# 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[1]

- 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

[1] https://circl.lu/pub/tr-38/

# Blackmail

## Types

- Data availability $\rightarrow$ data encryption
- Data leaks
- Service availability $\rightarrow$ denial of service attacks

# Blackmail

## Example

# 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
  - $\rightarrow$ do not support business model of attackers
  - Check contracts with suppliers / customers focusing on outages
- Ransomware recommendations[2] $\rightarrow$ offline backups
- DDOS recommendations[3] $\rightarrow$ know the right contacts

[2] https://circl.lu/pub/tr-41/

[3] https://www.circl.lu/pub/dfak/DDoSMitigation/

# Hijack of IT infrastructures

- Use infrastructure as base to attack third parties
  - Distribute malware $\rightarrow$ 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 $\rightarrow$ 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 compromized?
- 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