as well as with affected parties administrators.

All sensible data (such as personal data, system configurations, and known vulnerabilities with their locations) are encrypted if they must be transmitted over unsecured environment as stated below (see section 3.3).

## 3.3 Communication and authentication

itrust consulting "Information Exchange" procedure is applied:

- In view of the types of information that malware.lu CERT deals with, telephones will be considered sufficiently secure to be used even unencrypted;
- Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data;
- If it is necessary to send highly sensitive data (i.e. information classified as Confidential) by e-mail, encryption (preferably PGP) will be used;
- All e-mail or data communication originating from malware.lu CERT will be digitally signed, using the generic PGP key mentioned above, or the malware.lu CERT's team members own signature keys.

# 4 Services

## 4.1 Incident response

malware.lu CERT assists system administrators in handling the technical and organisational aspects of incidents. In particular, it provides assistance or advice with respect to the following aspects of incidents management:

### 4.1.1 Incident triage

- Investigating whether indeed an incident occurred;
- Determining the extent of the incident.

### 4.1.2 Incident coordination

- Determining the initial cause of the incident (e.g. vulnerability exploited, etc.);
- Facilitating contact with other sites which may be involved;
- Facilitating contact with appropriate law enforcement officials, if necessary;
- Making reports to other CSIRTs;
- Composing announcements to users, if applicable.

### 4.1.3 Incident resolution

- Helping to remove the vulnerability;
- Helping to secure the system from the effects of the incident;
- Collecting evidence of the incident.

In addition, malware.lu CERT collects statistics concerning incidents processed, and notifies the community as necessary to assist it in protecting against known attacks.

To make use of malware.lu CERT's services please refer to section 1.11 for points of contact. Please remember that amount of assistance will vary as described in section 3.1.

## 4.2 Proactive services

malware.lu CERT coordinates and maintains the following services to the extent possible depending on its resources:

- Information provision such as a list of security contacts, repository of malwares and technical analyses;
- Site security auditing and consulting.

Detailed information about obtaining these services is available from the malware.lu CERT website: http://www.malware.lu.

# 5 Incident reporting form

malware.lu CERT has created a local form designated for reporting incidents to the team. malware.lu CERT strongly encourages anyone reporting an incident to fill it out. The current version of the form is available from: https://malware.lu/assets/files/cert/STA_C005_Incident%20reporting%20form_v1.0.docx.

# 6 Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, malware.lu CERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.