An Overview of Security Incidents Targeting Citizen

How the Attackers Are Deceiving Us?

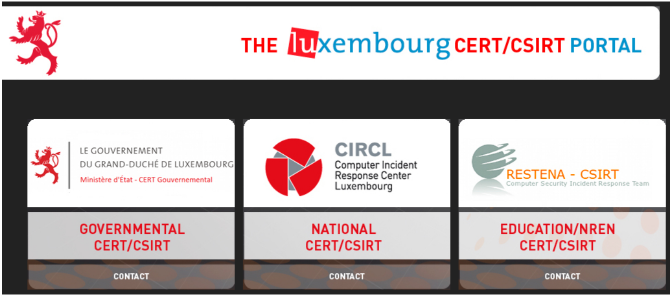
CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy - *TLP:WHITE*

`info@circl.lu`

25 March 2014

CIRCL



THE luxembourg CERT/CSIRT PORTAL

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État - CERT Gouvernemental

GOVERNMENTAL
CERT/CSIRT

CONTACT

CIRCL
Computer Incident
Response Center
Luxembourg

NATIONAL
CERT/CSIRT

CONTACT

RESTENA - CSIRT
Computer Security Incident Response Team

EDUCATION/NREN
CERT/CSIRT

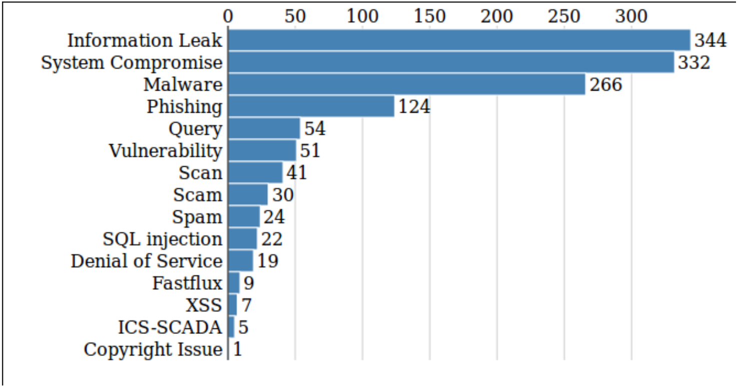
CONTACT

- The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to receive, review, report and respond to computer security threats and incidents.
- CIRCL is like "a fire brigade" which can react when computer security incidents occur.

CIRCL Statistics

- CIRCL started as a fully operational national CSIRT team in October 2010
  - In **2011**, we processed more than **4500** events for the past 12 months
  - More than 220 technical investigations and analysis were conducted in 2011
  - In **2013**, we processed **35958** events and conducted more than **1006** technical investigations
- The increase of attacks can be explained by the improved reporting process but also the growing attack surface:
  - More connected equipments and mobile devices
  - A significant increase of users and web applications

Type of Incidents in Luxembourg (2013)



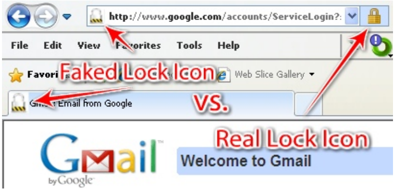
- Cybercriminals/attackers often search for direct financial gains using different techniques.
- The support from the victim is often required for the the criminal objectives...

The Attackers Principles

- Principle of shortest or fastest path of attack
- Principle of the cheapest path of attacks
- **Principle of the weakest link**
- **Principle of psychological acceptability**

Principles are based on the recurring patterns discovered in the various attacks.

Phishing or the art of making a website acceptable



http://www.google.com/accounts/ServiceLogin?:

Welcome to Gmail

image from bitofprevention.com

- Attackers rely on user interfaces complexity
- A common security recommendation : "look for the small lock"
- What's the correct lock? the one of the left? or the one on the right?
- The attacker is able to collect passwords...

Phishing or the art of making a website acceptable

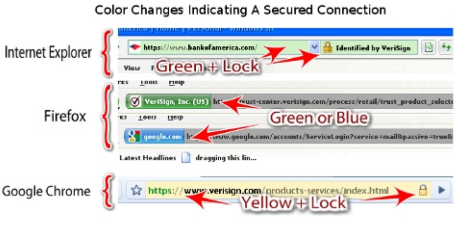
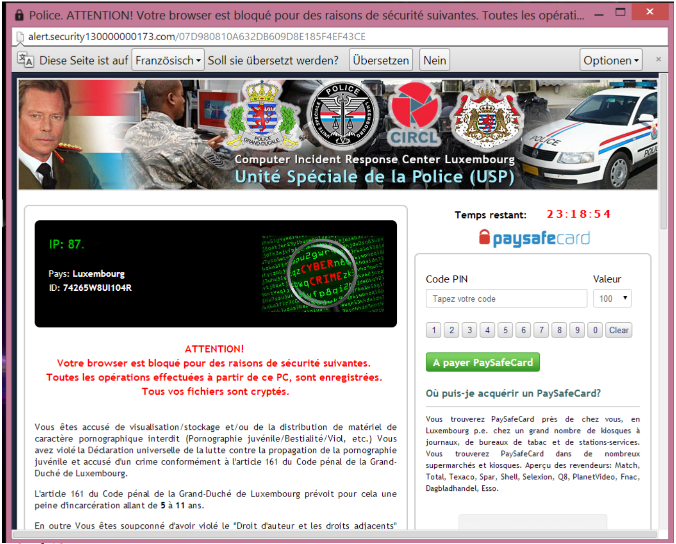

Color Changes Indicating A Secured Connection
Internet Explorer
https://www.bankofamerica.com/
Identified by VeriSign
Green + Lock
Firefox
VeriSign, Inc. (US)
trust-center.verisign.com/process/retail/trust_product_selecte
Green or Blue
google.com
www.google.com/accounts/ServiceLogin?service=mail&passive=true&
Latest Headlines
dragging this lin...
Google Chrome
https://www.verisign.com/products-services/index.html
Yellow + Lock

Figure 1

image from bitofprevention.com

- Internet browsers try to improve the situation for SSL website
- Is it really an improvement? or even more confusion?
- If confusion is still there, the attacker is still able to collect passwords...

Ransomware - Using Fear



Police. ATTENTION! Votre browser est bloqué pour des raisons de sécurité suivantes. Toutes les opérati...
alert.security130000000173.com/07D980810A632DB609D8E185F4EF43CE
Diese Seite ist auf
Französisch
Soll sie übersetzt werden?
Übersetzen
Nein
Optionen
POLICE GRAND-DUCALE
POLICE
UNITÉ SPÉCIALE
LUXEMBOURG
CIRCL
POLICE
CYBERCRIME

Computer Incident Response Center Luxembourg

Unité Spéciale de la Police (USP)

IP: 87.[redacted]

Pays: **Luxembourg**

ID: **74265W8UI104R**

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 juvénile/Bestialité/Viol, etc.) Vous avez violé la Déclaration universelle de la lutte contre la propagation de la pornographie juvénile 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 soupconné d'avoir violé le "Droit d'auteur et les droits adjacents"

Temps restant: 23:18:54

Code PIN: Tapez votre code

Valeur: 100

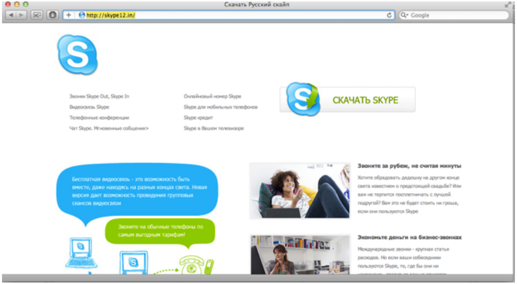
Où puis-je acquérir un PaySafeCard?

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, Dagbladhandel, Esso.

Ransomware - Using Fear

- The potential victim searches for dubious content.
- The attackers manage compromised server with such content or keywords.
- The attackers compromised the victim accessing the server.
- As the victim is in doubt and fear prosecution, the victim pays the attacker.
- This is a kind of vicious circle for the benefit of the attacker.

Do you download the right software?



Бесплатная видеосвязь - это возможность быть вместе, даже находясь на разных концах света. Новая версия дает возможность проведения групповых сеансов видеосвязи

Звоните на обычные телефоны по самым выгодным тарифам!

Звоните за рубеж, не считая минуты

Хотите обрадовать дядюшку на другом конце света известием о предстоящей свадьбе? Или вам не терпится посплетничать с лучшей подругой? Вам это не будет стоить ни гроша, если они пользуются Skype

Экономьте деньги на бизнес-звонках

Международные звонки - крупная статья расходов. Но если ваши собеседники пользуются Skype, то, где бы они ни

- A subtile trick, the real Skype URL shown (when you move your mouse over) is different than the fake Skype URL when you click on it.
- Then the victim clicks and download the malicious Skype software.

What should I do to limit the risks of such attack?

- Keep your software up to date including browsers and add-ons (e.g. Java, flash, quicktime...)
- Dedicate a browser for your sensitive activities (e.g. web banking or alike)
- Disable unused plugins and use NoScript or similar trusted add-ons in your browser
- Use a bootable CD/USB like tails[1] to access suspicious sources
- Keep an eye on your laptop (e.g. use unique stickers to cover screws) and don't leave it unattended
- Think twice before doing an action on Internet (e.g. open suspicious URLs, inserting USB keys, open document from unknown sources)

[1] https://tails.boum.org/

Contact

- Don't hesitate to contact us or report incidents via
- `https://www.circl.lu/`
- info@circl.lu