# Malware repositories

## A need for CERTs, from VX heavens to malware.lu

CIRCL
Computer Incident
Response Center
Luxembourg

Team CIRCL - *TLP:GREEN*
Steve Clement - 0x9BE4 AEE9

September 28, 2012

# What are malware repositories?

- Nasty places for amazing things
- From hash to binary samples, they've got it
- The work you are doing, already done

# Why CERTs need malware repositories?

- Forensic analysis (finding malicious files in a sea of files)
- Reversing malware and finding similar samples
- Building analysis tools from a malware dataset
- Overcoming the malware naming mess
- Validating IoC[1] against a malware dataset
- Security research (e.g. finding similar shared functions among malware, obfuscation techniques, . . . )

[1] Indicators of Compromise

# Malware repositories - a new trend?

- `http://vx.netlux.org` - VX heavens (founded in 1999 and went off-line in 2012) - Error 451: Unavailable for legal reasons
- `http://virusshare.com` - @VXShare
- `http://malwr.com` - @malwr
- `http://fordrop.org` - @fordrop —— @jberggren
- maldb[2] (CSRRT-LU) - research project in 2006
- other private initiative like VirusTotal (now Google. . . ) or some trusted communities
- `http://malware.lu` - @malwarelu

[2] `http://www.foo.be/malwaredb/malwaredb_handout.pdf`

# What about malware.lu?

- Creator: Paul Rascagnères
- Maintainer: Paul Rascagnères & Hugo Caron
- Number of samples: 3,103,389
- Number of users: 1038
- Number of articles: 30
- (.lu) 2nd country in August to submit samples to virustotal.com

# malware.lu Access and API

- Access is restricted to registered/accepted users (register@malware.lu)
- Users can lookup a specific hash, download a malware or upload a new sample
- API is accessible via Web access or HTTP REST API[3]

[3] `http://www.malware.lu/user/api.html`

# Future/potential improvements to malware repositories

- Similar API across the malware lookup services (from Cymru hash lookup to VT API)?
- Common malware repository/lookup for the CERT community?
  - A reverser might ask for a specific hash (but only within the CERT community)
  - Another CERT got the sample and can share it with the requestor
- Ensuring a preservation of the malware repositories
- Need: courage

# plug - Hack.lu - HAL/23-25 October 2012 / Luxembourg


http://2012.hack.lu/index.php/List (@Hack_lu)

(Beer workshop say what?!)

# Acknowledgments and Contact Info


- Team CIRCL - via ticketing - info@circl.lu

GPG fingerprint: CA57 2205 C002 4E06 BA70 BE89 EAAD CFFC
ID: 0x22BD4CD5

- Alexandre Dulaunoy - alexandre.dulaunoy@circl.lu

GPG fingerprint: 3B12 DCC2 82FA 2931 2F5B 709A 09E2 CD49
ID: 0x44E6CBCD

- Steve Clement - steve.clement@circl.lu

GPG fingerprint: 3F4D 8CF6 08F9 4F88 2815 2CB1 69A2 0F50
ID: 0x9BE4AEE9