Incident Response and Forensics

Overview and challenges

CIRCL
Computer Incident
Response Center
Luxembourg

CIRCL - *TLP:WHITE*

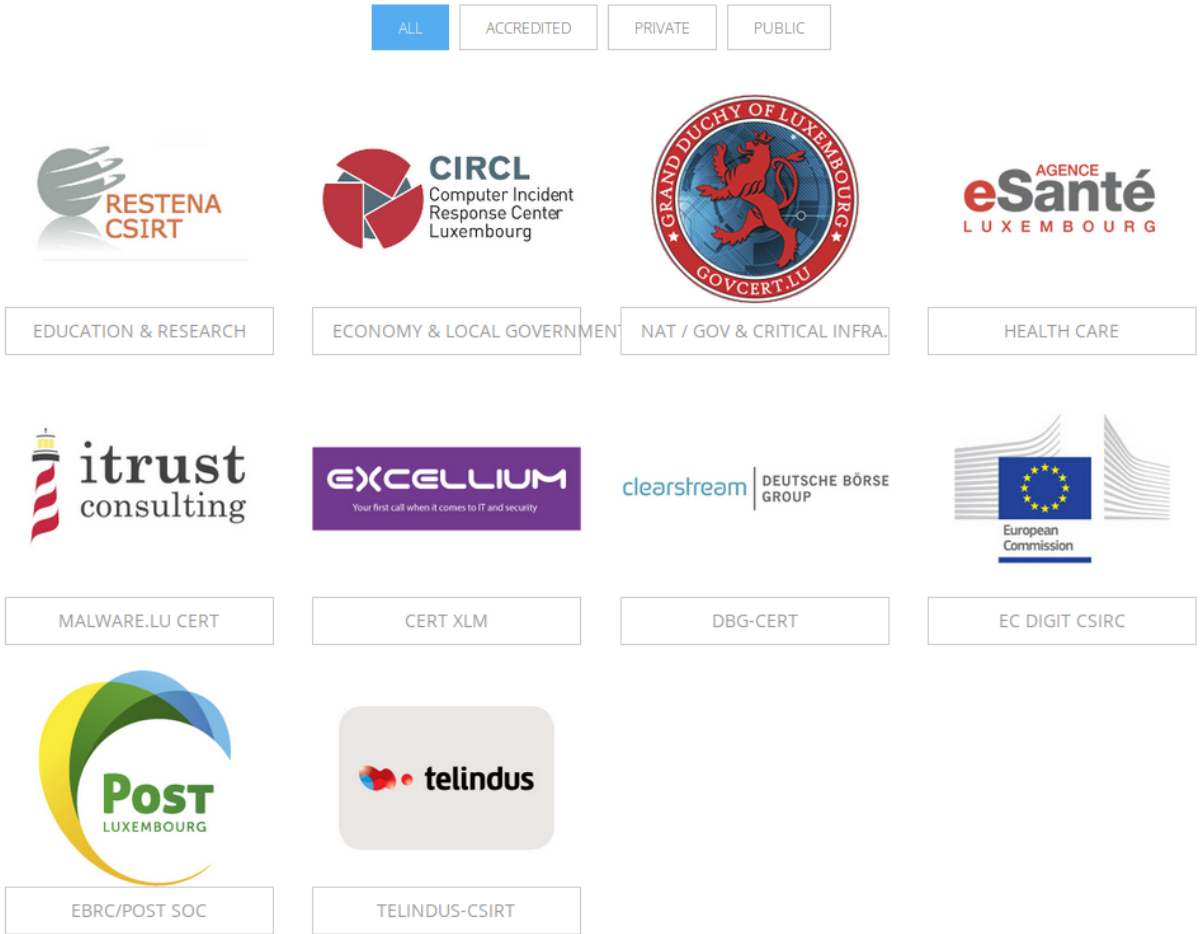
info@circl.lu

2019-10-17

CERT History

- Morris worm / Internet worm
  - 2. November 1988
  - Robert Tappan Morris
  - Exploiting: Finger, Sendmail, Passwords
  - Intention: Measure size of the Internet
  - Program bug $\rightarrow$ Denial of Service
  - Result: Internet down
- Mitigation challenges
  - Analyze malware
  - Identify vulnerabilities
  - Advisories
  - Provide/Get information
  - Point of contact
- Computer Emergency Response Team
  - Carnegie Mellon University

CERT.LU



Luxembourg CERT Landscape

CIRCL
Computer Incident
Response Center
Luxembourg

- The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents.

- CIRCL is the CERT for the private sector, communes and non-governmental entities in Luxembourg.

- Visit `https://www.circl.lu/` for projects and services

Proactive security & Incident detection

- Paste monitoring:

```
...
http://migXXXXX.lt/index.php?cPath=999999.9 union all select [t]
http://www.XXXX.lu/index.php?cat=999999.9 union all select 1,[t],3--&page=16&lang=fr
http://www.XXXX.lv/?id_p=news_al&id=999999.9 union all select 1,[t],3,4,5
http://XXXXXXX.org/view_cat.php?%20cat=999999.9 union all select [t],2
http://www.XXXXX.mu/info/?id=13' and [t] and '1'='1
...
```

- Leak Detection:

```
...
pascal.XXXX@club-internet.XX:tp100b
XXybakXXXXX@sbXXXXXX.net:sr15926
arbaXXXXXXX@XXXenet.XX:x-men1
angelbroXXX@XXXX.net:asb1061
atXXXXXXX75@hotmail.com:chelatitina
XXXXXXXXXXX@mil.be:hitler
adamgXXXXXX@yahoo.com:122179
michaeXXXXt@hotmail.com:misslittle
adamXXXXXXX@XXXXX.XX:aczcover
naseemXXXXX@gmail.com:doctor
jspaccarXXX@ciXXXXi.XX:raleigh1
edytXXXXXXX@02.pl:edyta71
...
```

Proactive security & Incident detection

- Reports and Advisories:

TR-54 - Sextortion scam emails - I know your password

Overview

During the past few days, we have received an increasing number of reports about scam attempts.

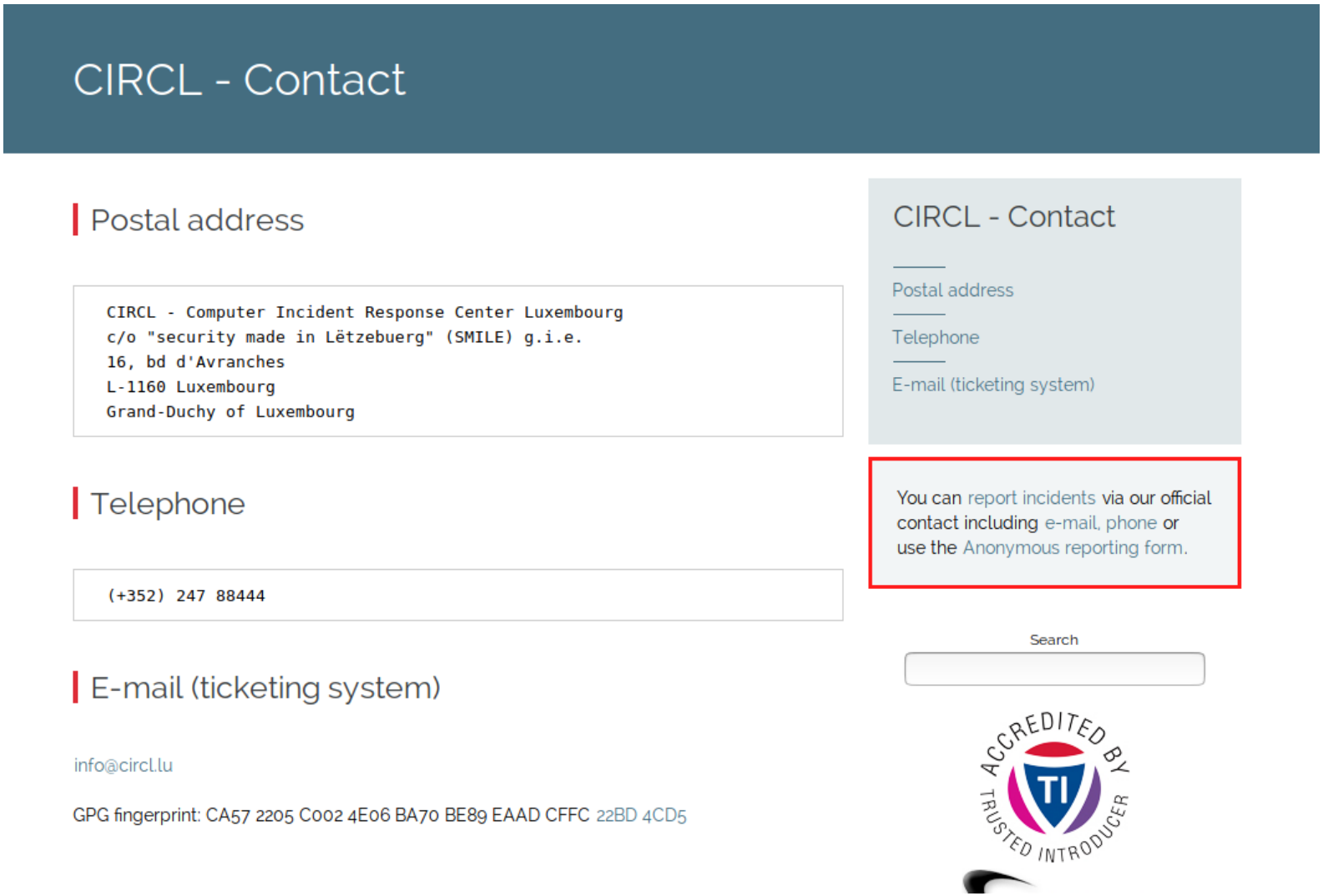
Usually the malicious emails involved in the scam start with sentences such as **I know that XYZ is your password**, with the scary part being that **XYZ** is in fact a real password of the targeted user.

In one example, as displayed below, the attacker explains that they compromised the victim's PC by infecting it with a remote access malware. They also state that they have activated the webcam of the PC and recorded a video clip of the victim.

The attackers claim that the victim is required to pay a ransom in Bitcoins in order to get the movie destroyed - refusing to do so would lead to the attackers spreading the movie to all of the contacts of the victim.

While these kind of sextortion scams are rather old, the quality of these recent occurrences has raised the bar massively, due to the fact that the attackers seem to posses and threaten with a real password of the victim.

Report an incident



CIRCL - Contact

Postal address

CIRCL - Computer Incident Response Center Luxembourg
c/o "security made in Lëtzebuerg" (SMILE) g.i.e.
16, bd d'Avranches
L-1160 Luxembourg
Grand-Duchy of Luxembourg

Telephone

(+352) 247 88444

E-mail (ticketing system)

info@circl.lu

GPG fingerprint: CA57 2205 C002 4E06 BA70 BE89 EAAD CFFC 22BD 4CD5

CIRCL - Contact

Postal address

Telephone

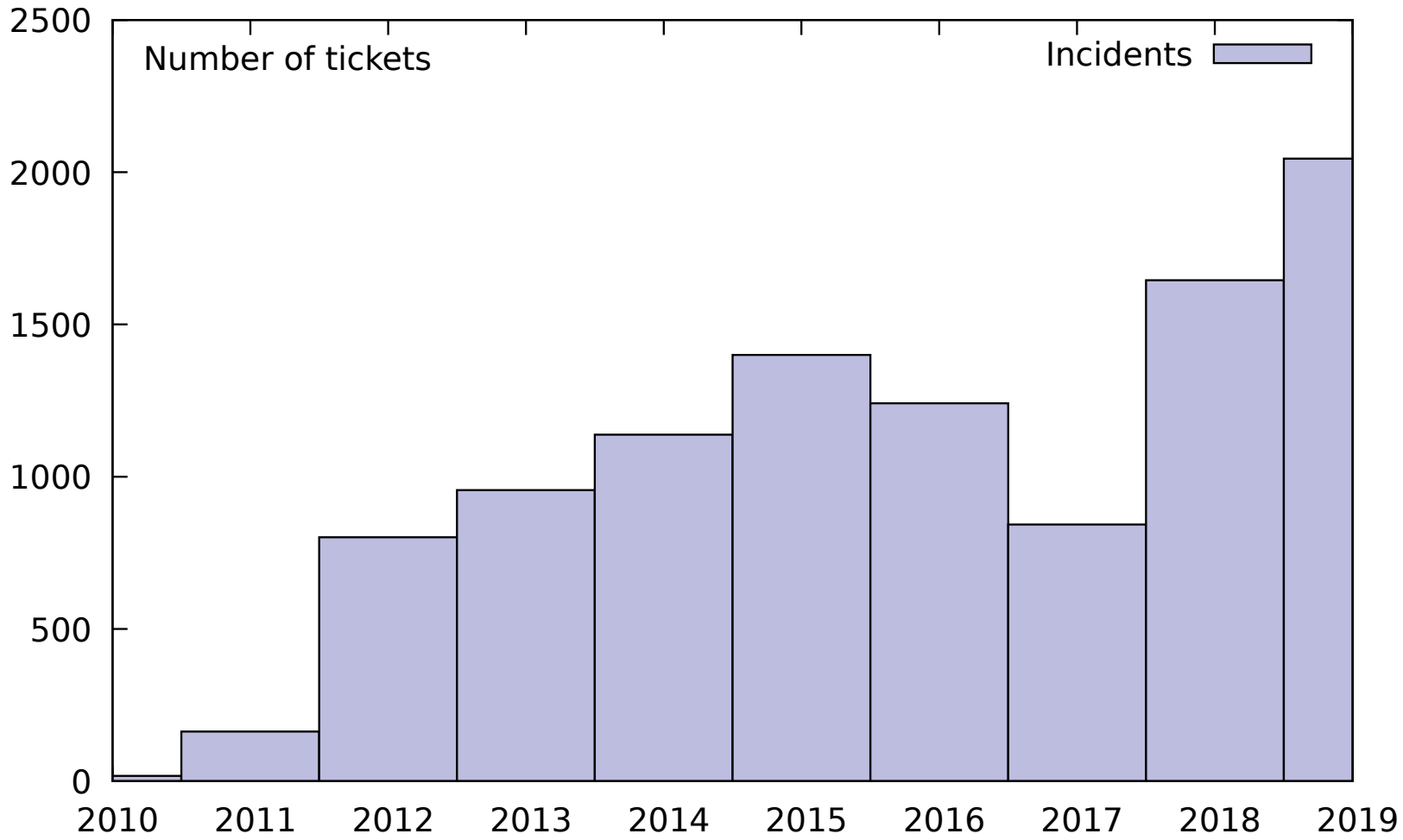
E-mail (ticketing system)

You can report incidents via our official contact including e-mail, phone or use the Anonymous reporting form.

Search

ACCREDITED BY TI TRUSTED INTRODUCER

Statistics: Incidents per year



Forensic Analysis

- Post-mortem Analysis
  - → `https://www.circl.lu/pub/tr-22/`
  - → `https://www.circl.lu/pub/tr-30/`
- Memory Forensics
  - → `https://www.circl.lu/pub/tr-22/`
  - → `https://www.circl.lu/pub/tr-30/`
- Network Forensics
- Reverse Engineering
- Code-Deobfuscation
- Mobile Forensics
- Cloud Forensics

Exercise: Data Exfiltration

- USB Key: Are there data hidden?
  - Windows Explorer
  - Show hidden files
  - CMD: `dir`
  - Open the file
  -
  - Other ideas?
- Answers:

  >
  >
  >
  >

- Creating xxx:

  >
  >
  >
  >

Exercise: Data Exfiltration

- USB Key: Are there data hidden?
  - Windows Explorer
  - Show hidden files
  - CMD: `dir`
  - Open the file
  -
  - Other ideas?
- Answers:

```
> dir /r          # Windows Vista +
>
> notepad H:\test.txt:123.txt
> mspaint H:\text.txt:123.png
```

- Creating ADS:

```
> File name syntax: <filename.ext>:<stream-name.ext>
>
> type F:\123.txt >> H:\test.txt:123.txt
> type F:\123.png >> H:\test.txt:123.jpg
```

Exercise: Hide data outside the partition

- Investigate disk layout

```
# fdisk -l /dev/sda
  Disk /dev/sda: 7,6 GiB, 8178892800 bytes, 15974400 sectors
  Units: sectors of 1 * 512 = 512 bytes

  Device     Boot Start    End Sectors  Size Id Type
  /dev/sda1        2048 526335  524288  256M  7 HPFS/NTFS/exFAT
```

- Hide a text message

```
#
-
```

- Hide a binary

```
#
-
```

- Access hidden data

```
#

#
```

Exercise: Hide data outside the partition

- Investigate disk layout

```
# fdisk -l /dev/sda
  Disk /dev/sda: 7,6 GiB, 8178892800 bytes, 15974400 sectors
  Units: sectors of 1 * 512 = 512 bytes

  Device     Boot Start    End Sectors  Size Id Type
  /dev/sda1        2048 526335  524288  256M  7 HPFS/NTFS/exFAT
```

- Hide a text message

```
# echo -n "MySecret_123456" | dd of=/dev/sda seek=100
  15 bytes copied, 0,00227001 s, 6,6 kB/s
```

- Hide a binary

```
# dd if=/bin/dd of=/dev/sda seek=101
  76000 bytes (76 kB, 74 KiB) copied, 0,0344384 s, 2,2 MB/s
```

- Access hidden data

```
#

#
```

Exercise: Hide data outside the partition

- Investigate disk layout

```
# fdisk -l /dev/sda
  Disk /dev/sda: 7,6 GiB, 8178892800 bytes, 15974400 sectors
  Units: sectors of 1 * 512 = 512 bytes

  Device     Boot Start    End Sectors  Size Id Type
  /dev/sda1        2048 526335  524288  256M  7 HPFS/NTFS/exFAT
```

- Hide a text message

```
# echo -n "MySecret_123456" | dd of=/dev/sda seek=100
  15 bytes copied, 0,00227001 s, 6,6 kB/s
```

- Hide a binary

```
# dd if=/bin/dd of=/dev/sda seek=101
  76000 bytes (76 kB, 74 KiB) copied, 0,0344384 s, 2,2 MB/s
```

- Access hidden data

```
# dd if=/dev/sda bs=512 skip=100 count=1 | xxd | less

# dd if=/dev/sda bs=1 skip=$((512*101)) count=76000 of=dd.exe
```

Demo: Modify data on RO mounted device

- Message in a forensic book

  "Nothing will prevent your Linux system to modify data on a read only mounted device"

- Leads to a new exercise for CIRCL DFIR 1.0.1 training
- I will
  - Targeted tamper of evidences
  - Only use Linux on-board-tools
  - Be `root`
  - Cheat (A little bit)
- I will not
  - Remount in RW mode
- Any ideas?

Demo: Modify data on RO mounted device

```
mount
mount -o ro,remount /dev/sda1 /media/michael/CIRCL_DFIR/
mount
```

Demo: Modify Document

```
strings -td /dev/sda1 | grep "World"
     .....
     82434 Hello World!
     .....

echo $((82434/512))
     161

dd if=/dev/sda1 bs=512 skip=161 count=1 of=161.raw
ll
hexer 161.raw

dd if=161.raw bs=512 seek=161 count=1 of=/dev/sda1
mount
```

Demo: Review Document