

Cyber Security Research in Luxembourg and abroad or Improving Data Sharing to Increase Security Research Opportunities



CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy -
TLP:WHITE

NCSRA Symposium 2015



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.
- Our core objective is to support the building of a secure economy.

Cyber security needs data for analysis

- In the scope of the EU-PI project, CIRCL developed a modular software¹, web service and API to review the security of URLs.
- Depending of the URL to review, it can be difficult to estimate a level of trust.
- URL Abuse includes a series of modules in order to review an URL.
- Then the various indicators can be used by the users (or an analyst) to determine the degree of trust.

¹<https://github.com/CIRCL/url-abuse>

URL Abuse user-interface overview

http://saysuevent.com/wp-admin/css/Sichern/Sie/Ihre/Online-Banking-Konto/sparkasse.de

7 of the 63 scanners know this URL as malicious. [More details.](#)

Known phishing website on Google Safe Browsing. [More details.](#)

Contact points from Whois: phishing@godaddy.com,malware@godaddy.com,tanitimom@tanitimom.com.tr,abuse@godaddy.com

184.168.236.1

Information from BGP Ranking:

- PTR Resource Record: p3nlhg136c1136.shr.prod.phx3.secureserver.net
- Announced by: AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC,US ([26496](#))
- This ASN is at position 555 in the list of 15758 known ASNs (0.0018228837996073497).

The total alert count on URLquery is 1.

Has 168 unique entries in CIRCL Passive DNS. 5 most recent one(s):

- saysuevent.com
- etotheipplusone.net
- bitcoinz.cc
- scorneddely.com
- digimind.com

Contact points from Whois: phishing@godaddy.com,malware@godaddy.com,abuse@godaddy.com,noc@godaddy.com

Unable to resolve in IPv6

Standing on the shoulders of existing data

- Degree of maliciousness of an Internet Service Provider using BGP Ranking².
- Historical view of DNS records from Passive DNS³.
- Historical perspective of SSL certificate usage and trust (Passive SSL).
- Distance analysis of the submitted URLs with legitimate URLs.

²<http://bgpranking.circl.lu>

³<https://www.circl.lu/services/passive-dns/>

BGP Ranking - The benefit of sharing for innovation

- Project started in 2011 as a scientific experiment to rank the maliciousness of Internet Service and Hosting Provider.
- BGP Ranking project is fully open source including **a 4-years dataset of cyber security metrics** per ISP (BGP ASN).
- The project is an operational services used by various incident responders or Internet security services (e.g. URL Abuse in EU-PI).
- A recent paper from Georgia Tech, *ASwatch: An AS Reputation System to Expose Bulletproof Hosting ASes published at SIGCOMM '15*.
 - *Researchers created a new model and used **CIRCL BGP Ranking to compare their improved model**.*
 - *ASwatch research provides **concrete improvements** that will be used in CIRCL BGP Ranking.*

Contributions of users against cybercrime

- Attackers tend to localize more their attacks and focus on specific groups of potential targets.
- Having **localized information from potential victims** helps to analyse current threats, incidents and attackers behavior.
- Localized dataset (e.g. Passive DNS) helps to detect potential abused or "phished" services.
 - What are the most used web banking services in a country?
 - Can you build a golden list of URLs?
- EU-PI regionalized the submission of potential phishing links. The localized information can support additional researches.

Conclusion

- Having **open data sharing** models helps researchers and private organizations to experiment.
- Providing **open source** software increases peer review and especially **reproducibility** of past experiments.
- Peta-scale datasets and privacy challenges is still an opportunity for improved **data-structure research**.
- Localized and expanded cyber security datasets sharing opportunities are still huge.

Contact

- info@circl.lu
- <https://www.circl.lu/>
- Security researchers? MSc and PhD opportunities -
<https://www.circl.lu/projects/internships/>
- OpenPGP fingerprint: CA57 2205 C002 4E06 BA70 BE89 EAAD
CFFC 22BD 4CD5