

# Challenges for law firms: IT security threats and incidents for law firms - practical examples



**CIRCL**  
Computer Incident  
Response Center  
Luxembourg

Gerard Wagener - *TLP:WHITE*

CIRCL

May 12, 2017



**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

# Direct financial attacks

---

## Definition

- Attacks on IT systems touching financial activities
- Internal systems
- External systems

## Example

- Online banking systems
- Interception of One Time Passwords (OTP)
- Accounting systems
- Human resource management software

# Direct financial attacks

## Recommendations<sup>1</sup>

---

- Prepare the worst case
  - Check contracts with payment providers
  - Check insurance clauses
  - File a complaint? → equipment might be imaged
  - How to handle financial losses → accounting
- **Use dedicated computers**
  - Hardened → switch of unnecessary services
  - Limit administrative rights
  - Block Internet browsing
- Remove smart cards from the readers

---

<sup>1</sup><https://circl.lu/pub/tr-38/>

# Blackmail

---

## Types

- Data availability → data encryption
- Data leaks
- Service availability → denial of service attacks

# Blackmail

## Example

Police. ATTENTION! Votre browser est bloqué pour des raisons de sécurité suivantes. Toutes les opérati... — □ ×

alertsecurity13000000173.com/07D980810A632DB609D8E185F4EF43CE

Diese Seite ist auf Französisch Soll sie übersetzt werden? Übersetzen Nein Optionen ×



Computer Incident Response Center Luxembourg  
Unité Spéciale de la Police (USP)

IP: 87.

Pays: Luxembourg  
ID: 74265WBUI104R

**ATTENTION!**  
**Votre browser est bloqué pour des raisons de sécurité suivantes.**  
**Toutes les opérations effectuées à partir de ce PC, sont enregistrées.**  
**Tous vos fichiers sont cryptés.**

Vous êtes accusé de visualisation/stockage et/ou de la distribution de matériel de caractère pornographique Interdit (Pornographie Juvenile/Bestialité/Viol, etc.) Vous avez violé la Déclaration universelle de la lutte contre la propagation de la pornographie Juvenile et accusé d'un crime conformément à l'article 161 du Code pénal de la Grand-Duché de Luxembourg.

L'article 161 du Code pénal de la Grand-Duché de Luxembourg prévoit pour cela une peine d'incarcération allant de 5 à 11 ans.

En outre Vous êtes soupçonné d'avoir violé le "Droit d'auteur et les droits adjacents"

Temps restant: 23:18:54

**paysafecard**

Code PIN Valeur

Tapez votre code 100

1 2 3 4 5 6 7 8 9 0 Clear

**A payer PaySafeCard**

Où puis-je acquérir un PaySafeCard?

Vous trouverez PaySafeCard près de chez vous, en Luxembourg p.e. chez un grand nombre de kiosques à journaux, de bureaux de tabac et de stations-services. Vous trouverez PaySafeCard dans de nombreux supermarchés et kiosques. Aperçu des revendeurs: Match, Total, Texaco, Spar, Shell, Selexion, Q8, PlanetVideo, Fnac, Deglohandel, Esso.

# Blackmail

## Recommendations

---

- Prepare the worst case
  - Interact with the attackers?
  - Pay ransom?
  - Do you have bitcoins or alternatives?
  - File a complaint?
  - **We do not recommend to pay**
  - → do not support business model of attackers
  - Check contracts with suppliers / customers focusing on outages
- Ransomware recommendations<sup>2</sup> → offline backups
- DDOS recommendations<sup>3</sup> → know the right contacts

---

<sup>2</sup><https://circl.lu/pub/tr-41/>

<sup>3</sup><https://www.circl.lu/pub/dfak/DDoSmitigation/>

# Hijack of IT infrastructures

---

- Use infrastructure as base to attack third parties
  - Distribute malware → infect other machines
  - Storage of stolen data from third parties
  - Use infrastructure as proxy to attack third parties
- Collateral effects of cloud solutions (shared infrastructures) due to badly behaving neighbors
  - Denial of Service attacks on physical infrastructure
  - Infrastructure blacklisted → access denial to services
  - Hardware seized by law enforcement



# Data exfiltration

## Attacks

---

- Social engineering via phone using spoofed phone numbers
- Spear phishing attack (e.g. receive email which infects computer)
- Watering hole attack (e.g. compromise first favorite web site of a target which attacks the target)
- Installation of remote access tools RATs
- Collect information and sent it to command and control server
- Stay over a long period of time
- Specialized groups for leading data exfiltration operations
- Opportunist attacks on poorly secured document indexing systems

# Data exfiltration

## Mitigation

---

### Frequently asked questions

- Which systems were compromised?
- Since when the systems started to exfiltrated data?
- Which **kind** of data has been exfiltrated?
- Who is the adversary?
- How was the data used by the adversary?

# Data exfiltration

## Recommendations

---

- Check IT supplier contracts if logs can be requested
- Do an unplanned request for logs to the IT provider
- Measure time
- Check accuracy of the log files: timestamps, correlation items
- Test correlations see if entire information flow paths can be reconstructed
- Prepare a legal argumentation for supporting logging necessary activities if needed
- **Share** information with other communities such that the attacks cannot be reproduced

# Conclusions

---

- Popular attack vectors
  - Direct financial attacks
  - Blackmail
  - Abuse of IT infrastructure
  - Data exfiltration
  - Abuse of document indexing systems
- Prepare organizational actions in advance
- Share information for instance via MISP
- Contact [info@circl.lu](mailto:info@circl.lu)